Comprendre l'informatique quantique

troisième édition

septembre 2020

Olivier Ezratty

À propos de l'auteur

Olivier Ezratty — olivier (at) oezratty.net , www.oezratty.net , @olivez

consultant et auteur — +33 6 67 37 92 41

Olivier Ezratty forme et conseille les entreprises dans l'élaboration de leurs stratégies d'innovation autour des *deep techs* et en particulier, de l'intelligence artificielle et des technologies quantiques. Il leur apporte une vision à 360° : scientifique, technologique, marketing ainsi que la connaissance des écosystèmes dans les industries numériques.

Il a réalisé depuis 2005 des missions diverses d'accompagnement stratégique et de conférences ou formations dans différents secteurs tels que le secteur **médias/télécoms** (Orange, Bouygues Télécom, TDF, Médiamétrie, BVA), la **finance et l'assurance** (groupe BPCE, Caisse des Dépôts, Crédit Agricole, Crédit Mutuel-CIC, Generali, MAIF, Société Générale), dans l'**industrie et les services** (Schneider, Camfil, Vinci, NTN-STR, Econocom, ADP, Air France, Airbus) et le **secteur public** (Ministère des Armées, CEA, Météo France, Bpifrance, Business France). Ces missions couvrent des conférences, séminaires et formations ainsi que l'assistance à la définition de stratégies produits, d'innovation ouverte et de promotion d'écosystèmes.

Ses contributions s'appuient sur un fort investissement dans l'écosystème de l'innovation et sous différentes casquettes, notamment dans l'univers entrepreneurial :

- Formateur sur l'intelligence artificielle et l'informatique quantique auprès de **Cap Gemini Institut**.
- Membre depuis fin 2015 du Conseil Scientifique de l'**ARCEP**.
- Expert référent à l'**IHEDN** dans la promotion 2019/2020.
- Expert auprès de **Wilco** – ex Scientipôle Initiative – depuis 2007, dans l'accélérateur santé depuis 2016.
- Membre du jury de divers **concours entrepreneuriaux** comme le Grand Prix de l'Innovation de la Ville de Paris ou le Concours National i-Lab et le Concours i-Nov.

Il intervient comme conférencier dans divers établissements d'enseignement supérieur tels que CentraleSupelec, l'Ecole des Mines de Paris, Télécom Paristech, l'EPITA, Les Gobelins, HEC, Neoma Rouen et SciencePo, sur l'intelligence artificielle, les technologies quantiques ainsi que sur sur l'entrepreunariat et le product management, en français comme en anglais selon les besoins.

Olivier Ezratty est l'auteur du **Rapport du CES de Las Vegas**, publié à la fin janvier de chaque année entre 2006 et 2020, et du **Guide des Startups** qui est devenu une référence en France avec plus de 400 000 téléchargements à date, mis à jour tous les ans (23e édition et 13e année en 2019), l'ebook **Les usages de l'intelligence artificielle** en octobre 2017, novembre 2018 et novembre 2019 et **Comprendre l'Informatique Quantique** en septembre 2018, 2019 et 2020. Le tout étant publié sur le blog « Opinions Libres » (http://www.oezratty.net) qui traite de l'innovation technologique vue sous les angles scientifiques, technologiques, entrepreneuriaux et des politiques publiques de l'innovation. Comme photographe amateur, il est aussi le co-initiateur en 2012 de « Quelques Femmes du Numérique ! » devenu une association en 2016, et qui vise à augmenter la place des femmes dans les métiers du numérique, en sensibilisant les jeunes à ces métiers.

Et avant tout cela, Olivier Ezratty débute en 1985 chez **Sogitec**, une filiale du groupe Dassault, où il est successivement Ingénieur Logiciel, puis Responsable du Service Études dans la Division Communication. Il initialise des développements sous Windows 1.0 dans le domaine de l'informatique éditoriale ainsi que sur SGML, l'ancêtre de HTML et XML.

Entrant chez **Microsoft France** en 1990, il y acquiert une expérience dans de nombreux domaines du mix marketing : produits, canaux, marchés et communication. Il lance la première version de Visual Basic en 1991 ainsi que Windows NT en 1993. En 1998, il devient Directeur Marketing et Communication de Microsoft France et en 2001, de la Division Développeurs dont il assure la création en France pour y lancer notamment la plate-forme .NET et promouvoir la plate-forme de l'éditeur auprès des développeurs, dans l'enseignement supérieur et la recherche ainsi qu'auprès des startups.

Olivier Ezratty est ingénieur **Centrale Paris** (1985), devenu CentraleSupelec en 2015.

Ce document vous est fourni à titre gracieux et est sous licence « Creative Commons »
dans la variante « Paternité-Pas d'Utilisation Commerciale-Pas de Modification 2.0 France »

Voir http://creativecommons.org/licenses/by-nc-nd/2.0/fr

ISSN 2680-0527

Illustration de couverture : création personnelle associant une sphère de Bloch décrivant un qubit et le symbole de la paix au-dessus d'une liste presque exhaustive des noms de scientifiques et entrepreneurs qui sont cités dans l'ebook, présentés sous forme d'un opérateur quantique de très grande dimension illustrant la richesse scientifique et humaine du domaine et la transmission !

Table des matières

Pourquoi

Cet ebook est la troisième édition d'un ouvrage compilant à l'origine une série de 18 articles que j'avais publiés entre juin et septembre 2018. Avait suivi une seconde édition très enrichie en septembre 2019 qui atteignait la bagatelle de 504 pages. Cette troisième édition encore très enrichie est dans la même lignée. Elle apporte son lot de nouveautés à 360° dans de nombreuses dimensions sur le vaste sujet des technologies quantiques : historiques, scientifiques, technologiques, entrepreneuriales, géopolitiques, philosophiques et sociétales. Le tout en essayant à chaque fois d'améliorer la pédagogie de ce sujet complexe. Elle a de plus bénéficié de la « grande pause » du covid-19 !

Mes premiers écrits sur l'informatique quantique remontent aux Rapports du CES 2015, 2016, 2017 et 2018. Ce domaine m'intriguait car il semblait très prometteur mais en même temps assez difficile d'accès, avec des concepts assez mal vulgarisés. J'admettais n'y rien comprendre et mettais sérieusement en doute la compréhension du sujet par les médias relayant diverses annonces sur le sujet. Cet ebook visait à combler ces lacunes de compréhension.

Quelques années plus tard, les technologies quantiques sont rentrées dans le langage courant, même si elles restent encore largement incomprises par le grand public, si ce n'est par une bonne part des spécialistes du monde des technologies. Si les arcanes de la physique et du calcul quantiques sont difficiles d'accès, on comprend toutefois mieux les solutions qui pourront être concoctées avec.

Les annonces plus ou moins fracassantes des grands acteurs des technologies que sont Google, IBM et Honeywell ne sont pas évidentes à décoder mais elles plantent le décor. Elles ont élevé les technologies quantiques au rang de secteurs stratégiques pour les états développés. Tous les gouvernements s'en sont emparés d'une manière ou d'une autre, les jugeant clés pour occuper une place dans le futur, si ce n'est acquérir ou préserver leur souveraineté technologique. Comme la plupart des nouvelles technologies, celles qui sont issues du quantique sont « duales », à savoir qu'elles ont des usages civils et militaires. La France a eu du retard à l'allumage dans cette prise de conscience et s'est rattrapée en 2020 avec le lancement d'un plan national quantique à la hauteur des enjeux.

S'il n'a pas encore atteint le volume et la quantité d'autres secteurs comme celui de l'intelligence artificielle, l'écosystème des startups et PMEs des technologies quantiques continue de se développer dans le monde entier. J'inventorie dans cet ebook plus de 260 startups et PMEs dans le monde dont presque 10% en France, ce qui est fort honorable. On est ici dans le royaume des « deep techs » si ce n'est des « hard techs » avec des startups qui sont encore au stade de la recherche appliquée, et parfois encore fondamentale. L'intérêt de ce secteur technologique est qu'il est encore très incertain. Cela ouvre des portes intéressantes aux scientifiques et innovateurs créatifs tandis que dans d'autres marchés, les jeux sont presque faits et les positions plus difficiles à bouger[1].

On peut évaluer le degré de développement d'un secteur technologique au niveau de bullshit qui l'entoure. Il existe au niveau de certains scientifiques qui peuvent exagérer les performances de leurs travaux[2]. On voit ainsi fleurir des entreprises qui intègrent le quantique dans leur positionnement. Soit de manière totalement artificielle, soit en s'appuyant sur des principes quantiques du 20e siècle. Comme les transistors et les lasers s'appuient sur la physique quantique (effet tunnel, effet photoélectrique, etc), toutes les technologies numériques d'aujourd'hui peuvent revendiquer d'être quantiques ! Il faut donc apprendre à distinguer l'ancien (première révolution quantique) du nouveau (seconde révolution quantique).

---

[1] Voir Les technologies quantiques ou la nouvelle ruée vers l'or par Geneviève Fournier, novembre 2019.

[2] Voir la création du compte Twitter « Quantum Bullshit Detector » au printemps 2019, qui sert à identifier de manière binaire ce qui relève du bullshit ou pas. Dans Revolt! Scientists Say They're Sick of Quantum Computing's Hype par Sophia Chen, décembre 2019. Les auteurs seraient peut-être des étudiants d'UCLA.

Mais le véritable bullshit est ailleurs, avec ces dérivations abusives du quantique dans les fausses médecines quantiques et autres gouroutisations en tout genre. Je les dénonce dans cet ebook dans une longue rubrique dédiée aux fumisteries quantiques.

Cet ouvrage a aussi une autre saveur, différente des précédents que j'ai pu rédiger dans le domaine des deep techs. Il est le résultat d'une aventure humaine inédite au cœur de l'écosystème quantique français. Elle a véritablement démarré en 2016. J'avais alors décidé de sélectionner le thème de l'informatique quantique pour ma conférence traditionnelle sur les deep techs du **Web2day** de Nantes… pour l'édition 2018. Histoire de ne pas me lancer seul dans l'aventure et aussi de respecter une parité de genre à laquelle je suis attaché, j'ai proposé en juin 2017 à **Fanny Bouton** de rejoindre le projet, ce qu'elle a accepté immédiatement. Elle apportait et apporte toujours un regard différent et complémentaire du mien, plus lié aux inspirations de la science-fiction et aux usages.

Cela a abouti à la conférence **Le quantique, c'est fantastique** du 14 juin 2018 (vidéo)[3] et à de nombreuses interventions qui ont suivi, en solo ou à deux dans les entreprises et dans le secteur public (ARCEP, IHEDN, Ministère des Armées, Commission Européenne, etc). Nous avons aussi visé un public féminin, pour contribuer le plus en amont possible à une féminisation du secteur[4].

Pour préparer tout cela, nous avons eu l'occasion de rencontrer des chercheurs et chercheuses de haut vol en France et même de l'étranger : **Alain Aspect**, le vénérable vérificateur de l'intrication quantique en 1982, **Philippe Grangier**, co-auteur de l'expérience d'Alain Aspect et l'un des fondateurs de la cryptographie quantique, **Philippe Duluc** et **Cyril Allouche** d'Atos, **Daniel Estève**, grand spécialiste des qubits supraconducteurs au CEA à Saclay, **Patrice Bertet** qui travaille dans son laboratoire, **Maud Vinet** du CEA-Leti à Grenoble, qui y pilote le projet des qubits silicium, **Eleni Diamanti** du CNRS LIP6, spécialiste des communication quantiques et coordinatrice avec Iordanis Kerenidis du hub quantique de Paris, **Pascale Senellart** du CNRS C2N, spécialiste de la génération de qubits photons, cofondatrice de la startup Quandela et coordinatrice du hub Quantum de Paris-Saclay, **Elham Kashefi** du CNRS LIP6, spécialiste des télécommunications quantiques et cofondatrice de Veriqloud, **Alexia Auffèves** du CNRS Institut Néel, spécialiste de la thermodynamique quantique et coordinatrice du hub quantique QuEng de Grenoble, **Tristan Meunier** du CNRS Institut Néel, **Iordanis Kerenidis** du CNRS, spécialiste du quantum machine learning, les équipes de métrologie quantique de **Thales TRT** et plein d'autres encore.

Nous avons aussi fait le tour de presque toutes les **startups** du secteur en France et même rencontré quelques-unes d'ailleurs (Canada, USA, UK). Nous avons aussi rencontré à différents niveaux la sphère politique et publique pour la sensibiliser au sujet (cabinets ministériels, Mounir Mahjoubi, Cédric O, Bpifrance, la DGE, et même, furtivement, Emmanuel Macron). Nous étions convaincus qu'il fallait que l'Etat s'empare du sujet. Le gouvernement britannique l'avait fait dès 2013. Il était temps que l'on se bouge ! Ce fut fait avec la création en avril 2019 de la mission parlementaire pilotée par la députée Paula Forteza, la présentation de son rapport en janvier 2020, puis la concoction de la feuille de route de l'Etat entre février et juin 2020. En grande partie, en pleine crise du covid.

Bref, pendant ces années, nous avons été « embedded » dans l'écosystème scientifique et entrepreneurial. Nous avons appliqué l'un des principes d'Heisenberg, à savoir que l'outil de mesure influe sur la grandeur à mesurer. C'était et cela reste une belle aventure humaine avec de vrais gens, des passions, des convictions, des hauts et des bas, et au bout du compte, un beau résultat avec une recherche et un entrepreneuriat français des technologies quantiques qui sont dynamisés et mieux positionnés qu'il y a quelques années. Et l'aventure ne fait que démarrer !

---

[3] Le journal La Tribune publiait le même jour un dossier de quatre pages de mon cru sur l'informatique quantique. Voir Le quantique, la prochaine révolution de l'informatique ?, Olivier Ezratty, juillet 2018.

[4] Avec une formation d'une journée chez Roland Berger et avec Axelle Lemaire en avril 2019, auprès de lycéennes chez Magic Makers en septembre 2019, de jeunes et de parents dans l'événement Startup4Teens en février 2020, un débat début mars 2020 avec Alexia Auffèves, Elham Kashefi et Pascale Senellart animé par Fanny Bouton et organisé chez Talan, un autre auprès d'un public féminin de tous âges dans l'événement Tech4All organisé par l'école 42 et Digital Ladies en mars 2020, à chaque fois en partenariat avec l'association *Quelques Femmes du Numérique*

Un sujet complexe mais vulgarisable

Après avoir balayé de nombreux pans de la science et des deep techs, je peux résolument positionner l'informatique quantique, et la physique quantique qui la sous-tend, au top du top de l'échelle de la complexité. La physique quantique est difficile d'abord car elle s'appuie sur des éléments contre-intuitifs (la dualité ondes-particules, l'intrication à distance) et sur un formalisme mathématique pas évident même après être passé par les classes préparatoires et une école d'ingénieurs généraliste comme j'ai pu le faire… il y a quelques décennies.

Vous pourriez ainsi bien tourner en rond longtemps pour piger cette perle, la définition de l'intrication d'une particule[5] ! Tout ça pour dire que deux particules intriquées ont des états quantiques corrélés au lieu d'en avoir chacune un, individuel, indépendant et différent !

"deux particules sont dites dans un état intriqué lorsque l'état des deux particules n'est pas factorisable en un produit tensoriel de deux états à une particule."

source : Wikipedia, "Inégalités de Bell"

Nous décoderons et expliquerons donc cette notion de produit tensoriel et de factorisation !

Cela traduit la difficulté à traduire ce champ scientifique en langage naturel ainsi que le lien ténu entre la mécanique quantique et de nombreux concepts mathématiques qui peuvent facilement nous échapper.

Comme l'indiquait **Richard Feynman**, lorsque l'on étudie la mécanique quantique, si l'on croit que l'on a tout compris, c'est que l'on n'a pas tout compris et que l'on se raconte des histoires. **Alain Aspect** le confirme, exprimant toujours des doutes sur sa compréhension de l'intrication quantique dont il a pourtant prouvé l'existence avec des photons dans la fameuse expérience de 1982 qui porte son nom. La mécanique quantique est le règne physique et métaphorique du "peut-être", "ou pas" et du "en même temps"[6], d'une approche probabiliste du monde qui présente de ce point de vue quelques vagues points communs avec l'approche connexionniste de l'intelligence artificielle[7].

Il faut l'admettre avec humilité, la pédagogie de l'informatique quantique est un art nouveau et difficile. La méthode "*au ralenti*", avec de l'écrit complète bien les conférences qui vont toujours trop vite pour nos cerveaux embrumés par un trop grand nombre de nouveaux concepts.

Cet ouvrage reste du domaine de la vulgarisation et n'a pas la prétention de la parfaite exactitude scientifique, même si de nombreuses parties ont été relues et corrigées par quelques chercheurs spécialistes du domaine. Il se positionne de manière intermédiaire : plus technique que la moyenne de la couverture média de l'informatique quantique, ainsi que des rapports de cabinets d'analystes et de conseil, mais bien moins que la littérature scientifique qui est généralement largement inaccessible pour les non-spécialistes. Pour faciliter la compréhension de ces nouveaux concepts, j'ai créé ou recréé de nombreux schémas explicatifs. Je me pose souvent des questions pratico-pratiques.

L'ingénierie y a aussi la part belle. C'est le paradis de l'ingénieur généraliste et des geeks curieux ! En plus de la mécanique quantique, on y trouve donc de l'informatique, de la thermodynamique, de la cryogénie, des matériaux nouveaux, des semiconducteurs, des supraconducteurs, des radiofréquences, de la photonique, des mathématiques, du développement logiciel, des questions économiques, géopolitiques, de la sociologie et même de la philosophie. C'est une véritable boîte de Pandore et c'est passionnant !

---

[5] Elle est extraite de la page Wikipedia sur les inégalités de Bell.

[6] Qui fait évidemment penser à l'expression macronienne « *en même temps* ». Et l'on commence à parler de « politique quantique », qui n'est que métaphorique, bien entendu. Elle est élaborée par le Président Arménien Armen Sarkissian cité dans Quantum politics and a world turned upside down, et dans le Financial Times dans Quantum politics and a world turned upside down, septembre 2018. Mais à vrai dire, ce qui est ici quantique relèverait plutôt de la théorie du chaos. Le quantique a sa part de chaos, certainement, mais pas que cela.

[7] Je décris cette approche dans Les usages de l'intelligence artificielle, novembre 2019 (624 pages).

Nouvelle vague pour le numérique

Pourquoi l'informatique quantique devient-elle est un sujet important ? D'abord, parce qu'elle commence à faire parler d'elle, au travers de la communication de grands acteurs du numérique comme IBM, Google, Intel ou Microsoft, avec des annonces impressionnantes qu'il faut cependant prendre avec des pincettes, avec beaucoup de recul et décoder posément.

Mais surtout, parce qu'elle pourrait impacter sérieusement de nombreux champs scientifiques puis certains usages du numérique. Elle permettra théoriquement de résoudre des problèmes appartenant à des classes de complexité que les ordinateurs traditionnels, même les plus grands supercalculateurs géants, ne pourront a priori jamais traiter.

L'autre raison de cet intérêt soudain pour l'informatique quantique est que nous sommes encore aux débuts d'une longue histoire qui va voir la science et l'industrie se sédimenter, avec la création de nouveaux leaders, et le développement d'un écosystème d'acteurs. Le tout, dans un domaine où subsiste une énorme incertitude scientifique et technologique. Il est très difficile d'évaluer la faisabilité de la création d'ordinateurs quantiques opérationnels à grande échelle. Les chercheurs que nous avons rencontrés ont parfois calmé nos ardeurs. Pour certains, il faudra patienter encore quelques décennies avant d'en voir la couleur ! D'autres sont plus optimistes. L'ennemi : le bruit ! Ce bruit qui génère des erreurs dans l'évolution des qubits pendant les calculs quantiques et qui est à la fois difficile à éviter et à corriger.

C'est une étude de cas vivante des plus intéressantes. Les phases d'incertitudes sont les périodes pendant lesquelles certaines formes de leadership se construisent. La France va une fois encore se poser la question de son leadership supposé ou mérité sur le sujet. Sur un sujet encore jeune, sommes-nous prêts à relever le défi ? A investir ? Où faut-il le faire ? Que faudrait-il faire pour y arriver ? Ce sont des questions lancinantes qui ont eu leur lot de réponses sur l'intelligence artificielle, avec plus ou moins de bonheur comme nous avons pu le constater avec le Rapport de la Mission Villani publié en mars 2018 et le plan qui a suivi[8]. En prenant un nouveau sujet plus en amont, peut-être aurons-nous plus de chances de mieux nous en sortir. C'est en amont des grandes vagues que les positions se prennent. C'était l'intérêt de la mission parlementaire pilotée par la députée Paula Forteza entre avril 2019 et janvier 2020, puis du plan qu'a consolidé l'Etat pour faire en sorte que la France ne rate pas cette révolution et y prenne sa place en tant que producteur de technologies et pas simplement de consommateur comme c'est le cas dans plein d'autres domaines du numérique.

Sommaire et résumé

Cet ebook est un gros pavé. Cela ne vous surprendra pas. J'essaye d'y couvrir tous les recoins du sujet à 360°. Son cœur en est le calcul quantique mais j'y traite des autres technologies quantiques comme la cryptographie quantique et post-quantique, les télécommunications quantiques ainsi que la métrologie quantique. J'y évoque même, en aparté, la chimie quantique relativiste et le domaine des lasers !

Voici les grandes parties de l'ebook et leur résumé associé, qui constitue une sorte d'*executive summary*. Il constitue d'ailleurs la trame modulable de conférences, formations et séminaires sur le sujet des technologies quantiques que je peux réaliser.

Dans cette troisième édition, chacune des parties a été revue, mise à jour, améliorée et complétée. L'historique à la fin de l'ebook contient la liste des principales modifications. Il en est une, transversale, qui intéressera particulièrement les ingénieurs généralistes et ceux qui veulent comprendre comment les ordinateurs quantiques sont faits d'un point de vue pratique.

[8] J'avais décortiqué le rapport Villani dans Ce que révèle le Rapport Villani en mars 2018.

J'ai ainsi décortiqué leurs composants électroniques, leurs cryostats, étudié la question de l'avantage énergétique du calcul quantique et analysé les matériaux avec lesquels ils sont construits.

Pourquoi l'informatique quantique ?

- L'informatique quantique sert à dépasser les limites des processeurs traditionnels pour des applications spécifiques d'optimisation, de simulation de prédiction et de cryptographie dont la complexité croit de manière exponentielle avec la taille du problème.
- Pourquoi les technologies classiques sont-elles pour l'instant insuffisantes pour atteindre cet objectif ?

Scientifiques

- C'est le "*hall of fame*" du sujet où je mets en évidence les efforts de dizaines de scientifiques de renom qui ont découvert puis fait progresser la mécanique quantique, puis l'informatique quantique. Cela établit une chronologie approximative du domaine, une histoire des idées et rend aux Césars du quantique ce qui leur revient.
- C'est aussi une approche didactique des grandes découvertes de la physique quantique, avec les débats associés qui ont notamment confronté les scientifiques, en particulier autour des années 1920 et 1930. J'y décompose quelques équations quantiques bien connues dont la fameuse fonction d'onde d'Erwin Schrödinger.

Basiques

- Quels sont les fondements de la physique quantique qui sont utilisés dans les technologies quantiques et en particulier dans les ordinateurs quantiques ? L'intrication, la superposition, la dualité ondes-particules et l'épineuse question de la mesure. Cela ne sera pas un cours de mécanique quantique complet, mais juste les bases permettant de mieux comprendre la suite.
- Nous y couvrons aussi la supraconductivité, la superfluidité, les lasers et les masers qui sont des propriétés et technologies très largement utilisées dans les technologies quantiques.
- Une nouvelle rubrique est consacrée aux polaritons et à leurs applications aussi bien dans le calcul quantique que dans la métrologie quantique. Ce sont des objets quantiques hybrides associant lumière et matière.
- Une autre nouvelle rubrique sur le « quantique extrême » décrit les branches de la physique quantique qui dépassent le cadre des usages courants des technologies quantiques et ont plutôt trait à la physique des particules et à la cosmologie.

Qubits

- Les ordinateurs quantiques exploitent au niveau le plus bas des qubits, des entités qui ont deux états simultanés (par superposition) et peuvent se combiner via des portes quantiques (via l'intrication). Les portes quantiques agissent de manière programmatique sur ces qubits. En fin de calcul, on évalue la valeur des qubits pour lire le résultat, sous forme de 0 et de 1. Le calcul quantique est en quelque sorte numérique au début et à la fin, mais analogique au milieu.
- Nous y détaillons les modèles mathématiques utilisés pour décrire l'état des qubits et la fameuse sphère de Bloch qui l'incarne pour les visualiser en trois dimensions.
- Nous faisons aussi un tour du côté des principaux concepts et de l'abondant jargon de l'algèbre linéaire qui sont utilisés dans la physique et dans le calcul quantique.
- Nous balayons rapidement les types de qubits qui utilisent trois principaux types de particules: des **atomes** (ions piégés, atomes froids), des **électrons** (supraconducteurs à effet Josephson, spins d'électrons, fermions de Majorana ou cavités dans des diamants dopés à l'azote) et des

photons. Ces différentes approches sont nécessaires. Il est possible que seule l'une d'entre elle porte ses fruits. On ne sait pas véritablement prédire laquelle à ce stade même si chacun a sa petite idée sur le sujet.

Ordinateur quantique

- Nous définissons les éléments de comparaison clés des ordinateurs quantiques, au-delà même des fameux critères de DiVincenzo.
- Nous voyons dans le détail comment est organisé un ordinateur quantique typique, à base de portes quantiques universelles, avec ses qubits, ses registres, ses portes, ses outils de mesure et ses liens avec l'informatique classique.
- Le problème du bruit qui affecte les qubits et comment il peut être évité ou donner lieu à des corrections, que l'on appelle les QEC (Quantum Error Corrections).
- Certains ordinateurs quantiques actuels doivent être réfrigérés à moins de 20 mK, une température proche du zéro absolu. Nous étudions en détail les systèmes de cryogénie associés et leur ingénierie, à base de réfrigérateur à dilution à sec exploitant de l'hélium gazeux.
- Avec les techniques actuelles de type qubits supraconducteur, un ordinateur quantique tient dans quelques mètres-cubes et consomme environ 25 kW, ce qui est très raisonnable compte-tenu de la puissance de calcul fournie. C'est un outil destiné aux centres de calcul, exploitable à distance dans le cloud. Nous étudions les questions énergétiques du calcul quantique.
- Dans une nouvelle partie, je fais le tour des nombreuses matières premières utilisées dans les technologies quantiques, leur origine, les procédés de transformation et les questions d'approvisionnement. Nous y verrons que, une fois n'est pas coutume, la dépendance vis à vis de la Chine est assez modérée.

Algorithmes et usages

- Les notions de suprématie et d'avantage quantiques. L'émulation d'algorithmes quantiques sur des calculateurs traditionnels.
- Les ordinateurs quantiques exploitent des algorithmes quantiques qui servent à résoudre des problèmes de calculs complexes bien plus rapidement qu'avec des supercalculateurs. Ces algorithmes sont très différents de ceux de l'informatique traditionnelle. De tels algorithmes quantiques sont régulièrement inventés depuis le début des années 1990 après ceux de Deutsch-Jozsa, Grover et Shor.
- Les grandes applications de l'informatique quantique portent sur la simulation de physique des matériaux, en biologie moléculaire, des optimisations complexes et aussi le machine learning.
- Les algorithmes quantiques sont souvent hybrides, associant du calcul traditionnel et du calcul quantique.
- J'y décris aussi le fameux algorithme de téléportation de l'état d'un qubit qui, vous serez déçus, n'a rien à voir avec la téléportation de Star Trek.
- Les gains de performance quantiques et la notion de certification des algorithmes.

Complexité

- Les théories de la complexité des problèmes, les classes de complexité classiques et quantiques et les limitations des ordinateurs quantiques.

Outils de développement

- L'offre d'outils de développement en distinguant ceux qui sont issus de laboratoires de recherche de ceux qui proviennent de sociétés privées.
- Une nouvelle partie couvre les offres d'accès en cloud à des ordinateurs quantiques.

Applications métiers

- En complément de la partie sur les principaux algorithmes quantiques, nous faisons un tour des applications potentielles de l'informatique quantique dans différents secteurs d'activité comme les transports, la santé, l'énergie et la chimie, la finance, le marketing, la défense et l'aérospatial, le renseignement, la défense, l'industrie et la recherche.
- Nous y décrivons quelques études de cas documentées de cas d'usages prototypes dans les grandes entreprises de ces différents secteurs d'activité.

Acteurs des calculateurs quantiques

- Cette partie rentre dans le détail des différentes technologies de qubits. Elle est beaucoup plus riche et scientifiquement documentée dans cette édition 2020 de l'ebook. Nous y faisons le tour des principaux acteurs industriels de l'informatique quantique avec notamment D-Wave, IBM, Google, Rigetti, IonQ, Intel, Honeywell et Microsoft. Avec leurs technologies et le point où ils en sont.
- S'y ajoute une nouvelle partie sur les technologies de calcul concurrentes ou complémentaires du calcul quantique : supercalculateurs, processeurs supraconducteurs, processeurs adiabatiques et réversibles, calcul probabiliste et processeurs optiques.

Startups et PME du calcul quantique

- Nous y traitons des investisseurs spécialisés dans les technologies quantiques.
- J'y inventorie tour à tour les startups et PME de composants matériels, de calculateurs quantiques et dans les logiciels quantiques.
- C'est une étude de cas "in vivo" d'écosystème en cours de constitution, très en avance de phase par rapport à l'émergence du marché correspondant.
- Le niveau de détail fourni dépend à la fois de la communication des startups et du temps d'investigation de ma part à leur sujet.

Télécommunications et cryptographie quantiques

- C'est le marché le plus mûr de l'informatique quantique, conséquence directe des menaces que fait peser à long terme le calcul quantique sur la cryptographie à clés publiques.
- Le marché comprend deux composantes : la cryptographie quantique qui permet de transporter des clés de sécurité sans qu'elles soient violables pendant leur transport, et la cryptographie post-quantique qui permet de se prémunir des capacités de déchiffrement que l'algorithme de Shor donnera aux possesseurs d'ordinateurs quantiques.
- La cryptographie quantique fait partie du domaine plus vaste des télécommunications quantiques, utilisables notamment pour relier des ordinateurs quantiques entre eux ou relier des capteurs quantiques à des calculateurs quantiques. On l'associe parfois à la notion « d'Internet quantique ».

Métrologie quantique

- Quelles sont les applications quantiques dans les outils de mesure de précision : du temps, des fréquences de la lumière, de la gravité et du magnétisme ?
- Cette partie est un ajout de l'édition de septembre 2019 et enrichie dans l'édition 2020. J'y traite notamment du système international de mesure qui est en vigueur depuis 2019 et que l'on peut qualifier de « quantique ». Nous verrons pourquoi.

Technologies quantiques dans le monde et en France

- Je couvre l'organisation des écosystèmes quantiques dans un grand nombre de pays avec leurs grands laboratoires, les initiatives des états, les personnalités qui comptent. Avec notamment les USA, le Canada, le Royaume-Uni, l'Autriche, la Suisse, les Pays-Bas, la Chine, le Japon, Singapour et l'Australie.
- Suit le cas particulier de la France avec notamment, une cartographie de ses laboratoires de recherche, ses industriels et le plan quantique national français.

Entreprises

- Proposition d'une démarche simple pour aborder la thématique de l'informatique quantique dans l'entreprise.

Société

- Quels sont les questions philosophiques et éthiques soulevées par l'informatique quantique ? Les biais et l'explicabilité des algorithmes à l'heure de l'informatique quantique, les grandes différences avec ces mêmes questions lorsqu'elles sont appliquées au deep learning. Risque-t-on de voir le calcul quantique concentré dans les mains de quelques acteurs ou pays ?
- Le jargon du quantique et ses dérives. La volonté de puissance sur les données, la nature et la compréhension du monde. Les enjeux en termes de formation. Le marketing de l'offre et ses exagérations.

Fumisteries quantiques

- Un passage par la médecine quantique avec quelques-uns de ses fondamentaux scientifiques qui méritent le détour à bas niveau puis les approches à haut niveau qui relèvent dans l'ensemble de la charlatanerie. Comment glisse-t-on des unes aux autres ?
- J'y couvre d'autres fumisteries quantiques diverses détectées dans l'industrie comme le management quantique - évoqué au second degré - et le marketing quantique.

Glossaire

- Un glossaire introduit dans la version de 2019 qui décrit les termes techniques employés dans l'ebook. Un bon moyen de vérifier ses connaissances sur le sujet. Ne serait-ce que pour l'auteur !

Guide de lecture

Voici une tentative de priorisation des parties à lire en priorité en fonction de votre activité et niveau scientifique. D'une manière générale, cet ouvrage se positionne de manière intermédiaire entre les ouvrages scientifiques de référence du domaine et les livres blancs de vulgarisation qui peuvent être produits par les sociétés de conseil ou les grands fournisseurs. Il a beau être volumineux, il reste superficiel sur la plupart des sujets traités tellement le champ est large !

Les physiciens peuvent y trouver un tour de l'état de l'art couvrant l'ensemble des dimensions des technologies quantiques au-delà du domaine qu'ils maîtrisent déjà.

Les informaticiens, ingénieurs et étudiants dans les filières scientifiques sont le cœur de cible de l'ouvrage sachant que celui-ci présente, vulgarise et remet en contexte les concepts scientifiques et mathématiques utilisés. Les bases mathématiques et informatiques à maîtriser pour suivre sont situées au niveau d'environ Bac+2/+3. Après, tout dépend de l'âge car plus on remonte dans le temps de l'enseignement supérieur, moins ces concepts étaient enseignés.

Les écoles d'ingénieur généralistes enseignent plus souvent la physique quantique dans les troncs commun qu'elles le faisaient il y a quelques décennies.

Les non techniciens et décideurs pourront consulter les parties portant sur les usages ainsi que sur l'état des lieux dans les pays et les questions sociétales.

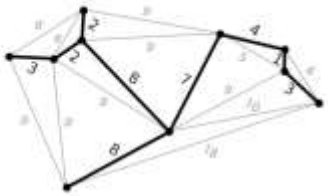
Parties de l'ouvrage	Physiciens	Informaticiens	Ingénieurs et étudiants scientifiques	Non techniciens	Décideurs
Pourquoi					
Scientifiques					
Basiques					
Qubits					
Ordinateur quantique					
Algorithmes et usages					
Complexité					
Outils de développement					
Applications métiers					
Acteurs des calculateurs					
Startups du calcul quantique					
Télécommunication et cryptographie					
Métrologie quantique					
Technologies quantiques dans le monde					
Technologies quantiques en France					
Entreprises					
Société					
Fumisteries quantiques					

Pourquoi l'informatique quantique ?

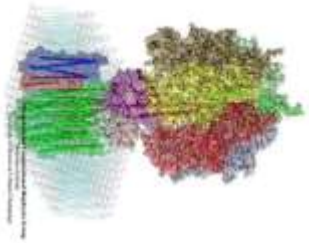
L'une des motivations de l'informatique quantique est de pouvoir résoudre des problèmes que les ordinateurs traditionnels ne savent pas et ne sauront peut-être jamais traiter convenablement. Il s'agit des problèmes de nature exponentielle, dont la complexité augmente exponentiellement avec la quantité des données à traiter. Le schéma *ci-dessous* présente quelques exemples de problèmes complexes de nature exponentielle.

Cela commence avec divers problèmes d'optimisation comme celui du parcours du livreur ou de véhicules autonomes dans le trafic. Lorsque la combinatoire à optimiser est très grande, les algorithmes classiques trouvent leurs limites sur les ordinateurs traditionnels.

Cela se complique avec l'optimisation du trafic de parcs de véhicules autonomes de villes intelligentes du futur. Aujourd'hui, on optimise son trajet avec Google Maps ou Waze en s'appuyant sur l'état du trafic. Celui-ci est variable et la durée du trajet finale n'est pas toujours optimale et ne correspond pas forcément à la durée prévue.



optimisations combinatoires
trajets, placements, cartes, finance



simulations moléculaires
matériaux et biologie

intelligence artificielle
machine learning et deep learning

factorisation
de très grands nombres entiers

C'est un système soumis à de très nombreuses contraintes ou de modèles multivariés, lorsque l'on dispose de l'ensemble des données associées. Avec une flotte intégralement autonome, on devrait pouvoir théoriquement optimiser le trajet individuel de chaque véhicule en fonction de leur lieu de départ et de destination. Les algorithmes classiques pourraient fonctionner avec une quantité limitée de véhicules mais au-delà de quelques centaines de véhicules et trajets, les capacités de calcul traditionnelles seraient largement saturées. Le quantique arriverait alors à la rescousse !

En second lieu intervient la simulation du fonctionnement de la matière au niveau des particules. Elle est régie par les règles de la mécanique quantique qui dépendent d'équations connues mais dont la résolution est un problème d'optimisation complexe à résoudre, passant par la recherche d'un minimum énergétique, particulièrement pour comprendre l'interaction de nombreux atomes dans des molécules ou des structures cristallines complexes. Cela concerne aussi bien la simulation chimique que celle du vivant.

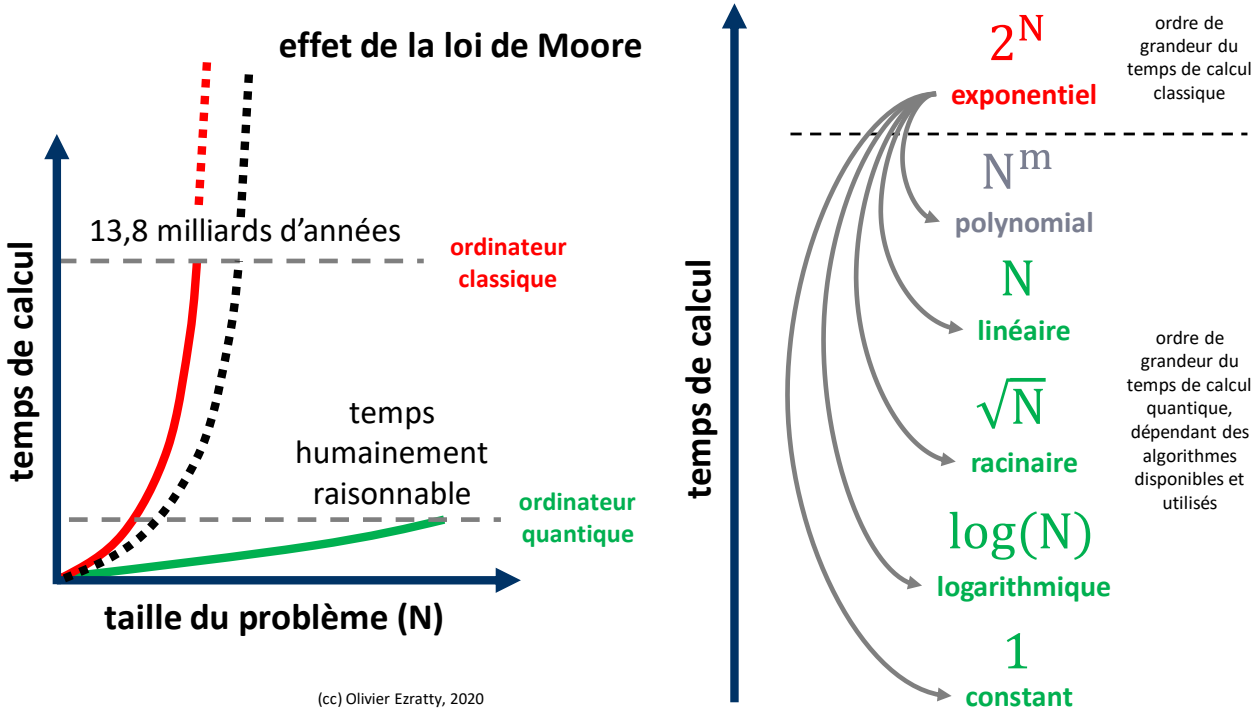
L'informatique quantique pourrait ainsi servir à simuler le quantique du monde réel dans l'infiniment petit. Rassurez-vous, cela n'ira pas au point de simuler un être vivant en entier. Cela sera déjà une prouesse fantastique que de le faire un niveau du repliement d'une seule protéine sur elle-même !

L'entraînement de modèles de machine learning et de réseaux de neurones est un troisième domaine d'application. Il est aujourd'hui à la portée des ordinateurs classiques, équipés de GPU comme ceux de Nvidia ou les processeurs neuromorphiques qui mettent en œuvre dans le silicium des portes logiques dont l'organisation est très proche de la logique des réseaux de neurones. Aujourd'hui, la puissance de calcul disponible rend difficile l'entraînement de réseaux de grande taille. Pour ne prendre que l'exemple des réseaux convolutifs de reconnaissance d'images, ceux-ci ont une résolution d'image en entrée généralement limitée à 227x227 pixels.

Enfin, nous pouvons citer la factorisation de nombres entier qui intéresse notamment la NSA et les services de renseignement pour casser les codes de sécurité sur Internet de type RSA qui reposent sur l'envoi de clés publiques. Nous aurons l'occasion de creuser cela en détails.

D'autres applications pourront émerger pour différents marchés comme la finance ou l'assurance. Nombre d'applications métiers sont concernées par les problèmes d'optimisation complexes et restent à inventer, notamment à destination d'applications grand public.

Pour mieux comprendre l'intérêt de l'informatique quantique, le schéma *ci-dessous* met en abyme le temps de calcul comparé de problèmes très complexes entre calcul classique et calcul quantique.



Dans les cas extrêmes, les temps de calcul sur ordinateurs classiques de problèmes exponentiels, même avec les plus puissants des supercalculateurs du moment, dépasseraient l'âge de l'Univers, soit 13,85 milliards d'années sachant que la Terre restera encore vivable dans le meilleur des cas pendant seulement 2 milliards d'années, modulo les effets à court terme - à l'échelle cosmique - du réchauffement planétaire. L'effet de la loi de Moore resterait marginal dans l'histoire, en pointillé dans le graphe : tout d'abord, comme nous allons le voir, il ralentit sérieusement, et même s'il ne ralentissait pas, son impact resterait marginal. Les temps de calcul de problèmes exponentiels resteraient exponentiels malgré le doublement supposé de la puissance des machines tous les 18 mois à deux ans. Alors que l'ajout d'un simple qubit permet de théoriquement doubler la puissance d'un ordinateur quantique, surtout du côté de son espace mémoire.

Comparativement, des ordinateurs quantiques pourraient en théorie, un de ces jours, résoudre ces mêmes problèmes dans un temps raisonnable à l'échelle d'une vie humaine, en heures, journées, semaines ou mois. La notion de raisonnable dépend évidemment de la nature du problème à résoudre. Je raisonne au conditionnel car on n'est pas vraiment sûr d'y arriver.

Le bénéfice principal du calcul quantique est de modifier les échelles de temps de résolution d'un problème. Dans l'échelle à droite, on voit de tels ordres de grandeur. Les problèmes exponentiels sont dits « intractables » car leur temps de calcul évolue dans des proportions folles avec leur taille. Les autres temps de calcul, polynomiaux, linéaires, racinaires ou logarithmiques, évoluent beaucoup moins vite avec N. En théorie, le quantique permet de passer d'un niveau de cette échelle à un niveau plus bas. Il est utile lorsque N est grand, parfois à partir seulement d'une cinquantaine ! Le calcul quantique permet aussi de gagner en échelle d'espace, notamment mémoire, pour réaliser ces calculs.

dessin de François Cointe, publié avec son autorisation, source : https://www.lemagit.fr/dessin/Google-presente-son-ordinateur-quantique

Les barrières technologiques si ce n'est scientifiques à franchir sont cependant encore immenses avant d'y parvenir.

L'informatique quantique n'est pas juste là pour aller plus vite que l'informatique traditionnelle dans son champ opératoire actuel. Elle sert à résoudre des problèmes inaccessibles aux ordinateurs classiques, même en s'appuyant sur un éventuel mouvement perpétuel de la loi de Moore, qui, on le sait, n'est pas du tout assuré. On pourrait ainsi affirmer que le potentiel de disruption de l'informatique quantique est "multi-mooresque". Ce n'est pas un marché de remplacement mais un marché de complément des outils actuels du calcul haute performance (HPC, High Performance Computing).

Comment augmente-t-on actuellement la puissance des ordinateurs classiques ? On s'appuie sur quelques techniques connues, certaines n'ayant pas encore été explorées à fond. Nous avons l'augmentation de la densité des processeurs en transistors qui permet d'aligner plus de fonctions dans un processeur mais sans forcément en augmentant sa rapidité. Nous créons des architectures multicœurs qui permettent de paralléliser les traitements pour peu que les logiciels associés le permettent. Mais elles rencontrent des limites, formalisées par la **loi d'Amdahl** qui décrit les limites hautes d'accélération de système de calcul parallèles.

L'accélération de traitements peut provenir de processeurs utilisant des tenseurs (multiplicateurs de matrices) ou des processeurs neuromorphiques (imitant le fonctionnement des neurones biologiques, avec une mémoire intégrée comme avec les memristors).

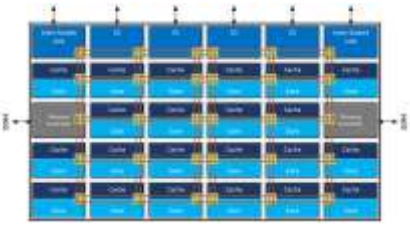
Le tout étant intéressant pour l'entraînement et l'inférence des réseaux de neurones du deep learning utilisés notamment dans la reconnaissance d'images et celle du langage.

Nous pouvons passer par l'optronique en remplaçant les électrons par des photons pour faire circuler l'information. Cela permettrait en théorie de créer des processeurs allant 20 à 25 fois plus vite que les processeurs CMOS actuels et d'atteindre 100 GHz. Mais ces processeurs sont difficiles à mettre au point et à intégrer, il est presque impossible de créer des équivalents des transistors avec des photons. Les matériaux utilisés sont différents de ceux des processeurs CMOS. On passerait ainsi du silicium à l'indium, au gallium et autres métaux plutôt rares.

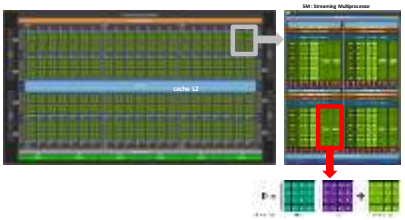
La barrière de la chaleur limite l'augmentation de la vitesse d'horloge des processeurs. Elle plafonne de manière courante à 4 GHz dans les processeurs Intel du marché et peut monter à 6 GHz avec des refroidissements de compétition[9].

[9] Voir à ce sujet Minimum Energy of Computing, Fundamental Considerations par Victor Zhirnov, Ralph Cavin et Luca Gammaitoni, 2014 (40 pages) qui compare au passage l'efficacité énergétique du vivant et de l'électronique.

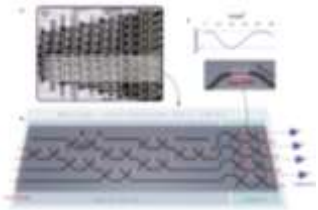
vitesse d'accès mémoire



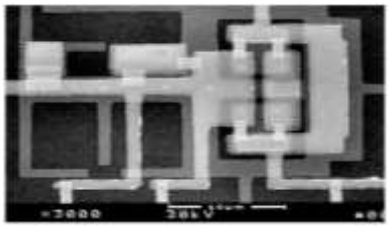
multicœurs spécialisés



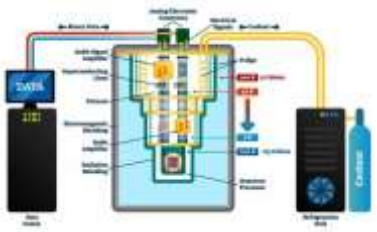
tenseurs et neurones à impulsions



optronique et III/V



transistors supraconducteurs



calcul quantique

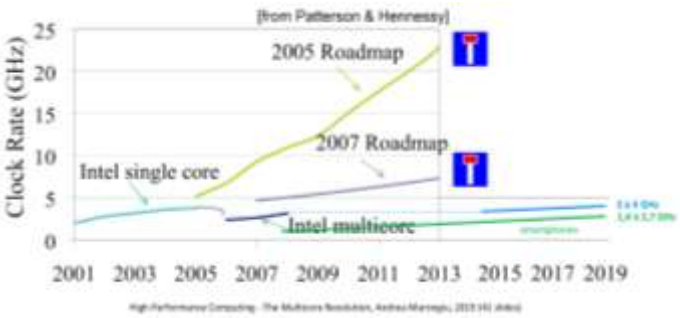
Cela tient à la fin en 2006 de l'application de la règle de **Robert Dennard** (1932, Américain) établie en 1974. Cette règle indiquait que lorsque l'on augmente la densité des transistors, on pouvait stabiliser la puissance consommée par unité de surface des chipsets. Cela venait du fait que la tension et l'intensité électrique des transistors pouvait baisser au gré de la densité, tout en augmentant la fréquence d'horloge. A partir de 65 nm, cette règle a sauté.

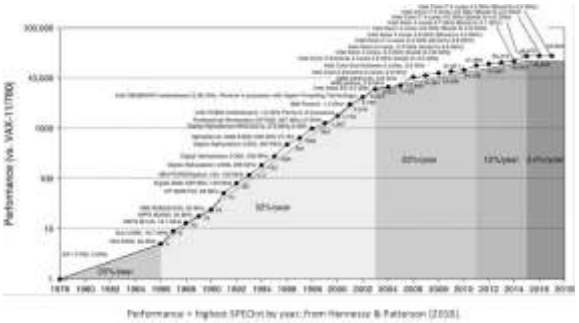
Les fuites dans les transistors devenaient trop importantes et la consommation électrique est partie en flèche. C'est elle qui empêche la montée de la fréquence des processeurs. Au début des années 2000, Intel prévoyait pourtant dans ses roadmaps de monter la fréquence d'horloge de ses processeurs à 20 GHz.

Il a dû rebrousser chemin dès 2007 et d'ailleurs, bien trop tard pour pouvoir prendre pied dans le marché émergent des processeurs pour smartphones qui devaient fonctionner en mode basse consommation. Cela a ouvert un boulevard pour les processeurs à base de noyaux arm.

La puissance de calcul disponible par kW consommé augmentait régulièrement, doublant tous les 1,57 ans entre 1946 et 2009, selon la loi empirique de **Jonathan Koomey** édictée en 2010. Ce doublement est cependant passé à une fois tous les 2,6 ans après 2000, du fait de l'arrêt de la loi de Dennard.

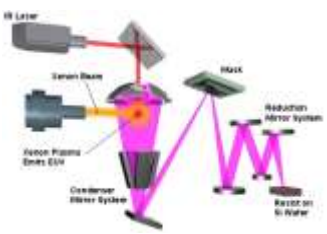
Mais après 2006, la densité des transistors a continué d'augmenter. La fin de la règle de Dennard a entraîné un phénomène dont on parle peu : celui du **dark silicon**. Comme les chipsets chauffent trop, on est obligé de ne pas les utiliser en entier. On combine alors des méthodes diverses : soit des désactivations à la demande en fonction des besoins, soit une mise en veilleuse de certaines portions ou cœurs, soit une baisse de tension, soit une baisse sélective de fréquence d'horloge.





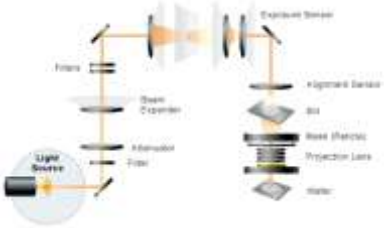
C'est d'ailleurs ce qui est utilisé dans les processeurs à base de noyaux arm des chipsets de smartphones, dont les cœurs ne tournent pas à la même vitesse, dans les architectures dites big.LITTLE.

Pour créer des transistors avec une intégration en-dessous de 10 nm, il faut faire appel à des systèmes de gravure utilisant l'extrême ultra-violet. En effet, leur résolution dépend de la longueur d'onde de la lumière utilisée pour projeter un masque sur une résine photosensible. Pour diminuer la taille des transistors, il faut augmenter cette fréquence pour diminuer la longueur d'onde, et donc passer de l'ultra-violet actuel à l'extrême ultra-violet.

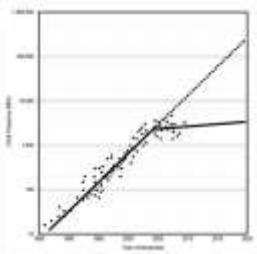


Extreme Ultra Violet (EUV)
difficile à mettre au point <= 10 nm

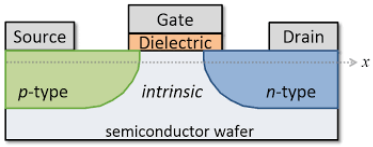
limites techniques du CMOS



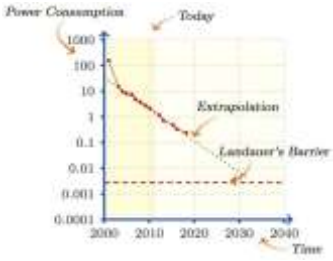
taille maximale des réticules
limite haute de la taille des chipsets



barrière de la chaleur
limite la fréquence des processeurs



effets quantiques indésirables vers 5 nm
diélectrique
= 6 atomes d'épaisseur



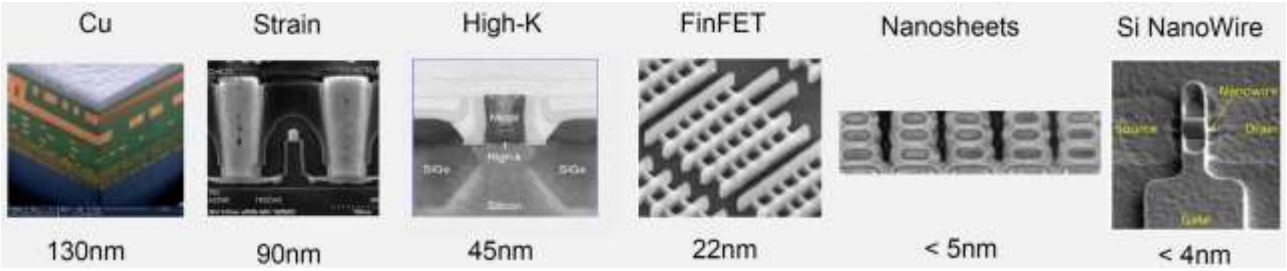
barrière de Landauer
limite basse de consommation

Cela fait presque 10 ans que ces machines de gravure EUV sont mises au point, et de manière très laborieuse. Elles sont cependant en production depuis 2019, notamment chez TSMC et Samsung pour de la gravure en 7 nm. L'un des avantages de l'EUV est d'éviter le « multiple patterning » qui consiste, entre autres, à graver un sillon de transistor sur deux ou sur trois par passe pour améliorer la précision et éviter les effets de bord intempestifs.

Lorsque l'on miniaturise les transistors en deçà de 5 nm, on voit apparaître des effets quantiques indésirables et l'équation d'indétermination d'Heisenberg que nous verrons plus loin commence à faire mal. Ce qui n'empêche toutefois pas les roadmaps de Samsung et TSMC de prévoir d'atteindre les 3 nm d'ici 2025, grâce notamment à la technique des nanowires et des nanosheets[10].

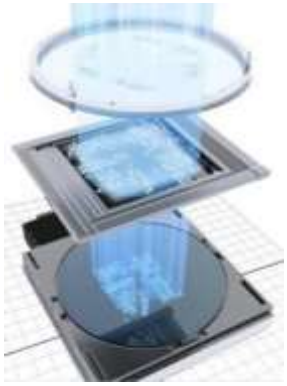
[10] Voir Beyond CMOS, Superconductors, Spintronics, and More than Moore Enablers de Jamil Kawa, Synopsys, mars 2019 (43 slides), une bonne présentation qui décrit les différentes pistes d'amélioration de la puissance des composants dont les Cold CMOS, les semiconducteurs fonctionnant à une température voisine de l'azote liquide (-70°C) dans compter les transistors supraconducteurs à effet Josephson. Le schéma de la page suivante en est issu.

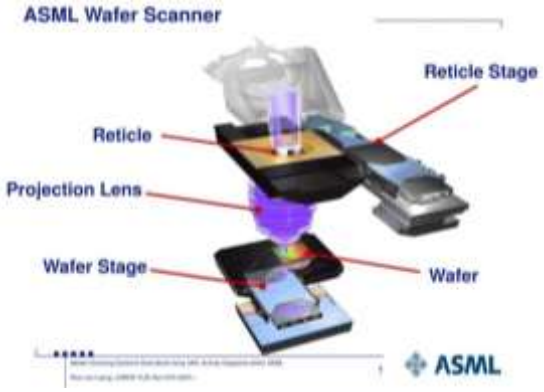
En août 2020, TSMC annonçait cependant pouvoir lancer la production de composants gravés en 3 nm dès 2022, en associant la gravure en EUV et en conservant la technologie FinFET classique qui sévit depuis plus de 10 ans. Comme quoi ils ont encore un peu de mou sous la pédale ;



Deux autres limites sont à prendre en compte comme la barrière de **Rolf Landauer** (chercheur chez IBM, en 1961) qui indique le minimum d'énergie nécessaire pour modifier une information. C'est une barrière théorique contestée par certains physiciens[11]. Et elle est contournable comme nous le verrons avec la technique du calcul adiabatique et réversible.

Enfin, il existe une limite de taille des réticules, ces systèmes optiques de gravure d'un processeur dont la taille est physiquement limitée, notamment optiquement. Les illustrations *ci-contre* issues d'**ASML**, le leader mondial de la lithogravure de semiconducteurs, permettent de comprendre cela.





Les plus grands processeurs mono-composants de 2020 étaient le **Nvidia** A100 avec ses 54,4 milliards de transistors gravés en 7 nm suivi de peu par le **Graphcore** GC200 avec ses 59,4 milliards de transistors et 1472 cœurs, lancé en juillet 2020.

La startup américaine **Cerebras** a tout de même lancé en 2019 un processeur carré de 21,5 cm de côté, occupant tout un wafer de 30 cm, qui contourne la limite de taille de réticule en étant gravé en plusieurs passes, pour ses 84 unités principales de traitement reliées par des couches métal. Il contient 18 Go de mémoire cache, ce qui lui permet d'accélérer l'entraînement de réseaux de neurones. Les techniques de fabrication génèrent des défauts et plus de 1% des 412 000 unités de traitement sont défectueuses et sont court-circuitées lors de l'exécution des logiciels. Il consomme 15 kW qui sont évacués par un système de refroidissement spécifique à base de flux d'eau circulant de manière orthogonale vis-à-vis du processeur.

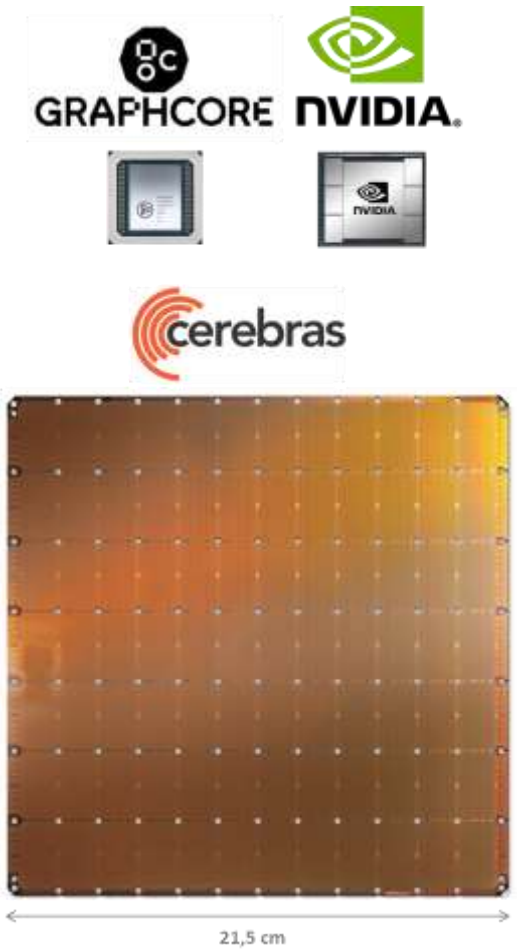
[11] Source du schéma sur la limite de Landauer : Reversible Circuits : Recent Accomplishments and Future Challenges for an Emerging Technology, Rolf Drechsler and Robert Wille, 2012 (8 pages).

L'informatique quantique permettra de passer outre les diverses limitations des processeurs CMOS actuels pour certaines tâches. Elle ne les remplacera toutefois pas du tout pour les tâches actuellement accomplies par les ordinateurs et mobiles actuels.

Typiquement, la compression et la décompression de vidéo ou d'audio ne sont pas des tâches adaptées au calcul quantique. Elles sont d'ailleurs réalisées dans des unités de traitement spécialisées des processeurs généralistes du marché que l'on appelle des DSP.

De même, les applications manipulant de très gros volumes de données ne sont pas adaptées au calcul quantique pour tout un tas de raisons que nous étudierons, notamment parce que la vitesse d'alimentation des qubits en données n'est pas très élevée mais aussi en raison de la nature même des algorithmes quantiques, surtout ceux qui sont connus aujourd'hui. Sans compter les questions de taux d'erreur du calcul quantique.

Comme ses usages ne seront pas les mêmes, il est difficile d'anticiper le paysage informatique qui germera. Les prévisions de Ray Kurzweil sur l'avènement d'une singularité qui s'appuient fortement sur la prolongation ad-vitam de la loi de Moore mériteront en tout cas d'être ajustées !



Dans cet ouvrage, nous étudierons aussi rapidement quelques autres pistes envisagées pour dépasser les limites actuelles du calcul qui peuvent apporter un gain de puissance intermédiaire entre le calcul classique et le calcul quantique.

Nous avons ainsi les transistors fonctionnant à des températures supraconductrices, de l'ordre de 4K, avec de nouveaux projets financés depuis 2014 par l'agence **IARPA** américaine, le calcul à recuit digital, poussé par **Fujitsu** au Japon, le **calcul réversible** et/ou adiabatique, les **processeurs probabilistes** ainsi que différentes formes d'**accélérateurs optiques**. La rédaction de cet ouvrage m'a poussé à me plonger dans les arcanes des supercalculateurs et processeurs spécialisés pour mieux en comprendre les forces et les faiblesses. Lorsque l'on compare des puissances de calcul, il vaut mieux savoir de quoi l'on parle des deux côtés des comparaisons !

Ce sont des solutions « de backup » en cas d'échec à créer des ordinateurs quantiques traitant l'épineux problème du bruit que nous aurons aussi l'occasion de creuser. Elles seront aussi fréquemment complémentaires du calcul quantique dans le cadre du calcul hybride. Dans d'autres cas comme pour les transistors supraconducteurs, il peut s'agir de technologies habilitantes permettant à certains types d'ordinateurs quantiques de « scaler ».

L'histoire des technologies est ainsi faite d'exploration de branches multiples. Certaines n'aboutissent pas. D'autres s'entre-aident. Enfin, certaines peuvent renaître de leurs cendres après avoir végété plusieurs décennies.

Scientifiques

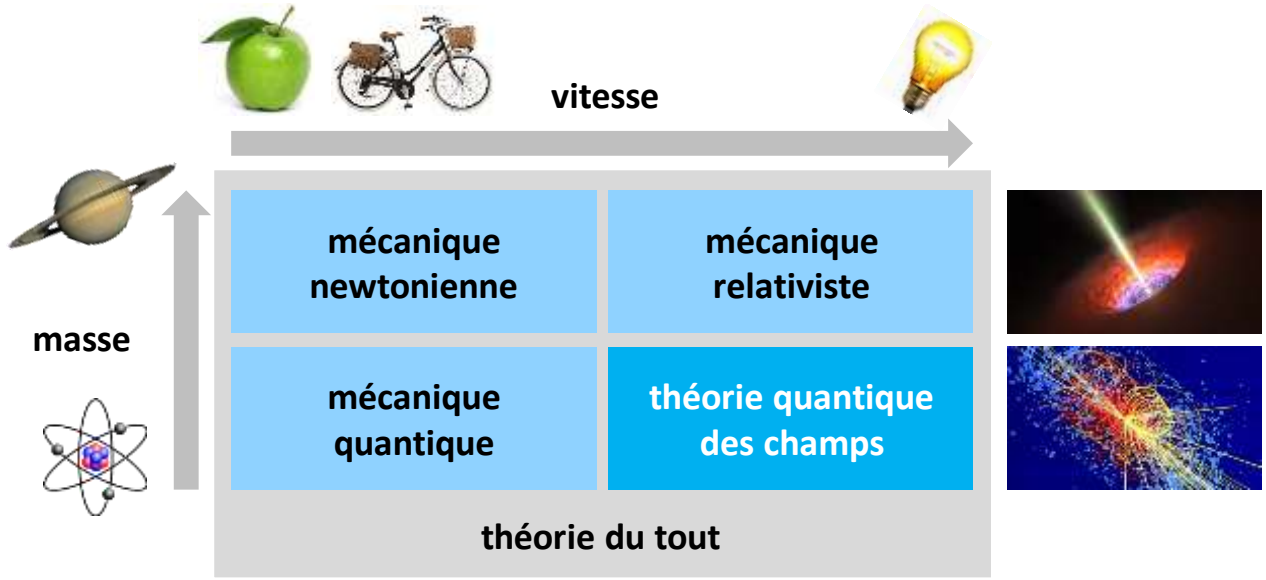
Après avoir posé le décor et le sommaire de cet ebook sur l'informatique quantique, nous allons faire un petit retour en arrière pour découvrir la riche histoire de cette discipline.

Chaque épopée scientifique et technologique est avant tout une grande Histoire humaine. Celles de la mécanique quantique et de l'informatique quantique n'y échappent pas. Je vais ici rendre hommage aux scientifiques qui ont rendu tout cela possible et continuent encore de plancher dessus pour ceux qui sont encore de ce monde.

La physique ou mécanique quantique s'intéresse à l'infiniment petit et à ses différences par rapport à la mécanique classique, souvent dite newtonienne, qui régit de manière prédictible le fonctionnement des objets de taille raisonnable, au-delà de quelques microns et jusqu'à la taille des planètes et des étoiles. La mécanique quantique s'intéresse particulièrement aux interactions entre la lumière et la matière.

La mécanique classique est régie par les lois de Newton avec les équations du mouvement de la matière, par les lois de Maxwell qui décrivent les champs électromagnétiques et les forces associées et par la physique statistique qui décrit les milieux continus comme les gaz et les fluides et d'où émergent les principes de la thermodynamique.

Dans l'infiniment grand, on fait appel à la théorie de la relativité et à son lien avec la gravitation qui explique la courbure de l'espace-temps. Elle est indispensable pour interpréter les phénomènes extrêmes que sont les trous noirs ou les étoiles à neutrons. Elle permet d'interpréter l'Histoire de l'Univers, mais pas entièrement.



S'y ajoute enfin la théorie quantique des champs qui décrit les phénomènes qui se produisent avec les particules élémentaires circulant à très haute vitesse, comme celles que l'on observe dans les accélérateurs de particules avec les quarks ou les bosons de Higgs[12]. Le physicien Richard Feynman est l'un des pères de l'électrodynamique quantique qui est un sous-ensemble de la théorie quantique des champs.

[12] Voir ce cours de vulgarisation sur les particules élémentaires, quark dans les neutrons et protons, Les particules élémentaires par Guillaume Lumin et Franck Stevens, 2012.

La physique n'est toujours pas complète ni totalement unifiée. Certains phénomènes physiques observables lui résistent encore. On ne sait pas expliquer précisément l'origine précise de la gravitation et on cherche toujours la matière et l'énergie noires qui expliqueraient la cohésion des galaxies. L'Homme aimerait bien tout savoir et tout expliquer mais il est fort probable que cette quête sera toujours en devenir, ne serait-ce que sur la forme qu'avait l'Univers avant le Big Bang.

La théorie du tout recherchée par nombre de physiciens serait un formalisme permettant d'unifier l'ensemble des théories de la physique et en particulier la théorie de la relativité et la mécanique quantique. C'est un champ très sérieux, mais en devenir, de la physique[13]. Des propositions nombreuses émergent pour générer cette théorie du tout et en faire le tri n'est pas toujours évident[14].

Vous pouvez passer cette partie et aller directement à la suivante sur les grands basiques de la physique quantique si l'Histoire des sciences ne vous intéresse pas. Cette partie sert surtout de référence pour bien mémoriser qui est qui dans l'Histoire de la mécanique et de l'informatique quantiques. J'y couvre cependant quelques fondamentaux scientifiques importants comme les équations de Maxwell et de Schrödinger.

Un topo sur l'informatique quantique démarre immanquablement par un "101" de la mécanique quantique. Il requiert de couvrir quelques basiques, même s'ils sont parfois abstraits. Mon objectif sera de raccommoder les morceaux avec le fonctionnement pratique des ordinateurs quantiques. Comprendre la mécanique et l'informatique quantique relève de l'assemblage d'un vaste puzzle. On ajoute les pièces une par une. Le puzzle n'est jamais complet. Au bout d'un certain temps, on y voit une image qui permet d'avoir une vue d'ensemble sans forcément que le puzzle soit terminé. C'est ce qui vous arrivera probablement au terme de la lecture de la partie scientifique de cet ebook.

La physique quantique est une science qui a pris forme aux débuts du XXe siècle. Malgré ses enrichissements constants, elle a fait preuve d'une étonnante solidité pour résister à l'épreuve du temps. Comme presque toutes les sciences, elle résulte des travaux de très nombreux scientifiques et chercheurs et d'allers et retours entre expérimentation, construction de théories descriptives et explicatives et de modèles mathématiques. La mécanique quantique n'explique cependant pas au plus bas niveau ce qu'elle modélise mathématiquement et que l'on peut observer pratiquement, comme l'intrication.

L'histoire des idées de la mécanique quantique est une aventure humaine qui a rassemblé des talents immenses qui se sont confrontés et qui ont fait évoluer pas à pas leur compréhension de l'infiniment petit. Régulièrement, de nouvelles générations de scientifiques ont remis en question l'état des lieux de leurs prédécesseurs[15].

---

[13] Le physicien américano-japonais Michio Kaku estime que cette théorie du tout sera finalisée d'ici 2100. Voir Michio Kaku thinks we'll prove the theory of everything by 2100, avril 2019. On ne sera probablement pas là pour le vérifier à ce moment-là ! Ce Michio Kaku n'est pas un marginal. Il est à l'origine de la théorie des cordes. Il définit très bien l'articulation entre les différentes branches de la physique et cette théorie du tout dans A theory of everything?.

[14] C'est par exemple le cas du Wolfram Physics Project lancé en avril 2020 par Stephen Wolfram, un physicien, mathématicien et informaticien prolixe anglo-américain. Cela faisait suite à un épais ouvrage publié en 2002 « A new kind of science ». L'idée de l'auteur est d'expliquer tout, le monde, la physique, l'univers, à partir d'un seul outil : les automates cellulaires, les graphes et les fractales. Le monde serait discret à petite échelle, y compris pour celle du temps. Son Physics Project se focalise sur l'unification de la physique avec le même outillage. Voir la centaine de pages de présentation du projet, le livre blanc qui applique cela à la physique quantique. La position des physiciens est plus que circonspecte face à ces théories. Les documents n'ont pas été évalués par des tiers dans des revues à comité d'auteur et l'approche scientifique est au minimum déficiente sur un point clé : elle n'élabore pas de théorie qui serait vérifiable par l'observation ou l'expérimentation comme ce fut le cas pour tous les fondements de la physique quantique (superposition, fonction d'onde, écrasement de fonction d'onde, raies spectrales diverses, …). En 2002, sa théorie était démontée par Scott Aaronson dans une revue de lecture de 14 pages, notamment au sujet des inégalités de Bell, ainsi que dans A New Kind of Science par Cosma Rohilla Shalizi de Carnegie Mellon, qui n'y va pas par quatre chemins.

[15] Savoureuse est cet écrit de Max Planck de 1950 qui attribue l'évolution de la pensée scientifique au décès des anciennes générations : « *A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die and a new generation grows up that is familiar with it*".

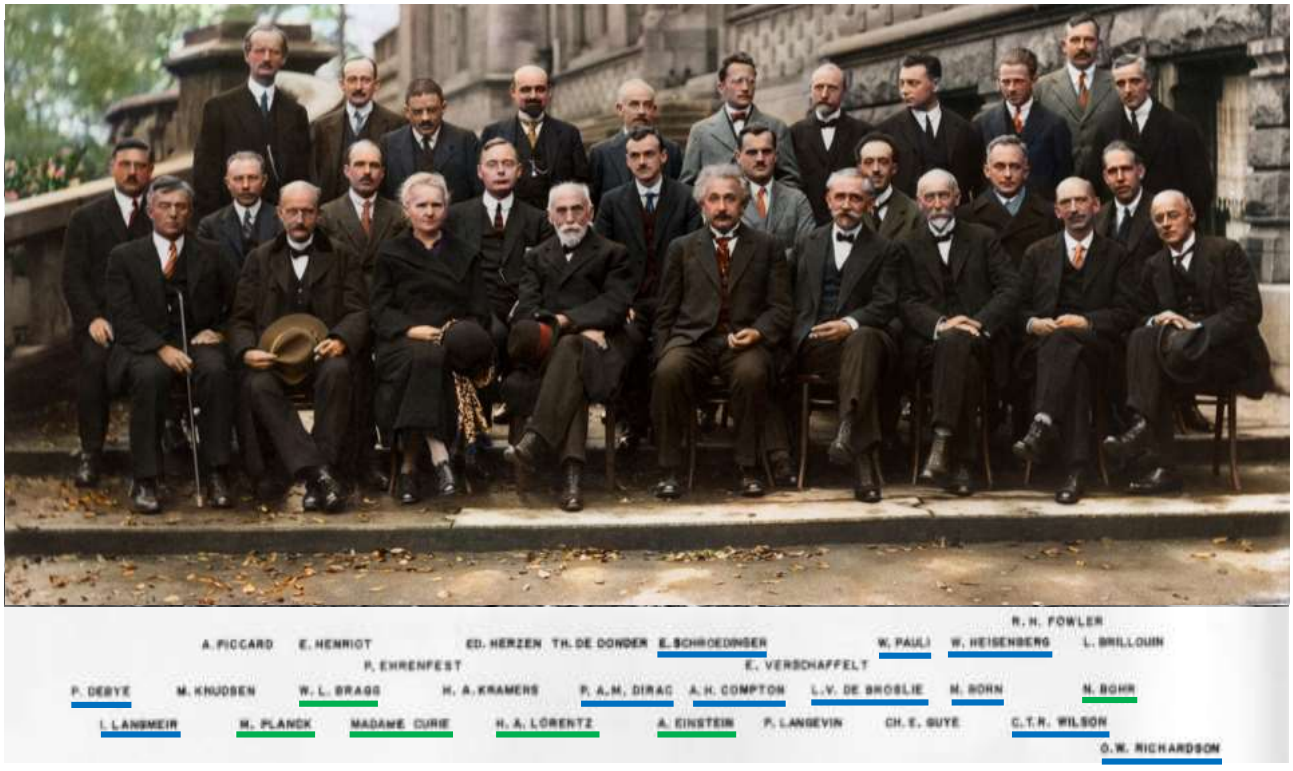
Dans la mécanique quantique comme dans une bonne part de l'histoire de la physique, cette compréhension a associé des physiciens et des mathématiciens. Les physiciens ont mené de nombreuses expériences pour identifier des paradoxes, des inconnues, bâtir des théories puis les vérifier par l'expérience, parfois avec plusieurs décennies de latence. Ils ont dû aussi verser dans la philosophie pour interpréter le sens de leurs découvertes.

Les mathématiciens ont bâti des modèles de représentation des données, comme les matrices et l'algèbre linéaire, qui jouent un très grand rôle dans la mécanique quantique pour décrire les états des quanta et leur évolution dans l'espace et dans le temps. Cette algèbre linéaire est au cœur du fonctionnement des qubits des ordinateurs quantiques. Très souvent, les représentations mathématiques de la physique quantique dépassent les interprétations physiques.

Nombre de ces scientifiques ont laissé une trace mémorable connue des connaisseurs voire même du grand public. On ne présente plus le célébrissime chat de Schrödinger et le principe d'indétermination d'Heisenberg... même si les détails sont différents des images d'Epinal les concernant. Comme souvent, des centaines d'autres contributeurs moins connus ont aussi apporté leur pierre à l'édifice et il faut aussi leur rendre hommage. Comme la vie en général, c'est aussi une grande course de relais.

Vous n'y trouverez pas d'inventeur à la Roland Moreno ou d'entrepreneurs sauce Steve Jobs ou Elon Musk, même si les fondateurs de startups telles que le Canadien D-Wave font partie des pionniers entrepreneurs de ce secteur d'activité naissant.

Ce côté collectif de la mécanique quantique est incarné par l'épisode mythique du cinquième **Congrès de Physique Solvay de 1927**, tenu à l'Institut de physiologie de Bruxelles. La photo associée qui immortalise l'épisode a été coloriée après coup.



Ce congrès rassemblait les plus grands mathématiciens et physiciens de l'époque dont presque tous les pères historiques de la mécanique quantique avec MaxPlanck, Albert Einstein, Niels Bohr, Louis de Broglie, Erwin Schrödinger, Max Born, Werner Heisenberg et Paul Dirac[16].

[16] Que des pères et pas de mère ! Marie Curie était bien présente mais n'était pas une spécialiste de la physique quantique.

17 des 29 participants ont obtenu un Prix Nobel, dont 6 en étaient déjà détenteurs au moment de la réunion (noms soulignés en vert, les autres étant en bleu). C'était probablement l'un des plus gros concentrés de jus de cervelle au mètre carré de l'histoire de l'humanité !

Les congrès Solvay ont lieu tous les 3 à 4 ans depuis leur création en 1911 par l'entrepreneur et chimiste **Ernest Solvay**. Ils sont thématisés. Celui de 1927 portait sur les électrons et les photons, qui sont au cœur de la mécanique quantique. Un congrès sur deux portait sur la mécanique quantique, le dernier du genre ayant eu lieu en 2011. La 27ème et édition la plus récente se tenait en 2017.

Voici donc quelques-uns de ces protagonistes et leurs grandes contributions associées avec au passage, des indications de qui a influencé qui, les grandes contributions étant généralement organisées par ordre chronologique. Pour certains comme Maxwell, Schrödinger et Dirac, je rentre dans le détail des équations dont ils sont à l'origine.

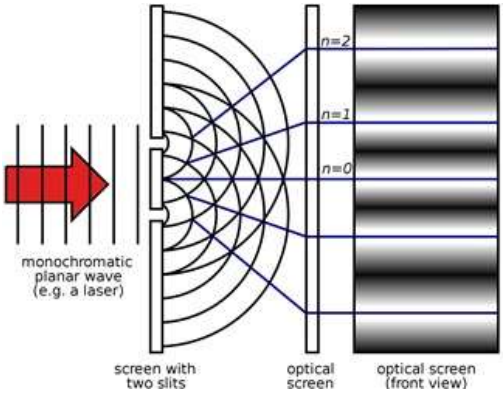
Précurseurs

Nous commençons avec les physiciens et mathématiciens des XVIIIe et XIXe siècles qui ont posé des jalons scientifiques qui ont permis à leurs successeurs du XXe siècle de formaliser les bases de la physique quantique. Notez que je n'indique pas toujours la source des schémas. Ils font partie d'explications scientifiques courantes qui font maintenant partie du domaine public. La chronologie suit à peu près celle des grandes découvertes.

C'est parti pour ce tour historique !

Thomas Young (1773-1829, Anglais) est un des grands polymaths de la science, s'investissant tour à tour dans l'optique, la médecine, la linguistique, l'égyptologie et la musique. Il détermine surtout la nature ondulatoire de la lumière qu'il prouve avec l'expérience des doubles fentes dites de Young vers 1806, illustrée *ci-dessous*. Elle génère des interférences qui créent une illumination alternant lumière et absence de lumière liée à la nature ondulatoire de la lumière.

Cette expérience est l'un des éléments qui conduit bien plus tard à la création de la théorie des ondes électromagnétiques par James Maxwell. Son expérience a été ensuite rééditée avec des électrons, en 1927, avec un résultat voisin, illustrant la dualité onde-particule de l'électron, élaborée par le Français Louis de Broglie en 1924. Thomas Young a aussi travaillé sur les principes de la réfraction et de la vision trichromatique humaine ainsi que dans la mécanique des fluides et dans la notion de capillarité et de tension de surface.



Thomas Young était aussi égyptologue. Il a contribué à l'étude des hiéroglyphes de la fameuse pierre de Rosette, qui a ensuite servi à Jean-François Champollion.

William Rowan Hamilton (1805-1865, Irlandais) est un mathématicien et astronome. Vers 1827, il invente de nouvelles formulations mathématiques des lois de la physique qui intègrent l'électromagnétisme. En mécanique quantique, on parle souvent d'Hamiltonien ou de fonction hamiltonienne. Il s'agit d'opérateurs servant à décrire l'énergie totale d'un système de particules élémentaires (détails) comprenant son énergie cinétique et son énergie potentielle.

L'équation de Schrödinger créée en 1926 décrit l'évolution dans le temps d'un hamiltonien. Ce concept est aussi utilisé dans les ordinateurs quantiques à recuit quantique de D-Wave que nous aurons l'occasion de décrire dans le détail dans cet ebook.

Niels Henrik Abel (1802-1829, Norvégien) est un mathématicien à l'origine de ce que l'on appelle les groupes abéliens. Ses travaux portent sur la semi-convergence des séries numériques, des suites et séries de fonctions, les critères de convergence d'intégrale généralisée, sur la notion d'intégrale elliptique et sur la résolution d'équations algébriques. Il est mort à 26 ans de la tuberculose ! C'est bien dommage pour un tel génie !

Avec William Rowan Hamilton, Charles Hermite et Emmy Noether, c'est l'un des fournisseurs des fondements mathématiques utilisés dans la mécanique quantique. L'appellation "abéliens" et "non abéliens" est associée aux anyons, les quasi-particules qui sont la base de l'informatique quantique topologique. Pourquoi ces concepts de mécanique quantiques inventés bien avant sa mort font-ils référence à ce mathématicien ? Notamment parce que la distinction entre abéliens et non abéliens est lié à leur représentation mathématique commutative (= "abélien", quand A*B = B*A) ou non commutative ("non abélien", lorsque A*B n'est pas égal à B*A) ! Les opérations non commutatives les plus courantes sont les multiplications de matrices. Ainsi la multiplication d'une matrice (p x q) x (q x p) donnera une matrice (p x p) alors que dans l'autre sens, (q x p) x (p x q) générera une matrice (q x q), q et p étant ici des nombres de lignes et/ou colonnes.

La non-commutativité est souvent rencontrée dans le calcul quantique. Ainsi, l'ordre dans lequel on mesure l'état des qubits influe sur les résultats sur les opérateurs utilisés sont non commutatifs. C'est même une technique à part entière qui est exploitée dans le Measurement Based Quantum Computing (MBQC) que nous aurons l'occasion de décrire.

Charles Hermite (1822-1901, Français) est un mathématicien très prolixe, qui a fait avancer la théorie des nombres, les formes quadratiques, la théorie des invariants, les polynômes orthogonaux, les fonctions elliptiques et l'algèbre. Ses principaux travaux sont concentrés sur la période 1848-1860. On lui doit la notion d'hermitiens, une notation mathématique utilisée en mécanique quantique et l'explication va s'arrêter là car après, c'est bien trop compliqué.

Les matrices hermitiennes sont des matrices composées de nombres réels dans la diagonale et pouvant être complexes dans le reste, et qui sont égales à leur transconjuguée. A savoir, leur transposée dont on a inversé la valeur des nombres complexes (i devient –i et réciproquement).

Voir l'exemple *ci-contre*. Les matrices décrivant les opérations des portes quantiques dans les ordinateurs quantiques sont des matrices hermitiennes. Elles ne changent pas la longueur des vecteurs qui sont transformés par ces matrices.

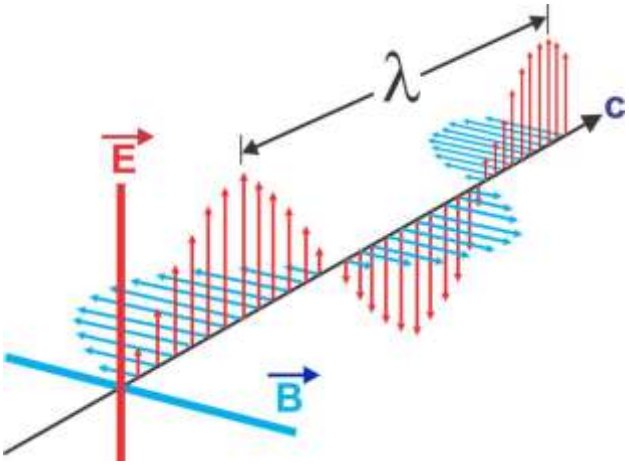
$$A = \begin{pmatrix} 3 & i & -5i \\ -i & -2 & 5 \\ 5i & 5 & 10 \end{pmatrix}$$ est une matrice hermitienne :

$$\overline{A} = \begin{pmatrix} 3 & -i & 5i \\ i & -2 & 5 \\ -5i & 5 & 10 \end{pmatrix} \text{ et } (\overline{A})^T = \begin{pmatrix} 3 & i & -5i \\ -i & -2 & 5 \\ 5i & 5 & 10 \end{pmatrix} = A$$

James Clerck Maxwell (1831-1879, Ecossais) est le créateur à partir de 1865 de la théorie des champs électromagnétiques, associant un champ électrique et un champ magnétique orthogonaux au sens de propagation des ondes comme dans le schéma *ci-dessous*, et se déplaçant à la vitesse de la lumière. Cette théorie explique les interactions entre lumière et lumière comme la réflexion, la diffraction, la réfraction et les phénomènes d'interférences.

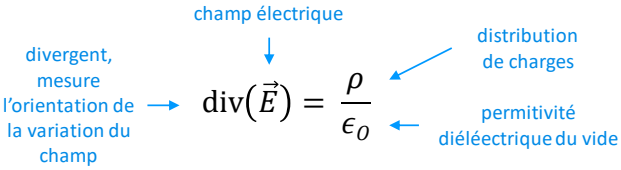
La recherche étant un processus très incrémental, le travail de Maxwell s'appuyait et améliorait le formalisme de travaux de ses prédécesseurs et notamment Faraday, Gauss et Ampère.

Les équations de Maxwell illustrent le fait que lorsqu'ils sont constants, les champs électriques et magnétiques sont indépendants et en régime variable, ils deviennent interdépendants, l'un générant l'autre et réciproquement, d'où la notion d'ondes et de champs électromagnétiques. Dans les équations de Maxwell, le champ électromagnétique est maintenant représenté par un tenseur électromagnétique, une matrice 4x4 dont la diagonale est nulle et dont la moitié des composantes décrivent le champ électrique l'autre le champ magnétique. Ces quatre dimensions correspondent à l'espace (3) et au temps (1).



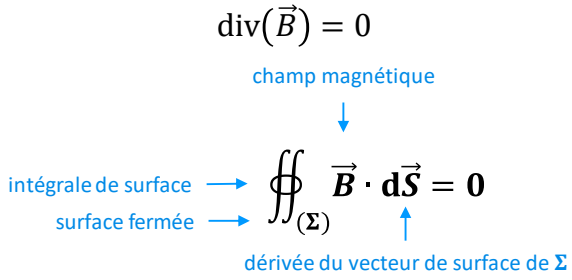
On décompte en fait quatre grandes équations de Maxwell[17] :

- L'équation de **Maxwell-Gauss** qui décrit comment un champ électrique est généré par des charges électriques. A chaque point dans l'espace, le champ électrique est orienté des charges positives vers les charges négatives dans des directions qui dépendent de la position des charges dans l'espace.



équation de **Maxwell-Gauss** qui décrit le champ électrique généré par des charges électriques

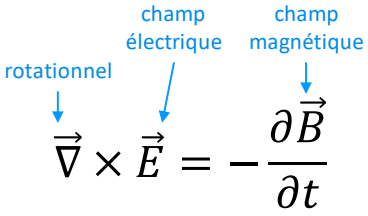
- L'équation de **Maxwell-flux** énonce qu'un champ magnétique est toujours engendré par un dipôle regroupant une charge positive et une charge négative reliées entre elles et inséparables. Mathématiquement, cela se traduit par le fait que la divergence du champ magnétique est nulle et qu'il n'existe pas de monopôle magnétique.



A savoir qu'il n'y a pas de ligne de champ magnétique qui s'échappe à l'infini comme c'est le cas avec un champ électrique.

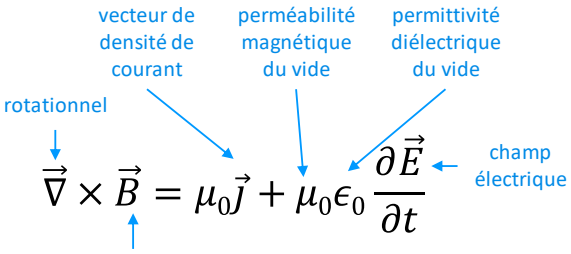
[17] Voir ces explications bien faites et visuelles des équations de Maxwell : A plain explanation of Maxwell's equations.

- L'équation de **Maxwell-Faraday** décrit comment la variation d'un champ magnétique induit un champ électrique. C'est le principe de fonctionnement des alternateurs électriques. L'opérateur mathématique rotationnel utilisant un signe nabla correspond à une opération vectorielle différentielle. Il y est égal à la dérivée première du champ magnétique sur le temps.



équation de **Maxwell-Faraday** qui relie le champ magnétique au champ électrique

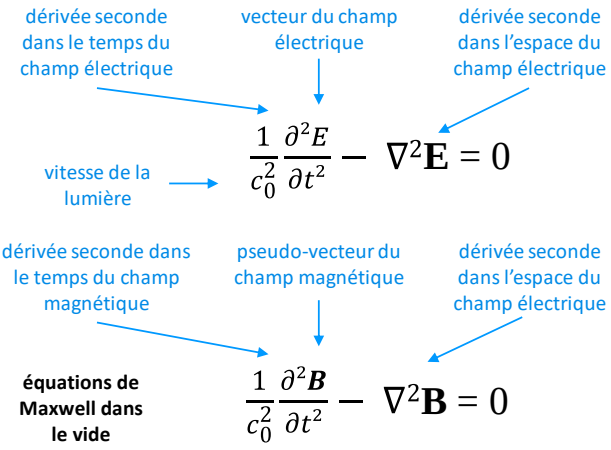
- L'équation de **Maxwell-Ampère** énonce à l'envers que les champs magnétiques sont générés par les courants électriques via le théorème d'Ampère ou par la variation d'un champ électrique. Cette interdépendance entre champs magnétiques et champs électriques variables explique la circulation d'ondes électromagnétiques auto-entretenues. On retrouve à gauche le rotationnel du champ magnétique.



équation de **Maxwell-Ampère** qui relie le champ électrique au champ magnétique

Nous sommes dans le même cas de représentation qu'avec l'équation de Schrödinger que nous verrons plus loin : les équations de Maxwell ont plusieurs représentations possibles, qui troublent la compréhension pour le néophyte. Les équations de Maxwell sont à « géométrie variable ». Maxwell a d'abord publié vingt équations à vingt inconnues en 1865.

En 1873, il les réduisait à huit équations. En 1884, Oliver Heaviside et Willard Gibbs passaient aux quatre équations vectorielles aux dérivées partielles déjà évoquées plus haut.



équations de Maxwell dans le vide

Ces quatre équations vectorielles se réduisent à deux équations tensorielles pour des ondes électromagnétiques propagées dans le vide (*ci-dessus à droite*). La non-interaction avec d'autres éléments explique l'indépendance dans cette équation entre les champs électriques et magnétiques.

Les ondes électromagnétiques n'ont été mises en évidence expérimentalement qu'après le décès de Maxwell, par **Heinrich Hertz** (1857-1894) entre 1886 et 1988. Ce dernier a aussi découvert l'effet photoélectrique en 1886.

La description des ondes électromagnétiques par Maxwell va avoir un impact phénoménal dans les télécommunications électromagnétiques et dans l'optronique. Elle servira de fondements à la mécanique quantique élaborée par Max Planck en 1900.

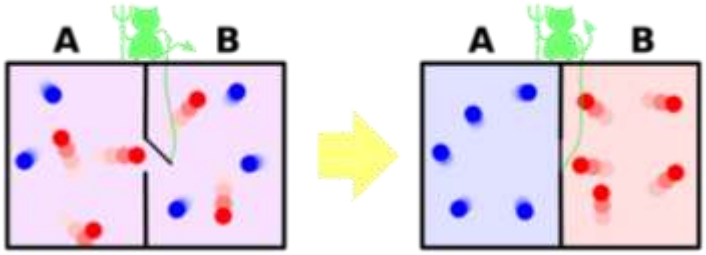
Il est aussi à l'origine de la loi statistique de distribution des gaz **Maxwell–Boltzmann**. Elle modélise la distribution des vitesses des particules d'un gaz parfait. Elle ne tient pas compte des interactions entre particules et n'est pas applicable dans les conditions extrêmes, comme à très basse température. Elle est notamment remplacée par la statistique des **condensats de Bose-Einstein** pour les bosons (particules à spin entier comme l'hélium 4, qui peuvent cohabiter dans un même état quantique et niveau d'énergie).

Elle l'est aussi par la statistique de **Fermi-Dirac** pour les fermions (particules à spins demi-entier comme les électrons ou l'hélium 3, qui ne peuvent pas cohabiter dans un même état quantique et d'énergie).

Maxwell est le concepteur en 1867 de l'expérience de pensée dite du **démon de Maxwell** qui rendrait possible la réversibilité de processus d'échanges thermodynamiques et invaliderait le second principe de la thermodynamique[18].

Elle repose sur deux boîtes contenant deux gaz différents où bien un gaz à deux températures différentes sont séparées par un trou et une obturation contrôlée par un « démon ». Lorsque l'on ouvre la porte, les gaz se mélangent.

Une fois mélangé (*à gauche, source Wikipedia*), le démon contrôlerait celles des molécules pouvant aller d'une boîte à l'autre, tirant parti de l'énergie cinétique naturelle des gaz. Cela permettrait en théorie et au bout d'un certain temps de revenir à l'équilibre antérieur dans une situation de non équilibre (*à droite*).



Il a fallu attendre plusieurs décennies pour trouver la faille, notamment via Léo Szilard en 1929 et Léon Brillouin en 1948. Au départ, l'explication était que le démon a besoin de dépenser de l'énergie pour obtenir de l'information sur l'état des molécules de gaz pour les trier. Il y a donc consommation d'énergie pour modifier l'équilibre stable obtenu pour mélanger les gaz. L'explication « à jour » est quelque peu différente. Le coût énergétique provient de la remise à zéro de la mémoire du démon, qui consiste ultimement en un seul bit d'information[19].

Tout ceci a eu des retombées sur la notion de valeur énergétique de l'information et conduit, bien plus tard, à la création du champ de la thermodynamique de l'information, c'est-à-dire de l'étude des empreintes énergétiques et entropiques de l'information, notamment en calcul quantique. Ce champ a ensuite été investi par Rolf Landauer, connu pour son étude de la génération de chaleur des circuits de gestion de l'information irréversibles et par Charles Bennett et Gilles Brassard, les coinventeurs du protocole BB84 dont nous reparlerons, puis par Paul Benioff, à l'origine de l'idée du calcul quantique.

On doit enfin à Maxwell la création de pistes de création de la photographie en couleur s'appuyant sur les trois couleurs primaires de la vision humaine.

Ludwig Boltzmann (1844-1906, Autrichien) est un physicien, père de la physique statistique, défenseur de l'existence des atomes face une forte opposition des scientifiques jusqu'au début du XX^{e} siècle, et créateur d'équations décrivant la dynamique des fluides et des gaz en 1872. Il est aussi à l'origine de l'interprétation probabiliste du second principe de la thermodynamique qui établit l'irréversibilité des phénomènes physiques, en particulier lors des échanges thermiques.

---

[18] Voir l'explication du démon de Maxwell dans Démon de Maxwell, FuturaScience.

[19] Voici l'explication détaillée par Alexia Auffèves (CNRS) : on peut comprendre l'opération de reset d'un bit de mémoire en considérant un moteur de Carnot ultime, constitué d'une seule particule qui peut se trouver à gauche ou à droite d'un certain volume thermostaté. Gauche = 0, Droite = 1. Il y a deux opérations possibles : la compression. La particule se trouve initialement à gauche ou à droite du volume qui la contient (on ne sait pas) et on comprime ledit volume pour qu'à la fin elle se trouve nécessairement à gauche. C'est une opération d'initialisation où le bit est remis dans l'état 0. Comme pour toute compression, il faut payer, ici dans ce cas ultime, le travail à dépenser est kT log 2. C'est le fameux travail de Landauer, qui pose une borne énergétique à toutes les opérations logiquement irréversibles. La seconde opération est la détente. Au début, on sait que la particule se trouve à gauche ou à droite. On positionne une paroi, une poulie avec une masse au bout et on laisse la détente s'opérer tout en extrayant un travail élémentaire équivalent à kT log 2. C'est une machine de Szilard. Ces deux manipulations ont été réalisées expérimentalement en 2011 à l'ENS Lyon. Elles montrent l'empreinte énergétique de l'information et constituent la solution ultime au paradoxe du démon de Maxwell.

L'irréversibilité est associée à la création d'entropie. Boltzmann s'est essayé à la philosophie alors qu'il défendait l'existence des atomes. Dépressif, il est mort en se suicidant !

Henri Poincaré (1854-1912, Français) est un mathématicien et physicien, précurseur de la théorie de la relativité et des ondes gravitationnelles. On lui doit une fonction probabiliste qui porte son nom et qui est l'équivalent en optique de la représentation de Bloch que nous verrons plus tard qui décrit mathématiquement l'état des qubits. Il est aussi l'auteur de la conjecture mathématique qui porte son nom et qui a été démontrée en 2003 par le Russe Grigori Perlman.

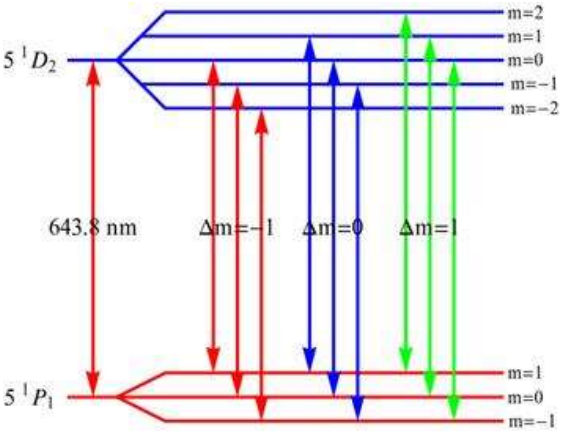
Elle est relative à l'existence de sphères dans des espaces quadri-dimensionnels. C'était un cousin germain de Raymond Poincaré (1860-1934), président de la République Française pendant la première guerre mondiale.

David Hilbert (1862-1943, Allemand) est un mathématicien prolifique à qui l'on doit à la fin du 19e siècle les fondamentaux mathématiques qui sont exploités dans la physique quantique, et notamment ses espaces dits de Hilbert utilisant des vecteurs permettant de mesurer des longueurs, des angles et de définir des orthogonalités. On les utilise pour représenter l'état des qubits avec des vecteurs et nombres complexes.

Ses travaux n'avaient cependant rien à voir à l'origine avec la mécanique quantique qui n'était alors pas encore formulée.

Pieter Zeeman (1865-1943, Hollandais) est un physicien, prix Nobel de physique en 1902 avec Hendrik Lorentz pour la découverte de l'effet qui porte son nom entre 1896 et 1897. L'effet Zeeman se manifeste lorsque des atomes excités sont soumis à un champ magnétique. Cela affecte leur spectre d'émission ou d'absorption qui voit ses raies spectrales séparées en plusieurs raies. L'effet s'observe par une spectroscopie qui décompose les rayons lumineux avec un prisme.

Les raies spectrales se décomposent en un nombre pair (effet Zeeman normal) ou impair de raies (effet anormal). La décomposition dépend de l'intensité du champ magnétique traversé.

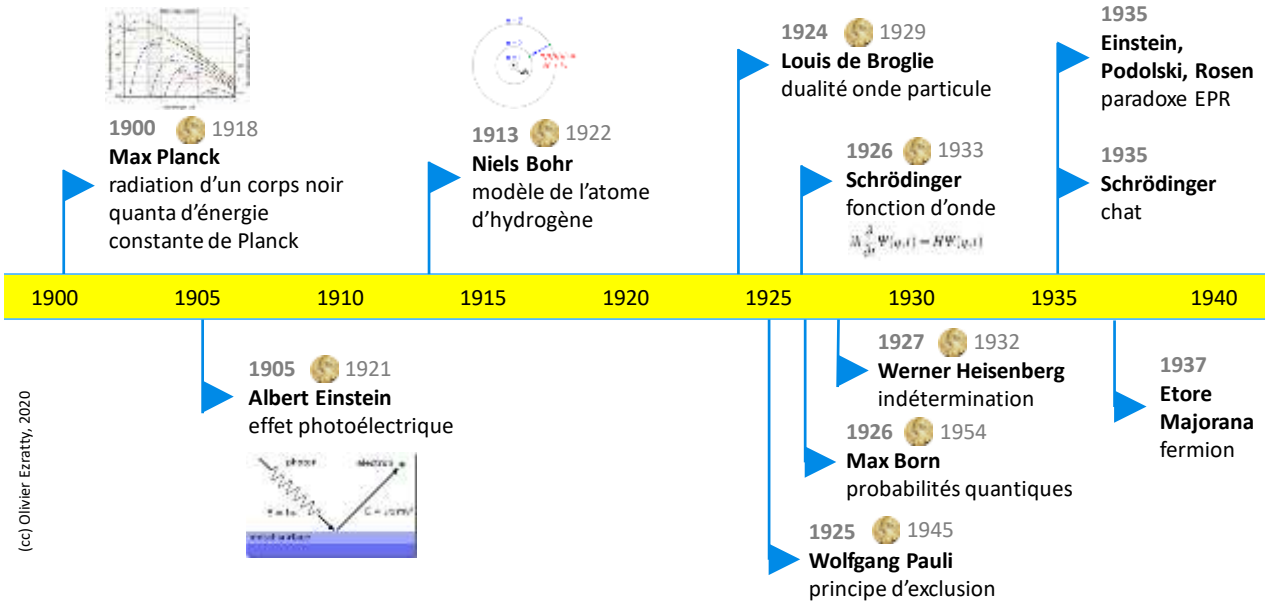


Elle s'accompagne d'une polarisation de la lumière générée dont la nature et l'intensité dépendent de l'orientation du champ magnétique relativement au faisceau de lumière comme le montre l'illustration Wikipedia *ci-contre*. L'effet Zeeman s'explique par le principe d'exclusion de Pauli, élaboré en 1925, et par des transitions de niveau d'énergie d'électrons d'une même couche et ayant des moments magnétiques différents. En astronomie, la mesure de l'effet Zeeman permet d'en déduire les champs magnétiques intenses dans les étoiles ainsi que dans la Voie Lactée. Elle est aussi exploitée dans les spectroscopies de résonance magnétique (nucléaire et électronique) dans les scanners IRM.

Hendrik Antoon Lorentz (1853-1928, Pays-Bas) était un physicien qui a travaillé sur la nature de la lumière et la constitution de la matière. Il fait le lien entre la lumière et les équations de l'électromagnétisme de Maxwell. On lui doit les transformations de Lorentz qui expliquent les résultats des expériences de Michelson-Morley entre 1981 et 1887 qui montraient le caractère immuable de la vitesse de la lumière, quel que soit le référentiel. Avec Henri Poincaré, il est l'un des contributeurs clés de la théorie de la relativité formalisée par Albert Einstein.

Fondateurs

La mécanique quantique a vu le jour avec Max Planck, puis a pris forme sur trois décennies et demies, en gros jusqu'en 1935 avec les contributions successives d'Einstein, Bohr, De Broglie, Born, Schrödinger, Heisenberg et Dirac pour ne prendre que les plus connues.

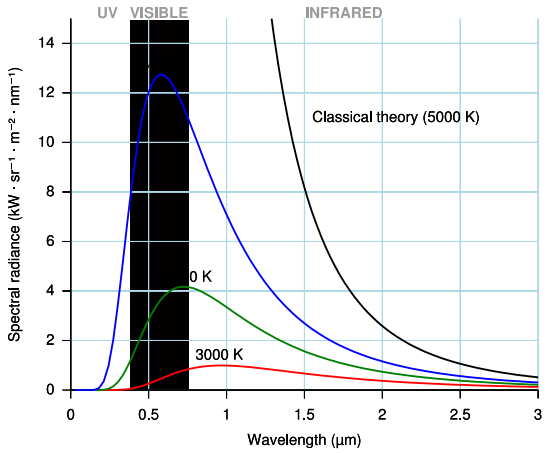


Voici donc un tour des grands physiciens et mathématiciens qui ont établi les bases de la physique quantique. Ce sont tous des européens qui vont pour une bonne part s'expatrier aux USA avant la seconde guerre mondiale[20].

[20] Le déroulé de cette histoire est bien raconté, formules mathématiques à l'appui par Didier Robert de l'Université de Nantes dans Des mathématiques dans la mécanique quantiques, 2014 (86 slides).

Max Planck (1858-1947, Allemand) est un physicien, initialement spécialisé dans la thermodynamique. En 1900, il développe la théorie des quantas, émettant l'hypothèse que les échanges d'énergie entre lumière et matière se font par des quanta discrets. Ce rayonnement n'est pas continu mais varie par seuils, par paliers d'une certaine quantité d'énergie, d'où le terme de "quanta" et de "physique quantique". Sa théorie lui permet d'expliquer pour la première fois l'énigmatique rayonnement du corps noir, un corps qui absorbe tout rayonnement magnétique incident.

Les exemples de corps noir sont une cavité fermée comme un four, un métal chauffé qui devient rouge, orangé, puis blanc en fonction de la température, ou une étoile comme le Soleil. Le spectre d'ondes électromagnétiques émis par un corps noir dépend uniquement de sa température selon le schéma *ci-contre* et pas du tout de sa matière. Plus la température est élevée, plus le spectre électromagnétique émis par le corps noir glisse vers les fréquences élevées, donc vers le violet et l'ultraviolet avec le niveau de la température.



Max Planck élabore une formule décrivant le spectre électromagnétique du corps noir qui est rapidement vérifiées par l'expérience. Elle permettait de résoudre l'énigme de la catastrophe ultraviolette, expression de Paul Ehrenfest liée à l'analyse du rayonnement du corp noir avec les équations de l'époque et qui faisaient diverger à la hausse l'énergie générée par un tel corps dans l'ultraviolet. Max Planck est ainsi l'un des premiers à formuler les bases de la mécanique quantique, mais de manière incomplète[21]. Il obtient le prix Nobel de physique en 1918.

On lui doit également la constante qui porte son nom (h) et qui est exploitée dans son explication du rayonnement d'un corps noir. Cette constante fut ensuite utilisée dans l'équation selon laquelle l'énergie du changement d'état d'un atome est égale à la fréquence du rayonnement multipliée par la constante de Planck.

Lorsqu'un électron change d'orbite dans un atome d'hydrogène, cela émet ou absorbe une onde électromagnétique dont l'énergie est égale à la constante de Planck multipliée par la fréquence lumineuse émise. Malgré les nombreuses validations expérimentales réalisées quelques années plus tard, Max Planck exprima jusqu'à sa mort des doutes sur les principes même de la mécanique quantique !

Planck est aussi à l'origine de deux constantes infinitésimales : le temps ou bien durée de Planck qui est $t_P=10^{-44}$s et la longueur de Planck qui est $l_P=1{,}616255*10^{-35}$m. Elles sont reliées entre elles par les équations *ci-dessous*. Le temps de Planck est celui qui serait nécessaire à un photon pour parcourir la distance de Planck.

En gros, ce sont les dimensions de l'infiniment petit en-dessous desquelles toute observation est impossible avec les connaissances actuelles de la physique.

$$t_P = \sqrt{\frac{\hbar G}{2\pi c^5}} = \sqrt{\frac{\hbar G}{c^5}} = \frac{\ell_P}{c}$$

$$\ell_P = \sqrt{\frac{\hbar G}{c^3}}$$

$\hbar$ est la constante de Planck réduite ;
G est la constante gravitationnelle ;
c est la vitesse de la lumière dans le vide ;
ℓ_P est la longueur de Planck.

La longueur de Planck l_P est tellement petite qu'un photon utilisé pour l'observer aurait une fréquence et une énergie tellement élevées qu'il générerait un trou noir autour de lui et serait donc inobservable !

[21] Etienne Klein raconte bien le cheminement intellectuel de Max Planck dans la vidéo "La naissance de la physique quantique" (2016).

En cosmologie classique d'aujourd'hui, le mur de Planck correspond dans l'histoire de l'expansion de l'Univers au moment où 10^{-43}s après le big bang, sa taille aurait été de 10^{-35}m, soient respectivement la durée et la longueur de Planck.

Albert Einstein (1879-1955, Allemand puis Américain) est un physicien que l'on ne présente plus, prix Nobel en 1921 pour son interprétation de l'effet photoélectrique en 1905, qui est devenue l'un des fondements de la mécanique quantique après Planck et avant De Broglie, Heisenberg et Schrödinger. Dans On a Heuristic Viewpoint Concerning the Production and Transformation of Light, il détermine que les quantas de Planck sont en fait des photons.

Ce sont des quantités discrètes d'énergie lumineuse dont l'énergie est égale à la fréquence électromagnétique des ondes transportées multipliée par la constante de Planck. De manière symétrique à ce que fera plus tard Louis De Broglie avec l'électron, il émet l'hypothèse qu'un photon se comporte à la fois comme une onde et comme un corpuscule. Il réconciliait ainsi les théories corpusculaires de **René Descartes** (1596-1650, Français, en 1633) et d'**Issac Newton** (1642-1726, Anglais, en 1704) avec celles à base d'ondes de **Christiaan Huygens** (1629-1695, Hollandais, en 1778) pour décrire la lumière.

L'effet photoélectrique est utilisé dans les cellules de panneaux solaires photovoltaïques. Il explique aussi la photosynthèse dans les plantes, qui permet la production de glucose.

Il correspond à la capacité d'un photon à déloger un électron d'une orbite généralement intérieure d'un atome et de créer du courant électrique[22].

En plus des travaux de Max Planck sur le rayonnement du corps noir, l'interprétation d'Einstein s'appuyait sur les travaux antérieurs de **Heinrich Hertz** (1857-1894, Allemand) qui découvrit en 1887 que la lumière peut arracher un électron à du métal et de **Philipp Lenard** (1862-1947, Allemand) qui étudia en 1902 l'effet photoélectrique et détermina qu'il ne se déclenche qu'à partir d'une certaine fréquence de la lumière projetée. Ce dernier obtint le prix Nobel de physique en 1905. Devenu fervent Nazi et opposé à Einstein par rivalité scientifique puis par antisémitisme virulent, il est passé dans les oubliettes de l'Histoire.

Les équations de l'effet photoélectrique d'Einstein ont été vérifiées ensuite par les expériences de **Robert Andrews Milikan** (1868-1953, Américain) entre 1909 et 1914. Elles lui permirent de mesurer la charge électrique d'un seul électron. Cela valut le prix Nobel de physique à ce dernier en 1923.

Bien entendu, Einstein est aussi à l'origine de la théorie de la relativité restreinte et générale qui couvrent plutôt l'infiniment grand alors que la mécanique quantique touche l'infiniment petit. Aussi curieux que cela puisse paraître, Einstein n'a jamais obtenu le prix Nobel pour ses travaux sur la relativité malgré son impact considérable sur la physique et l'astronomie. En cause, entre autres, les questions de paternité de cette théorie par rapport aux travaux antérieurs de **Heindrick Lorentz** et

[22] Les couches d'électrons des atomes sont numérotées de 1 à N, leur nombre quantique. On démarre aussi la numérotation par K (première couche proche du noyau avec un maximum de 2 électrons) puis L (8 électrons au maximum), M (avec un maximum de 18 électrons mais en pratique 8), etc. L'effet photoélectrique concerne essentiellement les couches K et L. L'électron éjecté est ensuite remplacé par un électron d'orbite extérieure, ce qui génère un nouveau photon, dans les rayons X ou en fluorescence, selon l'énergie du photon incident. Cela émet alors un photon de rayon X du fait du différentiel d'énergie entre couches électroniques ou bien un électron dit « Auger » du nom de Pierre Auger. Ce phénomène a été découvert autour de 1923 par ce dernier et par Lise Meitner. Une autre variante de l'effet photoélectrique est l'effet Compton, lorsque l'énergie élevée d'un photon incident dans les rayons gamma va dégager un électron de la couche de valence et générer un autre photon. Enfin, lorsque l'énergie du photon incident est encore plus élevée, l'interaction a lieu au niveau du noyau de l'atome visé et génère un électron et un positron.

Henri Poincaré ainsi que la contribution de son ancien professeur **Hermann Minkosvki** (1864-1909, Allemand) qui créa la notion d'espace-temps quadri-dimensionnelle en 1908.

En 1925, Einstein prédit un comportement particulier de la matière, le condensat de Bose-Einstein qui se manifeste lorsque l'on refroidit des gaz à très basse température. Les atomes se trouvent alors dans un état quantique d'énergie minimale présentant des propriétés physiques particulières. C'est le cas de l'hélium superfluide, découvert en 1938, et qui, à très basse température, n'a plus de viscosité, à savoir qu'il peut se déplacer sans dissiper d'énergie. Bose est le nom du chercheur indien **Satyendranath Bose** (1894-1974) avec qui Einstein avait travaillé pendant les années 1920 et à qui l'on doit les "bosons", qui vérifient les caractéristiques des condensats de Bose-Einstein.

Les bosons comprennent les particules élémentaires sans masse telles que les photons et les gluons mais aussi certains atomes comme le deutérium ou l'Hélium 4 ainsi que certaines quasi-particules comme les paires d'électrons supraconducteurs que sont les paires de Cooper. Nous verrons un peu plus loin que c'est une question de somme de spin de ces particules qui détermine le fait qu'il s'agit de bosons par opposition aux fermions.

Albert Einstein a aussi entretenu le débat philosophico-scientifique sur la mécanique quantique, principalement face à Niels Bohr. Il portait sur le fait que la mécanique quantique ne semblait pas décrire complètement le monde physique.

Einstein voulait trouver une interprétation réaliste de la physique. Il ne pouvait se satisfaire d'une description probabiliste de l'état des électrons et autres quantum. Il n'adhérait pas à l'interprétation de la physique quantique selon laquelle l'observateur et la mesure « font » le réel alors qu'il pensait que le réel existe indépendamment de la mesure.

Le débat entre Albert Einstein et Niels Bohr se charpentait autour de diverses expériences de pensées culminant lors du Congrès Solvay de 1927 et portant sur la question du déterminisme. Le point d'orgue se situe néanmoins en 1935 avec la publication du fameux **paradoxe EPR**, du nom de ses auteurs Albert Einstein, Boris Podolsky et Nathan Rosen.

Le papier posait la question de l'incomplétude de la mécanique quantique de l'époque[23]. Il cherchait à expliquer la non-localité des quanta permettant une action instantanée à distance entre deux quanta via l'intrication. Cette non-localité était la conséquence de la fonction d'onde de Schrödinger[24]. Elle n'était pas encore observée physiquement en 1935. Pour les auteurs, la théorie quantique à base de la fonction d'onde de Schrödinger était soit incomplète, soit deux quantum ne pouvaient pas être synchronisés instantanément à distance. Pour eux, une théorie physique est complète si chaque composante de la réalité a une contrepartie dans la théorie qui permet d'en prédire le comportement, comme un accord à la source (des quanta intriqués) se modélisant avec des variables cachées. Ce qui sous-tend la notion de déterminisme, un principe absent de la fonction d'onde de Schrödinger.

Le papier EPR se termine en queue de poisson en indiquant qu'il devrait être possible de bâtir une théorie complète de la mécanique quantique[25]. On a ensuite souvent attribué à Einstein l'idée qu'il existait des variables cachées. Il semble cependant qu'il n'en ait jamais fait état dans ses écrits malgré ce qu'affirmait John Bell qui interprétait un peu trop rapidement la position d'Einstein.

---

[23] Voir Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, par Albert, Einstein, Boris Podolsky et Nathan Rosen 1935 (4 pages).

[24] Le repère d'Einstein était la physique classique et relativiste qui agissait localement. La gravité est locale et se transmet à la vitesse de la lumière. Toutes les théories physiques d'avant la physique quantique étaient locales ou EPR-locales. Les actions à distance intégraient toutes un délai, couplé généralement à une atténuation avec la distance comme pour la gravité.

[25] L'article du New York Times de 1935 était dû à une « fuite » provoquée par Boris Podolsky, le plus jeune des 3 d'EPR.

L'explication de l'intrication par des « variables cachées » provient plutôt de Louis de Broglie avec son hypothèse d'onde pilote élaborée en 1927[26], une idée poursuivie ensuite par David Bohm dans les années 1950. Avec ses « inégalités », l'Américain John Stewart Bell démontrait en 1964 que l'existence de telles variables cachées était incompatible avec les principes de la mécanique quantique.


The New York Times.

NEW YORK, SATURDAY, MAY 4, 1935. TWO CENTS

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

L'expérience d'Alain Aspect de 1982 portant sur l'intrication de photons a confirmé cela.

Comble de l'Histoire, Einstein n'a pas réussi avant sa mort à parfaire sa théorie de la relativité générale qui était aussi incomplète que ne l'était pour lui la mécanique quantique. Il voulait notamment réconcilier la mécanique quantique et la gravité.

Attention cependant aux images d'Epinal ! Il se dit et s'écrit bien trop souvent qu'Einstein était « contre » la mécanique quantique ou « n'y croyait pas ». Ce n'est pas tout à fait cela puisqu'il en était à l'origine avec Max Planck. Il remettait d'abord en cause le principe d'indétermination en 1927 et 1930, puis trouvait que la théorie était incomplète pour expliquer l'intrication, avec le paradoxe EPR de 1935 et enfin, il s'opposait à l'absence de réalisme de la théorie quantique. Cette incomplétude subsiste plus de 80 ans après, car on n'explique toujours pas physiquement l'origine de l'intrication dans certaines conditions, notamment à longue distance. On se contente de l'observer physiquement et de la décrire mathématiquement[27].

Cela reste un débat ouvert aujourd'hui puisque l'on continue à cogiter sur les différentes interprétations possibles de la physique quantique. Cela fait partie du champ de la philosophie de la physique quantique que nous couvrons plus loin dans cet ebook.

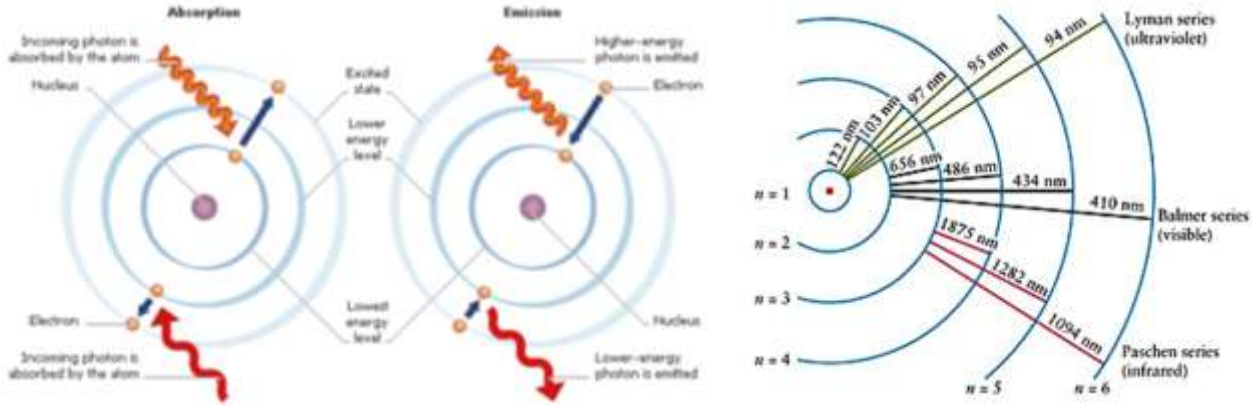
Niels Bohr (1885-1962, Danois) est un physicien, prix Nobel de physique en 1922, à l'origine de la création en 1913 d'un modèle descriptif de l'atome d'hydrogène avec son noyau fait d'un proton et un électron tournant autour du noyau sur des orbites précises correspondant à un niveau d'énergie cinétique des électrons multiple de $h/2\pi$, h étant la constante de Planck et n = 1, 2, 3, etc. Ce modèle permettait d'expliquer les raies spectrales observées dans l'analyse de l'énergie de l'hydrogène.

Ces raies avaient été notamment observées dans les expériences de **Johann Balmer** (1825-1898) de 1885, de **Theodore Lyman** (1874-1954) de 1906 et de **Friedrich Paschen** (1865-1947) en 1908.

Niels Bohr utilisait comme base les travaux de l'Anglais **Ernest Rutherford** (1871-1937) qui découvrit en 1911 la structure des atomes avec leur noyau chargé positivement, grâce à ses protons, et leurs électrons tournant autour du noyau. Ce dernier, chez qui Niels Bohr faisait son post-doc en 1911, s'appuyait lui-même sur le Japonais **Hantaro Nagaoka** (1865-1950) qui prédit en 1903 la structure des atomes avec un noyau chargé positivement et des électrons chargés négativement tournant autour, dénommée « modèle saturnien ».

[26] Voir Albert Einstein, David Bohm et Louis de Broglie sur les variables cachées de la mécanique quantique par Michel Paty, 2007 (29 pages) qui remet bien les pendules à l'heure sur la position d'Albert Einstein sur le sujet des variables cachées. L'auteur, né en 1938, est un physicien doublé d'un philosophe des sciences.

[27] Voir les abondantes fiches Einstein Bohr debates et Interpretations of quantum mechanics sur Wikipedia, d'où provient le tableau de la page suivante. Nous y revenons dans une partie sur la philosophie de la physique quantique.



Les électrons avaient été découverts par **Joseph John Thomson** (1856-1940, Anglais) en 1897 en analysant les rayons émis par une cathode dans un tube cathodique, déviés ussi bien par un champ électrique que par un champ magnétique et détectés par une couche de phospore. Il obtient le Prix Nobel de Physique en 1906.

Ernest Rutherford avait aussi imaginé l'existence des neutrons qui ne fut vérifiée expérimentalement qu'en 1932 par l'Anglais **James Chadwick** (1891-1974). **Marie Curie** (1867-1934) avait bien découvert le polonium et le radium en 1898 et certains effets de la radioactivité mais pas l'existence des neutrons.

Selon Niels Bohr, les électrons émettent ou absorbent un photon lorsqu'ils changent d'orbite. Il est donc aussi l'un des fondateurs de la mécanique quantique, complétant les travaux de Planck et Einstein. Il a longtemps débattu sur le sujet, notamment avec Albert Einstein à partir du Congrès Solvay de 1927 que nous avons déjà évoqué au sujet d'Einstein.

Par la suite, les travaux de Louis de Broglie sur la dualité ondes-particules démontraient que les orbites des électrons étaient un multiple entier de leur longueur d'onde associée.

Avec Werner Heisenberg, Pascual Jordan et Max Born, Niels Bohr est à l'origine de l'interprétation dite de **Copenhague** de la physique quantique qui s'appuie sur trois principes clés[28] :

- La description d'une onde-particule est réalisée par sa fonction d'onde, et aucune autre information "cachée" ne peut servir à décrire son état. Il faut se résoudre à accepter cette approche probabiliste de la description d'un quantum, liée à sa dualité onde-particule.
- Lorsqu'une mesure de l'état d'un quantum est réalisée, sa fonction d'onde composite de plusieurs états est réduite à la fonction d'onde de l'un des états possibles du quantum. C'est l'effondrement ou écrasement de la fonction d'onde (ou du paquet d'onde, selon les appellations).
- Lorsque deux propriétés sont reliées par une relation d'incertitude, on ne peut pas mesurer les deux propriétés avec une précision supérieure à ce que permet la relation d'incertitude (principe d'indétermination d'Heisenberg). Qui plus est, lorsque l'on mesure la position d'une particule, on affecte son mouvement, et réciproquement.

C'est la principale interprétation de la mécanique quantique. Il y en a beaucoup d'autres qui sont inventoriées ci-dessous dans un tableau issu de Wikipedia. Nous aurons l'occasion de détailler un eu plus l'interprétation de Copenhague et d'évoquer cette question vers la fin de l'ebook dans la partie dédiée à la philosophie de la physique quantique.

[28] Voir aussi Seven ways to skin Schrödinger's cat de Richard Webb, 2016 qui décrit les différentes écoles de pensée de la physique quantique. Voir aussi les autres interprétations de la physique quantique dans The Biggest Myth In Quantum Physics Starts With A Bang d'Ethan Siegel, dans Forbes, 2018, d'où est issu le schéma *ci-dessus*.

Interpretation	Year published	Author(s)	Deterministic?	Ontologically real wavefunction?	Unique history?	Hidden variables?	Collapsing wavefunctions?	Observer role?	Local dynamics?	Counterfactually definite?	Extant universal wavefunction?
Ensemble interpretation	1926	Max Born	Agnostic	No	Yes	Agnostic	No	No	No	No	No
Copenhagen interpretation	1927	Niels Bohr, Werner Heisenberg	No	No[1]	Yes	No	Yes[2]	Causal	Yes	No	No
de Broglie–Bohm theory	1927–1952	Louis de Broglie, David Bohm	Yes	Yes[3]	Yes[4]	Yes	Phenomenological	No	No	Yes	Yes
Quantum logic	1936	Garrett Birkhoff	Agnostic	Agnostic	Yes[5]	No	No	Interpretational[6]	Agnostic	No	No
Time-symmetric theories	1955	Satosi Watanabe	Yes	No	Yes	Yes	No	No	No[7][8]	No	Yes
Many-worlds interpretation	1957	Hugh Everett	Yes	Yes	No	No	No	No	Yes	Ill-posed	Yes
Consciousness causes collapse	1961–1963	John von Neumann, Eugene Wigner, Henry Stapp	No	Yes	Yes	No	Yes	Causal	No	No	Yes
Stochastic interpretation	1966	Edward Nelson	No	No	Yes	Yes[9]	No	No	No	Yes[10]	No
Many-minds interpretation	1970	H. Dieter Zeh	Yes	Yes	No	No	No	Interpretational[11]	Yes	Ill-posed	Yes
Consistent histories	1984	Robert B. Griffiths	No	No	No	No	No	No	Yes	No	Yes
Transactional interpretation	1986	John G. Cramer	No	Yes	Yes	No	Yes[12]	No	No[13]	Yes	No
Objective collapse theories	1986–1989	Ghirardi–Rimini–Weber, Penrose interpretation	No	Yes	Yes	No	Yes	No	No	No	No
Relational interpretation	1994	Carlo Rovelli	No[14]	No	Agnostic[15]	No	Yes[16]	Intrinsic[17]	No[18]	No	No
QBism	2010	Christopher Fuchs, Rüdiger Schack	No	No[19]	Agnostic[17]	No	Yes[19]	Intrinsic[19]	Yes	No	No

A noter que le fils de Niels Bohr, **Aage Niels Bohr** (1922-2009, Danois), fut prix Nobel de physique en 1975 pour ses travaux portant sur la structure du noyau des atomes[29] , témoignant de la suite dans les idées à l'échelle familiale !

Emmy Noether (1882-1935, Allemande) est la créatrice du théorème qui porte son nom en 1915 à l'Université de Göttingen en Allemagne[30]. A l'origine du champ de l'algèbre abstraite, c'est le fondateur de la mécanique Lagrangienne, précurseur de la théorie d'Hamilton. A cette époque, elle ne pouvait pas enseigner à l'Université car ce rôle était interdit aux femmes. Son théorème n'a été publié qu'en 1918 et elle ne put officiellement enseigner qu'à partir de 1919.

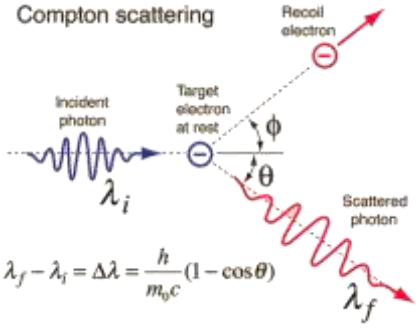
Elle ne reçut ainsi un salaire de l'Université qu'à partir de 1923. Son théorème relie les principes de conservation et les symétries. C'est l'un des fondements de la physique des particules. Ses travaux ont notamment aidé Albert Einstein à peaufiner les bases de la théorie de la relativité générale qu'il avait élaborée en 1915[31].

$$\frac{d}{dt}\left(\sum_a \frac{\delta L}{\delta \frac{dq_a}{dt}} \delta q_a\right) = 0$$

Ce dernier l'admirait particulièrement. De confession juive comme lui, elle dû s'expatrier aux USA en 1933 où elle ne vécut que deux ans. Elle est décédée relativement jeune, à 53 ans.

Arthur Holly Compton (1892-1962, Américain) est un physicien devenu prix Nobel de physique de 1927 pour la découverte en 1922/1923 de l'effet qui porte son nom et qui démontre l'aspect corpusculaire des photons. Son expérience fait interagir un photon avec un électron libre autour d'un atome, validant les théories de Planck et Einstein sur l'effet photoélectrique. L'effet Compton est en effet une variante de cet effet, appliqué aux rayons X et gamma qui sont des photons de haute énergie.

Elle s'applique à la réception d'un photon X ou gamma qui a une énergie supérieure à celle de l'électron éjecté. L'effet est utilisé dans les radios à rayons X. Le photon X est ralenti et dévié avec une énergie inférieure et devient un photon diffusé. On appelle aussi cela un choc élastique. Les rayons X sont émis lors de transitions électroniques entre les couches atomiques K, L et M (les premières autour du noyau de l'atome). Les angles d'émission de l'électron éjecté et du photon réémis dépendent du niveau d'énergie du photon incident.



[29] Voir Quantum Model of the Atom de Helen Klus, 2017.

[30] Voir In her short life, mathematician Emmy Noether changed the face of physics Noether linked two important concepts in physics: conservation laws and symmetries, par Emily Conover, 2018.

[31] Voir Women in Science: How Emmy Noether rescued relativity, par Robert Lea, février 2019.

Jacques Salomon Hadamard (1865-1963, Français) est un mathématicien qui a donné son nom à la porte de Hadamard utilisée dans les ordinateurs et algorithmes quantiques. Il avait notamment travaillé sur les nombres complexes, la géométrie différentielle et les équations aux dérivées partielles, en particulier pendant les années 1920. Il s'était aussi intéressé au processus créatif des mathématiciens en étudiant celui de centaine de collègues physiciens.

On lui doit notamment les transformées qui portent son nom, des opérations matricielles carrées de 2^n valeurs complexes ou entières de côté. La porte quantique qui porte le nom de Hadamard en son hommage est utilisée en calcul quantique pour créer une superposition des états $|0\rangle$ et de $|1\rangle$ avec une transformée de Hadamard de type H_1. Nous la verrons plus tard lorsque nous décrirons l'architecture d'un ordinateur à portes quantiques. Cette superposition est l'une des bases de l'accélération procurée par le calcul quantique, en complément du principe d'intrication qui relie les qubits entre eux de manière conditionnelle et seul, permet une accélération exponentielle.

$$H_0 = 1$$

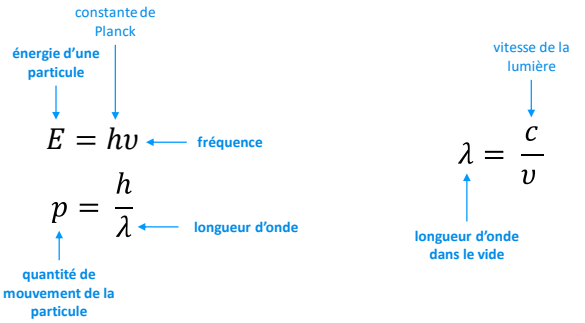
$$H_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$H_2 = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

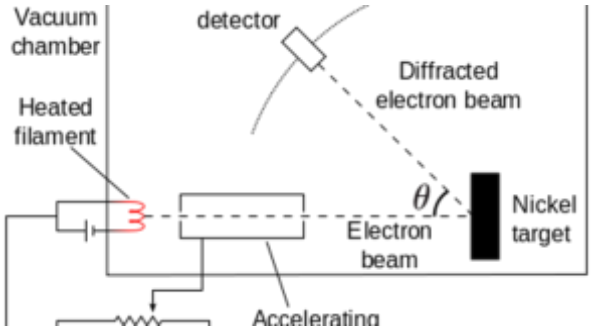
$$H_3 = \frac{1}{2^{3/2}}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Louis de Broglie (1892-1987, Français) est un mathématicien et physicien à qui l'on doit, en 1923 et 1924, l'extension du dualisme ondes corpuscules, appliqué alors uniquement aux photons, aux électrons, atomes, protons et neutrons[32]. Selon ce principe, les particules élémentaires peuvent présenter des propriétés de corpuscule (avec une position, une trajectoire et éventuellement une masse) et d'ondes (délocalisée, se diffusant dans toutes les directions, génèrant des interférences) selon les circonstances.

C'est le cas des électrons qui ont une masse et peuvent interférer les uns avec les autres, des atomes ainsi que des photons. Louis de Broglie exprimait cette dualité avec une équation : λp=h, où λ est une longueur d'onde, p une quantité de mouvement et h est la constante de Planck. Cela lui valut le prix Nobel de physique en 1929. C'est le principal contributeur Français à la mécanique quantique d'entre-deux-guerres.

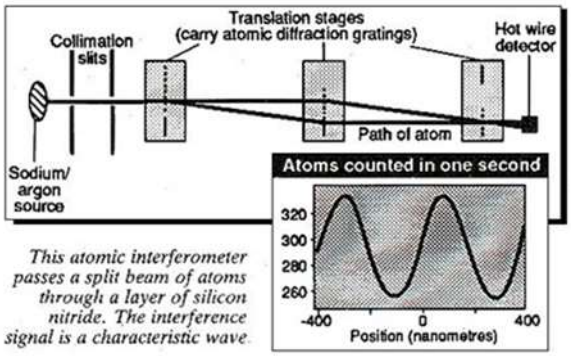


La dualité ondes-particules fut confirmée en 1927 pour ce qui concerne les électrons, par les expériences des équipes de l'Ecossais **George Paget Thomson** (1892-1975) de l'Université d'Aberdeen et de **Clinton Davisson** (1881-1958) et **Lester Germer** (1896-1971) des Bell Labs aux USA (*ci-contre*), qui ont partagé en 1937 un prix Nobel de physique pour ces expériences fondamentales.



[32] Le frère de Louis de Broglie, Maurice de Broglie (1875-1960), était aussi physicien. Il avait étudié les rayons X et la spectrographie. Les deux frères ont fait partie de l'Académie des Sciences en France.

La confirmation de la dualité onde-particule a été ensuite vérifiée pour les neutrons en 1988, par **Roland Gähler** et **Anton Zeilinger** (source) et pour des atomes en 1991 par **Olivier Carnal** et **Jürgen Mlynek** (source du schéma *ci-contre*) ! Elle est même vérifiable avec des molécules de plusieurs atomes. Un point historique mérite d'être rappelé : les travaux de Louis de Broglie amenèrent à la création de l'expression « mécanique ondulatoire ».



This atomic interferometer passes a split beam of atoms through a layer of silicon nitride. The interference signal is a characteristic wave.

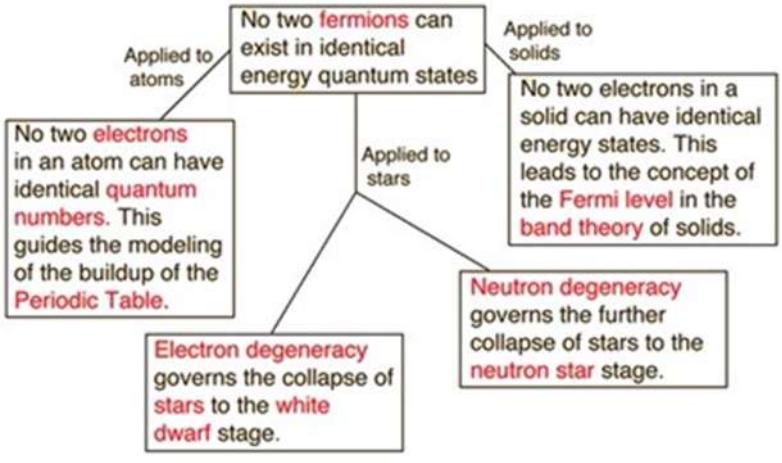
Celle-ci ne fit cependant pas long feu et fut remplacée par la « mécanique quantique » quelques années après avec les travaux de Schrödinger, Heisenger, Born et autres Dirac. Il n'y a qu'en France que la notion de mécanique ondulatoire a été utilisée jusque dans les années 1970. J'en ai trouvé la trace dans diverses publications scientifiques de l'époque.

Wolfgang Pauli (1900-1958, Autriche/USA) est à l'origine du principe d'exclusion qui porte son nom élaboré en 1925 et selon lequel deux électrons ne peuvent pas avoir le même état quantique dans un atome. Il participe à la découverte du spin de l'électron entre 1925 et 1927, ainsi que du neutrino en 1930 et dont l'existence ne sera prouvée expérimentalement qu'en 1956. Il obtient le prix Nobel de physique en 1945. L'histoire de ses découvertes est plus complexe qu'il semble.

En 1924, il découvre d'abord le spin du noyau des atomes, qui sert à expliquer la structure hyperfine des spectres atomiques, à savoir l'existence de raies spectrales très proches observées lors de leur excitation.

Elles ne s'expliquent pas par les quanta et niveaux d'énergie des couches d'électrons dans les atomes. En 1925, il introduit un nouveau degré de liberté des électrons qu'il ne qualifie pas au début.

Il s'ajoute aux trois premiers paramètres qui décrivent l'état d'un électron dans un atome, les nombres quantiques. Le premier est le niveau d'énergie de l'électron dans un atome (la couche où il se trouve), le second est le nombre quantique azimutal (qui définit la sous-couche d'électrons) et troisième est le nombre quantique magnétique (qui permet de distinguer les orbitales d'électron dans l'atome).



Ce quatrième degré de liberté est identifié par **George Uhlenbeck** (1900-1988, Pays-Bas/USA) et **Samuel Goudsmit** (1902-1978, Pays-Bas/USA) comme étant le spin de l'électron[33]. En 1925, Wolfgang Pauli formule également le principe d'exclusion selon lequel des électrons dans un même système (un atome) ne peuvent pas se trouver simultanément dans le même état quantique, un principe qui sera ensuite étendu à tous les fermions, soit les particules à spin demi-entier.

[33] Georges Uhlenbeck et Samuel Goudsmit étaient étudiants de **Paul Ehrenfest** (1980-1933, Autriche/Pays-Bas). Son laboratoire avait accueilli quelques futurs illustres physiciens comme Enrico Fermi, Robert Oppenheimer, Werner Heisenberg et Paul Dirac. Ehrenfest était un spécialiste de la physique statistique. Il a notamment contribué à la compréhension des changements de phase de la matière.

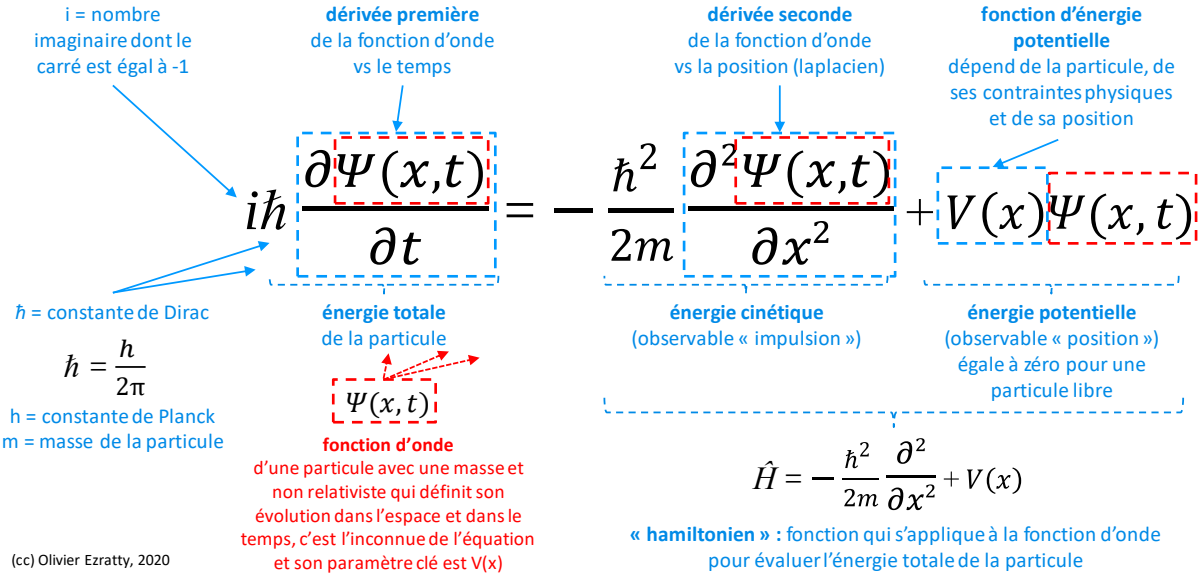
L'état quantique d'un électron est défini avec les quatre nombres quantiques, ou degrés de liberté, que nous venons d'évoquer.

Le spin d'électron est décrit comme un sens de polarisation magnétique ou comme une rotation angulaire de l'électron dans un sens ou l'autre, mais ce n'est qu'une image et pas une représentation physique. Ce spin est utilisé dans des qubits silicium dont nous reparlerons.

137 est un nombre qui a joué un rôle important dans sa vie. Il se trouve que 1/137 est une valeur qui correspond approximativement à la constante de structure fine, un ratio que l'on retrouve à plusieurs endroits dans la physique quantique et qui compare des données de même dimension. C'est par exemple le ratio entre la vitesse d'un électron de la couche basse d'un atome d'hydrogène et la vitesse de la lumière ou la probabilité d'émission sur l'absorption d'un photon pour un électron. 137 est un peu le 42 de la physique quantique (liste complète). Et Pauli est mort des suites d'une opération d'un cancer du pancréas, alors que sa chambre d'hôpital avait le numéro 137 !

Erwin Schrödinger (1887-1961, Allemand) est un physicien, prix Nobel en 1933 pour la création de sa fonction d'ondes, élaborée en 1926, ou équation de Schrödinger, qui décrit l'évolution dans le temps et l'espace de l'état ondulatoire d'une particule quantique dotée d'une masse, à savoir les probabilités de trouver le quantum à un endroit donné et moment donné. Pour cette édition 2020 de l'ebook, je me tente à une explication dans le détail de cette équation.

L'équation de Schrödinger est une variante des équations de la mécanique newtonienne qui définissent l'énergie totale d'un objet comme étant la somme de son énergie cinétique et de son énergie potentielle.



Voici de quoi comprendre les éléments de cette équation et leurs implications :

- Son **inconnue** est la fonction d'onde de la particule qui décrit son comportement probabiliste dans l'espace et le temps : ψ(x, t). x indique la position de la particule dans l'espace, sur une, deux ou trois dimensions, et t le temps. Quelle valeur est retournée par cette fonction ? C'est un nombre complexe dont le module au carré donne une probabilité d'obtenir la particule à cet emplacement et au temps t ! Cette combinaison encode en pratique l'amplitude et la phase de l'onde.
- L'équation illustre le principe de la **conservation de l'énergie**. L'élément à gauche de l'équation décrit l'énergie totale de la particule à un moment et un endroit donné. L'élément à droite comprend l'énergie cinétique de la particule et son énergie potentielle.

- Le **carré du module la fonction d'onde** ψ(x, t) correspond donc à la probabilité de trouver la particule à l'endroit x au moment t. Pour un électron, qui est la particule la plus couramment analysée avec cette équation, c'est une indication de la probabilité de le trouver à une distance donnée du noyau de l'atome autour duquel il gravite. En toute logique, la somme des probabilités de trouver la particule quelque part est égale à 1. C'est ce que l'on appelle la contrainte de normalisation. L'une de ses dérivées est la fonction de Max Born que nous verrons plus loin.

  Le module d'un nombre complexe est la taille de son vecteur. Si z = a + ib, le module $|z|$ de z est donc la racine carrée de la somme des carrés de a et b, cf. *ci-dessous*.

  $\mathbf{z} = a + ib$

  $|z| = \sqrt{a^2 + b^2}$

  module d'un nombre complexe c'est la taille du vecteur qui le représente dans un espace à deux dimensions.

  $|\psi(x,t)|^2$

  carré du module probabilité de trouver la particule à la position r au temps t. Si elle est indépendante du temps, le système est dans un état stationnaire.

  $\int_{-\infty}^{+\infty} |\psi(x,t)|^2 \, dx = 1$

  l'intégrale de la propabilité de trouver la particule à la position x sur toutes les positions x est égale à 1

- C'est une équation aux **dérivées partielles** à savoir qu'elle relie ses composantes via des fonctions dérivées, en l'occurrence de premier degré (la mesure d'une « pente » sur une courbe) et de second degré (la mesure d'une accélération). La fonction d'onde de la particule apparaît trois fois dans l'équation : à gauche de l'équation avec une dérivée première sur le temps de la fonction d'onde, à droite avec une dérivée seconde sur sa position et avec une simple multiplication avec la fonction V(x).
- L'**énergie potentielle de la particule** est définie par la fonction V(x) qui dépend seulement de la position dans l'espace de la particule et des contraintes physiques, notamment électromagnétiques, qui lui sont imposées. Lorsqu'une particule est libre et se déplace sans contraintes, cette fonction renvoie une valeur nulle. Cette fonction V(x) est la principale variable de l'équation de Schrödinger.
- L'équation est **linéaire** car tous ses opérateurs sont linéaires. Ce qui fait entre autres chose que toute combinaison de solutions de l'équation devient une nouvelle solution de l'équation. Cela permet de décomposer une fonction d'onde en plusieurs fonctions d'ondes élémentaires que l'on appelle les « états propres » de l'objet quantique. Ils correspondent aux différents niveaux d'énergie de la particule qui sont discrets lorsque la particule est contrainte dans l'espace, comme les électrons dans un atome. On peut en effet dans ce cas déduire la notion de quantification de l'état de la particule à partir de l'équation de Schrödinger (démonstration).
- L'équation de Schrödinger est **résolue analytiquement** dans un nombre de cas limités comme pour l'électron d'un atome d'hydrogène, une particule libre, une particule dans un puits de potentiel ou dans une boîte ou un oscillateur harmonique quantique. Dans les cas les plus complexes, la résolution de l'équation passe par des méthodes non analytiques, par du calcul brut et de la simulation. C'est d'ailleurs l'un des champs d'application des simulateurs quantiques que de résoudre l'équation de Schrödinger dans les cas où les méthodes analytiques ne sont pas disponibles. Tout objet micro ou macro a une fonction d'onde de Schrödinger, jusqu'à l'Univers tout entier, en reprenant les travaux de Hugh Everett que nous évoquerons plus loin. Mais l'équation n'a de sens pratique que pour les objets nanoscopiques.
- L'opérateur qui agit sur la partie droite et qui cumule la dérivée seconde et la fonction d'énergie potentielle est dénommé **hamiltonien**, qui décrit l'énergie totale du système. On retrouve cette expression dans le calcul à recuit quantique chez D-Wave. Nous y reviendrons.

- Cette équation est un **postulat général** qui a été validé de manière expérimentale dans un grand nombre de cas[34]. Son interprétation a donné lieu à de nombreux débats, à savoir, est-ce qu'il s'agit d'un simple modèle probabiliste ou est-ce qu'il décrit la réalité ? Nous traitons de cela dans le chapitre sur la philosophie de la physique quantique.

- L'équation de Schrödinger générique présentée jusqu'à présent est dite **dépendante du temps**. Cette équation est présentée de diverses manières selon les besoins et les annotations. La dérivée seconde de la fonction d'onde sur la position de la particule est parfois présentée avec le signe nabla au carré (∇^2). Un nabla opère une dérivée sur une fonction scalaire ou vectorielle.

  Le ∇^2 opère une dérivée seconde, appelée aussi laplacien. La forme la plus concise de l'équation de Schrödinger est à droite, avec deux opérateurs : le hamiltonien à gauche ($\hat{H}$) et l'opérateur d'énergie à droite ($\hat{E}$) qui s'appliquent tous deux à la fonction d'onde de la particule étudiée.

$$\left[-\frac{\hbar^2}{2m}\nabla^2 + V\right]\Psi = i\hbar\frac{\partial}{\partial t}\Psi$$

$$\hat{H}\psi(x,t) = \hat{E}\psi(x,t)$$

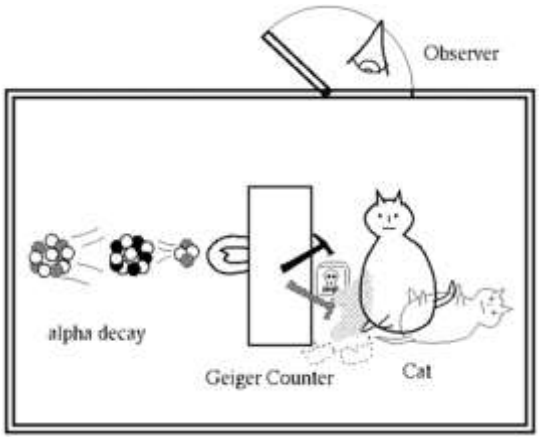
- Il existe une forme **indépendante du temps** de l'équation de Schrödinger qui s'applique aux particules en état stationnaire[35].

$$\left[-\frac{\hbar^2}{2m}\nabla^2 + V(r)\right]\Psi(r) = \hat{E}\psi(r)$$

  Dans cette version de l'équation de Schrödinger, l'opérateur d'énergie E est une simple constante, un nombre réel.

On doit aussi à Erwin Schrödinger sa fameuse expérience de pensée quelque peu alambiquée visant à expliquer la notion d'états superposés avec son chat à la fois vivant et mort dans une boîte[36]. On y a placé une fiole de poison dont l'ouverture est provoquée par la désintégration d'un atome radioactif de radium via un compteur Geiger détectant cette radiation ionisante. La radiation est faite de particules alpha, comprenant deux protons et deux neutrons. C'est l'équivalent d'un atome d'hélium 4 sans ses électrons.

Comme le radium a une chance sur deux de se désintégrer après sa demi-vie, le chat a une chance sur deux d'être vivant et mort, tant que l'on n'ouvre pas la boîte. Lorsqu'on l'ouvre, il est vivant ou mort. Tant que la porte n'est pas ouverte, il est censé être à la fois vivant et mort. Sauf que le chat peut mourir juste après l'ouverture de la boite si l'atome de radium se désintègre à ce moment-là ! Et une fois que le chat est mort, il ne peut pas être ressuscité. Sa superposition entre vivant et mort est une vue de l'esprit car la mort n'est pas réversible contrairement à la modification de l'état d'un quantum.



[34] Voir la vidéo Quantique - D'où vient l'équation de Schrödinger?, de Benoît Hébert, professeur de physique en classes préparatoires. La démonstration n'est pas abordable au commun des mortels !

[35] Dixit Wikipedia : « *Une onde stationnaire est le phénomène résultant de la propagation simultanée dans des sens opposés de plusieurs ondes de même fréquence et de même amplitude, dans le même milieu physique, qui forme une figure dont certains éléments sont fixes dans le temps. Au lieu d'y voir une onde qui se propage, on constate une vibration stationnaire mais d'intensité différente, en chaque point observé. Les points fixes caractéristiques sont appelés des nœuds de pression.* ».

[36] L'expérience de pensée du chat a été publiée dans une série de trois papiers en 1935, quelques temps après la publication du paradoxe EPR d'Einstein, Podolsky et Rosen. Voir The Present Status of Quantum Mechanics par Erwin Schrödinger, 1935 (26 pages). L'histoire du chat n'occupe que neuf lignes dans ce long document qui porte sur la question de la superposition, de la mesure et de l'intrication. Le chat qui n'y apparait que trois fois en tout et pour tout y est donc anecdotique mais c'est ce que tout le monde a retenu. Ce qui est bien normal : le reste est bien moins facile à appréhender !

De plus, la notion de demi-vie d'un atome radioactif ne relève pas directement de la superposition des états de quantas. Un atome radioactif est soit en un état désintégré, avec une certaine probabilité que cela intervienne liée à sa demi-vie, soit en état normal. La désintégration qui relève de la fission n'est pas un processus réversible. C'est toutefois bien un processus quantique, qui s'explique par les fluctuations quantiques du vide.

Il n'y a donc pas de véritable superposition quantique des états de l'atome de radium entre état d'origine et état désintégré comme pour les états énergétiques d'un électron ! Un atome de radium donné n'est jamais à la fois en état normal et en état désintégré. Si c'était le cas, le chat serait d'ailleurs presque immédiatement mort dans cette expérience de pensée[37]. Pour que l'expérience du chat soit véritablement quantique, il faudrait éventuellement qu'elle s'appuie sur un atome de radium traversant un miroir semi-réfléchissant avec une chance sur deux de le traverser dans un cadre quantique, auquel cas on se rapprocherait d'une interprétation quantique[38].

N'oublions pas que cette expérience de pensée visait à mettre en évidence le fait que la superposition ne s'appliquait qu'à l'infiniment petit et pas aux objets macroscopiques. L'Histoire a plus retenu le principe de superposition et pas cette différence entre le microscopique et le macroscopique.

Mais je ne vais pas me permettre de remettre en question un tel génie ! Oublions tout de même le chat et retenons la fonction d'onde de Schrödinger et la notion de superposition des états qui n'a de sens qu'à l'échelle microscopique ! Dans sa vie privée, Schrödinger était un grand coureur de jupons. Il était même capable de mener plusieurs liaisons en même temps, appliquant à sa vie privée le principe de la superposition quantique[39].

Max Born (1892-1970, Allemand) est un physicien et mathématicien à l'origine de la représentation mathématique des quanta sous forme matricielle. C'est à lui que l'on doit en 1926 l'explication statistique de la probabilité de trouver un électron dans un état énergétique donné à partir de sa fonction d'onde, élaborée par Schrödinger la même année. Ce principe est appliqué aux qubits, où la somme du carré des probabilités des deux états du qubit est égale à 1, reprise dans la sphère de Bloch.

Sachant que les probabilités α et β sont en fait des nombres complexes. Werner Heisenberg était l'assistant de Max Born ! Ce dernier a obtenu le prix Nobel de physique en 1954.

Werner Heisenberg (1901-1976, Allemand) est un physicien, prix Nobel de physique en 1932, à qui l'on doit en 1927 la création du fameux principe d'incertitude, ou plutôt d'indétermination, selon lequel on ne peut pas mesurer avec précision à la fois la position et la vitesse d'une particule élémentaire, ou, plus généralement, deux grandeurs arbitraires. Il est surtout à l'origine d'une bonne partie du formalisme mathématique de la physique quantique avec les matrices qui portent son nom.

Cette formulation matricielle et à base d'algèbre linéaire de la mécanique quantique conduit à représenter l'état d'un système quantique sous forme de vecteurs qui permettent au passage de représenter mathématiquement la superposition des états quantiques.

---

[37] Vous pouvez appliquer cette expérience de pensée à la cuisson du mi-cuît au chocolat. Tant que vous ne le sortez pas du four après les 9 minutes de cuisson réglementaires mais avec un four dont vous ne connaissez pas la puissance, vous ne savez pas s'il est bien cuit ou pas, et coulant au milieu avant de le sortir. Il est en état de superposition entre pas assez cuit, bien cuit et trop cuit. Par contre, s'il est trop cuit, il sera difficile de revenir en arrière, comme pour le chat à moitié mort de Schrödinger au cas où il serait mort. La surcuisson comme la mort du chat sont irréversibles. Ce n'est donc pas une véritable superposition d'états quantiques.

[38] L'interprétation sur la désintégration se trouve dans la fiche Wikipedia du chat de Schrödinger.

[39] Voir cette belle émission de France Culture qui raconte sa vie : Schrödinger, l'homme derrière le chat, mai 2020 (une heure) avec Charles Antoine (Sorbonne Universités, chercheur en physique de la matière condensée) et Michel Bitbol (ENS Lyon, chercheur en philosophie des sciences).

Son principe d'indétermination est une conséquence de ce formalisme. Il a été décrit mathématiquement de manière simplifiée en 1928 par **Earle Hesse Kennard** (1885-1968, Américain) dans l'équation *ci-contre*, où le produit de l'écart type de la position et la vitesse est supérieur à la moitié de la constante de Dirac.

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

On peut d'ailleurs utiliser cette équation pour améliorer la précision d'une mesure d'une grandeur quelconque, en baissant celle d'une autre grandeur caractérisant un quantum[40]. On parle de la mesure de couple d'observables de l'état d'un quantum, celle-ci pouvant faire appel par exemple à une énergie, une position, une fréquence ou une vitesse.

Une conséquence du principe d'Heisenberg est que toutes les particules de l'Univers sont en mouvement constant. Si elles étaient stables, on aurait connaissance de leur position (fixe) et de leur vitesse (nulle), violant le principe d'indétermination. Une autre conséquence est qu'un vide parfait ne pourrait pas exister car la valeur et l'évolution des champs magnétiques et gravitationnels qui le traversent seraient stables, violant une fois encore l'indétermination d'Heisenberg. Cela explique l'étonnante fluctuation du vide quantique que nous allons creuser un peu plus loin. Le théorème de non-clonage de l'état de qubits tire aussi son origine du principe d'indétermination.

Pour certains, ce principe d'indétermination serait une interprétation simplificatrice appliquée à la compréhension de la nature corpusculaire de la matière. Il mène à se poser la question de la position et de la vitesse d'un électron, alors qu'il n'aurait pas de position précise. Il n'y aurait pas là d'incertitude qui traduirait une méconnaissance de notre part. Nous tentons d'appliquer à l'électron des concepts de mécanique classique qui ne lui seraient pas applicables.

Ou tout du moins, qui ne sont pas observables de près. En tout cas pour l'interprétation dite de Copenhague de la mécanique quantique.

En pratique, les particules quantiques ne sont pas des particules physiques classiques et on ne peut donc pas en mesurer aussi bien la vitesse que la position. On ne peut les décrire que par leur fonction d'onde (de Schrödinger). Plus généralement, Heisenberg énonce le principe selon lequel dans l'infiniment petit, la mesure influe sur la grandeur à mesurer. Le schéma *ci-contre*[41] illustre le phénomène au niveau macroscopique : si vous éclairez un insecte avec la lumière du soleil et une loupe pour mieux l'observer, vous risquez de le faire brûler !

C'est le même problème avec les différents systèmes d'imagerie médicale, comme ceux qui sont à base de rayons X et qui, en cas d'usage répéter, affecter négativement les organes observés.

Enfin, comme nombre de ses confrères de son époque, Werner Heisenberg s'est intéressé aux liens entre science, mécanique quantique et philosophie et dès 1919. Il fut assistant de Niels Bohr entre 1924 et 1927, avant de partir pour l'Université de Leipzig. Il a aussi eu Max Born comme professeur !

[40] Cette technique de mesure est utilisée dans le "quantum squeezing" qui est intégré dans la dernière version du LIGO pour la mesure des ondes gravitationnelles : NIST Team Supersizes 'Quantum Squeezing' to Measure Ultrasmall Motion, 2019.

[41] Source de l'image : It's only when you look at an ant through a magnifying glass on a sunny day that you realise how often they burst into flames.

Paul Dirac (1902-1984, Anglais) est un mathématicien et physicien parmi les fondateurs de la physique quantique du 20e siècle. On lui doit l'équation sur le spin des électrons en 1928 qui fait partie des bases de la physique quantique relativiste (*ci-dessous*). Son équation est une sorte de variante de l'équation de Schrödinger pour les particules relativistes libres, les fermions (électrons, protons, neutrons, quarks, neutrinos) qui sont des particules à spin demi-entier. Relativistes au sens, se déplaçant à une vitesse proche de celle de la lumière.

Dans l'équation de Dirac, la fonction d'onde de l'électron ψ comprend quatre composantes de nombres complexes qui intègrent le temps et l'espace.

L'équation de Dirac lui permet de prédire l'existence d'une particule qui sera appelée plus tard le positron, sorte d'électron avec une charge positive[42].

$$\left(\beta mc^2 + c\sum_{n=1}^{3}\alpha_n p_n\right)\Psi(x,t) = i\hbar\frac{\partial\Psi(x,t)}{\partial x}$$

Dirac introduit aussi en 1939 la notation bra-ket, dit de Dirac, qui définit les états de quantum, en <phi|psy> en algèbre linéaire. Nous verrons cela plus loin dans ce document. La constante de Dirac ou constante de Planck réduite est sinon la constante de Planck *h* divisée par 2π, appelée aussi « h-bar » pour son symbole de h barré en italique : *ħ*. Cette constante de Dirac est notamment utilisée dans la fonction d'onde de Schrödinger que nous avons déjà détaillée.

Il obtient le Prix Nobel de Physique en 1933, donc à 31 ans. Les prix Nobel des débuts du 20eme siècle pouvaient être attribués à de jeunes scientifiques, ce qui semble passé de mode depuis ! Le plus jeune prix Nobel de Physique fut Lawrence Bragg, qui l'obtint à 25 ans en 1915 pour sa découverte de la réfraction des rayons X réalisée à l'âge de 22 ans[43].

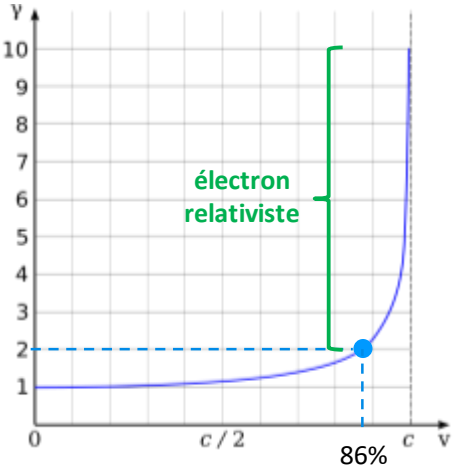
Dans quel cas a-t-on à faire à des particules relativistes, notamment pour ce qui est des électrons ? On considère généralement qu'un électron devient relativiste lorsque le total de sa masse et de son énergie cinétique est au moins le double de la masse au repos. C'est un ratio qui correspond au facteur de Lorentz. Il correspond à une vitesse d'au moins 86% de celle de la lumière. Mais des phénomènes relativistes peuvent intervenir avant. En équivalent newtonien, la vitesse d'un électron autour du noyau d'un atome d'hydrogène est d'environ c/137, c étant la vitesse de la lumière.

facteur de Lorentz = masse relativiste de l'électron (m_{rel}) vs masse au repos (m_e)

$$\gamma = \frac{1}{\sqrt{1-(v^2/c^2)}}$$

$$m_{rel} = \frac{m_e}{\sqrt{1-(v_e/c)^2}}$$

rayon de Bohr $a_0 = \frac{4\pi\epsilon_0\hbar^2}{m_e e^2}$



Pour des électrons de couches intérieures d'atomes lourds, cette vitesse peut dépasser c/2. C'est le cas des électrons de la première couche de l'atome d'or, qui circulent à 58% de la vitesse de la lumière.

[42] Les positrons sont découverts expérimentalement par Carl Anderson en 1932. Il obtiendra le Prix Nobel de physique en 1936.

[43] Paul Dirac se distingait par sa timidité et par son expression orale parcimonieuse dans les réunions ou pendant les repas. Au point que ses collègues de Cambridge avaient défini l'unité "dirac" comme étant le moyen de s'exprimer de la manière la plus concise dans une réunion, à savoir, au rythme d'un seul mot par heure. Son comportement était équivalent lors des Congrès Solvay auxquels il participait, notamment celui de 1927. Il a cependant du battre un record dans son discours d'acceptation de son prix Nobel fin 1933. Il fait tout de même six pages ! La moitié cependant des 12 pages du discours d'Erwin Schrödinger, également récipiendaire du prix Nobel de physique cette année-là.

Cela affecte la position des électrons relativistes dans les orbites (quantiques) basses des atomes lourds comme les lanthanides, qui font partie des terres rares. Le rayon de Bohr qui définit l'orbitale moyenne d'un électron diminue inversement proportionnellement à la masse apparente de l'électron. Du fait que la masse apparente de l'électron augmente, ce rayon de Bohr est donc plus petit pour les électrons relativistes. Cela modifie ainsi la structure des orbitales d'électrons des atomes lourds et les niveaux d'énergie des transitions entre orbitales qui absorbent ou émettent des photons.

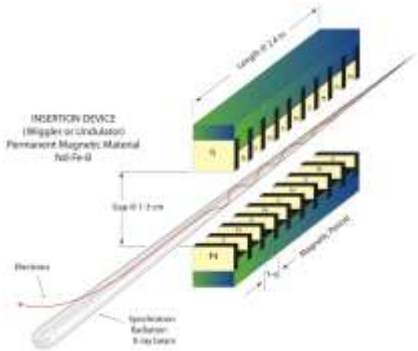
Cela explique la couleur de l'or et de l'argent, du fait de modification relativiste d'orbites de couches d'électrons entre lesquelles se produisent des transitions liées à l'absorption de photons. Le bleu est absorbé dans le cas de l'or, expliquant sa couleur jaune ! Sans l'effet relativiste, l'or serait blanc.

Cela a tout un tas d'implications dans la chimie de ces matériaux et notamment de leur organisation en cristaux[44]. Cet effet relativiste explique aussi pourquoi le mercure est liquide à température ambiante[45]. Tout cela donne lieu à un champ de la chimie que l'on appelle la chimie quantique relativiste[46]. Elle contribue aussi à expliquer le fait que la dimension des atomes n'est pas proportionnelle à leur nombre de protons et d'électrons[47].

Les particules deviennent aussi relativistes dans les **accélérateurs de particules** comme le LHC du CERN près de Genève (le plus grand du monde), l'ESRF de Grenoble (European Synchrotron Radiation Facility, spécialisé dans la génération de rayons X « durs », à très haute fréquence) ou dans le synchrotron de lumière SOLEIL situé à Saint-Aubin près de Saclay juste à côté du CEA et pas loin du nouveau campus des grandes écoles CentraleSupelec et ENS Paris-Saclay.

Le synchrotron SOLEIL utilise des électrons accélérés à une vitesse relativiste et des onduleurs qui génèrent des faisceaux de lumière 10 000 fois plus denses que la lumière du Soleil[48]. Des instruments équivalents existent dans le monde comme l'Advanced Photon Source du DoE de l'Argonne National Laboratory près de Chicago.

Les **Lasers à Électrons Libres** (LEL) exploitent des sources d'électrons relativistes. Ce sont des lasers de génération de lumière cohérente (spatialement et temporellement, les photons émis ont la même fréquence, la même polarisation et la même phase) qui exploitent des sources d'électrons relativistes provenant de synchrotrons. L'interaction entre ces électrons et un fort champ magnétique alternatif permet de générer de la lumière cohérente dans des gammes de fréquences électro-magnétiques allant de l'infrarouge jusqu'aux rayons X, en passant par la lumière visible et l'ultra-violet[49].



---

[44] Voir d'autres exemples dans Relativistic Effects in Chemistry More Common Than You Thought de Pekka Pyykko, 2012 (24 pages).

[45] Voir Why is mercury liquid? Or, why do relativistic effects not get into chemistry textbooks?, Lars J. Norrby, 2018 (4 pages).

[46] Voir Relativistic quantum chemistry par Trond Saue, 2019 (110 slides) et An introduction to Relativistic Quantum Chemistry par Lucas Visscher (107 slides). Le formalisme mathématique de la chimie quantique relativiste est bien documenté dans le volumineux Introduction to Relativistic Quantum Chemistry de Kenneth Dyall et Knut Faegri, 2007 (545 pages).

[47] Voir ce tableau périodique des éléments avec une indication des tailles des atomes.

[48] Voir la conférence Electrons relativistes comme sources de lumière par Marie-Emmanuelle Couprie, Synchrotron Soleil, 2011 (1h25). Les électrons circulent dans le synchrotron à une vitesse proche de celle de la lumière. SOLEIL alimente plus de 25 instruments d'analyse couvrent le spectre allant de l'infrarouge aux rayons X, avec notamment de nombreuses applications en microscopie de précision, dont une microscopie qui utilise de la lumière blanche très bien colimatée et polarisée. On peut utiliser ces instruments pour analyser la structure en trois dimensions de molécules organiques comme des protéines complexes, telles que les glycoprotéines qui entourent les virus. Cela permet même d'étudier la manière dont ces protéines se combinent avec celles des cellules attaquées. ou Sont aussi analysés les ribosomes qui servent à produire les protéines dans les cellules.

[49] Source de l'illustration : X-ray diffraction: the basics par Alan Goldman (31 slides).

On trouve enfin des particules relativistes en **astrophysique** et, par exemple, dans les sources de rayons cosmiques ainsi que dans les jets relativistes de plasma produits au centre de galaxies et de quasars[50].

Pascual Jordan (1902-1980, Allemand) est un physicien qui a collaboré avec Max Born et Werner Heisenberg et a contribué à poser les fondements mathématiques de la mécanique quantique, notamment au niveau du calcul matriciel. Comme Philipp Lenard, il a été quelque peu oublié, comme Philipp Lenard, du fait de son adhésion au Parti Nazi pendant les années 1930, même s'il a été réhabilité au sortir de la seconde guerre mondiale grâce à l'intervention de Wolfgang Pauli. Dans le champ philosophique, il s'est intéressé à la notion de libre arbitre.

Linus Pauling (1901-1994, américain) est un biochimiste connu pour avoir cofondé les champs scientifiques de la chimie quantique et de la biologie moléculaire. Il avait eu l'occasion de rencontrer en Europe les fondateurs de la mécanique quantique (Erwin Schrödinger, Niels Bohr) en 1926-1927. On lui doit notamment la description des liaisons chimiques sur une période étalée entre 1928 et 1932 et notamment l'hybridation des orbitales qui explique la géométrie des molécules. Il a publié la somme "The Nature of the Chemical Bond" en 1939.

Il a obtenu le prix Nobel de Chimie en 1954 puis le prix Nobel de la Paix en 1962 pour son activisme politique en faveur du désarmement nucléaire. Il est considéré comme étant à l'origine de la chimie computationnelle qui permet de simuler numériquement la structure des molécules et que nous évoquons dans la rubrique sur les applications quantiques dans la santé page 288.

James Chadwick (1891-1974) est un physicien anglais à qui l'on doit la découverte des neutrons en 1932 qui lui valut le Prix Nobel de physique en 1935. Cette découverte est tardive par rapport à la mécanique quantique et à la découverte des électrons. La physique nucléaire a en effet progressé parallèlement à la physique quantique qui avait surtout trait aux interactions entre électrons et photons. Avant la découverte des neutrons, les scientifiques pensaient que le noyau des atomes comprenait des protons et des électrons.

John Von Neumann (1903-1957, Hongrois puis Américain) était un polymathe, surtout mathématicien extrêmement prolifique. Il a participé à la création des fondements mathématiques de la mécanique quantique, notamment dans la somme "Mathematical Foundations of Quantum Mechanics" publié en 1932. Il transposait les grands principes de la mécanique quantique en modèles et équations d'algèbre linéaire.

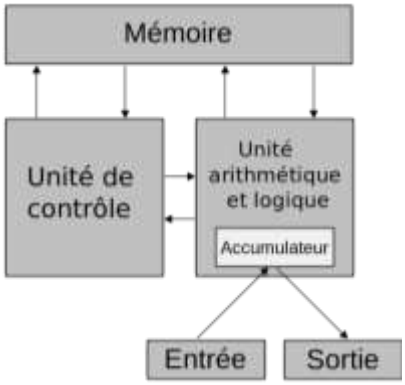
Cela touche par exemple les d'états quantiques qui sont représentés par une position dans un espace de Hilbert, les observables qui sont des projections dans les espaces de Hilbert et le phénomène de l'indétermination qui s'explique par la non-commutativité des opérateurs de mesure.

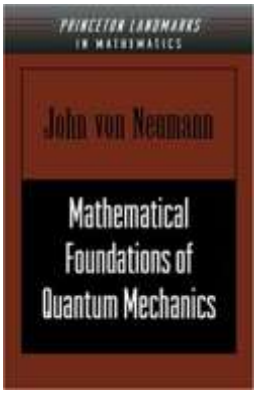
Il y déclarait que l'introduction de variables cachées pour y intégrer du déterminisme était peine perdue car cela rentrerait en contradiction avec les autres prédictions (vérifiées) de la physique quantique. Trois ans avant le papier EPR d'Einstein/Podolsky/Rosen ! On lui doit la création de la notion de l'entropie (de Von Neumann), en 1932, qui est associée aux notions d'opérateurs et de matrices densités qu'il a créées en 1927 et qui décrivent l'état d'un système quantique.

---

[50] L'équation de Dirac est à relier à l'**équation de Klein-Gordon** (1926) qui s'applique aux bosons (comme les particules élémentaires gluons et les pions) qui sont les particules à spin entier ou nul. La mécanique quantique relativiste est un large champ de la physique, utilisée en particulier dans la physique des particules élémentaires. Je n'ai pas découvert d'usages de cette branche de la physique dans les technologies quantiques courantes. Mais c'est probablement une recherche incomplète. Voir les grands fondements de cette mécanique quantique relativiste dans Relativistic Quantum Mechanics par David J. Miller, University of Glasgow, 2008 (116 slides).

Il a aussi participé au projet Manhattan aux USA en modélisant les explosions et les lentilles permettant de compresser le plutonium dans les bombes A. On lui doit aussi les concepts de base dans la théorie des jeux et surtout des ordinateurs classiques et qui sont encore en vigueur. Les ordinateurs utilisent ainsi presque tous une architecture de Von Neumann avec mémoire, registres, unité de contrôle, unité de calcul, entrées et sorties.





Boris Podolsky (1896-1966, Russe puis Américain) a conçu le paradoxe EPR avec Albert Einstein et Nathan Rosen en 1935 sur l'intrication quantique et les questions de non localité des propriétés des quanta intriqués. C'était un spécialiste de l'électrodynamique qui porte sur l'analyse des champs électriques et électromagnétiques. Eyant émigré aux USA, selon les archives russes, il aurait été un espion du KGB après-guerre et aurait renseigné l'URSS sur les programmes atomiques américains entre 1942-1943. Son nom de code était… « Quantum ».

Nathan Rosen (1909-1995, Américain puis Israélien) est le troisième larron du paradoxe EPR qui faisait partie de l'interprétation ou école de Copenhague, expliquant la logique probabiliste de la mécanique quantique par les interactions entre quantums et outils de mesure. Selon cette interprétation, il n'est pas nécessaire de trouver des variables cachées pour expliquer le fonctionnement de quanta intriqués. Emigrant en Israël en 1953, il y fonde l'institut de physique de l'Université Technion à Haïfa. Il a aussi travaillé sur les trous noirs.

Ettore Majorana (1906-circa 1938, Italien) a imaginé l'existence d'un fermion en 1937 en s'appuyant sur les équations de Dirac, une particule qui serait sa propre antiparticule[51]. Son existence aurait été découverte en 2012 et aurait vérifiée en 2016, même si c'est toujours contesté par de nombreux physiciens. Ces fermions de Majorana doivent permettre de concevoir des ordinateurs quantiques universels dits topologiques qui permettent de gérer des codes de correction d'erreurs très efficaces nécessitant un faible nombre de qubits physiques.

C'est la voie d'exploration choisie par Microsoft après les travaux de Michael Freedman et Alexei Kitaev à la fin des années 1990. Ettore Majorana se serait suicidé après une dépression, et d'après Etienne Klein, parce qu'il avait du mal à supporter la pression de son génie[52] ! Mais sa disparition reste énigmatique car on n'a jamais retrouvé trace de son corps !

Alonzo Church (1903-1995, Américain) est un mathématicien à qui l'on doit des travaux dont sont dérivés la thèse dite de Church-Turing selon laquelle n'importe quel calcul automatique peut-être réalisé avec une machine de Turing. La thèse de Church-Turing étendue édicte que le temps de calcul d'un problème est équivalent au pire à un polynôme fonction de la taille du problème. Elle est non démontrable. Elle est à l'origine de la création du lambda calculus en 1936, un langage de programmation abstrait universel qui a notamment inspiré la création de LISP.

[51] Voir cette intéressante conférence d'Etienne Klein en 2016 sur l'œuvre d'Ettore Majorana.

[52] Si on avait pu échanger ce trait avec celui de Donald Trump, le monde aurait été meilleur !

Qu'en est-il des autres, connus, inconnus ou moins célèbres du Congrès Solvay de 1927 ? Nombre d'entre eux n'étaient pas des contributeurs de la mécanique quantique. Ils étaient présents du fait d'un équilibre historique de ces Congrès, associant notamment une équipe fixe ainsi qu'une proportion stable de Belges, Français, Allemands et Anglais.

Il y avait par exemple **Émile Henriot** et **Marie Curie** qui étaient focalisés sur la radioactivité, **Paul Langevin** (avec qui Marie Curie avait eu une liaison en 1910, après la mort accidentelle de son mari Pierre Curie en 1906), ainsi qu'un bon nombre de chimistes. Deux noms méritent cependant d'être cités qui avaient un lien avec la physique quantique.

Léon Brillouin (1889-1969, Franco-Américain) qui est moins connu en France du fait de son expatriation aux USA pendant la seconde guerre mondiale. Il a contribué aux avancées de la mécanique quantique entre les deux guerres mondiales. Il a notamment rapproché la mécanique quantique de la cristallographie. Il a surtout découvert les phénomènes de diffraction des ondes traversant les cristaux ("Brillouin scattering").

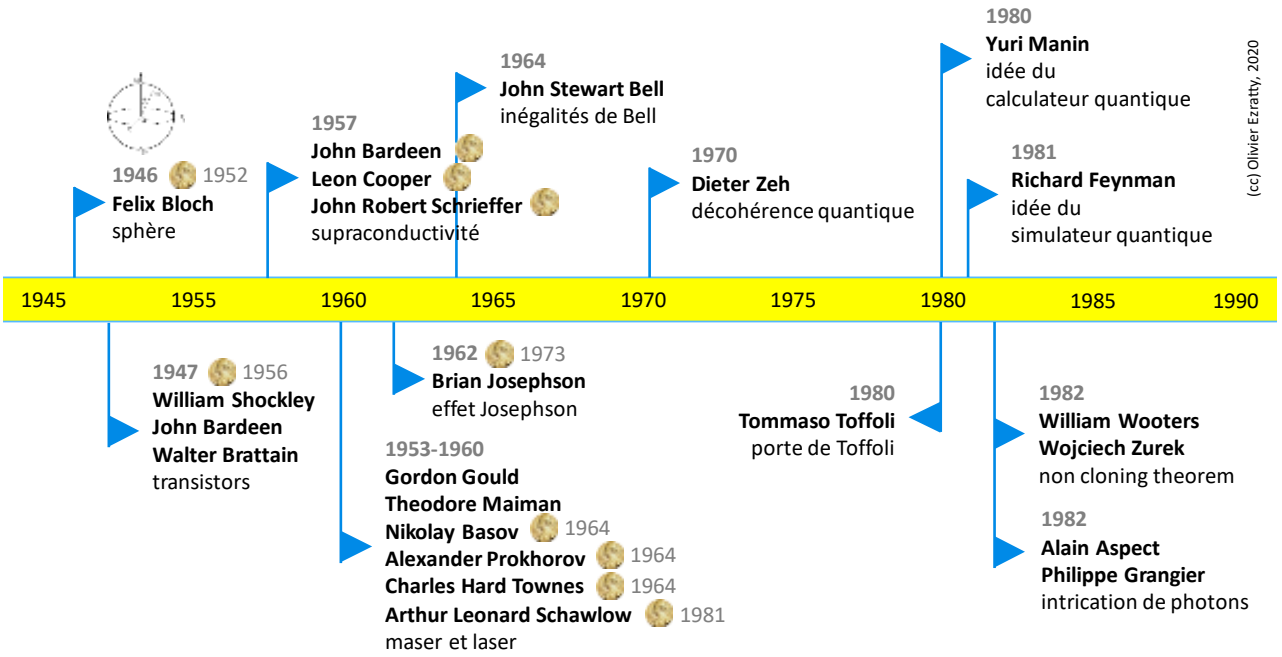
Et puis, enfin, **Hendrik Anthony Kramers** (1894-1952, Hollandais) qui a assisté Niels Bohr dans la création de la théorie des quanta et de la mécanique quantique.

Après-guerre

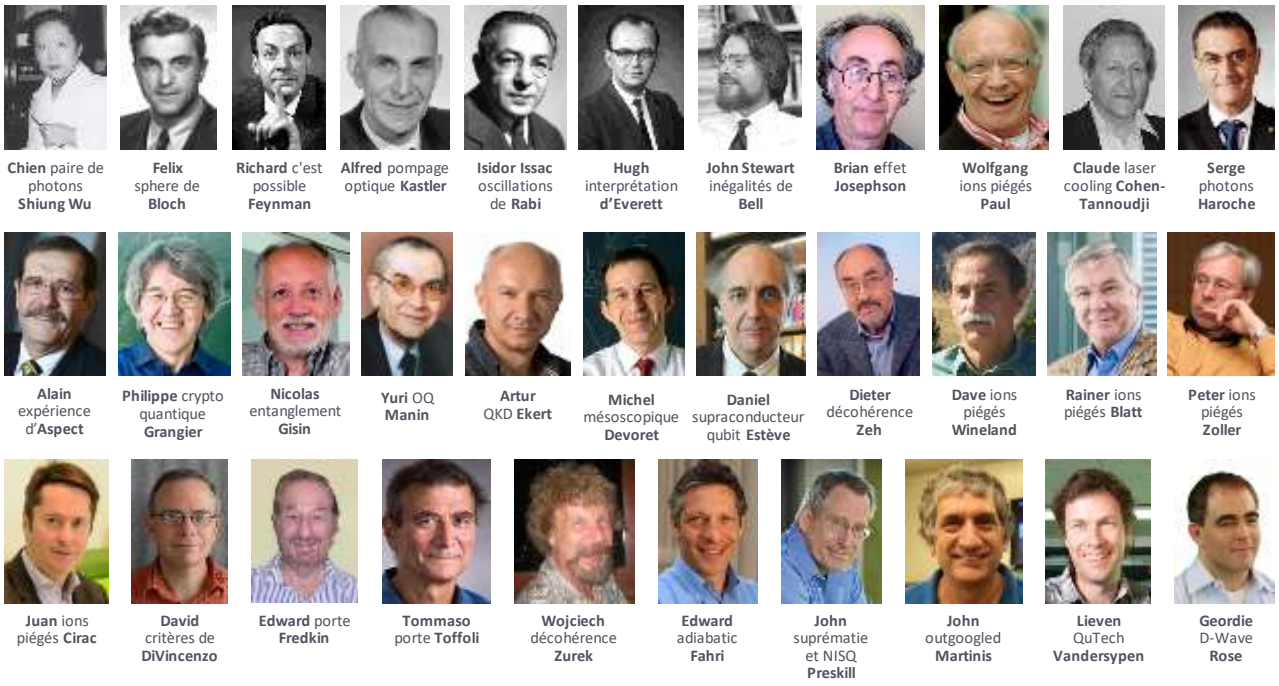
La mécanique quantique a connu un calme relatif entre les années 1935 et 1960. Les physiciens étaient alors surtout occupés par l'arme et l'énergie nucléaires. Cela a conduit à délaisser quelque peu la mécanique quantique, ou tout du moins à l'utiliser surtout dans le cas de la physique nucléaire, même si son apport était tout relatif dans ce cas.

On peut citer trois branches importantes issues des applications de la première révolution quantique : les **transistors**, inventés en 1947 par William Shockley, John Bardeen et Walter Brattain, les **masers** et les **lasers** inventés entre 1953 et 1960 par Gordon Gould, Theodore Maiman, Nikolay Basov, Alexander Prokhorov, Charles Hard Townes et Arthur Leonard Schawlow, une partie d'entre eux seulement ayant reçu le prix Nobel associé à ces découvertes, les **cellules photovoltaïques** qui transforment la lumière en électricité mais aussi le **GPS**.

Les transistors et les lasers sont à la base d'une bonne partie des technologies numériques d'aujourd'hui. Et l'énergie photovoltaïque fait bien entendu partie du mix des énergies renouvelables.



La période des Trente Glorieuses est dominée dans la physique quantique par les travaux de John Stewart Bell en 1964 et par leur vérification par l'expérience d'Alain Aspect en 1982. Nous avons aussi une date clé avec 1981 qui marque les débuts symboliques de l'informatique quantique, imaginée par Richard Feynman.



L'appellation de **seconde révolution quantique** couvre les avancées à partir des années 1990, où l'on a commencé à contrôler les propriétés quantiques de quanta individuels, au niveau de photons (polarisation, …), d'électrons (spin) et d'atomes ou d'ions ainsi que de la superposition et l'intrication des états, ce qui a notamment permis l'émergence de la cryptographie et des télécommunications quantiques, en plus des prémisses du calcul quantique. La définition d'origine de cette seconde révolution quantique n'est cependant pas si précise que cela[53].

Felix Bloch (1905-1983, Suisse puis Américain) est un physicien à qui l'on doit notamment la représentation physique de l'état d'un qubit dans une sphère qui porte son nom, la sphère de Bloch, élaborée en 1946 dans un papier sur le magnétisme nucléaire. Comme d'autres physiciens de son temps, il a contribué au projet Manhattan. Il fut prix Nobel de physique en 1952 pour ses travaux sur la résonance magnétique nucléaire. Il fut aussi le premier directeur du laboratoire de physique des particules international CERN en 1954.

Chien-Shiung Wu (1912-1997, Chinoise puis Américaine) est une scientifique qui a surtout contribué aux développements de la physique nucléaire et au projet Manhattan aux USA, notamment pour son procédé de séparation par diffusion gazeuse de l'uranium 238 et de l'uranium 235. Elle a aussi contribué au développement de la physique quantique en conduisant la première expérience relative à la synchronisation de paires de photons en 1947[54], avant l'expérience d'Alain Aspect de 1982.

[53] L'appellation a été lancée simultanément et indépendamment en 2003 par Alain Aspect et par Jonathan Dowling et Gerard Milburn. Ce dernier est aussi connu pour être l'un des trois protagonistes du modèle KLM de calcul quantique à base de photons, créé en 2001 conjointement avec Emanuel Knill et Raymond Laflamme.

[54] Voir notamment The Angular Correlation of Scattered Annihilation Radiation, Wu et Shaknov, 1949.

Cette expérience était différente et s'appuyait sur la mesure de la corrélation angulaire de photons dans les rayons gamma (très haute fréquence et haute énergie) générés par la rencontre d'électrons et de positrons.

Hugh Everett (1930-1982, Américain) est un physicien à qui l'on doit la formulation des états relatifs et d'une fonction d'onde globale de l'Univers intégrant les observations, les observateurs et les outils d'observation des phénomènes quantiques. Il avait rencontré Niels Bohr avec d'autres physiciens à Copenhague en 1959 pour présenter sa théorie. Il avait été poliment écouté mais ses interlocuteurs ont raconté qu'il ne comprenait rien à la physique quantique.

Everett était aussi un contributeur du rapprochement de la théorie de la relativité et de la mécanique quantique, notamment autour de la gravitation quantique. On lui attribue l'hypothèse des mondes multiples ou multiverses, expliquant l'intrication quantique et la non-localité. On la doit en fait à **Bryce DeWitt** (1922-2004, Américain) qui a interprété ses travaux en 1970. DeWitt a aussi travaillé sur la formulation de théories sur la gravité quantique.

John Wheeler (1911-2008, Américain) supervisa la thèse de Hugh Everett. C'était un spécialiste de la gravitation quantique. Il a surtout travaillé dans le domaine de la physique nucléaire, notamment dans le projet Manhantan ainsi que sur les premières bombes H américaines. Il a aussi travaillé sur la matière nucléaire à très haute densité que l'on trouve dans les étoiles à neutrons. Il a développé le concept de trous de vers (wormholes).

A noter qu'il a eu comme élève et thésard un certain Richard Feynman et il a aussi collaboré avec Niels Bohr.

John Stewart Bell (1928-1990, Irlandais) a relancé la recherche en mécanique quantique dans les années 1960 sur la notion d'intrication. On lui doit les "inégalités de Bell" qui mettent en avant les paradoxes soulevés par l'intrication quantique. Le théorème de Bell de 1964 indique qu'aucune théorie de variables cachées locales - imaginée par Einstein en 1935 - ne peut reproduire les phénomènes de la mécanique quantique[55]. Il est cependant plutôt pro-einsteinien dans sa démarche et favorable à une interprétation réaliste de la physique quantique[56].

Il définit en fait le moyen de vérifier ou invalider l'hypothèse de l'existence de variables cachées expliquant l'intrication quantique. Les inégalités de Bell ont été violées par les expériences du Français Alain Aspect en 1982 puis 1998, démontrant l'inexistence de ces variables cachées locales. Avant cette expérience, les inégalités de Bell avaient été démontrées théoriquement par John Clauser, Michael Horne, Abner Shimony et Richard Holt en 1969 dans ce que l'on appelle les inégalités CHSH[57]. Les travaux de John Bell ont été complétés en 2003 par eux d'**Anthony Leggett** (1938, Anglo-Américain, prix Nobel de physique en 200 ») avec ses inégalités applicables à d'hypothétiques variables cachées non locales[58].

Anton Zeilinger (1945, Autrichien) arrivait à violer expérimentalement ces inégalités en 2007. Selon Alain Aspect, cela ne remettait cependant pas en cause le modèle à variables cachées non locales proposé par David Bohm.

---

[55] Voir cette explication du théorème de Bell dans un document de Tim Maudlin à l'occasion des 50 ans du théorème : What Bell Did, 2014 (28 pages). Et le document d'origine de Bell : On the Einstein-Podolsky-Rosen paradox, John S. Bell, 1964 (6 pages).

[56] Voir What Bell Did par Tim Maudlin, 2014 (28 pages) qui décrit bien le paradoxe EPR et la contribution de Bell.

[57] Voir Proposed experiment to test local hidden-variable theories, 1969 (5 pages).

[58] Voir Nonlocal Hidden-Variable Theories and Quantum Mechanics: An Incompatibility Theorem, Anthony Leggett, 2003 (25 pages).

Claude Cohen-Tannoudji (1933, Français) est notamment ancien élève de Normale Sup où il a suivi les enseignements des mathématiciens Henri Cartan et Laurent Schwartz et du physicien Alfred Kastler. Il devient Prix Nobel de Physique en 1997 en même temps que Steven Chu, qui fut plus tard Ministre de l'Energie de la première présidence de Barack Obama. Ce Ministère (DoE, Department of Energy) une des agences fédérales les plus investies dans les technologies quantiques, notamment parce qu'ils opèrent les plus grands supercalculateurs du pays.

Claude Cohen-Tannoudji doit son prix Nobel à ses travaux sur le refroidissement d'atomes par laser qui permis d'atteindre des températures extrêmement basses, inférieures au milli-Kelvin (voir sa lecture). A noter qu'Alain Aspect a un temps travaillé dans son équipe. Alain Aspect raconte que c'est en lisant un livre « somme » de Claude Cohen-Tannoudji, Bernard Diu et Franck Laloë « Mécanique quantique » paru en 1973 qu'il a découvert la physique quantique.

Serge Haroche (1944, Français), prix Nobel de physique en 2012, a créé des qubits avec des atomes couplés à des cavités supraconductrices contenant quelques photons. On compte **Jean-Michel Raymond**[59] et **Michel Brune** parmi ses collaborateurs. Serge Haroche a été le premier à mesurer le phénomène de décohérence de quanta (perte de superposition) dans une expérience en 1996. Cette expérience a été menée à l'ENS avec des atomes de rubidium. Serge Haroche fait aussi partie du conseil scientifique d'Atos.

Serge Haroche est un des scientifiques français les plus réservés sur le devenir de l'informatique quantique, en tout cas pour le calcul à portes universelles. Il croit plus à la voie de la simulation quantique[60].

Alain Aspect (1947, Français) invalide donc le paradoxe EPR et les inégalités de Bell en 1982 dans une expérience menée au laboratoire de SupOptique du bâtiment 503 de la faculté d'Orsay, puis confirmée dans d'autres expériences en 1998. Elle valide l'intrication de photons distants ayant interagi par le passé et le principe de la non localité des propriétés quantiques[61]. Après son travail sur l'intrication des photons, il s'est intéressé au contrôle par laser des atomes froids, à commencer par ceux d'hélium.

Cela a amené à la création d'une filière prometteuse du calcul quantique en France, celle des atomes froids, incarnée par la startup Pasqal, dont le directeur scientifique est Antoine Browaeys, un ancien thésard de Philippe Grangier, lui-même ancien thésard d'Alain Aspect. En compagnie d'autres scientifiques, Alain Aspect fait aussi partie du conseil scientifique d'Atos.

Il continue de diffuser la bonne parole sur la physique quantique et sur ses expériences, notamment dans des MOOC réalisés pour l'école Polytechnique où il continue d'enseigner. Il explique très bien sa fameuse expérience dans diverses conférences dont celle-ci[62].

J'ai pu le rencontrer avec Fanny Bouton en mai 2018 à l'Institut d'Optique de Palaiseau près de Paris. Nous avons aussi enregistré un épisode des entretiens Decode Quantum avec lui en juin 2020, diffusé à la fin de l'été 2020.

---

[59] Voir son intéressante conférence Informatique quantique ou comment utiliser l'étrangeté du monde microscopique, Jean-Michel Raymond, 2015 (1h36mn). Voir aussi le support de présentation (56 slides).

[60] Voir ainsi cette interview de Serge Haroche : « L'ordinateur quantique reste une utopie », par Erwan Cario, avril 2020.

[61] L'expérience a été depuis multipliée à l'envie. En 2017, des chercheurs de Varsovie arrivaient ainsi à intriquer un photon avec des milliards d'atomes de rubidium. Voir Quantum entanglement between a single photon and a trillion of atoms, 2017.

[62] Voir cet excellent débat entre Alain Aspect et Etienne Klein : Les intrigantes intrications du monde quantique, février 2020 (59 mn). Voir aussi From Einstein's Doubts to Quantum Technologies: A New Quantum Revolution par Alain Aspect, février 2020 (1h05).

Philippe Grangier (1957, Français) est un ancien thésard d'Alain Aspect avec qui il avait travaillé sur l'expérience de ce dernier en 1982 avec Gérard Roger et Jean Dalibard. C'est l'un des spécialistes mondiaux de la cryptographie quantique, notamment de la CV-QKD. Il est à l'origine de la startup associée, Sequrnet, créée en 2008 et fermée en 2017, probablement crée un peu trop tôt par rapport aux besoins du marché.

Dieter Zeh (1932-2018, Allemand) est le découvreur du phénomène de la décohérence quantique en 1970, c'est-à-dire, la fin du phénomène de superposition d'états de quantum, lorsque les particules sont perturbées par leur environnement et que la phase est modifiée. La notion de décohérence est clé dans la conception d'ordinateurs quantiques. L'objectif étant de retarder autant que possible ce phénomène qui résulte de l'interaction entre les quantums et leur environnement[63].

Wojciech Zurek (1951, Polonais) qui est un physicien spécialiste de la décohérence quantique qui a contribué aux fondements de la physique quantique appliquée aux calculateurs quantiques. On lui doit le théorème du non clonage qui veut qu'il soit impossible de cloner un qubit à l'identique sans que les qubits résultants soient ensuite intriqués. Il est aussi à l'origine du concept de darwinisme quantique qui expliquerait le lien en le monde quantique et le monde physique macro.

Anton Zeilinger (1945, Autrichien) est un physicien prolifique qui a notamment fait avancer le champ de la téléportation quantique dans les années 2000. En 1991, il valide la dualité onde-particule des neutrons. Il a été aussi le premier à réaliser la téléportation d'un qubit. C'est un spécialiste de l'intrication quantique, ayant prouvé qu'il était possible d'intriquer plus de deux quantums ou qubits. Il a créé des fondements théoriques et expérimentaux de la cryptographie quantique.

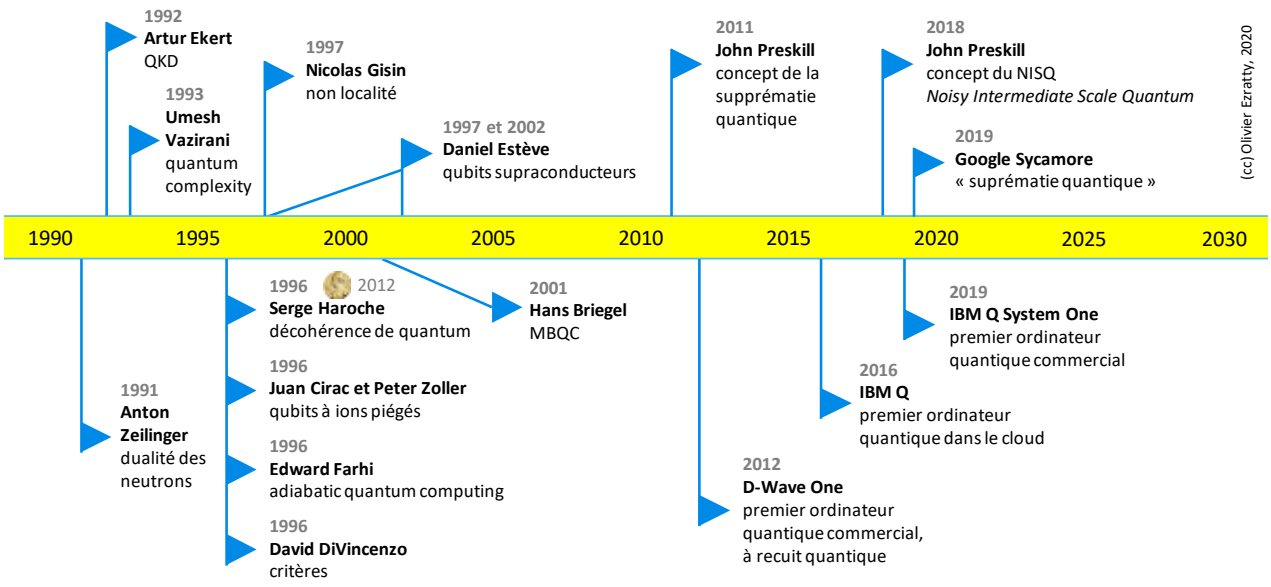
On lui doit aussi avec deux collègues la notion d'état superposé GHZ (Greenberger-Horne-Zeilinger) qui permet de démontrer l'inexistence de variables cachées dans l'intrication quantique d'au moins trois particules et avec un nombre fini de mesures. La notion date de 1989 et sa validation expérimentale de 1999.

Physiciens de l'informatique quantique

Je complète cette histoire par un tour d'horizon des physiciens de l'informatique quantique, qui sont souvent des spécialistes de l'optique ou de la matière condensée, comme les supraconducteurs, servant à créer des qubits.

J'y mets particulièrement en valeur les physiciens et physiciennes français, notamment ceux que j'ai eu l'occasion de rencontrer depuis trois ans dans mes périgrinations quantiques. Cet inventaire est aussi bien objectif que subjectif. Objectif car il comprend une bonne part des grands noms du domaine. Subjectif car j'y ai ajouté une bonne dose de physiciens que je connais, ce qui créé un biais... de la mesure, comme en physique quantique.

[63] Dieter Zeh est notamment l'auteur de On the Interpretation of Measurement in Quantum Theory en 1970 (8 pages).



Richard Feynman (1918-1988, Américain) est l'un des pères de l'électrodynamique quantique, ce qui lui valut le prix Nobel de physique en 1965. Il théorise en 1981 la possibilité de créer des ordinateurs quantiques analogiques capables de simuler des phénomènes quantiques pour résoudre des problèmes de simulation du fonctionnement de la matière[64]. Il est aussi à l'origine de l'explication quantique de la superfluidité de l'hélium à très basse température dans une série de papiers publiés entre 1953 et 1958.

Enfin, il est surtout connu du grand public scientifique pour son grand talent de vulgarisateur.

Brian Josephson (1940, Anglais) est un physicien de l'Université de Cambridge, prix Nobel de physique en 1973 à 33 ans[65], ce qui est très rare, pour sa prédiction de l'effet qui porte son nom en 1962 alors qu'il n'avait donc que 22 ans et était doctorant à l'Université de Cambridge. L'effet Josephson décrit le passage de courant par effet tunnel dans un circuit supraconducteur et les effets de seuils associés. Le courant traverse une fine barrière isolante de quelques nanomètres d'épaisseur.

En-dessous d'une certaine tension, le courant se met à osciller. Il est généré par les électrons organisés en paires de Cooper du nom de Leon Cooper qui les a découverts en 1952. Ces électrons en paires sont de spins opposés (polarité magnétique) et se constituent du fait du rapprochement des ions métalliques à leur passage.

Le système se comporte comme une résistance associée à une inductance en boucle, l'oscillation étant contrôlable par un champ magnétique et pouvant se faire avec deux états énergétiques distincts.

La supraconductivité a été découverte pour sa part en 1911 par le Hollandais **Heike Kamerlingh Onnes** (1853-1926).

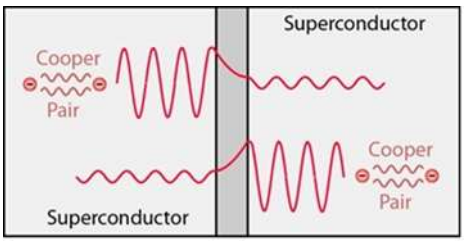
---

[64] Voir Simulating Physics with Computers publié en 1981 ainsi que Quantum Mechanical Computers, également de Richard Feyman, publié en 1985 (10 pages). Il y décrit comment un ordinateur quantique pourrait réaliser des opérations mathématiques similaires à celles des ordinateurs traditionnels. Il conclue en disant que l'on pourrait créer des ordinateurs où un bit tiendrait dans un seul atome, ce qui donnerait encore du mou à la loi de Moore !

[65] Brian Josephson partagea ce prix Nobel de Physique 1973 avec deux scientifiques qui l'avaient précédé pour l'aider à faire sa prédiction. Leo Esaki (1925, Japon, toujours vivant début 2020) pour sa découverte de l'effet tunnel dans les semiconducteurs en 1958 et Ivar Giaever (1929, Norvège, toujours vivant également) qui trouva que cet effet pouvait se produire dans des matériaux supraconducteurs en 1960.

C'est la base des qubits supraconducteurs et de leurs portes quantiques ! Le physicien et prix Nobel de physique Serge Haroche explique l'effet Josephson dans cette vidéo de son cours du Collège de France de 2011.

A noter que Brian Josephson s'intéresse depuis sa découverte à la méditation transcendantale.



Yuri Manin (1937, Russe et Allemand) est un mathématicien prolifique qui, avec Paul Benioff et Richard Feynman, fait partie des premiers scientifiques à avoir proposé l'idée de créer des ordinateurs quantiques, et en 1980 dans son livre "Computable and Uncomputable". Juste avant Richard Feynman en 1981. Ils participaient à la conférence "Physics & Computation" du MIT en 1981.

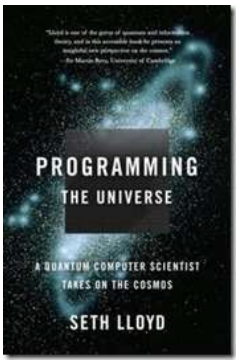
Elle rassemblait un bon nombre de noms connus de l'informatique quantique comme Tommaso Toffoli et Edward Fredkin (*ci-contre, source*).

On y trouvait aussi Rolf Landauer. C'est pour cette conférence que Richard Feynman avait publié Simulating Physics with Computers.

Tommaso Toffoli (1943, Italien puis Américain) est un ingénieur connu pour la création, au début des années 1980, de la porte quantique à son nom, une porte conditionnelle à trois entrées qui est très utilisée en programmation quantique. Après avoir œuvré au MIT, il est devenu enseignant à l'Université de Boston où il officie depuis 1995. A l'instar de Stephen Wolfram, il s'intéresse notamment aux automates cellulaires et à la vie artificielle.

Edward Fredkin (1934, Américain) est professeur de Carnegie Mellon. On lui doit notamment la porte quantique d'interversion de qubits à deux entrées (SWAP) qui porte son nom. Il est aussi le concepteur de la notion d'ordinateur réversible avec Tommaso Toffoli au MIT. C'est aussi un inventeur prolixe bien au-delà de l'informatique quantique et à l'origine des transpondeurs d'identification de véhicules et de la géonavigation automobile.

C'est enfin un promoteur de la notion de "philosophie digitale" qui réduit le monde et son fonctionnement à un programme géant quantique, une théorie qu'il partage avec **Seth Lloyd** (1960, Américain), intiateur du Quantum Machine Learning et du concept de qRAM et auteur de "Programming the Universe". Cette idée a été remise au goût du jour par Elon Musk qui pense que l'Univers est un programme gigantesque et que nous vivons dans une simulation. Le respect « automatique » de lois physiques élémentaires est-il un « programme » ? Epineuse question philosophique et sémantique ! A noter que Seth Lloyd a été mis à pieds du MIT en 2019 parce qu'il n'aurait pas informé sa direction de financements provenant de Jeffrey Epstein.



Wolfgang Paul (1913-1993, Allemagne), prix Nobel de physique en 1989 est un physicien qui conceptualise les ions piégés dans les années 1950. On lui doit les pièges qui portent son nom et servent à contrôler des ions piégés.

Les physiciens **Juan Cirac** (1965, Espagnol) et **Peter Zoller** (1952, Autriche) théorisent, conçoivent et testent les premiers qubits à ions piégés en 1996 à partir des travaux de Wolfgang Paul.

Rainer Blatt (1952, Autrichien et Allemand) de l'Université d'Innsbruck est un physicien expérimentateur spécialiste, entre autres choses, des qubits réalisés avec des ions piégés. Il est le premier à avoir pu intriquer l'état quantique de deux ions piégés en 2004 puis huit ions en 2006. Il a aussi cofondé la startup Alpine Quantum Technologies qui ambitionne de commercialiser un ordinateur quantique à base d'ions piégés, en toute logique.

David Wineland (1944, Américain) est un physicien du NIST basé à Boulder connu pour ses avancées dans le domaine des ions piégés et leur refroidissement par laser en 1978. Il a aussi créé la première porte quantique à base d'un seul atome en 1995. Il a obtenu le Prix Nobel de physique en 2012 conjointement avec le Français Serge Haroche, pour ses avancées dans le refroidissement d'atomes et d'ions par lasers, une technique qu'il a expérimentée pour la première fois en 1978 suivie de la première porte quantique appliquée à un ion piégé en 1995 et l'intrication entre quatre ions piégés en 2000.

Christopher Monroe (1965, Américain) est un physicien américain connu pour ses travaux sur les ions piégés et pour avoir cofondé la startup IonQ en 2015. Il avait travaillé sur les ions piégés avec David Wineland dans le laboratoire du NIST dans le Maryland. Il y a démontré la possibilité d'intriquer des ions, de gérer de la mémoire quantique avec des ions et de créer des simulateurs quantiques analogiques. Il avait aussi dirigé un laboratoire dans l'Université du Michigan au début des années 2000.

Edward Farhi (1952, Américain) est un physicien ayant travaillé dans de nombreux domaines, notamment dans la physique des particules à haute énergie, en particulier au LHC du CERN à Genève. Il est surtout le créateur d'algorithmes adaptés aux ordinateurs quantiques adiabatiques. Ce sont les algorithmes utilisés dans les ordinateurs quantiques de D-Wave qui permettent de faire converger un système complexe de qubits vers une solution de problèmes d'optimisation, une méthode que l'on appelle le recuit quantique ("quantum annealing").

Daniel Estève (1954, Français) est un physicien spécialiste de l'informatique quantique, responsable du laboratoire Quantronique du CEA à Saclay, lancé en 1984. Il planche en particulier sur les qubits supraconducteurs à effet tunnel exploitant une jonction Josephson de type transmon. Il a créé un premier qubit opérationnel en 1997, le quantronium, suivi d'un autre prototype en 2002. On peut considérer qu'il est l'un des grands pionniers de cette branche.

Daniel Estève fait partie du conseil scientifique d'Atos. Je l'avais notamment rencontré début juin 2018 avec Fanny Bouton et il nous avait brossé un beau tableau de l'histoire des qubits supraconducteurs.

Michel Devoret (1953, Français) est un ingénieur télécom devenu physicien, co-fondateur du laboratoire Quantronique avec Daniel Estève au CEA de Saclay entre 1985 et 1995, qui est un des pionniers mondiaux des qubits supraconducteurs à base de l'effet Josephson et notamment de la filière des cat-qubits à correction d'erreur intégrée qui est mise en œuvre par la startup française Alice&Bob. Il est depuis 2002 professeur à l'Université de Yale aux USA. Il est cofondateur de la startup américaine QCI, qu'il a quittée en 2019/2020.

Il a aussi travaillé avec John Martinis, alors à l'Université de Santa Barbara, pour faire un inventaire en 2004 des bases de la création de qubits supraconducteurs[66].

Artur Ekert (1961, Polonais et Anglais) est un physicien en mécanique quantique connu pour être l'un des créateurs du champ de la cryptographie quantique. Petite anecdote : il avait rencontré Alain Aspect en 1992 pour lui parler de cette inspiration après avoir découvert les expériences de ce dernier. C'est un bel exemple d'inventions par étapes, un chercheur en inspirant un autre ! Il enseigne à Oxford et dirigeait jusqu'à 2020 le CGT de Singapour. Il y réside depuis une quinzaine d'années. Il fait aussi partie du conseil scientifique d'Atos.

Nicolas Gisin (1952, Suisse) est un physicien spécialiste de la communication quantique. Il a démontré la non localité quantique avec une expérience en 1997 sur une distance de 10 km, étendant la performance réalisée en laboratoire par Alain Aspect en 1982. Comme Philippe Grangier, c'est un spécialiste de la cryptographie quantique. Il est notamment le cofondateur de la startup IDQ en 2001, une startup suisse spécialisée dans la génération de nombres véritablement aléatoires à partir de photons traversant un miroir dichroïque. Elle appartient à SK Telecom depuis 2018.

David DiVincenzo (1959, Américain) était un chercheur chez IBM et il est à l'origine des critères qui portent son nom et qui définissent les besoins minimums d'un ordinateur quantique à portes universelles. Il est maintenant chercheur et professeur à l'Université d'Aix la Chapelle en Allemagne. Il fait partie du conseil scientifique d'Atos en compagnie notamment d'Alain Aspect, Serge Haroche, Artur Ekert et Daniel Estève.

John Preskill (1953, Américain) est professeur à Caltech. C'est le créateur de la notion de suprématie quantique en 2011 et du NISQ en 2018, les Noisy Intermediate-Scale Quantum, la dénomination des calculateurs quantiques actuels et à venir dans un futur proche, qui sont de taille intermédiaire et sujets à un bruit quantique qui en limite les capacités. C'est aussi un excellent vulgarisateur[67]. Il intervient régulièrement dans des conférences où il fait le point de l'état de l'art du calcul quantique. C'est un peu le Yoda du domaine.

Lieven Vandersypen (1972, Belge) est à l'origine un ingénieur en mécanique ayant fait une thèse à Stanford, puis passé par IBM à San Jose où il s'est intéressé aux MEMS. Il démontra l'usage de l'algorithme de Shor pour factoriser le nombre 15. Il est ensuite devenu chercheur à l'Université TU Delft aux Pays-Bas et dans sa spin-off QuTech. C'est un pionnier des qubits à base de spins d'électrons. A ce titre, il travaille notamment avec Intel qui teste chez QuTech ses chipsets de qubits silicium et dans laquelle Intel a investi $50M en 2015.

---

[66] Dans Implementing Qubits with Superconducting Integrated Circuits (41 pages)

[67] Voir sa présentation qui fait un tour d'horizon de l'état de l'art de l'informatique quantique Quantum Computing for Business, John Preskill, décembre 2017 (41 slides).

Christophe Salomon (1953, Français) est un physicien spécialisé en photonique et atomes froids, directeur de recherche au LKB (Normale Sup à Paris). Il s'intéresse notamment à la superfluidité de gaz quantiques (condensats Bose-Einstein) et à la mesure du temps avec des horloges atomiques au césium dont il est un grand spécialiste mondial. A l'origine Centralien, il a ensuite fait une thèse en spectroscopie laser puis réalisé un post-doc au laboratoire JILA conjoint entre le NIST et l'Université du Colorado. Il est aussi membre de l'Académie des Sciences depuis 2017.

John Martinis (1958, Américain), est un physicien de l'UCSB et Google. Il dirigea les efforts dans l'informatique quantique de ce dernier autour des qubits supraconducteurs entre 2014 et 2020. Il avait piloté l'équipe de physiciens à l'origine de l'expérience de suprématie quantique de Google, publiée dans Nature en octobre 2019. Il a fait son post-doc dans le laboratoire Quantronics de Daniel Estève au CEA à Saclay, donc également dans les qubits supraconducteurs.

Jason Alicea (Américain) est un professeur de physique théorique de l'IQIM, Institute for Quantum Information and Matter, de l'Université Caltech en Californie. C'est un spécialiste de la matière condensée, de l'informatique quantique topologique à base d'anions non abéliens et des fermions de Majorana qui en sont une des versions. C'est une piste de réalisation de qubits explorée par Microsoft et Nokia, ce dernier via les Bell Labs aux USA.

Jürgen Mlynek (1951, Allemand) est un physicien spécialiste de l'optronique et de l'interférométrie. Il était le coordinateur du conseil stratégique à l'origine du lancement de l'European Flagship project sur le quantique en 2018. On lui doit comme, évoqué au sujet de Louis De Broglie, l'expérience validant la dualité ondes-particules des atomes réalisée en 1990 avec Olivier Carnal à l'Université de Constance, avec de l'hélium.

Marie-Anne Bouchiat (1934, Française) est une spécialiste de la physique des atomes de rubidium et notamment de leur contrôle par pompage optique. Ce sont les fondements de la création d'ordinateurs quantiques à base d'atomes froids. Sa fille **Hélène Bouchiat** (1958, Française) est également physicienne et spécialiste de la matière condensée, dans le laboratoire LPS de l'Université Paris-Sud et membre de l'Académie de Sciences depuis 2010, comme sa mère qui y siège depuis 1988.

Elisabeth Giacobino (1946, Française) est une spécialiste de la physique des lasers, de l'optique non-linéaire, de l'optique quantique et de la superfluidité, en liaison notamment avec le contrôle des atomes froids. Elle officiait au CNRS au sein du laboratoire Kastler-Brossel de l'ENS. Elle fait partie du comité scientifique de sélection des projets du flagship quantique européen ainsi que de l'ANR.

Jean Dalibard (1958, Français) est un physicien chercheur à l'ENS et enseignant à Polytechnique ainsi qu'au Collège de France. C'est un spécialiste de l'optique quantique et des interactions entre les photons et la matière[68]. Il avait participé avec Philippe Grangier au montage de l'expérience d'Alain Aspect en 1982 alors qu'il était scientifique du contingent à l'Institut d'Optique. Il est membre de l'Académie des Sciences depuis 2020.

[68] Voir notamment sa leçon sur les atomes froids au Collège de France qui décrit bien comment on refroidit des atomes à très basses températures avec des lasers.

Jacqueline Bloch (1967, Française) est une ingénieure-chercheuse qui travaille sur le couplage entre lumière et matière à l'aide de semi-conducteurs. Directrice de Recherche au sein du Centre de Nanosciences et de Nanotechnologies (C2N) du CNRS, c'est une grande spécialiste des polaritons, des quasi-particules qui associent des photons et des dipôles magnétiques à base d'arséniure de gallium. Ceux-ci ont des applications potentielles dans la création de simulateurs quantiques à base de réseaux de polaritons ainsi que pour la métrologie quantique (source).

Jean-Michel Gérard (1962, Français) est un physicien du laboratoire IRIG du CEA à Grenoble et directeur du laboratoire PHELIQS (PHotonique, ELectronique et Ingénierie QuantiqueS) qui associe l'Université de Grenoble et le CEA (c'est une UMR : Unité Mixte de Recherche). Il travaille notamment sur la création de sources de photons uniques à base de quantum dots ainsi que sur des détecteurs de photons uniques à base de nanofils supraconducteurs et sur des diodes laser OPO.

Pascale Senellart (1972, Française) est une physicienne, directrice de recherche du CNRS au laboratoire C2N de Palaiseau. Elle est médaille d'argent CNRS 2014. Elle a inventé un procédé de production de photons uniques et indiscernables, fabrication comprise. Elle est cofondatrice et directrice scientifique de la startup Quandela qui est spécialisée dans la commercialisation de ces sources de photons. Ce sont des composants à base de quantum dots semiconducteurs piégés dans une structure 3D et alimentés par un laser.

Ces sources de photons peuvent servir à différents usages comme la création d'ordinateurs quantiques à base de photons ou à des systèmes de télécommunications quantiques. Pascale est aussi coordinatrice du hub Quantum du plateau de Saclay qui a été lancé en novembre 2019 et qui rassemble les différents laboratoires de recherche publics et privés ainsi que les établissements d'enseignement supérieur.

Maud Vinet (1975, Française) coordonne au CEA-Leti de Grenoble la filière des qubits silicium. Elle avait auparavant contribué à l'industrialisation de la technologie SOI utilisée par SOITEC et FD-SOI[69], commercialisée par STMicroelectronics, deux technologies qui réduisent la consommation électrique et améliorent la performance des chipsets en CMOS, notamment dans la mobilité. Le Leti est focalisé sur l'ingénierie de la création de qubits à base de composants silicium fabricables en technologie CMOS.

Nous décrirons ces travaux plus en détail plus loin dans cet ebook. La filière des qubits silicium associe plusieurs laboratoires en plus du CEA-Leti : l'IRIG (aussi du CEA), l'Institut Néel du CNRS, le LPMMC et diverses entités de l'UGA (Université Grenoble Alpes). Maud pilote aussi un projet du Flagship quantique européen qui coordonne la recherche fondamentale sur les qubits silicium attribué en mars 2020, après avoir obtenu avec Tristan Meunier (Néel) et Silvano de Francesci (IRIG) un financement européen ERC de 14M€ en 2018 pour le projet QuQube de qubits silicium.

Alexia Auffèves (1976, Française) est directrice de recherche du CNRS, spécialiste de la thermodynamique quantique. Basée à l'institut Néel de Grenoble, elle étudie notamment les notions d'échelle de temps, d'irréversibilité et leurs liens avec la mesure et la décohérence des qubits. Ses travaux récents portent sur la formalisation de l'avantage énergétique du calcul quantique par rapport au calcul classiques et à la manière de le préserver avec l'augmentation du nombre de qubits tout en tenant compte des capacités de refroidissement des cryostats.

[69] FD-SOI = Fully-Depleted Silicon on Insulator. La technologie utilise d'une part une couche d'isolant en oxide de silicium et d'autre part, des canaux de transistors en silicium non dopé entre le drain et la source, limitant les fuites entre ces deux derniers.

Elle a aussi développé une ontologie de la mécanique quantique dénommée CSM (Contexts, Systems and Modalities) avec Philippe Grangier et la philosophe Naila Farouki[70]. Elle contribue activement aux efforts coordonnés des laboratoires de Grenoble pour la création d'ordinateurs quantiques autour de la notion de quantum engineering, en tant que coordinatrice de QuEng, ainsi qu'à la vulgarisation grand public de la mécanique quantique[71].

Eleni Diamanti (1977, Franco-grecque) est une grande spécialiste de la cryptographie et des télécommunications quantiques. Directrice de recherche au CNRS, elle est enseignante-chercheuse au LIP6 et à l'Université Paris-Sorbonne. Elle coordonne le hub quantique de Paris avec Iordanis Kerenidis depuis avril 2020. Je l'avais croisée lors de L'Echappée Volée en juillet 2018 où elle réalisait la performance d'expliquer l'informatique quantique en 8 minutes (vidéo).

Hélène Perrin (c. 1975, Française) est une spécialiste des atomes froids, œuvrant au Laboratoire de Physique des Lasers (LPL) de Paris 13. Elle pilote avec Pascal Simon le projet Quantum Simulation SIM, un simulateur quantique à base d'atomes froids, l'une des branches de l'informatique quantique parallèlement avec celle des ordinateurs quantiques à portes universelles. Elle donne aussi des cours sur l'informatique quantique, dont un excellent, fourni en bibliographie et cité plusieurs fois sur les qubits supraconducteurs et à ions piégés.

[70] Voir Contexts, Systems and Modalities: a new ontology for quantum mechanics par Alexia Auffèves et Philippe Grangier, 2015 (9 pages). Voir aussi la page Wikipedia associée. Ce travail a été articulé sur un total de sept publications parues entre 2015 et 2019.

[71] Voir Donner du sens à la mécanique quantique par Sylvain Guilbaud, une interview dans le journal du CNRS avec Alexia Auffèves et Philippe Grangier, 2016.

Andrew S. Dzurak (Australien) est le Directeur de l'unité de fabrication de nanotechnologies du centre de recherche CQC2T de l'UNSW qui en fabrique les qubits silicium, l'Australian National Fabrication Facility. Andrew Dzurak est un pionnier des qubits silicium sur lesquels il travaille depuis 1998. Il en pilote la recherche au CQC2T en travaillant sur le contrôle et la lecture des qubits silicium. C'est l'une des stars du quantique australien.

Il avait créé les premiers doubles qubits silicium à base de phosphore en 2015. C'est le boss de Michelle Simmons (*ci-dessous*).

Michelle Simmons (1967, Anglo-Australienne) est une physicienne de l'Université de Nouvelle Galle en Australie (UNSW), spécialisée dans la branche de l'informatique quantique qui s'appuie sur le contrôle de spins d'électrons dans du silicium. Elle est la cofondatrice de la startup Silicon Quantum Computing (Australie, $66M). C'est une spinoff de son université et de son laboratoire Centre of Excellence for Quantum Computation and Communication Technology (CQC2T).

Andrea Morello (1972, Italien) est un des chercheurs stars de l'UNSW en Australie. Il est Program Manager de l'ARC Centre of Excellence for Quantum Computation and Communication Technology (CQC2T) et dirige le laboratoire de technologies quantiques de l'UNSW. Lors de ses études, il était passé par Laboratoire National des Champs Magnétiques Intenses du CNRS à Grenoble. C'est aujourd'hui l'un des spécialistes des qubits silicium.

Christine Silberhorn (1974, Allemande) est une chercheuse spécialisée dans l'informatique quantique à base de photons. Officiant dans l'Université de Paderborn située entre Dortmund et Hanovre dans le groupe Integrated Quantum Optics qu'elle y dirige. Son laboratoire conçoit et fabrique des composants d'optronique intégrés, des sources de photons intriquées et des systèmes de réseaux quantiques. Elle planche aussi sur les mémoires quantiques optiques.

Stephanie Wehner (1977, Allemande) est une physicienne spécialisée dans le développement de protocoles de communication quantique, basée à l'université de Delft aux Pays-Bas. Elle coordonne la « Quantum Internet Alliance", l'un des projets du Flasgship Quantique européen qui ambitionne de déployer un réseau Internet protégé par clés quantiques (QKD) en mode réseau maillé. Elle a démarré sa vie professionnelle dans la cybersécurité, détectant les failles de systèmes.

Perola Milman (c. 1975, Française) est une spécialiste de la théorie de l'informatique quantique et notamment des photons et ions piégés. Elle a en particulier démontré la capacité d'intrication de molécules. Elle est enseignante-chercheuse du Laboratoire Matériaux et Phénomènes Quantiques de l'Université Paris Diderot. Elle enseigne sur la théorique quantique de la lumière ainsi que sur l'intrication quantique.

Sara Ducci (1971, Française) est une autre enseignante-chercheuse du même Laboratoire Matériaux et Phénomènes Quantiques (MPQ) où elle avait cofondé en 2002 une équipe en charge de dispositifs optiques non linéaires. Elle est spécialisée dans les sources de photons doubles, notamment à base de semiconducteurs III-V. Elle s'intéresse aussi à la caractérisation (mesure de l'état…) et à la manipulation des photons. Elle enseigne aussi à l'Ecole Polytechnique.

Jacquiline Romero (c. 1985, Philippines) est une physicienne spécialiste de l'optique quantique et de l'intrication qui fait de la recherche en Australie dans l'Université de Queensland après avoir réalisé son doctorat au Royaume Uni à Glasgow. Elle travaille notamment sur les architectures neuromorporphiques optiques et sur l'encodage dense d'informations dans des photons utilisant plusieurs de leurs caractéristiques en plus de l'habituelle phase.

Patrice Bertet (c. 1976, France) fait partie de l'équipe de Daniel Estève du CEA-SPEC. Il a fait sa thèse chez Serge Haroche sur les atomes de Rydberg puis fait un passage à l'Université de Delft. Il a participé aux débuts des qubits supraconducteurs (quantronium du CEA et chez Delft). Il s'est ensuite consacré aux circuits QED (quantum electro dynamics) qui sont à base de cavités puis aux qubits transmon.

Il travaille sur l'association de qubits supraconducteurs et de mesure de leur état avec des spins d'électrons, notamment à base de NV centers, ces derniers pouvant aussi servir de mémoire quantique par échange de photons micro-ondes avec les qubits supraconducteurs.

Audrey Bienfait (c. 1990, France) est une ancienne thésarde de Patrice Bertet au CEA-SPEC qui fait maintenant ses recherches à l'ENS Lyon dans l'équipe de Benjamin Huard. Elle est lauréate du Bruker Prize 2018 pour sa thèse sur la résonance paramagnétique électronique ou "ESR - Electron Spin Resonance" en régime quantique et du Michelson Postdoctoral Prize 2019 en mars 2020 pour ses travaux sur l'intrication de qubits supraconducteurs via des phonons.

Sébastien Tanzilli (France) est le directeur du laboratoire de physique InPhyNi de Nice. Il est spécialisé en photonique et plus particulièrement en cryptographique quantique à clés continues ou discrètes (CV-QKD et DV-QKD), en optique quantique fondamentale ainsi que dans les systèmes quantiques hybrides pour l'étude et la réalisation de réseaux de communication quantique. Il était aussi le président du GDR-IQFA jusqu'en 2019, une communauté des chercheurs en physique quantique en France (IQFA = Information Quantique, Fondements & Applications).

Virginia D'Auria (Italie) est une chercheuse spécialisée dans les systèmes de transmission en optique quantique à variables continues et discrètes et hybrides DV/QV. Passée par le laboratoire LKB de l'ENS Paris, elle a aussi travaillé sur les détecteurs de photons. Elle fait partie depuis 2010 du groupe de photonique de l'InPhyNi et travaille sur les communications quantiques à variables discrètes et continues compatibles avec les fibres optiques des opérateurs télécoms.

Fabio Sciarrino (1978, Franco-Italien) dirige le laboratoire Quantum Information Lab de l'Université Sapienza à Rome qui est spécialisé en photonique. Son équipe est à l'origine de nombreuses avancées dans le domaine, notamment dans l'échantillonnage de bosons, une catégorie d'expérience permettant d'avancer dans la création d'ordinateurs quantiques à base de qubits photons. Il collabore à ce titre avec l'équipe de Quandela et du C2N de Palaiseau (Pascale Senellart).

Jelena Vucokic (c. 1975, Serbe) est enseignante chercheuse à Stanford, spécialisée en photonique quantique. Elle y dirige le Nanoscale and Quantum Photonics Lab et le Q-FARM (Quantum Fundamentals, ARchitecture and Machines initiative), un laboratoire quantique interdisciplinaire. Elle contribue aux développements en photonique qui serviront au développement d'ordinateurs quantiques optiques. Elle avait fait sa thèse à Caltech en 2002.

Francesca Ferlaino (1977, Italienne) et une chercheuse typiquement européenne, étant passée par plusieurs laboratoires de plusieurs pays. Elle est directrice de recherche à l'IQOQI d'Innsbruck en Autriche où elle dirige le laboratoire Dipolar Quantum Gases. C'est une spécialiste des atomes froids et des condensats Bose-Einstein, notamment à base d'erbium. C'est de la recherche en physique fondamentale très en amont de la création éventuelle de qubits ou de métrologie quantique.

Marcus Huber (Autriche) est un responsable de groupe de recherche de l'IQOQI à Vienne, spécialisé dans l'intrication quantique, la mesure de l'état des qubits et la thermodynamique quantique en général. En plus de l'IQOQI, il a aussi œuvré dans les Universités de Bristol, de Genève et de Barcelone. Il est un grand avocat de la publication ouverte de travaux de recherche, étant à l'origine du site Quantum-Journal.org, sorte de Arxiv du quantique.

Tracy Northrup (c. 1975, Autriche) est une chercheuse spécialisée dans les ions piégés et les cavités optiques pour les piéger, l'une des grandes branches du calcul quantique. Elle dirige le laboratoire Quantum Interfaces Group de l'Université d'Innsbrück qui est l'une des plus actives dans le domaine des ions piégés, une grande spécialité autrichienne.

Anne Matsuura (c. 1970, Japonaise-Américaine) est une physicienne qui dirige depuis 2014 le laboratoire de recherche quantique des Intel Labs « Quantum & Molecular Technologies ». Elle pilote les efforts de l'Américain dans la création d'ordinateurs quantiques supraconducteurs et silicium, avec une vision d'ensemble de l'architecture matérielle. Son parcours impressionnant démarre avec une thèse à Stanford dans les synchrotrons, passe par les labs de l'US Air Force et par In-Q-Tel (le fonds d'investissement de la CIA) et a dirigée l'European Theoretical Spectroscopy Facility à partie de la Belgique.

Sarah Sheldon (c. 1986, Américaine) fait partie depuis 2013 des équipes d'IBM qui planchent sur l'informatique quantique, basées au centre de recherche TJ Watson à Yorktown dans l'Etat de New York. Elle est notamment active dans le domaine de la qualité des qubits supraconducteurs et de leurs portes quantiques et des codes de correction d'erreurs. Elle avait obtenu son doctorat au MIT en 2013 avant de faire un post-doc chez IBM.

Stefanie Barz (c. 1980, Allemande) est enseignante en optique quantique à l'Université de Stuttgart. Elle s'intéresse notamment à la cryptographie et aux télécommunications quantiques. Elle a notamment travaillé sur le blind computing. Elle pilote le projet SiSiQ financé par le Ministère de la Recherche allemand et doté de 3,6M€ de financements européens.

Alexei Grinbaum (1978, Franco-Russe) est un chercheur du CEA-Saclay dans le laboratoire LARSIM d'Etienne Klein. Il planche sur les fondations de l'informatique quantique et sur la philosophie de la physique quantique[72]. Il est notamment l'auteur de l'ouvrage « Les robots et le mal » publié en 2018. Il s'intéresse en particulier à l'éthique des sciences, à leur acceptation par la société et à l'innovation responsable.

[72] Voir notamment Narratives of Quantum Theory in the Age of Quantum Technologies par Alexei Grinbaum, 2019 (20 pages).

Frédéric Grosshans (Français) est un chercheur du CNRS (LIP6 Paris-Sorbonne) spécialisé dans la QKD, les répéteurs et les réseaux quantiques. Il est aussi le co-directeur avec Nicolas Treps (du LKB) du Quantum Information Center Sorbonne de l'Alliance Paris Sorbonne lancé en septembre 2020 qui fédère la recherche et la formation quantique de plusieurs entités parisiennes.

Cet inventaire de scientifiques, *ci-dessus* comme *ci-dessous* n'est pas bâti sur des critères rigoureux et quantifiés. Ce sont des personnalités que j'ai découvertes au fil de l'eau dans mes recherches d'informations sur le sujet. Il résulte aussi, souvent, de rencontres, surtout pour ce qui est des scientifiques français.

Créateurs d'algorithmes quantiques

Terminons ce long "hall of fame" avec quelques-uns des principaux contributeurs à la création d'algorithmes quantiques, une discipline relativement nouvelle qui a vu le jour au début des années 1990.

Paul Benioff

Umesh Virkumar QFT **Vazirani**

David algorithme de **Deutsch**

Peter algorithme de **Shor**

Lov recherche **Grover**

Andrew QEC **Steane**

Aram algorithmes **Harrow**

Scott algorithmes **Aaronson**

Bettina software **Heim**

Gil ça ne marchera jamais **Kalai**

Dave Wecker

Alan chimie quantique **Aspuru-Guzik**

John Watrous

Kristel QRTL **Michielsen**

Miklos Santha

Matthias Troyer

Cyril Allouche

Philippe Duluc

Elham protocoles **Kashefi**

Stephanie QCC **Wehner**

Shi simulateur **Yaoyun**

Iordanis Kerenidis

Ryan Babbush

Daniel QEC **Gottesman**

Michael Freedman

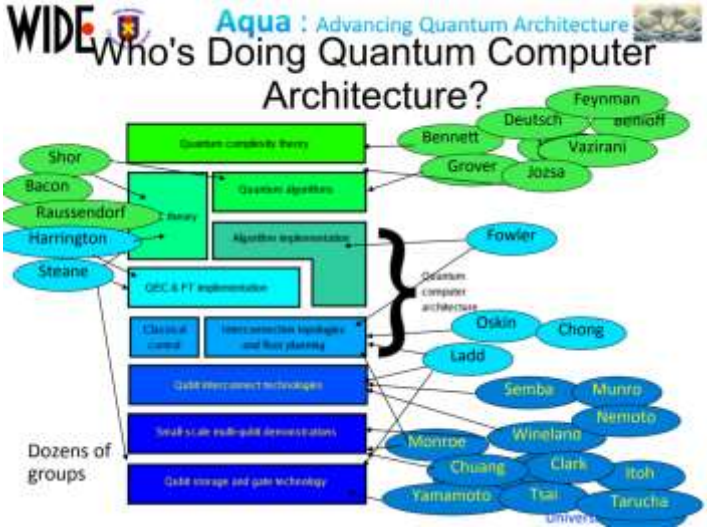
Alexei Kitaev

Leo Kouvenhoven

Charles Marcus

Benoît Quipper **Valiron**

Autre manière de voir les choses, extraite de la présentation Quantum Computer Architecture Rod Van Meter, 2011 (89 slides). Histoire de n'oublier personne !



Avec en vert, les spécialistes des algorithmes quantiques, en bleu clair, ceux des codes de correction d'erreurs, et en bleu foncé, ceux des couches physiques des qubits.

Tous ne sont malheureusement pas cités dans cet ouvrage. Cette liste continuera certainement de s'enrichir d'année en année tant le domaine est en évolution permanente.

Paul Benioff (1930, Américain) est un physicien pionnier de l'informatique quantique théorique dont il a défini les bases théoriques dans les années 1980, parallèlement à Richard Feynman dont l'idée concernait la simulation quantique. Son modèle prévoyait la possibilité de réaliser du calcul quantique réversible. A noter qu'il est passé quelques temps par le CNRS en France entre 1979 et 1982, à l'Université de Marseille-Luminy.

Alexander Holevo (1943, Russe) est un mathématicien russe spécialiste de l'information quantique et à qui l'on doit le théorème qui porte son nom selon lequel on ne peut pas récupérer plus de N bits d'information utile d'un registre de N qubits et créé en 1973[73]. C'est la conséquence de la réduction du paquet d'onde qui rabat l'état du qubit sur ses états propres $|0\rangle$ et $|1\rangle$ au moment de la lecture. Il a aussi développé les bases mathématiques de la communication quantique.

Umesh Virkumar Vazirani (1945, Indien) est enseignant à l'Université de Berkeley. C'est l'un des fondateurs du calcul quantique, avec son papier coécrit en 1993 avec son étudiant Ethan Bernstein, Quantum Complexity Theory, pas facile à piger pour le profane. Il est aussi le créateur de l'algorithme de la transformée de Fourier quantique (QFT) qui utilisé moins d'un an plus tard par Peter Shor pour la création son fameux algorithme de factorisation de nombres entiers qui a servi d'aiguillon pour le financement de la recherche dans le calcul quantique aux USA.

Peter Shor (1959, Américain) est un mathématicien devenu le père de l'algorithme du même nom en 1994 qui permet la factorisation d'entiers en nombres premiers, à base de transformées de Fourier quantiques, construit avec un algorithme de transformée quantique de Fourier (QFT). Il est aussi à l'origine d'un algorithme de correction d'erreurs d'amplitude (flip error) et de phase à neuf qubits pour les ordinateurs quantiques dénommé « Shor code ».

On lui doit indirectement tout le mouvement de la cryptographie post-quantique qui vise à créer des systèmes de cryptographie résistant au cassage de clés publiques via son algorithme… avec des calculateurs quantiques qui n'existent pas encore. Peter Shor a créé son fameux algorithme de factorisation alors qu'il travaillait aux Bell Labs. Il enseigne les mathématiques appliquées au MIT depuis 2003.

David Deutsch (1953, Israélien et Anglais) est un physicien du laboratoire d'informatique quantique de l'Université d'Oxford au Royaume-Uni. Il est l'auteur d'un algorithme de recherche qui porte son nom, avec deux variantes, une première en 1985 et une seconde en 1992 co-créée avec Rochard Jozsa. L'algorithme est très performant mais n'a pas de véritable utilisation pratique. On lui doit l'idée de l'ordinateur quantique à portes universelles en 1985, complétant celle de simulateur quantique de Richard Feynman de 1981.

Michael Freedman (1951, Américain) est un mathématicien Médaille Fields en 1986 qui a fondé et dirige le laboratoire Microsoft Station Q à Santa Barbara en Californie. Il est l'un des pères de l'informatique quantique topologique avec Alexei Kitaev. Et puis, au passage, il a aussi obtenu la médaille Fields en 1986 pour ses travaux sur la conjecture de Poincaré, démontrée plus tard en 2006 par Grigori Perelman.

[73] Ce théorème valide indirectement le fait qu'il est difficile de faire du « big data » avec un ordinateur quantique au sens du stockage et de l'analyse de gros volumes d'information. Par contre, l'algorithme de Grover permet de retrouver rapidement une aiguille dans une botte de foin, nous le verrons plus loin.

Alexei Kitaev (1963, Russe et Américain) est avec Michael Freedman l'un des pères du concept d'ordinateur quantique topologique en 1997, utilisé par Microsoft. Il était chercheur chez Microsoft Research au début des années 2000 et est maintenant à l'Université de Caltech. On lui doit aussi de nombreux travaux sur les codes de correction d'erreurs dont la création des *surface codes* et de la *magic states distillation* (avec **Sergey Bravyi**) ainsi que l'algorithme d'estimation de phase quantique (Quantum Phase Estimate), utilisé dans l'algorithme de Shor de factorisation de nombres entiers.

Aram Harrow (Américain) est un spécialiste prolifique des algorithmes quantiques. Il enseigne au MIT à la fois la physique quantique et l'informatique quantique. Au MIT, il est entouré de Peter Shor et Charles Bennett. Il est l'auteur de l'algorithme quantique HHL de résolution d'équations linéaires qu'il a créé conjointement avec Avinatan Hassidim et Seth Lloyd[74]. Il s'intéresse aussi à la création d'algorithmes hybrides classiques/quantiques.

Daniel Gottesman (1970, Américain) est un physicien du Perimeter Institute de Waterloo au Canada. Il a fait sa thèse à Caltech sous la supervision de John Preskill. Il est connu pour ses travaux sur les codes de correction d'erreurs quantiques (QEC) et est coauteur du théorème de Gottesman–Knill. Selon ce dernier, on peut simuler de manière efficace (sous-entendu, sans décalage exponentiel) un algorithme quantique sur un calculateur classique dans certaines conditions.

Cela concerne les algorithmes qui utilisent des portes quantiques dites du groupe de Clifford (les portes unitaires dites de Pauli), une rotation de phase d'un quart de tour (de la sphère de Bloch), la porte de superposition d'Hadamard et la porte conditionnelle CNOT. Ce théorème prouve donc indirectement qu'un jeu de porte basique est insuffisant pour générer un avantage quantique exponentiel.

Gil Kalai (1955, Israélien) est un professeur de mathématiques de l'Université Hébraïque de Jérusalem et à Yale. Il est l'inventeur de nombreux algorithmes. Son ambition est de démontrer mathématiquement qu'il sera impossible aux ordinateurs quantiques universels de monter en puissance. En cause, leur taux d'erreurs, même avec des codes de correction d'erreurs et la notion de qubits logiques qui assemblent des qubits physiques.

Scott Aaronson (1981, Américain) enseigne les sciences de l'information à l'Université d'Austin au Texas. C'est un grand spécialiste des algorithmes quantiques et des théories de la complexité. Il est notamment à l'origine d'un algorithme quantique d'échantillonnage de bosons ("boson sampling"). Les bosons sont les particules de spin entier comme les photons alors que les particules comme les électrons, les neutrons et les protons sont des fermions, avec un spin 1/2.

Les bosons peuvent fonctionner en meute, comme les photons dans un laser, tandis que les fermions ne peuvent cohabiter au même endroit dans le même état.

Andrew Steane (1965, Anglais) est un professeur de physique de l'Université d'Oxford. Il est à l'origine de codes de correction d'erreurs quantiques qui portent son nom et qu'il a conçus en 1996. Ce code corrige les erreurs de flip et de phase sur un seul qubit.

[74] Voir Quantum algorithm for linear systems of equations, 2009 (24 pages).

Dorit Aharonov (1970, Israël) est une chercheuse en algorithmie quantique. Elle a fait son doctorat en Computer Science en 1999 à l'Université Hébraïque de Jérusalem sur le thème "Noisy Quantum Computation" puis un post-doc à Princeton et à Berkeley. On lui doit le « quantum threshold theorem" co-démontré avec Michael Ben-Or qui stipule qu'en dessous d'un certain seuil de taux d'erreur, on peut appliquer des codes de correction d'erreur de manière récursive pour obtenir un taux d'erreur arbitrairement bas de qubits logiques. Son oncle est **Yakir Aharonov** (1932, Israélien), un physicien qui avait notamment travaillé avec David Bohm.

Alan Aspuru-Guzik (circa-1978, Américain) est un directeur de recherche de l'Université de Toronto, anciennement à Harvard, qui a notamment créé divers algorithmes de chimie quantique, un sujet que j'aborderais dans la partie consacrée aux algorithmes quantiques. Il est aussi le cofondateur de la startup Zapata Computing qui développe des frameworks logiciels pour le calcul quantique, notamment dans la simulation chimique.

Elham Kashefi (1973, Iranienne) est une spécialiste des protocoles de communication quantiques ainsi que du « blind quantum computing », que nous aurons l'occasion d'expliquer. Elle est aussi co-fondatrice de la startup de télécommunications quantiques sécurisées VeriQloud. Elle gère des recherches à cheval entre Edimbourg et Paris au LIP6 (Jussieu). Elle a créé le protocole de blind computing BFK en 2009 avec Anne Broadbent et Joe Fitzsimons qui est associé au MBQC.

Avec son équipe du LIP6, elle est à l'origine de la création d'un site sur le zoo des protocoles de communication quantique[75]. Et comme cela ne suffit pas, elle est aussi versée dans les Quantum Physical Unclonable Functions (QPUF), des identifieurs physiques d'objets de nature quantique et inclonables que nous explorerons dans une édition à venir de cet ebook.

Mazyar Mirrahimi (circa 1980, Iranien) est un mathématicien qui a trempé dans la physique quantique. Il est actuellement directeur du laboratoire Quantic de l'Inria qui est spécialisé dans les codes de correction d'erreurs et les algorithmes quantiques, entre autres sujets. Ceux-ci sont utilisés par les cat-qubits supraconducteurs de la startup Alice&Bob.

Zaki Leghtas (Maroc/France) est un chercheur basé en France dans l'équipe de Mazyar Mirrahimi qui est notamment spécialisé dans les codes de correction d'erreur. Il est notamment l'un des créateurs des cat-codes qui permettent de corriger les erreurs du calcul quantique avec un nombre minimum de qubits. Il est passé par le laboratoire de Michel Devoret à Yale avant de rejoindre l'équipe Quantic de l'Inria en 2015.

Shi Yaoyun (1976, Chinois) est professeur à l'Université du Michigan et aussi dirigeant du laboratoire quantique d'Alibaba. Il est à l'origine de divers records de simulation quantique sur des clusters de serveurs que nous allons décrire dans cet ebook. Il avait obtenu un PhD en computer science à Stanford.

Kristel Michielsen (cica-1969, Belge) est une physicienne œuvrant à l'université d'Aix la Chapelle en Allemagne. Elle a contribué à de nombreux travaux en informatique quantique aussi bien côté physique que côté algorithmes. Elle est à l'origine de la création de l'échelle QTRL, pour Quantum Technology Readiness Level qui sert à évaluer le niveau de maturité des technologies quantiques et que nous allons évoquer dans la partie dédiée aux pratiques dans la recherche.

[75] Voir https://wiki.veriqloud.fr/index.php?title=Protocol_Library.

John Watrous (Canadien) est un chercheur de l'Université de Waterloo au Canada spécialisé dans les algorithmes quantiques et les théories de la complexité. Il a déjà collaboré avec Scott Aaronson. Il est l'auteur du volumineux The Theory of Quantum Information, 2018 (598 pages).

Ryan Babbush (circa-1989, Américain) est un chercheur de Google spécialisé dans la création d'algorithmes de simulation de phénomènes physiques quantiques impossibles à simuler sur supercalculateurs. Il vise à créer des solutions commerciales de chimie quantique. Dans une présentation de février 2020, on y découvre que la simulation chimique avec le processeur Sycamore de Google ne peut pas dépasser 12 qubits à cause du taux d'erreur dans les calculs.

Matthias Troyer (1968, Autrichien) est professeur de physique computationnelle à l'ETH Zurich. Il a rejoint Microsoft Research à Redmond début 2017. Il est l'un des créateurs du langage Q# de programmation quantique ainsi que du framework open source ProjectQ lancé en 2016 par l'ETH Zurich. Il s'intéresse notamment à la simulation chimique avec des ordinateurs quantiques. Il avait obtenu son doctorat à l'ETH Zurich en 1994.

Iordanis Kerenidis (c. 1980, Grec) est un chercheur du laboratoire IRIF (Institut de Recherche en Informatique Fondamentale) du CNRS, spécialisé en cryptographie, en communication quantique, dans les théories de la complexité quantique et surtout, dans le quantum machine learning. A noter qu'il a fait sa thèse au MIT sous la direction de Peter Shor et travaillait dans le même bureau que Scott Aaronson ! Il fait partie de l'équipe fondatrice de la startup américaine QCWare. Il y dirige la R&D en algorithmie quantique.

Il coordonne aussi l'écosystème parisien quantique (PCQC) avec Eleni Diamanti. Il était l'un des membres de la mission parlementaire sur le quantique pilotée par la députée Paula Forteza entre avril 2019 et janvier 2020.

Benoît Valiron (1980**,** France) est un chercheur du laboratoire LIRI du CNRS et l'un des rares enseignants des algorithmes et de la programmation quantiques. Il officie à CentraleSupelec et à l'Université d'Orsay. Ce spécialiste de la programmation quantique est le co-auteur du langage de programmation quantique open source Quipper à la création duquel il avait contribué alors qu'il était à University de Pennsylvanie.

Bettina Heim (c. 1980) est une développeuse de Microsoft spécialisée en logiciels quantiques. Elle est responsable du développement du compilateur du langage de programmation quantique Q# dont Microsoft fait la promotion depuis 2017 et qui fait partie de leur Quantum Development Kit, pour l'instant tournant sur émulateurs quantiques sur processeurs traditionnels.

Cristian Calude (1952, Roumain/Néo-Zélandais) et **Elena Calude** (Roumaine/Néo-Zélandaise) sont un couple de chercheurs de l'Institute of Information Sciences, de l'Université d'Albany à Auckland en Nouvelle Zélande. Ils sont spécialistes de l'algorithmie quantique, des algorithmes quantiques hybrides et des théories de la complexité.

Ewin Tang (2000, Américaine) a publié en juillet 2018 un papier démontrant un algorithme de recommandation classique aussi performant qu'un algorithme conçu pour les ordinateurs quantiques de D-Wave et conçu notamment par Iordanis Kerenidis en France[76]. Ce dernier a répondu en trouvant une faille dans le raisonnement. Vu de près, l'algorithme quantique de ce dernier était toutefois plus performant. Elle avait 18 ans à l'époque. Donc, à surveiller de près !

Sophia Economou (c. 1980, Gréco-Américaine) est une physicienne, professeure associée du Département de Physique du Virginia Tech College of Science. Elle travaillait auparavant à l'US Naval Research Laboratory. C'est une spécialiste du contrôle de spins de quantum dots semiconducteurs et de leurs interfaces spin-photons. Elle est aussi créatrice d'algorithmes avancés de simulation moléculaire sur ordinateurs quantiques.

Philippe Duluc (1961, Français) est CTO en charge du big data et de la cybersécurité chez Atos. Il pilote les efforts du groupe Atos dans l'informatique quantique qui comprend notamment les émulateurs quantiques aQML à base de processeurs Intel et plus récemment Nvidia ainsi que les outils logiciels associés tels que myQML. Ingénieur de l'armement issu de l'Ecole Polytechnique et de l'ENSTA, il était initialement spécialisé dans la cybersécurité, notamment dans le groupe Bull.

Cyril Allouche (Français), dirige les efforts de R&D en informatique quantique chez Atos depuis leurs débuts en 2015. Il est l'un des rares français dans les équipes européennes du Flagship Quantique de l'Union Européenne. Philippe Duluc et Cyril Allouche sont les "implémenteurs" de la vision quantique de Thierry Breton, le CEO d'Atos jusqu'en 2019. C'est l'un des rares industriels français du numérique à faire le pari de l'informatique quantique. Si ce n'est le seul !

Ça en fait du monde ! Nous croiserons une bonne part de ces personnages lors des parties suivantes de cet ebook au gré des thèmes abordés. Et des contributeurs plus jeunes, parfois de moins de 40 ans, s'ajouteront plus tard à cette liste pour faire avancer la discipline de l'informatique quantique qui ne fait que commencer à poindre du nez !

Décoder la recherche

Dans ce voyage dans le paysage des sciences et technologies quantiques, j'ai découvert de près le monde de la recherche. Je dois reconnaître que je ne le connaissais pas bien avant cette aventure. J'y ai notamment découvert un certain nombre d'aspects que j'inventorie ici-même, notamment sur les pratiques et le jargon. Si vous êtes chercheur, c'est du b-a-ba. Pour les autres, cela précisera des connaissances un peu floues que vous auriez sur le sujet.

Long terme

Le premier point qui surprend dans les technologies quantiques et que l'on peut retrouver dans d'autres branches de la physique et des sciences dits dures est la dimension long terme de la recherche. La temporalité se chiffre en décennies. Dans pas mal de cas, elle démarre avec des intuitions, de la créativité, des passions, de la rigueur et des travaux qui ne font pas forcément l'unanimité dans l'establishment du moment[77].

---

[76] Voir A quantum-inspired classical algorithm for recommendation systems, Ewin Tang, juillet 2018 (32 pages) et Major Quantum Computing Advance Made Obsolete by Teenager par Kevin Harnett, juillet 2018.

[77] Voir Quantum Computing: Dream or Nightmare? par Serge Haroche et Jean Michel Raimond, Physics Today, 1995 (2 pages) qui exprimaient leur scepticisme sur le calcul quantique. Serge Haroche continue à véhiculer ce scepticisme.

Les travaux d'Alain Aspect qui démarrent dans la seconde moitié des années 1970 n'ont pas d'application industrielle immédiate. Heureusement, il est bien aidé par de nombreux laboratoires, notamment en termes d'instrumentation. Ses travaux ont depuis abouti à la création de nombre des branches des technologies quantiques. Artur Ekert s'était ainsi inspiré des travaux d'Alain Aspect pour faire avancer le champ de la cryptographie quantique au début des années 1990.

Il en va ainsi de nombre de travaux de recherche en physique fondamentale, comme dans la physique de la matière condensée, qui aboutissent maintenant à la fois à la création de qubits ainsi qu'à la grande diversité des applications de la métrologie quantique.

Mais tout cela ne se planifie pas à l'avance. Il faut préserver la sérendipité de la recherche. La valorisation intervient plus tard, par les rencontres entre spécialistes de disciplines différentes et complémentaires. Les innovateurs sont soit les chercheurs eux-mêmes, soit plus généralement d'autres, ingénieurs et entrepreneurs, qui savent dénicher les recherches à fort potentiel de valorisation. D'où l'importance de les rapprocher dans les écosystèmes d'innovations.

Cela génère pas mal d'incompréhensions du côté des pouvoirs publics qui sont tentés de trop évaluer et mesurer la performance de la recherche fondamentale, si ce n'est la financer, avec uniquement des critères issus du monde des entreprises. Par contre, et c'est particulièrement vrai pour les technologies quantiques, les travaux des chercheurs nécessitent une évaluation entre pairs. Cela les rend difficiles d'accès pour les décideurs des pouvoirs publics et donne l'impression que les chercheurs sont juges et parties. Pour éviter que cela rende méfiant, il faut faire de la traduction simultanée et vulgariser un maximum. Cela doit d'ailleurs pousser les chercheurs à communiquer vis-à-vis du grand public, ce qu'ils ne font pas forcément naturellement dans ces disciplines très pointues. C'est surtout une question de leadership. Bref, chacun doit faire face à ses propres défis !

Publications

Ce document contient de nombreuses références à des publications scientifiques. Je le fais quasi systématiquement et en particulier lorsque je découvre une nouvelle issue de la presse généraliste ou scientifique généraliste. J'en cherche toujours la publication scientifique d'origine.

Les publications scientifiques ont parfois lieu d'abord dans le fameux site **Arxiv** de l'université Cornell. Ce sont des « prépublications » d'articles qui ne sont pas encore passées par des revues à comité de lecture. Ces articles sont donc sujets à caution. Ils permettent cependant aux auteurs de récupérer des commentaires de lecteurs avisés. Leur quantité et qualité dépend de la notoriété des auteurs, du sujet, du nombre de chercheurs qui le maîtrisent et de l'écho qu'a obtenu cette première publication.

La publication de l'article dans une revue à comité d'auteur peut intervenir ensuite, entre 9 et 18 mois après. Il peut l'être aussi bien à l'identique qu'après des révisions suggérées par les « referees » des comités de relecture, voir même avec un changement de titre. Dans ces cas, la version publiée sur Arxiv n'est pas forcément la plus récente. L'avantage est que son accès est libre. En règle générale, lorsque je découvre l'existence d'un article, je le recherche sur Google Search avec le nom suivi de « filetype:PDF » et je le trouve en accès gratuit dans plus de 90% des cas dans Arxiv ou encore sur le site ResearchGate, le réseau social de référence des chercheurs.

Les revues à comité d'auteur de référence pour les technologies quantiques comprennent notamment **Nature** et ses différentes déclinaisons thématiques, **Science**, **PRX**, **Physical Review Research**, **Physical Review Letters**, **Quantum Science and Technology**, **Journal of Applied & Computational Mathematics**, **International Journal of Quantum Information, Quantum Engineering**, **Advanced Quantum Technologies**, **Quantum Journal**, **Quantum Information Processing**, **IEEE Journal of Quantum Electronics** et **IEEE Transactions on Quantum Engineering**. On y trouve heureusement peu ou pas de revues prédatrices sans comités d'auteurs et faisant payer les chercheurs pour les publications de leurs travaux.

Les thèses de doctorat sont plus faciles à récupérer et sont généralement publiées librement. Elles sont de bonnes sources d'informations bibliographiques car, au-delà d'un point particulier qui fait éventuellement avancer l'état de l'art, elles en font d'abord généralement un bon inventaire.

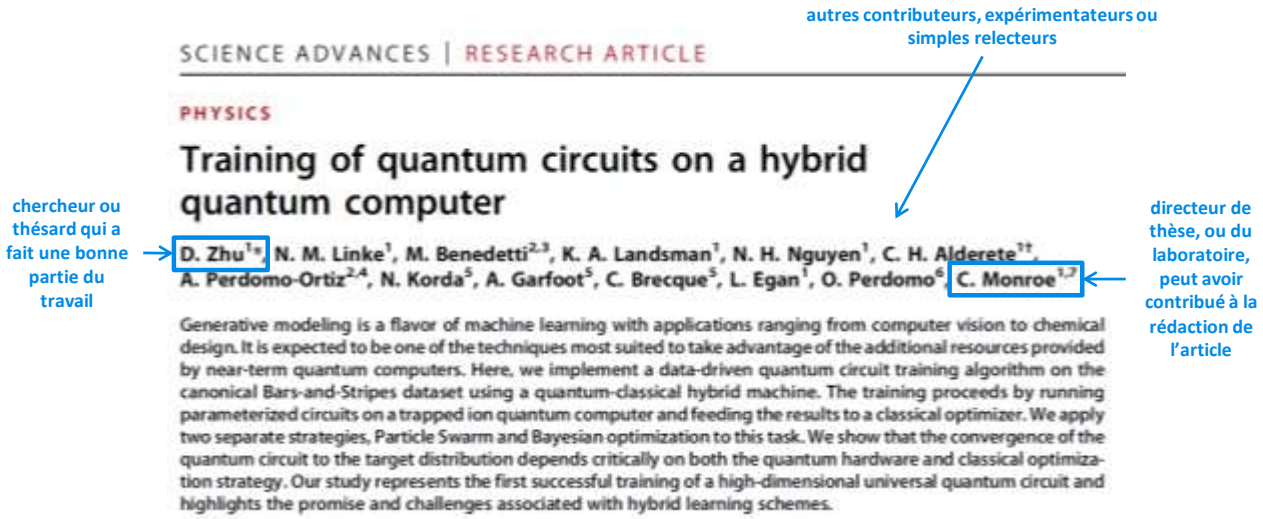
Si la pédagogie de l'auteur est de bon niveau, cela peut être très utile pour l'apprentissage et la mise à niveau des connaissances. Une bibliographie généralement fournie permet ensuite d'approfondir le sujet en découvrant les textes fondamentaux.

Pour des publications plus courtes, de quelques dizaines de pages, une très abondante bibliographie (et le titre) indiquent souvent qu'il s'agit surtout d'une revue synthétique de l'état de l'art.

Dans une publication scientifique, plusieurs auteurs sont généralement cités. Il peut y avoir un très grand nombre. En général, au-delà de trois auteurs, le premier est celui qui a fait le plus gros boulot et en général un thésard. Il/elle a traité les données d'expérience et rédigé une bonne part du document, mais cela peut dépendre de pays, des laboratoires et des encadrants de thèses. Le dernier est le directeur de thèse ou du laboratoire de recherche[78]. Dans ce dernier cas, l'avant-dernier auteur est le directeur de thèse qui a encadré le travail de près.

Entre les deux se trouvent les autres contributeurs, expérimentateurs ou simples relecteurs actifs. Lorsque l'on cite un article et que l'on souhaite éviter de citer tous les auteurs, on utilise l'expression « et al » qui est une abréviation du latin « et alia » signifiant « et les autres ».

Dans de nombreux pays comme aux USA, l'habitude est fréquente de citer les auteurs avec l'initiale de leur prénom et de leur *middle name*, ce qui ne rend pas ensuite leur recherche facile, en particulier pour des auteurs chinois. C'est notamment le cas lorsque les contributeurs sont très nombreux.



[78] C'est le cas de ces centaines de publications avec le fameux Didier Raoult qui y est cité comme le dernier contributeur, en tant que directeur de laboratoire mais pas forcément directeur de thèse.

Certains papiers, comme celui de la suprématie quantique de Google sont complétés par des « *supplemental materials* » avec des détails techniques pouvant être très intéressants, notamment pour décrire l'ingénierie de dispositifs. On peut les repérer car ils sont généralement cités à la fin des papiers principaux.

Il existe une catégorie à part de papiers scientifiques : les **review papers** qui font un état de l'art d'un domaine. Leur bibliographie est en général imposante, parfois aussi longue que le papier lui-même. Ce sont de bonnes bases de départ pour étudier un sujet, surtout si le papier n'est pas trop ancien.

On découvre ces publications scientifiques en suivant les flux RSS de revues spécialisées de renom et, en complément, via l'actualité scientifique de médias en ligne ou de la presse scientifique de vulgarisation. J'en découvre aussi en compulsant les présentations de conférences scientifiques qui sont parfois des puits sans fonds plein de présentations très intéressantes. Cela remplit régulièrement ma « baignoire » à vider de contenus à scanner pour y trouver telle ou telle pépite[79].

Dans le cas des technologies quantiques, les médias de la « tech » relaient souvent les publications en les habillant de sensationnalisme, et parfois avec plusieurs mois de décalage.

Celui-ci provient souvent de la propension des communicants des laboratoires ou des chercheurs eux-mêmes (plutôt dans les pays anglo-saxons) à exagérer la portée de leur publication. Elle est plus forte lorsque la communication vient d'une grande entreprise comme Google ou lorsque l'article a été rédigé par des communicants du laboratoire.

Le travail du veilleur technologique que j'essaye d'être est de faire le tri. Lorsque la presse française relaie une information, il faut commencer souvent par identifier l'article d'origine qui est éventuellement cité en fin d'article. On va parfois y découvrir une erreur de traduction qui change la portée du propos.

Ensuite, il faut trouver l'article scientifique d'origine avec les méthodes décrites un peu plus haut. Une fois tout cela réalisé, le gros du travail consiste à classifier l'information : de quoi parle-t-on et comment cela se situe-t-il dans l'écheveau des technologies quantiques[80].

En général, un article présentant une avancée qui permettra de réaliser l'ordinateur quantique à température ambiante ou devançant tous les autres devient une simple avancée très ponctuelle dans la mise au point d'un type particulier de qubit. C'est le chien velu passé à la douche !

Dans d'autres cas, la publication scientifique pose d'autres problèmes au lecteur : elle est inaccessible, faisant référence à des bases mathématiques et physiques complexes. Je tombe ainsi souvent sur un ensemble de poupées russes de concepts inconnus faisant appel à d'autres concepts inconnus et ainsi de suite. Les papiers fondateurs sont cependant souvent ceux qui n'abusent pas du jargon et qui arrivent à traiter une grande question fondamentale en la rendant compréhensible par un maximum de spécialistes de leur discipline et au-delà. C'est souvent le cas des publications dans Nature.

Comment vérifier l'ensemble, surtout dans la mesure où les spécialistes de mon réseau n'ont pas encore eu le temps de le faire ? Il faut soit patienter soit s'attaquer à la compréhension de ces concepts, soit chercher quelqu'un qui a pu vulgariser la chose. En général, il sera Américain.

Enfin, j'utilise Arxiv dès que je tombe sur une startup peu loquace sur ce qu'elle conçoit. Une recherche avec le nom des fondateurs scientifiques permet d'identifier les travaux de recherche sur lesquels ils ont travaillé et qu'ils ont probablement l'intention de valoriser dans leur startup fraîchement lancée.

---

[79] En voici un exemple sur les technologies supraconductrices de l'IEEE.

[80] Divers outils tentent d'automatiser ce travail de tri, comme In Laymans Terms: Semi-Open Relation Extraction from Scientific Texts par Ruben Kruiper et al, mai 2020 (13 pages). Il s'applique pour l'instant au domaine de la biologie.

Dans les centaines de notes de bas de page de ce document, je prends sinon la liberté de ne pas utiliser les conventions de description cryptiques des articles qui figurent dans les abondantes bibliographies des publications scientifiques. J'utilise la convention titre en clair + premier auteur/auteurs selon le nombre + date de publication + nombre de pages ou de slides, qui permet d'identifier d'un coup d'œil la volumétrie du document.

Rôles

Dans la plupart des pays du monde, en technologies quantiques comme ailleurs, on peut distinguer plusieurs rôles.

Les **doctorants** sont des étudiants qui font une thèse de doctorat. Elle dure de trois à cinq ans selon les pays. Cette thèse complète une formation supérieure équivalente à notre BAC+5 soit dans l'Université, soit pour ce qui est de la France, dans une grande école scientifique. Ils sont les plus nombreux dans les laboratoires de recherche. La durée des thèses en France est jugée trop courte, de trois ans.

Le **post-doc** ou chercheur post-doctoral est un chercheur qui vient d'obtenir une thèse de doctorat et qui mène des travaux de recherches dans un laboratoire dans le cadre d'un CDD. C'est l'antichambre d'un poste de chercheur à temps plein, le Graal de la titularisation. C'est un statut qui n'est pas spécifique à la France.

Les **chargés de recherche** en France sont des chercheurs fonctionnaires recrutés sur concours ouverts dans les grands établissements publics de recherche comme le CNRS ou l'Inria.

L'**habilitation à diriger des recherches** (HDR) permet à un chercheur titulaire de diriger la thèse d'un ou plusieurs doctorants comme directeur de thèse et pour obtenir un grade de professeur des universités. Les règles varient d'un pays à l'autre, comme le fait d'avoir réalisé deux thèses de doctorat et d'avoir publié des travaux reconnus internationalement dans son domaine.

Cette habilitation a remplacé le doctorat d'Etat en 1984 en France. L'HDR est considérée comme étant un diplôme. Il est délivré sur candidature libre par la commission de recherche des Universités qui délibère sous forme de jury.

Un **directeur de recherche** en France a la possibilité de déterminer de manière autonome le champ de ses travaux de recherche. Il encadre plusieurs doctorants s'il arrive à les financer et à les recruter. Ils sont aussi sélectionnés par concours dans les établissements de recherche. Comme pour les chargés de recherche, il existe plusieurs grades dans la fonction, liés à l'avancement dans le temps et le mérite.

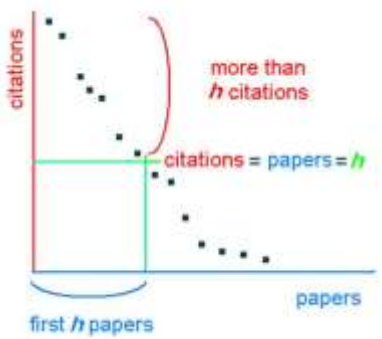
Enfin, en France, une **Unité Mixte de Recherche** (UMR) est un laboratoire de recherche en France qui associe un laboratoire du CNRS et un laboratoire tiers comme celui d'une Université, d'un autre organisme de recherche ou d'une entreprise privée. C'est une entité administrative issue de la signature d'un contrat pluriannuel, en général de quatre ans, entre les parties prenantes. La plupart des laboratoires de recherche associés à des grandes écoles (LKB de l'ENS par exemple) ou universités qui sont cités dans ce document sont des UMR.

N'oublions pas en plus de ces rôles, celui des **techniciens de laboratoires** qui mettent en place les expériences et dont on parle moins et d'**ingénieurs** qui peuvent jouer un rôle dans la création de nombreux instruments scientifiques.

h-index

Le h-index qui tire son nom de son créateur Jorge Hirsch en 2005 est un indice qui quantifie la productivité et l'impact scientifique d'un chercheur. Il est basé sur le niveau de citations de ses publications scientifiques dans les revues à comité de lecteurs. C'est un peu l'équivalent d'un PageRank pour un site web, mais en plus simple. Le h-index est un nombre entier qui correspond au nombre d'articles h qui ont obtenu chacun plus de h citations dans d'autres articles.

Le niveau de h-index peut servir de donnée quantitative pour obtenir un poste de chercheur résident (10-12), de professeur (>18) ou de membre d'une académie des sciences (>45). Comme tout indice composite[81], il génère des effets pervers : course aux publications sans grande valeur (« publish or perish »), références croisées entre chercheurs complices, auto-citations, abondance de co-auteurs, etc. A grosse maille, cela reste cependant un indicateur intéressant de l'influence des chercheurs et de leur prolixité. En moyenne, le h-index d'un chercheur en physique est proche de sa durée de carrière depuis sa thèse de doctorat. Il évolue évidemment dans le temps.



Il est plein de défaut comme tous les indicateurs quantitatifs. Par exemple, le h-index de base ne fait pas la distinction entre auteur principal et co-auteur. D'où l'abondance d'auteurs cités dans de nombreux papiers, certains n'y ayant eu qu'une contribution marginale.

L'indice est généralement calculé à partir des données de **Google Scholar** mais on le trouve parfois calculé uniquement dans le site SemanticScholar. L'indice le plus sérieux est fourni par le site **Web of Science** car sa base de données est la plus propre.

J'ai compilé le h-index de nombreux chercheurs dans les domaines couverts par cet ebook. On y trouve quelques bizarreries avec un prix Nobel, Brian Josephson, avec un h-index assez bas de 19. C'est lié au fait que ses premiers travaux fondateurs ont été souvent cités mais pas ceux qui ont suivi dont l'impact académique était donc plus faible.

A l'envers, le top du h-index est chez Nicolas Gisin (129), Anton Zeilinger (125), Yoshihisa Yamamoto (112) et David Wineland (109). Les stars françaises sont Serge Haroche, prix Nobel (89), Michel Devoret (99), Jean Dalibard (89), Philippe Grangier (71) et Alain Aspect (70). Les chercheurs français quadragénères sont en bonne position avec notamment Pascale Senellart (48), Maud Vinet (43), Antoine Browaeys (38), Patrice Bertet (38), Alexia Auffèves (37), Mazyar Mirrahimi (34) et Sara Ducci (31). Les h-index sur Web of Science sont différents, un peu plus fiables, et en général de plus faibles valeurs pour tous les chercheurs, en respectant à peu près le classement trouvé sur Google Scholar.

Fake news

La science n'est pas exempte de fake news. Dans tous les domaines scientifiques, certains chercheurs ou bien non scrupuleux ou manquant de rigueur peuvent présenter des résultats contestables de leurs expériences, agréger et compiler des données en les bidouillant, ou simplement, en mettant la poussière sous le tapis de données embarrassantes. Cela peut aussi arriver dans les technologies quantiques en particulier lorsqu'il s'agit d'évaluer la qualité de qubits expérimentaux. Il faut en général être expert du domaine pour identifier ce genre d'abus. Mais ils sont assez rares dans les technologies quantiques.

Avec une connaissance technologique généraliste du domaine, on peut commencer à flairer les entourloupes ou exagérations. C'est ce que je fais dans cet ebook concernant IBM avec leur volume quantique, Honeywell avec leur ordinateur quantique « le plus puissant du monde » ou avec les expériences de suprématie quantique de Google ou des chinois.

Poster sessions

Dans une conférence scientifique, une « poster session » est en général une partie de la conférence dédiée à la présentation de projets de chercheurs lors d'un break, dans une zone dédiée.

[81] On pense notamment au classement de Shanghai des universités.

Les chercheurs y exposent un poster qui décrit leurs travaux de recherche et discutent avec les participants à la conférence qui déambulent dans la zone d'exposition. C'est un exercice d'humilité sauce « témoin de Jehovah ».

Figures de mérite

Cette expression courante chez les chercheurs décrit en gros un cahier des charges et les métriques de succès à atteindre pour faire aboutir une technologie donnée. On peut considérer que les critères de DiVincenzo de technologies de qubits en sont une figure de mérite de succès.

International

A l'heure des plans quantiques nationaux, rappelons tout de même que la collaboration internationale est intense entre chercheurs. La plupart de ceux et celles que j'ai croisés dans les laboratoires français collaborent avec des collègues soit en Europe dans le cadre de projets Europe 2020, du Flagship Européen ou pour certains ERCs. Ils collaborent aussi avec des chercheurs hors de l'Union Européenne, notamment en Asie, ainsi qu'aux USA et en Australie. Cela peut aussi prendre la forme d'Unités Mixtes Internationales du CNRS comme celles qui sont établies au Japon et à Singapour.

La connaissance est assez ouverte et perfuse bien à l'échelle mondiale. C'est favorisé par les nombreux congrès scientifiques internationaux où les connaissances se nouent et les projets communs se lancent. C'est l'une des raisons pour laquelle je ne crois pas à l'existence d'un supposé ordinateur quantique dont les capacités défieraient l'entendement et qui serait caché dans les sous-sols d'un datacenter secret de la NSA pour casser toutes les clés RSA d'Internet.

Le nationalisme scientifique dans les technologies quantiques intervient finalement plus en aval de la recherche, lorsqu'il s'agit de la transformer en avantage industriel. Les technologies ont souvent leur « sauce magique », comme dans les procédés de fabrication de semi-conducteurs. Il en a toujours été ainsi dans les technologies du numérique.

Technology Readiness Level

Cette notion est très couramment utilisée dans les deep techs qui décrit le niveau de maturité d'une technologie avec une échelle allant de 1 à 9. Elle suit une classification relativement normalisée créée initialement par la NASA en 1975[82], puis par l'Union Européenne et divers autres organismes.

Cette gradation peut avoir plusieurs usages. Elle sert notamment à évaluer le niveau de risque et de maturité pour un investisseur dans une startup. Elle est principalement utilisée dans les industries aérospatiales, dans la défense et dans l'énergie. Les deep techs très avancées sont aussi le terrain de jeu du TRL et les technologies quantiques n'y échappent pas.

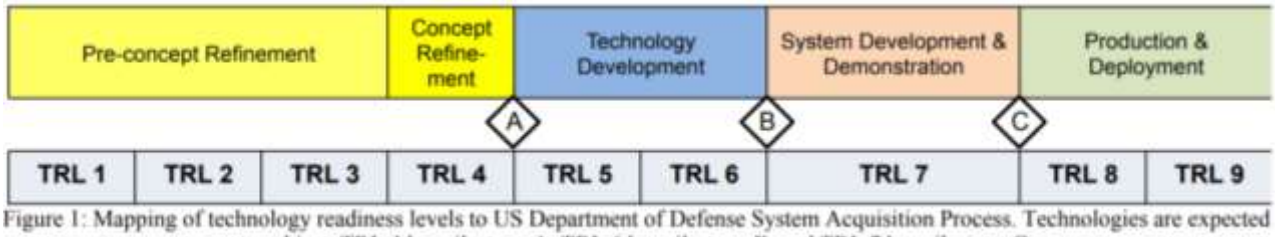
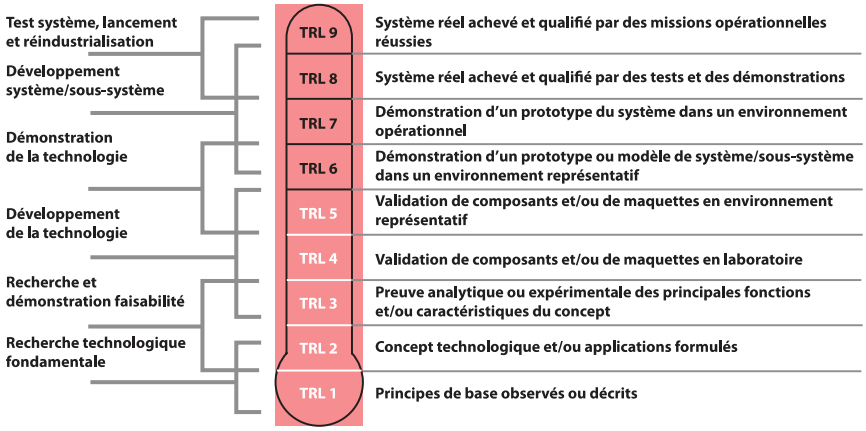


Figure 1: Mapping of technology readiness levels to US Department of Defense System Acquisition Process. Technologies are expected to achieve TRL 4 by milestone A, TRL 6 by milestone B, and TRL 7 by milestone C.

[82] Voir Technology Readiness Levels at 40: A Study of State-of-the-Art Use, Challenges, and Opportunities par Alison Olechowski et al, 2015 (11 pages) qui est la source du schéma.

Le TRL s'étale sur 9 niveaux que voici [83]:

- **TRL 1** : principes de base décrits ou observés, au stade de la théorie ou de l'expérimentation.
- **TRL 2** : concepts technologiques formulés et pas encore forcément expérimentés.
- **TRL 3** : preuve de concept réalisée en laboratoire, au niveau du procédé technique.
- **TRL 4** : technologie validée en laboratoire dans son ensemble.
- **TRL 5** : maquette de technologie dans un environnement proche de l'usage.

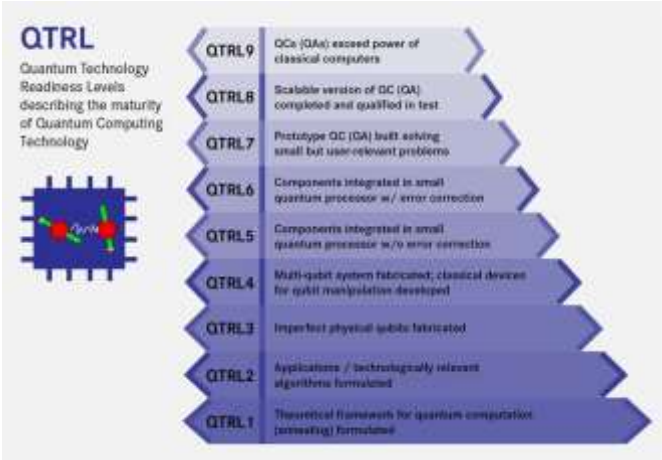


- **TRL 6** : prototype de la technologie démontré dans un environnement représentatif du cas d'usage visé.
- **TRL 7** : prototype évalué en environnement opérationnel.
- **TRL 8** : système complet évalué et qualifié.
- **TRL 9** : système complet, opérationnel et qualifié en production.

Il manque à cette échelle la pertinence de la solution par rapport aux besoins du marché, mais c'est une considération plus marketing que technique[84].

La chercheuse **Kristel Michielsen** a proposé une échelle adaptée au calcul quantique, la QTRL, pour Quantum Technology Readiness Level *ci-dessous*[85]. L'évaluation qu'elle fait de certaines technologies est douteuse. Ainsi, elle place les ordinateurs à recuit quantique de D-Wave en TRL 8 et 9. Ce qui est correct du point de vue commercial puisque ces ordinateurs sont bien commercialisés. Ceci étant, si ceux-ci sont bien disponibles physiquement, il n'est pas prouvé qu'ils servent à grand-chose pour l'instant. Les mauvaises langues les positionneraient à peine aux niveaux 2 ou 3 !

La spécificité des technologies quantiques est que de nombreuses startups du hardware sont créées alors qu'elles ont des TRL très bas. C'est particulièrement vrai de celles qui se lancent dans la conception de qubits adoptant des technologies pas encore éprouvées, même en laboratoire. Dans le quantique, les notions de « MVP » (minimum viable product) sont très différentes du monde du numérique. Elles reposent sur des critères plus scientifiques que fonctionnels, sachant que les éléments de mesure ne sont pas toujours partagés par les acteurs, comme pour la caractérisation de la qualité des qubits pour le calcul quantique.



[83] Source du schéma *ci-dessus* Quelques explications sur l'échelle des TRL (Technology readiness level), DGA, 2009 (15 pages). Voir aussi Technology Development Stages and Market Readiness par Surya Raghu, juin 2017 (35 slides).

[84] Voir TRL, MRL, POC, WTF ? par Massis Sirapian de l'Agence de l'Innovation de la Défense, avril 2019.

[85] Voir sa présentation Simulation on/of various types of quantum computers, Kristel Michiels, mars 2018 (40 slides).

Basiques

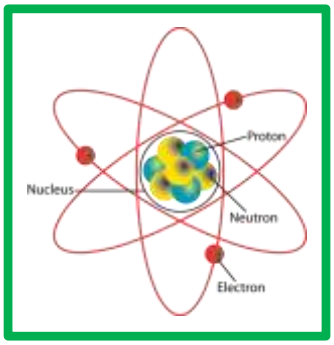
Après avoir fait le tour des plus grands contributeurs de la mécanique et de l'informatique quantique, passons aux grands fondamentaux de la physique quantique qui nous permettront de comprendre la suite et notamment le fonctionnement des qubits et de leurs diverses techniques de mise en œuvre.

Plusieurs années d'études sont nécessaires pour comprendre les arcanes de la mécanique quantique et ceux qui sont passés par là sont toujours dans l'interrogation à son sujet. Mais on peut se contenter de quelques basiques ici présents pour se préparer à comprendre le fonctionnement des calculateurs quantiques.

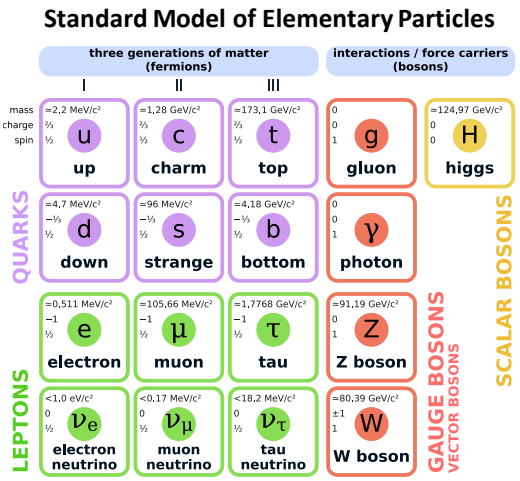
La mécanique quantique est apparue il y a un peu plus d'un siècle pour expliquer le fonctionnement et la dynamique des particules élémentaires. Les principales particules élémentaires à qui s'appliquent les principes de la mécanique quantique sont les **photons** et les **électrons**, mais cela concerne aussi les **atomes** soit neutres soit ionisés[86]. Les effets quantiques les plus connus se manifestent sur la phase des photons ainsi que sur les niveaux d'énergie ou les spins d'électrons, ces derniers étant liés en approximation à leur orientation magnétique[87].

la physique quantique s'intéresse aux particules de l'échelle atomique et sub-atomique

à cette échelle, la matière a des comportements qui ne correspondent pas aux observations « macro »



atomes



Le point essentiel est de bien appréhender la notion de **superposition d'états** qui est à la base du fonctionnement des qubits et l'une des sources de l'énorme capacité de traitement des calculateurs quantiques. L'**intrication** vient juste après et permet d'expliquer comment fonctionnent les portes quantiques dans les calculateurs quantiques, que nous verrons dans la partie dédiée au fonctionnement de ces derniers.

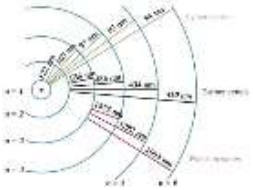
Tous les qubits connus d'ordinateurs quantiques s'appuient sur des combinaisons variables d'effets quantiques associant des électrons et des photons. A part le cas des qubits réalisés à base de photons, tous les autres sont à base de différents comportements quantiques d'électrons. C'est le cas des qubits à base de supraconducteurs à effet Josephson qui exploitent des effets très particuliers que nous expliquerons plus tard, reposant sur le comportement des électrons de matériaux supraconducteurs. Les ions piégés, les atomes froids, les cavités de diamants, les qubits silicium et même les qubits à base d'anyons et des hypothétiques fermions de Majorana exploitent eux-aussi les effets quantiques qui impliquent des variations de niveau d'énergie d'électrons.

---

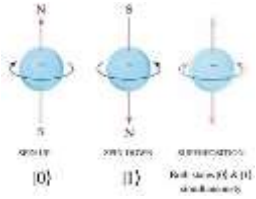
[86] Pour mémoire, voici la dimension des particules élémentaires : 10^{-10} pour un atome, 10^{-15} pour le diamètre d'un noyau d'atome d'hydrogène, donc d'un proton unique et 10^{-18} pour celui d'un électron.

[87] Les atomes ont aussi un moment magnétique quantifiable (discret), comme découvert en 1922 dans l'expérience de Stern-Gerlach avec des atomes d'argent envoyés dans un champ magnétique non homogène pour observer leur déviation.

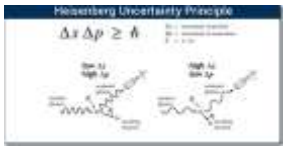
Des phénomènes quantiques peuvent se manifester avec d'autres particules élémentaires comme les neutrons et les protons mais ce ne sont pas à ce jour des pistes explorées par les chercheurs dans le contexte du calcul quantique.



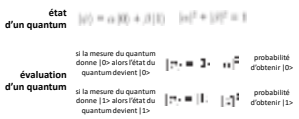
quantification



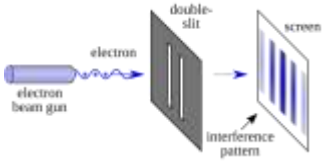
superposition d'états



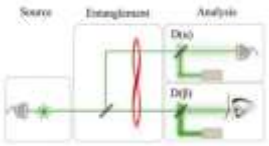
indétermination



réduction d'états



dualité onde-particule



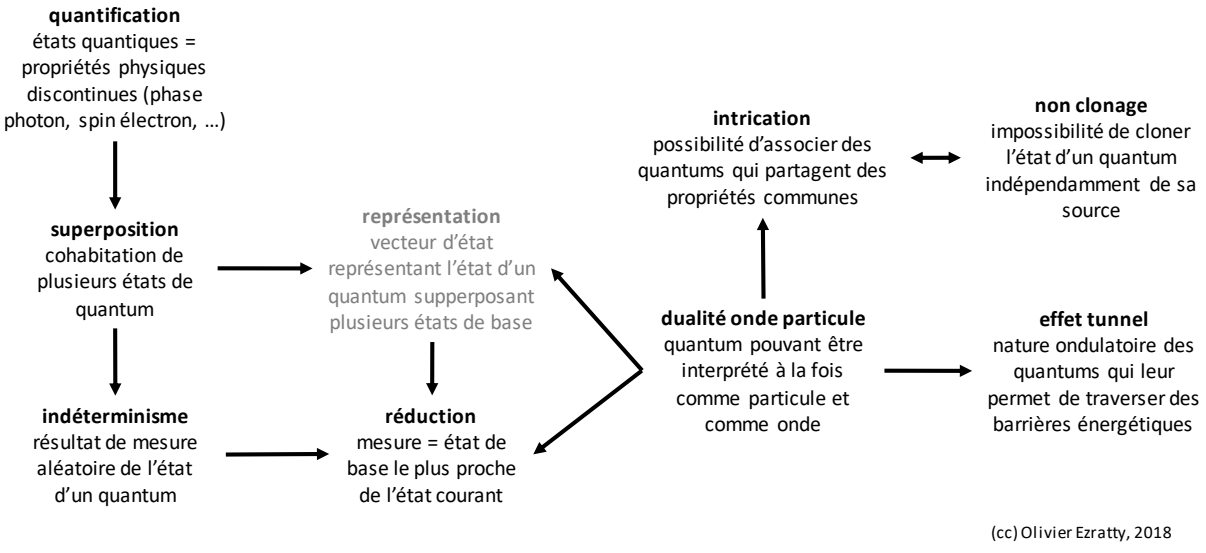
intrication

non clonage

effet tunnel

Voici un petit schéma de mon cru qui connecte entre eux les principes de base de la physique quantique que nous allons explorer. Il fournit quelques relations de causalité entre ces différents principes. Ainsi, c'est la quantification des propriétés d'un quantum qui aboutit à leur superposition. Cette dernière entraine l'indéterminisme de la mesure de l'état d'un quantum et la notion de réduction.

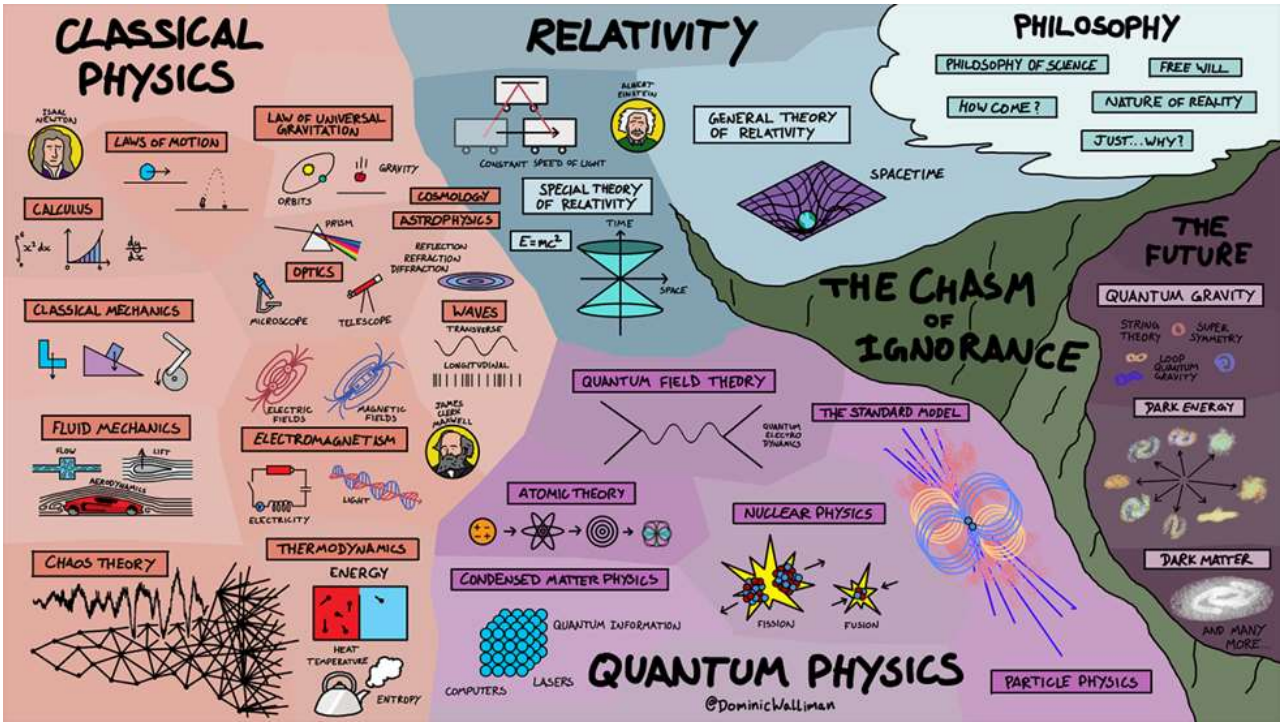
liaisons entre concepts de la physique quantique



L'ensemble est représenté mathématiquement par un vecteur d'état qui contient deux nombres complexes, pour ce qui est des quantums à deux états possibles. Les propriétés mathématiques des vecteurs d'état s'expliquent par la dualité onde-particule des quantums et la possibilité d'additionner les ondes liées aux différents états des quantums. La dualité onde-particule est liée à la notion d'intrication qui elle-même explique le théorème de non clonage ainsi que l'effet tunnel. C'est peut-être approximatif mais permet de se faire une idée de l'architecture d'ensemble.

J'ai ajouté deux champs à ce panorama, celui des **supraconducteurs** et de la **superfluidité** qui sont utilisés à différents endroits dans les ordinateurs quantiques (qubits supraconducteurs et connectique, réfrigération à dilution). Depuis la troisième édition de cet ouvrage, cette partie contient également une rubrique sur les **lasers et les masers** à titre documentaire, ce d'autant plus que les lasers sont très utilisés dans les technologies quantiques couvertes ici-même. Nous couvrons aussi le cas particulier des **polaritons**.

En parcourant de nombreux ouvrages sur la physique quantique et l'informatique quantique, j'ai pu constater que la pédagogie y était des plus variée. Le formalisme mathématique y prend rapidement le dessus de la description physique des phénomènes quantiques. Il est tellement prédominant qu'il ne correspond pas forcément à la réalité physique des quantums. Il est généralement très mal expliqué comme nous le verrons dans la partie suivante pour ce qui est du modèle de représentation de la sphère de Bloch.



source : https://dominicwalliman.com/post/153828312160/here-is-the-map-of-physics-as-an-image

Je vais toutefois essayer de vous épargner cela dans ce qui suit à la fois parce que c'est un véritable tonneau des Danaïdes et parce que cela perdrait une grande majorité de lecteurs. Et même avec ces précautions, rien ne dit que tous vont suivre. Dans la physique quantique, il faut avoir systématiquement l'humilité de reconnaître que l'on ne sera pas forcément compris et/ou que l'on s'est mal expliqué !

Voyons donc cela dans le détail !

Quantification

En physique quantique, les quantums correspondent à des propriétés physiques de particules élémentaires matérielles ou immatérielles qui sont discontinues et non continues. Cela peut correspondre à des états énergétiques, des polarisations pour les photons, ou des orientations magnétiques pour les électrons.

Les orbites des électrons autour de noyaux d'atomes sont définies de manière discrète comme nous l'avons vu sur l'atome d'hydrogène avec les travaux de Max Planck en 1900, Albert Einstein en 1905 et Niels Bohr en 1913.

propriétés discontinues de la matière à l'échelle nanoscopique

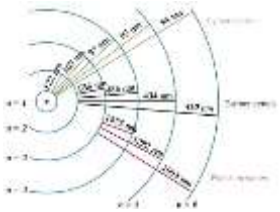
notamment au niveau des états énergétiques

découvertes dans l'interaction lumière/matière et l'effet photoélectrique

=> créer des qubits avec des états bien distincts et à l'échelle de particules (atomes, électrons, photons)

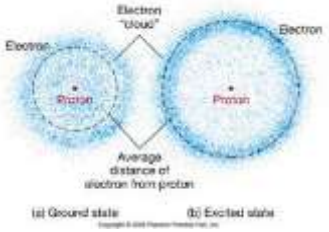
concept : Ludwig Boltzmann, 1877

découverte : Max Planck, 1900 puis Albert Einstein, 1905

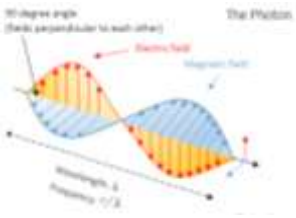


atomes
niveaux d'excitation

ions
niveaux d'excitation



électrons
spin magnétique (up, down)
courants supraconducteurs



photons
polarisation (H, V),
fréquence, phase, …

Il existe aussi une correspondance entre l'énergie des photons et les transitions énergétiques discontinues des électrons en orbite autour des atomes. Dans le calcul quantique, ce principe est utilisé un peu partout, surtout pour distinguer deux états clairement séparés dans les qubits.

Les qubits utilisés dans les calculateurs quantiques doivent s'appuyer sur des quantums qui n'ont que deux états possibles qui peuvent être à la fois initialisés, modifiés et ensuite mesurés. Même les qubits supraconducteurs s'appuient sur deux niveaux d'énergie clairement distincts du courant oscillant qui traverse leur isolant à effet Josephson.

A noter que les atomes forment des oscillateurs harmoniques et vibrent aussi à des amplitudes quantifiées dans des structures cristallines, selon le modèle Einstein élaboré en 1907.

Superposition

La superposition a un lien direct avec la quantification qui porte sur les différents états des particules élémentaires.

Les particules quantiques peuvent avoir plusieurs états simultanément, comme le sens de magnétisation du spin d'électron qui est orienté vers le haut ou vers le bas – cf schéma *ci-dessous* –, la polarisation linéaire des photons, qui est horizontale ou verticale après passage au travers de filtres polarisants, ou la fréquence ou l'énergie d'un courant oscillant dans un qubit supraconducteur.

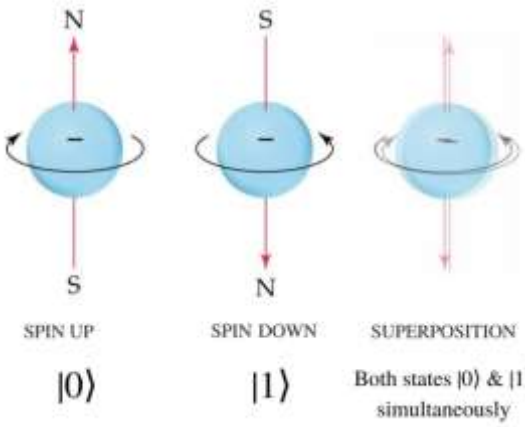
les objets quantiques peuvent être arrangés dans des états superposés

conséquence de la dualité ondes-particules

interprétation inexacte :
la matière « vibre » à haute fréquence entre ces différents états

interprétation plus appropriée :
superposition d'ondes

=> utilisé pour gérer l'information dans les qubits et registres de qubits et permettre le parallélisme du traitement sur les états des registres de qubits



Le principe de la superposition veut qu'une particule élémentaire puisse être simultanément dans plusieurs de ces états quantiques. Dans une interprétation de physique classique, cela serait explicable par une fréquence très élevée des modifications d'états de ces particules. Elle est peut-être inexacte pour les spécialistes mais c'est un moyen intuitif de se représenter ce principe de la superposition.

En calcul quantique, ce principe est utilisé dans les qubits, leur permettant d'avoir en même temps la valeur 0 et 1 au lieu d'avoir seulement l'une des deux valeurs comme avec les bits traditionnels. C'est cela qui permet aux calculateurs quantiques de paralléliser les calculs à un niveau inégalé comparativement aux meilleurs supercalculateurs classiques. S'il n'y a qu'un élément de mécanique quantique à retenir pour comprendre les ordinateurs quantiques, c'est bien celui-ci !

Dualité ondes particules

Les particules élémentaires ont des comportements qui relèvent à la fois des particules avec une masse, une énergie et un mouvement et comme des ondes avec une fréquence et une longueur d'onde, et des effets d'interférences et le fait qu'elles peuvent s'additionner pour donner d'autres ondes. Un peu comme les couleurs (photons) et les sons (ondes acoustiques) se mélangent.

Diverses expériences comme celle des doubles fentes de Young montrent que les électrons qui sont des particules matérielles avec une masse se comportent à la fois comme des particules et comme des ondes, générant des interférences. Les équations de Planck, Einstein et Bohr donnent la correspondance entre photons et états énergétiques d'atomes liés à la position orbitale des électrons.

une particule physique comme un électron ou un atome peut se comporter à la fois comme de la matière (avec une masse) **ou une onde** (avec des interférences)

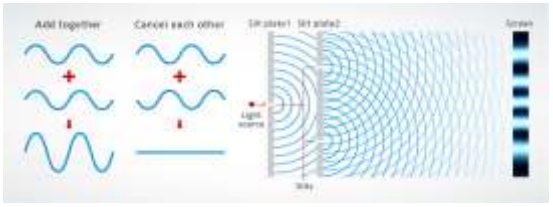
vérifié dans l'expérience des fentes de Young avec un faisceau d'électrons

s'applique aussi aux **photons** ainsi qu'avec des atomes et molécules de grande taille

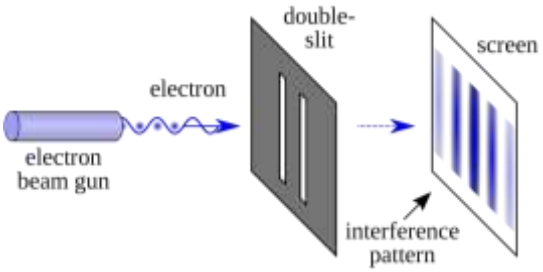
=> exploité dans le calcul quantique pour créer des interférences entre qubits via les portes à deux qubits ou plus

concept : Louis de Broglie, 1924.

validation : George Paget Thomson, Clinton Davisson et Lester Germer, 1927.



phénomène d'annulation d'ondes avec des photons



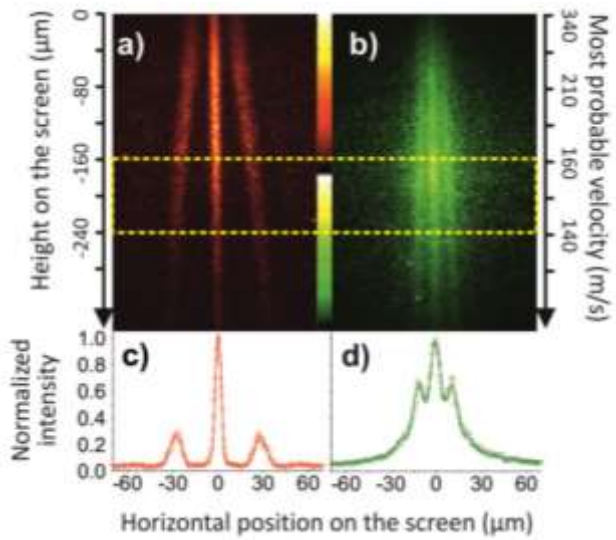
même phénomène observé avec des électrons

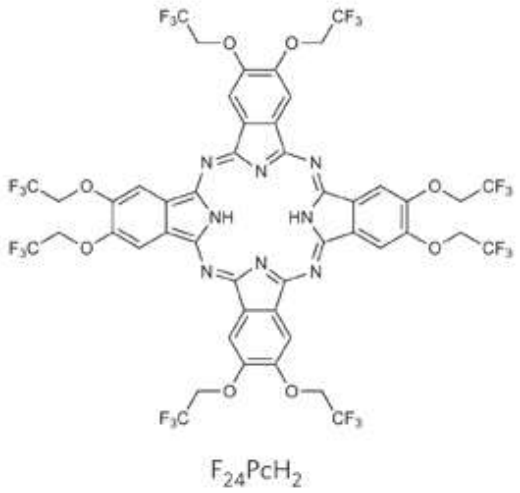
La dualité ondes/particules est utilisée dans nombre d'ordinateurs quantiques pour faire interagir des qubits physiques comme des ions piégés avec de l'énergie sous forme de photons émis par des lasers. Les qubits peuvent aussi interférer les uns avec les autres en reproduisant une partie de ce mécanisme d'interférence ondulatoire.

Cette dualité ondes-particules explique aussi pourquoi le formalisme mathématique de la physique quantique s'appuie sur des vecteurs qui peuvent s'additionner comme des ondes.

On comprend donc que les électrons ont cette capacité à se comporter comme des particules et comme des ondes.

La dualité onde-particule a été vérifiée avec des atomes en 1991 dans des expériences d'interférométrie comprenant des lasers et des optiques classiques. L'expérience des fentes de Young a été réalisée en Autriche en 2002 sur des molécules de fullerène (C60, formée de 60 atomes de carbone, *ci-contre*[88]) et en 2012 sur des molécules de 58 et 114 atomes, cette dernière dénommée $F_{24}PcH_2$ est faite de fluor, carbone, oxygène, hydrogène et azote[89]. Voir l'illustration *ci-dessous* avec la forme de la molécule. En 2019, ce même genre d'expérience était réalisé avec une molécule un peu plus complexe, un polypeptide de 15 acides aminés qui sert d'antibiotique, la gramicidine A1[90].





Mais qu'en est-il des photons ? Ils peuvent se comporter dans certaines conditions comme des particules. Lorsqu'ils atteignent un atome, ils peuvent ainsi lui transmettre un mouvement cinétique.

C'est ce qui permet de générer un phénomène physique un peu contre-intuitif : le refroidissement d'atomes avec des lasers. La température est liée au mouvement des atomes dans leur milieu gazeux, liquide ou solide. Baisser la température revient à ralentir le mouvement des atomes.

On utilise l'effet Doppler pour ce faire. On éclaire les atomes en mouvement avec un laser dont la fréquence est positionnée juste en-dessous du niveau d'absorption d'énergie des atomes en question.

Ceux des atomes qui se déplacent vers la lumière vont absorber les photons, car la fréquence apparente des photons est plus élevée et génère une énergie légèrement supérieure au niveau d'absorption. Cela réduit l'énergie cinétique des atomes en question.

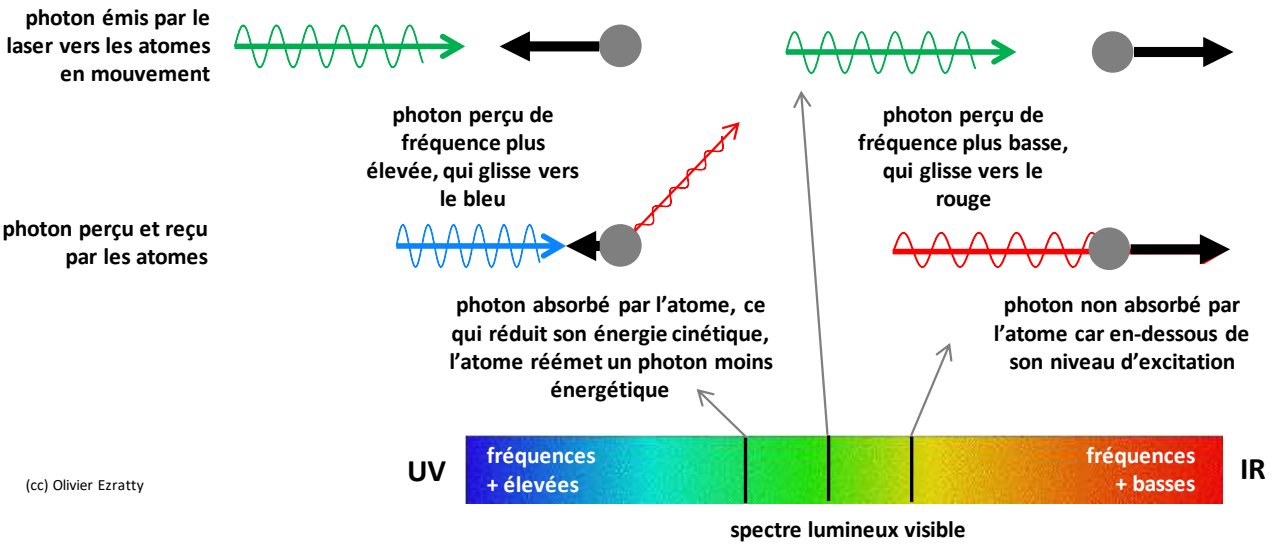
Ceux qui se déplacent dans l'autre direction ne les absorberont pas car la fréquence apparente du photon incident est trop faible pour changer l'état énergétique des atomes. Grâce au mouvement aléatoire des atomes dans toutes les directions, au bout d'un certain temps, la température d'ensemble baisse. Magique ! Mais ce phénomène s'atténue une fois que la vitesse des atomes descend en-dessous d'un certain seuil, reflétant l'atténuation de l'effet Doppler (« Doppler shift »).

---

[88] Voir Quantum interference experiments with large molecules par Olaf Nairz, Markus Arndt et Anton Zeilinger, 2002 (8 pages).

[89] Voir Real-time single-molecule imaging of quantum interference par Thomas Juffmann et al, 2012 (16 pages). Voir également la vidéo de l'expérience. Highly Fluorinated Model Compounds for Matter-Wave Interferometry de Jens Tüxen, 2012 (242 pages) décrit pour sa part le dispositif expérimental de vérification de la dualité onde-matière de grandes molécules.

[90] Voir A natural biomolecule has been measured acting like a quantum wave for the first time, novembre 2019, qui fait reference à Matter-wave interference of a native polypeptide par Armin Shayeghi et al, octobre 2019 (10 pages).



Ces techniques sont utilisées pour refroidir des atomes à des températures voisines du zéro absolu[91]. Elles sont notamment employées pour préparer des « atomes froids » et des « ions piégés » utilisés dans certains types d'ordinateurs quantiques, souvent par combinaison avec des pièges magnétiques ou électroniques. La mesure de l'effet Doppler sert par ailleurs à évaluer la vitesse d'éloignement des étoiles et galaxies et d'en déduire le phénomène d'expansion de l'Univers.

Le record en 2019 était de 50 nK, obtenu par des chercheurs du JILA, le laboratoire commun du NIST et de l'Université du Colorado[92].

Réduction d'états et mesure

La réduction des états quantiques explique dans le détail la nature de l'indétermination de la mesure de l'état des quantums.

Lorsque l'on mesure un état d'un quantum, celui-ci est affecté par la mesure. La mesure change l'état du quantum. Celui-ci se rabat en quelque sorte, et de manière probabiliste, sur l'état de base le plus proche de son état avant la mesure et que l'on appelle un "observable".

L'état "pur" avant la mesure est une combinaison d'états de base du quantum. Par exemple, une combinaison de polarisation verticale et horizontale pour un photon.

On appelle aussi cela "*l'écrasement de la fonction d'onde de Schrödinger*" (ou « effondrement », ou écrasement du paquet d'ondes). Pourquoi donc ? Parce que qu'un quantum multi-états superpose plusieurs états distincts qui sont représentés chacun par une fonction d'onde liés à chaque observable. L'état composite de deux fonctions d'ondes est aussi une fonction d'onde.

Lorsque l'on mesure l'état d'un tel quantum, l'état de base le plus proche des états superposés est le plus souvent détecté, mais l'autre état l'est aussi dans une moindre proportion. La probabilité dépend de l'état du quantum mesuré.

Prenons l'exemple d'un photon de polarité intermédiaire entre la polarité horizontale ou verticale, ou de polarisation circulaire. Il va devenir un photon polarisé horizontalement ou verticalement après sa mesure de polarité. La notion de réduction est une autre application pratique du fameux principe selon lequel la mesure de l'état d'un quantum influe sur la grandeur à mesurer dans l'infiniment petit, alors que ce n'est pas le cas dans la mécanique newtonienne classique.

---

[91] Source de l'illustration : https://sites.ualberta.ca/~ljleblan/background/laser-cooling.html.

[92] Voir JILA Researchers Make Coldest Quantum Gas of Molecules, février 2019. Le record de 50 nK a été obtenu en refroidissant par lasers un gaz de 25 000 molécules de potassium–rubidium.

Le principe d'indétermination d'Heisenberg dit précisément que l'on ne peut pas mesurer à la fois la position et la vitesse d'une particule élémentaire. Intuitivement, cela se comprend : en mécanique newtonienne, l'outil de mesure est en général plus petit que la grandeur à mesurer, comme pour évaluer la vitesse des astres et des planètes.

à la lecture de l'état d'un quantum, il va se rabattre sur l'un des états possibles selon une probabilité d'être dans chacun de ces états de base (excité ou au repos)

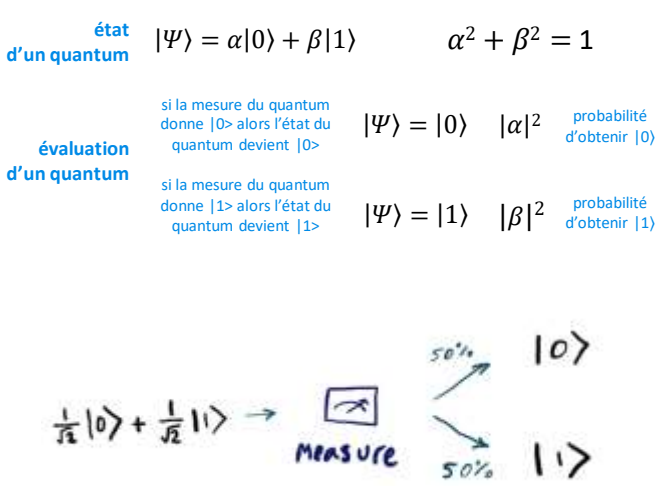
une seconde mesure donne le même résultat

« écrasement de la fonction ou du paquet d'onde de Schödinger »

phénomène de la décohérence qui dégrade progressivement la superposition et l'intrication des quantums et qubits

=> mesure des qubits en fin de calcul et dans les codes de correction d'erreurs

formalisation : Erwin Schrödinger, 1926



Dans l'infiniment petit, l'outil de mesure est habituellement bien plus grand que la grandeur physique à mesurer. D'où la perturbation sur la grandeur à mesurer !

Pour les puristes, la notion de vitesse et de position des particules n'a pas de sens, pour ce qui est par exemple d'un électron. Sa caractérisation passe par sa nature ondulatoire et par sa description via la fonction d'onde de Schrödinger.

En informatique quantique, ce principe de réduction est en œuvre lors de la mesure de l'état d'un qubit, qui modifie sa valeur en la rabattant à $|0\rangle$ ou $|1\rangle$. Le poids statistique des $|0\rangle$ ou le $|1\rangle$ obtenus dépend de l'état quantique mesuré.

C'est illustré dans le schéma *ci-dessus*. Nous reviendrons sur la signification de α et β dans la partie suivante sur les qubits, ces deux variables étant en fait des nombres complexes.

La subtile information contenue dans un qubit qui est représentée par un nombre complexe ou un vecteur à deux dimensions est réduite à $|0\rangle$ ou $|1\rangle$ au moment de sa mesure. Mathématiquement, on a donc bien une réduction d'une information riche comportant au moins l'équivalent de deux nombres flottants à un simple bit ! Et c'est sans parler des effets de l'intrication !

Cette réduction intervient au dernier moment après les calculs. Pendant ces derniers, les qubits sont modifiés par des portes quantiques qui conservent la richesse de leur information et la combinatoire de leurs valeurs liée à la superposition.

Le sujet de la mesure des états quantiques est cependant bien plus vaste que cela et sort du champ de cette édition de l'ebook. Un grand nombre de notions restent à traiter comme la mesure projective, la mesure faible, la mesure douce (gentle) et la mesure non destructive.

Indétermination

Le principe de l'indétermination d'Heisenberg veut que l'on ne puisse pas mesurer avec précision à la fois la position et la vitesse d'une particule élémentaire ou deux grandeurs complémentaires, et plus généralement pour tout couple de grandeurs physiquecomplémentaires.

La précision d'une grandeur est antagoniste de l'autre grandeur. On utilise d'ailleurs ce principe pour améliorer la précision d'une mesure… en diminuant celle d'autre grandeur mesurable. Au même titre, on ne peut pas observer en même temps une particule élémentaire dans son état particule et dans son état ondulatoire, un principe édicté par Niels Bohr vers 1928.

à l'échelle nanoscopique, la précision de la mesure de la vitesse et de la position d'une particule sont antinomiques, plus l'une est élevée, plus l'autre est faible

cela s'applique à toute paire de paramètres d'un quantum (longueur d'onde, position, vitesse, polarisation, …)

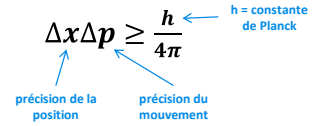
version dérivée : à l'échelle nanoscopique, l'outil de mesure influe sur la grandeur à mesurer

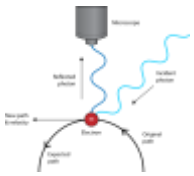
ça marche aussi dans les sondages

=> exploité en métrologie quantique.

=> explique la fluctuation quantique du vide

découverte : Werner Heisenberg, 1926





expérience du microscope d'Heisenberg : le photon envoyé sur l'électron va affecter sa trajectoire et sa mesure

Intrication

Des quantums peuvent être intriqués, à savoir qu'ils peuvent avoir la même fonction d'onde ou représentation quantique alors qu'ils sont distants. Donc, être dans un état quantique similaire, sans être pour autant strictement identique, ne serait-ce qu'au niveau de leur localisation spatiale. C'est le principe de la non-localité des propriétés quantiques de quantums intriqués qui perturbait Einstein en 1935. L'intrication est dénommée "entanglement" en anglais.

Ainsi, avec une paire de quantums intriqués, une mesure effectuée sur un quantum aura instantanément un effet sur l'autre quantum, sans attendre un délai de transmission d'information à la vitesse de la lumière entre les deux quantums. C'est le principe de la "non localité" des propriétés quantiques.

Les particules intriquées ne sont pas liées par hasard. Elles ont généralement un passé commun. Par exemple, deux photons intriqués peuvent être produits avec un miroir biréfringent et séparés par des miroirs dichroïques, créant deux photons de polarisations orthogonales. L'action sur l'un des deux photons a un impact sur l'autre photon comme l'a démontré Alain Aspect dans sa fameuse expérience réalisée en 1982.

deux particules quantiques peuvent être préparées dans un état qui reste corrélé même à distance

si on modifie l'état quantique de l'une, cela modifiera instantanément l'état de l'autre

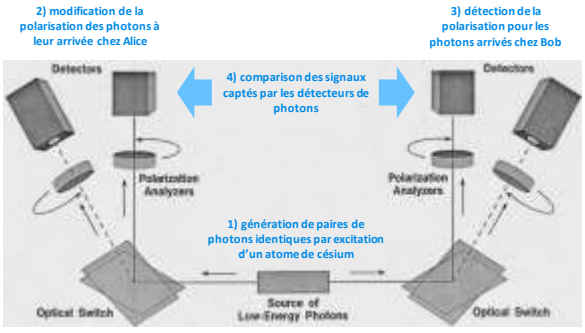
notion de « non localité » vérifiée sur des photons en 1982 par Alain Aspect

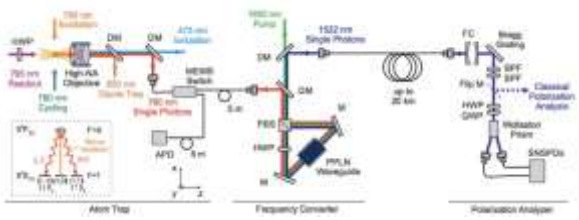
inexploitable pour transmettre une information plus vite que la lumière

=> exploitée pour relier les qubits entre eux de manière conditionnelle et dans les télécommunications quantiques

formalisme : Erwin Schrödinger, 1926 puis 1935

vérification : Alain Aspect et Philippe Grangier, 1982





expérience d'intrication de photons de 2020 avec conversion de longueur d'onde

Une expérience de 2019 menée à l'Université de Glasgow a même permis de photographier une représentation de l'état de photons intriqués[93]. Malgré tout, on est tout de même capable d'intriquer des particules qui n'ont pas forcément de passé commun[94].

En informatique quantique, l'intrication est utilisée dans les portes quantiques à deux ou trois qubits, pour les relier entre eux. Une fois intriqués, les qubits ont des états quantiques indissociables. L'intrication permet de générer des interférences entre les qubits. Sans elle, aucun algorithme quantique ne pourrait fonctionner.

Dans la science à la frontière de la science-fiction, certains imaginent exploiter l'intrication quantique pour analyser l'état de l'intérieur d'un trou noir[95] ! Cela sort du cadre de cet ouvrage !

Non clonage

Le théorème d'impossibilité du clonage quantique a été énoncé en 1982 dans un article publié dans Nature par William Wootters, Wojciech Zurek et Dennis Dieks. L'article n'est toujours pas disponible en open source sur un site tel qu'Arxiv, s'auto-appliquant le principe du non clonage ! Mais une version résumée est consultable ici (*ci-dessous*).

l'état d'un quantum ne peut pas être répliqué à l'identique et de manière indépendante dans un autre quantum

toute copie génère des états intriqués indissociables

démontrable mathématiquement par l'absurde (*ci-contre*)

=> exploité dans la sécurisation des télécommunications quantiques (QKD)

=> créé des contraintes dans le calcul quantique (mémoire, cache, …)

découverte : James Park en 1970
puis William Wooters et Wojciech Zurek en 1982

Il interdit la copie à l'identique de l'état d'un quantum. Le théorème se démontre mathématiquement en six lignes (*ci-dessus*) même si chaque mot de la démonstration nécessite quelques recherches préalables pour être compris ! Je la refais page 121. Il a comme conséquence qu'il est impossible de copier l'état d'un qubits pour l'exploiter indépendamment de son original.

Dans les ordinateurs quantiques, on peut bien dupliquer des qubits via des portes quantiques et l'intrication, mais les qubits résultants sont intriqués et donc en quelque sorte synchronisés. La lecture de la copie détruit l'original par projection de l'état des deux qubits sur le 0 ou le 1 le plus proche de leur état initial.

Cela a un impact direct sur la conception d'algorithmes quantiques et notamment sur les codes de correction d'erreurs des ordinateurs quantiques. Heureusement, ces codes de correction d'erreurs ne nécessitent pas de lire le contenu des qubits clonés et échappent donc aux foudres du théorème de non-clonage.

---

[93] Voir Scientists unveil the first-ever image of quantum entanglement, juillet 2019… par le chercheur français Paul-Antoine Moreau.

[94] Voir Qubits that never interact could exhibit past-future entanglement par Lisa Zyga, juillet 2012.

[95] Voir Can entangled qubits be used to probe black holes?, de Robert Sanders, 2019.

Effet tunnel

La double nature corpusculaire et ondulatoire de la matière lui permet de traverser des obstacles. Ces obstacles peuvent être des “murs énergétiques”. Le phénomène a été découvert en 1927 par le physicien allemand Friedrich Hund (1896-1997).

L’effet tunnel est exploité dans les ordinateurs à recuit quantique de D:Wave.

Il sert à faire converger un système de qubits de spins (“hamiltonien”, avec un niveau d’énergie totale donné) vers un minimum énergétique correspondant à la résolution d’un problème de combinatoire complexe ou de recherche de minimum énergétique comme en chimie ou en biologie moléculaire.

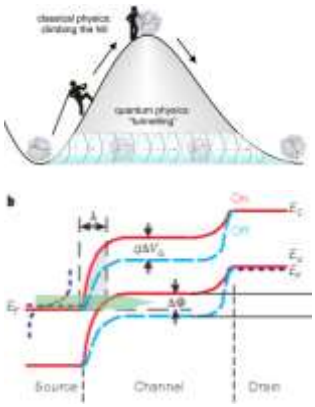
la double nature corpusculaire et ondulatoire de la matière lui permet de traverser des obstacles

ces obstacles peuvent être des “murs énergétiques”

=> exploité dans les transistors et les microscopes à effet tunnel

=> utilisé dans les ordinateurs à recuit quantique de D-Wave pour déterminer le minimum énergétique d’un système complexe (dit « hamiltonien »)

découverte : Henri Becquerel, 1896.



Il l’est aussi dans les transistors, inventés en 1947 !

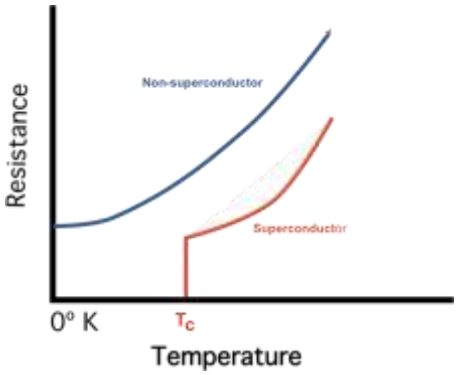
Supraconductivité

Le phénomène de la supraconductivité a été découvert expérimentalement en 1911 avec du mercure à 4,2K par **Heike Kamerlingh Onnes** (1853-1926), Cornelis Dorsman, Gerrit Jan Flim et Gilles Holst à l’Université de Leiden aux Pays-Bas. Notons le faux-ami en anglais : la supraconductivité devient *superconductivity*.

Son interprétation n’a été formulée qu’en 1957 par John Bardeen[96], Leon Neil Cooper et John Robert Schrieffer de l’Université de l’Illinois, qui ont bâti ce que l’on appelle la **théorie BCS**[97].

La supraconductivité se manifeste lorsque l’on baisse la température de certains matériaux. A partir d’un certain niveau, ils n’opposent plus de résistance au courant électrique. Dans la conductivité habituelle, les électrons se baladent d’atomes en atomes et, ce faisant, transforment une partie de leur énergie cinétique en chaleur, liée au mouvement des atomes.

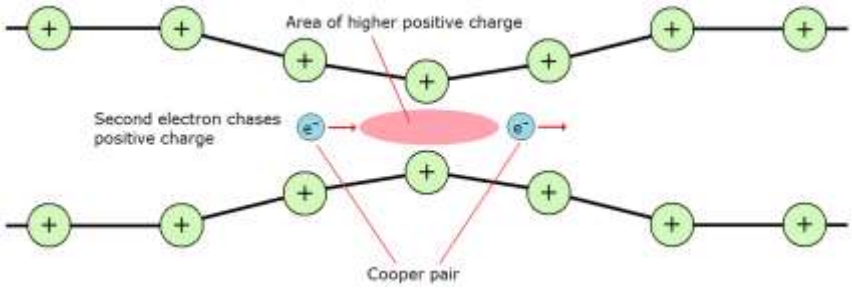
En supraconductivité, les électrons s’arrangent en paires, dites de Cooper, qui circulent entre les atomes et sans friction.



[96] John Bardeen est détenteur de deux prix Nobel de physique, l’un en 1956 pour l’invention du transistor avec William Shockley et Walter Brattain et l’autre pour l’interprétation de la supraconductivité en 1972 avec Leon Neil Cooper et John Robert Schrieffer. Cooper a cocréé la théorie BCS à 27 ans et a obtenu le prix Nobel correspondant à 42 ans. Né en 1930, il est toujours de ce monde.

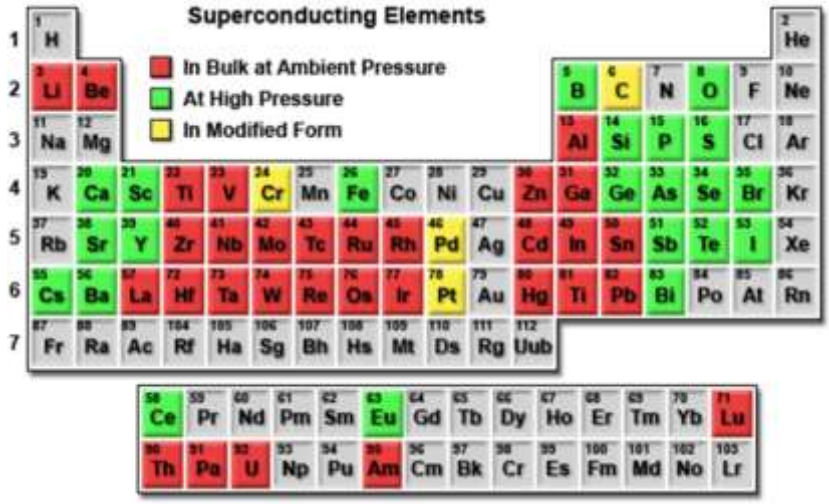
[97] Une timeline précise de la découverte du principe de la supraconductivité est fournie dans la présentation 50 Years of BCS Theory “A Family Tree” Ancestors BCS Descendants, de Douglas James Scalapino, John Rowell et Gordon Baym, 2007 (52 slides). Voir aussi l’excellent ouvrage The rise of superconductors de P.J. Ford et G.A. Saunders 2005 (224 pages) qui raconte bien l’histoire de la découverte puis de l’interprétation de la supraconductivité. Avant la théorie BCS, un grand nombre de physiciens s’étaient cassés les dents sur l’explication de la supraconductivité : Albert Einstein, Niels Bohr, Lev Landau, Max Born, Felix Bloch, Léon Brillouin, John Bardeen (co-inventeur du transistor), Werner Heisenberg et Richard Feynman

La structure des atomes du métal conducteur est aussi modifiée. Il se produit des ondulations des atomes qui suivent et accompagnent le mouvement des paires de Cooper. On appelle cela des phonons [98]. Les paires de Cooper sont des électrons de spins opposés.



C'est notamment là que la mécanique quantique intervient pour expliquer la supraconductivité. Le fonctionnement des électrons dans ces paires est formalisé par leur fonction d'onde. Tout le formalisme mathématique associé est celui de la mécanique quantique. Heike Kamerlingh Onnes a aussi découvert qu'un champ magnétique dont le niveau dépend de la température pouvait faire disparaître l'effet supraconducteur[99].

Une cinquantaine d'éléments sont supraconducteurs à basse température mais le seuil de la supraconductivité en température et pression est très variable. La supraconductivité est aussi possible avec des matériaux composites comme des alliages de germanium, de titane et de niobium ou à base de cuivre (les cuprates). C'est notamment le cas de l'aluminium et du mercure. Dans la pratique, un alliage de niobium et de titane est le plus souvent utilisé[100].



On le retrouvera plus loin dans les câbles supraconducteurs de lecture de l'état de qubits supraconducteurs à effet Josephson.

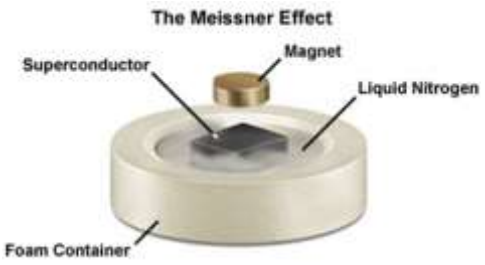
L'effet supraconducteur est maximum pour les atomes qui ont un grand nombre d'électrons de valence, à savoir dans la dernière couche orbitale et de nombre quantique le plus élevé.

[98] Source de l'illustration : Superconducting properties of ZrNi2-xTMxGa (TM = Cu, Co) and ZrNi2AlxGa1-x Heusler Compounds (77 pages). Lien supprimé car site générant une détection dans l'antivirus Avast.

[99] Voir cette présentation détaillée : Superconductivity and Electronic Structure par Alexander Kordyuk, 2018 (145 slides).

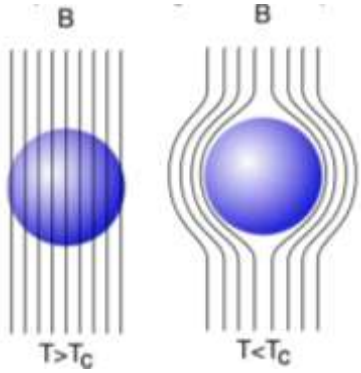
[100] Voir Superconductivity 101. Les propriétés supraconductrices de l'alliage niobium-titane ont été découvertes en 1962. Celui-ci est très utilisé dans le refroidissement des scanners IRM mais aussi dans de nombreux instruments scientifiques, notamment dans le réacteur expérimental de fusion nucléaire ITER de Caradache.

La supaconductivité explique des phénomènes inattendus comme la lévitation d'aimants au-dessus de supraconducteurs plongés dans le l'azote liquide, une expérience favorite de Julien Bobroff.



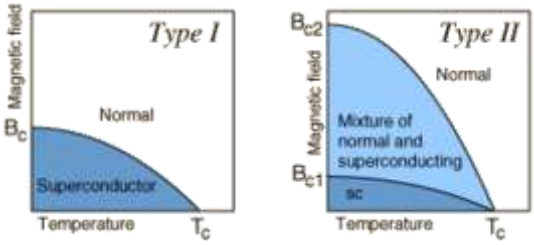
Des céramiques supraconductrices, découvertes à partir de 1986 peuvent être utilisées dans cette expérience saisissante[101].

Le champs magnétique est alors expulsé de l'intérieur du matériau supraconducteur. C'est l'effet Meissner, découvert en 1933 par **Walther Meissner** (1882-1974, Allemand), qui ne s'applique qu'à certains supraconducteurs dits de type I. Il explique la répulsion démontrée dans de nombreuses expériences.



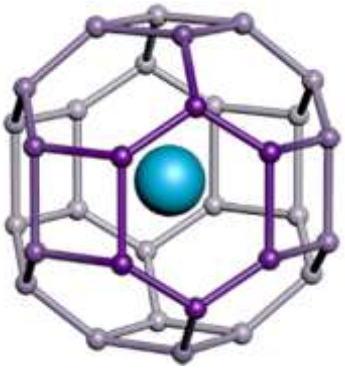
Le type II qui ne génère pas ce phénomène comprend les alliages de niobium titane qui sont fréquemment utilisés avec un ratio 1 pour 1 de chaque dans l'alliage.

Dans les supraconducteurs de type II, il existe une phase intermédiaire entre la phase métallique classique et la phase supraconductrice qui laisse passer le champs magnétique partiellement[102].



Le Graal de la supraconductivité serait de l'obtenir à température ambiante, permettant par exemple de réduire les pertes en ligne du transport de l'électricité.

Les scientifiques ont commencé à découvrir des alliages métalliques supraconducteurs au-dessus de 77K à la fin des années 1980, soit la température de l'azote liquide. La plupart sont des cuprates (à base de cuivre). Un record a été obtenu en 2019 avec une molécule associant du lanthanium et de l'hydrogène (LaH_{10}) et à -23°C, donc une température presque ambiante. Dans ce dernier cas, cela ne fonctionne toutefois qu'à une pression énorme de 218 GPa, soit plus de 2 millions de fois la pression atmosphérique qui est de 101 325 pascals[103]. Un dernier record a été battu avec de l'hydrogène métallique en 2020 par des chercheurs du CEA et à 17°C et 400 GPa[104].



Ce n'est donc pas très pratique ! D'où les projets d'utilisation de simulateurs ou ordinateurs quantiques pour faire jouer les équations de la supraconductivité et identifier des matériaux qui seraient supraconducteurs à température ambiante ou presque ambiante[105].

---

[101] Les céramiques supraconductrices à haute température ont été découvertes en 1986 par Georg Bednorz et Alex Müller, combinant du lanthanium, du barium du cuivre et de l'oxygène, et supraconductrices à 30K, un record pour l'époque. Cela leur a valu le Prix Nobel en 1987, un délai très rapide après leur découverte.

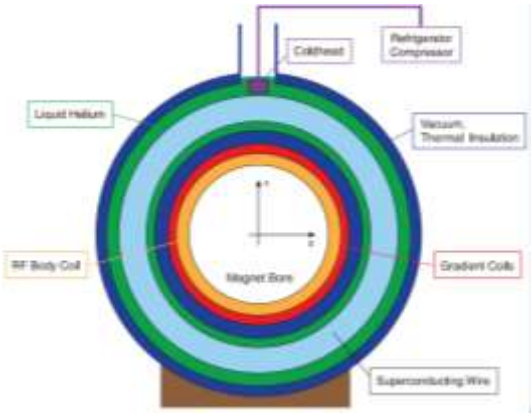
[102] Source de l'illustration.

[103] Voir Quantum Crystal Structure in the 250 K Superconducting Lanthanum Hydride par Ion Errea, juillet 2019 (20 pages).

[104] Voir Voici l'hydrogène métallique - enfin !, par Jean-Baptiste Veyrieras, mai 2020.

[105] Une autre solution consiste à baisser la température ambiante. Voir Novel approach to Room Temperature Superconductivity problem par Ivan Timokhin et Artem Mishchenko, 1ier avril 2020 (4 pages).

La supraconductivité est couramment utilisée dans les **scanners IRM**[106]. Ceux-ci exploitent des aimants géants supraconducteurs qui sont refroidis à l'hélium liquide. Les scanners sont enrobés d'une protection pour contenir le magnétisme à l'intérieur du scanner. Le câblage de bobines y est réalisé en niobium-titane et est intégré dans une matrice de cuivre. C'est le même alliage que celui des fils supraconducteurs qui servent à lire l'état des qubits supraconducteurs.



source de l'illustration à droite : Helium Reclaim in Magnetic Resonance Imagers de Dan Hazen, MKS Instruments (5 pages).

La supraconductivité est exploitée dans le train à grande vitesse maglev **Chuo Shinkansen** expérimenté au Japon depuis 2013 et dont la vitesse commerciale doit atteindre 505 km/h. Il utilise une suspension magnétique qui exploite la supraconductivité. Cela entraîne des infrastructures hors de prix. La consommation électrique au passager/kilomètre est du triple des Shinkansen traditionnels mais compétitive face aux avions. La démonstration est intéressante mais ce genre de moyen de transport n'a pas forcément vocation à se répandre. Une ligne Tokyo-Nagoya de 286 km doit ouvrir en 2027.

La supraconductivité a aussi été étudiée pour améliorer le rendement de moteurs et de générateurs électriques avec les HTS Synchronous Motors (High-Temperature Superconducting). Elle permet d'en réduire la taille et d'en améliorer le rendement. Ils utilisent des matériaux supraconducteurs qui se contentent d'un refroidissement à l'azote liquide mais certains systèmes font tout de même appel à du refroidissement par hélium. Les études ont démarré dans les années 1980 et ces moteurs et générateurs commencent à être déployés dans la marine militaire et dans la production d'énergie éolienne, notamment chez **ASMC**, **Sumitomo Electric**[107] et avec le projet européen **EcoSwing** (qui implique la division cryostats de Sumitomo).

Des câbles supraconducteurs ont été lancés pour transmettre de l'électricité sans perte d'énergie et avec une plus grande capacité permettant de répondre à la demande qui est en augmentation constante. Ils sont notamment proposés par le fabricant français de câbles Nexans qui en a installé un à Long Island. Leur câble sous-terrain de 600 m est en opération depuis 2008. Il permet d'alimenter 300 000 foyers en électricité[108]. Mais c'est complexe à mettre en œuvre. Le projet a couté en tout $46,9M.

[106] Imagerie à résonance magnétique nucléaire.

[107] Voir Design of MW-Class Ship Propulsion Motors for US Navy by AMSC par Swarn S. Kalsi, 2019 (50 slides).

[108] Source de l'information : Long Island HTS Power Cable, Department of Energy, 2008 (2 pages). En plus de Nexans, le système de cryogénie a été fourni par Air Liquide.

Pour ce qui concerne les ordinateurs quantiques, la supraconductivité est utilisée en particulier dans les qubits supraconducteurs qui utilisent l'effet Josephson qui nous avons déjà décrit dans une partie précédente.

La supraconductivité pourrait aussi servir à créer des processeurs CMOS fonctionnant à basse température et capables d'opérer jusqu'à 100 GHz, soit vingt-cinq fois plus rapidement que les processeurs serveurs actuels (3 à 4 GHz maximum chez AMD et Intel)[109]. Une équipe du MIT communiquait en juillet 2019 sur une proposition de technique de création de neurones artificielles à impulsion (spiking neurons) avec des circuits supraconducteurs à effet Josephson exploitant des nanofils[110]. Reste à créer un prototype pour tester tout cela ! Ces différentes recherches menées depuis deux décennies ne semblent pas avoir encore abouti commercialement.

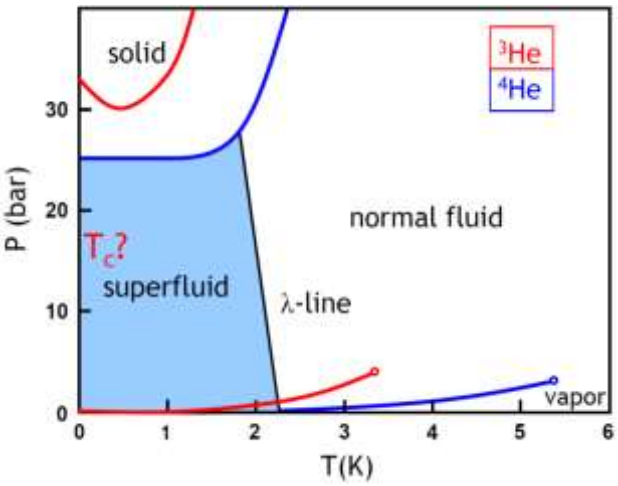
Enfin, une quantité impressionnante d'aimants supraconducteurs à haute puissance sont utilisés dans les accélérateurs de particules comme le **LHC** du CERN à Genève. Il y en a sur plus de 21 km de long ! La supraconductivité permet de créer un courant de 11 850 ampères générant un puissant champ magnétique de 8,33 tesla qui créé une force centripète maintenant les particules accélérées dans le grand cercle de l'accélérateur. Ces aimants sont refroidis par 10 000 tonnes d'hélium 4 superfluide à 1,9K. Leurs câbles sont constitués de filaments de niobium-titane entourés de cuivre. Le tout consomme 40MW. C'est le frigo le plus grand et le plus puissant du monde !

Superfluidité

Un autre phénomène qui relève de la mécanique quantique est à décrire, celui de la superfluidité. Il se manifeste notamment avec l'hélium superfluide qui, à pression ambiante, ne gèle jamais, aussi basse soit la température.

Lorsque l'on en verse dans un vase, il a tendance à remonter par capillarité sur le bord du vase et à s'écouler à l'extérieur de celui-ci. Il peut même traverser des capillaires très fins[111].

Ce sont des propriétés physiques très utiles pour la réfrigération cryogénique, en particulier pour descendre à des températures inférieures à 1K.



L'hélium a été liquéfié pour la première fois en 1908 et à 4,2K par Heike Kamerlingh Onnes, le découvreur de la supraconductivité en 1911. Sa superfluidité a été mise en évidence indépendamment en 1938 par **Pyotr Kapitsa** (1894-1984, URSS, dont nous reparlerons au sujet de la résistance qui porte son nom), **John Frank Allen** (1908-2001, USA) et **Don Misener** (1911-1996, USA)[112].

Il existe deux isotopes de l'hélium : l'hélium 3 avec un seul neutron, le moins abondant, et l'hélium 4 avec deux neutrons, le plus courant. Ce dernier est un boson, de spin entier, ce qui lui donne des propriétés différentes de l'hélium 3 qui est un fermion avec un spin demi-entier. A basse température, l'hélium 3 se comporte comme des condensats de Bose-Einstein, qui sont des gaz et pas des liquides.

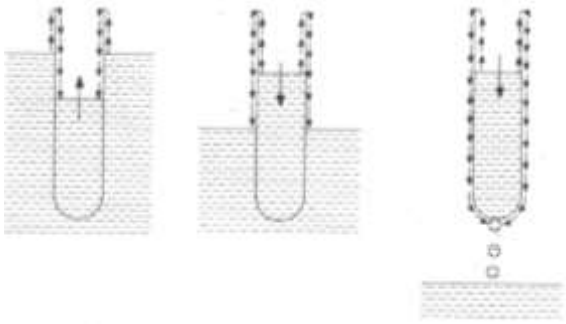
---

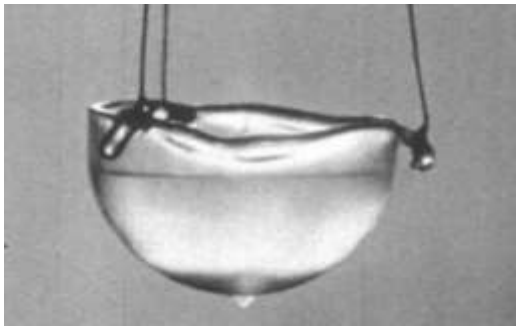
[109] Voir Superconductor ICs: the 100-GHz second generation par Darren Brock, Elie Track et John Rowell d'Hypress, 2000 (7 pages).

[110] Voir A Power Efficient Artificial Neuron Using Superconducting Nanowires par Emily Toomey, Ken Segall et Karl Berggren, 2019 (17 pages).

[111] Source du schéma : Helium 4 (14 slides).

[112] Voir Viscosity of Liquid Helium below the λ-Point, Piotr Kapitsa, Nature 74, 141 (1938) et Flow of liquid helium II, Joan F. Allen, Don Misener, 1938 (pages). Pyotr Kapitsa a obtenu le prix Nobel en 1978 pour ses travaux dans le domaine des basses températures.

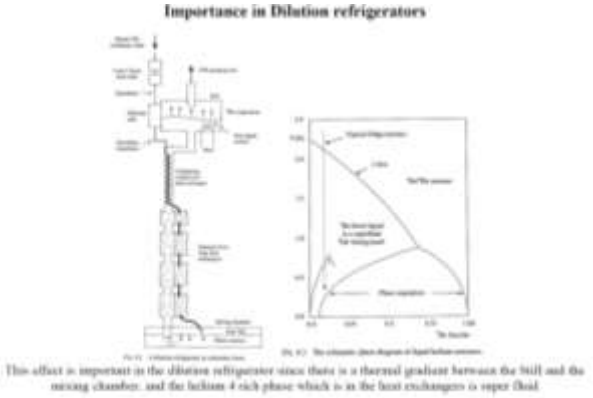




Il devient superfluide à plus basse température que l'hélium 4, soit 1 mK en l'absence d'un champ magnétique (cf le diagramme *ci-dessus*), vs 2,17K pour l'hélium 4. Sa superfluidité n'a été découverte qu'en 1973[113]. Ce sont les différentes propriétés de l'hélium 3 et 4 qui servent à faire fonctionner les systèmes de cryogénie à dilution qui équipent nombre d'ordinateurs quantiques dont la température opérationnelle est située entre 10mK et 20mK. Nous allons étudier cela en détail.

La demande industrielle d'hélium est répartie dans de nombreux secteurs d'activité. Le premier est l'imagerie médicale pour le refroidissement des aimants de systèmes d'IRM. Le second correspond aux industries micro-électroniques dont font partie celles de l'informatique quantique.

La superfluidité fait partie du champ de l'hydrodynamique quantique que nous retrouverons avec les fluides de lumière au sujet des polaritons.



source du schéma à droite : Intelligas Consulting.

Lasers et masers

Les masers et lasers sont des applications de trois découvertes et inventions successives :

Les **cavités résonantes** Fabry-Pérot, des noms de Charles Fabry[114] (1867-1945) et Alfred Pérot (1963-1925). Leur système servait à l'origine à la création d'un interféromètre. Elles ont été inventées en 1898.

L'**émission stimulée** formalisée par Einstein en 1917. Il se manifeste lorsqu'un atome reçoit un photon d'énergie équivalente à une transition entre deux niveaux d'énergie. Il réémet alors deux photons identiques à celui qui a été reçu et le niveau d'énergie de l'atome est réduit au niveau bas.

Le **pompage optique** inventé par Alfred Kastler en 1949 à l'ENS, ce qui lui valut le prix Nobel de Physique en 1966.

---

[113] David Morris Lee (1931), Douglas Dean Osheroff (1945) et Robert Coleman Richardson (1937-2013) ont obtenu le Prix Nobel de physique en 1996 pour leur découverte de la superfluidité de l'hélium 3.

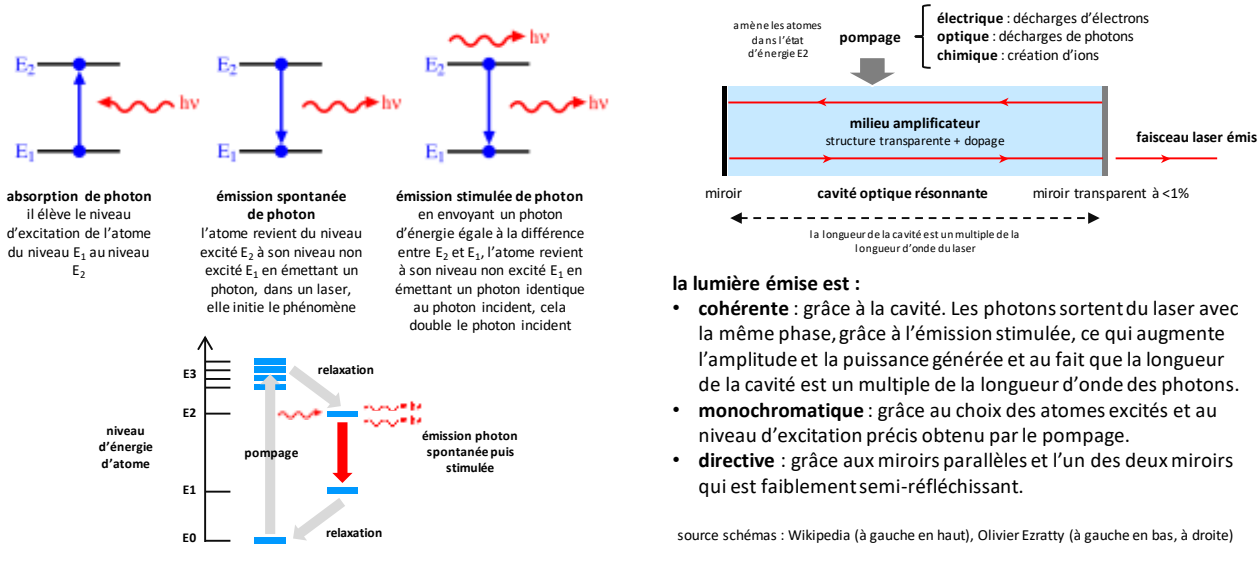
[114] On doit à Charles Fabry la création de l'Institut d'Optique dont il a été le premier directeur en 1926 de la grande école d'ingénieurs qui s'appelait à l'origine SupOptique ou Ecole Supérieure d'Optique.

Il permet de générer une inversion de population, créant une proportion élevée d'atomes excités au niveau E_2 dans le schéma ci-dessous par rapport au niveau E_1. Le pompage optique passe souvent par des niveaux d'énergie supérieurs à E_2 dans les schémas *ci-dessous*, avec une transition non radiative de ces niveaux au niveau E_2 puis du niveau E_1 au niveau fondamental de l'atome E_0. Si le pompage était réalisé uniquement entre les niveaux E_1 et E_2, leur proportion s'équilibrerait et l'effet laser ne pourrait pas se déclencher. On utilise un pompage à trois niveaux pour les lasers à impulsions et à quatre niveaux pour les lasers continus.

Un laser comprend une cavité résonante remplie d'un milieu à gain ou amplificateur. Le pompage de ce milieu à gain est optique, électrique ou chimique. Une fois au niveau d'énergie élevé (E_2 dans le schéma *ci-dessous*), l'atome descend au niveau d'énergie E_1 de manière spontanée ou stimulée, le mécanisme pouvant s'autoentretenir puisque les photons d'émission spontanée génèrent ensuite l'émission stimulée de photons identiques en fréquence, phase et amplitude.

L'émission stimulée est entretenue grâce au placement des atomes au sein d'une cavité transparente, remplie de solide, liquide ou gaz, dotée de miroirs qui piègent ainsi les photons[115]. L'un des miroirs est légèrement semi-réfléchissant, permettant à la lumière amplifiée de sortir en partie. La lumière résultante de ce processus est directive (grâce aux miroirs), monochromatique (grâce au choix des atomes excités et de la finesse de la cavité) et cohérente (les photons sont en phase grâce à l'émission stimulée et au fait que la longueur de la cavité est un multiple de la longueur d'onde du laser). La fréquence des photons émis par le laser dépend des matériaux utilisés dans la cavité et de la longueur optique de la cavité. Côté ordre de grandeur, un laser rouge de 1mW émet $3x10^{15}$ photons par secondes.

le laser et le maser sont des applications de l'effet photoélectrique et de l'interaction lumière-matière



la lumière émise est :

- **cohérente** : grâce à la cavité. Les photons sortent du laser avec la même phase, grâce à l'émission stimulée, ce qui augmente l'amplitude et la puissance générée et au fait que la longueur de la cavité est un multiple de la longueur d'onde des photons.
- **monochromatique** : grâce au choix des atomes excités et au niveau d'excitation précis obtenu par le pompage.
- **directive** : grâce aux miroirs parallèles et l'un des deux miroirs qui est faiblement semi-réfléchissant.

source schémas : Wikipedia (à gauche en haut), Olivier Ezratty (à gauche en bas, à droite)

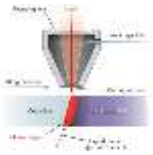
Les lasers (light amplification by stimulated emission of radiation) sont apparus conceptuellement en 1958 dans un article d'Arthur Leonard Schawlow et Charles Hard Townes. Le premier **laser à gaz** a été créé en 1960 par Theodore Maiman, à l'hélium-néon. On a eu ensuite successivement des **lasers à cristaux dopés** (comme le rubis qui est de l'Al_2O_3 dopé au Cr^{3+}, ou le YAG, du grenat d'Yttrium et d'Aluminium $Y_3^{3+}Al_5^{3+}O_{12}^{2-}$), des **lasers chimiques**, des **lasers à diodes** laser semi-conductrices (les plus courants aujourd'hui, en général à base d'arséniure de gallium, ou AsGa), des **laser à fibres** et enfin, des **lasers à électrons libres**, que nous avions déjà rapidement survolés dans la partie sur la mécanique quantique relativiste.

[115] On parle en général de cavités Fabry-Pérot. Leur système inventé en 1898 servait à l'origine à la création d'un interféromètre.

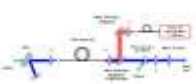
Les lasers fonctionnent soit par impulsion, soit en continu[116]. Le premier mode permet d'obtenir des niveaux de puissance très élevés. A noter que pour créer des lasers très puissants, on créé des amplificateurs laser qui sont des chaînes de lasers avec un laser amorce qui est relié à une série de lasers qui amplifient successivement la lumière générée par le laser précédent.

Les gammes de fréquences couvertes par les lasers vont de l'infrarouge à l'ultra-violet. Il existe même des types de lasers à fréquence ajustable. Les lasers à électrons libres vont jusqu'aux rayons X.

gas	cristaux dopés	chimiques	diodes	fibres	électrons libres
argon ionisé krypton ionisé hélium-néon cuivre-néon azote CO_2 excimère	rubis Nd-YAG terres rares titane chrome OPO	hydrogène-fluor deuterium-fluor	AsGa DFB VCSEL	Ytterbium Erbium Nd^{3+}	





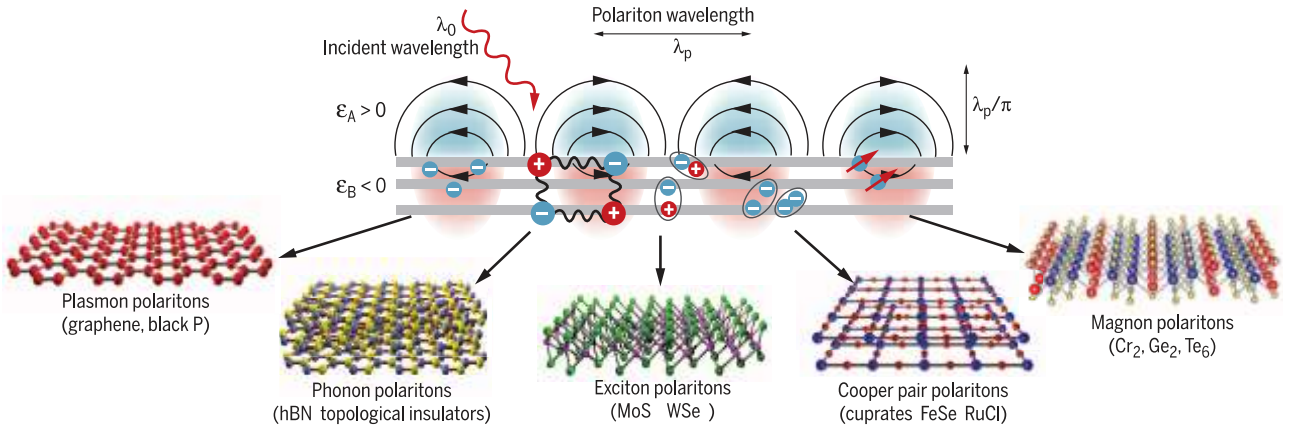
Les usages des lasers sont très nombreux : la découpe dans l'industrie ainsi que le perçage de diamants (1965), la lecture de codes-barres (1974), l'impression laser (1981), les scanners bureautiques, les Laserdisc, les CD (1982) et les DVD (1995), la chirurgie notamment en ophtalmologie (glaucome, décollement de la rétine, rectification de la courbure de la cornée), la chirurgie esthétique, en dermatologie, pour le détatouage, pour l'épilage, les télécommunications, les pointeurs laser, les capteurs de profondeur, les capteurs de mise au point pour les smartphones, le capteur de FaceID des iPhone, l'événementiel, la mesure et l'alignement dans le BTP, les LiDAR, l'impression 3D en stéréolithographie, la microscopie confocale (images de très faible profondeur), la cytométrie en flux (comptage de cellules), l'analyse de puces à ADN, les sources lumières de projecteurs vidéo, la mesure de vitesse, le décapage de certains matériaux, les armes, la fusion nucléaire, les optiques adaptatives dans les télescopes, le refroidissement d'atomes, les télécommunications quantiques, la cryptographie quantique et enfin, le calcul quantique. Bref, les lasers sont un peu partout !

Le Maser (1953) ou "Microwave Amplification by Stimulated Emission of Radiation" ont été inventés avant le laser, en 1953, par Nikolay Basov, Alexander Prokhorov et Charles Hard Townes, devenus prix Nobel de physique en 1964. Ils sont l'équivalent du laser, mais émettant des micro-ondes au lieu de lumière visible. Les micro-ondes sont des ondes électromagnétiques de fréquence moins élevée que l'infrarouge dans le spectre électromagnétique. Les premiers Masers étaient réalisés avec de l'ammoniaque et généraient des photons micro-onde de 24 GHz. Suivirent des Masers à hydrogène en 1960.

Polaritons

Nous allons évoquer sur quelques pages un domaine de la physique quantique rarement évoqué au sujet des technologies quantiques, celui des polaritons. Il est encore majoritairement situé dans le champ de la recherche fondamentale mais pourrait avoir un intérêt dans différents domaines comme dans le calcul quantique. Il est par contre déjà appliqué dans le domaine de la métrologie quantique.

[116] Voir 50 ans de laser par Hélène Perrin, 2010 (48 slides), une très bonne vulgarisation du fonctionnement des lasers et de leur histoire, et le cours Les LASERS et leurs applications par Sébastien Forget du LPL de l'Université Paris 13 Nord (196 slides). Voir aussi la bonne vulgarisation de Le laser, un concentré de lumière, CEA, 2014 (28 pages).



Les polaritons sont des quasi-particules quantiques du domaine des interactions fortes entre lumière et matière. Ils résultent du couplage entre des photons et une onde de polarisation électrique. Ces ondes se manifestent en particulier dans des plasmons (oscillations d'électrons libres dans des métaux), des phonons (oscillations d'atomes, en particulier dans des structures cristallines) et des excitons (paires d'électrons-trous d'électrons générées par des photons dans des semi-conducteurs[117]). La matière en question peut être un gaz d'atomes, des semiconducteurs classiques massifs ou sous forme de couches minces insérées dans des cavités optiques, voire des jonctions supraconductrices Josephson.

Les photons d'excitation ont une longueur d'onde correspondante à la fréquence de résonance du milieu associé, souvent située dans la lumière visible ou dans l'infrarouge. Les polaritons ont des propriétés mixtes de photons habillés par des excitations électroniques. Ils se comportent comme des bosons (spin entier) qui peuvent occuper le même état quantique et fonctionner « en meutes », comme les courants supraconducteurs à base de paires de Cooper (électrons appariés) ou les condensats Bose-Einstein (BEC)[118].

Il se dit par extrême simplification pour expliquer la cinématique des polaritons que la matière semi-conductrice y reçoit des photons qui l'excitent. Elle émet à son tour des photons pour sortir de son état excité, le tout dans un cycle itératif très rapide, les photons circulant en circuit fermé dans la cavité. En pratique, les champs électromagnétiques et de polarisation se copropagent dans le milieu de manière identique, notamment en polarisation et en fréquence, et avec une relation de phase fixe (sans déphasage ou avec un déphasage de 180°, soit π). Les polaritons présentent surtout l'intérêt de générer de fortes non-linéarités qui sont très recherchées en photonique comme nous l'avons cité au niveau des qubits photons[119].

Grâce aux états dégénérés dans lesquels les polaritons peuvent être préparés et au fait qu'ils interagissent entre eux, les polaritons constituent un fluide quantique hors équilibre que l'on appelle "fluide quantique de lumière", souvent abusivement qualifié de « lumière liquide ».

---

[117] L'appellation de polariton a été créée par Joseph John Hopfield (1933, Américain) en 1958 et concernait à ce moment les exciton polaritons. Voir Theory of the Contribution of Excitons to the Complex Dielectric Constant of Crystals, Joseph John Hopfield, 1058 (14 pages). Hopfield est aussi connu dans le champ des réseaux de neurones dans l'IA avec ses « Hopfield networks ».

[118] Selon l'échelle d'interaction, les polaritons fonctionnent dans un régime semiclassique ou quantique. Dans le premier cas, le champ électromagnétique interagit avec un champ de polarisation macroscopique. Le champ de polaritons présente alors les propriétés d'un champ classique mais son quantum élémentaire est le fruit d'un "habillage" dipôle-photon descriptible seulement par la mécanique quantique. Dans le second cas, le champ électromagnétique interagit avec un seul quantum de champ de polarisation qui a été isolé d'une manière ou d'une autre, comme par exemple un qubit supraconducteur ou un exciton dans une boîte quantique. On est alors dans le régime quantique du couplage fort, dit « hamiltonien de Jaynes-Cumings », où les niveaux d'énergies sont discrets et correpsondent chacun à un nombre donné de quantum d'excitations dans le système. Les polaritons-excitons en cavité sont de manière très générale dans le premier régime.

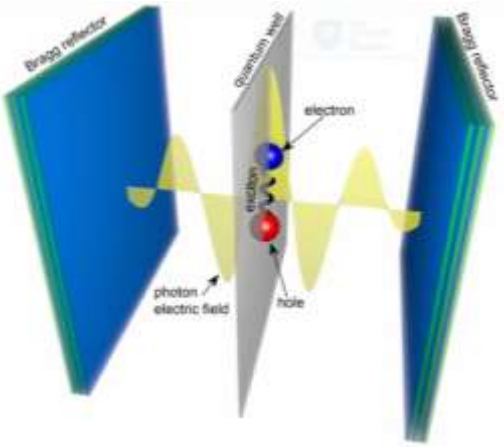
[119] Source de l'illustration : Polaritons in van der Waals materials par D. N. Basov et al, 2016 (9 pages) qui au passage fait un bon inventaire de différents types de polaritons et de leurs domaines d'applications. Voir aussi ce très dense « review paper » Quantum Fluids of Light par Iacopo Carusotto et Cristiano Ciuti, 2013 (68 pages).

Les polaritons peuvent ainsi générer des ondes de surface et des phénomènes de propagation typiques de fluides quantiques comme la superfluidité.

Les polaritons interagissent aussi entre eux, ce qui n'est pas le cas des photons dans le vide[120]. On peut expérimentalement contrôler la distribution spatiale de la densité, de la phase et de la vitesse de ces fluides de lumière[121].

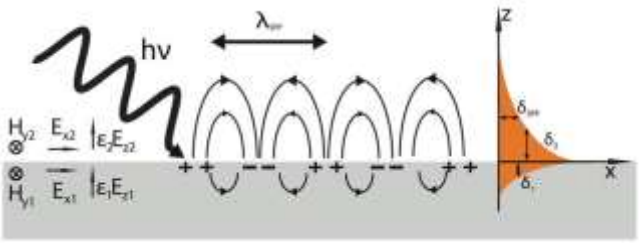
Il existe de nombreuses variantes de polaritons qui dépendent de la nature de l'excitation électronique de la matière sachant que j'utilise d'abord leur dénomination en anglais puis en français :

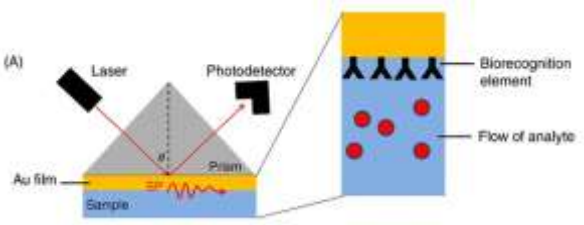
- Les **phonon-polaritons** (polaritons phononiques) qui résultent du couplage entre un photon infrarouge et un phonon optique provoqué par l'oscillation mécanique de deux ions adjacents de charge opposée dans une structure cristalline. Cette oscillation produit un moment dipolaire électrique oscillant. Ce phénomène a été découvert par **Kirill Tolpygo** (1916-1994, Russe) en 1950 et, de manière indépendante, par **Kun Huang** (1919-2005, Chinois) en 1951.
- Les **exciton-polaritons** résultent du couplage d'un photon avec un exciton dans une cavité semiconductrice. Un exciton est une quasi-particule constituée d'une paire électron-trou d'électron reliée par des forces de Coulomb, générée par des photons d'excitation. La notion d'exciton a été créée par **Yakov Frenkel** (1894-1952, Russe) en 1931. Comme tous les types de polaritons, ceux-ci ont deux bandes d'énergie : le polariton haut et bas. C'est une propriété générale du régime de couplage fort entre dipôle électrique et champ électromagnétique. Ici, le niveau est haut lorsque le photon et le semiconducteur sont excités et en phase et bas lorsqu'ils sont en opposition de phase.



  La recherche planche sur la création de transistors utilisant des exciton polaritons depuis quelques années (source du schéma) ainsi que sur le contrôle de quantum unique[122].

- Les **surface plasmon polaritons** (SPP, polaritons plasmoniques de surface) résultent du couplage entre des plasmons de surface et des photons. Un plasmon est une oscillation quantifiée de gaz d'électrons de haute densité. Un plasmon de surface est une oscillation cohérente d'électrons se produisant à l'interface entre deux matériaux différents, souvent un métal et un diélectrique ou entre le métal et l'air. Un polariton plasmonique de surface est une telle oscillation provoquée par un photon incident[123].





[120] Voir la pédagogique présentation Swimming in a sea of light: the adventure of photon hydrodynamics par Iacopo Carusotto, 2010 (28 slides). Présentation réalisée avec le concours, entre autres, de Elisabeth Giacobino et Alberto Bramati du CNRS. Voir aussi la très bien illustrée présentation Quantum fluids of light par Jacqueline Bloch, février 2020 (58 slides).

[121] Source : description du projet ANR : Fluides Quantiques de Lumière – QFL lancé en 2016.

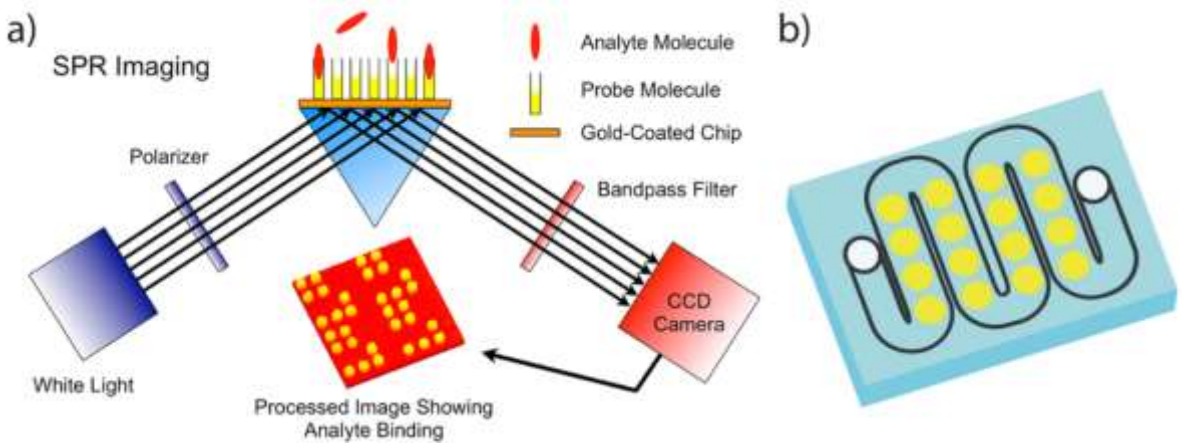
[122] Le mécanisme de "polariton blockade" permet en principe de manipuler les polaritons excitonique de cavité à l'échelle du quantum unique. Voir Towards polariton blockade of confined exciton–polaritons par Aymeric Delteil, 2019 (4 pages).

[123] Source du schéma : Wikipedia.

Les SPP servent notamment à créer des capteurs quantiques optiques de température et de détection de la concentration de différents composants par réfractivité puis spectroscopie, notamment dans les medtechs (détection de molécules organiques diverses, détection d'interaction entre protéines), les analyses biologiques (toxines, drogues, additifs) ou pour la détection de gaz[124].

Ces SPR (Surface Plasmon Resonance) peuvent être bien plus performants que les capteurs à spectroscopie dans le proche infrarouge tels que ceux de Scio[125]. Ils mesurent la lumière polarisée réfléchie d'une diode laser au niveau de son intensité, de son angle, de sa longueur d'onde, de sa phase ou encore de sa polarisation.

Comme dans de nombreux systèmes d'analyse biologique, on peut créer des matrices 2D (microarrays) intégrant un grand nombre de molécules de détection et détecter autant de composants différents dans l'échantillon à analyser[126]. Les SPR sont couramment commercialisés par des sociétés telles que **Bioptix**, **Cytiva**, **Carterra**, **Horiba**[127], **IBIS Technologies**, **Lifeasible** et **Xantec**.



- Les **cavity-polaritons** (polaritons de microcavité) sont une variante de l'exciton polariton où le photon est piégé dans une microcavité et où l'exciton est confiné dans un puit quantique. Ils sont notamment réalisés en semiconducteurs III-V de type indium, arsenic et gallium. Le piégage des photons est souvent réalisé à l'aide de deux miroirs de Bragg se faisant face pour créer une cavité optique qui ont la particularité d'utiliser des couches de diélectriques pour réfléchir la lumière très efficacement et sur toutes les longueurs d'ondes. Ces miroirs sont fabriqués en épitaxie par jet moléculaire permettant une croissance cristalline cohérente, sur substrat cristallin d'arséniure de gallium (GaAs).

---

[124] Source de l'illustration : Surface Plasmon Resonance (SPR) par Lifeasible. Le principe général de cet instrument consiste à utiliser une diode laser pour éclairer en biais une surface en or (via un angle contrôlable mécaniquement) et à capter le rayon réfléchi avec un détecteur. La surface en or est recouverte d'une molécule spécifique (« biorecogition element » dans le schéma) qui a tendance à s'associer à une molécule que l'on souhaite détecter (dans le « flow of analyte » en phase liquide). Les molécules détectées peuvent être des peptides, des polypeptides, des protéines, des enzymes, des vitamines, des séquences d'ADN ou d'ARN ou des anticorps (notamment pour diagnostiquer des cancers). L'association modifie la réflectivité de l'or et permet la détection de la molécule cible.

[125] Voir Recent advances in Surface Plasmon Resonance for biosensing applications and future prospects par Biplob Mondal et Shuwen Zeng, août 2020 (31 pages). Le second auteur est du laboratoire XLIM de Limoges.

[126] Voir Surface Enzyme Chemistries for Ultrasensitive Microarray Biosensing with SPR Imaging par Jennifer B. Fasoli et al, 2015 (10 pages) d'où vient l'illustration associée.

[127] Dont le centre de recherche européen est situé à Palaiseau à côté du C2N du CNRS, de Télécom Paris, de Thales et de l'Institut d'Optique.

Le résultat est monocristallin et peut contenir plus d'une centaine de couches d'alliages différents, d'épaisseurs comprises entre 5nm et 50nm, contrôlées à la monocouche atomique près[128]. Ces polaritons de microcavités ont été découverts en 1992 par Claude Weisbuch (France)[129].

- Les **intersubband-polaritons** résultent du couplage d'un photon infrarouge ou terahertz avec une excitation intersousbande. Ils peuvent notamment servir à créer des détecteurs infrarouges.
- Et puis les **Bragg-polaritons** ("Braggoritons"), les **plexcitons** (plasmons + excitons), les **magnon polaritons** (magnon, ondes de spins dans des matériaux ferro-magnétiques + photons) et les **similaritons** (photons amplifiés dans des fibres optiques).

Bref, tous ces "machin-ons" relèvent de l'interaction entre les photons et différentes formes de matière et notamment d'électrons. Quel rapport avec l'informatique quantique ? Ils sont en fait nombreux, même si je ne vais pas forcément souvent les citer dans cet ebook.

Les polaritons sont utilisés dans différents dispositifs optiques liés aux qubits photons, notamment pour le transport de photons et dans les détecteurs de photons uniques[130].

Ils pourraient à terme permettre de créer des qubits photons pouvant interagir les uns avec les autres. C'est ce qui ressortait notamment d'une publication du MIT et de Harvard de Vladan Vuletic et Mikhail Lukin en 2018 qui démontraient l'interaction de trois photons dans un atome placé dans un état de Rydberg, constituant un « polariton Rydberg »[131]. Un autre projet de recherche de Singapour utilise des excitons polaritons pour créer des qubits photons présentant la particularité de pouvoir fonctionner à température ambiante, et s'appuyant sur des portes à un qubit et une porte $\sqrt{\text{SWAP}}$ à deux qubits[132].

Les polaritons de microcavités peuvent servir à créer des simulateurs quantiques analogiques[133]. Ils sont implantés dans des structures semi-conductrices III-V sous forme de matrices 2D. L'un des domaines d'application, pas très grand public, est la simulation de structures gravitationnelles comme celle d'un rayonnement de Hawking à l'horizon d'un trou noir. Et pourquoi pas, pour simuler le fonctionnement d'un réfrigérateur à dilution associant l'hélium 3 et 4 à très basse température, que nous aurons l'occasion d'étudier dans une partie à venir.

Les polaritons sont aussi le champ de comportements topologiques de la matière et constituent peut-être une voie alternative aux fermions de Majorana pour créer des qubits avec un faible taux d'erreurs. Ce sont des voies plus long terme que les technologies de qubits étudiées dans cet ouvrage, mais dignes d'intérêt.

D'autres applications, déjà citées, visent le champ très diversifié de la métrologie quantique.

---

[128] Voir Fluides quantiques de lumière dans les microcavités à semi-conducteurs par Jacqueline Bloch et Alberto Amo, Reflets de la Physique, 2016 (6 pages) ainsi que Cavity polaritons for new photonic devices par Esther Wertz, Jacqueline Bloch, Pascale Senellart et al, 2010 (12 pages).

[129] Voir Observation of the coupled exciton-photon mode splitting in a semiconductor quantum microcavity par Claude Weisbuch et al, 1992 (4 pages).

[130] Voir Nanoscale Quantum Optics par I. D'Amico et al, 2019 (45 pages).

[131] Voir Physicists create new form of light par Jennifer Chu, 2018 qui fait référence à Observation of three-photon bound states in a quantum nonlinear medium par Qi-Yu Liang et al, 2018 (5 pages).

[132] Nous définirons ce type de porte quantique dans une rubrique dédiée de cet ebook. Voir Quantum computing with exciton-polariton condensates par Sanjib Ghosh et Timothy C. H. Liew, octobre 2019 (6 pages). Tim Liew est un chercheur du laboratoire MajuLab conjoint entre le CNRS et l'Université Nationale de Singapour.

[133] Voir Microcavity Polaritons for Quantum simulation par Thomas Boulier, Alberto Bramati, Elisabeth Giacobino, Jacqueline Bloch et al, mai 2020 (21 pages) ainsi que Polaritonic XY-Ising machine par Kirill P. Kalinin, Alberto Amo, Jacqueline Bloch et Natalia G. Berloff, 2020 (12 pages).

En France, les polaritons sont notamment la spécialité d'Elisabeth Giacobino (CNRS, ANR), Jacqueline Bloch (CNRS C2N[134]), Alberto Bramati (LKB ENS), Alberto Amo (Phlam-CNRS Lille), Le Si Dang et Maxime Richard (CNRS Institut Néel Grenoble).

Extreme quantum

Au-delà des basiques de la physique quantique évoqués *ci-dessus*, de nombreuses autres branches de la physique quantique existent qui méritent d'être citées dans cet ouvrage. Elles peuvent avoir des impacts divers sur les technologies quantiques, notamment du côté de la métrologie. Elles servent aussi en cosmologie. Elles sont enfin malheureusement utilisées et détournées par de nombreuses fausses sciences et arnaques que nous évoquerons dans la partie dédiée aux fumisteries quantiques.

Théorie quantique des champs

La théorie quantique des champs (TQC) ou Quantum Field Theory (QFT) en anglais est une branche de la physique quantique qui s'intéresse à la physique des particules élémentaires, notamment leur création ou leur disparition lors d'interactions diverses, comme les paires d'électrons et positrons. On reproduit généralement ces phénomènes dans les accélérateurs de particules[135].

La QFT couvre aussi les mécanismes de la matière condensée comme les condensats Bose-Einstein ou l'hélium superfluide et plus généralement, le comportement des quasiparticules, des comportements collectifs complexes, comme les paires (d'électrons) de Cooper dans les matériaux supraconducteurs.

La QFT combine des éléments de la mécanique quantique, de la relativité restreinte et des notions classiques de champs électromagnétiques. Elle s'appuie sur un formalisme mathématique encore plus ardu à assimiler que celui de la mécanique quantique. Il exploite notamment la notion de lagrangien et d'intégrales de lagrangiens sur le temps décrivant l'évolution des champs et les interactions entre les champs de plusieurs particules.

La QFT visait notamment à expliquer ou modéliser la structure fine de l'atome d'hydrogène (correspondant à raies spectrales proches non explicables par les sauts quantiques d'énergie classiques), l'existence du spin des particules (qui explique ces raies spectrales), l'émission spontanée de photons par des atomes lors de leur retour à leur état fondamental ainsi que les mécanismes de la radioactivité.

Les bases de la QFT ont émergé sous l'impulsion de nombreux scientifiques à partir de 1928 : **Paul Dirac**, **Wolfgang Pauli**, **Vladimir Fock** (1898-1974, Russe), **Shin'ichirō Tomonaga** (1906-1979, Japonais), **Julian Schwinger** (1918-1994, Américain), **Richard Feynman** et **Freeman John Dyson** (1923-2020, Américain[136]). Shin'ichirō Tomonaga, Julian Schwinger et Richard Feynman ont reçu en 1965 le prix Nobel de physique pour leurs travaux sur l'électrodynamique quantique qui fait partie de la QFT.

Ils avaient notamment résolu au début des années 1950 le problème des valeurs infinies d'énergies générées par les modèles initiaux de la QFT en utilisant une technique d'ajustement dénommée **renormalisation**.

---

[134] La salle blanche du C2N de Palaiseau permet de prototyper tout un tas de nanostructures. Les semiconducteurs utilisés pour gérer des polaritons sont d'ailleurs fabriqués avec des techniques voisines des sources de photons uniques de l'équipe de Pascale Senellart, également du C2N, et de la startup associée, Quandela.

[135] Voir The History of QFT, un site de Stanford, qui résume bien l'histoire de la QFT.

[136] On lui doit aussi la notion de sphère de Dyson qui dimensionne le niveau de contrôle technologique de sources d'énergie par des civilisations extra-terrestres, avec une sphère captant la totalité de l'énergie d'une étoile.

Les physiciens peinent encore à intégrer la théorie de la relativité générale dans la QFT, empêchant cette dernière de devenir une « théorie du tout » expliquant l'intégralité des phénomènes physiques connus de l'Univers.

La QFT est exploitée dans trois principaux domaines :

- Dans la **physique des particules** à hautes énergies explorées dans les accélérateurs de particules comme le LHC du CERN. Elle a été complétée sur ce point par le modèle standard que nous verrons plus loin.
- Dans la **physique de la matière condensée** avec la supraconductivité, la superfluidité et l'effet Hall quantique. C'est le cadre de la **QED** (l'électrodynamique quantique), lancée par Paul Dirac en 1928, qui étudie notamment la production de positrons et les interactions positrons/électrons (attraction, annihilation, création de paires, effet Compton). La sous-branche **cQED** (cavity QED) étudie les relations entre matière et photons dans des cavités optiques. Elle est utilisée par les physiciens de la matière condensée qui travaillent sur les qubits supraconducteurs.
- En **cosmologie** pour modéliser l'origine et l'évolution de l'Univers ainsi que certains mécanismes d'interaction entre trous noirs et champs quantiques.

Fluctuation quantique du vide

L'une des conséquences de la QFT est la notion de fluctuation quantique du vide, aussi appelée énergie du vide. En s'appuyant sur le principe d'indétermination d'Heisenberg qui veut que les quanta soient en perpétuelle fluctuation, la QFT modélise les fluctuations de point zéro ou encore l'énergie du vide, soit le niveau d'énergie minimum des systèmes quantiques.

Dans ce cadre, le principe d'Heisenberg peut être considéré comme un prédicat généralisé. Selon ces modèles, le vide total n'existerait pas. Des fluctuations élémentaires entraînent la création de paires de particules virtuelles électron et positron, qui s'annihilent rapidement, et générant au passage des photons. Le tout à des fréquences élevées mais avec des niveaux d'énergie extrêmement faibles.

Sous l'influence d'un champ électromagnétique environnant, cela conduit à une polarisation du vide. Cette dernière conduit même à rendre le vide biréfringent, son indice de réfraction dépendant de la polarisation de la lumière qui le traverse. Le phénomène n'est cependant potentiellement observable qu'avec un champ électromagnétique très intense.

Les modèles théoriques initiaux indiquaient initialement que cette énergie du vide serait infinie à l'échelle de l'Univers. Ils ont été ensuite corrigés via la méthode dite de renormalisation, déjà citée précédemment. Ces fluctuations élémentaires du vide expliqueraient l'émission spontanée de radiations par les électrons dans les atomes ainsi que la radioactivité spontanée[137].

Le concept d'énergie du vide tient sa source chez **Max Planck** en 1911 au moment où il publie un article contenant une équation d'énergie d'un milieu qui contient une constante fixe, sorte de plancher énergétique de ce milieu. Sans qu'il puisse pour autant l'interpréter. Il faut attendre 1916 pour que le chimiste **Walther Nernst** (1864-1941, Allemand[138]) interprète cette constante comme étant le niveau d'énergie du vide en l'absence de tout rayonnement.

---

[137] Au demeurant, en plus de ces fluctuattions élementaires, le vide est sans cesse traversé, même dans les régions les plus reculées de l'espace, par des ondes électromagnétiques, sans compter les effets de la gravitation. L'Univers est donc rempli de radiations dont le bruit cosmologique diffus qui est un reliquat du big bang, avec une température de 2,7K. Il en va de même dans une boîte mise sous vide car toute matière émet un rayonnement. Voir à ce sujet la conférence Le vide quantique, source d'énergie et d'émerveillement par Michel Spiro, directeur de l'IN2P3, 2003 (1h23mn). Même si le titre est misleading et ne provient probablement pas de l'intervenant.

[138] Walther Nernst a joué un rôle clé dans le lancement des Congrès Solvay à partir de 1911.

Selon la QFT, l'Univers est une vaste soupe contenant des champs fluctuants en permanence, que ce soit les fermions (leptons et quarks) et les bosons (champs de force comme les gluons qui collent ensembles les constituant élementaires des noyaux atomiques que sont les protons et les photons). Cette notion de niveau d'énergie minimum est une version moderne de la notion d'éther - un vide pas complètement vide - qui dominait la physique du XIX^{e} siècle, notamment chez James Clerck Maxwell. Le bain électromagnétique dans lequel le vide est plongé complété par l'énergie du vide donnerait à celui-ci des propriétés de viscosité.

Le modèle de l'énergie du vide est cependant encore incomplet. Il pas encore totalement corroboré par les expériences comme nous le verrons au sujet de l'effet Casimir. On est face à des théories moins abouties que la mécanique quantique « classique ». L'une des solutions évoquées consiste à supposer que les fermions ont une énergie du vide négative et les bosons, une énergie du vide positive, les deux s'équilibrant. Mais ce n'est pas démontré expérimentalement, en particulier pour les particules d'énergie normale non relativistes.

Il y aurait aussi un lien entre l'énergie du vide et l'énergie sombre de l'Univers tout comme la gravité. Mais c'est très spéculatif. Cela pourrait contribuer à expliquer les 73% de l'énergie contenue dans l'Univers, parfois dénommée énergie noire. Sa densité est très faible, de 10^{-13} Joules/cm^2.

Il existe différentes manières de vérifier l'existence de cette fluctuation quantique du vide. La plus connue est liée à l'effet Casimir que nous allons étudier *ci-dessous*. Récemment, des scientifiques français et allemands ont aussi réussi à interagir avec cette fluctuation quantique du vide dans un semiconducteur[139].

Effet Casimir

Le physicien **Hendrik Casimir** (1909-2000, Hollandais) prédisait en 1948 l'existence d'une force attractive entre deux plaques parallèles conductrices et non chargées électriquement[140]. Ce physicien avait obtenu son doctorat en 1931 à l'Université de Leiden aux Pays-Bas. Il avait aussi visité Niels Bohr à Copenhague et avait été un assistant de recherche de Wolfgang Pauli en 1938. L'effet Casimir est interprété comme étant lié à l'existence de l'énergie quantique du vide.

L'expérience imaginée par Casimir utilise des surfaces métalliques miroirs parallèles aussi parfaitement planes que possible. Elles créent une cavité Fabry-Perot similaire à celle que l'on trouve dans les lasers.

L'effet Casimir est couramment attribué aux fluctuations quantiques du vide. Les changements temporaires de niveau d'énergie dans les points de l'espace compris entre les deux miroirs génèreraient de manière spontanée des paires de particules et d'antiparticules de durée de vie très brève et des photons associés à leur annihilation. Ces fluctuations du vide ont lieu dans et hors du volume de la cavité. Mais à cause de l'effet d'interférence induit par la cavité, les fluctuations à certaines fréquences y sont réduites. La densité d'énergie électromagnétique dans la cavité se trouve ainsi plus faible que la densité d'énergie hors de la cavité. Ce sont des fluctuations quantiques spontanées[141].

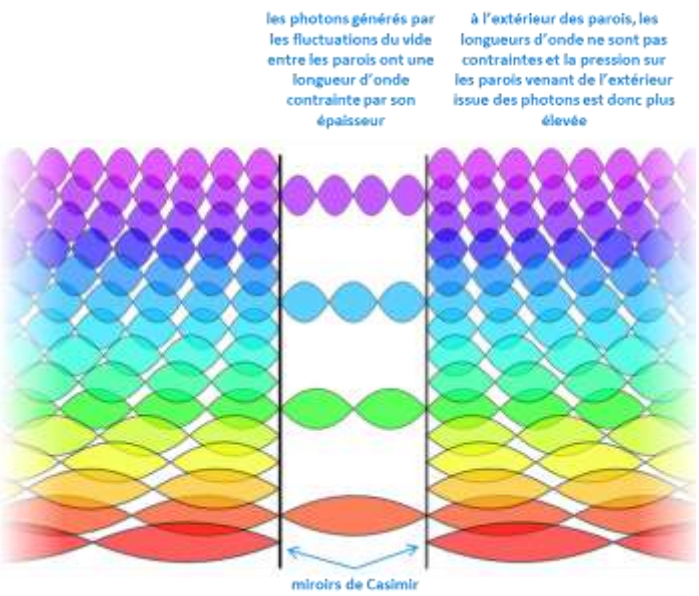
---

[139] Voir Understanding vacuum fluctuations in space, août 2020. Voir aussi Electric field correlation measurements on the electromagnetic vacuum state par Ileana-Cristina Benea-Chelmus, Jérôme Faist et al, 2018/2020.

[140] Voir On the attraction between two perfectly conducting plates, par Hendrik Casimir, 1948 (3 pages) et Electromagnetic vacuum fluctuations, Casimir and Van der Waals forces par Cyriaque Genet, Astrid Lambrecht et al, 2004 (18 pages).

[141] Voir un bon panorama de l'effet Casimir avec The Casimir effect and the physical vacuum par G. Takács, 2014 (111 slides). Voir aussi The Casimir Effect par Kyle Kingsbury, 2014 (82 slides) qui décrit bien les dispositifs expérimentaux d'évaluation de l'effet Casimir et évoque quelques cas d'usage dans les MEMS. Et puis Zero-Point Energy and Casimir-Effect par Gerold Gründler 2013 (47 pages) qui retrace bien l'histoire de l'effet Casimir en remontant aux travaux de Planck en 1911.

L'effet ne s'explique pas par la simple pression supérieure à l'extérieur vis-à-vis de celle qui sévit entre les deux plaques. Dans le détail, les longueurs d'onde des photons générés par le vide à l'extérieur des plaques peuvent être de toute taille et notamment longues tandis qu'à l'intérieur des plaques, ces longueurs d'onde sont contraintes par la distance entre les plaques et ne peuvent être que de 1/n de cette distance. Le spectre électromagnétique spontané du vide est donc plus large hors des plaques qu'à l'intérieur, créant une pression plus forte à l'intérieur qu'à l'intérieur, ce qui a donc tendance à faire se rapprocher les plaques entre elles, mais très légèrement.



Pour deux miroirs parallèles de surface A et une distance L entre les deux miroirs, la force d'attraction entre les deux miroirs suit la formule *ci-contre*. En pratique, L est compris entre 0,2 µm et 5 µm et est habituellement de 1 µm. C'est une échelle « macroscopique ».

$$F_{\mathrm{Cas}} = \frac{\hbar c \pi^2 A}{240 L^4}$$

Selon le principe d'Heisenberg qui sert à expliquer l'effet, l'énergie et le temps peuvent être liés par la formule *ci-contre*. Il montre indirectement que pendant un temps très court, une faible quantité d'énergie peut être créée.

$$\Delta E \cdot \Delta t \geq \frac{\hbar}{2}$$

Le cumul macroscopique de ces opérations s'annihile, permettant d'éviter de violer le principe de conservation de l'énergie. Cela permet au passage d'expliquer pourquoi les hurluberlus qui prétendent capter l'énergie du vide pour produire de l'électricité gratuite ne sont pas prêts d'y arriver.

Les expériences ne sont pas forcément concluantes à 100% et les données générées ne collent pas parfaitement avec les modèles contrairement à nombre d'expériences de la mécanique quantique classique. La raison en serait qu'il est difficile d'obtenir des surfaces parfaites.

Les premières expériences validant l'effet Casimir ont été réalisées presque 50 ans après la définition de cet effet[142]. La première est celle de **Steve Lamoreaux** (Américain) en 1996, utilisant des plaques parallèles. Sa mesure donnait un résultat éloigné de 5% vis-à-vis des prévisions. Les instruments de précision utilisés détectaient alors une force d'un milliardième de Newton.

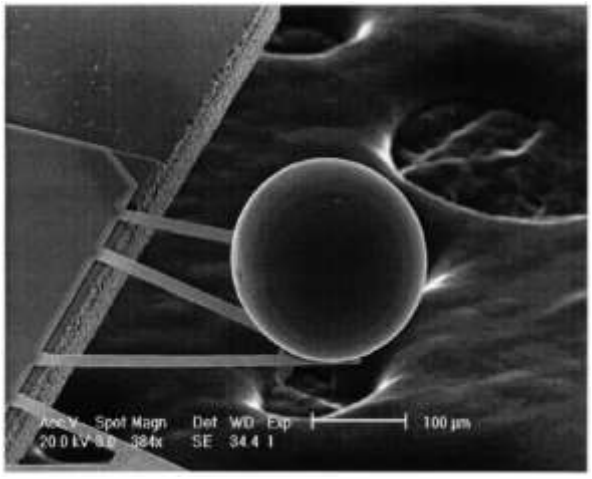
Le modèle a été amélioré dans d'autres expériences réalisées en 1998 puis en 2012 qui exploitaient une géométrie d'électrodes associant un plan et une sphère en polystyrène de 200 µm de diamètre recouverte d'or (schémas *ci-dessous*)[143]. Les différences entre les modèles et les mesures sont maintenant de l'ordre de 1%, ce qui reste significatif en physique.

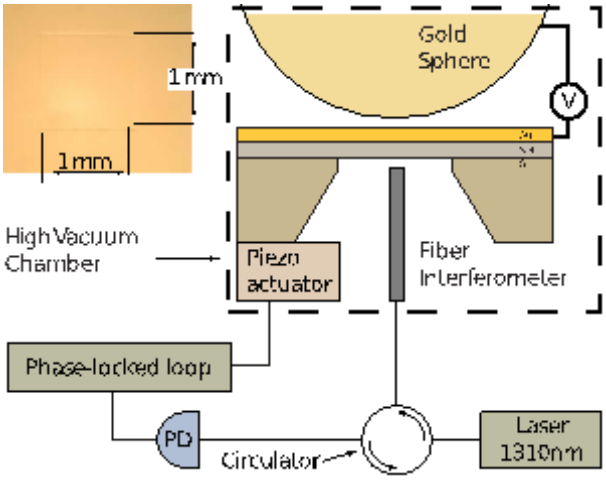
L'effet Casimir permettrait d'expliquer plusieurs autres phénomènes physiques couramment observés comme le moment magnétique anormal de l'électron et le déplacement de Lamb. Le premier phénomène décrit une dérive de ce moment par rapport aux équations de Dirac.

---

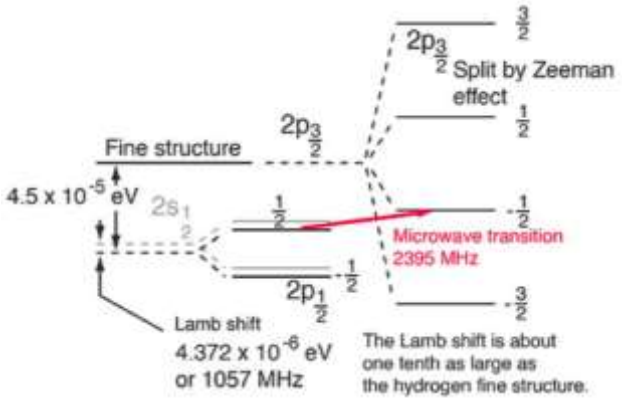
[142] La difficulté expérimentale consiste à annuler toutes les autres forces s'exercant entre les deux plaques et elles sont toutes beaucoup plus importantes que l'effet Casimir, notamment les forces électrostatiques et les forces de van der Waals.

[143] Voir Physicists solve Casimir conundrum par Hamish Johnston, 2012 qui fait référence à Casimir Force and In Situ Surface Potential Measurements on Nanomembranes par Steve Lamoreaux et al, 2012 (6 pages).





Le second provient de **Willis Eugene Lamb** (1913-2008, Américain), Prix Nobel de physique en 1955, qui avait fait sa thèse sous la supervision de Robert Oppenheimer. Le déplacement de Lamb est un écart d'énergie observé entre deux niveaux de structure fine de l'atome d'hydrogène, soit deux niveaux d'énergie très proches[144]. L'effet s'explique par les perturbations apportées par l'énergie du vide sur l'électron dans ces deux niveaux d'énergie voisins, créant la génération spontanée de photons qui sont rapidement absorbés par l'électron.



L'effet a été découvert en 1947 par Willis Eugene Lamb et interprété la même année par **Hans Albrecht Bethe** (1906-2005, Allemand). Il a servi au développement de l'électrodynamique quantique d'après-guerre[145]. La polarisation du vide explique une partie de ce décalage à hauteur de 27 MHz pour un total de 1057 MHz[146]. Le calcul fait intervenir la constante de structure fine α (à peu près 1/137) qui décrit la contribution de l'énergie du vide au moment magnétique anormal de l'électron.

Il existe aussi un effet Casimir dynamique, le **Dynamic Casimir Effect** (DCE) découvert par **Gerald Moore** en 1969. Il génère des paires de particules par le mouvement des miroirs utilisés dans l'expérience de Casimir[147]. Comme pour l'effet Casimir, l'énergie observée est infinitésimale. Pour que l'énergie soit significative, il faudrait que les miroirs se déplacent à des vitesses relativistes, ce qui n'est pas bien pratique. Et il n'y a pas de problème de conservation de l'énergie. On peut produire autant de paires que l'on souhaite de cette façon. L'énergie nécessaire est apportée par le mouvement du miroir. Le vide sert simplement de milieu non-linéaire !

L'interprétation de l'effet Casimir fait encore débat. Certains physiciens l'expliquent par d'autres mécanismes que l'énergie du vide.

---

[144] Voir Willis Eugene Lamb (1913–2008) La passion de la précision par Jean-Christophe Pain, 2007 (3 pages).

[145] Source du schéma et explications associées : The Lamb Shift.

[146] Ce phénomène de polarisation du vide dans l'effet Lamb est décrit dans The Vacuum Polarisation Contribution to the Lamb Shift Using Non-Relativistic Quantum Electrodynamics par Jonas Frafjord, 2016 (61 pages).

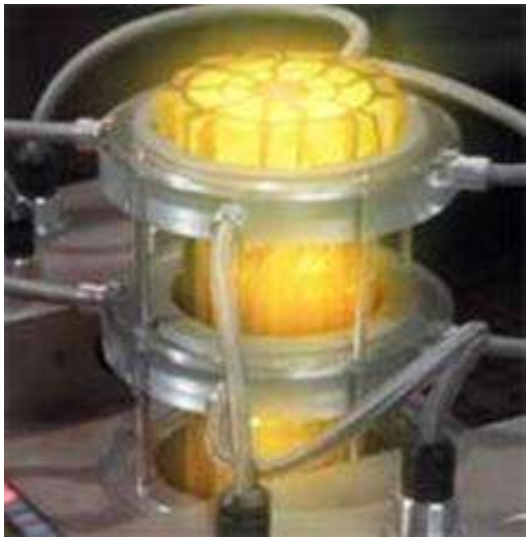
[147] Voir Electro-mechanical Casimir effect par Mikel Sanz, Enrique Solano et al, 2018 (10 pages).

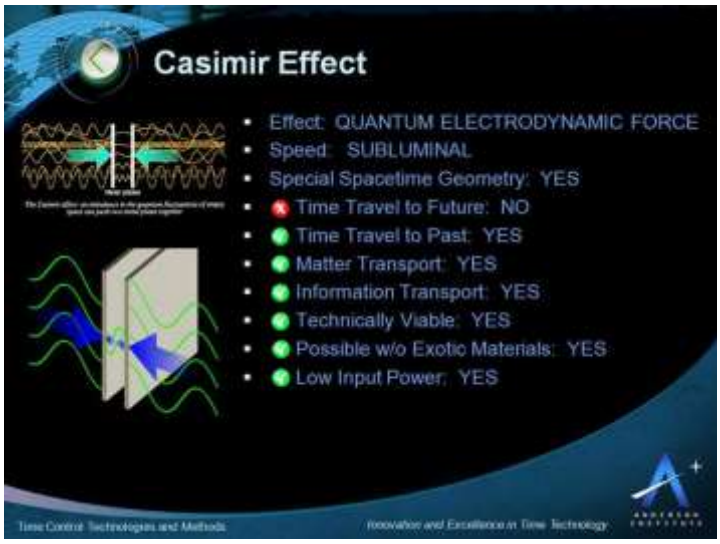
Ils s'appuient notamment sur les forces de **van der Walls** (1837-1923, encore un Hollandais…) qui voient les atomes s'attirer ou se repousser les uns les autres en fonction de leurs distances respectives[148]. Cette force infinitésimale s'exercerait cependant plutôt à l'échelle microscopique tandis que l'effet Casimir opère plutôt à l'échelle macroscopique.

Notons que les physiciens français sont assez actifs dans le domaine, et notamment **Astrid Lambrecht**, actuellement directrice de l'INP du CNRS, l'Institut de Physique qui coiffe les laboratoires de physique du CNRS[149]. L'effet Casimir pourrait avoir un intérêt en métrologie quantique pour créer des capteurs et notamment des NEMS/MEMS.

Ces théories sur l'énergie du vide et l'effet Casimir sont aussi exploitées de manière frauduleuse par les créateurs de soit-disantes machines capables de capter l'énergie du vide, qui ne captent rien du tout en pratique vu que cette énergie est faible et ne peut pas être captée. C'est un peu pour cette raison que j'ai creusé le sujet dans cette édition de l'ebook. Vous avez par exemple un certain **David Lewis Anderson**, à l'origine de l'**Anderson Institute** créé en 1990, qui prétend pouvoir utiliser l'effet Casimir pour voyager dans le passé et pour créer un générateur d'électricité « gratuite »[150].

Dans d'autres cas, l'effet Casimir est exploité de manière scientifique mais "border line" pour imaginer des scénarios qui relèvent de la science fiction comme pour traverser des trous de vers[151].





Théories unificatrices

La quête de la **théorie du tout** occupe bon nombre de physiciens depuis près d'un siècle. Elle vise à unifier l'ensemble des théories de la physique et en particulier, celle de la physique quantique et celles de la relativité. En complément de la QFT ont été développées un très grand nombre de théories explicatives et unificatrices de la physique.

---

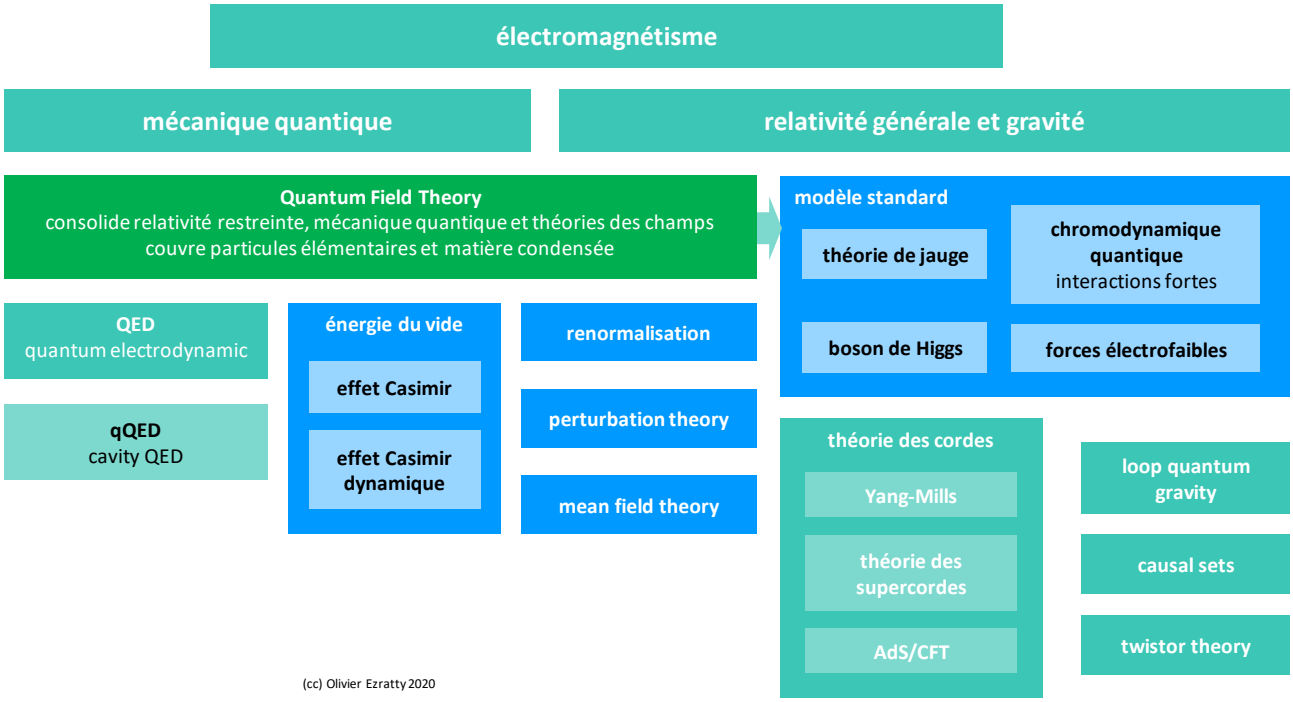
[148] Voir The origin of Casimir effect: Vacuum energy or van der Waals force? par Hrvoje Nikolic, 2018 (41 slides) et l'encore plus sceptique The Casimir-Effect: No Manifestation of Zero-Point Energy par Grold Gründler, 2013 (15 pages) ainsi que All wrong with the Casimir effect par Astrid Karnassnigg, 2014 (3 pages). Voir enfin The Casimir effect: a force from nothing par Astrid Lambrecht, 2007 (5 pages).

[149] Voir The Casimir effect theories and experiments par Romain Guérout, Astrid Lambrecht et Serge Reynaud, LKB, 2010 (28 slides) ainsi que Casimir effect and short-range gravity tests LKB, 2013 (15 slides). Astrid Lambrecht présidait notamment le groupe Casimir RNP qui regroupait des chercheurs du monde entier travaillant sur l'effet Casimir. Le groupe était actif entre 2009 et 2014.

[150] Son site web semble inactif depuis 2012. Voir cette interview radio du gars de 2019 qui défie l'entendement dans son côté baratinesque. Et qui montre comment un interviewer sans background scientifique peut se faire berner par un illuminé parlant sérieusement. Dans Voir Is Time Travel Real?, 2019 et le site de l'Anderson Institute.

[151] Voir One Theory Beyond the Standard Model Could Allow Wormholes that You Could Actually Fly Through - Universe Today par Matt Williams, août 2020 qui fait référence à Humanly traversable wormholes par Juan Maldacena et Alexey Milekhin, août 2020.

Leur arborescence est des plus complexes et aucune théorie n'est considérée aujourd'hui comme aboutie et complète[152]. Je tente un schéma d'organisation de ces différentes théories *ci-dessous*.



- La **chromodynamique quantique** fournit une description de l'interaction forte qui permet de lier les quarks entre eux via les gluons pour former des particules appelés hadrons, qui comprennent les protons et les neutrons que l'on trouve dans les noyaux des atomes.

  Murray Gell-Mann (1929-2019, Américain, prix Nobel de physique en 1969) et Georges Zweig (1935, Russe puis Américain, ancien thésard de Richard Feynman) avaient proposé chacun de leur côté l'existence des quarks en 1963. La chromodynamique quantique est une extension de la théorie quantique des champs élaborée en 1972 par Murray Gell-Mann et Harald Fritzsch.

- Le **modèle standard** décrit l'architecture des particules élémentaires connues et leurs interactions. Il modélise les forces fondamentales électromagnétiques, faibles et fortes. Il ne lui manque que la gravité pour être complet. C'est ce modèle qui prévoyait notamment l'existence des quarks qui sont les particules massives constituant les neutrons et les protons, en plus d'autres particules élémentaires comme le fameux boson de Higgs dont l'existence a été prouvée au LHC du CERN en 2012. L'expression modèle standard date de 1975. Le modèle standard est une théorie dite de jauge du fait des symétries mathématiques qu'elle présente. Ce n'est pas la première du genre car l'électromagnétisme de Maxwell est aussi une théorie de jauge (entre champs magnétiques et électriques). Les particules du modèle standard ne couvrent pas la fameuse matière noire dont on ne connaît pas encore la nature.

- La **théorie des cordes** associe la relativité générale et la mécanique quantique pour proposer une explication quantique de la gravité, appuyant son fonctionnement sur une nouvelle particule sans masse, le graviton. Selon cette théorie, les particules élémentaires ne sont pas ponctuelles, mais de minuscules cordes, ouvertes ou fermées, dont les types de vibrations définissent la nature de la particule. Leur taille est de l'ordre de grandeur de 10^{-35} m, soit l'infinitésimale longueur de Planck. Selon cette théorie, l'Univers serait un ensemble de cordes vibrantes. Le graviton rejoindrait les trois autres forces de la nature intermédiées par des particules sans masse : les ondes électromagnétiques par les photons, les interactions fortes par les gluons qui relient les

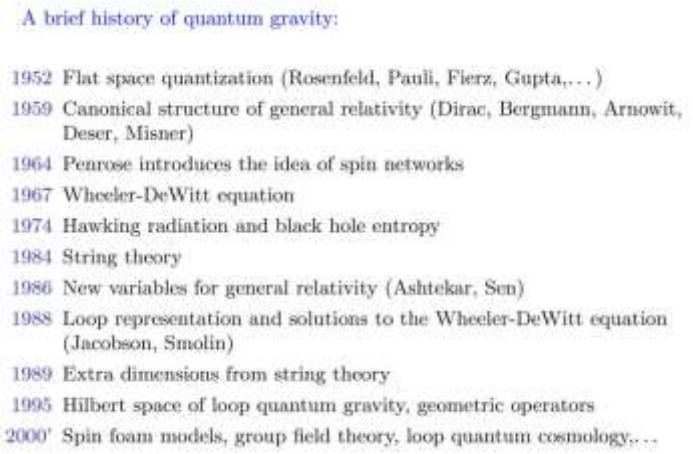
[152] Voir De l'infiniment petit à l'infiniment grand : l'Univers dans tous ses états par Godefroy Kugel, 2011 (26 pages) qui propose un bon exercice de vulgarisation du sujet.

quarks entre eux dans les protons et neutrons et les interactions faibles assurées par les bosons W et Z qui régissent le fonctionnement des noyaux des atomes et notamment la radioactivité[153]. La théorie des cordes couvre essentiellement les bosons de toutes sortes.

- La **théorie des supercordes** est une extension de la théorie des cordes qui ajoute les fermions au modèle de la théorie des codes qui se focalisaient sur les bosons. Elle s'appuie sur la notion de supersymétrie qui étend le modèle standard en faisant correspondre à chaque type de boson un type de fermion. La théorie a pris forme en 1943 avec Werner Heisenberg sous la forme de la théorie S-matrix puis pris son essort à partir de 1984. Elle utilise 10 dimensions pour décrire la physique, bien au-delà des quatre dimensions classiques (trois pour la position et une pour le temps). Elle utilise aussi la notion de « branes » qui décrit des particules ponctuelles dans ces espaces multidimensionnels. Cette théorie n'est pas unique pour autant puisqu'il en existe cinq variantes, que certains essayent d'unifier dans la **M-theory** qui s'appuie sur 11 dimensions. C'est un puits sans fond !

- La théorie de la **gravitation quantique à boucles** (loop quantum gravity) concurrence la théorie des supercordes pour expliquer la gravité. Elle discrétise les effets de la gravité en présentant l'espace comme étant une structure maillée avec des aires et volumes d'espace quantifiés, et de quantas de champ gravitationnel reliés entre eux par des liens caractérisés par un spin[154].

  Pour cette théorie créée en 2001, l'Univers serait une gigantesque mousse de spin (spin foam). Ses principaux promoteurs sont **Carlo Rovelli** (du Centre de Physique théorique de Marseille) et **Lee Smolin** (de l'Institut Perimeter pour la physique théorique de Waterloo[155]). Les germes de la théorie datent de 1952, avec plein d'étapes intermédiaires[156]. La théorie est surtout un modèle mathématique et topologique. Elle ne semble pas formuler de méthode expérimentale permettant de la valider.


A brief history of quantum gravity:

1952 Flat space quantization (Rosenfeld, Pauli, Fierz, Gupta,...)
1959 Canonical structure of general relativity (Dirac, Bergmann, Arnowit, Deser, Misner)
1964 Penrose introduces the idea of spin networks
1967 Wheeler-DeWitt equation
1974 Hawking radiation and black hole entropy
1984 String theory
1986 New variables for general relativity (Ashtekar, Sen)
1988 Loop representation and solutions to the Wheeler-DeWitt equation (Jacobson, Smolin)
1989 Extra dimensions from string theory
1995 Hilbert space of loop quantum gravity, geometric operators
2000' Spin foam models, group field theory, loop quantum cosmology,...

Je n'ai cité ici que les principales théories car elles sont bien plus nombreuses que cela. Des amateurs plus ou moins éclairés s'essayent d'ailleurs aussi à l'exercice de la création d'une théorie du tout, avec plus ou moins de bonheur et sans échos de la communauté scientifique[157].

---

[153] Les bosons W transforment les quarks up en quarks down et les neutrinos en électrons. Les quarks up et down sont les deux types de quarks. Leur proportion 2 up + 1 down pour les protons et 1 up + 2 down pour les neutrons. Un quark a une taille voisine de celle d'un électron, de l'ordre de 10^{-16} cm. De son côté, la radioactivité émet des rayons alpha via les forces fortes, des particules comprenant deux protons et deux neutrons (atome d'hélium 4 sans électron), les rayons beta générés par les forces faibles qui sont des électrons ou des positrons et enfin, des rayons gamma qui sont des photons de très haut niveau d'énergie.

[154] En ce sens, elle rappelle la récente théorie du tout bâtie par Stephen Wolfram publiée au printemps 2020.

[155] Voir Lee Smolin Public Lecture Special: Einstein's Unfinished Revolution, 2019 (1h13mn) où il décrit les lacunes de la mécanique quantique.

[156] Source de la chronologie : The philosophy behind loop quantum gravity par Marc Geiller, 2001 (65 slides).

[157] Voir par exemple le site Unified Theory Research Team qui annonce publier en septembre 2020 un modèle de théorie du tout dénommé **MME** pour Model of Material and Energy. Le site prétend que son modèle qui est présenté comme une approche algorithmique permet de tout expliquer, du fonctionnement de toutes les particules jusqu'aux briques de la vie. L'équipe porteuse de ce projet comprend deux Français : Pierre Lepeltier et Frédéric Lepeltier. Le premier, Normalien littéraire, se présente comme étant le CEO de l'Unified Theory Research Team depuis 32 ans. Autant dire que ce genre de modèle ne risque pas de faire l'unanimité chez les physiciens.

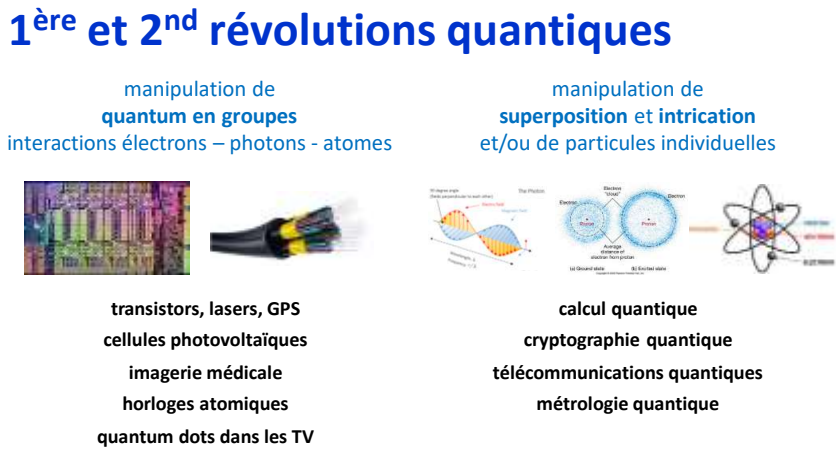
Applications quantiques

La physique quantique est mise en œuvre depuis l'après-guerre dans quasiment tous les produits courant de l'électronique, de l'informatique et des télécommunications.

Cela correspond à la **première révolution quantique**. On y retrouve les transistors, inventés en 1947, qui utilisent l'effet tunnel et sont à la base de toute l'électronique et de l'informatique d'aujourd'hui, les cellules photovoltaïques qui s'appuient sur l'effet photoélectrique, les lasers qui exploitent aussi l'interaction lumière matière et sont utilisés dans un très grand nombre d'applications.

Nombre de solutions d'imagerie médicale s'appuient sur des effets quantiques divers, notamment l'imagerie à résonance magnétique.

Le GPS s'appuie sur des horloges atomiques. Les quantum dots des écrans LCD utilisent aussi des variantes de l'effet photoélectrique. La liste est longue et nous n'allons pas détailler tous ces usages !



La **seconde révolution quantique** couvre les usages de la physique quantique qui combinent tout ou partie de la capacité à contrôler des quantums individuels (atomes, électrons, photons), à utiliser l'intrication ou la superposition quantiques. On doit les appellations de première et seconde révolution quantiques à Alain Aspect, Jonathan Dowling et Gerard Milburn en 2003[158]. Le premier et les deux suivants l'ont créée simultanément et de manière indépendante. Aux USA, la paternité revient donc aux derniers tandis qu'en France, elle est attribuée au premier !

La définition de la seconde est un peu à géométrie variable selon les auteurs. Elle couvre aussi bien diverses applications récentes de la physique quantique que celles de l'informatique quantique qui intègrent le calcul, les télécommunications et la cryptographie quantiques.

Cet ebook est très focalisé sur les calculateurs quantiques mais ce n'est pas la seule application nouvelle de la seconde révolution quantique.

On compte au moins trois autres grands domaines dans ce vaste secteur :

- La **cryptographie quantique** qui est un moyen de diffusion de clés quantiques inviolables grâce au principe de l'intrication entre photons, et qui repose soit sur des communications par fibre optique, soit en liaison spatiale avec des satellites comme le font les Chinois avec le satellite Micius depuis 2017. Nous traitons du sujet dans une partie dédiée à partir de la page 473. Il faut la distinguer de la **cryptographie post-quantique** qui est destinée à remplacer les solutions actuelles de cryptographie pour les rendre résistantes aux attaques réalisées avec l'algorithme de Shor tournant dans des ordinateurs quantiques. Nous nous y intéresserons à partir de la page 483.

[158] Voir Speakable and unspeakable in quantum mechanics par John S. Bell, édition de juin 2004 (289 pages) qui contient une préface d'Alain Aspect sur la seconde révolution quantique, datée de février 2003, pages 18 à 40. On retrouve l'expression dans Quantum technology: the second quantum revolution par Jonathan P. Dowling et Gerard J. Milburn, juin 2003 (20 pages) ainsi que Quantum Technology : the Second Quantum Revolution par Jonathan Dowling, 2011 (60 pages). Les écrits de Dowling font un catalogue très large « à la Prévert » de technologies quantiques diverses attribuables à cette seconde révolution quantique. L'ouvrage The Second Quantum Revolution: From Entanglement to Quantum Computing and Other Super-Technologies par Lars Jaeger, 2018 (331 pages) s'étend de manière plus large sur les différentes facettes de la seconde révolution quantique.

- Les **télécommunications quantiques** qui permettent, grâce à l'intrication quantique de photons ayant un passé commun, de communiquer à distance et instantanément l'état de quantums. C'est un cas plus général que la cryptographie quantique qui en est un cas particulier. C'est un domaine en devenir car pour l'instant, on peut certes envoyer une information très rapidement, mais pas l'exploiter directement.

  En particulier, l'information a beau être transmise instantanément, donc plus vite que la lumière, on ne peut pas pour autant exploiter cette bizarrerie dans la transmission d'informations classiques[159]. Cela peut cependant servir pour distribuer des traitements quantiques sur plusieurs processeurs quantiques et notamment pour le « blind computing » que nous évoquons aussi à différents endroits dans cet ebook.

- La **métrologie quantique**, qui permet de mesurer des ordres de grandeur de l'infiniment petit avec une très grande précision. C'est un vaste domaine scientifique qui fait l'objet de nombreux travaux de recherche et à la commercialisation de solutions industrielles. Il comprend les horloges atomiques ultra précises[160], les accéléromètres et gyromètres à atomes froids qui utilisent de l'interférométrie atomique et les magnétomètres à base de cavités de diamants comme ceux de Thales.

  Table 1. Quantum Metrology and Sensing Technologies

Technology	Technological Readiness*	Potential Market
Measurement		
Atomic clocks	Commercial	$50–$500 million
Meters for voltage, current, and resistance	Commercial	—
Sensors		
Gravimeters and other atomic interferometers	Commercial	< $50 million
Quantum inertial motion units	Medium-term	$50–$500 million
Atomic magnetometers	Commercial	$50–$500 million
Magnetoencephalography	Commercial	$50–$500 million
Quantum electron microscopes	Medium-term	$50–$500 million
Quantum-assisted nuclear spin imaging	Long-term	< $50 million
Signal measurement	Medium-term	—

  Sources: European Commission (2017) United States Air Force Scientific Advisory Board 2015, interviews

  Il y a aussi les gravimètres qui en sont une variante pour mesurer la gravité avec précision, que fabrique notamment le Français Muquans qui est basé à Bordeaux, et divers systèmes avancés d'imagerie médicale[161]. Ce sont des marchés de taille modeste. Une rubrique dédiée de cet ebook est consacrée à la métrologie à partir de la page 506.

La quantique ou le quantique ?

Vous avez peut-être entendu Emmanuel Macron ou ... Julien Bobroff parler de « la quantique » alors que la majorité des chercheurs et entrepreneurs que je connais parlent « du quantique » en général. Quelle expression est donc la bonne ?

Les premiers féminisent « la quantique » car c'est une expression diminutive de « la physique quantique » et de « la mécanique quantique », qui pourrait même s'appliquer aux « technologies quantiques », à « l'informatique quantique » et à « la cryptographie quantique ». Les conjugaisons courantes au masculin sont « l'ordinateur quantique » et « le calcul quantique ». Nous avons aussi « Le Lab Quantique » créé en 2020 par Quantonation et Bpifrance.

---

[159] Mais… « *Les états intriqués ne peuvent pas être utilisés pour communiquer d'un point à un autre de l'espace-temps plus vite que la lumière. En effet, les états de ces deux particules sont seulement coordonnés et ne permettent pas de transmettre une information : le résultat de la mesure relatif à la première particule est toujours aléatoire. Ceci est valable dans le cas des états intriqués comme dans le cas des états non-intriqués. La modification de l'état de l'autre particule, pour instantanée qu'elle soit, conduit à un résultat tout aussi aléatoire. Les corrélations entre les deux mesures ne pourront être détectées qu'une fois les résultats comparés, ce qui implique nécessairement un échange d'information classique, respectueux de la relativité. La mécanique quantique respecte ainsi le principe de causalité* ». Source : https://fr.wikipedia.org/wiki/Intrication_quantique.

[160] Voir par exemple ces travaux du NIST sur une horloge atomique à base de rubidium, l'élément le plus fréquemment utilisé dans les horloges atomiques. NIST Team Demonstrates Heart Of Next-Generation Chip-Scale Atomic Clock, mai 2019.

[161] Voir Quantum camera snaps objects it cannot 'see', par Belle Dume, mai 2018. C'est une variante de Diffraction Free Light Source for Ghost Imaging of Objects Viewed Through Obscuring Media par Ronald Meyers, 2010 (22 pages). Yanhua Shih (Université de Maryland) US Army Research Laboratory, travaille depuis 2005 sur le sujet. Quantum Imaging de Yanhua Shih, 2007 (25 pages). Quantum Imaging – UMBC (47 slides).

Est-ce à dire que l'ordinateur est plus important que l'informatique, les technologies et la cryptographie ? Google Count nous répond : ordinateur quantique (137 000 pages), informatique quantique (195 000 pages), cryptographie quantique (29 600 pages) et technologies quantiques (39 500). Et il retourne 17 400 résultats pour « la quantique » et 37 100 pour « le quantique ». Bref, numériquement parlant, ce débat n'est pas tranché radicalement ! On peut aussi attribuer la masculinisation du terme à l'homophonique « cantique » intégré dans la sempiternelle expression « Le cantique des quantiques » mais c'est un peu léger.

Alors, on se lance dans une écriture inclusive sauce « le/la quantique » ? En fait, « quantique » est un adjectif qualificatif non genré associable aussi bien à des termes féminins que masculins. Par exemple : une chocolatine quantique ou un pain au chocolat quantique :). Donc, vous faites comme vous voulez en fonction des circonstances.

Les anglophones n'ont pas ce souci. C'est « quantum *placeholder* », sans genre, et on n'en parle plus !

Autre variante d'argutie : doit-on parler de « physique quantique » ou de « mécanique quantique » ? Vous avez quatre heures... :) !

Qubits

On peut comprendre le fonctionnement d'un ordinateur quantique sans trop se plonger dans la mécanique quantique au-delà de la compréhension de ses mécanismes de base, vus dans la partie précédente, et surtout celui de l'intrication. Par contre, il faut se plonger un peu dans quelques éléments de mathématiques, d'algèbre linéaire et de trigonométrie, ce que nous allons commencer à faire ici.

Le premier élément de base d'un ordinateur quantique est l'inévitable qubit. Vous avez certainement déjà entendu parler de cet objet mystérieux capable d'être simultanément dans la valeur 0 et 1. Les explications courantes s'arrêtent le plus souvent là et vous tombez immédiatement dans l'expectative, vous demandant comment cela peut ensuite bien fonctionner. Qu'est-ce qui rentre et qu'est-ce qui sort d'un ordinateur quantique ? Comment on le programme ? Comment on l'alimente en données ?

Nous allons donc commencer ici par expliquer le fonctionnement logique, mathématique et matériel de ces qubits[162]. Dans la partie suivante, nous irons plus loin en décrivant tour à tour les registres, les portes, l'organisation et l'architecture complète d'un ordinateur quantique en nous appuyant sur l'exemple courant des ordinateurs quantiques à qubits supraconducteurs. A chaque fois, lorsque nécessaire, nous ferons le parallèle avec les ordinateurs traditionnels.

Pour pouvoir suivre cette partie, il faut connaître quelques basiques mathématiques : la trigonométrie, les vecteurs et matrices et avoir déjà entendu parler des nombres complexes qui utilisent le fameux nombre imaginaire i dont le carré vaut -1[163].

Principe des qubits

Les qubits sont les éléments de manipulation de base de l'information dans les ordinateurs quantiques. Ils s'opposent aux bits de l'informatique traditionnelle. Avec eux, on passe d'un monde déterministe à un monde probabiliste.

Dans l'informatique classique, les bits correspondent à des charges électriques circulantes qui traduisent le passage ou l'absence d'un courant électrique. Un bit est de valeur 1 si le courant passe soit de 0 si le courant ne passe pas. La lecture d'un bit donne 1 ou 0.

	bits : 0 ou 1	**qubits : 0 et 1**
états	2 états possibles exclusifs	2 états possibles simultanés
initialisation	0 ou 1	0
représentation interne	0 ou 1	vecteur à deux dimensions
dimensionnalité interne	1 binary digit	2 nombres flottants
modifications	portes logiques	portes quantiques
lecture	0 ou 1, déterministe	0 ou 1, probabiliste

Elle est déterministe, à savoir que si l'on répète l'opération de lecture plusieurs fois, ou l'opération de lecture après une réédition du calcul, on obtiendra normalement le même résultat.

C'est vrai aussi bien pour le stockage de l'information que pour son transport et pour les traitements dans des processeurs. Ceci est valable modulo les erreurs qui peuvent intervenir dans le parcours. Celles-ci interviennent le plus souvent au niveau de la mémoire et sont corrigées via des systèmes… de correction d'erreurs utilisant de la redondance.

---

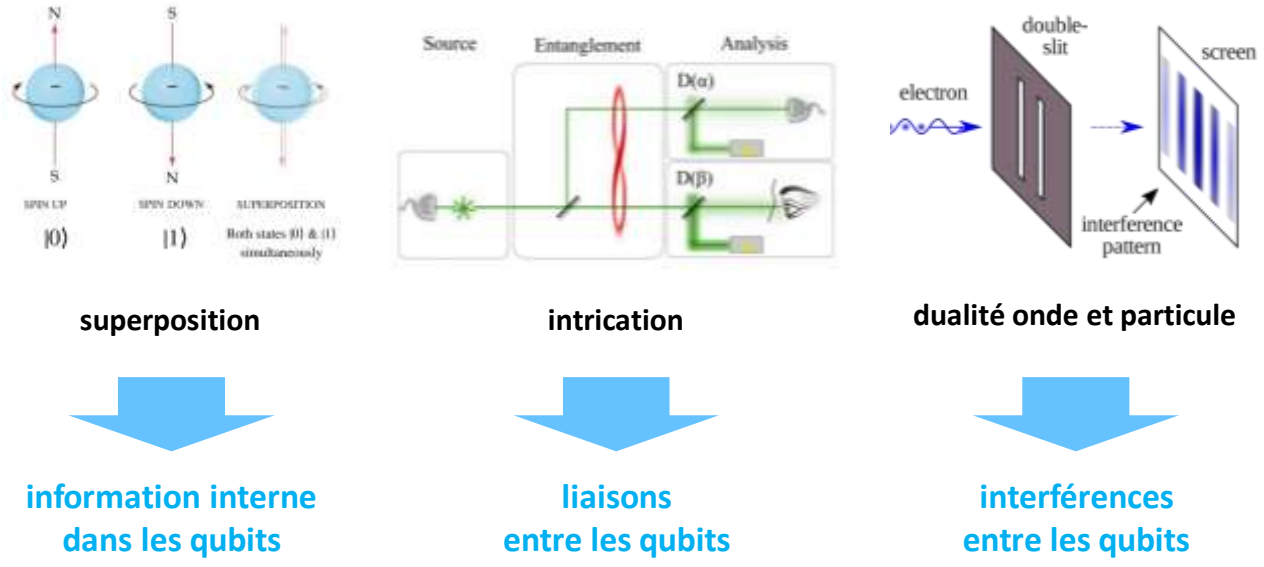
[162] L'appellation qubit, fusion de quantique et bit, est apparue en 1995 dans Quantum coding de Benjamin Schumacher, avril 1995 (34 pages).

[163] Les nombres complexes ont été créés par le polymathe Girolamo Cardano (1501-1576, Italien) et le mathématicien algébriste Raffaele Bombelli (1526-1572, Italien) entre 1545 et 1569. Les nombres complexes servaient notamment à résoudre des équations polynomiales associant des cubes et des carrés qui occupaient les mathématiciens italiens depuis la fin du quinzième siècle. Voir A Short History of Complex Numbers par Orlando Merino, 2006 (5 pages).

Dans un qubit, tout change ! Si les qubits sont généralement initialisés à |0⟩, les opérations portant dessus vont généralement les amener à avoir un état de superposition entre |0⟩ et |1⟩. Ces états correspondent à l'état de base ("ground state") et à l'état excité ("excited state") d'un système quantique à deux états possibles. Ces qubits peuvent donc être à la fois à la valeur |0⟩ et |1⟩, et dans une proportion qui est variable et qui correspond à la notion de superposition d'états évoquée dans la partie précédente sur les fondements de la mécanique quantique. A la fin des calculs, lorsque l'on lit la valeur d'un qubit, on retrouve |0⟩ ou |1⟩. La richesse des valeurs du qubits se manifeste donc uniquement pendant les calculs et non pas à leur initialisation où lors de leur lecture à la fin des calculs. C'est un concept que vous ne comprendrez complètement que lorsque nous aurons décrit quelques algorithmes quantiques lors d'une partie suivante de cette série.

Voici en résumé les trois principes de base les plus importants sur les huit de la partie précédente qui sont utilisés dans les qubits :

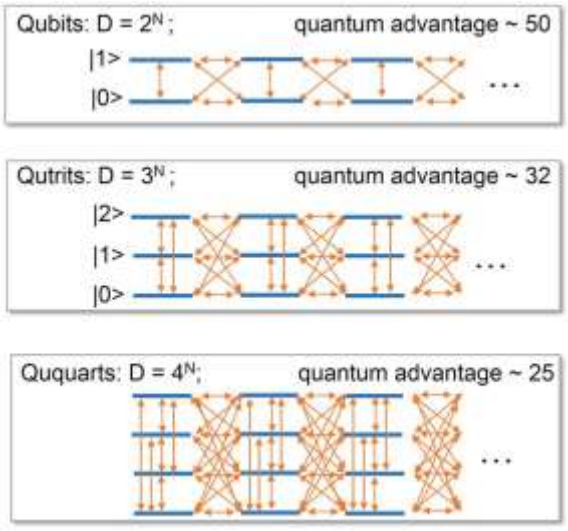
- La **superposition** permet d'avoir des qubits qui sont à la fois dans un état |0⟩ et |1⟩ et nous verrons plus tard dans quelle proportion et comment on la représente mathématiquement. C'est elle qui apporte la puissance de représentation de données dite exponentielle du calcul quantique.
- L'**intrication** permet de relier entre eux les qubits pour les synchroniser, souvent de manière conditionnelle, mais sans pouvoir en lire leur contenu ni les modifier de manière indépendante ni les copier. Elle est mise en œuvre dans les ordinateurs quantiques à portes universelles par le biais des portes quantiques à deux qubits ou plus. Elle permet la capacité logique du calcul quantique.
- La **dualité onde-particule** permet d'interagir dans certains cas avec les qubits ou de faire interagir les qubits entre eux par interférences dans le cadre d'algorithmes quantiques. C'est une des manières de générer des résultats dans des algorithmes quantiques. Elle permet de faire ressortir un résultat parmi plein de valeurs superposées dans les états de registres de qubits.



Ici, nous allons d'abord creuser le modèle mathématique de représentation des qubits et comprendre comment on peut se le représenter physiquement et mentalement.

Nous ferons alors un tour des différents types de qubits physiques. Les modèles mathématiques de représentation des qubits ne dépendent pas de leur type physique. Seules les caractéristiques de l'ordinateur sont affectées comme le taux d'erreur et la nature des portes quantiques physiques de base dites "universelles" agissant sur les qubits sachant que toutes les portes quantiques sont exécutables sur les ordinateurs quantiques.

Les qubits ne sont pas les seules manières de gérer de l'information quantique. Des ordinateurs quantiques peuvent aussi être construits à partir de **qutrits** (trois états quantiques possibles), de **ququarts** (quatre états possibles) et plus génériquement, de **qudits** (d = nombre d'états quantiques possibles)[164]. Ils permettent d'obtenir un avantage quantique avec un nombre d'objets quantiques plus réduit qu'avec des qubits. Des laboratoires de recherche en sont à l'origine, comme Berkeley qui travaille sur des qubits supraconducteurs à plus de deux niveaux[165]. D'autres font cela avec des photons en gérant plusieurs de leurs propriétés. Ils ne sont pas cependant courants, ne serait-ce que parce qu'ils modifient les modèles de programmation.



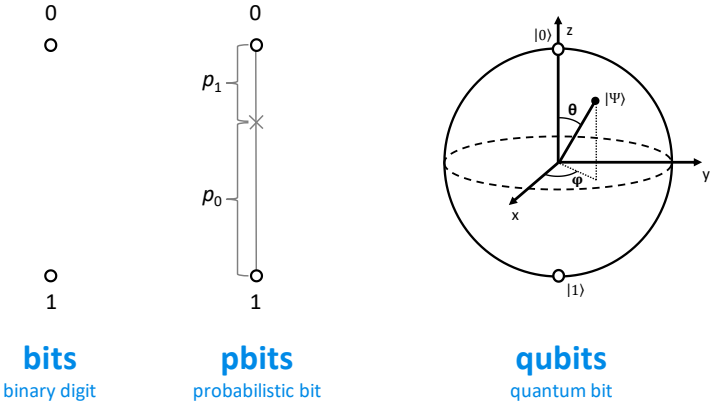
Cela reste cependant des objets de recherche théorique et de laboratoires. Aucun projet d'ordinateur quantique commercial basé sur ces types d'objets quantiques semble être sur les rails. Par ailleurs, ils auraient un impact sur la conception d'algorithmes quantique. La plupart des algorithmes sont conçus pour des ordinateurs quantiques à portes universelles à base de qubits. Ceci étant, des compilateurs pourraient probablement transformer automatiquement des portes quantiques classiques en portes adaptées à ce type de qubits.

Sphère de Bloch

Dans un modèle probabiliste classique, un pbit ou bit probabiliste aurait une probabilité p d'avoir la valeur 0 et 1-p d'avoir la valeur 1[166]. Ce serait un modèle probabiliste linéaire.

Dans un qubit, c'est bien différent ! Le modèle de représentation mathématique de l'état d'un qubit s'appuie sur des nombres complexes et sur la métaphore géométrique de la fameuse **sphère de Bloch**.

Ce modèle est lié à la représentation de l'état d'un qubit ou de tout quantum à deux états par un vecteur à deux dimensions dont la longueur, dite "norme", est toujours de 1.

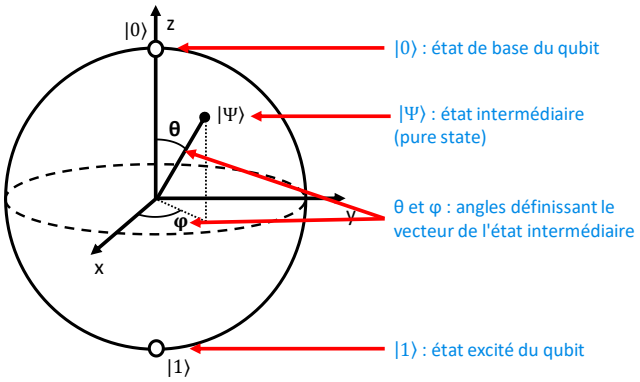


[164] Voir par exemple Ultracold polar molecules as qudits par JM Hutson et al, 2020 qui traite de qudits à base de molécules diatomiques fluor-calcium et rubidium-césium qui permettent de gérer quatre niveaux quantique par molécule. Cela réduit le nombre de qubits nécessaires de log2(d), d étant le nombre de niveaux d'états des qudits.

[165] Voir Quantum Simulations with Superconducting Qubits par Irfan Siddiqi, 2019 (66 slides) qui est la source de l'illustration.

[166] Les modèles probabilistes linéaires sont utilisés dans les processeurs probabilistes évoqués dans un petit chapitre dédié de cet ebook.

Ce vecteur a la particularité d'être défini par deux nombres complexes α et β selon la formule déjà vue $|\Psi\rangle=\alpha|0\rangle+\beta|1\rangle$. Dans la sphère de Bloch, l'état $|0\rangle$ d'un quantum à deux états est figuré par la position d'un vecteur de longueur 1 allant du centre de la sphère vers le pôle Nord de la sphère et l'état $|1\rangle$ est un vecteur allant du centre de la sphère à son pôle Sud.



Les états intermédiaires sont représentés par des vecteurs partant du centre de la sphère qui sont toujours de longueur 1 avec un angle θ par rapport à la verticale z et un angle φ par rapport à l'axe x situé allant du centre de la sphère à son équateur et autour de l'axe z. Histoire de simplifier les choses, les états $|0\rangle$ et $|1\rangle$ qui sont opposés dans la sphère de Bloch sont dits "orthogonaux" alors qu'ils sont opposés dans la sphère. Nous allons rapidement comprendre pourquoi

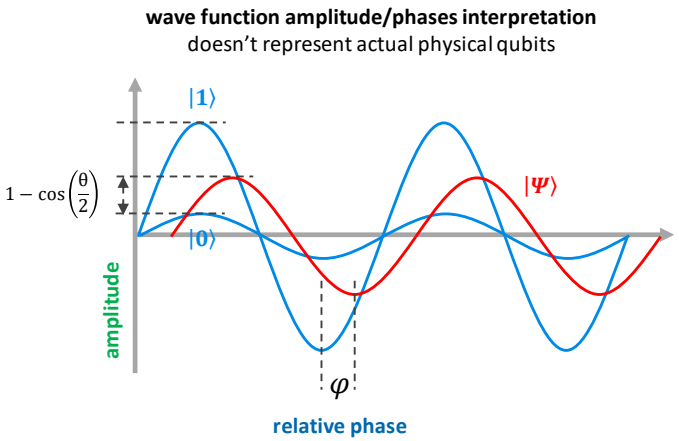
Règle de Max Born

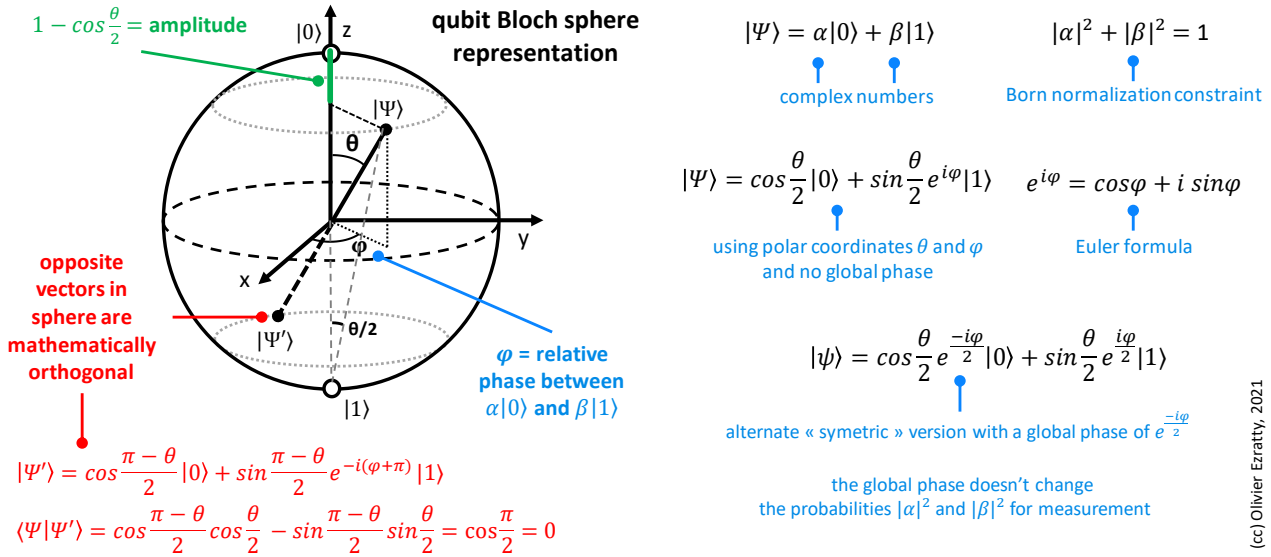
Les équations décrivant l'état d'un qubit indiquent que celui-ci est la superposition de l'état $|0\rangle$ et de l'état $|1\rangle$. Dans les équations, α est un nombre complexe dont le carré décrit la probabilité d'obtenir l'état $|0\rangle$ et β est un nombre complexe dont le carré décrit celle d'avoir l'état $|1\rangle$. La somme des probabilités des deux états doit donner 1. Ce n'est effectivement pas $\alpha+\beta$ mais $\alpha^2+\beta^2$ qui donnent 1. Pourquoi donc ?

Ce modèle probabiliste a été élaboré par **Max Born** en 1926. Son application aux qubits en est une version simplifiée. Il donne au carré du module de la fonction d'onde d'un quantum la signification d'une densité de probabilité de présence d'une particule élémentaire. C'est lié au fait que l'état $|0\rangle$ et l'état $|1\rangle$ correspondent non pas à une position précise d'une particule mais sont représentés par la fonction d'onde de **Schrödinger** qui décrit la distribution probabiliste de l'état du quantum dans le temps et dans l'espace. Elle est ici appliquée dans l'espace.

L'état d'un qubit est représenté par un vecteur à deux dimensions dans un espace dit de Hilbert, ce qui est une information bien plus riche qu'un 0 ou un 1 d'un simple bit ou même qu'une probabilité linéaire entre 0 et 1. Ce vecteur à deux dimensions comprend les deux composantes complexes α et β que nous venons de définir.

Par convention, la représentation d'un qubit est indépendante de sa phase globale qui est supprimée de l'équation pour faire en sorte que α soir un nombre réel. Le passage de la fonction d'onde de Schrödinger à la représentation α/β du qubit avec ces nombres complexes est lié à la nature ondulatoire des quanta. Après suppression de la phase globale (expliquée dans le schéma *ci-dessous*), la partie complexe β intègre la phase de l'onde de l'objet quantique du qubit tandis que sa partie réelle α comprend un nombre réel lié à son amplitude.





Le paradoxe à bien comprendre est le suivant : comme il existe un nombre infini de positions dans la sphère de Bloch, un qubit pourrait stocker en théorie une quantité importante d'information, en tout cas, bien plus qu'un bit. Malheureusement, comme à la lecture, on ne peut obtenir qu'un 0 ou un 1 classiques, ou une moyenne des deux en répétant la lecture plusieurs fois après le même calcul et que celui comprend des erreurs incontournables, on ne peut pas récupérer plus d'information qu'un bit. Toujours à cause de ce sacré théorème de Holevo [167]!

Trigonométrie dans la sphère de Bloch

Second mystère à résoudre, pourquoi donc l'angle θ est-il divisé par deux dans les équations décrivant un état quantique dans la sphère de Bloch dans les calculs de sinus et de cosinus des formules donnant α et β ? Cela vient de ce que l'état |1⟩ est placé en bas de la sphère pour que l'espace des états du qubit occupe toute la sphère et pas seulement son hémisphère nord.

J'ai dû compiler plusieurs sources d'informations pour comprendre cela et l'expliquer avec le schéma *ci-dessous*[168] ! Vous n'êtes pas obligés d'y passer du temps.

Comme l'état |1⟩ est mathématiquement orthogonal par construction à l'état |0⟩, leur angle "mathématique" calculé doit être de 90° (π/2). Or, l'angle θ est du double de cet angle dans la sphère car il est de π (pour mémoire π*2 = circonférence de 360°).

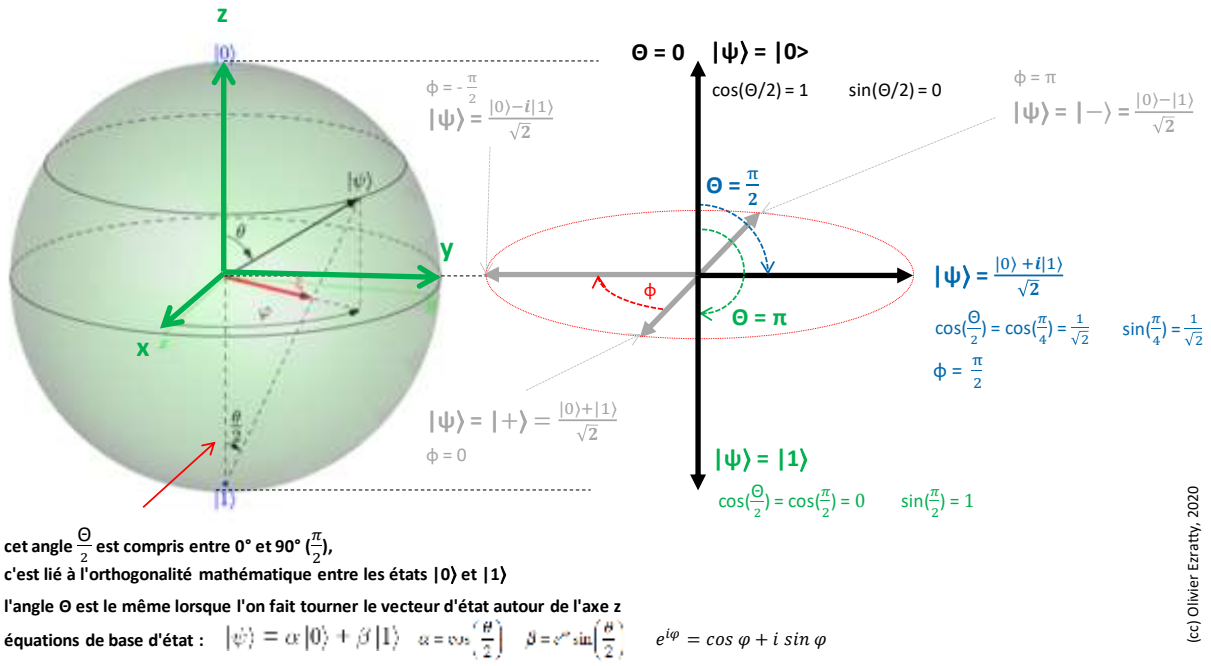
Donc, on divise θ par deux pour relier la représentation géométrique dans la sphère avec la représentation mathématique de l'état du qubit, et surtout, pour permettre un étalement de tous les états d'un qubits sur l'ensemble de la sphère. Dans cette représentation, α est un nombre réel car c'est un simple cosinus lorsque la phase globale du qubit a été supprimée par factorisation de α et β.

[167] Pour en savoir plus et avec une meilleure exactitude scientifique, vous pouvez consulter la fiche Wikipedia de la fonction d'onde ainsi que celle de la probabilité d'amplitude. On trouve d'autres explications dans l'exemple des niveaux d'orbites d'électrons dans l'atome d'hydrogène dans Quantum Mechanics and the hydrogen atom (19 slides). L'interprétation physique de la règle statistique de Max Born reste en tout cas ouverte si l'on en juge par ce papier de juin 2018 d'Arkady Bolotin, Quantum probabilities and the Born rule in the intuitionistic interpretation of quantum mechanics (14 pages).

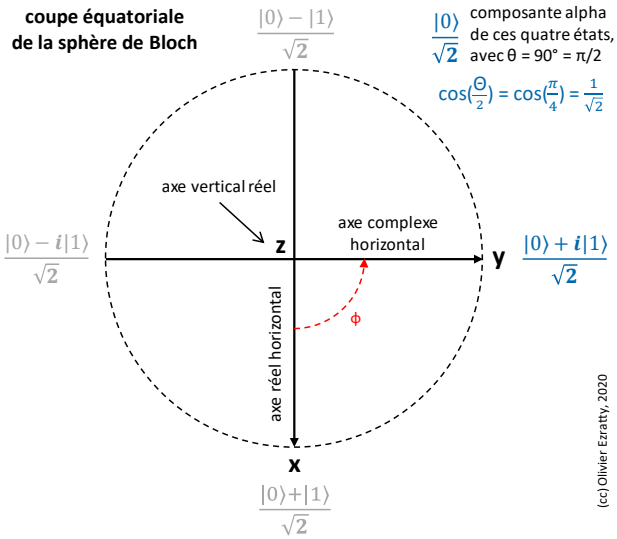
[168] C'est décrypté dans The Bloch Sphere de Ian Glendinning, 2005 (33 slides) qui explique cela par l'orthogonalité mathématique des deux états |0⟩ et |1⟩ qui sont pourtant opposés dans la sphère de Bloch. C'est encore mieux expliqué dans Why is theta/2 used for a Bloch sphere instead of theta ? qui a définitivement éclaircit ce mystère pour moi.

Dans ce cas, seul β est un nombre complexe. Il l'est dès lors que le qubit n'est pas dans le plan croisant l'axe x (θ = 0) et l'axe z (φ= 0) de la sphère de Bloch. Ce nombre complexe associe une partie réelle pour la direction z et une partie complexe pour les dimensions x et y qui sont orthogonales à z. Sachant qu'après application d'une rotation autour de l'axe z, on va en général réintroduire un nombre complexe dans le α du qubit transformé, que l'on ne factorise pas forcément pour retirer la phase globale du qubit.

La représentation sur la sphère de Bloch est un modèle mathématique probabiliste. Elle ne correspond pas à un modèle physique, comme l'angle de polarisation d'un photon ou le spin d'un électron, malgré les similitudes.



Lorsque le vecteur d'état du qubit est horizontal dans la sphère, c'est-à-dire qu'il va jusqu'à son équateur, nous sommes dans un état superposant l'état |0⟩ et l'état |1⟩ à égalité, mais avec une phase relative entre |0⟩ et |1⟩ qui est liée à l'angle horizontal du vecteur φ par rapport à l'axe z comme dans le schéma ci-dessous. Cette information riche d'un qubit est modifiée ensuite par des portes quantiques.



Une porte quantique qui s'applique à un seul qubit, applique une rotation à l'état du qubit dans sa sphère de Bloch. Cette rotation est appliquée via une matrice de nombres complexes 2x2, dite matrice orthogonale de déterminant 1.

De déterminant 1 car elle ne va pas modifier la longueur du vecteur après son application. Cette longueur restera toujours de 1. Nous examinerons la diversité de ces portes quantiques dans la partie suivante de cette série.

En règle générale, les portes quantiques ne génèrent pas toutes les positions de vecteurs dans la sphère de Bloch. Ce sont souvent des demi ou quarts de tours. Les points de la sphère les plus souvent utilisés sont les points cardinaux : le 0, le 1, puis les quatre points correspondant à la superposition 0 et 1 qui sont sur l'équateur de la sphère. Mais pour obtenir toute la puissance de calcul quantique, on a besoin de faire des tours plus petits que des quarts de tours, avec les portes R à phase variable, que nous verrons plus loin.

Autre point clés : des vecteurs opposés de la sphère de Bloch sont toujours mathématiquement orthogonaux. C'est ainsi le cas des états $|+\rangle$ et $|-\rangle$ situés sur l'équateur de la sphère.

On doit finalement cette sphère de Bloch à trois scientifiques : **Erwin Schrödinger** pour sa fonction d'onde de 1926, **Max Born** pour son modèle probabiliste associé, créé la même année et à **Felix Bloch** (1903-1983, Suisse) qui a représenté l'état d'un quantum à deux niveaux sur la sphère en 1946. En optique et pour décrire les différents types de polarisation d'un photon (horizontale/verticale, circulaire droite et gauche, elliptique), la sphère de Bloch s'appelle la sphère de Poincaré, du nom du mathématicien français **Henri Poincaré** (1854-1912)[169].

Cycle de vie d'un qubit

Une manière de comprendre le fonctionnement d'un ordinateur quantique à portes universelles est de suivre la vie d'un qubit lors des traitements. C'est un objet mathématique un peu particulier :

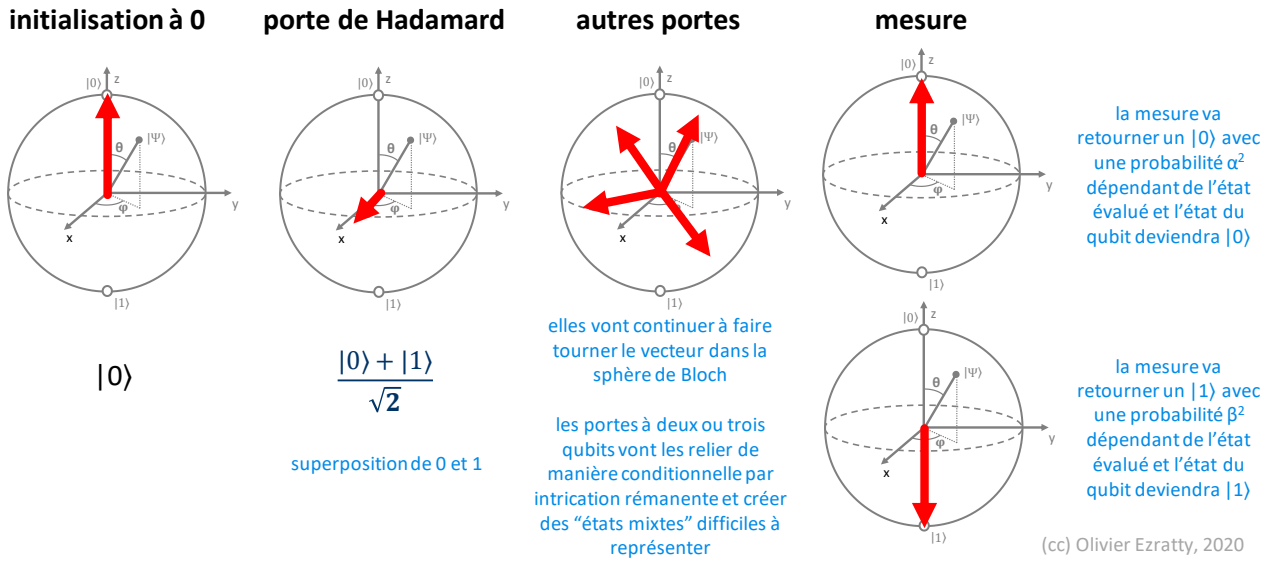
- On l'**initialise** toujours à $|0\rangle$, correspondant à l'état de base, en général au repos, du qubit. Cette initialisation consomme d'ailleurs de l'énergie.
- On le **modifie** ensuite de manière programmatique avec des portes quantiques pour lui faire prendre des valeurs qui sont des vecteurs dans la sphère de Bloch. La porte de Hadamard est l'une des plus courantes et elle créé un état de superposition entre un $|0\rangle$ et un $|1\rangle$. Les manipulations mathématiques de ce vecteur consistent ensuite à le faire tourner dans la sphère de Bloch avec des portes quantiques à un qubit que nous verrons dans la partie suivante consacrée à la description du fonctionnement d'un ordinateur quantique. Ces manipulations reviennent à multiplier le vecteur représentant le qubit $[\alpha, \beta]$ par une matrice de deux lignes et deux colonnes de nombres complexes conservant la norme du vecteur, qui doit rester à 1. Les portes quantiques à plusieurs qubits relient les qubits entre eux et en font évaluer les valeurs d'un qubit de manière conditionnelle en fonction des valeurs d'un ou de deux autres qubits. Sans ces différentes portes quantiques, on ne pourrait pas faire grand-chose avec les qubits.
- L'**information dans les qubits** qui est manipulée lors des calculs est "riche" avec une dimension de deux nombres réels, les angles θ et φ, ou le vecteur $[\alpha, \beta]$.
- A part le cas où le qubit est initialisé à l'état $|0\rangle$ ou inversé à l'état $|1\rangle$, celui-ci est en **état de superposition** entre ces deux états. La représentation mathématique d'un qubit et son incarnation visuelle dans la sphère de Bloch montrent qu'un qubit peut-être dans une infinité d'états superposés différents.
- Lorsque l'on **lit la valeur du qubit**, on retombe sur un 0 ou un 1 binaires classiques avec un retour probabiliste dépendant des paramètres du vecteur de l'état du qubit dans la sphère de Bloch.
- Donc, nous avons un 0 en entrée, un 0 ou un 1 en sortie, et une **infinité d'états** entre les deux pendant les calculs !

---

[169] Voici quelques sources d'information associées à cette partie : Lectures on Quantum Computing de Dan C. Marinescu et Gabriela M. Marinescu, 2003 (274 pages), The Bloch Sphere de Ian Glendinning, 2005 (33 slides), The statistical interpretation of quantum mechanics, discours d'acceptation du prix Nobel de physique de Max Born en 1954 (12 pages) ainsi que l'excellent livre The mathematics of quantum mechanics de Martin Laforest, 2015 (111 pages), qui décrit les basiques mathématiques de l'informatique quantique avec les nombres complexes, les vecteurs, les matrices et tout le toutim.

Tout ça pour dire que la richesse mathématique du qubit intervient pendant les traitements et seulement pendant les traitements. Mais ni au départ, ni à l'arrivée des traitements. La magie mathématique de l'ordinateur quantique est là !

Voici ce cycle de vie du qubit illustré dans le schéma *ci-dessous* :



Algèbre linéaire et qubits

Le calcul quantique nécessite d'appréhender tout un tas de concepts de l'algèbre linéaire que nous allons balayer rapidement ici-même. Ils sont associés à un formalisme mathématique de description des phénomènes quantiques qui sont indispensables pour créer un algorithme quantique[170].

C'en est au point où, du fait des mécanismes de l'intrication quantique, il est souvent préférable d'utiliser et manipuler la notation mathématique de description de l'état des qubits et des opérations les concernant que d'essayer se créer une image mentale physique de ce qui se passe dans les qubits eux-mêmes. Il est difficile de « visualiser » dans l'espace le fonctionnement de cette intrication à grande échelle.

On retrouve cela dans la description des fameux états de Bell qui décrivent deux qubits intriqués. Cette intrication se démontre mathématiquement. La démonstration que nous ferons plus loin prouve qu'un tel état ne peut pas se décomposer en deux états de qubits indépendants.

Manque de bol, ce formalisme mathématique est plutôt abscons et difficile à digérer pour ceux qui n'en ont pas la patience, y compris votre serviteur !

Je vais tout de même tenter de vulgariser quelques concepts et conventions mathématiques de la mécanique quantique qui s'appliquent au cadre du calcul quantique. Ce sont d'ailleurs des notations, outils et conventions dont je ne fournirai pas forcément l'origine à chaque fois. Cela vous permettra surtout de s'y retrouver dans certaines des publications scientifiques sur le sujet.

Commençons par l'algèbre linéaire. C'est la branche des mathématiques des espaces vectoriels et des transformations linéaires.

Un phénomène est linéaire s'il ses effets sont proportionnels aux causes. Cela se traduit par la vérification des deux équations *ci-contre*.

$$f(\lambda x) = \lambda f(x) \; pour \; tout \; \lambda, x \in \mathbb{R}$$

$$f(x+y) = f(x) + f(y) \; pour \; tout \; x, y \in \mathbb{R}$$

[170] Voir notamment Calcul quantique : algèbre et géométrie projective, thèse d'Anne-Céline Baboin, 2013 (186 pages) et A propos du formalisme mathématique de la mécanique quantique de Thierry Paul (28 pages).

R étant un espace vectoriel, λ un nombre réel, x étant un vecteur de l'espace vectoriel R et f(x) une fonction s'appliquant à ce vecteur. Dans un espace à une seule dimension, un exemple classique de fonction linéaire est f(x) = ax + b. Une fonction polynomiale du genre $f(x) = ax^2 + b$ n'est évidemment pas linéaire car elle évolue de manière non proportionnelle à x.

Un **observable** est un état de base mesurable par un capteur sur un quantum ou un qubit. La mesure provoque l'écrasement de la fonction d'onde (ou la réduction du paquet d'onde) du quantum sur l'un des états de base. Si on mesure deux fois de suite l'état d'un quantum ou d'un qubit, la mesure donnera le même résultat. Dans la nature, un quantum peut avoir plusieurs états, comme le niveau d'excitation d'un électron d'un atome d'hydrogène. Dans les qubits, les observables sont généralement matérialisés mathématiquement par un 0 ou un 1 qui représentent leurs deux états quantiques distincts. La base des observables est l'ensemble des états de base d'un système quantique, donc ce qui correspond à 0 et 1 pour un qubit.

Une **base orthonormée** d'un espace vectoriel comprend des vecteurs de base qui sont mathématiquement tous orthogonaux les uns avec les autres et dont la longueur est de 1. Dans la représentation de l'état des qubits, cette base de vecteurs est constituée des états $|0\rangle$ et $|1\rangle$. Leur orthogonalité mathématique est une base de départ malgré le fait qu'ils sont opposés dans la sphère de Bloch pour des raisons de représentation dans cette sphère. D'autres bases de référence orthonormées peuvent servir d'observables, en particulier lorsque des photons sont manipulés, avec des références de phase différentes de la référence de départ.

C'est le cas des états situés sur la sphère de Bloch dans l'axe x et représentés avec $|+\rangle$ et $|-\rangle$ comme *ci-contre*.

$$|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

L'état d'un qubit est donc représenté dans cet espace orthonormé à deux dimensions comprenant les vecteurs d'état représentant les états de base $|0\rangle$ et $|1\rangle$. C'est un **vecteur de nombres complexes** dans un **espace de Hilbert** à deux dimensions. On le représente verticalement avec les nombres complexes α et β associés aux états $|0\rangle$ et $|1\rangle$ et dont la somme des carrés fait 1. Cette représentation décrit l'état de superposition entre $|0\rangle$ et $|1\rangle$ dans le qubit. Cette combinaison linéaire des états $|0\rangle$ et $|1\rangle$ décrit le phénomène de la **superposition** d'états au sein d'un qubit.

Cet espace à deux dimensions remplace l'espace de dimension infini qui caractérise une fonction d'onde f(x) de Schrödinger, x pouvant prendre n'importe quelle valeur. C'est donc une **représentation simplifiée** de l'état quantique d'un qubit. En manipulant ces symboles, les vecteurs et matrices, on en oublie la nature ondulatoire des quantums manipulés. Cela isole la représentation physique des qubits de leur traitement mathématique dans les calculs.

Dans la **notation de Dirac**, un état quantique est représenté par $|\Psi\rangle$, le **ket** de l'état quantique Ψ. Le **bra** du même vecteur d'état, représenté par $\langle\Psi|$ est la transposée conjuguée (ou transconjugée ou adjointe) du « ket ». C'est le vecteur « horizontal » $[\bar{\alpha}, \bar{\beta}]$. La barre au dessus des α et β décrit l'opération de conjugaison des nombres complexes avec inversion du signe de la partie complexe du nombre (-i au lieu de +i ou le contraire).

$$\overset{\text{ket de } \Psi}{|\Psi\rangle} = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \qquad \overset{\text{bra de } \Psi}{\langle\Psi|} = [\bar{\alpha}, \bar{\beta}]$$

$$|\Psi\rangle = \begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{i}{\sqrt{2}}\end{bmatrix} \quad \langle\Psi| = [\frac{1}{\sqrt{2}}, \frac{-i}{\sqrt{2}}]$$

$\bar{\alpha}$ est le conjugué de α avec négation de la partie complexe, idem pour $\bar{\beta}$.

Le **produit scalaire** de deux qubits $\langle\Psi_1|\Psi_2\rangle$ est la projection mathématique du vecteur d'état Ψ_2 sur le vecteur Ψ_1. Cela donne un nombre complexe. Lorsque les vecteurs sont orthogonaux, le produit scalaire est égal à 0.

Lorsque les deux vecteurs sont identiques, $\langle\Psi|\Psi\rangle$ est la norme de Ψ et est toujours égale à 1. En anglais : produit scalaire = scalar product ou inner product.

$$\overset{\text{produit scalaire (inner product)}}{\langle\Psi|\Psi\rangle} = \left[\bar{\alpha}, \bar{\beta}\right] \times \begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha^2 + \beta^2 = 1$$

Le **produit externe** de deux vecteurs représentant un qubit, l'un en bra et l'autre en ket, donne un opérateur ou matrice de densité qui est une matrice 2x2. En anglais, produit externe = outer product.

Lorsque le bra correspond à la transconjuguée du ket, il s'agit d'un opérateur de densité d'un état pur. Cette notion d'opérateur de densité sera ensuite élargie à une combinaison de qubits.

produit externe (outer product)

$$|\Psi\rangle\langle\Psi| = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \times [\bar{\alpha}, \bar{\beta}] = \begin{bmatrix}\alpha\bar{\alpha} & \alpha\bar{\beta}\\ \beta\bar{\alpha} & \beta\bar{\beta}\end{bmatrix}$$

Les **produits tensoriels** sont utilisés pour décrire l'état de registres quantiques de plusieurs qubits. L'état d'un registre de N qubits est le produit tensoriel de ces N qubits représentés par leur vecteur ket vertical. Cela donne un vecteur (vertical) pouvant prendre 2^N valeurs différentes, représentant chacune une combinaison différente de 0 et de 1. Un registre quantique superpose ces 2^N états différents avec un poids de chacun de ces états représenté par un nombre complexe.

La somme de ces poids au carré donne 1. D'une manière générale, le produit tensoriel de deux vecteurs de dimension m et n donne un vecteur de dimension m*n. Et pour ce qui est de matrices à deux dimensions, le produit tensoriel d'une matrice de dimension m*n par une matrice de dimension k*l donnera une matrice de dimension mk*nl. Les produits tensoriels utilisent le signe ⊗.

un état d'un registre de 8 qubits est un produit tensoriel de 8 qubits, un état basique (« basic state »).

$$|1\rangle\otimes|1\rangle\otimes|1\rangle\otimes|1\rangle\otimes|1\rangle\otimes|1\rangle\otimes|1\rangle\otimes|1\rangle$$
$$= \begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}$$

un état basique est un produit tensoriel, un vecteur de dimention $N=2^8$ soit 256, chaque élément étant 0 ou 1.

$$|01010001\rangle = \begin{matrix}|00000000\rangle\\|00000001\rangle\\\vdots\\|01010000\rangle\\|01010001\rangle\\\vdots\\|11111110\rangle\\|11111111\rangle\end{matrix}\begin{bmatrix}0\\0\\\vdots\\0\\1\\\vdots\\0\\0\end{bmatrix}$$

l'état d'un registre est donc la somme des probabilités d'état de chaque combinaison de 0 et de 1 et la somme des probabilités c_i au carré fait 1.

$$|\psi\rangle = c_1|00000000\rangle + \cdots + c_{82}|01010001\rangle + \cdots c_{255}|11111110\rangle + c_{256}|11111111\rangle$$
$$= \sum_{i=1}^{N} c_i\,|i\rangle$$

En algèbre linéaire, les transformations (U) qui s'appliquent à un jeu de qubits sont linéaires et à ce titre ont des propriétés diverses qui sont liées au calcul matriciel. Ces transformations ou opérations sont dites unitaires car elles utilisent des **matrices unitaires**, à savoir des matrices carrées qui, multipliées par leur matrice adjointe, donne une unité (égalité) selon la formule $U^*\times U=U\times U^*=I$. Une matrice unitaire a plusieurs propriétés dont celle consistant à avoir des vecteurs propres orthogonaux (nous verrons cette notion plus loin) et d'être diagonalisable.

Les qubits peuvent subir des **transformations non unitaires** lors de deux situations : lorsque leur état est mesuré – via une matrice projective sur un état de base, qui n'est pas unitaire et ne contient qu'un seul 1 et des zéros pour le reste - et lorsqu'ils subissent le phénomène de la décohérence. Le caractère non non unitaire d'une mesure est associé à son caractère irréversible.

Les **mesures projectives** classiques consistent en une projection du vecteur d'état sur l'axe |0⟩/|1⟩ dans la sphère de Bloch suivie d'une mesure. En opérant auparavant une rotation dans la sphère de Bloch, elles permettent de connaître l'état d'un qubit par rapport à un repère orthonormé différent de celui des états de base |0⟩ et |1⟩ comme le |+⟩ et le |-⟩ vus précédemment.

Tous ces éléments de notation d'algèbre linéaire quantique sont bien résumés dans le tableau *ci-dessous*[171].

[171] Il provient de Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages).

Un **état pur** (pure state) décrit l'état d'un qubit isolé. C'est la combinaison des deux états observables du qubit respectant la distribution probabiliste de Max Born.

Un **état basique** (basic state) d'un registre de qubits, représenté par un ket, est une combinaison donnée de 0 et de 1 de qubits dans un registre. Un registre de N qubits peut donc avoir 2^N états basiques différents.

Notation	Description
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1-i$
$\|\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a *bra*.
$\langle\varphi\|\psi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = (A^T)^*$. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$.
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$. Equivalently, inner product between $A^\dagger\|\varphi\rangle$ and $\|\psi\rangle$.

Des **états quantiques** sont séparables lorsqu'ils sont mathématiquement le résultat du produit tensoriel de chacun des états purs qui le composent.

A contrario, l'**intrication,** ou un état intriqué de deux qubits, se produit lorsqu'il ne peut pas être évalué sous la forme du produit tensoriel de deux états purs.

En clair, il ne peut pas être la combinaison de deux qubits indépendants. Cela se démontre mathématiquement et simplement par l'absurde pour les états $|00\rangle$ et $|11\rangle$ d'un registre de deux qubits. Dans ces paires, la mesure de la valeur de l'un des qubits détermine celle de l'autre, ici, identique.

démonstration de l'impossibilité de créer un état EPR par le produit tensoriel de deux qubits, ici $|\Psi_1\rangle$ et $|\Psi_2\rangle$

$$|\Psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$$
$$|\Psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$$

calcul du produit tensoriel de deux qubits hypothétiques

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle)$$

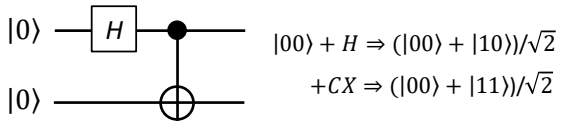
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle)$$

$$\alpha_1\beta_2 = 0 \text{ et } \beta_1\alpha_2 = 0 \quad incompatibles\ avec\ \alpha_1\alpha_2 = \frac{1}{\sqrt{2}} \text{ et } \beta_1\beta_2 = \frac{1}{\sqrt{2}}$$

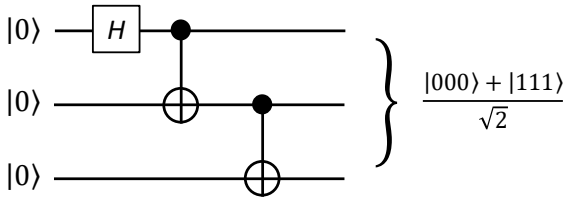
car si $\alpha_1 = 0$ alors $\alpha_1\alpha_2 = 0$
car si $\beta_2 = 0$ alors $\beta_1\beta_2 = 0$

Sachant que la création de telles paires intriquées de qubits passe par des opérations de préparation. Deux qubits placés côte à côte ne sont pas intriqués par magie ! La paire utilisée dans l'exemple *ci-dessus* peut-être générée par deux portes quantiques, une porte H (Hadamard) et une porte CNOT, que nous verrons plus loin.

Seules les portes quantiques à plusieurs qubits génèrent des qubits intriqués, dans un registre de qubits. Ici avec un exemple de création d'une paire de Bell associant les états $|00\rangle$ et $|11\rangle$.



Un état dit **GHZ** (pour Greenberger–Horne–Zeilinger, que l'on distingue des fréquences en GHz avec le Z majuscule) avec trois qubits intriqués superposant les états $|000\rangle$ et $|111\rangle$ est préparé avec une porte de Hadamard et deux CNOT consécutives comme indiqué dans le schéma *ci-contre*. Nous définirons cette porte un peu plus loin.

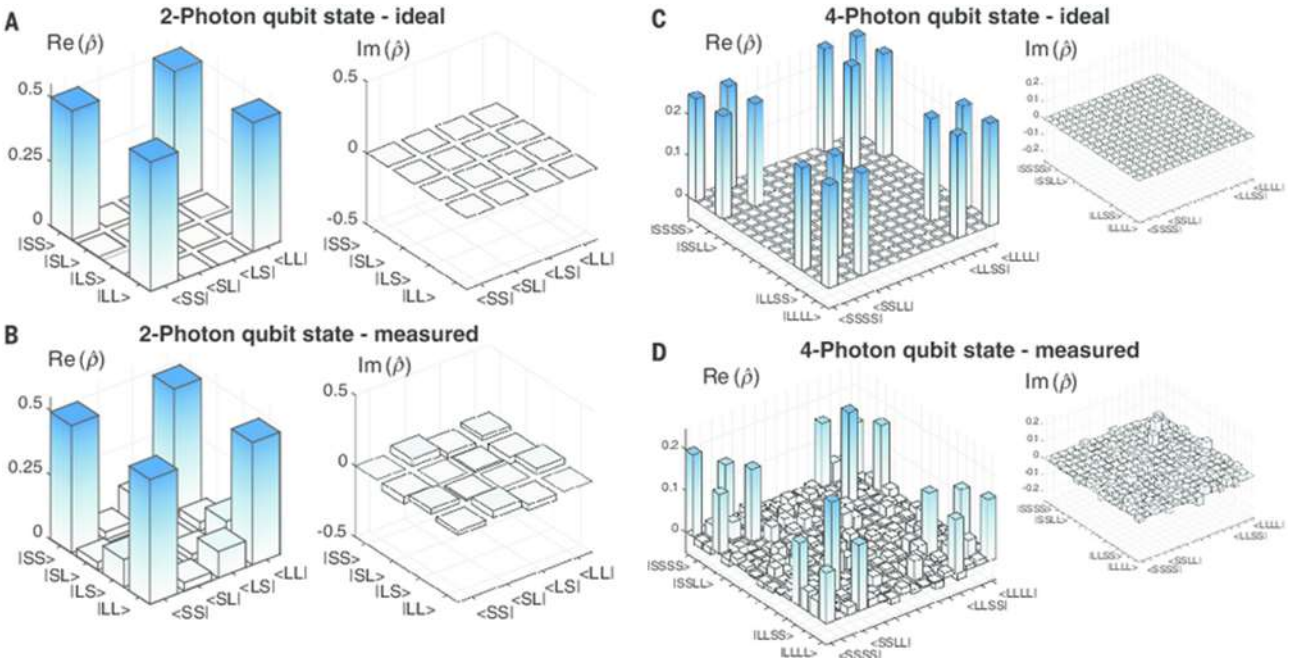


Ces paires de Bell et états GHZ sont notamment exploités dans les codes de correction d'erreurs.

Une **matrice densité,** souvent représentée par le signe ρ (rho), est une matrice de nombres complexes qui sert à décrire un système physique, ici, un registre de qubits. Elle décrit des états appelés mélanges statistiques qui associent plusieurs états possibles du registre (combinaison de $|0\rangle$ et de $|1\rangle$).

La matrice comprend l'ensemble des états quantiques possibles d'un registre, associant la mécanique quantique et la physique statistique. On peut déduire de la matrice densité les valeurs espérées des observables, à savoir le poids des |0⟩ et |1⟩ pour chaque qubit.

Ces matrices sont hermitiennes (symétriques) et de norme 1. La représentation graphique de ces matrices est souvent utilisée pour évaluer la fidélité de portes quantiques à deux ou trois qubits dans les publications de chercheurs. L'exemple ci-dessous illustre cela en comparant l'état théorique d'une matrice de densité pour 2 qubits et 4 qubits et le résultat de la mesure[172].



Les vecteurs d'état, ou kets, décrivent un **état pur**. Les matrices densités générées à partir d'un état d'un seul qubit (ket) sont dites pures.

Leur combinaison statistique classique donne un **état mixte** (mixed state) qui est incarné par la matrice densité qui en résulte comme illustré *ci-dessous*. Ces états mixtes correspondent à des états difficiles à isoler d'un point de vue pratique.

un état mixte est une combinaison probabiliste de plusieurs états de registres quantiques. Ψ_i est un de ces états représenté sous la forme d'un vecteur vertical avec 2^N entrées, N étant le nombre de qubits du registre.

$$\{(\boldsymbol{p_i}|\Psi_i)\}$$

l'opérateur ou matrice de densité de cet état mixte est l'addition de ces différents états multiplié par leur probabilité (la somme des probabilités fait 1, sans passer par le carré comme pour un état pur). Avec N qubits, l'opérateur de densité est une matrice carrée de 2^N de côté.

$$\boldsymbol{\rho} = \sum_i \boldsymbol{p_i} \, |\Psi_i\rangle\langle\Psi_i|$$

$$\sum_i \boldsymbol{p_i} = \mathbf{1}$$

la matrice de densité d'un seul qubit est une matrice 2x2 résultat du produit intérieur de l'état ⟨Ψ|.

$$\boldsymbol{\rho} = |\Psi\rangle\langle\Psi|$$

Dans le calcul quantique, un état mixte est généré par les portes quantiques qui génèrent l'intrication de qubits.

Voici ce à quoi ressemble un des états de cet état mixte, $|\boldsymbol{\Psi i}\rangle\langle\boldsymbol{\Psi i}|$.

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_N \end{pmatrix} \begin{pmatrix} \bar{a}_1 & \bar{a}_2 & \cdots & \bar{a}_N \end{pmatrix} = \begin{pmatrix} a_1\bar{a}_1 & a_1\bar{a}_2 & \cdots & a_1\bar{a}_N \\ a_2\bar{a}_2 & a_1\bar{a}_2 & \cdots & a_2\bar{a}_N \\ \vdots & & & \vdots \\ a_N\bar{a}_1 & a_N\bar{a}_2 & \cdots & a_N\bar{a}_N \end{pmatrix}$$

[172] Source : Generation of multiphoton entangled quantum states by means of integrated frequency combs, 2016.

Les matrices densité sont particulièrement utiles pour décrire des **états intriqués** comme les paires de Bell comme l'illustre la matrice *ci-contre*.

exemple avec une paire EPR rassemblant deux vecteurs d'état |00⟩ et |11⟩

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(1,0,0,1)^T$$

une matrice densité d'une paire de Bell est simple à créer à partir du vecteur ket représentant l'état superposé |00⟩ et |11⟩

$$\frac{1}{\sqrt{2}}(1,0,0,1)^T \frac{1}{\sqrt{2}}(1,0,0,1)^T = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

La visualisation de la matrice densité d'une combinaison de qubits utilise la technique de la **tomographie**. Elle revient à réaliser une opération répétée d'opérations et de mesures de l'état des qubits pour remplir une matrice densité moyennant les résultats. Cela peut notamment servir à évaluer la fidélité des qubits.

Sinon, un **mélange statistique** est la partie diagonale de la matrice de densité et la **trace** d'une matrice est la somme des valeurs des éléments de sa diagonale.

Reste à définir les notions d'**eigenvector**, **eigenvalue**, **eigenstate** et **eigenspace** qui sont souvent utilisées en mécanique et en calcul quantiques ainsi d'ailleurs que dans le machine learning, en particulier dans les algorithmes de réduction de dimensions comme la PCA (Principal Components Analysis). Ces notions permettent de définir la structure de certaines matrices carrées. Pour une telle matrice A, un eigenvector x ou vecteur propre de A est un vecteur qui vérifie l'équation $Ax = \lambda x$, λ étant un nombre réel que l'on nomme eigenvalue ou valeur propre. Ces eigenvectors ont la particularité de ne pas changer de direction une fois multipliés par la matrice A. Pour une eigenvalue λ, l'eigenspace associé, ou espace propre, est l'ensemble des vecteurs x qui satisfont $Ax = \lambda x$.

Ces eigenvalues s'évaluent en calculant le déterminant de la matrice $A - \lambda I$, I étant la matrice d'identité (1 dans les cases de la diagonale et 0 ailleurs). On trouve alors les valeurs de qui résolvent $0 = A - \lambda I$. C'est une équation polynomiale ayant un degré inférieur ou égal à la taille de la matrice carrée.

Les eigenvectors de référence d'une matrice A permettent de reconstituer un espace orthonormé lié à la matrice. Par exemple, une matrice de projection dans un plan en 3D aura comme eigenvectors principaux deux vecteurs orthogonaux situés dans le plan et un vecteur orthogonal au plan. Cette multiplication donne λx avec λ étant non nul si l'eigenvector est dans le plan en question et 0 si le vecteur est orthogonal au plan[173]. Une matrice A peut être celle d'une porte quantique. Un eigenvector d'une porte quantique est donc un ket dont la valeur n'est pas modifiée par la porte quantique.

C'est facile à se représenter pour la porte S, de changement de phase, que nous verrons plus loin. Les kets |0⟩ et |1⟩ étant dans l'axe de rotation, ils ne sont pas modifiés par celle-ci.

Ce sont donc des eigenvectors de la porte S et l'eigenvalue correspondante est de 1. C'est toujours le cas pour les matrices des portes quantiques puisque les vecteurs représentant les états quantiques, les kets, ont toujours une longueur de 1.

La recherche des eigenvectors et eigenvalues d'une matrice A revient à la diagonaliser. La diagonalisation d'une matrice carrée consiste à trouver la matrice qui la multipliera pour la transformer en matrice remplie uniquement dans sa diagonale. Plus précisément, une matrice A est diagonalisable si on peut trouver une matrice P et une matrice diagonale D telles que $P^{-1}AP = D$ (P^{-1} étant la matrice inverse de P, telle que $P^{-1}P = PP^{-1} = I$, I étant la matrice identité avec des 1 dans la diagonale et des 0 ailleurs). Une matrice carrée de dimension n est diagonalisable si elle a n vecteurs propres.

Et les eigenstates ? C'est un autre nom donné aux eigenvectors, mais par les physiciens ! A ce stade, je ne vous embêterai probablement pas plus avec les eigentrucs !

Dans les équations de Maxwell, Schrödinger, Dirac et autres que nous avons vues sont utilisées des notations bonnes à rappeler ici autour du symbole nabla : ∇, utilisé parfois avec une flèche $\vec{\nabla}$.

[173] C'est bien expliqué dans le cours de Gilbert Strang du MIT, 2011 (51 minutes).

$$\nabla = \left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\right)$$

opérateur **del** ou **nabla** en calcul vectoriel : dérivée première sur les dimensions du vecteur

$$\nabla f = \left(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}\right)$$

gradient d'une fonction scalaire f, renvoit un vecteur avec la direction de la plus grande variation du champ scalaire et l'intensité de cette variation

$$\nabla.\vec{G} = \left(\frac{\partial G_x}{\partial x}, \frac{\partial G_y}{\partial y}, \frac{\partial G_z}{\partial z}\right)$$

divergence d'une fonction vectorielle G, exprime sa tendance à évoluer localement

$$\nabla \times \vec{G} = \left(\frac{\partial G_z}{\partial y} - \frac{\partial G_y}{\partial z}, \frac{\partial G_x}{\partial z} - \frac{\partial G_z}{\partial x}, \frac{\partial G_y}{\partial x} - \frac{\partial G_x}{\partial y}\right)$$

rotationnel ou **curl** d'une fonction vectorielle G qui transforme un champ de vecteur en champ de vecteur décrivant la variation de ce champ dans l'espace

Nabla désigne généralement le gradient d'une fonction scalaire ou vectorielle, à savoir sa dérivée première. Une fonction scalaire s'applique à un vecteur, souvent de trois dimensions x, y et z d'un espace euclidien. Elle renvoie un nombre. Une fonction vectorielle renvoie un vecteur ! Cela aboutit aux notions de gradient et de laplacien qui s'appliquent à une fonction scalaire et correspondent à des dérivées premières et secondes dans l'espace, et de divergence et de rotationnel (ou curl) qui s'appliquent à une fonction vectorielle. Un laplacien peut aussi s'appliquer à une fonction vectorielle. Nous n'irons pas pu loin que cela dans cet ebook pour ce qui est de ces fonctions.

$$\nabla^2 f = \nabla.\nabla f = \left(\frac{\partial^2 f}{\partial x^2}, \frac{\partial^2 f}{\partial y^2}, \frac{\partial^2 f}{\partial z^2}\right)$$

laplacien d'une fonction scalaire f qui s'applique à un vecteur renvoyant un scalaire, c'est une sorte de dérivée seconde de la variation de la fonction dans l'espace

$$\nabla^2 \vec{G} = \left(\frac{\partial^2 G_x}{\partial x^2} + \frac{\partial^2 G_x}{\partial y^2} + \frac{\partial^2 G_x}{\partial z^2}, \frac{\partial^2 G_y}{\partial x^2} + \frac{\partial^2 G_y}{\partial y^2} + \frac{\partial^2 G_y}{\partial z^2}, \frac{\partial^2 G_z}{\partial x^2} + \frac{\partial^2 G_z}{\partial y^2} + \frac{\partial^2 G_z}{\partial z^2}\right)$$

laplacien d'une fonction vectorielle G qui s'applique à un vecteur renvoyant un vecteur

Cet inventaire ne serait pas complet sans décrire un objet mathématique encore plus étrange : le **permanent d'une matrice** carrée n*n, inventé par Louis Cauchy en 1812.

$$\text{per}(A) = \sum_{\sigma \in \mathfrak{G}} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

La formule *ci-dessus* en décrit le contenu. Le Π dénote une multiplication de valeurs de la matrice d'indices i et σ(i). σ est une fonction de permutation des entiers compris entre 1 et n, la dimension de la matrice (nombre de colonne et de lignes). Le sigma porte sur l'ensemble des fonctions σ du groupe des permutations S_n (dénommé aussi groupe symétrique) qui fait une taille de n! (factorielle de n). Les valeurs $a_{i,\sigma(i)}$ sont les cases de la matrice de coordonnées i et σ(i).

Voici ce que cela donne avec n=2 et n=3 sachant qu'au-delà, cela devient moins lisible :

$$\text{perm}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad + bc \qquad \text{perm}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh + ceg + bdi + afh$$

Le permanent est donc un nombre réel qui résulte de n! (factorielle de n) additions de multiplications de n valeurs de la matrice. Les permanents sont notamment utilisés pour évaluer des matrices qui représentent des graphes. Ils le sont aussi dans la simulation numérique classique de l'échantillonnage du boson que nous aurons l'occasion de décrire dans la partie dédiée aux qubits photons[174]. Contrairement au calcul du déterminant, *ci-dessous*, qui peut être simplifié, celui du permanent reste un problème classiquement intractable.

Le **déterminant d'une matrice** est une variante de son permanent (*ci-contre*). sgn(σ) est le signe des permutations, qui est +1 si le nombre d'interversions nécessaires pour créer la permutation est pair et -1 s'il est impair. Olé !

$$\det(A) = \sum_{\sigma \in Sn} \left(\text{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}\right)$$

[174] Le temps de calcul d'un permanent augmente de manière plus rapide qu'une exponentielle d'une valeur fixe (M^n) dès que n devient très grand par rapport à M. Donc, par exemple, avec M=2, 2^n est bien plus petit que n! dès que n est supérieur à 4. Comme la simulation numérique du boson requiert un déterminant qui dépend de la taille de la simulation, elle est encore plus lourde à calculer qu'un problème exponentiel.

Et voici ce que cela donne pour n=3. A noter que le groupe des permutations comprend la permutation qui ne change pas l'ordre des éléments.

$$\det\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh - ceg - bdi - afh$$

A noter que les déterminants ont des propriétés particulières telles que det(AB)=det(A).det(B)= det(B).det(A)=det(BA) ce qui peut faciliter le calcul du déterminant d'une matrice si on peut la factoriser en plusieurs matrices.

Voilà pour la définition des basiques de l'algèbre linéaire du calcul quantique. J'ai zappé plein d'autres définitions et règles de calcul. Il s'agissait de préciser certaines notions qui sont fréquemment utilisées dans la littérature scientifique sur le calcul quantique et dans nombre d'ouvrages de référence cités dans cet ebook. Ce que nous venons de voir vous servira peut-être à compulser une partie de la littérature scientifique sur le calcul quantique.

Non-linéarités

Ajoutons un point général portant sur les non-linéarités. Elles sont souvent évoquées en physique quantique, notamment pour créer des qubits. On en entend aussi parler dans les mathématiques des réseaux de neurones. Si les principes mathématiques sont voisins, leur signification n'est pas la même dans ces différents scénarios.

Les qubits supraconducteurs exploitent l'effet Josephson et un oscillateur anharmonique permettant d'éviter que les états d'énergie de la boucle supraconductrice soient séparés par un même niveau d'énergie. C'est un effet non-linéaire. Cela facilite le pilotage par des micro-ondes du changement d'état des qubits entre $|0\rangle$ et $|1\rangle$ par une fréquence qui est supérieure à celle qui permettrait de passer de l'état $|1\rangle$ à l'état $|2\rangle$, ce que l'on cherche à éviter.

Les non-linéarités sont aussi recherchées en photonique, notamment pour créer des portes quantiques à deux qubits photons de qualité. Les non-linéarités se manifestent lorsque des milieux solides modifient les caractéristiques de photons comme leur polarisation et de manière non linéaire par rapport au champ électrique qui est appliqué au solide. Ce phénomène se manifeste dans l'effet Kerr qui voit l'indice de réfraction de matériaux changer de manière non-linéaire (quadratique) en fonction du champ électrique qui leur est appliqué. A contrario, l'effet Pockels utilisé dans des modulateurs optiques voit la réfraction modifiée de manière linéaire en fonction du champ électrique appliqué. Cette non-linéarité en optique intervient aussi dans de nombreux dispositifs comme les lasers de puissance.

Enfin, la question des non-linéarités se pose au sujet des fonctions d'activation des réseaux de neurones dans l'intelligence artificielle. Celles-ci utilisent par exemple des sigmoïdes à partir de fraction d'exponentielles.

Comment donc exécuter de telles fonctions d'activation dans du calcul quantique qui repose uniquement sur de l'algèbre linéaire ? L'une des premières solutions imaginées consiste à utiliser une porte quantique non linéaire, non réversible et dissipative dite D[175]. D'autres s'appuient sur l'usage de mémoire quantique[176].

Types de qubits

D'un point de vue physique, les qubits des calculateurs quantiques sont des dispositifs matériels qui intègrent des particules élémentaires qui ont deux états possibles que l'on peut initialiser, modifier avec des portes quantiques puis dont on peut évaluer l'état par observation ou mesure.

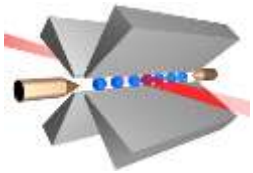
---

[175] Méthode proposée par Sanjay Gupta dans Quantum Neural Networks, 2001 (30 pages).

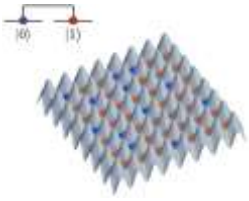
[176] Voir Quantum Algorithms for Deep Convolutional Neural Network, par Iordanis Kerenidis et al, 2020 (36 pages).

Il s'agit parfois de particules élémentaires individuelles, comme avec les atomes (ions piégés et atomes froids), des électrons (qubits silicium, NV centers, anyons pour le calcul topologique) ou des photons ! Et une seule à la fois ! Dans le cas des qubits supraconducteurs, l'état quantique s'appuie sur un grand nombre d'électrons arrangés en paires de Cooper qui partagent un même état quantique, les paires d'électrons qui se créent à température supraconductrice.

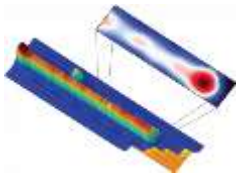
supraconducteurs



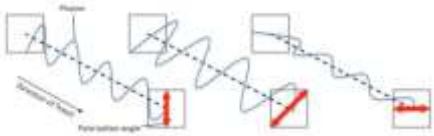
ions piégés



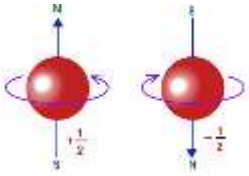
atomes froids



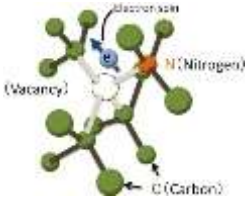
fermions de Majorana



photons



spin d'électrons piégés

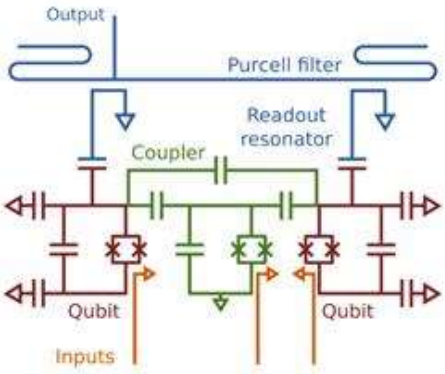


centres NV (diamant)

Voici les principaux types de qubits qui sont étudiés, expérimentés ou utilisés en production actuellement :

Les **supraconducteurs** : le qubit prend la forme de l'état d'un courant supraconducteur qui traverse une barrière très fine, en général en oxyde de métal comme l'aluminium, et en s'appuyant sur l'effet Josephson[177]. Il existe plusieurs types de qubits supraconducteurs, de flux, de phase et de charge. Ne rentrons pas dans les détails. Dans tous les cas, il s'agit de créer une superposition de deux états bien distincts d'un courant oscillant à haute fréquence et traversant la jonction Josephson dans une boucle supraconductrice. L'oscillation est rendue possible par le fait que la boucle intègre l'équivalent d'une inductance et d'une résistance.

L'oscillation du courant est activée par l'application de micro-ondes de fréquences situées entre 5 et 10 GHz transmises par voie conductrice et physique. Ce ne sont pas des micro-ondes émises par la voie "radio", elles circulent sur des câbles coaxiaux. L'état du qubit est pour sa part mesuré avec un résonateur intégré dans le circuit qui reçoit une micro-onde et la renvoie avec un décalage de phase ou pas permettant d'identifier l'état du qubit. *Ci-contre*, la schématique de deux qubits supraconducteurs de Google Sycamore, reliés eux-mêmes par un troisième qubits qui sert de coupleur dynamique entre deux qubits.



C'est la technique la plus couramment employée aujourd'hui, notamment par IBM, Google, Rigetti et Intel pour le calcul quantique à circuits universels et avec les ordinateurs à recuit quantique du Canadien D-Wave qui utilisent un autre arrangement de qubits de qualité moins bonne du côté du bruit et du taux d'erreurs.

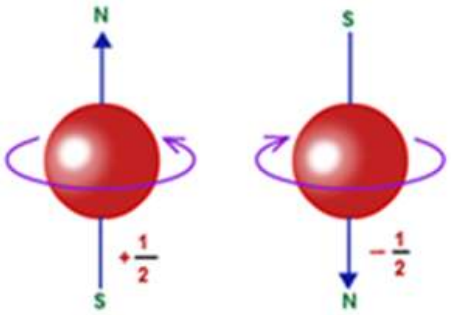
[177] Voir Digital readout and control of a superconducting qubit par Caleb Jordan Howington, 2019 (127 pages).

Elle est relativement facile à fabriquer car elle s'appuie sur les techniques de création de circuits CMOS même si certains des matériaux sont différents, comme le niobium qui est utilisé chez D-Wave[178]. Notons, nous le verrons plus tard, que l'équipe de Daniel Estève au CEA de Saclay fait partie des précurseurs de la création de tels qubits supraconducteurs.

La technique présente des inconvénients : les générateurs de radiofréquence sont généralement situés à l'extérieur de l'enceinte cryogénisée du processeur quantique, ce qui multiplie le câblage. Les fréquences de contrôle des qubits doivent être différentes pour des qubits adjacents ce qui donne des plans d'allocation de fréquences voisins de ceux que les opérateurs télécoms utilisent pour le téléphone cellulaire.

Le **spin d'électron** : haut ou bas, une sorte de sens de polarisation magnétique, que l'on retrouve dans les ordinateurs à base de quantum dots, notamment chez Intel ou dans des prototypes de qubits réalisés au CEA-Leti à Grenoble. Ces qubits sont intégrés dans des circuits à base de semi-conducteurs CMOS à base de silicium. Le silicium est souvent complété des dopants ou compléments divers, comme des éléments dits "III-V" de type germanium. On y trouve aussi de l'aluminium, du titane, du paladium, du platine et de l'hafnium.

Ils bénéficient donc de la réutilisation de processus de fabrication de composants CMOS déjà bien maitrisés. Ces qubits sont cependant pour l'instant plutôt "bruyants", même en les exploitant à des températures proches du zéro absolu. Le plan consiste à en aligner des batteries pour créer des qubits logiques, un concept que nous étudierons dans la prochaine partie. Ce serait à ce jour la seule technologie réellement scalable en termes de nombre de qubits. Les qubits des autres technologies sont en effet difficilement miniaturisables.



Qui plus est, fonctionnant à une température très basse, inférieure à 20 mK, ils limitent la puissance qui peut être consommée pour les contrôler dans leur enceinte cryogénique. A contrario, les qubits CMOS pourraient fonctionner à une température moins froide de 1K, qui permettrait de dépenser un peu plus d'énergie pour les contrôler dans l'enceinte cryogénique.

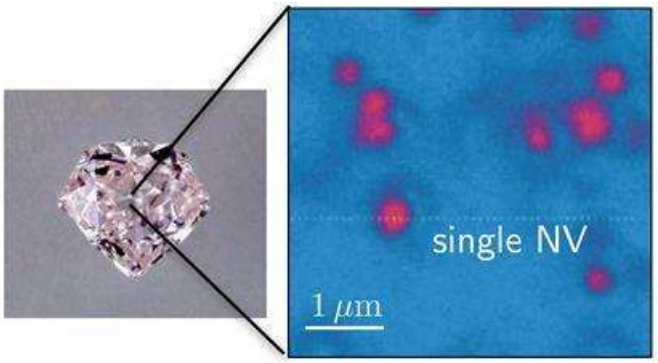
Les **centres NV** (pour Nitrogen Vacancy) : ce sont des structures de diamant artificiel dans lesquelles un atome de carbone a été remplacé par un atome d'azote et à proximité duquel se situe une lacune d'atome de carbone.

Les défauts dans les diamants ont été étudiés à partir de 1930 avec l'examen de l'absorption de l'infrarouge[179]. Cela permettait de distinguer deux catégories de diamants : type I avec une bande d'absorption de 8 µm dans l'infrarouge et type II sans cette bande. Les défauts expliquent la couleur des gemmes de diamants. Il fallu attendre 1959 pour découvrir que ces impuretés étaient liées à la présence d'azote, à 7,8 µm et que les atomes d'azote étaient bien isolés dans le diamant. En 1975, on découvrait qu'un traitement thermique permettait de contrôler la diffusion des atomes d'azote dans le diamant. Ces centres d'azote donnent une couleur au diamant. Avec quatre formes : un atome d'azote isolé par une lacune, deux atomes d'azote, trois atomes d'azote entourant une lacune et quatre atomes d'azote.

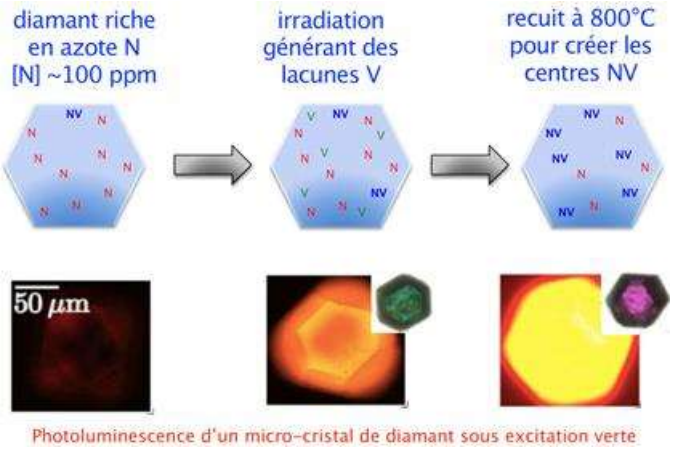
[178] Voir Practical realization of Quantum Computation Superconducting Qubits (36 slides).

[179] Dans Les défauts du diamant : de la couleur des gemmes à un outil pour les nanosciences de Jean-François Roch, 2011 (42 minutes) et Centres NV du diamant du matériau aux applications, 2015 (52 slides) racontent très bien la découverte des centres NV.

C'est la première forme qui est intéressante dans les différents usages évoqués dans cet ouvrage, notamment en métrologie quantique. On peut visualiser ces défauts avec un microscope confocal (à faible profondeur de champ) en les illuminant avec un faisceau laser vert qui va générer de la lumière rouge[180]. Ces diamants à NV centers sont légèrement roses. Ces propriétés permettent de générer des sources de photons uniques grâce à l'isolation d'un NV center.



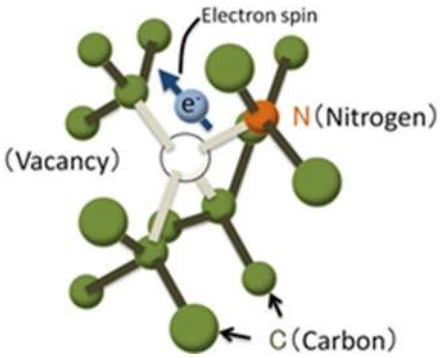
Pour produire ces NV centers, on utilise des diamants artificiels riches en azote. Les lacunes sont générées par irradiation. Un recuit sous vide à environ 800°C-900°C déplace les lacunes à côté des atomes d'azote dans la structure cristalline[181]. C'est lié au fait que les atomes d'azotes sont aussi grands que ceux du carbone. La lacune crée une petite barre d'électrons qui servent d'aimant virtuel via leur spin. Ils ont deux orientations possibles : parallèle ou orthogonale au champ magnétique ambiant. On peut les contrôler individuellement.



Photoluminescence d'un micro-cristal de diamant sous excitation verte

On peut aussi produire des diamants à NV centers avec du dépôt sous vide d'hydrogène et de méthane (CVD, pour Chemical Vapor Deposition) pour créer une structure cristalline parfaite de diamant puis avec de l'implantation ionique avec des faisceaux d'ions d'azote.

La structure du carbone environnant un NV center protège bien la zone de la cavité. L'état de la lacune est instable et quantique. Il est excité par lasers et micro-ondes. La lecture de l'état du qubit est réalisée par une mesure de brillance de fluorescence.



La startup américaine **QDTI** planchait commercialement sur cette technique pour créer des qubits. Mais elle a pivoté pour s'intéresser aux usages médicaux de la métrologie quantique à base de diamants. Il ne semble rester que la startup **Quantum Brilliance** (2019, Australie) qui se soit positionnée sur ce créneau.

[180] Voir Scanning Confocal Optical Microscopy and Magnetic Resonance on Single Defect Centers de A. Gruber et al, 1997 (4 pages) qui est la source de l'illustration vus également dans les slides de Jean-François Roch.

[181] Source de l'illustration : Centres NV du diamant du matériau aux applications, de Jean-François Roch, 2015 (52 slides). Une thèse décrit bien les différentes techniques de création de centers NV : Engineering of NV color centers in diamond for their applications in quantum information and magnetometry, Margarita Lesik, 2015 (139 pages).

Voici, *ci-dessous*, un schéma d'ensemble du mécanisme de contrôle de ces qubits[182].

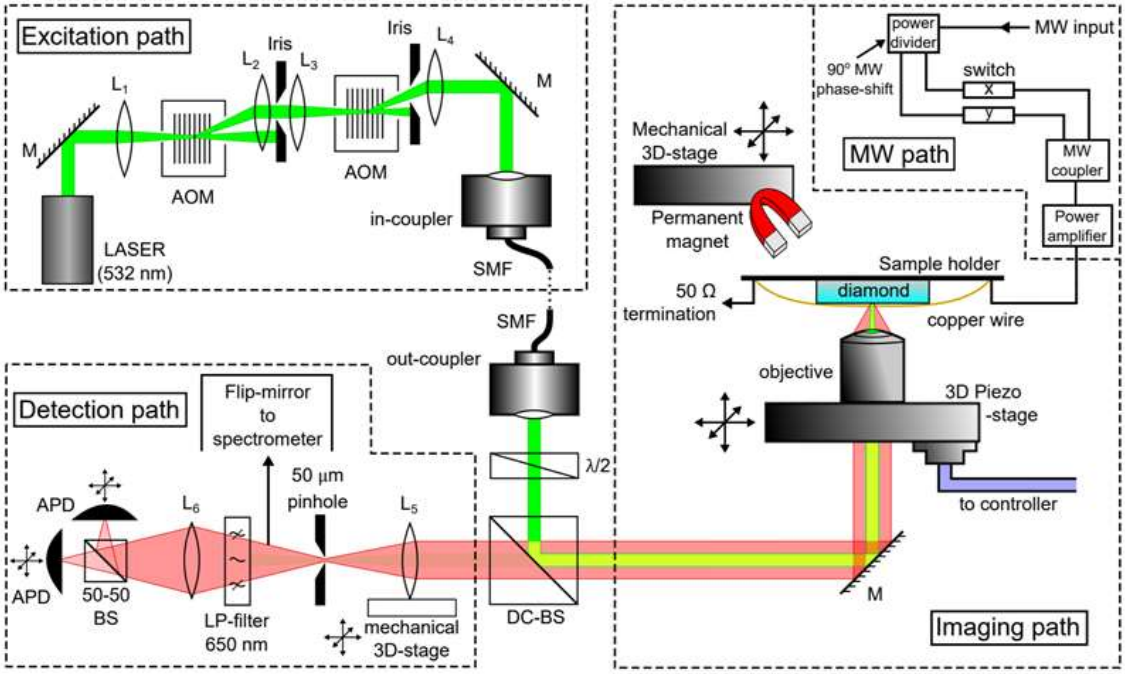
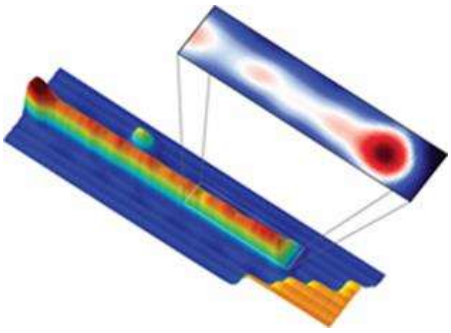


Figure A.1.: Schematic representation of the utilized setup for the characterization of NV centers. Experimental setup utilized for optical characterization and coherent spin manipulation of NV centers, comprising of a home-built confocal microscope, a scanning-stage for the imaging of diamond, and external magnet and microwave apparatus. The excitation wavelength is 532 nm. In the figure, mirrors are represented by M, lenses by L_i, single-mode optical fiber by SMF, beam-splitters by BS, and avalanche photo-diodes by APD.

Les **fermions de Majorana** : ce sont des anyons ou quasi-particules qui sont des états particuliers de nuages d'électrons organisées par paires. Pratiquement, ce sont des spins d'électrons aux deux bouts de fils supraconducteurs. On peut d'ailleurs considérer à ce titre là que c'est une variation des qubits supraconducteurs.

De ce fait, ces ordinateurs quantiques doivent aussi être refroidis à une température voisine du zéro absolu, aux alentours de 10mK.



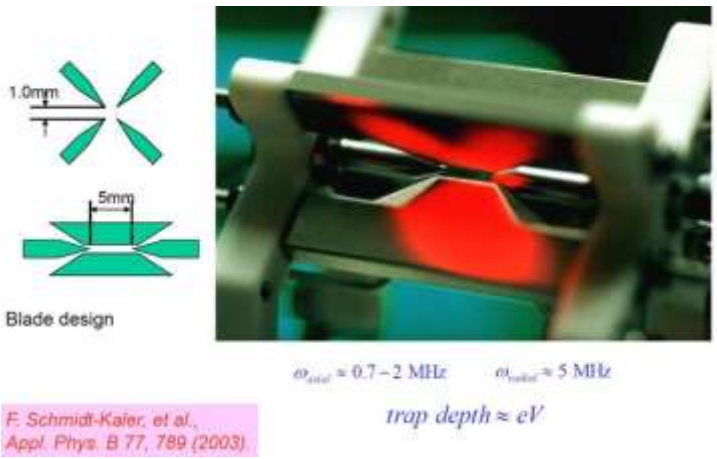
C'est la voie choisie par Microsoft et une équipe de Nokia aux USA. Sachant que l'existence des fermions de Majorana est à peine prouvée. Et les quasi-particules sur lesquelles planchent les équipes de Microsoft ne seraient pas des fermions de Majorana. Il y a de quoi y perdre son latin ! Nous reviendrons dessus plus loin.

Les **ions piégés** : il s'agit d'ions d'atomes qui sont maintenus sous vide et suspendus par suspension électrostatique. Un pompage optique est réalisé pour leur initialisation. Un laser sert à la mesure et exploite le phénomène de fluorescence des ions excités par le laser. Le magnétisme est utilisé pour l'activation des portes quantiques. Les lasers permettent d'intriquer des qubits. La startup IonQ issue de l'Université de Maryland planche là-dessus tout comme l'université d'Innsbruck en Autriche et sa spinoff AQT (Alpine Quantum Technologies).

[182] Vu dans Forefront engineering of nitrogen-vacancy centers in diamond for quantum technologies 2017 (235 pages).

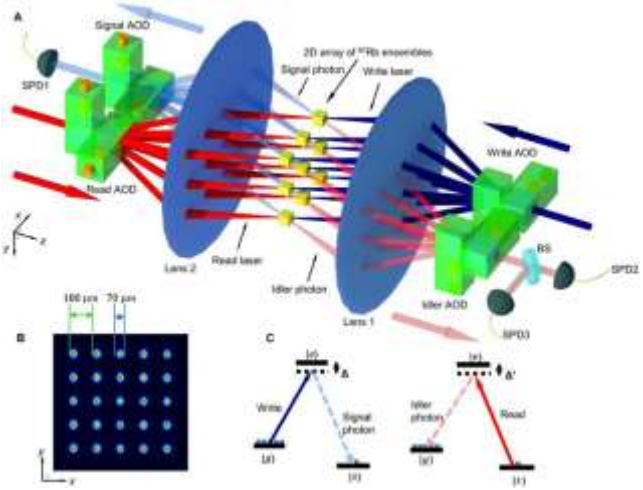
Dans un tel système, plusieurs ions sont piégés de manière équidistante les uns des autres. Ils sont généralement alignés en rang d'oignons et confinés dans un piège magnétique et électrique.

Il est pour l'instant difficile de faire "scaler" ce genre d'arrangement au-delà d'une centaine d'ions. Par contre, ils présentent l'avantage de bien pouvoir être intriqués les uns avec les autres, ce qui est moins le cas des qubits à base de supraconducteurs.



Les **atomes froids** : ce sont des atomes refroidis à très basse température, en général avec des techniques utilisant des lasers et l'effet Doppler. Les atomes utilisés sont des atomes neutres (pas ionisés) et assez souvent, le rubidium, un métal alcalin. On utilise ces atomes à l'état de Rydberg, que l'on excite avec de hauts niveaux d'énergie pour les intriquer.

L'état quantique de ces atomes froids est leur niveau d'énergie. Les atomes froids servent à créer aussi bien des qubits pour ordinateurs quantiques à portes quantiques universelles ou des simulateurs quantiques analogiques. Les états de Rydberg sont notamment étudiés par l'équipe de Michel Brune et Igor Dotsenko au LKB de l'ENS à Paris. La startup française **Pasqal** planche sur cette piste. Nous examinerons son activité et sa technologie page 439. Des chercheurs chinois et américains ont à ce jour réussi à intriquer jusqu'à 25 qubits faits à partir d'atomes de rubidium[183].



Pour ce qui est du niveau atomique, les qubits à **résonance magnétique nucléaire** (NMR) ont été testés par le passé et visiblement complètement abandonnés car ils ne scalent pas du tout.

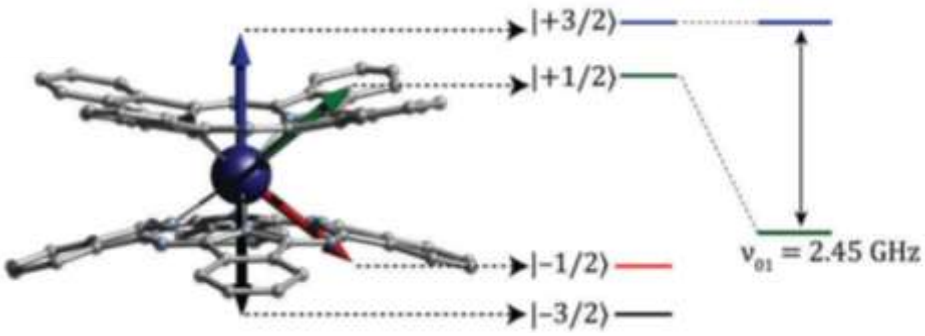
La technique des **aimants moléculaires** est aussi explorée, notamment à l'Institut Néel de Grenoble. Ils y sont fabriqués avec du terbium et ont quatre niveaux quantiques possibles. Le petit nom de ces aimants est SMM pour Single Molecule Magnets. Ils permettent donc de créer non pas des qubits mais des qudits, avec d=4, qualifiant un quantum supperposant quatre états différents. La molécule utilisée est du TbPc2 aussi dénommée bis(phthalocyaninato)terbium(III) (source).

On mesure leur état avec un interféromètre de mesure de phase. L'avantage de ces qudits est qu'ils sont très stables. L'inconvénient est qu'il est relativement difficile de les contrôler[184].

[183] Voir Experimental entanglement of 25 individually accessible atomic quantum interfaces, 2018 (11 pages) qui est la source du schéma.

[184] Voir Molecular spin qudits for quantum algorithms, 2017 (13 pages). Ces travaux sont réalisés en partenariat avec L'institut Technologique de Karlsruhe en Allemagne. Et aussi la thèse Quantum information processing using a molecular magnet single nuclear spin qudit de Clement Godfrin, 2017 (191 pages).

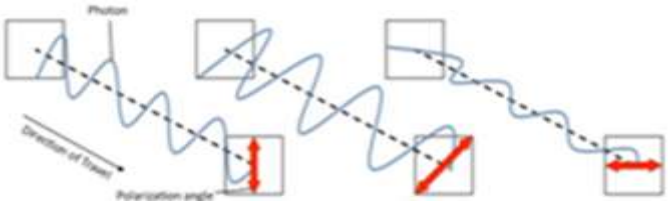
SMM en TbPc2 (terbium)
aimants moléculaires avec quatre niveaux de spin



source : Molecular spin qudits for quantum algorithms, 2017 (13 pages)

Les **photons** : leur état quantique est en général leur polarisation horizontale ou verticale. Cela fait partie du champ de l'optique linéaire. On manipule en général des photons individuels. Les portes quantiques sont réalisées à l'aide de dispositifs optiques avec des filtres dichroïques ou polarisants. L'avantage est que ces qubits fonctionnent à température ambiante, mais les sources de photons et leurs détecteurs doivent cependant être refroidis à des températures comprises en général entre 4K et 10K, ce qui est bien moins exigeant que les 15 mK des qubits supraconducteurs ou des 1K des qubits silicium.

Ce type de qubit n'est pour l'instant utilisé qu'en laboratoire et à petite échelle. Les qubits à base de photons sont dits « volants » (flying) à contrario des autres qui sont statiques. De plus, le nombre de portes quantiques enchaînables dépend du layout physique des circuits qui font circuler la lumière.

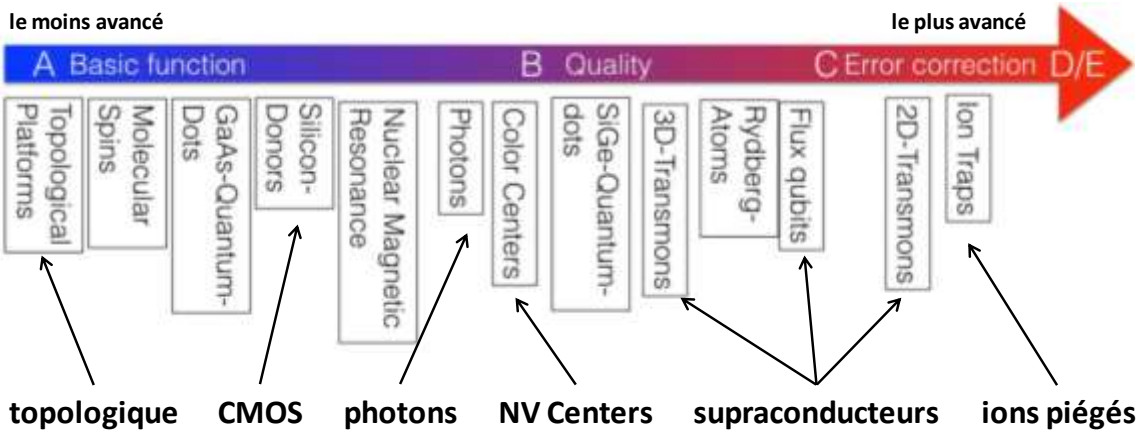


Aucune de ces techniques n'est pour l'instant éprouvée à grande échelle. Elles ont toutes leurs avantages et inconvénients qui se situent dans plusieurs dimensions :

- La **stabilité des qubits** qui s'évalue notamment par leur durée de cohérence des qubits. Associé au temps d'activation des portes quantiques et au taux d'erreur, il conditionne le nombre de portes quantiques que l'on peut enchaîner dans un algorithme.
- La **topologie de l'organisation des qubits** et la manière dont ils sont reliés entre eux, qui va conditionner pas mal de paramètres comme la vitesse d'exécution et la profondeur des algorithmes qui pourront être exploités.
- La possibilité de les **intriquer à grande échelle** et, si possible, sans être limité aux qubits immédiatement voisins.
- Le **niveau d'erreurs** dans les qubits qui s'évalue au niveau des portes quantiques à un seul qubit et à deux qubits ainsi que de la mesure en fin de calcul.
- La **température de fonctionnement** des qubits et de l'électronique d'accompagnement. Il est fréquent d'avoir besoin de réfrigérer tout ou partie de l'ensemble à des températures cryogéniques inférieures à 20 mK. Cela génère quelques inconvénients que nous verrons plus loin.
- Le **niveau de miniaturisation** des qubits et de ce qui les entoure, qui conditionne la capacité à en augmenter le nombre. Cela favorise plutôt les qubits à spin d'électrons.
- Le **processus de fabrication** qui dépend de nombreux paramètres. Dans le cas des atomes froids par exemple, il n'est pas nécessaire de créer des circuits spécialisés alors qu'il en faut pour toutes les autres technologies.

Nous verrons tout cela plus tard quand nous aborderons les différentes offres et projets d'ordinateurs quantiques.

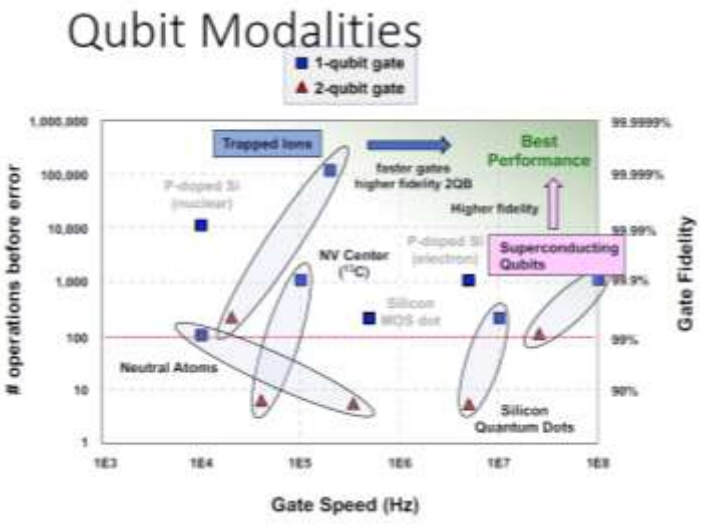
Le niveau d'avancement des qubits évolue rapidement. Il est décrit dans cet excellent document de l'équivalent allemand de l'ANSSI[185]. Il évoque d'autres technologies que celles qui sont citées dans mon inventaire et que je ne cite pas car elles ont pour l'instant peu de chances d'aboutir et n'ont été adoptées par aucun industriel ou aucune startup.



source : Entwicklungsstand Quantencomputer 2018 (231 pages)

Voici une autre manière de présenter les choses[186]. Elle segmente les types de qubits selon trois dimensions : la fréquence d'horloge des portes quantique (donc en gros, le nombre de portes exécutables à la seconde), le nombre d'opérations avant l'apparition d'erreurs et la fidélité des portes quantiques (séparant les portes à un et à deux qubits). Ces deux derniers axes sont à peu près homothétiques car le nombre d'opération avant que les erreurs soient générées dépend du taux d'erreur.

Il dépend aussi de l'algorithme utilisé ! On y voit aussi que les ions piégés ont des portes de qualité meilleure que les qubits supraconducteurs mais sont assez lents. Les qubits silicium sont pour l'instant assez rapides (a priori, ils semblent l'être autant que les qubits supraconducteurs) mais moins fidèles. Les atomes froids sont moins rapides et seraient moins fiables. Il manque un dernier axe : le nombre de qubits aujourd'hui et la capacité de la technologie à « scaler ». A noter que le tableau a été réalisé en 2019 et est donc peut-être périmé sur certains types de qubits.



Dans une partie consacrée aux acteurs du calcul quantique, nous rentrons plus en détail dans la science et la technologie des principaux types de qubits, à partir de la page 304.

[185] Voir Entwicklungsstand Quantencomputer (*état des lieux de l'informatique quantique*, en anglais, 2018 (231 pages).

[186] Voir Introduction to Quantum Computing par William Oliver du MIT, décembre 2019 (21 slides). Le schéma provient de Engineering Quantum Computers par William D. Oliver, décembre 2018 (15 slides).

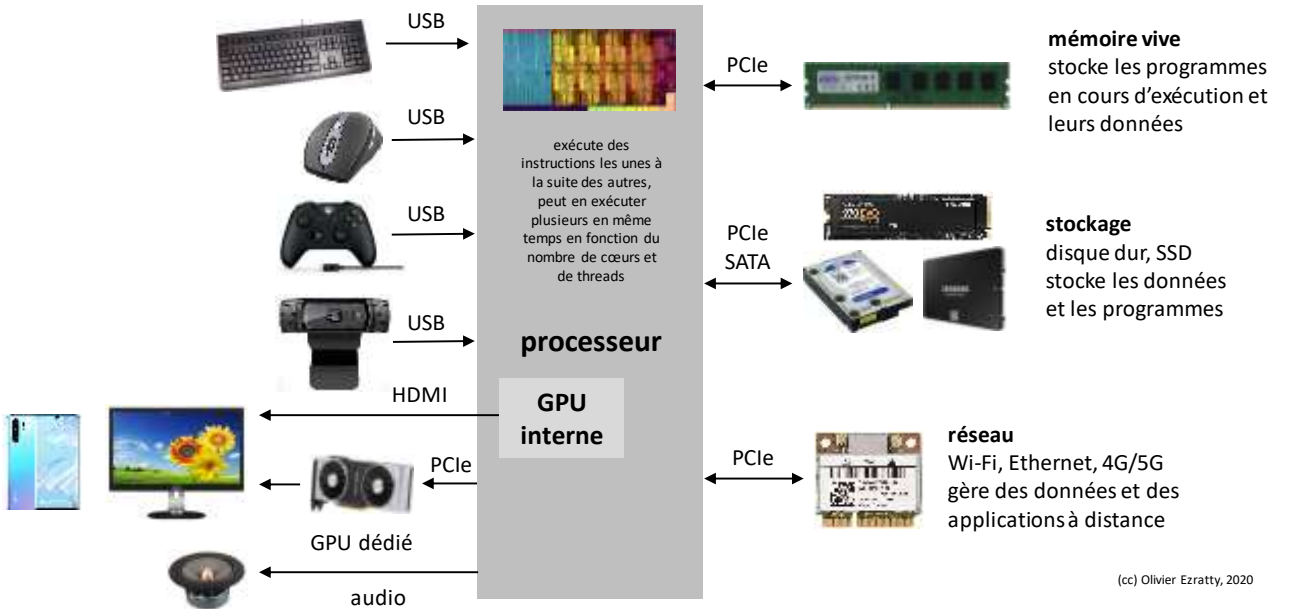
Ordinateur quantique

Après avoir décrit les principes de base de la physique quantique puis ceux des qubits, nous allons aller plus loin et décrire le fonctionnement opérationnel et physique d'un ordinateur quantique[187].

Il ne suffit en effet pas de répéter à l'envie que les qubits sont capables d'avoir à la fois la valeur 0 et 1. Il reste à comprendre comment ils sont mis en œuvre d'un point de vue pratique ! La compréhension de cette mise en œuvre est ensuite à relier aux algorithmes quantiques. Qui plus est, les architectures d'ordinateurs quantiques dépendent étroitement des caractéristiques de leurs qubits et les algorithmes utilisés ne sont pas forcément les mêmes selon ces architectures !

Certains comme le Français **Atos** ont cependant créé des outils de programmation quantiques qui se veulent indépendants des architectures matérielles. Un peu comme un compilateur C ou C++ qui peut générer du code binaire exécutable sur des processeurs différents. Cela peut fonctionner s'il existe une équivalence théorique entre les différents modèles d'ordinateurs quantiques. Il se trouve que c'est à peu près le cas donc tout va bien.

Pour être précis, dans ce qui suit, nous allons nous appuyer sur l'architecture d'ordinateurs quantiques universels à portes quantiques qui est la plus courante, celle des qubits à base de supraconducteurs à effet Josephson. Elle est notamment utilisée par IBM, Google, Intel et la startup américaine Rigetti. Une bonne part des éléments évoqués ici sont cependant applicables aux calculateurs quantiques utilisant d'autres types de qubits.



Mais avant, et comme rappel pédagogique, voici les grandes composantes d'un ordinateur traditionnel qui sont valables pour les smartphones, les tablettes, les ordinateurs personnels, les consoles de jeux et les serveurs. Le nœud gordien de l'ordinateur classique est son processeur qui est de plus en plus généraliste. Il récupère les données et programmes dans un système de stockage pour les copier en mémoire vive entièrement ou à la volée en fonction des besoins. Le processeur va ensuite lire les instructions des programmes en mémoire pour les exécuter les unes après les autres.

---

[187] J'ai consulté un très grand nombre de sources d'informations pour réaliser cette partie, à la fois côté recherche et côté fournisseurs comme chez IBM ou D-Wave. A noter Quantum Computing Gentle Introduction du MIT, publié en 2011 (386 pages) qui décrit avec précision certains mécanismes des ordinateurs quantiques comme les méthodes de lecture de l'état des qubits. Il décrit aussi assez bien les fondements mathématiques utilisés dans les calculateurs quantiques. Vous pouvez aussi profiter d'une vidéo de 8 minutes d'un beau gosse américain, Dominic Walliman, qui vulgarise bien les basiques de l'ordinateur quantique !

Les données et programmes peuvent être récupérés à distance sur un réseau ou sur des serveurs distants sur Internet. L'ensemble est contrôlé par des interfaces physiques en entrée (clavier, souris, touchpad, manette de jeu, webcam, micros) et en sortie (un ou plusieurs écrans, audio). L'écran est alimenté par un processeur graphique qui est soit externe au processeur, pour les besoins de puissance comme en CAO ou pour les jeux vidéo, ou intégré au processeur comme c'est le cas pour tous les processeurs Intel de laptops et desktops.

Selon les configurations, le processeur est entouré d'un nombre plus ou moins grand de composants externes qui sont intégrés dans la carte mère. C'est le cas du chipset Z390 d'Intel qui complète les processeurs Core et gère une bonne part des entrées/sorties de l'ordinateur. Les modems Wi-Fi et cellulaires sont associés à des antennes. Il faut évidemment ajouter une alimentation interne et externe et une batterie pour les dispositifs mobiles.

Du côté thermique, c'est le processeur et le GPU qui chauffent le plus dans cet ensemble et qui requièrent une forme de refroidissement. Dans les systèmes embarqués comme dans les smartphones, celui-ci se fait par conductance de la chaleur et par air. Dans les PC, c'est complété par un ou plusieurs ventilateurs. Dans les cas les plus extrêmes, on utilise un circuit d'eau comme caloriporteur pour améliorer le dégagement de chaleur.

L'une des raisons du dégagement de cette chaleur est l'aspect non réversible des traitements des processeurs classiques. Nous verrons plus loin que les portes quantiques des processeurs quantiques sont réversibles ce qui modifie favorablement l'équation énergétique !

Paramètres clés

Avant de désosser un ordinateur quantique type, faisons un détour par la définition des paramètres clés de performance des ordinateurs quantiques. La plus connue est celle de **David DiVincenzo**, crée en 2000 alors qu'il était chercheur chez IBM. Il est maintenant enseignant chercheur à l'Université d'Aix la Chapelle en Allemagne[188].

Alors que les qubits individuels existaient à peine, il définissait les caractéristiques techniques de base d'un ordinateur quantique à portes universelles comme suit :

- Des **qubits bien caractérisés** : l'ordinateur quantique utilise des qubits qui exploitent des particules élémentaires pouvant avoir deux états distincts et mesurables. On en connait bien les caractéristiques physiques. L'architecture est scalable au sens où elle permet d'aligner un grand nombre de qubits en batterie.
- Des **qubits initialisables** : en général, à la valeur $|0\rangle$ appelée souvent "ground state" pour les quantums associés, correspondant, par exemple, au niveau d'énergie le plus faible d'une particule élémentaire, d'une quasiparticule ou d'un atome artificiel comme pour les qubits supraconducteurs.
- Des **temps de cohérence** largement supérieurs au temps d'activation des portes quantiques. Le temps pendant lequel les qubits sont en état de cohérence (superposition d'états, pas d'écrasement intempestif de l'état des qubits sur les états de base, qubits intriqués) doit être supérieur à la durée d'activation des portes pour que l'on puisse exécuter un algorithme contenant un enchainement suffisamment long d'un grand nombre de portes quantiques. Le ratio espéré est au moins de 1000 pour 1 pour pouvoir exécuter jusqu'à quelques centaines de portes quantiques d'affilée sachant que cette quantité va intégrer les longues suites de portes quantiques utilisées par les codes de correction d'erreurs.

[188] Dans The Physical Implementation of Quantum Computation de David P. DiVincenzo, 2000 (9 pages).

- Un jeu de **portes quantiques universelles** : qui doit permettre de créer toutes les transformations unitaires possibles, notamment à un et deux qubits. Les qubits doivent pouvoir être contrôlés physiquement avec un jeu de portes quantiques jouant le rôle de portes quantiques universelles à partir desquelles on va pouvoir reproduire toutes les autres portes quantiques classiques, notamment toutes les rotations dans la sphère de Bloch. L'architecture physique des qubits conditionne la nature des portes quantiques universelles qui agissent sur les qubits. Le jeu de portes universelles exploité dans un processeur quantique n'est pas le même d'une technologie à l'autre. Par contre, un jeu de portes quantiques à un qubits permettant de créer toutes les transformations unitaires associées, complété par une porte CNOT à deux qubits, devrait faire l'affaire.
- La **capacité à mesurer l'état des qubits** à la fin des calculs, qui semble évidente. Cette mesure ne doit pas influencer l'état des autres qubits du système. Il faudrait idéalement avoir un taux d'erreur de la mesure qui soit largement inférieur à 0,1%.

critères de DiVincenzo (IBM, 2000)	**valeurs courantes**
qubits bien caractérisés	supraconducteurs, ions piégés, …
initialiser tous les qubits	à valeur 0 (ground state)
temps cohérence >> activation porte quantique	100 µs vs 10-650 ns
jeu de portes quantiques universelles	X, H, CNOT, SWAP, …
mesurer les qubits à la fin du calcul	avec erreur < 0,1%

autres critères pratiques	**valeurs courantes**
nombre de qubits	<=72 en UQ et 2048 en QA
température d'opérations	15 mK ou température ambiante

David DiVincenzo ajoutait deux autres critères optionnels qui servent plutôt aux communications quantiques :

- La possibilité de **convertir des qubits statiques** en qubits pouvant se déplacer, notamment des photons. Ces qubits mouvants sont appelés en anglais des flying qubits.
- Puis une manière de **transporter ces qubits mouvants** d'un point à l'autre de manière fiable et à distance. Cela permettra de gérer des télécommunications quantiques, des architectures distribuées de calculateurs quantiques et de mettre en place des architectures de *blind computing* permettant de distribuer des traitements en protégeant leur confidentialité. La technologie deviendra vite indispensable pour permettre la répartition de calculs quantiques sur plusieurs processeurs quantiques, un peu comme on le fait avec les chipsets multi-coeurs ou avec les architectures de répartition de traitement sur plusieurs CPU et plusieurs serveurs. Cela sera utile pour les architectures de qubits qui seront limitées en nombre de qubits par systèmes de cryogénie qui ne pourront en consolider que quelques centaines grand maximum. Il faudra donc pouvoir relier des qubits de processeurs distants pour permettre leur intrication selon les algorithmes utilisés. Différentes techniques d'interconnexion quantiques sont possibles. La plus générique est optique et elle est faiblement contrainte par la distance. A courte distance, des liaisons par micro-ondes sont envisageables, notamment pour coupler des qubits supraconducteurs[189].

[189] L'Université de Princeton associée à celle de Konztanz en Allemagne travaille de son côté sur l'interconnexion optique entre processeurs quantiques CMOS. C'est documenté dans Quantum Computing Advances With Demo of Spin–Photon Interface in Silicon, 2018. La magie consiste à transférer l'état quantique d'un spin d'électron à un photon au niveau de sa phase.

Les critères de DiVincenzo relèvent du basique. D'un point de vue pratique et opérationnel, on caractérise de manière complémentaire les ordinateurs quantiques par d'autres paramètres :

- Le **nombre de qubits** qui va conditionner la puissance de calcul. Comme celle-ci augmente théoriquement de manière exponentielle avec le nombre de qubits, c'est un paramètre clé. Aujourd'hui, on dépasse à peine les 50 qubits opérationnels de qualité. Le nombre de qubits est à évaluer à la fois dans le temps présent mais dans sa capacité à évoluer. Certaines technologies sont plus faciles à miniaturiser que d'autres. Et il faut intégrer dans cette miniaturisation à la fois les chipsets quantiques de qubits et les éléments qui les contrôlent. Aujourd'hui, les qubits à ions piégés ou en photonique scalent moyennement. Les qubits supraconducteurs scalent tout aussi moyennement. Les qubits à atomes froids scalent un peu mieux. Les qubits silicium (spins d'électrons et quantum dots) scaleraient le mieux en théorie, sachant que pour ce faire, il faudrait pouvoir les intriquer, ce qui reste encore difficile.
- La **connectivité entre les qubits** qui va conditionner la rapidité d'exécution des algorithmes quantiques. Plus cette connectivité est grande, plus rapide sera l'exécution du code. Avec une faible connectivité, le compilateur du code quantique devra multiplier les opérations pour relier les qubits entre eux d'un code, notamment des portes SWAP que nous verrons plus loin. Cette connectivité varie beaucoup d'une technologie à l'autre. Dans les technologies 2D comme avec les qubits supraconducteurs et silicium, elle est limitée aux qubits avoisinants. Elle semble meilleure avec certains types de qubits à ions piégés.
- La capacité à **paralléliser les traitements** sur plusieurs zones différentes de qubits sans perturbation qui, comme la connectivité, va conditionner la rapidité d'exécution d'algorithmes quantiques.
- La **fidélité** des qubits lors de l'exécution de portes quantiques et pour la lecture de leur état. C'est elle qui va conditionner la capacité à enchaîner de nombreuses étapes de calcul. Cela permet de qualifier la profondeur de traitements supportée.
- La **durée d'exécution** des portes quantiques et de la mesure de l'état des qubits. La première est évidemment importante pour que les algorithmes s'exécutent aussi rapidement que possible. Mais la seconde l'est tout autant car elle intervient dans les codes de correction d'erreurs et conditionne donc tout autant la durée d'exécution d'un logiciel quantique.
- La **température de fonctionnement** des processeurs et de leur appareillage qui est très dépendante du type de qubits. Le Graal est bien entendu de fonctionner à température ambiante. Les ordinateurs quantiques actuellement opérationnels, à base de supraconducteurs, fonctionnent tous à très basse température autour de 15 mK (1 mK = 1 milli-kelvin, 0 kelvin = 0 absolu étant situé à –273,15°C), mais certains types de qubits à l'état de recherche sont censés fonctionner à température ambiante, comme ceux qui sont à base de photons et les NV Centers (cavités dans du diamant dopé à l'azote). A ceci près que ce n'est pas forcément le cas de l'appareillage associé comme les générateurs et détecteurs de photons. Le fonctionnement à très basse température est un moyen de préserver la cohérence des qubits. Mais il limite la quantité d'énergie consommable autour des qubits pour en contrôler localement l'état. Un fonctionnement à 1K permet de consommer plus d'énergie pour contrôler les qubits qu'un fonctionnement à 15 mK. C'est ce qui serait possible avec les qubits silicium.
- La **consommation totale d'énergie**, que nous aurons l'occasion de creuser et qui doit être étudiée de manière globale en intégrant l'ensemble des composantes de l'ordinateur quantique : le processeur lui-même, toute son électronique de contrôle ainsi que le système de cryogénie.
- La « **rackabilité** » des ordinateurs quantiques est aussi importante pour faciliter leur déploiement dans les data-centers. Elle est notamment prévue par la startup Pasqal ainsi que pour les générateurs de photons de Quandela ainsi que pour les processeurs optiques de LightOn. Elle est associée à des questions de poids, d'encombrement, de refroidissement et d'alimentation.

Ces trois derniers paramètres opérationnels jouent un rôle lorsque l'on déploie des ordinateurs ou des accélérateurs quantiques dans un data-center.

Toutes ces considérations permettant de jauger les capacités d'un ordinateur quantique impliquent la création d'une nouvelle discipline : le benchmarking d'ordinateurs quantiques ! Elle nécessite évidemment des moyens intellectuels et physiques qui dépassent ceux du test de simples smartphones ou laptops !

Comme l'indique Kristel Michielsen[190], les benchmarks peuvent s'appuyer lorsque le nombre de qubits est inférieur à 50 à une comparaison du rendu des algorithmes entre ordinateurs quantiques et leur simulation sur supercalculateurs. Au-delà, cela sera plus difficile.

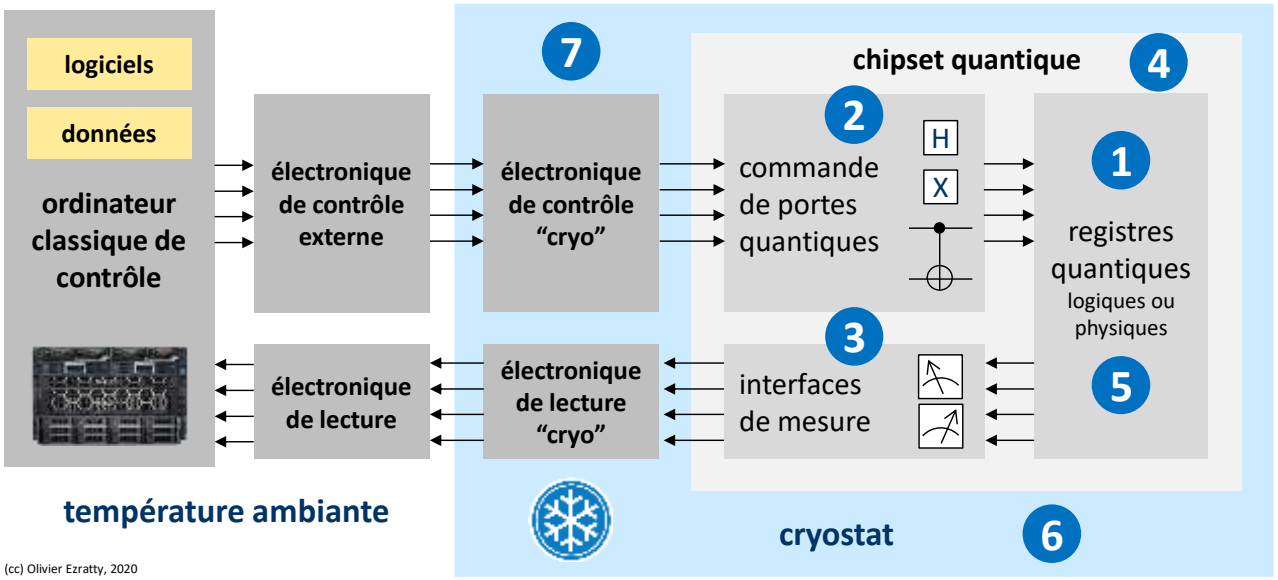
Les ordinateurs quantiques benchmarkés auront généralement des caractéristiques dissemblables : des portes quantiques universelles différentes nécessitant l'assemblage de différentes portes quantiques par les compilateurs pour exécuter un même algorithme, et des codes de correction d'erreurs différents, adaptés au taux d'erreurs des qubits et des portes quantiques des ordinateurs comparés. Les dissemblances seront bien plus importantes qu'entre deux processeurs Intel et AMD ou deux processeurs de smartphones !

Poupées russes

Nous allons démarrer ici par une vue d'ensemble de l'architecture générale d'un ordinateur quantique. Tout d'abord, un peu comme pour les GPU externes, les ordinateurs quantiques sont mis en œuvre comme des coprocesseurs d'ordinateurs traditionnels qui les alimentent. Un ordinateur quantique est toujours un coprocesseur d'un ordinateur traditionnel, comme peut l'être un GPU pour les jeux vidéo ou pour l'entrainement de réseaux de neurones dans le deep learning.

Ces ordinateurs classiques servent à exécuter les programmes destinés au processeur quantique pour les traduire en opérations physiques à réaliser sur les qubits et à en interpréter les résultats. Des données sont utilisées pour initialiser l'état des qubits.

L'ordinateur traditionnel pilote de près le fonctionnement de l'ordinateur quantique en déclenchant à un rythme précis les opérations sur les qubits qui sont réalisées par les portes quantiques. Ce déclenchement tient compte du temps d'exécution des portes quantiques et du temps de cohérence connu des qubits, c'est-à-dire, le temps pendant lequel les qubits restent en état de superposition.



[190] Dans Benchmarking gate-based quantum computers, 2017 (33 pages).

En plus de son ordinateur classique de contrôle, notre ordinateur quantique comprend au minimum les composantes labellisées de 1 à 7 que nous allons analyser une par une, d'abord avec une vue d'ensemble ci-dessous, puis avec une vue plus détaillée juste après[191]. Sachant que nous prenons ici l'exemple d'ordinateurs quantiques à base de qubits supraconducteurs ou silicium. Les autres types d'ordinateurs quantiques présentent des similitudes et des différences que nous citerons.

❶ Les **registres quantiques** sont des collections de qubits. En 2020, le record benchmarké était de 53 qubits supraconducteurs. Les registres quantiques stockent l'information manipulée dans l'ordinateur et exploitent le principe de superposition permettant de faire cohabiter un grand nombre de valeurs dans ces registres et d'opérer des opérations dessus simultanément. L'intrication des qubits contibue ensuite également à la puissance du calcul quantique.

❷ Les commandes de **portes quantiques** sont des dispositifs physiques agissant sur les qubits des registres quantiques, à la fois pour les initialiser et pour y effectuer des opérations de calcul. Ces portes sont appliquées de manière itérative, au gré des algorithmes à exécuter. Ce sont elles qui peuvent aussi servir à gérer des codes de correction d'erreurs, que nous verrons plus loin.

❸ Des **dispositifs physiques de mesure de l'état des qubits** permettent d'obtenir le résultat des calculs à la fin du processus d'exécution séquentielle des portes quantiques. On applique généralement ce cycle d'initialisation, de calculs et de mesure plusieurs fois pour évaluer le résultat. On obtient alors par moyenne une valeur comprise entre 0 et 1 pour chaque qubit des registres de l'ordinateur quantique. Les valeurs lues par les dispositifs physiques de lecture sont ensuite converties en valeurs numériques et transmises à l'ordinateur classique qui pilote l'ensemble et permet l'interprétation des résultats. Dans les cas courants, comme chez D-Wave ou IBM, le calcul est répété au moins 1000 fois dans l'ordinateur quantique. Les dispositifs de lecture sont reliés à leur électronique de contrôle via des fils supraconducteurs dans le cas des qubits d'ordinateurs supraconducteurs.

❹ Le **chipset quantique** comprend les registres quantiques, les portes quantiques et les dispositifs de mesure lorsqu'il s'agit de qubits à supraconducteurs ou à quantum dots. Les dispositifs sont plus hétérogènes pour les autres types de qubits, notamment ceux qui exploitent des lasers et des photons pour l'initialisation, les portes quantiques et la mesure des qubits. Les chipsets actuels ne sont pas très grands. Ils font la taille d'un capteur photo full-frame ou double-format pour les plus grands d'entre eux. Chaque qubit est relativement grand, leur taille se mesurant en microns alors que les transistors de processeurs modernes en CMOS ont des tailles maintenant inférieures à 10 nanomètres.

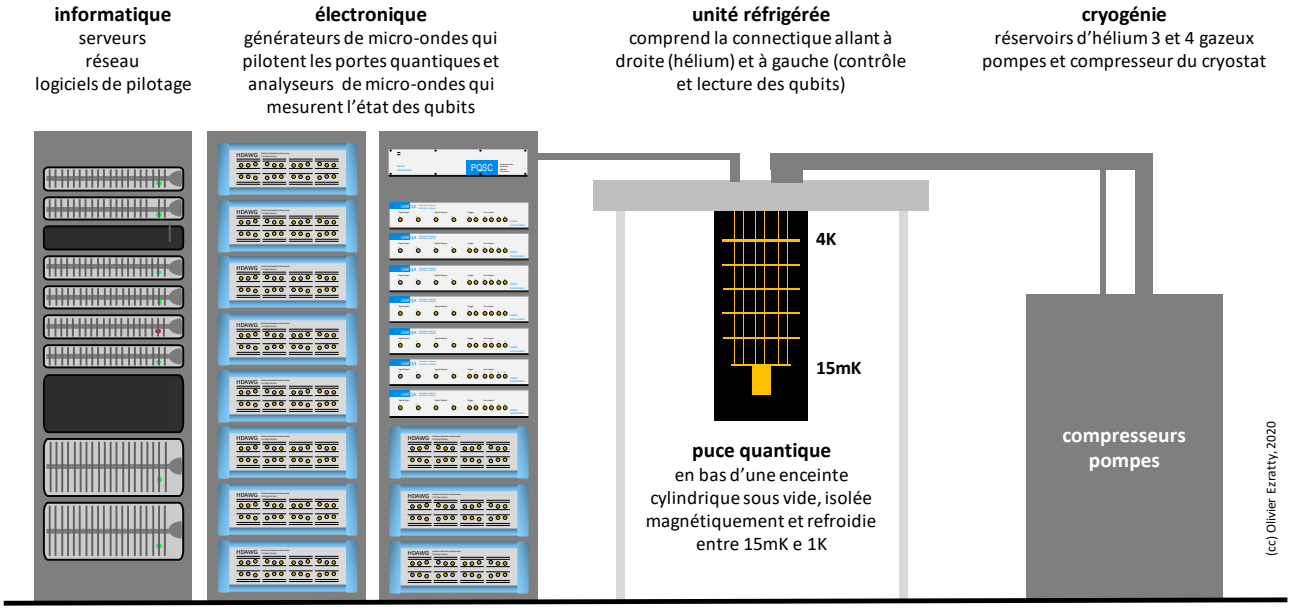
❺ Les **qubits logiques** regroupent des qubits physiques pour permettre une mise en œuvre de correction d'erreurs à l'échelle physique de l'ordinateur. D'autres méthodes utilisent des corrections d'erreurs au niveau algorithmique par l'utilisation de codes de correction d'erreurs à base de portes quantiques. La gestion des erreurs engendrées par les opérations effectuées sur les qubits est un des plus gros casse-tête de la mise au point d'ordinateurs quantiques.

❻ Une **enceinte cryogénisée** maintient généralement l'intérieur de l'ordinateur à une température voisine du zéro absolu. Elle contient une partie de l'électronique de commande et le ou les chipsets quantiques pour éviter de générer des perturbations empêchant les qubits de fonctionner, notamment au niveau de leur intrication et cohérence ainsi que pour réduire le bruit de leur fonctionnement. Le Graal serait de pouvoir faire fonctionner des qubits à température ambiante mais les architectures correspondantes comme dans les NV centers (ou cavités de diamants) ne sont pas encore opérationnelles.

[191] Pour réaliser le schéma *ci-dessus* qui explique tout cela, je me suis inspiré du slide 14 de la présentation Quantum Computing (and Quantum Information Science) de Steve Binkley, US Department of Energy, 2016 (23 slides).

❼ L'**électronique de contrôle** dans l'enceinte du cryostat. L'électronique de commande des qubits pilote les dispositifs physiques qui servent à initialiser, modifier et lire l'état des qubits. Dans les qubits supraconducteurs, les portes quantiques sont activées avec des générateurs de micro-ondes de fréquences comprises entre 5 et 10 Ghz situés en général à l'extérieur du cryostat. Ces micro-ondes circulent sur des fils électriques conducteurs entre leur source et le processeur quantique. Leurs générateurs prennent encore de la place. Ils ne sont pas très miniaturisés à ce stade, générant un facteur limitant du nombre de qubits qui sont intégrables dans un calculateur quantique. Mais comme nous le verrons plus loin, des travaux intéressants visent à intégrer ces générateurs et lecteurs de micro-ondes dans l'enceinte du cryostat, ne serait-ce que pour limiter le câblage.

Voyons donc tout cela en détail, le schéma ci-dessous étant une représentation grossière de l'ensemble d'un ordinateur quantique à qubits supraconducteurs ! L'appareillage en bleu correspond aux générateurs et analyseurs de micro-ondes d'origine Zurich Instruments dans le cas présent et qui servent à contrôler les qubits.

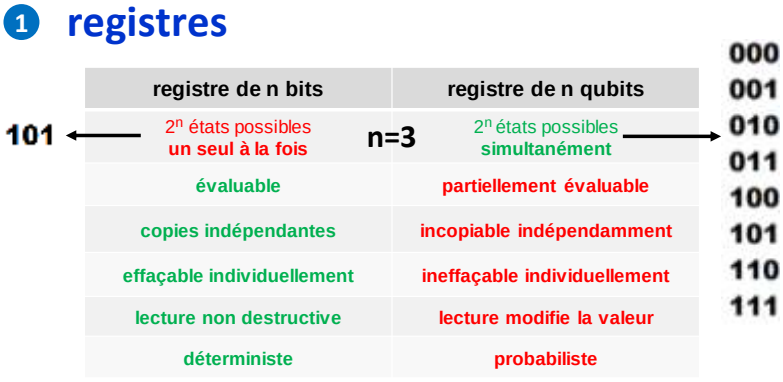


Registres

Dans un ordinateur quantique, les qubits sont organisés par blocs qui constituent des registres. Un peu comme les registres 32 ou 64 bits des processeurs classiques actuels. L'histoire ne dit pas encore si les ordinateurs de plusieurs millions de qubits utiliseront des registres de cette taille ou des registres de taille raisonnable.

Les architectures envisagées sont diverses, comme celles qui utiliseraient des registres de qubits qui seraient ensuite reliés entre eux de diverses manières, via des portes quantiques et/ou de l'intrication.

La principale différence entre un registre de n qubits et un registre traditionnel de n bits est la quantité d'information qui peut y être manipulée simultanément. Dans les ordinateurs classiques, ce sont par exemple des registres de 32 ou 64 bits qui stockent des entiers ou des nombres flottants sur lesquels sont réalisées des opérations mathématiques élémentaires.



Les qubits présentent l'avantage de pouvoir osciller en permanence entre la valeur 0 et 1, selon le principe de la superposition des états quantiques. L'oscillation est une vue de l'esprit qui ne correspond pas forcément à la réalité physique mais permet de se faire une idée conceptuelle de cette notion de superposition.

Un registre de n qubits peut donc avoir toutes les valeurs possibles à un moment donné. Pour prendre l'exemple d'un registre de 3 bits et de 3 qubits, le premier stockera une seule valeur à la fois comme 101 (5 en base 2) tandis que le registre de trois qubits va faire cohabiter par superposition toutes les valeurs possibles de ce registre, qui sont au nombre de 2 puissance 3, soient 8. C'est ce qui permet de faire des calculs à combinatoire exponentielle.

Ces 2^n états ne correspondent toutefois pas véritablement à une capacité de stockage d'information. C'est une capacité de superposition d'états auxquels on applique ensuite des traitements pour faire ressortir les combinaisons que l'on recherche selon un algorithme donné. Cela permet de tester plein d'hypothèses en parallèle pour faire ressortir la meilleure. L'information pertinente est ce résultat qui se manifeste après lecture sous la forme d'un registre classique de bits. La combinatoire de toutes les valeurs de registres pendant les calculs n'est pas une information utile en soi. C'est l'information qui en est extraite qui a de la valeur.

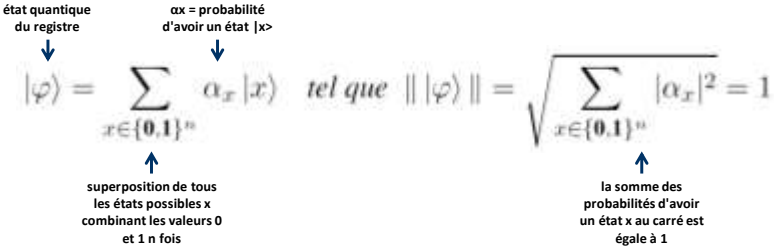
Ne croyez donc pas ceux qui vous font miroiter des applications de type "big data" grâce à la combinatoire des états des qubits. Comme cette combinatoire n'intervient que pendant les calculs et ni en entrée ni en sortie, il faut raison garder !

Si vous voyez cela dans un rapport d'analyste ou le marketing d'un fournisseur, vous serez à peu près sûr que leur auteur n'a pas compris grand-chose au calcul quantique ou tout du moins aux questions d'échelles en termes de nombre de qubits à aligner.

Qui plus est, les algorithmes quantiques ne sont dans la pratique pas efficaces pour réaliser des traitements de big data[192].

Et à supposer que cela puisse fonctionner, il faudrait prendre en compte le temps de chargement d'éventuels gros jeux de données dans les ordinateurs quantiques, qui pourraient aussi leur faire perdre leur avantage algorithmique[193].

Les états superposés des registres vérifient une loi de distribution probabiliste selon laquelle le total de la probabilité de chaque état superposé au carré est égal à 1[194]. Un calcul quantique va faire évoluer dans le temps la probabilité de chacune des combinaisons d'états de qubits (|x⟩ dans la formule *ci-contre*).



un algorithme quantique va créer un état de superposition de valeurs dans un registre quantique et va faire évoluer de poids de ces valeurs pour atténuer certaines et en faire ressortir une en particulier qui est la réponse à la question posée

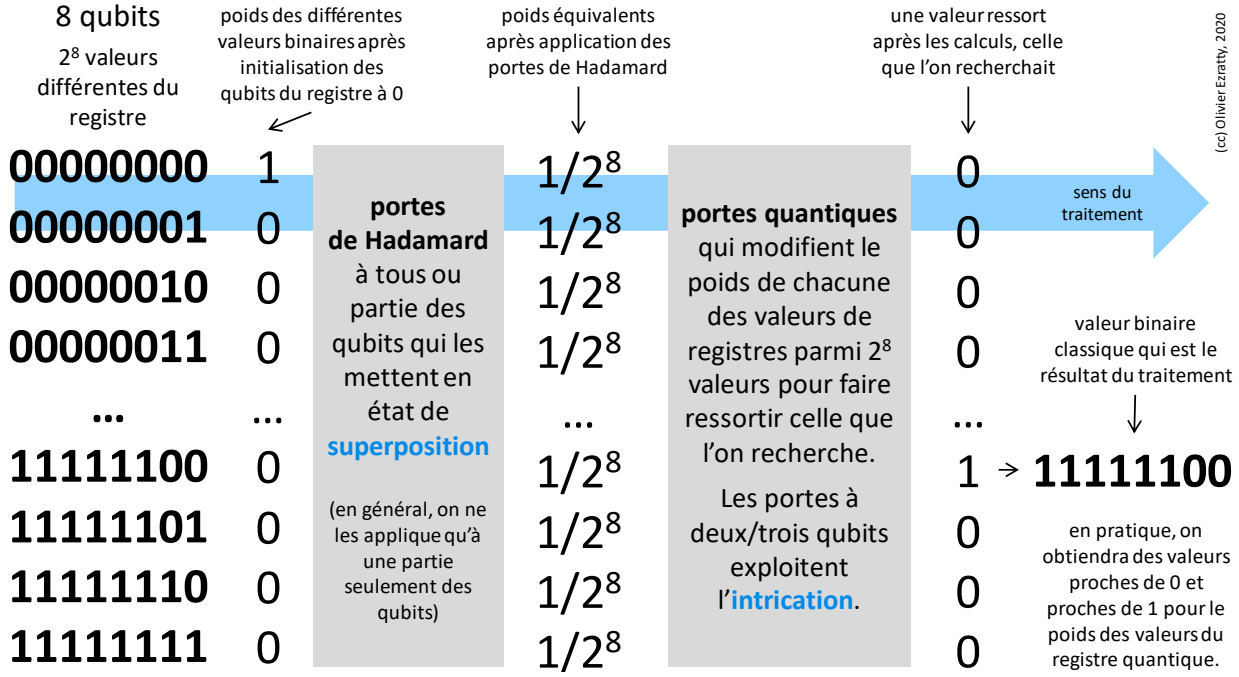
[192] Il commence cependant à apparaître des exceptions avec des méthodes hybrides d'accélération d'accès à des bases de données combinant des algorithmes classiques sur ordinateurs traditionnel et des algorithmes quantiques. Voir Quantum computers tackle big data with machine learning de Sarah Olson, Purdue University, octobre 2018.

[193] C'est très bien expliqué dans l'excellent panorama Quantum Computing: Progress and Prospects de l'académie des sciences US, 2019 (272 pages) : "*Large data inputs cannot be loaded into a QC efficiently. While a quantum computer can use a small number of qubits to represent an exponentially larger amount of data, there is not currently a method to rapidly convert a large amount of classical data to a quantum state (this does not apply if the data can be generated algorithmically). For problems that require large inputs, the amount of time needed to create the input quantum state would typically dominate the computation time, and greatly reduce the quantum advantage.*".

[194] Ce schéma est inspiré de Modèles de Calcul Quantique (30 pages), de Pablo Arrighi et Simon Perdrix, un document très bien fait qui explique avec quelques formules mathématiques pas trop compliquées comment fonctionne le calcul quantique. Il explique notamment très bien l'algorithme de Deutsch-Jozsa sur lequel je reviendrai dans la partie suivante de cette série.

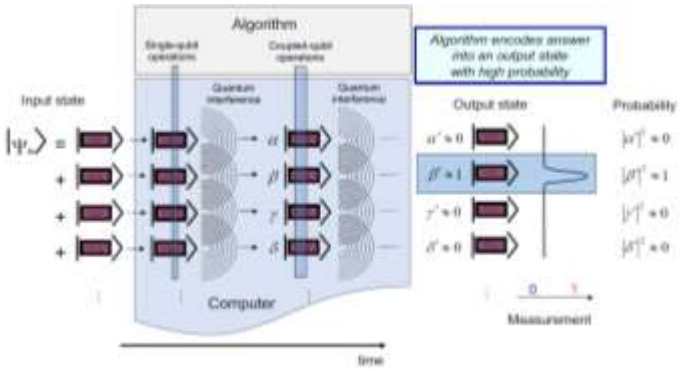
L'idée est de faire converger après plusieurs opérations la valeur du registre quantique vers la valeur recherchée que l'on lit ensuite de manière classique pour obtenir une suite de n 0 et 1 contenant la réponse. Comme par exemple un nombre premier diviseur d'un nombre entier fourni en entrée.

Ceci est renforcé par le fait que lorsqu'on lit le contenu d'un qubit, on récupère 0 ou 1 et donc une seule combinaison des 0 et 1 des qubits du registre. En le faisant plusieurs fois de suite après avoir exécuté l'ensemble de l'algorithme, on récupère un % de 0 et un % de 1. Idem pour tous les qubits d'un registre.



Voici *ci-dessus* une autre représentation graphique du principe évoqué. C'est juste pour la pédagogie car dans la pratique, on n'applique pas de porte de Hadamard à tous les qubits d'un registre et les valeurs qui ressortent ne sont pas pile poil 0 et 1 pour le poids de chacune des valeurs possibles du registre. On obtient fait généralement des valeurs proches de 0 et 1. La puissance de calcul vient dans un premier temps de la superposition puis de l'intrication[195].

Autre manière un peu plus simple et plus imagée de présenter les choses : tous les états de registres sont à gauche, le calcul génère des interférences entre ces états pour faire sortir à droite l'un des états qui est la réponse au problème posé [196]. L'exemple s'appuie sur l'utilisation de seulement deux qubits qui donnent quatre états différents « binaires » des qubits.



On ne récupère donc pas 2^n valeurs dans la pratique, mais n bits. On peut répéter l'opération plusieurs fois pour obtenir une moyenne sous forme de nombres flottants. Mais cela dépend des algorithmes. Pour la majorité d'entre eux, une information binaire en sortie est suffisante comme pour l'algorithme de factorisation de nombres entiers de Peter Shor.

---

[195] Dans A quantum computer only needs one universe par Andrew Steane, 2003 (10 pages), ce dernier insiste sur le rôle clé de l'intrication. Il juge que la superposition n'explique pas tant que cela le gain de puissance du calcul quantique.

[196] Voir Introduction to Quantum Computing par William Oliver du MIT, décembre 2019 (21 slides).

On est de toutes manières contraint par le **théorème de Holevo** de 1973 qui prouve qu'avec n qubits, on ne peut pas récupérer plus que n bits d'information après un calcul quantique (source) !

Au stade actuel de mise au point des qubits, leur taux d'erreur est situé aux environs de 0,5% environ et il faudrait idéalement qu'il soit de 0,01% voire 0,0001%. Ce taux d'erreur s'évalue d'ailleurs au niveau de la stabilité de chaque qubit pris isolément et des opérations de portes quantiques portant sur deux qubits. La superposition des valeurs dans les registres quantiques est préservée pendant les opérations de portes quantiques qui présentent la particularité de ne pas faire sortir les qubits de leur état de superposition. Seule la mesure le fait. C'est la magie des algorithmes quantiques que de l'exploiter pour faire ressortir à la fin le résultat recherché. Vous suivez ?

Cela ne présente donc pas grand intérêt de comparer l'énorme combinatoire des registres qubits avec le nombre de particules dans l'Univers comme certains le font souvent. Ce ne sont pas des données équivalentes. Une combinatoire d'états n'est pas homothétique avec un nombre d'objets.

Avec un nombre d'objets donné, la combinatoire de ces objets représentera toujours un nombre largement supérieur au nombre d'objets pris en référence. Imaginez donc la combinatoire pour positionner dans l'espace toutes les particules élémentaires de l'Univers !

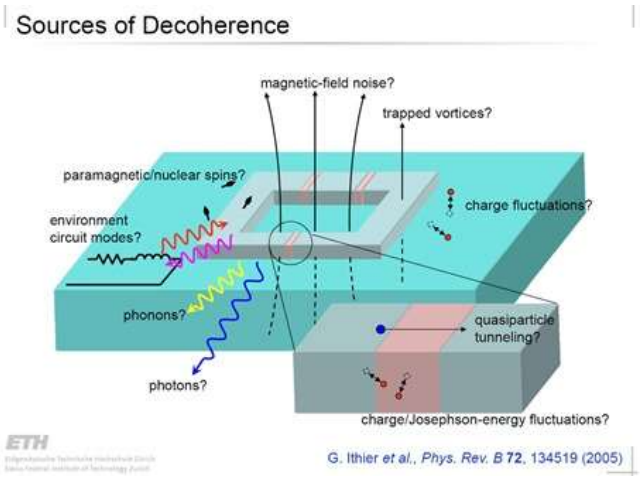
Par contre, sorti de cette combinatoire, les qubits ont plein d'inconvénients en opposition totale avec les bits classiques. On ne peut ni copier classiquement ni effacer individuellement la valeur des qubits lorsqu'ils sont ensuite intriqués entre eux. Leur mesure les modifie. Ce sont des objets probabilistes délicats à manipuler. Par contre, sans en connaître la valeur interne (le fameux vecteur représenté par la sphère de Bloch vue dans la partie précédente), on peut agir dessus avec des portes quantiques, que l'on va voir juste après.

Un qubit est cohérent lorsqu'il est bien en état de superposition entre les deux niveaux possibles du qubit physique. Le temps de cohérence est une indication de la durée pendant laquelle les qubits d'un registre restent cohérents, donc en état de superposition.

Pour être précis, le temps de cohérence est celui au bout duquel les qubits perdent leur cohérence. Il se mesure généralement avec deux paramètres :

- **T1** pour la fin de cohérence liée à une perte d'amplitude (« energy relaxation »).
- **T2** pour un déphasage, à savoir une rotation autour de l'axe z dans la sphère de Bloch.

Lorsque l'on effectue une mesure de l'état d'un qubit, on provoque sa décohérence puisque la mesure amène le qubit dans l'un de ses deux états de base possibles, en supprimant la superposition. D'autres événements physiques peuvent provoquer cette fin de superposition, ou décohérence. Ils proviennent du "bruit", des chocs entre atomes et autres perturbations physiques[197]. On y voit notamment évoqué le bruit magnétique, ce qui explique pourquoi D-Wave isole ses enceintes d'ordinateur quantique avec 16 couches métalliques pour limiter l'impact du magnétisme terrestre sur ses qubits.



[197] Voici un petit inventaire des sources de bruit pour ce qui est des qubits supraconducteurs. Le schéma de cette page est issu de la présentation Sources of decohence, de l'ETH Zurich, 2005 (23 slides).

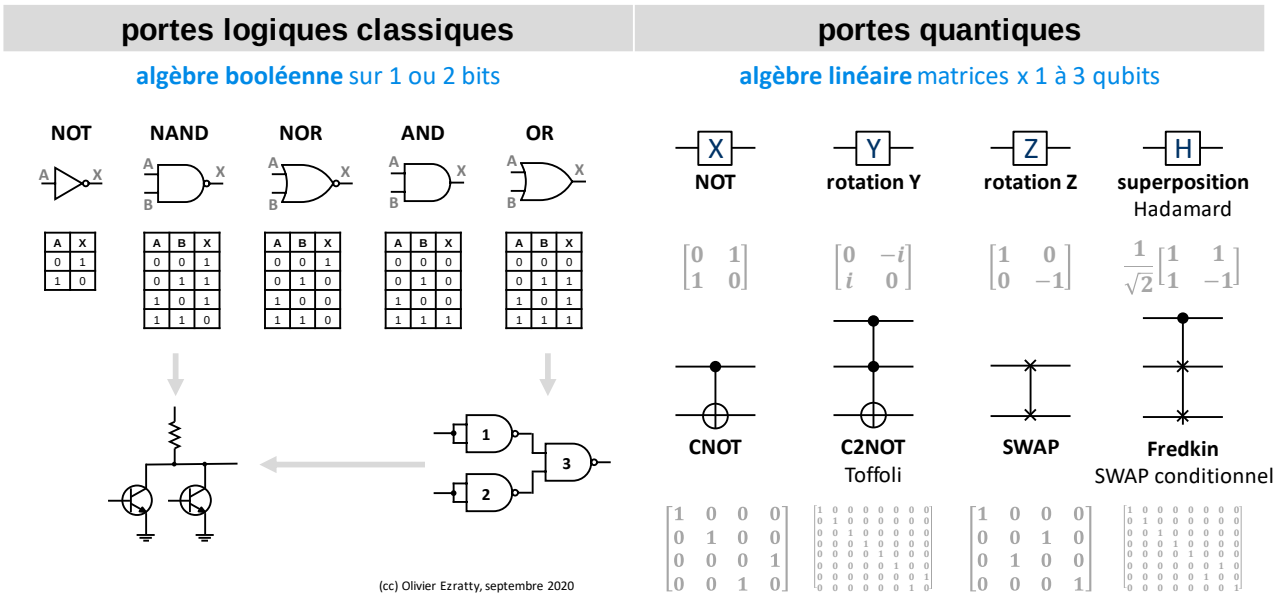
La gravitation tout comme les fluctuations quantiques du vide contribuent aussi à la décohérence des qubits[198]. On évite une partie de ces effets en refroidissant les qubits à une température proche du zéro absolu, mais ce n'est pas suffisant. Les chercheurs travaillent donc d'arrache-pied pour faire en sorte que le temps de cohérence des qubits soit le plus long possible et que le bruit qui affecte les qubits le plus faible possible.

C'est une situation paradoxale : les qubits restent cohérents, donc en état de superposition, si on ne les dérange pas, mais on passe son temps à les déranger avec les opérations des portes quantiques qui agissent dessus ! En termes physiques, on veut donc en obtenir le beurre et l'argent du beurre !

Portes

Dans l'informatique classique, les portes logiques exécutent de l'algèbre booléenne exploitant des tables de décision dépendant des bits en entrée. Plusieurs types de portes logiques à une et deux entrées sont utilisés, dont la porte NAND qui est intéressante car elle est universelle et n'utilise que deux transistors. On peut théoriquement créer les autres portes booléennes à un et deux bits avec des portes NAND. En général, les portes logiques sont cependant panachées dans les circuits.

Un processeur **Intel** Core i5/7 avec environ 5 milliards de transistors va comprendre aux alentours d'un milliard de portes logiques. Un processeur est évidemment très complexe avec des portes qui gèrent l'accès à une mémoire cache et aux registres et la lecture de programmes qui définissent les portes à utiliser dans les calculs. A partir de là, on peut presque tout faire ! Ces opérations sont générées à la fréquence d'horloge du processeur, exprimée le plus souvent en GHz. Les portes logiques classiques à deux bits (NAND, NOR, XOR, AND, OR) sont irréversibles car elles détruisent de l'information lors de leur exécution.



Les qubits qui stockent chacun un vecteur à deux dimensions subissent de leur côté des opérations via des portes quantiques appliquables à un seul ou à plusieurs qubits. Les portes à un qubit appliquent des opérations d'algèbre linéaire sous forme de matrices 2x2 de nombres réels et complexes comme représentées *ci-dessus*. Ces portes sont parfois dénommées « unaries » (unary) dans la littérature anglophone.

Les portes quantiques modifient l'information des qubits sans la lire. Elles ne sont pas destructrices de l'état des qubits ou de leur cohérence contrairement aux systèmes de mesure qui interviennent en fin de calcul. Tout du moins, en faisant abstraction du bruit qui les affecte.

[198] Voir notamment Gravitational Decoherence, 2017 (78 pages).

Les portes quantiques sont dites unitaires car elles appliquent des transformations matricielles unitaires à l'ensemble des qubits sur lesquelles elles portent. Dans les portes à un seul qubit, les vecteurs à deux dimensions représentant l'état des qubits sont multipliés par des matrices unitaires 2x2 qui provoquent une rotation du vecteur représentant la valeur du qubit en état de superposition dans la sphère de Bloch. La norme du vecteur reste stable, à 1.

Voici les principales portes quantiques utilisées côté programmation :

- Porte **X (**ou NOT) **:** réalise une inversion (bit flip). Un |0⟩ devient un |1⟩ et réciproquement. Mathématiquement, elle intervertit le α et le β du vecteur à deux composantes qui représente l'état du qubit. Elle génère une rotation de 180° dans la sphère de Bloch autour de l'axe X.

  Cette porte est souvent utilisée pour initialiser à |1⟩ l'état d'un qubit en début de processus qui est par défaut initialisé à |0⟩.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Porte **Y** : réalise une rotation de 180° autour de l'axe Y dans la sphère de Bloch.

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

- Porte **Z** : applique un changement de signe sur la composante β du vecteur du qubit, soit une inversion de phase et une rotation de 180° par rapport à l'axe Z. Les portes X, Y et Z sont dites **portes de Pauli**[199].

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Porte **S** : génère un changement de phase, ou une rotation d'un quart de tour autour de l'axe Z (vertical). C'est l'équivalent d'une demi-porte Z. Aussi appelée « phase gate ».

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

- Porte **T** : équivalent d'une demi-porte S, qui génère un changement de phase d'un huitième de tour. Avec deux de ces portes, on génère une porte S. Cette porte qui ne fait pas partie du groupe de Clifford (défini … plus tard) a la particularité de permettre par intégration multiple dans une série de portes de permettre la création de n'importe quelle position du qubit dans la sphère de Bloch.

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

- Portes **R** à changement de phase (Phase shift) : ce sont des variantes des portes de Pauli, avec des rotations différentes du demi ou quart de tour dans la sphère de Bloch, utilisant un angle arbitraire. La porte R_z tourne autour de l'axe z, la R_x autour de l'axe x et R_y autour de l'axe y[200].

$$R_m = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^m}} \end{bmatrix}$$

  Lorsque les axes x, y et z ne sont pas précisés, il s'agit de z, l'axe vertical de la sphère de Bloch, comme dans la matrice *ci-dessus*. La rotation est réalisée sur un tour complet divisé par m. Les portes R_z modifient la phase d'un qubit et pas son amplitude. Ainsi, la mesure de son état |0⟩ ou |1⟩ n'est pas affectée par cette porte. Elle retournera les deux |0⟩ ou |1⟩ dans les mêmes proportions, avant et après l'application d'une porte R_z. Ce sont en effet les deux seuls points d'une sphère qui ne bougent pas lors d'une rotation autour d'un axe les reliant.

- Porte **H** (Hadamard-Walsh) **:** met un qubit à |0⟩ ou |1⟩ dans un état superposé "|0⟩ et |1⟩". Elle est fondamentale pour générer cette superposition d'états dans les registres que nous avons décrite dans la partie sur les registres.

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

  La porte de Hadamard est notamment utilisée pour initialiser un registre quantique afin de générer cette combinatoire de 2^n valeurs différentes cohabitant simultanément dans un registre de n qubits.

---

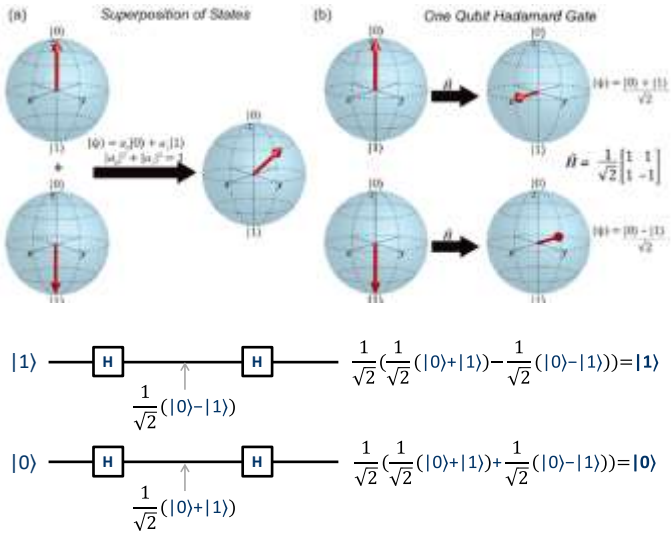
[199] Source de l'illustration : Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages).

[200] C'est bien expliqué dans The Prelude, Microsoft, 2017.

Voici une représentation de l'effet de cette porte sur un qubit initialisé à |0⟩ ou |1⟩ (source).

Notons que si l'on applique deux fois de suite une porte de Hadamard à un qubit, on revient au point de départ. En d'autres termes : HH = I (I = opérateur d'identité)[201].

Le formalisme mathématique appliqué à un seul qubit l'illustre simplement. Mais ceci fonctionne en théorie, seulement si le taux d'erreur des portes est nul. Comme il ne l'est pas, on n'obtient pas un |0⟩ ou un |1⟩ parfaits.



une porte de Hadamard chaînée deux fois régénère le même état de départ pour |0⟩ et |1⟩

Nous avons ensuite des portes à deux ou trois qubits. A part la porte SWAP et ses dérivées, ces portes sont des portes conditionnelles qui appliquent une transformation de l'état d'un qubit cible en fonction de l'état d'un ou deux qubits de contrôle. Ces portes conditionnelles mettent en œuvre le principe de l'intrication de l'état des qubits qui sont en jeu. La relation de dépendance entre les qubits concernés reste valable après l'exécution de ces portes.

- La **porte CNOT**, ou « où exclusif », qui est une inversion de la valeur d'un qubit conditionnée par la valeur |1⟩ d'un autre qubit. C'est un équivalent quantique de la porte XOR en électronique classique. Autrefois appelée porte Feynman (C).
- La **porte C2NOT** ou de **Toffoli** est une inversion de la valeur d'un qubit conditionnée par la valeur |1⟩ de deux autres qubits.
- La **porte CZ**, ou Control-Z, qui est une porte Z conditionnelle de changement de phase.
- La **porte CS**, ou Control-S, qui permet un changement de phase d'un qubit contrôlé par l'état d'un qubit.
- La **porte SWAP** intervertit les valeurs quantiques de deux qubits. Elle peut d'ailleurs être générée à partir de l'enchaînement de trois portes CNOT consécutives. Il en existe une variante dite racine carrée de SWAP ($\sqrt{\text{SWAP}}$) qui s'arrête à mi-chemin d'un SWAP. Elle est notamment envisagée dans les qubits silicium.

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

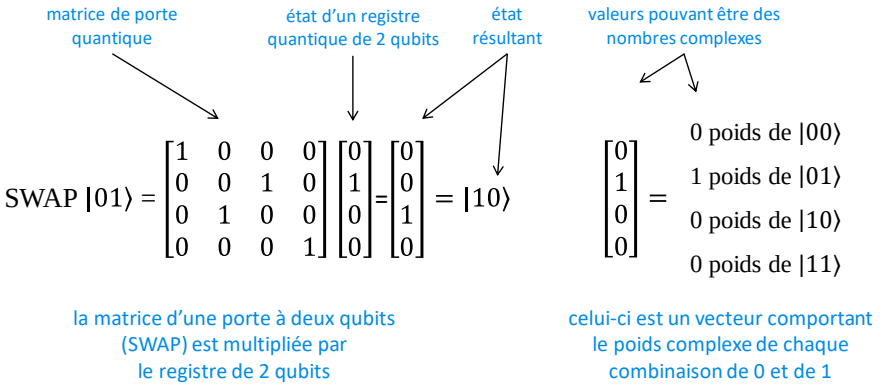
$$\sqrt{\text{SWAP}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{2}(1+i) & \frac{1}{2}(1-i) & 0 \\ 0 & \frac{1}{2}(1-i) & \frac{1}{2}(1+i) & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- La **porte de Fredkin** est une porte SWAP conditionnée par l'état d'un troisième qubit. Elle a donc trois entrées.
- Les portes **R à phase contrôlée** sont l'équivalent des portes R de changement de phase à un qubit, conditionnées par l'état d'un qubit de contrôle. Si l'algorithme, comme une transformée de Fourrier quantique, demande à ce que m soit grand, il n'est pas évident d'assurer la fiabilité de la porte car la précision demandée devient très grande par rapport aux erreurs de phase engendrées par le système quantique. Or les erreurs de phase sont difficiles à corriger ! Le record de précision d'une telle porte a l'air d'avoir été atteint par Honeywell avec ses qubits à ions piégés présentés en 2020 qui ont une précision de rotation de 1/500 tour.

[201] Dans la notation usuelle, une porte H appliquée à |0⟩ donne un état |+⟩ et une porte H appliquée à |1⟩ donne un état |−⟩.

Cela nous rappelle que pendant les opérations, le calcul quantique est analogique. Il n'est numérique qu'au niveau des commandes et des résultats mesurés, qui redeviennent des bits classiques.

Les portes à 2 ou 3 qubits y appliquent des transformations matricielles de respectivement 4x4 ou 8x8 entrées aux qubits en entrée. Soit 1 qubit = 2 nombres, 2 qubits = 4 nombres, 3 qubits = 8 nombres, la taille des matrices de transformation de l'état des qubits étant de 2 puissance le nombre de qubits transformés.



Pourquoi donc ? Parce que ces matrices s'appliquent à un vecteur dont les éléments sont chacun des états superposés possibles de la combinaison des qubits, et ce nombre d'états est 2^N, N étant le nombre de qubits.

Le calcul quantique à portes universelles fait appel à des "*ancillae qubits*" ou qubits de contrôle pouvant être combinés avec les qubits du calcul. On n'en lit pas la valeur à la fin des traitements. C'est une sorte de poubelle de qubits utilisés pendant les calculs. Ils sont utilisés dans divers algorithmes ainsi que pour mettre en œuvre les codes de correction d'erreurs (QEC) expliqués plus loin.

Les portes quantiques ont la particularité d'être logiquement réversibles. On peut revenir en arrière si bon nous chante et sans perdre d'information en appliquant dans l'ordre inverse les portes quantiques qui viennent d'être appliquées à un registre de qubits[202]. L'intérêt de la réversibilité est de ne pas consommer autant d'énergie qu'avec des portes réversibles comme dans l'informatique traditionnelle.

Mais cela dépend de nombreux paramètres et des technologies de qubits, notamment le coût énergétique du déclenchement de chaque porte quantique. Nous creuserons cette question plus avant dans la rubrique sur l'énergie du calcul quantique. C'est d'ailleurs une voie possible de réduction de consommation d'énergie pour les ordinateurs traditionnels, mais dont l'exploration est laborieuse. Il est en effet possible de créer des portes logiques traditionnelles réversibles[203] !

La notion de réversibilité d'un calcul quantique permettrait d'éviter de jeter de l'énergie par la fenêtre. On pourrait exécuter un algorithme quantique, lire le résultat de manière non destructrice si il aboutit à des qubits dans des états de base |0⟩ ou |1⟩, dite base computationnelle, puis dérouler à l'envers cet algorithme et revenir au point de départ initial… avec des qubits initialisés à |0⟩ ! Autre point à noter : elle aurait un autre impact qui serait de doubler le temps de calcul.

Le bruit quantique perturberait probablement l'opération et introduirait des erreurs mais pas suffisamment pour réduire l'impact énergétique de la méthode[204].

---

[202] Voir Synthesis and Optimization of Reversible Circuits - A Survey par Mehdi Saeedi et Igor Markov, 2011 (34 pages), qui fait le point sur l'impact algrithmique de la réversibilité, à la fois dans le calcul classique et dans le calcul quantique.

[203] Voir par exemple Generalized Reversible Computing and the Unconventional Computing Landscape de Michael Frank, 2017 (34 slides) et Foundations of Generalized Reversible Computing de Michael Frank, 2017 (18 pages).

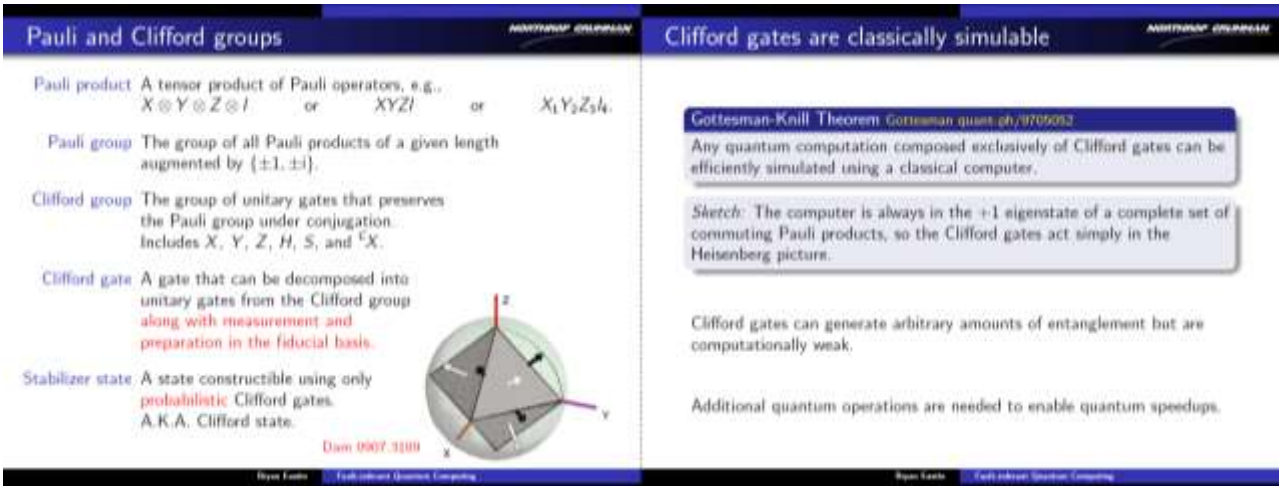
[204] Voici quelques sources d'information sur le sujet des portes quantiques qui ont éclairé ma lanterne : Universality of Quantum Gates de Markus Schmassmann, 2007 (22 slides), An introduction to Quantum Algorithms de Emma Strubell, 2011 (35 pages), L'ordinateur quantique, note de l'Ambassade de France à Washington de Daniel Ochoa et Jean-Baptiste Kempf, 2008 (70 pages), Equivalent Quantum Circuits de Juan Carlos Garcia-Escartin and Pedro Chamorro-Posada, 2011 (12 pages) et The Future of Computing Depends on Making It Reversible de Michael P. Frank, 2017.

Ceci étant dit, les qubits peuvent subir d'autres opérations. Ils peuvent être stockés en mémoire quantique comme nous le verrons plus loin. Ils peuvent aussi servir à encoder deux bits au lieu d'un seul, dans ce que l'on dénomme le « superdense coding » et que l'on utilise surtout dans les télécommunications quantiques[205].

Les mathématiques des portes quantiques ont donné lieu à la création de nombreux concepts, théorèmes portant sur des groupes de portes quantiques. Ils sont associés à la notion de **portes quantiques universelles**, capables de générer toutes les autres portes quantiques.

La classification des portes commence avec les **portes de Pauli** à un qubit qui appliquent des rotations d'un demi-tour autour des axes X, Y et Z de la sphère de Bloch de représentation des qubits.

Le **groupe de Pauli** applicable à n qubits comprend les portes issues de la combinaison de ces trois portes de Pauli et des opérations d'inversion de signe sur le α ou le β des qubits (±1 et ±i). Sur un qubit, le groupe de Pauli comprend les portes ±I, ±iI, ±X, ±iX, ±Y, ±iY, ±Z et ±iZ (I étant l'identité).



On y ajoute le **groupe de Clifford** à n qubits qui comprend les portes à un et plusieurs qubits qui normalisent le groupe de Pauli applicable à n qubits, à savoir que les portes U de ce groupe, combinées aux portes du groupe de Pauli σ avec $U\sigma U^*$ génèrent des portes du groupe de Pauli. Une porte de Clifford est une porte quantique qui peut être décomposée en portes du groupe de Clifford. Ces dernières comprennent les portes de Pauli (X, Y, Z) et les portes H, S (rotation de 90°) et CNOT (aussi appelée ^{C}X pour *controlled*-X). Le groupe de Clifford est très grand dès que n>1. Sa taille est respectivement de 24, 11 520 et 92 897 280 éléments pour n=1, 2 et 3[206].

Selon le **théorème de Gottesman-Knill**, le groupe de Clifford contient des portes simulables en temps polynomial sur ordinateurs classiques. Comment faire pour obtenir une accélération exponentielle du calcul par rapport à du calcul classique dans la mesure où le groupe de Clifford comprend déjà la porte CNOT qui est une porte à deux qubits mettant en œuvre l'intrication ?

Il faut passer par des portes à plus de deux qubits mettant en œuvre de l'intrication pour obtenir cette accélération[207]. Cela peut aussi passer par l'usage des portes R à phase contrôlée qui ne font pas partie du groupe de Clifford.

---

[205] Voir From Classical to Quantum Shannon Theory 2019 (768 pages) qui décrit l'application de la théorie de l'information de Shannong à l'informatique quantique. Ainsi que On superdense coding, août 2018, de Fred Bellaiche, un ingénieur d'Econocom qui publie de très intéressants articles scientifiques bien vulgarisés sur le quantique.

[206] Source : Clifford group par Maris Ozols, 2008 (4 pages). Clifford est le nom d'un mathématicien anglais, William Kingdon Clifford (1845-1879) qui n'est pas lié au groupe qui porte son nom.

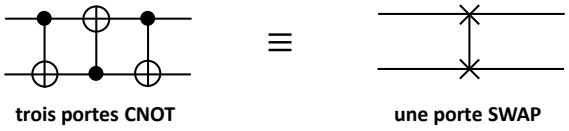
[207] Voir On the role of entanglement in quantum computational speed-up par Richard Jozsa et Noah Linden, 2002 (22 pages).

Un **jeu de portes quantiques universel** a la propriété de permettre la reconstitution de toutes les opérations unitaires sur un ensemble de qubits. D'un point de vue pratique, il permet de créer par assemblage toutes les portes quantiques connues à un, deux et trois qubits. Voici quelques jeux de portes universelles connus :

- Toffoli + Hadamard.
- CNOT + T (huitième de tour) + Hadamard.
- CNOT + S (quart de tour) + Hadamard.

Selon Artur Ekert, presque toutes les portes à deux qubits sont universelles.

La combinaison de portes universelles mises en œuvre physiquement dans les ordinateurs quantiques dépend cependant de leur type et des dispositifs physiques qui agissent sur les qubits (micro-ondes, lasers ou autres).



les portes universelles permettent de reconstituer les autres portes logiques
il en faut deux, une simple et une à deux qubits pour tout faire

On distingue des jeux de **portes discrètes** (Hadamard, Z, T, CNOT) qui ne font au mieux que des demi et des quarts de tours dans la sphère de Bloch et des jeux de **portes continues** qui permettent de générer des rotations de n'importe quel angle dans la sphère de Bloch. Ces derniers permettent de générer toutes les portes R à phase contrôlée que nous venons de voir et qui sont indispensables pour les algorithmes à base de QFT (transformée de Fourier quantique).

Cela nous amène à évoquer rapidement le **théorème de Solovay-Kitaev** selon lequel un jeu de portes quantiques dense et fini dans l'espace SU(2) permet de reconstituer n'importe quelle porte de cet espace avec un taux d'erreur maximal ε, le nombre de portes à enchaîner étant d'un ordre de grandeur polynomial de log(1/ε). L'espace SU(2) est le groupe spécial unitaire de dimension deux (**S**pecial **U**nitary group).

Il comprend les matrices unitaires (de déterminant 1) à coefficients complexes et de dimension 2.

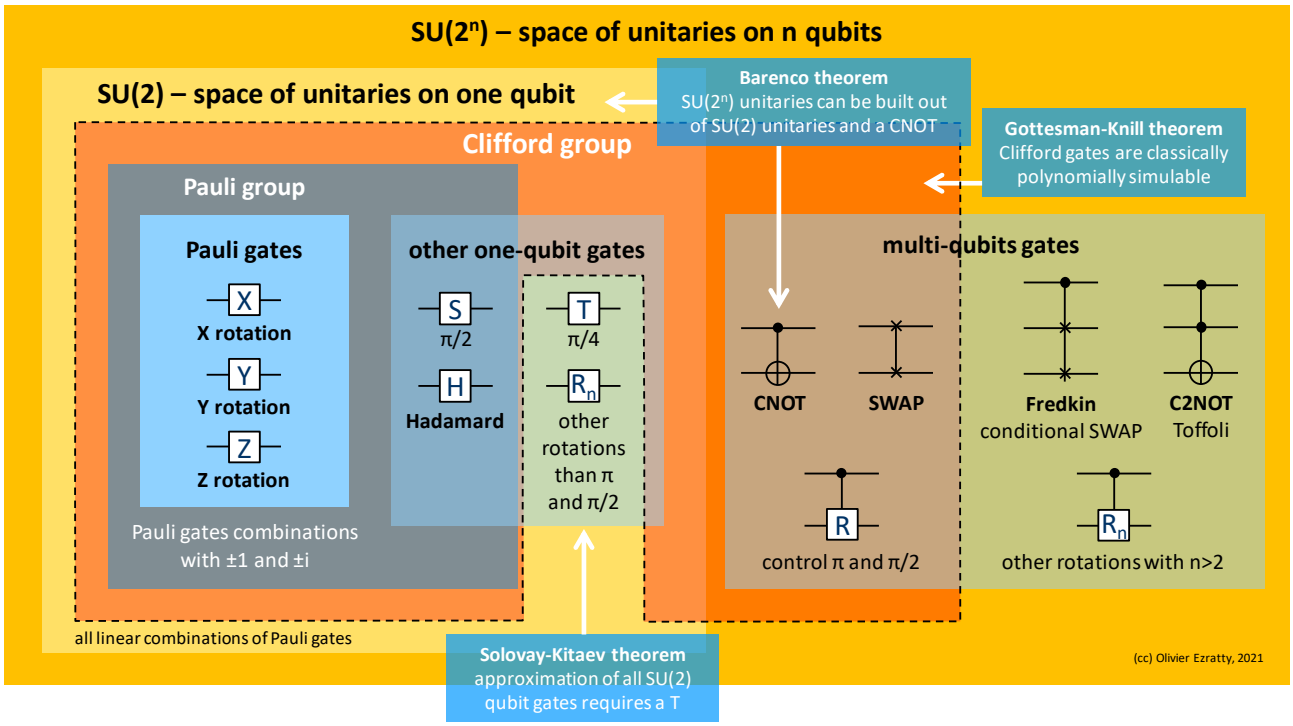
$$\mathrm{SU}(2) = \left\{ \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} : \ \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1 \right\}$$

Cette recherche d'un jeu de portes quantiques discrètes permettant par approximation de générer un jeu de portes continues de rotations arbitraires est important pour certains algorithmes que nous verrons plus loin, notamment la transformée de Fourier discrète qui est exploitée dans l'algorithme de Shor.

Voici *ci-dessous* l'effet de l'enchaînement de portes T et H qui au gré des combinaisons permettent de bien couvrir les différentes positions de la sphère de Bloch, validant le théorème de **Solovay-Kitaev**[208].

[208] Voir Non-Clifford Gates, Universal Quantum Gate Sets & the T-Operator par Francisca Vasconcelos, 2017 (5 pages et 12 slides).

Voici pour conclure cette partie un schéma maison résumant ces grandes classes de portes quantiques. En clair, SU(2^n) est l'espace des transformations unitaires opérables sur n qubits. Il couvre tous les calculs quantiques potentiellement réalisables sur n qubits. SU(2) comprend toutes les transformations unitaires réalisables sur seulement un qubit. Le groupe de Clifford comprend les portes à un et deux qubits discrètes (rotation d'un demi ou d'un quart de tour plus portes conditionnelles). Les portes T (huitième de tour) et R comme Control-R avec des angles différents de π et π/2 ne sont pas dans le groupe de Clifford. On en a besoin pour pouvoir bien couvrir SU(2) et SU(2^n). En pratique, l'ajout de la porte T suffit à créer un jeu de portes universelles.



Ces notions d'algèbre linéaire ont aussi un lien avec les techniques de correction d'erreurs du calcul quantique que nous verrons plus loin[209].

Entrées et sorties

Les microprocesseurs traditionnels sont composés de portes logiques fixes, gravées dans le silicium, et de bits 'mobiles', se présentant comme des impulsions électriques qui se propagent dans le circuit à travers les différentes portes. Le tout à une certaine fréquence, qui se compte souvent en GHz, réglée par une horloge à quartz.

Dans un ordinateur quantique, la première étape des traitements consiste à mettre le système quantique représenté par son ou ses registres quantiques dans un état initial. On dit que l'on "prépare le système". Les différents registres sont d'abord configurés physiquement dans l'état $|0\rangle$, chaque qubit étant à $|0\rangle$. L'initialisation qui suit consiste à faire agir différents opérateurs comme la transformation de Hadamard pour créer une superposition $|0\rangle+|1\rangle$ ou la porte X pour modifier cette valeur $|0\rangle$ en $|1\rangle$.

Une fois cette initialisation réalisée sont lancées séquentiellement des opérations de portes sur les qubits en fonction de l'algorithme à exécuter. Enfin, on lit la valeur des qubits à la fin des traitements, ce qui a pour effet de modifier leur état quantique.

[209] Voir Fault-tolerant Quantum Computing de Brian Easti, 2014 (55 slides), d'où proviennent les deux slides de la page précédente.

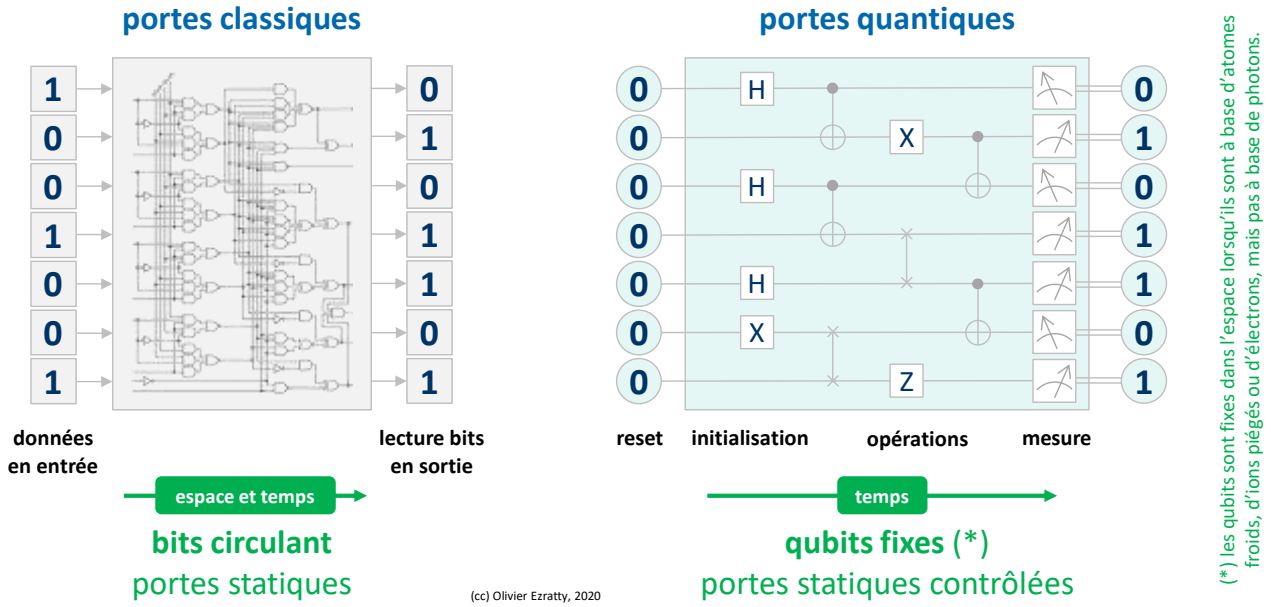
Physiquement, les qubits sont de deux sortes : stationnaires ou mouvants (flying). Ceux qui reposent sur des électrons piégés, des ions piégés et des courants supraconducteurs sont stationnaires. Les flying qubits sont à base de photons qui eux circulent physiquement de portes quantiques en portes quantiques.

Dans les cas de qubits stationnaires, les portes quantiques ne bougent pas non plus. Elles sont activées dynamiquement par des circuits électroniques ou des lasers et opèrent sur les qubits.

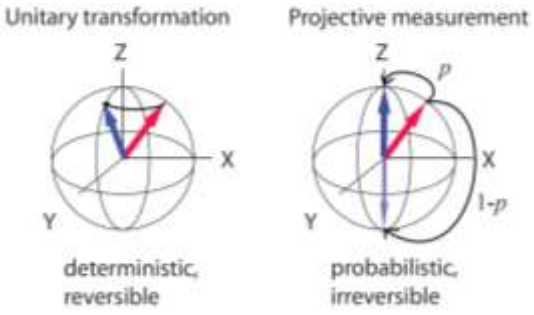
Les diagrammes de représentation des algorithmes quantiques pour ordinateurs quantiques à portes universelles (*ci-dessous* à droite) sont en fait le plus souvent des schémas temporels alors que pour les portes logiques classiques, il s'agit un diagramme physique.

J'ai mis beaucoup de temps à comprendre cela car une partie de la littérature technique sur les processeurs quantiques assimile les lignes horizontales de ces algorithmes à des "fils" reliant les qubits en entrée à des qubits en sortie, ce qui est entièrement faux.

Dans la partie droite décrivant un algorithme quantique, il n'y a pas de fils physiques reliant les qbits entre une entrée et une sortie, les portes étant sur leur chemin. C'est un schéma temporel, en tout cas pour toutes les architectures de qubits à l'exception de ceux qui exploitent des photons qui eux se déplacent dans l'espace !



Alors que les portes quantiques sont réversibles, la lecture de l'état des portes est irréversible. Ce n'est pas une rotation dans la sphère de Bloch mais une projection sur l'axe Z de l'amplitude, qui va rendre un $|0\rangle$ ou un $|1\rangle$ avec une probabilité dépendante de l'état du qubit[210]. La mesure de l'état d'un qubit modifie cet état. Il se retrouve dans l'état $|0\rangle$ ou $|1\rangle$. La mesure n'est pas irréversible dans seulement deux cas : si les qubits sont déjà parfaitement à l'état $|0\rangle$ ou $|1\rangle$.



[210] Source du schéma : A computationally universal phase of quantum matter de Robert Raussendorf (41 slides).

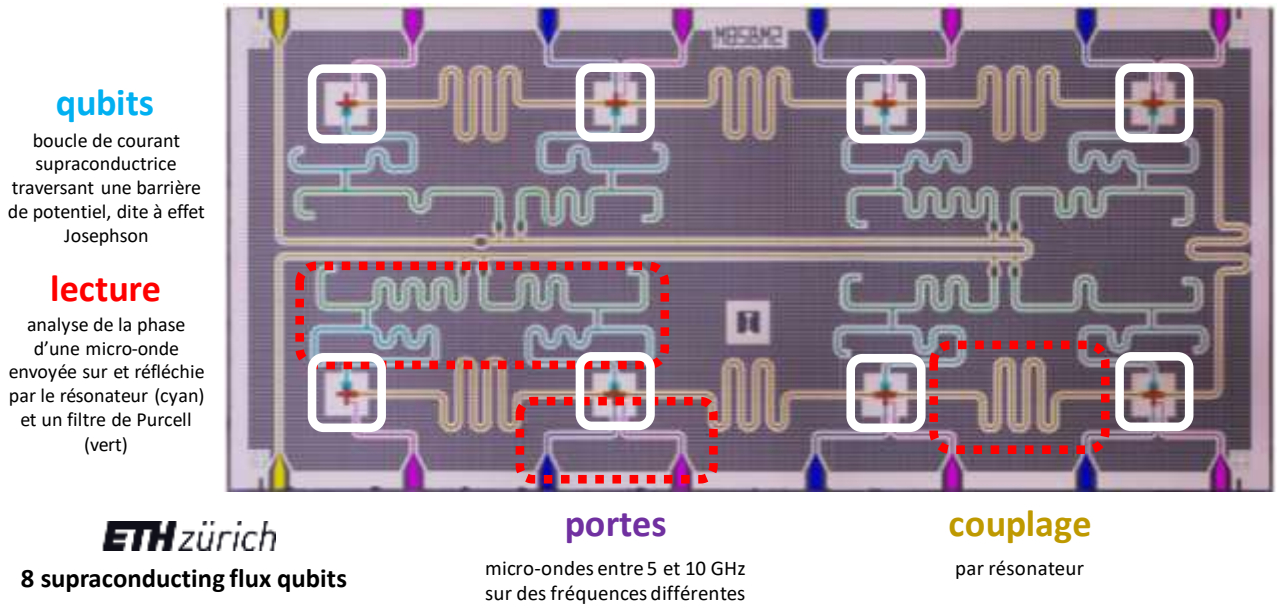
Layout physique

Pour mieux comprendre l'explication précédente, voici un *layout* de chipset de 8 qubits supraconducteurs, issu de l'ETH Zurich qui date déjà de quelques années[211].

Ce n'est qu'un exemple illustratif car les layouts physiques sont très variables d'un type de qubit à un autre. Mais le principe décrit ici est commun à tous les ordinateurs quantiques à base de supraconducteurs. L'exception qui confirme la règle est celle des ordinateurs utilisant des qubits à base de photons qui circulent – très rapidement – dans les circuits et qui traversent des portes quantiques.

On y voit que, dans le circuit :

- Les **qubits** sont situés dans les rectangles blancs. Ce sont eux qui intègrent une boucle à effet Josephson. Ils sont physiquement immobiles dans le circuit.
- Ils sont reliés entre eux par des **circuits de couplage** qui servent à contrôler leur intrication.
- Des **contacts bleus et violets** permettent d'agir sur les qubits et d'activer, selon la fréquence, des portes quantiques. Ils permettent avec le circuit d'intrication d'activer des portes universelles utilisées par combinaison pour recréer les autres portes quantiques nécessaires à l'exécution des algorithmes. Dans la pratique, avec les qubits supraconducteurs, ces "pins" sont alimentés via des câbles par des sources de courants à très haute fréquence, dites micro-ondes, comprises entre 5 et 10 GHz. Ces fréquences doivent être différentes entre les qubits adjacents d'un même circuit. C'est la combinaison de ces fréquences qui va déclencher différents types de portes quantiques et d'intrications entre qubits adjacents.
- La **mesure** a lieu avec d'autres circuits, eux aussi fixes dans le composant. Dans les qubits supraconducteurs, ce sont des magnétomètres qui sont ensuite reliés avec l'extérieur de l'enceinte sous vide et réfrigérée par des câbles supraconducteurs.



Dans un ordinateur quantique, on cherche à faire en sorte que les qubits interagissent entre eux mais le moins possible avec leur environnement jusqu'à ce que l'on mesure leur état ! C'est l'une des raisons pour lesquelles ils sont généralement refroidis à une température proche du zéro absolu et isolés magnétiquement de l'extérieur. Le choix des matériaux des chipsets joue aussi un rôle pour minimiser le bruit qui pourrait affecter les qubits et les faire sortir de leur état de superposition.

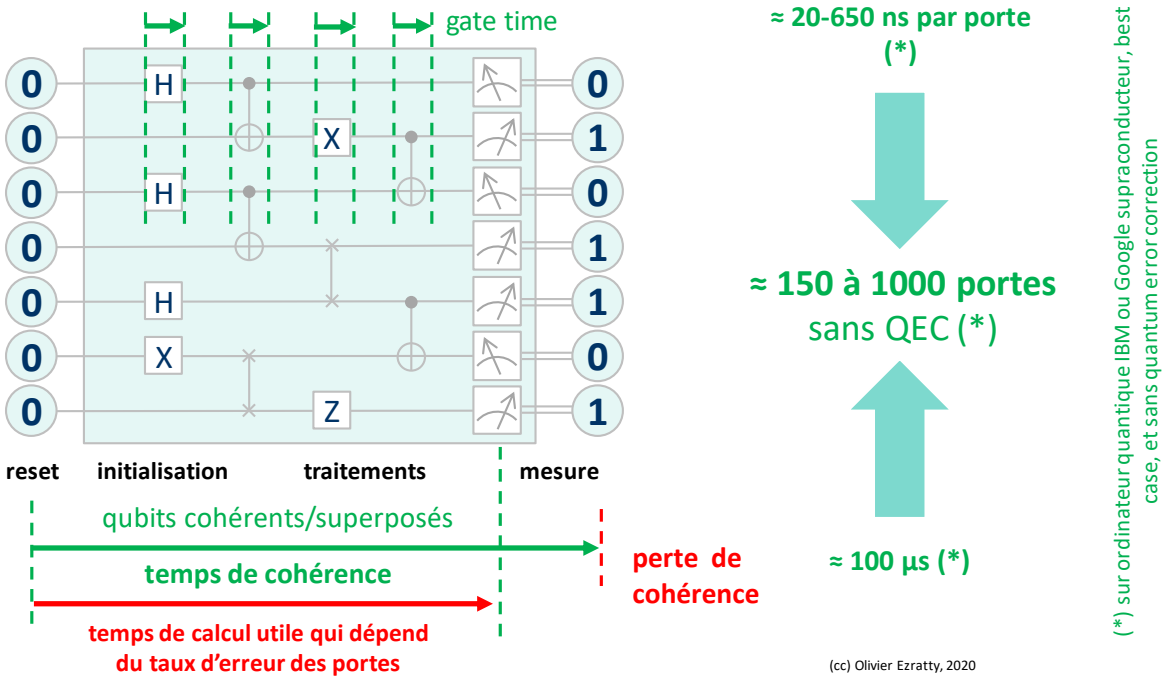
[211] Source de l'image : The European Quantum Technologies Roadmap 2017 (30 pages) et la thèse Digital quantum computation with superconducting qubits de Johannes Heinsoo, ETH Zurich, 2019 (271 pages).

Dans le schéma *ci-dessous*, voici le pourquoi du comment de la relation entre le temps d'activation des portes ("gate time") et le temps de cohérence pendant lequel les qubits restent en place et surtout, restent intriqués et en état de superposition. Et je vous passe les histoires de temps de "relaxation" après l'activation des portes.

Sachant que l'intrication ne concerne a priori qu'une partie des qubits des registres. Les ordres de grandeur de ces temps pour un ordinateur quantique classique, notamment supraconducteur, donnent au mieux un rapport de 1 à 500 entre temps de portes et durée de cohérence. Ce qui veut dire que l'on sera limité pour ce qui est du nombre de portes quantiques utilisables dans un algorithme, ce d'autant plus qu'une bonne part de ces portes sera utilisée pour les codes de correction d'erreurs. Dans les premières générations d'ordinateurs quantiques d'IBM, les portes X, d'Hadamard et CNOT duraient respectivement 130 ns, 130 ns et 650 ns.

Ces indications fournissent une limite haute du nombre de portes qui peuvent être enchaînées dans un algorithme quantique. A noter que ces temps sont plus longs pour les ordinateurs quantiques à ions piégés mais les gate time y sont aussi plus longs. Dans les qubits CMOS, les temps de cohérence sont plus longs et les gate time sont faibles.

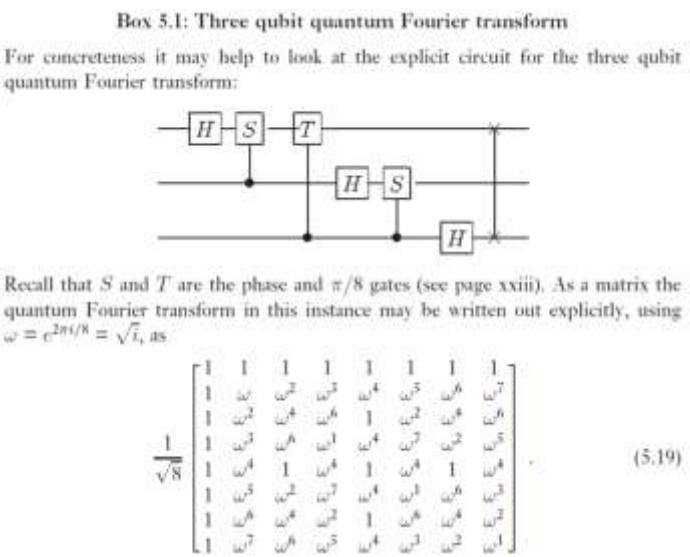
Le temps de calcul effectif est cependant souvent encore plus limité par le taux d'erreurs des portes quantiques. Il contraint ce que l'on appelle la profondeur du calcul, à savoir le nombre de portes quantiques que l'on peut enchaîner sans que le taux d'erreur des portes pollue trop les résultats. Les algorithmes doivent donc optimiser le nombre de cycles de portes à exécuter, celui-ci étant par ailleurs contraint par la connectivité physique entre les qubits.



Dans les schémas décrivant des algorithmes quantiques, comme celui *ci-dessous*, la double barre après la mesure de l'état d'un qubit indique par convention que l'on a récupéré un bit normal, à 0 ou 1. Au passage, tout ceci rappelle qu'il y a autant de qubits en sortie qu'en entrée dans un calcul quantique puisque ce sont physiquement les mêmes !

Mathématiquement parlant, une suite de portes quantiques dans un ordinateur quantique est représentable par une matrice de 2^N x 2^N nombres complexes, N étant le nombre de qubits utilisés. Elle peut être donc immense dès que N dépasse 10. Multipliée par le "tenseur" comprenant les N qubits en entrées (initialisés à 0), elle génère une combinaison de N qubits en sortie.

Le schéma *ci-contre* en est un exemple avec la matrice correspondant à un algorithme de transformée de Fourier quantique appliquée à un jeu de 3 qubits[212]. 2^3 donne 8 qui correspond aux deux dimensions de la matrice de transformation de l'algorithme. Imaginez alors la taille de la matrice pour 2^{1024} ! La taille de cette matrice devient gigantesque dès que N dépasse 50. On utilise de telles matrices dans les émulateurs d'algorithmes quantiques à base de supercalculateurs classiques. Au-delà d'une cinquantaine de qubits, la taille de la matrice devient trop grande pour rentrer en mémoire des plus grands supercalculateurs.



Box 5.1: Three qubit quantum Fourier transform

For concreteness it may help to look at the explicit circuit for the three qubit quantum Fourier transform:

Recall that S and T are the phase and $\pi/8$ gates (see page xxiii). As a matrix the quantum Fourier transform in this instance may be written out explicitly, using $\omega = e^{2\pi i/8} = \sqrt{i}$, as

$$\frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}. \quad (5.19)$$

Cela explique pourquoi les émulateurs d'ordinateurs quantiques sur supercalculateurs sont limités à environ une cinquantaine de qubits. Au-delà, la taille de la matrice à simuler est bien trop grande par rapport à la capacité mémoire de ces supercalculateurs.

On n'est cependant peut-être pas obligé de simuler une matrice entière. Il est peut-être possible de simuler en mémoire l'état du registre des qubits avec un vecteur de N fois deux nombres complexes. En fait, je ne sais pas trop !

Cryogénie

Poursuivons ce tour de l'architecture physique d'un ordinateur quantique type avec la partie cryogénie[213]. Je vais pas mal la détailler car c'est une merveille d'ingénierie et elle présente plein de ramifications techniques avec différentes composantes et capacités des calculateurs quantiques.

Lorsque l'on observe deprès un ordinateur quantique issu des grands acteurs du secteur, on y décèle un petit air de famille avec ces « chandeliers » mystérieux où est logé le processeur, entouré d'un improbable ensemble de fils dorés et de plusieurs étages de plaques circulaires en or. Il s'agit d'un assemblage des éléments d'un cryostat pour refroidir le processeur à très basse température ainsi que de câbles de contrôle et de lecture des qubits ainsi que de composants électroniques divers, passifs et actifs pour assurer ce contrôle[214].

Le technologie des qubits supraconducteurs est l'une de celles qui nécessitent de refroidir les qubits à une température aussi basse que possible pour éviter toutes les perturbations du monde extérieur[215]. L'isolation de l'ensemble doit être la plus totale au niveau de la température, du magnétisme, du vide et même des vibrations mécaniques.

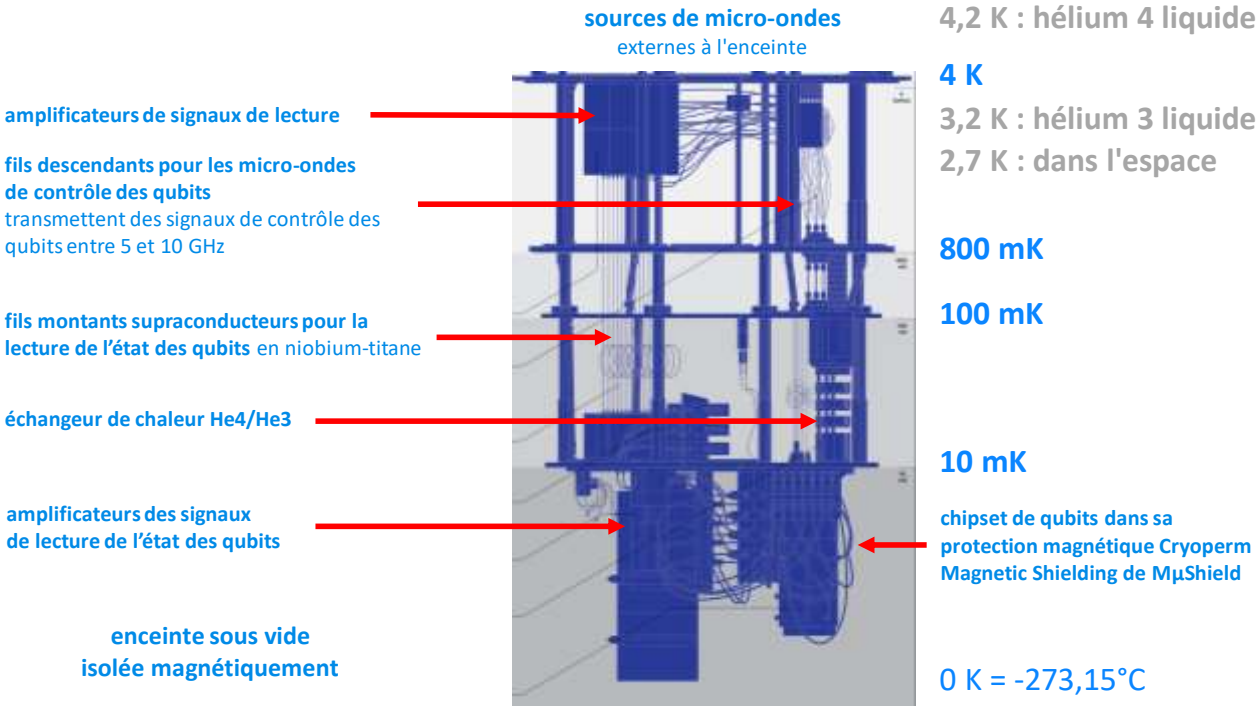
---

[212] Source du schéma : Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages).

[213] Par définition, la cryogénie opère en dessous de 123K ou -150°C. Sachant que -153,15°C est la température en-dessous de laquelle les gaz permanents, à savoir les gaz de l'air ambiant, se condensent tous en liquide à pression ambiante.

[214] Une visite du laboratoire IBM Q est disponible dans la vidéo A Tour of an IBM Q Lab qui date de 2016.

[215] Elle est régie par l'équation $k_B T < \hbar\omega$. La constante de Boltzmann multiplée par la température doit être inférieure au produit de la constante de Dirac et de la fréquence en Hz des micro-ondes utilisées. C'est ça qui nous mène à adopter une température d'environ 15 mK pour les qubits supraconducteurs.



exemple pour un ordinateur quantique à supraconducteurs IBM

le schéma *ci-dessus*, hors commentaires, est issu de Quantum Computers Strive to Break Out of the Lab, 2018.

La partie réfrigérée d'un calculateur quantique à qubits supraconducteurs ou silicum est généralement organisée par étages sachant que plus on descend dans les étages, plus il fait froid :

- Au niveau supérieur, un étage que l'on ne voit généralement pas dans les schémas et les photos et qui est à 50K. C'est par là qu'arrivent à la fois les câbles électroniques de contrôle et de lecture des qubits ainsi que les fluides utilisés pour la réfrigération.
- Un niveau en-dessous, on atteint 4K, soient 4°C au-dessus du zéro absolu (273,15°C)[216].
- L'étage du dessous est à 800 mK dans cet exemple d'ordinateur quantique IBM. Entre ces deux étages se situe la température la plus basse de l'espace qui est de 2,7 K et correspond aussi au fond diffus cosmologique, le rayonnement fossile thermique de l'Univers primordial.
- Un avant-dernier étage est généralement situé à une température de 100 mK.
- L'étage le plus bas où est situé le processeur quantique est refroidi entre 10 et 25mK, généralement autour de 15mK. On l'appelle aussi la « mixing chamber cold plate ». Une cold plate est une plaque en cuivre d'un étage et la chambre de mixage est le dernier niveau en bas du système de réfrigération à dilution que nous allons creuser plus loin[217].

Nous allons maintenant étudier les caractéristiques détaillées de la cryogénie à très basse température[218] utilisée dans ces ordinateurs quantiques.

---

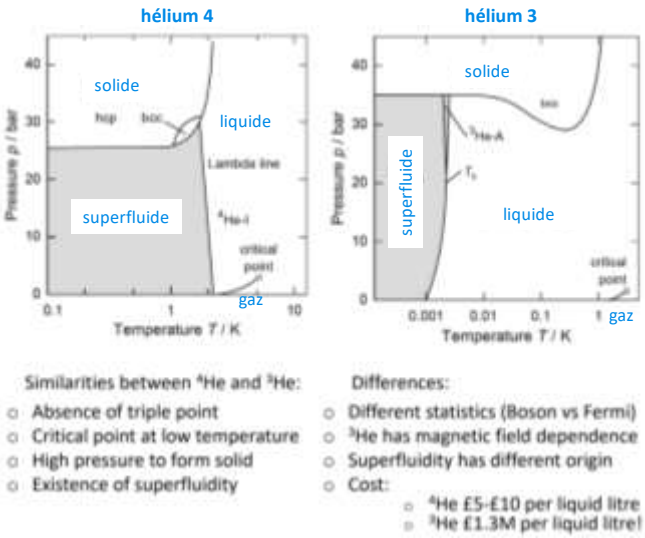
[216] L'échelle de Kelvin démarre au zéro absolu. Cette température où la matière ne bouge littéralement plus est inatteignable. On s'en approche de manière asymptotique. Le record de la température la plus basse est de 450 pK (pico-kelvins) atteinte grâce à l'étonnante technique de refroidissement d'atomes par laser et effet Doppler, déjà décrite page 68.

[217] Dans Top 5 Trends in Quantum Technologies to Look for in 2020 par QuantumXchange, janvier 2020, on trouve : "*Interestingly, IBM and Google are taking different approaches in the infrastructure of quantum computers. IBM's hardware resembles a chandelier with rings whereas the Google device looks like a chip*". Qui montre qu'ils n'ont pas du tout compris qu'IBM et Google avaient à la fois un chandelier et un chipset. Ils n'ont donc pas exploré l'architecture matérielle d'un ordinateur quantique supraconducteur !

[218] Voir Cryostats Design ^{4}He and ^{3}He cryostats par Guillaume Donnier-Valentin, CNRS Institut Néel, 2011 (91 slides), Some Fundamentals of Cryogenic and Module Engineering with regard to SRF Technology, Bend Petersen, ESY Cryogenic Group MKS (95 slides) et Development of Helium-3 Compressors and Integration Test of Closed-Cycle Dilution Refrigerator System, 2016 (5 pages).

Elle utilise la technique de la **réfrigération par dilution** qui s'appuie sur l'association de deux isotopes de l'hélium : l'hélium 4 et l'hélium 3 qui ont des propriétés différentes et complémentaires[219]. Ils ont une température d'ébullition de respectivement 4,2K et 3,2K.

L'hélium 4 est superfluide à 2,17K tandis que le 3 l'est à une température bien plus basse, de 2,5 mK (à pression ambiante). Le cryostat exploite la combinaison de trois phases : une phase gazeuse He3 et deux phases liquides, l'une en He3 et l'autre avec un mélange He3+He4, avec évaporation de l'He3 dans une zone mixte[220].



Alors que nous avons vu que l'hélium 4 se liquéfie à 4,2K à température ambiante, l'hydrogène devient liquide à 20,3K[221]. L'oxygène se liquéfie à 90,2K et l'azote à 77,4K. A noter la faible densité de l'hélium 4 qui est de 125g/L à 4,2K[222].

Un cryostat à hélium 4 peut descendre à 1K. Avec seulement de l'hélium 3, on peut descendre jusqu'à 300 mK. C'est le mix des deux qui permet de descendre à cette température de 15 mK requise pour les qubits supraconducteurs[223].

On distingue deux types de réfrigérateurs à dilution : « à sec » (dry) et « humides » (wet).

Dans les **réfrigérateurs à dilution humides**, un premier système réfrigère l'enceinte à 4K avec de l'hélium 4 liquide. Un second système dit à dilution exploite un mélange d'hélium liquide 3 et 4 avec un flux circulant dans des conduits reliant les plaques métalliques pour descendre à moins de 15 mK dans l'étage du bas.

---

[219] L'hélium a été découvert indirectement en 1868 par la découverte d'une raie spectrale inexpliquée du spectre lumineux du soleil par les astronomes Pierre Jules Janssen (1827-1907, France) et Joseph Norman Lockyer (1836-1920, Royaume-Uni). Il a été ensuite isolé pour la première fois en 1895 par le chimiste écossais William Ramsay (1852-1916).

[220] Voir cette vidéo Quantum Cooling to (Near) Absolute Zero d'Andrea Morello de l'UNSW qui explique bien le refroidissement par dilution, 2013 (10 minutes).

[221] La cryogénie à base d'hydrogène liquide utilise une autre variation, non pas isotopique de la molécule H2 d'hydrogène, mais de spin. La molécule H2 existe sous deux formes, avec les deux atomes d'hydrogène ayant le même spin (orthohydrogène) ou un spin opposé (parahydrogène). A 300K, le ratio est de 75% d'orthohydrogène et de 25% de parahydrogène. A basse température, le ratio est différent et la conversion entre orthohydrogène et parahydrogène est exothermique, servant à la réfrigération.

[222] Les schémas comparant les diagrammes de phase de l'hélium 4 (*à gauche*) et de l'hélium 3 (*à droite*) proviennent de Cryostat design below 1K par Viktor Tsepelin, octobre 2018 (61 slides). J'ai ajouté les légendes en bleu. Un diagramme de phase indique la phase de l'élément en fonction des conditions de température (en X en échelle logarithmique) et de pression (en Y, 1 bar = pression atmosphérique). On y voit que dans le régime utilisé en-dessous de 1K, l'hélium 3 est liquide et l'hélium 4 est superfluide. C'est cette différence qui permet de faire fonctionner la réfrigération à ces basses températures.

[223] La première liquéfaction de l'hélium eu lieu en 1908 à Leyden aux Pays-Bas par Kamerlingh Onnes. Le concept de cryostat à dilution a été proposé par Heinz London en 1951 et fut expérimenté en 1965 dans l'Université de Leiden pour atteindre 220 mK. La température record passait à 60 mK en 1972 puis à 1,75 mK en 1999.

Ce système était utilisé jusqu'au début des années 2000, et le relai a été ensuite pris par les systèmes à sec qui sont plus simples à opérer, notamment pour créer des ordinateurs quantiques faciles à installer chez des clients. Les systèmes à dilution humides sont toutefois encore utilisés pour diverses expériences de physique où le système à sec n'est pas approprié, mais hors calcul quantique.

réfrigération à dilution humide (wet)

peu de vibrations

plus efficace énergétiquement

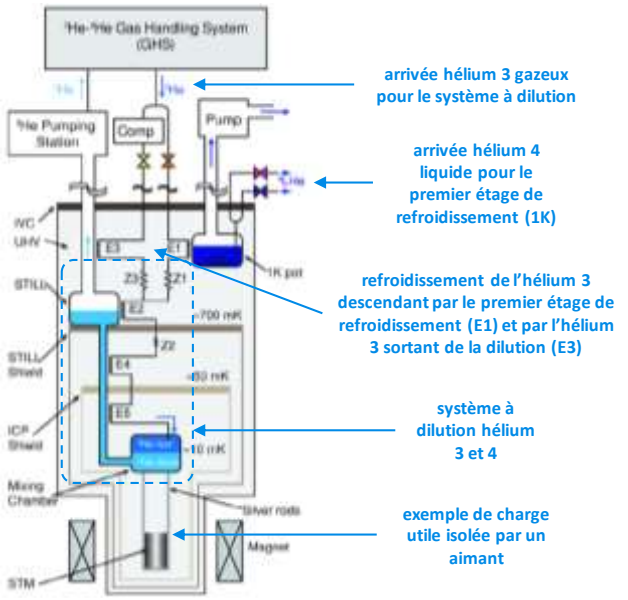
alimenté en hélium 3 et 4 liquide qui très très cher

il faut régulièrement ajouter de l'hélium 3 et 4 dans le système du fait de pertes

scellement pour mise sous vide

n'est plus utilisé pour le calcul quantique à qubits supraconducteurs ou équivalents

risques dans la manipulation de l'hélium liquide



Eviter l'usage d'hélium liquide permet au passage de plus facilement intégrer les calculateurs quantiques dans des datacenters.

Les **réfrigérateurs à dilution à sec** ou dits également cryostats sans cryogène (cryogen free) n'utilisent pas d'hélium liquide. Ils sont alimentés par de l'hélium 3 et 4 gazeux. Ils comprennent comme les systèmes humides deux étages : l'étage bas de la dilution est à peu près le même avec une détente contrôlée de l'hélium 3 qui baigne en bas dans de l'hélium 4 liquide dans une chambre de dilution. Cela couvre le refroidissement à moins de 1K.

C'est l'étage haut qui change et s'appuie sur la technique des « têtes pulsées » qui gèrent la cryogénie jusqu'à environ 4K avec du gaz d'hélium 4 et un gros compresseur externe qui est refroidi par eau. Cette technique est maîtrisée depuis une vingtaine d'années et progresse de manière incrémentale depuis. Son arrivée coïncide avec les premières expériences de qubits supraconducteurs. Les réfrigérateurs à dilution à sec sont généralement utilisés pour la cryogénie de qubits nécessitant de descendre à moins de 1K. Le schéma suivant en explique le fonctionnement si vous voulez savoir à quoi servent ses différentes composantes.

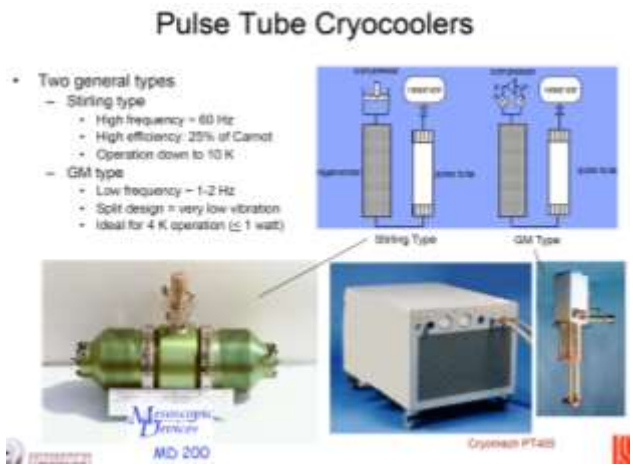
Les têtes pulsées sont associées à un système de compression et détente de type **Stirling** ou **Gifford-McMahon**. Le plus fréquemment utilisé semble être ce dernier, notamment chez **Cryo-Mech**[224]. Il utilise un piston ! Le Stirling est utilisé pour refroidir des dispositifs infrarouges mais pas pour des systèmes à dilution.

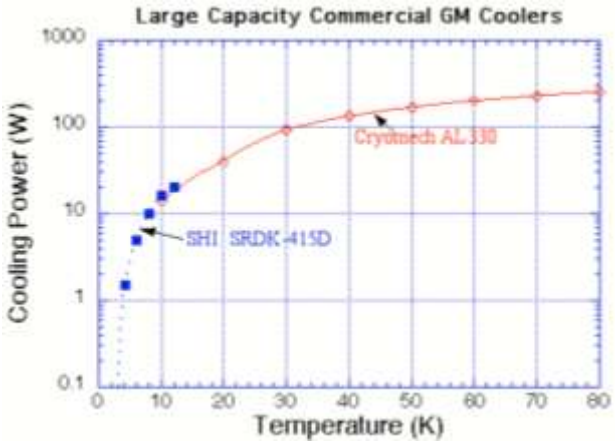
On peut observer dans la courbe à droite que la puissance de refroidissement disponible descend rapidement avec la température. Elle est située aux alentours de 1W à 4K. Les têtes pulsées permettent de descendre jusqu'à une température d'environ 2,8K. Mais aussi bien du côté de la tête pulsée que du système à dilution, aucune pièce mécanique mobile n'entre en jeu à l'intérieur du cryostat. Cela évite notamment de générer des vibrations intempestives pouvant perturber le câblage et les qubits. L'écoulement des gaz et des liquides produit très peu de perturbations au niveau de la dilution.

[224] Voir Lecture 2.2 Cryocoolers, Université du Wisconsin (25 slides) qui est la source des schémas utilisés pour décrire les systèmes Stirling et Gifford-McMahon.

Un système de réfrigération est souvent évalué en % du cycle de Carnot. Ce cycle qui date de 1824 décrit un cycle thermodynamique parfait exploitant quatre processus thermodynamiques parfaitement réversibles avec échange travail/chaleur[225]. Le rendement d'une machine thermique n'est jamais parfait, à 100% de ce cycle.

Pour une tête pulsée, un rendement parfait de Carnot serait d'environ 1,4%, à savoir qu'il faudrait 70W d'énergie pour en extraire 1W à 4,2K [226]! En pratique, on dépense environ 10 kW, soit 152 fois plus ! On obtient donc un **rendement de Carnot** inférieur à 1%. C'est <1% de 1,4% ! En effet, on dépense plus de 10 kW pour obtenir 1W de puissance à 4,2 K. Alors… à 15 mK pour obtenir 10 µW ? On n'évalue pas le rendement de Carnot de l'étage 15 mK car celui-ci fonctionne de manière isobare, soit à pression constante, le cycle thermique étant lié à une variation de phase de l'hélium 3. Celui-ci est alimenté par échanges de chaleur entre la tête pulsée et le circuit d'hélium 3 gazeux.





Il existe un troisième circuit, en rouge dans le schéma *ci-dessous* qui sert à prérefroidir le cryostat au démarrage, lors de sa mise en température. On procède en trois temps : en lançant d'abord la tête pulsée qui refroidit les étages 50K et 4K avec de l'hélium 4 gazeux et le compresseur externe d'environ 12 kW[227] (en jaune dans le schéma). Puis en utilisant le circuit de prérefroidissement qui va faire circuler un mélange hélium 3 et 4 jusqu'aux étages du bas, et qui aura été refroidit par la tête pulsée (circuit en rouge dans le schéma).

Enfin, le troisième système à dilution prend le relai du second et est lancé pour pouvoir descendre à 15 mK dans la cold plate du bas (en bleu clair dans le schéma).

En adoptant une analogie spatiale, la tête pulsée et son compresseur de 7 à 12 kW sont l'équivalent du premier étage d'une fusée Saturn V. Le système de prérefroidissement est l'analogue du second étage et le système à dilution est l'analogue du troisième étage qui envoie le module lunaire et le LEM vers la lune, mais avec une masse bien plus faible que celle de l'ensemble de la fusée et sans avoir à gérer la gravité terrestre. L'extraction de la gravité terrestre sur une grande masse est l'équivalent du refroidissement à 50K et 4K d'une grande masse métallique à l'intérieur du cryostat. Alors que le système à dilution se charge de refroidir de 4K à 15 mK une plus petite masse, la cold plate du bas et la charge utile qui lui est rattachée.

Ces systèmes sont très complexes et requièrent de l'optimisation avec un grand nombre de paramètres. La modélisation d'un cryostat pourrait d'ailleurs bénéficier un jour du calcul quantique, ce d'autant plus que les fluides utilisés sont dans un état quantique (superfluide).

---

[225] Voir Cryogenic Systems par Pete Knudsen, 2018 (71 slides) qui décrit bien le principe du cycle de Carnot.

[226] Voir Lecture 5 Refrigeration & Liquefaction (Part 1) par J. G. Weisend II (17 slides).

[227] Chez CryoMech, les compresseurs adaptés à ces systèmes à dilution consomment de 7,9 à 12kW; du PT410 au PT420. Il faut ajouter environ 4kW pour le GHS (Gas Handling System) qui gère les circuits de la dilution avec leurs pompes et contrôles ainsi que pour l'ordinateur et le tableau de bord de l'ensemble.

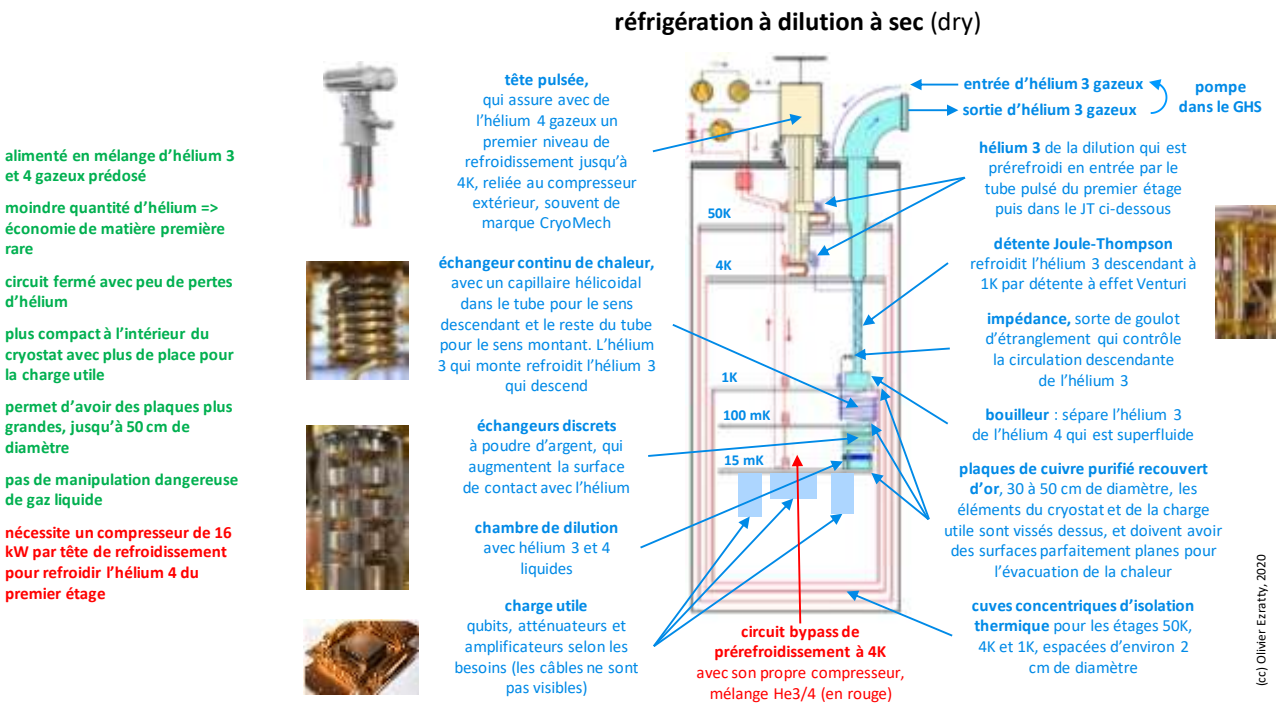


schéma trouvé dans Cryostat design below 1K par Viktor Tsepelin, octobre 2018 (61 slides), illustrations provenant de la documentation de CryoMech, de Janis, de Dry dilution refrigerator with 4He-1K-loop par Kurt Uhlig, 2014 (16 pages), The 3He–4He Dilution Refrigerator, 2012 (41 pages) et d'IBM, légendes maison.

Dans l'ensemble du cryostat, une bonne partie de la puissance est consommée pour descendre jusqu'à 1K, ne serait-ce que parce que la masse à refroidir est la plus importante. Le cylindre qui protège la partie refroidie à 4K reçoit les radiations thermiques de la partie à 50K. Cela fait une grande différence thermique à absorber.

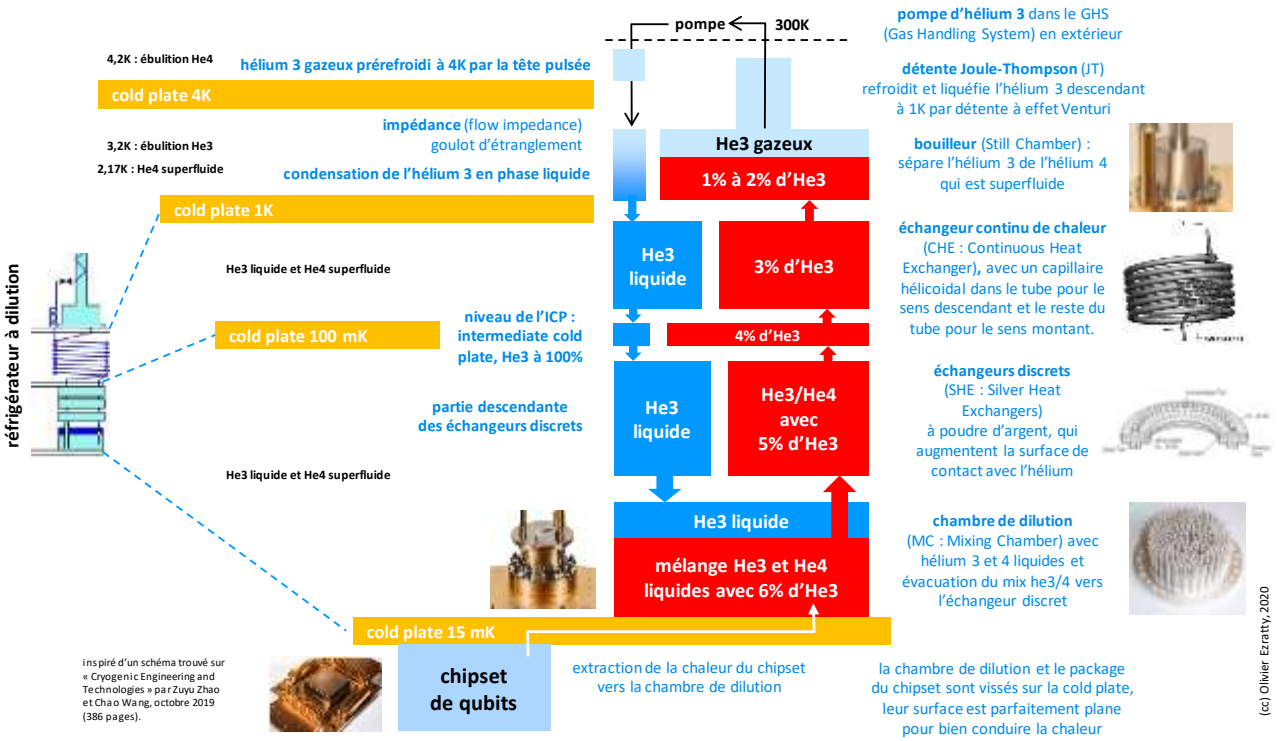
Dans un cryostat d'environ 16 kW, environ le tiers seulement de cette puissance sert au système de dilution qui sert à descendre à 15 mK. Elle correspond aux pompes du GHS, le Gas Handling System qui contient toutes les pompes et circuits de gaz à l'extérieur du cryostat, et à la part de l'énergie dépensée dans la tête pulsée qui est exploitée par le système à dilution.

Le système à dilution n'utilise pas de compresseur. L'hélium 3 qui circule à l'extérieur est juste entraîné par une pompe située dans le GHS. La raison est que l'hélium 3 qui retourne dans le cryostat est refroidi par la tête pulsée. Donc en pratique, toute la chaleur du cryostat est évacuée par le compresseur de la tête pulsée qui est lui-même refroidi par de l'eau.

Le schéma *ci-dessous* détaille le fonctionnement du système à dilution ainsi que la phase (liquide ou gazeuse) ainsi que la concentration d'hélium 3 et 4 dans chaque étage et composant. On y voit le circuit descendant d'hélium 3 qui devient liquide à partir de la condensation au niveau du bouilleur.

Dans le circuit montant à partir de la chambre de dilution (mixing chamber), c'est un mélange liquide d'hélium 3 et 4 qui monte et dont la concentration en hélium 3 descend au gré des étages. C'est seulement dans le bouilleur que l'hélium 3 devient gazeux. L'hélium 4 reste liquide et est évacué vers le bas. Il a d'ailleurs tendance à grimper par superfluidité. Une astuce permet de couper ce film ascendant et de renvoyer l'hélium 4 vers le bas.

L'hélium 3 qui arrive dans la chambre de dilution tout en bas doit y aboutit à une température à peine au-dessus de 1mK de la température de la chambre. Il est prérefroidi par l'hélium 3 qui remonte. Le seul moyen d'y arriver consiste à augmenter les surfaces de contact, ce que l'on fait dans les échangeurs discrets compris juste en-dessous de la cold plate du niveau 100 mK.



Ces cryostats à sec utilisent tout de même un cryogène, de l'azote liquide à 77K[228], qui sert à filtrer le gaz d'hélium pour lui enlever ses impuretés. Ce filtrage fait appel à de la poudre de zéolite, des cristaux microporeux d'aluminosilicate.

Le réservoir d'azote liquide qui sert à ce prérefroidissement est appelé « cold trap »[229]. Ce filtrage est complété dans l'étage 4K du cryostat par un autre système de filtrage à base de poudre de charbon actif qui fonctionne mieux à basse température et qui augmente les surfaces de contact avec le gaz pour mieux le filtrer.

En règle générale, la thermalisation complète d'un cryostat de calcul quantique dure environ 24h. L'étage dit « 1K » était en fait à environ 1,2K pour la cryogénie humide et est autour de 800 mK pour la cryogénie à sec. La puissance consommée est identique entre la phase de thermalisation et le maintient en tempéture des instruments une fois celui-ci la thermalisation achevée.

La **cryogénie à 10-20 mK** est spécifique aux ordinateurs quantiques dont les qubits doivent être réfrigérés à très basse température, essentiellement ceux qui sont à base d'électrons (supraconducteurs, NV centers, fermions de Majorana). L'état des qubits supraconducteurs est à un niveau d'énergie correspondant à 50 mK, d'où le besoin d'une température inférieure pour le capter avec un minimum de perturbations.

En théorie, les qubits silicium devraient se contenter d'un refroidissement à 1K mais pour l'instant, on les refroidit encore à environ 15mK. Une équipe australienne vient de créer un proof of concept de qubits silicium fonctionnant même à 1,5K et une autre d'Intel et Qutech à 1,1K[230].

---

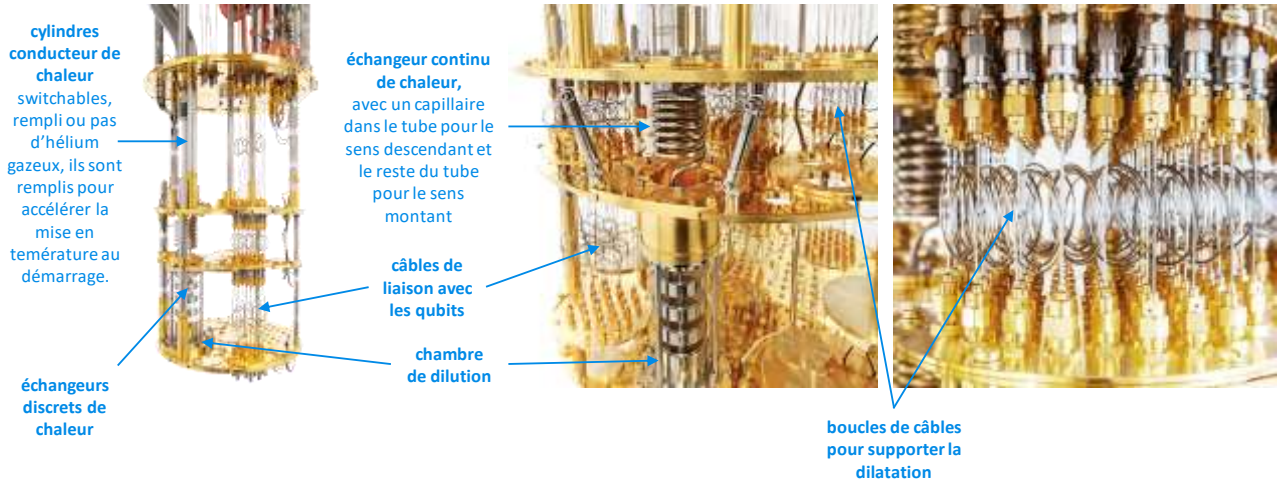
[228] LN2 pour liquid nitrogen, l'azote gazeux étant une molécule de deux atomes d'azote.

[229] De l'azote liquide est aussi parfois employé pour prérefroidir la structure métallique du cryostat lors de la mise en température. C'est sans lien avec le circuit d'hélium. Cela permet de gagner jusqu'à cinq heures pour la thermalisation du cryostat. Mais ce procédé n'est pas couramment utilisé pour les cryostats de calculateurs quantiques. Il sert au prérefroidissement de charges utiles plus lourdes pour des expériences de physique utilisant des appareillages pouvant aller jusqu'à plusieurs centaines de kilogrammes, y compris des aimants supraconducteurs. Cette technique n'est pas utilisée pour le calcul quantique.

[230] Voir Hot qubits made in Sydney break one of the biggest constraints to practical quantum computers par UNSW, avril 2020 lié à Operation of a silicon quantum processor unit cell above one kelvin par Andrew Dzurak et al, avril 2020 (dans nature) et en février 2019 sur Arxiv. Le test était réalisé sur 2 qubits avec un taux de fiabilité de porte de 98.6% assez moyen mais en ligne avec ce qui est actuellement obtenu avec des qubits silicium. Voir aussi Universal quantum logic in hot silicon qubits, 2019 (11 pages).

Pour les autres types de qubits, les besoins de réfrigération sont différents : les qubits à ions piégés ne sont pas réfrigérées en théorie mais le prototype de processeurs à ions piégés d'Honeywell annoncé début mars 2020 est refroidi à 12,6K, une température qui se satisfait de cryostats fonctionnant seulement à l'hélium 4.

Dans les processeurs quantiques à base de photons, l'optronique traversée par les photons (miroirs, prismes, interféromètres) n'est pas réfrigérée mais les sources de photons et les détecteurs de photons le sont, à des températures comprises entre 1K et 10K. La cryogénie associée est bien plus légère et consomme moins d'énergie au regard des cryostats à dilution.



détails d'un cryostat BlueFors (source), commentaires maison

A contrario, certains cryostats à sec descendent à des températures comprises entre 5 et 10 mK. Ils sont dédiés à des expériences de physique sans rapport avec le calcul quantique comme la recherche de matière noire (la détection des « WIMP », Weakly Interacting Massive Particles) et l'analyse de radiations cosmiques qui utilise des calorimètres fonctionnant entre 5 mK et 7 mK[231].

Pour obtenir des **températures encore plus basses**, de moins de 3 mK, on utilise une technique complémentaire, la démagnétisation nucléaire adiabatique (ADR ou Adiabatic Demagnetization Refrigeration)[232]. Elle n'est pas nécessaire pour le calcul quantique. On peut ajouter ce type de réfrigération à un cryostat à dilution. Le principe consiste à utiliser un sel paramagnétique qui est magnétisé avec un champ assez fort, de 6 Tesla ou plus. Cela va chauffer le sel, chaleur qui est évacuée via un bain d'hélium liquide à 4K. La suppression du champ magnétique refroidit le sel par détente. La difficulté du processus tient au cycle échauffement-refroidissement qui peut perturber l'appareillage à refroidir. On le traite en combinant plusieurs dispositifs qui se relaient pour lisser la courbe de température du système. Le procédé est éprouvé de longue date mais la puissance de refroidissement disponible est très faible.

Nous allons creuser cette technique un peu plus loin dans ce document au sujet de la startup Kiutra[233] qui utilise cette technique pour obtenir des températures plus classiques de quelques centaines de mK, l'un de ses avantages étant de ne pas générer de vibrations. Ces températures sont intéressantes pour réfrigérer des qubits silicium.

---

[231] C'est le cas par exemple du bolomètre du **CUORE** (Cryogenic Underground Observatory for Rare Events) installé en Italie. Le cryostat comprend cinq tubes à pulsations et refroidit à 10 mK une charge utile de 750 kg de dioxyde de tellurium. Il cherchait des signes de désintégration bêta qui auraient pu prouver l'existence de fermions de Majorana. Et n'en a pas trouvé au bout du compte.

[232] On doit la création du procédé à William Giauque (1895-1982, USA) en 1927. Il fut lauréat du Prix Nobel de Physique en 1949.

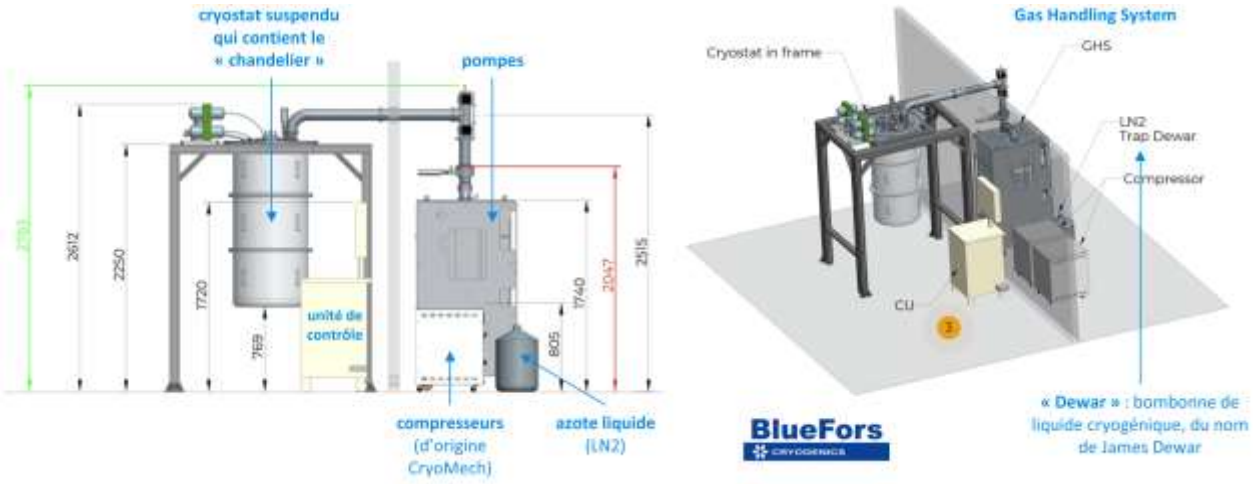
[233] Voir aussi Cryogenic Fluids par Henri Godfrin, 2011 (50 slides), de l'Institut Néel de Grenoble qui comprend une équipe de recherche de pointe sur la cryogénie. Avec un record de 100 µK obtenus avec le cryostat DN1 qui utilise la désaimantation nucléaire.

D'autres techniques existent qui permettent de gérer un refroidissement très localisé. C'est le cas de l'**effet Doppler** qui fonctionne sur des atomes froids en suspension dans le vide. C'est aussi le cas d'un système mis au point par les chercheurs du VTT Technical Research Centre en Finlande qui permettrait le refroidissement de composants au silicium avec une technique de refroidissement électronique à base de phonons.

Sachant que ces Finlandais ne sont pas loin de BlueFors, le leader du marché ! Il semble cependant que cette capacité de refroidissement soit très faible, très localisée, et nécessite tout de même de prérefroidir le système à au moins 244 mK. Il faut donc tout de même exploiter un cryostat à dilution base d'hélium 3 et 4[234].

A contrario, les technologies quantiques font aussi appel à d'**autres formes de cryostats** que ceux qui sont présentés ici pour le calcul quantique. Ainsi, les capteurs quantiques de Thales à NV centers utilisent-ils un refroidissement miniaturisé fonctionnant à l'azote liquide et n'occupant d'un demi décimètre-cube[235]. La température requise est moins basse, située autour de 70K. C'est bien chaud par rapport à 15 mK !

Un cryostat de calculateur quantique est divisé en **deux grandes parties** avec le compresseur, les pompes et les réservoirs d'azote liquide et d'hélium gazeux qui sont positionnés dans une pièce, et l'enceinte réfrigérée dans une autre pièce. C'est assez logique puisque le compresseur va générer de la chaleur qu'il faudra dégager, via une conduite entrante et sortante d'eau.



Avec les réfrigérateurs à dilution fonctionnant à sec, les contraintes de sécurité sont assez légères par rapport aux modèles humides. Ces derniers pouvaient utiliser jusqu'à 80 litres d'hélium liquide qui pouvait exploser s'il était réchauffé trop brutalement car l'expansion du gaz est importante par rapport à son état liquide, dans un rapport de 1 à 700.

---

[234] Voir Thermionic junction devices utilizing phonon blocking par Emma Mykkänen et al, 2020 (9 pages). On peut y lire : "*The cooling power for this sample is about 2 pW/µm2 at 300 mK". "Our best-performing sample is S2 (subchip with 1-mm diameter and 0.4-mm height). Its maximal absolute and relative temperature reductions are 83 mK (at 244 mK) and 40% (at 170 mK), respectively*". Donc, faut déjà atteindre 244 mK avant de commencer, et il est donc nécessaire de tout de même faire appel à un cryostat à hélium 3 et 4.

[235] Source de l'image : Closed Cycle Refrigerator par John Wilde, 2018 (11 slides). Ce sont en général des systèmes utilisant un moteur Stirling. Thales Cryogenics produit de tels systèmes de réfrigération miniaturisés. Le RM2 refroidit une charge utile à 77K pour une masse de 275g et un budget thermique de 400 mW à cette température. Il est notamment utilisé pour le refroidissement de caméras infrarouge dans des systèmes embarqués. On trouve également ce genre de petits cryostats chez SunPower (USA), capables de descendre à 40K et avec une masse plus grande de 1,2 kg. Ricor (1967, USA) est un autre fabricant de ce genre de mini-cryostats.

Il fallait manipuler des bombonnes d'hélium liquide et remplir des réservoirs avec un équipement de protection pour se protéger des projections[236].

On retrouve cet agencement au CEA-IRIG de Grenoble qui déployait en juin 2019 deux systèmes commerciaux de **BlueFors**, *ci-dessous*. Je l'avais visité fin juin 2019. Ce sont des systèmes à environ 1M€ la pièce. La thermalisation, ou la baisse de température à moins de 20 mK, dure au minimum 24 heures pour une installation à température ambiante.

Les équipes du CEA ont installé un dispositif qui permet de changer l'échantillon testé en seulement 7 heures. La thermalisation peut ainsi être déclenchée pendant la nuit, et au petit matin, les expériences peuvent reprendre.

Les phénomènes de **dilatation et compression** des matériaux sont significatifs à très basse température. Cela impacte la conception de l'ensemble du dispositif et des choix de matériaux. Les matériaux utilisables sont des aciers spéciaux au nickel, chrome, de l'aluminium, du bronze, du cuivre, des matériaux composites, du niobium-titane pour le câblage, des alliages nickel-cuivre, de l'indium pour les joints, du kapton et du mylar pour l'isolation.

Le système réfrigéré est généralement placé **sous vide**. La gestion du haut vide et de l'ultra vide (Ultra High Vacuum) sont des spécialités industrielles. Sachant que les cryostats d'ordinateurs quantiques supraconducteurs et silicium se contentent de haut vide entre 5 et 10 mBar. Ils utilisent des pompes du commerce provenant par exemple de **Pfeiffer** (Allemagne). Le pompage n'a lieu qu'au démarrage du système et est désactivé une fois celui-ci thermalisé à basse température. Le refroidissement à 15 mK n'a pas besoin de pompage par ultra-vide car en pratique, à cette température, tous les gaz deviennent solides et se déposent sur les parois du matériel, générant un vide de très bonne qualité.

L'abus de pompage pour générer de l'ultra-vide pourrait faire circuler des poussières de ces gaz solidifiés en endommager les qubits ou le reste du matériel embarqué dans le cryostat. L'ultra-vide est utilisé pour les calculateurs à base d'atomes froids.

Les fuites thermiques sont très nombreuses comme par exemple au niveau des câbles qui entrent et sortent de l'enceinte ou par radiation.

[236] Le taux d'oxygène dans la pièce pouvait aussi diminuer dangereusement du fait de l'évaporation accidentelle d'azote ou d'hélium liquide. Il faut aussi éviter le contact avec les matériaux cryogénisés, notamment les métaux. Il faut des pièces assez grandes et faire attention aux parties en hauteur des pièces où l'hélium peut se loger car il est plus léger que l'air.

De nombreuses couches de matériaux isolants thermiquement sont intégrées dans le cryostat. Ce sont des cylindres empilés comme des poupées russes la tête en bas comme on peut le voir dans les illustrations suivantes. Ils sont fabriqués en aluminium, cuivre et acier. Chaque cylindre et plaque joue un rôle d'isolant thermique vis-à-vis du cylindre inférieur.

Le calculateur quantique est **isolé magnétiquement** de l'extérieur. L'isolation magnétique utilise plusieurs enceintes en poupées russes réalisées dans des alliages divers, dont le **Mu-metal**, un alliage de nickel, fer et molybnène, des alliages en aluminium et d'autres alliages supraconducteurs. Le processeur quantique peut être lui aussi protégé par une protection magnétique. IBM utilise un Cryoperm Magnetic Shielding de **MµShield**.

Indépendamment de cette isolation magnétique, les cryostats de laboratoires de recherche sont souvent complétés par des systèmes d'**aimants supraconducteurs** qui occupent la partie basse du cylindre du cryostat. Ils ont une forme cylindrique qui entoure un instrument de mesure. Ces aimants sont aussi alimentés par de l'hélium liquide pour garantir l'effet supraconducteur qui sert à générer des champs magnétiques intenses de plusieurs Teslas. Ces champs servent à monter des expériences diverses, notamment en astronomie ou en physique fondamentale. Ils sont parfois utilisés dans le calcul quantique, notamment avec les qubits silicium[237].

Chez D-Wave, le champ magnétique est réduit à un nano-Tesla (nT) dans l'enceinte du calculateur, à comparer au champ magnétique terrestre qui peut atteindre 65 micro-Teslas, ce qui nous fait donc un ratio de 1 pour 65 000. D-Wave communique sur un ratio de 1 pour 50 000.

Les principaux fournisseurs de cryostats destinés aux calculateurs quantiques sont les Finlandais **BlueFors Cryogenics** qui équipent IBM et Rigetti, l'anglais **Oxford Instruments** que l'on retrouve chez D-Wave et Microsoft, l'American **Janis** qui est utilisé par Google, le Hollandais **Leiden Cryogenics**[238] qui fabrique des cryostats les plus puissants du marché, surtout utilisé pour des expériences de physique et le Français **CryoConcept** qui est notamment installé au CEA ou à l'Ecole Normale de Paris. La majorité de leurs clients sont cependant des laboratoires de recherche, non inventoriés dans le schéma *ci-dessus*.

[237] Chez CryoConcept, des aimants de 8 ou 14 Tesla peuvent être installés sur l'étage 4K à côté de l'unité de dilution.

[238] Voir la brochure Leiden Cryogenics BV (28 pages).

Leiden Cryogenics a été créé en 1992 par Giorgio Frossati et Alex Kamper. Le premier avait travaillé sur la réfrigération à dilution depuis les années 1970. Il avait notamment inventé les échangeurs de chaleur à poudre d'argent. A ses débuts, il travaillait à Grenoble au Centre de Recherche sur les Très Basses Températures, devenu le centre de recherches sur la Matière Condensée et les Basses Températures (MCBT) de l'Institut Néel du CNRS. Giorgio Frossati est ensuite devenu professeur à l'Université de Leiden aux Pays-Bas. Il y construit un réfrigérateur à dilution atteignant une température record de 1,85 mK avec une puissance de 25 µW à 10 mK. Les technologies d'échangeurs thermiques qu'il a mis au point ont été commercialisées sous licence à Oxford Instruments ! Et BlueFors a été créé par des post-docs de Georgio Frossati ! Petit monde !

CryoConcept (2014[239], France, dont l'acquisition par Air Liquide était annoncée en septembre 2020) se différencie avec des cryostats générant un très faible niveau de vibrations via leur technologie UltraQuiet, ce qui est utile pour préserver la cohérence des qubits. Leurs cryostats sont déployés par différents acteurs tels que le CEA à Saclay. Ils sont aussi utilisés à l'ENS[240] et à l'international au Japon et aux USA et plutôt dans la recherche.

Le faible niveau de vibration de leur cryostat est lié à l'absence de contact à froid entre le tube pulsé et la platine froide. Ils se focalisent sur la réduction des basses vibrations à 1,4 Hz. Elles sont liées au déplacement du gaz et aux cycles de détente dans les flexibles du cryostat. Ils utilisent des accéléromètres sensibles aux basses fréquences pour les mesurer. Cette absence de vibration est très utile pour l'usage de cryostats contenant des bolomètres qui servent à réaliser des expériences de physique comme pour la recherche de matière noire. Ce marché a démarré avec des cryostats « humides » avant de passer aux modèles « à sec » depuis une dizaine d'années.

A l'époque où ils avaient démarré, le marché des cryostats à très basse température était balbutiant. Les achats des laboratoires se faisaient à l'unité. Maintenant, ils passent par des commandes de cinq à une dizaine d'unités. C'est lié à la lenteur de mise en place des expériences dans le calcul quantique. Les laboratoires ont besoin de machines qui opèrent et évoluent en parallèle pour aller plus vite dans les phases d'expérimentation, surtout lorsque des variantes de circuits de qubits sont testées.

Depuis 2018, CryoConcept collabore avec le CEA-Leti dans la production de deux cryostats pour équiper le projet QuCube de qubits silicium. Pour l'instant, ils n'ont pas encore de clients de cryostats destinés au calcul quantique à l'étranger. Ils vendent aux USA, au Japon et en Corée sur un marché tiré par la recherche de matière noire et la bolométrie.

MyCryoFirm (2013, France) produit aussi des cryostats, mais descendant seulement à 3K et donc, inadaptés aux usages du calcul quantique en général. Ils ciblent plutôt le champ de la recherche en physique fondamentale ainsi que celui des capteurs quantiques.

La **quantité d'énergie absorbée** est assez faible dans les cryostats. Cela limite l'énergie qui peut être dégagée par les qubits eux-mêmes et surtout par les circuits d'atténuation des micro-ondes et d'amplification utilisés pour la lecture de l'état des qubits.

Ci-contre, un petit comparatif de ces budgets thermiques par fournisseur.

	cryostat	pulse tubes	minimum temperature	20mK stage	100mK stage	MC cold plate
BLUEFORS	LD250	1	10 mK	12 µW	250 µW	30 à 50 cm
	XLD400	2	8 mK	14 µW	450 µW	30 à 50 cm
	XLD1000	2	8 mK	34 µW	1000 µW	30 à 50 cm
JANIS	JDry-500-QPro	1	7 mK	14 µW	500 µW	50 cm
OXFORD INSTRUMENTS	TritonXL	2	5 mK	25 µW	1000 µW	43 cm
	TritonXL-Q	2 ou 4	7 mK	25 µW	850 µW	50 cm
	Proteox	1	10 mK	?	500 µW	36 cm
CryoConcept	HD200	1	10 mK	11 µW	350 µW	30 à 50 cm
	HD400	1	10 mK	10 µW	400 µW	30 à 50 cm
Leiden Cryogenics	CF2400 Maglev	2	4 mK	? µW	2000 µW	49 cm
	CF1400 Maglev	2	8 mK	? µW	1000 µW	49 cm

[239] CryoConcept a en fait été créé en 2001 par transfert de technologie du CEA où Olivier Guia avait travaillé. La société a eu plusieurs propriétaires différents dont le Français Segula Technologies et l'Américain CryoMagnetics. Olivier Guia a repris l'activité de la société en 2014. Ils ont alors réintégré la R&D en interne et notamment récupéré la maîtrise technologique qui était au CEA.

[240] Voir l'équipement quantique de l'ENS dans leur Labtour.

Le budget thermique de réfrigération des **BlueFors** varie de 12 µW (LD250) à 30 µW (XLD1000) à 20 mK, et de 250 µW (LD250) à 1000 µW (XLD1000) à 100 mK. Le TritonXL d'**Oxford Instruments** dispose également d'un budget thermique de 1000 µW à 100 mK[241] mais avec deux têtes pulsées, tandis que le nouveau Proteox atteint 500 µW… avec une seule tête pulsée. Il est complété par un système amovible pour les câbles de contrôle des qubits en supportant jusqu'à 140.

Le **Janis** JDry-500-QPro a un budget thermique de 14 µW à 20 mK et 450 µW à 100 mK (*ci-dessus*, compilation maison).

Le record actuel se trouve chez **Leiden Cryogenics** avec un cryostat récent doté d'un budget thermique de 2000 µW à l'étage 100 mK, mais dont le budget à 20 mK n'est pas indiqué dans leur littérature. A l'étage 4K, le budget thermique disponible est aux alentours de 1W. Mais attention, ces performances extrêmes au-delà de 500 µW sont souvent obtenues avec deux têtes pulsées au lieu d'une et donc, un doublement du compresseur extérieur et de la puissance consommée. Le tout avec un double système de réfrigération à dilution pour descendre en-dessous de 1K. On peut aussi avoir des systèmes avec une seule tête pulsée et deux systèmes à dilution.

L'américain **CryoMech** fournit des compresseurs et les têtes pulsées de premier étage qui sont utilisés par ces différents cryostats, comme les PT415 et PT420 (*à droite*). Son principal concurrent est la filiale SHI Cryogenics Group de **Sumitomo** (Japon, *à gauche*)[242]. Ces compresseurs associés aux têtes pulsées sont les principaux consommateurs d'énergie d'un ordinateur quantique et jusqu'à 12 kW. Le reste, à savoir les pompes du GHS et l'ordinateur de contrôle du reste du cryostat consomment entre 3 et 4 kW. Les têtes pulsées ont bénéficié de décennies de progrès. Elles utilisent un système de détente de gaz compressé à l'extérieur du cryostat sans pièce rotative dans le cryostat[243]. Le refroidissement du compresseur est à eau, avec un débit de 5 à 12 litres par minute selon sa température entrante.

[241] Voir la très intéressante présentation 50 years of dilution refrigeration, par Graham Batey d'Oxford Instruments, 2015 (26 slides).

[242] Il existe d'autres fabricants de têtes pulsées et de compresseurs comme Fabrum Solutions (Nouvelle-Zélande) mais ce dernier ne vise que des températures de 77K destinées à la production d'azote liquide.

[243] Ces têtes pulsées sont notamment utilisées dans l'industrie des semiconducteur, dans les machines de dépôt sous vide (CVD, MOCVD) et à plasma. Elles descendent à 10K ce qui est suffisant pour la production de semiconducteurs.

Le budget thermique de l'étage étage le plus froid est conditionné par l'équation : $Q_m = 84\dot{n}_3T^2$ dans laquelle Q_m est la puissance de refroidissement en W, $\dot{n}_3$ la vitesse d'écoulement en mol/s de l'hélium 3 dans le cryostat à cet étage et T est la température de l'étage en Kelvin. Cette loi que l'on peut appeler simplement «$Q=84NT^2$» explique que le budget thermique à 15 mK soit très faible au regard du budget aux étages supérieurs (jusqu'à 25 µW à 15 mK, 1 mW à 100 mK et 1,5W à 4K).

Il existe une autre contrainte liée à la résistance de Kapitsa qui limite les échanges de chaleur entre l'hélium 3 et l'échangeur de chaleur. Ces échanges sont proportionnels à T^4. Si on souhaite donc multiplier par 10 les échanges de chaleur, il faudrait multiplier par 10000 les surfaces d'échanges dans les parties basses du système à dilution !

On le fait en utilisant des poudres d'argent qui sont intégrées dans les échangeurs discrets de chaleur au-dessus de la chambre de dilution. Ces poudres sont structurées de manière à maximiser la surface d'échange de chaleur avec le gaz d'hélium qui y circule. Dans le même temps, leur procédé de dépôt doit maximiser la surface de contact à plat avec l'intérieur des petites cuves où elles sont situées.

Une chose et son contraire qui constituent la sauce magique des fabricants de cryostats. A l'Institut Néel du CNRS à Grenoble, les équipes ont créé leurs propres systèmes de cryogénie, capable de thermaliser un système quantique en seulement trois heures.

Ils disposent pour cela de chercheurs dédiés, comme Henri Godfrin. Les circuits quantiques doivent aussi être dotés de radiateurs miniatures pour dégager l'énergie générée par les portes quantiques. Selon le CEA, ces radiateurs feraient entre 1 mm et 1 micron d'épaisseur[244].

Au final, un ordinateur quantique est de taille raisonnable. Dans les laboratoires, le calculateur quantique lui-même tient dans un cylindre d'environ 50 cm de diamètre et un peu plus d'un mètre de haut. L'électronique de commande externe tient dans quelques racks de serveurs et dispositifs de contrôle. Le système de cryogénie occupe environ deux mètres cubes. Le tout dans une pièce certes bien aérée mais de taille raisonnable.

Chez D-Wave qui est le seul fournisseur d'ordinateurs quantiques commerciaux, les machines font environ 27 mètres cube. C'est plutôt raisonnable compte-tenu de la puissance de calcul qui sera un jour accessible à ces ordinateurs et qui dépassera largement celle de supercalculateurs qui occupent de leur côté de vastes salles blanches et consomment des mégawatts d'électricité.

Notons pour terminer que le marché mondial des systèmes de cryogénie, toutes catégories confondues serait d'environ $1,8B en 2020[245]. Rappelons que la science des basses températures qui est utilisée dans l'informatique quantique a bénéficié d'avancées nombreuses issues d'autres domaines : l'espace et notamment les télescopes spatiaux où une bonne partie des instruments doivent être refroidis comme les capteurs infrarouges ou les bolomètres, les accélérateurs de particules avec leurs aimants supraconducteurs et enfin, l'imagerie médicale, notamment l'IRM, qui a aussi besoin de basses températures pour refroidir ses aimants supraconducteurs.

---

[244] Selon Robert Whitney dans Energetics of quantum computing, 2018 (13 slides).

[245] Voir Cryocooler Market by Type (GM, PT, JT, Stirling, and Brayton Cryocoolers), Services (Technical Support, Repair, Preventive Maintenance), Heat Exchanger Type (Recuperative and Regenerative), Application, and Geography - Global Forecast to 2022, décembre 2019. Ce marché représentait $1,4B en 2018 et avec une croissance annuelle prévue de 9,3% d'ici 2027. Mais attention, le marché des cryostats pour ordinateurs quantiques est un tout petit morceau de ce marché.

Composants

Passons maintenant à l'équipement qui se trouve à l'intérieur du cryostat : les plaques de cuivre, les câbles, les capteurs et, surtout, l'électronique embarquée qui contrôle les qubits et lit leur état.

Dans les systèmes quantiques actuels à base de qubits supraconducteurs, des câbles coaxiaux en cuivre transportent des **photons micro-ondes** à des fréquences situées entre 5 et 10 GHz pour agir sur les qubits (reset et portes quantiques). Les micro-ondes sont générées par des appareils situés généralement à l'extérieur de l'enceinte réfrigérée. Les fréquences inférieures à 5 GHz et supérieures à 10 GHz sont éliminées par filtrage. Ces micro-ondes sont aussi atténuées et filtrées en entrée à l'étage du haut qui est à 4K. L'atténuation est importante et de 60db, réalisée en trois étapes de 20 db qui à chaque fois divisent par 100 la puissance transmise. Elle sert à limiter le bruit thermique qui est véhiculé dans les câbles. Il est réduit de manière à ne représenter par plus d'un millième des photons qui aboutissent dans les qubits. Chaque filtre absorbe de l'énergie qui doit être dissipée aux étages où ils sont placés.

La conduction thermique d'un câble Q se calcule comme suit, avec le produit de la conductivité du câble k, sa section A, le gradient de température T_2-T_1 et L la longueur du câble.

$$Q = kA \frac{T2-T1}{L}$$

Des **câbles supraconducteurs coaxiaux** - ayant une résistance théoriquement nulle à basse température - relient les qubits à leur système de lecture (donc, dans le sens montant dans les schémas). Ils sont réalisés en alliage de niobium et de titane (NbTi). Ce sont eux qui comprennent des boucles servant à absorber le phénomène de contraction du métal qui intervient lors du refroidissement[246]. Leur signal est amplifié avant de sortir du cryostat.

Ces câbles proviennent du Japonais **Coax Co**. Il semblerait que cette société soit la seule au monde capable de les produire[247]. Le câble qui fait 2 mm de diamètre comprend une enveloppe extérieure conductrice et un conducteur central, tous deux en niobium-titane (source), qui sont séparés par un isolant en téflon (PFTE) ou kapton.

Les câbles descendants de contrôle des qubits par micro-ondes sont réalisés dans des matériaux divers et notamment en alliages cuivre-nickel, cuivre-bérylium ou de bronze. Après le passage par l'étage 4K, ils sont remplacés par des versions supraconductrices pour limiter leur conduction de chaleur. Entre les deux sont intercalés des atténuateurs de 20 dB. S'y ajoutent des câbles classiques en paires torsadées transportant du courant continu et qui alimentent les composants électroniques actifs intégrés dans le cryostat, notamment les amplificateurs de lecture de l'état des qubits.

Cela donne un bon **encombrement de fils**. La photo *ci-dessous à droite* présente l'intérieur d'un cryostat de Google avec ses rangées de fils reliant différents étages du calculateur. Et c'est le câblage pour seulement une 53 qubits. La forêt de câbles est déjà bien dense. Il semble qu'il soit possible de miniaturiser tout cela notamment avec des câbles dressés à plat. Mais comme ces calculateurs sont encore des engins de laboratoire, la miniaturisation à la japonaise n'est pas encore passée par là.

---

[246] Voir Challenges in Scaling-up the Control Interface of a Quantum Computer par D. J. Reilly de Microsoft, décembre 2019 (6 pages) qui indique que les câbles supraconducteurs ont une résistance et une capacitante lorsqu'ils sont traversés par des micro-ondes et qu'ils ont donc un dégagement thermique dont il faut tenir compte.

[247] Voir We'd have more quantum computers if it weren't so hard to find the damn cables, de Martin Giles, janvier 2019.

Ces divers câbles ont un autre inconvénient : ils coûtent très cher. L'unité est à plusieurs milliers de dollars. Pour un ordinateur quantique à qubits supraconducteurs à 53 qubits d'aujourd'hui, ce câblage coute plus cher que tout le cryostat, soit plus d'un demi-million de dollars. Cela explique d'ailleurs le fait que les fabricants de cryostats tels que **Bluefors** proposent aussi leur propre système de câblage optimisé comme leur High Density Wiring à 168 câbles, qui a l'air dimensionné pour supporter 56 qubits. Cela permet de vendre plus de valeur par machine ! Il en va de même avec le système ammovible de câbles du récent Proteox d'**Oxford Instruments**.

Les **plaques de chaque étage** du cryostat sont généralement constituées de cuivre pur à 99,99% et à très faible teneur en oxygène, afin de maximiser leur conductivité thermique[248]. Elles sont recouvertes d'une fine couche d'or de quelques microns d'épaisseur qui joue un rôle de protection contre l'oxydation et les radiations.

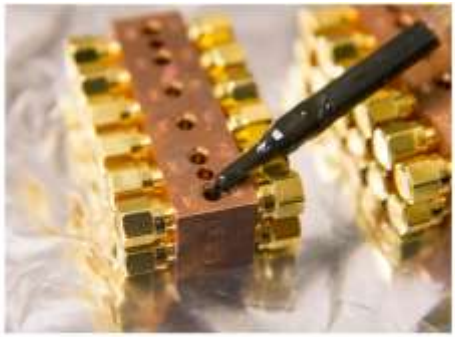
Ci-contre, un exemple de plaque d'un cryostat de BlueFors. Ces plaques sont trouées sur mesure pour laisser passer tous les câbles que nous venons de citer, sans compter les éléments du cryostat. Sachant que tous les trous doivent être utilisés.

Il faut éviter que des rayons infrarouges puissent passer d'un niveau à l'autre et générer des fuites thermiques descendantes. Ces plaques doivent être des écrans optiquement totalement étanches pour ne pas laisser passer un seul photon !

La tendance est à l'augmentation de la taille des plateaux des étages. Sachant que leur taille va décroissant de haut en bas à cause des cylindres concentriques qui les englobent.

[248] C'est de l'OFHC pour oxygen-free high thermal conductivity. Source de cette information : Flying Qubit Operations in Superconducting Circuits d'Anirudh Narla 2018 (219 pages).

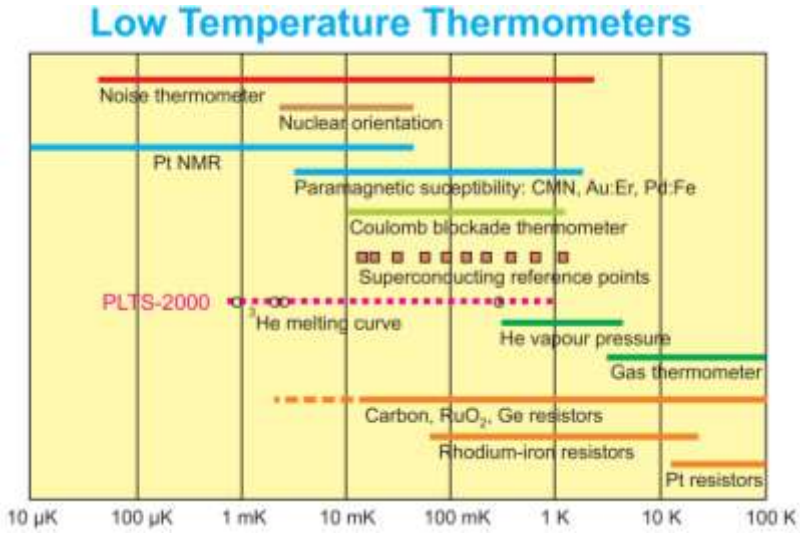
Dans les cryostats pour ordinateurs quantiques, le standard actuel pour le plateau du bas est de 30 cm à 40 cm pour la recherche et 50 cm en production, pour pouvoir y placer plus de composants électroniques. Il pourrait bientôt atteindre 100 cm ! L'infrarouge est également filtré avec une résine **Eccosorb** qui entoure les câbles supraconducteurs dans l'étage le plus bas du système. Cette résine est un mélange d'époxy et de poudre métallique. Elle est injectée dans des filtres en cuivre (OFHC) qui entourent les câbles dans l'étage le plus froid du cryostat (*ci-contre*)[249]. La résine est généralement fournie par la société **Laird Performance Materials** (UK).



(A) ECCOSORB injection. Inject slowly and at a flat angle such that the liquid creeps onto the edge of the fill opening and into the cavity. Injecting too fast or steep will cause a planar bubble to form which blocks the opening (see Figure 2.8b).

On doit pouvoir **mesurer** la pression (ambiante, gaz), la température (un peu partout) et le débit (de gaz) à température cryogénique. Des capteurs spécifiques sont ainsi installés pour ce faire dans l'enceinte du cryostat, attachés à différents endroits du « chandelier ».

On mesure les températures avec des thermomètres cryogéniques[250] ! On en trouve notamment chez **Lake Shore Cryotronics** avec ses Cernox qui descendent jusqu'à 100 mK et résistent bien au champ magnétique ambiant et ses thermomètres à oxyde de ruthénium qui descendent à 10 mK. A moins de 20 mK, on utilise des thermomètres à bruit qui exploitent des jonctions Josephson (et la boucle est bouclée…). Certains thermomètres sont placés sur les plaques à l'opposé des tubes d'échange de chaleur et de la boîte à mélange.



Le **processeur quantique** consiste pour les qubits supraconducteurs et silicium en une puce de quelques centimètres carrés. Elle est intégrée dans un boîtier en cuivre OFHC (Oxygen-Free High thermal Conductivity) qui est purifié et débarrassé de l'oxygène qui limite sa conductivité thermique Ce boîtier est agrémenté de connecteurs coaxiaux pour qu'il puisse être alimenté en micro-ondes. Dans les derniers processeurs supraconducteurs d'IBM et Google à 53 qubits, il faut plus de 160 de ces connecteurs. Le boîtier est lui-même intégré dans deux petites enceintes concentriques en aluminium et en Cryoperm (de l'Américain **MμShield**) d'isolation magnétique.

L'**électronique de contrôle** intégrée dans le cryostat doit répondre à un cahier des charges rigoureux[251]. On ne peut pas placer sa carte mère de PC comme cela à ces basses températures.

---

[249] Voir quelques explications sur la résine Eccosorb dans Improving Infrared-Blocking Microwave Filters par Graham Norris, 2017 (114 pages) et Development of Hardware for Scaling Up Superconducting Qubits and Simulation of Quantum Chaos par Michael Fang, 2015 (56 pages).

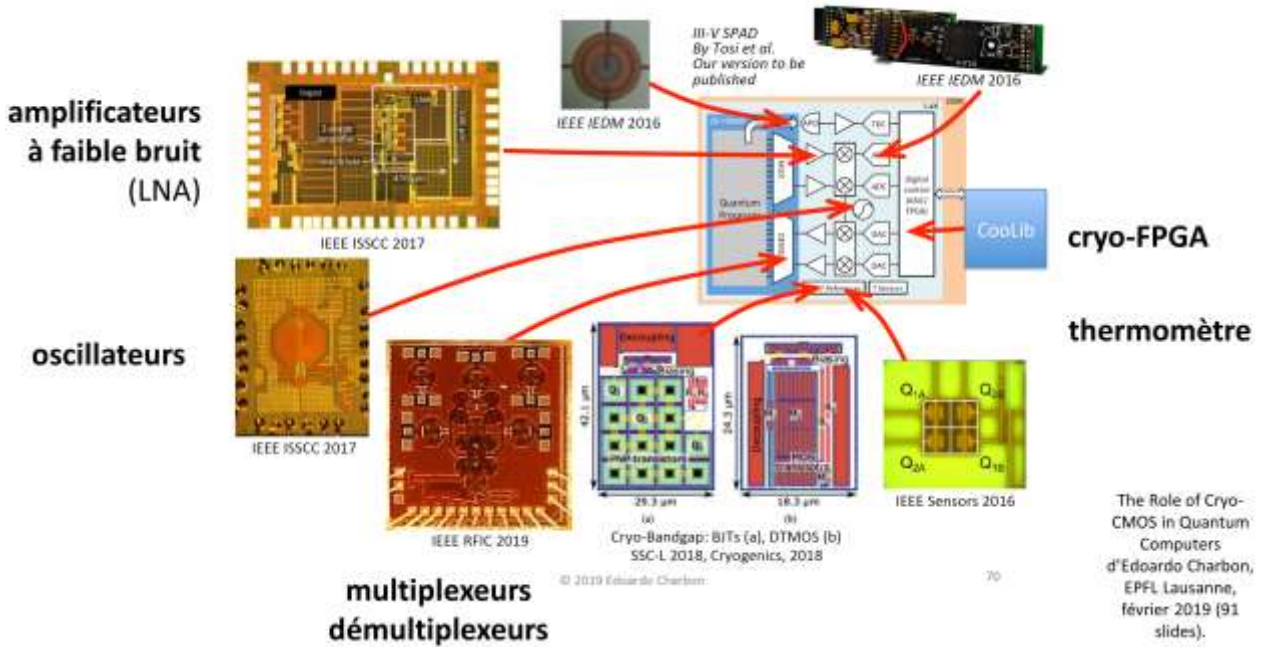
[250] Source du schéma : Thermometry at low temperature par Alexander Kirste, 2014 (31 slides). On y voit qu'il existe une bonne dizaine de types de thermomètres descendant à moins de 1K. Le plus couramment utilisé exploite le blocage de Coulomb à base de jonction à effet tunnel. La tension électrique de la jonction varie linéairement avec la température cryogénique.

[251] Voir Engineering cryogenic setups for 100-qubit scale superconducting circuit systems par S. Krinner et al, 2019 (29 pages) qui décrit bien les enjeux de contrôle de qubits supraconducteurs. Ils proposaient en 2018 une approche optimisée de câblage et d'électronique permettant d'embarquer jusqu'à 150 qubits supraconducteurs dans un cryostat.

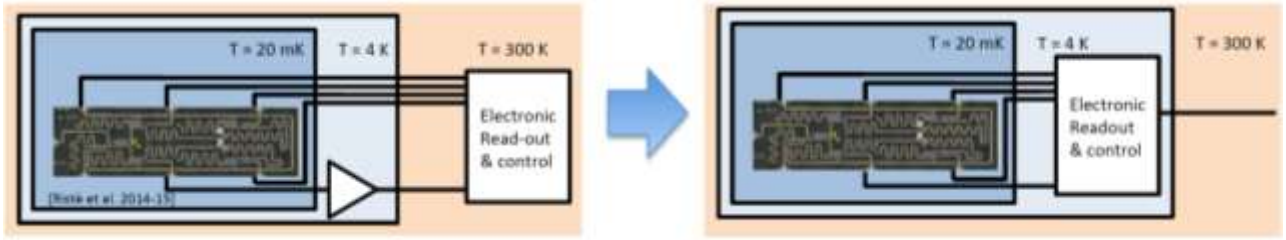
L'exemple *ci-dessous* décrit la grande variété des composants qui peuvent être intégrée dans l'étage 1K-4K et dans l'étage du processeur à moins de 20 mK[252].

Il faut donc créer des composants certifiés pour fonctionner à ces températures-là : amplificateurs, multiplexeurs de données, oscillateurs de fréquences, contrôle électronique de la mesure de l'état des qubits, thermomètres et autres capteurs divers, etc.

La tendance est au déport à l'intérieur du cryostat d'un maximum de cette électronique de contrôle, allant jusqu'à y intégrer les générateurs de micro-ondes de contrôle et de lecture des qubits supraconducteurs ou silicium, sachant qu'il en faut au minimum trois par qubits supraconducteur. La chaleur qu'ils dégagent est limitée pour ne pas augmenter la température des qubits par la puissance thermique de la réfrigération[253]. A 10-20mK, cela ne représente qu'à peine 25 µW de puissance dissipable. À 4K, elle est d'environ 1 W.



L'autre approche consiste à miniaturiser ces circuits, mais dans l'étage 4K du cryostat. Elle et notamment étudiée chez TU Delft[254] et pour l'électronique de lecture de l'état de qubits silicium. L'auteur appelle cela **QuRO**, pour Quantum Read-Out. La lecture de l'état des qubits silicium est réalisée par réflectométrie de photons micro-ondes sur des quantum dots.



[252] Source du schéma : The Role of Cryo-CMOS in Quantum Computers d'Edoardo Charbon, EPFL Lausanne, février 2019 (91 slides).

[253] Voir Cryogenic Control Beyond 100 Qubits de Ian Conway Lamb, 2017 (103 pages) qui décrit bien les enjeux technologiques des composants fonctionnant à température cryogénique, ici pour des qubits supraconducteurs. Et la version courte : Cryogenic Control Architecture for Large-Scale Quantum Computing, de Ian Conway Lamb et al, 2017 (8 pages). Voir aussi Semiconductor devices for cryogenic amplification de Damien Prêle, 2013 (30 slides) et Cryo-CMOS Circuits and Systems for Quantum Computing Applications de Bishnu Patra et al, 2018 (14 pages).

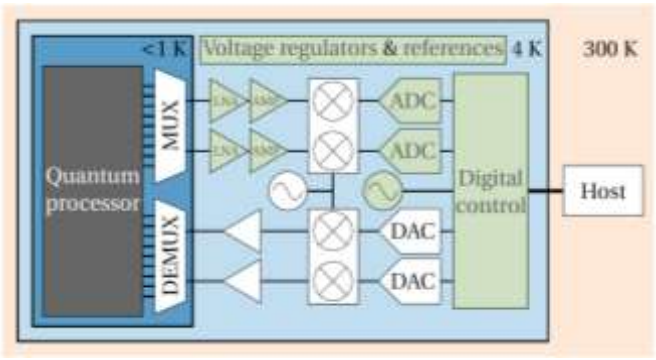
[254] Voir Cryogenic electronics for the read-out of quantum processors par Harald Homulle, TUDelft, 2019 (185 pages).

La technique permet de multiplexer la lecture de l'état des qubits avant l'envoi de l'information hors de l'enceinte cryogénisées. Cela simplifie donc le câblage en sortie. Leur prototype utilise un amplificateur à faible bruit (LNA) en CMOS complété par un amplificateur à transistor en SiGe (silicium-germanium), suivi par un convertisseur analogique/numérique (ADC) mis en œuvre dans un FPGA Xilinx Artix 7.

Ce dernier permet de multiplexer l'état de plusieurs qubits en sortie. Ils ont prévu le radiateur en cuivre de refroidissement du circuit pour son intégration avec l'étage 4K de la réfrigération à dilution. Ils se sont appuyés pour ce faire sur des composants passifs et actifs standards du marché opérant correctement à 4K.

Ce prototypage ne concernait pas les circuits DAC d'action sur les qubits en « écriture » (reset et portes quantiques). Il correspond une part du coût variable des traitements d'un algorithme quantique, notamment lié aux codes de correction d'erreur qui s'appuient sur des mesures répétées. L'économie d'énergie de leur système est donc probablement minimale. L'intérêt porte aussi sur la connectique et sa scalabilité avec l'augmentation du nombre de qubits. Le fait de rapprocher l'électronique de lecture de l'état des qubits de ceux-ci permet aussi d'accélérer les traitements de codes de correction d'erreurs qui exploitent la mesure d'états de qubits.

La même approche a été adoptée par **Intel** en collaboration avec QuTech pour son composant Horse Ridge de pilotage de qubits supraconducteurs et silicium capable de gérer les pulsations de micro-ondes de ce pilotage de fréquence allant de 2 à 20 GHz. Ce composant est placé dans l'étage 4K du cryostat[255]. Nous en parlons plus en détail dans la partie consacrée à l'investissement d'Intel dans les qubits supraconducteurs.



Une équipe américano-australienne (UNSW, Purdue, Microsoft)[256] conçoit de son côté un circuit CMOS de contrôle de qubits pouvant être de type supraconducteur gatemon, silicium ou à base de fermions de Majorana. Il est installé à l'étage 100mK, juste à côté du circuit des qubits sur un même support PCB (au cas où il s'agit de qubits silicium car pour des qubits supraconducteurs, le chipset de qubits serait un étage en-dessous, au niveau du 15 mK). Le circuit semble utiliser une source porteuse micro-onde externe au cryostat. La lecture se fait ici avec des circuits extérieurs (ADC et FPGA). C'est un peu l'inverse de la solution d'Harald Homulle. Le CMOS de test est réalisé en FDSOI en 28nm. Le chipset simplifie grandement la circuiterie de contrôle venant de l'extérieur. Le détail de l'installation est présenté dans les deux illustrations suivantes.

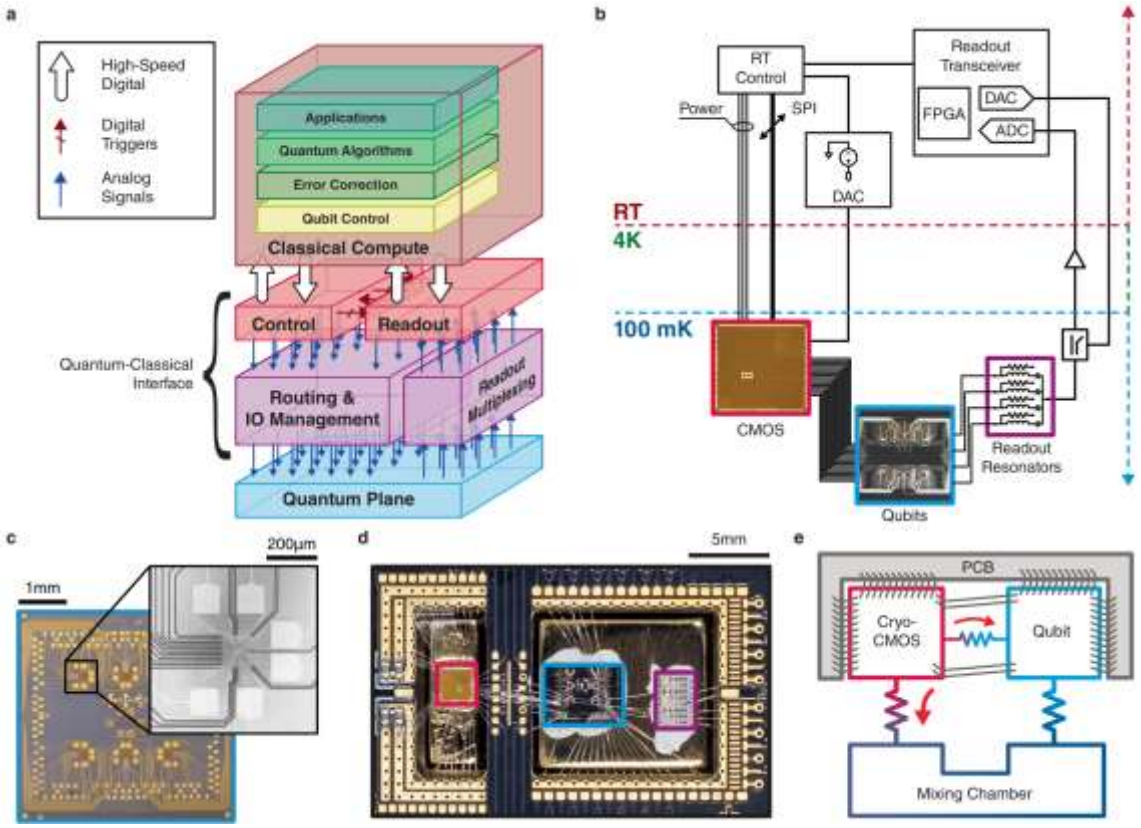
Le contrôle des qubits peut aussi faire appel à des circuits de génération et de lecture de micro-ondes supraconducteurs, leur intérêt étant un dégagement thermique moindre[257].

---

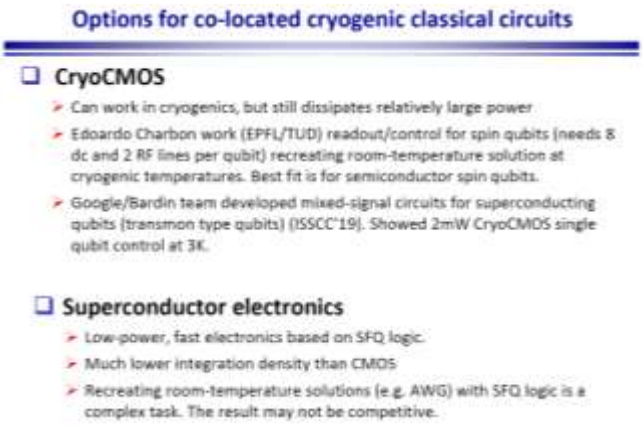
[255] Voir Cryo-chip overcomes obstacle to large-scale quantum computers par QuTech, février 2020.

[256] Voir A Cryogenic Interface for Controlling Many Qubits par D.J. Reilly et al, décembre 2019 (7 pages).

[257] Voir Quantum Computer Control using Novel, Hybrid Semiconductor-Superconductor Electronics par Erik P. DeBenedictis de Zettaflops, 2019 (15 pages) qui décrit une approche de circuits de contrôle de qubits mixant supraconducteurs (JJ) et des circuits adiabatiques, des Cryogenic Adiabatic Transistor Circuits (CATCs). Le papier fait au passage un tour d'horizon de l'efficacité énergétique des composants CryoCMOS et divers supraconducteurs connus (RQL, AQFP, …). .



Une startup se démarque dans ce créneau, **SeeQC** (USA) qui conçoit un circuit intégré supraconducteur assurant toutes les fonctions de pilotage des qubits, génération de micro-ondes et lecture d'état compris. Il est installé à l'étage 4K du cryostat. Ils n'ont pas encore l'air de travailler avec les principaux acteurs des qubits supraconducteurs qui pourraient y faire appel (IBM, Google, Rigetti) à moins qu'ils visent plutôt ceux qui conçoivent des qubits silicium qui fonctionnent aussi à température supraconductrice[258].



Dans ce domaine, citons aussi les amplificateurs cryogéniques à base de SQUID supraconducteurs à effet Josephson TWPA – *travelling wave parametric amplifier* – qui sont développés par l'**UGA** et le **LPMMC** à Grenoble[259].

Les composants de tests ont été fabriqués dans la Nanofab de l'Institut Néel de Grenoble. Le CEA-Leti développe aussi des amplificateurs CryoCMOS à faible bruit. Tout cela donc, pour lire l'état des qubits au sein du cryostat.

On peut aussi citer un projet chinois allant dans le même sens, de générateur de micro-ondes supraconducteur pour le contrôle de qubits supraconducteurs s'appuyant sur un FPGA d'origine **Xilinx**[260].

---

[258] Source du slide qui positionne les CryoCMOS et ce genre de circuit supraconducteur : Single Flux Quantum Logic for Digital Applications par Oleg Mukhanov de SeeQC/Hypres, août 2019 (33 slides).

[259] Voir A photonic crystal Josephson traveling wave parametric amplifier par Luca Planat et al, octobre 2019 (17 pages).

[260] Voir Scalable and customizable arbitrary waveform generator for superconducting quantum computing par Jin Lin, 2019 (9 pages).

Dernière approche, faisant l'objet de recherche à l'Université du Wisconsin et celle de Syracuse en liaison avec SeeQC, intégrer les circuits de contrôle et de lecture SFQ des qubits directement dans le processeur quantique qui devient ainsi hybride classique/quantique. La génération de micro-ondes pour le contrôle et la lecture utilise aussi des SFQ, des transistors supraconducteurs à basse consommation. Cette conception a été d'abord simulée numériquement en 2018 puis testée à petite échelle en réel en 2019[261].

Cette technique est en fait opérationnelle chez **D-Wave** depuis ses débuts. En effet, ses puces utilisant des qubits supraconducteurs de flux comprennent aussi des circuits SFQ supraconducteurs de génération des micro-ondes de contrôle et de lecture d'état des qubit, ce pour 2000 qubits ! C'est une prouesse technologique méconnue de D-Wave. Elle leur permet de simplifier énormément le câblage qui aboutit au processeur quantique.

Une fois que l'on est capable de générer tous les signaux micro-ondes à l'intérieur du cryostat, il reste à échanger dans les deux sens avec l'extérieur de manière numérique. Cela peut passer par des signaux multiplexés sur du cuivre, de la fibre optique, voire, c'est à l'étude, des ondes radio à très haute fréquences (dans les THz). L'idée étant de maximiser l'isolation thermique et du vide avec l'extérieur. Une fibre optique présente l'avantage d'être en verre, qui ne génère pas de dilatation à froid et est un faible conducteur de la chaleur.

Correction d'erreurs

L'un des écueils des qubits est qu'ils génèrent des taux d'erreurs non négligeables lorsque l'on agit sur eux avec des portes quantiques ainsi que lors de la mesure de leur état. C'est aussi le cas lorsqu'on les transmet sous forme d'états de photons dans des moyens de télécommunications optiques comme de la fibre. La correction d'erreur en informatique classique porte plus sur la mémoire, le stockage et les télécommunications. Dans les technologies quantiques, le calcul est gros consommateur de codes de correction d'erreurs.

Fidélité du calcul quantique

Dans un ordinateur quantique à portes universelles, on qualifie habituellement trois types d'erreurs : les erreurs sur les portes quantiques à un seul qubit, celles des portes à deux qubits puis celles de la mesure de la valeur des qubits.

Ces taux d'erreurs sont compris entre 0,1% et plusieurs 1%, ce qui est bien supérieur aux taux d'erreurs courants de l'informatique traditionnelle qui sont négligeables[262]. La « fidélité » est 100% moins le taux d'erreur en question.

---

[261] Voir Quantum–classical interface based on single flux quantum digital logic par Robert McDermott, 2018 (19 pages), Digital coherent control of a superconducting qubit par Edward Leonard Jr. et al, 2018 (13 pages). Le schéma page 10 laisse à penser que la génération de micro-ondes est toujours réalisée à l'extérieur du cryostat. C'est lié au fait que l'expérience contient une double commande des qubits : par courant continu pour piloter la génération de micro-ondes par le SFQ à proximité des qubits, et de manière traditionnelle à l'extérieur du cryostat. Cela leur permet de comparer la fidélité des deux méthodes. Et puis Digital coherent control of a superconducting qubit, par Oleg Mukhanov (CTO et cofondateur de SeeQC), Robert McDermott et al, septembre 2019 (39 slides) et Hardware-Efficient Qubit Control with Single-Flux-Quantum Pulse Sequences par Robert McDermott et al, 2019 (10 pages).

[262] En calcul classique, les erreurs sont très rares. On parle de perturbations par particules isolées (PPI) et de single event upset en anglais (SEU) qui déclenchent des "soft errors" ou erreurs logiques. Le SER (Soft Error Rate) cumule le SDC (Silent Data Corruption, non détecté) et le DUE (Detected and Unrecoverable Error, détectée, mais non corrigeable). L'unité de mesure des erreurs est le FIT (Failure in Time) qui correspond à une erreur sur un milliard d'heures d'utilisation. Le MTBF des équipements électroniques (Mean Time Between Failure) se chiffre généralement en années ou en dizaines d'années. Les erreurs sont généralement provoquées par des particules isolées (ions, électrons, photons), issues notamment de rayons cosmiques. Cela affecte notamment l'électronique embarquée dans l'aérospatiale, qui doit donc être durcie pour y résister, ainsi que celle qui est employée sur Terre mais en altitude. La mémoire est souvent plus affectée que les processeurs. D'où les systèmes de correction d'erreur qui utilisent par exemple un bit de parité et du contrôle de redondance cyclique utilisé dans les télécommunications.

Le schéma maison *ci-dessous*[263] consolide une comparaison de quelques niveaux de fidélité des qubits d'ordinateurs quantiques supraconducteurs, à ions piégés et atomes froids, ces informations étant fournies par leurs fournisseurs. On y constate que le taux d'erreur de portes à deux qubits et de la lecture est généralement plus élevé que le taux d'erreur des portes à un qubit[264]. Il faut donc être toujours vigilant et s'intéresser en particulier à la fidélité des portes à deux qubits ce d'autant plus que ce sont elles qui sont à l'origine d'une bonne part de la puissance de calcul quantique.

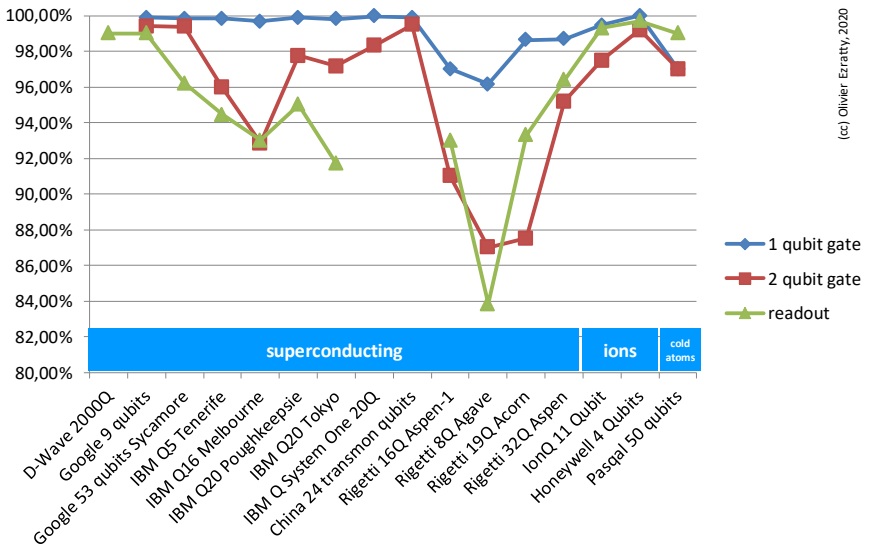
La meilleure fidélité obtenue en juin 2020 était de 99,989% pour les portes à un qubit pour le processeur d'Honeywell à 4 ions piégés et de 99,38% pour les portes à deux qubits de Google Sycamore de 53 qubits[265].

chaque porte quantique à un ou deux qubits génère des erreurs tout comme la lecture des résultats à la fin des opérations

ces erreurs s'accumulent avec le nombre de portes quantiques enchaînées

cela fausse les calculs d'autant plus que le nombre de portes quantiques à enchaîner est élevé

des méthodes de correction d'erreurs permettent de réduire ce taux d'erreur et de prolonger le temps de calcul opérationnel



taux de fiabilité des portes à un et deux qubits et de la mesure des résultats en %. le plus proche de 100% est le meilleur. source des données : https://quantumcomputingreport.com/scorecards/qubit-quality/ et Google, D-Wave. intègre le record de 53 qubits de Google rendu public le 20 septembre 2019, les 4 qubits à ions piégés d'Honeywell dévoilés en mars 2020, et les 24 qubits supraconducteurs chinois de 2019.

La fidélité des portes à un qubit de Google est de 99,84% ce qui est une performance compte tenu du nombre de qubits. Le taux de fidélité des portes CZ à deux qubits des 24 qubits supraconducteurs chinois est de 99,5% et sujet à caution[266].

Ces taux d'erreurs sont pour l'instant prohibitifs dès que l'on enchaîne plusieurs portes quantiques d'affilée. À chaque opération, les taux d'erreurs s'additionnent, ou le taux de fiabilité se multiplie et sa résultante diminue si l'on veut être puriste. Imaginez l'enchaînement de quelques dizaines de portes quantiques à deux qubits ! A ce train, le taux d'erreur peut largement dépasser 50% d'erreurs à la fin de l'algorithme et, généralement, bien avant que l'on atteigne la limite fatidique du temps de cohérence des qubits. C'est une situation intenable.

D'où le fait que l'on évalue toujours la puissance d'un ordinateur quantique non pas simplement au nombre de qubits alignés mais au nombre d'opérations enchaînables avec un taux d'erreur raisonnable en fin de calcul. Pour éviter ce genre de contrainte quantitative, il faudrait disposer de qubits présentant des taux d'erreurs de portes quantiques de l'ordre de 10^{-10} voire 10^{-15}.

---

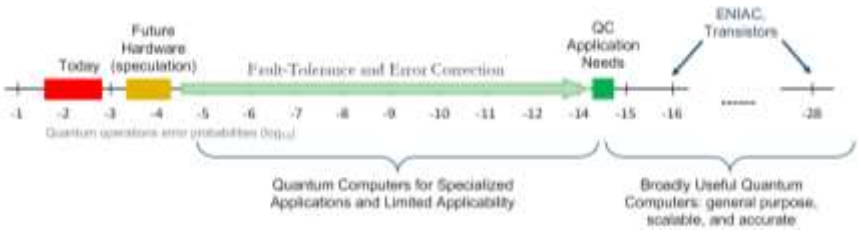
[263] Source des données sur la fiabilité des qubits : Qubit Quality sur le site Quantum Computing Report, avril 2019.

[264] Voir An introduction to quantum error correction de Mazyar Mirrahimi, 2018 (31 slides) ainsi que Introduction to quantum computing par Anthony Leverrier et Mazyar Mirrahimi, mars 2020 (69 slides) qui la complète bien.

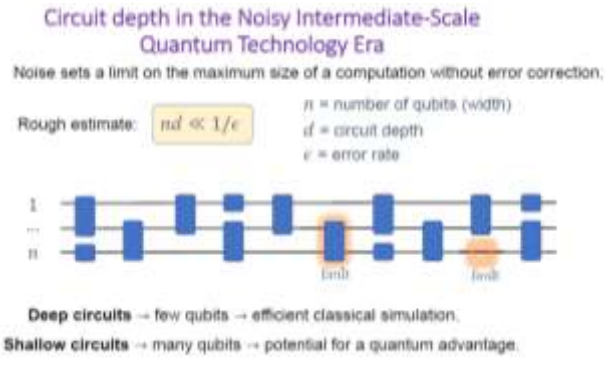
[265] Voir le papier de la NASA et Google qui décrit la performance de Google : Quantum Supremacy Using a Programmable Superconducting Processor par Eleanor G. Rieffel et al, août 2019 (12 pages).

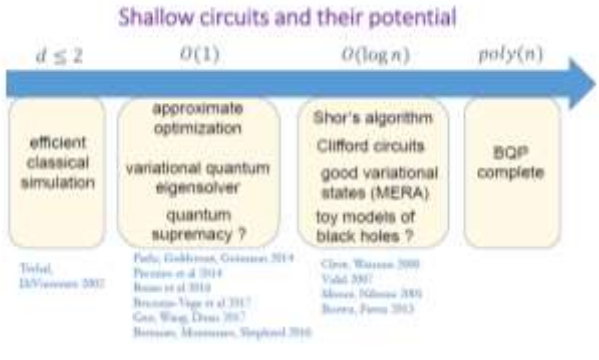
[266] Source des données : Superconducting Quantum Computing par Xiaobo Zhu, juin 2019 (53 slides).

Le schéma *ci-contre* illustre ce décalage entre les qubits physiques d'aujourd'hui et le besoin pour réaliser des calculs fiables (sans correction d'erreurs)[267].

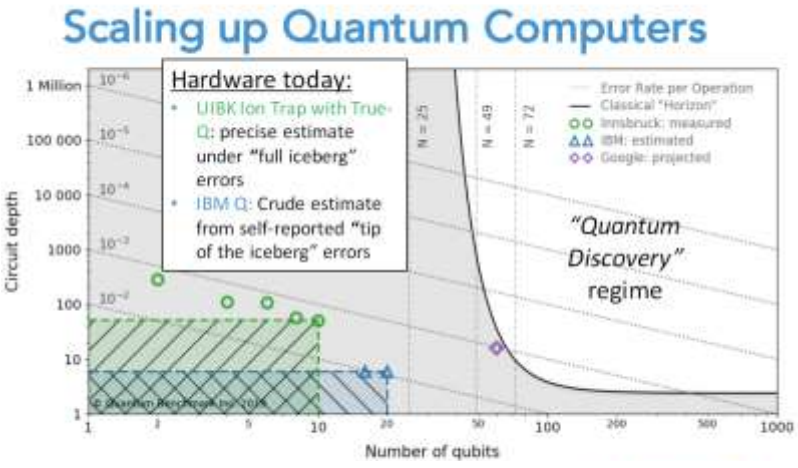


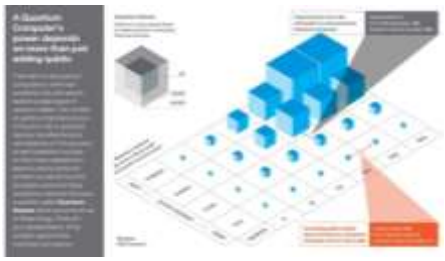
Une formule permet d'évaluer la dépendance entre le taux d'erreur des portes quantiques (e), le nombre de qubits (n) et le nombre de portes enchaînables (d), appelé « profondeurs de circuit » (circuit depth) : nd < 1/e [268]. Plus le taux d'erreurs baisse, plus la profondeur exploitable de circuits augmente, et le périmètre des algorithmes utilisable s'élargit.

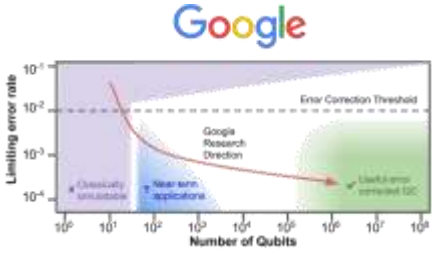




C'est présenté d'une autre manière dans ce schéma de **Quantum Benchmark** avec en abscisses le nombre de qubits et en ordonnées la profondeur des circuits (nombre de portes enchaînables dans un calcul quantique), conditionné par les pointillés en biais qui correspondent aux taux d'erreur des portes quantiques. La zone blanche est celle de la suprématie quantique [269] aussi dénommée « *quantum discovery regime* ».







[267] Source du schéma : How about quantum computing? par Bert de Jong, juin 2019 (47 slides).

[268] Source du schéma : Quantum advantage with shallow circuits Robert König, 2018 (97 slides)

[269] Slides présentés par Joseph Emerson de Quantum Benchmark à la conférence Quantum Computing Business organisée à Paris le 20 juin 2019 par Bpifrance. Ils positionnent Google tout près de la zone d'intérêt avec leurs 72 qubits, mais des benchmarks publics de ces qubits n'ont pas encore été publiés après l'annonce de leur réalisation en mars 2018. Les 53 qubits de la génération Sycamore annoncée en octobre 2019 sont cependant à peu près au même endroit (losange violet).

Tout ceci explique pourquoi IBM communique sur le couple nombre de qubits et le taux d'erreurs et sur la notion de **volume quantique** que nous décrirons plus loin. Microsoft et Google font de même dans leur pédagogie, sans pour autant avoir adopté la métrique simplificatrice du volume quantique d'IBM.

Pour qu'un ordinateur quantique serve à quelque chose, il faut à la fois disposer de beaucoup de qubits, d'un faible taux d'erreurs des portes quantiques et de la mesure de leur état et enfin un long temps de cohérence des qubits pour pouvoir exécuter des algorithmes sans contrainte de durée[270].

Évaluation du taux d'erreurs

Comment évalue-t-on le taux d'erreur des portes quantiques et de la mesure de l'état des qubits ? On utilise principalement le processus de **Randomized Benchmarking** (RBM) qui consiste à enchaîner une séquence de portes quantiques aléatoire dont on connaît à l'avance le résultat et à comparer le résultat obtenu avec celui que l'on connaît. Le taux d'erreur augmente au gré du nombre de portes quantiques enchaînées et de leur type. On peut évaluer le taux d'erreur d'une porte donnée avec l'**Interleaved RBM** qui injecte ladite porte périodiquement dans le jeu de portes aléatoires utilisé. On mesure alors la différence de taux d'erreur entre la séquence avec et sans ces portes quantiques ajoutées[271].

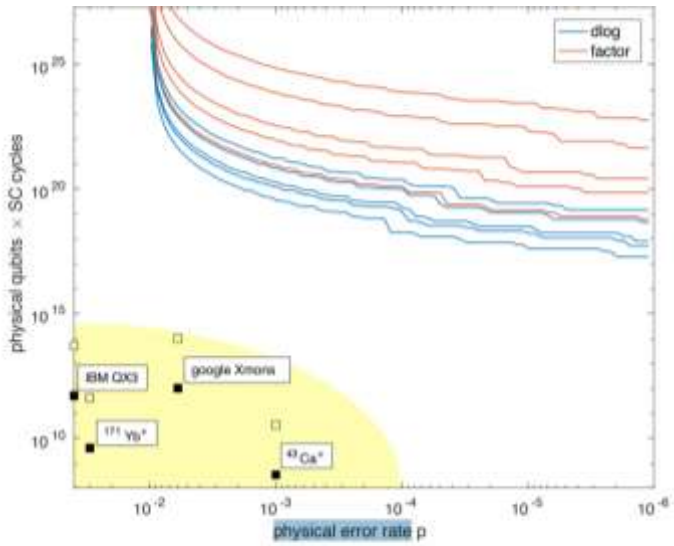


Figure 2.4: Comparison of algorithmic demands with currently achieved hardware performance. The plot shows required resources as number of qubits times rounds of error correction in the surface code for dlog (blue) and factoring (orange) for common key sizes as a function of the physical error rate p. The squares show current realizations assuming one day run time (solid) or 100 days (empty), the yellow area shows expected near-term progress. Both scales are logarithmic.

Il faut fouiller ailleurs pour en savoir plus[272]. La méthode RBM présente quelques inconvénients pour quantifier de manière propre le bruit. Elle n'est apparemment pas adaptée à la détection de modèles de bruits quelconques.

Plusieurs autres méthodes existent comme la **tomograghie d'états quantiques** (quantum state tomography) qui s'appuie sur une mesure répétée d'état de qubits qui permet de reconstruire une matrice densité moyenne et les erreurs associées, pour un qubit ou deux qubits après un calcul.

Une autre méthode existe basée sur des outils mathématiques qui identifient une correspondance entre le taux de bruit des portes à un et deux qubits d'un algorithme et le taux de bruit total de l'algorithme complet. Bref, en reliant le bruit macro (algorithme) au bruit micro (portes quantiques).

---

[270] Sources : IBM Bolsters Quantum Capability, Emphasizes Device Differentiation, 2017, et pour Microsoft, un extrait de la vidéo Future Decoded Quantum Computing Keynote, novembre 2017.

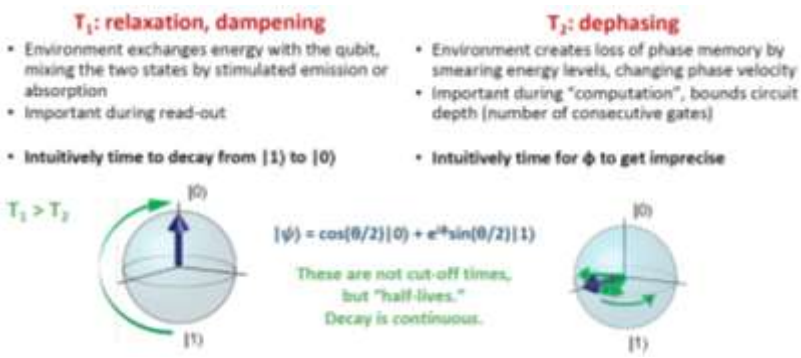
[271] J'ai trouvé cette information dans Quantum Computing: Progress and Prospects 2018 (206 pages), page 2-20. Le processus de benchmarking de portes quantiques est détaillé dans Randomized benchmarking for individual quantum gates d'Emilio Onorati et al, 2018 (16 pages). L'origine de la méthode est Scalable noise estimation with random unitary operators de Joseph Emerson et al, 2005 (8 pages). Voir cet autre protocole de test, plus récent : Efficient learning of quantum noise par Robin Harper et al, 2019 (15 pages).

[272] Comme dans le rapport Entwicklungsstand Quantencomputer déjà cité (*état des lieux de l'informatique quantique*) de l'ANSSI allemande, qui date de 2018 et qui met en évidence l'énorme décalage entre les performances des qubits, notamment chez IBM et Google, et le besoin lié à la factorisation de nombres entiers pour casser des clés RSA courantes. Voir aussi Efficient learning of quantum noise par Robin Harper et al, Nature Communications, 2019 (15 pages) ainsi que Characterization, certification and validation of quantum systems par Martin Kliesch, avril 2020 (87 pages).

Types d'erreurs

On peut distinguer trois types d'erreurs à corriger :

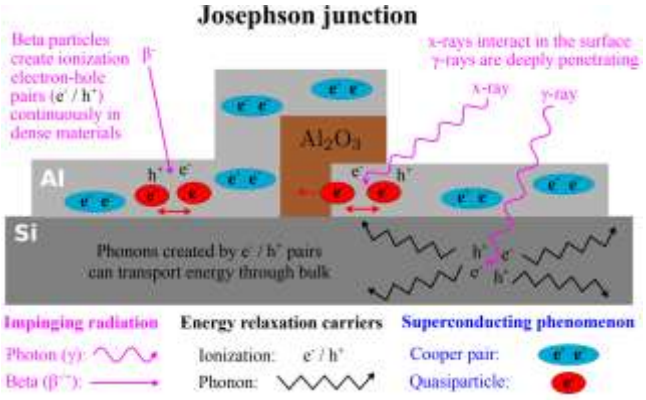
- Les **erreurs de flip** comme *ci-contre* dans la sphère de Bloch, sont des erreurs d'amplitude rabattant le vecteur de $|1\rangle$ vers $|0\rangle$.
- Les **erreurs de phase** sont des rotations autour de l'équateur[273].



- Les **erreurs de fuite** (leakage errors) qui voient le qubit dériver et se stabiliser dans un autre état énergétique que le $|0\rangle$ ou le $|1\rangle$ de base. Cela peut se produire dans le niveau $|2\rangle$ d'un qubit supraconducteur, que l'on cherche à éviter, ou avec des variantes de niveaux d'énergie hyperfins de qubits à ions piégés.

Leurs sources sont multiples, qui entraînent notamment la **décohérence** progressive des qubits qui affecte notamment les états intriqués. Elles sont liées aux interactions diverses entre les qubits et leur environnement immédiat[274]. On compte notamment :

- Les **erreurs de calibrage** des portes quantiques qui interviennent notamment dans celui des qubits supraconducteurs. Ce sont elles qui peuvent notamment déclencher les erreurs de fuite.
- Le **bruit thermique** issu des composants alentours des qubits. C'est la raison de l'existence d'atténuateurs autour des qubits supraconducteurs et de leur fonctionnement à très basse température.
- Le bruit d'origine **électrique** et **magnétique** qui peut avoir pas mal d'origines selon les qubits.
- Les erreurs issues des **fluctuations quantiques du vide**[275], que nous avons étudiées rapidement dans une partie précédente.
- Celles qui sont issues des **effets de la gravité**[276]. Ces deux types d'erreurs semblent être cependant mineurs par rapport aux précédents.
- Les effets de la **radioactivité**, qui se manifestent par l'émission de rayons X, gamma et de particules beta et leurs effets ionisants. Le phénomène peut être partiellement réduit avec un épais blindage en plomb du processeur[277].



---

[273] Source du schéma : How about quantum computing? par Bert de Jong, juin 2019 (47 slides).

[274] N'importe quelle opération sera d'ailleurs génératrice d'erreur. Une erreur peut être générée au moment de la correction, au moment de la détection ou au moment de l'application d'une porte. Ne rien faire sur un qubit peut aussi générer des erreurs du fait de son temps de cohérence fini.

[275] Voir Observation of quantum many-body effects due to zero point fluctuations in superconducting circuits par Sébastien Léger, Nicolas Roch et al, Institut Néel, 2019 (8 pages) qui décrit le phénomène sur des qubits supraconducteurs.

[276] Voir au sujet de la gravité : A model of quantum collapse induced by gravity par Franck Laloë, 2020 (14 pages).

[277] Voir Impact of ionizing radiation on superconducting qubit coherence par Antti P. Vepsäläinen et al, août 2020 (24 pages).

D'une manière générale, les erreurs sont générées par des interactions diverses, électromagnétiques ou mécaniques, entre les qubits et leur environnement immédiat et sont associées au phénomène de la décohérence quantique. Le premier objectif des physiciens est évidemment de réduire ces sources d'erreur physiques.

Ils progressent régulièrement mais arrivent à peine à gagner un à deux ordres de grandeur en taux d'erreur alors qu'il en faudrait une bonne dizaine dans un monde idéal.

Catégories de codes de correction d'erreurs

La principale solution de traitement du bruit explorée depuis plus de deux décennies consiste à mettre en œuvre des codes de correction d'erreurs que l'on appelle **QEC** pour Quantum Error Correction ou plutôt **QECC** pour QEC Codes[278]. L'autre solution envisagée est celle du NISQ, pour Noisy Intermediate Scale Quantum computers, ces ordinateurs quantiques actuels qui sont bruités et non corrigés. On fait cela avec des algorithmes, souvent hybrides classiques/quantiques, qui se satisfont de cette situation. Deux autres approches existent comme le calcul à recuit quantique, notamment chez D-Wave, qui est aussi bruité, et la simulation quantique, qui reproduit des phénomènes physiques quantiques avec des dispositifs quantiques bruités.

Les codes de correction d'erreurs s'appliquent aussi bien au calcul quantique à portes universelles qu'aux télécommunications quantiques. Dans le premier cas, ils sont intégrés dans la notion de calcul quantique à tolérance de panne (**FTQC** – fault-tolerance quantum computing) qui est synonyme de **LSQC** (large-scale quantum computing).

Il faut d'ailleurs distinguer les codes de correction d'erreurs logiques et les codes physiques qui sont directement gérés dans le matériel comme les codes bosoniques dont font partie les cat-codes[279], le GKP et les codes binomiaux. Ces derniers mettent en œuvre dans une cavité un « chat de Schrödinger » qui permet de gérer un espace de projection servant à la correction d'erreur, comme dans les algorithmes de correction d'erreur à base de codes stabilisateurs que nous verrons plus loin.

Le schéma *ci-dessous* en bleu propose un inventaire des principaux codes de correction d'erreurs avec leur origine et date de création[280]. Ce zoo des algorithmes de correction d'erreur est très dense[281]. C'est un champ scientifique très riche des technologies quantiques et qui évolue régulièrement depuis 1995. Il comprend plusieurs familles de codes de correction d'erreurs.

Les plus connus sont les **codes stabilisateurs** qui corrigent les erreurs de flip et/ou de phase à trois, cinq (Laflamme), sept (Steane) ou neuf qubits (Shor). Ces codes répliquent plusieurs fois par intrication les qubits de calcul pour leur faire subir le même traitement en parallèle et à comparer les résultats en sortie d'algorithmes pour conserver les résultats statistiquement dominants.

Le tout sans lire la valeur des qubits qui ferait effondrer tout le système et en respectant donc le théorème de non-clonage des qubits. Cela passe par l'utilisation de qubits auxiliaires qui servent à détecter des syndromes d'erreurs sans affecter les qubits du calcul. L'astuce consiste à dupliquer l'information sur plusieurs qubits de telle manière que la mesure permettant de détecter si une erreur est intervenue modifiera probablement l'état de ces qubits mais sans détériorer l'information qu'ils contiennent.

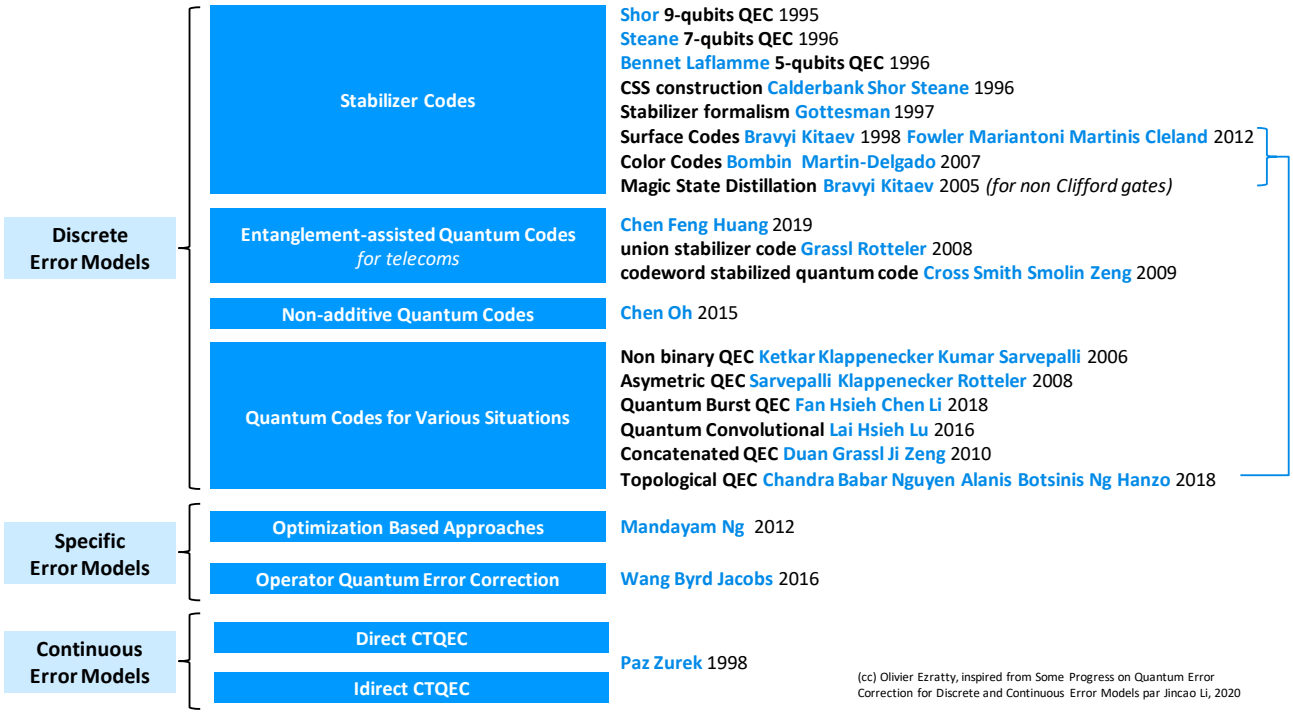
---

[278] Ce thème a comme de nombreuses spécialités quantiques sa propre conférence. Voir International Conference on Quantum Error Correction et les vidéos de toutes les présentations de l'édition 2019.

[279] Ils sont employés par la startup Alice&Bob. Sachant que leur création remonte aux travaux de Michel Devoret, repris par un bon nombre de ses thésards, dont Zaki Leghtas, avec qui ont travaillé les fondateurs d'Alice&Bob. L'actualité des codes de correction d'erreurs est incessante. Ainsi, une proposition émergeait récemment de QEC qui va plus loin que les cat-code et ne dépend pas de l'architecture matérielle. Voir Novel error-correction scheme developed for quantum computers, mars 2020 qui fait référence à Quantum computing with rotation-symmetric bosonic codes par Arne L. Grimsmo, Joshua Combes et Ben Q. Baragiola, septembre 2019.

[280] Illustration inspirée d'un schéma découvert dans Some Progress on Quantum Error Correction for Discrete and Continuous Error Models par Jincao Li, 2020 (15 pages).

[281] Voir Quantum Error Correction for Beginners par Simon J. Devitt, William J. Munro, et Kae Nemoto, 2013 (41 pages).



On s'arrange donc pour que les mesures que l'on devra faire permettant de détecter si une erreur est intervenue ou pas, effectuent des modifications sur l'état qui préservent la structure de l'information.

Le bestiaire de la QEC comprend aussi les codes topologiques dont les **codes de surface** et les **color codes**[282] et plein d'autres spécimens comme le protocole **DFS** (Decoherence Free Subspaces) qui encode l'information quantique dans un sous-espace qui n'est pas affecté par les erreurs physiques ou des codes dits holographiques.

Il existe aussi une méthode à base de **réseaux de neurones**, issue de chercheurs de l'Université d'Erlangen en Allemagne[283]. Les codes de correction d'erreurs ne sont pas les seuls dans l'arsenal contre les erreurs. On peut aussi y intégrer les **algorithmes quantiques** qui sont eux-mêmes résistants aux erreurs.

Cela fait du monde et pas mal de concepts à digérer ! Nous allons juste effleurer le sujet en couvrant les principaux principes utilisés dans la QEC. Les références bibliographiques vous permettront de creuser la question.

Le principe général d'un code de correction d'erreur classique est illustré dans le schéma *ci-dessous* avec une correction en six étapes[284] :

1. **Réplication** et **encodage** : le qubit à corriger va d'abord être répliqué un certain nombre de fois via des portes CNOT sur plusieurs qubits auxiliaires (ici 2). Les qubits résultants sont intriqués.
2. **Traitement** : un traitement a lieu qui va potentiellement générer une erreur. Cela peut aussi bien être un calcul qu'une transmission télécom du qubit.
3. **Détection d'erreur** : un ou des syndromes d'erreurs sont détectés via des portes quantiques qui associent les qubits à d'autres qubits auxiliaires. Nous détaillerons ce procédé un peu plus loin.

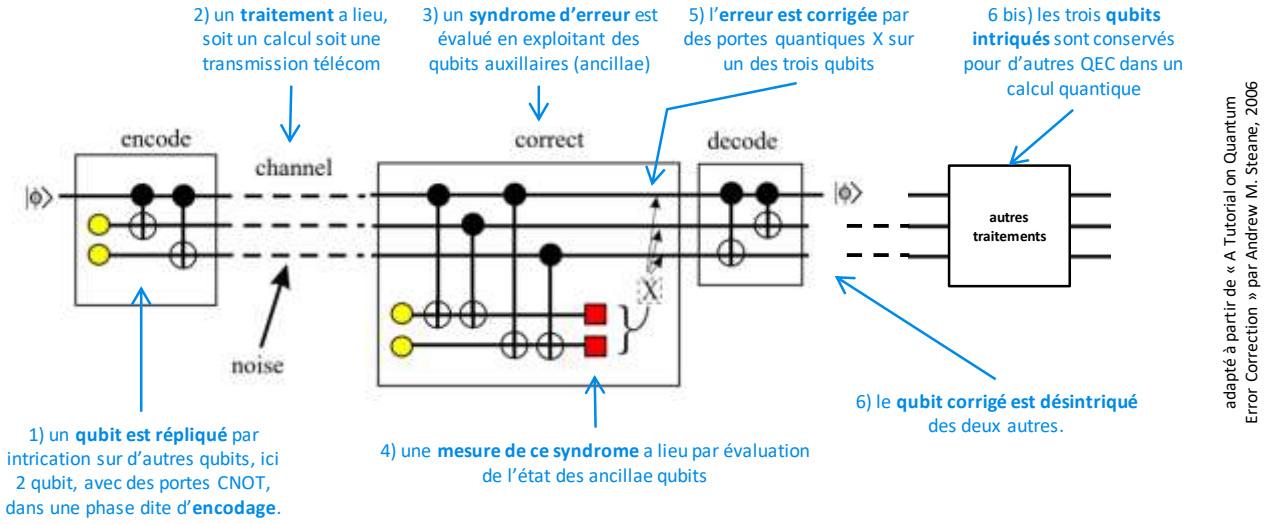
---

[282] Les color codes sont des variantes de codes stabilisateurs. Voir quelque explications dans The Steep Road Towards Robust and Universal Quantum Computation par Earl T. Campbell, Barbara M. Terhal et Christophe Vuillot, 2016 (10 pages).

[283] Voir Neural networks enable learning of error correction strategies for quantum computers, octobre 2018 et Reinforcement Learning with Neural Networks for Quantum Feedback, Thomas Fösel et al, 2018 (7 pages).

[284] Inspiré de A Tutorial on Quantum Error Correction par Andrew M. Steane, 2006 (24 pages). Voir aussi An introduction to quantum error correction par Mazyar Mirrahimi, 2018 (31 slides).

4. **Mesure de syndrome d'erreur** : l'état de ces qubits auxiliaires est mesuré pour devenir des bits classiques. Lorsque plusieurs qubits sont mesurés, cela permet d'obtenir l'indice du qubit à corriger dans ceux du dessus dans le schéma.
5. **Correction d'erreur** : la mesure sert ensuite à corriger le qubits défectueux avec une porte X (ou Z si l'on corrige une erreur de phase). Il existe des formes alternatives de QEC ne passant pas par la mesure du syndrome par lecture de qubit mais par son utilisation directe avec des portes quantiques qui corriger le qubit défectueux sans passer par des bits classiques.
6. **Consolidation** : enfin, les qubits corrigés sont éventuellement désintriqués. Cette consolidation semble être appliquée pour les codes de correction d'erreur utilisés dans les télécommunications quantiques. Pour la correction d'erreur appliquée au calcul quantique, l'ensemble des trois qubits corrigés doit pouvoir être conservé pour passer à l'étape suivante, à savoir une autre opération de calcul à corriger.



Les schémas habituels de présentation de codes de correction d'erreur comme celui de Shor sur Wikipedia n'en présentent pas toujours la totalité ou alors ce sont des versions sans mesure/correction mais avec une correction directe des erreurs[285].

Ils ne précisent pas non plus l'endroit où l'on positionne les codes de correction d'erreur dans un algorithme quantique. Il semble que l'on doive le faire à plusieurs étapes du calcul quantique. Un code de correction d'erreurs va être répété un nombre de fois qui est à peu près proportionnel à la profondeur de calcul de son algorithme quantique. Cela va être le rôle des compilateurs de réaliser ce positionnement. Il pourra dépendre de la connaissance dont il dispose des taux de fidélité des portes quantiques utilisées dans la configuration. La QEC va au passage augmenter la durée du calcul d'un à plusieurs ordres de grandeur dépendant du ratio de qubits physiques par qubits logiques. La correction d'erreur peut être aussi vue comme un moyen de ralentir la décohérence des qubits et de prolonger le temps de calcul.

Si on reprend la généalogie de ces codes, il faut commencer par les QEC les plus simples qui corrigent les erreurs de signe de qubits avec trois qubits. Un algorithme voisin corrige les erreurs de phase de qubits[286] en exploitant des portes de Hadamard de superposition d'état.

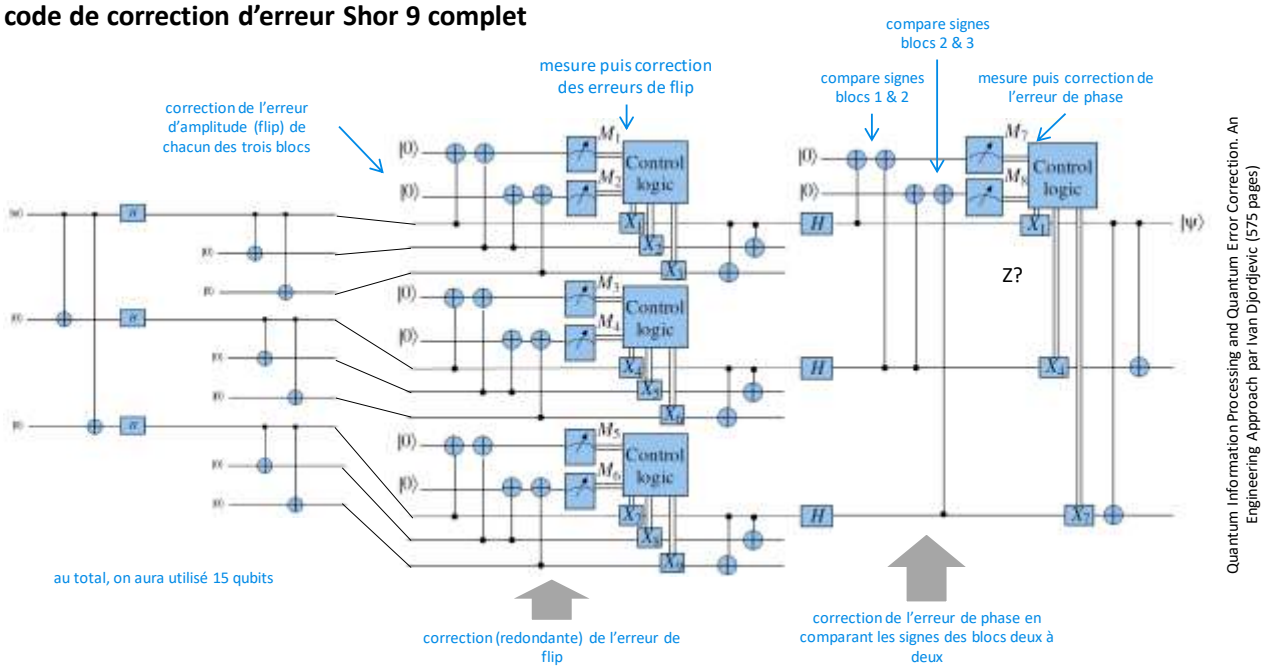
---

[285] Voir Quantum Error Correction An Introductory Guide par Joschka Roffe, 2019 (29 pages) qui explique le fonctionnement générique des codes de correction d'erreurs ainsi que Quantum Error Correction for Beginners par Simon Devitt, William Munro et Kae Nemoto, 2013 (41 pages). Ce sont les deux principales sources d'information qui m'ont permis de rédiger ces pages sur la QEC. Voir aussi une description de divers codes de correction d'erreurs dans Software for Quantum Computation, une thèse de Daniel Matthias Herr de l'ETZ Zurich, 2019 (164 pages).

[286] Source du schéma : Quantum error correction par Fred Bellaiche, avril 2018.

Le **code de correction d'erreur de Shor** de 1995 à 9 qubits est une synthèse de ces méthodes, qui conduit un qubit donné à être répliqué 8 fois. Ce code permet de corriger à la fois les erreurs de flip et de phase[287]. Voici à quoi ressemble un tel code complet[288].

code de correction d'erreur Shor 9 complet



Raymond Laflamme (1960, Canada) a démontré en 1996 qu'il faut au moins disposer de cinq qubits physiques pour créer un « qubit logique » intégrant la correction d'erreurs de flip et de phase[289].

En pratique, le code de **Steane** à 7 qubits est le plus utilisé car il n'est pas redondant comme celui de Shor. Ces codes à 3, 5, 7 et 9 qubits font partie d'un groupe générique appelé **codes stabilisateurs** formalisé par Daniel Gottesman en 1997. Nous allons maintenant creuser un peu leur fonctionnement.

Projections et stabilisateurs

Nous allons comprendre comment une correction d'erreur fonctionne sans lire l'état du qubit à corriger. Reprenons le cas d'un code de correction d'erreur de flip simple à trois qubits.

Ces trois qubits intriqués peuvent subir une erreur X_1, X_2 ou X_3 ou pas d'erreur (I = identité). X est une porte de Pauli d'inversion d'amplitude. Elle va entraîner l'inversion d'amplitude du qubit intriqué correspondant comme indiqué dans les équations *ci-contre*.

$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{I} \alpha|000\rangle + \beta|111\rangle,$$
$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{X_1} \alpha|100\rangle + \beta|011\rangle,$$
$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{X_2} \alpha|010\rangle + \beta|101\rangle,$$
$$|\psi_L\rangle = \alpha|000\rangle + \beta|111\rangle \xrightarrow{X_3} \alpha|001\rangle + \beta|110\rangle.$$

Ces nouveaux états correspondent à trois erreurs et à l'absence d'erreur. Ces quatre états présentent l'intérêt d'être mathématiquement orthogonaux pour toutes les valeurs de l'α et du β qui caractérisent l'état du qubit à corriger. L'astuce consiste à réaliser une mesure de ces valeurs dans l'espace vectoriel correspondant à ces quatre valeurs et pas dans la base computationnelle d'origine du qubit.

---

[287] Le détail du processus est bien documenté dans la fiche Wikipedia de la correction d'erreur quantique.

[288] Adapté d'un schéma trouvé dans Quantum Information Processing and Quantum Error Correction. An Engineering Approach par Ivan Djordjevic (575 pages).

[289] C'est démontré dans A Theory of Quantum Error-Correcting Codes par Emanuel Knill et Raymond Laflamme, 1996 (34 pages). Mais aussi indépendamment dans Mixed State Entanglement and Quantum Error Correction par Charles H. Bennett, David P. DiVincenzo, John A. Smolin et William K. Wootters, 1996 (82 pages).Voir aussi Magic States de Nathan Babcock (28 slides).

Cela ne détruira donc pas l'état de superposition l'état d'origine du qubit. L'extraction de syndrome est appelée un "stabilizer code" ou code de stabilisation, qui va alimenter les qubits auxiliaires (ancila). Cela permet de corriger avec des portes X les qubits qui ont ... flippé ! Le procédé est le même pour évaluer et corriger une erreur de phase mais avec des portes Z à la place de portes X.

code de correction d'erreur de flip à trois qubits

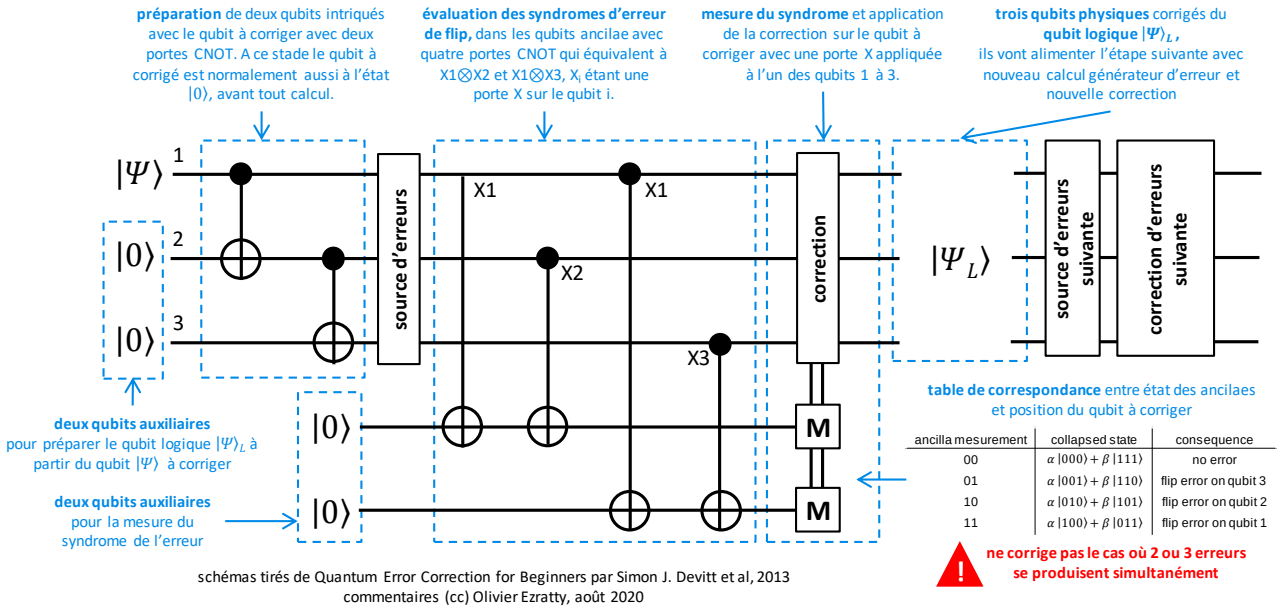


table de correspondance entre état des ancilaes et position du qubit à corriger

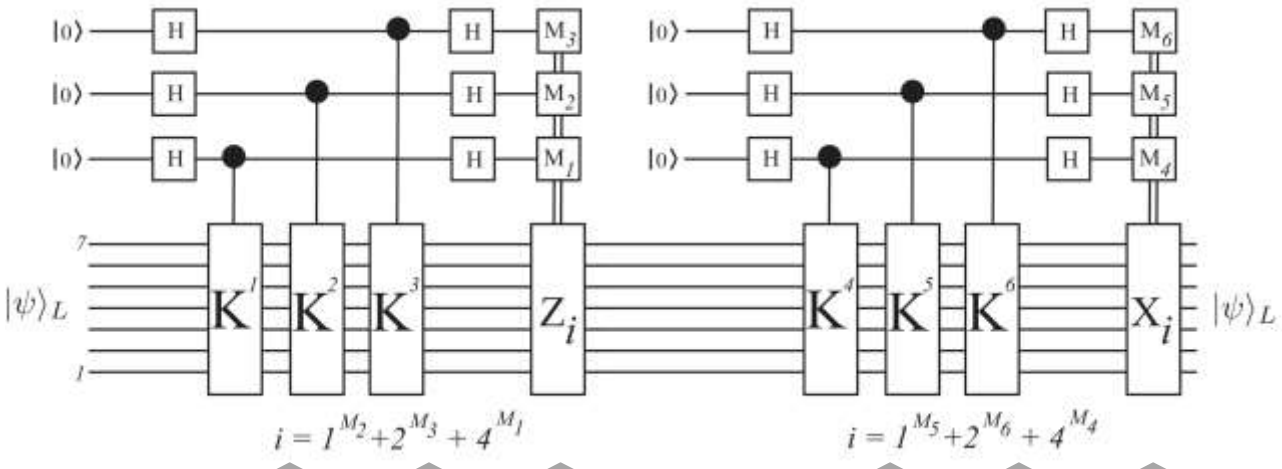
ancilla mesurement	collapsed state	consequence
00	$\alpha\|000\rangle + \beta\|111\rangle$	no error
01	$\alpha\|001\rangle + \beta\|110\rangle$	flip error on qubit 3
10	$\alpha\|010\rangle + \beta\|101\rangle$	flip error on qubit 2
11	$\alpha\|100\rangle + \beta\|011\rangle$	flip error on qubit 1

ne corrige pas le cas où 2 ou 3 erreurs se produisent simultanément

schémas tirés de Quantum Error Correction for Beginners par Simon J. Devitt et al, 2013
commentaires (cc) Olivier Ezratty, août 2020

L'inconvénient de la solution est qu'elle ne peut pas détecter les erreurs qui interviendraient en même temps sur deux ou trois des qubits intriqués. Aucun code de correction d'erreurs n'est capable de corriger toutes les erreurs !

code de correction d'erreur 7 qubits complet dit [[7,1,3]] dans le formalisme des stabilisateurs



K_1 à K_6 sont des codes stabilisateurs de détection de bit de parité

détection d'erreur de phase

calcul de i, l'adresse du qubit à corriger

correction de l'erreur sur le qubit i

schémas tirés de Quantum Error Correction for Beginners par Simon J. Devitt et al, 2013

détection d'erreur de flip

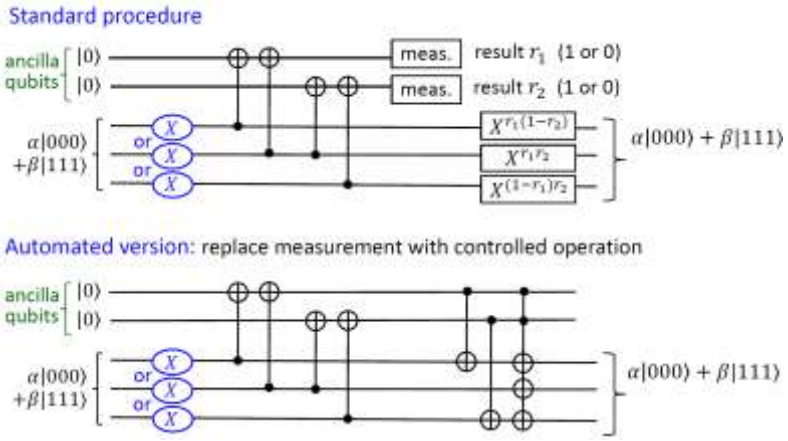
calcul de i, l'adresse du qubit à corriger

correction de l'erreur sur le qubit i

Le formalisme des codes stabilisateurs décrit de manière générique les codes de correction d'erreurs que nous venons d'étudier avec trois paramètres : **[[n, k, d]]**. n est le nombre de qubits physiques utilisé dans le code. k est le nombre de qubits logiques, en général 1, et d est le plus petit nombre d'erreurs qui peuvent être corrigées simultanément ("*the smallest number of simultaneous qubit errors that can transform one valid codeword into another*"... pas facile à suivre !). Dans cette notation, le code de Shor à 9 qubits est un [[9, 1, 3]], celui de Steane est [[7, 1, 3]], celui de Laflamme est un [[5, 1, 3]] et un code de correction de flip ou de phase à trois qubits est un [[3, 1, 1]].

Les codes stabilisateurs utilisent une table de syndrome qui fournit une correspondance entre les erreurs sur chaque qubit et le syndrome détecté. Il faut donc que le nombre de qubits auxiliaires de création de cette table soient en nombre suffisant pour identifier celui des qubits du qubit logique à corriger. Dans l'exemple ci-dessus avec un qubit logique à 7 qubits physiques, les 3 qubits auxiliaires permettent d'identifier huit scénarios, suffisants pour déterminer lequel des 7 qubits physiques doit être corrigé. Le huitième scénario est l'absence d'erreur, donc pas de correction.

Il semble que l'on puisse appliquer la correction dans les qubits de deux manières : celle qui est présentée jusqu'à présent avec une mesure des qubits auxiliaires de parité générant des bits classiques permettant de déterminer sur quels qubits appliquer une porte quantique de correction d'erreur, et une autre méthode permettant de se passer de la mesure et d'appliquer directement la correction avec des portes quantiques.



La première solution semble être plus couramment utilisée mais la seconde permettrait de mieux gérer l'équilibre énergétique de l'ensemble, la lecture des qubits auxiliaires et le passage par un canal classique consommant plus d'énergie l'entropie générée par les erreurs (comparaison *ci-dessus*[290]). Le mécanisme autonome est aussi une voie permettant éventuellement de rendre la correction d'erreur autonome au sein d'un processeur quantique, sans passer par la partie classique au cas où la commande des qubits est réalisée en étant très proche de ces derniers.

Portes et états non discrets

Un code de Shor et Steane peut corriger toute erreur de Pauli, y compris de porte Y, qui est égale à iZX. Ils peuvent corriger toute combinaison linéaire de portes I, X, Y et Z avec des nombres complexes. Cela vient du fait que toute opération unitaire sur un qubit peut s'exprimer sous la forme d'une combinaison de IXYZ avec des facteurs complexes : U = aI + bX + cY + dZ. Cela veut donc dire, indirectement, que ces QEC devraient pouvoir corriger les erreurs analogiques et continues comme de légères variations d'amplitudes ou de phase, soit des rotations de quelques degrés dans la sphère de Bloch.

Pour corriger ces erreurs correspondantes à des portes hors du groupe de Clifford telles qu'une porte T (huitième de rotation dans la sphère de Bloch), on utilise cependant également des **magic states** qui alimentent des circuits réalisés avec des portes du groupe de Clifford. Ces états sont préparés par un processus dénommé **magic state distillation**[291].

---

[290] Vue dans Quantum error correction (QEC) par Alexander Korotkov (39 slides).

[291] Voir Universal quantum computation with ideal Clifford gates and noisy ancillas par Sergey Bravyi et Alexei Kitaev, 2004 (15 pages). Il existe d'autres solutions comme A fault-tolerant non-Clifford gate for the surface code in two dimensions par Benjamin J. Brown, mai 2020, qui s'applique aux surface codes.

Ces codes sont très importants pour bien tirer parti du calcul quantique. C'est lié au fait que l'avantage quantique par rapport au calcul classique se manifeste uniquement avec un jeu de portes classiques universel qui doit comprendre une porte qui n'est pas dans le groupe de Clifford, en général de type T. Et pour corriger les erreurs de cette porte, il faut des codes de correction d'erreur spécifiques comme le **magic state distillation**, qui est en quelque sorte un code de correction d'erreurs de codes de correction d'erreurs.

Correction d'erreurs en continu

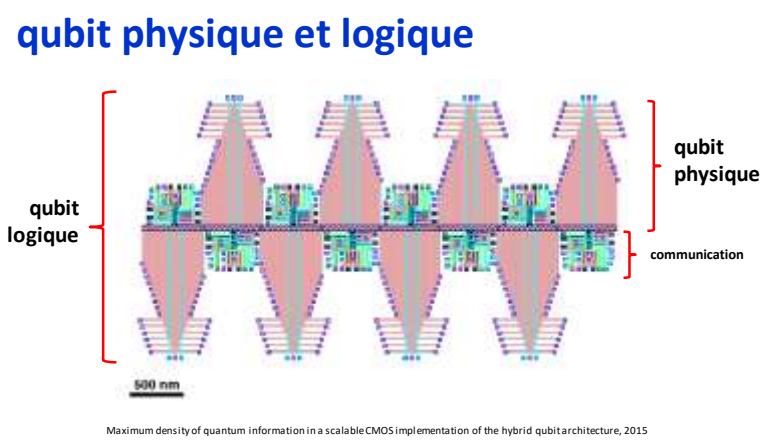
Juan Pablo Paz et Wojciech Hubert Zurek proposaient en 1998 un code de correction d'erreur fonctionnant en continu, le CTQEC, pour "continuous-time QEC" s'appuyant sur des équations différentielles et agissant à des intervalles de temps réduits. Il existe deux méthodes permettant d'agir directement sur l'information (direct CTQEC) ou via des qubits auxiliaires (indirect CTQEC). Je n'ai pas encore compris l'intérêt et le domaine d'application de ce type de QEC. Cela pourrait peut-être servir du côté des télécommunications quantiques.

Qubits logiques

Aujourd'hui et sur les calculateurs quantiques disponibles en ligne comme ceux d'IBM allant jusqu'à quelques dizaines de qubits, c'est le rôle des logiciels de mettre en œuvre des codes de correction d'erreur dynamiques et plus précisément, des compilateurs qui vont transformer le code du développeur en code machine exécutable au niveau physique des qubits et intégrant la QEC.

À terme, les qubits logiques pourront être mis en œuvre entièrement dans l'architecture matérielle, celle-ci n'exposant à l'ordinateur classique que des qubits logiques et non physiques. Cela simplifiera au passage la connectique entre l'ordinateur classique de contrôle et le calculateur quantique.

Une QEC (Quantum Error Correction) peut être ainsi réalisée au niveau matériel par création d'assemblage de qubits qui généreront des qubits logiques physiques prêts à l'emploi. En voici un exemple ancien avec sept qubits physiques supraconducteurs pour constituer un qubit logique[292]. Le nombre de qubits physiques à assembler pour créer un qubit logique dépend du taux d'erreurs des qubits.



Maximum density of quantum information in a scalable CMOS implementation of the hybrid qubit architecture, 2015

Plus le taux d'erreurs des qubits est élevé, plus grand doit être le nombre de qubits assemblés. Ce nombre peut atteindre plusieurs milliers de qubits [293]. Ce qui veut dire que pour avoir ne serait-ce que quelques centaines de qubits logiques à même d'atteindre la suprématie quantique pour des algorithmes quantiques assez simples, il faudrait disposer de plusieurs dizaines de millions de qubits physiques.

---

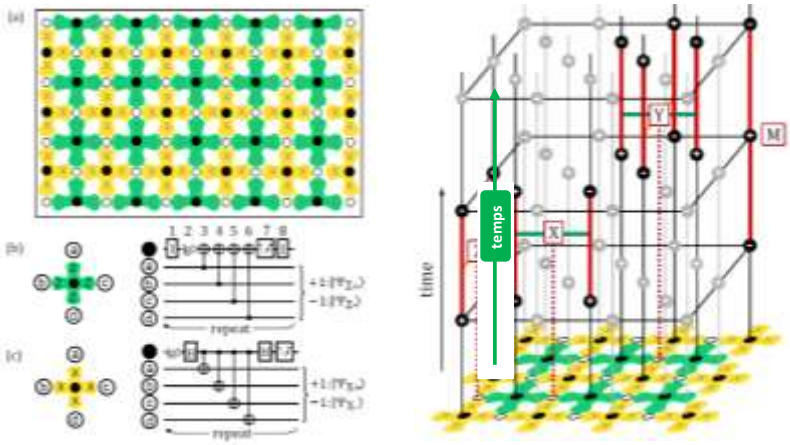
[292] Il vient de Maximum density of quantum information in a scalable CMOS implementation of the hybrid qubit architecture, 2015 (17 pages).

[293] Voir What determines the ultimate precision of a quantum computer? par Xavier Waintal, 2019 (6 pages) qui décrit pour sa part les limites des codes de correction d'erreur. Voici quelques autres contenus utiles sur la correction d'erreurs : Error mitigation in quantum simulation, Xiao Yuan, IBM Research, 2017 (42 minutes), Code Used To Reduce Quantum Error In Logic Gates For First Time, 2019, Scientists find a way to enhance the performance of quantum computers par l'University of Southern California, 2018 et Cramming More Power Into a Quantum Device de Jay Gambetta et Sarah Sheldon, mars 2019 à propos du niveau d'erreurs de l'IBM Q System One annoncé en janvier 2019.

On en est encore bien loin ! Les estimations courantes sont de 10 000 qubits physiques pour obtenir un qubit logique. Ainsi, la startup **PsiQuantum** prévoit-elle de générer 100 qubits logiques (photons) à partir d'un million de qubits physiques. Du côté des architectures physiques, les **qubits topologiques** sont une version analogique des *surface codes* qui devraient permettre de réduire ce ratio de qubits logiques/physique, tout comme les cat-qubits, déjà évoqués.

Pour les qubits qui peuvent être organisés de manière à être bien reliés physiquement avec leurs voisins immédiats, la correction d'erreurs la plus souvent envisagée s'appelle le **surface code**, datant de 2012[294].

Elle comprend des matrices de qubits de traitement (en blanc dans le schéma *ci-contre*) reliés à des qubits de mesure (en noir) via des portes de **Pauli X** (inversion) et **Pauli Z** (changement de phase).



Surface codes: Towards practical large-scale quantum computation, 2012

Cela donne deux qubits auxiliaires pour deux qubits physiques organisés dans la logique ci-dessous permettant de corriger des erreurs de flip et de phase. Cela constitue un code stabilisateur de type [[5, 1, 2]] rassemblant quatre blocs à quatre cycles (schéma *ci-dessous*, à droite). Ces surface codes sont tolérants à un taux d'erreurs plus élevé des qubits, par contre, ils demandent un plus grand nombre de qubits physiques par qubits logiques. La création de surface code crée une contrainte de conception pour les qubits physiques qui doivent pouvoir être reliés à leurs voisins immédiats dans une structure 2D. Cela procure actuellement un avantage à la topologie des qubits de Google par rapport à celle d'IBM pour les qubits supraconducteurs, que nous visualiseront dans une partie suivante.

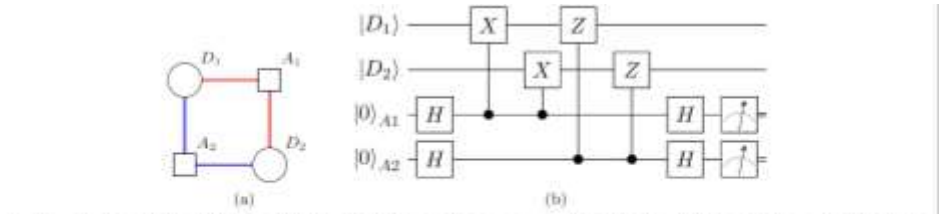
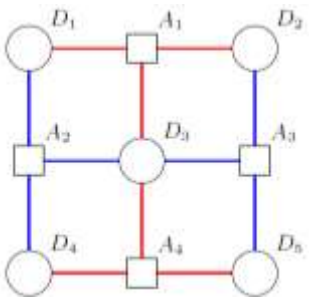


Figure 7. The surface code four-cycle. (a) Pictorial representation. The code qubits, D_1 and D_2, are represented by the circular nodes. The ancilla qubits, A_1 and A_2, are represented by the square nodes. The red and blue edges depict controlled-X and controlled-Z operations controlled on the ancilla qubits and acting on the code qubits. (b) An equivalent surface code four-cycle in circuit notation.



Fault Tolerant Quantum Computing

Dans le calcul quantique, la QEC est la voie permettant de créer du calcul quantique à tolérance de panne et son corollaire, le calcul quantique à grande échelle, respectivement **FTQC** pour fault-tolerance quantum computing et **LSQC** pour large-scale quantum computing.

Le FTQC s'appuie sur quelques principes généraux : une préparation d'états tolérante aux erreurs, des portes quantiques tolérantes aux erreurs, une mesure tolérante aux erreurs et une correction d'erreur elle-même tolérante aux erreurs.

[294] Les surface code sont bien formalisés dans l'épais Surface codes towards practical large-scale quantum computation, 2012 (54 pages) mais leur source d'inspiration est plus ancienne et provient de Quantum codes on a lattice with boundary par Sergey Bravyi et Alexei Kitaev, 1998 (6 pages). En pratique, la structure des surface codes est assez complexe et met en jeu des sous-structures activées et désactivées dans la matrice des qubits.

En effet, les codes de correction d'erreurs peuvent eux-mêmes introduire des erreurs puisqu'ils font appel à des portes quantiques et des mesures d'état eux-mêmes générateurs d'erreurs. Par ailleurs, les codes de correction d'erreurs ne corrigent pas toutes les erreurs qui peuvent se produire. Ils augmentent le taux de fidélité apparent des qubits corrigés.

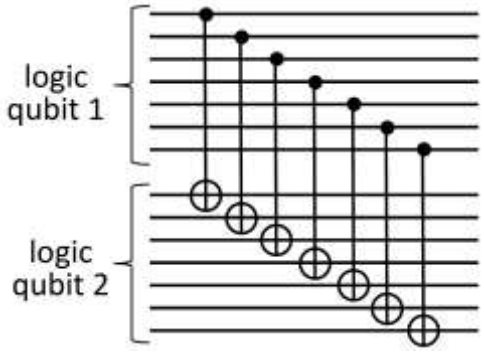
La FTQC suppose aussi l'usage de codes de correction d'erreurs de manière répétée pendant de longs calculs, sans que cela introduise plus d'erreurs que cela n'en corrige. La QEC permet ainsi en théorie d'exécuter des algorithmes de longueur arbitraire alors que sans QEC, on est limité comme pour les 20 séries de portes de la suprématie quantique de Google avec Sycamore d'octobre 2019.

Dans le détail, il s'agit de s'assurer que les méthodes de calcul et de QEC employées empêchent les erreurs de se propager en cascade. On va ainsi éviter de relier un qubit par intrication avec trop de qubits dans les QEC. De ce point de vue-là, une QEC à base de Steane code à 7 qubits est appropriée. Il faut éviter la trop grande propagation des erreurs, surtout via les portes à plusieurs qubits. Ainsi, il faut tenir compte du fait qu'une porte CNOT propage les erreurs de flip du qubit de contrôle vers le qubit cible et les erreurs de phase de la cible vers le contrôle.

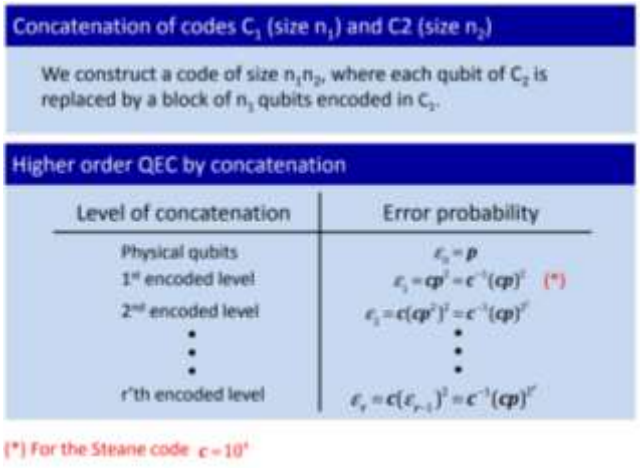
D'un point de vue opérationnel, la création de FTQC passe par la minimisation du nombre d'ancilla qubits et par l'optimisation du choix des QECC en fonction du type d'erreurs générées par chaque type de qubits et de portes quantiques.

La FTQC intègre un dispositif particulier pour la correction d'erreurs provenant de portes quantiques utilisant l'intrication : les **portes transversales**.

Il s'agit d'arrangement de liens entre qubits logiques reliés entre eux par des portes à deux qubits. Le schéma *ci-contre* illustre bien ce genre de liaison entre deux qubits logiques utilisant un Steane code à 7 qubits via une porte CNOT. Chacun des qubits physique des qubits logiques est relié un par un entre les deux qubits logiques.



L'un des problèmes est que la correction d'erreur génère un overhead qui croîtrait plus vite que le gain exponentiel de l'ordinateur quantique (2^{4n} vs 2^n selon Quantum Benchmark) [295]. On peut se consoler avec le **threshold theorem** démontré par Dorit Aharonov et Michael Ben-Or en 1999[296] selon lequel il est possible de réaliser de la correction d'erreur jusqu'à un taux d'erreur apparent souhaité arbitraire si le taux d'erreur des portes à un qubit est inférieur à un seuil donné qui est dépendant du code de correction d'erreurs utilisé et des caractéristiques des qubits.



Ce taux serait situé entre 0,1% et 1% mais est sujet à caution. La conséquence de ce théorème est de permettre l'application de codes de correction d'erreurs de manière récursive jusqu'à atteindre le taux d'erreurs souhaitable pour exécuter un algorithme donné.

---

[295] Pour en savoir plus au sujet de la correction d'erreur, voir notamment cette présentation Surprising facts about quantum error correction d'Andrew Darmawan, Nicolas Delfosse, Pavithran Iyer et David Poulin, 2017 (178 slides).

[296] Voir Fault-Tolerant Quantum Computation With Constant Error Rate par Dorit Aharonov et Michael Ben-Or, 1999 (63 pages).

Cette récursivité exploite la **concaténation** de codes de correction d'erreur[297].Ainsi, un QEC va générer des qubits logiques qui pourront eux-mêmes servir ensuite de qubits physiques virtuels pour une nouvelle QEC, ainsi de suite. À chaque récursivité, le taux d'erreur apparent va baisser. Et on s'arrête lorsque l'on atteint un taux d'erreur compatible avec l'usage attendu des qubits. La concaténation peut d'ailleurs être optimisée en utilisant différents types de QEC à chaque niveau de la récursivité[298].

Mais ce théorème n'a été démontré à ce stade que pour les codes de correction d'erreur de Steane à 7 qubits, pas pour les surface codes, et pour des taux d'erreurs stables avec le nombre de qubits physiques. Il présuppose que le taux d'erreurs des qubits n'augmente pas avec leur quantité. Or, ce n'est pas ce que l'on observe actuellement avec la majorité des types de qubits ! Cela a un impact que nous étudierons dans la partie de cet ebook consacrée à l'énergie.

Une question lancinante peut se poser : si on doit accumuler des codes de correction d'erreur, ne risque-t-on pas de se heurter au mur de la décohérence des qubits qui intervient assez rapidement, notamment dans les qubits supraconducteurs ? Bien non. Les codes de corrections d'erreur ont comme effet direct de prolonger artificiellement le temps de cohérence des registres de qubits et de plusieurs ordres de grandeur[299]. En effet, chaque correction revient à faire un reset des temps de décohérence T1 (flip) et T2 (phase) des qubits. Cela explique pourquoi Google publiait une version optimisée de l'algorithme Shor de factorisation d'entiers avec 20 millions de qubits et durant 8 heures.

Mémoire quantique

Evoquons la mémoire quantique ou la **qRAM,** une mémoire quantique capable de stocker l'état quantique de qubits pour les utiliser ensuite pour alimenter des registres d'ordinateurs quantiques[300]. L'état quantique d'un registre va devoir stocker des qubits en état de superposition.

Avec n qubits, cette mémoire pourra donc stocker en théorie 2^n états différents de ce registre. Elle ne servira pas à stocker autant d'information provenant d'un ordinateur traditionnel mais à conserver l'état d'un registre de qubits d'un ordinateur quantique.

Elle est nécessaire à certains types d'algorithmes quantiques comme l'algorithme de recherche de Grover que nous verrons dans la partie suivante.

Cette mémoire est une sorte de buffer tampon. En effet, selon le théorème de non clonage, le contenu de cette mémoire ne peut être la copie de l'état d'autres registres quantiques. C'est une sorte de ligne à retard de l'état des qubits. Elle est d'ailleurs utilisée dans les répéteurs de clés quantiques de type QKD.

Petit détail de taille : aucune des différentes architectures de mémoires quantiques étudiées depuis deux décennies n'est au point ! Les recherches vont cependant bon train mais avec des usages visés qui sont plutôt dans les télécommunications sécurisées et pour la création de répéteurs optiques.

L'une des méthodes les plus prometteuses de mémoire quantique utilise des phases de photons[301].

---

[297] Source de l'illustration du dessus : Introduction to quantum computing par Anthony Leverrier et Mazyar Mirrahimi, mars 2020 (69 slides).

[298] Voir Dynamic Concatenation of Quantum Error Correction in Integrated Quantum Computing Architecture par Ilkwon Sohn et al, 2019 (7 pages).

[299] Voir Extending the lifetime of a quantum bit with error correction in superconducting circuits, par Nissim Ofek, Zaki Leghtas, Mazyar Mirrahimi, Michel Devoret et al, 2016 (5 pages) qui montre que grâce à une QEC à base de cat-codes, la durée de vie des qubits supraconducteurs peut être étendue d'un facteur 20 !

[300] Voir Architectures for a quantum random access memory, des Italiens Vittorio Giovannetti et Lorenzo Maccone et de l'Américain Seth Lloyd, 2008 (12 pages).

[301] Comme dans Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble, 2017 (13 pages), un papier auquel a contribué le Français Julien Laurat du CNRS.

Les travaux les plus avancés sont réalisés avec le stockage de l'état de polarisation circulaire d'un photon unique piégé dans une structure en rubidium refroidie par laser dans un piège magnéto-optique et ainsi rendue transparente. C'est ce qu'ont réalisé des scientifiques chinois en 2019[302]. Les atomes de rubidium sont refroidis à 200 µK, ce qui est bien bas par rapport aux 15mK d'un ordinateur quantique supraconducteur.

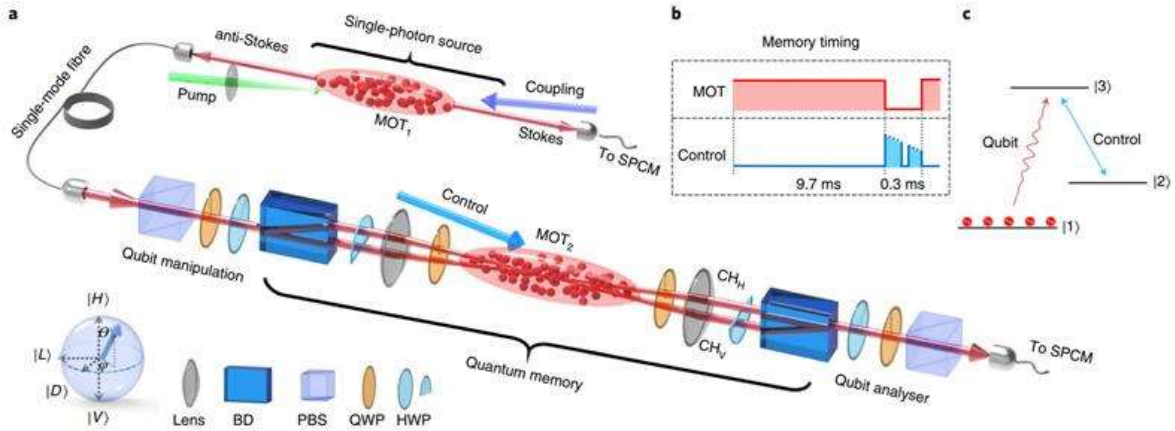


Fig. 1 | Experimental set-up and energy level scheme of the single-photon quantum memory. a, Schematic of the experimental optical set-up. The cold atoms in the first magneto-optical trap (MOT_1) serve as a nonlinear optical medium for producing time-frequency entangled photon pairs, while the cold atoms in the second magneto-optical trap (MOT_2) are the medium for the quantum memory. The anti-Stokes photon is coded with an arbitrary polarization state through the QMU consisting of a QWP and HWP. After the QMU, the two orthogonal linear polarizations are separated into two beams by a polarization beam displacer (BD) that are coupled into the two balanced spatial channels CH_H and CH_V of the quantum memory. The memory read-outs are recombined at the second BD and the polarization state is measured by the qubit analyser. **b**, The memory operation timing shows the MOT sequence and the optimized control laser intensity time-varying profile in each experimental cycle. **c**, The atomic energy level scheme of the quantum memory based on EIT.

On trouve des travaux voisins au Canada, avec l'exploitation du rubidium dont la transparence est contrôlée dynamiquement pour piéger un photon unique[303]. En pratique, les photons sont mémorisés pendant un millième de seconde. C'est suffisant pour un traitement dans un répéteur de télécommunication optique mais moins évident pour du calcul quantique.

Des mémoires optiques sont aussi testées avec de l'ytterbium, une terre rare contrôlable à haute fréquence. Le procédé est voisin du précédent et consiste à conserver la polarisation d'un photon unique dans un piège magnétique mais plutôt pour des applications de répéteurs optiques dans des lignes de communication sécurisée à longue distance[304]. Le stockage d'un état quantique est aussi possible dans des spins d'électrons[305] ainsi qu'avec des NV centers.

Energie

L'une des motivations à créer des ordinateurs quantiques réside dans leur capacité de calcul qui augmente théoriquement de manière exponentielle avec leur nombre de qubits. Cela devrait permettre de réaliser des calculs qui seront à terme inaccessibles aux ordinateurs classiques. Dans certains cas, ils seront seulement un peu plus rapides, dans ce que l'on appelle l'avantage quantique. C'est d'ailleurs un bénéfice bon à prendre dans pas mal de circonstances.

---

[302] Comme relaté dans HKUST Physicist Contributes To New Record Of Quantum Memory Efficiency, 2019, qui fait référence à Efficient quantum memory for single-photon polarization qubits (8 pages).

[303] Avec Physicists create new, simpler-than-ever quantum 'hard drive for light', de Kate Willis, Université d'Alberta, 2018. L'article d'origine est Coherent storage and manipulation of broadband photons via dynamically controlled Autler-Townes splitting, octobre 2017 (17 pages).

[304] Voir Des mémoires quantiques grâce à l'ytterbium par Alexandre Couto, août 2018, qui fait référence à Simultaneous coherence enhancement of optical and microwave transitions in solid-state electronic spins, décembre 2017 (10 pages). Ce sont des travaux conjoints entre l'Université de Genève, notamment Nicolas Gisin, et le CNRS.

[305] Voir Storing quantum information in spins and high-sensitivity ESR, par deux chercheurs dont Patrice Bertet du groupe Quantronics du CEA/CNRS, septembre 2017 (13 pages).

Est-ce que l'avantage en termes de capacité de calcul se manifeste aussi d'un point de vue de la consommation d'énergie ? C'était le cas apparent de la démonstration de suprématie quantique de Google Sycamore en octobre 2019 qui affichait un rapport de un à un million en consommation d'énergie par rapport au supercalculateur IBM Summit de référence, y compris avec l'algorithme optimisé proposé par IBM. Mais c'était comme nous le verrons dans la partie dédiée aux qubits supraconducteurs une sorte de trompe l'œil réalisée avec un calcul ne servant à rien.

Le calcul quantique à grande échelle nécessitera un très grand nombre de qubits pour pouvoir mettre en jeu de la correction d'erreurs. Le pilotage de ces qubits demandera une électronique classique consommatrice d'énergie. La scalabilité énergétique du calcul quantique dépendra en priorité de la capacité à réduire la consommation associée. Heureusement, des solutions existent allant dans ce sens que nous avons notamment étudiées dans la partie précédente liée aux composants électroniques et que nous allons mettre ci en perspective.

Repères classiques

La référence de comparaison est celle des plus grands supercalculateurs du monde qui consomment plusieurs MW (mégawatts) et prennent bien plus de place qu'un ordinateur quantique. Livré en 2019 au centre de recherche d'Oak Ridge du Département de l'Energie dans le Tennessee, l'IBM Summit consomme ainsi 13 MW pour une puissance crête de 200 PFLOPS et dont 3,9 MW rien que pour le refroidissement (source). Ces MW consommés par des milliers de chipsets CPU Power9s et des GPU généralistes Nvidia V100 nécessitent un complexe système de refroidissement par eau qui consomme deux tonnes d'eau par minute. Le Summit occupe 500 m^2 et pèse 349 tonnes, à comparer à environ 2 tonnes pour un ordinateur quantique à qubits supraconducteurs qui tient en version laboratoire dans une pièce à température ambiante faisant à peu près 20 m^2, et en version industrielle, dans un cube d'environ 2,75m de côté, ce qui donne aussi un "avantage masse" et un "avantage surface" en l'état actuel des choses.

Le plus grand supercalculateur commercial début 2019 était le HPC4 du groupe Italien ENI, avec 18,6 PFLOPS sur 1600 nœuds HPE Proliant DL380 équipés de chipsets 24 cœurs Intel Skylake et de 15 Po de stockage, pour une consommation supérieure à 10 MW et un coût total de $100M[306]. Mi 2020, le record passait au Fujitsu Fugaku et ses 514 PFLOPS consommant 30 MW.

En France, le supercalculateur Joliot-Curie conçu par Atos était inauguré en juin 2019 au CEA à Bruyères-le-Chatel pour le GENCI (Grand Equipement National de Calcul Intensif). Sa puissance au lancement de 9,4 PFLOPS devait atteindre 22 PFLOPS après ses évolutions planifiées en 2020. La version initiale consommait un peu moins de 1MW. Elle était équipée de GPU Nvidia de la génération Tesla, sans tenseurs. Le Jean Zay lancé fin 2019, d'origine HPE, avec ses 1300 GPU Nvidia V100 avec tenseurs et refroidis par eau et 14 PFLOPS, se contentait de 1MW.

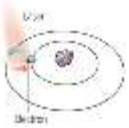
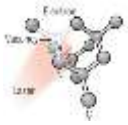
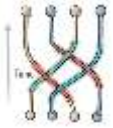
Ces repères sont importants mais ne doivent pas nous faire croire que l'on va remplacer à terme ces supercalculateurs par des ordinateurs quantiques. Nombre des applications de calcul scientifique qu'ils servent à réaliser ne sont pas adaptées au calcul quantique. On en aura donc toujours besoin. Par contre, lorsque les ordinateurs quantique scaleront, ils permettront de réaliser des calculs inaccessibles aux supercalculateurs classiques et, probablement, avec une enveloppe énergétique plus réduite.

Consommation énergétique du calcul quantique

A ce jour, la consommation énergétique d'un calculateur quantique est relativement raisonnable. Un ordinateur quantique actuel à qubits supraconducteurs consomme environ 25 kW dont 16 kW pour la cryogénie. C'est le cas chez D-Wave, Google et IBM. Cette consommation d'énergie équivaut à une trentaine de serveurs Intel ou à deux racks de serveurs Nvidia DGX dans un datacenter.

[306] Voir Eni Launches 18.6-Petaflop Supercomputer, Michael Feldman, janvier 2019.

Les calculateurs quantiques à base d'atomes froids ou de photons consomment encore moins d'énergie, notamment parce qu'ils n'ont pas besoin d'un refroidissement cryogénique à 15 mK. Ces derniers se contentent de refroidissement des sources et détecteurs de photons entre 4K et 10K.

	atomes		électrons				photons
							
puissance consommée	**ions piégés**	**atomes froids**	**supra-conducteurs**	**silicium**	**NV centers**	**fermions de Majorana**	**photons**
cryogénie	2KW	N/A	16 KW	12 KW	16 KW	16 KW	3W
pompe vide/ultra vide [1]	vide	ultra-vide 100W	vide	vide	vide	vide	vide
contrôle des portes quantiques	2KW chauffage des ions, lasers, générateurs de micro-onde, électronique de lecture (CMOS)	5,8KW chauffage des atomes, laser, électronique de contrôle (SLM, etc) et de lecture (CMOS)	1 à 5 KW dépend des architectures selon que la génération des micro-ondes est dans le cryostat ou pas		N/A	N/A	300 W sources et détecteurs de photons, contrôle des portes quantiques
PCs et réseau	1 KW	1 KW	1 KW	1 KW	1 KW	1 KW	700 W
# qubits de réf.	10-50	100-1000	53	50	N/A	N/A	20
total	**5 KW**	**7 KW** (1)	**25 KW** (2)	**21 KW**	**N/A**	**N/A**	**4 KW** (3)

[1] : coût énergétique fixe, pour le démarrage

configuration type pour calculateur de Pasqal (1), Google (2), Quandela/QuiX (3), estimation doigt mouillé pour les autres cas

(cc) Olivier Ezratty, septembre 2020

Lorsque l'on alignera des milliers de qubits dans ces machines, leur consommation électrique augmentera du fait de l'énergie à dépenser pour l'activation électronique des portes quantiques et de la correction d'erreurs[307]. Les qubits consomment très peu d'énergie en tant que tels. Par contre, le pilotage des portes quantiques par envoi de rayons lasers (ions piégés, atomes froids, photons) ou de micro-ondes (supraconducteurs, silicium) augmente linéairement avec l'augmentation du nombre de qubits. La correction d'erreurs nécessitant un grand nombre de qubits physiques par qubits logiques, elle génère un autre facteur multiplicateur de consommation d'énergie. Celle-ci va d'ailleurs dépendre de la fidélité des qubits physiques. Plus elle sera élevée, moins il faudra aligner de qubits physiques pour créer un qubit logique.

La ventilation de la consommation électrique d'un ordinateur quantique peut se décomposer de la manière suivante :

Electronique de contrôle : sa consommation d'énergie est très variable d'une technologie à l'autre et elle dépend du nombre de qubits gérés. Elle est actuellement élevée pour le contrôle de qubits supraconducteurs à base de micro-ondes produites à l'extérieur du cryostat chez IBM et Google. Leur production avec des CryoCMOS dans le cryostat, qui est étudiée chez Google, Intel et ailleurs peut diminuer sensiblement la consommation d'énergie associée. Dans les qubits à base d'ions piégés, le contrôle est réalisé avec des lasers et des micro-ondes générées classiquement. Pour les atomes froids, le contrôle exploite un laser et une matrice SLM qui supporte potentiellement un millier de qubits avec une consommation d'énergie modeste. C'est dans l'électronique de contrôle que se situe la principale partie variable de la consommation d'énergie en fonction du nombre de qubits. Pour les qubits photons, la consommation d'énergie semble plus importante dans la détection des photons (environ 7,5W par qubit) que pour leur génération (environ 1mW par qubit, source : Quandela).

[307] C'est la thèse de Joni Ikonen, Juha Salmilehto et Mikko Mottonen dans Energy-Efficient Quantum Computing 2016 (12 pages).

Cryogénie : elle va consommer jusqu'à 16 kW pour les qubits supraconducteurs et silicium et un peu moins pour les autres types de qubits du fait de températures moins basses, comme les 4K à 10K des générateurs et détecteurs de photons pour les qubits photons. On n'a pas besoin de cryogénie pour les atomes froids. Ils sont en fait refroidis par laser et par mise sous ultra-vide. La consommation de la cryogénie est continue, sans variation entre la phase de thermalisation et la phase d'utilisation. Par contre, la durée de la mise en température est variable et impacte la consommation à la mise en route. Elle est de 24h pour des cryostats de qubits supraconducteurs et silicium.

Vide : les qubits supraconducteurs et silicium nécessitent une mise sous vide, les ions piégés et les atomes froids utilisent pour leur part de l'ultravide. Les photons n'en ont pas besoin. Le processus de mise sous vide dépend des systèmes. Dans les qubits supraconducteurs et silicium, il résulte de l'usage de pompes et du refroidissement. Chez Pasqal pour des atomes froids, la pompe ne nécessite que 100W. La mise sous vide de systèmes à base d'ions piégés et d'atomes froids fait par contre appel à un système de bandelettes chauffantes couvrant la chambre à vide avec un processus qui peut durer des semaines. C'est un coût fixe car une fois le vide généré, le chauffage est stoppé et le vide reste stable pendant les opérations de calcul. Une fois le vide réalisé, la consommation associée est donc nulle ou tout du moins minime.

Informatique de contrôle : c'est le point commun de toutes les architectures. Elles ont toutes besoin d'un à trois serveurs de contrôle qui pilotent les dispositifs de contrôle et de lecture de l'état des qubits en exploitant le logiciel quantique compilé et transformé en instructions à bas niveau de pilotage de l'initialisation, du contrôle et de la lecture des qubits. Ces serveurs sont reliés en réseau aux utilisateurs, soit localement, soit en cloud et via un switch réseau classique. Ils représentent un coût fixe limité dont la consommation est estimée à environ 1kW. Une partie de l'informatique de contrôle pourrait être déplacée dans le cryostat pour les qubits supraconducteurs et silicium, afin d'y déporter par exemple les codes de correction d'erreurs autonomes. L'ordinateur de contrôle ne piloterait alors que des qubits logiques et pas les qubits physiques de la configuration.

Une bonne part de ces composantes d'un ordinateur quantique a un coût énergétique variable en fonction du nombre de qubits, y compris du côté de la cryogénie. En effet, l'électronique embarquée dans les cryostats dégage de la chaleur en proportion approximative avec le nombre de qubits physiques utilisés. Il faut évacuer cette chaleur avec le cryostat. La consommation de l'électronique de contrôle dépend aussi généralement du nombre de qubits. Il semble que, jusqu'à un millier de qubits, cette électronique de contrôle soit un coût fixe pour les atomes froids. Seule la mise sous vide et l'ordinateur de contrôle semblent être des coûts fixes dans l'histoire.

Autre facteur à prendre en compte : les inévitables progrès qui entraîneront une réduction de la consommation électrique, notamment relativement à chaque qubit. Cela pourra être le cas par exemple des lasers pour les qubits à base d'atomes froids, d'ions piégés et de photons. Cela le sera aussi avec les composants de génération et de lecture de micro-ondes pour les qubits supraconducteurs et silicium, qui seront progressivement intégrés dans les cryostats.

Contraintes thermiques du calcul quantique

Les systèmes de qubits qui fonctionnent à température cryogénique sont contraints par la puissance de refroidissement des cryostats et par le dégagement thermique qui se produit au sein du cryostat.

Le cas des qubits supraconducteurs et silicium est le plus épineux. Le dégagement thermique intervient au niveau des filtres d'atténuation des micro-ondes de pilotage des qubits et dans les amplificateurs des micro-ondes de lecture de l'état des qubits. S'y ajoute le dégagement thermique des systèmes de génération de micro-ondes au cas où celui-ci est intégré dans le cryostat.

Tout cela doit rentrer dans le budget thermique actuel des cryostats que nous avons vu dans la partie correspondante. Il est limité à 1W à l'étage 4K et à 25 µW à l'étage 15 mK. On pourra sans doute créer des cryostats encore plus puissants avec 2 voire 10 têtes pulsées et autant de dilution. Cela permettra de gagner un ordre de grandeur pour la puissance de refroidissement disponible.

Mais il est clair que cela va générer une contrainte pour la scalabilité du nombre de qubits, surtout pour les LSQC (large scale quantum computers) qui vont nécessiter un très grand nombre de qubits physiques par qubits logiques pour la correction d'erreurs. Il se chiffre en millions de qubits physiques !

Les options disponibles pour réduire la consommation électrique de l'électronique de contrôle et de mesure des qubits consistent à utiliser des composants supraconducteurs comme chez D-Wave ou SeeQC. Avec des CryoCMOS, le dégagement thermique est plus grand. Mais les composants supraconducteurs prennent plus de place ! Compromis difficile !

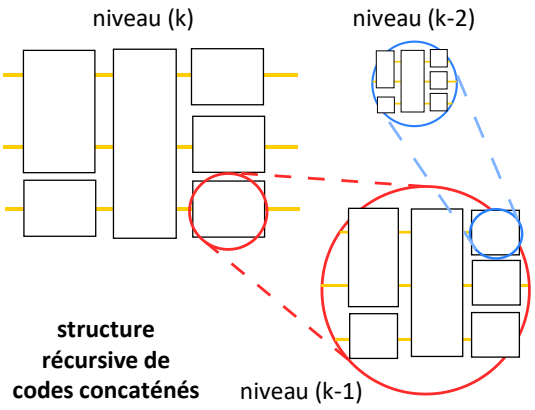
L'autre manière d'être moins contraint consiste à faire fonctionner les qubits à plus haute température. C'est ce que permettent les qubits silicium, qui se contentent d'une tempéature comprise entre 100mK et 1K au lieu de 15 mK pour les supraconducteurs. Cela augmente le budget thermique consommable pour l'électronique de contrôle à l'étage des qubits.

Coût énergétique de la correction d'erreurs

La correction d'erreurs constitue un paramètre important qui va conditionner la consommation d'énergie d'un calculateur quantique. Le paramètre clé est le ratio entre le nombre de qubits physiques et de qubits logiques. Celui-ci peut être très élevé et dépasse 10 000 dans certaines estimations. Sachant que l'on ne sait pas encore aligner un tel nombre de qubits en pratique. Ce ratio dépend de la fidélité des qubits.

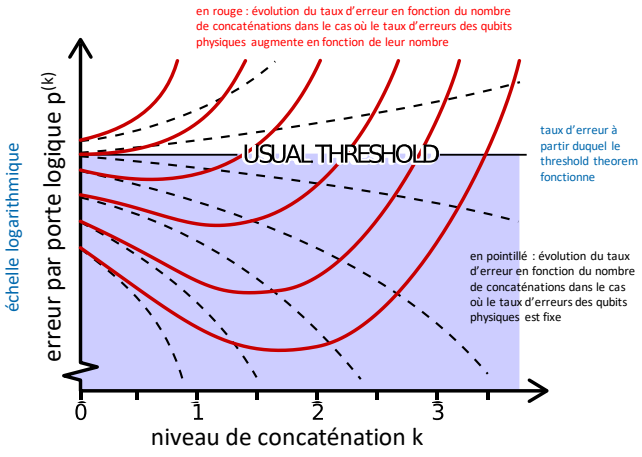
Plus celle-ci est élevée, plus le ratio de qubits physiques/logiques est faible. Pour faire du calcul LSQ (large scale quantum computing), on va démultiplier le nombre de qubits et générer une forte consommation d'énergie. Pour les qubits supraconducteurs, cela peut aboutir à être bloqué par la capacité thermique des cryostats.

Cependant, les codes de correction d'erreurs utilisés de manière récursive par concaténation risquent de se heurter simultanément à un autre mur : celui de la non-linéarité de la fidélité des qubits avec leur nombre.



le principe des poupées russes des codes de correction d'erreur concaténés.

chaque bloc fonctionnel d'un algorithme de code de correction d'erreur de niveau k peut lui-même contenir un code de correction d'erreur de niveau inférieur k-1 et ainsi de suite.



le pointillé en noir indique l'évolution du taux d'erreur des qubits logiques en fonction du nombre de concaténations, avec un taux d'erreur stable en fonction du nombre de qubits. en rouge, les mêmes évolutions, avec un taux d'erreur qui augmente avec le nombre total de qubits physiques. Il montre que la concaténation atteint ses limites au bout de seulement une à deux concaténations de codes de correction d'erreurs.

source : Limitations in quantum computing from resource constraints par Marco Fellous-Asiani, Jing Hao Chai, Robert S. Whitney, Alexia Auffèves et Hui Khoon Ng, juillet 2020 (8 pages)

A savoir que la fidélité des qubits décroit généralement avec l'augmentation du nombre de qubits. Cela a comme conséquence d'inverser l'effet de la concaténation de codes de correction d'erreurs à partir de deux ou trois concaténations.

Le taux d'erreur des qubits logiques augmente alors, au lieu de diminuer [308]. Pour que les codes de correction d'erreur soient efficaces, il faudrait que le taux d'erreur des qubits soit au moins dix fois inférieur à leur niveau actuel.

On doit de plus intégrer le fait qu'actuellement, les algorithmes quantiques sont exécutés des milliers de fois pour en moyenner le résultat, comme le fait IBM avec ses calculateurs quantiques en ligne. Cela augmente le coût énergétique d'un calcul quantique car cela en rallonge la durée de trois ordres de grandeur.

Réversibilité des calculs classiques et quantiques

Nous allons étudier ici l'impact de la réversibilité sur la consommation énergétique du calcul quantique. Il nous faut d'abord définir les notions de réversibilité logique et physique du calcul.

La **réversibilité logique** d'un calcul est liée à la capacité à revenir en arrière après une ou plusieurs opérations. Il faut pour cela que l'information obtenue après un calcul permette d'obtenir les données qui l'ont généré. Cela se comprend à l'échelle d'une porte logique classique ou d'une porte quantique élémentaire et jusqu'à un calcul complet. Si la réversibilité logique est possible au niveau de toute porte utilisée, alors elle le devient ipso-facto pour un calcul complet[309]. Les calculateurs classiques d'aujourd'hui sont généralement logiquement irréversibles. Les portes logiques à deux bits passent leur temps à détruire de l'information car elles génèrent un bit à partir de deux bits. En gros, on en jette à chaque fois un et on ne peut pas revenir en arrière d'une simple opération logique NAND, OR ou AND. Mais on pourrait créer des portes logiques ne détruisant pas d'information et générant autant de bits en sortie qu'en entrée. Cela permettrait d'aboutir à un calcul logiquement réversible.

La **réversibilité physique**, ou thermodynamique, d'un calcul est associée au fait qu'elle ne génère pas d'entropie. Ce n'est pas le cas actuellement dans le calcul classique qui est gros consommateur d'énergie parce que les portes logiques ne sont pas réversibles logiquement et physiquement.

L'irréversibilité logique du calcul classique conduit à une dépense énergétique dont le plancher est la fameuse limite de Landauer qui fait que le calcul classique est aussi thermodynamiquement irréversible. Mais il est possible de faire autrement. Nous allons l'étudier à part dans une partie dédiée au calcul adiabatique et réversible. La réversibilité thermodynamique devient ici un moyen physique d'obtenir la réversibilité logique. La mise en œuvre de cette réversibilité logique en rembobinant les calculs permettrait d'obtenir en retour une réversibilité thermodynamique. En effet, l'énergie dépensée dans le calcul aller pourrait être récupérée dans le calcul retour.

Le calcul quantique à portes universelles présente la caractéristique et d'être logiquement résersible du fait de l'emploi d'opérations unitaires, qu'il s'agisse de portes quantiques à un qubit ou à plusieurs qubits. Seule la mesure des états est logiquement irréversible puisque, dans le cas général, elle rabat l'état des qubits sur un état de base qui n'est pas forcément celui des qubits à la fin des calculs[310]. La mesure de l'état serait réversible seulement dans le cas où les résultats sont parfaitement alignés sur les états de base des qubits $|0\rangle$ et $|1\rangle$. Si on ne faisait pas de mesure en fin de calcul, on pourrait théoriquement exécuter un algorithme ou une partie d'algorithme à l'envers pour revenir en arrière dans le calcul.

---

[308] C'est ce qui ressort de Limitations in quantum computing from resource constraints par Marco Fellous-Asiani, Jing Hao Chai, Robert S. Whitney, Alexia Auffèves et Hui Khoon Ng, juillet 2020 (8 pages).

[309] Voir ces explications détaillées sur la réversibilité du calcul classique : Synthesis of Reversible Logic Circuits par Vivek Shende et al, 2002 (30 pages).

[310] Le Measurement Based Quantum Computing qui s'appuie surtout sur de la mesure pendant tout le calcul est irréversible par construction. C'est d'ailleurs pour cela qu'il aussi dénommé 1WQC pour one way quantum computing.

On ne parle cependant pas à l'heure actuelle de réversibilité physique ou thermodynamique du calcul quantique. Tout d'abord, le bruit quantique qui génère des erreurs dans les portes quantiques n'est pas nécessairement d'origine thermique comme nous l'avons vu dans la partie précédente dédiée aux codes de correction d'erreurs.

C'est un peu l'équivalent des frottements dans la physique classique. Le calcul quantique serait pratiquement réversible en l'absence de bruit et si les mesures étaient non-perturbantes.

Pour obtenir une irréversibilité physique du calcul quantique hors mesure, il faudrait en plus de la maîtrise du bruit que les éléments de l'électronique de contrôle des qubits s'appuient aussi sur des opérations physiquement et thermodynamiquement réversibles ou tout du moins économes en énergie. C'est envisageable dans certains designs où ce contrôle des qubits, comme dans les qubits supraconducteurs et silicium, pourrait exploiter des composants cryogéniques adiabatiques et réversibles intégrés dans le cryostat.

Une autre voie explorée est celle de l'ABQC pour **Asynchronous Ballistic Quantum Computing** promue par l'équipe de Michael P. Frank des Sandia Labs aux USA. Elle exploiterait des qubits volants circulant dans des circuits matériels avec des portes quantiques mises en œuvre par des dispositifs matériels comme dans le calcul classique et non par des opérations. Les circuits seraient des réseaux physiques plutôt que des séries d'opérations sur des qubits statiques. Le système fonctionnerait de manière asynchrone pour éviter que les qubits devant interagir entre eux n'aient pas besoin d'arriver en même temps, ce qui est très difficile à contrôler. Ces chercheurs envisagent de mettre en œuvre ces qubits avec des jonctions Josephson en on retrouve derrière la startup américaine **SeeQC**, la seule qui soit investie dans la création de composants supraconducteurs[311].

Sans passer par l'épineuse case de la mesure en fin de calcul, le calcul réversible quantique peut aussi faire appel à de la mémoire quantique et à un « décalcul » (uncompute) des résultats qui ne sont plus nécessaires comme ceux qui sont réalisés au niveau des qubits intermédiaires (ancilla qubits)[312].

La réversibilité quantique n'est cependant pas l'élément clé de réduction de la consommation énergétique du calcul quantique. C'est un moyen parmi d'autres et d'impact assez modéré.

Dans le calcul quantique, la quête de frugalité énergétique concerne surtout la partie classique du contrôle des qubits qui consomme plusieurs ordres de grandeur d'énergie de plus que les portes quantiques pilotées. La réduction de la consommation d'énergie du calcul quantique peut intégrer diverses techniques qui n'ont pas de lien avec la réversibilité, principalement des composants électroniques CryoCMOS fonctionnant à basse température (en général à 4K) et des composants supraconducteurs qui réduisent la consommation d'énergie grâce à la supraconductivité. Le tout, en faisant des économies des encombrants câblages et filtres actuellement utilisés.

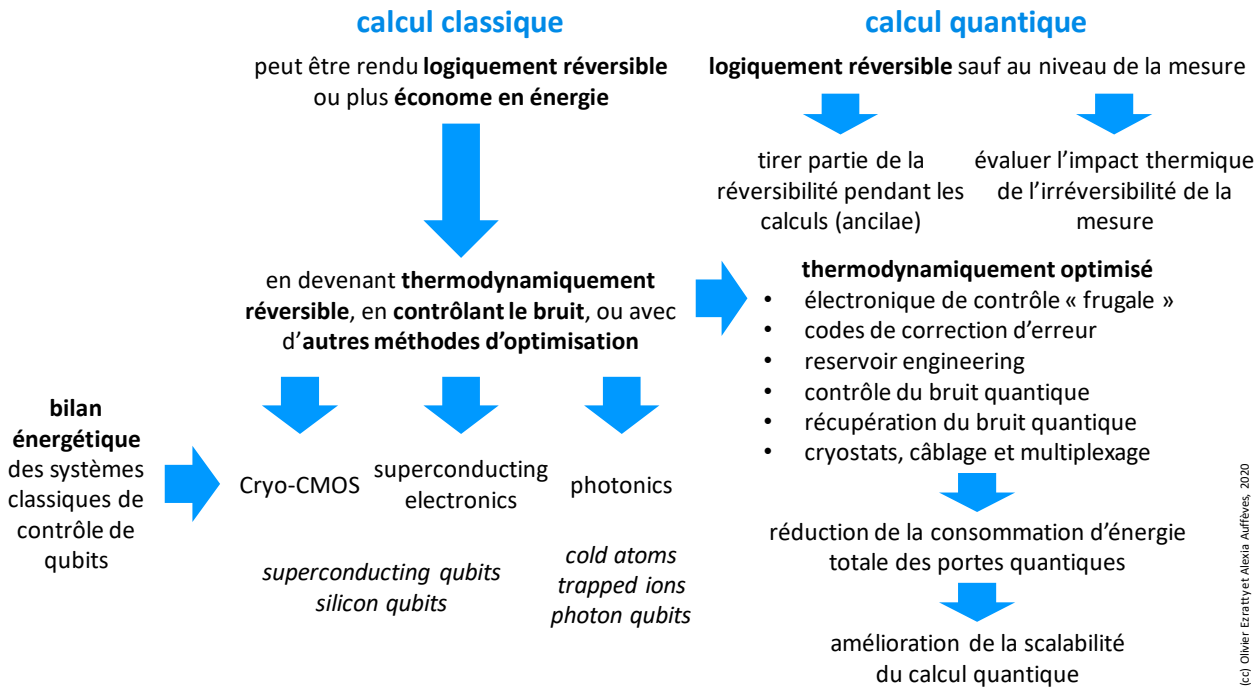
On le voit donc ici, la question énergétique du calcul quantique est complexe et multidimensionnelle. Elle associe des éléments classiques et quantiques dont il faut pouvoir évaluer l'impact relatif en termes d'économies d'énergie et de scalabilité. C'est ce qui en fait une discipline d'ingénierie.

Tout cela associe de nombreux éléments de thermodynamique fondamentale, d'ingénierie électronique classique et de physique quantique. C'est un domaine qui est notamment exploré par l'équipe de Michael Frank des Sandia Labs, déjà citée, ainsi que par celle d'Alexia Auffèves du CNRS Institut Néel à Grenoble. Le schéma *ci-dessous* positionne les uns vis-à-vis des autres tous ces concepts avec un lien étroit entre les aspects énergétiques du calcul classique et ceux du calcul quantique. La frugalité énergétique est diverse et dépasse de loin celle qui viendrait de la réversibilité.

---

[311] Voir Pathfinding Thermodynamically Reversible Quantum Computation par Karpur Shukla et Michael P. Frank, janvier 2020 (28 slides) ainsi que Asynchronous Ballistic Reversible Computing using Superconducting Elements par Michael P. Frank et al, avril 2020 (27 slides).

[312] Voir Putting Qubits to Work – Quantum Memory Management par Yongshan Ding and Fred Chong, juillet 2020.



Impact énergétique des architectures distribuées

La tentation est grande de créer des ordinateurs quantiques de plus en plus grands, avec des cryostats géants dans le cas des qubits supraconducteurs. Une autre approche consisterait à créer des architectures distribuées de calculateurs quantiques reliés entre eux par connexion quantique à base de photons intriqués.

Cela permettrait en théorie de créer des clusters de calcul qui vus de l'extérieur ne feraient qu'un seul calculateur. Cela serait conditionné par les techniques de conversion d'état des qubits en photons et par la connectivité au niveau qubits entre les processeurs quantiques du cluster.

Il faudra y ajouter le poid énergétique des solutions de télécommunications quantiques. Celui-ci devrait cependant être relativement raisonnable par rapport à la consommation des nœuds du cluster.

Impact énergétique des usages

Une autre question plus long terme mérite d'être posée : est-ce que l'avantage énergétique du calcul quantique est plus ou moins prononcé selon les algorithmes et les usages ? Qu'en sera-t-il si et lorsque les usages du calcul quantique se généraliseront à grande échelle ? Va-t-on finalement créer une nouvelle source de consommation d'énergie qui s'ajoutera aux sources existantes, déjà abondantes dans le numérique ? Quel en sera son impact ? Comment peut-il être limité ?

A ce stade, il est trop tôt pour se prononcer. La réponse à la question viendra en grande partie de l'émergence ou non de solutions quantiques destinées à des usages en volume, comme pour le guidage de véhicules autonomes ou la santé personnalisée. Sans des solutions destinées à des usages en volume, les calculateurs quantiques seront dédiés à des applications de niche équivalentes à celles des supercalculateurs actuels qui sont surtout utilisés dans la recherche fondamentale et appliquée.

Les usages en volume ne pourront de leur côté voir le jour que lorsque l'on aura réglé les problèmes de scalabilité du calcul quantique et pour pouvoir opérer des millions de qubits faiblement bruités. Cette scalabilité sera probablement associée au traitement des questions de consommation énergétique. Et la boucle sera bouclée !

Matières premières

Lorsqu'une nouvelle technologie voit le jour, il est maintenant d'usage de se poser d'autres questions en plus de celles qui touchent à l'énergie que nous venons de voir : qui des matières premières utilisées ? Quelles sont leur sources d'approvisionnement, leurs réserves mondiales, leur coût économique et environnemental d'extraction, les matières premières des consommables le cas échéant, et enfin, les processus de recyclage de ces matières premières, surtout si elles sont polluantes ?

Nous allons inventorier ici les différentes matières premières utilisées dans et autour des technologies quantiques de tous types, surtout les ordinateurs quantiques. Nous allons au passage *spoiler* quelques-uns des éléments descriptifs des différents types de qubits qui sont couverts plus loin dans ce document.

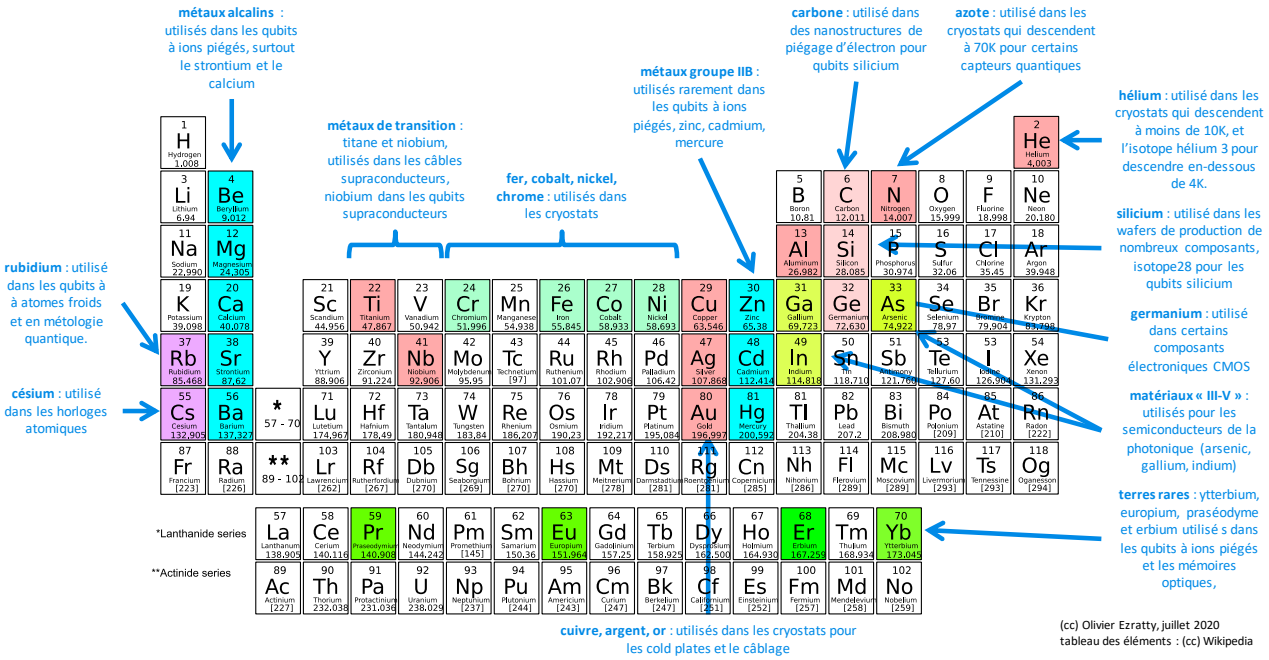
Tous ces éléments sont positionnés dans un tableau périodique maison, *ci-dessous*.

Il y aurait fort à écrire et à expliquer sur la logique de ce tableau et sur la catégorisation de ses éléments[313]. On passera pour cette fois-ci.

Nous avons principalement deux types de matériaux à étudier : ceux qui rentrent dans la composition de qubits ou de circuits électroniques, puis les matériaux d'accompagnement, notamment pour les câbles et autres structures porteuses ainsi que les gaz utilisés dans les cryostats.

Les matériaux utilisés dans les qubits sont parfois assez rares (strontium, ytterbium, berylium). Ils ont des caractéristiques qui expliquent leur choix qui se situent surtout au niveau de leurs transitions énergétiques qui correspondent à des longueurs d'ondes de lasers ou de micro-ondes utilisables pratiquement avec les sources du marché. D'autres contraintes expliquent leur choix comme la stabilité de certains de ces niveaux énergétiques. Certains matériaux sont très rares mais leurs besoins dans les technologies quantiques restent marginaux en proportion de leur production et de leur consommation mondiale.

éléments utilisés dans les technologies quantiques



[313] Voir aussi ce très beau poster illustré : The Periodic Table of the Elements, in Pictures.

C'est tout du moins le cas tant que l'on ne fabrique pas des millions de calculateurs quantiques les exploitant. On n'est pas encore au stade de la phagocytation de la consommation de certains éléments par une filière donnée, comme cela peut être le cas pour les smartphones concernant certaines terres rares et des minerais comme le fameux coltan[314].

D'autres spécificités sont parfois à prendre en compte qui portent sur les isotopes utilisés qui sont parfois les plus rares de leurs éléments. C'est le cas pour l'hélium (3) utilisé dans la cryogénie en-dessous de 4K ou pour le césium (133) pour les horloges atomiques ou encore le rubidium (87). Le silicium (28) est utilisé dans les qubits silicium et, s'il est l'isotope le plus abondant, nécessite toutefois un raffinage couteux.

Je n'évoque pas dans cet inventaire les matériaux utilisés dans la production de semi-conducteurs, comme le fluor et autres solvants divers. Et ils sont très nombreux !

Nous ne traiterons pas non plus du recyclage des ordinateurs quantiques, une question qui ne se pose pas encore vu leur nombre actuel très limité. On peut cependant la réduire à celle, plus générique, du recyclage d'appareils électroniques divers.

Hélium

Privilège de l'ancienneté oblige, nous allons commencer par un grand paradoxe du tableau des éléments. L'hélium est en effet le second élément de la création de l'Univers après l'hydrogène. Il y est encore le second élément le plus abondant. La fusion nucléaire fait le reste pour créer tous les autres éléments au sein des étoiles de première et de seconde génération. Et pourtant, cet élément est plutôt rare sur Terre et ses réserves s'amenuisent. C'est un gaz noble, inerte, qui n'interagit chimiquement avec aucun autre élément car sa couche d'électrons est complète avec deux électrons. Plus léger que l'air, il a tendance à quitter l'atmosphère. Comme nous l'avons vu en détail dans la rubrique sur les cryostats, l'hélium est utilisé pour le refroidissement des qubits à base d'électrons, surtout supraconducteurs et silicium.

Dès que l'on a besoin de descendre en-dessous de 1K, on doit faire appel à un mélange de deux isotopes de l'hélium, le 4 qui est le plus courant et le plus stable (avec deux neutrons) et le 3 qui est bien plus rare (avec un seul neutron). Pour la cryogénie au-dessus de 1K, on peut se contenter d'hélium 4.

Cela fait au moins une décennie que nombre de spécialistes s'inquiètent d'une pénurie de la fourniture d'hélium 4. Il est couramment utilisé pour le refroidissement des aimants supraconducteurs des accélérateurs de particules comme au CERN ainsi que dans les scanners IRM ou, plus simplement, pour gonfler des ballons. On l'utilise également comme gaz neutre pour la production de semiconducteurs. Heureusement, de nouvelles sources de gaz naturel d'où peut être extrait l'hélium 4 sont apparues, notamment en Tanzanie et au Qatar[315]. Mais une faible croissance annuelle de la demande d'à peine 1,6% est trop élevée par rapport aux prévisions de production. Notons qu'Air Liquide est un des grands acteurs de ce marché mondial, exploitant notamment une grande unité d'extraction et de production d'hélium 4 au Qatar, reliée à leur exploitation de gaz.

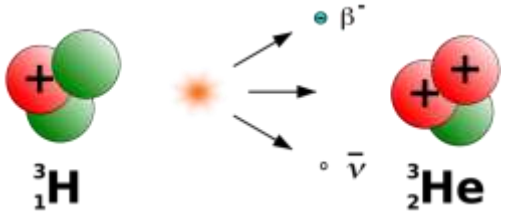
L'isotope hélium 3 est plutôt rare, donc cher ! C'était historiquement un sous-produit du stockage de bombes H à base de tritium, ce dernier se désintégrant progressivement pour produire de l'hélium 3. Il était donc récupéré dans les stocks de bombes H ! Avec les réductions de stocks d'armes nucléaires, la production de l'hélium 3 passe par d'autres voies, dans des centrales nucléaires spécialisées.

---

[314] Le coltant est la contraction de colombite-tantalite. Il sert à récupérer du tantale et du niobium. S'il est une source importante pour le tantale, il est en fait secondaire pour le niobium par rapport à d'autres minerais. Voir Mineral Commodity Summaries 2020 de l'USGS, l'équivalent du BRGM français (204 pages) qui ma aidé à créer cette partie.

[315] Voir Helium – Macro View Update, Edison Investment Research, février 2019 (21 pages).

On peut produire du tritium par irradiation du lithium ou désintégration contrôlée du tritium, un isotope de l'hydrogène avec un proton et deux neutrons, dans des installations nucléaires spécialisées, comme celles qui sont maîtrisées par le Département de l'Energie US.



Cet hélium 3 est notamment produit dans le site de Savannah du Département de l'Energie US en Caroline du Sud[316] et dans la centrale Canadienne CANDU[317]. Le prix de l'hélium 4 gazeux est d'environ 20€ le litre tandis que celui de l'hélium 3 est de 2K€ à 3K€ le litre.

hélium 4
2 protons
2 neutrons
+abondant

$5-$20 par litre de gaz
>100L par ordinateur

hélium 3
2 protons
1 neutron
rare

$1500 à $2000 le litre de gaz
>$10K d'hélium 3 / par ordinateur

Et il en faut 15 à 18 litres par cryostat pour un peu plus de 100 litres de gaz d'hélium 4 ! Les gaz sont achetés séparément et mélangés au bon dosage par le fabricant du cryostat à sec. A la fin, il faut donc débourser au moins 30 à 40K€ d'hélium 3 et 4 par cryostat à sec.

DoE Savannah River Site in South Carolina

L'hélium 4 qui alimente la tête pulsée et passe par le gros compresseur doit de son côté être très purifié.

La France dispose de capacités de production de l'hélium 3 situées notamment dans un réacteur nucléaire du CEA à Grenoble. Mais elle ne les exploite pas forcément pour les ordinateurs quantiques car cette production est trop chère[318]. On peut aussi trouver de l'hélium 3 sur la surface de la Lune mais il n'est pas très pratique d'aller l'y extraire et le récupérer même si c'est technologiquement possible[319] ! L'intérêt de sa récupération est que cet isotope pourrait être intéressant pour alimenter des réactions à fusion nucléaire, le jour où cela fonctionnera.

L'hélium 3 est donc un véritable goulot d'étranglement insoupçonné de la fabrication d'ordinateurs quantiques supraconducteurs et silicium ! On ne peut même pas l'éviter pour ce dernier qui demande une température d'environ 1K[320].

---

[316] Voir Savannah River Tritium Enterprise (4 pages). L'hélium 3 est aussi exploité dans diverses applications spécialisées : dans les détecteurs de neutrons utilisés dans les systèmes de sécurité, dans l'exploration pétrolière, dans l'imagerie médicale ainsi que dans les recherches dans la fusion nucléaire.

[317] Voir CANDU Reactor, Wikipedia.

[318] Voir Crise de l'hélium l'inquiétude persiste 2013 (2 pages), Isotope Development & Production for Research and Applications (IDPRA), Supply and Demand of Helium-3, 2016, Responding to The U.S. Research Community's Liquid Helium Crisis, 2016 (29 pages) et How helium shortages will impact quantum computer research par James Sanders, avril 2019.

[319] Voir There's Helium in Them Thar Craters!.

[320] L'hélium 4 est utilisé pour refroidir les aimants supraconducteurs des systèmes d'IRM. Il sert aussi à refroidir les aimants du LHC au CERN. Les contraintes sont différentes : il s'agit juste d'obtenir de la supraconductivité pour les aimants de focalisation des faisceaux de particules. La température requise est située entre 1,8K et 4,5K, soit bien plus « chaud » que les 15 mK des processeurs quantiques reposant sur des électrons (supraconducteurs, silicium, NV Centers, fermions de Majorana). D'un autre côté, les volumes à cryogéniser sont bien plus importants. Dans certains cas cependant, la température requise peut descendre en-dessous de 1K, notamment pour la recherche de matière noire. Dans le LHC du CERN, des aimants de 9 Tesla sont refroidis à 1,8K avec des cryostats de 18 kW qui exploitent 120 tonnes d'hélium 4.

Silicium

Le silicium entre dans la composition de nombreux composants semi-conducteurs utilisés dans ou autour des processeurs quantiques. Il est très abondant sur Terre, étant le second élément le plus abondant de l'écorce terrestre après l'oxygène. Mais celui qui sert à fabriquer les semi-conducteurs provient de mines de quartz assez peu nombreuses.

Elles présentent l'avantage de produire des quartzs composés d'au moins 97% de silicium, plus facile à raffiner. Ceux-ci servent ensuite, après raffinage, à produire les lingots de silicium qui sont ensuite découpés en tranches, les wafers, pour être ensuite gravés avec des transistors qui associent de l'oxyde de silicium et différents matériaux comme l'hafnium.

Pour graver des qubits silicium, on a besoin de l'isotope 28 du silicium car le spin nul de son noyau d'interfère pas avec celui des électrons piégés dont l'état est justement leur spin. Les wafers de silicium sur lesquels sont gravés les qubits doivent être recouverts d'une couche de silicium 28. C'est la variante la plus abondante de l'élément. Il est associé à l'isotope 29 à plus de 4% dans les wafers habituels destinés à la production de composants CMOS.

D'un point de vue du spectaculaire, le silicium 28 avait fait parler de lui en 2010 lorsque des chercheurs allemands avaient créé une boule de cristal parfaite en silicium 28 pour déterminer avec précision le nombre d'Avogadro qui détermine le nombre d'éléments, ici des atomes, dans une mole[321]. Les tests avaient été réalisés sur un échantillon de 5 kg et pour un coût d'un million d'Euros. En 2014, une équipe américaine améliorait la pureté du silicium 28 à 99,9998% en utilisant un système de pompage d'ions silicium dans un champ magnétique qui permet de les séparer par la masse[322].

Cela continuait en 2017 avec du ^{28}Si à 99,999%[323] produit par une équipe de chercheurs russes et allemands. L'intérêt du ^{28}Si était de permettre un comptage précis du nombre d'atomes de silicium dans la masse considérée, du fait de sa structure cristalline parfaite, dimensionnée par interférométrie à rayons X. Le nombre d'Avogadro déterminé par l'expérience de 2010 était $N_A = 6{,}022\ 140\ 84(18) \times 10^{23}$. L'ambition de ces deux projets était de créer un nouvel étalon matériel du kilogramme, celui de 1889 conservé en France se dégradant par oxydation.

Finalement, en 2018, le nombre d'Avogadro était redéfini dans le système international de mesure comme une constante légèrement différente, de $6{,}022\ 140\ 76 \times 10^{23}$ mol^{-1}. Indirectement, ces deux expériences ont toutefois permis de faire avancer le savoir-faire de la purification du silicium 28, à une époque où l'on évoquait à peine son intérêt pour créer des qubits en silicium. Cela illustre bien la sérendipité de la science et de ses débouchés.

---

[321] Voir An accurate determination of the Avogadro constant by counting the atoms in a 28Si crystal par B. Andreas, 2010 (4 pages). Le silicium 28 était obtenu par centrifugation de gaz de fluorure de silicium (SiF4), ensuite transformé en SiH4 qui servait alors à créer le cristal par dépôt sous vide du silicium purifié. Le tout était réalisé dans différents laboratoires en Russie à Nizhny-Novgorod et Saint Petersbourg. Les chercheurs impliqués provenaient aussi d'Italie, d'Australie, du Japon, de Suisse et di BIPM en France, issus de leurs respectifs bureaux des poids et mesure.

[322] Voir Purer-than-pure silicon solves problem for quantum tech par Jonathan Webb, 2014 qui fait référence à Enriching ^{28}Si beyond 99.9998 % for semiconductor quantum computing par K J Dwyer et al, 2014 (7 pages).

[323] Voir A new generation of 99.999% enriched ^{28}Si single crystals for the determination of Avogadro's constant par N V Abrosimov et al, 2017 (12 pages) qui décrit très bien le processus de purification du silicium 28, source de l'illustration dans cette page.

Le procédé de purification du silicium est complexe. Il passe par la production de tétrafluor de silicium (SiF_4) tous isotopes confondus. L'enrichissement en ^{28}Si est réalisé dans une centrifugeuse, à l'origine au « Central Design Bureau of Machine Building » de Saint-Petersbourg, en fait, une ancienne usine d'enrichissement de plutonium réaffectée à cet usage en 2004.

Le gaz était transformé en silane ($^{28}SiH_4$) à l'**Institute of Chemistry of High-Purity Substances** de l'académie des sciences russes de Nizhny-Novgorod. C'est alors qu'il pouvait être déposé par déposition sous vapeur (CVD) sur du silicium, en le libérant de l'hydrogène. Le lingot réalisé peut alors être étiré pour créer un silicium parfaitement cristallin prêt pour être découpé en tranches, les wafers.

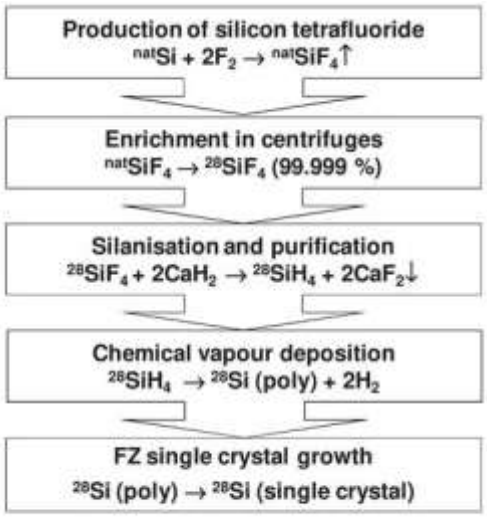


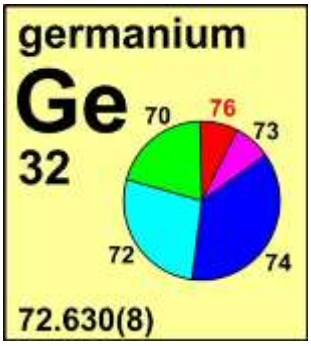
Figure 4. Main technological steps of the ^{28}Si crystal production (^{nat}Si: silicon of natural isotopic composition).

Les chercheurs du CEA-Leti travaillent aussi avec ces équipes russes de Nizhny-Novgorod sur le procédé de dépôt sous vide du ^{28}Si sur des wafers de 300 mm[324]. **Air Liquide** est d'ailleurs partenaire avec le laboratoire de Nizhny-Novgorod pour ce procédé de dépôt CVD (chemical vapor deposition) de ^{28}Si sur une couche mince de 30 à 60 nm pure à 99,992%[325] au-dessus d'un wafer silicium classique. Sachant qu'Air Liquide maîtrise aussi la conversion du SiF_4 en silane.

Germanium

Le germanium est un métalloïde semi-conducteur qui fait partie de la famille III-V. Il est utilisé dans de nombreux domaines : en photonique, dans les transistors bipolaires à hétérojonction SiGe qui sont exploités pour l'amplification de signaux faibles d'hyperfréquences ainsi que dans les chipsets de qubits silicium.

Dans ce dernier cas, il doit être purifié isotopiquement pour générer du ^{73}Ge qui correspond à 7,36% de sa proportion (en violet dans le chart *ci-contre*). C'est un isotope stable, naturel et non radioactif. Le germanium est généralement extrait de minerais de zinc et aussi de zinc-cuivre. Il était produit à hauteur de 130 tonnes en 2019, la Chine en étant le principal pourvoyeur avec 85 tonnes (source). Les données sur les réserves connues sont variables et seraient d'environ 9000 tonnes, situées principalement en Chine, au Canada et aux USA. Avec le gallium et l'indium qui sont aussi des matériaux III-V, le germanium est considéré comme étant une ressource critique.



La purification isotopique du germanium est assurée par les mêmes équipes russes de Nizhnii Novgorod que celles qui produisent du ^{28}Si. Elle utilise un procédé de la centrifugation de tétrafluorure de germanium voisin de celui qui est utilisé pour produire ce dernier et expliqué *ci-dessus*[326].

[324] Voir 99.992% 28Si CVD-grown epilayer on 300 mm substrates for large scale integration of silicon spin qubits par V. Mazzocchi du CEA-Leti et des collègues français et russes, 2018 (7 pages).

[325] Voir Quantum computing: progress toward silicon-28, avril 2018.

[326] Voir Production of germanium stable isotopes single crystals par Mihail Fedorovich Churbanov et al, avril 2017 (6 pages).

Rubidium

Le rubidium est un métal alcalin utilisé pour créer des qubits à atomes froids qui sont excités dans des états très énergétiques dits de Rydberg. On l'utilise aussi en métrologie quantique, notamment pour créer des horloges atomiques.

C'est un métal alcalin, mou et argenté dont la température de fusion n'est que de 39,3 °C (*ci-dessous*, à l'état fondu, source Wikipedia). Dans un calculateur à atomes froids, le métal est utilisé de manière très parcimonieuse. Il est fourni dans des ampoules de quelques grammes à l'état solide. Il est chauffé dans une petite boîte pour être sublimé en gaz qui alimente ensuite l'enceinte sous vide où les lasers vont piéger des atomes individuels. Le métal coûte environ $85 le gramme et de l'ordre de $1600 les 100g. Il est facilement accessible auprès d'entreprises de chimie. Il en est produit seulement 5 tonnes par an dans le monde, notamment en Chine, au Canada, en Namibie et au Zimbabwe[327].

C'est un sous-produit de l'extraction de césium et de lithium. L'isotope ^{87}Ru est le plus couramment utilisé et représente 27,8% des atomes de rubidium disponibles. Il est radioactif mais avec une demi-vie plus longue que l'âge de l'Univers, donc autant dire qu'il est très stable.

Les réserves mondiales sont estimées à 100 000 tonnes, qui permettent de tenir le coup assez longtemps au rythme actuel de production et de consommation.

Niobium

Le niobium est un métal de transition qui est utilisé dans les qubits supraconducteurs ainsi que dans les câbles de micro-ondes de lecture d'état de qubits supraconducteurs et siliciums. La fabrication de ces câbles est dominée par le Japonais Coax Co et ils coûtent très cher : environ $3K la pièce. Et il en faut trois par qubits supraconducteurs qui sont positionnés entre les étages 4K et 15mK dy cryostat.

Dans l'industrie, il est utilisé dans les aciers spéciaux à forte résistance, dans les aimants supraconducteurs, dans les accélérateurs de particules, dans la soudure à l'arc, dans les prothèses osseuses associé au titane, en optique, comme catalyseur de la synthèse de caoutchouc, dans les réacteurs d'avions, dans les turbines à gaz, etc. La production mondiale était estimée à 68 000 tonnes par an en 2018, le Brésil en représentant 88%, suivi du canada pour un peu plus de 9%, généré par une seule mine.

Elle provient de l'exploitation du pyrochlore, un minerai associant calcium, sodium, oxygène et niobium.

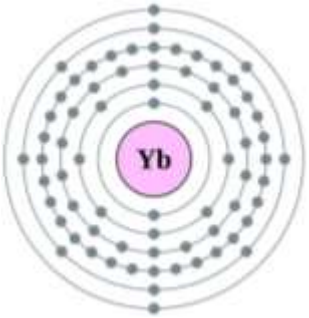
Il n'est pas bien cher et se trouve à $45 le kilo, mais sous sa forme ferroniobium. Les réserves seraient de 9 millions de tonnes, de quoi donc tenir 130 ans au rythme actuel. Mais en pratique, le niobium est considéré comme étant une ressource « à risque » car la demande est en forte croissance.

[327] Chaque humain de 70 kg en contient environ 0,36g. On ne va pas pour autant créer une variante de Soylent Green pour l'exploiter. L'extraction de rubidium au Canada est assurée par Tantalum Mining Corporation qui appartient au groupe chinois Sinomine Resources depuis juin 2019.

Ytterbium

L'ytterbium est une terre rare de la série des lanthanides qui est utilisée dans les qubits à ions piégés, les mémoires quantiques, les horloges atomiques, le dopage de certains lasers et, plus rarement, dans les qubits à atomes froids.

Il est sinon utilisé pour renforcer certains aciers spéciaux.



Le métal est extrait de la monazite, une structure rocheuse cristalline tétraédrique d'oxyde de phosphore associé à diverses terres rares, qui n'en contient que 0,03%. La production suit un cycle complexe avec usage d'acide sulfurique et d'échanges ioniques. Les applications quantiques en utilisent l'isotope 171, l'un des 7 isotopes non radioactif de l'élément. Il représente 14% de sa proportion dans les roches d'où il est extrait. Cet isotope est probablement plus cher que le tout-venant qui est commercialisé entre $500 et $1K le kilogramme.

Il en est produit environ 50 tonnes par an, notamment en Chine, aux USA, au Brazil, en Inde et en Australie, avec des réserves estimées à un million de tonnes, ce qui permet aussi de tenir quelques temps. Les besoins pour créer des ions piégés sont de l'ordre de moins d'un gramme par processeur quantique.

Erbium

Cette terre rare de la famille des lanthanides est utilisée dans les mémoires quantiques, dans certains qubits à atomes froids et dans certains lasers (type Er:YLF pour yttrium lithium fluoride ou Er:YAG pour oxyde d'yttrium et d'aluminium). On le trouve dans certaines fibres optiques utilisées dans des amplificateurs optiques.

Enfin, il peut servir à créer des alliages de vanadium utilisables dans des cryostats grâce à une capacité thermique massique élevée. C'est une capacité d'absorption de la chaleur ramenée à la masse.

La Chine en est le principal producteur, suivi des USA, par extraction à partir de xénotime (minerai de phosphate) et d'euxénite (un minerai contenant aussi du niobium, du titane et de l'yttrium). Le minerai est attaqué à l'acide chlorhydrique ou sulfurique puis neutralisé à la soude. Après de nombreux traitements chimiques, les ions d'erbium sont extraits par échanges ioniques à base de résines polymères.

L'erbium est alors obtenu en chauffant son oxyde avec du calcium à 1450°C et sous atmosphère d'argon. Bref, tout cela constitue un long et couteux processus chimique, probablement assez polluant mais réalisé sur de faibles volumes.

Il est en effet produit à raison d'environ 500 tonnes par an. Le prix du gramme est d'environ $20, ce qui est tout à fait abordable pour l'intégrer dans des mémoires ou qubits des à base d'atomes froids.

Strontium

Le strontium est le métal alcalin le plus souvent utilisé pour créer des qubits à ions piégés, dans l'isotope 87, l'un des cinq les plus courants de l'élément avec 7% du total. Il est utilisé comme colorant rouge dans les feux d'artifice.

Le Mexique et l'Allemagne en sont les principaux producteurs avec une production mondiale estimée à 220 000 tonnes par an et des réserves supérieures au milliard de tonnes. Il est notamment utilisé dans certaines thérapies anticancéreuses. Côté quantique, son usage anecdotique est évoqué pour des qubits à ions piégés.

Le strontium est considéré comme étant toxique. C'est le cas de tous ces métaux rares qui, purs, s'oxydent rapidement quoi qu'il arrive. Ils explosent notamment au contact de l'eau.

Or

Dans les technologies quantiques, l'or est surtout utilisé sous forme de couche fine recouvrant les plaques de cuivre des « cold plates » dans les cryostats. Elles servent à empêcher l'oxydation du cuivre et ajoutent une bonne conductivité thermique. Les quantités utilisées sont faibles par rapport à la production d'or et à ses réserves mondiales.

Titane

Le titane est surtout utilisé dans les câbles micro-ondes de lecture d'état de qubits supraconducteurs, associé au niobium. Cela en fait des câble très chers, à $3K l'unité sur quelques dizaines de centimètres de longueur.

Dans l'industrie, il est utilisé pour sa résistance à la corrosion et en particulier dans l'industrie aérospatiale. Certains sous-marins ont une coque entièrement en titane. L'oxyde de titane sert de pigment blanc pour les peintures. On en trouve beaucoup sur Terre puisque c'est le cinquième métal en termes d'abondance. Mais seuls quelques minerais en contiennent une concentration suffisamment élevé pour que sa production soit rentable. Les principaux pays producteurs sont l'Australie, l'Afrique du Sud, le Canada et la Norvège à raison de 4,2 millions de tonnes par an. Les réserves sont supérieures à 600 millions de tonnes.

Azote

L'azote est utilisé à l'état liquide dans les cryostats pour le nettoyage de l'hélium gazeux qui les alimente. Il se trouve également dans les NV Centers. Ce n'est pas une denrée rare. Mais sa production sous forme liquide est assez consommatrice d'énergie.

Autres matériaux

De nombreux autres matériaux relativement courants sont utilisés dans les technologies quantiques.

Le **cuivre** se trouve dans les cold plates des cryostats et une partie de la connectique. Si l'on évoque l'épuisement de cette ressource, sa consommation liée aux technologies quantiques est mineure[328]. Dans certains cas, on utilise du cuivre purifié à 99,99% et notamment débarrassé des impuretés et de l'oxygène (OFHC pour oxygen-free high conductivity), pour améliorer sa conductivité thermique et sa conductance électrique. On en utilise aussi beaucoup dans les enceintes de confinement pour le calcul à base d'ions piégés.

Le **carbone** est exploité à divers endroits et notamment dans les technologies à base de nanotubes de carbone comme par la startup C12 Quantum Electronics. Or ce carbone doit être purifié pour n'en conserver que l'isotope 12. Ce carbone 12 est acquis sous forme de méthane dans des bouteilles acquises aux USA pour $10K. Il est purifié à 99,997%. La séparation isotopique du carbone 12 utilise un procédé chimique appliqué à du CO^2. Le carbone est aussi utilisé dans les NV centers.

L'**aluminium** est utilisé dans certains qubits supraconducteurs ainsi que pour une partie de la connectique dans les cryostats. Il est abondant.

L'**argent** est surtout utilisé sous forme de poudres dans certains échangeurs de chaleur des systèmes de réfrigération à dilution.

Le **fer** est utilisé sous forme d'acier dans la structure porteuse des ordinateurs.

---

[328] Voir Raréfaction des métaux : demain, le « peak all » par Matthieu Auzanneau, mai 2012.

Le **césium** est surtout utilisé dans les horloges atomiques, dans son isotope 133. Les réserves sont suffisamment abondantes par rapport aux besoins identifiés. Elles sont surtout situées au Canada.

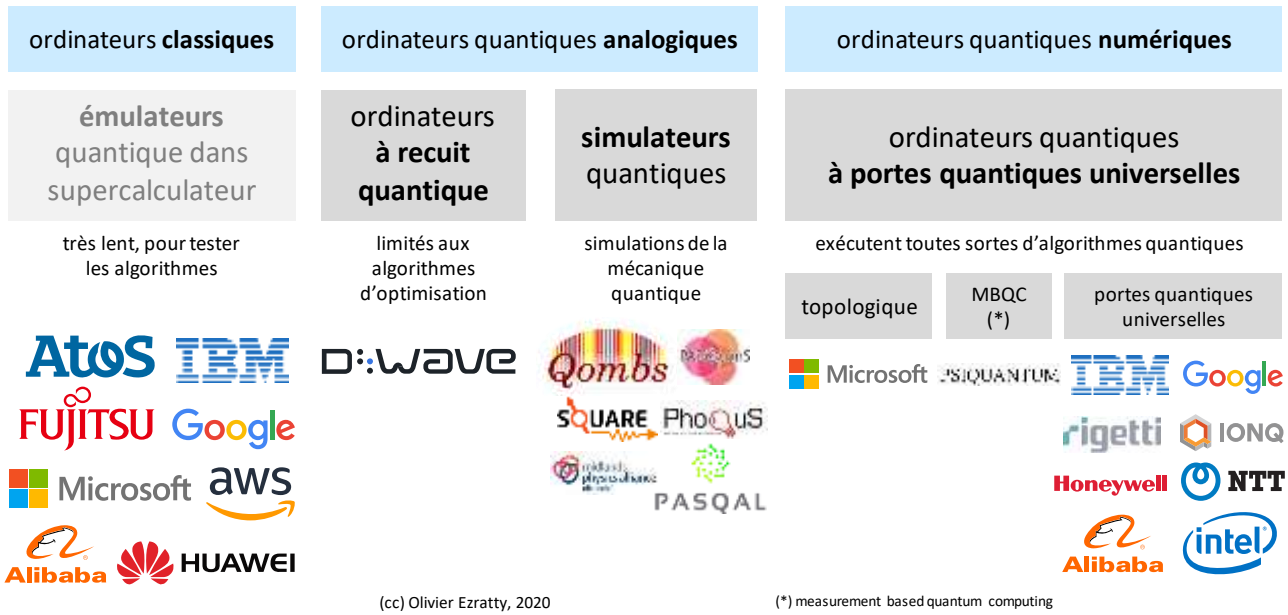
Le **gallium** et l'**indium** jouent en complément du germanium un rôle clé dans les composants III-V utilisés principalement en photonique. C'est l'un des rares domaines des technologies quantiques où il existe une forte dépendance vis-à-vis de la Chine en source d'approvisionnement.

Enfin, le **bérylium**, le **manganèse**, le **calcium**, le **zinc**, le **cadmium** et le **mercure** peuvent être utilisés dans les qubits à ions piégés. Mais les plus courants sont l'ytterbium et le calcium.

Elément	Calcul	Métrologie & autres	Rareté	Cleanliness
Hélium 3	Cryostats			
Hélium 4	Cryostats	Cryostats		
Silicium 28	Qubits silicium			
Rubidium	Atomes froids	Atomes froids		
Niobium	Câbles, qubits supra			
Ytterbium	Ions piégés, mémoire			
Erbium	Atomes froids, mémoire			
Strontium	Ions piégés			
Or	Cold plates			
Titane	Câbles			
Gallium		Photonique		
Germanium		Photonique		
Indium		Photonique		
Azote	Cryostats	NV Centers		
Aluminium	Cryostats, qubits supra			
Argent	Cryostats			
Césium		Horloges		
Carbone	NV Centers, nanotubes	NV Centers		

Grandes catégories d'ordinateurs quantiques

Il y a ordinateur quantique et ordinateur quantique. On oppose souvent les ordinateurs quantiques adiabatiques du Canadien D-Wave aux ordinateurs quantiques universels d'IBM ou Google.



Catégories de calculateurs quantiques

Mais il faut compter en tout avec au moins six catégories d'ordinateurs quantiques que voici :

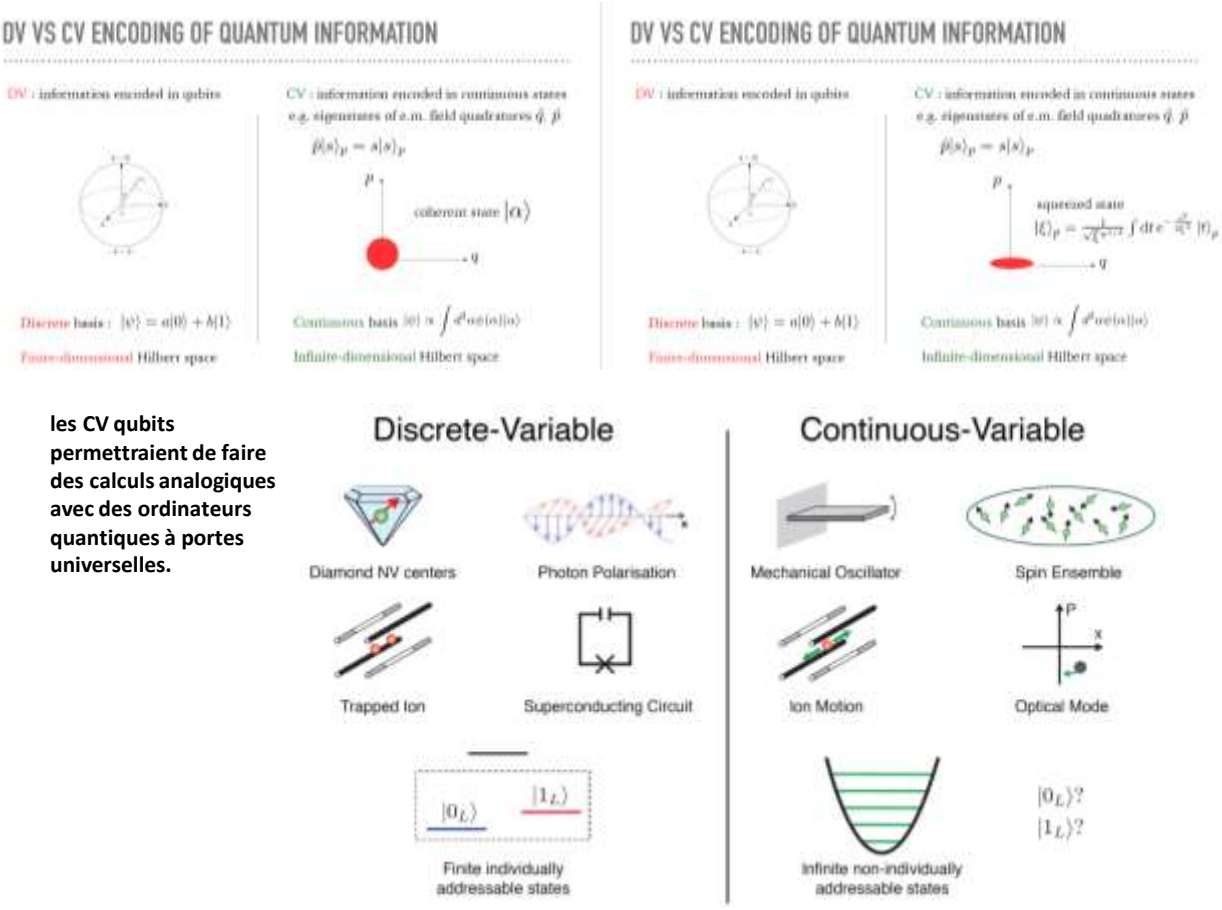
- Les **émulateurs quantiques** qui sont utilisés pour réaliser des simulations de l'exécution d'algorithmes quantiques dans des ordinateurs traditionnels qui vont de simples laptops à des supercalculateurs, selon le nombre de qubits à émuler. Ils transforment ces algorithmes, les portes quantiques et les qubits pour exploiter les capacités de traitement d'ordinateurs traditionnels. Cela permet de tester des algorithmes quantiques sans ordinateurs quantiques. Mais c'est bien plus lent ! Les émulateurs quantiques sont parfois dénommés simulateurs quantiques, mais cette appellation est à éviter. Elle peut en effet être confondue avec… les simulateurs quantiques, qui sont des ordinateurs quantiques analogiques simulant des phénomènes de physique quantique, par exemple relevant du magnétisme ou de la structuration de molécules organiques ou inorganiques.

  A ce jour, les supercalculateurs peuvent simuler jusqu'à l'équivalent d'une quarantaine à une cinquantaine de qubits, mais nous avons vu précédemment que des records avaient été battus avec plus de 100 qubits, avec un faible nombre de portes quantiques. C'est ce que proposent IBM, Microsoft, Google et le Français Atos. Simuler des ordinateurs quantiques de cette manière demande beaucoup de puissance à la fois côté mémoire, pour stocker 2^N états de registres quantiques à N qubits, ainsi que pour les traitements associés qui reposent sur des multiplications de matrices en nombres flottants. Des records dans ce domaine sont régulièrement battus.

  En 2017, l'émulation de 45 qubits était réalisée sur un supercalculateur du Département de l'Energie US (du National Energy Research Scientific Computing Center ou NERSC) exploitant 8192 processeurs Intel Xeon Phi, ce qui s'explique par la présence d'un centre de recherche conjoint avec Intel au NERSC. Le record était battu la même année par IBM avec la simulation de 56 qubits. Pour simuler 49 qubits, il faut rien moins qu'un Péta-Octets de mémoire vive !

- Les **ordinateurs quantiques à recuit simulé** comme ceux du Canadien D-Wave. Ils s'appuient sur des qubits de qualité moyenne et sont adaptés à l'exécution d'une partie seulement des algorithmes quantiques connus et avec un gain en puissance de calcul intéressant mais contesté par certains spécialistes. Cette technique utilise une évolution lente et contrôlée d'un ensemble de qubits reliés entre eux dans des matrices de qubits ("lattice"). On l'initialise dans un état voisin de la solution et le système converge vers la solution qui relève souvent de la recherche d'un minimum énergétique comme pour la simulation d'interactions atomiques dans des molécules ou l'optimisation de la durée d'un parcours complexe.

- Les **simulateurs quantiques analogiques** servent de simulateurs de phénomènes quantiques sans passer par la case des qubits avec leurs deux états 0 et 1. Ils fonctionnent de manière analogique et non numérique, à savoir que les paramètres reliant les qubits entre eux sont continus. Ce sont pour l'instant surtout des outils de laboratoires. La technique la plus couramment utilisée est celle des atomes froids contrôlés par lasers. Elle peut d'ailleurs être exploitée aussi bien pour créer des ordinateurs quantiques analogiques que des ordinateurs quantiques universels à base de qubits et de portes quantiques. On peut considérer que les ordinateurs quantiques à recuit simulé et les simulateurs quantiques analogiques font partie tous deux de la catégorie des ordinateurs quantiques analogiques, avec des nuances d'architecture.
- Les **ordinateurs quantiques à variables continues**, ou analogiques à portes universelles. Ils utilisent des qubits qui stockent des grandeurs variables entre 0 et 1 et sont manipulables avec des portes quantiques[329]. Cette catégorie de calcul quantique a été proposée en 1999 par Seth Lloyd et Samuel Braunstein[330]. Elle est notamment proposée par la startup **Xanadu**.



les CV qubits permettraient de faire des calculs analogiques avec des ordinateurs quantiques à portes universelles.

- Les **ordinateurs quantiques universels** utilisent des qubits avec des portes quantiques capables d'exécuter tous les algorithmes quantiques et avec un gain de vitesse optimum par rapport aux supercalculateurs ainsi que vis à vis des ordinateurs quantiques adiabatiques[331]. Ils sont pour l'instant limités à une cinquantaine de qubits. Le niveau de bruit quantique des qubits nuit à l'efficacité des calculs et impose de démultiplier les qubits et l'enchaînement des portes quantiques pour gérer des codes de correction d'erreurs quantiques (QEC).

[329] Voir Universal Quantum Computing with Arbitrary Continuous-Variable Encoding, 2016 (5 pages) ainsi que Continuous-variable quantum computing in the quantum optical frequency comb par Olivier Pfister, 2019 (16 pages).

[330] Voir Quantum Computation over Continuous Variables par Seth Lloyd et Samuel L. Braunstein, février 1999 (9 pages).

[331] En voici un panorama rapide dans Quantum Computing Circuits and Devices, avril 2018 (18 pages).

En attendant que ces ordinateurs quantiques montent en puissance avec des qubits de qualité, on se contente de qubits de qualité intermédiaire. Cette sous-catégorie d'ordinateurs quantiques universels est baptisée NISQ pour "Noisy Intermediate-Scale Quantum" par John Preskill[332]. Elle décrit les ordinateurs quantiques universels existants et à venir dans un futur proche supportant 50 à quelques centaines de qubits et à même de dépasser les capacités des supercalculateurs. Avant l'émergence de LSQ, large scale quantum computers, avec un très grand nombre de qubits physiques ou logiques présentant un faible taux d'erreur compatible avec les besoins logiciels.

- Les MBQC, ou **Measurement Based Quantum Computers**, sont une variante d'ordinateurs et méthodes qui utilisent des qubits, mais exploités différemment, avec une mise en intrication de l'ensemble des qubits suivie d'une lecture de l'état de certains qui permet d'avancer pas à pas dans la résolution d'algorithmes en simulant des portes quantiques. Cette méthode est particulièrement intéressante pour les systèmes où des portes quantiques à deux qubits sont difficiles à réaliser, notamment avec les qubits photons. La startup PsiQuantum prévoit d'utiliser une variante de cette technique. J'en détaille le procédé dans une rubrique dédiée *ci-dessous*.
- Le **calcul topologique** s'appuie sur des qubits et une organisation de qubits particulière qui est résistante au bruit. Le modèle de programmation de ces qubits à bas niveau est différent de celui des ordinateurs quantiques universels. C'est la voie choisir par Microsoft, en compagnie des Hollandais de QuTech. Sa mise au point semble pour l'instant très laborieuse.

Cet inventaire n'est un apéritif car nous aurons l'occasion plus loin de détailler ces architectures. Le gros des explications sur les qubits et les entrailles d'un ordinateur quantique type portera sur la catégorie dominante du calcul quantique à portes universelles. Nous creuserons un peu le fonctionnement du calcul à recuit quantique dans la partie dédiée à D-Wave. Nous verrons rapidement les autres catégories.

Measurement Based Quantum Computing

Le Measurement Based Quantum Computing est une approche très particulière du calcul quantique. Et pour cette édition de l'ebook, j'essaye de partager ce que j'ai pu comprendre de son fonctionnement que je me suis fait expliquer par **Elham Kashefi**, une grande spécialiste du sujet. Et ce n'est qu'une version très résumée probablement approximative.

Le MBQC consiste à exploiter l'initialisation de qubits intriqués puis d'effectuer des mesures pas à pas sur certains qubits pour obtenir en bout de course un résultat sur les derniers qubits mesurés. Il existe sous plusieurs variantes, le *one way quantum computing* (1WQC) [333] qui utilise des matrices bidimentionnelles de qubits permettant de créer des « cluster states » et le *measurement-only QC* qui ne fait que de la mesure, sans intrication préalable. Nous allons nous focaliser ici sur la première méthode qui semble la plus couramment étudiée.

Le MBQC permet d'exécuter des algorithmes quantiques classiques à portes universelles. A quoi cela peut-il servir de se faire de tels nœuds dans le cerveau ? Cette méthode est particulièrement intéressante dans les calculateurs quantiques à base de qubits sur lesquels il est difficile de créer des portes quantiques à plusieurs qubits exploitant l'intrication.

---

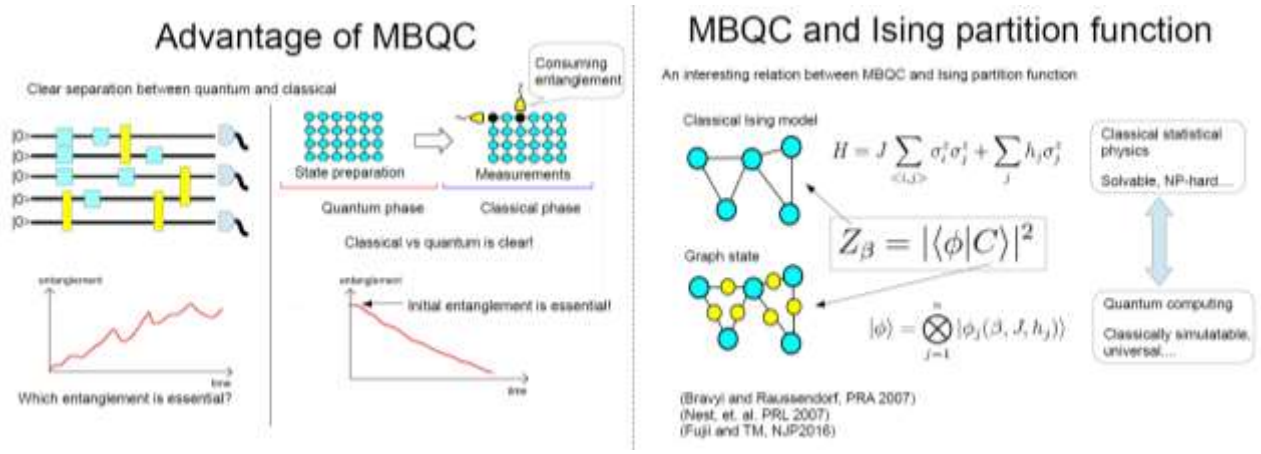
[332] Dans Quantum Computing in the NISQ era and beyond en 2018.

[333] Le procédé a été conçu en 2000 par Robert Raussendor et Hans Briegel. Voir A computationally universal phase of quantum matter, de Robert Raussendorf, 2018 (41 slides), Measurement-based Quantum Computation d'Elham Kashefi, University of Edinburgh (50 slides) et la très complète Introduction to measurement based quantum computation de Tzu-Chieh Wei de l'Université Stone Brook, 2012- (88 slides) et un one pager : Universal measurement-based quantum computation with Mølmer-Sørensen interactions and just two measurement bases. D'autres sources d'information à creuser : Blind quantum computation de Charles Herder (10 pages), Cluster-state quantum computation, de Michael Nielsen, 2005 (15 pages), Fault-tolerant quantum computation with cluster states par Michael Nielsen et Christopher Dawson, 2004 (26 pages), 2D cluster state (50 slides), Quantum Computing with Cluster States de Gelo Noel Tabia, 2011 (18 pages), Quantum picturalism for topological cluster-state Computing de Clare Horsman 2011 (18 pages) et Cluster State Quantum Computing de Dileep Reddy et al, 2018 (11 pages.

Le modèle était initialement adapté aux calculateurs à base d'atomes froids mais il prend tout son sens avec les qubits photons pour lesquels ces portes à deux qubits sont difficiles à mettre au point. Les photons sont aussi indiqués car ils permettent de gérer facilement des angles de rotation dans la sphère de Bloch qui sont utilisées dans les portes quantiques à un qubit du procédé, via un contrôle de la phase des qubits-photons.

Dans le MBQC, on fait un peu les choses à l'envers vis à vis du calcul quantique classique : on intrique d'abord les qubits, on applique dessus des portes à un qubit et on les mesure progressivement alors que dans le calcul quantique classique à portes universelles, on n'intrique les qubits que progressivement et on ne réalise des mesures qu'en fin de calcul.

Modulo celles que l'on peut éventuellement faire sur des qubits auxiliaires lors de la correction d'erreurs comme nous l'avons vu précédemment.



Un calcul MBQC est **logiquement irréversible**, contrairement au calcul à base de portes quantiques universelles. En effet, le processus de mesure d'états des qubits ne peut pas être inversé logiquement sauf lorsque l'état des qubits lus correspond pile-poil à leurs états de base |0⟩ et |1⟩. Un calcul quantique à portes universelles est l'équivalent de l'application d'une transformation unitaire incarnée par une matrice géante carrée de dimension 2N à un jeu de N qubits initialisés à l'état |0⟩. Cette matrice peut être inversée en déroulant à l'envers les portes quantiques qui ont servi à la créer. Dans le MBQC, ce n'est pas possible. Cette irréversibilité du calcul MBQC explique pourquoi il est aussi appelé 1WQC pour One Way Quantum Computing. On ne peut pas revenir en arrière. Quelle en est la conséquence ? Bien, je ne sais pas encore... !

Ce modèle est aussi **probabiliste**, du fait de la nature probabiliste des mesures d'état des qubits à chaque étape du calcul. Les mesures successives permettent d'obtenir de l'information sur l'état des qubits qui permet de redevenir déteministe dans la suite du calcul en appliquant une sorte de correction d'erreur à la volée. Un peu comme si on utilisait des codes de correction d'erreurs à 3 qubits.

Le MBQC s'appuie par définition des **algorithmes hybrides** puisque leur déroulement dépend d'interactions entre la partie quantique et l'exploitation des mesures par un ordinateur classique de pilotage de l'ensemble.

Les qubits utilisés dans le MQBC à base de cluster states sont de quatre classes : ceux qui sont préparés et mesurés (les qubits auxiliaires), ceux qui sont uniquement mesurés pendant le calcul, ceux qui sont uniquement préparés (mais mesurés en fin de calcul) et ceux qui sont ni préparés ni mesurés (qui servent au reste du calcul).

Le principe repose sur l'enchaînement de séquences dites NEMC avec quatre étapes :[334]

[334] Sources d'informations utilisées : Advanced Quantum Algorithms par Giulia Ferrini et al, 2019 (30 pages) et An introduction to Quantum Computing par Elham Kashefi, School of Informatics University of Edinburgh, 2020 (119 slides).

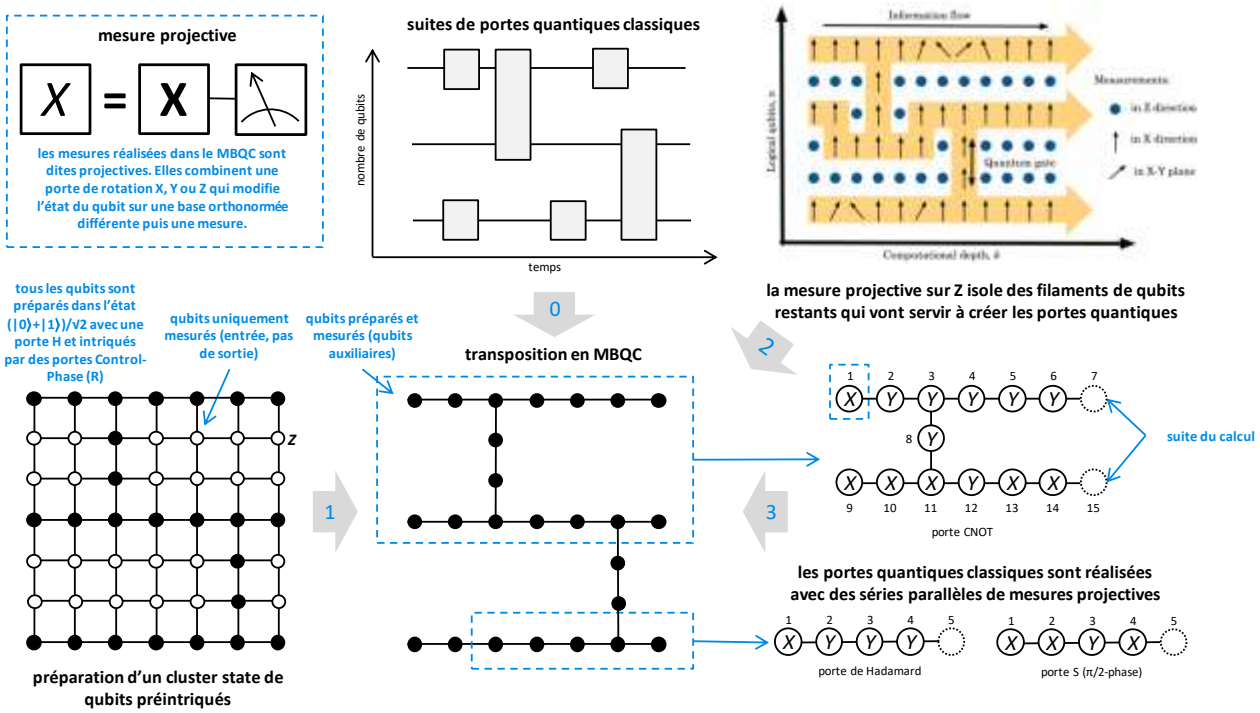
- L'utilisation d'un ensemble de **qubits auxiliaires** (étape N), ceux du premier type.
- L'**intrication** entre certains des qubits (étape E) dans des groupes dénommés « cluster states ». Le système n'intrique pas tous les qubits du calculateur. Il le fait groupe par groupe, qui sont les clusters. L'intrication est par exemple générée par une série de portes Control-Phase (ou control R) sur des qubits initialisés dans l'état $|+\rangle = |0\rangle + |1\rangle)/\sqrt{2}$ avec une porte H appliquée à l'état $|0\rangle$. Comme ces portes sont commutatives, l'ordre dans lequel elles sont exécutées pour préparer l'intrication n'a pas d'importance ce qui a un impact sur la parallélisation des traitements. Un cluster est un graphe quelconque de qubits intriqués, le plus courant étant une matrice 2D de qubits tous intriqués avec leur voisins immédiats.
- La **mesure de l'état de qubits** intermédiaires pendant le calcul (M). Elle est réalisée avec une technique dite de mesure projective. Elle consiste à appliquer d'abord une ou plusieurs portes à un qubit X ou Y sur les qubits pour les faire tourner dans leur sphère de Bloch puis à mesurer leur état. Un peu comme si on faisait pivoter l'axe $|0\rangle/|1\rangle$ de la sphère de Bloch pour changer de repère.

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

$$|\pm_\alpha\rangle = \frac{|0\rangle \pm e^{i\alpha}|1\rangle}{\sqrt{2}}$$

  La base projective de mesure se présente sous la forme d'états du type $|\pm_\alpha\rangle$, α étant en général un demi ou un quart de tour dans la sphère de Bloch. Un qubit mesuré est toujours une ressource intermédiaire et n'est pas une ressource en sortie. Cela permet d'obtenir une information qui permet de manipuler ensuite les qubits et de propager le calcul. Les mesures projectives Z ont pour effet de supprimer les qubits mesurés du cluster.
- Ces **corrections** successives rendent le calcul déterministe (étape C) avec des portes X et Z. Elles sont appliquées en fonction du résultat des mesures projectives réalisées en (M). Aucune porte de correction n'agit ici sur un qubit déjà mesuré. Ce modèle permet d'appliquer n'importe quelle porte à un qubit qui est en fait une combinaison de $R_z(\gamma)R_x(\beta)R_z(\alpha)$, à savoir des rotations autour des trois axes de la sphère de Bloch d'angles γ, β et α[335].

Voici tout cela résumé dans le schéma composite suivant :



[335] La décomposition de portes quantiques en méthode de calcul pouvant servir au MBQC a été brevetée par Krysta Svore de Microsoft qui y dirige le groupe QuArC.

Ce que je viens de décrire permet (enfin) d'interpréter la partie basse-droite de l'illustration *ci-dessus* qui explique comment sont réalisées en MBQC des équivalents des portes quantiques CNOT (à deux qubits), H ou S. Chaque cercle *X* ou *Y* est une mesure projective X et Y qui combine une porte X ou Y suivie d'une mesure d'état. La mesure obtenue conditionne le type de mesure projective réalisée juste après dans l'ordre indiqué (1 à 15 et 1 à 5).

Deux formes de mesures affectent le fonctionnement de la matrice de qubits : des mesures Z séparent les qubits en creusant des « sillons » dans la matrice, un peu comme des pacmans, puis des mesures classiques le long des « fils » ou sur les « ponts » entre ces fils simulent des portes à un qubit comme celle de Hadamard et la porte CNOT à deux qubits. L'enchaînement des opérations dépend du résultat des mesures. Le résultat du calcul est situé dans les derniers qubits dont l'état n'est pas encore mesuré… et qui sera mesuré en dernier lieu[336].

Cette combinaison de séquences NEMC permet de reproduire le fonctionnement de portes quantiques à un et deux qubits. Un calcul quantique complet est un enchaînement de NEMC multiples qui se termine par la mesure de l'état des qubits qui restent ! Le reste, ce sont des maths dont je vous passe le détail.

Les conséquences de ce que nous venons de voir sont multiples :

- Le MBQC demande **plus de qubits** que dans un modèle à base de circuits classiques. Dans le schéma, on voit qu'une simple porte X ou Y résulte de la combinaison de quatre portes X et Y et d'autant de mesures. Cela créé au passage une « pression » sur la partie classique du calcul, liée à la mesure. Mais on se rattrape (plus loin) avec le parallélisme.
- Le MBQC ne dispense pas de la mise en oeuvre de **codes de correction d'erreurs** tels que ceux que nous avons étudiés dans une partie précédente. Eux aussi vont multiplier par plusieurs ordres de grandeur le nombre de qubits physiques nécessaires au calcul. Ils pourraient être facilités si l'on pouvait organiser les qubits en matrices 3D, la troisième dimension servant à aligner les qubits nécessaires à la correction d'erreurs, notamment avec des surface codes. Par contre, le modèle MBQC contenant ses propres mécanismes de correction d'erreurs, il est moins gourmand en qubits additionnels pour la correction d'erreurs nécessaires à la création d'ordinateurs quantiques « fault tolerant ».
- La **dimension temporelle** du calcul est modifiée par rapport au calcul quantique classique. Comme on peut paralléliser les opérations couplant portes et mesures, le MBQC est un peu le Nutella sur la tartine : on peut l'étaler ! La profondeur du calcul disponible n'est plus liée à la capacité à enchaîner des portes quantiques dans la durée comme dans le schéma milieu-haut de l'illustration précédente, mais à en exécuter un grand nombre en parallèle sur un très grand nombre de qubits (modulo la correction d'erreurs). En effet, les séquences de portes-mesures labellisées 1, 2 ... n vont pouvoir être réalisées simultanément par groupe 1, 2 ... n, n étant limité à 15. On a donc quasiment besoin d'une profondeur de calcul physique limitée par le nombre maximum de portes à enchaîner pour réaliser une CNOT. C'est un argument en faveur des qubits photons. La profondeur d'un algorithme ne dépend plus de la capacité à enchaîner des portes quantiques à un et deux qubits mais à la capacité d'intrication des qubits au démarrage dans les clusters states du modèle. Bref, on remplace du calcul quantique séquentiel par du calcul quantique massivement parallèle. C'est l'approche de la startup PsiQuantum.
- Le modèle MBQC est facilement exploitable pour tirer parti d'algorithmes de téléportation et de **calcul quantique distribué**. Des clusters states vont pouvoir être reliés entre eux via des liaisons optiques distantes. C'est aussi l'un des outils du blind computing[337].

---

[336] Source des illustrations : Basics of quantum computing and some recent results de Tomoyuki Morimae, 2018 (70 slides).

[337] Voir à ce sujet Measurement-based and Universal Blind Quantum Computation par Anne Broadbent, Joseph Fitzsimons et Elham Kashefi, 2016 (41 pages).

- Enfin, il existe un lien direct entre le MBQC et le **ZX Calculus**. Ce dernier est un modèle de graphes qui permet de formaliser le MBQC, ses cluster states et les corrections d'erreur associées[338].

Les startups qui se sont lancées dans ce créneau sont **PsiQuantum** (USA) et **Pasqal** (France) dont nous détaillons les approches dans la rubrique dédiée aux startups et PME du calcul quantique. Les algorithmes sont spécifiques à ce genre d'architecture[339]. Il n'est pas encore expérimentable car il demande un grand nombre de qubits qui ne sont pas encore pratiquement disponibles.

Coût et prix

Au vu de la faible maturité du marché, c'est presque une question qui n'a pas de sens. Les seuls ordinateurs quantiques qui sont commercialisés aujourd'hui sont ceux du canadien D-Wave, et à un prix unitaire de $15M. Le reste de l'offre est accessible en cloud ou gratuitement ou à des tarifs généralement abordables.

Le prix d'un ordinateur quantique dépend de plusieurs paramètres dont le coût de fabrication et d'intégration de ses composants, les économies d'échelle, la marge du constructeur qui intègre les coûts du marketing et de la vente, le coût de maintenance et celui d'éventuels consommables. Ce sont des composantes dynamiques : plus le volume de ventes augmente, plus grandes sont les économies d'échelle. Or les volumes sont pour l'instant très faibles. Ils pourraient le rester longtemps jusqu'au jour où des applications émergeront qui toucheront un grand nombre d'utilisateurs et justifieront la fabrication en volume de ces ordinateurs. Il faut bien entendu y ajouter les coûts fixes de la R&D qui sont plus long à amortir si les volumes de vente sont limités.

Reprenons une par une les grandes composantes matérielles d'un ordinateur quantique avec cette analyse d'économies d'échelle :

- Le ou les **ordinateurs de contrôle** : c'est du standard tout comme la connectique réseau associée.
- Le **chipset** : celui a beau être fabriqué en technologies CMOS ou avoisinantes, leur volume de fabrication est très faible. Les économies d'échelle sont donc quasiment inexistantes. On économise ce composant dans le cas des qubits à base d'atomes froids mais il est remplacé par des composants optiques spécialisés pour orienter les faisceaux laser de contrôle des atomes.
- Les **composants électroniques** de contrôle des portes quantiques : leur technologie dépend du type de qubit utilisé. Dans les ordinateurs supraconducteurs, ce sont des générateurs de micro-ondes du marché mais la tendance est à créer des circuits cryogéniques spécialisés.
- La **cryogénie** : ce sont des systèmes standards mais commercialisés en faible volume. Ils peuvent coûter jusqu'à $1M pour les qubits supraconducteurs et silicium. Leur coût est de un à deux ordres de grandeur plus faible pour la cryogénie de composants comme ceux des qubits photons.
- Le **câblage** : il coute très cher pour les calculateurs à base de qubits supraconducteurs, autant que le cryostat. A long terme, celui-ci disparaîtra pour laisser la place à des circuits de contrôle des qubits qui seront miniaturisés.

---

[338] Evoqué dans Universal MBQC with generalised parity-phase interactions and Pauli measurements par Aleks Kissinger et John van de Wetering, 2019 (21 pages).

[339] Voir par exemple Changing the circuit-depth complexity of measurement-based quantum computation with hypergraph states, mai 2019 (16 pages). L'article décrit une méthode de MBQC basée sur l'exploitation de portes de Toffoli (CCZ) et Hadamard (H). Elles permettent de simuler du calcul quantique topologique, réducteur du taux d'erreur du calcul quantique.

- Les **consommables** : dans les ordinateurs quantiques fonctionnant à très basse température, il y a au minimum de l'azote liquide et de l'hélium 3 et 4 gazeux. Ces deux derniers ne sont pas des consommables et fonctionnent en circuit fermé dans le système de cryogénie à sec.

Au gré de la maturation des technologies quantiques, certaines structure de coût augmenteront, d'autres baisseront. Le jeu des économies d'échelle fera le reste. Au nez, on peut donc prévoir que le prix des D-Wave à $15M puisse rester quelques temps une fourchette haute du prix d'un ordinateur quantique en tout cas, à qubits supraconducteur.

Il faudrait refaire le calcul pour les autres types de qubits notamment les ions piégés, les atomes froids et les photons. La ventilation des coûts serait probablement assez différente.

Dans la pratique, nombre d'ordinateurs quantiques seront utilisables comme des ressources dans le cloud et avec un coût plus modéré. C'est ce que proposent déjà IBM, Rigetti, D-Wave, Microsoft et Amazon (avec des machines tierces pour ces deux derniers).

Incertitude quantique

La prospective dans l'informatique quantique est art difficile. On navigue entre les optimistes et les pessimistes.

Optimistes

Google**,** IBM **et** Microsoft pensent atteindre relativement rapidement une véritable suprématie quantique et créer des ordinateurs quantiques de plus de 100 qubits de qualité d'ici moins d'une décennie. Leur communication se fait à plusieurs niveaux : pour le grand public, elle est simplificatrice et destinée à marquer les esprits, quitte à enjoliver la mariée. C'est ce que l'on a pu voir avec l'annonce de la suprématie quantique de Google en septembre-octobre 2019 qu'il fallait regarder de très près pour pouvoir prendre du recul à son sujet !

Kenneth Regan pensait en 2017 qu'un industriel – probablement Google – devait prétendre avoir atteint la suprématie quantique en 2018 et qu'il serait rapidement contredit par la communauté scientifique[340]. C'est ce qui est arrivé en 2019. Voilà une prévision bien vue !

Pour les spécialistes qui peuvent décortiquer leurs publications scientifiques, le regard est évidemment plus nuancé, notamment au sujet de la fiabilité des qubits qu'ils génèrent. Ils communiquent beaucoup sur leurs efforts pour réduire le bruit des qubits pour les rendre plus fiables[341].

Pour **Alain Aspect**, il n'y aurait pas d'obstacle scientifique à la création d'ordinateurs quantiques fiables. Il pense que l'incertitude est uniquement une question technologique et d'ingénierie mais qu'il faudra quelques décennies pour la lever. Ce ne serait donc qu'une affaire de patience ! Rien n'empêche cependant une accélération de ce processus, s'il est alimenté par de bons talents et des moyens.

Les optimistes comprennent aussi les nombreuses startups qui se lancent dans le calcul quantique au niveau matériel et présentent toutes des solutions qui devraient fonctionner à grande échelle d'ici même pas cinq ans. On en trouve dans tous les types de qubits : supraconducteurs (IQM), silicium (Quantum Motion), atomes froids (Pasqal, Atom Computing), ions piégés (IonQ, Universal Quantum) et photons (PsiQuantum qui prévoit un million de qubits dans moins de cinq à dix ans, Orca Computing, Quandela).

---

[340] Dans Predictions we didn't make, en janvier 2018.

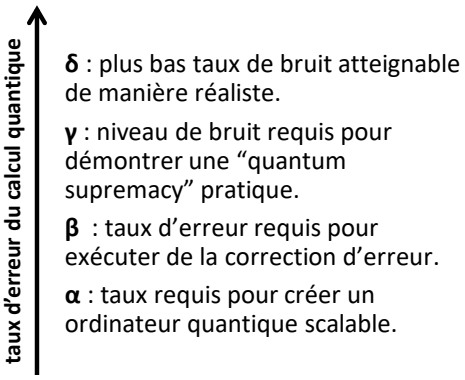
[341] Voir The Era of quantum computing is here. Outlook: cloudy de Philipp Ball paru en avril 2018 dans Science.

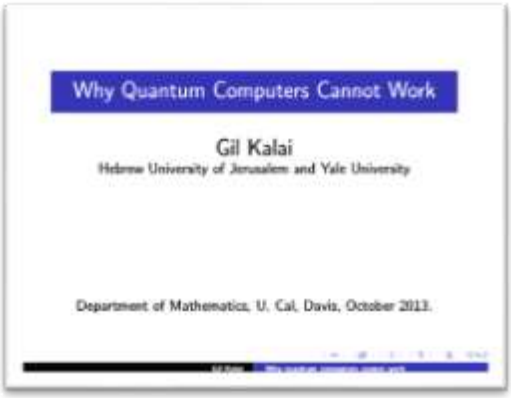
Pessimistes

Le pessimisme est aussi de rigueur pour les perspectives du calcul quantique. Il provient de quelques chercheurs, qui ne sont pas forcément spécialisés dans le domaine où ils s'expriment. Ils sont surtout pessimistes sur la capacité à traiter convenablement la question du bruit qui affecte les qubits, de manière indifférenciée par rapport à leur type.

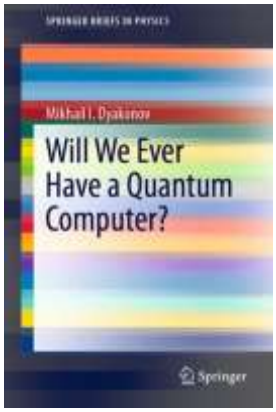
Le premier et plus connu de ces pessimistes est le chercheur israélien **Gil Kalai** qui pense que l'on n'arrivera jamais à créer des ordinateurs quantiques avec un faible taux d'erreurs[342]. Selon lui, on ne peut pas créer d'ordinateurs quantiques stables à cause du bruit qui affecte les qubits.

C'est illustré dans l'échelle *ci-dessous* qui positionne le plus bas niveau de bruit raisonnablement atteignable bien au-dessus du niveau requis pour faire fonctionner un calculateur quantique scalable. Il travaille sur la création de modèles mathématiques visant à prouver l'impossibilité d'outrepasser ces erreurs, même avec les codes de correction d'erreurs quantiques. Vouloir absolument prouver qu'une prouesse technologie est impossible est une curieuse approche pour un scientifique qui pourrait plutôt chercher des solutions !





Un autre détracteur du calcul quantique est le chercheur russe **Mikhail Dyakonov** (né en 1940 en URSS) qui officie dans le Laboratoire Charles Coulomb (L2C) du CNRS et de l'Université de Montpellier. Il a exprimé son point de vue dans un article largement relayé dans le monde fin 2018 devenu ensuite un livre[343]. Son argumentaire est plus intuitif mais moins bien documenté que celui de Gil Kalai[344].



Nous avons aussi **Serge Haroche** pour qui l'ordinateur quantique universel est une chimère, toujours à cause de ce satané bruit. Il pense par contre que la voie de la simulation quantique, notamment à base d'atomes froids, est raisonnable et réaliste. Malgré tout, Serge Haroche n'est pas à proprement parler un spécialiste des architectures d'ordinateurs quantiques.

---

[342] Il documente son point de vue dans la présentation Why Quantum Computers Cannot Work qui date de 2013 (60 slides) qui reprend les points de How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation de 2011 (16 pages) ainsi que The Argument Against Quantum Computers de Katia Moskwitch publié en février 2017. Gil Kalai déclare sans ambages : "*My expectation is that the ultimate triumph of quantum information theory will be in explaining why quantum computers cannot be built*".

[343] Voir The Case Against Quantum Computing, 2018. Il en a même fait un ouvrage, Will We Ever Have a Quantum Computer?, 2020. Ainsi qu'un débat sur le sujet lancé par Scott Aaronson dans Happy New Year! My response to M. I. Dyakonov. Voir aussi Skepticism of Quantum Computing de Scott Aaronson qui décortique 11 objections sur l'ordinateur quantique. Voir aussi Noise stability, noise sensitivity and the quantum computer puzzle" par Gil Kalai, 2018 (1h04mn).

[344] Voir une réponse à cet argumentaire dans The Case Against 'The Case Against Quantum Computing' par Ben Crige, janvier 2019.

En France, le chercheur **Xavier Waintal** (CEA-IRIG à Grenoble) émet de sérieuses réserves sur la possibilité de créer des ordinateurs quantiques à grande échelle. Là, encore, la cause en est le bruit. Il appuie son raisonnement sur diverses bases physiques à plus bas niveau que celui de Gil Kalai : le fonctionnement des qubits est un problème quantique à n-corps très complexe et le fait que les codes de correction d'erreurs traitent généralement de seulement deux types d'erreurs (flip, phase) mais pas de toutes les sources d'erreurs.

Il recommande d'exploiter la théorie de champs moyens (mean-fields theory) qui permet de modéliser les interactions complexes entre les qubits et leur environnement[345].

Cristian Calude et **Alastair Abbot** évoquent le fait que l'avantage des principaux algorithmes quantiques utilisables en pratique générerait une accélération modeste quadratique (racine carrée du temps classique) qui pourrait être atteinte sur ordinateurs classiques avec des approches heuristiques[346].

Cette réserve est aussi manifeste chez **Ed Sperling** qui faisait le point du domaine en novembre 2017 en rappelant tous les obstacles à surmonter[347].

Gérer l'incertitude

Il est difficile de faire la part des choses entre l'incertitude scientifique et l'incertitude technologique. La première est généralement plus difficile à lever que la seconde.

Ce lot d'incertitudes pose des questions existentielles sur la manière de gérer un tel cycle d'innovation au long cours. Quand faut-il investir ? A quel moment les positions de marché sont-elles prises ? Est-ce que la recherche fondamentale est découplée de l'industrialisation ? Le calcul quantique est-il une simple affaire d'ingénierie ?

On remarquera que les pessimistes ne sont pas américains et la plupart des optimistes le sont. Il y a donc, vu de loin, un biais culturel. Ces variantes de cultures d'innovation et économiques ont un impact sur les approches industrielles. Les grands industriels du numérique tels que IBM, Google, Intel et Microsoft peuvent se permettre d'investir en R&D sur le quantique avec une vision très long terme. Ils ont la profitabilité, le cash et la capacité à attirer des compétences pour se le permettre.

Des startups plus ou moins bien financées au Canada et aux USA comme D-Wave, Rigetti ou IonQ peuvent aussi adopter une vision assez long terme, même si elle dépend toujours de leur capacité à commercialiser des prototypes d'ordinateurs quantiques et d'avoir des investisseurs à même de les accompagner sur de nombreuses années avant de voir la couleur de leur retour sur investissement. Les montants correspondants ne sont pas forcément délirants. Rigetti a levé à ce jour $190M, ce qui est une paille au regard de nombreuses licornes mondiales de l'Internet « sans deep techs ».

Les problèmes d'ingénierie à résoudre concernent les matériaux utilisés dans les qubits, la correction d'erreurs, la cryogénie à grande échelle pour pouvoir intégrer un grand nombre de qubits dans un ordinateur et bien évidemment les avancées algorithmiques et logicielles. L'approche requise est éminemment pluridisciplinaire avec des mathématiques, de la physique fondamentale, de la thermodynamique et de la chimie, et enfin, du code, y compris du machine learning qui est notamment employé pour le calibrage de qubits.

---

[345] Voir What determines the ultimate precision of a quantum computer? par Xavier Waintal, 2017 (6 pages) que nous avions déjà cité et What limits the simulation of quantum computers? par Yiqing Zhou, E. Miles Stoudenmire et Xavier Waintal, 2020 (14 pages). Xavier Waintal a notamment développé des algorithmes classiques de simulation de problèmes à N-corps. Ils sont utilisés par diverses équipes de chercheurs de la physique de matière condensée, notamment ceux qui travaillent sur la matière topologique et les fermions de Majorana. Ils fonctionnent sur laptops et sur supercalculateurs.

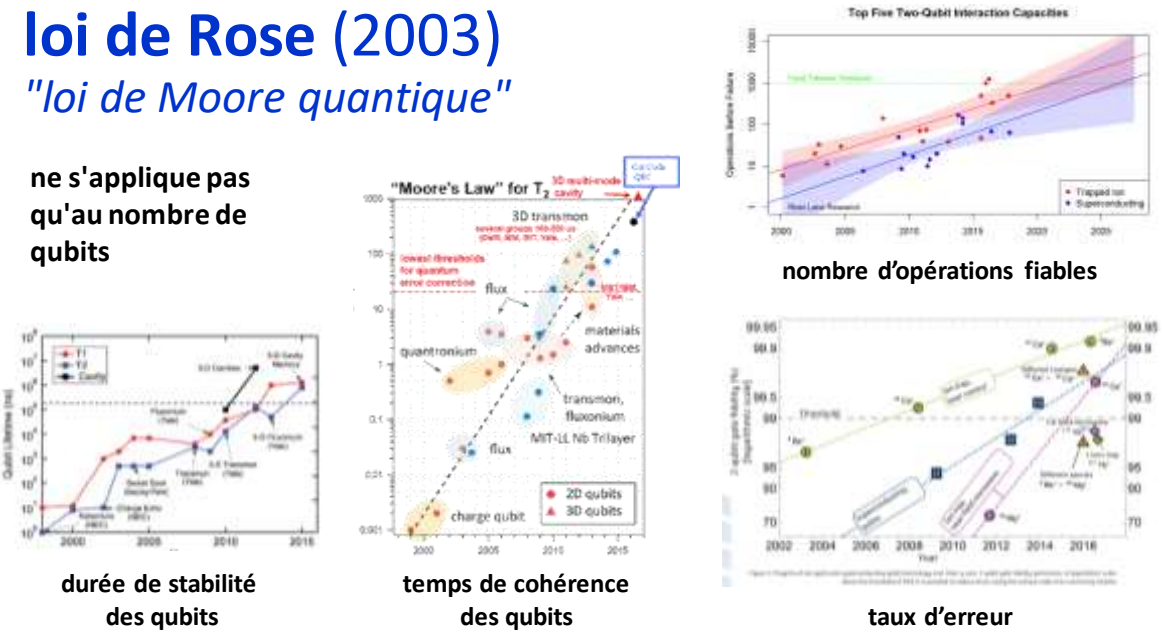
[346] Dans The development of a scientific field par Alastair Abbott et Cristian Calude, juin 2016.

[347] Dans Quantum Madness, de Ed Sterling, novembre 2017.

On peut aussi extrapoler les évolutions de ces dix dernières années dans l'informatique quantique. Cofondateur de D-Wave en 1999, Geordie Rose édicta en 2003 son propre équivalent de la loi empirique de Moore, la loi de Rose, prédisant un doublement tous les ans du nombre de qubits dans un ordinateur quantique. Jusqu'à présent et depuis 2007, D-Wave a tenu cette promesse.

Mais cette loi exponentielle est aussi observée dans l'évolution d'autres paramètres de fonctionnement des ordinateurs quantiques comme la durée de stabilité des qubits, leur taux d'erreur et le nombre d'opérations consécutives réalisées de manière fiable[348]. Modulo le fait que les schémas ci-dessous mériteraient d'être réactualisés.

J'ai cherché à comprendre pourquoi les prévisions de création d'ordinateurs quantiques viables étaient toujours à assez long terme, entre 5 et 50 ans. L'une des réponses vient de la durée des cycles dans la recherche associée.



Par exemple, pour obtenir un prototype de chipset de qubits silicium, il faut compter entre un et six mois de fabrication avec jusqu'à 160 étapes de fabrication. Le temps est allongé lorsque le processus de fabrication est nouveau et qu'il faut régler les machines. Après cette fabrication, il faut passer par l'étape de caractérisation et de packaging des composants. La caractérisation vise à tester qualitativement et à sélectionner les composants fabriqués. Cela peut durer jusqu'à un mois et dans le meilleur des cas descendre à une semaine.

Ensuite, pour mener les tests, la thermalisation de l'ordinateur dure environ 24 heures et le changement de chipset à tester dure au minimum entre 3 et 7 heures comme nous l'avons découvert dans la partie sur la cryogénie. Finalement, les cycles de *test & learn* sont souvent très longs, bien plus longs que dans le logiciel !

[348] Une partie des schémas ci-dessous proviennent de Technical Roadmap for Fault-Tolerant Quantum Computing, un rapport UK publié en octobre 2016 et de cette autre source

Algorithmes quantiques

Après avoir désossé un ordinateur quantique avec ses qubits, ses registres, ses portes et son frigo, voyons-donc comment on peut l'exploiter.

L'ordinateur quantique utilise des algorithmes dits quantiques qui ont la particularité d'être bien théoriquement plus efficaces que leurs équivalents conçus pour des ordinateurs traditionnels. Ces algorithmes ne sont pour l'instant pas très nombreux et leur performance relative vis-à-vis d'algorithmes traditionnels pas toujours évidente à prouver. Elle est même parfois contestée. L'assertion « *l'ordinateur quantique est plus rapide que les ordinateurs traditionnels* » est donc discutable et discutée et s'analyse au cas par cas.

Richard Feynman avait décrit l'idée de créer des simulateurs quantiques en 1982[349]. Son idée consistait à créer des dispositifs exploitant les effets de la mécanique quantique pour les simuler tandis que cette simulation serait quasiment impossible avec des ordinateurs traditionnels. Cela correspond aujourd'hui à l'un des usages des ordinateurs quantiques, comprenant notamment la simulation des interactions atomiques dans des structures inertes ou biologiques. On doit même faire la distinction entre simulateurs quantiques analogiques et ordinateurs quantiques numériques, à base de qubits et de portes quantiques, un sujet que nous aborderons dans la partie concernant les différents types d'ordinateurs quantiques du marché.

Des mathématiciens planchent depuis le milieu et la fin des années 1980 sur la création d'algorithmes adaptés aux simulateurs et ordinateurs quantiques, bien avant que l'on ait vu l'ombre de la couleur de ces derniers.

Ainsi, les premiers algorithmes quantiques ont été publiés au début des années 1990 alors que les premiers systèmes quantiques à deux qubits ont apparus aux alentours de 2000/2002. Les chercheurs créent régulièrement de nouveaux algorithmes depuis 25 ans, indépendamment des lents progrès du côté des ordinateurs. Le Quantum Algorithm Zoo en identifie une soixantaine de classes dans la littérature scientifique et 420 algorithmes (en juillet 2020). C'est un nombre encore modeste au regard des algorithmes non quantiques qui se comptent en milliers.

La création d'algorithmes quantiques est donc un objet de recherche parallèle avec la partie matérielle des ordinateurs quantiques. Ce n'est pas la première fois dans l'Histoire qu'il en est ainsi. L'emblématique **Ada Lovelace** planchait sur la création des premiers algorithmes et lignes de code devant tourner sur la machine de **Charles Babbage**, qui ne vit le jour qu'en 2002 à Londres, 153 ans après sa conception (vidéo) (voir l'exemple de programme *ci-dessous*). Elle avait annoté en 1842/1843 une traduction de son cru d'un papier de l'Italien **Luigi Federico Menabrea** qui décrivait la machine de Babbage. Il fallut attendre 102 ans pour que les premiers ordinateurs voient le jour à la fin de la seconde guerre mondiale ! Un beau jeu de patience !

Cela rappelle aussi les schémas d'hélicoptères de **Léonard de Vinci** qui datent de 1487-1490. Un premier hélicoptère propulsé par l'énergie humaine et créé par l'Université de Toronto a volé en 2013, AeroVelo (vidéo) suivi d'un autre spécimen assez voisin issu de l'Université de Maryland qui volait en 2018 (vidéo) ! Donc, avec plus de cinq siècles de décalage ! Et même en tenant compte le vol du premier hélicoptère motorisé en 1907, le décalage reste supérieur à quatre siècles. Cette même Université de Maryland est d'ailleurs l'une des plus en pointe dans le monde dans les ordinateurs quantiques à base d'ions piégés ! Comme quoi !

Après-guerre, l'Histoire se répéta en partie pour nombre de travaux du vaste champ de l'intelligence artificielle, où les chercheurs planchaient également sur des algorithmes, notamment à base de réseaux de neurones, avant que les ordinateurs puissent les exécuter convenablement.

---

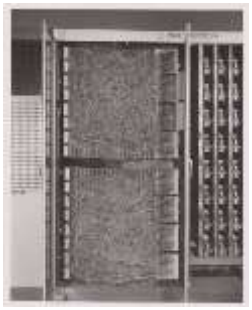
[349] Dans Simulating Physics with Computers, Richard Feynman, 1982 (22 pages).

Les premiers ordinateurs gérant en 1957 des perceptrons, les ancêtres des réseaux de neurones artificiels d'aujourd'hui, étaient rudimentaires. L'essor du deep learning depuis 2012 est en partie lié à la puissance des machines et des GPU à même d'entraîner de tels réseaux de neurones. Le matériel a une fois encore rejoint les algorithmes qui étaient en avance sur leur temps.

Ada Lovelace
1842, premier programme pour la machine de Babbage qui ne vit jamais je jour

ENIAC
1945, premier ordinateur

McCulloch & Pitts
1943, concept des neurones artificiels



Mark I Perceptron computer
1957, premier processeur synaptique

Alexnet sur Nvidia GTX 580
2012, premier réseau de neurones avec un taux de reconnaissance d'image avec moins de 30% d'erreurs !

Léonard de Vinci
1487, vis aérienne

Paul Cornu, 1907
premier vol d'hélicoptère motorisé
1,5 m d'altitude

AeroVelo, 2013
premier vol d'hélicoptère à force humaine

Aujourd'hui encore, une bonne part des algorithmes quantiques qui sont inventés ne sont pas encore exécutables à grande échelle sur les ordinateurs quantiques disponibles ni même sur des émulateurs quantiques à base d'ordinateurs traditionnels. Les qubits sont disponibles dans un nombre bien trop faible pour qu'ils servent à quelque chose et surtout, qu'ils soient plus performants que des ordinateurs traditionnels. Les supercalculateurs émulent difficilement plus de 50 qubits et aucun ordinateur quantique opérationnel ne dépasse ce nombre de qubits.

Dans une autre analogie avec le passé de l'Histoire de l'Informatique, nous en sommes encore dans le quantique à aborder la programmation via des « couches basses » de langage machine.

Un peu comme pour les programmeurs en langage machine ou en assembleur d'il y-a 30 à 50 ans, ou plus récemment, pour ceux qui ont programmé à bas niveau des systèmes embarqués ou des pilotes de périphériques dans la micro-informatique. Les algorithmes quantiques actuels sont les couches les plus basses des solutions logicielles qui restent à inventer puis à assembler.

La création d'algorithmes quantiques requiert une capacité d'abstraction sans commune mesure avec celle des algorithmes et programmes traditionnels. Une nouvelle génération de mathématiciens et développeurs capables de raisonner avec le formalisme mathématique de la programmation quantique devra se développer au gré de la maturation des ordinateurs quantiques. Ils devront être capables de conceptualiser des algorithmes qui ne sont pas faciles à se représenter physiquement. Qui plus est, ces algorithmes devront aussi, c'est la moindre des choses, être bien plus efficaces que leurs équivalents pour ordinateurs traditionnels ou supercalculateurs.

Les principaux algorithmes quantiques exploitent les portes quantiques que nous avons vues dans la partie précédente. Il est cependant possible qu'un jour, le niveau d'abstraction de création de logiciels quantique s'élève au point qu'il ne soit plus nécessaire de comprendre le fonctionnement à bas niveau des portes quantiques. C'est une conjecture, rien de plus !

Qui plus est, l'algorithmie quantique est aussi variée que les types d'ordinateurs quantiques qu'il est ou sera possible de créer.

En plus des algorithmes à base de portes quantiques[350], il faut en effet ajouter :

- Les algorithmes pour **ordinateurs à recuit quantique** comme ceux de D-Wave qui sont basés sur l'initialisation de relations entre qubits de qualité moyenne dans des matrices et sur la recherche d'un minimum énergétique s'appuyant notamment sur l'effet tunnel. Ils permettent l'exécution d'un grand nombre d'algorithmes quantiques.
- Les **simulateurs quantiques analogiques** qui servent à simuler des phénomènes quantiques permettant de prédire par exemple l'organisation des atomes dans des molécules. On y trouve notamment les simulateurs quantiques à atomes froids.
- Les **ordinateurs quantiques à variables continues** qui utilisent des objets quantiques dont on peut mesurer une grandeur physique continue et non pas binaire. Ils sont principalement à base de photons[351].
- Les **ordinateurs quantiques topologiques**, qui n'existent pas encore. C'est la voie de recherche de Microsoft et de quelques laboratoires de recherche, notamment en Chine. Nous en reparlerons page 358.
- Les **algorithmes hybrides** associant algorithmes traditionnels et algorithmes quantiques ou bien des algorithmes à portes quantiques classiques et à base de MBQC[352]. C'est notamment le cas du Variational Quantum Eigensolver (VQE) qui permet la résolution de problèmes de simulation chimique aussi bien que d'entraînement de réseaux de neurones.
- Les **algorithmes quantum inspired** qui sont des algorithmes destinés à des ordinateurs classiques s'inspirant d'algorithmes quantiques pour la résolution de problèmes complexes. Leur création a démarré bien avant que les premiers ordinateurs quantiques expérimentaux voient le jour.

En pratique, les ordinateurs quantiques bruités intermédiaires qui émergent en ce moment et domineront le paysage pendant au moins une bonne décennie ne peuvent pas exécuter des algorithmes « profonds ». A savoir qu'à cause du taux d'erreur des portes quantiques, on est limité en séries de portes quantiques qui peuvent être enchaînées. On doit donc se limiter aux algorithmes qui sont adaptés à l'usage d'un faible nombre de portes quantiques.

C'est le cas pour la **VQE** (Variational Quantum Eigensolver), les **QAOA** (Quantum Approximate Optimization Algorithm), le Variational Quantum Factoring et certains algorithmes de Quantum Machine Learning (Support Vector Machine, Principal Component Analysis et Quantum Variational Autoencoder). Nous aurons l'occasion d'en étudier quelques-uns par la suite.

Suprématie et avantage quantiques

Avant de rentrer dans le détail des algorithmes quantiques, il nous faut expliquer la signification de la notion de "suprématie quantique" qui a été abondamment utilisée dans la communication de certains acteurs tels que Google et depuis au moins 2017.

---

[350] Aussi appelés UQCM pour Universal Quantum Cloning Machine.

[351] Voir par exemple Perspective: Toward large-scale fault-tolerant universal photonic quantum computing de S. Takeda et al, April 2019 (13 pages) ainsi que Continuous-variable quantum neural networks par Nathan Killoran et al, juin 2018 (21 pages) qui porte sur l'usage de qubits à variables continues pour créer des réseaux de neurones.

[352] Voir Hybrid Quantum Computation de Arun, 2011 (155 pages). C'est aussi la source du schéma des portes réalisées en MBQC.

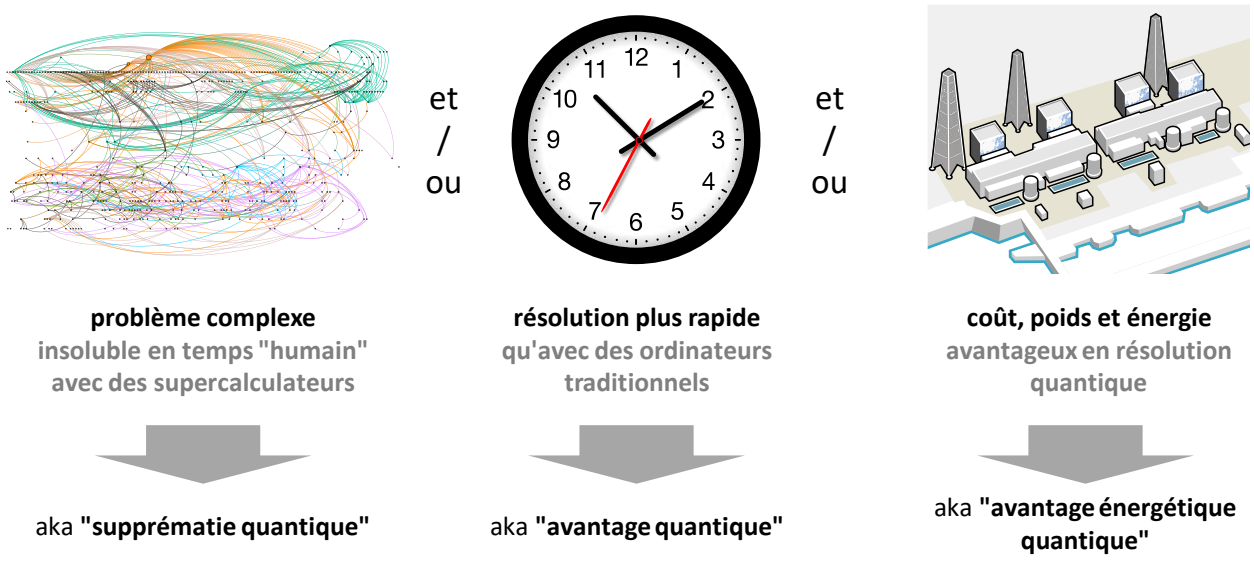
L'appellation a été créée par l'Américain John Preskill dans une communication au Congrès Solvay en 2011[353].

Une "suprématie quantique" est atteinte lorsqu'un algorithme traitant un problème donné n'est exécutable que sur un ordinateur quantique, ce problème ne pouvant pas être résolu sur le plus puissant des supercalculateurs[354].

Un « avantage quantique » correspond au cas où un ordinateur quantique exécute un algorithme bien plus rapidement que sur les supercalculateurs les plus puissants.

De nombreux spécialistes affirment que le seuil de 50 qubits de qualité - avec un faible taux d'erreurs et un long temps de décohérence - constituera une étape clé de l'atteinte d'une suprématie quantique. « Une » parce qu'elle est définie au cas par cas.

Cette appellation ne signifiera pas qu'un ordinateur quantique donné est suprêmement plus puissant que tous les supercalculateurs du moment. L'appellation devra être utilisée pour des couples d'algorithmes quantiques et d'ordinateurs quantiques, et avec des tests réalisés sérieusement avec le meilleur possible des algorithmes adapté aux meilleurs supercalculateurs sachant que ceux-ci sont aussi mouvants.



Robert König (Université Technique de Munich), David Gosset (Université de Waterloo au Canada) et Sergey Bravyi (IBM) démontraient ainsi en octobre 2018 que les ordinateurs quantiques peuvent réellement réaliser des opérations inaccessibles aux ordinateurs classiques, mais en s'appuyant seulement sur le cas d'un algorithme particulier[355].

Certains benchmarks de D-Wave et Google réalisés en 2015 et montrant la supériorité de la solution quantique (dite adiabatique ou à recuit quantique) ont été ensuite contredits par la création d'algorithmes optimisés pour des supercalculateurs sous certaines conditions. Cette suprématie quantique naviguera donc dans un premier temps dans des sables mouvants.

Elle interviendra certainement d'ici quelques années pour quelques algorithmes qui ne peuvent avoir d'équivalents optimisés pour les supercalculateurs. On apprenait le 20 septembre 2019 que Google avait atteint cette suprématie, avec un algorithme de *random numbers sampling* et sur 53 qubits. L'algorithme ne sert pas à grand-chose et exploite la superposition sur l'ensemble des 53

[353] Elle est décrite dans Quantum Computing and the Entanglement Frontier, 2011.

[354] Voir Quantum supremacy: Some fundamental concepts par Man-Hong Yung, janvier 2019 (2 pages) selon lequel il y aurait trois manières de démontrer la suprématie quantique : l'échantillonnage du boson, l'IQP et les circuits quantiques chaotiques.

[355] Voir First proof of quantum computer advantage, octobre 2018 et Quantum advantage with shallow circuits, avril 2017 (23 pages).

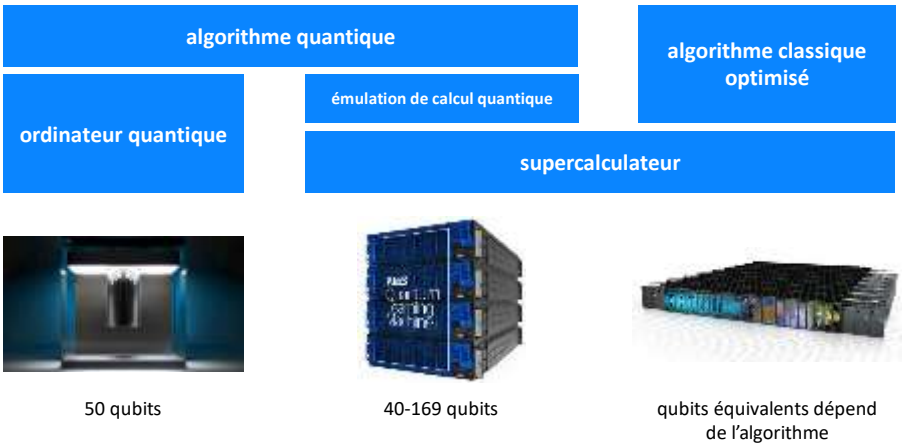
qubits supraconducteurs utilisés. Nous en parlerons en détail dans la rubrique dédiée à Google dans les ordinateurs supraconducteurs.

Ariel Bleicher rappelle à juste titre que les supercalculateurs et ceux qui les exploitent n'ont pas dit leur dernier mot et cherchent aussi à améliorer leurs propres algorithmes[356]. A long terme, le quantique supplantera certainement les supercalculateurs pour un grand nombre d'algorithmes.

La comparaison entre ordinateurs quantiques et supercalculateurs peut se faire de deux principales manières. La première consiste à exécuter sur ces derniers un algorithme classique équivalant fonctionnellement à l'algorithme quantique évalué (à droite dans le schéma *ci-dessous*). La seconde exploite des émulateurs quantiques à architecture non quantique, le plus souvent, des supercalculateurs qui émulent l'exécution d'un algorithme quantique (au centre dans le schéma *ci-dessous*).

La dynamique de progrès de ces deux comparables face au quantique est différente.

Dans le premier cas, c'est la combinaison de l'ingéniosité humaine à créer de nouveaux algorithmes classiques et à l'évolution de la performance des supercalculateurs.



Dans le second cas, il s'agit de l'amélioration de cette performance matérielle mais aussi de méta-algorithmes d'exécution d'algorithmes quantiques sur des machines traditionnelles, et généralement réparties sur plusieurs processeurs et serveurs.

Les principales limitations des supercalculateurs pour simuler des algorithmes quantiques relèvent plus de leur mémoire vive que de leur capacité de traitement. Il faudrait 16 Po de mémoire pour simuler complètement 50 qubits en double-flottant. Si on passe à 96 qubits, la mémoire nécessaire pour simuler l'ensemble sur supercalculateur est multipliée par 2^{46*2}. La loi de Moore de la mémoire ne peut donc pas suivre le rythme d'une augmentation linéaire du nombre de qubits alignés dans un ordinateur quantique.

Malgré tout, le nombre de qubits simulables sur des supercalculateurs est aussi en augmentation constante, avec de nombreux diables dans les détails. Les Chinois sont les plus actifs dans cette course à la simulation, notamment chez Alibaba et Huawei avec plusieurs records établis en 2018.

Il existerait trois principales méthodes de simulation d'un circuit de N qubits et d'un certain niveau de profondeur d'enchaînements de portes quantiques[357] :

- La première méthode consiste à gérer en mémoire le vecteur d'état complet du registre quantique en mémoire. Avec N qubits, c'est le produit tensoriel des vecteurs d'état de chaque qubits qui comprennent deux nombres complexes alpha et beta. Cela donne un vecteur de 2^N nombres complexes, soient 2^{N+1} nombres flottants. L'action de portes quantique sur ce grand vecteur con-

[356] Voir Quantum Algorithms Struggle Against Old Foe: Clever Computers d'Ariel Bleicher, février 2018. Cela fait écho aux découvertes d'algorithmes pour ordinateurs classiques aussi performants que ceux qui sont conçus pour ordinateurs quantiques, comme celui d'Ewin Tang dans la recommandation, déjà évoqué page 61.

[357] Voir Classical Simulation of Intermediate-Size Quantum Circuits, Alibaba, 2018 (12 pages). Voir aussi What limits the simulation of quantum computers? par Yiqing Zhou. Miles Stoudenmire et Xavier Waintal, mars 2020 (14 pages) qui fournit un cadre théorique et pratique de l'optimisation de l'émulation de code quantique. A noter des travaux portant sur l'émulation de modules de qubits supraconducteurs avec… des qubits supraconducteurs. Voir Quantum computer-aided design: digital quantum simulation of quantum processors par Thi Ha Kyaw et al, 2020 (23 pages).

siste à lui appliquer les matrices de transformation de portes quantiques à une, deux ou trois qubits qui font respectivement 2x2, 4x4 ou 8x8 nombres complexes. Cette méthode est mise en œuvre sur des supercalculateurs dotés d'énormes capacités de mémoire, de l'ordre de plusieurs Po. La méthode est pour l'instant limitée à une cinquantaine de qubits. On peut l'optimiser dans la mesure où ces vecteurs sont généralement remplis d'un grand nombre de zéros. A noter qu'après application de portes quantiques impliquant de l'intrication, le vecteur d'état ne sera plus factorisable en état de qubits individuels.

- La seconde méthode consiste à mesurer les amplitudes des 2^N combinaisons de 0 et de 1 de chaque qubit. Cela donne donc 2^N nombres flottants à évaluer pour chaque rang de portes quantiques, soient, si je comprends bien, deux fois moins d'informations qu'avec la première méthode. La méthode est plus facile à distribuer sur plusieurs serveurs[358]. Alibaba utilisait ainsi un cluster de 10 000 serveurs à 96 CPUs. En septembre 2019, ils simulaient 70 qubits sur une profondeur de 34 portes quantiques avec 1449 instances de leur Cloud Elastic Computing Service (ECS) comprenant chacune 88 chipsets Intel Xeon avec 160 Go de mémoire. Donc, un total de 127 512 processeurs[359] !
- La troisième consiste à gérer la matrice de transformation des qubits contenant 2^{2N+2} nombres flottants. Pourquoi ? Parce qu'elle a comme côté le vecteur d'état du registre de qubits de 2^{N+1} nombres flottants. C'est la méthode la plus consommatrice de mémoire qui est peu utilisée pour les nombres élevés de qubits.

Il y a tout d'abord le cas d'**Origin Quantum**, une startup chinoise multirôles (matériel, logiciel) en partenariat avec l'équipe de Guang-Can Guo de l'**Université des Sciences et Technologies de Chine** qui ont simulé 64 qubits avec un algorithme de 22 couches (layers, depth, nombre de séquences de portes quantiques enchaînées) sur un cluster de 128 nœuds[360]. Ils utilisent une méthode permettant de transformer des combinaisons de portes CZ (portes de Pauli Z conditionnelles) et de portes à un qubit en sous-circuits plus simples qui n'ont pas besoin d'être intriqués. Ils pensaient aussi pouvoir simuler 72 qubits sur une profondeur de 23 couches de portes quantiques sur un supercalculateur tournant pendant 16 heures.

Ces travaux montrent que deux paramètres clés conditionnent les capacités de simulation : non seulement le nombre de qubits mais également le nombre de séquences de portes quantiques à enchaîner. Plus on augmente le nombre de qubits, moins on peut simuler de séquences de portes quantiques. Mais cela reste utile pour quelques algorithmes quantiques tels que les QFT (transformées de Fourier quantiques).

Second record, celui d'**Alibaba** sur 81 qubits et quarante séquences de portes quantiques[361]. Leur simulation Taizhang exploite une méthode créée par Igor Markov et Shi Yaoyun en 2005[362] qui permet de ventiler un algorithme quantique de manière distribuée sur une ferme de milliers de serveurs. L'Alibaba Quantum Laboratory est géré par ce même Shi Yaoyun, professeur à l'Université du Michigan. Leurs simulations portaient notamment sur des architectures de 100 qubits sur 35 couches (10x10x35), 121 qubits sur 31 couches (11x11x31) et 144 qubits sur 27 couches (12x12x27). Les architectures retenues sont celles de matrices de qubits, d'où les nombres carrés de qubits.

---

[358] Les méthodes de partitionnement de la simulation quantique sont bien décrites dans Distributed Memory Techniques for Classical Simulation of Quantum Circuits, Ryan LaRose de l'Université du Michgan, juin 2018 (11 pages).

[359] Voir Alibaba Cloud Quantum Development Platform: Large-Scale Classical Simulation of Quantum Circuits, septembre 2019 (5 pages).

[360] Voir Researchers successfully simulate a 64-qubit circuit, Science China Press, juin 2018.

[361] Voir Alibaba Says Its New "Tai Zhang" Is the World's Most Powerful Quantum Circuit Simulator, mai 2018 et Alibaba announced that it has developed the world's strongest quantum circuit simulator "Taizhang", mai 2018.

[362] Voir Simulating quantum computation by contracting tensor networks, Igor Markov et Shi Yaoyun, 2005 (21 pages).

Reference	General Technique	Qubits	Depth	# of Amplitudes
Intel [6]	Full amplitude-vector update	42	High	All
ETH [5]	Optimized full amplitude-vector update	5×9	25	All
IBM [7]	Tensor-slicing with minimized communication	7×7 7×8	27 23	All 2^{37} out of 2^{56}
Google [8]	Preprocessing using undirected graphical model	7×8	30	1
USTC [9]	Qubit partition with partial vector update	8×9	22	1
Sunway [10]	Dynamic programming qubit partition	7×7 7×7	39 55	All 1
Alibaba	Undirected graphical model with parallelization	9×9	40	1

TABLE I: A very broad overview of existing simulators. The final column reports the number of amplitudes that are computed by that simulator.

Troisième record en 2018, celui de **Huawei** et de son service « HiQ Cloud » capable de simuler de 42 à 169 qubits[363]. La méthode est voisine de celle d'Alibaba. Les 42 qubits sont simulés en « pleine amplitude ». 81 qubits étaient simulés avec « une seule amplitude » et 169 qubits sur une seule amplitude et avec un petit nombre de portes quantiques.

D'autres records ont été battus aux USA comme celui de **Google** avec la NASA, l'Université d'Illinois et le laboratoire d'Oak Ridge avec 49 à 121 qubits sur le supercalculateur Summit de ce dernier, comprenant 9216 CPUs PowerPC et 26 648 Nvidia V100[364].

Ce même laboratoire d'Oak Ridge est à l'origine de **XAAC** (eXtreme-scale ACCelerator programming framework) un framework pour Eclipse qui permet de gérer des calculs hybrides associant ordinateurs quantiques et supercalculateurs comme le Titan équipé de GPU Nvidia installé à Oak Ridge[365]. Il est capable de transformer du code quantique pour ordinateurs à portes quantiques ou à modèles adiabatiques en code exécutable sur toute architecture quantique.

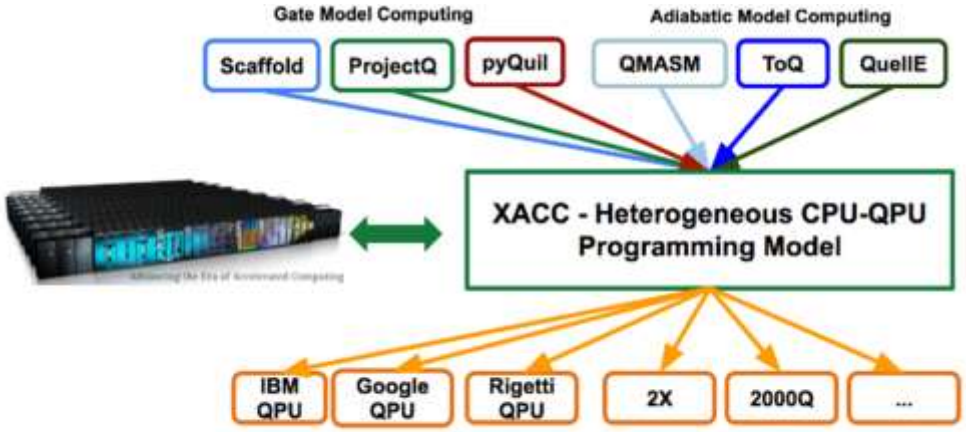


Figure 1: The XACC CPU-QPU programming model enables quantum acceleration in classical HPC applications in a quantum language and hardware agnostic manner.

En 2018, des chercheurs d'IBM démontraient en tout cas que la suprématie quantique était assurée à terme, même avec des ordinateurs quantiques pouvant enchaîner un nombre fini et contraint de portes quantiques[366].

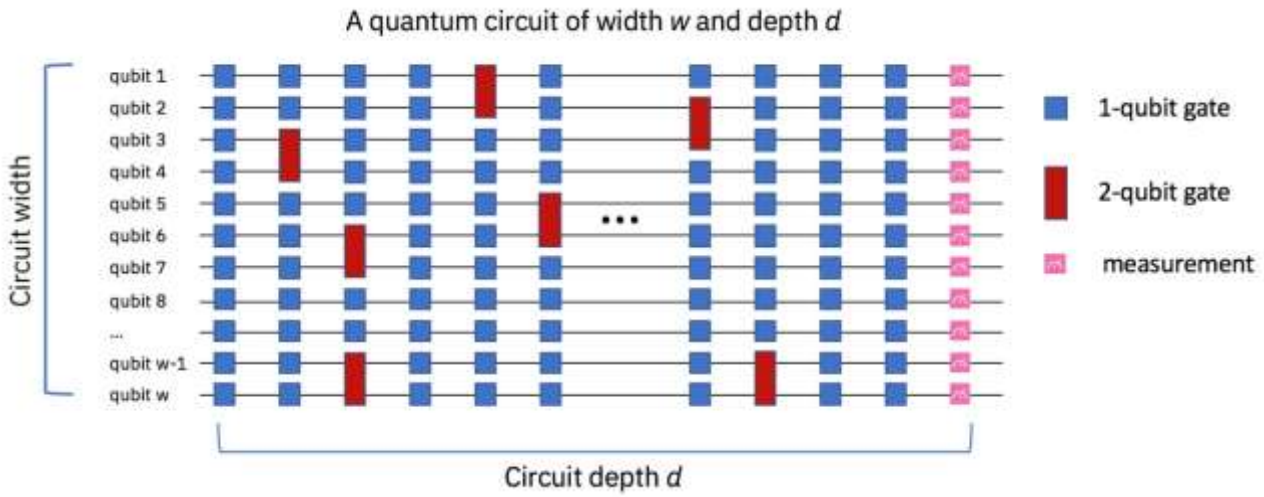
---

[363] Voir Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform, octobre 2018.

[364] Voir Establishing the Quantum Supremacy Frontier with a 281 Pflop/s Simulation, mai 2019 (11 pages). Ce Summit a dû consommer une bonne part de la production de Nvidia V100 ! Voici également la liste des records de qubits et de simulation de qubits dans https://quantumcomputingreport.com/scorecards/qubit-count/.

[365] Le schéma vient de Eclipse Science and Open Source Software for Quantum Computing, 2017. Voir l'article qui décrit XAAC : A Language and Hardware Independent Approach to Quantum-Classical Computing, juillet 2018 (15 pages).

[366] Voir Scientists Prove a Quantum Computing Advantage over Classical, par Bob Sutor, octobre 2018, Quantum advantage with shallow circuits, Sergey Bravyi, David Gosset, Robert Koenig, 2017 (23 pages) et la video Quantum advantage with shallow circuits, IBM Research, décembre 2017 (44 minutes).



Il faudra en tout cas se méfier des annonces des IBM et autres Google lorsqu'ils prétendront avoir atteint cette suprématie quantique, ou, tout du moins, de la manière dont ces annonces seront décrites dans les médias. Et la découverte inopinée de l'atteinte de la suprématie quantique par Google en septembre 2019 avec 53 qubits et un algorithme optimisé pour ne doit pas échapper à notre vigilance[367] !

Il faut donc attendre d'avoir des éléments d'informations complets pour juger, comme l'indiquent fort bien Cristian et Elena Calude de l'Université d'Auckland en Nouvelle Zélande[368]. Ils arguent aussi du fait que l'on compare une limite haute de performance, celle d'un ordinateur quantique précis, à une limite basse qui est la meilleure performance dans la résolution du même problème dans un supercalculateur. Or, il est plus facile de démontrer qu'un truc existe que son inexistence.

Une suprématie quantique est donc un comparable entre l'existence d'une performance quantique et la supposition de la non-existence d'une performance équivalente dans le non-quantique. Les auteurs rappellent aussi un critère qui manque parfois à l'analyse : il vaudrait mieux que l'algorithme testé serve à quelque chose ! Ce qui n'est pas toujours évident avec certains algorithmes quantiques, comme nous le verrons plus loin.

Usages des applications quantiques

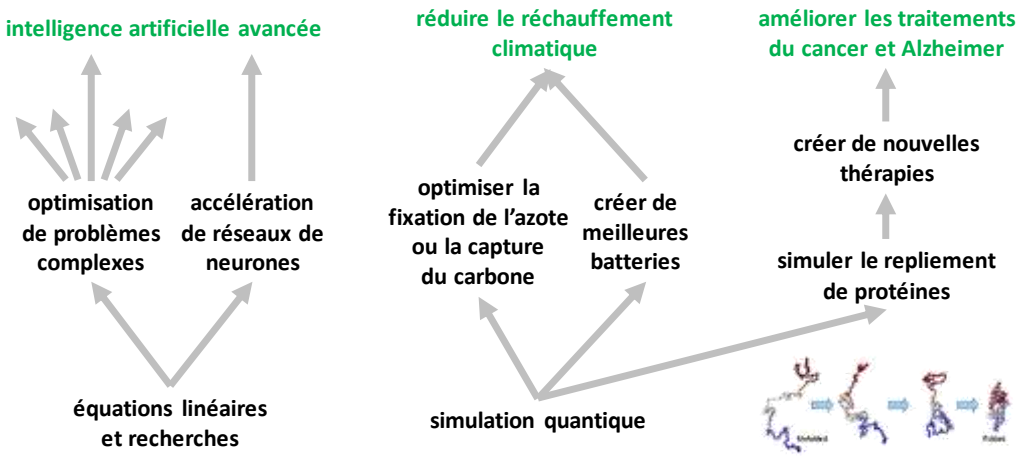
Avant de rentrer dans le lard des algorithmes quantiques, faisons un détour de leur utilité pratique connue à ce jour.

Ils sont organisés *ci-dessous* en trois niveaux verticaux : les fonctions de base, les algorithmes puis les applications concrètes.

Tout ceci relève encore largement de la prospective car nombre de ces solutions demanderont des puissances en termes de nombre et de qualité de qubits qui ne seront pas disponibles avant plusieurs années voire décennies.

[367] Voir Interpréter la suprématie quantique de Google par Olivier Ezratty, septembre 2019.

[368] Dans The road to quantum computing suppremacy, publié fin 2017.



Dans un ordre vaguement chronologique, nous aurons tout d'abord des applications d'algorithmes de recherche et d'optimisation basés sur les équations linéaires en général sachant que tous les algorithmes quantiques reposent sur des équations linéaires. On peut y caser les solutions de résolution de problèmes complexes, comme la détermination du parcours optimal d'un commercial, un sujet bien connu. Sa variante est la solution d'optimisation du trafic individuel de nombreux véhicules dans une ville en tenant compte de l'ensemble des trajets planifiés pour chacun d'entre eux. De tels algorithmes pourraient aussi améliorer la conception de circuits intégrés où l'on cherche généralement à minimiser les liaisons entre blocs fonctionnels, transistors et à minimiser la consommation d'énergie, des formes d'optimisation sous-contraintes adaptées aux traitements quantiques.

Cette catégorie de solutions comprend aussi l'accélération de l'entraînement des réseaux de neurones du deep learning. L'avantage par rapport aux techniques existantes s'appuyant sur des processeurs neuromorphiques n'est pas encore évidente et démontrée.

Qui plus est, la faisabilité de ces réseaux de neurones est établie sur architectures traditionnelles, à base de GPUs comme ceux de Nvidia ou de TPU (Tensor Processing Units) comme ceux de Google, sans compter les processeurs à base de memristors qui sont encore au stade du laboratoire.

En second lieu, dans le vaste champ de la simulation quantique, nous aurons d'abord des applications dans la chimie et la physique des matériaux pour simuler les interactions entre atomes dans les molécules et les structures cristallines, qui dépendent elles-mêmes des lois de la mécanique quantique. Cela servira si tout va bien à inventer de nouvelles solutions comme des batteries plus efficaces, chargeables plus rapidement et avec une plus grande densité énergétique, des procédés chimiques de captation du carbone ou de fixation de l'azote, ainsi que la création de matériaux supraconducteurs à température ambiante. Ce sont des hypothèses non encore validées à savoir que les algorithmes quantiques complétés d'ordinateurs quantiques bien dimensionnés avec des centaines de qubits logiques seront à même de permettre aux chercheurs d'avancer dans ces domaines-là.

En dernier lieu et avec des quantités de qubits bien plus importantes, donc à plus lointaine échéance, la simulation quantique pourra éventuellement passer à la simulation de molécules biologiques. Cela commencera avec celle de peptides, puis de polypeptides, et enfin, de protéines et d'enzymes. Les molécules biologiques ont la particularité d'être très complexes, avec des structures pouvant atteindre des dizaines de milliers d'atomes.

Le top du top serait la capacité à simuler l'assemblage puis le fonctionnement d'un ribosome, qui fait plus de 100 000 atomes. C'est la structure moléculaire la plus magique du vivant, celle qui assemble les acides aminés pour construire les protéines à partir du code de l'ARN messager issu de la transposition de l'ADN des gênes. Suivrait alors la simulation du fonctionnement d'une cellule entière.

Mais là, on est à la frontière de la science-fiction, même en étant très optimiste sur l'informatique quantique ! Ce d'autant plus qu'à ce niveau de complexité, le chaos règne !

Classes d'algorithmes quantiques

Comme nous l'avons vu dans la partie précédente qui décrit la structure d'un ordinateur quantique, un algorithme quantique va intégrer à la fois la partie initialisation des données puis celle des calculs et enfin de la mesure du résultat. Elle s'appliquera à un registre de n qubits qui sont physiquement initialisés à zéro, puis modifiés par des portes quantiques.

Le résultat correspond à la mesure de l'état de ces mêmes qubits à la fin de l'exécution de l'algorithme. En général, il faudra effectuer le calcul dans son intégralité et mesurer à chaque fois l'état des qubits en sortie, puis faire une moyenne des valeurs obtenues. La question étant de savoir : combien de fois doit-on répéter le calcul ? Cela dépend de sa nature et de la vitesse à laquelle il fait converger vers 0 et 1 l'état des qubits.

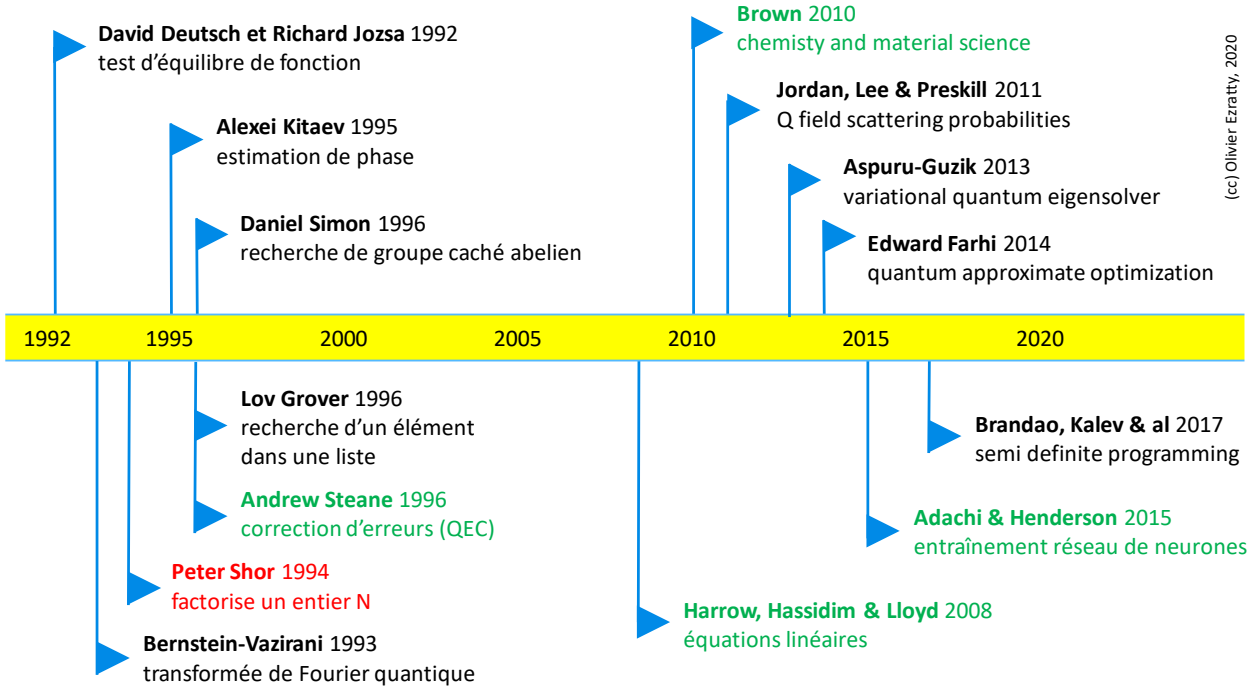
L'algorithme doit être compatible avec les caractéristiques de l'ordinateur quantique. Les principales sont le temps de cohérence et la durée d'exécution des portes quantiques.

Le nombre de portes quantiques à exécuter devra permettre d'exécuter l'algorithme dans un temps inférieur au temps de cohérence au bout duquel les qubits perdront leur état de superposition. Cette vérification est généralement réalisée par les compilateurs de code quantique.

Elle devra tenir compte des codes de correction d'erreurs qui sont souvent mis en œuvre sous la forme de sous algorithmes préfabriqués intégrés dans l'algorithme "métier" créé par le développeur.

Il en va de même des portes quantiques utilisées dans les outils de développement. Certaines portes quantiques, notamment s'appliquant sur deux ou trois qubits, sont utilisées par les développeurs mais seront converties par le compilateur en un jeu de portes quantiques universelles supportées par l'ordinateur quantique. Cela va aussi multiplier le nombre de portes quantiques par rapport à l'algorithme initial. Dans la pratique, l'ordinateur va donc exécuter un nombre de portes quantiques bien plus grand que celles de l'algorithme conçu par le développeur.

L'une des considérations importantes de la création d'algorithmes quantiques est de s'assurer qu'ils sont plus efficaces que leurs équivalents optimisés pour des ordinateurs ou supercalculateurs traditionnels. Des théories permettent de vérifier cela pour évaluer la montée en puissance exponentielle, polynomiale, logarithmique ou linéaire du temps de calcul en fonction de la taille du problème à réaliser, ou une combinaison des quatre. Mais rien ne remplace l'expérience !



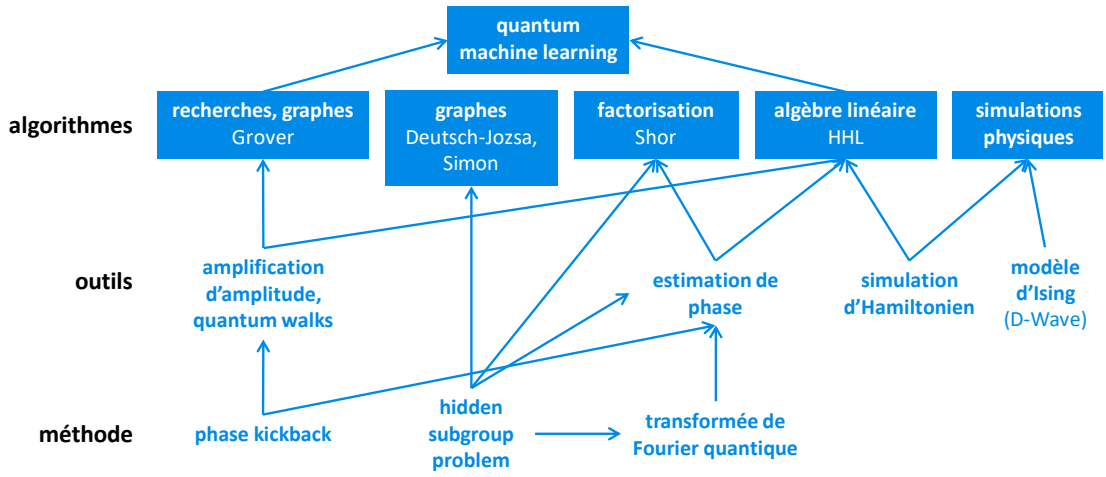
Les algorithmes quantiques sont des applications pratiques de l'algèbre linéaire, cette branche des mathématiques qui gère des espaces vectoriels et des transformations linéaires à base de matrices. Elles sont appliquées dans des espaces à deux dimensions, les vecteurs qui définissent les états de qubits. Leur manipulation s'appuie sur des calculs matriciels qui permettent de modifier l'état des qubits sans en lire le contenu. Leur lecture n'intervient qu'à la fin des calculs.

Cela rend difficile la programmation conditionnelle, du genre : faire tel calcul si tel résultat intermédiaire a telle valeur ou vérifie telle condition. Mais les portes quantiques conditionnelles (CNOT & co) permettent d'émuler ce genre de comportement dans un algorithme quantique.

A ce jour, quatre principales catégories d'algorithmes quantiques sont disponibles et que nous détaillerons plus loin :

- Les **algorithmes de recherches** basés sur ceux de Deutsch-Jozsa, Simon et de Grover.
- Les **algorithmes basés sur les transformées de Fourier quantiques** (QFT), comme celui de Shor qui sert à la factorisation de nombres entiers qui a déclenché un phénomène de pompiers-pyromanes, les pyromanes étant ceux qui veulent créer des ordinateurs quantiques capables de casser les clés de sécurité publiques de type RSA et les pompiers étant ceux qui cherchent à protéger les communications numérique avec des algorithmes résistant à la factorisation rapide de nombres entiers.
- Les **algorithmes qui cherchent un point d'équilibre d'un système complexe** comme dans l'entraînement de réseaux de neurones, la recherche de chemin optimal dans des réseaux ou l'optimisation de processus.
- Les **algorithmes de simulation de mécanismes quantiques** qui servent notamment à simuler les interactions entre atomes dans des structures moléculaires diverses, inorganiques et organiques.
- Les **autres algorithmes** divers. Certains visent à simplement reproduire des algorithmes classiques avec des qubits comme cet algorithme de multiplications quantiques[369]. D'autres sont plus exotiques comme cet algorithme qui utilise une mesure d'états faiblement destructrice de l'état des qubits pour faire de la *differential privacy*, un sujet lié aux questions de vie privée[370].

La roadmap *ci-dessus* illustre le rythme de création de ces nouveaux algorithmes sur les trois dernières décennies.



inspiré d'un schéma trouvé sur Quantum Computing Algorithms Andreas Baertschi 2019 (45 slides)

[369] Voir A New Approach to Multiplication Opens the Door to Better Quantum Computers, par Kevin Harnett, 2019.

[370] Voir Gentle Measurement of Quantum States and Differential Privacy, Scott Aaronson and Guy Rothblum, avril 2019 (85 pages).

Et l'histoire ne fait que commencer parce que la dynamique d'innovation exponentielle du thème est pour l'instant limitée par l'imagination humaine et surtout, par les capacités d'expérimentation[371].

Algorithm	Description	Reference
Algorithms Based on QFT		
Shor's; $O\left(n^2 (\log N)^3\right)$	Integer factorization (given integer N find its prime numbers); discrete logarithms, hidden subgroup problem, and order finding	Peter W. Shor, "Algorithms for Quantum Computation Discrete Log and Factoring," AT&T Bell Labs, shor@research.att.com
Simon's; *exponential*	Exponential quantum-classical separation. Searches for patterns in functions	Simon, D.R. (1995), "On the power of quantum computation", Foundations of Computer Science, 1996 Proceedings., 35th Annual Symposium on: 116–123, retrieved 2011-06-06
Deutsch's, Deutsch's – Jozsa, an extension Deutsch's algorithm	Depicts quantum parallelism and superposition. "Black Box" inside. Can evaluate the input function, but cannot see if the function is balanced or constant	David Deutsch (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". Proceedings of the Royal Society of London A. 400: 97 David Deutsch and Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". Proceedings of the Royal Society of London A. 439: 553
Bernstein/Vazirani; *polynomial*	Superpolynomial quantum-classical separation	Ethan Bernstein and Umesh Vazirani. *Quantum complexity theory.* In Proc. 25th STOC, pages 11–20, 1993
Kitaev	Abelian hidden subgroup problem	A. Yu. Kitaev. *Quantum measurements and the Abelian stabilizer problem*, arXiv:quant-ph/9511026, 1995
van Dam/Hallgren	Quadratic character problems	Wim van Dam, Sean Hallgren, *Efficient Quantum Algorithms for Shifted Quadratic Character Problems.* CoRR quant-ph/0011067 (2000)
Watrous	Algorithms for solvable groups	John Watrous, Quantum algorithms for solvable groups, arXiv:quant-ph/0011023, (2001)
Hallgren	Pell's equation	Sean Hallgren. *Polynomial-time quantum algorithms for pell's equation and the principal ideal problem*, Proceedings of the thirty-fourth annual ACM symposium on the theory of computing, pages 653–658. ACM Press, 2002.
Algorithms Based on Amplitude Amplification		
Grover's; $O\left(\sqrt{N}\right)$	Search algorithm from an unordered list (database) for a marked element, and statistical analysis	Lov Grover, *A fast quantum mechanical algorithm for database search*, In Proceedings of 28th ACM Symposium on Theory of Computing, pages 212–219, 1996
Traveling Salesman Problem; $O\left(\sqrt{N}\right)$	Special case of Grover's algorithm	https://en.wikipedia.org/wiki/Travelling_salesman_problem

Les algorithmes quantiques actuels se ramènent souvent aux mêmes méthodes de génération d'interférences et de transformées de Fourier quantiques. Dans le calcul à recuit quantique, on fait appel aux simulations d'Hamiltoniens et aux modèles d'Ising[372].

Les algorithmes quantiques sont classifiables et explicables à haut niveau, mais leur compréhension détaillée n'est pas une partie de plaisir. Il faut soit avoir une capacité de vision conceptuelle assez développée, et en particulier une maitrise des mathématiques poussée[373].

Dans ce qui suit, je vais donc vous décrire quelques algorithmes mais en reconnaissant que je n'ai pas véritablement tout compris de leur fonctionnement dans les qubits et opérations de portes quantiques appliquées dessus.

Le quantique est ainsi fait en général : on n'a jamais tout compris ! Décrire cela est donc un véritable exercice d'humilité intellectuelle.

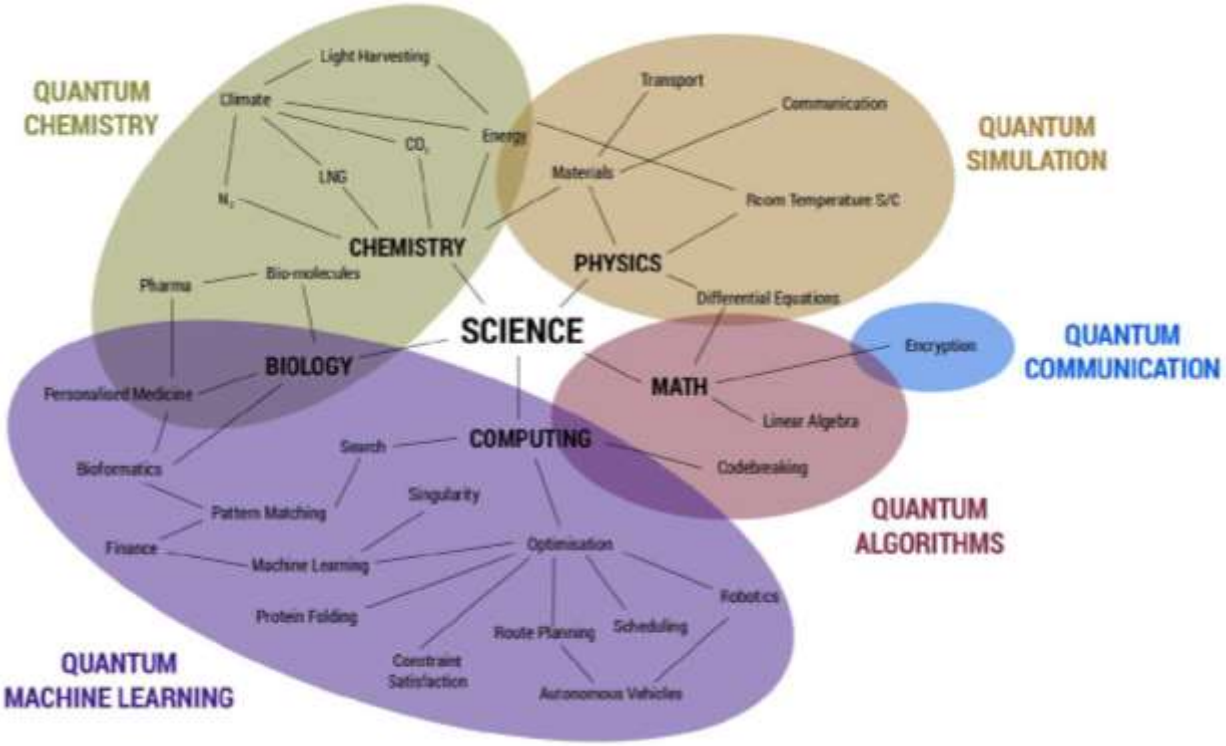
---

[371] Source d'inspiration du schéma sur les algorithmes : Quantum Computing Algorithms par Andreas Baertschi, 2019 (45 slides).

[372] Voir Quantum computing (QC) Overview par Sunil Dixit de Northrop Grumman, septembre 2018 (94 slides) d'où est extrait le tableau d'algorithmes de cette page.

[373] Voici quelques sources d'information pour creuser la question : Quantum Computing Applications d'Ashley Montanaro de l'Université de Bristol, 2013 (69 slides), Introduction à l'information quantique de Yves Leroyer et Géraud Sénizergues de l'ENSEIRB-MATMECA, 2016-2017 (110 pages), un cours récent intéressant sur la partie algorithmique, An Introduction to Quantum Computing de Phillip Kaye, Raymond Laflamme et Michele Mosca, Oxford, 2017 (284 pages), Lecture Notes on Quantum Algorithms de Andrew M. Childs, University of Maryland, 2017 (174 pages), Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages) et A Course in Quantum Computing for the Community College de Michael Locef, 2016 (742 pages) qui pose de manière très détaillée les fondements mathématiques de l'algèbre linéaire avec les nombres complexes, les formules d'Euler, les espaces vectoriels et de Hilbert, le calcul matriciel, les tenseurs, eigenvectors et eigenvalues, et les algorithmes quantiques. Il nécessite plusieurs semaines pour être parcouru et compris. C'est un cours pour la seconde et troisième année du Foothill Community College de Los Altos Hills en Californie (donc Bac+1/+2 en équivalent français). En complément, voici quelques vidéos sur ce même sujet : Quantum Algorithms d'Andrew Childs en 2011 (2h31), Language, Compiler, and Optimization Issues in Quantum Computing de Margaret Martonosi, 2015 (39 minutes et slides) et What Will We Do With Quantum Computing? de Aram Harrow, MIT, 2018 (32 minutes).

Voir aussi cette cartographie d'applications du calcul quantique qui est cependant un peu fantaisiste, reliant le machine learning à « singularity », ce qui ne veut pas dire grand-chose (*ci-dessous*)[374].



Algorithmes de recherche

L'un des premiers algorithmes quantiques inventés est celui de David Deutsch, avec sa déclinaison dite de **Deutsch-Jozsa**, coinventée avec Richard Jozsa et qui date de 1992. Cet algorithme permet de caractériser la fonction d'une "boite noire" que l'on appelle un "oracle" dont on sait à l'avance qu'elle va retourner pour toutes ses entrées, soit toujours la même valeur, 0 ou 1, soit les valeurs 0 et 1 à parts égales. L'algorithme permet donc de savoir si la fonction f() est équilibrée ou pas. Elle est appliquée à un ensemble de qubits n.

Les qubits en entrée sont tous initialisés à 0 sauf un qui l'est à 1 puis ils sont chacun mis en superposition entre 0 et 1 via des portes de Hadamard. Les qubits ont donc simultanément toutes les valeurs possible avec 2 puissance n+1 combinaisons de valeurs.

Il est facile de comprendre pourquoi cet algorithme quantique est bien plus efficace que sa version traditionnelle : en calcul traditionnel, il faudrait scanner plus de la moitié des valeurs possibles en entrée de manière séquentielle alors que dans la version quantique, elles sont toutes analysées en même temps.

Le résultat est donc obtenu avec quelques séries de portes quantiques, presque instantanément, et il est parfaitement déterministe.

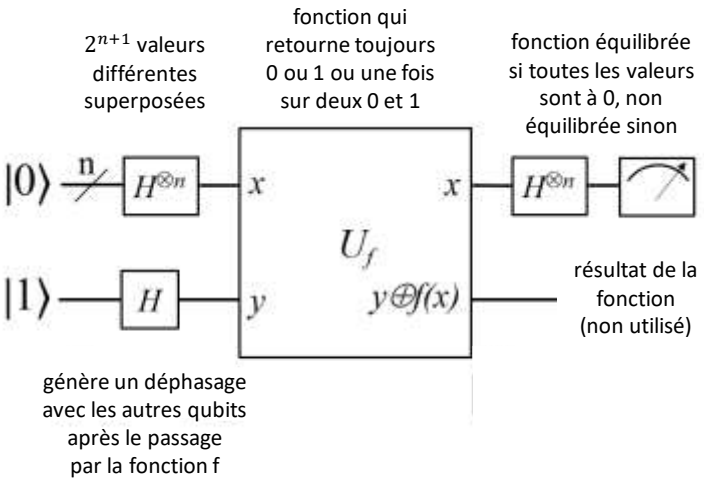
Ces qubits en superposition traversent la boîte noire qui contient un ensemble de portes avec une fonction à évaluer. On mesure alors en sortie le résultat pour voir si la fonction est équilibrée ou pas grâce à d'autres portes de Hadamard.

[374] Source : Silicon Photonic Quantum Computing de Syrus Ziai, PsiQuantum, 2018 (72 slides).

Deutsch-Jozsa

vérifie qu'une fonction f est équilibrée ou non

$O(2^{N-1} - 1) \Rightarrow O(4)$



L'initialisation du dernier qubit à 1 sert à générer une interférence avec les autres qubits qui va impacter les valeurs sortant des portes H après le passage par l'oracle. La fonction f est constante si la totalité des mesures donne 0 et déséquilibrée si au moins d'un des qubits en sortie retourne 1[375]. Les explications données sont toujours incomplètes pour bien comprendre ces algorithmes. Elles n'indiquent pas bien où se retrouve le bit de sortie de la fonction de l'oracle qui est soit de 0 soit de 1.

L'intérêt pratique ? C'est un exemple d'algorithme ultra puissant qui n'a aucune utilité pratique connue à ce jour. On est bien avancés ! Qui plus est, il existe des algorithmes probabilistes classiques très efficaces qui effacent une bonne part du gain de puissance quantique de l'algorithme de Deutsch-Jozsa.

C'est le cas en particulier de l'algorithme de recherche de Monte Carlo qui évalue la fonction d'oracle sur un nombre limité d'entrées choisies aléatoirement. La probabilité d'erreurs est dépendante du nombre d'évaluations et décroit très rapidement[376].

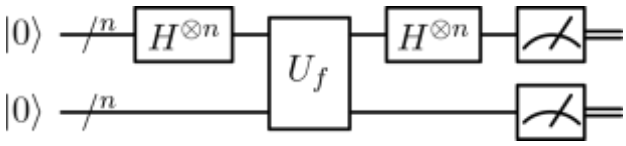
Alors, le quantique ne sert donc à rien ? Non, bien sûr. D'autres algorithmes moins performants mais bien plus utiles ont vu le jour depuis ce patient zéro de l'algorithmie quantique !

L'algorithme de **Simon** est une variante plus sophistiquée de celui de Deutsch-Jozsa. Il consiste à trouver les combinaisons de valeurs qui vérifient une condition imposée par la fonction "boite noire".

Simon

recherche de sous-ensemble dont les membres vérifient une condition imposée par une fonction f

$O(\sqrt{2^N}) \Rightarrow O(N)$



Le gain de performance est très intéressant et cette fois-ci, les applications existent, notamment pour résoudre des problèmes de parcours dans des graphes. Le gain de performance est typique de ce que le quantique apporte : on passe d'un calcul classique qui est de temps exponentiel ($2^{N/2}$) à un temps linéaire en N.

L'autre algorithme le plus connu de cette catégorie est celui de **Grover**, créé en 1996. Il permet de réaliser une recherche quantique rapide dans une base de données. Un peu comme l'algorithme de Deutsch-Jorza, il permet de scanner une liste d'éléments pour trouver ceux qui vérifient un critère.

---

[375] Pour savoir comment cela fonctionne dans le détail, vous pouvez voir les formules mathématiques associées ainsi que la présentation Deutsch-Jozsa Algorithm d'Eisuke Abe, 2005 (29 slides). Mais ce n'est pas des plus évident !

[376] Voir à ce sujet le document Modèles de Calcul Quantique (30 pages).

Il utilise aussi la superposition d'états de qubits pour accélérer le traitement par rapport à une recherche séquentielle traditionnelle dans une base non triée et non indexée. L'amélioration de performance est significative par rapport à une base non triée, à ceci près que dans la vraie vie, on utilise généralement des bases indexées !

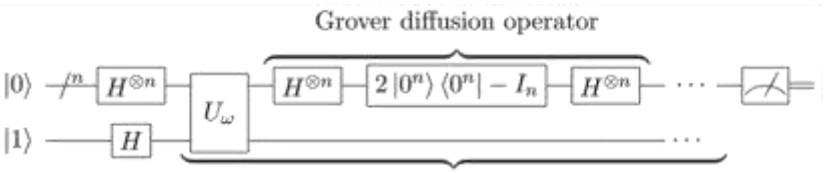
recherche un élément donné dans une base non indexée

$O(N) \Rightarrow O(\sqrt{N})$

fonction qui indique si la valeur trouvée est la bonne

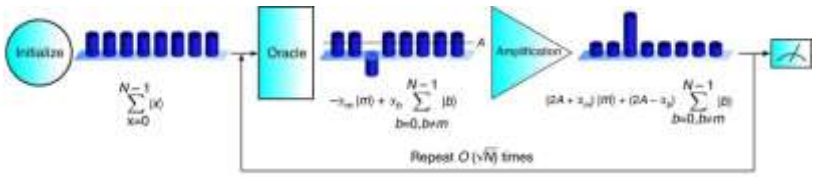
suite d'opérations qui va amplifier la bonne réponse et atténuer les autres réponses

mesure de la bonne réponse qui émerge



initialisation identique à celle de l'algorithme de Deutsch-Jozsa

Repeat $O(\sqrt{N})$ times



L'algorithme de Grover utilise aussi une fonction "oracle" ou "boite noire" qui va indiquer si un ensemble de qubits en entrée vérifie un critère de recherche ou non, comme pour vérifier qu'un numéro de téléphone donné a été trouvé dans une liste de numéros de téléphone.

Dans un tel cas, la fonction compare le numéro de téléphone recherché et celui qui lui est soumis pour répondre 1 s'ils sont identiques et 0 sinon. La boite noire étant quantique, elle va évaluer cette fonction pour 2^N registres de qubits en même temps. Elle sortira donc un 1 une fois et des 0 autrement.

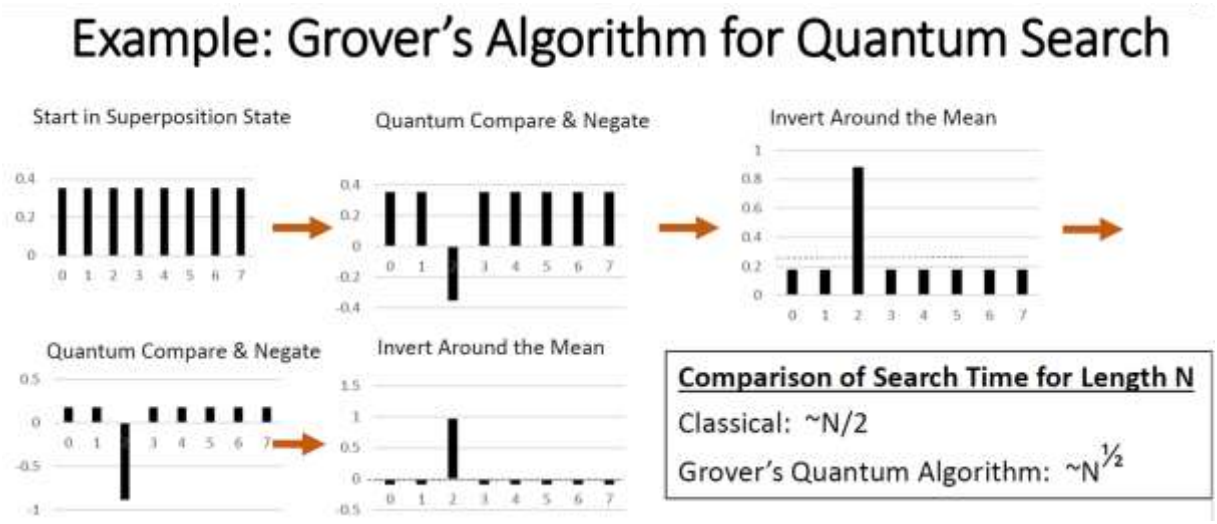
La question étant de savoir si un 1 est sorti une fois et à quelle entrée il correspond. Pour ce faire, là aussi avec des portes de Hadamard, l'algorithme va amplifier graduellement la combinaison de qubits du résultat à une valeur 1 et faire converger les autres combinaisons de qubits vers 0.

Il sera alors possible de mesurer le résultat et on obtiendra la combinaison de qubits avec la valeur recherchée. C'est bien expliqué dans le schéma *ci-dessous*[377].

Le temps de calcul est proportionnel à la racine carrée de la taille de la base et l'espace de stockage nécessaire est proportionnel au logarithme de la taille de la base. Un algorithme classique a un temps de calcul proportionnel à la taille de la base. Passer d'un temps N à sqrt(N) est donc un gain intéressant, mais il ne transformera pas un problème de taille exponentielle en problème de taille polynomial (2 puissance N vers N puissance M).

Par contre, cet algorithme peut ensuite être exploité pour être intégré dans d'autres algorithmes comme ceux qui permettent de découvrir le chemin optimal dans un graphe ou le nombre minimal ou maximal d'une série de N nombres.

[377] Source du schéma : Quantum Computing Explained for Classical Computing Engineers de Doug Finke, 2017 (55 slides). Le lien ne semble plus opérationnel en juillet 2019.



Notons cependant que l'algorithme de recherche de Grover nécessite l'emploi d'une mémoire quantique (QRAM) qui n'est pas encore au point[378] !

Ces différents algorithmes de recherche sont déclinés en diverses variantes et sont exploités en pièces détachées dans d'autres algorithmes quantiques.

QFT et Shor

Les transformées de Fourier classiques permettent d'identifier les fréquences qui composent un signal. En théorie du signal, cela permet d'identifier les composantes de base d'un son en le décomposant en fréquences.

En astrophysique, on détermine la composition atomique des étoiles par une décomposition du spectre lumineux, mais celle-ci est opérée par un prisme optique et pas par transformée de Fourier. Il en va de même pour les capteurs en proche infrarouge de type Scio qui déterminent la composition des aliments. Un prisme et le principe de la diffraction permettent donc de réaliser optiquement une transformée de Fourier.

La transformée de Fourier quantique a été inventée par **Don Coppersmith** (USA) en 1994. Elle est utilisée dans divers autres algorithmes et en particulier dans celui de Shor qui sert à factoriser des nombres entiers. Elle n'est pas une transformée parfaite qui réalise une décomposition complète en fréquences d'un signal.

Elle sert à identifier la fréquence d'amplitude la plus forte d'un signal donné. Elle ne peut pas servir à du traitement fin du signal comme on le fait dans des DSP (Digital Signal Processors) traditionnels.

La QFT s'appuie sur deux types de portes logiques : des portes de Hadamard pour réaliser une superposition et des portes R à phase contrôlée à deux qubits dont la phase est inversement proportionnelle à 1 jusqu'à N. Ce qui pose un énorme problème de précision dans le calcul : plus N est grand, plus l'angle de rotation du qubit dans sa sphère de Bloch va être faible et plus les erreurs de phase seront impactantes. Cela nécessite d'ailleurs un contrôle très précis de l'activation des qubits.

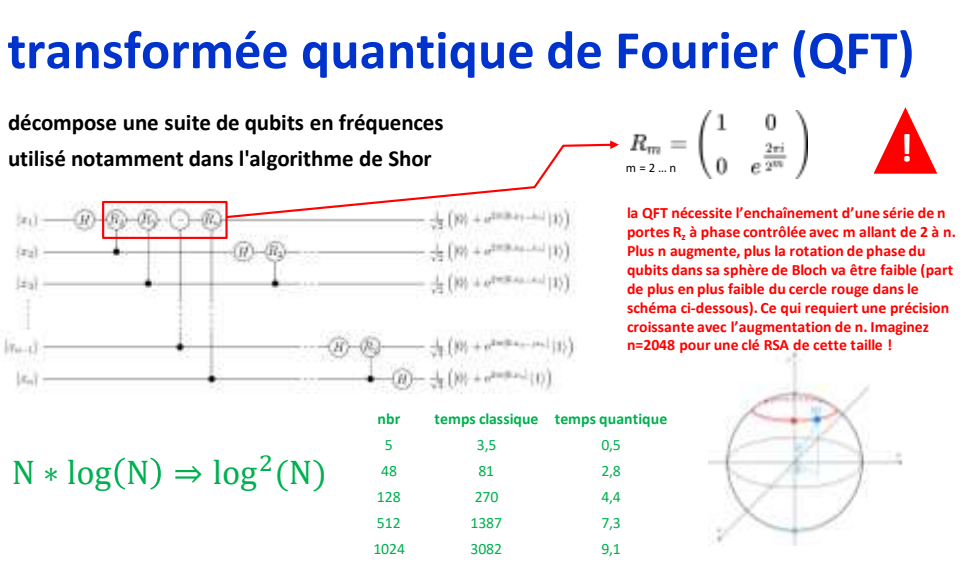
En pratique, les portes R à phase contrôlées sont générées par une combinaison de portes H, Z et T, plus une CNOT pour l'intrication du qubit de contrôle avec le qubit cible.

[378] C'est notamment documenté dans Quantum algorithms for linear algebra de Anupam Prakash, 2015 (92 slides).

Et il en faut beaucoup ! Par exemple pour une porte R_{15}, il faut employer 127 portes H/Z/T pour obtenir une précision de 10^{-5}, ce qui est énorme[379]. On peut optimiser cela avec des qubits auxiliaires. Et il faut évidemment intégrer les codes de correction d'erreurs associés qui ajoutent un bon ordre de grandeur en nombre de portes quantique en profondeur de calcul. Cela impacte surtout la durée du calcul puisque les codes de correction d'erreurs sont censés rallonger la durée de la cohérence des qubits.

Pour une porte R_{2048}, la dernière d'une longue série pour casser une clé RSA de 2048 bits ? C'est à peu près le même nombre de portes.

Cela vient du théorème Solovay-Kitaev que nous avons vu dans une partie précédente, selon lequel cette décomposition dépend uniquement du taux d'erreur ciblé[380].



Dans le cas des qubits supraconducteurs, la génération de portes à phase variable passe par l'envoi d'une impulsion micro-onde plus courte.

Le gain de vitesse généré par l'algorithme de Shor par rapport au calcul classique ? Le temps de calcul passe de N*log(N) pour les meilleures transformées de Fourier simples à $\log^2(N)$ pour la QFT. On passe donc d'un ordre de grandeur linéaire à un ordre de grandeur logarithmique. C'est un gain appréciable mais pas très impressionnant. Mais comme il peut s'appliquer à des N qui sont eux-mêmes des puissances de 2, l'accélération est intéressante.

La factorisation de **Shor** permet de décomposer des entiers en nombres premiers bien plus rapidement qu'avec un ordinateur traditionnel. Elle utilise une QFT vue précédemment. Le fonctionnement de l'algorithme est décrit dans le schéma *ci-dessous*[381] et dans cette explication assez claire vue dans une vidéo de PBS[382].

L'une des premières mises en œuvre de l'algorithme de Shor eu lieu en 2001 chez IBM avec un ordinateur quantique expérimental de 7 qubits, pour factoriser le nombre 15. Depuis, on est juste passé à un nombre à 5 chiffres, 56153[383], mais avec un autre algorithme de factorisation que celui de Shor. C'est en fait un algorithme d'optimisation qui fonctionnait sur ordinateur à recuit quantique du Canadien D-Wave ! Le record à ce jour atteint en 2016 serait la factorisation de 200 099 avec 897 qubits sur D-Wave mais avec un autre algorithme que celui de Peter Shor.

---

[379] Voir Efficient decomposition methods for controlled-R n using a single ancillary qubit par Taewan Kim et Byung-Soo Choi, 2018 (7 pages) et Approximate quantum Fourier transform with O(n log(n)) T gates par Yunseong Nam et al, 2020 (6 pages).

[380] La principale méthode de décomposition de portes R_n est documentée dans Optimal ancilla-free Clifford+T approximation of z-rotations par Neil J. Ross et Peter Selinger, 2016 (40 pages). C'est coton !

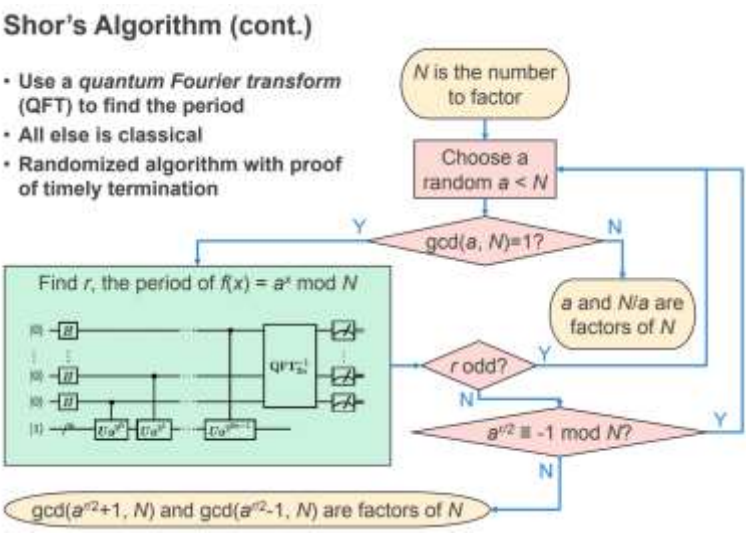
[381] Source du schéma : Quantum Annealing de Scott Pakin, NSF/DOE Quantum Science Summer School juin 2017 (59 slides).

[382] Voir aussi On Shor's algorithms, the various derivatives, their implementation and their applications par Martin Ekera, 2019 (135 slides) qui décrit bien dans le détail le fonctionnement de l'algorithme de Shor.

[383] C'est documenté dans Quantum factorization of 56153 with only 4 qubits, 2014 (6 pages).

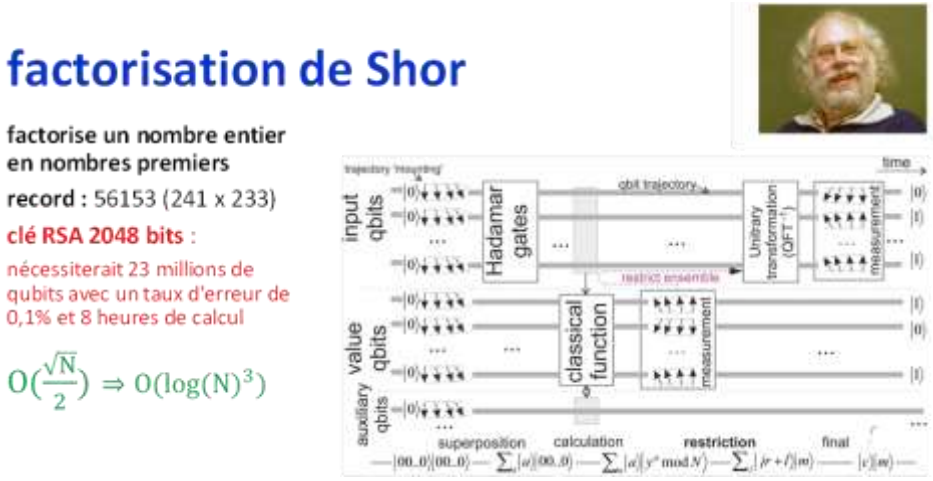
Comme quoi il ne faut pas jeter le bébé D-Wave avec l'eau du bain du quantique universel !

Il faut surtout retenir que l'algorithme de Shor permet en théorie de casser les clés publiques de la cryptographie RSA qui est couramment utilisée dans la sécurité sur Internet. Les clés publiques fonctionnent en envoyant un très long nombre entier à un destinataire qui possède déjà son diviseur. Il lui suffit de diviser le grand nombre envoyé par son diviseur pour récupérer l'autre diviseur et décoder le message ainsi chiffré.



Celui qui ne possède pas le diviseur ne peut pas exploiter la clé complète sauf à disposer d'une énorme puissance de calcul traditionnelle pour trouver ses diviseurs. Jusqu'à présent, seuls les supercalculateurs de la NSA pouvaient casser les clés de taille raisonnable comprises aux alentours de 256 à 400 bits. Mais à 512, 1024 bits et au-delà, la tâche est inaccessible en un temps raisonnable pour ces supercalculateurs.

En théorie, cela deviendrait accessible à des ordinateurs quantiques. Pour casser une clé publique RSA de 1024 bits, il faudra encore patienter car cela nécessite de créer des ordinateurs quantiques avec un très grand nombre de qubits fonctionnant en cohérence et avec des codes de correction d'erreurs de compétition.



Il faut à peu près deux fois plus de qubits logiques que de bits dans une clé RSA. Pour factoriser une clé RSA de 2048 bits, il faudra disposer d'au minimum 4098 qubits logiques[384]. Or, en raison du bruit généré dans les qubits, il est estimé qu'il faudrait des milliers si ce n'est des dizaines de milliers de qubits physiques par qubits logiques. Donc, une telle clé requiert plusieurs dizaines de millions de qubits d'aujourd'hui alors que l'on a du mal à en aligner plus d'une cinquantaine ! On en est donc très très loin.

A noter que l'algorithme de Shor permet aussi de casser la cryptographie utilisant des courbes elliptiques, qui concurrencent la cryptographie RSA. Au passage, une part de la cryptographie utilisée dans le protocole du Bitcoin passerait également à la moulinette Shor, ce que nous verrons plus loin dans ce document.

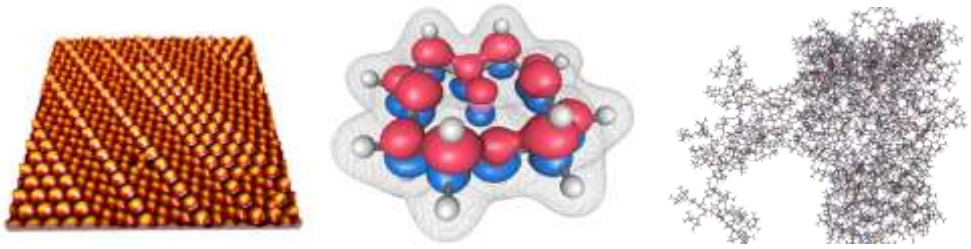
[384] La formule est de 2xN+2 qubits. Voir Factoring using 2n + 2 qubits with Toffoli based modular multiplication par Thomas Haner et al, 2017 (12 pages) et Circuit for Shor's algorithm using 2n+3 qubits par Stephane Beauregard, 2013 (14 pages)..

En tout cas, l'algorithme de Shor terrorise les spécialistes de la sécurité depuis une bonne dizaine d'années. Cela explique l'intérêt pour l'exploitation de clés quantiques, censées être inviolables car leur interception peut être détectée par son récipiendaire légitime, ainsi que de la "post quantum cryptographie" consistant à faire évoluer les algorithmes et méthodes de cryptographie pour les rendre (théoriquement) inviolables par des ordinateurs quantiques utilisant l'algorithme de Shor. Les deux méthodes étant probablement combinables. Nous aurons l'occasion de traiter de cela plus tard.

Simulation de physique quantique

Les algorithmes de simulation quantique servent à reproduire dans un ordinateur les phénomènes de la mécanique quantique qui gouvernement le comportement de quantums dans des ordinateurs traditionnels ou quantiques. Ils sont exploitables en particulier pour simuler l'interaction entre les atomes dans des molécules pour la création de nouveaux matériaux. Ils peuvent aussi simuler des phénomènes physiques liés au magnétisme ou à l'interaction entre les photons et la matière. Cela revient à résoudre des « problèmes à N-corps », soit calculer l'interaction entre plusieurs particules en fonction des lois physiques qui régissent leur interaction.

La simulation quantique concerne aussi l'étude des matériaux supraconducteur (notamment à (relativement) haute température, -70°C), au superfluides à basse température, au magnétisme de certains matériaux qui dépend de la température ainsi qu'aux interactions entre le graphène et la lumière[385].



supraconductivité
interactions graphène/lumière
superfluidité

capture du carbone
photosynthèse
nouvelles batteries

repliement de protéines
interactions entre protéines
drug discovery

A plus haut niveau se situe la simulation des interactions atomiques dans des molécules de la biologie moléculaire, donc, de la chimie organique, allant progressivement des plus petites aux plus grandes des molécules : acide aminés, peptides, polypeptides, protéines et peut-être bien plus tard, de molécules ultra complexes comme les ribosomes qui fabriquent les protéines à partir des acides aminés.

La constitution et le fonctionnement de ces grosses molécules font partie des plus grands mystères chimiques de la vie que l'Homme aimerait bien expliquer. Cela peut aussi servir à faire des simulations "macro" comme celle du fonctionnement de trous noirs ou d'étoiles à neutrons en astronomie.

Tous ces algorithmes ambitionnent de simuler les processus atomiques ou moléculaires qui interviennent dans la nature ou à créer de tels mécanismes artificiels qui n'existent pas encore dans la nature.

Comme les algorithmes classiques, les algorithmes quantiques de simulation utilisent des modèles d'approximation. Les algorithmes quantiques permettront à terme d'augmenter la taille des problèmes simulés.

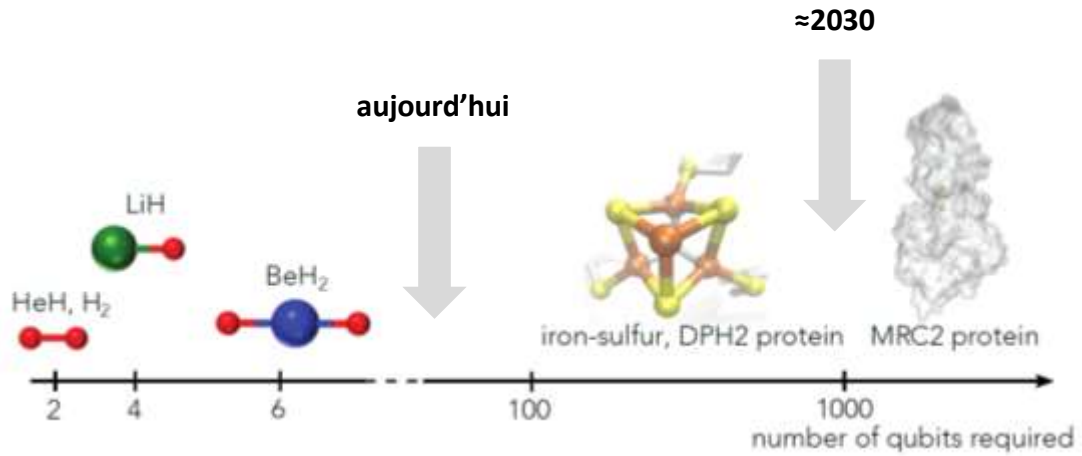
[385] Voir cette intéressante conférence de Jacqueline Bloch à l'Académie des Sciences qui en fait un excellent panorama : Simulateurs quantiques : résoudre des problèmes difficiles, mai 2018 (29 mn).

Ces algorithmes s'exécutent de manière la plus performante dans les ordinateurs quantiques universels à base de qubits.

En attendant, on les exécute dans des ordinateurs à recuit quantique comme ceux de D-Wave voire dans des ordinateur quantiques dits analogiques, ou dénommé simulateurs quantiques, sans architectures à base de registres de qubits. Les plus courants et qui sont encore des objets de laboratoire sont les ordinateurs à base d'atomes froids comme le rubidium. Comme ces algorithmes visent souvent à déterminer un niveau d'énergie minimum d'un système complexe, le système adiabatique à recuit simulé de D-Wave est assez adapté à la tâche pour des problèmes relativement simples.

A partir de 50 électrons dans une molécule, les ordinateurs classiques ne peuvent plus simuler leur dynamique, ce qui correspond à quelques atomes à peine. Pour les molécules simples, les applications relèvent de la physique des matériaux : capture du carbone ou de l'azote, nouvelles batteries, découverte de mécanismes supraconducteurs utilisables ensuite dans les scanners médicaux, idéalement fonctionnant à température ambiante.

Ceci devrait être accessible avec des ordinateurs quantiques universels dotés de 50 à quelques centaines de qubits de qualité. Pour les simulations de biologie moléculaire, il faudra probablement attendre bien plus longtemps avant que cela soit possible et disposer d'ordinateur avec des milliers voir des centaines de milliers de qubits. Le schéma *ci-dessous* positionne de manière assez optimiste le nombre de qubits nécessaires pour simuler le fonctionnement une protéine des mitochondries, la MRC2[386].



source : Quantum optimization using variational algorithms on near-term quantum devices, 2017

Voici quelques exemples d'algorithmes de simulation quantique :

- Simulating a quantum field theory with a quantum computer de John Preskill, 2018 (22 pages) qui porte sur la simulation de champs quantiques qui régissent l'interaction de la matière à très bas niveau.
- Computation of Molecular Spectra on a Quantum Processor with an Error-Resilient Algorithm, 2018 (7 pages) sur la simulation du fonctionnement des atomes d'hydrogène dans des ordinateurs quantiques à qubits supraconducteurs.

[386] Il est issu de Quantum optimization using variational algorithms on near-term quantum devices, issu de chercheurs d'IBM en 2017 (30 pages).

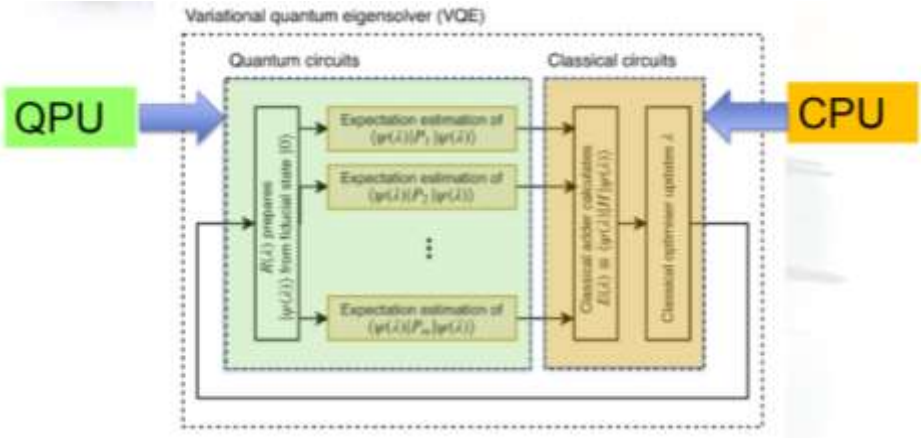
- Des chercheurs réussissent le contrôle quantique d'une molécule, de Román Ikonicoff, mai 2017 qui pointe sur Preparation and coherent manipulation of pure quantum states of a single molecular ion, 2017 (38 pages), décrivant un algorithme de simulation hybride associant calcul classique et calcul quantique pour étudier le spectre de l'hydrogène. La partie quantique n'utilise que deux qubits supraconducteurs !
- Un exemple de simulation de molécule d'hydrure de béryllium (3 atomes, BeH2) avec seulement 6 qubits par IBM en 2017 dans Tiny Quantum Computer Simulates Complex Molecules par Katherine Bourzac.
- La simulation de l'électrolyse de l'eau provoquée par de la lumière avec des usages évidents pour la production d'énergie stockable, notamment dans les piles à combustible (à base d'hydrogène). C'est l'un des très nombreux exemples issus de la présentation Enabling Scientific Discovery in Chemical Sciences on Quantum Computers, décembre 2017 (34 slides) par Ber De Jong de Berkeley.
- Solving strongly correlated electron models on a quantum computer de Wecker, Troyer, Hastings, Nayak et Clark, 2015 (27 pages), qui utilise les ordinateurs quantiques à recuit quantique pour simuler la dynamique des semi-conducteurs.
- Faster phase estimation de Svore, Hastings et Freedman, 2013 (14 pages) qui est utilisé dans les simulations quantiques de molécules.
- Simulated Quantum Computation of Molecular Energies de Wiebe, Wecker et Troyer, 2006 (21 pages) qui porte sur la détermination de l'état d'équilibre de molécules simples.
- L'amélioration d'algorithmes de simulation de processus chimiques de catalyse proposée par des cherheurs de Microsoft et d'ETZ Zurich dans Quantum computing enhanced computational catalysis par Vera von Burg, Matthias Troyer et al, juillet 2020 (104 pages). Les ordres de grandeur des besoins sont d'environ 4000 qubits logiques, soit des millions de qubits physiques.
- Simulation of Electronic Structure Hamiltonians Using Quantum Computers de James Whitfield, Jacob Biamonte et Alan Aspuru-Guzik, 2010 (22 pages) qui porte aussi sur la simulation du fonctionnement de molécules simples. Alan Aspuru-Guzik est l'une des grandes références mondiales dans le domaine.
- Des simulations moléculaires hybrides associant algorithmes classiques et quantiques vues dans Quantum Machine Learning for Electronic Structure Calculations, octobre 2018 (16 pages).

Dans Quantum Computation for Chemistry, d'Alán Aspuru-Guzik, 2009 (51 slides), on découvre que les caractéristiques des ordinateurs quantiques nécessaires pour simuler l'état de molécules organiques de complexité moyenne telle que le cholestérol, il faudrait 1500 qubits et surtout, pouvoir enquiller des milliards de portes quantiques, ce qui est actuellement impossible au vu des temps de cohérence bien trop courts des ordinateurs quantiques existants. Et on parle probablement d'un nombre de qubits logiques et pas physiques.

Il faudrait donc probablement aligner des millions de qubits physiques pour pouvoir réaliser ce genre de simulation[387].

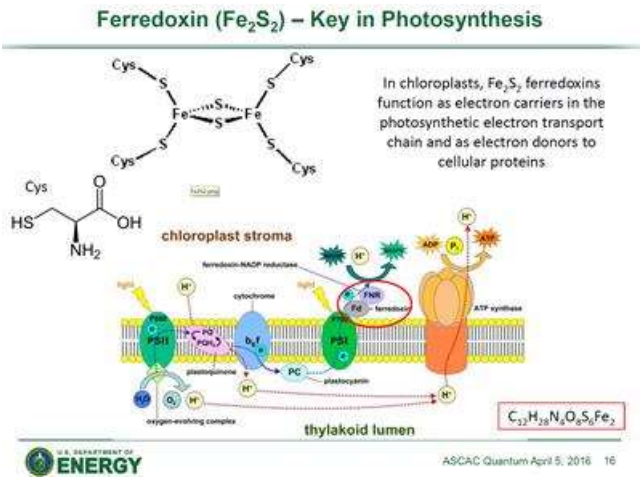
[387] Voir aussi dans le même registre, Quantum Computation for Chemistry and Materials de Jarrod McClean, Google 2018 (36 slides).

Alan Aspuru-Guzik est notamment le coinventeur de la classe des algorithmes hybrides **Variational Quantum Eigensolver** (VQE) qui permet de découvrir un minimum énergétique d'une équation complexe. Nous en parlons aussi dans la rubrique sur les algorithmes hybrides[388].



Cet algorithme est exécutable avec un ordinateur quantique à portes universelles avec une profondeur raisonnable de portes quantiques (nombre d'étapes dans l'algorithme)[389].

L'une des applications de la simulation quantique moléculaire est de mieux comprendre le fonctionnement de la photosynthèse pour éventuellement l'améliorer ou l'imiter, comme ci-dessous avec l'implication des différentes formes de ferrédoxine, des molécules relativement simples à base de fer et de souffre qui servent à transporter les électrons de l'effet photoélectrique mis en œuvre dans la photosynthèse dans les plantes[390]. Les recherches algorithmiques sur la simulation de cette molécule ont fait passer en quelques années la durée de simulation théorique quantique de 24 milliards d'années à une heure !



La simulation de la photosynthèse peut ouvrir la voie à une meilleure capture du carbone, entre autres pour produire du fuel synthétique. Des recherches font d'ailleurs aussi progresser le domaine, sans calcul quantique pour l'instant[391]. Matthias Troyer explique comment cet algorithme a été optimisé[392].

Dans le même domaine, la simulation de l'enzyme nitrogénase qui transforme l'azote en ammoniaque dans les cyanobactéries permettrait de produire des engrais avec beaucoup moins d'énergie que les processus habituels Haber-Bosch de production de l'ammoniaque qui sont très consommateurs d'énergie. L'idée est de réduire les besoins de chauffage du catalyseur.

Il y présente les bénéfices d'autres formes d'optimisations, par simplification du modèle, pour la simulation de supraconducteurs.

---

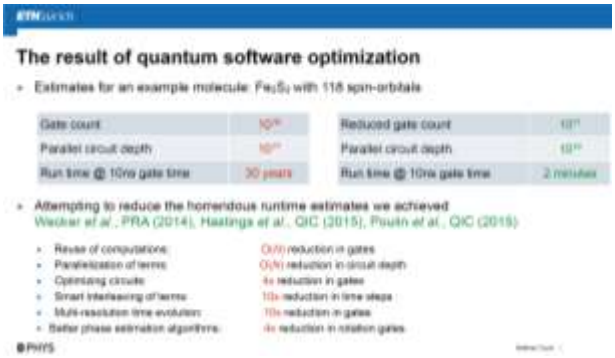
[388] Source du schéma : Accelerated Variational Quantum Eigensolver par Daochen Wang, Oscar Higgott et Stephen Brierley, 2019 (11 pages).

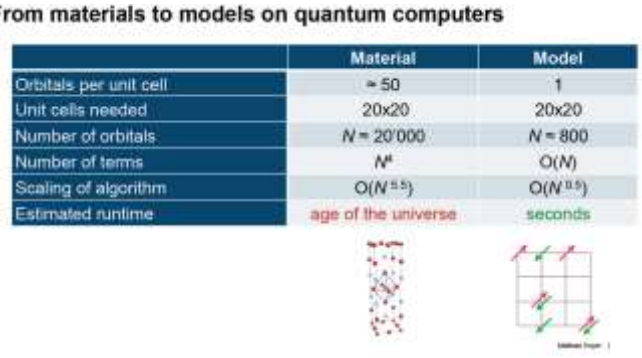
[389] Voir An adaptive variational algorithm for exact molecular simulations on a quantum computer par Sophia Economou et al, 2019 (9 pages) qui indique notamment : "*VQE is much more suitable for NISQ devices, trading in the long circuit depths for shorter state preparation circuits, at the expense of a much higher number of measurements*".

[390] Le schéma sur la ferredoxine provient de Quantum Computing (and Quantum Information Science) de Steve Binkley, US Department of Energy, 2016 (23 slides).

[391] Comme vu dans Semi-Artificial Photosynthesis Method Produces Fuel More Efficiently Than Nature, septembre 2018

[392] Dans What Can We Do with a Quantum Computer, Matthias Troyer, ETZ Zurich, 2016 (41 slides), source de l'illustration de droite.





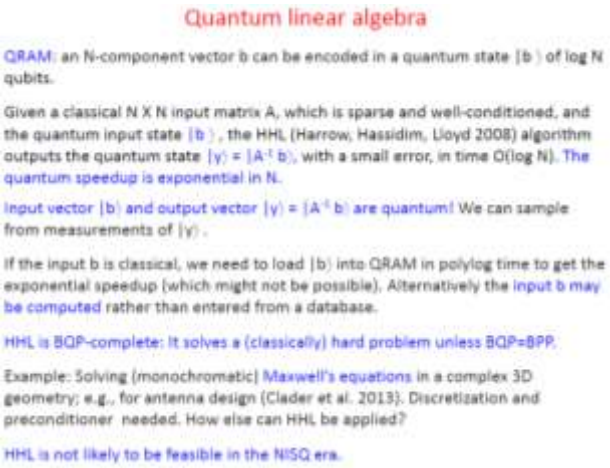
S'il faudra être patient pour voir la couleur de nombre de ces simulations, cela n'empêche pas de nombreux chercheurs d'explorer des moyens de simuler le repliement de protéines, l'une des tâches de simulation de molécule organique les plus complexes[393].

Le top du top de la simulation moléculaire quantique arrivera probablement bien plus tardivement. Il s'agit de la simulation du repliement des protéines, une voie clé pour créer de nouvelles thérapies diverses, notamment pour traiter certaines pathologie neurodégénératives ou divers cancers. Différents algorithmes quantiques ont déjà été créés pour ce faire et notamment celui de Aspuru-Guzik de Harvard en 2012, qui a même été testé à petite échelle sur le premier ordinateur quantique adiabatique, le D-Wave One. Reste à évaluer les ordres de grandeur des ordinateurs quantiques nécessaires pour résoudre ces problèmes de chimie organique. Il n'est pas impossible qu'ils relèvent de l'impossible ou de l'extrême long-terme [394]!

Equations linéaires

De nombreux autres algorithmes quantiques existent qui permettent de réaliser des opérations mathématiques complexes comme la résolution d'équations différentielles, l'inversion de matrices ou le traitement de divers problèmes d'algèbre linéaire. Ils sont ensuite utilisés ailleurs comme dans la QML.

L'algorithme le plus connu est le **HHL** qui reprend le nom de ses créateurs Harrow, Hassidim et Lloyd, créé en 2009. Il permet de résoudre des équations linéaires, avec un gain de performance exponentiel.



Machine learning

Et si le calcul quantique permettait d'accélérer les traitements de l'intelligence artificielle, notamment dans le machine learning et le deep learning ? C'est un de ses domaines d'applications mais nous verrons qu'il n'est pas si évident que cela. A ce stade de maturité de l'IA, le calcul quantique n'a pas l'air de rendre possible ce qui ne le serait pas avec les processeurs classiques, y compris les processeurs spécialisés du moment à base de tenseurs (multiplication de matrices) ou de neurones à impulsions. Mais c'est un domaine en progrès constants.

---

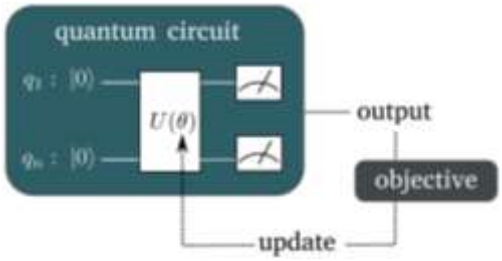
[393] Voir par exemple Evolution, energy landscapes and the paradoxes of protein folding de Peter Wolynes, 2015 (13 pages).

[394] Pour en savoir plus, voir Quantum Information and Computation for Chemistry, 2016 (60 pages), qui inventorie très bien les divers travaux algorithmiques de simulation quantique de chimie organique.

Divers algorithmes quantiques ont être créés ces dernières décennies qui couvrent le champ du machine learning classique et avec quelques incartades dans les réseaux de neurones et le deep learning[395]. On les regroupe sous l'appellation de QML pour Quantum Machine Learning. Ils tirent tous partie de la superposition des états dans un grand espace de Hilbert avec 2^N états pour N qubits. Ils s'appuient notamment sur les nombreuses solutions d'algèbre linéaire apportées par le calcul quantique.

Voici quelques algorithmes quantiques de ce vaste champ de la QML qui couvre pour l'instant plutôt le domaine du machine learning supervisé :

- Le **SVM** (support vector machine), une méthode traditionnelle de segmentation du machine learning qui repose souvent sur des inversions de matrices[396].
- La **PCA** sert à déterminer les variables clés d'un jeu de données (Principal Component Analysis)[397]. Cela revient à chercher les vecteurs propres d'un ensemble de données.
- Il existe aussi un algorithme quantique hybride de **régression non linéaire**, une des méthodes de base de prédiction de valeur quantitative du machine learning[398].
- Les **circuits variationnels** (variational circuits) sont une famille d'algorithmes hybrides qui associent un algorithme quantique et un algorithme traditionnel qui pilote ce dernier[399]. Le VQE, déjà cité, en fait partie. Ils permettent notamment de trouver plus rapidement des minimums globaux, un point de contention classique de la convergence dans le machine learning.



  Ces algorithmes seraient adaptés à des applications sur des calculateurs NISQ (ordinateurs quantiques des prochaines années qui sont bruités).
- Le quantique peut aussi servir à développer des systèmes de **recommandation** utiles en marketing ou dans les contenus[400].
- Des algorithmes quantiques de **réseaux de neurones convolutionnels**, de taille encore modeste pour l'instant[401]. Ils sont aussi envisagés en exploitant les calculateurs à recuit quantique de D-Wave[402].

---

[395] Voir cette vulgarisation du sujet dans Machine Learning in the Quantum Era - Machine Learning unlocks the potential of emerging quantum computers par Loïc Henriet (Pasqal), Christophe Jurczak (Quantonation) et Leonard Wossnig (Rahko), novembre 2019. Elle met en evident le potential des qubits à base d'atomes froids pour la QML.

[396] Voir Support Vector Machines on Noisy Intermediate-Scale Quantum Computers par Jiaying Yang, 2019 (79 pages) qui porte sur l'usage de SVM sur des calculateurs NISQ et Quantum Machine Learning with Support Vector Machines par Anisha Musti, avril 2020.

[397] Voir Quantum principal component analysis par Seth Lloyd, Masoud Mohseni et Patrick Rebentrost, du MIT et Google, juillet 2013 (9 pages) qui pose bien les bases du sujet.

[398] Voir Nonlinear regression based on a hybrid quantum computer, 2018 (7 pages), issu de chercheurs de plusieurs laboratoires en Chine.

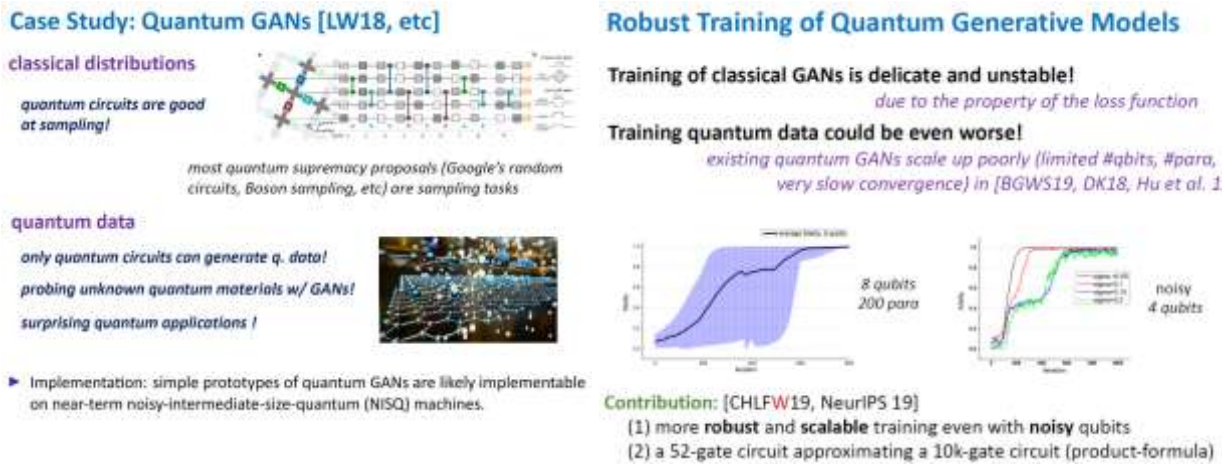
[399] Voir Universal Variational Quantum Computation de Jacob Diamonte, 2019 (5 pages).

[400] Voir Quantum Recommendation Systems de Iordanis Kerenidis, 2016 (22 pages, et vidéo) est une proposition d'algorithme de machine learning quantique pour de la recommandation. L'algorithme quantique de Iordanis Kerenidis avait été remis en question par une proposition d'algorithme classique par la jeune Ewin Tang en 2018. Mais Iordanis mettait en avant qu'avec certains paramètres de recommandation, l'algorithe quantique était toujours nettement supérieur. Toujours, pour peu qu'une machine soit là pour l'exécuter. Voir Un ado sème le doute sur l'utilité du quantique par Laurent Delattre, 2018, qui ne s'était pas rendu compte qu'Ewin Tang était une femme et qu'à 18 ans, on est majeur, en tout cas en France.

[401] Voir Quantum Convolutional Neural Networks, par Iris Cong et al, mai 2019 (12 pages). Voir aussi Quantum Neurons: analyzing the building blocks of quantum deep learning algorithms par Zachary Cetinic et al, décembre 2019 (12 pages).

[402] Voir Adiabatic Quantum Computation Applied to Deep Learning Networks par Jeremy Liu et al, mai 2018 (28 pages).

- Des algorithmes quantiques de **réseaux de neurones de graphes** qui ont pas mal d'applications, notamment en chimie et biologie[403].
- Le **feature mapping** dans le deep learning et les réseaux de neurones convolutifs, pour détecter des formes de manière efficace[404].
- La **descente de gradient** pour la rétropropagation dans l'entraînement des réseaux de neurones[405].
- Des algorithmes quantiques de **GAN** (Generative Adversarial Networks) qui génèrent des contenus synthétiques à partir de contenus existants en vérifiant leur plausibilité via un réseau de neurones de reconnaissance[406]. Mais cela n'est pas encore au point.



Le tableau *ci-dessous* positionne les différentes accélérations quantiques associées à divers algorithmes utilisés dans le machine learning et le deep learning[407]. Les accélérations en log(N) sont plus importantes que celles qui sont exprimées en racine carré de N[408].

Method	Speedup	AA	HHL	Adiabatic	QRAM
Bayesian Inference [107, 108]	$O(\sqrt{N})$	Y	Y	N	N
Online Perceptron [109]	$O(\sqrt{N})$	Y	N	N	optional
Least squares fitting [9]	$O(\log N^{(*)})$	Y	Y	N	Y
Classical BM [20]	$O(\sqrt{N})$	Y/N	optional/N	N/Y	optional
Quantum BM [22, 62]	$O(\log N^{(*)})$	optional/N	N	N/Y	N
Quantum PCA [11]	$O(\log N^{(*)})$	N	Y	N	optional
Quantum SVM [13]	$O(\log N^{(*)})$	N	Y	N	Y
Quantum reinforcement learning [30]	$O(\sqrt{N})$	Y	N	N	N

[403] Voir Quantum Graph Neural Networks par Guillaume Verdon et al, 2019 (10 pages).

[404] Voir Supervised learning with quantum enhanced feature spaces, Aram Harrow et al, 2018 (22 pages) décrit l'usage du quantique pour détecter des formes complexes, bien au-delà de ce que peuvent faire les réseaux de neurones convolutionnels ("feature mapping").

[405] Voir Quantum algorithms for feedforward neural networks de Jonathan Allcock, Iordanis Kerenedis et al, 2018 (18 pages) et Quantum Circuit Parameters Learning with Gradient Descent Using Backpropagation par M Watabe et al, 2020 (15 pages).

[406] C'est bien documenté dans Quantum generative adversarial learning de Seth Lloyd et Christian Weedbrook, 2018 (5 pages) ainsi que dans Quantum generative adversarial learning in a superconducting quantum circuit, 2018 (5 pages). Les illustrations viennent de Applications and Training of Quantum Generative models par Xiaodi Wu de l'University du Maryland, Q2B Workshop, décembre 2019 (11 slides et vidéo) et Quantum Wasserstein Generative Adversarial Networks par Xiaodi Wu et al, octobre 2019 (23 pages).

[407] Le tableau provient de Quantum Machine Learning par Jacob Biamonte et al, mai 2018 (24 pages).

[408] Côté sources d'information sur ce sujet, j'ai aussi parcouru Application of Quantum Annealing to Training of Deep Neural Networks (2015), Machine learning & artificial intelligence in the quantum domain, 2017 (106 pages), On the Challenges of Physical Implementations of RBMs, 2014, avec notamment Yoshua Bengio et Ian Goodfellow parmi les auteurs, illustrant l'intérêt des spécialistes de l'IA pour le quantique et Quantum Deep Learning, 2014, le tout étant extrait de Near-Term Applications of Quantum Annealing, 2016, Lockheed Martin (34 slides).Voir aussi Quantum machine learning for data scientists, 2018 (46 pages).

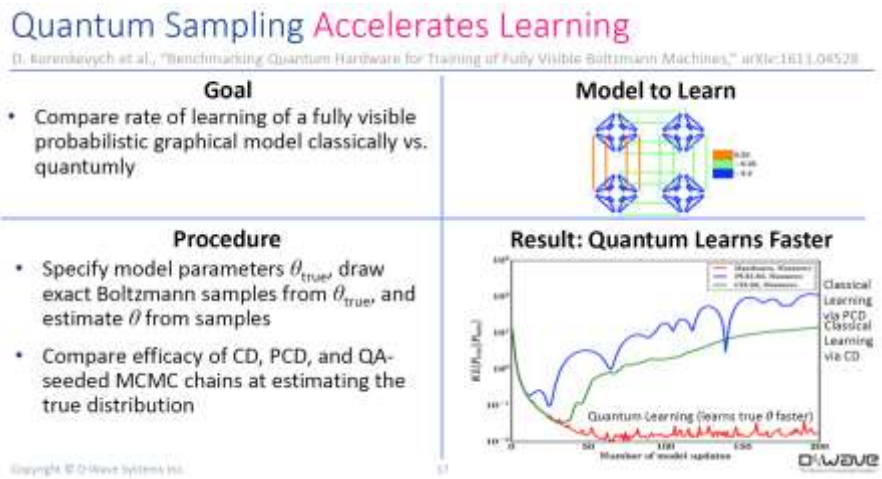
Le tout, avec une amélioration souvent exponentielle de vitesse de traitement, modulo le nombre de fois où le calcul doit être réalisé qui dépend de la profondeur du calcul en nombre de portes à exécuter sans compter l'overhead des codes de correction d'erreur[409]. Mais aucun de ces algorithmes n'a pu être testé à grande échelle, du fait de l'absence de processeur quantique disposant de plus d'une cinquantaine de qubits.

Table 1.1 The Characteristics of the Main Approaches to Quantum Machine Learning

Algorithm	Reference	Grover	Speedup	Quantum Data	Generalization Performance	Implementation
K-medians	Aïmeur et al. (2013)	Yes	Quadratic	No	No	No
Hierarchical clustering	Aïmeur et al. (2013)	Yes	Quadratic	No	No	No
K-means	Lloyd et al. (2013a)	Optional	Exponential	Yes	No	No
Principal components	Lloyd et al. (2013b)	No	Exponential	Yes	No	No
Associative memory	Ventura and Martinez (2000)	Yes		No	No	No
	Trugenberger (2001)	No		No	No	No
Neural networks	Narayanan and Menneer (2000)	Yes		No	Numerical	Yes
Support vector machines	Anguita et al. (2003)	Yes	Quadratic	No	Analytical	No
	Rebentrost et al. (2013)	No	Exponential	Yes	No	No
Nearest neighbors	Wiebe et al. (2014)	Yes	Quadratic	No	Numerical	No
Regression	Bisio et al. (2010)	No		Yes	No	No
Boosting	Neven et al. (2009)	No	Quadratic	No	Analytical	Yes

The column headed "Algorithm" lists the classical learning method. The column headed "Reference" lists the most important articles related to the quantum variant. The column headed "Grover" indicates whether the algorithm uses Grover's search or an extension thereof. The column headed "Speedup" indicates how much faster the quantum variant is compared with the best known classical version. "Quantum data" refers to whether the input, output, or both are quantum states, as opposed to states prepared from classical vectors. The column headed "Generalization performance" states whether this quality of the learning algorithm was studied in the relevant articles. "Implementation" refers to attempts to develop a physical realization.

La QML est aussi l'un des champs d'application du recuit quantique chez D-Wave. Ce dernier est adapté à la recherche d'un minimum énergétique qui revient à rechercher un niveau minimum d'erreurs dans l'ajustement du poids des neurones d'un réseau[410]. Ils ont notamment testé un modèle de RBM (Restricted Bolzmann Machine)[411].

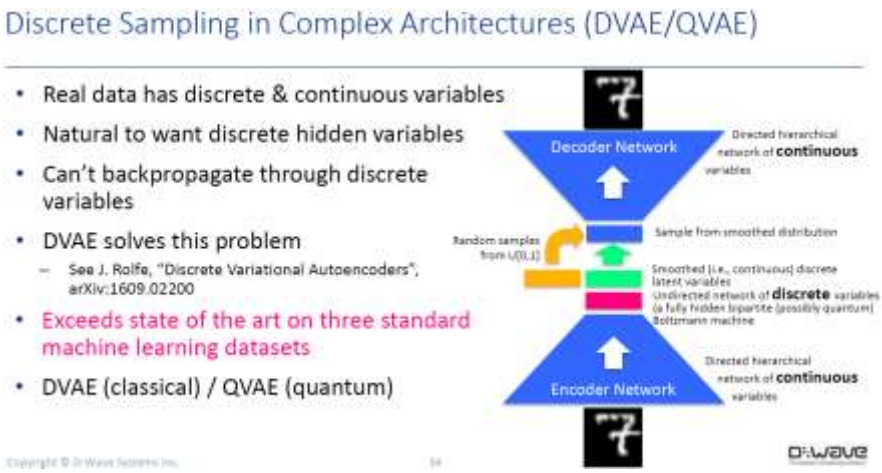


[409] Voir Accelerated Variational Quantum Eigensolver, de Daochen Wang, Oscar Higgott, et Stephen Brierley, 2019 (11 pages) qui propose une méthode de machine learning permettant de réduire la profondeur des circuits quantiques utilisés (nombre de portes quantiques à exécuter). Voir aussi Quantum advantage with shallow circuits de Robert König et al, 2018 (97 slides). On retrouve cette liste d'algorithmes de machine learning en version quantique dans Quantum Machine Learning What Quantum Computing Means to Data Mining de Peter Wittek, 2014 (178 pages).

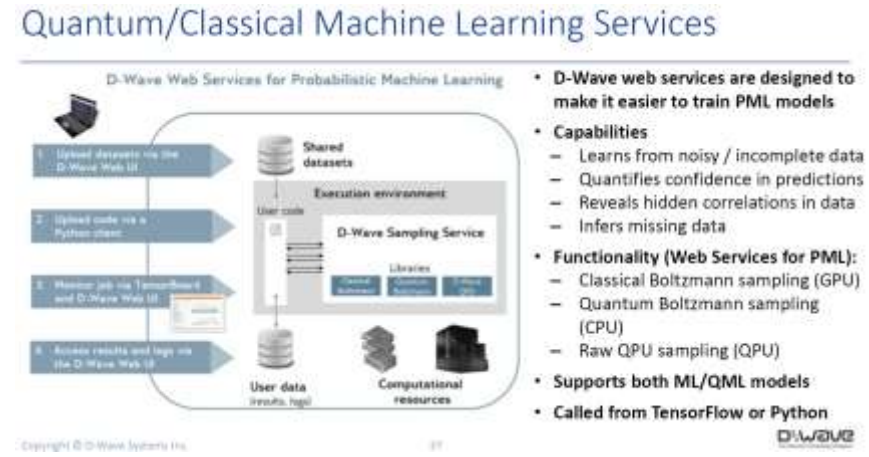
[410] Source des exemples : D-Wave Quantum Computing – Access & application via cloud deployment, Colin Williams, 2017 (43 slides).

[411] Voir Benchmarking Quantum Hardware for Training of Fully Visible Boltzmann Machines par Dmytro Korenkevych et al, Kindred AI et D-Wave, 2016 (22 pages).

Ils l'ont aussi fait avec un algorithme hybride de reconnaissance d'image dans un réseau de neurones, à base de circuit variationnel et d'algorithme hybride. Mais d'image de très basse résolution !



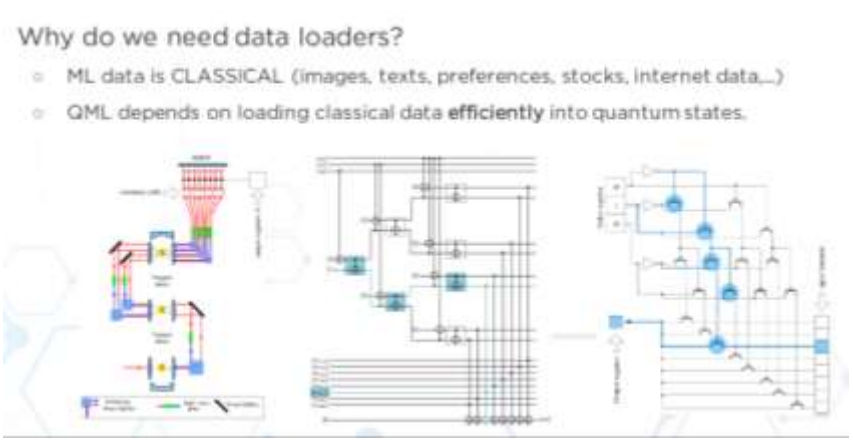
D-Wave propose des services de machine learning dans son offre Leap de cloud computing quantique.



Mais ils ne sont pas les seuls. De nombreuses startups sont spécialisées dans le Quantum Machine Learning, comme **QC Ware**. Avec une réserve souvent émise : l'avantage quantique apporté par le recuit quantique est souvent contesté a posteriori par de nouveaux algorithmes classiques. L'avantage quantique s'attaque à une cible mouvante !

De nombreux points restent à traiter pour opérationaliser la QML au-delà de l'émergence de processeurs quantiques suffisamment puissants et fiables[412] :

- Le **chargement des données d'entraînement** qui peuvent être volumineuses et qui peut nécessiter la gestion de mémoires quantiques, qui ne sont pas encore opérationnelles à ce jour. Ce chargement peut prendre du temps et impacter à la baisse le gain de temps procuré par la QML.



  Il devait faire appel à une mémoire quantique (QRAM pour quantum random access memory)… qui n'existe pas encore même si des pistes existent pour en créer ou s'en passer, comme les Quantum Data Loaders[413].

[412] Voir Quantum machine learning: a classical perspective, par Cilibertoet et al, 2020 (26 pages) qui fait un bon inventaire à date de la question. Le document conclut cependant que l'avantage quantique n'est pas evident à démontrer à ce stade : "*Despite a number of promising results, the theoretical evidence presented in the current literature does not yet allow us to conclude that quantum techniques can obtain an exponential advantage in a realistic learning setting*".

- La **lecture des résultats** des algorithmes de QML, surtout lorsque ceux-ci sont des données classiques qui prennent la forme de nombres réels.
- L'usage dans les réseaux de neurones classiques de **fonctions d'activation non-linéaires** comme les sigmoïdes. Alors que les portes quantiques appliquent toutes des transformations linéaires[414]. Il existe cependant des contournements à ce problème, sur lesquels Iordanis Kerenidis a travaillé[415]. Il existe d'autres parades[416].
- La QML doit tirer à profit les **erreurs et le bruit** générés par le calcul quantique plutôt que les subir. Des travaux vont dans ce sens.
- La QML doit prouver qu'elle apporte un véritable **gain en temps de calcul** par rapport aux processeurs les plus avancés d'aujourd'hui[417].
- La QML doit aussi tenir compte de l'attente côté **explicabilité des algorithmes**. La décomposition du processus d'entraînement et d'inférence de ces réseaux de neurones quantiques sera probablement différente par rapport à leur mise en œuvre dans des processeurs plus traditionnels[418].

A contrario, les développements d'algorithmes de QML ont pu servir de sources d'inspiration pour améliorer des algorithmes fonctionnant avec du calcul classique.

Comme nous le verrons dans la rubrique sur les entreprises et startups du calcul quantique, celles qui se sont spécialisées dans la QML ne manquent pas. En général, elles fournissent des outils de développement et des moyens pour créer des preuves de concept de QML. Mais leur gagne-pain est souvent la réalisation de projets de machine learning sur calculateurs classiques ou au mieux des algorithmes « quantum inspired ». Il faut bien vivre en attendant de disposer de processeurs quantiques plus puissants !

Dans le registre de l'IA, le projet européen H2020 **Quromorphic** lancé en juillet 2019 vise à créer un processeur quantique dédié à l'exécution de réseaux de neurones s'inspirant du fonctionnement du cerveau[419]. Dans l'esprit, on sent un lien de parenté avec le très controversé flagship Européen Humain Brain Project qui est piloté par le chercheur suisse Henri Markram. Quromorphic implique IBM Zurich, ETH Zurich, TUDelft, Volkswagen et des Universités espagnoles et allemandes.

---

[413] Voir Quantum embeddings for machine learning par Seth Lloyd, janvier 2020 (11 pages). Source de l'illustration : Quantum Computing Applications, présentation de Iordanis Kerenidis de Qc-Ware au Lab Quantique, 2 juin 2020 (52 slides).

[414] L'astuce est expliquée dans Quantum Neuron: an elementary building block for machine learning on quantum computers, de Yudong Cao, Gian Giacomo Guerreschi et Alan Aspuru-Guzik en 2017 (30 pages).

[415] Voir Quantum Algorithms for Deep Convolutional Neural Network, par Iordanis Kerenidis et al, 2020 (36 pages) qui est évoqué dans Deep Convolutional Neural Networks for Quantum Computers par Jonas Landman, 2020.

[416] Voir par exemple Continuous-variable quantum neural networks, par Nathan Killoran et Al, juin 2018 (21 pages). Le système utilise des circuits quantiques à variables continues.

[417] Voir Quantum Machine Learning: Algorithms and Practical Applications, Iordanis Kerenidis, Qc-Ware, Q2B Conference, décembre 2019 (34 slides) qui inventorie quelques gains potentiels d'algorithmes de QML.

[418] Ces techniques seront concurrencées par les futurs processeurs neuromorphiques à base de memristors qui permettront de faire converger plus rapidement les réseaux par rétropropagation. Les memristors permettront de placer au même endroit dans un circuit les fonctions de calcul du neurone et la mémoire associée, accélérant de plusieurs ordres de grandeur l'accès à celle-ci lors des calculs. C'est encore un domaine de recherche, opéré notamment par Julie Grollier du laboratoire du CNRS situé chez Thalès TRT à Palaiseau, et que j'ai pu rencontrer en mai 2018.

[419] Voir Quantum computer: We're planning to create one that acts like a brain de Michael Hartmann et Heriot-Watt leads on next-gen computers, novembre 2018. Le projet est piloté par Michael Hartmann de l'IPaQS (Institute of Photonics and Quantum Sciences) de l'Université Heriot Watt au Royaume Uni, conjointement avec l'ETH Zurich, l'Université de Delft (Pays-Bas), l'Université Basque (Espagne), IBM Zurich et Volkswagen (Allemagne). 2,2M€ issus du programme FET Open ont été attribués au projet par la Commission Européenne (détails). Mon interprétation ? L'objectif du projet a été accomodé à la sauce de la science-fiction pour récupérer des financements communautaires. Le reste est de la photonique.

Vus les participants, on peut imaginer que cela reposera sur des qubits supraconducteurs. Le projet a été financé à hauteur de 2,9M€ en 2019 et doit se terminer en 2022. Ce projet semble quelque peu survendu en l'état, pour récupérer ces financements européens[420].

Bon, de là à utiliser ces algorithmes dans la robotique[421], il faudra patienter un peu ! Ce n'est plus de la technologie, c'est de la science-fiction et du *click-bait*. C'est l'un des nombreux exemples d'escroquerie intellectuelle quantique sur lesquels nous reviendrons en évoquant les « fumisteries quantiques » à la fin de cet ebook.

Nous avons jusqu'à présent survolé la QML. Mais le machine learning classique peut-être utile à la physique et au calcul quantiques. Nous le verrons concernant Google qui a par exemple utilisé un algorithme de deep learning pour optimiser le plan de fréquences micro-ondes de contrôle des qubits du processeur Sycamore qui leur a permis d'atteindre la fameuse et controversée « suprématie quantique » en septembre 2019.

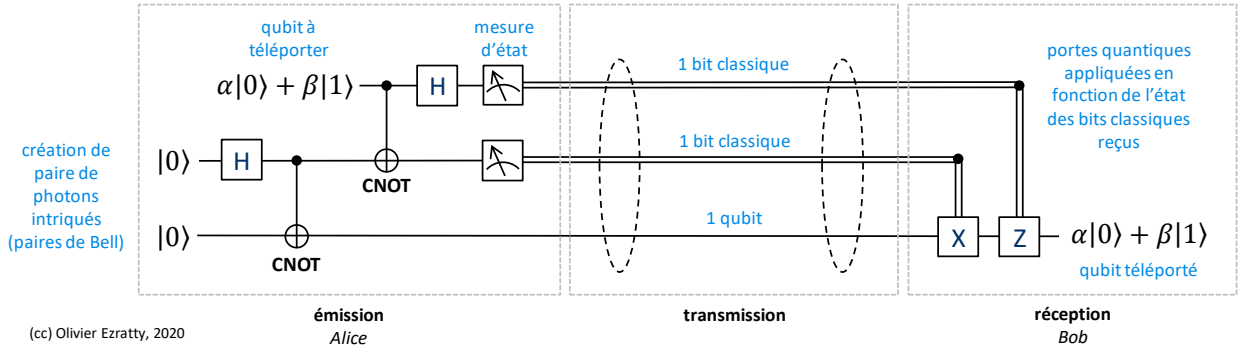
Le machine learning peut aussi servir à modéliser et simuler le fonctionnement de la matière condensée, avec un impact sur la mise au point de qubits divers, notamment supraconducteurs[422].

Notons enfin l'existence d'une association qui fait du prosélytisme sur le champ de l'IA et de l'informatique quantique, la fondation **IAIQT** basée en Suisse.

Téléportation

L'un des algorithmes quantiques à base de portes quantiques le plus intriguant est celui de la téléportation de qubit. Cet algorithme a été créé par Charles H. Bennett (USA), Gilles Brassard (Canada), Claude Crépeau (Canada), Richard Jozsa (USA), Asher Peres (Israël) et William K. Wootters (USA) en 1993[423].

Il permet de téléporter l'état d'un qubit d'un endroit à un autre. Le principe de cet algorithme consiste à exploiter un canal d'intrication quantique préexistant pour transmettre l'état d'un qubit d'une extrémité à l'autre de ce canal. La téléportation expoite la transmission de deux bits classiques dans le protocole qui servent à reconstituer le qubit envoyé à l'arrivée. De ce fait, la transmission de ce dernier ne peut pas avoir lieu plus vite que la lumière.



Du fait du théorème de non clonage quantique, cette téléportation est un « move » et pas un « copy » (ou un « cut & paste » au lieu d'un « copy & paste »). L'état du qubit transféré est ainsi détruit de son point de départ[424]. La principale utilisation de cet algorithme et de ses nombreuses variantes se situe dans les systèmes de cryptographie quantique que nous découvrirons plus loin.

---

[420] Voir Quantum computer: we're planning to create one that acts like a brain, janvier 2019.

[421] Comme décrit dans The Rise of Quantum Robots de Daniel Manzano (avril 2018).

[422] Voir Machine learning & artificial intelligence in the quantum domain par Vedran Dunjko et Hans J. Briegel, 2017 (106 pages).

[423] Voir Teleportation as a quantum computation de Gilles Brassard, 1996 (3 pages).

[424] Voir Quantum Teleportation in a Nutshell de Fabian Kössel, 2013 (35 slides).

Elle pourrait également se manifester plus tard dans des architectures distribuées d'ordinateurs quantiques. A noter que cet algorithme peut être testé en local dans un calculateur quantique, comme c'est proposé par IBM dans ses Q Systems avec Qiskit. On télétransporte alors un qubit en faisant un peu du surplace !

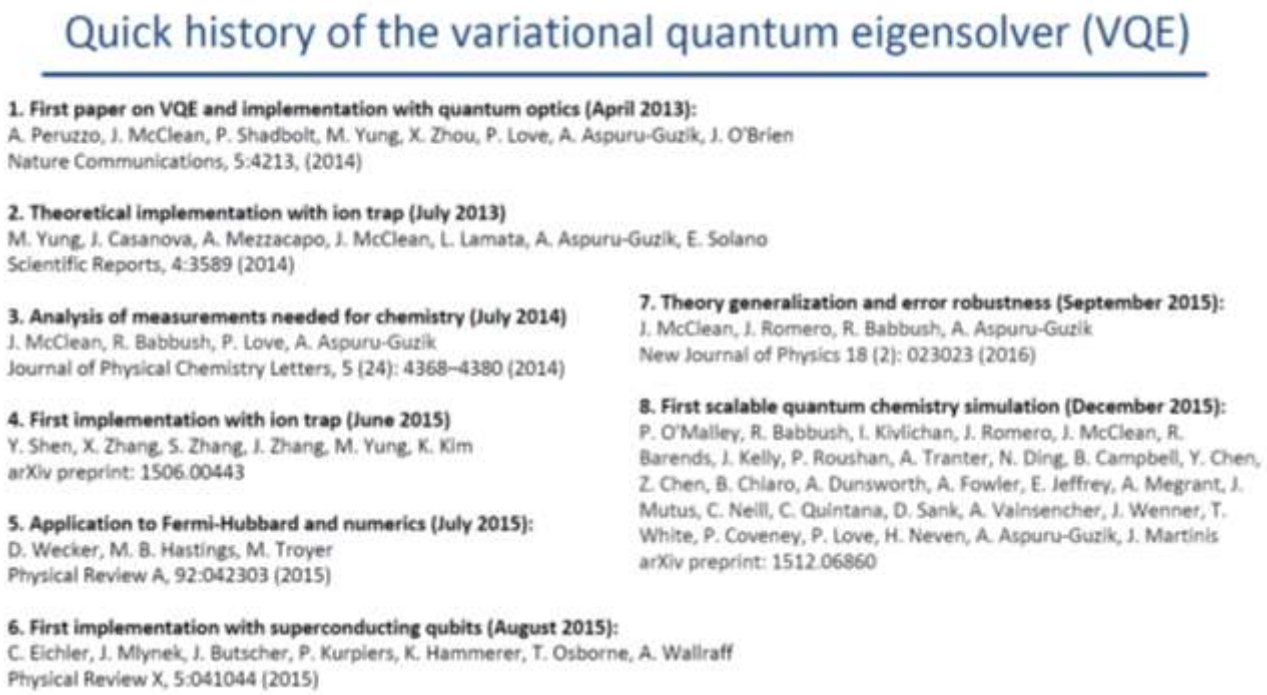
Algorithmes hybrides

Une autre branche d'algorithmes quantiques se développe depuis quelques années, celle des algorithmes hybrides qui associent une composante traditionnelle et une composante quantique. A vrai dire, tout algorithme quantique a besoin d'un soutien d'un ordinateur classique pour le pilotage de l'ordinateur quantique et l'activation de ses portes quantiques[425].

Les algorithmes hybrides répartissent les calculs de part et d'autre et font en sorte que la partie quantique de l'algorithme ne couvre que la partie qui ne peut pas l'être dans la partie classique. A terme, il est probable qu'une majorité d'algorithmes quantiques seront hybrides[426].

Ces algorithmes hybrides pourront être mis en œuvre dans des outils de développement et langages à même de contrôler à la fois la partie classique et la partie quantique d'un supercalculateur ou d'un système distribué.

C'est notamment le cas du modèle de programmation **XACC** (eXtreme-scale ACCelerator)[427]. Il permet de développer un code hybride qui tient compte des caractéristiques du calculateur quantique, notamment de son taux d'erreurs. Il s'interface avec les modèles de programmation d'ordinateurs quantiques d'IBM et Rigetti.



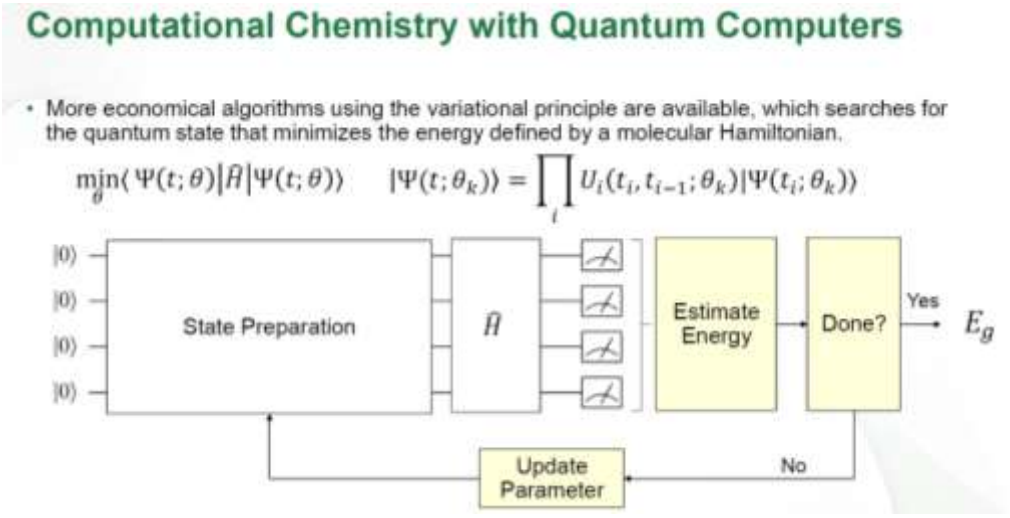
[425] Voir A Hybrid Quantum-Classical Approach to Solving Scheduling Problems, Tony T. Tran et al, (9 pages), Hybrid Quantum Computing Apocalypse 2018 (6 pages) selon lequel les Chinois auraient réussi à faire tourner un fermion de Majorana, The theory of variational hybrid quantum-classical algorithms Jarrod McClean et al (23 pages).

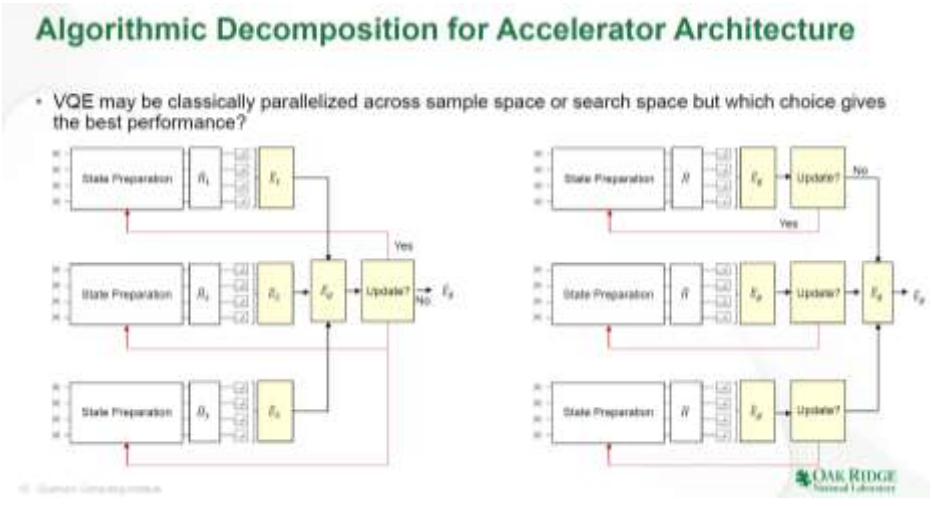
[426] A ce titre, les brevets d'algorithmes quantiques déposés par Accenture sont inquiétants car ils sont à la limite des *patent trolls*. Voir par exemple le brevet Multi-state quantum optimization engine, USPTO 10,095,981B1, validé en octobre 2018 (20 pages). Un second brevet validé en avril 2019 concerne une solution de machine learning qui aide un algorithme à décider quelle partie exécuter en classique et quelle partie exécuter en quantique. C'est l'USPTO 10,275,721.

[427] Voir Hybrid Programming for Near-term Quantum Computing Systems, de A. J. McCaskey et al, du laboratoire d'Oak Ridge, 2018 (9 pages).

L'un des algorithmes pouvant être traité dans des architectures hybrides est le **Quantum Approximate Optimization Algorithm (QAOA)**, créé par Edward Farhi en 2014. C'est un algorithme d'optimisation combinatoire notamment utilisé dans des problèmes de graphes et de gestion de coupes (MaxCut). Il présente l'intérêt de requérir une faible profondeur de portes quantiques[428].

L'autre algorithme hybride le plus prisé est le **Variational Quantum Eigensolver** (VQE)[429]. Créé en 2013[430], il sert à la recherche d'un minimum énergétique d'un système complexe. Il sert notamment à faire de la simulation de structures de molécules dans la chimie inorganique et organique. Il combine une partie classique qui détermine un point de départ approximatif et une partie quantique qui affine le résultat. Il peut même servir pour l'entraînement d'un modèle de machine learning[431]. Ce type d'algorithme présente l'avantage de pouvoir être traité dans des architectures distribuées avec plusieurs processeurs classiques et quantiques. Le gain du VQE provient de la capacité du calcul quantique à explorer l'espace des possibles en parallèle. L'approche est itérative et la vitesse de convergence dépendant de facteurs liés au système physique simulé, à la modélisation numérique ainsi qu'à la qualité recherchée du résultat.





[428] Voir An Introduction to Quantum Optimization Approximation Algorithm de Qingfeng Wang et Tauqir Abdullah, décembre 2018 (16 pages) et QAOA: Quantum Approximate Optimization Algorithm de Peter Shor (25 slides).

[429] Source des schémas : Quantum Computing for Scientific Discovery: Methods, Interfaces, and Results de Travis Humble du Quantum Computing Institute, Oak Ridge National Laboratory, mars 2018 (47 slides).

[430] L'historique vient de Towards an experimentally viable variational quantum eigensolver with superconducting qubits, 2016 (18 slides).

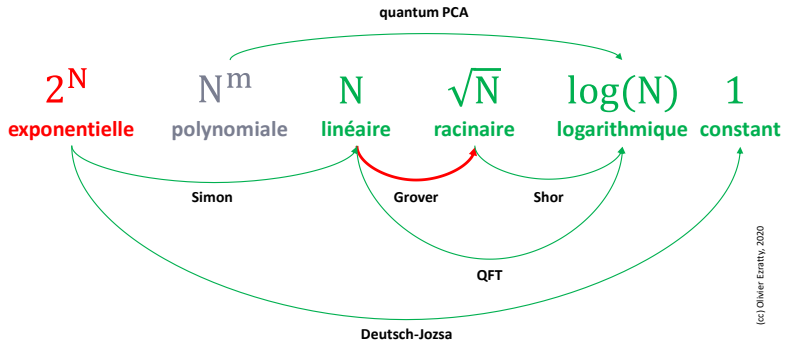
[431] Il est maintenant possible de se passer de la partie classique de l'algorithme comme expliqué dans An adaptive variational algorithm for exact molecular simulations on a quantum computer, de Sophia Economou et al, 2019 (9 pages).

Gains de performance quantiques

Pour conclure, j'ai consolidé le schéma *ci-dessous* qui résume les gains de performance de quelques-uns des algorithmes déterministes que nous venons de voir. Les niveaux de complexité (exponentielle, polynomiale, linéaire, …) sont génériques.

Les niveaux précis de complexité de chaque algorithme sont associés à ces classes de manière approximative.

Ainsi, N*log(N) qui est la complexité d'une transformée de Fourier classique est linéaire car N grandit bien plus vite que log(N) et log(N) puissance 3 est une complexité de niveau logarithmique (pour l'algorithme de Shor et une QFT, Quantum Fourier Transform).



Attention au fait qu'un gain exponentiel est aussi obtenu lorsque l'on passe de N ou Racine de N vers log(N). Une QFT génère donc un gain similaire à l'algorithme de Deutsch-Jozsa.

Complexité	n	$n \log_2 n$	n^2	n^3	1.5^n	2^n	$n!$
$n = 10$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	4 s
$n = 30$	< 1 s	< 1 s	< 1 s	< 1 s	< 1 s	18 min	10^{25} ans
$n = 50$	< 1 s	< 1 s	< 1 s	< 1 s	11 min	36 ans	∞
$n = 100$	< 1 s	< 1 s	< 1 s	1s	12,9 ans	10^{17} ans	∞
$n = 1000$	< 1 s	< 1 s	1s	18 min	∞	∞	∞
$n = 10000$	< 1 s	< 1 s	2 min	12 jours	∞	∞	∞
$n = 100000$	< 1 s	2 s	3 heures	32 ans	∞	∞	∞
$n = 1000000$	1s	20s	12 jours	31,710 ans	∞	∞	∞

Les échelles de temps sont plus parlantes dans le tableau *ci-dessus*[432] :

L'idéal en gains de performances est de traverser plusieurs classes de complexité, et surtout, à partir d'un problème exponentiel. Dans la pratique, les principaux algorithmes sautent une à deux classes de complexité mais pas forcément à partir de la classe des problèmes exponentiels. Mais mon schéma est trompeur. N peut aussi croitre de manière exponentielle selon la taille d'un problème. L'exemple classique est celui de l'algorithme de Shor.

Le point de départ est un N qui est en fait une taille de clé RSA qui elle-même est évaluée en puissance de 2. Une clé de 1024 bits fait 2^{1024}. Si on passe de 2^{256} à 2^{1024}, la croissance de la taille de la clé est exponentielle. Et là, on obtient donc avec l'algorithme de Shor un gain de performance exponentiel en passant d'une racine carrée de 2^{1024} à $\log(2^{1024})$, soit 1024 (en log base 2) ! On passe donc de 2^{512} à 1024, ce qui représente bien un gain parfaitement exponentiel.

L'algorithme de Deutsch-Jozsa a la particularité de traverser tous les niveaux de complexité mais nous avons vu qu'il n'avait malheureusement pas d'application pratique connue.

Il faut aussi intégrer le fait que la complexité de certains problèmes peut être contournée sur des ordinateurs classiques avec des approches probabilistes qui permettent aussi de réduire d'un ou plusieurs étages le niveau de complexité de problèmes exponentiels.

En conclusion, les algorithmes quantiques sont séduisants mais ils ne sont pas pour autant toujours la panacée.

Ceci doit aussi tenir compte du phénomène d'émulation que génère le calcul quantique sur le calcul classique. Chaque nouvelle performance quantique titille les créateurs d'algorithmes classiques pour supercalculateurs qui veulent en créer des équivalents pour ces machines.

---

[432] Source du tableau : Complexité en temps, Ecole Polytechnique (25 pages).

C'est ce qu'a fait Toshiba en 2019 avec un algorithme d'optimisation classique 10 fois plus performant que l'état de l'art. Mais un gain linéaire de x10 n'est pas un progrès exponentiel[433].

Ceci étant dit, même si un gain polynomial est considéré comme classique et mineur dans les théories de la complexité, il peut selon les applications avoir une valeur pratique non négligeable et rendre le calcul quantique attractif, sans passer par le Graal de l'accélération exponentielle.

Certification d'algorithmes

La vérification et la certification d'algorithmes quantiques et des résultats de leur utilisation est un nouveau sujet important. La factorisation de nombres entiers est évidemment facile à vérifier. Mais lorsqu'un algorithme quantique sert à simuler des interactions physiques comme celles d'atomes dans des molécules, c'est moins évident.

Des travaux théoriques montrent que l'on peut prouver de manière polynomiale qu'un résultat d'algorithme quantique est exact[434]. Malheureusement, par contre, on ne peut pas expliquer dans le détail l'origine du résultat en le décomposant. Ni prouver que le résultat trouvé, aussi valide soit-il, soit le meilleur de tous s'il y en a plusieurs de bons.

Voir aussi Quantum cloud computing with self-check, de Rainer Blat & Al, mai 2019, qui évoque des calculs de simulation quantique sur 20 qubits à ions piégés avec un contrôle des résultats sur l'ordinateur quantique aussi rapide que sur PC.

L'autre point clé est de s'assurer dans le cas de l'usage d'un ordinateur quantique distant, que le résultat récupéré correspond bien au calcul soumis et qu'un intrus ne s'est pas interposé dans l'histoire ni n'a pu altérer le calcul du côté de l'ordinateur quantique. L'une des méthodes consiste à s'appuyer sur le concept du **blind computing** développé en 2009 par Anne Broadbent, Joseph. Fitzsimons et Elham Kashefi[435].

Le **CEA List** annonçait en juin 2020 avoir créé QBrick, un environnement de spécification, programmation et vérification formelle d'algorithmes quantiques. Ils avaient l'habitude de faire cela pour des systèmes embarqués critiques où la certification par preuve formelle est très importante. Ils investissent maintenant le champ de la programmation quantique et ont expérimenté leur modèle avec la QPE, l'algorithme de phase quantique qui entre dans celui de Shor pour la factorisation de nombres entiers. Ce sont des travaux qui associent le laboratoire LRI commun à l'Université Paris-Saclay et CentraleSupelec[436].

---

[433] Toshiba Promises Quantum-Like Advantage on Standard Hardware par Tiffany Trader, 2020 qui fait référence à Combinatorial optimization by simulating adiabatic bifurcations in nonlinear Hamiltonian systems par Hayato Goto et al, avril 2019 (9 pages).

[434] Voir How to Verify a Quantum Computation d'Anne Broadbent, 2016 (37 pages) qui démontre que tous les résultats d'algorithmes quantiques peuvent être vérifiés avec des algorithmes classiques polynomiaux en réalisant plusieurs tests et en chiffrant les données en entrée. Je n'ai pas compris plus que cela de la méthode ! Voir aussi Verification of quantum computation: An overview of existing approaches, Alexandru Gheorghiu, Theodoros Kapourniotis et Elham Kashefi, 2018 (65 pages).

[435] Voir Universal blind quantum computation de Anne Broadbent, Joseph Fitzsimons et Elham Kashefi, 2008 (20 pages) et la présentation associée (25 slides).

[436] Voir Toward certified quantum programming par Sébastien Bardin, François Bobot, Valentin Perelle, Christophe Chareton et Benoît Valiron, 2018 (4 pages).

Complexité

Dans la partie précédente, nous avons fait le tour des principaux algorithmes quantiques connus, de leurs domaines d'applications et de leur performance relative.

Le calcul quantique est parfois présenté comme étant une solution miracle aux limites du calcul sur supercalculateurs. Il permettrait de résoudre des problèmes dits "intractables" sur des ordinateurs classiques. Mais au juste, quelle est la nature des problèmes qui peuvent être résolus avec un ordinateur quantique et qui ne peuvent pas l'être avec des ordinateurs classiques ? Et surtout, quelles sont les limites des ordinateurs quantiques ? Comment se situent-elles par rapport aux limites de l'intelligence artificielle ?

Nous allons voir que ces limites sont plutôt floues et mouvantes. Elles sont traitées dans un champ complet et méconnu de la science, celui des **théories de la complexité**. C'est un monde on ne peut plus abstrait où les spécialistes parlent un langage abscons fait de P, NP, BQP et autres complétudes. Ils gambergent depuis près d'un demi-siècle pour déterminer si **P = NP ou pas**, une question aussi importante que le rôle exact du nombre 42 dans le fonctionnement de l'Univers. C'est la science des classes de complexité de problèmes. Derrière ces mathématiques de la complexité se cachent des considérations techniques mais aussi philosophiques fondamentales pour l'Homme et son désir de toute puissance.

Les classes de complexité de problèmes sont des poupées russes plus ou moins emboitées les unes dans les autres. Elles tournent surtout autour de la question de la montée en charge du temps de résolution des problèmes en fonction de leur taille, mais aussi de l'espace mémoire nécessaire.

On ne sait résoudre dans un temps raisonnable que les problèmes dits polynomiaux ou plus simples que les polynomiaux. Un temps polynomial est proportionnel à une puissance donnée de N, N étant la dimension du problème à résoudre. L'informatique quantique permet dans certaines conditions de résoudre certains problèmes dits exponentiels, qui croissent de manière exponentielle avec leur taille. Au-delà se situent divers problèmes inaccessibles qui relèvent souvent de simulations complexes ou de résolutions par force brute. Les ordinateurs quantiques ne pourront pas résoudre tous les problèmes qui nous passeront par la tête, même le jour où l'on pourra aligner des gazillions de qubits avec un taux d'erreur infinitésimal.

Ces limites ont un impact indirect sur les prévisions concernant la création d'intelligences artificielles omniscientes capables de transcender le raisonnement humain et de résoudre tous les problèmes. Ces hypothétiques AGI (Artificial General Intelligence) seront limitées par les données et concepts qui les alimentent et par l'impossibilité de résoudre certains problèmes complexes, notamment ceux qui relèvent de la prévision et de la simulation et qui reposent sur la force brute plutôt sur des astuces algorithmiques permettant d'aboutir rapidement à la solution.

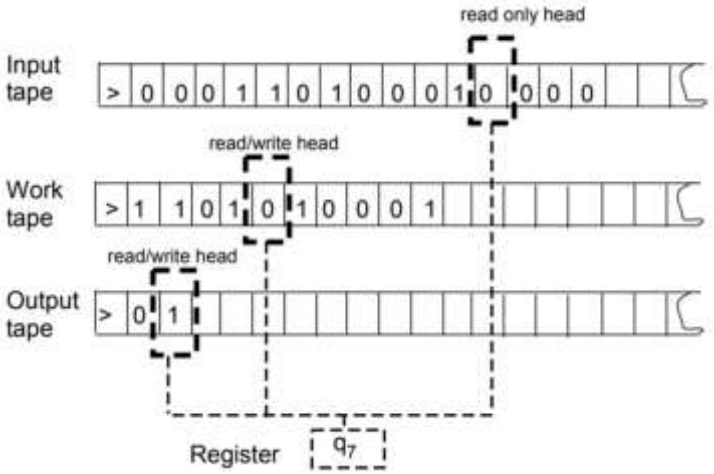
Le calcul ultime n'existe donc pas encore et l'Homme continuera à faire face à l'impossible et ne pourra pas résoudre tous les problèmes complexes qu'il rencontrera ! Le calcul quantique ne permet pas de dominer la nature et de mettre en équation l'Univers et d'en prévoir le fonctionnement au quantum près. Le hasard et l'imprévu continueront de jouer un rôle dans un monde très indéterministe et c'est tant mieux comme cela. C'est une petite leçon d'humilité pour l'Homme que de passer son temps à découvrir des limites scientifiques à ses besoins de contrôle !

Classes de complexité de problèmes

Pour rentrer dans ce sujet, il faut en passer par définir les grandes classes de problèmes par niveau de complexité. Elles font partie d'un champ entier de la logique et des mathématiques qui agite un petit monde de spécialistes. Me voilà donc une fois encore amené à devoir simplifier la complexité, et cette fois-ci, au sens littéral du terme.

Dans la pratique, les classes de complexité décrivent aussi bien des problèmes que l'on résout par force brute en testant plusieurs combinatoires (problèmes SAT) qu'avec des équations mathématiques complexes (différentielles, matricielles, …) permettant d'aboutir directement à la solution comme on le fait pour prédire la position des planètes en s'appuyant sur les lois de la mécanique newtonienne ou prédire le minimum énergétique d'un système complexe.

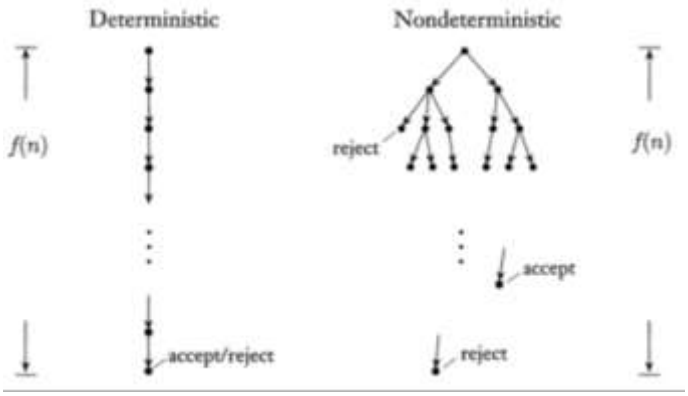
Les classes de problèmes font appel à une notion de machines déterministes et non déterministes de Turing. De quoi s'agit-il ? Les machines de Turing sont les modèles conceptuels d'ordinateurs créés par Alan Turing avant la seconde guerre mondiale. Elles modélisent les traitements informatiques en s'appuyant sur la notion de programmes et de données, incarnées par des rouleaux de papier continus, le premier pour le programme, le second pour les données en entrée et le troisième pour générer les résultats (*ci-contre*[437]).



Des étudiants d'un master de l'ENS Lyon ont réalisé une machine de Turing en Lego en 2012 à l'occasion du centenaire de la naissance d'Alan Turing (vidéo) et ce n'était pas la seule du genre (vidéo) ! Un Anglais en a aussi réalisé une en bois en 2015 (vidéo). Voilà de quoi s'éduquer ludiquement !

Le modèle théorique de Turing est utilisé depuis longtemps pour définir les classes de problèmes que l'on peut résoudre ou pas avec un ordinateur. Les ordinateurs sont tous métaphoriquement des machines de Turing, reproduisent cette logique en lisant des instructions de programmes et en gérant les données en mémoire vive (RAM) ou en stockage persistent (disque dur, SSD, …). Est associée à la notion de machine de Turing celle de la **thèse de Church-Turing**, des noms d'Alonzo Church et Alan Turing selon laquelle il existe une équivalence entre problèmes de calcul réalisable à la main et avec des ressources non limitées, ceux qui sont traitables avec une machine de Turing et ceux qui peuvent être résolus avec des fonctions dites récursives.

Dans une machine déterministe, la séquence des actions à réaliser est prédéfinie et séquentielle. Dans le modèle conceptuel de machine de Turing non déterministe, les règles de calcul peuvent imposer de réaliser plusieurs opérations différentes pour chaque situation évaluée. En gros, en explorant plusieurs voies en parallèle et en cherchant une réponse positive à une composante d'algorithme et en fermant des boucles de tests parallèles une fois les sous-solutions trouvées.



C'est plus ou moins le modèle de navigation dans l'arbre de décision de la version 2017 d'AlphaGo, dite AlphaGo Zero, qui évalue dans un réseau de neurones différents scénarios de jeu. Une machine non déterministe augmente la combinatoire de calcul par rapport à une machine déterministe. Et cette combinatoire passe de polynomiale à exponentielle.

[437] Source du schéma : Computational Complexity: A Modern Approach, Sanjeev Arora et Boaz Barak, 2007 (489 pages). C'est un bon document de référence sur les théories de la complexité.

La force d'AlphaGo Zero est d'utiliser des réseaux de neurones en quelque sorte récursifs pour réduire le nombre de branches de l'arbre de décision à tester pour sortir partiellement de la fatalité exponentielle de ce jeu.

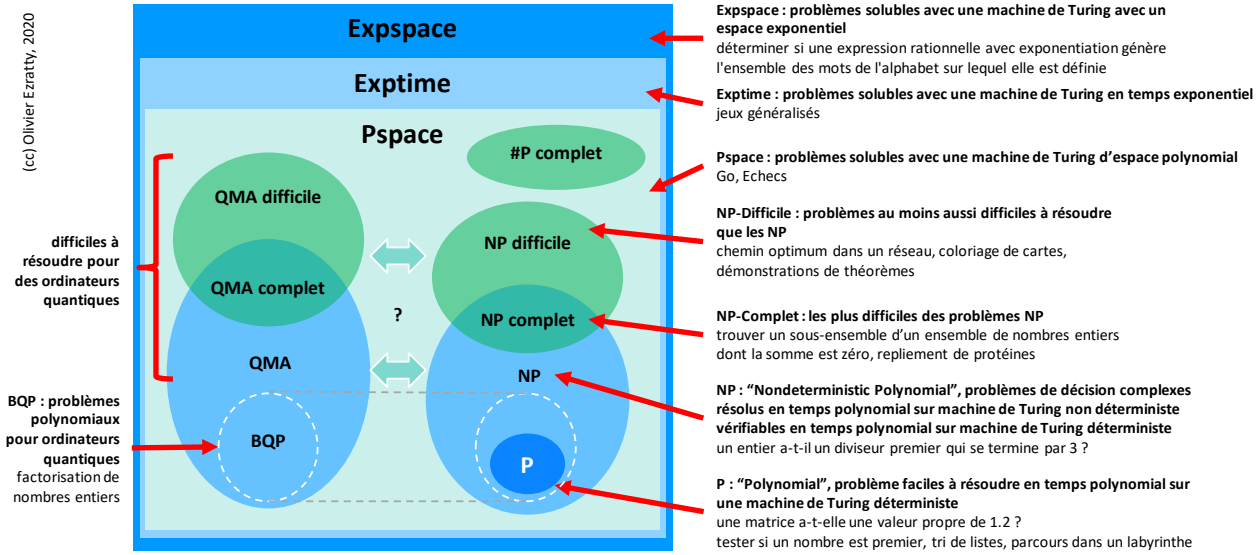
Classes de complexité génériques

Le niveau de complexité s'entend vis à vis du temps de calcul nécessaire et de l'espace mémoire nécessaire pour ces calculs.

On est souvent bloqué par le temps de calcul avant de l'être par la capacité mémoire. Mais certains problèmes comme celui de l'ordonnancement atteignent des limites de mémoire avant des limites de calcul.

L'association d'un problème à une classe de complexité est liée à la performance du meilleur algorithme connu pour résoudre ledit problème.

Les niveaux de classes de problèmes dans les théories de la complexité reposent souvent sur des modèles de boite noire ou d'oracles à qui un système pose des questions et obtient des réponses en fonctions des données fournies. C'est une logique de "force brute" et de scan d'hypothèses. La combinatoire à tester est plus ou moins grande selon les classes de problèmes.



Voici donc ces classes par niveau croissant de complexité sachant que nous passerons le plus de temps sur les classes NP et NP Complet.

L : ou LSPACE, ou DLOGSPACE, qui définit la classe des problèmes que l'on peut résoudre à une échelle logarithmique de mémoire consommée et sur une machine de Turing déterministe, soit, sur un ordinateur traditionnel. C'est le genre de classe idéale ! La complexité de calcul diminue rapidement avec la taille du problème. Malheureusement, très peu de problèmes complexes sont dans cette classe-là. On y trouve notamment les requêtes dans des bases de données relationnelles préalablement indexées, les recherches de séquences d'ADN et d'une manière générale les techniques de recherche utilisant des pointeurs et qui optimisent l'utilisation de la mémoire des ordinateurs.

NL : la classe des problèmes résolus à une échelle logarithmique sur une machine non-déterministe. Les logiciens cherchent toujours à savoir si si L=NL ! Cela pourrait durer quelque temps. Cela les occupe moins que P=NP.

P : qui définit les problèmes que l'on peut résoudre avec un temps qui croit de manière polynomiale avec le nombre de données à traiter et sur une machine déterministe. Si N est la taille du problème, la durée de traitement est proportionnelle à N puissance M, M étant un entier, si possible 2. C'est un problème facile à résoudre. Il est dit "tractable".

Cela comprend le tri de listes, la validation de l'existence d'un chemin dans un graphe, la recherche d'un chemin minimum dans un graphe, la multiplication de matrices ou l'évaluation d'un nombre pour savoir s'il est premier.

BPP : est une classe de problèmes qui peuvent être résolus par des approches aléatoires ("Bounded-Error Probabilistic Polynomial-Time"). Il semblerait que BPP=P mais ce n'est pas encore démontré.

NP : décrit la classe des problèmes dont il est facile de vérifier la validité d'une solution, à savoir que celle-ci peut être réalisée en un temps polynomial par une machine déterministe. L'autre définition de la classe est qu'elle contient les problèmes dont le temps de résolution est polynomial sur une machine non déterministe.

Ces problèmes plus complexes ont un temps de calcul au minimum exponentiel lorsque la méthode utilisée est dite naïve, pour tester toutes les hypothèses possibles. Ils sont dits intractables. En pratique, ce sont des problèmes particulièrement adaptés aux ordinateurs quantiques du fait de leur capacité à évaluer en parallèle 2 puissance N combinaisons.

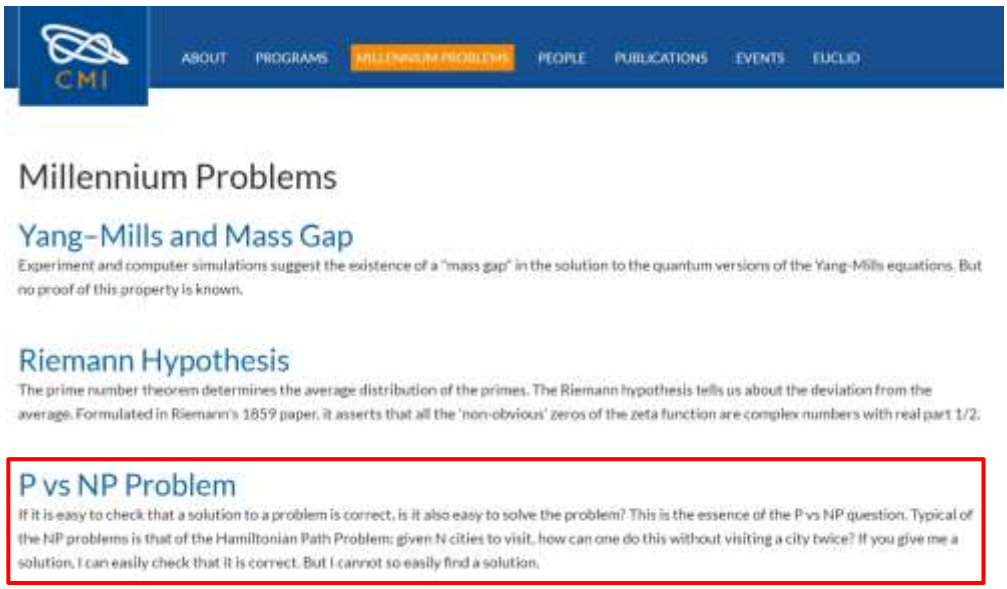
Quelques exemples de problèmes NP : l'arbre de Steiner pour déterminer si un réseau électrique permet de relier un nombre de maison à un certain prix, vérifier qu'une séquence d'ADN se retrouve dans plusieurs gênes et la distribution de tâches à différents agents pour minimiser le temps de leur réalisation. Les exemples théoriques des cours de complexité ont l'air de relever de problèmes futiles, nous en verrons quelques-uns plus tard. Mais côté métiers, ces problèmes ont des équivalents très concrets dans la logistique, la planification, la production, les transports, les télécoms, les utilities, la finance ainsi que dans la cryptographie.

A noter qu'un problème "décidable", c'est à dire qui requiert d'explorer un espace fini d'options, n'est pas forcément faisable d'un point de vue pratique. Même s'il peut être résolu en un temps fini, sa résolution peut prendre un temps trop long. Un problème exponentiel a une solution élégante si on peut en trouver une qui ait une durée polynomiale voir, dans le meilleur des cas, linéaire. Les temps polynomiaux *scalent* mieux que les temps exponentiels !

Un gros débat a cours depuis 1956 (Kurt Gödel) pour savoir si la classe P égale la classe NP. Si P = NP, il serait aussi simple de trouver un résultat quand on sait aussi le vérifier simplement. Le consensus général est que P n'est pas égal à NP. La démonstration de P<>NP ou de son contraire fait partie de l'un des sept défis mathématiques du Clay Mathematics Institute lancés en 2000 chacun dotés d'un prix de $1M (*ci-dessus*).

Parmi ces défis, on trouve la démonstration des équations de Navier-Stokes sur la mécanique des fluides et celle de l'hypothèse de Riemann sur la distribution des nombres premiers. Voilà de beaux problèmes à résoudre pour une hypothétique AGI (Artificial General Intelligence) capable de dépasser l'Homme dans sa capacité de conceptualisation. Et $7M à la clé, si le principe de l'AGI était vérifié, à savoir sa capacité à résoudre n'importe quel problème, à supposer que celui-ci soit décidable ! Ce qui se relie aux classes de complexité, sachant qu'en gros, jusqu'à 2-EXPTIME (définie plus loin), les problèmes sont décidables et ceux qui sont en dehors sont indécidables.

Le chercheur brésilien **André Luiz Barbosa** a publié en 2010 P ≠ NP Proof (25 pages) tout comme un papier invalidant le théorème de Cook selon lequel un problème booléen SAT est NP-Complet, The Cook-Levin Theorem is False, 2010 (11 pages). Il ne fait visiblement pas l'unanimité, ses travaux n'étant ni cités, ni repris.



$1M à la clé !

Du côté P vs NP, la formulation du défi à relever donne un exemple d'un tel problème : vous devez allouer 50 chambres de deux étudiants à 400 candidats mais certains candidats ne doivent pas cohabiter dans la même chambre. La combinatoire de choix des 100 étudiants parmi 400 est monstrueusement énorme, donc le problème n'est pas traitable facilement avec un supercalculateur et avec de la force brute. C'est bien un problème NP car une solution donnée est facile à vérifier car il suffit de vérifier qu'aucune des chambres ne contient une paire d'individus interdite. C'est un peu la théorie du tout ou du rien car si P = NP, tous les problèmes NP ont une solution efficace polynomiale. Si P ≠ NP, aucun des problèmes NP n'a de solution efficace « pure »[438].

La définition des classes de problèmes NP et NP-Complet est relativement récente[439]. J'ai parcouru un grand nombre de publications pour m'y retrouver mais elles étaient assez redondantes dans l'ensemble.

NP Complet : ils se définissent selon Richard Karp comme les problèmes dans lesquels les autres problèmes NP peuvent être réduits de manière polynomiale. A fortiori, ils n'ont pas de solution P (polynomiale) connue.

Ils sont encore non accessibles aux ordinateurs quantiques. C'est dans cette classe que l'on trouve les problèmes de logique booléenne de type SAT ou 3SAT dont je vous passe les détails car je risquerai de vous perdre et de me perdre par la même occasion ! Plus de 3000 problèmes NP-Complets sont identifiés à ce jour (liste).

On y trouve notamment le problème du remplissage optimum du coffre de la voiture lorsque l'on part en vacances ou lorsque l'on revient du Noël dans sa famille avec une flopée de cadeaux. Et puis le **problème du sac à dos** consistant à le remplir de manière optimale avec un jeu d'objets, pour obtenir la plus grande charge et sans dépasser un poids maximum ("Bin packing")[440].

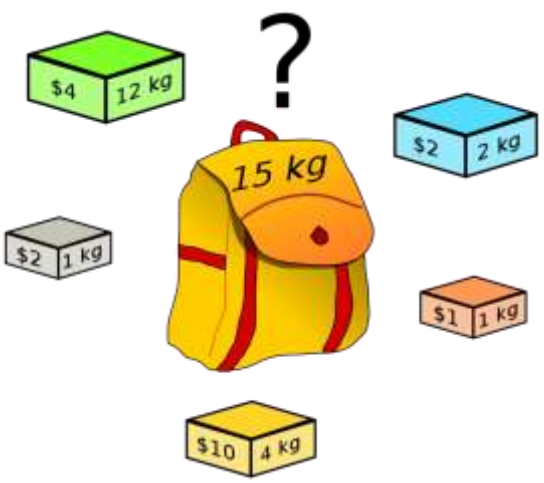
Il comprend aussi le **problème de la somme de sous-ensemble** consistant à trouver un sous-ensemble d'un ensemble de nombres entiers dont la somme est égale à un entier arbitraire.

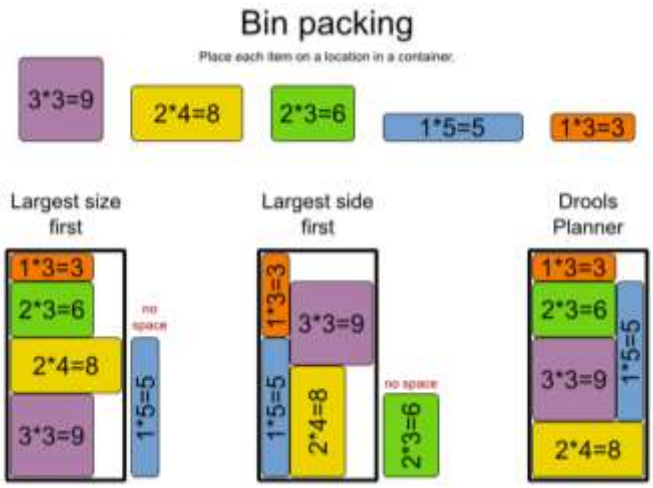
---

[438] La méthode classique de contournement consiste à résoudre ces problèmes vias des heuristiques qui permettent d'obtenir une solution approximative, donc qui n'est pas forcément optimale, et notamment via des approches probabilistes.

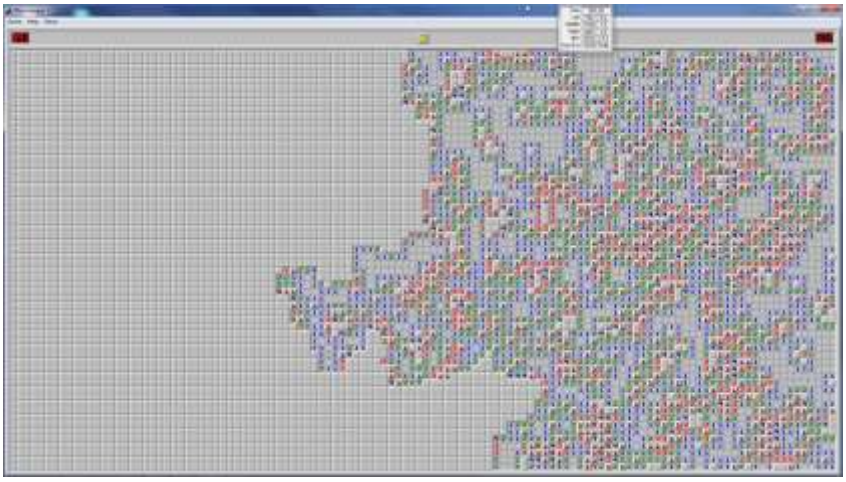
[439] Elle est issue de The complexity of theorem-proving procedures de Stephen Cook de l'Université de Toronto, 1971 (8 pages), mieux vulgarisé dans An overview of computational complexity (8 pages) et Reducibility about combinatorial problems, de Richard Karp, 1972 (19 pages) ainsi que dans Complexité et calculabilité d'Anca Muscholl du LaBRI, 2017 (128 slides).

[440] Sources des illustrations : Wikipedia et Stackoverflow.





Le **problème du démineur** consiste à localiser des mines cachées dans un terrain avec pour seules indications le nombre de mines dans les zones adjacentes et le nombre de mines total dans le champ. Le tout sans les faire exploser. C'est un jeu bien connu des utilisateurs de Windows, lancé en 1989 [441]! Il semblerait enfin que la simulation du repliement de protéines complexes soit un problème NP-Complet[442].



Ce serait donc un problème potentiellement très difficile à résoudre avec un ordinateur quantique avec de grandes protéines.

Il est démontré que si l'on trouvait une solution optimale à un problème NP-Complet, on trouverait toutes les solutions aux problèmes de cette classe. C'est la notion importante de réduction de problèmes.

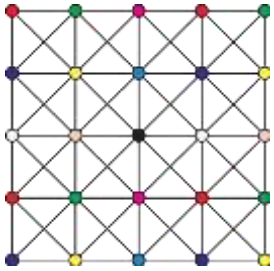
Le coloriage de graphes avec des couleurs différentes pour les nœuds, les branches ou les surfaces fait partie des problèmes NP, NP-Complet et NP-Difficile selon les cas. Les deux premiers cas nécessitant un nombre de couleurs dépendant du nombre maximum de connexions entre éléments du graphe et le dernier cas, relevant du coloriage de cartes dans des couleurs adjacentes différentes qui n'en nécessite que quatre au maximum, grâce à la démonstration informatique du théorème des quatre couleurs en 1976 par Kenneth Appel et Wolfgang Haken.

- Le coloriage de **nœuds** de graphes a des applications dans le placement d'antennes mobiles et dans l'allocation de registres mémoires pour un compilateur. Le problème est NP-Complet pour sa résolution et NP-Difficile pour trouver sa solution optimale.
- Celui des **branches** a des applications dans l'allocation de fréquences de réseaux de fibres optiques multimodes. Il permet aussi d'optimiser le placement d'objets ou personnes en fonction de leur compatibilité ou incompatibilités. Le coloriage optimum est un problème NP-Difficile.

[441] Source de l'illustration.

[442] Voir Is protein folding problem really a NP-complete one ? First investigations, 2013 (31 pages).

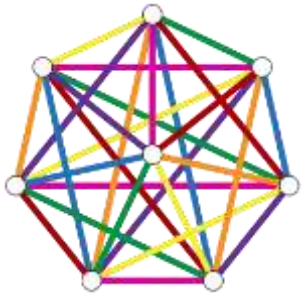
coloriage de graphes



nœuds

coloriage avec k couleurs : **NP-complet**
trouver le nombre minimum de couleurs : **NP-difficile**

allocation de fréquences radio télécoms



segments

coloriage avec k couleurs : **P**
coloriage optimum : **NP-difficile**

allocation de fréquences de fibres optiques multimodes

zones

déterminer si coloriage possible avec 3 couleurs : **NP-complet**
coloriage avec 4 couleurs : **P**

définition de zones de couverture d'antennes de réseaux télécoms
allocation de fréquences micro-ondes dans des réseaux de qubits supraconducteurs

- Celui des **zones** peut servir à définir les zones de couvertures d'antennes radio mobiles ou de satellites de télécommunications. Il peut même servir à allouer les fréquences micro-ondes d'activation de qubits supraconducteurs. Le coloriage avec trois couleurs est un problème NP-Complet.

D'une manière générale, de nombreuses classes de problèmes C ont une sous-classe C-Complet et C-Difficile. Un problème est C-Difficile s'il existe un type de réduction des problèmes de la classe C vers ce problème. Si le problème C-Difficile fait partie de la classe C, alors il est dit "C-Complet"[443].

NP Difficile : concerne les problèmes d'optimisation où l'on recherche un minimum ou un maximum avec une grande combinatoire. Un problème est NP-Difficile si tous les problèmes NP-Complets peuvent se réduire par simplification polynomiale à ce problème. C'est le cas de la résolution du **problème du voyageur du commerce** où l'on doit tester une grande combinatoire de parcours pour trouver celui qui est réalisé le plus rapidement pour passer via un nombre déterminé de villes. Il faut alors tester toutes les solutions.

Si un voyageur de commerce doit traverser 125 villes en moins de 30 jours, s'il existe une solution qui fonctionne dans ce laps de temps, alors le problème est NP. Mais rien ne dit que l'on a trouvé toutes les solutions ! La résolution du problème en-dessous d'un temps de parcourt arbitraire avec un retour au point de départ est un problème NP-complet. C'est ce que l'on appelle un circuit hamiltonien : un chemin parcourant un graphe passant une fois et une seule par chacun des nœuds et revenant à son point de départ.

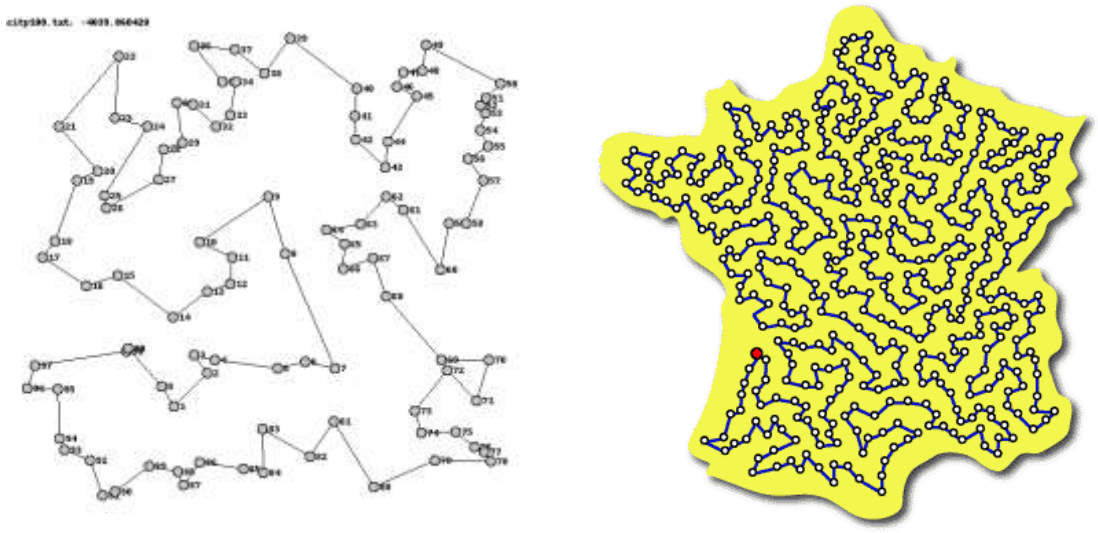
La détermination du temps de parcours le plus court est NP-difficile. L'algorithme de force brute pour le résoudre a un temps qui dépend de N! , N étant le nombre de nœuds du réseau. Le temps optimum connu est $N^2 * 2^N$. Le problème est difficile à résoudre au-delà de 20 étapes[444] !

---

[443] Pour en savoir plus, voir notamment Complexity Theory Part I (81 slides) et part II (83 slides), qui fait partie d'un cours de Stanford sur les théories de la complexité, Calculabilite et Complexite - Quelques resultats que je connais d'Etienne Grandjean de l'Université de Caen, 2017 (43 slides) ainsi que cette vidéo d'Olivier Bailleux (2017, 20 minutes). Elle est très claire mais vous serez très forts si vous arrivez à suivre et à tout assimiler ! L'auteur précise qu'il faut la regarder plusieurs fois en faisant souvent une pause !

[444] Voir le site The Traveling Salesman Problem qui donne quelques exemples de tels problèmes comme le parcours de tous les 49 687 pubs anglais ou des 49 603 lieux touristiques aux USA.

problème du voyageur de commerce



comment parcourir un graphe en un temps minimum, sans passer deux fois au même endroit et qui se termine au point de départ : **NP-difficile**

La classe des problèmes NP-Difficile contient aussi nombre de jeux de **Nintendo** comme Super Mario Bros, La Légende de Zelda et Pokemon[445]. Le calcul quantique ne permettrait pas de solutionner les plus complexes des problèmes NP-difficile.

PSPACE : est la classe des problèmes qui peuvent être résolus en espace polynomial sur une machine déterministe. NPSPACE est la classe des problèmes pouvant être résolus en espace polynomial sur une machine non déterministe. NPSPACE = PSPACE selon le théorème de Savitch.

EXPTIME : est la classe des problèmes décidés en temps exponentiel par une machine déterministe. Précisément, le temps de calcul de ces problèmes est une puissance de 2 exprimée sous forme d'un polynôme de N, N étant le niveau de complexité du problème. Ils sont intractables avec des machines traditionnelles.

Certains de ces problèmes peuvent être convertis en problèmes traitables de manière polynomiale par des ordinateurs quantiques. Les jeux d'échecs et de Go sur grille de taille arbitraire font partie de cette catégorie. Dans les grilles à taille limitée, l'effet exponentiel a des limites. Celles-ci ont été dépassées pour les échecs par Deep Blue en 1996 et pour le jeu de Go par AlphaGo de DeepMind en 2016 et 2017.

NEXPTIME : est la classe des problèmes décidés en temps exponentiel par une machine non-déterministe et avec un espace mémoire illimité.

EXPSPACE : est la classe des problèmes qui peuvent être résolus en espace exponentiel. Autant dire qu'ils sont difficiles d'accès aux machines d'aujourd'hui et même de demain.

2-EXPTIME : est une classe englobant les précédentes qui couvre les problèmes de décision pouvant être résolus par une machine de Turing déterministe en temps exponentiel d'exponentiel ! Soit un ordre de grandeur $O(2^{2^{P(n)}})$, P(n) étant un polynome de n.

[445] Voir Classic Nintendo Games are (Computationally) Hard, 2012 (36 pages).

Les classes précédentes (PSPACE, EXPTIME, NEXPTIME, EXPSPACE, 2-EXPTIME) ne correspondent pas à des problèmes pratiques faciles à identifier dans la vie courante. En tout cas, je n'en ai pas trouvé dans la littérature. Ils couvrent dans l'ensemble les problèmes de prévision de comportement de systèmes ultra-complexes avec de fortes interactions. S'il est possible que la modélisation du repliement d'une protéine soit un problème NP, quelle serait la classe du problème de simulation du fonctionnement d'une cellule vivante entière, voire d'un organisme multicellulaire ? Les interactions sont tellement nombreuses au niveau atomique, moléculaire et cellulaire que la classe de ce genre de problème est probablement située bien au-delà de NP-Difficile.

Il faudrait ajouter la classe #P des problèmes de décomptage du nombre de solutions de problèmes de classe P, qui sont résolus en temps polynomial. Proposée en 1979 par Leslie Valiant, elle a évidemment ses classes associées #P difficile et #P complet. Le calcul du permanent d'une matrice carrée remplie de 0 et de 1 est un problème #P complet d'après le théorème de Ben-Dor et Halevi démontré en 1993. En 2011, Scott Aaronson démontrait que le calcul du permanent d'une matrice était un problème #P difficile [446]. Tout ceci a un lien avec la simulation numérique de l'échantillonnage du boson qui est comparée à sa résolution par des systèmes à base de photons que nous étudierons dans une partie sur les qubits photons.

Il existe bien d'autres classes de complexité de problèmes que je ne vais pas décrire ici : EXP, IP, MIP, BPP, RP, ZPP, SL, NC, AC0, TC0, MA, AM et SZK ! Elles sont listées dans le site Complexity Zoo qui inventorie le zoo des classes de complexité de problèmes. Il semble il y en avoir plus d'une centaine[447].

Classes de complexité quantiques

On peut y ajouter une classification de problèmes par niveau de difficulté pour les ordinateurs quantiques, la correspondance avec les classes *ci-dessus* étant encore un problème… non entièrement résolu !

La classification est différente car les ordinateurs quantiques peuvent paralléliser les traitements tandis que les ordinateurs classiques assimilables à des machines de Turing ne peuvent le faire.

---

[446] Dans A Linear-Optical Proof that the Permanent is #P-Hard par Scott Aaronson, 2011 (11 pages).

[447] Pour en savoir plus sur le sujet des théories de la complexité, vous pouvez notamment parcourir le très documenté Computational Complexity A Modern Approach, de Sanjeev Arora et Boaz Barak de l'Université de Princeton, 2007 (489 pages).

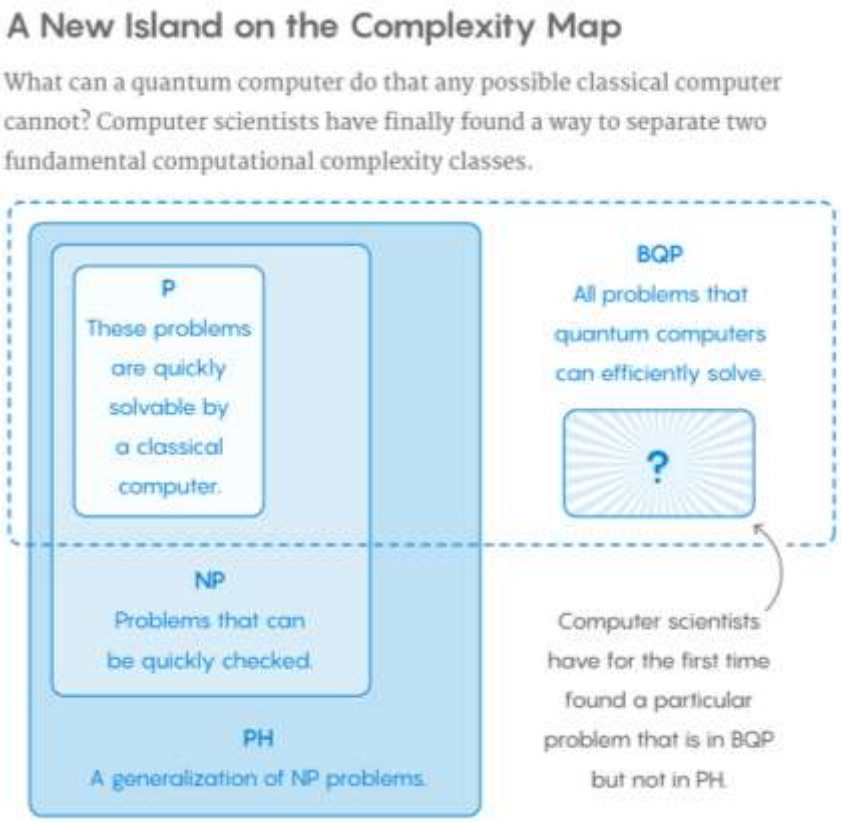
Il faudrait y ajouter une contrainte connue des ordinateurs quantiques : leur temps de cohérence qui est non seulement fini mais relativement court. Il contraint par la durée le nombre de portes quantiques que l'on peut enchaîner pour résoudre un problème. Et ce temps est inférieur au dixième de seconde pour un ordinateur quantique à base de supraconducteurs. C'est une contrainte que n'ont pas les ordinateurs traditionnels.

On peut y faire tourner un algorithme jusqu'à plus soif. Un problème trop complexe pour un ordinateur quantique serait donc aussi un problème qui nécessiterait d'enquiller un nombre de portes quantiques trop grand pour s'exécuter plus rapidement que le temps de cohérence.

PH : est la classe des problèmes qui peuvent être résolus par des ordinateurs traditionnels du présent et, surtout, par tout ordinateur traditionnel du futur ! PH signifie "Polynomial Hierarchy".

BQP : définit une classe de problème qui est traitable en temps polynomial sur un ordinateur quantique avec un taux d'erreur contraint. Cela peut dans certains cas correspondre à des problèmes P. La classe a été définie en 1993, au moment où apparaissaient les premiers algorithmes quantiques.

En débat, le fait de savoir si la classe BQP est véritablement différente de la classe P ! Il est déjà démontré que la classe P des problèmes polynomiaux est dans BQP. Mais est-ce que NP est dans BQP ? A priori non. C'est cependant difficile à prouver de manière générique. La relation exacte entre BQP et NP est encore inconnue.



Le point clé est de trouver des algorithmes qui font partie de BQP (traitables en quantique) et qui ne sont pas dans PH (traitables avec n'importe quelle architecture traditionnelle du présent et du futur). Cette incertitude a été levée très récemment [448]. Les deux logiciens ont trouvé des algorithmes à base d'oracles (boites noires) qui sont dans BQP mais pas dans PH.

Donc, qui ont un temps de résolution polynomial sur ordinateur quantique mais qui reste exponentiel sur ordinateur classique. Alea jacta est ! Mais je ne vais pas prétendre avoir compris cette belle démonstration ! Qu'en est-il au passage d'une éventuelle différence de complexité de problèmes gérable avec des ordinateurs quantiques à portes universelles vs les ordinateurs à recuit quantique de style D-Wave ?

[448] Voir Finally, a Problem That Only Quantum Computers Will Ever Be Able to Solve de Kevin Hartnett, 2018, qui fait référence à Oracle Separation of BQP and PH des Israéliens Ran Raz et Avishay Tal, mai 2018 (22 pages), présenté dans la conférence Electronic Colloquium on Computational Complexity. C'est la source de l'illustration de cette page.

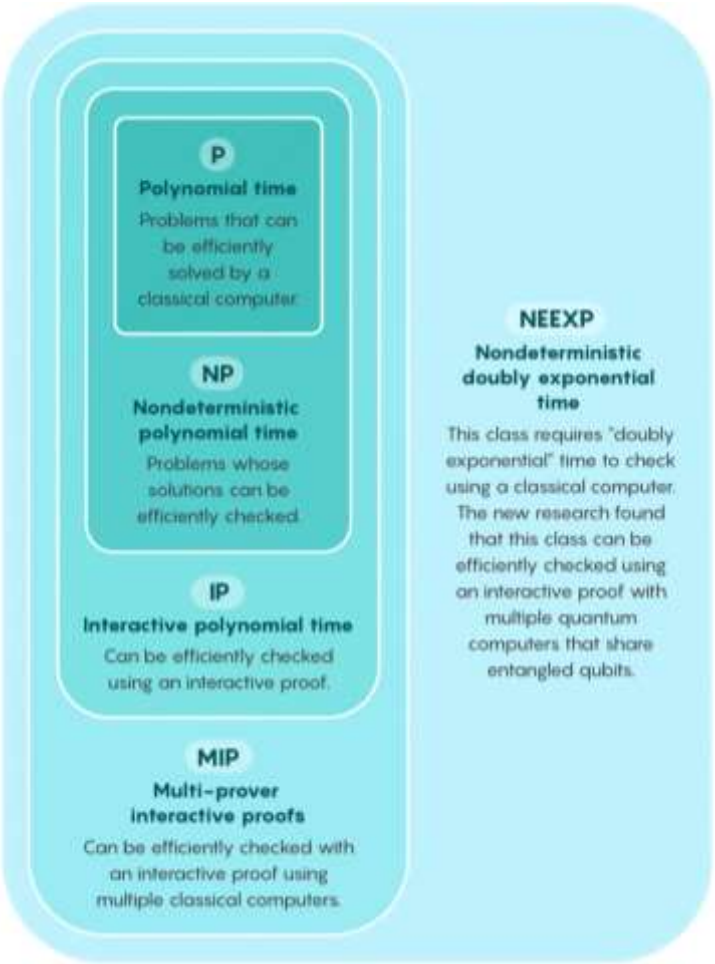
D'après plusieurs chercheurs[449], il n'y en aurait pas. Divers théorèmes montrent qu'un problème qui peut être résolu avec des portes quantiques universelles peut aussi l'être avec une architecture de recuit quantique à la D-Wave et réciproquement et dans un ordre de grandeur de temps équivalent.

QMA (pour Quantum Merlin Arthur) définit une classe de problèmes qui est vérifiable en temps polynomial sur un ordinateur quantique avec une probabilité supérieure aux 2/3. C'est l'analogue quantique de la classe de complexité "traditionnelle" NP. La classe QMA contient les classes P, BQP et NP[450]. Comme la classe NP, la classe QMA a deux sous-classes, QMA Complet et QMA Difficile. En pratique, ce sont des problèmes difficiles à résoudre avec des ordinateurs quantiques.

Malheureusement, la littérature sur le sujet n'en décrit pas la nature ou ne fournit pas d'exemples. C'est bien dommage pour ceux qui apprécient d'adopter un sens pratique des choses !

QCMA est une classe hybride entre QMA et NP. La preuve est fournie en temps classique polynomial mais la résolution relève du niveau QMA et est réalisée de manière quantique. Je n'ai pas bien compris et ce n'est pas bien grave.

Nombre de publications relèvent les limitations des algorithmes et ordinateurs quantiques. Un problème BQP qui n'est pas dans PH donne l'avantage au quantique. Mais des problèmes intractables exponentiels pour lesquels l'amélioration apportée par le quantique n'est que racinaire (racine carrée du temps classique) ne modifie pas leur nature exponentielle. C'est ce que relève Scott Aaronson[451]. Les problèmes NP Complets et au-delà restent inaccessibles aux ordinateurs quantiques. La force brute a des limites que même le calcul quantique ne permet pas de dépasser en théorie ! Cela explique en partie la difficulté à créer des algorithmes quantiques efficaces.



Enfin, **NEEXP** est une classe de problèmes qui requiert un temps de calcul doublement exponentiel pour sa résolution. Des travaux récents démontrent qu'un résultat peut être vérifié avec plusieurs ordinateurs quantiques avec des qubits intriqués. On est bien avancé car cela ne permet pas pour autant de résoudre les problèmes de ce type[452] !

---

[449] Voir Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation de Dorit Aharonov, Wim van Dam et Julia Kempe (du CNRS), 2008 (30 pages).

[450] Voir QMA-complete problems de Adam Bookatz, 2013 (18 pages).

[451] Voir The Limits of Quantum Computers (16 pages) ainsi que dans NP-complete Problems and Physical Reality (23 pages).

[452] Voir NEEXP in MIP* de Anand Natarajan et John Wright, 2019 (122 pages) et Computer Scientists Expand the Frontier of Verifiable Knowledge, 2019.

Il faut prendre en compte le fait que certains problèmes sont indécidables, à savoir qu'ils ne peuvent pas être résolus par un algorithme, quel que soit le temps dont on dispose[453]. Il en va ainsi de la détermination de l'arrêt d'un programme dans une machine de Turing.

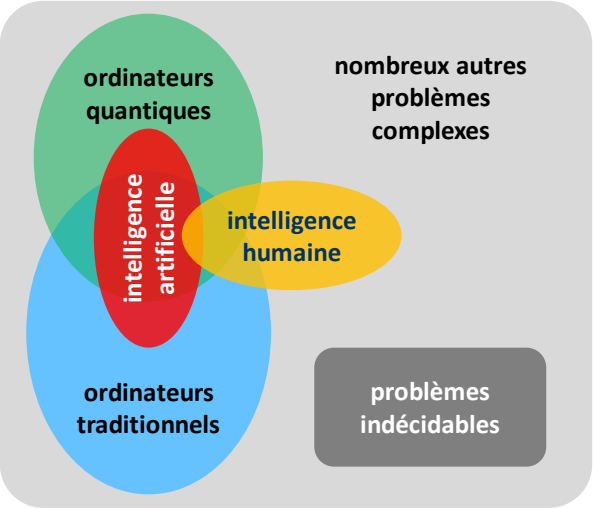
En d'autres termes, il n'existe pas de programme permettant de savoir si n'importe quel programme écrit dans un langage de programmation courant va s'arrêter ou boucler pendant une durée infinie.

Ce sujet a toutefois avancé en 2020 par la démonstration de l'égalité des classes de complexité MIP* et RE[454].

version plus simple

conséquence : l'Homme ne pourra jamais résoudre tous les problèmes !

la toute puissance (de l'IA ou autre) est un mythe



Dans le même ordre, le **théorème de Rice** démontre qu'aucune propriété non triviale d'un programme ne peut être décidée de manière algorithmique. Tout cela pour dire qu'il n'existerait pas de méthode automatique de détection de bugs dans un programme ou de certification qu'il s'exécute bien. Il existe cependant des méthodes de preuve formelle permettant de certifier l'exécution de programmes spécifiques. Cela passe par l'utilisation de spécifications formelles des programmes qui servent de référence pour l'évaluation de leur bon fonctionnement. C'est déjà très utilisé, sans quantique, dans l'informatique industrielle et dans les systèmes critiques comme dans l'aérospatial.

Contournements de science-fiction

Une autre barrière semble infranchissable aux ordinateurs de tout type : la barrière du temps de Planck, qui est de 10^{-43} secondes. Il serait impossible de réaliser un calcul élémentaire en moins de temps que ce temps de Planck. C'est une limite de la loi de Moore en plus de la barrière de la chaleur de Landauer qui définit la quantité d'énergie minimale nécessaire pour modifier une information. Mais cette barrière temporelle de Planck est loin d'être atteinte. Les ordinateurs à base de processeurs CMOS sont limités à une fréquence d'horloge de 4 à 6 GHz, donc $2*10^{-10}$ secondes.

Avec un processeur photonique pouvant atteindre théoriquement 100 GHz, on en serait à 10^{-11} secondes mais ceux-ci sont très difficiles à réaliser. Et cela donne de la marge, 10^{32}, avant d'atteindre la barrière temporelle de Planck.

Autre solution pour transcender les calculateurs quantique d'architecture connue et qui relève de la science-fiction : faire des calculs dans des mondes parallèles pour tester toutes les solutions à un problème complexe et consolider les résultats obtenus. C'est l'application du scénario de la série TV "Fringe" au calcul quantique.

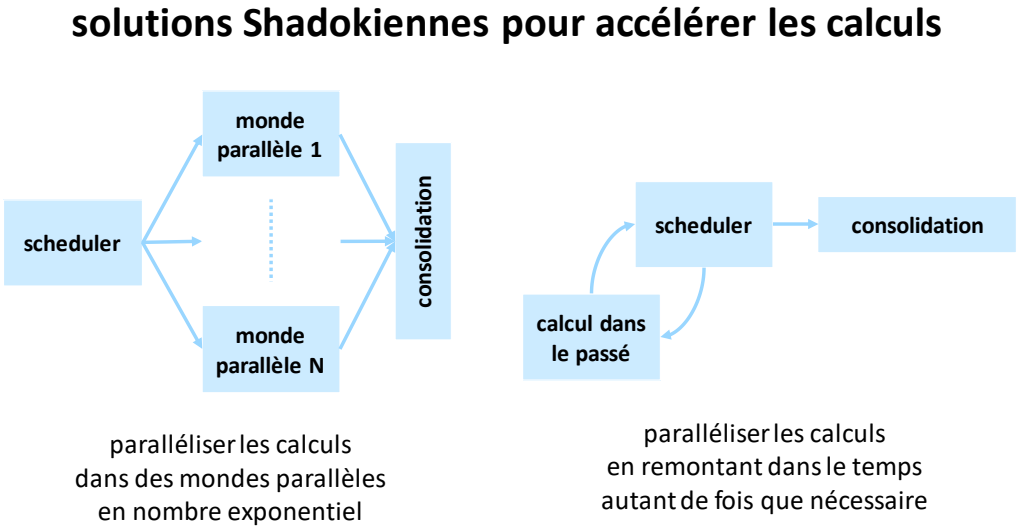
Il va sans dire que pour que cela ait un intérêt, il faudrait pouvoir faire cela dans un nombre exponentiel d'univers parallèles. Il faudrait donc aussi que la méthode soit "scalable". Si on ne pouvait l'utiliser que dans un nombre limité de mondes parallèles, cela n'aurait pas un grand intérêt !

---

[453] Comme vu dans Complexite algorithmique de Sylvain Perifel, 2014 (430 pages).

[454] La classe MIP* des problèmes qui peut être vérifiée grâce à l'intrication quantique est égale à la classe RE des problèmes qui ne sont pas plus difficile que les problèmes de l'arrêt d'un programme. **Voir** A quantum strategy could verify the solutions to unsolvable problems — in theory **par Emily Conover, 2020 qui fait référence à** MIP*=RE par Zhengfeng Ji et al, janvier 2020 (165 pages) et vu dans Mathematicians Are Studying Planet-Sized Quantum Computers With God-Like Powers par Mordechai Rorvig, 2020. Voir Landmark Computer Science Proof Cascades Through Physics and Math par Kevin Hartnett, mars 2020 qui vulgarise bien mieux la question.

On peut aussi imaginer remonter dans le temps pour refaire les calculs plusieurs fois et consolider également les résultats. Dans ces deux scénarios shadokiens, l'une des difficultés parmi d'autres serait de gérer le goulot d'étranglement de la consolidation des résultats.



Il faudrait un bus de données suffisamment rapide pour absorber une grande quantité d'information. On pourrait d'ailleurs se demander s'il n'est pas possible de réduire l'un des cas à l'autre voir de les combiner. Ainsi, si on calcule dans le passé, on peut choisir de le faire dans des passés simultanés ou dans des passés différents, histoire d'éviter de trop encombrer les passés. Tant qu'à faire !

Les deux méthodes pourraient peut-être aussi être opérantes avec des ordinateurs traditionnels. Mais l'ajout du quantique rend la chose plus crédible, si l'on peut dire. Revenir dans le passé ou se déplacer instantanément dans des mondes parallèles est probablement bien plus aisé avec des quantums.

Ce sont évidemment des hypothèses qui ne relèvent pas du domaine du possible, même en tortillant les lois de la physique au gré de ses désirs les plus fous. Scott Aaronson évoque pourtant quelques-uns de ces scénarios[455]. En pratique, au mieux peut-on tirer parti de la vitesse supraluminique de connexion entre qubits intriqués, qui peut servir dans certaines circonstances que nous aurons l'occasion d'explorer, mais qui n'accélèrent pas les calculs pour autant.

L'intractabilité des problèmes NP Complets et QMA pourrait faire partie des principes de base de la physique et rester des limites infranchissables. Jusqu'à ce que l'on trouve une parade astucieuse insoupçonnée ! Une AGI ou intelligence artificielle générale pourrait-t-elle le faire ? Cela devient un problème récursif… !

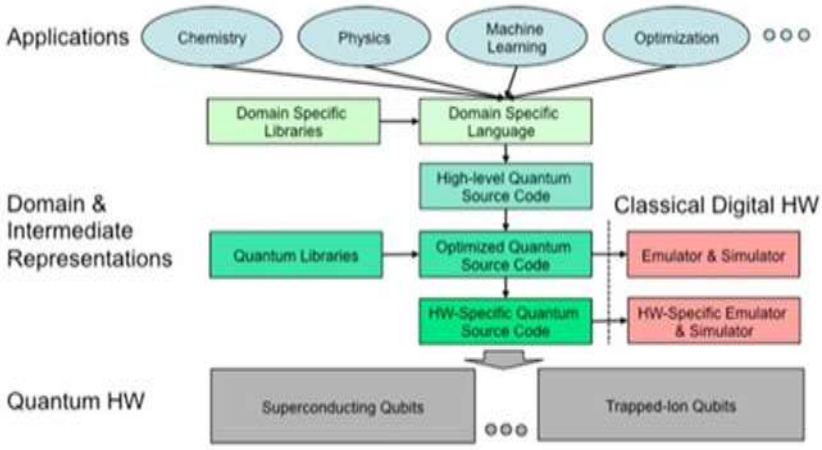
En attendant, les recherches vont surtout bon train pour permettre la création d'ordinateurs quantiques avec un grand nombre de qubits dotés de caractéristiques opérationnelles clés comme un long temps de cohérence et des taux d'erreurs aussi faibles que possibles. C'est le point de passage obligé pour pouvoir traiter des problèmes exponentiels de grande taille dans des applications métier courantes.

[455] Dans NP-complete Problems and Physical Reality, 2005 (23 pages).

Outils de développement

Après avoir fait le tour de quelques algorithmes quantiques de base puis des théories de la complexité qui permettent de détourer vaguement l'univers du possible pour le calcul quantique, il nous faut maintenant explorer les outils logiciels de l'informatique quantique. Comme pour tout le reste, c'est un monde entièrement nouveau et avec des paradigmes très différents par rapport à la création de logiciels classiques. On peut cependant y retrouver ses petits.

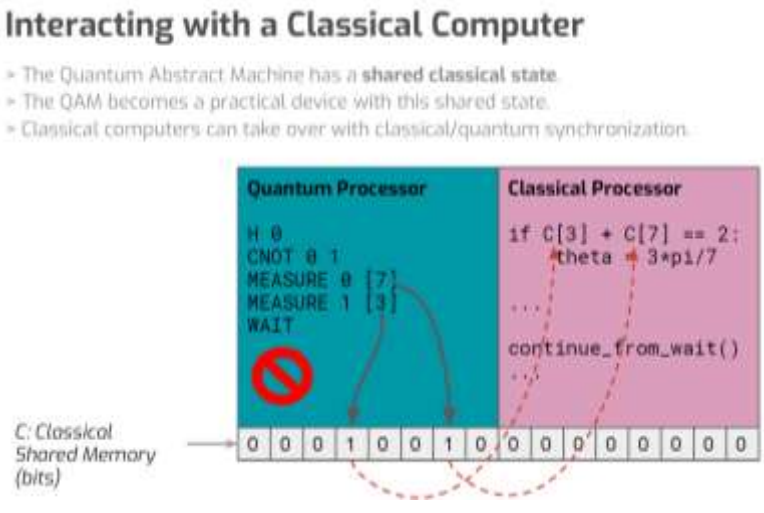
Qui dit algorithme dit programmation, langages de programmation et environnements de développement. Comme l'indique le schéma *ci-contre* (dont j'ai malheureusement perdu la source…), les logiciels quantiques sont organisés en couches superposées avec en partant du bas, les qubits physiques suivi du langage machine spécifique permettant de les piloter à base niveau.



Suit le "high level quantum source code" qui est en fait une sorte de macro-assembleur, pouvant tirer parti de bibliothèques de fonctions avec des algorithmes prêts à l'emploi (transformée de Fourier quantique, etc.) et enfin, d'éventuels langages de haut niveau adaptés à des besoins métiers spécifiques.

Dans les couches basses entre langage machine et le macro-assembleur se trouvent des fonctions de conversion des portes quantiques en portes quantiques universelles supportées par l'ordinateur quantique ainsi que les systèmes de codes de correction d'erreur qui peuvent demander l'exécution d'un grand nombre de portes quantiques.

Un compilateur quantique va aussi faire de l'optimisation en supprimant par exemple les séquences de portes quantiques qui ne changent pas l'état d'un qubit, comme deux portes de Hadamard ou X (NOT) consécutives. Il va aussi les arranger pour minimiser le nombre d'étapes de portes quantiques de la solution. Les architectures logicielles du quantique sont généralement hybrides et permettent de contrôler un ordinateur quantique à partir de logiciels procéduraux assez traditionnels.



Ils gèrent côte à côte l'exécution de logiciels classiques et de logiciels quantiques en manipulant de la mémoire traditionnelle en plus de celle des qubits, comme illustré dans le schéma *ci-dessus* originaire de la startup Rigetti.

L'ordinateur classique sert au minimum à contrôler l'exécution des algorithmes quantiques, ne serait-ce que pour déclencher les portes quantiques au bon moment, de manière séquentielle. Il peut aussi déclencher plusieurs algorithmes quantiques les uns après les autres. On peut imaginer qu'une application fera appel à plusieurs algorithmes quantiques et pas un seul.

Les classes d'outils de développement

On peut identifier quelques grandes classes d'outils de création de logiciels quantiques : les outils de programmation graphiques, les langages de scripting, les langages intermédiaires, les langages machine et les compilateurs.

Outils de programmation graphique

Ils permettent de spécifier la séquence des portes quantiques à exploiter pour créer des algorithmes directement exploitables dans des ordinateurs quantiques du cloud ou des émulateurs HPC dans le cloud.

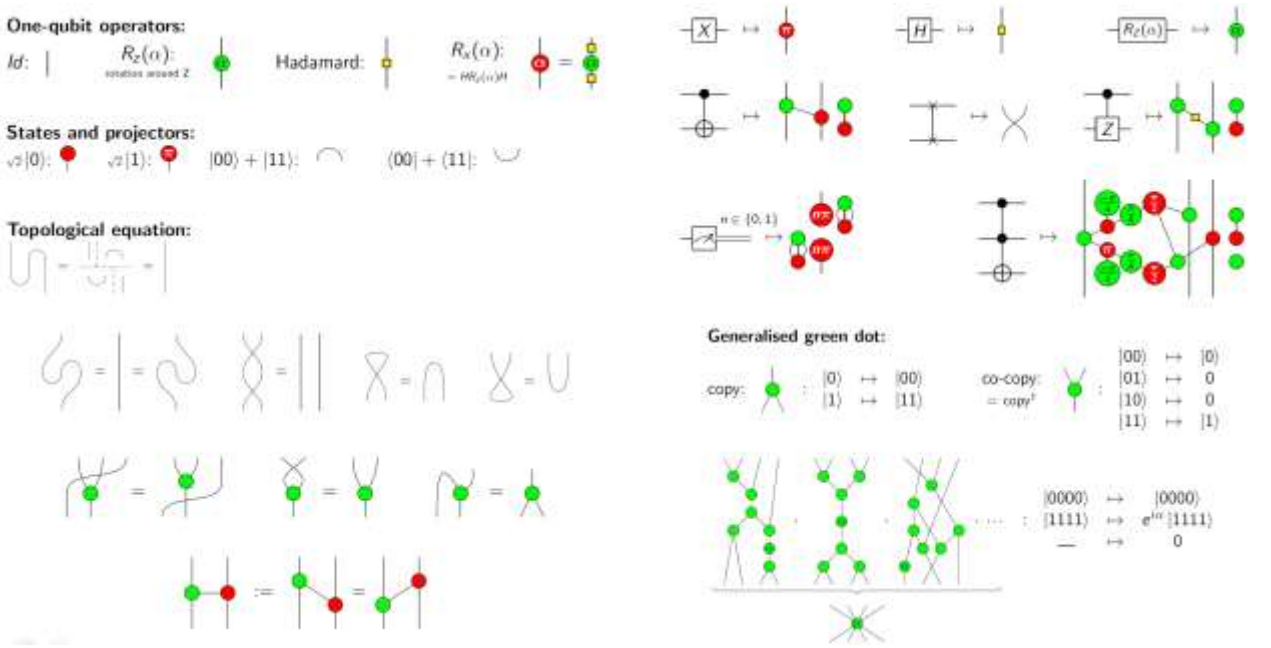
Ces outils peuvent faire fonctionner et visualiser l'état des qubits lorsque leur nombre est raisonnable. Ils permettent de vérifier la faisabilité de l'exécution de l'algorithme. L'un des exemples de tels outils est l'IBM Q Experience ou IBM Composer qui est proposé dans le cloud depuis 2016 (*ci-contre*) et avec un nombre croissant de qubits opérationnels. Cela avait démarré avec 5 et atteint maintenant 53 qubits.

On y trouve aussi des simulateurs graphiques de qubits avec lesquels on peut se faire la main pour comprendre comment enchaîner les portes quantiques sur quelques qubits et visualiser le résultat visuellement.

C'est notamment le cas de QuantumPlayground originaire de Google et de l'outil open source Quirk, ce dernier pouvant simuler jusqu'à 16 qubits. Il fonctionne en ligne et on peut le télécharger pour l'exécuter sur son propre ordinateur en local. Sa capacité n'est limitée que par la RAM dont vous disposez. Voici ci-dessous, un exemple de transformée de Fourier quantique réalisée en Quirk.

Enfin, ajoutons à cette catégorie d'outils un cas particulier, celui du **ZX-calculus**. C'est un langage de programmation graphique qui utilise des règles de composition topologiques. Il a été créé en 2008 par Bob Coecke et Ross Duncan[456]. Il permet de visualiser les modifications apportées à un jeu de qubits. Il s'appuie sur des transformations applicables à la représentation géométrique des portes quantiques qui permettent de simplifier les modèles. Il est notamment utile pour programmer un ordinateur quantique en MBQC (measurement base quantum computing) et pour modéliser visuellement des codes de correction d'erreurs.

Il en existe des variantes comme le ZW-calculus qui permet de mieux modéliser l'intrication ainsi que le ZH-calculus qui sert à la généralisation du modèle de programmation MBQC grâce à l'ajout d'une boîte incarnant la porte H de Hadamard et permet de plus facilement intégrer des portes de Toffoli dans ses diagrammes.



Il est associé à un outil de développement, **Quantomatic**, créé par Aleks Kissinger et Vladimir Zamdzhiev de l'Université d'Oxford[457]. Les contributeurs des travaux autour du ZX-Calculus comprennent des chercheurs du Loria sous la responsabilité de Simon Perdrix, un laboratoire de recherche situé à Nancy ainsi que Dominic Horsman du LIG de l'UGA à Grenoble[458]. Ils organisent leur propre conférence, la **QPL** (Quantum Physics and Logic) dont la dernière édition avait lieu en ligne début juin 2020.

Langages de scripting

Ils permettent de programmer en mode texte la structure des portes quantiques d'une solution. Ces outils permettent d'associer de la programmation classique avec enchainement de fonctions quantiques conditionnées par l'état de variables en mémoire classique.

On compte deux principaux types de langages quantiques : les langages impératifs et les langages fonctionnels.

---

[456] Voir Interacting Quantum Observables: Categorical Algebra and Diagrammatics de Bob Coecke1 et Ross Duncan, 2009 (80 pages).

[457] Voir Quantomatic: A Proof Assistant for Diagrammatic Reasoning, 2015 (11 pages).

[458] Voir Completeness of the ZX-Calculus par Renaud Vilmart, 2018 (123 slides) qui est la source des illustrations et Completeness of the ZX-Calculus par Emmanuel Jeandel, Simon Perdrix et Renaud Vilmart (73 pages) qui les explique.

- Les **langages impératifs** sont les langages de programmation procéduraux (objets ou pas) où l'on décrit les algorithmes pas à pas. On y range les langages habituels tels que C, C++, PHP ou Java.
- Les **langages fonctionnels** sont utilisés en définissant des fonctions diverses qui sont appelées de manière ad-hoc par le programme. Les boucles (for, while) sont remplacées par la récursivité de fonctions et il n'y a pas de variables modifiables. Ils permettent d'utiliser des types de données abstraits de haut niveau manipulés par les fonctions. L'ensemble est plus concis.

Table 1: A selection of some quantum programming languages.

Name	Style	Notes
QCL	Imperative	Has classical sublanguage, multiple high-level programming features.
qGCL	Imperative	Emphasis on algorithm derivation and verification.
LanQ	Imperative	Full operational semantics, proven type soundness.
Quipper	Functional	Focus on scalability, plans to include linear types for static checks (currently done at run-time).
QPL	Functional	Statically typed, denotational semantics in terms of CPOs of superoperators.
QML	Functional	Linearly typed, focused on weakening - not contraction. Quantum control and quantum data.
Qunin	Functional	Two sublanguages (untyped and linearly typed). Focus on ease of use and clean, functional style of programming.

source du tableau : Qumin, a minimalist quantum programming language, 2017 (34 pages).

Une bonne part des langages de programmation traditionnels peuvent être exploités en programmation impérative ou fonctionnelle, notamment dès lors qu'ils disposent de pointeurs de fonctions ou qu'ils supportent une logique événementielle. Dans une certaine mesure, JavaScript et Jquery peuvent-être utilisés comme des langages fonctionnels via leurs *call-back functions*. C'est aussi le cas du C++.

Chez les fournisseurs d'ordinateurs quantiques tels qu'IBM ou Rigetti, deux types de langages sont parfois proposés : un langage intermédiaire (Quil chez Rigetti) et un langage de plus haut niveau sous la forme d'extensions du langage de programmation Python (pyQuil chez Rigetti). Un outil de conversion converti le second dans le premier langage.

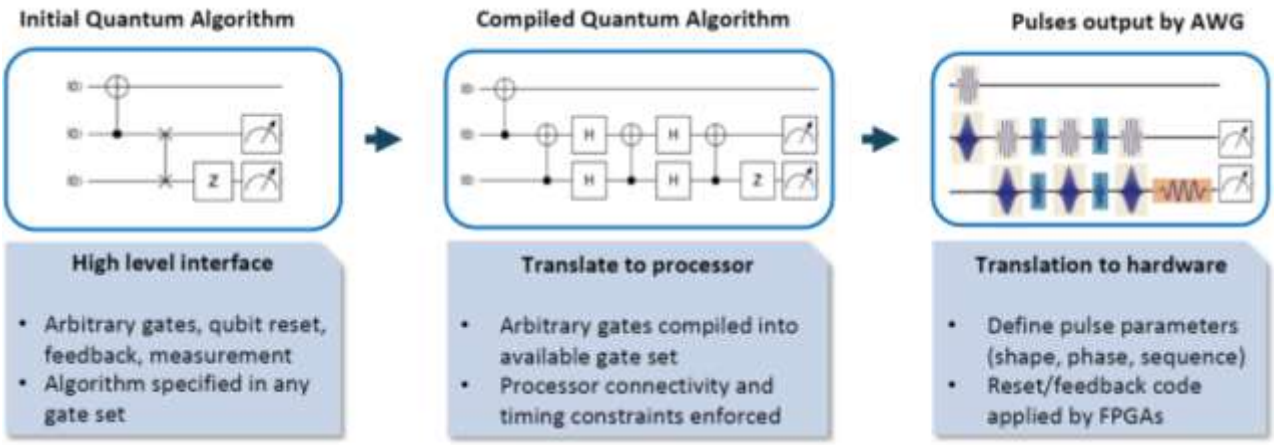
Langages machine

Ce sont les langages de plus bas niveau de programmation de l'ordinateur quantique, qui programment l'initialisation des qubits et l'activation des portes universelles qui agissent dessus puis la mesure des résultats. Ils sont généralement spécifiques à chaque type d'ordinateur quantique, voir à chaque ordinateur quantique.

Compilateurs

Les compilateurs exploitent le contenu des précédents outils, et surtout des langages de scripting, pour générer la séquence de contrôle des portes physiques de l'ordinateur quantique cible en langage machine, intégrant au passage les fonctions de corrections d'erreurs quantiques (QEC). Ces compilateurs vont transformer les portes logiques utilisées dans la programmation en portes physiques universelles exploitées par l'ordinateur quantique puis en commande des pulsations de commande des qubits, qui sont par exemples des séquences rythmées de micro-ondes dans le cas de qubits supraconducteurs[459].

[459] Source du schéma : How about quantum computing? par Bert de Jong, juin 2019 (47 slides).



Ils vont aussi calculer les temps d'activation des portes et vérifier que l'accumulation de ces temps d'activation est inférieure au temps de cohérence des qubits de l'ordinateur cible.

Comme l'aQASM d'Atos, ces outils de compilation peuvent être "multiplateformes" et supporter différentes architectures d'ordinateurs quantiques, au moins universels. La compilation n'est pas la même sur des ordinateurs quantiques topologiques. Ces compilateurs utilisent des langages de programmation quantiques. Les langages de programmation quantique sont généralement capables d'associer de la programmation procédurale classique avec de la programmation de registres et portes quantiques. Ils permettent de gérer parallèlement de la mémoire classique à des registres quantiques. Ils proviennent de la recherche ou de concepteurs d'ordinateurs quantiques comme IBM, Microsoft, Rigetti et D-Wave[460]. Les compilateurs peuvent aussi réaliser des optimisations spécifiques à certains types d'algorithmes[461].

Emulateurs

Les émulateurs, parfois appelés à tort simulateurs, sont des outils logiciels et/ou matériels qui émulent l'exécution d'algorithmes quantiques sur des ordinateurs traditionnels. Leur capacité est étroitement liée à la quantité de mémoire disponible[462]. Sur un laptop avec 16 Go de mémoire, on peut simuler environ 20 qubits. Des machines spécialisées comme l'aQML d'Atos sont conçues pour gérer une très grande quantité de mémoire vive permettant d'émuler un plus grand nombre de qubits, dépassant les 40 qubits. On peut aller jusqu'à utiliser des architectures distribuées et massivement parallèles pour réaliser de l'émulation au-delà de nombre de qubits.

Il ne faut pas les confondre avec les simulateurs quantiques, le nom donné aux ordinateurs quantiques analogiques.

On compte dans ce domaine des outils comme **Quirk**, **Quantum Circuit Simulator** est pour sa part disponible sous Android dans Google Play. Il y a aussi le **SimulaQron** de QuTech ainsi que **myQLM** d'Atos.

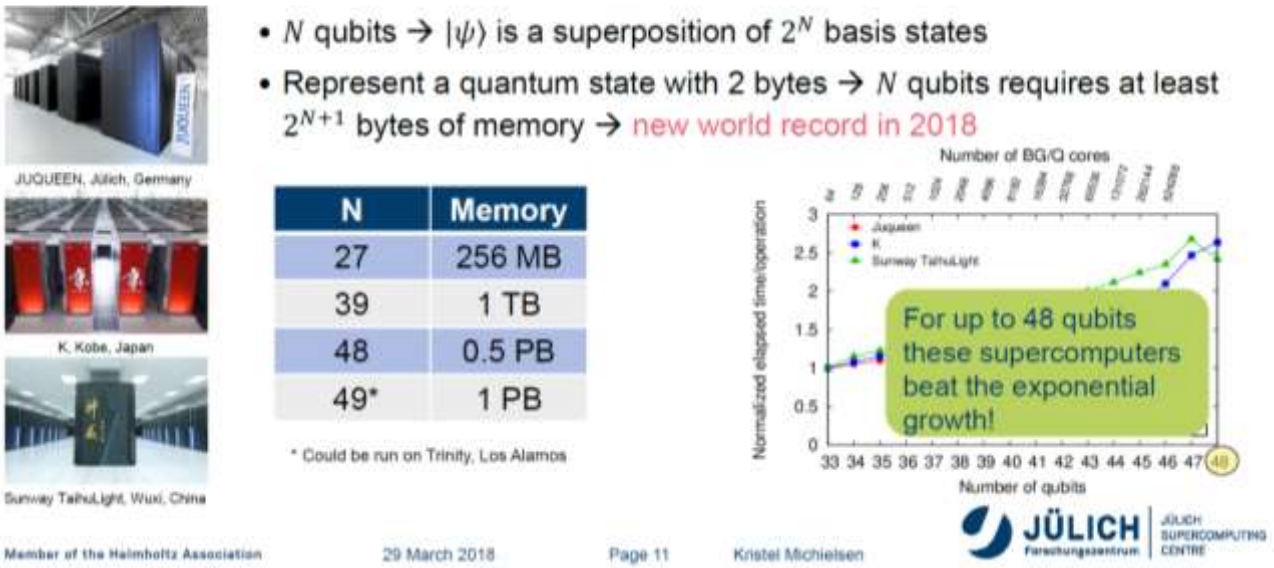
Citons aussi le logiciel d'origine française **Qode** qui permet d'éditer un circuit quantique et de générer le code associé correspondant aux environnements classiques Q#, Qiskit, QASM et Cirq. Il permet d'exécuter son « circuit » et d'afficher le résultat selon l'environnement. Il intègre des fonctionnalités avancées telles que des codes prédéfinis et la saisie d'expressions (site). Le code simulé peut ensuite alimenter les outils d'exécution de code quantique disponibles dans le cloud.

---

[460] Voir cette présentation qui décrit bien quelques-unes des tâches réalisées par des compilateurs quantiques : Opportunities and Challenges in Intermediate-Scale Quantum Computing de Fred Chong, 2018 (34 slides).

[461] C'est le cas de Partial Compilation of Variational Algorithms for Noisy Intermediate-Scale Quantum Machines par Pranav Gokhale et al, 2019 (13 pages) qui porte sur un compilateur en deux passes optimisé pour des algorithmes variationnels (VQE).

[462] Voir la liste des outils de simulation d'algorithmes quantiques sur https://quantiki.org/wiki/list-qc-simulators.



Outils de mise au point

Les logiciels quantiques ne sont pas faciles à déboguer ! Cela va certainement requérir de nouveaux outils de mise au point. Pour l'instant, ils sont intégrés dans les environnements et outils de développement proposés. On peut déboguer un algorithme pas à pas avec un simulateur de logiciel quantique tournant sur ordinateur traditionnel, pour comprendre comment évolue l'état des qubits étape par étape.

Lorsque les algorithmes tourneront sur des ordinateurs quantiques dépassant la suprématie quantique et impossibles à émuler sur ordinateur traditionnel, il faudra passer par d'autres moyens comme l'arrêt d'un algorithme quantique à une étape d'un programme, suivi de la lecture - probabiliste et répétée plusieurs fois – de l'état intermédiaire des qubits.

Outils de développement quantiques issus de la recherche

Voici un aperçu des principaux langages quantiques créés à ce jour, avec tout d'abord les langages indépendants des architectures matérielles et qui sont souvent issus de laboratoires de recherche.

Ils présentent l'inconvénient de ne pas être généralement reliés à des offres d'ordinateurs quantiques dans le cloud. Ils ont par contre souvent un certain privilège d'antériorité par rapport aux outils de développement des fournisseurs d'ordinateurs quantiques que nous verrons plus loin. C'est bien normal puisque les chercheurs sont les premiers à s'embarquer dans les domaines émergents, bien avant les acteurs privés. Ils ont souvent conçu les premiers langages de programmation quantique à une époque où l'on n'arrivait à aligner qu'à peine un à deux qubits !

Ce sont un peu les Kernighan et Richie (créateurs du langage C) et Bjarne Stroustrup (créateur du C++) du domaine ! Vous remarquerez au passage qu'un bon nombre de ces langages provient d'Europe.

- **QCL** ou Quantum Computation Language dispose d'une syntaxe et des types de données proches de ceux du langage C. Ce langage est l'un des premiers qui soit pour la programmation quantique, créé en 1998 par le chercheur Autrichien **Bernhard Ömer** de l'Austrian Institute of Technology à Vienne. Il est décrit dans Structured Quantum Programming, 2009 (130 pages) qui positionne très bien les différences conceptuelles entre langages de programmation classiques et quantiques.

Classical concept	Quantum analogue
classical machine model	hybrid quantum architecture
variables	quantum registers
variable assignments	elementary gates
classical input	quantum measurement
subroutines	operators
argument and return types	quantum data types
local variables	scratch registers
dynamic memory	scratch space management
boolean expressions	quantum conditions
conditional execution	conditional operators
selection	quantum if-statement
conditional loops	quantum forking

Table 2.1: *Classical and quantum programming concepts*

- **Q Language** est une extension du langage C++ qui fournit des classes permettant de programmer des portes quantiques (Hadamard, CNOT, SWAP, QFT pour transformée de Fourier quantique)[463].
- **QFC** et **QPL** sont deux langages fonctionnels définis par le Canadien Peter Selinger, le premier utilisant une syntaxe graphique et le second, une syntaxe textuelle[464].
- **QML** est un langage de programmation fonctionnel créé par les Anglais Thorsten Altenkirch et Jonathan Grattage[465].
- **qGCL** ou Quantum Guarded Command Language a été créé par Paolo Zuliani de l'Université de Newcastle[466].
- **ProjectQ** est un langage de scripting l'ETH Zurich qui prend la forme d'un framework Python open source, diffusé sur GitHub depuis 2016. Il comprend notamment un compilateur convertissant le code quantique en langage C++ pour son exécution dans un simulateur quantique à processeur traditionnel.[467]. Lancé début 2017, il supporte les ordinateurs quantiques d'IBM via leur langage OpenQASM Ce qui est normal puisque l'ETH Zurich est partenaire de ce dernier, ainsi que la simulation sur ordinateur traditionnel via une implémentation développées en C++ qui supporte jusqu'à 28 qubits. ProjectQ est compatible avec OpenFermion de Rigetti et Google, cité plus loin.

(a) After decomposing. (b) After CNOT mapping. (c) After optimization. (d) After mapping to hardware.

Figure 5: Individual stages of compiling an entangling operation for the IBM back-end. The high-level Entangle-gate is decomposed into its definition (Hadamard gate on the first qubit, followed by a sequence of controlled NOT gates on all other qubits). Then, the CNOT gates are remapped to satisfy the logical constraint that controlled NOT gates are allowed to act on one qubit only, followed by optimizing and mapping the circuit to the actual hardware.

[463] Il est documenté dans Toward an architecture for quantum programming, 2003 (23 pages), avec comme coauteur un certain Stefano Bettelli du Laboratoire de Physique Quantique de l'Université Paul Sabatier de Toulouse.

[464] Ils sont décrits dans Towards a Quantum Programming Language, 2003 (56 pages).

[465] Voir A functional quantum programming language, 2004 (15 pages). Les principes sont bien décrits dans la présentation Functional Quantum Programming (151 slides).

[466] Voir Compiling quantum programs, 2005 (39 pages).

[467] Voir ProjectQ: An Open Source Software Framework for Quantum Computing de Damian Steiger, Thomas Häner et Matthias Troyer, 2018 (13 pages) qui explique bien comment le compilateur optimise le code en fonction des portes disponibles dans l'ordinateur quantique.

- **Quipper** est un langage créé en 2013 qui s'appuie sur le langage classique Haskell, créé en 1990, auquel il fournit des extensions sous forme de types de données et de bibliothèques de fonctions[468]. Il manipule une version logicielle de QRAM, l'état des registres quantiques, indispensable à l'exécution d'algorithmes quantiques comme celui de Grover. Malgré tout cela, le langage ne semble pas avoir évolué depuis 2016. A noter que l'un de ses créateurs est le Français Benoît Valiron qui enseigne la programmation quantique à CentraleSupelec[469].

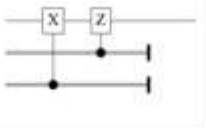
- **QWire** est un autre langage de programmation quantique voisin de Quipper, lancé en 2018, issu de l'Université de Pennsylvanie (Upenn)[470]. Il est associé à une solution de preuve formelle.

- **Qubiter** est un langage open source développé en Python utilisable au-dessus d'OpenQASM d'IBM et OpenFermion de Google. Il date de 2017.

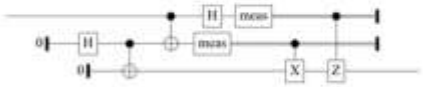
- **Scaffold** est un langage issu de l'Université de Princeton[471]. Il permet notamment de programmer du code traditionnel qui est ensuite transformé automatiquement en portes quantiques via sa fonction C2QG (Classical code to Quantum Gates). Scaffold peut notamment générer du QASM.

  En voici *ci-contre* un exemple de code, presque facile à comprendre ! Son développement a été également financé par l'IARPA.

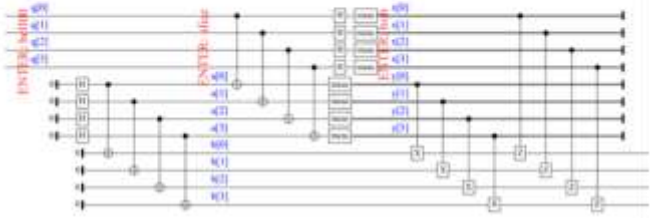
```
bob :: Qubit -> (Bit,Bit) -> Circ Qubit
bob b (x,y) = do
    b <- gate_X b `controlled` y
    b <- gate_Z b `controlled` x
    cdiscard (x,y)
    return b
```




```
teleport :: Qubit -> Circ Qubit
teleport q = do
    (a,b) <- bell00
    (x,y) <- alice q a
    b <- bob b (x,y)
    return b
```




```
teleport_generic_labeled :: (QData qa) => qa -> Circ qa
teleport_generic_labeled q = do
    comment_with_label "ENTER: bell00" q "q"
    (a,b) <- bell00_generic (qc_false q)
    comment_with_label "ENTER: alice" (a,b) ("a","b")
    (x,y) <- alice_generic q a
    comment_with_label "ENTER: bob" (x,y) ("x","y")
    b <- bob_generic b (x,y)
    return b
```



```
// Pauli X, Pauli Y, Pauli Z, Hadamard, S, and T gates
gate X(qreg input[1]);
gate Y(qreg input[1]);
gate Z(qreg input[1]);
gate H(qreg input[1]);
gate S(qreg input[1]);
gate T(qreg input[1]);

// Daggered gates
gate Tdag(qreg input[1]);
gate Sdag(qreg input[1]);

// CNOT gate defined on two 1-qubit registers
gate CNOT(qreg target[1], qreg control[1]);

// Toffoli (CCNOT) gate
gate Toffoli(qreg target[1], qreg control1[1], qreg control2[1]);

// Rotation gates
gate Rz(qreg target[1], float angle);        //Arbitrary Rotation

// Controlled rotation
gate controlledRz(qreg target[1], qubit control[1], float angle);

// One-qubit measurement gates
gate measZ(qreg input[1], bit data);
gate measX(qreg input[1], bit data);

//One-qubit prepare gates: initializes to 0
gate prepZ(qreg input[1]);
gate prepX(qreg input[1]);

//Fredkin (controlled swap) gate
gate fredkin(qreg targ[1], qreg control1[1], qreg control2[1])
```

[468] Il est documenté dans An Introduction to Quantum Programming in Quipper, 2013 (15 pages). Sa création a été financée par l'IARPA, l'agence fédérale du renseignement américain qui finance de la R&D comme le fait la DARPA dans la défense. L'IARPA est rattachée au DNI (Director of national Intelligence), le coordinateur du renseignement US rattaché à la Maison Blanche et à qui reportent les 17 patrons du renseignement US dont ceux de la CIA et de la NSA.

[469] Voir sa présentation Programmer un Ordinateur Quantique, 2017 (38 slides) et Quantum Computation Model and Programming Paradigm, 2018 (67 slides).

[470] Voir QWIRE: A Core Language for Quantum Circuits (13 pages) et A core language for quantum circuits par Jennifer Paykin et al, 2017 (97 slides).

[471] Voir Scaffold: Quantum Programming Language, 2012 (43 pages).

- **Qumin** est un langage quantique minimaliste conçu en Grèce en 2017[472]. Il est disponible en open source.
- **QuEST** (Quantum Exact Simulation Toolkit) est un émulateur quantique développé en langage C et supportant les APIs QUDA et les GPU de Nvidia, créé par des chercheurs de l'Université d'Oxford et open source. Le système permet de simuler de 26 à 45 qubits selon la mémoire RAM disponible, respectivement de 2 Go et 256 Go. Il date aussi de 2017.
- **Q.js** est un émulateur quantique graphique lancé en 2019, fonctionnant en JavaScript et fonctionnant donc dans un navigateur[473].
- **QuTiP** (Quantum Toolbox in Python) est un autre outil de simulation open source de qubits (surtout supraconducteurs) et de code quantique développé par Paul Nation d'IBM, Robert Johansson de Rakuten et Franco Nori de Riken (Japon) et de l'Université du Michigan. Le projet a démarré en 2011.
- **QNET** est un langage issu de Stanford, créé en 2012 qui permet notamment de simuler le fonctionnement de réseaux quantiques.
- S'ensuivent des langages de mise en œuvre quantique du **lambda calculus**, conceptualisé par Alonzo Church et Stephen Cole Kleene pendant les années 1930. Traduction en langage naturel ? Ce type de calcul permet de résoudre des problèmes très complexes et de type NP-complet, la classe des problèmes vérifiable en temps polynomial et dont la résolution requiert un temps exponentiel sur ordinateurs classiques et potentiellement polynomial sur ordinateurs quantiques !
- **eQASM** est un langage machine quantique intermédiaire issu de Delft University et de sa filiale QuTech. Il s'intercale entre des outils de programmation de haut niveau (QASM) et l'ordinateur quantique. C'est un langage compilé, d'où le « e » pour « exécutable ». C'est le compilateur qui va gérer les dépendances vis-à-vis des spécificités de l'implémentation matérielle du processeur quantique utilisé. Les tests ont pour l'instant été réalisés avec un chipset supraconducteur à 7 qubits[474].

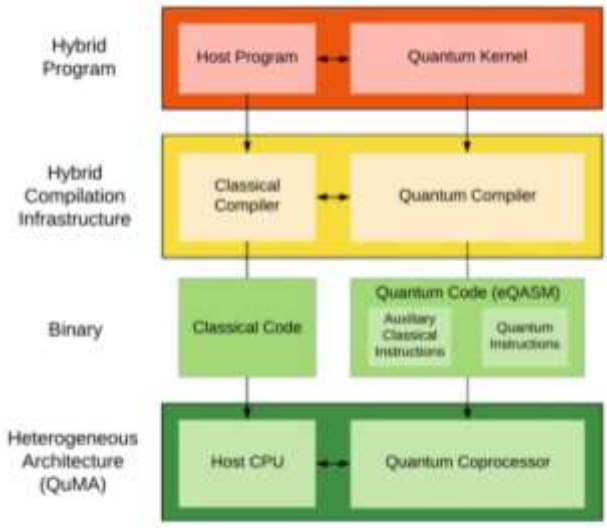


Fig. 1. Heterogeneous quantum programming and compilation model.

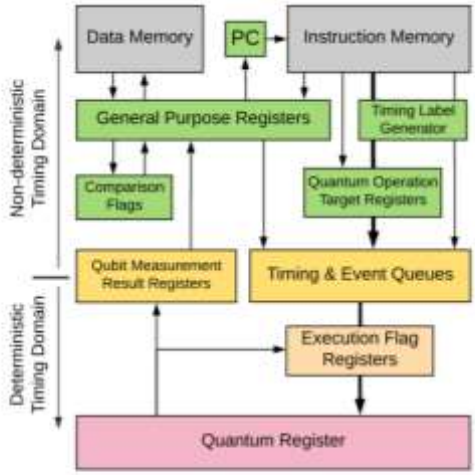


Fig. 2. Architectural state of eQASM. Arrows indicates the possible information flow. The thick arrows represent quantum operations, which read information from the modules passed through.

[472] Voir Qumin, a minimalist quantum programming language, 2017 (34 pages).

[473] Voir Quantum Programming: JavaScript (Q.js) - a drag and drop circuit editor par Stewart, 2020. Et https://quantumjavascript.app/.

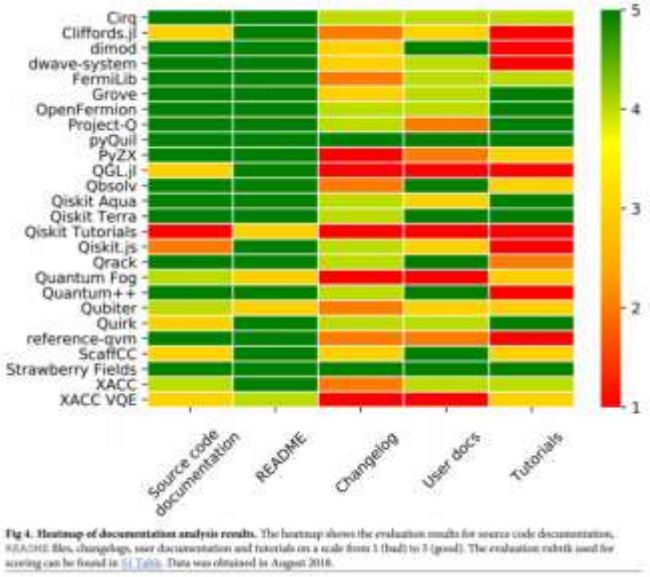
[474] Voir eQASM: An Executable Quantum Instruction Set Architecture, mars 2019 (14 pages).

- Des chercheurs du laboratoire **EPiQC** (Enabling Practical-scale Quantum Computation) de l'Université de Chicago proposent un compilateur permettant d'améliorer jusqu'à un facteur 10 la vitesse et la fiabilité des ordinateurs quantiques[475]. Là encore, il s'agit pour le compilateur de s'adapter à l'architecture matérielle sous-jacente. Leur vidéo explique le processus. L'équipe a notamment utilisé la bibliothèque TensorFlow de Google pour optimiser les paramètres de contrôle physiques des qubits.
- **Silq** est un langage de programmation quantique concis et statique proposé par une équipe de l'ETH Zuricha[476].
- **Yao.jl** est un package pour le langage Julia de création de circuits quantiques.

Une bonne majorité des outils logiciels de la programmation quantique sont open source. Open source software in quantum computing, de Mark Fingerhuth, Thomas Babej et Peter Wittek, décembre 2018 (28 pages), fait un inventaire détaillé de ces différents outils et les jauge à l'aune des canons de l'open source, le tableau colorié ci-dessous en étant la synthèse.

On y constate que la différenciation est surtout concentrée sur la documentation et les tutoriels.

Dans la pratique, peu de développeurs d'applications commerciales vont exploiter les langages évoqués dans cette partie.



Ils vont plutôt s'ancrer dans les langages issus des fournisseurs d'ordinateurs quantiques commerciaux que voici *ci-dessous*, même s'ils sont aussi open source. Ils se font facilement enfermer dans des approches « full stack » qui sont propriétaires dans la pratique.

Outils de développement des concepteurs de calculateurs quantiques

Avant même que les ordinateurs quantiques universels soient opérationnels à une échelle exploitable, la bataille des plateformes est déjà enclenchée. Les grands acteurs de l'ordinateur quantique ont presque tous adopté une approche d'intégration verticale de bout en bout allant de l'ordinateur aux outils de développement. C'est en particulier le cas chez IBM, Microsoft, Rigetti et D-Wave.

C'est bien illustré dans le schéma *ci-dessous* de synthèse qui décrit par ailleurs fort bien les principaux environnements de développement d'applications quantiques de Rigetti et IBM et dont est inspirée la partie qui les concerne ici même[477].

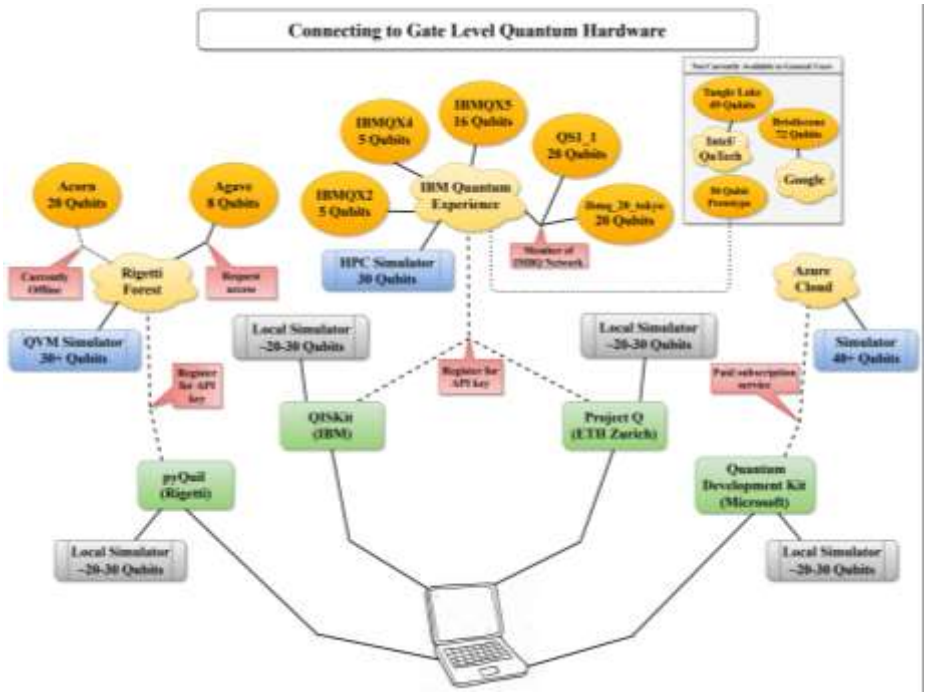
L'offre verticalisée des acteurs cités intègre souvent un langage quantique de bas niveau assimilable au langage machine, puis un langage de plus haut niveau assimilable au macro-assembleur des ordinateurs traditionnels, puis un framework open source exploitable le plus souvent en Python avec des fonctions prêtes à l'emploi, un environnement de développement, éventuellement, un simulateur graphique de portes quantiques et souvent, une offre d'accès à l'ensemble en cloud.

---

[475] Voir Research provides speed boost to quantum computers, avril 2019.

[476] Voir Swiss scientists launch high-level quantum computing language par ETH Zurich, juin 2020.

[477] Schéma découvert dans Overview and Comparison of Gate Level Quantum Software Platforms de Ryan LaRose, mars 2019 (24 pages).



Reste à inventer les langages avec un très haut niveau d'abstraction permettant de s'affranchir des portes quantiques ! Pour l'instant, il n'en existe pas à ma connaissance, sauf dans une certaine mesure autour des ordinateurs quantiques de D-Wave dont le modèle de programmation est particulier.

D-Wave

D-Wave est le plus ancien acteur du marché. Il propose une gamme complète d'outils logiciels qui ont bien évolué depuis sa création. L'architecture n'est d'ailleurs pas évidente à suivre[478]. La dernière itération de la plateforme logicielle de D-Wave s'appelle Ocean, qui comprend les briques de bas et de haut niveau pour le développement d'applications quantiques[479].

Le plus bas niveau d'accès aux ordinateurs D-Wave est le langage **QMI**, sorte de langage machine de définition des liens entre les qubits reliés entre eux dans le processeur quantique de l'ordinateur adiabatique. QMI est exploitable à partir des langages C, C++ Python et même Matlab, via l'interface SAPI (Solver API).

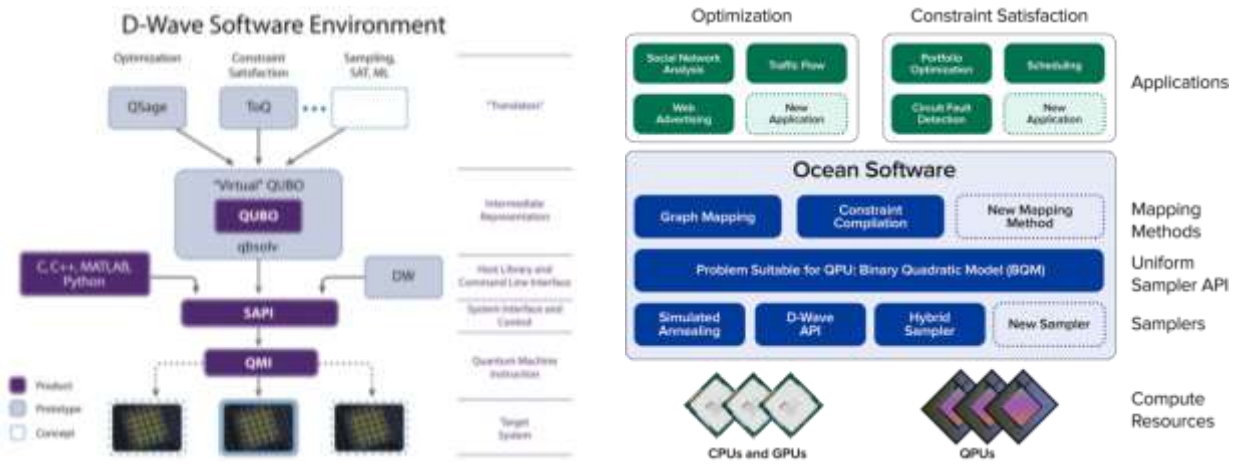
Au-dessus de QMI se situe une surcouche avec un plus haut niveau d'abstraction, **qbsolv**, qui est une bibliothèque open source depuis fin 2017. Elle permet de résoudre des problèmes d'optimisation en décomposant un problème QUBO (Quadratic Unconstrained Binary Optimization) pour le faire traiter par un ordinateur D-Wave ou un ordinateur traditionnel.

Les développeurs peuvent aussi faire appel au langage open source **QMASM** (Quantum Macro Assembler) qui est un langage de bas niveau adapté à la programmation sur ordinateur à recuit quantique D-Wave. C'est un outil tierce partie de D-Wave. Comme qbsolv, QMASM permet de décrire un "hamiltonien" fait de relations entre qubits à base de coupleurs qui sont dotés d'un poids comme le poids des synapses dans un réseau de neurone. Lors de l'exécution, l'ordinateur D-Wave cherche ensuite à déterminer un minimum énergétique de ce système pour le faire converger vers une solution. Cette méthode présente un inconvénient : il est préférable d'initialiser le système dans un état voisin de la solution recherchée et cet état ne peut être déterminé que par des calculs traditionnels. C'est un peu le serpent qui se mord la queue !

---

[478] La source du schéma de gauche est D-Wave Initiates Open Quantum Software Environment, janvier 2017. Et celle du schéma de droite, plus récent : https://www.dwavesys.com/software.

[479] D-Wave fournit un très bon document décrivant les problèmes qui peuvent être résolus avec leurs ordinateurs : D-Wave Problem-Solving Handbook, octobre 2018 (114 pages).



C'est en tout cas un modèle de programmation très différente de celui des portes quantiques universelles même s'il existe une équivalence théorique entre les modèles adiabatiques et à portes quantiques universelles comme nous l'avons vu dans la partie précédente.

QMASM est aussi intégré dans **Quadrant**, une plateforme complète pour le développement de solutions D-Wave dans le cloud appliquées au machine learning et lancée par D-Wave en 2018[480].

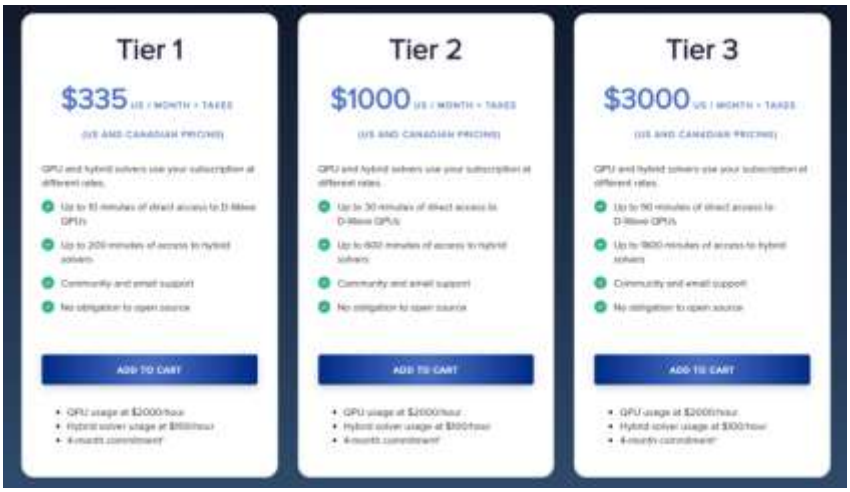
Le SDK Ocean de D-Wave comprend aussi **Hybrid**, un framework open source de création d'algorithmes hybrides.

On peut ajouter des surcouches tierces-parties comme **QSage**, un framework destiné à la résolution de problèmes d'optimisation et **ToQ**, un autre framework, pour résoudre des problèmes de satisfaction de contraintes ainsi que le SDK de la startup canadienne **1Qbit**. Avec ces surcouches, on commence à se rapprocher des solutions métiers.

En date d'août 2019, D-Wave, ses partenaires et clients avaient prototypé 150 algorithmes et solutions. Ils n'ont pas forcément généré d'avantage quantique certain, mais permettent aux clients de s'éduquer sur la programmation quantique. Nous les évoquerons dans une partie à venir sur les applications par marchés et sur l'offre des différents acteurs du marché.

L'offre de D-Wave est surtout proposée sous la forme de ressources en cloud, sous l'appellation **Leap**.

La version 2 de Leap était lancée en février 2020 [481]. Elle comprend notamment un nouveau service de solver hybride pouvant traiter des problèmes d'optimisation avec jusqu'à 10 000 variables ainsi qu'un nouvel environnement de développement interactif exploitant Python. Les tarifs vont de $335 à $3000 par mois pour accéder à de 10 à 90 minutes de calcul quantique.



[480] Voir D-Wave Announces Quadrant Machine Learning Business Unit, mai 2018.

[481] Voir D-Wave announces Leap 2, its cloud service for quantum computing applications par Emil Protalinski, février 2020.

IBM

La plateforme de développement logicielle quantique d'IBM est sous l'ombrelle **Qiskit**. Elle comprend **OpenQASM**, un langage de programmation qui complète son outil de programmation graphique en ligne Q Experience. OpenQASM comprend une douzaine de commandes[482].

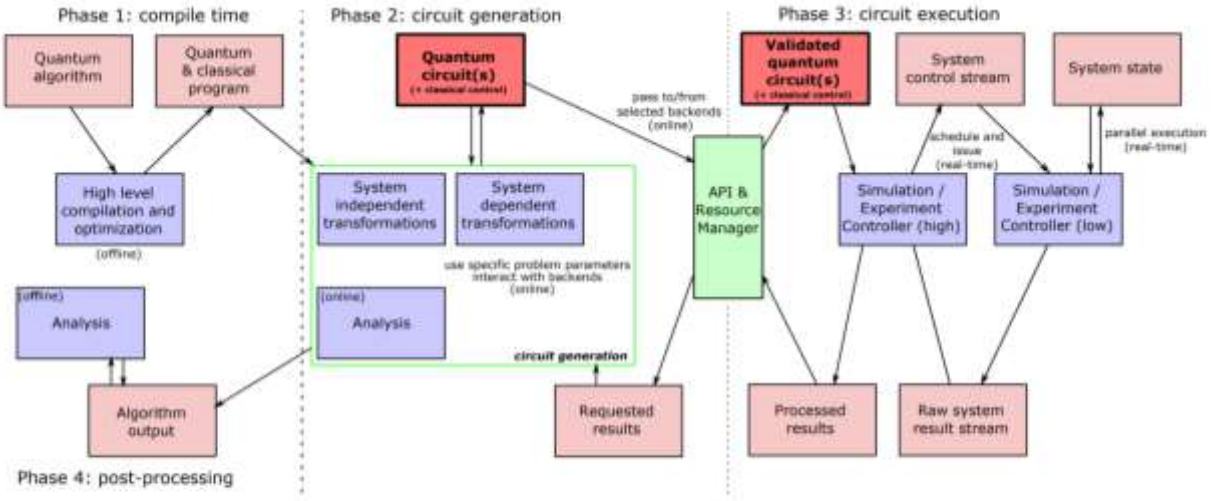


Figure 1: Block diagrams of processes (blue) and abstractions (red) to transform and execute a quantum algorithm. The emphasized quantum circuit abstraction is the main focus of this document. The API and Resource Manager (green) represents the gateway to backend processes for circuit execution. Dashed vertical lines separate offline, online, and real-time processes.

Un langage de scripting de haut niveau associé à OpenQASM est proposé par IBM : **Qiskit**, exploitable en Python, JavaScript et Swift (un langage généraliste d'Apple) et sur Windows, Linux et MacOS. Il a été lancé début 2017 et est publié en open source[483].

Qiskit est fourni avec de nombreux templates et exemples de codes permettant d'exploiter une vaste gamme d'algorithmes quantiques connus. Il comprend une fonction "circuit-drawer" qui génère une visualisation graphique des circuits quantiques programmés en passant par le langage de composition de documents open source LaTeX.

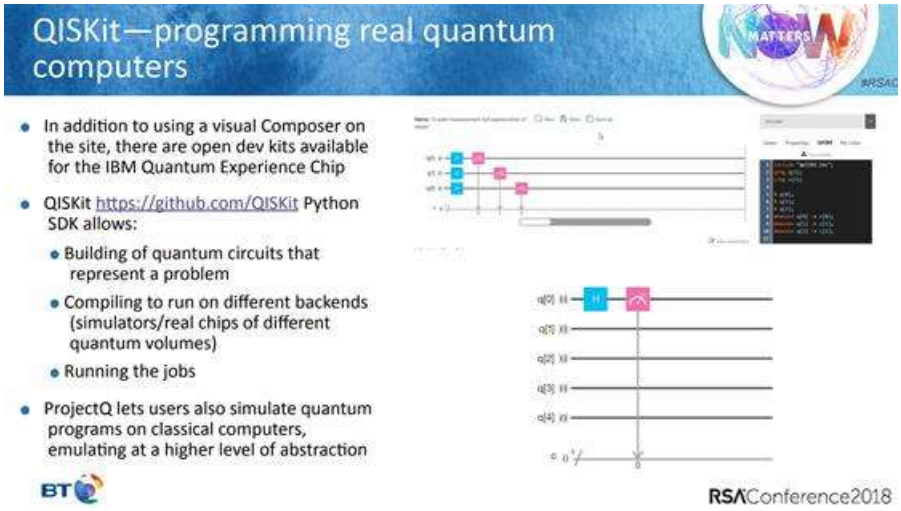
Quatre briques logicielles sont fournies dans Qiskit, la première et la quatrième étant celles d'usage les plus courants :

- Qiskit Terra fournit les principaux éléments de composition de son algorithme quantique.
- Qiskit Aer fournit un simulateur C++ qui permet de simuler des modèles de bruits de qubits.
- Qiskit Ignis est un framework qui permet d'analyser le bruit dans les circuits quantique et de mieux le gérer.
- Qiskit Aqua est une bibliothèque qui permet de développer du code pour des calculateurs NISQ, les premiers ordinateurs quantiques universels (Noisy Intermediate-Scale Quantum selon l'appellation de John Preskill). Elle comprend des algorithmes quantiques pour des applications diverses comme dans la simulation chimique, le machine learning et la finance.

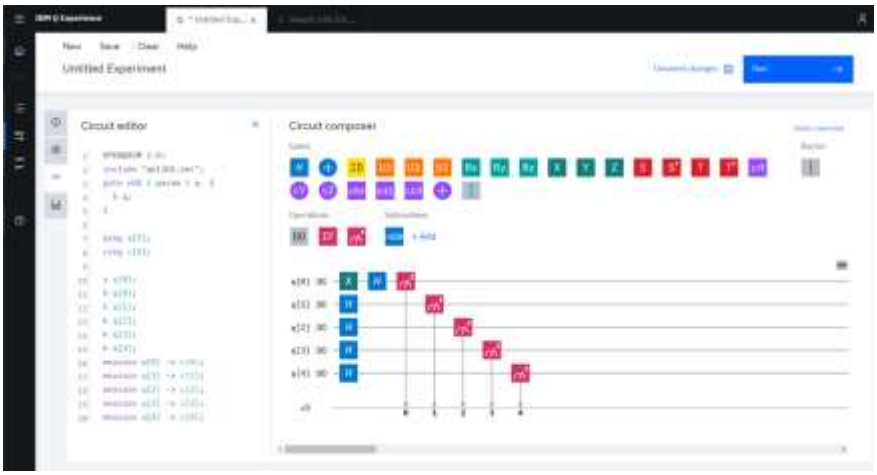
[482] Il est spécifié dans Open Quantum Assembly Language, 2017 (24 pages), ce document décrivant au passage les nombreuses tâches réalisées par le compilateur associé.

[483] Le slide ci-dessus qui décrit Qiskit est issu de la présentation Quantum Computing is Here Powered by Open Source 2018 (41 slides, vidéo).

La compilation du code quantique a ensuite lieu pour exécuter l'ensemble soit sur le simulateur HPC classique en cloud d'IBM soit sur un ordinateur quantique universel comme ceux d'IBM qui sont également accessibles dans le cloud comme Tenerife et Yorktown (5 qubits) ainsi que Melbourne (14 qubits), suivis de versions à 28 qubits lancées en 2020.



L'IBM Quantum Composer permet de programmer graphiquement en ligne son code pour l'exécuter sur un émulateur quantique ou sur les nombreux calculateurs quantiques d'IBM qui sont accessibles en ligne. L'outil permet d'interagir indifféremment avec le code en texte à gauche ou avec sa représentation graphique à droite.



L'émulateur simule pour sa part jusqu'à 32 qubits et il répond bien plus rapidement que les ordinateurs quantiques, en tout cas avec peu de qubits. On peut exécuter son code une fois ou 1024, 4096 ou 8192 fois pour obtenir une moyenne des résultats. Comme les batchs sont soumis les uns après les autres, on peut attendre jusqu'à une demi-heure pour que son code soit exécuté. La création de compte y est gratuite[484].

IBM propose aussi l'application mobile **Hello Quantum** qui permet de programmer avec quelques qubits.

Rigetti

La startup américaine développe des ordinateurs quantiques universels à base de qubits supraconducteurs dans la lignée de ce que fait IBM. Elle propose aussi une plateforme intégrée avec le langage de bas niveau **Quil** qui supporte un modèle de mémoire mixte classique et quantique[485].

Il fonctionne sur Windows, Linux et MacOS. Le langage utilise la classe gates pour décrire les opérations à opérer sur les qubits, indexés de 0 à n-1, pour n qubits et avec des portes quantiques.

---

[484] Les conditions d'utilisation précisent cependant : *"You may not use IBM Q in any application or situation where failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage, such as aircraft, motor vehicles or mass transport, nuclear or chemical facilities, life support or medical equipment, or weaponry systems"*. Sachant qu'avec 5 qubits émulés, il devrait être difficile de faire tout cela.

[485] Il est documenté dans A Practical Quantum Instruction Set Architecture, 2017 (15 pages).

Le langage permet de créer de la programmation conditionnelle en fonction de l'état des qubits. Il est complété par la bibliothèque **pyQuil** open source lancé début 2017 qui est comprend la bibliothèque Grove d'algorithmes quantiques de base (documentation).

Il s'exploite avec le langage de programmation Python. Le pyQuil de haut niveau (assembleur) génère le langage Quil de bas niveau (code machine).

En voici un simple exemple avec un seul qubit activé par une porte de Hadamard qui créé une superposition d'état 0 et 1 permettant de créer un générateur de nombre vraiment aléatoire. Utilisé de manière itérative dans une boucle classique, le programme peut générer une série aléatoire de 0 et de 1 avec 50% de chances d'avoir l'un ou l'autre permettant de créer un code binaire unique complètement aléatoire.

```
# random number generator circuit in pyQuil
from pyquil.quil import Program
import pyquil.gates as gates
from pyquil import api

qprog = Program()
qprog += [gates.H(0),
          gates.MEASURE(0, 0)]

qvm = api.QVMConnection()
print(qvm.run(qprog))
```

porte de Hadamard sur qubit 1

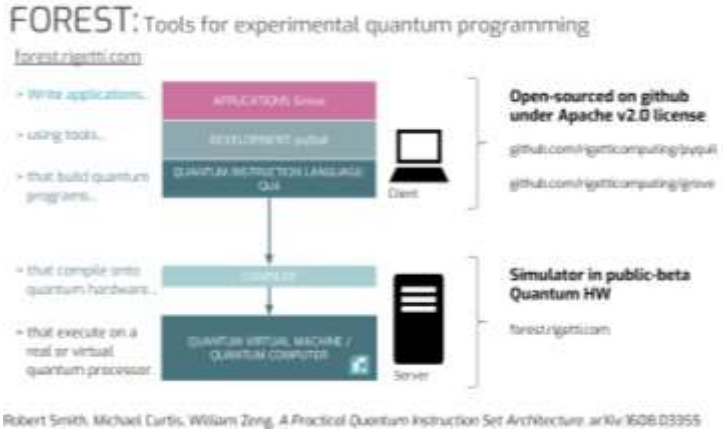
lecture de l'état du qubit superposé

sortie du résultat

Listing 2: pyQuil code for a random number generator.

Rigetti propose l'exécution de programmes quantiques dans ses ordinateurs en cloud et sur des émulateurs classiques via ses QVM, pour **Quantum Virtual Machines**[486].

Quil est utilisable à partir de l'environnement de développement **Forest** proposé par Rigetti. Ces outils sont open source, mais pas multiplateforme. Dommage !



Robert Smith, Michael Curtis, William Zeng, *A Practical Quantum Instruction Set Architecture*, arXiv:1608.03355

Fin 2017, Google et Rigetti, lançaient l'initiative open source **OpenFermion**. Ce framework développé en Python exploite aussi les travaux des universités de Delft (Pays-Bas) et de Leiden.

C'est une solution logicielle de création d'algorithmes quantiques de simulation de fonctions chimiques supportant tout ordinateur quantique, des ordinateurs quantiques universels aux ordinateurs quantiques adiabatiques de D-Wave. C'est une initiative intéressante car elle créé une ouverture multiplateforme sur un domaine d'application clé des ordinateurs quantiques.

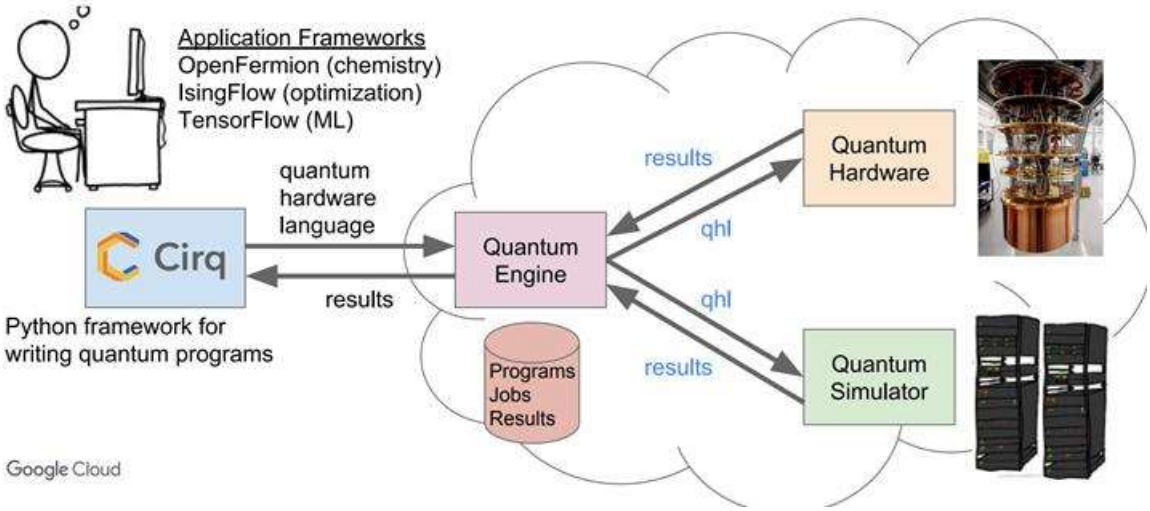
[486] C'est documenté dans pyQuil Documentation, juin 2018 (120 pages) qui contient de nombreux exemples de code comme celui *ci-dessus*.

Elle complète l'approche multiplateforme d'Atos[487]. En 2018, Rigetti lançait enfin un concours d'algorithmes quantiques avec $1M de prix mais avec un biais intéressant, mettant en regard les créateurs d'algorithmes quantiques et d'autres cherchant à en créer des équivalents fonctionnant sur ordinateurs classiques.

Le processus pourrait durer de 3 à 5 ans et n'est pas sans rappeler celui des XPrize[488].

Google

En plus d'OpenFermion qui est plutôt un framework de haut niveau, Google lançait le 19 juillet 2018 son propre langage quantique dénommé **Cirq** en open source. Il cible les NISQ, l'appellation de John Preskill déjà évoquée, des ordinateurs à portes quantiques universelles de taille et performance intermédiaire côté taux d'erreurs. C'est un framework pour Python. Il servira notamment à programmer les ordinateurs quantiques de Google notamment celui de 72 qubits qui a été annoncé en mars 2018 mais n'est toujours pas opérationnel.



source du schéma : An Update on Google's Quantum Computing Initiative, Kevin Kissel, novembre 2018 (40 slides).

Il doit supporter d'autres ordinateurs quantiques, pas encore précisés à ce stade. Il est aussi accompagné d'un simulateur[489]. Un outil de compilation de code OpenFermion en Cirq est aussi proposé.

En mars 2020, Google lançait enfin **TensorFlow Quantum**, une extension du célèbre framework open source pour le développement d'applications de machine learning et deep learning. Elle apporte des fonctions de calcul hybride classique/quantique pour du machine learning[490]. La bibliothèque intègre le support du langage de programmation quantique Cirq de Google.

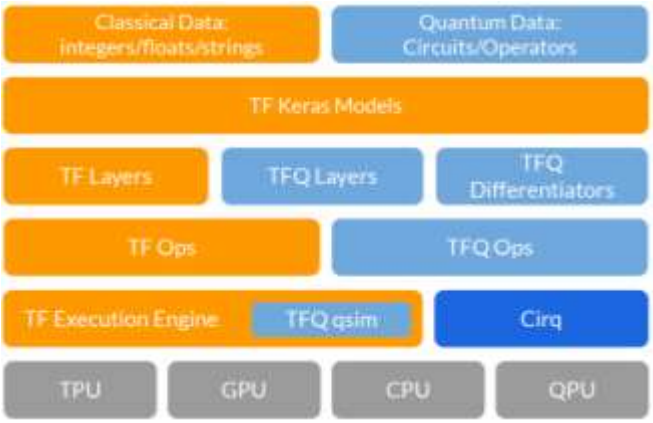
[487] Voir l'annonce en octobre 2017, OpenFermion: The Electronic Structure Package for Quantum Computers, 2018 (19 pages) et la documentation d'Openfermion.

[488] Voir Can You Make A Quantum Computer Live Up To The Hype? Then Rigetti Computing Has $1 Million For You d'Alex Knapp, Forbes, octobre 2018.

[489] Voir les explications dans Google Cirq and the New World of Quantum Programming de Jesus Rodriguez, juillet 2018.

[490] Voir TensorFlow Quantum: A Software Framework for Quantum Machine Learning par M Broughton et al, 2020 (39 pages, et vidéo associée).

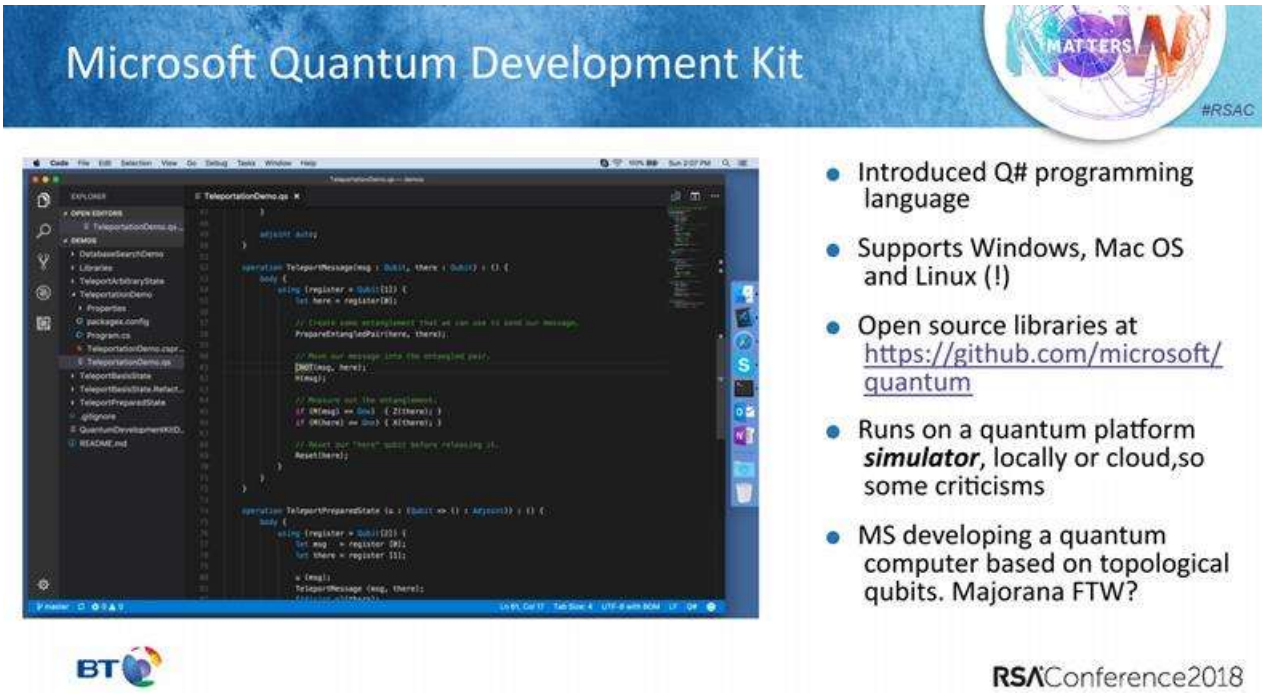
Dans un premier temps, elle est adaptée à l'usage d'émulateurs quantiques fonctionnant sur des ordinateurs traditionnels à base de CPU, GPU et TPU (Tensor Processing Unit, les processeurs spécialisés d'IA des data-centers de Google). A terme, des QPU (Quantum Processing Units) seront supportés. Pourquoi Google ne fait-il pas appel à son ordinateur quantique de 53 qubits ? Parce que c'est un objet de recherche et pas un outil de production intégrable à ce stade dans une offre en cloud.



Microsoft

L'éditeur a d'abord proposé trois briques pour les développeurs avec l'extension **LIQUi|>** du langage de scripting F# qui permet de faire de la simulation de programme quantique.

En décembre 2017, l'éditeur lançait le langage **Q#** qui semble surtout adapté à la programmation d'ordinateurs quantiques topologiques, qui n'existent pas encore, mais sont simulables sur ordinateurs classiques dans le cloud avec jusqu'à 30 qubits.



Q# a une syntaxe dérivée du langage C# de Microsoft[491]. Le tout est fourni sous la forme d'extensions de l'environnement de développement Visual Studio et dans le QDK, pour Quantum Development Kit. Un langage intermédiaire est généré par le compilateur, QIL. Il est censé être multiplateforme mais ne l'est pas encore. Microsoft aura certainement intérêt à rendre multiplateformes ses outils de développement pour capter l'attention et le temps des développeurs.

En juillet 2018, Microsoft lançait aussi **Quantum Katas**, un projet open source contenant des exemples de code quantique en Q# intégrés dans des tutoriels interactifs[492].

[491] Voir Q#: Enabling scalable quantum computing and development with a high-level domain-specific language, 2018 (11 pages).

[492] Voir Learn at your own pace with Microsoft Quantum Katas, juillet 2018.

Ils annonçaient en décembre 2018 une bibliothèque de simulation chimique codéveloppée avec Pacific Northwest National Labs[493], une sorte d'équivalent d'OpenFermion, qui est codéveloppé par Rigetti et Google. La bibliothèque complète le package logiciel de simulation de chimie quantique NWChem de PNNL.

Et en mai 2019, Microsoft annonçait qu'il allait rendre open source ses outils de développement quantiques, donc, au minimum Q# et le Quantum Development Kit.

IonQ

La startup issue de l'Université de Maryland planche sur la création d'ordinateurs quantiques à base d'ions piégés. Nous détaillerons cela plus tard. Comme Rigetti, ils veulent aussi créer une offre logicielle "full stack" adaptée à leur architecture d'ordinateur quantique, et proposée en cloud.

Intel

A ce stade, Intel n'est pas très avancé côté développement de logiciels quantiques. Ils ont créé à ce stade un logiciel de simulation quantique pour ordinateurs classiques[494], les deux premiers auteurs travaillant chez Intel et de dernier à Harvard. Il peut simuler jusqu'à une quarantaine de qubits.

Huawei

Fin 2018, Huawei lançait son propre framework de développement d'application quantique, compatible avec ProjectQ, et comprenant une interface graphique de création d'algorithme. Le tout s'intègre dans leur service en cloud HiQ de simulation quantique[495]. Il est fourni gratuitement pour la simulation allant jusqu'à 38 qubits. On peut aussi y simuler jusqu'à 81 qubits avec une profondeur de traitement de 30 et 169 qubits avec une profondeur de 20 (couches de portes quantiques enchaînables).

Atos

Atos n'est pas encore un fabricant d'ordinateurs quantiques même si leurs partenariats avec divers acteurs tels que le Finlandais IQM et le CEA laissent indiquer que cela pourrait les intéresser. Ils proposent pour l'instant une solution d'émulation de logiciels quantiques à base de machines à processeurs Intel et avec leur propre architecture mémoire optimisée, les aQLM. Ils simulent de 30 à 40 qubits et sont agnostiques vis à vis des architectures de qubits. Depuis juillet 2020, ils proposent une version de cet émulateur plus rapide qui est équipée de GPU Nvidia V100s, dénommé QLMe.

aQASM (Atos Quantum Assemby Programming Language) est un langage de programmation complétant Python qui permet de créer des algorithmes quantiques exécutables sur les émulateurs aQLM ou sur toute architecture physique d'ordinateur quantique à portes universelles (à terme). Le langage permet de définir des portes quantiques utilisant d'autres portes quantiques, l'équivalent des objets, fonctions ou des macros dans la programmation traditionnelle. Source du schéma *ci-dessous*.

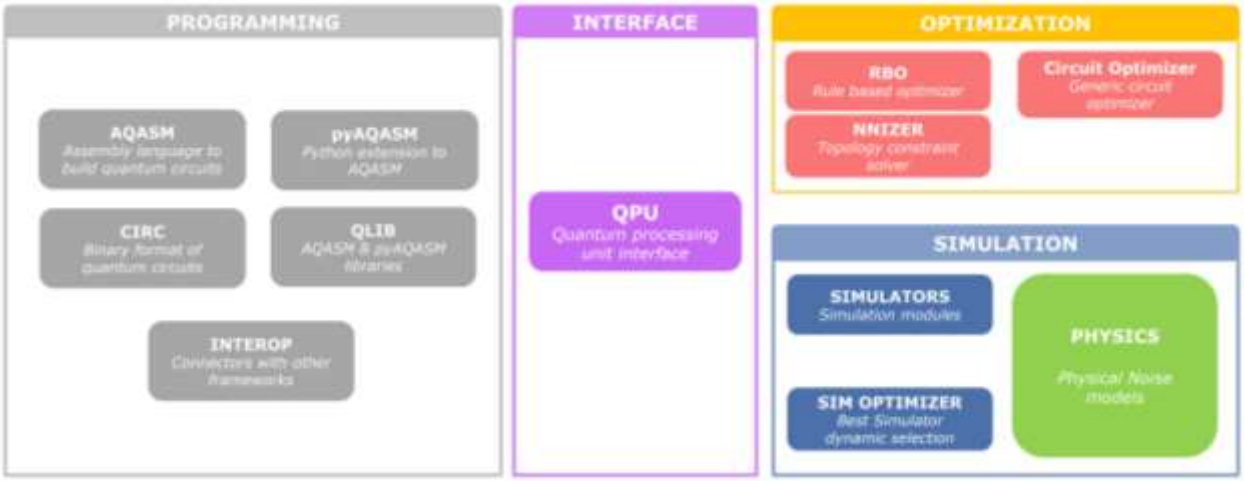
aQASM est une déclinaison du langage standard OpenQASM, évoqué plus haut. Ce langage est complété par une bibliothèque Python dénommée PyAQASM qui permet de générer des fichiers aQUASM. Le langage permet de programmer l'exécution répétitive de portes en boucles et de créer des fonctions réutilisables.

---

[493] Voir Simulating nature with the new Microsoft Quantum Development Kit chemistry library, décembre 2018. Le PNNL est un laboratoire de recherche cofinancé par le Département de l'Energie US et opéré par la fondation à buts non lucratifs Batelle Memorial Institute. Batelle opère de nombreux laboratoires US comme le Lawrence Livermoort National Laboratory, le Los Alamos National Laboratory et le Oak Ridge National Laboratory.

[494] Documenté dans qHiPSTER: The Quantum High Performance Software Testing Environment de Mikhail Smelyanskiy, Nicolas Sawaya, et Alan Aspuru-Guzik, 2016 (9 pages)

[495] Voir Huawei Unveils Quantum Computing Simulation HiQ Cloud Service Platform, octobre 2018.

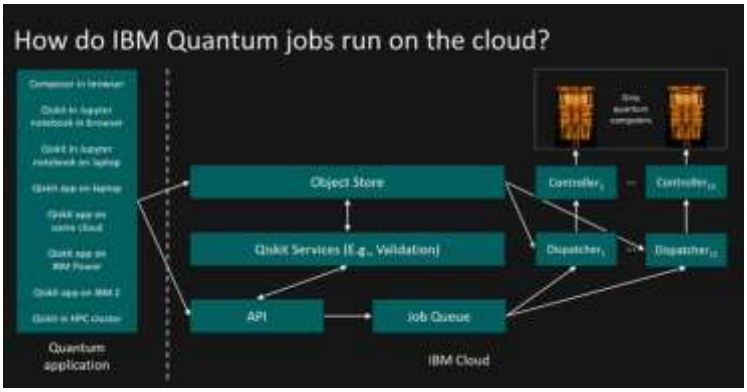


Le compilateur du code aQASM génère un code binaire CIRC qui est le langage pivot de bas niveau, ensuite converti dans le langage de contrôle d'ordinateurs quantiques universels spécifiques ou pour des supercalculateurs de simulation via l'interface QPU (Quantum Processing Unit Interface). Il est complété de plugins d'optimisation divers qui vont éliminer les portes qui ne servent à rien et adapter le code à l'architecture matérielle ciblée.

Cloud

Une bonne partie des calculateurs quantiques sont destinés à être proposés dans des offres de services en cloud. C'est déjà le cas de **D-Wave** avec son offre Leap, de **Rigetti** qui lançait son offre Cloud Services début 2019 et depuis juillet 2020, d'**Honeywell** avec son System Model HØ qui propose 6 qubits à ions piégés dans le cloud et de manière payante.

IBM proposait l'accès cloud à 18 calculateurs quantiques avec 5 à 53 qubits supraconducteurs en date de mai 2020 (*ci-contre*, une explication des briques logicielles de déploiement dans le cloud).

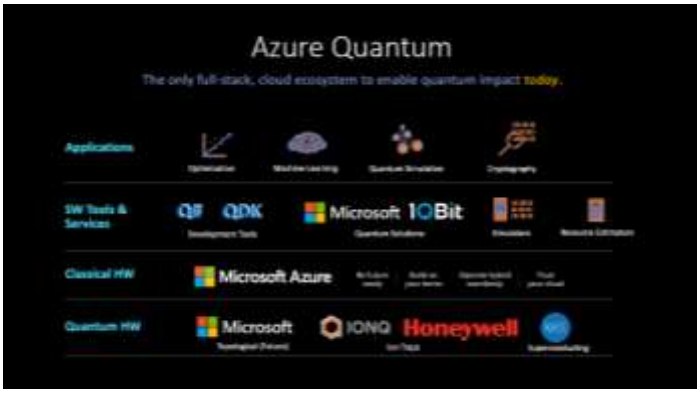


Alibaba a une offre voisine en Chine. On est ici dans le cadre d'offres verticalement intégrées, l'opérateur du service en cloud étant le concepteur des calculateurs quantiques.

Un second type d'offre est relatif aux ressources d'émulation quantique dans le cloud. Elles permettent d'exécuter des algorithmes quantiques sur des supercalculateurs ou data-centers classiques et avec un nombre réduit de qubits supporté. On trouve de telles solutions chez IBM, Microsoft, Google, Alibaba, Huawei et aussi Atos.

Une dernière approche lancée fin 2019 consiste pour des opérateurs en cloud à proposer l'accès à des calculateurs quantiques qu'ils n'ont pas conçus, éventuellement panachés avec des ressources d'émulation quantique sur serveurs classiques. C'est ce qu'ont annoncé quasiment en même temps Amazon et Microsoft fin 2019.

On ne sait pas dire si c'est lié aux lenteurs de la mise au point des fermions de Majorana mais en novembre 2019, **Microsoft** annonçait ainsi intégrer une offre de calcul quantique dans le cloud Azure, et en s'appuyant sur des fournisseurs tiers : **IonQ**, **Honeywell** (ions piégés) et **QCI** (supraconducteurs), sachant qu'aucun de ces trois acteurs n'a de calculateur quantique commercial en magasin.



Ils sont aussi associé à **1QBit** (Canada) pour proposer des briques applicatives logicielles quantiques[496]. Ils font notamment la promotion des algorithmes inspirés par le quantique (« quantum inspired algorithms ») qui s'appuient sur des ressources traditionnelles du cloud comme pour cette étude de cas d'optimisation de scanners d'IRM chez Case Western Reserve University[497]. Il faut toujours prendre ces annonces avec un grain de sel côté disponibilité pratique. Il a fallu en effet attendre mai 2020 pour que Microsoft annonce mettre tout cela à disposition de quelques clients poissons pilotes en mode « preview » !

Amazon se mettait donc aussi au cloud quantique fin 2019 avec trois composantes : l'offre de services en cloud Amazon Braket, l'AWS Center for Quantum Computing rattachée à l'université Caltech[498] et l'Amazon Quantum Solutions Lab, un programme d'évangélisation des clients qui rappelle l'initiative Q d'IBM[499]. Amazon utilise aussi l'appellation Quantum Compute Cloud (QC2) pour son offre. Braket permet l'accès aux ordinateurs quantiques de D-Wave (les 2000Q à 2048 qubits supraconducteurs à recuit quantique), IonQ (configuration non précisée mais probablement leur solution à 79 qubits qui ne fonctionne convenablement qu'avec 11 qubits) et Rigetti (16Q Aspen-4 à 16 qubits supraconducteurs). IonQ se retrouve ainsi proposé par Microsoft et par Amazon. Il est aussi adapté à l'exécution d'algorithmes hybrides associant du calcul classique et du calcul quantique ainsi qu'à de l'émulation d'algorithmes quantiques sur serveurs classiques sans que les configurations matérielles utilisée soient précisées ni les tarifs associés.

Amazon Braket est associé à un SDK maison s'appuyant sur le classique langage Python. Le développement est supporté dans l'environnement intégré open source Jupyter. Il comprend aussi le support du langage de programmation par contrainte OCL (Object Constraint Language). Comme Microsoft, Amazon est aussi partenaire d'éditeurs de logiciels quantiques. On retrouve quasiment les mêmes avec Xanadu, Zapata, Rahko, QcWare, 1Qbit et Qsimulate. Le service était mis en place opérationnellement en août 2020 pour le marché US.

---

[496] Voir Experience quantum impact with Azure Quantum, novembre 2019 et Microsoft Announces Azure Quantum with Partners IonQ, Honeywell, QCI, and 1QBit par Doug Finke, 2019. Microsoft annonçait par la même occasion avoir fédéré de nombreux autres partenaires dans les logiciels quantiques : ProteinQure, Entropica Labs, Jij, Multiverse Computing, Qu&Co, QcWare, OTI, Qubit Engineering, Qulab, QunaSys, Rahko, Riverlane, SolidStateAI, StrangeWorks, Xanadu, Zapata. Sans que leur rôle à chacun soit bien clair dans l'affaire. Voir la liste ici : Quantum Network – A community of pioneers par Microsoft, 2019.

[497] Voir How the quest for a scalable quantum computer is helping fight cancer par Jennifer Langston, juillet 2019.

[498] L'AWS Center for Quantum Computing est dirigé par le Brésilien Fernando Brandao (1983), qui est donc à la fois professeur à Caltech et directeur de ce laboratoire d'Amazon AWS. Il était auparavant chercheur chez Microsoft Research. C'est un bon généraliste puisqu'au départ physicien et maintenant spécialiste des algorithmes quantiques. En juin 2020, John Preskill, aussi enseignant à Caltech, annonçait qu'il allait passer un jour par semaine dans ce centre de recherche.

[499] Voir Amazon Braket – Get Started with Quantum Computing par Jeff Barr, décembre 2019 et la présentation de l'annonce Introducing Quantum Computing with AWS par Fernando Brandao et Eric Kessler (vidéo et slides, où l'on remarque la tour Eiffel d'atomes de Rydberg de la startup française Pasqal en slide 15). J'ai découvert dans les centaines de présentations de la conférence Reinvent d'Amazon de décembre où avait lieu cette annonce de Braket qu'Amazon présentait aussi le QLDB, ou Quantum Ledger Database, une brique logicielle de gestion de blockchain. Mais qui n'a l'air de n'avoir rien du tout de quantique. Et voici un nouveau quantum washing !

Voici un récapitulatif de ces offres de calcul quantique en cloud, faisant la distinction entre l'émulation de code quantique sur calculateurs classiques et exécution de code quantique sur ordinateurs quantiques.

Vue d'ensemble

J'ai essayé de consolider une vue d'ensemble des offres "propriétaires" de programmation quantique, en mettant de côté les langages de programmation fonctionnels et impératifs issus des laboratoires de recherche.

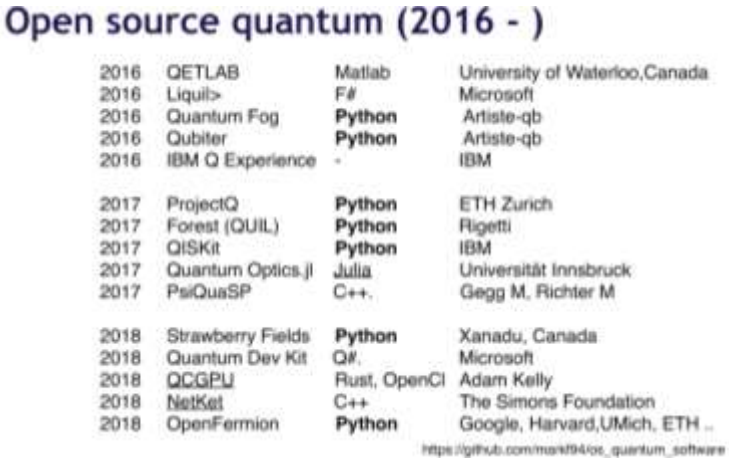
Cela donne le schéma maison suivant qui positionne les outils de développement des grands acteurs du marché en fonction de leur niveau[500]. A l'exception d'Atos, tous ces acteurs ont une approche d'intégration verticale allant du langage de programmation jusqu'aux architectures matérielles de qubits.

universal quantum languages	XAAC						
	ProjectQ				CirqProjectQ		
visual programming and integrated development environments	Q Experience	Forest			Quantum Playground	Visual Studio	
thematic quantum libraries (chemisty, finance, machine learning, ...)	QisKit Aqua	OpenFermion	Quadrant, Qsage, ToQ	PENNYLANE	OpenFermion	Quantum Chemisty PNNL	QLIB
generic quantum libraties / full-stack	QisKit	Grove QAOA	QUBO qbsolv	STRAWBERRY FIELDS	Cirq	Quantum Developer Kit	pyAQASM
high level machine language (quantum circuits)	QisKit Terra	pyquil	QMASM			Q#	AQASM
low level machine language	Open QUASM	quil	QMI	Blackbird	many machine languages		Cirq QPU
qubits and quantum gates	super-conducting	super-conducting	quantum annealing	photons	super-conducting	topologic	any

schema inspired from Alba Cervera-Lierta for the QWA 2018
https://medium.com/@quantum_wa/quantum-computing-languages-landscape-1bc6dedb2a35

[500] Je me suis notamment inspiré du schéma intégré dans l'article Quantum Computing languages landscape, AlbaCervera-Lierta de la Quantum World Association, septembre 2018. Je l'ai complété et y ai ajouté une colonne avec Atos.

Le plus intéressant dans tout cela est que nombreux sont les outils de développement qui permettent de se faire la main sur des algorithmes quantiques à petite échelle avant que de "gros" ordinateurs quantiques soient disponibles. A vous de jouer si le cœur vous en dit ! Et ils sont pour la plupart en open source[501].



Et voici ci-dessous un récapitulatif chronologique de l'apparition des différents outils de développement quantiques[502].

Year	Language	Reference(s)	Semantics	Host Language	Paradigm
1996	Quantum Lambda Calculi	[181]	Denotational	lambda Calculus	Functional
1998	QCL	[206–209]		C	Imperative
2000	qGCL	[241, 312–314]	Operational	Pascal	Imperative
2003	λ_q	[282, 283]	Operational	Lambda Calculus	Functional
2003	Q language	[32, 33]		C++	Imperative
2004	QFC (QPL)	[245–247]	Denotational	Flowchart syntax (Textual syntax)	Functional
2005	QPAlg	[141, 160]		Process calculus	Other
2005	QML	[10, 11, 113]	Denotational	Syntax similar to Haskell	Functional
2004	CQP	[102–104]	Operational	Process calculus	Other
2005	cQPL	[180]	Denotational		Functional
2006	LanQ	[188–191]	Operational	C	Imperative
2008	NDQJava	[298]		Java	Imperative
2009	Cove	[227]		C#	Imperative
2011	QuECT	[48]		Java	Circuit
2012	Scaffold	[1, 138]		C (C++)	Imperative
2013	QuaFL	[162]		Haskell	Functional
2013	Quipper	[114, 115]	Operational	Haskell	Functional
2013	Chisel-Q	[175]		Scala	Imperative, functional
2014	LIQUi|⟩	[292]	Denotational	F#	Functional
2015	Proto-Quipper	[234, 237]		Haskell	Functional
2016	QASM	[212]		Assembly language	Imperative
2016	FJQuantum	[82]		Feather-weight Java	Imperative
2016	ProjectQ	[122, 266, 272]		Python	Imperative, functional
2016	pyQuil (Quil)	[259]		Python	Imperative
2017	Forest	[61, 259]		Python	Declarative
2017	OpenQASM	[66]		Assembly language	Imperative
2017	qPCF	[213, 215]		Lambda calculus	Functional
2017	QWIRE	[217]		Coq proof assistant	Circuit
2017	cQASM	[146]		Assembly language	Imperative
2017	Qiskit	[4, 232]		Python	Imperative, functional
2018	IQu	[214]		Idealized Algol	Imperative
2018	Strawberry Fields	[147, 148]		Python	Imperative, functional
2018	Blackbird	[147, 148]		Python	Imperative, functional
2018	QuantumOptics.jl	[157]		Julia	Imperative
2018	Cirq	[271]		Python	Imperative, functional
2018	Q#	[269]		C#	Imperative
2018	$Q\|SI\rangle$	[174]		.Net language	Imperative
2020	Silq	[35]		Python	Imperative, functional

[501] Voir à ce sujet les présentations de la conférence FOSDEM 2019.

[502] Source : Quantum Software Engineering Landscapes and Horizons par Jianjun Zhao, 2020 (31 pages) qui fait un excellent tour d'horizon des outils de développement couvrant tout le cycle de creation de logiciels quantiques, y compris les épineuses questions du débogage et des tests.

Applications métiers

Les algorithmes évoqués dans une partie précédente sont dans l'ensemble de bien bas niveau. Il reste à les assembler dans des solutions métiers, marché par marché. Le secteur du calcul quantique est encore des plus immatures. Et pour cause puisque les ordinateurs quantiques sont très limités à ce stade.

Nous en sommes aujourd'hui dans une étape équivalente à celle de l'industrie informatique au milieu des années 1950, une époque où l'industrie du logiciel était plus que balbutiante. C'était aussi les débuts de l'intelligence artificielle avec le fameux Summer Camp de Darmouth de l'été 1956 dont certains des travaux, notamment sur la vision artificielle, n'ont pu aboutir que plus de 30 ans après, avec l'invention des réseaux convolutionnels de Yann LeCun, et depuis moins d'une demi-douzaine d'années, grâce aux progrès des GPU et autres processeurs spécialisés.

Evolution du marché

Bien malin serait celui qui prédirait à quelle vitesse les applications quantiques émergeront marché par marché. Suivra-t-elle une exponentielle de croissance du marché fulgurante digne de celles de la microinformatique et des smartphones ?

Je vais tenter l'exercice en reliant cette vitesse à quelques grandes évolutions à venir :

- L'apparition de **calculateurs quantiques universels** de plus d'une centaine de qubits logiques, ce qui pourrait arriver d'ici une dizaine d'années. En parallèle vont continuer à se développer les solutions d'optimisation adaptées aux ordinateurs à recuit quantique de D-Wave.
- La consolidation du marché des **outils de modélisation et de développement** de solutions quantiques. Les outils sont déjà bien nombreux comme nous avons pu le voir dans la partie précédente. Ils vont continuer de gagner en maturation, notamment en élevant leur niveau d'abstraction, et s'adapter aux évolutions du matériel. Des bibliothèques adaptées aux besoins de marchés spécifiques feront sans doute leur apparition comme dans la simulation moléculaire ou la finance.
- La **formation de développeurs** de solutions d'un nouveau genre capables de gérer des abstractions qui n'ont rien à voir avec les différentes formes de programmation procédurale qui dominent l'informatique actuelle, même dans ses variantes de programmation événementielle qui sont courantes dans la création de sites web et applications graphiques. Une nouvelle génération de concepteurs d'algorithmes et de développeurs verra le jour. Ce seront probablement des professionnels jeunes qui auront pu digérer les nouveaux concepts du quantique avec un esprit neuf.
- Les **premiers retours d'expériences** de projets pilotes, déjà engagés, notamment sur D-Wave. On continuera à se poser d'épineuses questions sur la comparaison objective entre algorithmes quantiques, architectures matérielles quantiques et leurs équivalents tournant (ou pas) sur supercalculateurs. Il faudra aussi faire le tri en "proof of concepts" et projets réellement déployés. Dans de nombreux marchés, l'ordinateur quantique sera d'abord un instrument de travail pour les chercheurs.
- L'émergence d'un **tissu de startups** qui dynamisera le marché, probablement légèrement en avance de phase par rapport aux éditeurs de logiciels traditionnels et aux entreprises de services numériques qui ne s'aventureront pas forcément en premier dans ce nouveau monde du quantique. Elles sont peu nombreuses à ce stade comme nous le verrons dans une partie à venir. Les places restent à prendre.

- L'apparition de solutions à base d'ordinateurs quantiques qui auront un **impact sur notre vie de tous les jours**. Donc, des applications grand public. Nous devrions en effet voir les usages du quantique évoluer progressivement des milieux de la recherche, à ceux des entreprises, puis des applications grand public. La première application grand public que l'on peut avoir en tête est celle de l'optimisation des transports. Mais d'autres applications restent à inventer.

Comme avant chaque grande révolution technologique, les prévisions sont difficiles à faire. Aucune de celles qui précédaient l'arrivée des micro-ordinateurs, d'Internet, du web 2.0 ou de la mobilité ont vu juste, notamment sur la hiérarchie d'importance de l'adoption des solutions à la fois dans les marchés grand public et professionnels.

Les prévisions de croissance du business autour du quantique du **BCG** illustrent cette forte incertitude. Elles sont présentées avec plusieurs scénarios : l'un, optimiste, qui fait démarrer la croissance vers 2030 et l'autre, très conservateur, qui le fait décoller seulement après 2040[503].

autres prévisions

$553M en 2023 selon MarketsandMarkets (2017).

$1,9B en 2023 selon CIR et de $2,64B en 2022 selon Market Research Future (2018).

$8,45B en 2024 selon Homeland Security (en 2018)

$10B en 2028 selon Morgan Stanley (2017)

$15B d'ici 2028 selon ABI Research (2018).

Repères :

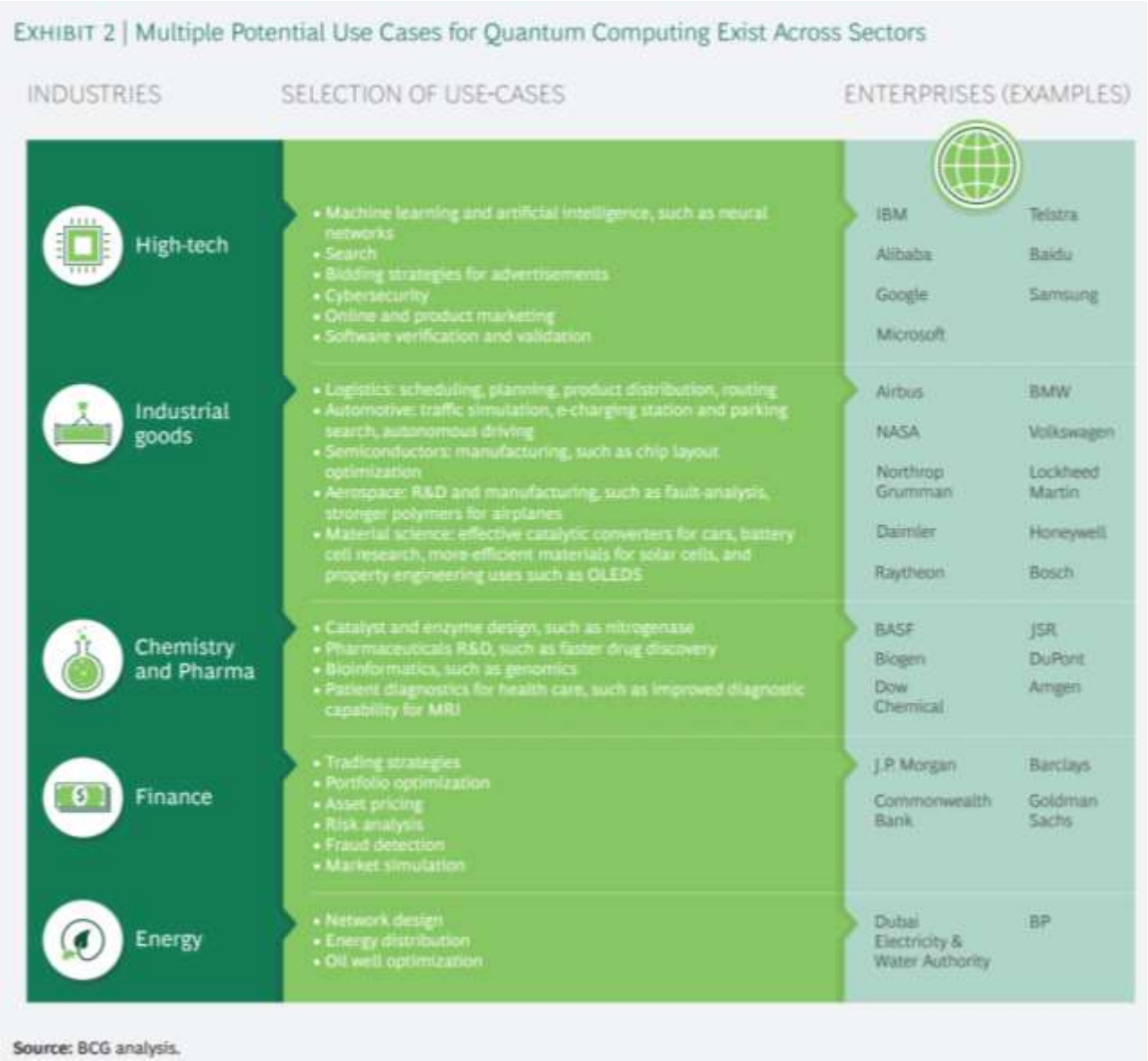
2018 worldwide markets
serveurs : < $90B
logiciel d'entreprise : $431B

Ils n'intègrent visiblement pas le scénario de l'émergence du NISQ, ou "Noisy Intermediate-Scale Quantum", décrit par John Preskill[504]. Il recouvre les calculateurs quantiques à venir dans un futur proche, ayant un nombre intermédiaire de qubits avec un bruit quantique acceptable pour démarrer des applications scientifiques.

Voici cependant ce que nous pouvons nous mettre sous la dent avec un inventaire à date des applications de l'informatique quantique classifiées par secteurs d'activités. Cela couvre à la fois quelques études de cas d'usage du quantique, souvent réalisées avec les seuls ordinateurs quantiques commerciaux, ceux de D-Wave, et sinon, des applications prospectives mais qui attendent encore les ordinateurs quantiques universels de taille critique qui pourront les exécuter.

[503] Dans The coming quantum leap in computing, BCG, mai 2018 (19 pages).

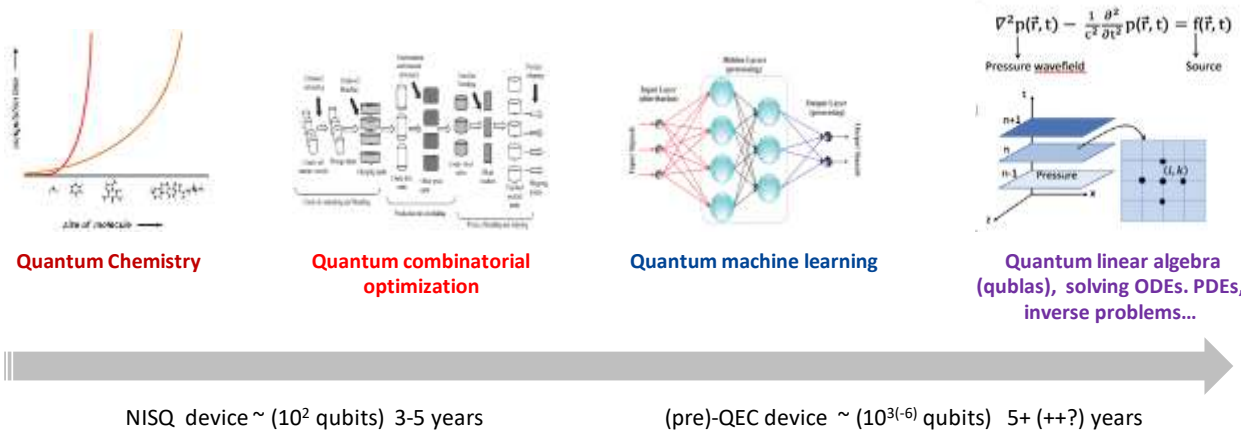
[504] Dans Quantum Computing in the NISQ era and beyond début 2018.



source des panoramas : The Next Decade in Quantum Computing and How to Play du BCG, 2018 (30 pages).

A noter que d'une manière générale, il n'y a pas de corrélation directe entre les applications de l'IA et celles du quantique. Le critère principal de l'intérêt du quantique est la complexité du problème plus que le volume de données à gérer. Le "big data" est loin d'être le cœur d'applications du quantique.

Chez **Total**, on a construit cette roadmap permettant de se faire une idée de l'ordre dans lequel les applications quantiques pratiques vont voir le jour en fonction du nombre de qubits disponibles.



source : Total, QCB Conference, 20 juin 2019

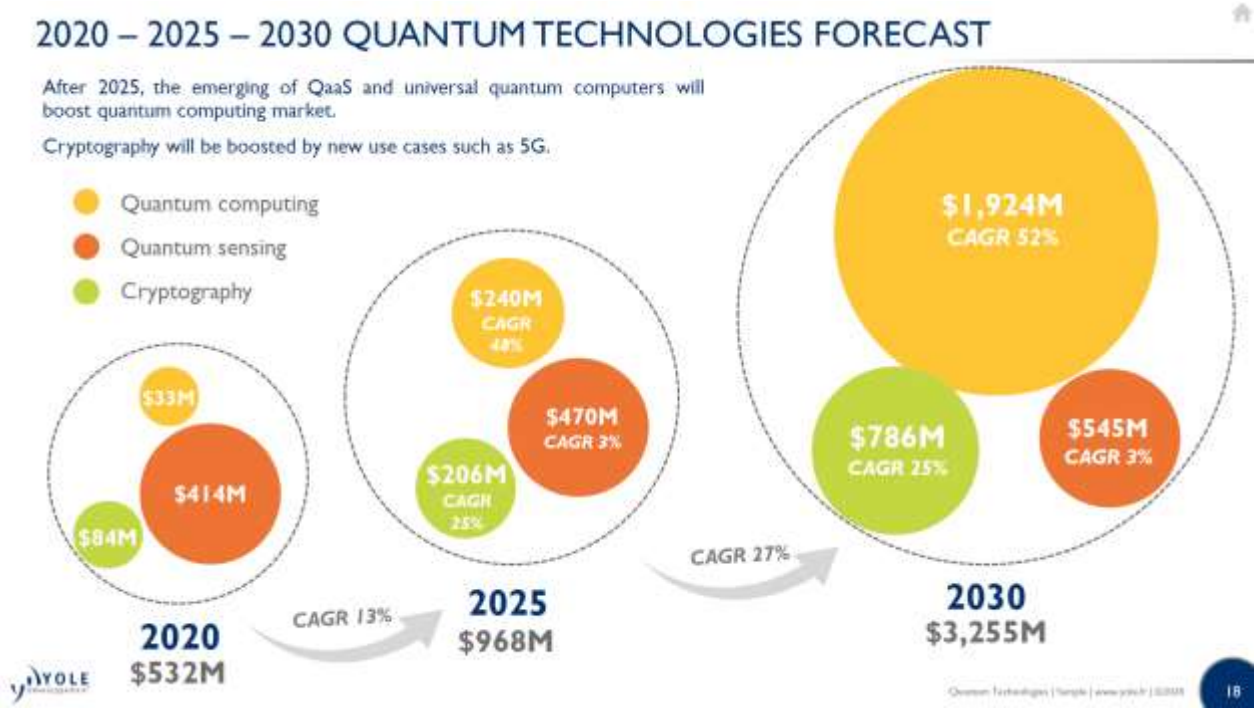
Diverses études de marché ont été publiées pour estimer la taille du potentiel d'affaire dans les technologies quantiques. Elles sont à géométrie variable, intégrant plus ou moins bien la forte incertitude autour du calcul quantique « scalable ».

Cela aboutit à des prévisions légèrement exagérées. Pour **Bank of America**, les technologies quantiques seront aussi importantes que les smartphones. La raison principale ? Les applications potentielles dans la santé. Seul problème : l'analyse à l'origine de ces précisions confond big data et quantique[505].

[505] Voir Quantum computing will be the smartphone of the 2020s, says Bank of America strategist par Chris Matthews, décembre 2019.

Début 2020, **McKinsey** prévoyait de son côté que l'informatique quantique pèserait 1000 milliards de dollars en 2035[506]. Il est facile d'identifier le biais chiffré de cette étude. Elle utilise un truc que l'on a connu il y a quelques années pour l'évaluation du marché des objets connectés et de l'intelligence artificielle. Cette évaluation ne porte pas sur le marché proprement dit des technologies quantiques mais sur le chiffre d'affaires généré par les entreprises qui feront appel à ces technologies, comme dans la santé, la finance ou les transports. C'est un peu comme si on évaluait le marché du logiciel (qui était d'environ $450B en 2019, source Gartner) en totalisant le chiffre d'affaire des entreprises qui utilisent du logiciel ! Ce qui ferait un montant bien plus élevé[507].

Une étude plus sérieuse du cabinet d'analyse français **Yole Development**[508] fait des prévisions plus précises portant sur le marché direct des technologies quantiques, avec un passage à $3,2B par an d'ici 2030, avec 17% de croissance annuelle moyenne, dont $650M de matériel, $1,37B de logiciels en cloud et $785M pour de la cryptographie quantique (QKD). Le marché des capteurs passerait de $400M en 2019 à $545M en 2030. Cette dernière croissance modérée me semble un peu faible car les capteurs quantiques sont les objets quantiques sur lesquels pèsent les plus faibles incertitudes technologiques et c'est un marché qui démarre à peine.



Ces études permettent indirectement de justifier les investissements dans de nouvelles technologies aussi bien au niveau des états que des investisseurs du secteur privé. Ce sont des prévisions qui ambitionnent d'être autoréalisatrices. Elles se heurteront néanmoins à la vitesse des progrès scientifiques dans le domaine.

Santé

Le secteur de la santé et plus précisément des biotechs est celui auquel on pense le plus pour développer les usages du calcul et de la simulation quantiques. C'est l'un des marchés verticaux où l'on trouve le plus grand nombre de startups dédiées.

---

[506] Voir L'informatique quantique pèsera 1000 milliards de dollars en 2035, selon McKinsey, mars 2020.

[507] Analyse partagée dans McKinsey Forecasts Quantum Computing Market Could Reach $1 trillion by 2035, avril 2020.

[508] Voir Quantum technologies: a jump to a commercial state, Yole Development, 2020 et leur sample de rapport Quantum Technologies Market and Technology Report 2020 –Sample, 2020 (22 slides). Ils se sont d'ailleurs inspirés de cet ouvrage pour deux slides : le 9 et le 14, ce dernier ayant été pompé tel que sans citation. Ce n'est pas bien !

Les grands laboratoires pharmaceutiques évaluent les technologies disponibles depuis quelques années en ayant commencé par conduire quelques projets pilotes sur des D-Wave.

Le rêve consiste à étendre les capacités des supercalculateurs d'aujourd'hui avec des calculateurs et simulateurs quantiques pour simuler les molécules du vivant « in silico », afin, principalement, de créer ou découvrir de nouveaux traitements. C'est le domaine de la « *in-silico drug discovery* ».

Le Graal consisterait à comprendre comment fonctionnent l'assemblage puis les opérations des ribosomes, ces complexes moléculaires comprenant 73 protéines et quatre grandes molécules d'ARN. Les ribosomes servent à fabriquer les protéines dans nos cellules à partir du code de l'ARN messager, lui-même synthétisé à partir de l'ADN. De milliers de ribosomes opèrent dans chaque cellule vivante et ils comprennent chacun plus de 250 000 d'atomes[509].

Cela s'inscrit dans une situation inquiétante pour les laboratoires qui découvrent de moins de nouveaux traitements. Le cycle de vie allant de la découverte à la mise sur le marché est de plus en plus onéreux, notamment pendant les phases de tests cliniques. Il coûte jusqu'à un milliard de dollars si ce n'est plus et les taux d'échecs sont nombreux. 45% des tests cliniques de thérapies cancéreuses échouent en phase III aux USA, et 97% des nouvelles thérapies testées ne sont pas approuvées par la FDA ! Si on pouvait mieux simuler numériquement les effets de traitements en amont des tests cliniques, on pourrait peut-être en augmenter le taux de succès.

C'en est au point où l'une des priorités est devenue, non pas la découverte de nouveaux traitements, mais le reciblage thérapeutique de traitements existants. Ils permettent d'accélérer les tests cliniques puisque l'on connaît à priori déjà leurs effets indésirables. Sachant que cela n'a pas empêché la longue polémique autour de la chloroquine en 2020.

Dans tous les cas de figure, le secteur a besoin d'outils de simulation et en particulier d'outils de simulation moléculaire. Pour créer des molécules, des plus simples (peptides) aux plus compliquées (protéines, anticorps, vaccins). Pour les modéliser en 3D. Pour analyser leurs interactions via leurs sites actifs avec les cibles à traiter comme des protéines de surfaces de cellules (glycoprotéines transmembranaires)[510]. Et aussi pour identifier des contre-indications. On peut créer de tels traitements ex-nihilo, mais le plus souvent, on le fait en partant d'un existant (protéine connue, enzyme, biomimétisme, …).

Les simulations moléculaires s'appuient sur le domaine de la chimie computationnelle. Celui-ci prend ses sources avec la description de la nature des liaisons chimiques par **Linus Pauling** à partir de 1928, qui lance le vaste champ de la chimie quantique. Il intervenait juste après la création de l'approximation de **Born-Oppenheimer** de 1927 (le Max Born de l'explication probabiliste de l'équation de Schrödinger et le Robert Oppenheimer de la bombe atomique) qui simplifiait l'équation de Schrödinger pour une molécule en séparant les noyaux des atomes des électrons. La même année avait été créé le modèle Thomas–Fermi de **Llewellyn Thomas** (1903-1992, Anglais) et **Enrico Fermi** (1901-1954, Italo-Américain) qui décrivait la structure électronique de systèmes à plusieurs corps (atomes).

[509] On voit souvent évoquer le nombre de 2,5 ou 3,5 millions d'atomes, mais c'est faux. Ce sont des « Daltons » qui sont des équivalents d'un douzième de la masse du carbone 12, soit à peu près la masse d'un atome d'hydrogène. Or, ces molécules organiques contenant en plus de l'hydrogène, beaucoup de carbone, d'azote, de phosphore et d'oxygène. Ces derniers contribuent à une bonne part de la masse de la molécule, d'où le fait qu'il faut diviser à peu près le nombre de daltons par 10 pour obtenir le nombre d'atomes d'une molécule organique.

[510] On pourrait ambitionner de simuler numériquement le fonctionnement d'une cellule entière avec l'ensemble de ses organelles. Cela devient assez compliqué dans la mesure où une cellule vivante comprendrait en moyenne 100 trillions d'atomes.

Le champ de la chimie computationnelle prend ses sources, bien plus tard, en 1964, avec la création des deux théorèmes Hohenberg–Kohn par **Walter Kohn** (1923-2016, Autrichien puis Américain) et **Pierre Hohenberg** (1934-2017, Franco-Américain). C'était suivi de près par les équations de **Kohn-Sham** (Lu Jeu Sham (1938, Chinois)) en 1965. Ils constituent les bases de la **DFT** (Density Functional Theory), un modèle mathématique permettant de décrire la structure de molécules au repos en fonction des interactions inter-atomiques et de la structure de leurs nuages d'électrons. Et de manière plus simple qu'avec l'équation de Schrödinger qui manipule trop de variables.

Walter Kohn a obtenu le prix Nobel de Chimie en 1998 pour ces travaux, en compagnie de **John Pople** (1925-2004, Anglais) qui avait contribué à la modélisation des orbitales électroniques dans les molécules.

La DFT fut suivie par les travaux de **Martin Karplus** (1930, Américain), **Michael Levitt** (1947, Israélo-Américain) et **Arieh Warshel** (1940, Israélo-Américain) qui contribuèrent à la modélisation numérique des réactions chimiques dans les années 1970. Ils obtinrent le Prix Nobel de Chimie en 2013 pour ces travaux. Le modèle de la DFT a été aussi simplifié par **Axel Becke** (1953, Canadien) en 1993 dans la DFT hybride.

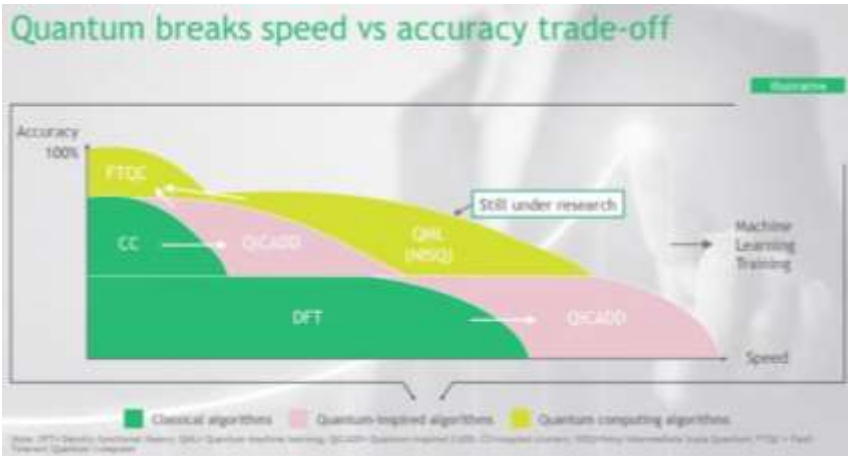
La simulation moléculaire fait face à des effets quasi-quantiques liés aux vibrations continues des molécules dans leur milieu aqueux[511]. Les liaisons chimiques oscillent à une fréquence d'une femto-seconde, les atomes vibrent collectivement à une picoseconde. Par contre, les processus chimiques plus complexes comme la production et le repliement de protéines s'étalent sur des échelles allant de la micro-seconde à la seconde.

Aujourd'hui, l'essentiel des calculs de simulation moléculaires sont réalisés avec des algorithmes adaptés aux supercalculateurs classiques, exploitant de plus en plus des GPU comme ceux de Nvidia ou les TPU de Google. Les premiers tests à petite échelle de simulation par algorithmes quantiues ont été réalisés sur D-Wave et calculateurs quantiques à qubits supraconducteurs.

Les simulateurs quantiques « analogiques » sont aussi des machines adaptées à la simulation de l'interaction des atomes au sein de molécules. L'approche la plus couramment utilisée, comme pour le QML (Quantum Machine Learning) est l'usage de calcul hybride associant des supercalculateurs et des processeurs quantiques.

[511] Voir Biologie quantique : le repliement des protéines reposerait sur la nature ondulatoire de la matière par Laurent Sacco, décembre 2019.

Les cabinets de conseil comme le BCG présentent ainsi des roadmaps de la simulation moléculaire étalées dans le temps et suivant le rythme d'évolution des calculateurs quantiques entre aujourd'hui, le NISQ (calcul bruité de taille intermédiaire) et le LSQ (large scale quantum computing appelé aussi FTQC pour fault-tolerant quantum computing)[512].



L'une des approches du calcul consiste à s'appuyer sur des frameworks génériques pouvant être distribués sur du calcul classique en architecture massivement parallèle puis, progressivement, sur du calcul quantique.

C'est le cas du framework **Tinker-HP** cocréé par Jean-Philip Piquemal, cofondateur de **Qubit Pharma**[513].

La plupart des startups du secteur (**ApexQubit**, **HQS Quantum Simulations**, **MentenAI**, **ProteinQure** et **Qulab**) adoptent des approches de calcul hybride, ne serait-ce que pour avoir quelque chose de pratique à commercialiser[514]. Comme dans le machine learning, l'une des méthodes hybrides la plus courante est la VQE (Variational Quantum Eigensolver)[515]. Une autre méthode se développe consistant à créer des algorithmes classiques qui s'inspirent des algorithmes quantiques. On parle ainsi de « quantum inspired »[516]. Le calcul quantique et quantum inspired complète le vaste champ de l'usage du machine learning qui est déjà très courant dans la découverte de molécules thérapeutiques[517].

La simulation peut porter sur l'articulation de molécules organiques simples comme le cholestérol ou le repliement des protéines qui est de plusieurs ordres de grandeur plus complexe[518]. Cette dernière prouesse relève donc du très long terme. Aujourd'hui, on arrive à simuler des peptides avec une dizaine d'acides aminés. Et les meilleurs algorithmes requièrent un nombre de qubits qui évolue selon la puissance 4 du nombre d'acides aminés[519]. Cette simulation est aussi à la limite du faisable en termes de complexité car elle est dans la classe des problèmes NP-Complet comme vu dans la partie dédiée aux théories de la complexité, à partir de la page 249.

---

[512] Voir Will Quantum Computing Transform Pharma R&D par Jean-Francois Bobier, avril 2020 (14 slides) et la version écrite Will Quantum Computing Transform Biopharma R&D? par Jean-François Bobier et al, décembre 2019. C'est la source des schémas de cette page.

[513] Voir Computational Drug Design & Molecular Dynamics par Jean-Philip Piquemal, avril 2020 (28 slides) et Tinker-HP: a massively parallel molecular dynamics package for multiscale simulations of large complex systems with advanced point dipole polarizable force fields par Louis Lagardère, Jean-Philip Piquemal et al, 201817 (17 pages).

[514] Voir Can Quantum Computing Play a Role in Drug Discovery? At least one Startup Thinks so par James Dargan, 2020, qui évoque le cas de Menten AI.

[515] Voir Quantum Chemistry and the Variational Quantum Eigensolver par S Kokkelmans et al, décembre 2019 (56 pages).

[516] Voir Quantum and Quantum-inspired Methods for de novo Discovery of Altered Cancer Pathways par Hedayat Alghassi et al, 2019 (27 pages)

[517] Voir Concepts of Artificial Intelligence for Computer-Assisted Drug Discovery par Xin Yang et al, 2019 (75 pages). Un bon papier de synthèse avec 879 références bibliographiques à donner le tourni !

[518] Voir Designing Peptides on a Quantum Computer par Vikram Khipple Mulligan, septembre 2019 (20 pages) qui présente Rosetta, un outil de conception quantique de protéine fonctionnant sur D-Wave.

[519] Voir Resource-Efficient Quantum Algorithm for Protein Folding par Anton Robert et al, août 2019.

La recherche de thérapies porte à 78% sur des molécules légères de moins de 900 Daltons, soit environ une centaine d'atomes. Sa fonction est de s'associer à une cible dans les cellules, souvent une protéine bien déterminée qui contrôle un métabolisme que l'on veut atténuer ou amplifier[520]. La découverte de petites molécules de quelques dizaines d'atomes pourrait rentrer dans le champ du possible des ordinateurs quantiques NISQ d'ici quelques années seulement.

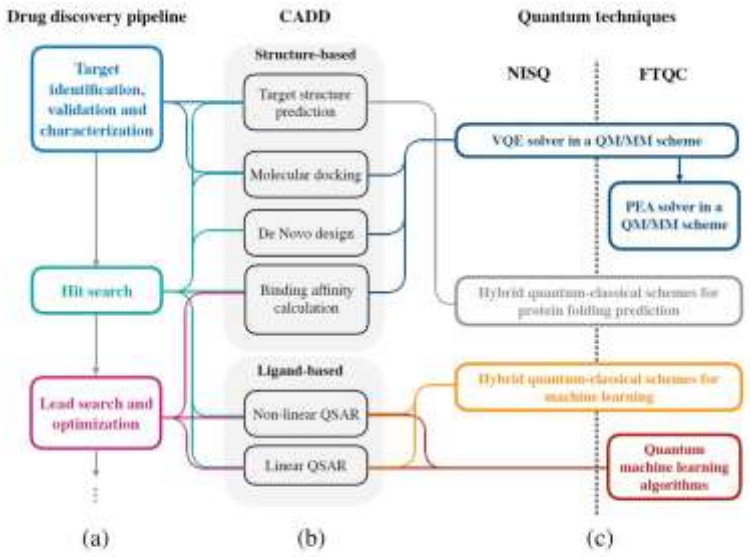


Fig. 1. (a) General workflow of drug discovery process. Here we focus on the early phase where computationally intensive quantum chemical analyses are involved. (b) Components of each stage of drug discovery that heavily involve quantum chemistry or machine learning techniques. (c) Quantum techniques that can be applied to the components listed in (b) and potentially yield an advantage over known classical methods. Here we make the separation between techniques for noisy intermediate scale quantum (NISQ) devices [21] and fault-tolerant quantum computing devices.

Les premières expérimentations de simulation moléculaire ont été réalisées sur des D-Wave. Ils sont adaptés à la recherche de minimums énergétiques, ce qui peut convenir en théorie à la simulation de l'organisation de molécules.

Une collaboration a ainsi été lancée en juin 2017 entre **Biogen**, la société de logiciels quantiques canadienne **1QBit** et **Accenture** pour la création de nouvelles molécules. **Biogen** (1978, USA) est une entreprise de biotechs de taille intermédiaire avec ses 7300 collaborateurs spécialisée dans le traitement de maladies neurodégénératives et de leucémies.

Leur usage du quantique visait le reciblage de molécules thérapeutiques. Il s'agit de trouver des correspondances entre des traitements existants et des cibles thérapeutiques, ici, dans les maladies neurodégénératives ou inflammatoires.

L'Américain **Amgen** est aussi actif dans la recherche de nouvelles thérapies mais sans grandes précisions publiques à ce stade. Ils sont partenaires depuis 2020 de la startup **QSimulate** (2018, USA).

Toujours sur des ordinateurs à recuit quantique de D-Wave, une application d'optimisation de radiothérapie a été expérimentée (*ci-contre*). Le principe consiste à minimiser l'exposition des patients aux rayons X tout en optimisant leur efficacité. C'est un problème complexe de simulation de diffusion d'ondes électromagnétiques dans le corps humain.

[520] Voir Potential of quantum computing for drug discovery par Alan Aspuru-Gusik et al, 2018 (18 pages). CADD = Computer Aided Drug Design. Le schema drug discovery pipeline / CADD / quantum techniques en est issu.

En juin 2019, **Merck** annonçait un partenariat de trois ans avec la startup **HQS Quantum Simulations** basée à Karlsruhe en Allemagne pour le développement d'algorithmes quantiques de simulation chimique.

A l'origine de sa propre société de conseil **Eigenmed**, David Sahner est un des promoteurs de la médecine de précision à base de techniques de machine learning de prédiction exploitant le quantum annealing de D-Wave[521]. Les exemples qu'il met en avant n'ont pas l'air d'être dimensionnés au point d'être réalisables uniquement sur D-Wave et pas de manière classique.

Omnicom Healthcare n'hésitait pas de son côté à promouvoir en 2017 l'usage du quantique dans la santé dans un libre blanc ne contenant strictement aucune information pertinente sur le sujet, ce d'autant plus qu'ils ont l'air de confondre les applications du machine learning analysant les données issues d'objets connectés avec la capacité des ordinateurs quantiques à gérer des problèmes intractables par les ordinateurs traditionnels[522].

La **DNA-Seq Alliance** associe la startup DNA-Seq et D-Wave, qui fait aussi du reciblage de molécules en associant génomique, cristallographie des protéines kinase, du calcul quantique et de la recherche de traitements efficaces en cancérologie.

Comme pour toute nouvelle technologie, les spécialistes du calcul quantique doivent apprendre à dialoguer avec les spécialistes de la bio-informatique. Heureusement, ces derniers font déjà le pont entre la biologie moléculaire et l'informatique et sont assez bien placés pour faire l'apprentissage des méthodes quantiques[523].

En dernier lieu, la pandémie du covid-19 a donné lieu à un regain d'intérêt pour le calcul quantique. Plusieurs acteurs du marché ont un peu mis la charrue avant les bœufs de ce point de vue-là. D-Wave a ainsi offert du temps de ses machines en cloud pour les chercheurs dans le domaine. En pratique, ce sont les supercalculateurs classiques qui ont contribué à faire du criblage de molécules pour la recherche de thérapies et pour réaliser des modèles 3D du covid et en particulier de ses glycoprotéines qui s'accrochent aux membranes des cellules humaines pour les attaquer et s'y reproduire à l'intérieur[524]. Mais dans un futur plus ou moins lointain, le calcul quantique aura probablement son mot à dire dans des pandémies du même genre[525].

Energie et chimie

Lorsque l'on s'éloigne des molécules organiques et du vivant, tout devient soudainement presque réaliste dans le calcul quantique ! En effet, les structures moléculaires que l'on souhaite étudier et simuler sont généralement plus simples que la chimie organique du vivant[526].

Les premières applications envisagées et plausibles concernent la création de matériaux innovants. Le secteur de l'énergie et de la chimie est intéressé par la résolution de problèmes complexes d'analyse et d'optimisation et par la simulation in silico de molécules et structures cristallines, et pour créer de nouveaux matériaux. Comme dans de nombreux domaines, les premières études de cas ont d'abord été réalisées avec les ordinateurs à recuit quantique de D-Wave. Ceux-ci semblent bien indiqués pour des simulations d'interactions atomiques dans des matériaux même si les accélérations qu'ils procurent ne sont pas forcément extraordinaires.

---

[521] Voir Predictive Health Analytics de David Sahner, 2018 (54 slides).

[522] Voir Exponential Biometrics: How Quantum Computing Will Revolutionize Health Tracking, 2017 (7 pages).

[523] Voir Thirteen tips for engaging with physicists, as told by a biologist par Ken Kosik, janvier 2020 qui décrit la manière de rapprocher les physiciens et les biologistes.

[524] Voir un exemple dans TACC Supercomputers Run Simulations Illuminating COVID-19, DNA Replication, mars 2020.

[525] Voir Covid-19: Quantum computing could someday find cures for coronaviruses and other diseases par Todd R. Weiss, avril 2020.

[526] Voir Enabling the quantum leap Quantum algorithms for chemistry and materials Report, janvier 2019 (115 pages) qui fait un bon tour d'horizon des méthodes de simulation chimique. C'est un compte-rendu d'un workshop organisé par la NSF.

Les simulations aussi peuvent toucher les flux d'air, d'eau et de tous liquides et notamment leurs turbulences. Elles peuvent notamment exploiter les fameuses équations de Navier-Stokes[527].

IBM simulait en septembre 2017 sur ordinateur quantique supraconducteur à 16 qubits le fonctionnement de molécules d'hydrure de bérylium et leur équilibre énergétique minimum, ce qui ne sert à rien en soi, mais est un bon début[528]. L'arrivée d'ordinateurs quantiques universels dépassant les 50 qubits chez IBM et Google rend possible leur usage dans ces domaines, et pour des structures atomiques un peu moins simples.

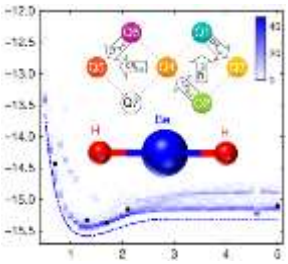
Les recherches vont bon train pour créer des batteries plus efficaces côté densité énergétique et vitesse de charge[529]. La simulation intervient le plus souvent pour comprendre le fonctionnement des réactions chimiques qui interviennent sur les cathodes et anodes et en particulier dans les structures cristallines d'intercalation et pour trouver le moyen d'améliorer la densité énergétiques et d'éviter les phénomènes d'usure des batteries. C'est l'un des axes de recherche de Volkswagen qui prévoit de faire cela à terme avec les ordinateurs quantiques de Google comme documenté dans cette annonce de novembre 2017.

La capture du carbone est un autre enjeu et des chercheurs simulent son fonctionnement moléculaire par biomimétisme. C'est un domaine d'application mis en avant par les chercheurs de Microsoft.

Chez le chimiste allemand **BASF**, l'idée est de simuler des polymères de synthèse, d'abord sur des supercalculateurs HP, puis à terme sur ordinateurs quantiques. **Dow Chemicals** collabore depuis 2017 avec l'éditeur de logiciels canadien **1Qbit** pour créer de nouvelles molécules, en s'appuyant sur les D-Wave.

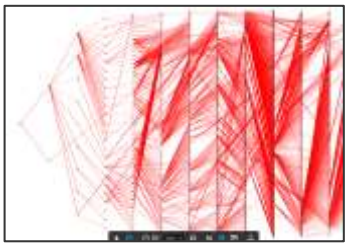
EDF est une autre grande entreprise française qui étudie de très près les usages du calcul quantique : l'évaluation de l'usage de matériaux, des statistiques de sécurité, l'optimisation combinatoire pour la gestion de smart grids et la gestion de batteries.

material ageing modelling



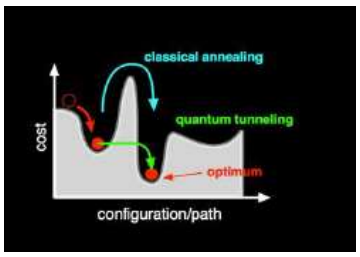
- Modelling ageing phenomena's with quantum physic laws.
- Stake : foresee material ageing patterns to gain operational margin.
- Contribute to regulatory studies for ASN IRSN

safety probabilistic study



- Decision support tool for real time risk analysis
- Recalculate risk based on operation current state and maintenance operation
- Avoid roll back in case uninttended events

combinatorial Optimization for energy management



- Smart charging : optimizing VEs charging for the grid operator/charging operator/user Decentralized energy systems, exploiting large data volume

source : EDF, QCB Conference, 20 juin 2019

[527] Voir Quantum Navier–Stokes equations, de Pina Milišić de l'Université de Zagreb, 2012 (12 pages) et Navier–Stokes equations using Quantum Computing, juillet 2020.

[528] Voir Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets, octobre 2017 (22 pages).

[529] Voir The Promise and Challenges of Quantum Computing for Energy Storage (4 pages).

En 2019, la **Dubai Electricity and Water Authority** (DEWA) planchait avec Microsoft pour résoudre des problèmes complexes de distribution d'énergie et d'eau. Il ne s'agissait que de tester quelques algorithmes sur des émulateurs Intel tournant sur Azure. Et pour cause, Microsoft ne disposait pas encore d'ordinateur quantique de son cru[530]. En 2020, la DEWA annonçait se former au calcul sur D-Wave. Monde d'infidèles[531] !

Chez **BP**, on travaille à la conception d'algorithmes d'optimisation de la prospection pétrolière. Il s'agit d'exploiter les données de différents capteurs, notamment sismiques, pour consolider des modèles de simulation de ce que le sol recèle.

Total est un des grands industriels français à s'intéresser de très près aux usages du calcul quantique. Ils veulent aussi optimiser la prospection et l'évaluation des réserves à partir de sondes sismiques. Ils envisagent de traiter les problèmes d'optimisation complexes du type **MINLP** (Mixed Integer Non Linear programming[532]) pour optimiser le raffinage, la planification, la production et le transport. Enfin, ils s'intéressent aussi à la simulation chimique quantique. La société a déjà une équipe d'une quinzaine de chercheurs et ingénieurs investis dans les applications du calcul quantique[533].

Ils annonçaient un partenariat avec **CQC** (UK) en 2020 pour développer des solutions de capture du carbone[534].

ExxonMobil était pour sa part l'une des grandes entreprises associées à IBM dans l'IBM Q Network, une communauté de grandes entreprises et laboratoires de recherche intéressés par les applications du calcul quantique.

D'autres industriels tâtent aussi du quantique. **Dow Chemical** est partenaire de **1Qbit** depuis juin 2017 pour des projets pilotes de simulation chimique quantique. **BP** s'intéresse aux applications de la cryptographie quantique (QKD) avec le Suisse **IDQ**. Enfin, **Mitsubish Chemical** ainsi que la filiale **Materials Magic** d'**Hitachi Metals** teste aussi le calcul quantique, avec IBM.

Transports

Au-delà des questions énergétiques évoquées ci-dessus, le marché des transports est surtout intéressé par les algorithmes d'optimisation de systèmes complexes[535].

En ligne de mire, l'optimisation de la planification de flottes d'avions pour le transport aérien, pour maximiser la capacité à répondre à la demande tout en optimisant le taux de remplissage des avions.

Le calcul quantique permet aussi l'optimisation de la gestion des aéroports et des portes pour les avions, pour minimiser le temps d'attente des passagers[536]. C'est un problème NP-difficile difficile à traiter avec des algorithmes classiques.

---

[530] Voir Microsoft and DEWA bringing quantum computing to Dubai, juin 2018.

[531] Voir DEWA organises training sessions on quantum computing in partnership with D-Wave, février 2020.

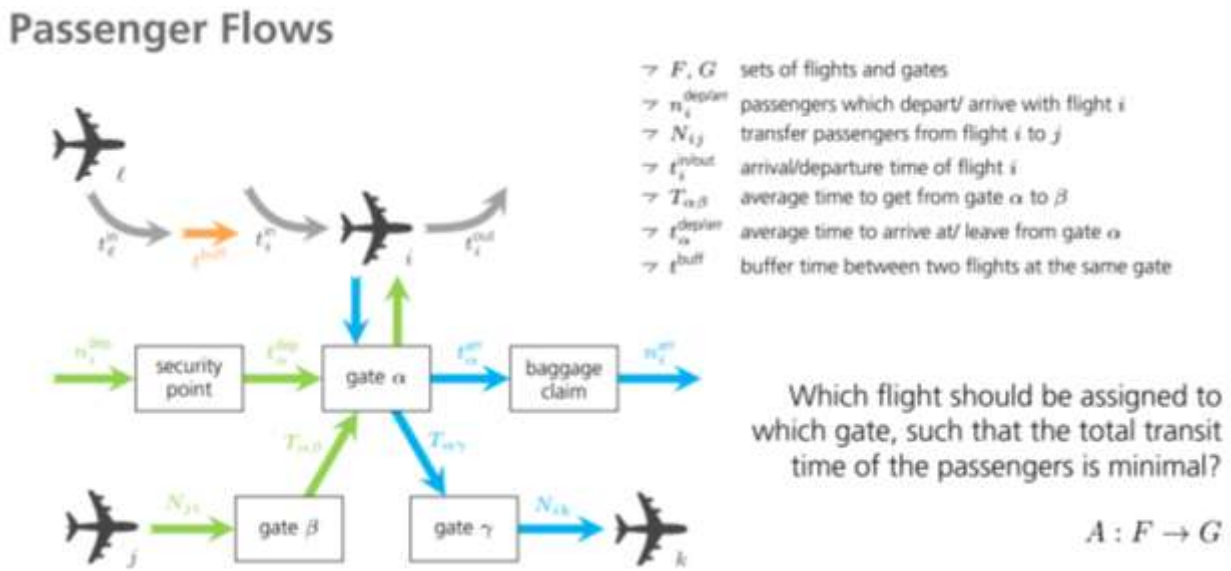
[532] Une version d'algorithme de résolution de problème MINLP existe pour D-Wave via leur framework QUBO. Voir Quantum Computing and Non-Linear Integer Optimization de Sridhar Tayur février 2019 (42 slides).

[533] Total s'est associé à des acteurs privés (IBM, Atos, Rigetti Qcware, Google) et divers laboratoires de recherche dans le monde : le PCQC (Paris), le LIRMM de Montpellier, le CERFACS, l'Université ParisSud, Jülich Forschungszentrum (Allemagne) et l'Université de Leiden.

[534] Voir CQC and Total Announce Multi-Year Collaboration to Develop Quantum Algorithms for Carbon Capture, Utilization and Storage (CCUS), avril 2020 et Total explore les algorithmes quantiques pour améliorer le captage de CO2, mai 2020.

[535] Voir cet inventaire de besoins, mais pas de solutions dans : Quantum Applications Transportation and Manufacturing de Yianni Gamvros, IBM, 2017 (20 slides).

[536] Voir Flight Gate Assignment with a Quantum Annealer par Elisabeth Lobe et Tobias Stollenwerk, du German Aerospace Center (ou DLR pour Deutsches Zentrum für Luft- und Raumfahrt e.V.), mars 2019 (15 slides). Le DLR est un équivalent d'un mélance de l'Onera et du CNES français. L'étude de cas exploite un D-Wave. Elle montre que la solution n'est pas évidente à mettre au point.



Ce sont des besoins qui peuvent être d'ailleurs traités à la fois par des algorithmes de machine learning pour tenir compte du passé ou avec des algorithmes quantiques d'optimisation qui s'appuient sur une description des paramètres du problème.

Les premiers font de la prédiction et les seconds de la simulation. La simulation permet d'éviter le biais du rétroviseur qui peut être induit par les méthodes de prédiction s'appuyant sur les données du passé. Une combinaison des deux méthodes est par ailleurs possible.

Le déploiement de flottes de véhicules autonomes est aussi une belle application cible des ordinateurs quantiques. Plus les véhicules seront autonomes, plus il faudra en automatiser et coordonner les parcours. Les problèmes à résoudre consisteront à déterminer pas à pas les trajets de flottes de véhicules pour optimiser le temps de parcours de chacun de ces véhicules. C'est l'objet d'une expérimentation réalisée en 2017 par **Volskwagen** sur D-Wave qui visait à optimiser les parcours d'une flotte de taxis à Beijing[537]. L'expérience utilise le jeu de données T-Drive publié par Microsoft datant de 2008 décrivant le parcours de 10 357 taxis.

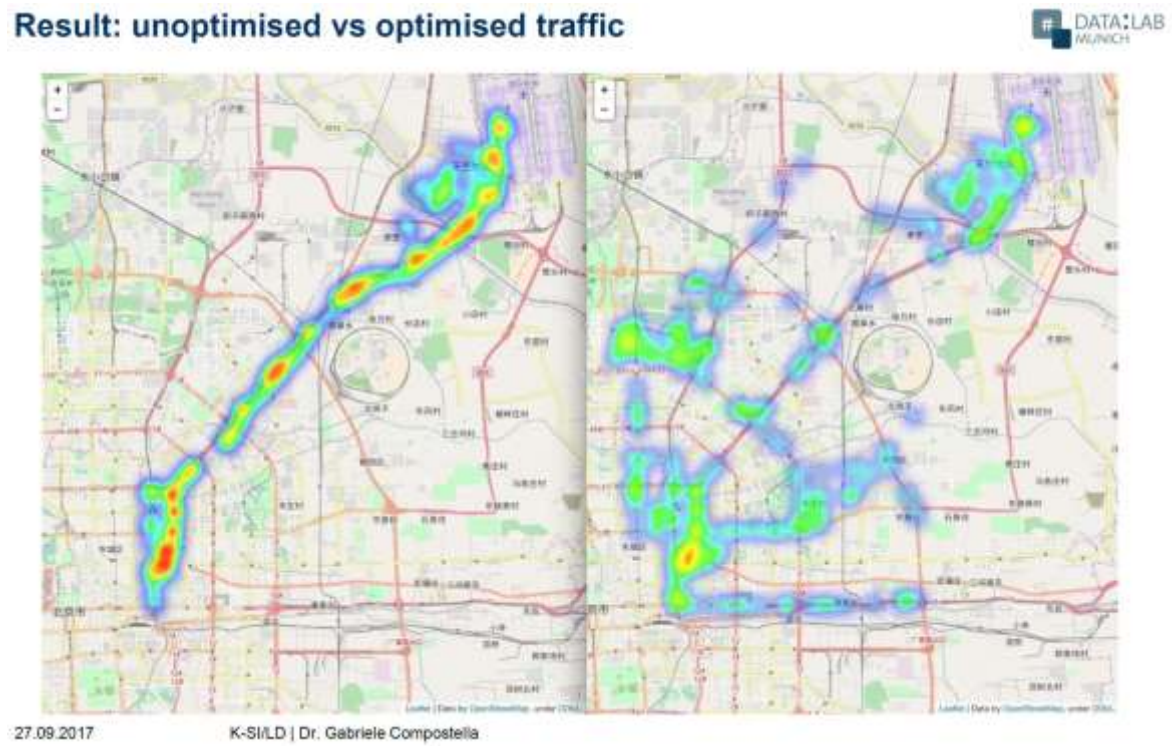
L'algorithme utilisé était le QUBO (Quadratic Unconstraint Binary Optimisation) qui est un mécanisme de recherche de niveau minimum d'énergie d'un système complexe. Le schéma ci-dessous présente le résultat de l'optimisation du parcours de 418 taxis faisant le trajet centre-ville-aéroport compte-tenu de celui des 10 357 véhicules[538].

On manque de recul pour estimer le dimensionnement des ordinateurs quantiques nécessaires pour gérer pratiquement ce genre de problèmes à grande échelle. De quelle capacité en qubits faudrait-il disposer pour optimiser un parc de centaines voire de millions de véhicules autonomes ?

Chaque chose en son temps… ! Ce genre de problème sera, si cela se trouve, trop lourd à gérer, même pour les ordinateurs quantiques les plus sophistiqués.

[537] Elle est documentée dans Quantum Computing at Volkswagen Traffic Flow Optimization using the D-Wave Quantum Annealer 2017 (23 slides).

[538] Les résultats sont publiés dans Traffic flow optimization using a quantum annealer, août 2017 (12 pages). Comme pour de nombreuses études de cas issues de D-Wave, celle-ci est aussi contestée par les spécialistes du calcul haute performance.



Daimler AG fait partie des grandes entreprises travaillant sur le quantique avec IBM, avec en tête des applications d'optimisation de logistique et de planification ainsi que tout ce qui touche au parcours des véhicules autonomes. Ils ont aussi lancé en 2018 une initiative avec IBM pour concevoir des batteries à base de lithium-souffre, améliorant la densité énergétique et permettant de se passer de métaux comme le cobalt et le nickel. Le tout grâce à de la simulation quantique.

Son confère allemand **BMW** étudie aussi les usages du quantique, en partenariat avec la startup **QCWare**.

Airbus est aussi impliqué dans le quantique. En 2015, une de leurs équipes basées à Newport au Royaume Uni se lançait sur le sujet. En 2016, l'avionneur investissait dans la startup américaine QC Ware. Ils ont expérimenté l'usage d'un D-Wave pour une analyse d'arbres de défaillances (FTA : fault tree analysis) qui sert à déterminer l'origine de pannes complexes avec un gain d'un facteur 4 par rapport aux méthodes traditionnelles. C'est un problème combinatoire NP-difficile plus facile à résoudre en programmation quantique. Airbus organise aussi depuis début 2019 son "Quantum Computing Challenge", une manière d'outsourcer le développement de solutions quantiques pour les aider à résoudre leurs problèmes métiers, dans la mécanique des fluides, les équations différentielles, l'optimisation du vol, la conception des ailes, le remplissage des soutes, etc[539].

En mai 2019, 475 équipes issues de de 57 avaient concuru à ce challenge. Elles provenaient principalement des USA et de l'Inde, suivis de l'Europe.

Finance

La finance est un autre beau terrain de jeu pour expérimenter des algorithmes quantiques[540]. A la fois parce que les entreprises du secteur sont assez friandes d'outils de prévision et d'optimisation et aussi parce que c'est un marché plutôt bien solvable. Ce n'est pas par hasard que ma première intervention de conférencier sur l'informatique quantique dans une entreprise ait eu lieu le 5 juillet 2018 à la **Société Générale** suivie d'une autre, en octobre 2018 chez **BNP-Paribas**.

---

[539] Voir Airbus gets aerodynamic with quantum computing par Michael Feldman, janvier 2019.

[540] Voir de panorama dans Quantum Computing and Finance de la Quantum World Association, août 2018, qui fait référence à Quantum computing for finance: overview and prospects, 2018 (13 pages).

Cette dernière a depuis créé une communauté interne d'une cinquantaine de personnes investiguant les usages du calcul quantique dans la banque. Ils organisaient même un événement à Paris fin février 2020 en y faisant intervenir notamment IBM, CryptoNext et QuantFi.

Les banques ont un besoin pressant de se transformer pour s'adapter aux changements technologiques et sociétaux constants. Elles manipulent des tombereaux de données qui ont de la valeur. Elles ont à optimiser de nombreuses facettes de leurs activités, à commencer par celle de portefeuilles d'investissements.

Elles veulent aussi détecter au plus près les risques de fraudes. L'optimisation d'actifs est la principale application imaginée pour l'informatique quantique. C'est de l'optimisation sous contraintes. Et là, sous un grand nombre de contraintes. Les actifs sont interdépendants. Les coûts de transactions sont variables selon les types d'actifs.

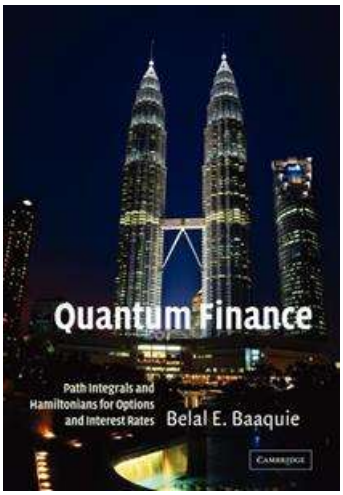
Question	Broad approach solution
Which assets should be included in an optimum portfolio? How should the composition of the portfolio change according to what happens in the market?	Optimization models
How to detect opportunities in the different assets in the market, and take profit by trading with them?	Machine learning methods, including neural networks and deep learning
How to estimate the risk and return of a portfolio, or even a company?	Monte Carlo-based methods

Table I. Financial problems addressed in this paper, and possible approaches.

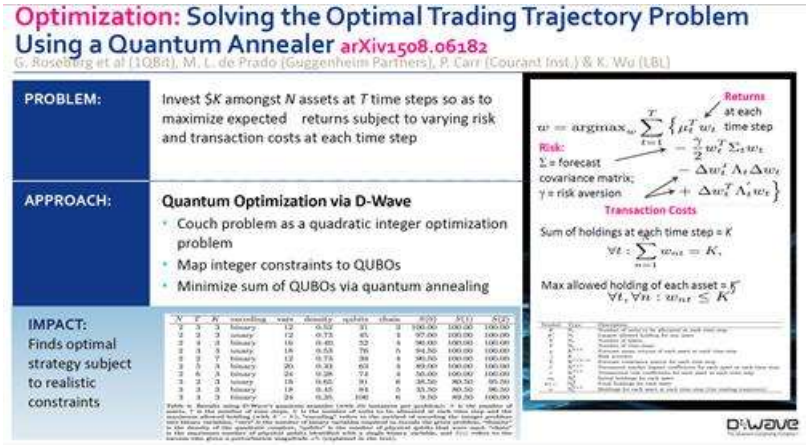
Leur évolution répond à des niveaux d'incertitude et de risques variables.

Il existe d'ailleurs un lien de parenté mathématique entre certaines équations de la finance et la physique quantique. C'est le cas de l'équation différentielle de Black-Scholes qui permet de prédire le prix de produits dérivés financiers qui sont indexés sur des cours tiers. Elle peut être en effet considérée comme une variante de la fonction d'onde de Schrödinger !

Ces équations sont décrites dans l'ouvrage "Quantum Finance" de Belal Baaquie qui date de 2007 ! Il en existe maintenant une très grande variété qui sont exploitables sur ordinateurs quantiques.



Un modèle d'optimisation quantique s'appuyant sur un D-Wave a été publié en 2015[541]. Il s'agissait d'optimiser les placements d'un montant donné dans un nombre d'actifs et sur une période donnée. L'algorithme principal utilisé était encore une fois le QUBO.



[541] Dans Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer, 2015 (13 pages).

En s'appuyant sur la modélisation de graphes, aussi adaptée aux D-Wave, une autre étude de cas permettait de modéliser l'instabilité des marchés[542].

Mais le recuit quantique n'est pas la seule technique utilisable pour traiter ce genre de problème.

Avant même qu'ils soient un tant soit peu opérationnels, les ordinateurs quantiques à architecture topologique que Microsoft essaye de mettre au point pourraient aussi servir à faire des prévisions de valeurs d'actions[543].

Atos a aussi publié un libre blanc sur les applications du quantique dans la finance[544].

Depuis 2017, IBM met en avant des partenariats avec **JPMorgan Chase**[545] et **Barclays**[546] qui étudieraient les usages du quantique dans l'optimisation de stratégies de trading, l'optimisation de portefeuille d'investissement, le pricing et l'analyse de risques. Un peu comme avec Watson à partir de 2013, ces banques en sont encore à l'évaluation du possible. Même si des algorithmes quantiques qui répondent à leurs besoins métiers sont envisageables, les capacités d'aujourd'hui des ordinateurs quantiques d'IBM sont tout à fait insuffisantes pour mettre quoi que ce soit en production.

De son côté, **D-Wave** est à l'origine avec quelques-uns de ses clients tels que la **Deutsche Bank** de la création du site web Quantumforquants, dédié aux usages du quantiques dans la finance.

La **NatWest** utilise des algorithmes « inspirés par le quantique » et s'exécutant sur calculateurs traditionnels pour optimiser ses portefeuilles d'investissement (HQLA pour High Quality Liquid Assets).

Goldman Sachs a de son côté recruté Will Zeng, de chez Rigetti Computing, qui avait développé le langage Quil.

A noter également l'investissement de la **Royal Bank of Scotland** (RBS) dans la startup 1Qbits, avec Fujitsu et Allianz.

Marketing

Le marketing est aussi un domaine où les algorithmes d'optimisation de systèmes complexes réalisés à base d'ordinateurs quantiques pourraient être intéressants.

---

[542] Voir ces slides dans cette présentation de D–Wave. Voir également cette présentation de D-Wave : Applications of Quantum Annealing in Computational Finance 2016 (29 slides) ainsi que le site QuantumForQuants créé par leurs soins.

[543] Comme documenté dans Decoding Stock Market Behavior with the Topological Quantum Computer 2014 (24 pages).

[544] Voir Quantum finance opportunities: security and computation, 2016 (20 pages). C'est aussi le cas de Everest Group avec Quantum Computing in the Financial Services Industry – Infinite Possibilities or Extreme Chaos, 2018 (15 pages, $990… qui n'en valent pas trop la peine).

[545] Voir JPMorgan Chase Prepares for FinTech's Quantum Leap, par Constantin Gonciulea, 2017. J.P. Morgan a recruté un vétéran d'IBM spécialisé dans le calcul quantique, Marco Pistoia, qui avait contribué au développement de Qiskit Aqua. Voir JP Morgan Chase poaches an IBM 'Master Inventor' with 26 patents for quantum computing par Hugh Son, janvier 2020. Cette activité quantique est intégrée dans leur « Quantitative Research Group ».

[546] Voir Why banks like Barclays are testing quantum computing, de Penny Crossman, juillet 2018. Voir aussi Barclays demonstrates proof-of-concept quantum clearing algorithm par Cliff Saran, octobre 2019 et Quantum Algorithms for Mixed Binary Optimization applied to Transaction Settlement par Lee Braine et al, octobre 2019 (8 pages).

Cela concerne l'optimisation du mix marketing, celui de plans médias, ou la maximisation de revenus publicitaires, divers domaines qui sont également investis par le champ de l'IA[547].

Chez **Volskwagen**, on expérimente un système de recommandation de véhicules dans les sites de vente en ligne, avec un D-Wave.

S'opposent ainsi encore une fois des logiques prédictives basées sur l'exploitation de données passées (modèle connexionnistes) et des logiques de simulation basées sur la connaissance de règles de fonctionnement du marché. Ces règles ne relèvent cependant pas de la notion de systèmes experts de l'IA, qui gèrent des prédicats logiques (machin entraîne bidule), mais des modèles de causalité plus complexes[548].

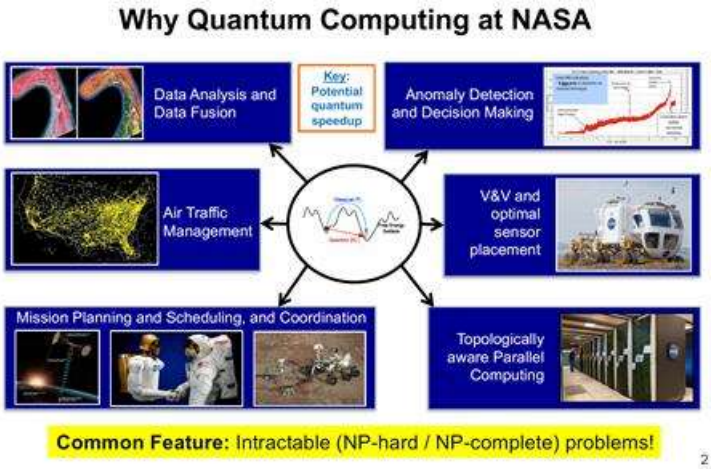
Défense et aérospatial

Le complexe militaro-industriel a toujours été un grand consommateur d'informatique de pointe. Il n'est donc pas étonnant qu'il s'intéresse au quantique. C'est évidemment le cas aux USA mais aussi en Europe, avec Airbus qui est l'un des premiers industriels à s'intéresser aux applications du quantique.

Voici quelques études de cas publiées d'utilisation du quantique dans ce vaste secteur.

Cela commence avec **Lockheed Martin** qui s'est associée avec **Google** et la **NASA** pour tester des ordinateurs de D-Wave. Ils ont développé une solution de preuve formelle de fonctionnement de logiciels.

La NASA a cofondé le laboratoire QuAIL (Quantum Artificial Intelligence Laboratory) avec Google, exploitant un D-Wave Two. Ils testent des algorithmes quantiques d'optimisation dans différentes directions. Pour optimiser le remplissage de vaisseaux spatiaux, une variante de l'algorithme du remplissage du coffre de voiture, sur les versions quantiques d'algorithmes de machine learning et deep learning, sur la décomposition de problèmes et l'informatique embarquée[549].



En 2015, **Raytheon** et **IBM** démontraient l'efficacité d'un algorithme quantique utilisant une "boite noire" ou "oracle" pour reconstruire une chaine de bits inconnue, le tout fonctionnant sur un ordinateur quantique universel d'IBM de 5 qubits[550]. On est cependant loin d'un cas d'usage.

Le groupe **Airbus** a de son côté créé une équipe basée sur leur site de Newport au Pays de Galle, qui s'attaque aux usages du quantique, notamment dans l'analyse d'imagerie aérienne (pas évident…) ou pour la conception de nouveaux matériaux (plus évident). Ils veulent aussi optimiser l'écoulement d'air sur les ailes, un problème qui relève aujourd'hui de la simulation par éléments

---

[547] Comme vu dans Les usages de l'intelligence artificielle en novembre 2018, Olivier Ezratty (522 pages).

[548] Voir par exemple Display Advertising optimisation by quantum annealing processor de Shinichi Takayanagi Kotaro Tanahashi et Shu Tanaka de la Waseda University ainsi que A quantum-inspired classical algorithm for recommendation systems d'Ewin Tang, juillet 2018 (36 pages). Ce dernier algorithme classique dépasse la performance d'un algorithme quantique réalisé pour ordinateurs quantiques de D-Wave.

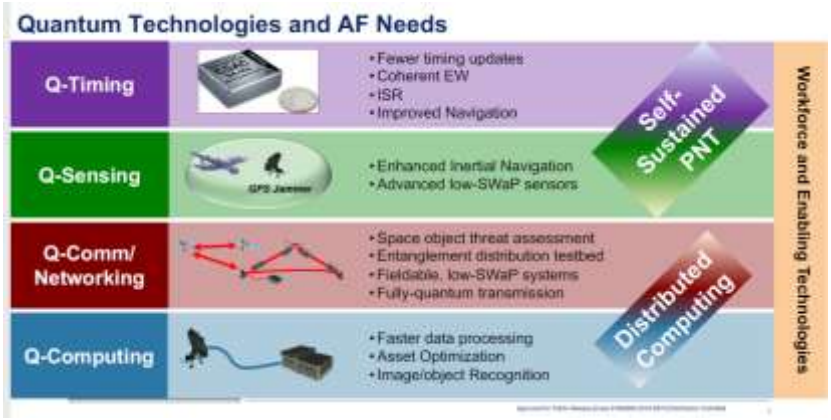
[549] C'est bien décrit dans Quantum Computing at NASA: Current Status de Rupak Biswas, septembre 2017 (21 slides) d'où provient le schéma de cette page.

[550] C'est documenté dans Demonstration of quantum advantage in machine learning (12 pages).

finis. Ils pourraient essayer d'optimiser les souffleries d'air climatisé dans les avions, la plus grosse source de bruit d'habitacle, devant les moteurs de l'avion !

Dans un domaine différent, les marines sont intéressées par la métrologie quantique et plus précisément par les outils de mesure de précision de la gravité qui permettent de détecter des sous-marins. En fait, des sonars quantiques ! Ce genre de métrologie est la spécialité de la startup française **Muquans**.

L'**US Air Force** a aussi identifié divers besoins pouvant être couverts par les quatre catégories de technologies quantiques [551] avec une mention spéciale pour la métrologie quantique dans la mesure du temps et la navigation. Ils s'intéressent aussi bien évidemment aux radars quantiques et enfin, au calcul quantique appliqué à des problèmes d'optimisation.



En France, la **DGA** a financé ou cofinancé depuis 2011 une vingtaine de thèses portant sur le quantique ainsi que huit projets pour 6,6 M€. L'Agence de l'Innovation de la Défense (qui est rattachée à la DGA) prévoyait de lancer un appel à projets pour les capteurs quantiques en 2020 et en 2021 de financer un projet de recherche de support de PQC dans du matériel dédié. En juillet 2020, elle concrétisait cela un appel à projet ASTRID portant sur les capteurs, la cryptographie et les communications quantiques et sur la création d'algorithmes de calcul quantique conjointement avec l'ANR[552].

Thales Alenia Space investi de son côté avec le CNES et la DGA dans les télécommunications quantiques par satellite.

L'usage des technologies quantiques dans le domaine militaire donne aussi lieu à des élucubrations hybridant le plausible et le décalé comme celles du politologue américain James Der Derian, directeur du Project Q de l'université de Sydney[553].

Renseignement

Le monde du renseignement et des écoutes ciblées est évidemment à l'affut du quantique. L'algorithme de Shor est la principale application visée par les organisations gérant les écoutes électroniques comme la **NSA** et tous ses confrères. Ce sont des pompiers pyromanes qui sont à la fois impatients de pouvoir décoder les informations interceptées auprès de cibles diverses (dépêches d'ambassades, informations techniques dans l'industrie, etc) et de protéger les communications sensibles de leurs propres Etats contre ce type de décryptage. Ils investissent donc simultanément dans l'informatique quantique (la dimension "pyromane") et dans les clés quantiques et la cryptographie post-quantique (la dimension "pompier").

---

[551] Source du schéma : Quantum Information Science at AFRL par Michael Hayduk, décembre 2019 (21 slides).

[552] Voir Recherche et innovation défense : lancement d'un nouvel appel à projets ASTRID sur les technologies quantiques, juillet 2020.

[553] Voir Drones, radars, nucléaire : comment le quantique va changer la guerre par Vic Castro, février 2020. Quelques remarques par rapport à cet article : les qubits à base d'atomes de Rydberg ne sont que l'un des types de qubits actuellement étudiés. Ils sont dits "à base d'atomes froids" et sont d'ailleurs la spécialité d'une startup française dénommée Pasqal. Il existe plein d'autres types de qubits. Le texte fait d'ailleurs une grosse confusion en qubits et portes logiques entre qubits. Ces portes relient des qubits entre eux. Ce sont souvent des systèmes à base de diffusion de micro-ondes, de photons émis par des lasers ou des coupleurs magnétiques. Les atomes de Rydberg sont des qubits et pas des coupleurs de qubits.

Par contre, ces investissements ne sont pas très publics. La NSA a bien communiqué depuis presque une dizaine d'années sur la dimension pompier mais très peu sur la dimension pyromane. Ils ont sûrement fait l'acquisition des diverses générations d'ordinateurs D-Wave pour se faire la main dessus, en liaison avec **Lockheed Martin** qui est l'un de leurs grands fournisseurs. La NSA entretien aussi un laboratoire conjoint avec le NIST et l'Université du Maryland, le QuICS, lancé en 2014.

On peut lever un bout de voile de ces activités en détectant les subventions de laboratoires et de startups attribuées par la IARPA, cette agence d'innovation du renseignement qui est pilotée par le DNI (Director of National Intelligence) qui coiffe l'ensemble du renseignement américain. Elle consolide le financement de recherche collaborative pour l'ensemble des agences de renseignement a déjà lancé cinq programmes autour des technologies quantiques : dans les qubits supraconducteurs (CSQ), les qubits logiques (LogiQ, avec IBM), la correction d'erreurs (MQCO, également avec IBM), la création d'outils de développement (QCS, avec Raytheon et GeorgiaTech) et sur le calcul à recuit quantique (QEO). Mais il n'est pas évident que cela ait significativement fait avancer l'état de l'art.

D'autres service de renseignement occidentaux ont peut-être aussi fait l'acquisition de D-Wave, notamment les britanniques du CGHQ. La NSA est aussi en relation avec IBM et Google pour explorer la voie des ordinateurs quantiques universels supraconducteurs.

Industrie

L'industrie au sens large du terme est un autre débouché pour l'informatique quantique. Dès qu'il y a un problème complexe d'optimisation pour de l'ordonnancement, de la logistique ou de l'aide à la conception de systèmes complexes, le quantique aura son mot à dire.

Le Japonais **JSR Corporation** fait partie des entreprises travaillant avec IBM dans le quantique, principalement pour la création de nouveaux matériaux.

Enfin, il semblerait que le quantique puisse servir aux outils de conception assistée par ordinateur[554]. Mais le document cité en note revient sur les basiques du calcul quantique sans être très disert sur les usages dans la CAO.

Le routage de circuits électroniques est aussi un problème NP-complet qui pourrait être en partie traité par des algorithmes quantiques, pour peu qu'ils disposent d'un nombre de qubits suffisant. Cela pourrait servir aux concepteurs de circuits de type ASIC et surtout FPGA, ces circuits dont la logique de fonctionnement est programmable dynamiquement via deux paramètres clés : les tables de décision des unités de traitement et les liaisons entre ces unités.

Approche expérimentale

Comme pour nombre d'applications de l'intelligence artificielle à leurs débuts, l'adoption de l'informatique quantique par les entreprises passera par l'évaluation des techniques, des outils et par l'expérimentation. Les grandes entreprises des marchés cités dans cette partie peuvent lancer quelques expérimentations.

Le démarrage ne sera pas évident car peu d'entreprises de services ou même d'éditeurs de logiciels et de startups maitrisent le développement d'applications quantiques. Tout du moins en France. Dans un premier temps, les grandes entreprises françaises peuvent se tourner vers Atos, la seule grande entreprise du numérique en France à avoir des ressources et compétences dans l'informatique quantique. Elles peuvent aussi se tourner vers IBM qui investit localement en compétences depuis quelques années déjà.

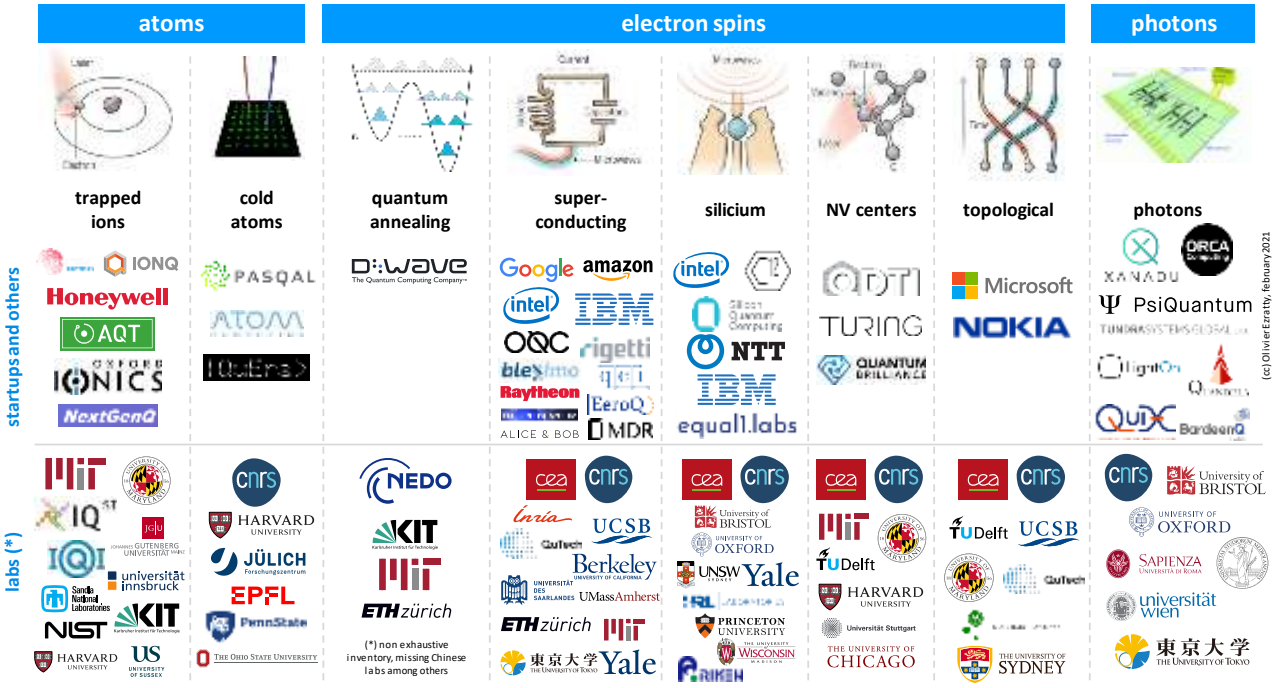
[554] Selon Quantum computing dans la CAO. Computer-Aided Design for Quantum Computation de Robert Wille, Austin Fowler et Yehuda Naveh (Google et IBM), 2018 (6 pages).

Un gros travail d'acculturation général à l'informatique quantique est à mener. C'est une tâche intellectuelle assez ardue. C'est un peu l'objet de de cette série d'articles que de vous mettre le pied à l'étrier en vous indiquant diverses pistes à explorer selon vos centres d'intérêt. Il faut en passer par là pour faire des choix éclairés sur le sujet.

Comme je vais le détailler dans les parties suivantes, la situation de l'offre d'ordinateurs quantiques est difficile à décoder. Nous avons d'une part l'offre commerciale opérationnelle du Canadien D-Wave qui est très décriée et qui est par contre opérationnelle, et de l'autre, des roadmaps d'ordinateurs quantiques universels comme chez IBM et Google, mais qui nécessitent encore de patienter au minimum quelques années avant de pouvoir les exploiter opérationnellement. J'en conclue que, malgré la polémique qui entoure D-Wave, il faut s'y intéresser et examiner ce que l'on peut faire avec. On n'est pas obligé de s'acheter un ordinateur quantique D-Wave à $15M pour commencer ! On peut les utiliser en cloud comme pour AWS ou un équivalent. Le coût technique de l'expérimentation est donc modeste. C'est surtout un coût en temps et intellectuel.

Acteurs des calculateurs quantiques

Nous voici à l'étape d'un panorama des acteurs que sont les acteurs du hardware du calcul quantique. On y trouve des laboratoires de recherche, de grandes sociétés établies et des startups[555].



Comme nous l'avions vu dans la partie dédiée aux types de qubits, il se dégage huit grandes catégories d'ordinateurs quantiques regroupées en trois catégories :

Les **atomes** :

- Les **ions piégés** que l'on trouve notamment chez IonQ, une spin-off de l'Université de Maryland ainsi que chez Honeywell ou la startup autrichienne Alpine Quantum Technologies.
- Les **atomes froids** comme le rubidium qui servent aussi bien à créer des ordinateurs quantiques analogiques que des ordinateurs à portes quantiques.
- La technique de la **résonance magnétique nucléaire** a été aussi envisagée mais abandonnée car elle ne donnait pas de résultats satisfaisants. Je ne la traite pas dans cet ouvrage.

Les **électrons** :

- Les qubits **supraconducteur** à effet Josephson utilisés par les ordinateurs quantiques universels d'IBM, Google, au CEA ainsi que dans les ordinateurs à recuit quantique de D-Wave.
- Les **qubit silicium** poussés notamment par Intel et le CEA-Leti.
- Les **NV centers** à base de diamants, avec assez peu d'acteurs industriels. Le CEA-SPEC s'intéresse à une approche hybride cavités diamants et supraconducteurs.
- Le **topologique** avec notamment les hypothétiques fermions de Majorana de Microsoft qui n'existent pas encore.

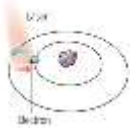
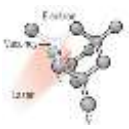
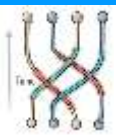
[555] Source des dessins de qubits : Scientists are close to building a quantum computer that can beat a conventional one par Gabriel Popkin dans Science Mag, décembre 2016.

Les **photons** :

- L'**optique linéaire** qui n'est pour l'instant pas très scalable mais potentiellement prometteuse.

Nombre des entreprises privées de ce cheptel sont associées avec des laboratoires de recherche américains ou européens. Google collabore avec l'Université de Santa Barbara en Californie, IBM et Microsoft avec celle de l'Université de Delft aux Pays Bas, et IBM avec celle de Zurich. On voit qu'il y a déjà beaucoup de monde qui travaille sur les calculateurs quantiques !

Ces catégories de technologies ont des niveaux de maturité très différents. Les qubits à base de supraconducteurs sont à ce jour les plus éprouvés. Les ions piégés, l'optique linéaire et les NV Centers ont du mal à "scaler". Les systèmes à base de spins d'électrons pourraient scaler mais il est difficile d'y gérer l'intrication des qubits. Enfin, les fermions de Majorana sont encore dans les limbes.

	atomes		électrons				photons
							
	ions piégés	**atomes froids**	**supra-conducteurs**	**silicium**	**NV centers**	**fermions de Majorana**	**photons**
nature des qubits	ions piégés électriquement et magnéti-quement	atomes piégés par des pinces laser	boucle de courant supraconductrice	électrons piégés dans un semi-conducteur	électrons d'une cavité de diamant près d'un atome d'azote	quasi-particules, paires d'anyons	photons circulant
états quantiques des qubits	niveau énergétique de l'ion piégé	niveau d'énergie de l'atome	phase de résonnance ou sens du courant	spin d'électron	niveau d'énergie des électrons du centre NV	sens de l'anyon	une propriété du photon (phase ou autre)
portes quantiques	laser ou électrodes	micro-ondes, lasers, états de Rydberg	micro-ondes >4GHzet effet Josephson	micro-ondes >20 GHz	micro-ondes	inversions 2D d'anyons	interférence, Mach Zehnder
mesure d'état	laser + fluorescence	laser + fluorescence	magnétomètre ou couplage à un résonateur micro-onde	consersion spins to charge	laser + fluorescence	fusion d'anyons	détecteur de photons uniques
# de qubits intriqués	32 qubits (IonQ)	51 qubits (simulation)	65 qubits (IBM)	4 qubits (Delft)	10 qubits (QDTI)	N/A	20 qubits (Chine)
dimension des qubits	$(1mm)^2$	atomes	$(100\mu)^2$	$(100nm)^2$		N/A	non applicable
fidélité portes unitaires	99,98%	>99%	99,84%	98%	92%	N/A	98%
fidélité portes à deux qubits	99,2%	99,6%	99,38%				
fidélité lecture	99,7%	97%	96%	98%	93%	N/A	>50%
durée portes	100µs	1µs	20-300 ns	≈5µs		N/A	1ms
temps de cohérence	>1mn	100µs	100µs	200µs-20ms		N/A	
cryogénie	300K ou supraco	15mK	15mK	100mK-1K	300K	15mK	générateurs et lecteurs en cryostat
rackable	no	yes	no	no	no	no	yes

(cc) Olivier Ezratty, avril 2020

Il y a de plus en plus de startups dans ce tableau, notamment issues d'Europe. Elles n'ont pas froid aux yeux face aux Google et IBM. On n'y trouve pas encore de startups chinoises. Pour l'instant, les investissements du pays en calcul quantique sont concentrés dans la recherche publique. Comme ils sont abondants, les chercheurs n'expriment pas encore le besoin de se faire financer par des capitaux privés. Les acteurs présentés dans cette rubrique sont cependant uniquement les grandes entreprises. Les startups du calcul quantique sont inventoriées dans une rubrique à part.

Recuit quantique

Le recuit quantique, “quantum annealing” en anglais, est une technologie particulière d’ordinateur quantique qui repose bien sur la mécanique quantique et des qubits, mais avec des caractéristiques et niveaux de performance intermédiaires entre ceux des supercalculateurs traditionnels et ceux des ordinateurs quantiques universels. Il n’existe qu’un seul acteur commercial sur ce marché : le Canadien **D-Wave**. Les laboratoires de recherche impliqués dans le procédé ne sont pas aussi nombreux que dans les différents types de d’ordinateurs à qubits exploitant des portes quantiques (« gate model »). Ils sont situés principalement au Japon où la technique a été inventée en 1998 par **Hidetoshi Nishimori**[556]. Mais on en trouve quelques-uns aux USA, y compris à l’**UCSB**[557].

qubits supraconducteurs à recuit

avantages

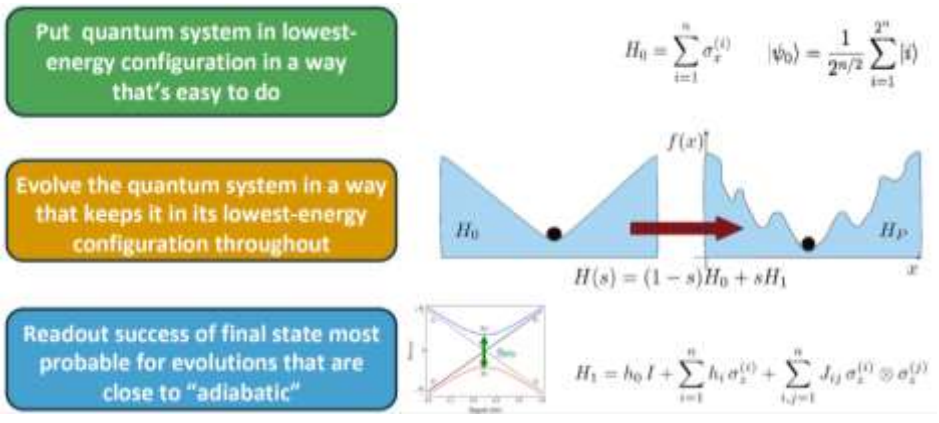
- offre complète d’**outils de développement**.
- écosystème de **startups logicielles**, notamment au Japon.
- ordinateurs disponibles **dans le cloud**.
- nombreuses **études de cas documentées** même s’il ne s’agit de de preuves de concept, et des expérimentations dans **l’optimisation des transports**.
- la plupart des algorithmes quantiques classique ont un **équivalent** en calcul à recuit quantique.

inconvénients

- une seule **offre commerciale** avec D-Wave.
- **taux d’erreur** très élevé du calcul.
- pas de **preuve opérationnelle** d’une supériorité quantique du calcul adiabatique.
- pas d’applications véritablement **déployées commercialement**. mais c’est vrai des autres types d’ordinateurs quantiques à ce stade.
- les **algorithmes sont tous hybrides**, nécessitant une préparation sur calculateur classique.

Le principe général consiste à établir des liaisons entre des qubits supraconducteurs de flux avec des « poids » via des coupleurs, un peu comme dans les réseaux de neurones de l’intelligence artificielle, puis à faire converger le système vers un point d’équilibre du système qui correspond à un minimum énergétique. Celui-ci conduit à modifier automatiquement les valeurs des qubits vers un résultat qui correspond à la solution du problème soumis. Le système est itératif avec plusieurs passes de recuit. A la fin du processus, l’état des qubits est lu et génère un 0 ou un 1 pour chacun d’entre eux en fonction du sens du flux magnétique de la boucle supraconductrice.

Le processus est dit adiabatique car il n’y a pas de transfert énergétique entre le chipset de l’ordinateur et son environnement. Le système doit cependant être initialisé dans un état proche de la solution du problème, évaluée avec un ordinateur classique[558].



[556] L’histoire et la science du calcul à recuit quantique sont bien décrits dans Adiabatic Quantum Computing par Tameem Albash et Daniel Lidar de l’Université de Californie du Sud, 2018 (71 pages).

[557] Voir la thèse Superconducting flux qubits for high-connectivity quantum annealing without lossy dielectrics, par Christopher M. Quintana, 2017 (413 pages), dirigée par John Martinis qui était alors chez Google.

[558] Source du schéma : How about quantum computing? par Bert de Jong, juin 2019 (47 slides).

Les algorithmes adiabatiques sont donc toujours des algorithmes hybrides qui ont demandé un calcul de préparation.

Côté recherche, cette voie était aussi explorée en 2016 par l'agence IARPA dans le projet **Quantum-Enhanced Optimization** (QEO) qui visait à créer un calculateur adiabatique n'ayant pas certaines des limitations de ceux de D-Wave, notamment en termes de connectivité et de qualité des qubits employés. Comme il se doit, au vu de la mission de la IARPA, l'objectif était d'accélérer la mise en production d'ordinateurs quantiques capables d'exécuter l'algorithme de Shor de factorisation de nombres entiers pour casser la sécurité à clés publiques de communications interceptées. Il ne semble pas que ce projet ait aboutit.

On peut aussi citer le projet européen **AVaQus** (Annealing-based VAriational QUantum processorS) qui rassemble cinq laboratoires (Institut de Física d'Altes Energies de Barcelone, Karlrsruher Institut für Technologie (KIT) de Karlsruhe, le CNRS de Grenoble, l'Université de Glasgow et le Consejo Superior de Investigaciones Científicas de Madrid), associés à trois startups **Delft Circuits** (Pays-Bas), **Qilimanjaro Quantum Tech** (Espagne) et **Heisenberg Quantum Simulations** (HQS) (Allemagne). Lancé en 2020, le projet doit se terminer en 2023 et était financé à hauteur de 3M€ en tant que projet FET, indépendamment du Quantum Flagship.

D-Wave
The Quantum Computing Company™

Situé à Vancouver, le Canadien **D-Wave** (1999, $205M) était pendant très longtemps le seul fournisseur d'ordinateurs quantiques commerciaux. Même s'il s'agit d'ordinateurs adiabatiques présentant des limitations techniques par rapport aux ordinateurs quantiques universels, ils ont l'avantage d'exister, de faire avancer le secteur et de permettre le test d'algorithmes quantiques dans une large gamme d'applications. Celles-ci semblent cependant demeurer des "proofs of concept" d'après les études de cas publiées. Rares sont celles qui semblent avoir été déployées pour des besoins opérationnels.

L'histoire de cette startup est fascinante pour ce qui est du timing. Créée en 1999, elle met huit ans à prototyper sa première puce contenant quatre qubits. Il leur faut en tout dix ans pour vendre un premier ordinateur quantique. Quelle patience pour leurs investisseurs ! Pendant ces dix ans, ils lèvent $31M. Ils obtiennent ensuite un financement de $1,2M en 2012 de la part d'InQTel, le fonds d'investissement de la CIA. Les levées de fonds suivantes, dont une partie est en obligations convertibles, leur permettent de tenir le coup, en plus des premières commandes. J'imaginais que certaines étaient confidentielles, provenant de la NSA, si ce n'est d'autres services de renseignement occidentaux, comme chez les partenaires de l'alliance "five eyes" que sont les pays du Commonwealth comme UK, l'Australie, le Canada et la Nouvelle-Zélande. En fait, ce n'est probablement pas le cas car ces services ne peuvent pas faire grand-chose de ces ordinateurs. En 2011, D-Wave signait un partenariat avec Lockheed Martin, qui travaille beaucoup pour la NSA. En tout, la startup a obtenu 13 tours de financements !

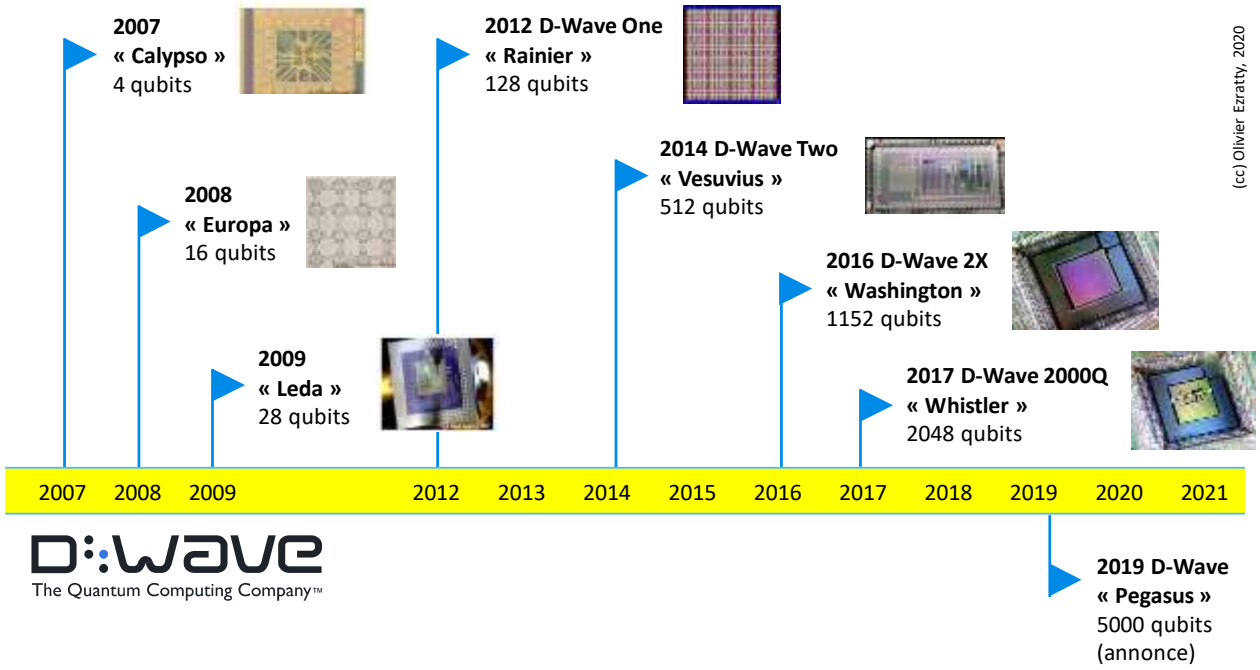
D-Wave a été créé par Geordie Rose (leur premier CTO et un moment CEO), Haig Farris, Bob Wiens et Alexandre Zagoskin, anciennement en charge de la recherche. Geordie Rose a obtenu un doctorat en physique des matériaux au milieu des années 1990 à l'University of British Columbia. La création de D-Wave est donc en ligne droite de ces travaux. Il rencontra Haig Farris pendant ses études alors que ce dernier enseignait l'économie.

L'équipe de direction de D-Wave de 2020 n'a plus grand chose à voir avec celle de ses créateurs. Un seul des cofondateurs en fait encore partie, Eric Ladizinsky, qui joue un rôle de Chief Scientist.

Le CEO depuis 2009 est Vern Brownell. Leur CTO Alan Baratz a rejoint la société en 2017. On sent une forme de reprise en main[559].

D-Wave a développé sa solution de bout en bout d'ordinateur adiabatique à recuit quantique. Cela commence avec les puces quantiques, puis va jusqu'à l'ordinateur complet.

C'est le premier ordinateur quantique complet de l'histoire avec un design permettant de facilement l'intégrer dans une salle blanche. La partie cryogénisée comprend une enceinte de cinq couches d'isolation magnétique. Le cryostat utilise un système de dilution à sec exploitant de l'hélium 3 et 4 gazeux. Il permet de refroidir la puce quantique à 12 mK. Le cryostat similaire à ceux qui équipent les ordinateurs quantiques d'IBM et Google comprend une tête pulsée alimentée par un compresseur CryoMech. La partie cryogénie consomme environ 16kW. C'est une bonne partie de la consommation électrique de l'ordinateur qui s'élève à 25 kW. Les 9kW qui restent sont surtout liés aux systèmes de contrôle informatique traditionnels qui sont externes à l'unité quantique de l'ordinateur.



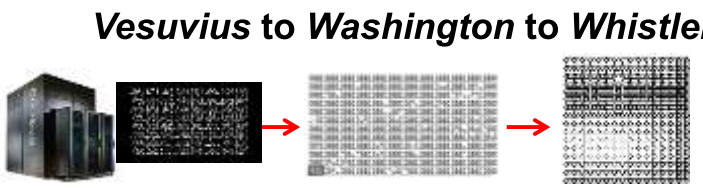
Leur roadmap a avancé régulièrement avec les trois premières générations de prototypes entre 2007 et 2009 puis, à partir de 2012, quatre générations d'ordinateurs commerciaux, à commencer par le D-Wave One en 2012 avec ses 128 qubits et jusqu'au D-Wave 2000Q de 2017 avec ses 2048 qubits et 5600 coupleurs reliant les qubits par paires et 128 000 jonctions Josephson[560]. Le maillage des qubits avec leur coupleur est baptisé « chimera » par D-Wave.

[559] Le cofondateur Geordie Rose a ensuite créé **Kindred.ai**, une startup qui vise à intégrer une intelligence générale (AGI) dans les robots. Il est devenu un véritable "singulariste". Ses interventions publiques sont assez déjantées. Il s'exprime ainsi sur les démons et sur les extraterrestres. Il quitte Kindred.ai début 2018 pour créer Sanctuary, une spin-off de Kindred, dédiée à l'AGI, la quête du Graal de l'intelligence artificielle générale !

[560] Voir Quantum annealing with manufactured spins par Mark Johnson et al, 2011 (6 pages) qui décrit les grandes lignes du procédé de D-Wave. Ainsi que Technical Description of the D-Wave Quantum Processing Unit par D-Wave, 2020 (56 pages) et les supplemental infomations associées (19 pages).

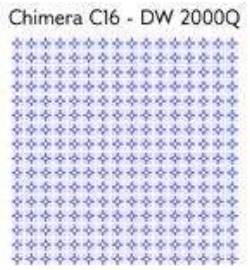
Le D-Wave 2000Q est commercialisé au prix catalogue de $15M. La puce quantique de cet ordinateur fait 5,5 mm de côté. Elle est fabriquée aux USA dans une unité de production de composants du Californien **Cypress Semiconductor** à Bloomington dans le Minnesota.

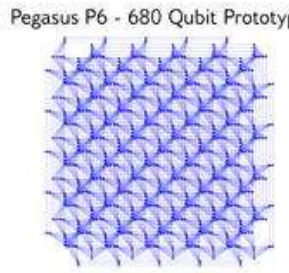
Début 2019, D-Wave annonçait la prochaine génération de leurs systèmes à base de 5640 qubits de la génération Pegasus qui devait être disponible avant la fin 2020[561].



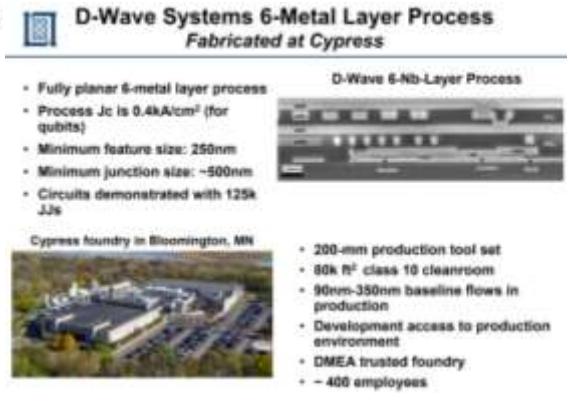
D-Wave Two	D-Wave 2X	D-Wave 2000Q
512 (8x8x8) qubit "Vesuvius" processor	**1152** (8x12x12) qubit "Washington" processor	**2048** (8x16x16) qubit "Whistler" processor
509 qubits working – 95% yield	**1097** qubits working – 95% yield	**2038** qubits working – 97% yield
1472 *J* programmable couplers	**3360** *J* programmable couplers	**6016** *J* programmable couplers
20 mK max operating temperature (**18 mK** nominal)	**15 mK** max operating temperature (**13 mK** nominal)	**15 mK** max operating temperature (*nominal to be measured*)
5% and **3.5%** precision level for *h* and *J*	**3.5%** and **2%** precision level for *h* and *J*	*To be measured*
20 us annealing time **12 ms** programming time	**5 us** annealing time (4X better) **12 ms** programming time	**5 us** annealing time **9 ms** programming time (25% better) **New:** anneal offset, pause, quench
6 graph connectivity per qubit	**6** graph connectivity per qubit	**6** graph connectivity per qubit

Dans cette nouvelle architecture, chaque qubit est relié à 15 autres qubits versus 6 dans la génération précédente ce qui permet de résoudre des problèmes plus complexes avec un nombre équivalent de qubits. Le tout avec des qubits dont le taux d'erreur serait diminué ce qui permettrait d'accélérer les calculs[562]. Cette version dénommée Advantage du D-Wave a été commandée par le Los Alamos National Laboratory en septembre 2019[563]. Elle était finalement lancée officiellement le 29 septembre 2020[564].





Device Count	C16	P6	P12	P16
Qubits	2048	680	3080	5640
Couplers	6000	4784	21764	40484
max degree	6	15	15	15



Les qubits de D-Wave sont de type rf-SQUID au niobium, exploitant des boucles de courant supraconductrices interrompues par deux barrières à effet Josephson qui sont contrôlées par des flux magnétiques variables. Le schéma *ci-dessous* explique tout cela.

---

[561] L'architecture Pegasus est décrite dans Next Generation Quantum Annealing System par Mark Johnson, mars 2019 (27 slides) ainsi que dans Next-Generation Topology of D-Wave Quantum Processors par Kelly Boothby et al, 2019 (24 pages).

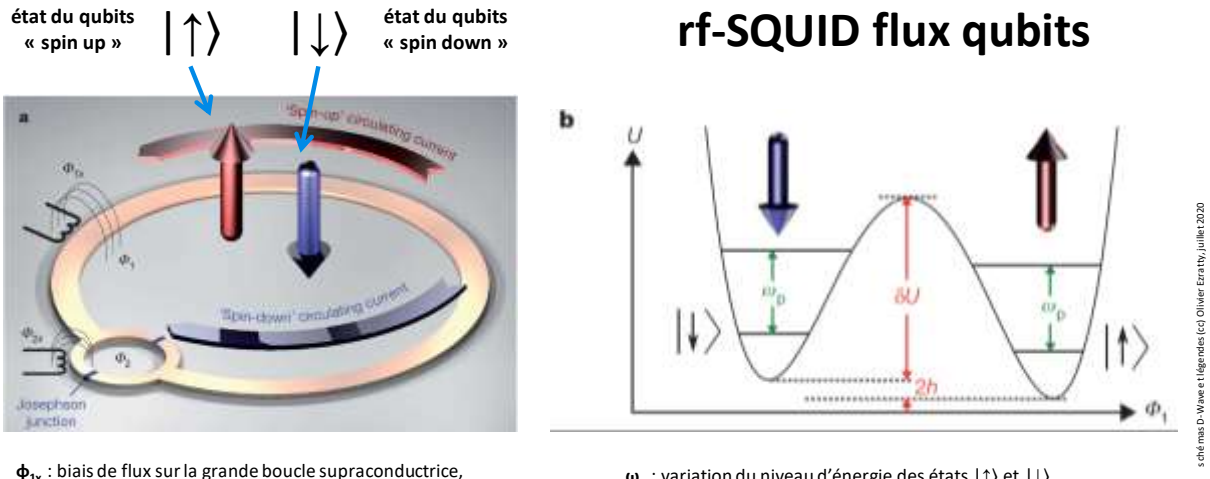
[562] La question reste ouverte de savoir si cette architecture est scalable et permet d'obtenir un réel avantage quantique. Ceci est remis en cause dans Fundamental Limitations to the Scalability of Quantum Annealing Optimizers par Tameen Albash et al, 2019. Les raisons : des questions de bruit et de thermodynamique.

[563] Voir Nuclear weapons lab buys D-Wave's next-gen quantum computer par Stephen Shankland, septembre 2019.

[564] Voir D-Wave Announces General Availability of First Quantum Computer Built for Business | D-Wave Systems par D-Wave, septembre 2020.

Le principe de base des D-Wave consiste à préparer ce que l'on appelle un "hamiltonien" d'un problème d'optimisation dit **modèle d'Ising**[565] ou **QUBO** (Quadratic Unconstrained Binary Optimization).

Ce sont des problèmes d'optimisation où les variables ne peuvent prendre que deux valeurs (-1 ou +1 ou 0 et 1) et où elles sont reliées entre elles par différents paramètres fixes qui sont définis sous la forme de nombres flottants à double précision (FP32). Cependant, les convertisseurs numériques/analogiques (DAC) de préparation des qubits introduisent un bruit d'échantillonnage significatif ce qui fait qu'au final, la précision des données du problème à résoudre n'est que de 4 à 5 bits.



Φ_{1x} : biais de flux sur la grande boucle supraconductrice, contrôle la différence de niveau d'énergie 2h entre les deux états du qubit, le sens du courant supraconducteur.

Φ_{2x} : biais de flux sur la petite boucle supraconductrice comprenant deux jonctions Josephson, qui contrôle le niveau d'énergie **δU** de passage d'un état de spin à l'autre

ω_p : variation du niveau d'énergie des états |↑⟩ et |↓⟩

δU : barrière de potentiel énergétique de passage entre état s

2h : différence de niveau d'énergie entre les deux états de base du qubit.

Le problème à résoudre est transformé en un système quantique avec plusieurs qubits interconnectés décrivant un équilibre énergétique donné. Cet hamiltonien doit être initialisé dans un état qui est proche de la solution du problème que l'on souhaite résoudre. Cet état initial a été évalué via un algorithme tournant sur ordinateur classique.

Le processus du recuit consiste à faire converger le système vers son minimum énergétique permettant de trouver les valeurs optimales des qubits (-1 ou +1 ou 0 et 1) en fonction des variables fixes du problème que sont les h_i (les deltas énergétiques entre les deux états de chaque qubit i) et J_{ij} (valeur du couplage entre les qubits i et j). On recherche donc un minimum énergétique d'un système complexe multi-paramètres dont les variables sont discrètes et ne peuvent prendre que deux valeurs possibles et dont les paramètres sont des nombres flottants.

Le recuit utilise l'effet tunnel quantique qui permet au système de trouver facilement des minimums globaux au lieu d'être coincé dans des minimums locaux, un problème qui rappelle celui de la descente de gradient dans l'entraînement de réseaux de neurones[566]. Il faut noter que les machines D-Wave nécessitent un calibrage au moment de leur installation.

[565] C'est un modèle de physique statistique créé pour résoudre des problèmes de simulation de matériaux ferro-magnétiques et para-magnétiques associant des particules ayant deux niveaux d'état (un moment magnétique +1 ou -1) qui sont reliées entre elles.

[566] Voir par exemple Architectural considerations in the design of a superconducting quantum annealing processor 2014 (9 pages) qui décrit l'architecture matérielle des processeurs de D-Wave de 2014, qui n'ont pas énormément change depuis.

« **modèle d'Ising** »

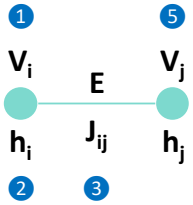
énergie totale du système (hamiltonien)

énergie nette des qubits

énergie de liaison entre les qubits

$$\mathcal{H}_P = \sum_{i=0}^{N} h_i \, \sigma_i^z + \sum_{i,j=0}^{N} J_{ij} \, \sigma_i^z \sigma_j^z$$

H_p : hamiltonien du système
h_i : différentiel d'énergie entre les deux états du qubit i
V_i : nœuds (vertices) comprenant le qubit i
J_{ij} : couplage entre les nœuds V_i et V_j
E = edges, liaisons entre qubits



processus de calcul :

en amont : conversion de son problème en modèle d'Ising ou QUBO (Quadratic Unconstrained Binary Optimization)

1. initialisation de l'état des qubits à $|\uparrow\rangle$ ou $|\downarrow\rangle$
2. définition des niveaux d'énergie h_i des qubits
3. élévation progressive des couplages J_{ij}
4. convergence du système vers H_p minimum
5. lecture de l'état $|\uparrow\rangle$ ou $|\downarrow\rangle$ des qubits qui donne la solution du problème de recherche de minimum énergétique de H_p

(cc) Olivier Ezratty, avril 2020

D'un point de vue pratique, l'initialisation du D-Wave 2000Q dure 25 ms, le temps de convergence du système (annealing) est de 20 µs et le temps de lecture dure 260 µs, ces deux étapes étant généralement répétées plusieurs fois et les résultats moyennés, une pratique qui équivaut à celle d'IBM avec ses propres calculateurs quantiques à portes universelles.

D-Wave est très peu dissert sur l'électronique de contrôle de ses qubits et sur les questions énergétiques associées.

Les signaux d'initialisation de l'hamiltonien sont multiplexés et envoyés en format numérique de l'extérieur vers la puce. Cela a l'air de bien simplifier le câblage de l'enceinte cryogénisée du calculateur par rapport aux calculateurs supraconducteurs d'IBM et Google, comme en témoigne l'illustration *ci-contre* d'un 2000Q. L'essentiel de ce que l'on peut voir dans les étages intermédiaires correspond au système de cryogénie à dilution.

C'est lié au fait, comme nous l'avons vu dans la partie de cet ebook dédiée aux circuits de contrôle des qubits, que D-Wave a intégré des circuits de génération de pulsations micro-ondes de contrôle des qubits directement dans sa puce. Ces circuits utilisent des composants SFQ, en gros, des transistors supraconducteurs utilisant des boucles à effet Josephson voisines de celles des qubits.

D'après D-Wave, ce type d'ordinateur serait capable de résoudre des problèmes dits NP-complets, une catégorie des problèmes de logique théoriquement résolus dans un temps polynomial sur D-Wave mais qui le sont en temps exponentiel sur machine classique[567]. C'est le cas des problèmes de routage, de définition de parcours de voyageurs du commerce et équivalents. Les D-Wave pourraient aussi servir à résoudre des problèmes de statistiques[568]. L'affirmation n'a pas été réellement prouvée à ce stade.

Qu'est-ce qui est quantique dans l'histoire ? Il s'agit surtout de l'effet tunnel qui permet au système de rechercher rapidement un minimum énergétique global d'un système à N-corps. Il est couplé à

[567] Voir Practical Annealing-Based Quantum Computing par Catherine McGeoch et al de D-Wave, juin 2019 (16 pages) qui fait un inventaire des bénéfices du calcul à recuit quantique, notamment au niveau de la taille des problèmes à résoudre qui ne doivent ni être trop petits car triviaux, ni trop grands car devant alors être décomposés en sous-problèmes gérable avec la capacité des processeurs actuels de D-Wave. Il semble que les problèmes à résoudre doivent avoir un minimum global et des minimums locaux, le premier étant difficile à trouver avec des méthodes classiques.

[568] Voir Applications of Quantum Annealing in Statistics par Robert C. Foster, 2019 (30 pages).

de la superposition des états d'orientation des flux électriques dans les boucles Josephson. Selon D-Wave, le système fait aussi appel à de l'intrication mais cela ne fait pas l'unanimité[569].

Les algorithmes conçus pour des ordinateurs à base de portes quantiques classiques que nous verrons plus loin sont exécutés séquentiellement. Tous peuvent théoriquement être convertis en algorithmes exécutables sur D-Wave et réciproquement avec des variations polynomiales de temps de calcul, ce qui va affecter le niveau de l'accélération[570]. Un même algorithme va demander beaucoup plus de qubits avec D-Wave qu'avec un ordinateur quantique universel, sachant que le rapport actuel est de 2048 vs 50 côté disponibilité, ce qui égalise les choses.

Il semblerait que l'équivalence concerne le nombre de portes quantiques à exécuter. Sur un D-Wave, il faudrait un nombre de qubits allant jusqu'à 32 fois le nombre de portes quantiques de l'algorithme quantique classique[571].

Selon **John Preskill**[572], il n'existe pas de base théorique convaincante de l'avantage du recuit quantique qui est une des formes d'ordinateur quantique adiabatique. Selon lui, cette architecture n'est pas théoriquement aussi scalable que les ordinateurs quantiques universels. D'autres pensent que les D-Wave ne peuvent générer qu'au mieux une accélération quadratique et pas exponentielle par rapport au calcul traditionnel[573]. Enfin, les qubits de D-Wave sont très bruyants, et génèrent des taux d'erreurs préjudiciables aux calculs[574].

En date de mi 2020, D-Wave avait installé quatre ordinateurs quantiques chez des clients et en opère plus d'une trentaine dans ses propres locaux, une bonne moitié étant dédiés à leur offre d'accès en cloud. Une partie étant maintenant disponible via l'offre cloud Amazon Braket.

Comme tous les grands acteurs du quantique, D-Wave a développé une plateforme logicielle supportant les couches basses de la création d'algorithmes quantiques pour ses machines que nous évoquons dans la partie de cet ebook dédiée aux outils de développement.

Ils ont aussi quelques partenaires logiciels comme **1QBit**. Les outils proposés comprennent à haut niveau Qsage, un outil qui sert à définir des problèmes d'optimisation, ToQ, un outil équivalent pour la programmation par contraintes, puis à un niveau intermédiaire, qbsolv qui permet de distribuer un problème complexe sur plusieurs passes de D-Wave et au niveau le plus bas, les instructions QMI pour piloter les qubits.

Ils proposent aussi Quadrant, un framework permettant de préparer des D-Wave pour résoudre des problèmes de machine learning. D-Wave a aussi un bon nombre de startups qui éditent des logiciels pour ses ordinateurs au Japon.

---

[569] Jonathan Dowling pensait dans la référence précédente que les seuls effets quantiques des D-Wave étaient l'effet tunnel et la superposition, mais sans intrication quantique.

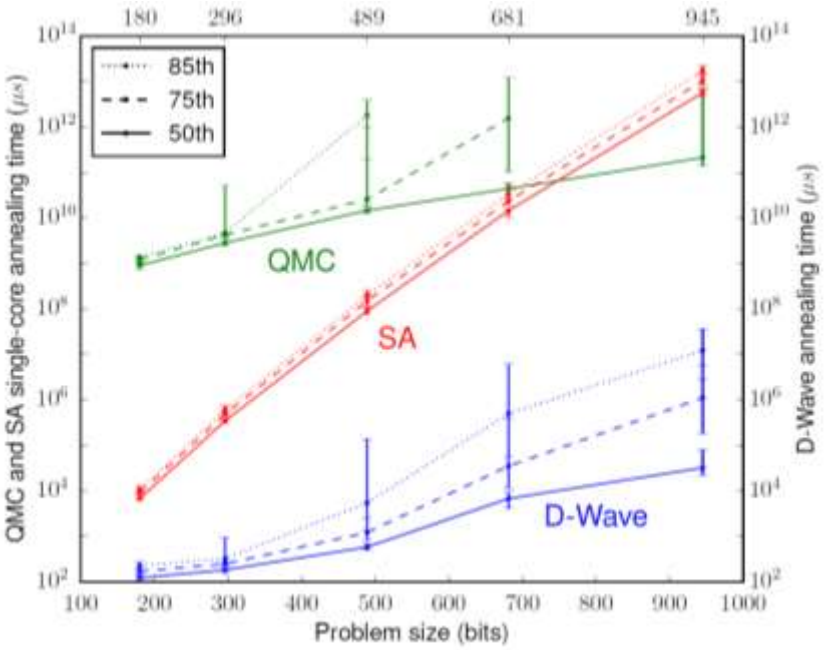
[570] C'est documenté dans Adiabatic quantum computation is equivalent to standard quantum computation, 2005 (30 pages) que nous avons déjà cité dans une partie précédente portant sur la complexité des problèmes gérables par des ordinateurs quantiques ainsi que dans How Powerful is Adiabatic Quantum Computation? de Wim van Dam, Michele Mosca et Umesh Vazirani, 2001 (12 pages).

[571] J'ai trouvé ça dans "Automatically Translating Quantum Programs from a Subset of Common Gates to an Adiabatic Representation" par Malcolm Regan et al vu dans Reversible Computation, conference proceedings, 11th International Conference, RC 2019, Lausanne, Switzerland, juin 2019 (246 pages).

[572] Dans Quantum Computing for Business, 2017 (41 slides).

[573] C'est l'avis de Jonathan P. Dowling dans Schrödinger's Killer App - Race to Build the World's First Quantum Computer par Jonathan P. Dowling, 2013 (445 pages), pages 208 à 216.

[574] Voir Analog errors in quantum annealing: doom and hope par Adam Pearson, 2019 (9 pages).



Comme les ordinateurs D-Wave sont les seuls qui soient utilisés chez des clients, les études de cas d’usage sont les plus nombreuses, même si elles sont assez exotiques et relèvent le plus souvent de “proof of concepts” et pas encore de mise en production. L’une des plus anciennes est celle Google et de la NASA réalisée avec un D-Wave de 2013 pour la résolution d’un problème d’optimisation et de combinatoire dans un graphe dont l’algorithme avait été conçu en 1994.

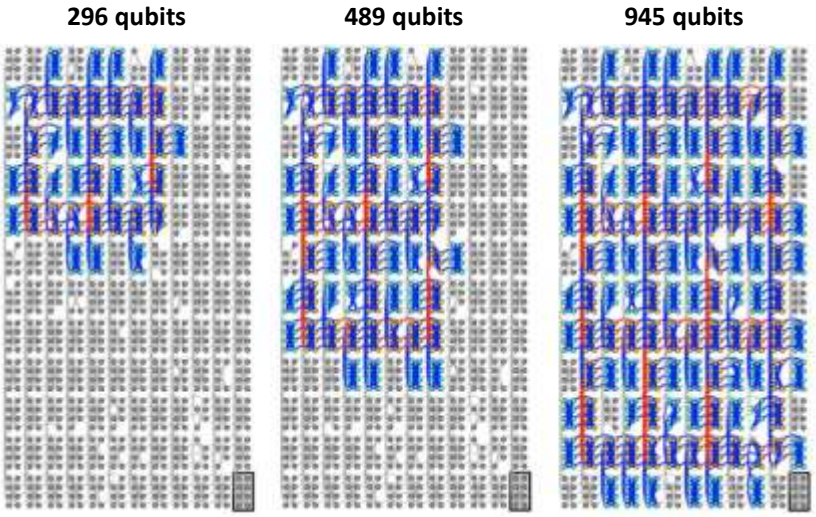
Google annonçait en 2015 avoir obtenu une performance 100 millions de fois supérieure à celle d’ordinateurs traditionnels, en fait, des PC[575]. Les éléments de comparaison portaient sur deux algorithmes leur étant destiné le “simulated annealing”, simulant l’ordinateur D-Wave sur ordinateurs classiques et une QMC (Quantum Monte Carlo) optimisée pour ordinateur traditionnel, et qui donne de meilleurs résultats en termes de montée en puissance que l'émulation du quantique sur HPC. Les critiques ont été nombreuses sur cette performance[576].

[575] Dans Google's D-Wave 2X Quantum Computer 100 Million Times Faster Than Regular Computer Chip par Alyssa Navarro dans Tech Times, novembre 2015. Et documentée dans What is the Computational Value of Finite Range Tunneling (17 pages).

[576] Dont Temperature scaling law for quantum annealing optimizers, 2017 (13 pages), qui pointe les limitations du recuit quantique.

Le layout physique de qubits utilisé pour résoudre ce problème exploitait respectivement 296, 489 et 945 qubits, comme illustré *ci-contre*. Ce layout n'est pas fondamentalement différent des ordinateurs supraconducteurs classiques, au nombre de qubits près[577].

Depuis que Google est passé à la suprématie quantique sur son propre processeur Sycamore à qubits universels supraconducteurs, on n'en parle évidemment plus.



"What is the Computational Value of Finite Range Tunneling" – Google, janvier 2016

D-Wave communique sur de nombreuses autres de ses références pilotes[578] :

- Chez l'équipementier japonais **Denso**, présentée au CES 2017 de Las Vegas, avec un système d'optimisation d'une flotte de véhicules de livraison de Toyota.
- Avec **Biogen**, **1Qbit** et **Accenture** pour du criblage de molécules visant à identifier des molécules pour un reciblage thérapeutique, avec un problème de colorisation de carte[579]. Difficile de dire ce que cela a généré en pratique. Leur partenaire **Menten AI** réalise des analyses de protéines.
- Avec **Lockheed-Martin** qui a pu produire des procédures de validation de logiciels embarqués en 6 semaines au lieu de 8 mois avec un D-Wave et son outil QVTRace[580].
- Avec **Volkswagen** pour gérer l'exploitation d'une flotte de taxis à Beijing et pour mettre au point de nouvelles batteries[581]. La solution a été utilisée en novembre 2019 pour optimiser le trajet de navettes pour le WebSummit de Lisbonne, en partenariat avec Here et le Data:Lab de Volkswagen à Munich.
- Avec la **NASA** qui a également expérimenté les D-Wave dans différents domaines, y compris pour la détection d'exoplanètes par analyse d'observations télescopiques par la méthode des transits ainsi que pour divers problèmes d'optimisation et de planification[582].
- Avec **GE Research**, pour une application hybride d'optimisation d'allocation de ressources pour de la maintenance.

---

[577] La matrice des chimera de D-Wave requiert un processus de conversion de son problème sur le maillage des qubits. Ce processus est jusqu'à présent surtout exploité pour des problèmes qui cadrent bien avec cette organisation des qubits. Pour un problème d'optimisation arbitraire, la conversion donne un résultat qui n'est pas probant en termes d'efficacité et d'accélération. C'est ce qui ressort des travaux de Daniel Vert, thésard au CEA LIST, dans On the limitations of the chimera graph topology in using analog quantum computers par Daniel Vert et al, CEA LIST, 2019 (5 pages) ainsi que dans Revisiting old combinatorial beasts in the quantum age: quantum annealing versus maximal matching, Daniel Vert et al, octobre 2019 (36 pages).

[578] J'en ai trouvé un inventaire relativement récent dans Quantum Applications par D-Wave, mai 2019 (96 slides).

[579] Décrit dans Programming with D-Wave Map Coloring Problem 2013 (12 pages).

[580] Voir Quantum Computing Approach to V&V of Complex Systems Overview, 2014 (31 slides) et Experimental Evaluation of an Adiabatic Quantum System for Combinatorial Optimization, 2013 (11 pages).

[581] Voir Forget quantum supremacy: This quantum-computing milestone could be just as important par Steve Ranger, décembre 2019.

[582] Voir la très intéressante présentation Quantum Computing at NASA: Current Status de Rupak Biswas, 2017 (21 slides) ainsi que Adiabatic Quantum Computers: Testing and Selecting Applications de Mark A. Novotny, 2016 (48 slides), dont de nombreux slides sont caviardés pour des raisons de confidentialité.

- Avec le retailer britannique **Ocado**, pour l'optimisation du fonctionnement de robots de manutention d'entrepôts.
- Pour la détection de la formation de réseaux terroristes en Syrie via la détection de déséquilibres dans les réseaux sociaux, réalisée par le **Los Alamos National Laboratory** en liaison avec l'**Université de Stanford**[583]. C'était un prototype, pas un système opérationnel.
- Avec des **simulations physiques de matière topologique et de changement de phase**[584].
- En avril 2020, D-Wave ouvrait un accès gratuit à ses ordinateurs en cloud aux chercheurs cherchant des **solutions à la pandémie covid-19**[585]. En pratique, les solutions développées relevaient de la résolution de problèmes d'optimisation comme pour optimiser le routage de patients vers les hôpitaux au Japon, la modélisation de la propagation du virus, la gestion d'agenda des infirmières dans les hôpitaux, l'évaluation du rythme de mutation du virus et du criblage de molécules. Reste à prouver que les D-Wave fournissent un véritable avantage quantique pour résoudre ces différents problèmes.

En résumé, le recuit quantique a beau être une technique contestée par nombre de spécialistes, elle a le mérite d'exister et d'être testable dans de nombreux cas d'usages[586]. Elle fera probablement des progrès intéressants à surveiller dans sa génération Pegasus.

Supraconducteurs

Après avoir décrit l'offre de D-Wave, passons à celle des ordinateurs quantiques supraconducteurs à portes quantiques universelles. En effet, d'un point de vue physique, les ordinateurs à recuit quantique de D-Wave et ceux de cette partie sont assez voisins, utilisant des variantes de l'effet Josephson dans des circuits supraconducteurs. La programmation et les capacités ne sont par contre pas du tout les mêmes.

Les qubits supraconducteurs occupent pour l'instant la voie royale de l'ordinateur quantique, étant exploités à la fois par IBM, Google, Intel, Rigetti, de nombreuses autres startups comme IQM en Finlande ou Alice&Bob en France, sans compter le CEA qui planche dessus et est même à l'origine d'une part des technologies de ce domaine.

Dans le quantique universel, ce sont les ordinateurs qui scalent le mieux pour l'instant, même si le résultat est modeste avec un record en date de 53 qubits opérationnels pour Google et IBM[587].

---

[583] Voir Using the D - Wave 2X Quantum Computer to Explore the Formation of Global Terrorist Networks par John Ambrosiano et al, 2017 (14 pages).

[584] Voir Observation of topological phenomena in a programmabale lattice of 1,800 qubits, août 2018 (37 slides).

[585] Voir Can Quantum Computers Help Us Respond to the Coronavirus? par Mark Anderson, avril 2020.

[586] Pour en savoir plus sur D-Wave, voici leurs explications sur la structure de leur matériel, une vidéo d'explication de la structure des chipsets de D-Wave, une vidéo de Linus, un bloggeur qui rentre dans les entrailles d'un D-Wave 2000Q de manière assez détaillée, D-Wave quantum computer de Gradu Amaierako Lana, 2016 (33 pages), la vidéo de l'intervention de Colin Williams à USI en juin 2018 à Paris (33 minutes) ainsi que Near-Term Applications of Quantum Annealing, 2016, une présentation de Lockheed Martin intéressantes sur les usages d'un ordinateur D-Wave (34 slides). Et les témoignages de leurs clients dans Qubits 2017. Voir aussi Brief description on the state of the art of some local optimization methods: Quantum annealing, Alfonso de la Fuente Ruiz, 2014 (21 pages).

[587] Voir un point général sur la question dans Superconducting Qubits Current State of Play par Morten Kjaergaard et al, MIT & Chalmers, 2020 (30 pages).

qubits supraconducteurs

avantages

- **technologie prioritaire** dans la recherche publique et dans le privé (IBM, Google, Rigetti, Intel, etc).
- **record de 53 qubits programmables** chez Google et IBM.
- atteinte d'une **suprématie quantique** par Google en octobre 2019.
- progrès constants dans la **réduction du bruit**.
- maîtrise des **technologies habilitantes** : cryostats, câblage, amplificateurs, logique, capteurs.
- **technologie potentiellement scalable** et déployable en 2D.

inconvénients

- **temps de cohérence** des qubits < 100 µs.
- **niveau de bruit** dans les qubits.
- **qubits hétérogènes** nécessitant un calibrage, notamment en fréquences d'activation par micro-ondes.
- technologie la plus **exigeante en cryogénie**, à <15 mK.
- **complexité du câblage** et des composants électroniques passifs et actifs pour le contrôle des qubits par micro-ondes.
- **couplage limité** entre qubits proches dans les structures 2D.
- **taille des qubits** et miniaturisation délicate.

Dans les qubits supraconducteurs, la circulation du courant est contrôlée par des portes à effet Josephson qui s'ouvrent en fonction de l'application d'un champ magnétique externe. C'est une sorte de robinet, un peu comme la base d'un transistor bipolaire.

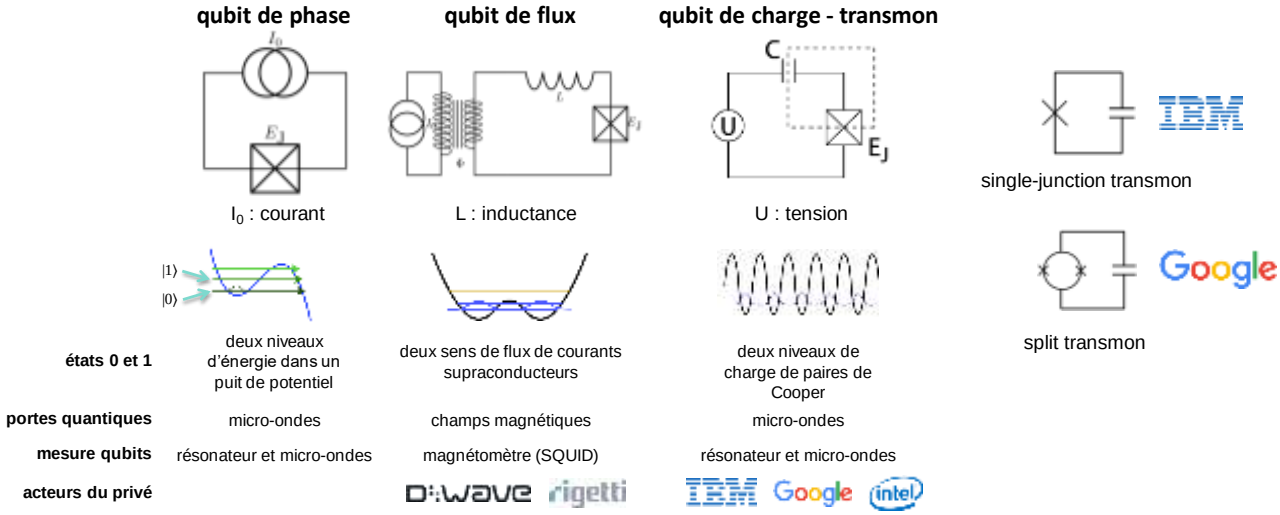
L'effet Josephson se manifeste par la circulation d'un courant au travers d'une fine barrière isolante nanométrique entre deux métaux supraconducteurs en fonction de la différence de phase du courant de part et d'autre de la barrière. On a pu créer des qubits supraconducteurs grâce à la capacité des portes à effet Josephson pour introduire une non-linéarité permettant de créer deux états bien distincts et séparés par une barrière énergétique unique. J'essaye d'expliquer cela dans un schéma un peu plus loin[588].

Les qubits supraconducteurs ont la particularité d'être les seuls qui sont macroscopiques, au sens où ils ne sont pas liés au contrôle d'une particule unique comme atome, électron ou un photon comme dans les autres technologies de qubits. En termes de taille, ce sont donc ipso-facto les plus gros qubits qui soient. A température supraconductrice, les électrons supraconducteurs d'une boucle Josephson se comportent cependant comme une particule unique. Cela vient du fait que les paires de Cooper sont l'un des rares ensembles de particules qui sont des bosons. Ils peuvent donc être condensés dans un même état quantique.

Ils forment des atomes artificiels avec des niveaux d'énergie contrôlables avec précision en fonction de leurs paramètres faits de barrière Josephson, capacités et inductances mises en série et/ou en parallèle[589].

[588] Source du schéma : A Quantum Engineer's Guide to Superconducting Qubits, par Philip Krantz et al, 2019 (67 pages), qui décrit bien les sources de bruit dans les qubits supraconducteurs et les mécanismes de leur contrôle ainsi qu'avec force détails la manière dont les micro-ondes sont utilisées pour à la fois générer les portes quantiques à un qubit et à deux qubits ainsi que mesurer l'état des qubits. Les prérequis pour pouvoir comprendre un tel papier sont nombreux : physique classique, physique quantique avec équation de Schrödinger et sphère de Bloch, génie électrique, supraconductivité, électromagnétisme, électronique, logique booléenne, traitement du signal et des micro-ondes.

[589] Cette propriété d'atome artificiel a été démontrée en 1985. Voir Energy-Level Quantization in the Zero-Voltage State of a Current-Biased Josephson Junction par John Martinis, Michel Devoret et John Clarke, 1985 (2 pages).



source des schémas : Implementing Qubits with Superconducting Integrated Circuits de Michel Devoret, 2004 (41 pages) et Flux Noise in Superconducting Qubits, 2015 (44 slides).

Il existe plusieurs types de qubits supraconducteurs qui diffèrent par la manière d'encoder l'information quantique dans deux états bien distincts[590] :

- **Qubits de phase** : ils utilisent des jonctions Josephson plus grandes que dans les qubits de charge. L'état du qubit correspond à deux niveaux d'énergie de courants dans une jonction Josephson. Cette approche est expérimentée par le NIST aux USA. Une équipe allemande (Jülich, Université de Munster) et russe (Institut Kotelnikov) proposait début 2020 d'utiliser des nanotubes de $YBa_2Cu_3O_{7-x}$ (aussi dénommé YBCO, pour yttrium, baryum, cuivreet oxyde, qui est supraconducteur à 92K) pour créer des qubits de phase contrôlables par un seul photon micro-onde[591].
- **Qubits de flux** : leur état correspond au sens de circulation du courant supraconducteur dans sa boucle. C'est le plus facile à comprendre et à visualiser. La mesure de l'état d'un tel qubit utilise un SQUID (superconducting quantum interference device) avec deux jonctions Josephson montées en parallèle, un magnétomètre qui va être capable de mesurer le sens du courant dans le qubit, donc son état 0 ou 1. C'est l'approche de D-Wave, de Rigetti, du MIT et de TU-Delft aux Pays-Bas.
- **Qubits de charge** : leur état correspond à des seuils de passage de courant dans la jonction Josephson de la boucle supraconductrice. De petites jonctions Josephson délimitent un îlot supraconducteur avec une charge électrique bien définie. Les états de base de tels qubits de charge sont les états de charge de l'îlot en couples d'électrons supraconducteurs appelés paires de Cooper. La variante la plus courante est celle du transmon. Elle est utilisée par IBM, par Google[592] ainsi qu'au CEA à Saclay.

  A ce jour, ce sont les qubits générant le taux d'erreur le plus faible dans les qubits supraconducteurs. On les départage au moins en deux catégories : les qubits avec une seule jonction Joseph-

[590] C'est bien expliqué dans Practical realization of Quantum Computation (36 slides) ainsi que dans une conférence de Serge Haroche du Collège de France de 2011.

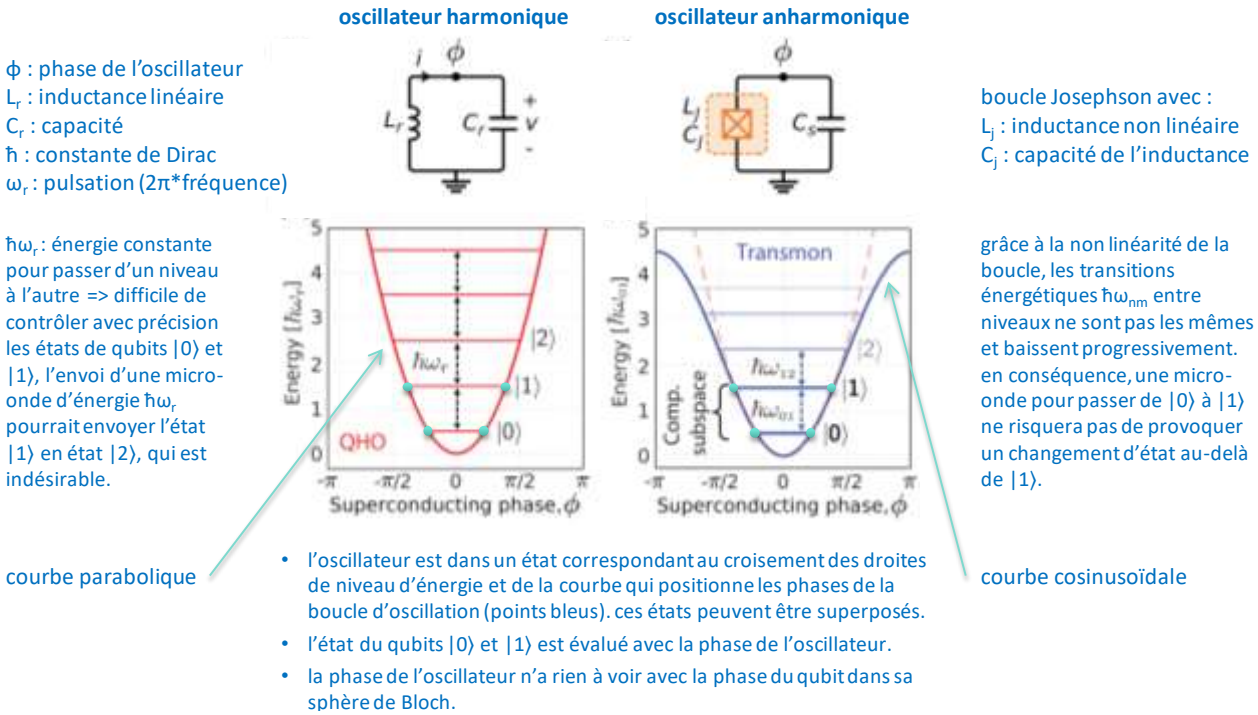
[591] Voir Energy quantization in superconducting nanowires, février 2020, qui fait référence à Energy-level quantization and single-photon control of phase slips in YBa2Cu3O7–x nanowires par M. Lyatti, février 2020.

[592] Pour « transmission-line shunted plasma oscillation qubit ».

son (single-junction transmon, utilisée par IBM) ou avec deux jonctions Josephson montées en parallèle (spit transmon, utilisée par Google)[593].

D'un point de vue historique, les premières boites de paires de Cooper ont été créées expérimentalement en 1997 au CEA de Saclay par **Vincent Bouchiat**. La première démonstration de qubit supraconducteur a été réalisée par l'équipe de **Yasunobu Nakamura** en 1999 chez NEC puis à **Delft** aux Pays-Bas la même année avec un qubit de flux, puis avec un qubit de phase en 2002 au NIST à Boulder et avec le quantronium en 2002, un qubit de flux, au CEA Saclay dans l'équipe de **Daniel Estève**. *Ci-dessous*, Daniel Esteve présentant le premier chipset à deux qubits de son laboratoire.

Pour ce qui suit, nous allons nous focaliser sur ces qubits transmon qui sont les plus courantes, et exploités par IBM, Google et Intel. Ce sont des oscillateurs anharmoniques et donc non linéaires. Leur non-linéarité provient de la jonction Josephson qui permet de mieux séparer deux états énergétiques de la boucle supraconductrice (*à droite* dans le schéma) qu'avec un simple résonateur linéaire couplant une capacité et une inductance (*à gauche*).



[593] Transmon est un diminutif de "**Trans**mission line shunted plas**mon** oscillation circuit" créé par Rob Schoelkopf, autrement dit, un circuit oscillateur à base de jonction Josephson shunté. Le shunt est devenu une capacité qui filtre les basses fréquences. Un plasmon dénomme le comportement collectif d'électrons libres de métaux, ici sous la forme de paires de Cooper supraconductrices.

Dans un oscillateur harmonique, les niveaux d'énergie sont espacés du même niveau d'énergie comme pour un photon dans une cavité. Les niveaux d'énergie y sont des multiples du premier niveau d'énergie ($\hbar\omega_r$ dans le schéma). Dans un oscillateur harmonique, la capacité a une énergie électrique (cinétique) et l'inductance, une énergie magnétique (potentielle, sorte de ressort).

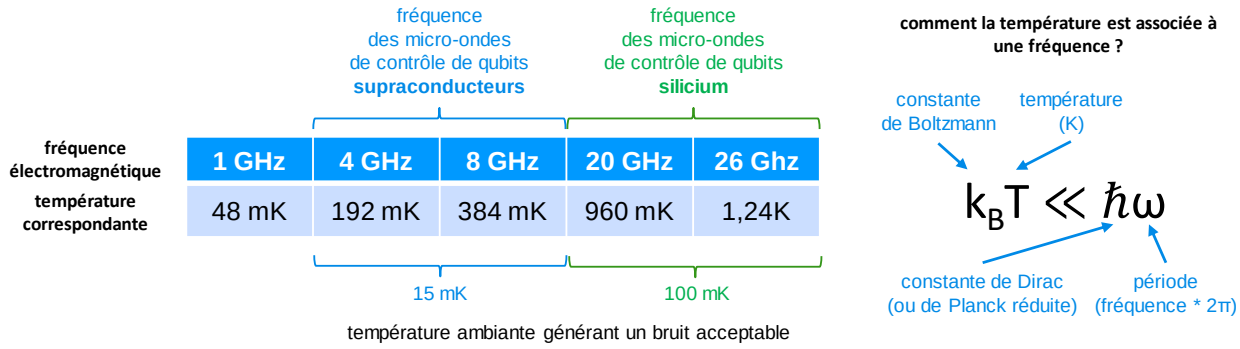
Les qubits correspondent à la superposition linéaire des deux premiers niveaux d'énergie. Ils doivent être bien séparables des suivants. Cette séparation est rendue possible parce que l'énergie envoyée pour passer d'un niveau à l'autre doit être différente d'un étage à l'autre.

Comme les étages supérieurs sont moins espacés, le niveau d'énergie pour les atteindre est plus faible. Ainsi, lorsque l'on active par des micro-ondes les qubits, ils ne risquent plus de passer à un niveau d'énergie supérieur. C'est l'intérêt de la non-linéarité.

L'oscillateur anharmonique de la boucle Josephson est assuré par une inductance non linéaire L_j. Le niveau d'énergie entre 0 et 1 de $\hbar\omega_{01}$ est supérieur aux niveaux d'énergies nécessaires pour passer aux étages supérieurs $\hbar\omega_{12}$ et $\hbar\omega_{23}$.

Le niveau d'énergie $\hbar\omega_{01}$ est calibré pour correspondre à des fréquences de micro-ondes générables couramment par de l'électronique de laboratoire, dans la bande des 4 à 8 GHz. Il est important d'éviter des fréquences trop élevée, notamment celles qui s'approchent du téra-Hertz.

En même temps, il ne doit pas être trop bas pour pouvoir être compatible avec la température de refroidissement du processeur et au bruit ambiant. Celles du contrôle des qubits supraconducteur autour de 5 GHz ont un niveau d'énergie équivalent à une température d'environ 250 mK, bien supérieure à la température de 15 mK couramment utilisée. Les micro-ondes de contrôle des qubits silicium sont situées aux alentours de 20 GHz et permettent de monter à 100 mK.



Comment fonctionnent les portes quantiques sur des qubits supraconducteurs ? Elles sont générées par des pulsations micro-ondes envoyées via des câbles coaxiaux sur les qubits[594]. Leur fréquence est ajustée sur le niveau d'énergie $\hbar\omega_{01}$ évoqué plus haut. Cette fréquence est calibrée pour être différente sur des qubits adjacents pour éviter les effets de bord[595]. L'axe de rotation de la porte quantique dans la sphère de Bloch est lié à la modulation d'amplitude de la micro-onde. La durée de l'impulsion va conditionner l'angle de la rotation. Cela permet de créer des portes T, S et R à phase autre que le quart ou le demi-tour dans la sphère de Bloch[596].

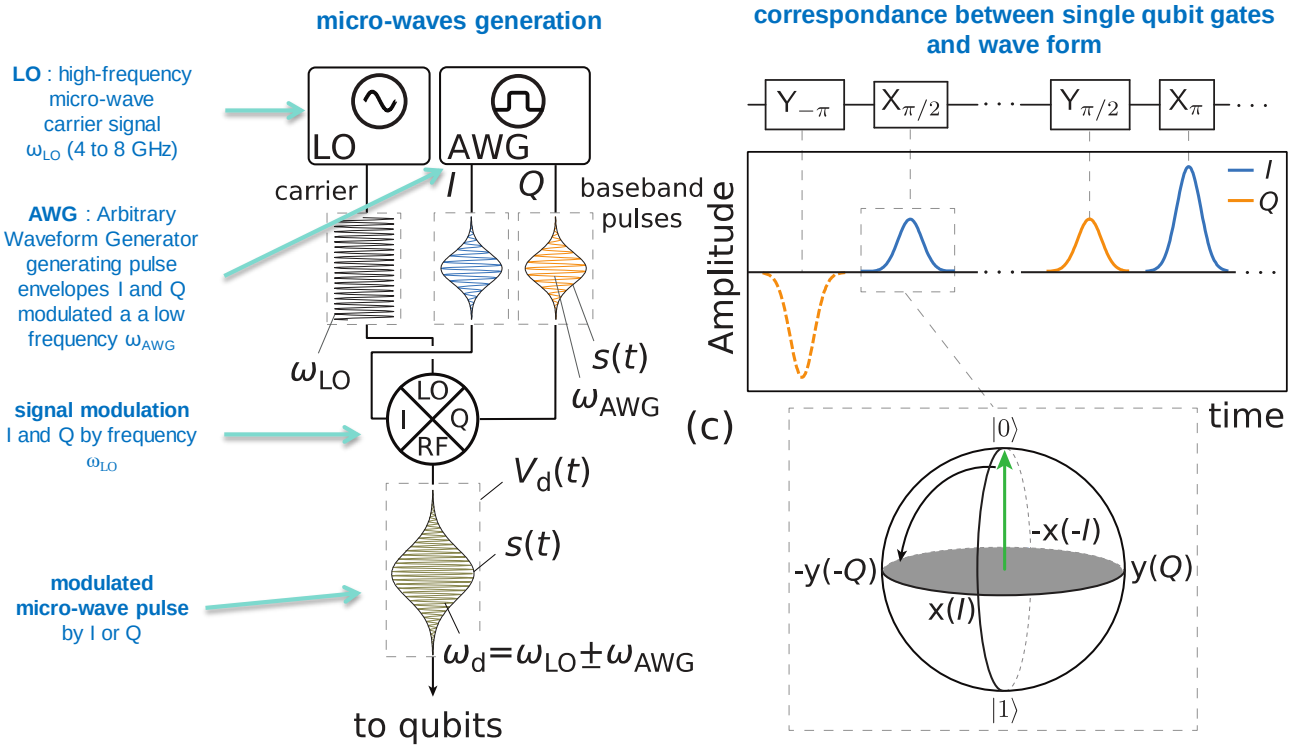
---

[594] Source des illustrations utilisées dans le schéma ci-dessus : A Quantum Engineer's Guide to Superconducting Qubits, par Philip Krantz et al, 2019 (67 pages).

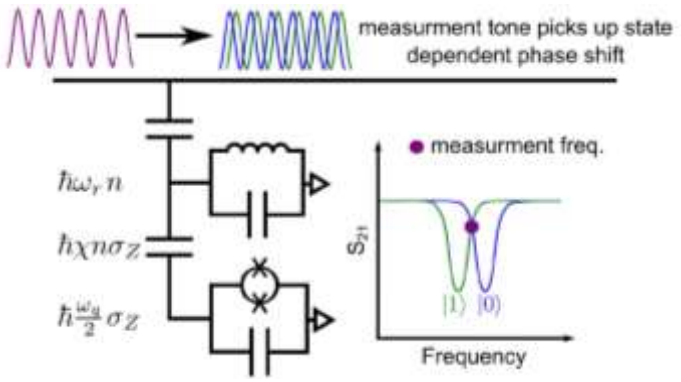
[595] Un calibrage précis de ces fréquences est d'ailleurs nécessaire du fait de la variabilité du comportement des boucles Josephson qui sont différentes l'une à l'autre en raison de l'imprécision des techniques de fabrication. Cette variabilité n'existe pas pour des qubits basés sur des particules uniques comme les ions piégés ou les atomes froids.

[596] Ces portes peuvent être optimisées en modulant la pulsation de manière optimale. Voir Implementing optimal control pulse shaping for improved single-qubit gates par J. M. Chow et al, mai 2020 (4 pages) qui anticipe au passage la capacité à générer des portes à un qubit en 1 ns, contre un minimum actuel plutôt situé aux alentours de 20 ns..

Les portes à deux qubits sont réalisées avec un circuit de couplage entre les deux qubits qui peut être une simple capacité ou un système contrôlable dynamiquement. Comme nous le verrons plus loin, ce couplage est géré par un qubit intermédiaire dans le processur Sycamore de Google.



La mesure de l'état d'un qubit supraconducteur dépend de leur type. Pour les qubits transmon qui sont les plus courants, un résonateur est utilisé à côté du qubit qui va émettre une micro-onde qui va être modifiée par le qubit et dont on analyse ensuite la phase pour identifier l'état 0 ou 1 du qubit[597]. Cette micro-onde est modulée sur une fréquence plus élevée que la fréquence d'activation des portes quantiques, comprise entre 7 et 8 GHz[598].



Ces interactions entre qubits supraconducteurs et photons micro-ondes font partie d'une branche de la physique quantique dénommé **électrodynamique quantique de circuits**, ou cQED en anglais, pour circuits quantum electrodynamics[599].

---

[597] Source du schéma : Google's quantum computer and pursuit of quantum supremacy par Ping Yeh, Google Santa Barbara, septembre 2019 (80 slides).

[598] D'autres techniques de mesure de l'état des qubits supraconducteurs sont envisagées, comme l'activation de la fluorescence du qubit. Elle passe par le saut de l'état |0⟩ à |2⟩ du qubits, la transition à l'état |1⟩ n'étant pas possible avec le photon d'excitation de la fluorescence. Voir la thèse Energy and Information in Fluorescence with Superconducting Circuits de Nathanaël Cottet, 2018 (227 pages).

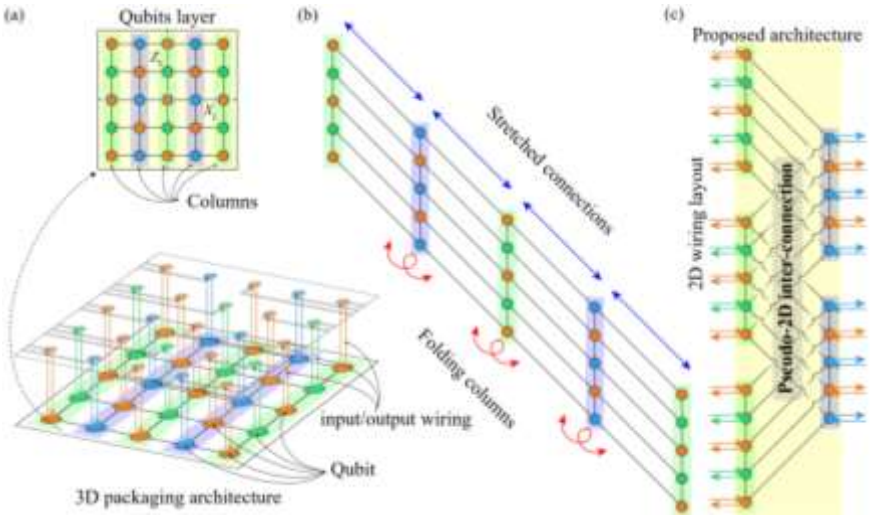
[599] Voir The Invention of Circuit Quantum Electrodynamics par Agustin Di Paolo, janvier 2019 qui décrit l'histoire et les fondamentaux de la QED. La cQED a été introduite en 2004 par les équipes de l'université de Yale qui s'était inspirée des travaux de Serge Haroche, devenu prix Nobel de physique en 2012 pour ses travaux sur l'interaction entre atomes froids et cavités supraconductrices. Voir à ce sujet l'excellent Circuit Quantum Electrodynamics par Alexandre Blais, Andreas Wallraf et al, mai 2020 (82 pages).

L'un des objectifs clés des chercheurs est de transformer ces photons micro-ondes en photons dans la bande visible/infrarouge pour permettre leur transport à longue distance, notamment via des moyens de télécommunication à base de fibre optique, qui deviendraient la base du calcul quantique distribué[600].

Un des problèmes à résoudre réside dans la connectique interne au chipset. Habituellement, un système en 3D est créé avec une couche pour la lecture et une autre pour les opérations des qubits.

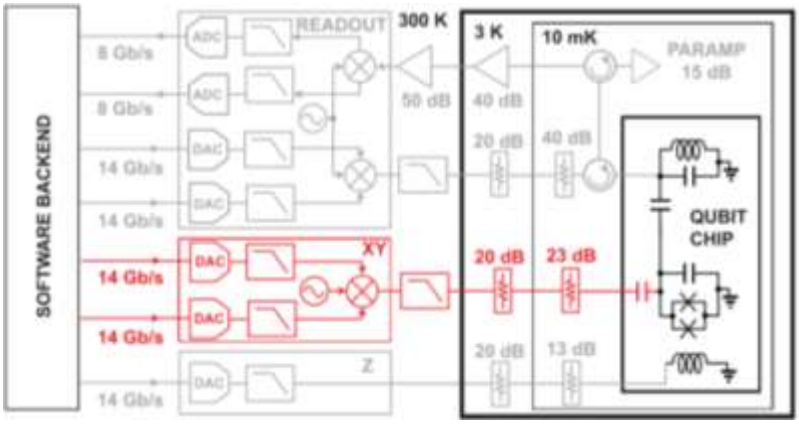
Cette topologie a pour conséquence de limiter la relation entre les qubits avec leurs voisins immédiats dans une structure en matrice.

Une équipe japonaise proposait en 2020 une solution originale consistant à mettre à plat la matrice et en rendant possible la connexion des éléments de contrôle en 2D. Mais au prix d'un recouvrement d'une partie des liaisons entre qubits[601].



Dans l'état de l'art actuel, les cryostats abritant ces qubits sont encombrés de câbles qui pilotent les qubits, d'atténuateurs et d'amplificateurs de micro-ondes pour la lecture de l'état des qubits[602].

Les convertisseurs numérique-analogiques gérant les micro-ondes à température ambiante gèrent pour leur part un très gros volume de données comme indiqué dans le schéma *ci-contre* correspondant à Sycamore de Google (octobre 2019). A ceci près que ces données sont gérées en temps réel. Il ne semble pas nécessaire de les stocker à moyen et long terme. Ce n'est pas un système de big-data !



Cette électronique et tringlerie est à la fois embarrassante et consommatrice d'énergie, dans des cryostats dont le budget thermique de refroidissement est limité, surtout dans les étages bas en-dessous de 1K.

A l'extérieur du cryostat se trouve un encombrant appareillage de générateurs de micro-ondes qui n'est pas du tout miniaturisé à ce stade. Il faut un rack de ces générateurs pour contrôler une centaine de qubits.

---

[600] Voir par exemple Microwave-to-optical conversion via four-wave mixing in a cold ytterbium ensemble par Jacob P. Covey et al, juillet 2019 qui portent sur cette conversion.

[601] Voir Wiring the quantum computer of the future: A novel simple build with existing technology par Jaw-Shen Tsai (Japon), avril 2020 qui fait référence à Pseudo-2D superconducting quantum computing circuit for the surface code par H. Mukai, février 2019 (8 pages).

[602] C'est bien expliqué dans Superconducting Circuits Balancing Art and Architecture de Irfan Siddiqi de Berkeley Lab, 2019 (34 slides) d'où est extrait le schéma suivant sur « The tyranny of wires ».

L'électronique utilisée est pour l'instant de l'appareillage de laboratoire de recherche comme l'illustre l'exemple *ci-dessous* de configuration pour tester un chipset de 5 qubits supraconducteurs, en 2015[603]. Pour un plus grand nombre de qubits, des générateurs de micro-ondes multiples sont exploités, comme ceux de **Zurich Instruments**, **Rohde & Schwarz** ou **Tektronix**. Ces générateurs externes sont appréciés pour la qualité des pulsations micro-ondes qu'ils produisent.

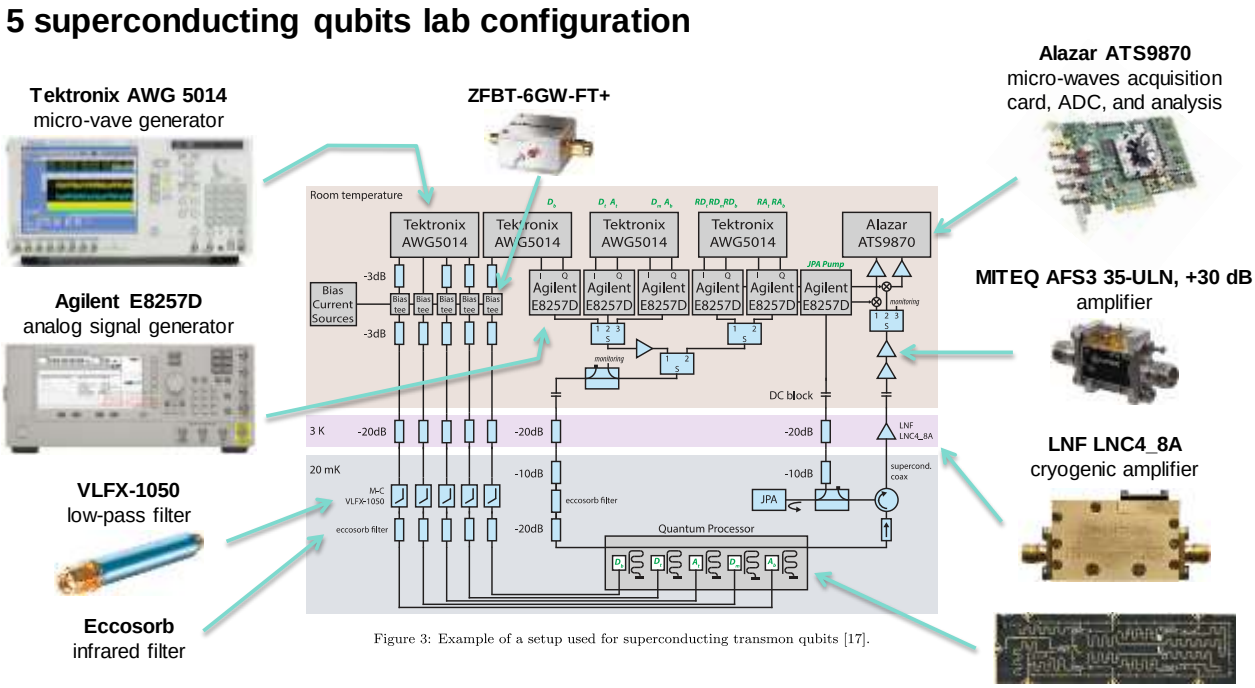
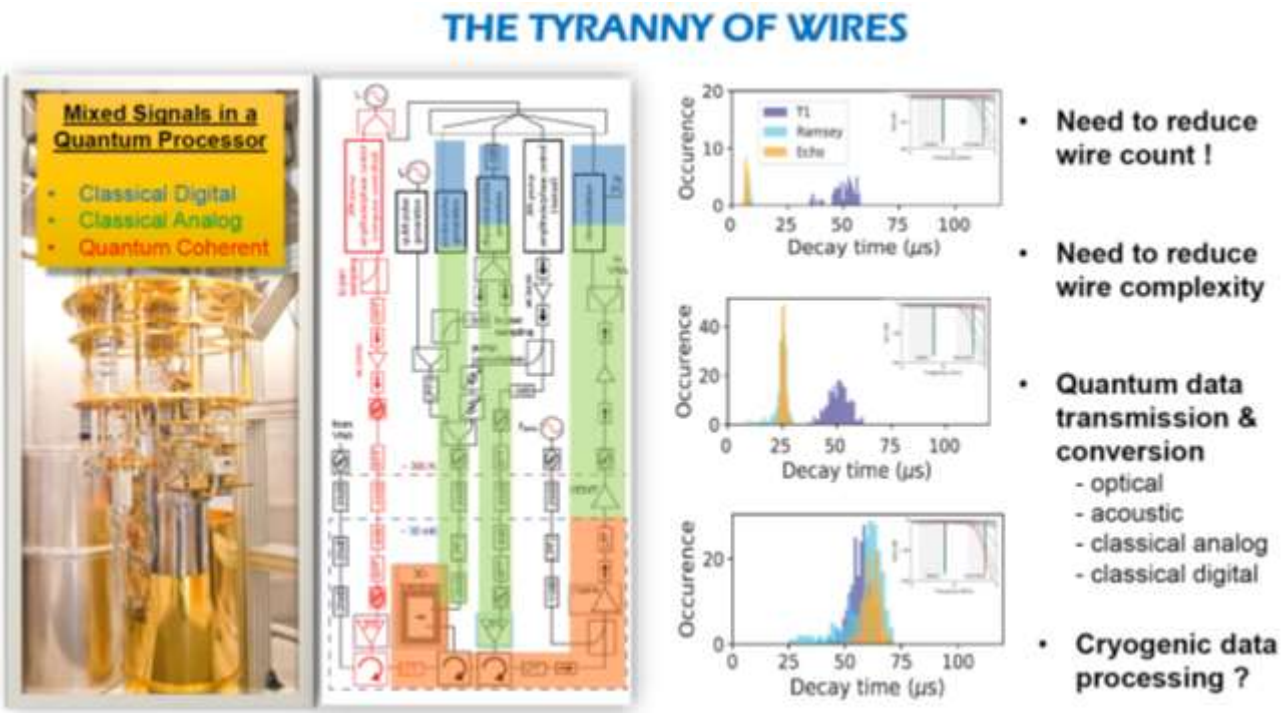


Figure 3: Example of a setup used for superconducting transmon qubits [17].

Nous avons déjà vu dans le chapitre sur l'électronique embarquée dans les cryostats de nombreuses tentatives de miniaturisation de tout ou partie de ces composants, le top ayant l'air d'être le chipset de contrôle très complet que met au point la startup SeeQC.



[603] Le schéma provient de The electronic interface for quantum processors par J.P.G. van Dijka et al, mars 2019 (15 pages). J'ai ai ajouté une photo des outils exploités dans la configuration.

Des questions se posent aussi sur la taille des qubits qui est de l'ordre du micron, ce qui rend difficile la création de grandes puces avec des millions de qubits. Une miniaturisation semble toujours possible mais elle est délicate à gérer car la qualité des qubits supraconducteurs semble baisser avec la diminution de leur taille[604].

Les qubits supraconducteurs sont assez performants du côté des taux d'erreur, même s'ils restent encore élevés, augmentent avec le nombre de qubits et nécessitent d'employer des codes de correction d'erreur et un fort ratio de qubits physiques par qubits logiques pour créer des ordinateurs quantiques exploitables. On n'est pas capable d'expérimenter cela car on manque encore de qubits physiques pour ce faire. On se contente donc de NISQ, ces calculateurs quantiques « bruyants » avec lesquels on peut enchaîner un nombre réduit de portes quantiques.

Les progrès sont toutefois constants dans la réduction du bruit des qubits dans cette technologie. Ce bruit a plusieurs origines comme les fluctuations de charge, les électrons baladeurs, les impuretés dans les matériaux notamment comportant des atomes d'oxygène et les perturbations magnétiques.

Pour ce qui est de la mesure de l'état des qubits supraconducteurs, une équipe de chercheurs canado-américaine propose une méthode optique de mesure miniaturisable[605]. Une variante a été proposée en 2018 par Robert McDermott de l'Université Wisconsin-Madison, l'objectif étant d'améliorer la fiabilité de la mesure. Elle serait pour l'instant de 92% et pourrait monter à 99%[606].

Les qubits supraconducteurs utilisent sinon souvent du **niobium** pour ses portes à effet Josephson, qui peut être remplacé par de l'**aluminium**, utilisé notamment chez Rigetti.

Les travaux d'IBM, Google, Intel et Rigetti dans les qubits supraconducteurs sont les arbres qui cachent la forêt. Un nombre important de laboratoires travaillent sur cette technologie au niveau fondamental et expérimental et partout dans le monde. Aux USA, comme à **Yale** ou au **MIT**[607], en Europe comme en Allemagne, en Suède au **WACQT** de l'Université Chalmers, en France au **CEA**, en Suisse à l'**ETH Zurich**[608], au **VTT** en Finlande[609], au **Japon** et un peu partout ailleurs.

L'équipe de physiciens de Daniel Estève au CEA de Saclay continue de travailler sur les qubits supraconducteurs tendance transmon avec en ligne de mire la création de qubits plus stables et générant moins d'erreurs. C'est une approche de recherche long terme qui fait partie du champ de la physique de la matière condensée. En d'autres termes, de la matière à très basse température[610].

---

[604] Voir Investigating surface loss effects in superconducting transmon qubits par J. M. Gambetta et al, 2016 (5 pages) ainsi que On-chip integrable planar NbN nanoSQUID with broad temperature and magnetic-field operation range par Itamar Holzman et Yachin Ivry du Technion, avril 2019 (7 pages) qui ont prototypé des SQUIDs miniaturisés de 45 nm x 165 nm.

[605] Voir Heisenberg-limited qubit readout with two-mode squeezed light, 2015 (12 pages).

[606] Dans Measurement of a Superconducting Qubit with a Microwave Photon Counter, mars 2018 (11 pages).

[607] Voir Quantum Computing @ MIT: The Past, Present, and Future of the Second Revolution in Computing par Francisca Vasconcelos, MIT, février 2020 (19 pages). Ils ont développé un chipset de 16 qubits supraconducteur, fabriqué par les **Lincoln Labs** du MIT.

[608] Avec l'équipe d'Andreas Wallraff de l'équipe QuSurf qui travaille sur des qubits supraconducteurs et leurs codes de correction d'erreur. Ce projet est financé par l'agence IARPA américaine. En 2019, ils en étaient à 7 qubits expérimentaux. C'est aussi supporté par le projet ScaleQIT (Scalable Superconducting Processors for Entangled Quantum Information Technology) financé par l'Union Européenne et par le projet OpenSuperQ du flagship européen.

[609] VTT s'est donné comme objectif de gérer de 50 à 100 qubits supraconducteurs. VTT dispose de sa propre unité de fabrication de circuits avec une salle blanche de 2600 m^2 voisine de celle du CNRS C2V de Palaiseau. Voir Engineering cryogenic setups for 100-qubit scale superconducting circuit systems par S. Krinner et al, 2019 (29 pages).

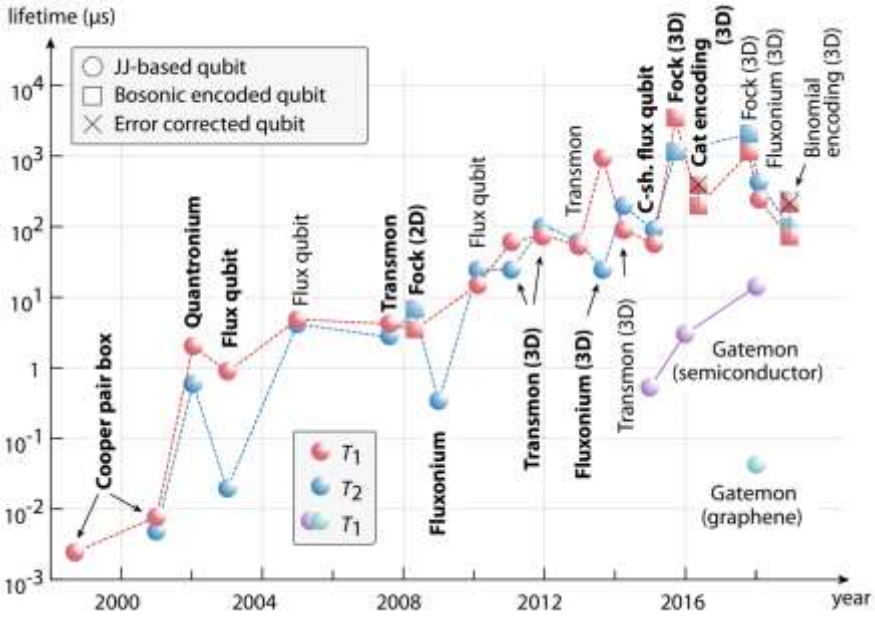
[610] Pour en savoir plus sur les qubits supraconducteurs et les défis de leur mise au point, voir notamment cette excellente présentation du MIT : Quantum Engineering of Superconducting Qubits, 2018 (58 slides) ainsi que Quantum Physics with Superconducting Qubits de Andreas Wallraff, de l'ETH Zurich, 2016 (49 slides). Voir également Quantum Computing: State of Play de Justin Dressel, 2018 (34 slides) qui comprend une bonne explication sur le fonctionnement des qubits supraconducteurs.

L'une des pistes de recherche menée au CEA consiste à associer des qubits supraconducteurs à des spins d'électron en NV centers, reliés par des micro-ondes. Les derniers pourraient servir de mémoire quantique ainsi que de moyen de mesure plus précis de l'état quantique de qubits supraconducteurs. Cette capacité des spins à servir de mémoire quantique provient d'un temps de cohérence des spins 1000 fois plus long que celui des qubits supraconducteurs (100 millisecondes vs 100 microsecondes). Ils travaillent aussi sur les moyens de convertir des micro-ondes en photons dans le visible ou l'infrarouge pour les transmettre dans des fibres optiques, autrement appelée conversion entre photons-micro-ondes et photons-optiques qui permettrait de relier des qubits supraconducteurs à longue distance.

Autre voie de recherche, le couplage de qubits supraconducteurs avec des spins nucléaires (au lieu d'être des spins d'électrons, sur noyaux de phosphore ou de bismuth) via des spins d'électrons.

Plusieurs autres techniques sont envisagées pour créer des qubits supraconducteurs résilients au bruit ou générant moins de bruit. C'est le cas des **cat-qubits** explorés notamment par la startup Alice&Bob qui valorise des travaux de nombreux laboratoires de recherche (Inria, ENS, …) ainsi que les travaux de Michel Devoret de l'Université de Yale, les **codes GKP**[611] ainsi que des **zero-π qubits** de Peter Brooks, Alexei Kitaev et John Preskill qui utilisent deux jonctions Josephson[612].

D'autres travaux visent à rallonger le temps de cohérence des qubits supraconducteurs, notamment à **Princeton**[613]. Celui-ci est en effet encore assez limité et de l'ordre de la centaine de microsecondes (µs)[614]. Il génère une contrainte sur le nombre de portes quantiques qui peuvent être exécutées dans un logiciel quantique, même si les erreurs accumulées deviennent prohibitives avant cette limite.



IBM est un des rares grands acteurs du numérique qui investit dans la recherche fondamentale et depuis très longtemps. Qui fait de la recherche fondamentale ?

---

[611] Voir Voir Quantum Error Correction with the GKP Code and Concatenation with Stabilizer Codes par Yang Wang, juillet 2019 (59 pages).

[612] Voir Protected gates for superconducting qubits par Peter Brooks, Alexei Kitaev et John Preskill, 2013 (31 pages). Il s'agit de qubits utilisant des portes quantiques corrigées par des codes de correction d'erreur en variables continues. Ils ont été expérimentés en 2019. Voir Control and coherence time enhancement of the 0–π qubit par Agustin Di Paolo, Arne Grimsmo, Peter Groszkowski, Jens Koch et Alexandre Blais, avril 2019 (22 pages) ainsi que Improving Quantum Hardware: Building New Superconducting Qubits and Couplers par Thomas Michael Hazard, 2019 (136 pages).

[613] Voir New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds par Alex P. M. Place et al, février 2020 (37 pages).

[614] Source du schema : Superconducting Qubits Current State of Play par Morten Kjaergaard et al, 2020 (30 pages).

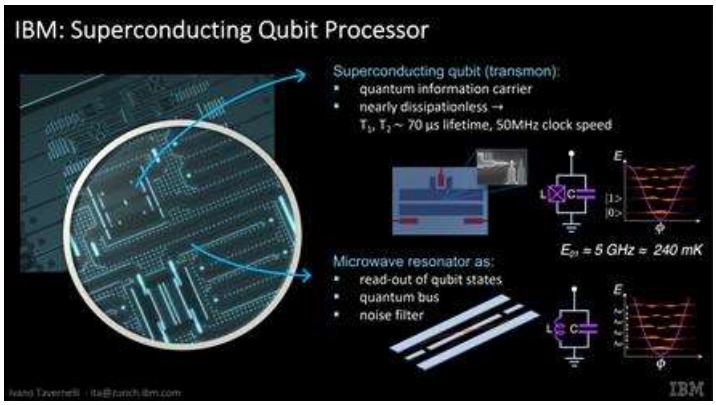
Principalement IBM, Microsoft, Google, les équipementiers et les opérateurs télécoms. Les Bell Labs issus du démantèlement d'AT&T en 1982 font maintenant partie de Nokia après être passée par Lucent et Alcatel-Lucent. Le reste des acteurs, tels qu'Apple se contente de créer des produits. Facebook fait un peu de recherche fondamentale en IA mais peu en physique fondamentale.

A ce titre, IBM est l'un des plus avancés dans la recherche sur le quantique universel, ayant tout misé sur les supraconducteurs à effet Josephson. Les efforts d'IBM dans le quantique sont sous l'aile de la marque IBM Q.

Ils sont pilotés par les chercheurs de leur site de Yorktown dans l'Etat de New York, en liaison avec différents laboratoires d'IBM dans le monde dont celui de Zurich, avec diverses universités américaines et avec l'Université ETH Zurich.

La technologie retenue par IBM est celle des qubits supraconducteurs « transmon » déjà couverte plus haut dans ce document[615]. En quelques années, IBM a fait évoluer le nombre de qubit de ses prototypes d'ordinateurs quantiques. On est ainsi passé de 5 qubits en 2016 (vidéo) à 14 qubits vers 2017. En 2017, IBM annonçait avoir atteint 50 qubits mais ceux-ci ont nécessité deux années de mise au point avant d'être utilisables[616].

En septembre 2019, IBM annonçait la mise à disposition de 53 qubits opérationnels dans le cloud, le même jour que la fuite sur la suprématie quantique de Google. Leurs efforts portent surtout sur la réduction du bruit pouvant affecter la qualité des calculs quantiques. Ils travaillent aussi sur l'utilisation de "surface codes", ces arrangements de qubits en matrices qui permettent de gérer la correction des erreurs. Mais ceux-ci ne sont pas du tout exploitables avec un tel nombre de qubits.



IBM propose un outil graphique en ligne de création de logiciels quantiques (*ci-contre*, avec la version 5 qubits lancée en 2016)[617]. Les qubits d'IBM dans le cloud sont déjà utilisés par des milliers de chercheurs, entrepreneurs et étudiants dans le monde.

Ceci étant, les qubits d'IBM ont été benchmarkés en 2017 par Kristel Michielsen et leur qualité semble bien faible[618].

En particulier, les portes CNOT semblent générer un fort taux d'erreurs.

---

[615] Le schéma provient de Quantum Computing with superconducting qubits: Applications in Chemistry and Physics, Ivano Tavernelli d'IBM Research, février 2019 (58 slides).

[616] Je m'y perds d'ailleurs un peu dans les annonces d'IBM avec leurs 5, 14, 17, 20, 50 et 53 qubits qui se sont succédées ces dernières années et qui mélangent des prouesses de laboratoire et des disponibilités opérationnelles dans le cloud. Les taux de fidélité de la version 53 qubits n'étaient pas encore publiée en mai 2020.

[617] Voici un petit tutoriel de programmation utilisant le SDK open source Qiskit qui supporte de son côté le langage de bas niveau OpenQASM qui pilote les qubits d'IBM. Voir aussi cette vidéo de vulgarisation de haut niveau par Talia Gershon.

[618] Dans Benchmarking gate-based quantum computers, 2017 (33 pages). Depuis, leur qualité semble cependant s'être améliorée.

IBM battait aussi un record d'émulation de 56 qubits en 2017, sur un supercalculateur classique de leur cru, le Vulcan BlueGene installé au Lawrence Livermore National Laboratory en Californie[619]. Il a été battu depuis par d'autres, déjà évoqués.

En janvier 2019 au CES de Las Vegas, IBM annonçait le Q System One, présenté comme étant le premier système informatique quantique universel intégré du monde, à usage scientifique et commercial. C'est un ordinateur quantique à qubits supraconducteurs à portes universelles de 20 qubits (vidéo).

L'innovation de cet ordinateur quantique mise en avant était à chercher du côté du design, créé avec les studios de design Map Project Office et **Universal Design Studio** (UK) et **Goppion** (Italie), un constructeur de dispositifs d'exposition haut de gamme pour musées qui a notamment conçu le dispositif de protection de La Joconde au Louvre et des bijoux de la Reine à la Tour de Londres.

L'ordinateur ferait 2,75 m de large, donc à peu près la taille d'un D-Wave. Cette annonce a donné l'impression à certains que cela préfigurait l'arrivée d'ordinateurs quantiques dans les foyers.

Il n'en est évidemment rien. Ces ordinateurs sont juste des machines permettant de se faire la main avec des algorithmes quantiques très simples qui sont d'ailleurs simulables sur un simple laptop dont le TCO (total cost of ownership) sera bien plus faible que celui de cette belle machine dont ni le prix ni la date de disponibilité n'ont encore été annoncés. Pour qu'un tel ordinateur quantique soit utilisable dans des applications industrielles, il faudrait qu'il dispose de centaines à des millions de qubits. Il faudra attendre quelques années si ce n'est décennies pour y parvenir.

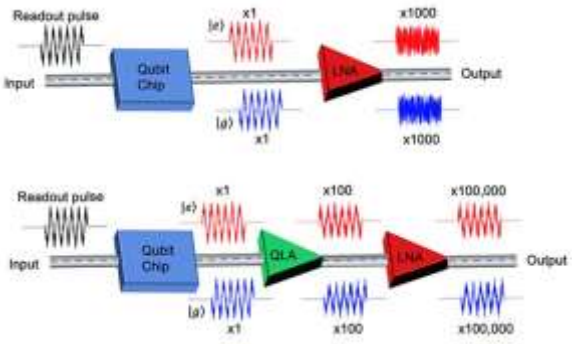
A noter qu'IBM commercialiserait son Q System One à $41M, soit trois fois plus qu'un D-Wave. Mais ce prix ne rime pas à grand-chose vu que l'ordinateur n'est pas réellement commercialisé. Il est surtout disponible dans le cloud comme nous l'avons évoqué dans une rubrique dédiée à ce sujet.

[619] Voir IBM Simulates a 56-Qubit Machine, 2017. La performance est documentée dans Breaking the 49-Qubit Barrier in the Simulation of Quantum Circuits, 2017 (24 pages).

Voici *ci-dessus* deux photos moins stylisées que celle du dessus de janvier 2019, correspondant à la présentation au CES de janvier 2020. On voit la machine mieux éclairée de face avec le chandelier ouvert pour les besoins de la présentation, l'éclairage du chandelier par le haut, le tout étant entouré de verre. La seconde photo est prise de côté et l'on voit l'arrière de la boîte. Celle-ci contient le compresseur et les pompes du cryostat ainsi que, derrière, les générateurs de micro-ondes et leurs lecteurs.

Et *ci-dessus* à droite, on peut voir l'atelier d'assemblage de l'ensemble. IBM adopte ainsi une approche préindustrielle dans la production de ses calculateurs quantiques, malgré leurs capacités fort limitées.

En janvier 2020, IBM communiquait dans le détail sur la méthode qu'ils utilisaient pour mieux gérer la lecture de l'état des qubits[620]. La lecture de l'état des qubits supraconducteurs est réalisée par l'envoi de quelques photons micro-ondes dans les 7 GHz aux résonateurs des qubits. Comme leur niveau de puissance est très faible, il doit être amplifié pour être interprété à l'extérieur du cryostat, mais sans ajouter de bruit. Jusque-là, tout est classique.



Pour ce faire, IBM utilise des amplificateurs à faible bruit (QLA pour quantum-limited amplifiers). Le Q System One représente cependant un progrès pour faire sortir l'ordinateur quantique des laboratoires. Il est censé gérer tout seul son calibrage.

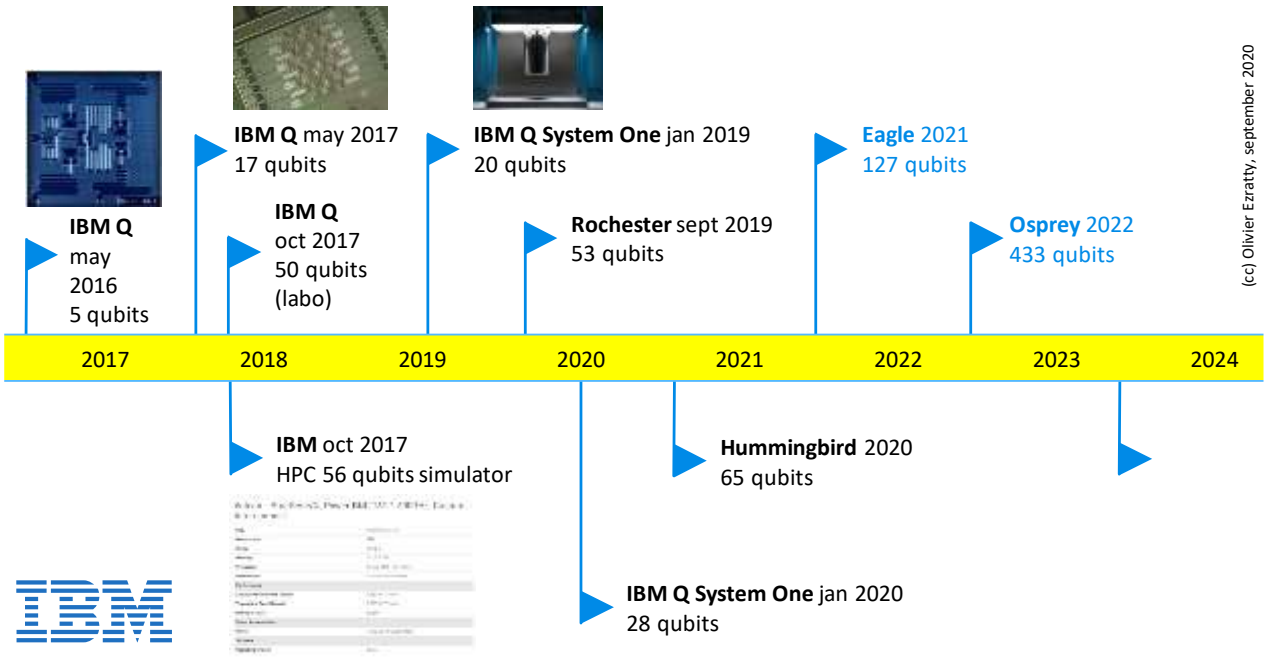
IBM lançait par la même occasion son premier IBM Q Quantum Computation Center pour ses clients à Poughkeepsie dans l'Etat de New York. A noter qu'IBM a aussi lancé en 2018 un centre de recherche quantique à Montpellier. C'était suivi d'un partenariat en Allemagne avec un institut Fraunhoffer en septembre 2019. Le tout est destiné à l'évangélisation des développeurs et des chercheurs pour les pousser à développer des logiciels avec leurs outils de développement et leurs ordinateurs quantiques dans le cloud.

Ils jouent la carte de la création d'une communauté avec l'IBM Q network lancé en 2017 et qui rassemble les grandes entreprises Fortune 500, laboratoires de recherche et startups intéressées par le développement de solutions quantique. Ce réseau propose l'accès à des ordinateurs quantiques de 5, 16 et 20 qubits dans le Cloud IBM, du support et de la formation.

IBM met en avant des chiffres mirifiques sur l'activité d'une communauté de 235 000 développeurs qui aurait exécuté le nombre impressionnant de 240 milliards de circuits, selon des données de juin 2020. Cela donne un million de circuits par personne.

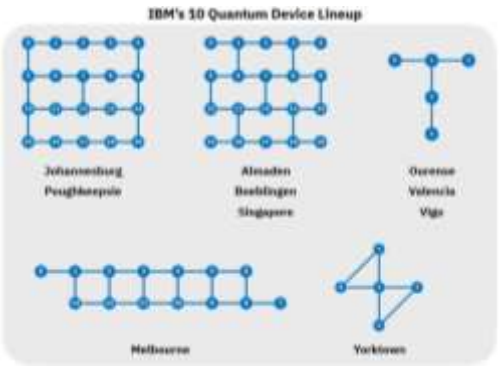
En moyenne, les programmes sont exécutés 4000 fois pour obtenir un résultat moyenné d'après les outils de configuration des batchs que j'ai pu tester. Ca fait donc 255 portes quantiques en tout qui ont été exécutées par utilisateur, soit quelques dizaines de cycles de portes quantiques.

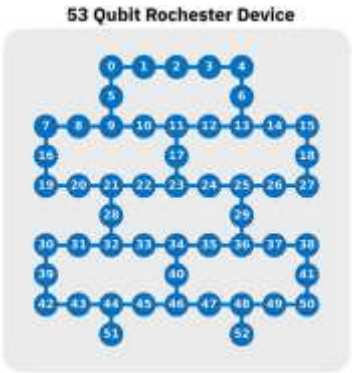
[620] Voir Rising above the noise: quantum-limited amplifiers empower the readout of IBM Quantum systems par Baleegh Abdo, janvier 2020.



Compte tenu des tâtonnements, cela veut dire un programme d'une dizaine de séries de portes quantique testé une demi-douzaine de fois. Bref, c'est un peu comme si tous les développeurs avaient testé un équivalent quantique d'un « Hello World », mais à la place, testé l'algorithme de Shor ou un équivalent. IBM se rattrape en citant le fait que plus de 235 publications scientifiques ont été faites qui citent l'usage de leurs calculateurs quantiques.

Les différents calculateurs quantiques d'IBM mis à disposition des développeurs dans le cloud n'ont pas du tout la même architecture de connectivité entre les qubits[621]. Cela impacte le type et la performance des algorithmes quantiques que l'on peut exécuter dessus.





En mai 2019, IBM indiquait qu'il faudrait tout de même attendre de trois à cinq ans pour qu'ils commercialisent des ordinateurs quantiques, indiquant indirectement que l'annonce du CES 2019 n'était pas une véritable annonce commerciale.

IBM semble attendre d'atteindre la suprématie quantique pour cette commercialisation, soit un peu plus que la cinquantaine de qubits de qualité et bien intriqués[622].

En septembre 2019, IBM annonçait la mise en service en octobre 2019 d'un processeur quantique de 53 qubits dans le cloud. C'était suivi de l'annonce d'une seconde mouture du Q System One au CES 2020 passant de 20 à 28 qubits. Il semble que ces 28 qubits soient de meilleure qualité que les 53 qubits d'octobre 2019.

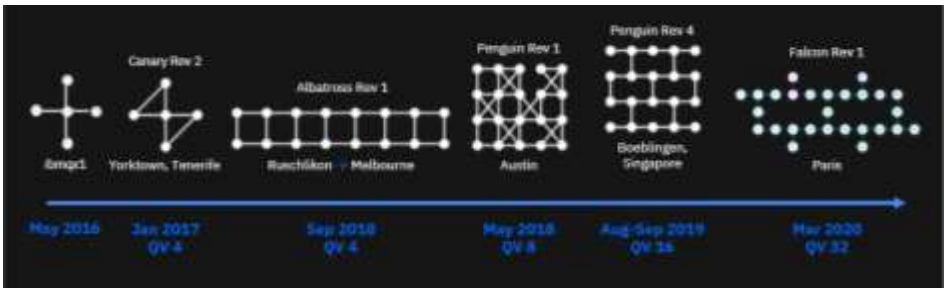
[621] Vu sur Quantum computation center opens par Doug McClure, 2019.

[622] Source : Norishige Morimoto, directeur d'IBM Research à Tokyo lors de l'IBM think Summit Taipei de mai 2019.

IBM communique depuis 2017 sur la notion de **volume quantique** pour évaluer la puissance de ses calculateurs quantiques. Cette notion a été reprise par **Honeywell** en mars 2020 puis par **IonQ** en octobre 2020. Son usage serait recommandé par le **Gartner Group**, qui aurait depuis 2019 au moins quatre analystes dédiés aux technologies quantiques.

Le volume quantique est un nombre entier censé associer la quantité de qubits et le nombre de portes quantiques qui peuvent être exécutées consécutivement sans que les erreurs qui s'accumulent soient préjudiciables à la précision des calculs. En effet, disposer de n qubits mais être limité par le nombre de portes quantiques que l'on peut enchaîner peut être préjudiciable à l'exécution de nombreux algorithmes quantiques. Certains sont gourmands en portes quantiques, d'autres non[623].

IBM indiquait ainsi les configurations de qubits leur ayant permis de passer d'un volume quantique de 4 avec 5 qubits en 2017 à 32 en mars 2020 puis à 64 en août 2020[624], avec 28 qubits.



C'est en apparence très simple. Mais dès que l'on cherche à comprendre d'où vient ce nombre magique, les choses se compliquent. Ce nombre agrège quatre facteurs clés de performance :

- Le **nombre de qubits physiques** du processeur.
- Le **nombre de portes quantiques** qui peuvent être enchaînées consécutivement sans que le taux d'erreur soit préjudiciable aux résultats.
- La **connectivité entre les qubits**, qui va impacter la longueur des algorithmes et potentiellement améliorer le volume quantique pour les qubits à forte connectivité comme avec les ions piégés.
- Le **nombre de portes quantiques** qui peuvent être réalisées en parallèle.

Ce volume quantique est évalué via un benchmark de calcul aléatoire consistant à enchaîner des portes quantiques aléatoires et qui doit donner un résultat correct dans deux tiers des cas. Pourquoi deux tiers ? Parce que le calcul quantique fournit un résultat probabiliste. Pour obtenir un résultat déterministe, on exécute le calcul plusieurs fois et on évalue la moyenne des résultats, jusqu'à des milliers de fois comme c'est proposé par IBM dans son système en cloud. Avec une moyenne de bons résultats aux deux tiers, on peut donc statistiquement converger vers un bon résultat au bout de quelques mesures. La précision du résultat va dépendre de ce nombre qui est habituellement de quelques milliers.

Dans la première définition de 2017 du volume quantique, il s'agissait du nombre maximum de qubits sur lequel le processeur pouvait effectuer ce calcul, élevé au carré[625]. La définition a évolué ensuite en 2019 pour devenir 2 à la puissance du nombre de qubits[626].

---

[623] Certains algorithmes peuvent ainsi se satisfaire d'un nombre limité de portes quantiques, comme celui de Deutsch-Josza qui sert à vérifier qu'une fonction est équilibrée ou pas (générant une fois sur deux 0 ou 1 ou tout le temps 0 ou 1), et se contente de seulement quatre séries de portes quantiques. A l'inverse, le fameux algorithme de factorisation de nombres entiers de Peter Shor requiert un nombre de séries de portes quantiques égal au cube du nombre de qubits utilisés.

[624] Voir IBM Delivers Its Highest Quantum Volume to Date, Expanding the Computational Power of its IBM Cloud-Accessible Quantum Computers, août 2020. Pour obtenir un volume de 64, IBM doit probablement aligner 8 qubits sur une profondeur de calcul de 8 séries de portes quantiques.

[625] Voir Quantum Volume de Lev Bishop, Sergey Bravyi, Andrew Cross, Jay Gambetta et John Smolin, 2017 (5 pages).

[626] Voir Validating quantum computers using randomized model circuits par Andrew W. Cross et al, 2019 (12 pages).

Le schéma **ci-contre** explique la manière dont les volumes quantiques de 2017 et 2019 sont évalués. Le schéma *ci-dessous* issu d'un document de Robin Blume-Kohout et Kevin Young [627] précise la manière dont le m (nombre de qubits) et le d (profondeur de calcul) sont évalués.

$$d \sim 1/(n\epsilon_{\text{eff}})$$

d = profondeur d'exécution maximale.
n = nombre de qubits
ϵ_{eff} = % d'erreur de portes quantiques à deux qubits

$$V_Q = dn = 1/\epsilon_{\text{eff}}$$

volume quantique de base = nombre de qubits * profondeur de calcul en portes quantiques.

$$V_Q = \min(n, d)^2$$

le volume devient min(n, profondeur)^2 pour éviter de truander la mesure avec un n=2 faible et un taux d'erreur faible.

$$V_Q = \max_{n' \leq n} \min\left[n', \frac{1}{n'\epsilon_{\text{eff}}(n')}\right]^2$$

formule de 2017 avec le scan de toutes les combinaisons de qubits n' inférieures au nombre de qubits disponibles, pour réaliser un algorithme aléatoire donné générant 2/3 de résultats corrects.

$$\log_2 V_Q = \underset{m}{\text{argmax}} \min(m, d(m))$$

formule de 2019, qui génère un résultat différent vs celle de 2017, avec un VQ qui est une puissance de 2 de la racine carrée de l'ancien volume quantique.

On y voit que le nombre de qubits obtenu pour évaluer le volume quantique est inférieur au nombre total de qubits du processeur, 8 pour 16 dans ce cas. Le benchmark ne permet d'enchaîner que 8 séries de portes quantiques d'affilée sur 8 qubits, pour 38 avec seulement deux qubits. Dans sa version 2017, le volume quantique est la surface du carré en gris contenant les carrés entourés de rouge.

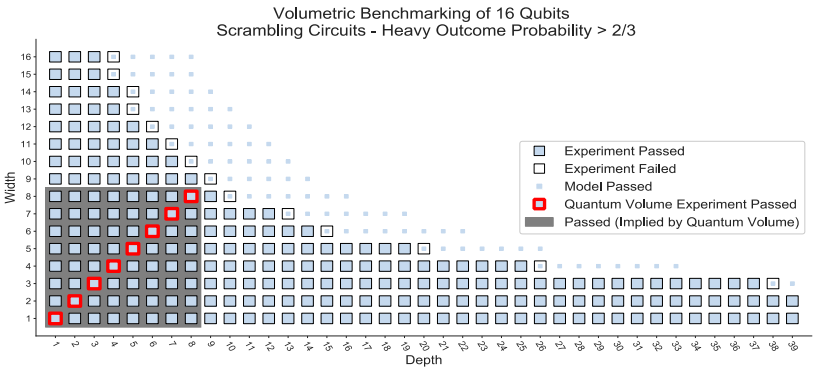
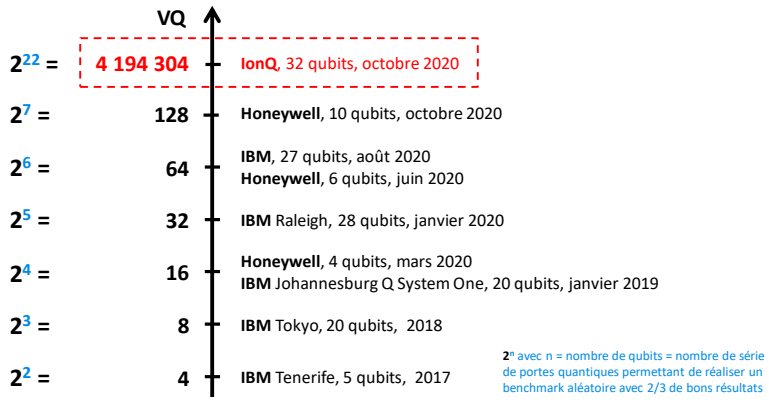


Figure 8(a). Volumetric benchmarking of a 16 qubit device using scrambling circuits. If at least 2/3 of the measurement results are heavy for a given width/depth pair, then the pair passes the test and is marked with a large, solid blue box. Using linear axes, the quantum volume experiments appear along the diagonal and are outlined with heavy, red lines. For this example, $\log_2(V_Q) = 8$. It is expected that scrambling circuits with both width and depth less than or equal to the quantum volume should succeed, and we highlight these with a gray background.

Dans sa version 2019, il devient 2^8, soit 256 au lieu de 64 (8x8). Ce n'est finalement que la taille de l'espace de Hilbert opérationnel du calculateur, soit le nombre d'état superposés différents qu'il est capable de gérer d'un point de vue pratique avec une profondeur de calcul égale au nombre des qubits correspondants.

Lorsqu'IBM annonce qu'un calculateur de 28 qubits atteint un volume quantique de 32, cela veut dire qu'ils n'arrivent à valider leur benchmark qu'avec 5 qubits parmi ces 28 qubits. Pour sa part, l'annonce d'IonQ d'un volume quantique supérieur à quatre millions correspond à 2^{22}, précisément 4 194 304.



Donc, à la capacité d'exécuter 22 séries de portes quantiques sur 22 des 32 qubits du processeur à ions piégés qu'ils ont annoncé en octobre 2020, avec deux tiers de résultats corrects sur le benchmark aléatoire utilisé. Ce record, pas encore bien documenté, semble lié à la bonne connectivité des qubits des ions piégés. Ceux-ci peuvent être ainsi tous intriqués directement les uns avec les autres contrairement aux qubits supraconducteurs qui sont, au mieux, intriquables qu'avec leur voisin immédiat.

[627] Dans A volumetric framework for quantum computer benchmarks, février 2019 (24 pages), Robin Blume-Kohout et Kevin Young proposent des benchmarks volumiques pour évaluer la performance des ordinateurs quantiques en s'appuyant sur le volume quantique d'IBM. Ce dernier propose aussi son propre code d'évaluation du volume quantique.

Cela permet de réaliser le benchmark en moins de séries de portes quantiques que sur des qubits supraconducteurs, qui requièrent beaucoup de portes SWAP générant des erreurs qui s'accumulent rapidement.

Le volume quantique est par ailleurs limité à une cinquantaine de qubits opérationnels. En effet, il ne peut être évalué qu'avec un benchmark comparant les qubits avec leur émulation sur un calculateur classique. Or, celle-ci est contrainte par la taille mémoire de ces derniers, qui atteint ses limites entre 50 et 55 qubits[628].

Les spécialistes du calcul quantique sont circonspects sur l'intérêt de cet indicateur qui est trop réducteur. Cet usage est ainsi contesté par le spécialiste des théories de la complexité et des algorithmes quantiques Scott Aaronson[629]. Il rappelait que le volume quantique qu'Honeywell pensait atteindre (et a atteint) à la mi-2020 était facilement émulable dans un ordinateur classique, même dans un laptop. Ce qui n'en fait pas quelque chose de particulièrement puissant. Et tandis que le volume quantique des ordinateurs quantiques s'agrandira, bien malin sera celui qui pourra indiquer à partir de cette valeur si un ordinateur quantique est capable de résoudre son problème[630] !

Scott Aaronson pense donc qu'il faut éviter cette mesure du quantum volume qui est un outil de simplification marketing d'IBM. La solution ? Elle consiste à décrire précisément les caractéristiques de la machine avec son nombre de qubits, leur connectivité, leur temps de cohérence (T1, T2), le taux d'erreur des portes quantiques à un et deux qubits, la profondeur de calcul qui en résulte et les besoins en ressources pour émuler l'ensemble sur un ordinateur classique. On trouve généralement ces indicateurs dans les publications scientifiques de chercheurs mais pas toujours dans la littérature marketing des constructeurs. Les commentaires de l'article de Scott Aaronson sont partagés et certains de ses lecteurs apprécient cependant cet indicateur simple à retenir. D'autres pensent que ce qui compte est l'avantage quantique, que l'on obtient lorsqu'un processeur quantique est capable de réaliser une opération utile qui prendrait beaucoup plus de temps sur un supercalculateur classique, avantage qui n'est pas encore atteint à ce jour.

Quittons cette histoire de volume quantique pour revenir à la roadmap d'IBM. Le 15 septembre 2020, ils annonçaient les détails de leur plan pour continuer à augmenter le nombre de qubits de leurs calculateurs quantiques[631].

On y apprenait qu'ils avaient déjà atteint un record de 65 qubits (« Hummingbird »), dépassant le record précédent de 53 qubits annoncé en septembre 2019. Ils prévoient d'atteindre 127 qubits en 2021 (« Eagle »), 433 qubits en 2022 (« Osprey ») et 1221 qubits en 2023 (« Condor »).

---

[628] Voir Why Is IBM's Notion of Quantum Volume Only Valid up to About 50 Qubits? par Jack Krupansky, octobre 2020.

[629] Dans Turn down the quantum volume, Scott Aaronson, publié juste après l'annonce d'Honeywell de février 2020.

[630] Imaginez un indicateur de la puissance de votre laptop agrégeant la fréquence d'horloge du processeur, son nombre de cœurs, la puissance de son CPU, la mémoire RAM, la capacité de stockage, son type (disque dur, SSD) etc ? Et là, de vous demander si vous allez pouvoir utiliser efficacement votre logiciel de montage vidéo, de dérushage de photos ou de jeu vidéo sur casque de réalité augmentée !

[631] Voir IBM's Roadmap For Scaling Quantum Technology par Jay Gambetta, septembre 2020, complété par IBM publishes its quantum roadmap, says it will have a 1,000-qubit machine in 2023 par Frederic Lardinois dans TechCrunch, même date.

Au programme : du multiplexage de signaux pour la lecture d'états des qubits, une connectique de circuit de type TSV (through-silicon via) pour simplifier le câblage, et enfin, ça c'est la création d'un cryostat maison baptisé « Goldeneye » dépassant les capacités actuelles du marché pour atteindre un million de qubits, sans faite l'acquisition d'une société spécialisée comme Leiden. La photo du laboratoire d'IBM *ci-dessus* illustre la taille de l'engin qui fait 3m de haut pour 2m de large.

En la décodant, on peut inférer des plaques circulaires trouées visibles dans les photos qu'ils s'apprêtent à utiliser une vingtaine de têtes pulsées, ce qui serait inédit. Le tout consommerait 320 kW. Ces plaques comprennent peu de trous pour laisser passer des câbles ce qui sous-entend un fort multiplexage des signaux de commande des qubits. IBM annonçait qu'il envisageait de se fournir en technologies à l'extérieur plutôt que de vouloir tout créer en interne.

Reste à savoir avec qui ils travaillent (Leiden pour la cryogénie ? SeeQC pour les composants de contrôle des qubits ? Autres ?). Affaire à suivre !

Google

Google a au moins quatre fers au feu pour ce qui est du calcul quantique.

- Il a commencé par **tester des algorithmes d'optimisation** sur des ordinateurs à recuit quantique de D-Wave dans le laboratoire QUAIL conjoint avec la NASA situé au Ames Research Center de Mountain View. Nous en avons déjà parlé dans la rubrique précédente dédiée à D-Wave.
- Il développe ses propres **processeurs quantiques** à base de qubits supraconducteurs à effet Josephson, sous la direction de John Martinis qui pilotait entre 2014 et 2020 l'activité hardware quantique de Google. Le tout en liaison avec l'Université de Santa Barbara en Californie d'où il venait avec une partie de son équipe chez Google[632].
- Il propose une **plateforme logicielle** de développement quantique autour du framework Cirq ainsi que, récemment, de TensorFlow Quantum pour les applications de « quantum machine learning ». Nous avions vu cela dans la rubrique sur les plateformes logicielles des grands acteurs du marché.
- Il offre d'abord des capacités de **simulation** d'algorithmes quantiques sur ses serveurs traditionnels dans le cloud.

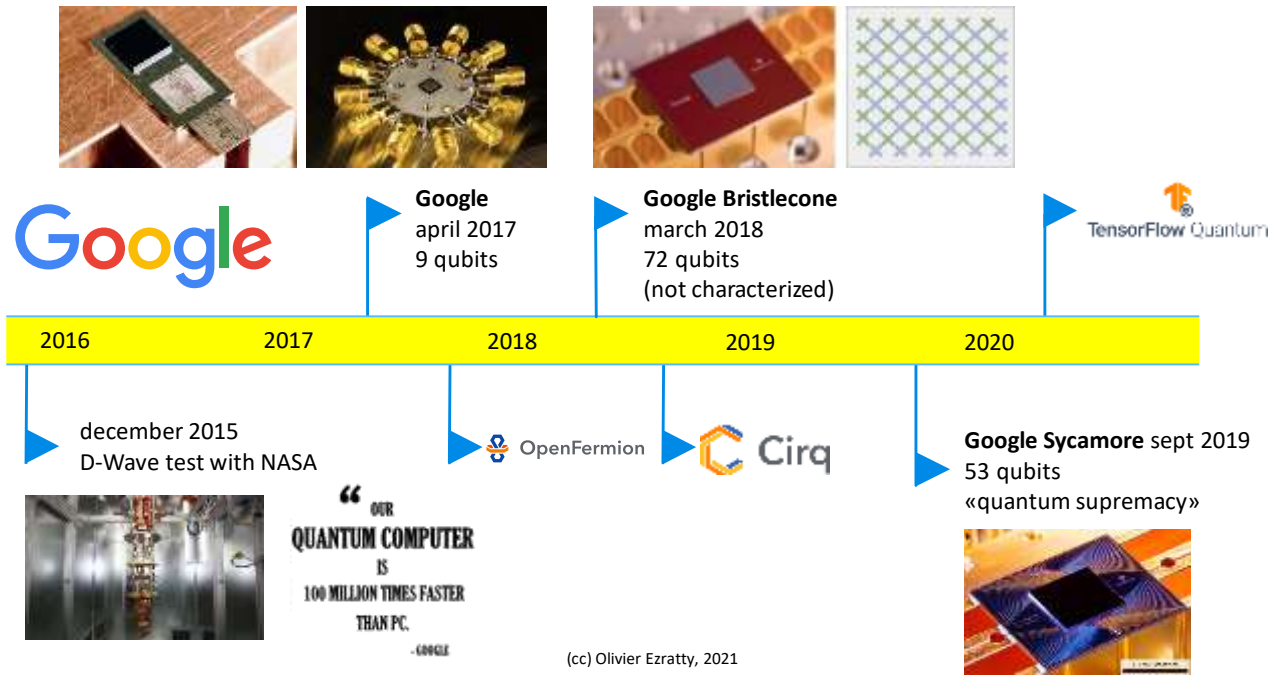
Dans cette rubrique, nous allons nous focaliser sur le second point. Google est sans doute avec IBM l'acteur le plus visible du marché avec ses prouesses à répétition, dont celle qui fut abondamment commentée et parfois critiquée de l'atteinte de la suprématie quantique en octobre 2019. Comme IBM, Google cherche à augmenter le nombre et la qualité des qubits de ses processeurs quantiques.

Le géant de Mountain View n'est pas un fournisseur de supercalculateurs. Il prévoit sans doute d'utiliser ses ordinateurs quantiques pour ses propres besoins destinés aux usages grand public et pour ses offres de cloud computing destinées aux entreprises.

---

[632] Voir Google's Head of Quantum Computing Hardware Resigns par Tom Simonite, avril 2020. Il a démissionné de Google en avril après avoir été rétrogradé à un rôle de conseil scientifique. Reste à savoir si ce changement de position était lié à des questions de management, de désaccords stratégiques ou par le fait que l'activité de Martinis était un peu décalée par rapport aux autres branches de Google dédiées au quantique, notamment les branches logicielles et cloud. Aucun ordinateur quantique de John Martinis n'était ainsi sorti des laboratoires pour être mis en ligne dans le cloud comme peut le faire IBM depuis 2016.

Cela pourra aussi servir plus largement aux autres filiales du groupe Alphabet et en particulier celle qui travaille dans la santé, Verily, qui sera très intéressée par les capacités de simulation moléculaires du quantique, pour inventer de nouveaux traitements.



Dès 2017, Google affichait son ambition d'atteindre la « suprématie quantique » définie par John Preskill[633]. En avril cette année-là, ils évoquaient un premier processeur de 9 qubits. En juin 2017, ils annonçaient vouloir atteindre 49 qubits stables.

Début 2018 était testé un chipset de 22 qubits de nom de code Foxtail. Mais assez discrètement. Et pour cause, puisqu'en mars 2018, c'était le tour d'une annonce d'un record de 72 qubits avec la génération Bristlecone, promettant un taux d'erreurs inférieur à 0,5% dans les paires de qubits couplées entre elles. Ce record n'a pas donné lieu à une publication scientifique vérifiable. Et pour cause, il semblerait que ce processeur n'ait pas pu être caractérisé (testé, benchmarké) avec succès.

En 2019, **Hartmut Neven**, le Directeur de Google en charge du calcul quantique, mettait en avant une loi empirique dite Dowling-Neven selon laquelle la puissance des ordinateurs doublait selon une double exponentielle.

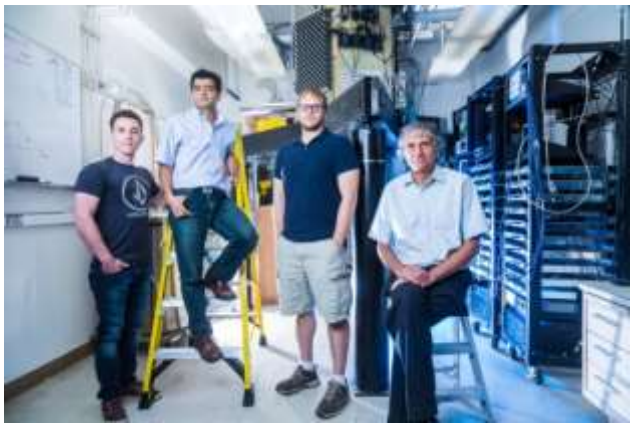
C'est franchement exagéré lorsque l'on examine leur méthode d'évaluation[634]!

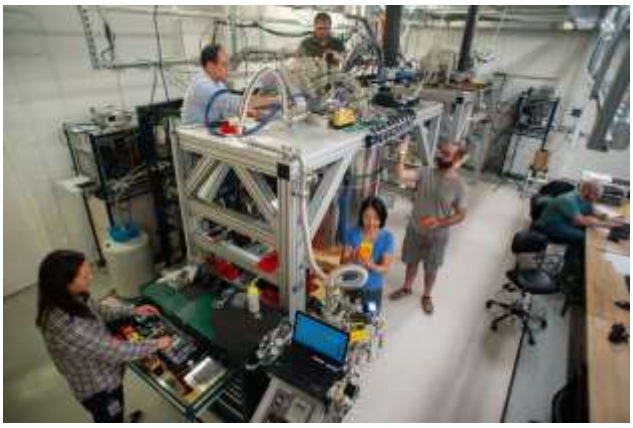
---

[633] Voir Google says it is on track to definitively prove it has a quantum computer in a few months' time par Tom Simonite, avril 2017. Voir aussi The Question of Quantum Supremacy, paru en mai 2018 et qui référence deux papiers sur la suprématie quantique recherchée par Google : Characterizing Quantum Supremacy in Near-Term Devices, 2016 (23 pages) et A blueprint for demonstrating quantum supremacy with superconducting qubits, 2017 (22 pages).

[634] Le raisonnement est le suivant : le nombre de qubits augmenterait jusqu'à présent de manière exponentielle, et la puissance double à chaque ajout d'un seul qubit. Le tout tous les six mois. Malheureusement, les données disponibles sur la puissance réelle des ordinateurs quantiques actuels ne sont pas conformes à cette loi. Il n'y a pas de doublement du nombre de qubits opérationnels tous les six mois ! Il y a même régression ! Google annonçait ainsi 72 qubits en mars 2018 et puis 53 qubits en octobre 2019. Chez IBM, on est dans l'embrouille totale entre le Q System One qui passait de 20 à 28 qubits entre janvier 2019 et janvier 2020, ce qui ne ressemble pas à un doublement tous les six mois. Par contre, on pourra éventuellement obtenir ce doublement sur d'autres technologies comme avec les ions piégés d'Honeywell ou les atomes froids de Pasqal. Dans sa présentation à la Q2B de décembre 2019, John Preskill mettait en avant une autre double exponentielle : les taux de fidélité des portes s'améliorent régulièrement, ce qui augmenterait le volume quantique de manière exponentielle. Dans le même temps, le coût de l'émulation du calcul quantique sur ordinateurs classique augmente de manière exponentielle avec le volume quantique. D'où une évolution doublement exponentielle de la puissance de calcul. Le bug ? Rien ne dit que la fidélité des portes quantiques va continuer de s'améliorer régulièrement. Voir A New Law to Describe Quantum Computing's Rise?, juin 2019.

Enfin, entre septembre et octobre 2019, Google annonçait avoir atteint « sa » suprématie quantique avec un chipset maison de 53 qubits dénommé Sycamore et avec un algorithme voisin de celui de l'échantillonnage du boson imaginé par Scott Aaronson en 2012[635]. Les documents scientifiques de la NASA et Google avaient été diffusés par erreur sur Internet, puis publiée officiellement dans la revue Nature en octobre 2019[636]. Ils font 70 pages en tout et avec un niveau de détail inédit[637]. Google y comparait leurs qubits avec le supercalculateur le plus puissant de l'époque, l'IBM Summit, installé à l'Oak Ridge National Laboratory du Département de l'Energie, dans le Tennessee[638]. Le calcul durant 200 secondes sur Sycamore prendrait 10 000 ans une fois émulé sur l'IBM Summit.





L'algorithme utilisé associe un générateur quantique de nombres aléatoires et un système qui permet de vérifier que les nombres générés sont bien aléatoires, avec donc une répartition homogène. Cette dernière partie scanne toutes les valeurs possibles (2^{53}) de superposition des qubits[639].

Le domaine d'application de cet algorithme serait de permettre de générer des nombres aléatoires certifiés. Sachant que cela existe déjà pour moins cher avec les générateurs de nombres aléatoires quantiques, comme ceux du Suisse IDQ. Cet usage de l'échantillonnage du boson (« boson sampling »)[640] est une approche qui ne fait pas l'unanimité pour établir une supériorité du calcul quantique par rapport au calcul classique[641].

---

[635] Voir Quantum Supremacy Using a Programmable Superconducting Processor par John Martinis, octobre 2019.

[636] Voir Hello quantum world! Google publishes landmark quantum supremacy claim par Elizabeth Gibney, octobre 2019.

[637] Voir Quantum supremacy using a programmable superconducting processor par Frank Arute, John Martinis et al, octobre 2019 (12 pages) et Supplementary information for "Quantum supremacy using a programmable superconducting processor" par Frank Arute, John Martinis et al, octobre 2019 (58 pages). Voir aussi Quantum supremacy using a programmable superconducting processor, une conférence de John Martinis à Caltech, novembre 2019 (une heure). Et une autre version, jouée à la conférence Q2B de QC Ware en décembre 2019 (19 slides et vidéo de 32 minutes). Enfin, voici cette vidéo de promotion de Google sur la suprématie : Demonstrating Quantum Supremacy, octobre 2019 (4'42").

[638] Voir Google researchers have reportedly achieved "quantum supremacy" par Martin Giles, dans la MIT Technology Review, septembre 2019 et la source du papier sur Internet, avec les illustrations. Ils utilisent un type d'algorithme qui ne sert pas à grand-chose mais qui favorise nettement le calcul quantique et requiert un nombre limité de portes quantiques, ce qui va bien aux processeurs quantiques générateurs de bruit. L'algorithme utilise en effet la superposition de tous les (53) qubits utilisés ce qui n'est pas le cas de tous les algorithmes. Voir aussi Why I Coined the Term 'Quantum Supremacy' par John Preskill, octobre 2019.

[639] On peut en trouver l'explication suivante dans Quantum Supremacy Is Coming: Here's What You Should Know de Kevin Harnett dans QuantaMagazine, juillet 2019.

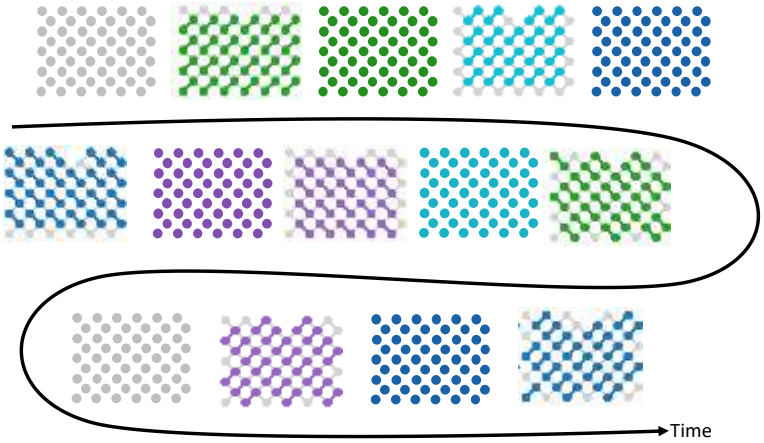
[640] Voir Lecture 3: Boson sampling par Fabio Sciarrino (63 slides) et An introduction to boson-sampling, Bryan Gard, Jonathan P. Dowling et al, 2014 (13 pages).

[641] Voir notamment la critique Quantum computers: amazing progress (Google & IBM), and extraordinary but probably false supremacy claims (Google) par Gil Kalai, septembre 2019 aini que The Quest for Quantum Computational Supremacy par Scott Aaronson, septembre 2019, qui est antérieur de trois semaines par rapport à l'annonce Google Sycamore mais reste valable (16 pages).

Cet algorithme présente plusieurs caractéristiques qui expliquent son choix :

- Il utilise la **superposition sur l'ensemble des qubits utilisés** (53), ce qui permet d'obtenir une performance maximale au niveau exponentialité de la puissance de calcul. Dans une bonne part des algorithmes quantiques, tous les qubits ne sont pas utilisables pour de la superposition.

  On doit mettre de côté des qubits qui servent de valeurs auxiliaires (ancilae) ou tampon. Résultat, l'avantage exponentiel diminue d'autant. Un tel algorithme ne pourrait donc pas bénéficier de la superposition de 2^{53} états mais par exemple tomber à 2^{30} états, où l'avantage quantique serait moins fort. Le processus alterne l'exécution de portes à un et deux qubits.



- Il utilise une **profondeur de 20 portes quantiques**. A savoir que l'algorithme testé à pleine charge n'enchaîne qu'une suite de 20 blocs de portes quantiques exécutées simultanément sur les qubits qui sont physiquement statiques dans leur circuit.

  C'est lié au bruit généré dans les qubits qui limite cette profondeur. De nombreux algorithmes nécessitent un plus grand nombre de portes quantiques, notamment celui de la factorisation de nombres entiers de Shor. Malgré tout, on peut exécuter un grand nombre d'algorithmes utiles avec cette profondeur de portes. Cela ouvre des portes sur des usages pratiques comme dans la simulation chimique.

- L'algorithme a l'air d'être de ce point de vue-là **voisin de celui de Deutsch-Jozsa** qui sert à tester si une fonction est équilibrée ou pas (est-ce qu'elle envoie toujours 0 ou 1 ou des 0 et des 1 à parts égales, sachant que c'est l'hypothèse de départ de la fonction). Ce dernier permet de passer d'un temps de classique exponentiel à un temps de calcul fixe. En langage de la complexité, on écrit cela $O(2^{N-1})$->$O(1)$. L'avantage est que le nombre de portes est fixe et limité, ce qui permet d'éviter le bruit généré par la séquence de portes.

- L'algorithme n'a **pas besoin d'exploiter des codes de corrections d'erreurs** qui consomment de nombreuses portes quantiques ainsi qu'un nombre de qubits plus grand de plusieurs ordres de grandeur (x100 à x10000). Et pour cause, il ne réalise pas un véritable calcul[642] ! Il ne fait donc pas avancer l'état de l'art pour aller dans la direction du FTQC (Fault Tolerant Quantum Computer).

Voici les données clés du benchmark :

Google Sycamore			
Nombre de qubits	53	qubits	qubits dans le processeur quantique
Couplers	84	couplers	associent les qubits par paires
Single qubits gates	1113	gates	portes unitaires de l'algorithme
Two qubits gates	430	gates	portes à deux qubits de l'algorithme
Gates depth	20	cycles	nombre de séries de portes quantiques exécutées
Nombre d'itérations	3000000	itérations	nombre de fois où le calcul est réalisé
Temps de calcul	600	secondes	temps de calcul total
Temps de calcul quantique	30	secondes	temps de calcul total dans le processeur quantique
Portes par cycle	55,65	gates / cycle	nombre de portes quantiques exécutées par série de portes

[642] Voir cependant The Google Quantum Supremacy Demo and the Jerusalem HQCA debate par Gil Kalai, décembre 2019, où il remet en cause les résultats de la suprématie quantique de Google, notamment au niveau de l'évaluation du bruit des qubits.

Le 21 octobre 2019, des chercheurs d'IBM publiaient un article où ils remettaient en cause la performance de Google en indiquant pouvoir exécuter leur algorithme en 2,5 jours au lieu de 10000 ans sur le supercalculateur IBM Summit[643].

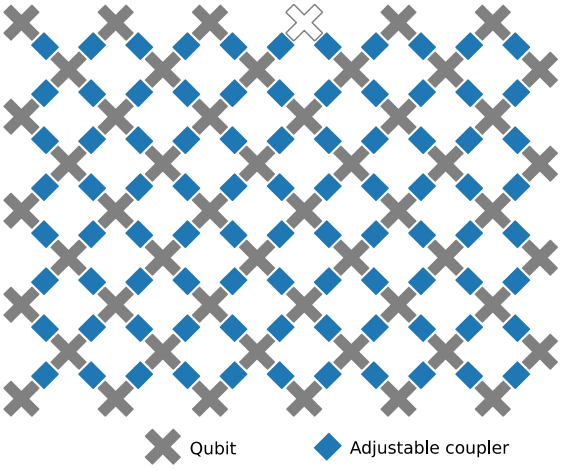
Mais en ajoutant 64 Po de SSD au système, ce qu'ils n'ont pas testé, mais juste évalué en termes de puissance d'émulation nécessaire. Cela représente environ 7 racks de SSD aux capacités de 2019. IBM souhaitait contredire ainsi l'affirmation de la suprématie quantique de Google, celle-ci devenant un plus banal avantage quantique[644].

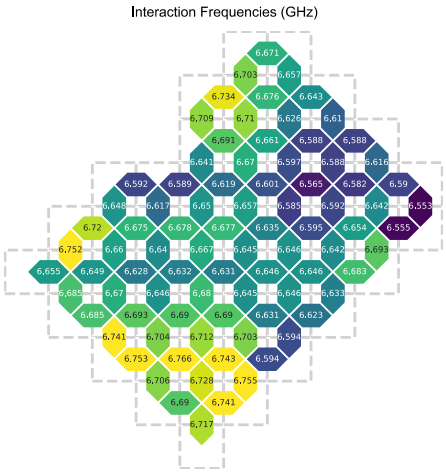
En décembre 2019, John Preskill faisait en tout cas remarquer que les réactions à l'annonce de Google étaient plus crédibles que d'autres dans les Tweets *ci-contre* [645]!

En effet, Google n'a pas réellement bénéficié du plan quantique de l'administration Trump lancé fin 2018 pour atteindre sa suprématie quantique.

La « collaboration » avec Google mise en avant par la fille du Président semble être une récupération politique sans aucun fondement.

Un calculateur quantique comme celui de Google présente un avantage côté consommation d'énergie dans le cas utilisé, avec un rapport d'environ un à million. Le raisonnement est le suivant : l'ordinateur quantique consomme aux alentours de 25 kW et l'IBM Summit, 12 MW à pleine charge, et le ratio de temps de calcul est de 2,5 mn vs 2,5 jours (1/1440) dans le cas le plus favorable au Summit. Cela fait une différence non négligeable ! Mais on compare probablement des choux et des carottes.





[643] Voir On "Quantum Supremacy" | IBM Research Blog par Edwin Pednault, octobre 2019 et Leveraging Secondary Storage to Simulate Deep 54-qubit Sycamore Circuits, par Edwin Pednaul et al, octobre 2019 (30 pages).

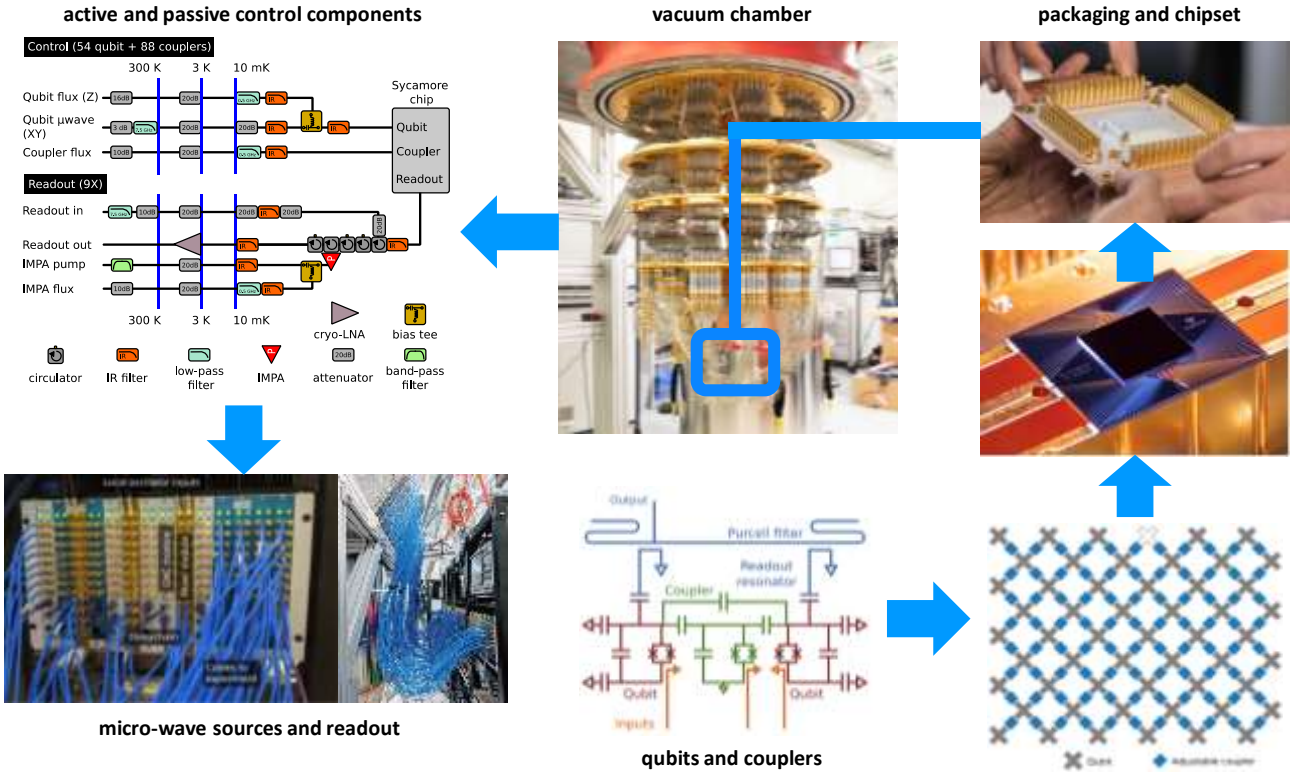
[644] Les arguties sur la suprématie quantique de Google sont allées bon train, notamment en intégrant la réponse courroucée et un peu de mauvaise foi d'IBM. Et puis Has Google Finally Achieved Quantum Supremacy?, octobre 2019 qui est assez bien documenté. Puis Quantum supremacy: the gloves are off par Scott Aaronson, octobre 2019 où il évoque le fait que cette affaire est l'équivalent de Kasparov contre Deep Blue, IBM jouant le rôle de Kasparov. Sans compter le débat sur la terminologie de la suprématie qui a une fois encore faire jaser, comme relaté dans Academics derided for claiming 'quantum supremacy' is a racist and colonialist term par Sarah Knapton, décembre 2019.

[645] Dans la conférence Q2B de QcWare à San José, décembre 2019.

Dans le détail, le système de Google n'impressionnait pas forcément les spécialistes des qubits supraconducteurs. Leur particularité est d'utiliser des coupleurs de qubits contrôlables. Il y en a 88 en tout qui relient entre eux les 53 qubits du chipset. Cela fait un total de 141 qubits.

Ces coupleurs sont en fait des qubits dont on contrôle la fréquence. Ils permettent de créer des portes quantiques à deux qubits rapides, agissant en 10 à 15 ns. Ces portes sont d'ailleurs plus rapides que les portes quantiques qui n'agissent que sur un seul qubit à la fois. Ces qubits et coupleurs sont contrôlés avec des micro-ondes véhiculées dans des câbles coaxiaux, à des fréquences comprises entre 5 et 7 GHz. Ils ont développé un code de calibrage des qubits à base de deep learning, ce qui a permis de définir les fréquences des micro-ondes d'activation des qubits pour éviter qu'elles se chevauchent entre qubits voisins.

Voici un zoom avant de l'électronique embarquée dans le calculateur, qui suis les grands classiques des systèmes à qubits supraconducteurs.



Le système exploite 54 générateurs de signaux micro-ondes externes pour les portes à un qubit (X et Y), 54 pour le réglage de fréquence des qubits et 88 pour le contrôle des qubits. Le tout est complété par 9 signaux micro-ondes de contrôle. L'ensemble de l'électronique de contrôle comprend 277 convertisseurs numériques-analogiques qui occupe 14 boitiers 6U en rack. Cela fait autant câbles coaxiaux qui aboutissent dans le cryostat.

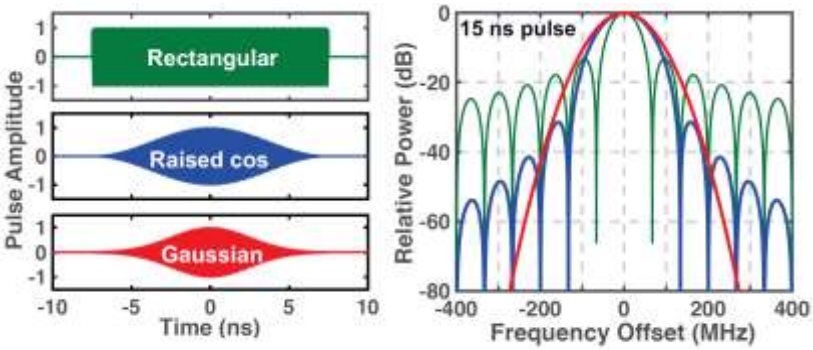
Pour la lecture de l'état des qubits, seuls quelques photons micro-ondes sont envoyés dans les qubits. Le résultat est amplifié de 100 db en plusieurs étapes, dont une au niveau de l'étage du processeur à 15 mK et une autre au niveau de l'étage 3K. Le processeur est entouré d'un blindage en Mu-metal, un autre en aluminium et d'un revêtement noir pour absorber les photons infrarouges. Le processeur est réalisé avec de l'aluminium et de l'indium et comprend deux chipsets superposés.

Quelles sont les étapes suivantes ? D'après Google, continuer à réduire le taux d'erreur des qubits et scaler jusqu'à une centaine de qubits.

Et enfin, générer de nouvelles prouesses, cette fois-ci avec des algorithmes vraiment utiles[646]. Google publiait ainsi coup sur coup deux papiers en avril 2020, l'un portant sur la résolution de problèmes de combinatoire et l'autre sur de la simulation chimique d'une molécule de quatre atomes. Cette fois-ci, sans évoquer la notion de suprématie[647] !

Ils travaillent aussi sur la création de chipsets CMOS de génération de micro-ondes de contrôle des qubits et fonctionnant à 3K[648]. Ces chipsets utilisent des générateurs de forme d'onde très simples permettant de consommer un minimum d'énergie.

Google utilise des micro-ondes de forme cosinusoidale présentant l'intérêt de créer des « trous » spectraux correspondant aux harmoniques des fréquences de passage des qubits de l'état |1⟩ à l'état |2⟩ et que l'on souhaite éviter correspondant à la longueur d'onde dite ω_{12} vue dans un schéma des pages précédentes.



Raised cosine: good compromise between sidelobes and pulse duration

On apprenait en tout cas le départ de John Martinis de Google en avril 2020[649]. Celui-ci pilotait l'équipe de recherche hardware de Google et était basé à Santa Barbara, dans l'Université UCSB d'où il venait. Il avait créé ce lab de Google en 2014.

Mais le projet quantique de Google était piloté depuis 2006 par son boss, **Hartmut Neven**, qui pilote à la fois la partie matérielle et la partie logicielle. John Martinis avait été rétrogradé au rang de conseiller scientifique au milieu de 2019. Bref, il devait y avoir de l'eau dans le gaz quantique.

John Martinis s'en est rapidement expliqué dans une interview. On y découvre le rôle du câblage dans le cryostat, un membre de l'équipe hardware voulant suivre une piste qu'il trouvait non productive mais qui était tout de même approuvée par Harmut Neven[650].

Plusieurs équipes de Google travaillent sur les briques logicielles quantiques. Il y a celles de Cirq, celles de TensorFlow Quantum et une autre équipe de Google X qui travaille visiblement sur des applications, sous la houlette de Jack Hidary[651].

---

[646] Voir ce papier, théorique, portant sur l'usage du calcul quantique, pas forcément avec les qubits de Google, pour étudier les trous noirs. Voir Google Scientists Are Using Quantum Computers to Study Wormholes par Ryan F. Mandelbaum, novembre 2019 qui fait référence à Quantum Gravity in the Lab: Teleportation by Size and Traversable Wormholes Adam R. Brown et al, novembre 2019 (20 pages).

[647] Voir Quantum Approximate Optimization of Non-Planar Graph Problems on a Planar Superconducting Processor par Google AI Quantum and Collaborators, avril 2020 (17 pages) qui porte sur trois familles de problèmes de combinatoire avec l'algorithme QAOA et Hartree-Fock on a superconducting qubit quantum computer par Google AI Quantum and Collaborators, avril 2020 (27 pages) avec un algorithme de simulation moléculaire du diimide ($(NH)^2$).

[648] Voir Control of transmon qubits using a cryogenic CMOS integrated circuit par Joseph Bardin, mars 2020 (35 minutes) et A 28nm Bulk-CMOS 4-to-8GHz <2mW Cryogenic Pulse Modulator for Scalable Quantum Computing, février 2019 (13 pages).

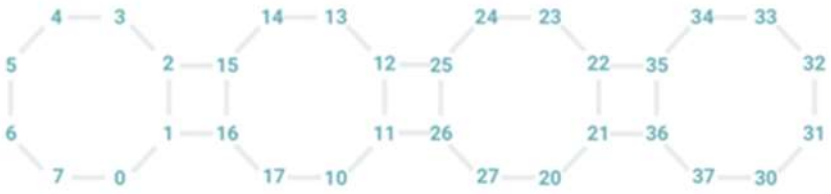
[649] Voir Google's Head of Quantum Computing Hardware Leaves, avril 2020.

[650] John Martinis s'explique en détails sur les raisons de son départ de Google dans une interview pour Forbes : Google's Top Quantum Scientist Explains In Detail Why He Resigned par Paul Smith-Goodson, 2020.

[651] Voir Alphabet Has a Second, Secretive Quantum Computing Team par Tom Simonite, janvier 2020.

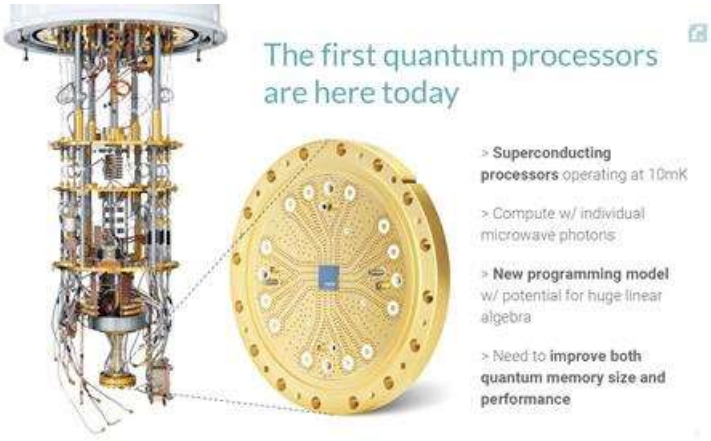
Rigetti (2013, USA, $190,5M) est le troisième larron du supraconducteur universel “commercial”. Avec D-Wave et PsiQuantum, c’est la troisième startup la mieux financée du secteur, ayant levé en tout $119M. La startup a été lancée par Chad Rigetti qui avait obtenu une thèse de doctorat à l’Université de Yale sur les qubits supraconducteurs en 2009[652].

Ils en sont actuellement à 32 qubits avec leurs chipsets Aspen-7 en déploiement chez Amazon Braket avec une connectivité assez réduite, schéma de connectivité *ci-contre*.



Ils avaient aussi une version de test à 128 qubits annoncée début août 2018 mais jamais utilisée. L’architecture de 128 qubits s’appuyait sur la démultiplication en 2D d’un modèle à base de 16 qubits.

Leurs taux d’erreur et temps de cohérence sont moins bons que ceux d’IBM et de Google, ce qui n’est pas de bon augure. Comme IBM et D-Wave, ils ont une approche d’intégration verticale. Cela va jusqu’à leur propre petite unité de fabrication pour leurs chipsets maison. Ils peuvent se le permettre car l’équipement revient à environ $10M, ce qui est raisonnable.



Ce coût modéré vient de ce que la création de circuits de qubits supraconducteurs se fait avec un niveau d’intégration très faible. Dans le cas de qubits silicium, il faut par contre disposer d’un équipement d’au moins $1B [653]!

Leurs qubits sont intriqués par des coupleurs paramétrables dynamiquement qui apporteraient plus de souplesse dans la gestion de l’intrication des qubits entre eux[654]. Ce sont des qubits transmons réglables exploitant des SQUID (magnétomètres) asymétriques. Cela fait penser à la technique utilisée par Google dans Sycamore.

Les autres particularités de Rigetti sont d’avoir fait des efforts dans l’optimisation de la partie physique et électrique du calculateur. Tout d’abord, en intégrant le câblage de contrôle et de mesure des qubits dans des nappes compactes. Elles ont fait l’objet d’un brevet[655]. Ils ont aussi développé leur propre électronique de génération de micro-ondes.

---

[652] Voir Quantum Gates for Superconducting Qubits, 2009 (248 pages).

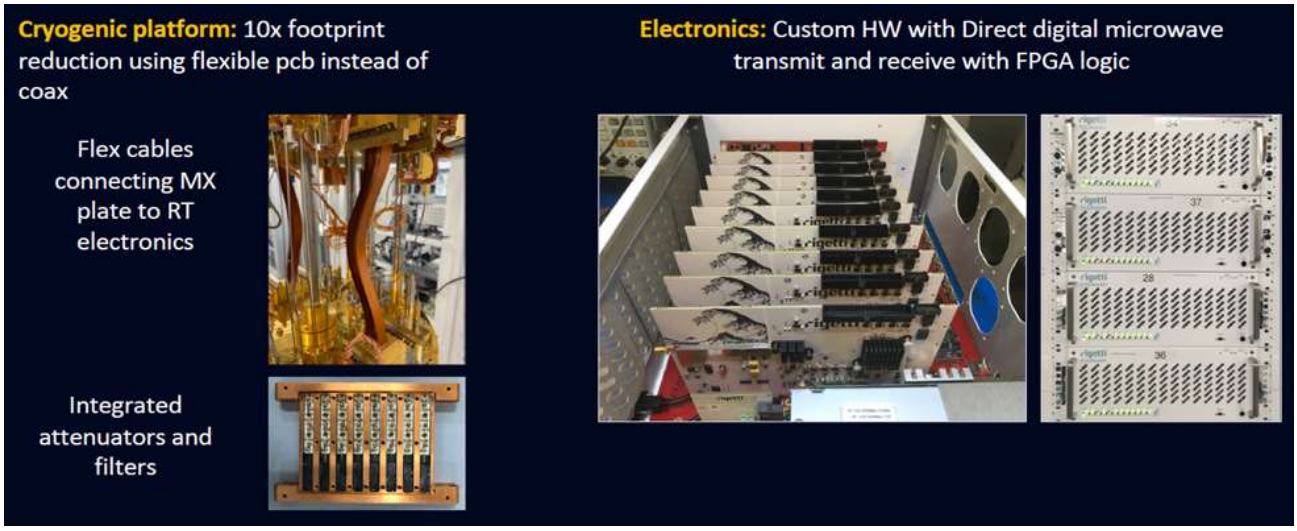
[653] Voir Quantum Cloud Computing Rigetti de Johannes Otterbach, 2018 (105 slides) et la vidéo correspondante. C’est la source de la double illustration avec la salle « jaune » de production et le chipset.

[654] C’est expliqué dans Demonstration of Universal Parametric Entangling Gates on a Multi-Qubit Lattice par M. Reagor et al, 2018 (17 pages).

[655] Voir Connecting Electrical Circuitry in a Quantum Computing System, USPTO 20190027800.

Ils ont aussi trouvé un moyen de limiter le crosstalk (interférence) entre les qubits[656]. Le temps de temps de cohérence des qubits est de 200 µs, ce qui est un best-in-class.

Les outils de développement proposés par Rigetti comprennent pyQuil pour le scripting et Quil pour la gestion des portes quantiques.



Ils sont tous deux open source et publiés sur Github. Quil permet de synchroniser des tâches sur la partie quantique et la partie traditionnelle de l'ordinateur (documentation), ce qui en soi, n'a rien d'extraordinaire par rapport à l'approche des autres acteurs de ce marché. Ils démontraient aussi en 2018 un usage de leur ordinateur quantique pour un algorithme de machine learning qui ne nécessite pas de passer par un algorithme hybride[657].

Rigetti avait acquis la startup QxBranch en juillet 2019 pour compléter son offre logicielle. Cette dernière était établie aux USA, au Royaume-Uni et surtout en Australie. En septembre 2020, leur filiale basée au Royaume-Uni annonçait le lancement d'un projet collaboratif d'accélération de commercialisation d'ordinateurs quantique, financé à hauteur de £10M privés/publics. Ils vont pour ce faire utiliser un cryostat de dernière génération Proteox d'Oxford Instruments. Voilà comment amadouer un pays et récupérer des financements publics !

Côté "Go to market", Rigetti propose l'accès à ses ordinateurs quantiques via le cloud, un peu comme le font IBM et D-Wave, avec leurs Quantum Cloud Services, en bêta depuis janvier 2019. Depuis début 2020, ils sont également distribués dans le cloud dans le service Amazon Braket.

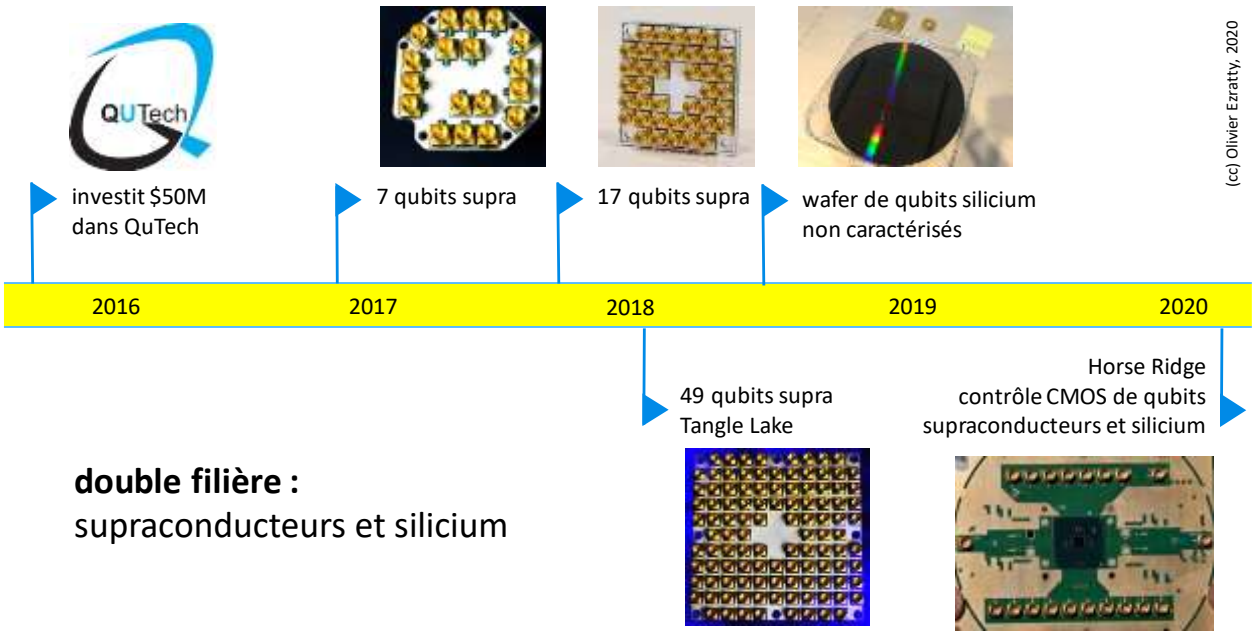
---

[656] Voir Methods for Measuring Magnetic Flux Crosstalk Between Tunable Transmons par Deanna M. Abrams et al, aoput 2019 (12 pages).

[657] Dans Quantum Kitchen Sinks: An algorithm for machine learning on near-term quantum computers de juillet 2018 (8 pages).

Au CES 2018, le CEO d'Intel avait fièrement brandi un chipset de 49 qubits lors de son keynote dans la grande salle de l'hôtel Monte Carlo, entre une démonstration de drone de passager et un discours sur l'intelligence artificielle. Ce processeur en technologie supraconductrice était impressionnant mais ne semble pas encore opérationnel. Dénommé Tangle Lake, ce chipset utilise une technologie supraconductrice voisine de celles d'IBM et Google. Il est en cours de test chez **Qutech** aux Pays-Bas. Il représente un enjeu clé pour Intel qui devrait éviter de rater cette grande vague technologique qu'est l'informatique quantique. Ils ont raté celle du mobile et ne sont pas bien en point dans l'intelligence artificielle face à Nvidia qui leur taille des croupières.

Intel a plusieurs fers au feu dans le quantique. Ils creusent à la fois la piste des qubits supraconducteurs et ont présenté à ce jour plusieurs puces allant jusqu'à une cinquantaine de qubits comme Tangle Lake, et celle des qubits CMOS, que nous évoquerons dans la prochaine partie, qui s'appuiera sur leur savoir-faire en industrialisation de production de composants de ce type, un savoir qui est rare et cher dans l'industrie.



Leurs chipsets quantiques supraconducteurs évoluent à un rythme voisin de ceux de Google et IBM dans les supraconducteurs. Ils en étaient ainsi à 7 qubits fin 2016, 17 qubits fin 2017 puis 49 qubits présentés en janvier 2017, tous en supraconducteurs.

En février 2020, Intel annonçait son composant Horse Ridge qui sert à piloter des qubits supraconducteurs et silicium à l'intérieur du cryostat. Il réalise cela grâce à la capacité à gérer des micro-ondes des bandes de fréquences 6 à 7 GHz (pour les qubits supraconducteurs) et de 14 à 20 GHz (pour les qubits silicium).

En fait, ils sont spécifiés pour aller de 2 à 20 GHz. C'est un composant cryo-CMOS intégrant de la mémoire SRAM réalisé en FinFET Low Power en intégration 22 nm, sur 4 mm^2. Il peut contrôler jusqu'à 128 qubits et opère à la température de 3K[658]. Il consomme 1,7 mW par qubit et un total de 330 mW. Cela tient dans l'enveloppe thermique de l'étage 4K d'un cryostat qui est en général d'environ 1W. Le composant est testé par QuTech aux Pays-Bas.

Nous avons déjà vu qu'Alibaba était très actif pour utiliser les ressources de ses datacenters pour faire de la simulation d'algorithmes quantiques dépassant les 50 qubits.

Il se trouve que le leader chinois du commerce en ligne est aussi partenaire l'**University of Science and Technology of China** (USTC) de l'Académie des Sciences Chinoises (CAS) pour la création d'ordinateurs quantiques à qubits supraconducteurs. Ils proposent l'accès dans le cloud à 11 qubits depuis début 2018, sur une plateforme technologique développée avec l'USTC.

Ils ont même annoncé en 2018 qu'ils créaient une filiale, Ping-Tou-Ge qui développe des NPU (processeurs neuromorphiques pour l'IA) et, à terme, des chipsets quantiques supraconducteurs[659].

Silicium

Les qubits à base de silicium sont une voie en devenir permettant d'utiliser des processus de fabrication existants de composants CMOS standards. Pour mémoire, le CMOS ("Complementary Metal Oxyde Semiconductor") est la technologie utilisée de manière dominante pour produire des processeurs dans le monde, pour les CPU (Intel, AMD), les GPU (Nvidia, AMD), les chipsets pour smartphones (Qualcomm, Samsung, Mediatek, HiSilicon, etc) et dans tout un tas de secteurs spécialisés (micro-contrôleurs, composants radio, …).

Dans les processeurs quantiques, c'est la voie choisie par quelques laboratoires de recherche dans le monde et par quelques entreprises privées telles que **Nokia / Bell Labs**, les **Lincoln Labs** aux USA[660], les **NTT Basic Research Laboratories** au Japon, et surtout, par **Intel** aux USA. En France, c'est l'une des deux voies d'exploration sérieusement étudiées au **CEA-Leti**, en collaboration avec l'Institut Néel du CNRS à Grenoble.

Il s'agit précisément de qubits de spin d'électron. Leur état quantique est généralement l'orientation du spin d'un électron piégé dans un puit de potentiel. Ils sont intéressants de par la potentielle immunité au bruit de l'environnement du spin d'électron piégé. En 2020, le nombre de qubits à base de silicium (silicium ou silicium+germanium) démontré était de deux avec une fidélité supérieure à 98% pour toutes les opérations. Les temps de lecture étaient de l'ordre de 5µs sachant que les temps de manipulations peuvent être plus rapides suivant les techniques utilisées. Les qubits de spin ont des dimensions de l'ordre de 100x100 nm et se prêtent donc à une forte densité et miniaturisation.

---

[658] Voir Intel and QuTech Unveil Details of First Cryogenic Quantum Computing Control Chip, 'Horse Ridge', février 2020 et la brochure de HorseRidge.

[659] Voir Alibaba Launches Chip Company "Ping-Tou-Ge"; Pledges Quantum Chip, septembre 2018.

[660] Les Lincoln Labs travaillent notamment sur le packaging 3D et la connectique des qubits silicium. Voir 3D integration and packaging for solid-state qubits par D. Rosenberg et al, 2019 (22 pages).

C'est à la fois cette dimension, le potentiel intrinsèque du silicium avec 10^{-7} de fidélité démontrée dans des échantillons de silicium massif et la possibilité d'intégrer l'électronique de contrôle dans le composant qui en font un candidat intéressant pour le calcul quantique à grande échelle[661].

qubits silicium

avantages

- **fort potentiel de scalabilité** pour créer des processeurs avec des millions de qubits, notamment par leur taille de 100x100 nm.
- **fonctionne à environ 1K** => plus grand budget thermique disponible pour les composants de contrôle.
- **hybridation possible** avec composants de contrôle des qubits (CryoCMOS ou supraconducteurs SFQ).
- adapté aux **architectures 2D** exploitables avec des surface code et équivalents pour la correction d'erreurs.
- peut s'appuyer sur les **fabs de production existantes.**
- **couplage possible** des qubits avec des fibres optiques pour de la communication inter-qubits longue distance.
- **vitesse d'exécution** des portes quantiques.

inconvénients

- **intrication de seulement deux qubits silicium** réalisée à date (UNSW, QuTech, Princeton, UTokyo).
- **fidélité des qubits** moyenne pour l'instant avec 98% pour les portes à deux qubits.
- **variabilité des qubits** à confirmer avec des mesures expérimentales pour l'instant contradictoires.
- **coûts de lancement de fabrication élevés** et justifiables uniquement pour de gros volumes de production.

Le principe général utilisé pour créer des qubits de ce type est le suivant[662] :

- L'**état quantique** du qubit est généralement le spin d'un électron individuel d'un atome piégé dans une structure semi-conductrice comprenant un puit de potentiel. Le spin est assimilable à l'orientation magnétique de l'électron.
- Les **portes quantiques à un qubit** utilisent le principe de l'ESR, ou "electron spin resonance". Comme pour les qubits supraconducteurs, ces portes s'appuient sur l'émission de micro-ondes envoyées par conduction vers les qubits, soit en utilisant des cavités électro-magnétiques, soit avec des lignes radiofréquence dans lesquelles circulent un courant alternatif qui crée un champ magnétique, soit enfin, en utilisant des micro-aimants. Les micro-ondes utilisées ont des fréquences situées entre 12 et 20 GHz plus élevées que celles des qubits supraconducteurs.
- Les **portes quantiques à deux qubits** sont créées en jouant sur l'interaction d'échange entre deux qubits voisins. Ces qubits sont mis en interaction l'un avec l'autre en jouant sur la barrière de potentiel qui sépare les deux qubits. Les manipulations, comme dans les portes à un qubit, sont effectuées via l'application de pulsations de courants continus. Les portes courantes à bas niveau de ce type sont la racine carrée d'une porte SWAP et une porte à phase contrôlée. Les autres portes sont constituées par programmation et assemblage de ces portes et des portes à un qubit classiques.
- La **mesure de l'état d'un qubit** utilise la conversion du spin d'électron, son orientation magnétique, en charge électrique (« spin to charge ») qui est ensuite exploitable par de l'électronique traditionnelle.

L'intérêt de cette technique est de permettre l'intégration d'un grand nombre de qubits dans un circuit, avec potentiellement jusqu'à des milliards de qubits sur un seul chipset. C'est même d'ailleurs semble-t-il la seule technologie qui permettrait d'atteindre ce niveau d'intégration.

---

[661] Un bon panorama à date des qubits silicium est fourni dans Scaling silicon-based quantum computing using CMOS technology: Challenges and Perspectives par Fernando Gonzalez-Zalba, Silvano de Franceschi, Tristan Meunier, Maud Vinet, Andrew Dzurak, 2020 (16 pages).

[662] Voir Silicon Qubits par Thaddeus D. Ladd 2018 (19 pages) qui décrit diverses méthodes autres que celle qui est ici évoquée.

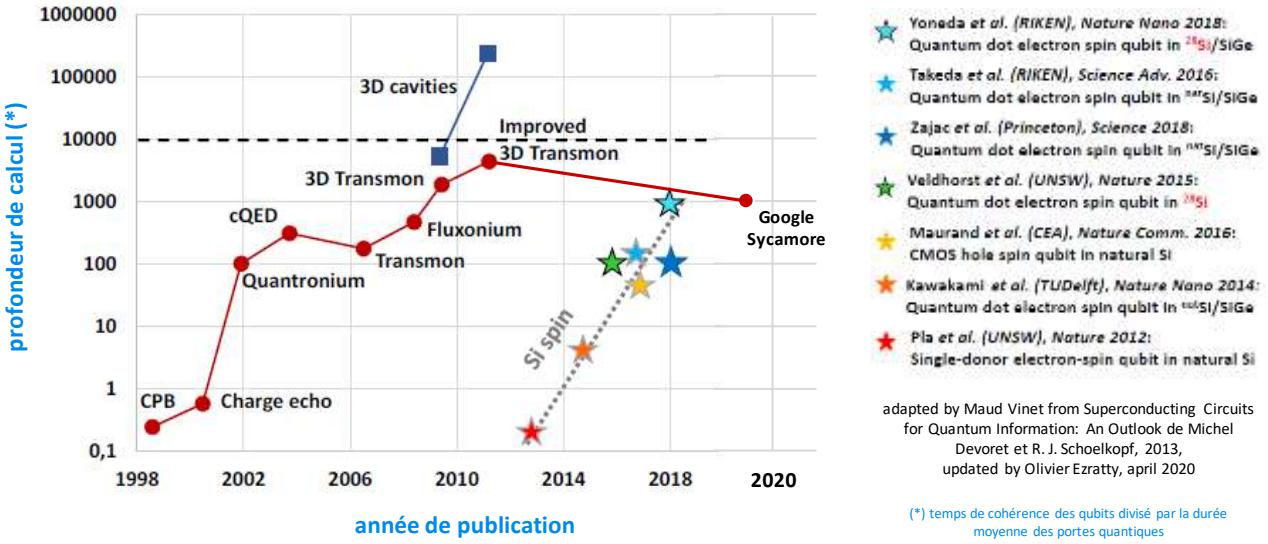
Le tout se ferait avec un temps de cohérence assez long des qubits et un taux d'erreur au moins aussi bon qu'avec les qubits supraconducteurs universels[663].

L'une des difficultés est de relier les qubits entre eux par couplage pour permettre l'exécution de portes quantiques à deux qubits, et à grande échelle. Ce couplage pourrait notamment passer par l'utilisation de photons et de couplage photons-spins.

Les micro-ondes de contrôle utilisées ont un niveau d'énergie plus élevé qui explique pourquoi les qubits silicium peuvent fonctionner en théorie aux alentours de 1K au lieu de 15 mK pour les qubits supraconducteurs. Ce niveau correspond à des micro-ondes de fréquence supérieures à 20 GHz, à comparer aux 4 à 8 GHz des micro-ondes de contrôle des qubits supraconducteurs.

Ces qubits manipulant des électrons individuels, ils seraient aussi moins sujets aux perturbations extérieures que les qubits supraconducteurs qui s'appuient sur des courants portés par des millions d'électrons. C'est l'une des raisons qui permettrait à cette technologie de mieux "scaler" en nombre de qubits. En effet, cette température plus élevée permet de placer une électronique de commande plus dense autour des qubits sans que cela n'échauffe trop le circuit. En effet, cette électronique dégage de la chaleur et cette chaleur acceptable est conditionnée par la température de fonctionnement des qubits. Plus cette température est basse, plus la chaleur acceptable dégagée par l'électronique de contrôle des qubits est basse.

Les données de références sont les suivantes : on ne peut consommer qu'un milliwatt d'énergie à 100 mK[664]. Cela limite l'électronique de contrôle à environ 10 000 transistors en technologie CMOS[665]. A noter qu'une fois mis au point, les qubits silicium vont nécessiter l'emploi de codes de correction d'erreurs en masse, comme les "surface codes".



[663] Un record de temps de cohérence de qubits silicium a été battu en 2020 par une équipe de l'Université de Chicago, atteignant 22 ms (T2). Soit 10 000 fois plus long que les temps de cohérence habituels situés aux alentours de 100µs que l'on trouve dans les qubits supraconducteurs. Ces qubits utilisent des doubles lacunes dans des structures en carbure de silicium. Voir Universal coherence protection in a solid-state spin qubit par Kevin C. Miao, David D. Awschalom et al, août 2020 (12 pages). Université de Chicago.

[664] On peut obtenir un milli-Watt de puissance de refroidissement avec un cryostat à double tête pulsée comme le BlueFors XLD1000 ou le Oxfors Instruments TritonXL.

[665] C'est expliqué dans 28nm Fully-Depleted SOI Technology Cryogenic Control Electronics for Quantum Computing, 2018 (2 pages), issu du CEA-Leti et de STMicroelectronics. Il évoque la bonne performance de composants CMOS réalisés en technologie FD-SOI et opérant à 4K. Là où le budget thermique disponible est d'ailleurs encore plus élevé qu'à 100 mK.A 4K, la puissance de refroidissement est de l'ordre du quart de Watt (250 milli-Watts).

Les progrès dans le CMOS sont plus récents et font la course par rapport aux qubits supraconducteurs en termes de qualité. Le schéma *ci-dessus* illustre cette évolution dans le temps entre 2013 et 2018[666], mais de manière incomplète. Notamment, on ne dispose pas de données sur l'évolution des opérations (en Y) après 2018.

En tout état de cause, elles ne semblent pas avoir encore dépassé les 1000. Et sachant qu'il s'agit d'un seul paramètre de comparaison le nombre de portes quantiques exécutables avant d'atteindre le phénomène de décohérence des qubits. Il n'intègre pas le taux d'erreurs des portes et la capacité d'intrication des qubits, qui n'est pas encore démontrée au-delà de deux qubits pour le silicium.

Au niveau de l'état de l'art, les Australiens, les chercheurs hollandais de QuTech[667] et Jason Petta à Princeton ont démontré des portes à deux qubits dans différentes géométries. Pour aller à l'étape suivante, la difficulté est de maîtriser le potentiel électrostatique entre les puits quantiques où sont stockés les électrons - et donc leur spin - avec un nombre de grilles qui permettent de disposer les qubits pas trop loin les uns des autres, typiquement de l'ordre de quelques dizaines de nanomètres.

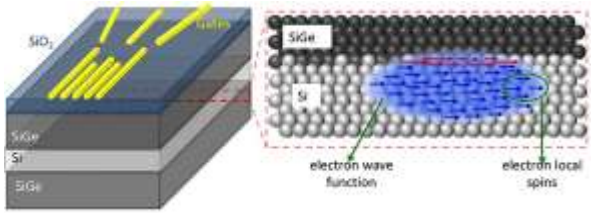
Notons que l'on peut associer des qubits CMOS et de la photonique. Ainsi, les états de qubits CMOS qui sont des spins d'électrons uniques peuvent être transmis à distance via des photons ce qui permet d'imaginer des architectures de calcul quantique distribuées[668].

Voici les principaux laboratoires de recherche qui creusent la piste du CMOS, très souvent dans de la recherche partenariale multi-laboratoires et multi-pays.

TU Delft QuTech

Le laboratoire hollandais **QuTech** issu de l'Université **TU Delft** et de la collaboration avec Intel travaille sur une architecture CMOS, sur des gaz bidimensionnels d'électrons à base de Si/SiGe et sur des qubits à base de germanium et SOI[669].

Le germanium est un matériau de la colonne IV comme le silicium. Son avantage dans les qubits est de permettre de créer des portes quantiques très rapides allant de 0,5 à 5 ns[670]. Le SOI pour "silicon on insulator" ou "silicium sur isolant" est une technologie issue des français CEA-Leti et SOITEC.



Elle ajoute une couche d'isolant en oxyde de silicium (SiO2 ou "BOX" pour « buried oxyde ») au-dessus des wafers de silicium et sur laquelle sont ensuite gravés les transistors et autres conducteurs des circuits.

---

[666] Ce schéma est de Maud Vinet et s'inspire de Superconducting Circuits for Quantum Information: An Outlook de Michel Devoret et Robert Schoelkopf, 2013 (7 pages). A noter qu'il date de 2013 donc n'indique pas les progrès réalisés depuis dans les qubits supraconducteurs. « *Operations per error* » est proportionnel au ratio entre la durée de vie des qubits et la vitesse des portes quantique sur ces qubits. Il n'intègre pas l'impact du taux d'erreur des qubits qui se manifeste en général bien avant avoir atteint cette limite de nombre de portes théoriquement exécutables.

[667] Voir A Crossbar Network for Silicon Quantum Dot Qubits, de R Li et al, 2017 (24 pages).

[668] Voir Coherent shuttle of electron-spin states par Lieven Mark Koenraad Vandersypen et al, 2017 (21 pages).

[669] L'équipe de Menno Veldhorst de QuTech publiait Reliable and extremely fast quantum calculations with germanium transistors en janvier 2020. Il s'agissait de démontrer la faisabilité de qubits à base de transistors au germanium avec deux qubits intriqués. La fidélité de porte à un qubit obtenue était de 99,9% et pour deux qubits, à 98%. Par contre, le temps de cohérence de ces qubits est très faible, en-dessous de la µs. Voir Fast two-qubit logic with holes in germanium par Menno Veldhorst et al, janvier 2020 dans Nature et souis sur Arxiv en avril 2019 (6 pages).

[670] Voir aussi Quantum control and process tomography of a semiconductor quantum dot hybrid qubit, 2014 (12 pages).

En 2020, QuTech annonçait mettre au point des qubits silicium « chauds », c'est-à-dire pouvant fonctionner aux alentours de 1K comme anticipé. Plus précisément à 1,1K[671]. Sachant que dans le même temps, l'UNSW affichait un fonctionnement à 1,5K[672].

TU Delft collabore sur la branche germanium avec deux Universités américaines : Purdue dans l'Indiana et celle du Wisconsin-Madison. Ils ambitionnent d'intégrer des millions de qubits dans des circuits en SiGe[673]. En septembre 2020, ils annonçaient avoir créé un processeur en qubits silicium et quantum dots à base de germanium de quatre qubits avec un couplage bidirectionnel, ouvrant la voie de la scalabilité dans cette branche[674].

Les Australiens sont parmi les plus actifs autour des qubits silicium, ce que soit dans les équipes du **CQC²T** de l'UNSW (University of New South Wales), dans la startup **SQC** de Michelle Simmons qui en est issue ou dans d'autres laboratoires.

Le laboratoire **CQC²T** (Center for Quantum Computing & Communication Technology) de l'**UNSW** qui est piloté par Michelle Simmons collabore avec le CEA-Leti dans la voix SOI.

L'UNSW fait avancer la fidélité des qubits CMOS, quantifie la variabilité des qubits et leur fidélité en fonction de la température. Ils obtenaient en 2019 un taux d'erreur de portes quantiques à deux qubits de 2% et une fidélité de 99,96% pour des portes à un qubit[675].

L'UNSW et de la Purdue University dans l'Indiana aux USA (financée par Microsoft) ont aussi expérimenté un système d'atomes de phosphore intégrés dans un substrat de silicium, les états des qubits étant le spin d'électrons des atomes de phosphore. La recherche porte surtout sur le couplage entre qubits, à base de liaisons entre dipôles électriques. Ils prévoient d'atteindre 10 qubits d'ici 2022[676]. L'UNSW a bénéficié d'un financement de $53M originaires de l'opérateur télécom Telstra, de la Commonwealth Bank et des gouvernements australiens et de la région Nouvelles-Galles du Sud.

L'équipe de l'UNSW prouvait en 2018 la faisabilité de la création de qubits dans des structures CMOS et mettait au point des protocoles de lecture de l'état des spins de ces qubits sans avoir de recours au moyennage via un processus dénommé "Pauli spin blockade" ouvrant la voie à la mise en œuvre de codes de correction d'erreurs et de la création d'ordinateurs quantiques à grande échelle en nombre de qubits[677].

---

[671] Voir Hot, dense and coherent: scalable quantum bits operate under practical conditions par QuTech, avril 2020 qui fait référence à Universal quantum logic in hot silicon qubits par L. Petit et al, avril 2020 dans Nature et octobre 2019 en pre-print (10 pages).

[672] Voir Hot qubits made in Sydney break one of the biggest constraints to practical quantum computers par UNSW, avril 2020.

[673] Dans Silicon provides means to control quantum bits for faster algorithms, juin 2018.

[674] Voir A four-qubit germanium quantum processor par N.W. Hendrickx et al, septembre 2020 (8 pages).

[675] Voir Quantum World-First: Researchers Reveal Accuracy Of Two-Qubit Calculations In Silicon, mai 2019.

[676] C'est documenté dans Silicon quantum processor with robust long-distance qubit couplings, 2017 (17 pages).

[677] Voir Tests show integrated quantum chip operations posible, octobre 2018.

L'équipe d'Andrea Morello du **CQC^{2}T** de l'UNSW étudie le couplage à distance de spins d'électrons via des liaisons photoniques dans le visible ou les ondes radio. Son équipe faisait écho de travaux étonnants en 2020 portant sur la création de qubits silicium exploitant le contrôle du spin d'électrons de couches intermédiaires d'atomes de silicium, permettant d'en augmenter la stabilité et de réduire les erreurs de flip (ou de charge, qui font lentement basculer l'état $|1\rangle$ en état $|0\rangle$)[678].

Elle arrivait aussi, par hasard, à contrôler le spin de noyaux d'atomes d'antimoine avec un champ électrique oscillant[679]. N'en jetez plus !

La spin-off **SQC** (Silicon Quantum Computing) de l'UNSW lancée par Michelle Simmons veut produire un démonstrateur de 10 qubits d'ici 2022.

En 2020, une équipe de l'**Université de Melbourne** montrait comment le machine learning pouvait aider au calibrage du placement des atomes de phosphore dans une structure 2D de qubits sur substrat silicium[680].

D'autres équipes australiennes travaillent sur des qubits de spin fonctionnant à température ambiante, un Graal intéressant à poursuivre pour peu que l'ensemble des composants fonctionne effectivement à température ambiante (on a vu que ce n'était pas le cas pour les ions piégés et cela ne l'est pas plus pour les qubits photons dont l'instrumentation doit être refroidie).

C'est le cas de la société **Archer Materials** (Australie) qui faisait parler d'elle en avril 2020 en suspendant sa cotation en bourse au moment de l'annonce d'un nouveau deal de fabrication de leur composant dénommé **^{12}CQ**. Le tout s'appuie sur des nanosphères de carbone et doit fonctionner à température ambiante[681]. Le 12 ne correspond pas au nombre de qubits du chipset (qui n'est pas précisé) mais au poids isotopique du carbone à spin nul utilisé pour créer ces nanosphères.

La société semble survendre clairement l'état d'avancement de son composant qui n'est pas vraiment caractérisé, notamment à grande échelle et pour ce qui est de l'intrication entre qubits. D'ailleurs, ils parlent de fonctionnement à température ambiante pour des qubits dont le temps de relaxation (= temps de cohérence) est de 175 ns à 300K. Ce qui ne permettrait pas d'exécuter un grand nombre de portes quantiques !

Aux USA, il faut compter avec les **Sandia Labs**, une filiale du groupe Honeywell qui travaille surtout pour le Département de l'Energie US (DoE) avec des laboratoires dans le Nouveau Mexique et en Californie. C'est une sorte de CEA américain en gestion déléguée dans le privé.

---

[678] Voir UNSW use flat electron shells from artificial atoms as qubits par Chris Duckett, février 2020 et Engineers Just Built an Impressively Stable Quantum Silicon Chip From Artificial Atoms par Michelle Starr, février 2020 qui font référence à Coherent spin control of s-, p-, d- and f-electrons in a silicon quantum dot par Andrea Morello et al, 2020 (7 pages).

[679] Voir Engineers crack 58-year-old puzzle on way to quantum breakthrough par UNSW, mars 2020 et Chance discovery brings quantum computing using standard microchips a step closer par Adrian Cho, mars 2020.

[680] Voir Machine learning to scale up the quantum computer par Muhammad Usman et Lloyd Hollenberg, Université de Melbourne, mars 2020. Vu aussi dans To Tune Up Your Quantum Computer, Better Call an AI Mechanic par le NIST associé à l'UNSW, mars 2020.

[681] Voir Archer Materials granted trading halt ahead of quantum computing chip agreement par Quantum Analyst, 2020 et Room temperature manipulation of long lifetime spins in metallic-like carbon nanospheres par Bálint Náfrádi, 2016 (32 pages) qui décrit en détails cette technique de piège de spin d'électron dans une nanosphère de carbone, qui n'est pas sans rappeler les nanotubes de la startup française C12 Nanotech. Archer affiche un partenariat avec IBM. Ce dernier n'étant pas prêt d'abandonner ses qubits supraconducteurs, il s'intéresse à Archer pour leur faire adopter la plateforme logicielle Qiskit.

Ils travaillent ainsi sur l'armement nucléaire des USA ! Ils travaillent notamment sur la physique des qubits silicium et leurs codes de correction d'erreurs. Ils visent une température d'opération intermédiaire de 100 mK. *Ci-contre*, leur architecture de qubit à base de double quantum dot de silicium (source).

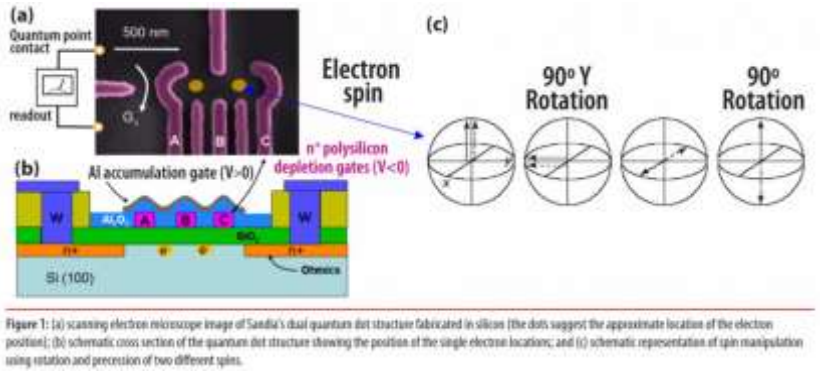


Figure 1: (a) scanning electron microscope image of Sandia's dual quantum dot structure fabricated in silicon (the dots suggest the approximate location of the electron position); (b) schematic cross section of the quantum dot structure showing the position of the single electron locations; and (c) schematic representation of spin manipulation using rotation and precession of two different spins.

L'**Université de Princeton** travaille notamment sur réalisation de porte CNOT à deux qubits en silicium à très haut niveau de fiabilité et faible temps d'opération, respectivement de 200ns et 99%[682]. Ce sont aussi des qubits à double quantum dots utilisant du silicium et du germanium. En octobre 2018, on apprenait que cette équipe de Princeton avait réussi à contrôler l'état de ses qubits CMOS avec de la lumière et exploiter un champ de micro-ondes pour échanger un quantum entre un électron et un photon[683].

Les laboratoires de **HRL Malibu**, une filiale de recherche commune de Boeing et General Motors, située en Californie et **Nokia** travaillent sur des qubits en arséniure de gallium qui nécessitent un refroidissement à moins de 1K. Il s'agirait de qubits avec de longs temps de cohérence permettant de faire des calculs avec un grand nombre de portes quantiques et codes de corrections d'erreurs.

Une équipe associant des chercheurs de Hongrie, Suède, Russes et de l'Argonne National Laboratory aux USA publiait aussi en 2019 des travaux sur la création de qubits fonctionnant à température ambiante et à base de défauts dans du carbure de silicium (SiC) qui rappellent un peu le fonctionnement des NV Centers[684].


UChicago team discovers innovative way to tune quantum signals

After decades of miniaturization, the electronic components we've relied on for computers and modern technologies are now starting to reach fundamental limits. Faced with this challenge, engineers and scientists around the world are turning toward a radically new paradigm: quantum information technologies.

Quantum technology, which harnesses the strange rules that govern particles at the atomic level, is normally thought of as much too delicate to coexist with the electronics we use every day in phones, laptops and cars. However, scientists with the University of Chicago's Pritzker School of Molecular Engineering announced a significant breakthrough: Quantum states can be integrated and controlled in commonly used electronic devices made from silicon carbide

Cela donnait lieu à une information totalement déformée parue en France dans L'informatique quantique fonctionnerait sur des ordinateurs normaux : pourquoi cette découverte est importante par Marcus Dupont-Besnard, décembre 2019 avec, je cite : « *Des chercheurs de l'université de Chicago ont découvert que les bits quantiques peuvent parfaitement fonctionner dans des appareils électroniques classiques du commerce* ».

---

[682] Vu dans Quantum CNOT Gate for Spins in Silicon, 2017 (27 pages).

[683] Voir How old-school silicon could bring quantum computers to the masses, octobre 2018 et In leap for quantum computing, silicon quantum bits establish a long-distance relationship par l'Université de Princeton, décembre 2019.

[684] Voir Scientists Find Yet Another Way to Get Qubits Working at Room Temperature par David Nield, mars 2020 et Novel Qubit Design Could Lead to Quantum Computers That Work at Room Temperature par Matt Swayne, mars 2020 qui font reference à Quantum well stabilized point defect spin qubits par Viktor Ivády et al, mai 2019 (20 pages).

C'est évidemment complètement faux et cela tient à un bug de traduction du terme « devices » qui s'applique aussi bien à un composant électronique (dans le cas présent) ou à un appareil (dans d'autres contextes)[685]! Il ne faut pas confondre le fait de pouvoir s'appuyer éventuellement sur les processus de fabrication actuels de composants CMOS pour créer des qubits et sur le fait d'exploiter des appareils électroniques du commerce d'aujourd'hui !



En **Chine**, toutes les pistes technologiques d'ordinateurs quantiques sont explorées les unes parallèlement aux autres et le CMOS n'y échappe pas. Leurs travaux sont cependant difficiles à évaluer et ils publient moins de prouesses dans les qubits silicium que pour les qubits à base de photons[686].

Au Japon, une équipe de **RIKEN** arrivait à mesurer l'état de qubits silicium sans l'altérer. Cette mesure non destructive utilise un modèle d'interaction d'Ising à base de ferromagnétisme qui évalue le spin d'atomes voisins de celui contenant l'électron de spin de qubit[687]. Ça a l'air intéressant mais présente sûrement des limitations restant à découvrir.

En Allemagne, à l'**Université d'Aix la Chapelle**, des chercheurs ont créé des quantum dots doubles de silicium avec du graphène[688]. Ce n'est pas sans rappeler les travaux de qubits confinés dans des nanotubes de carbone chez le Français **C12 Quantum Electronics**.

Le projet collaboratif européen **Mos-quito** associe les laboratoires de recherche européens planchant sur les qubits silicium fabriqués en technologie CMOS sur wafers 300 mm fabriqués par le CEA-Leti. En plus de ce dernier sont impliqués le Royaume Uni (London UCL, l'Université de Cambridge), la Suisse (EPFL), la Finlande, le Danemark et l'Italie (IMM). C'est un projet de trois ans financé par les deniers européens et qui est maintenant terminé. L'un des objectifs était d'étudier la performance de différents types de qubits individuels à base de spin dans le silicium pour fournir des recommandations pour les mettre en pratique à grande échelle.

Le CEA-Leti de Grenoble est le laboratoire européen en pointe sur la recherche appliquée dans les qubits CMOS à spins d'électrons et surtout, pour leur fabrication. L'équipe en charge du quantique y est pilotée par **Maud Vinet**. Le laboratoire est au cœur d'un écosystème de recherche quantique qui comprend le CNRS avec l'Institut Néel, l'IRIG du CEA et l'Université Grenoble Alpes.

---

[685] L'article fait référence à In surprise breakthrough, scientists create quantum states in everyday electronics par Louise Lerner, décembre 2019. Voir Electrical and optical control of single spins integrated in scalable semiconductor devices par Christopher Anderson et al, décembre 2019. Avec preprint de juin 2019 dans Arxiv (20 pages). Et Electrically driven optical interferometry with spins in silicon carbide, Kevin Miao et al, novembre 2019. Avec preprint dans Arxiv (17 pages).

[686] Voir Semiconductor quantum computation de Xin Zhang Hai-Ou Li et al, décembre 2018 (23 pages). Le document fait un état des lieux de la technologie des qubits CMOS mais sans préciser l'apport spécifique des laboratoires de recherche chinois.

[687] Voir Scientists succeed in measuring electron spin qubit without demolishing it, RIKEN, mars 2020 qui fait référence à Quantum non-demolition readout of an electron spin in silicon par J. Yoneda et al, 2020 (7 pages).

[688] Voir Bilayer graphene double quantum dots tune in for single-electron control par Anna Demming, mars 2020.

L'approche est pluridisciplinaire, ce qui est assez rare dans la recherche, avec un beau panel de chercheurs. Cette équipe grenobloise propose de s'appuyer d'une part sur les capacités technologiques du Leti, les connaissances des propriétés quantiques des nanostructures de silicium de l'IRIG et l'expertise de manipulation de spin de Néel pour dépasser l'état de l'art tant en qualité qu'en nombre des qubits. Sans compter les expertises en physique théorique de Néel que ce soit en thermodynamique quantique (Alexia Auffèves) ou en cryogénie (Henri Godfrin).

D'autre part, une recherche plus en amont sur la manipulation du spin dans les aimants moléculaires et dans les semiconducteurs III-V (non silicium) permet en parallèle d'accumuler des connaissances fondamentales sur les propriétés de spin et de développer en avance de phase de l'électronique ultra-rapide.

L'équipe de l'IRIG qui associe le CEA et l'Université de Grenoble et celles de l'Institut Néel implique aussi le CNRS et l'Université Joseph Fourier de Grenoble qui fait partie du CNRS apportent leur expertise dans la création d'électronique de contrôle fonctionnant à température cryogénique, dans le contrôle d'électrons individuels dans des structures semiconductrices.

D'autres chercheurs de l'IRIG aident à modéliser les composants semi-conducteurs des qubits. Les ingénieurs en microélectronique du Leti complètent l'ensemble avec une connaissance des processus de conception, d'intégration, de fabrication et de tests des circuits semiconducteurs.

L'objectif de cette équipée est de créer des qubits silicium à forte intégration et surtout une capacité à monter en puissance en termes de nombre de qubits. Les premiers qubits en technologie CMOS industrielle ont été créés en 2016.

Le CEA-Leti est l'un des rares laboratoires publics au monde disposant d'une plateforme de production de test de composants CMOS. Basée à Grenoble, elle comprend tout l'outillage de production de composants CMOS sur wafers de 200 et 300 mm. Elle permet de produire des composants en tout genre en CMOS silicium et en matériaux III-V (photonique, arséniure de gallium, nitrure de gallium, etc).

La salle blanche comprend des machines de lithogravure, notamment originaires du leader mondial ASML, avec une densité pouvant descendre à 20 nm, des machines pour le dépôt de matériaux semiconducteurs et conducteurs utilisant toutes les techniques imaginables (plasma, …) ainsi que pour l'ajout de dispositifs MEMS (micro-électro-mechanical systems).

Le tout occupe plusieurs bâtiments, dont le principal qui fait 185 m de long (vue Google Maps *ci-dessus*, sachant que la zone est maintenant floutée suite, probablement à la demande du CEA) sur 8000 m^2 [689]. L'usage de cette salle nécessite cependant d'avoir expérimenté le processus de fabrication en amont, comme le font les laboratoires du CNRS et réseau Renatech.

[689] D'autres salles blanches de recherche existent en France : celle du C2N à Maroussis, l'IEF à Orsay, celle de Thales TRT à Palaiseau, de l'IEMN à Lille, de Femto-ST à Besançon et le Laas à Toulouse. En production il y a surtout les fab 200 et 300 de STMicroelectronics à Crolles, près de Grenoble. Une partie de ces laboratoires sont associés dans le Réseau National des Grandes Centrales de Technologies (Renatech). Ils mettent leurs plateformes à disposition des entreprises en mode projet et contrats.

A Grenoble, le procédé de fabrication des qubits CMOS utilise des wafers SOI (silicon on insulator, avec un isolant en oxyde de silicium) de 300 mm sur lesquels est déposée une fine couche de silicium d'isotope 28 purifié à 99,992%.

La production validée pourrait ensuite être transférée vers de la production en volume dans des fabs commerciales comme celles de STMicroelectronics, Global Foundries ou Samsung qui supportent les processus FD-SOI sur lesquels le CEA s'appuie en général. Mais à ses débuts, la taille du marché des ordinateurs quantiques sera modeste. Et rien que dans un batch classique de 25 wafers, on pourra produire d'un seul coup quelques milliers de puces quantiques, de quoi alimenter une belle base de supercalculateurs quantiques.

À Grenoble, le Leti dispose aussi d'une plateforme de nanocaractérisation (PFNC ou NanoCarac) qui comprend sur 2500 m^2 des dizaines d'outils de métrologie permettant de vérifier la qualité des composants CMOS fabriqués. Avec Fanny Bouton, j'ai pu visiter tout cela en juillet 2018 et c'était impressionnant ! La double salle blanche du Leti cumule environ un milliard d'euros d'équipements avec des machines dont le coût s'étale de quelques millions à 80M€ ! En Europe, les plateformes équivalentes sont rares. On compte surtout celle d'IMEC situé à Louvain en Belgique et financée en partie par la région flammande. Sachant que la région Auvergne-Rhône-Alpes a aussi cofinancé certains équipements du CEA-Leti de Grenoble !

Ce sont des moyens bien plus lourds que pour produire des qubits supraconducteurs à cause du niveau d'intégration qui est plus élevé. Les qubits supraconducteurs sont en effet bien moins intégrés, faisant plusieurs dizaines de microns de largeur. Rigetti produit ses chipsets supraconducteurs en interne avec $10M d'équipement. Les qubits CMOS pourront descendre à une taille de $100nm^2$.

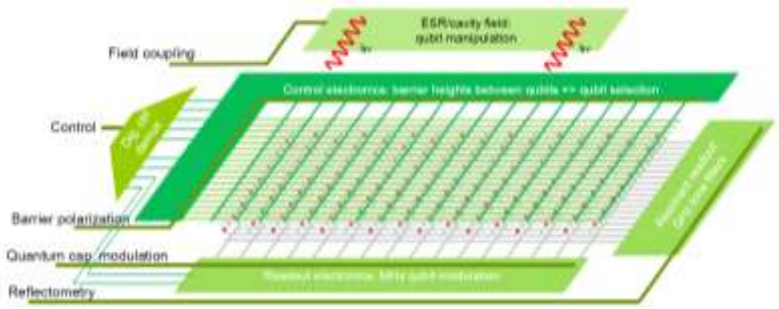
Les fabs classiques ne sont pas optimisées dans leurs processus de fabrication pour créer des qubits CMOS. Cela nécessiterait un gros travail de tuning et un besoin de flexibilité pas évident à obtenir. Avec une densité de 100 nm, on pourrait théoriquement caser un milliard de qubits dans une puce CMOS de 1 cm2.

L'équipe grenobloise doit progresser par étapes sur une période de six ans démarrée en 2019 : démonstration d'une porte à deux qubits à base de silicium, démonstration de simulation quantique dans un réseau 4x4 à base de matériau III-V, démonstration de six qubits intriqués dans du silicium, développement de codes de corrections d'erreurs et algorithmes adaptés et fabrication de 100 qubits en réseau 2D dans du silicium au terme de ce parcours.

L'architecture 2D de ces chipsets CMOS est conçue au sein de cette équipe pluridisciplinaire. Elle comprend plusieurs couches avec les qubits en silicium puis l'électronique intégrée de contrôle et de mesure d'état. Les qubits sont répartis en 2D, mais l'intégration des composants est également verticale dans les composants. La couche de mesure est située en-dessous des qubits tandis que la couche permettant d'activer les qubits avec des portes quantiques est au-dessus.

Pour N^2 qubits, il leur faudrait 2N lignes de contrôle (horizontale, verticale) au lieu de $2N^2$ ce qui générerait un gain appréciable en connectique.

La technique fonctionnerait pour générer des portes quantiques à un et deux qubits[690].

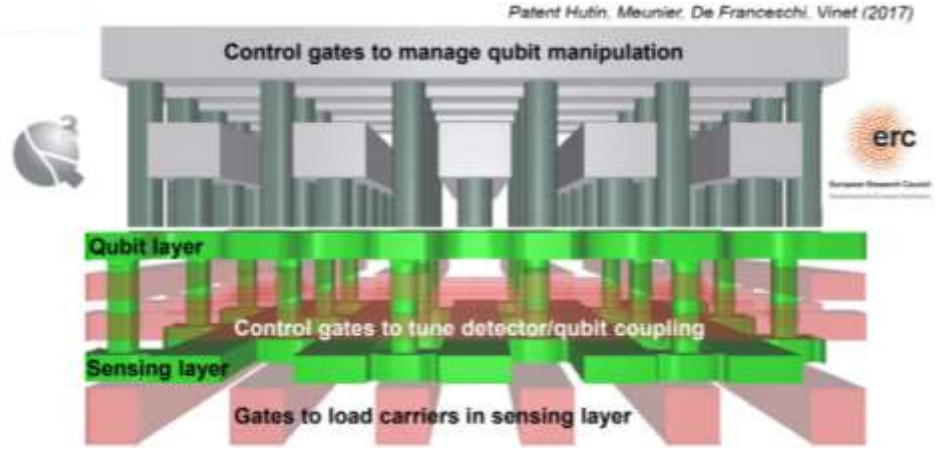


[690] La technique est décrite dans Towards scalable silicon quantum computing par matias.urdampilleta, Maud Vinet, Tristan Meunier, Yvain Thonnart et al, 2020 (4 pages) ainsi que dans la présentation Silicon Based Quantum Computing, Maud Vinet 2018 (28 slides) d'où est issu le shéma vert de la page.

Le grand défi de ces architectures est leur variabilité, à savoir les différences de comportement d'un qubit à l'autre et d'un circuit à l'autre. Elle entraîne un besoin de calibrage précis, qubit par qubit, des micro-ondes de contrôle et de lecture de l'état des qubits. Comme pour les qubits supraconducteurs, ce calibrage peut faire appel à des logiciels de machine learning dédiés.

Ils utilisent des matériaux supraconducteurs pour la couche métal de ces circuits, à base de nitrure de titane.

Cela procure une faible résistance et réduit le bruit de mesure de l'état des qubits. Il y a donc aussi de la supraconductivité dans les qubits au silicium !



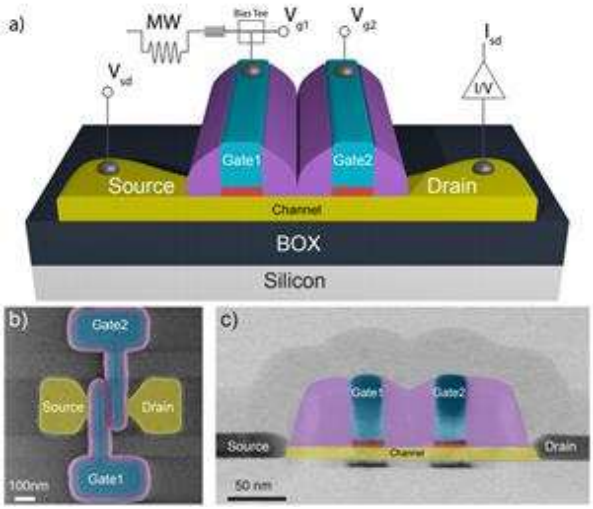
Le CEA travaille aussi sur la technologie **CoolCube** permettant de disposer les composants en 3D (détails), ce qui permettrait de résoudre divers problèmes de mise à l'échelle. Elle serait applicable aux qubits CMOS et plus largement, à d'autres applications du CMOS. Les publications de référence de ces équipes sur les qubits CMOS sont nombreuses[691].

En octobre 2018, l'équipe grenobloise associant Silvano De Franceschi (INAC, CEA), Tristan Meunier (Institut Néel, CNRS) et Maud Vinet (CEA-Leti) obtenait un financement européen **ERC Synergy Grant** de 14M€ pour leur projet QuQube qui sera étalé sur 6 ans pour produire un processeur quantique de 100 qubits CMOS à spin d'électrons[692]. Dans les pistes complémentaires explorées à Grenoble, le Leti conçoit des circuits électroniques cryogéniques ("CryoCMOS Circuits") qui pourront se rapprocher des circuits de contrôle des qubits dans l'enceinte thermalisée. Il faut en effet répartir des générateurs de courant continu et des démodulateurs (à température ambiante), des amplificateurs et mélangeurs (à 4K), des résonateurs utilisant une technologie Cryo CMOS (fonctionnant à 1K) et des composants électroniques devant tourner à moins de 1K.

[691] On compte notamment A CMOS silicon spin qubit, 2016 (12 pages) qui définit les bases du qubit CMOS à double quantum dots (*schéma ci-contre*), SOI technology for quantum information processing, 2016 qui complète cette description ainsi que Conditional Dispersive Readout of a CMOS Single-Electron Memory Cell par Simon Schaal et al, 2019 (9 pages) qui décrit dans le cadre d'un partenariat avec l'Université de Londres, le travail sur la lecture de l'état d'un qubit quantum dot CMOS. Et puis Towards scalable silicon quantum computing de Maud Vinet et al, 2018 (4 pages).

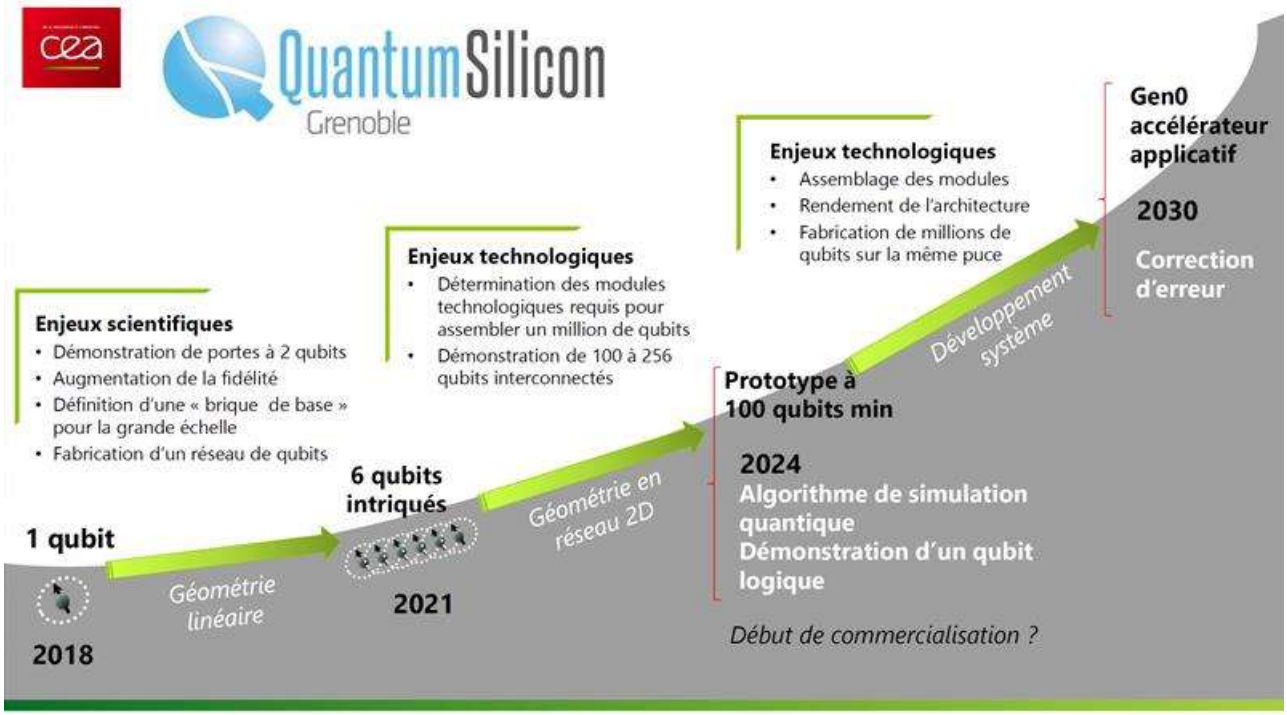
[692] Voir Un ERC Synergy Grant pour la recherche grenobloise sur les technologies quantiques, octobre 2018 (6 pages). Un European Research Council Synergy Grand finance des « moonshots » dans la recherche européenne associant au moins deux laboratoires de recherche. 14M€ est le financement maximum d'un tel projet. 10M€ de financement de base et 4M€ qui peut notamment financer des investissements lourds où l'accès à de grosses infrastructures. On pense immédiatement à la fab 200/300 du CEA-Leti à Grenoble !

Grenoble travaille sur la conception de circuits de couplage entre spin d'électrons et photons ("Spin-Photon Coupling"). Ils doivent servir à créer des systèmes de couplages entre qubits distants. A l'Institut Néel, on cherche à déplacer sur de longues distances des spins d'électrons ("Long distance coherent spin shuttling").



Ici, une longue distance signifie 5 µm ! Mais cela fait de quoi relier des qubits entre eux, donc cela vaut le coup[693]. Tout cela pour dire que les équipes de Grenoble mettent au point de nombreuses briques centrales et périphériques du puzzle que constitue la création d'un ordinateur quantique à qubits silicium[694].

Depuis mars 2020, l'équipe de Grenoble coordonne un nouveau projet du Flagship quantique européen, le **QLSI**. Ce projet vise à coordonner la recherche fondamentale dans les qubits silicium. Il rassemble le CEA, le CNRS Institut Néel, Atos, SOITEC et STMicrolectronics pour la France, l'IMEC (Belgique), Quantum Motion et UCL (UK), Infineon, IHP, U Konstanz, Fraunhofer et RWTH Aachen (Allemagne), UCPH (Danemark), TU Delft, U Twente et TNO (Pays-Bas) et U Basel (Suisse).

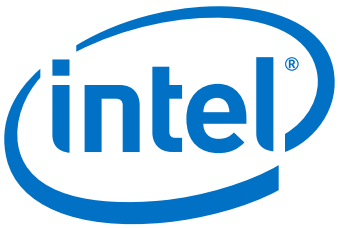


Le projet est doté de 15M€ sur quatre ans à se répartir entre toutes ces entités. L'objectif est de permettre la fabrication et le test de 16 qubits silicium avec une fidélité de portes supérieure à 99%, sa mise à disposition dans le cloud, et la préparation d'une roadmap pour pouvoir scaler au-delà du millier de qubits.

---

[693] Voir à ce sujet Coherent long-distance displacement of individual electron spins, 2017 (27 pages).

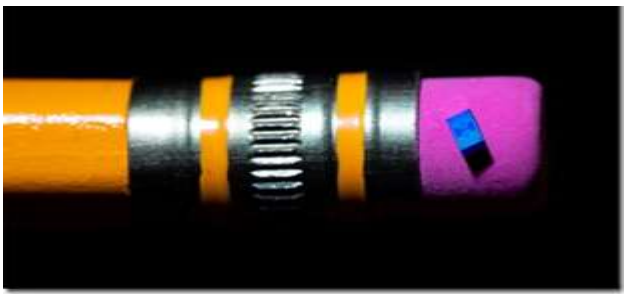
[694] Voir Quantum Silicon Grenoble, le projet sur lequel mise le rapport Forteza pour un ordinateur quantique made in France par Manuel Moragues, janvier 2020.



En plus des qubits supraconducteurs, **Intel** travaille aussi sur la piste des composants silicium utilisant des spins d'électrons avec un premier wafer produit avec des chipsets de 26 qubits en 2017. Les travaux quantiques d'Intel sont gérés sous la direction d'**Anne Matsuura**[695] et de **James Clark** pour le hardware.

Le choix des qubits à base de silicium et de spins d'électron résulte d'une forme de biais cognitif : Intel maitrise la fabrication de composants CMOS et recherche donc une technologie quantique qui puisse s'appuyer sur ce savoir-faire. Mais il y a une grande logique à poursuivre cette voie qui semble l'une des rares capable de scaler en nombre de qubits. Les puces de qubits sont prototypées dans les Intel Labs de Portland.

En juin 2018, Intel faisait une annonce de plus avec une puce très intégrée utilisant cette technologie CMOS, censée pouvoir compter jusqu'à 1500 qubits (*ci-contre*).



Elle est fabriquée dans la fab D1D située dans l'Oregon, avec une densité de gravure de 50 nm, six fois plus grande que la génération du début de 2018.

Mais bien entendu, sans aucune information sur le bruit généré, qui est indispensable pour le bon fonctionnement du système ni d'ailleurs, le nombre exact de qubits de la puce en question. Que ce soit pour Tangle Lake en supraconducteurs ou pour les différentes versions à spins d'électrons, on est donc dans un brouillard quantique sur la qualité de l'ensemble.

Le hollandais QuTech et Intel travaillent bien ensemble. QuTech a bénéficié de $50M d'investissements de la part d'Intel en 2015 pour explorer la voie des qubits silicium. L'investissement global d'Intel reste cependant modeste sur le quantique en apparence. Il peut en tout cas l'être tant que l'on n'en est pas au niveau de la fabrication en série.

Intel annonçait en 2018 avoir réussi à contrôler un processeur CMOS à 2 qubits avec la gestion de portes quantiques à un et deux qubits intriqués exécutant les algorithmes de Deutsch-Jozsa et Grover à toute petite échelle. Ces qubits en silicium et germanium fabriqués par Intel dans l'Oregon étaient testés par le Laboratoire Vandersypen de l'Université de Delft qui fait partie de QuTech[696]. Depuis 2018, Intel est resté assez discret sur ses avancées dans les qubits silicium[697].

Début 2020, Intel annonçait avoir développé avec QutTech le composant **Horse Ridge** que nous avons déjà évoqué dans la partie dédiée aux qubits supraconducteurs. C'est un composant CMOS fonctionnant à 4K qui sert à générer les micro-ondes de pilotage de qubits aussi bien supraconducteurs que silicium. C'est une contribution intéressante, mais pas unique au monde, pour rendre le contrôle des qubits scalable. La startup **SeeQC** plaçant également ce contrôle, en composant supraconducteur, à l'étage 4K.

---

[695] Voir Intel's quantum efforts tied to next-gen materials applications, janvier 2019 et Intel's spin on qubits and quantum manufacturability tous deux de Nicole Hemsoth, novembre 2018 ainsi que Leading the evolution of compute, Anne Matsuura, juin 2018 (26 slides).

[696] Voir A programmable two-qubit quantum processor in silicon, mai 2018 (22 pages).

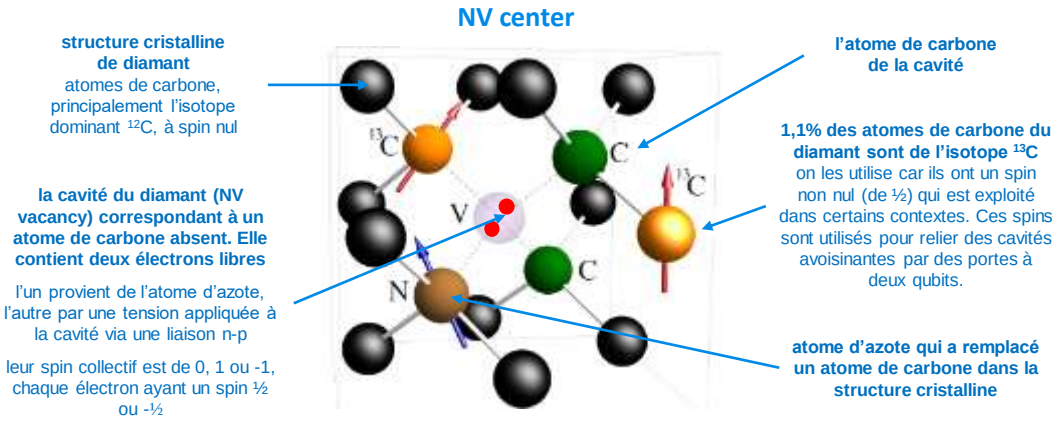
[697] Voir cependant What Intel Is Planning for The Future of Quantum Computing: Hot Qubits, Cold Control Chips, and Rapid Testing, par Samuel Moore, août 2020, qui fait un point, assez pédagogique, de l'approche d'Intel avec les qubits silicium.

NV centers

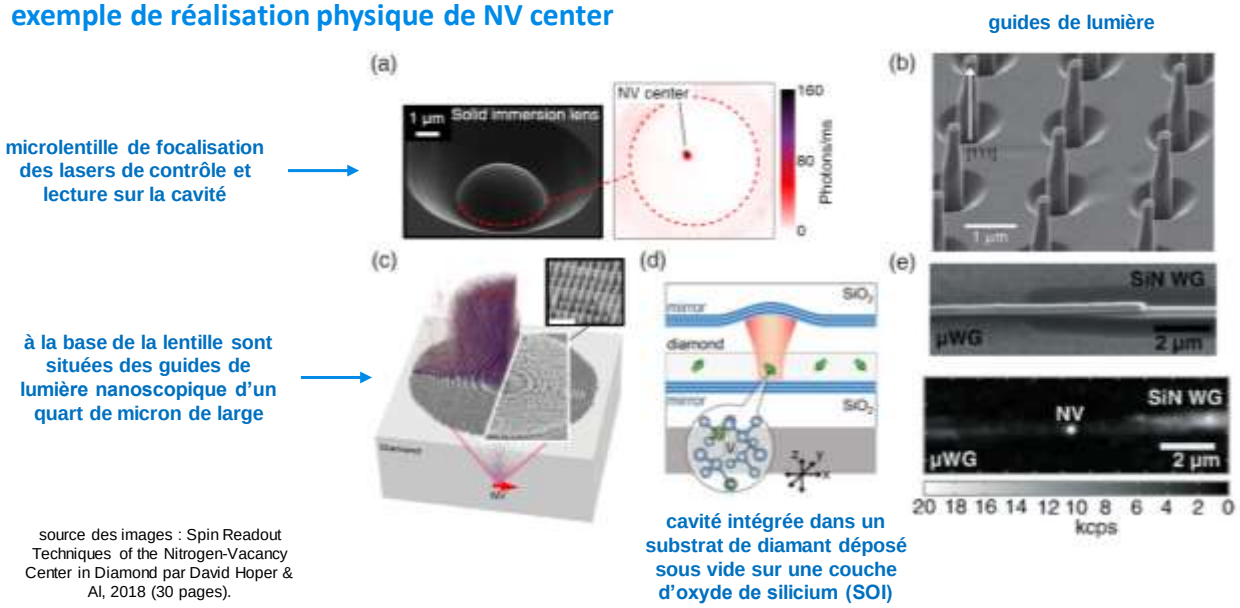
Cette technologie de qubits repose sur le contrôle de spin d'électrons piégés dans des défauts artificiels de structures cristallines de carbone dont un atome de carbone est remplacé par un atome d'azote et un autre atome de carbone remplacé par un vide sans atome, la lacune ou la cavité.

Cette cavité comprend un électron libre qui est généré par une tension électrique appliquée à une jonction n-p obtenue par dopage du diamant. L'électron libre est couplé à un autre électron libre, issu de l'atome d'azote proche de la cavité. La cavité comprend deux autres paires d'électrons de l'atome d'azote de la cavité, de spin total nul.

On contrôle le spin collectif de ces deux électrons libres tout comme celui du noyau d'azote de la cavité et éventuellement des atomes de carbone ^{13}C avoisinants[698]. Le spin cumulé des deux électrons de la cavité est de 0, 1 ou -1 car il ajoute deux spins d'électrons qui sont de ½ ou -½. Ce spin d'électrons est contrôlé une combinaison de micro-ondes et de champ magnétique. Les NV centers utilisés couramment sont dénommés NV^- du fait de l'ajout d'un électron externe dans la cavité. Les NV centers sans cet électron ne sont pas utilisés couramment.



Voici un schéma qui décrit à quoi peut ressembler un NV center en pratique sachant qu'il doit y avoir plusieurs réalisations possibles.



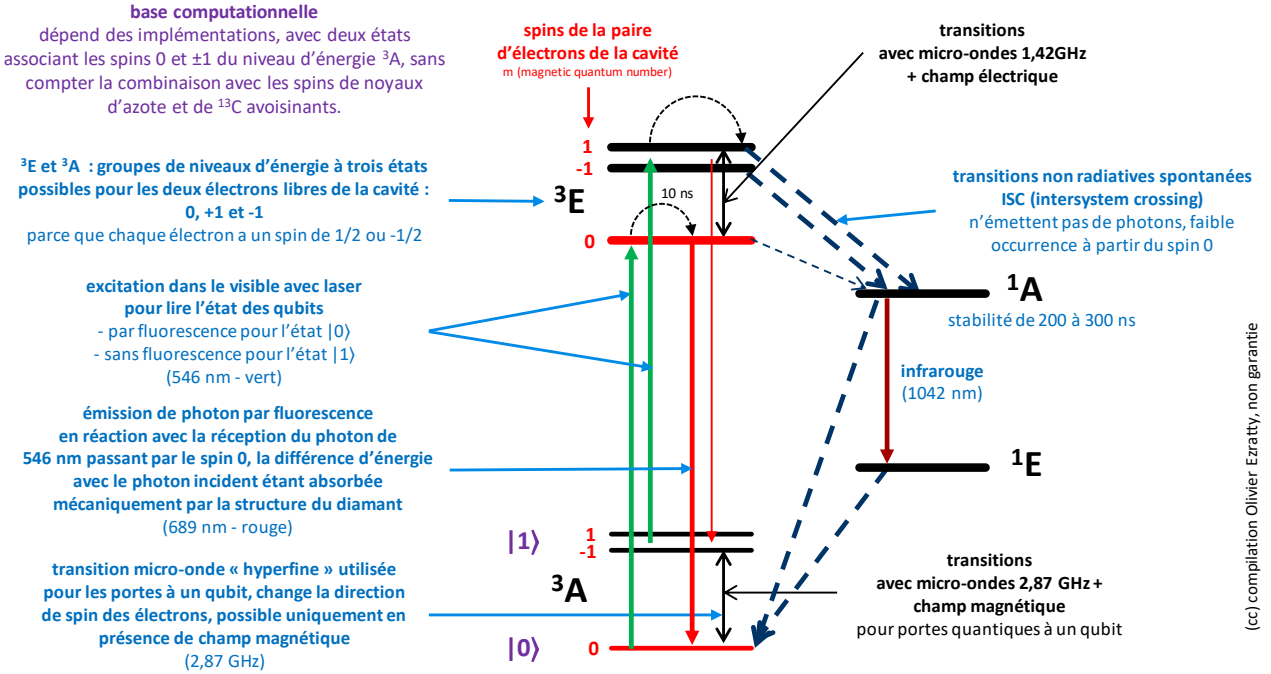
source des images : Spin Readout Techniques of the Nitrogen-Vacancy Center in Diamond par David Hoper & Al, 2018 (30 pages).

[698] Environ 1,1% des atomes de carbone du diamant sont d'isotope ^{13}C. L'isotope le plus courant est le ^{12}C. Le ^{14}C est présent à l'état de trace et sert à dater les objets carbonés grâce à sa demi-vie de 5730 ans. Voir Coherent control of an NV− center with one adjacent ^{13}C par Burkhard Scharfenberger et al, 2014 (24 pages).

Il est intégré dans un circuit fabriqué sur un wafer de silicium SOI avec une couche d'isolant SiO_2. Il est recouvert d'une lentille à base d'une matrice permettant de bien focaliser le laser de contrôle et de lecture d'état[699].

Pour poursuivre l'explication du fonctionnement de ces qubits un peu complexes, voici un diagramme des niveaux d'énergie de la cavité et de ses électrons libres. Chaque barre horizontale représente un niveau d'énergie.

Les flèches verticales représentent les transitions énergétiques importantes. Vers le haut, après réception d'un photon issu d'un laser ayant la longueur d'onde indiquée. Cela génère soit un changement d'état qui dégénère ensuite via l'état ^1A dans une transition spontanée non radiative qui n'émet pas de photon mais transmet une énergie mécanique à la structure cristalline et revient à l'état de base $|0\rangle$, soit une émission d'un photon d'énergie inférieure dans le rouge, une part de l'énergie étant également absorbée mécaniquement par la structure du diamant. La présence ou l'absence de ces photons rouges permet d'identifier l'état du qubit à $|0\rangle$ (photon rouge) ou $|1\rangle$ (pas de photon rouge).



Les qubits NV centers fonctionnent à température ambiante sur le papier[700]. En pratique on utilise une température de 4K, qui est loin d'être ambiante. Dans le grand froid, tout est relatif [701]! La raison est qu'à cette température, les raies spectrales des différents états énergétiques de la cavité sont différentes, mieux espacées et plus faciles à distinguer[702].

---

[699] Voir Spin Readout Techniques of the Nitrogen-Vacancy Center in Diamond par David Hoper et al, 2018 (30 pages).

[700] Voir A programmable two-qubit solid-state quantum processor under ambiant conditions par Yang Wu de l'USTC d'Hefei en Chine, 2018 (5 pages). Il décrit un NV center gérant deux qubits à température ambiante exploitant le spin des électrons de la cavité et du noyau de l'atome d'azote associé.

[701] La technique est notamment documentée dans Quantum information processing with nitrogen vacancy centers in diamond par Gang-Qin Liu et Xin-Yu Pan, 2018 (15 pages) ainsi que dans Diamond NV centers for quantum computing and quantum networks de Lilian Childress et Ronald Hanson, 2017 (5 pages).

[702] Cette interdépendance entre raies spectrales hyperfines et température n'est pas unique aux cavités de diamants. Elles sont courantes dans les structures cristallines car la température modifie plein de paramètres comme l'agencement relatif des atomes dans les cristaux qui conduit à modifier les gradients électriques et magnétiques et donc les spins, etc.

Cela réduit les erreurs de lecture de l'état des qubits. D'ailleurs, le schéma ci-dessus n'est pas forcément exact car il semble associer des données liées à la température ambiante comme l'émission d'infrarouge à 1042 nm lors de la mesure d'un qubit à l'état |1⟩.

Le principe général d'opération de ces qubits est le suivant [703]:

- L'**état quantique** du qubit utilise une base computationnelle à deux états, avec le |0⟩ correspondant au niveau de base d'énergie ^{3}A à spin nul et le |1⟩ à ce même niveau mais à spin non nul. Parfois, la base computationnelle est |+1⟩ et |-1⟩ correspondant aux deux niveaux de spin non nul de la base ^{3}A. Diverses techniques qui restent à creuser ici font aussi appel au spin du noyau de l'atome d'azote avoisinant et/ou à celui des atomes de ^{13}C proches. Ceux-ci servent à l'intrication entre qubits ainsi qu'à gérer de la mémoire quantique du fait de leur plus grande stabilité que l'état de spin de la cavité.
- Les **portes quantiques à un qubit** sont activées par micro-ondes et exploitent les transitions énergétiques hyperfines de fréquence 2,87 GHz[704]. Ces transitions fonctionnaient de concert avec un champ magnétique pour la zone A et un champ électrique pour la zone E. On utilise la combinaison dans la zone A pour modifier la combinaison d'états avec et sans spin par le phénomène de superposition.
- Les **portes quantiques à deux qubits** utilisent différentes méthodes : le couplage de NV centers par des photons intriqués, par un couplage magnétique, ou par le contrôle du spin du noyau des atomes de carbone ^{13}C avoisinants via l'usage de micro-ondes servant à créer une porte CNOT[705]. Par contre, je n'ai pas bien compris comment on pouvait ensuite scaler, par exemple, en couplant les spins de noyaux à d'autres NV centers dans le composant.
- La **mesure de l'état d'un qubit** utilise la captation de la fluorescence de la cavité activée par laser et avec un capteur CCD, un peu comme pour les ions piégés. Le principe général consiste à illuminer la cavité avec un laser à un niveau d'énergie élevé dans le vert (546 nm). Celui-ci va exciter le niveau ^{3}A en ^{3}E mais sans changer le spin. L'état ^{3}E de spin non nul va générer une transition non radiative passant par l'état ^{1}A. L'état ^{3}E de spin nul va générer l'émission d'un photon rouge de 689 nm qui sera détecté par le capteur CCD. En pratique, la mesure du spin de l'électron de la cavité peut exploiter différentes méthodes avec chacune leurs avantages et inconvénients : SCC (spin to charge conversion[706]), NMR (lecture assistée par le spin de noyau des atomes avoisinants) et uniquement par photonique, sachant que des lasers sont utilisés dans les trois cas.

La technologie n'est pas facile à industrialiser à grande échelle, qu'il s'agisse du chipset lui-même où des lasers de contrôle.

Les principaux pays impliqués sont la Chine (qui est partout), les Pays-Bas (TU Delft), l'Australie (Université de Melbourne), l'Allemagne (Université d'Ulm), le Japon (NII et NTT), certains laboratoires en France (comme le CEA SPEC) et bien entendu à différents endroits aux USA.

---

[703] Je me suis initialement inspiré d'un schéma de la lecture 3 du cours d'Hélène Perrin, février 2020. Puis ai intégré d'autres sources d'information. Voir notamment The nitrogen-vacancy colour centre in diamond par Marcus Doherty, Joerg Wrachtrup et al, 2013 (101 pages) qui décrit en particulier les variations de niveaux d'énergie des NV centers en fonction de leur température.

[704] Comme nous l'avons vu au sujet des ions piégés, les transitions hyperfines sont des transitions énergétiques d'électrons de faible niveau d'énergie, ici dans le régime des micro-ondes, qui sont en général liées à l'interaction entre les polarités magnétiques du noyau des atomes avec le champ magnétique généré par les électrons. Sachant qu'ici, on parle d'électrons qui ne tournent pas autour du noyau d'un atome mais dans une cavité.

[705] Voir quelques explications détaillées dans Colour centers in diamond par Joerg Wrachtrup, 2017 (36 slides).

[706] Expliqué en detail dans Spin readout via spin-to-charge conversion in bulk diamond nitrogen-vacancy ensembles par Harishankar Jayakumar, septembre 2018 (5 pages).

L'actualité « commerciale » sur les qubits à base de NV Centers n'est pas très riche depuis quelques années avec aucune startup positionnée dans le calcul quantique. Il y avait bien **QDTI** mais ils ne font maintenant que de la métrologie quantique. Il reste **Quantum Brilliance** (2019, Australie).

qubits NV centers

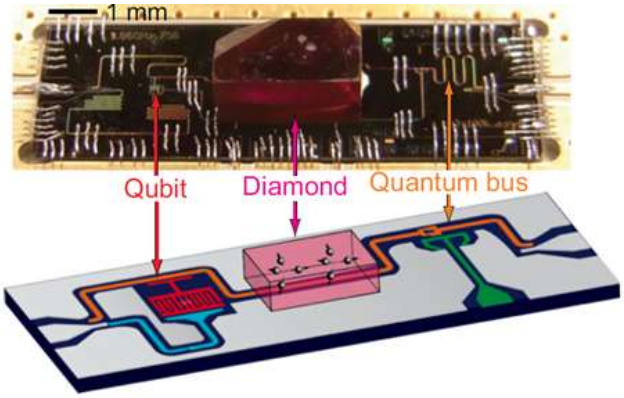
avantages

- **fonctionne à 4K** donc cryogénie plus simple.
- **temps de cohérence** assez long.
- **solidité mécanique** de la structure en diamant.
- les NV centers peuvent servir à créer de la **mémoire quantique auxilliaire** de qubits d'autres typer, comme des qubits supraconducteurs.

inconvénients

- **aucun acteur privé** investi dans les qubits à NV centers.
- **complexité des lasers de pilotage** de l'état des qubits => pas facile à rendre scalable.
- applications centrées sur la **magnétométrie quantique**.

Il semble en effet que les NV Centers aient des usages plus prometteurs en métrologie quantique pour la création de magnétomètres de précision ou pour créer de la mémoire quantique interopérable avec des qubits réalisés éventuellement dans d'autres technologies comme des qubits supraconducteurs dans des systèmes hybrides. C'est une piste explorée récemment par l'Université de Delft[707], au Japon[708] ainsi que par le CEA-SPEC avec Patrice Bertet[709] (schéma *ci-contre* de qubit supraconducteur lié à un qubit mémoire en NV center).



Il existe aussi des variantes de la technique des NV centers avec des défauts introduits dans du carbure de silicium dopé au phosphore qui présenteraient l'avantage de créer des qubits dont la mesure est plus précise car reposant sur l'émission d'une fluorescence de fréquence étroite[710].

Dans la même veine, le **MIT** prototypait en 2020 un chipset associant des NV Centers qui remplacent l'azote par du silicium et du germanium. Ils atteignent 128 qubits mais ces qubits ne sont pas encore opérationnels[711].

Topologique

Il faut distinguer dans cette catégorie d'ordinateurs quantique la notion de "topologique" qui définit un type de qubits à base d'anyons et les "fermions de Majorana" qui sont une variante d'anyons pour créer des qubits topologiques.

De tous les types de qubits, ce sont les plus mystérieux et complexes à appréhender, et donc à vulgariser en langage naturel. On nage en pleine méta-complexité [712]!

---

[707] Voir Diamond-based 10-qubit register with coherence more than one minute, novembre 2019.

[708] Voir Coherent Coupling between a Superconducting Qubit and a Spin Ensemble par Shiro Saito et al, 2012 (7 pages).

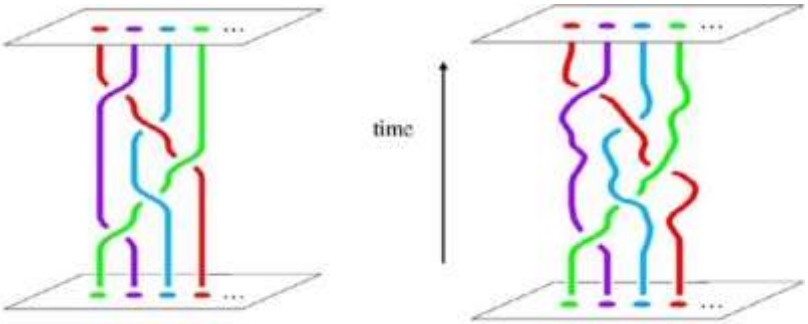
[709] Voir Quantum technologies with hybrid systems, Patrice Bertet et al, 2015 (8 pages).

[710] Voir Study Takes Step Toward Mass-Producible Quantum Computers, 2017.

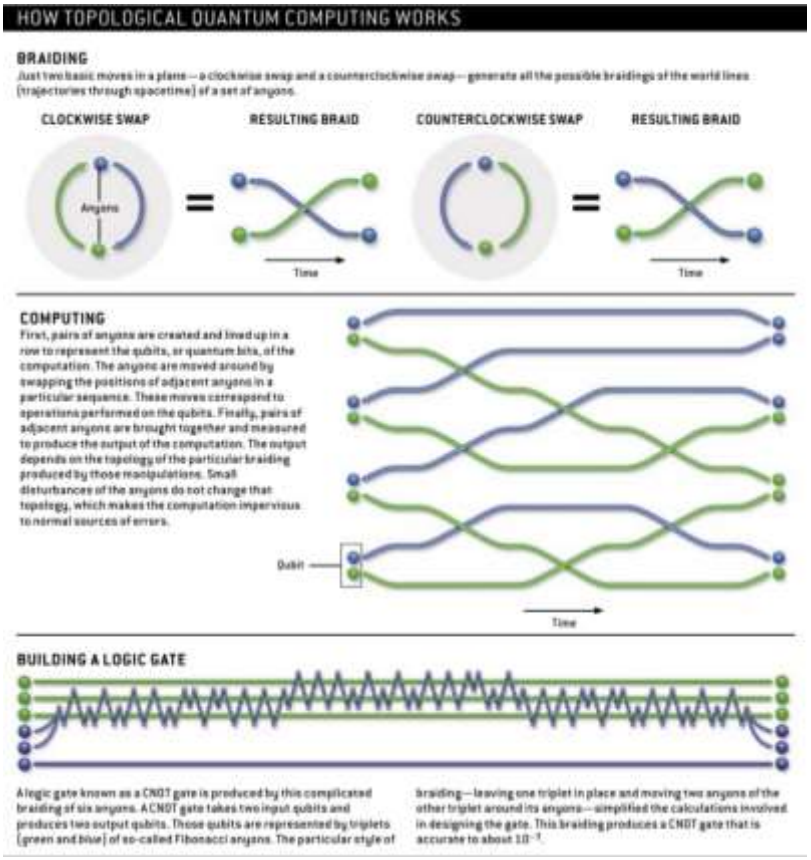
[711] Voir Large-scale integration of artificial atoms in hybrid photonic circuits par Noel H. Wan et al, Nature, 2020.

Le principe du calcul quantique topologique repose sur la notion d'anyons qui sont des "quasi-particules" intégrées dans des systèmes à deux dimensions. Sachant qu'il y a des anyons abéliens et non abéliens ! Les anyons sont des structures physiques asymétriques et à deux dimensions dont la symétrie peut être modifiée. Cela permet d'appliquer des principes de topologie avec des ensembles de permutations successives appliquées aux couples d'anyons qui se trouvent à proximité dans des circuits[713].

Les algorithmes s'appuient sur les concepts d'organisations topologiques de tresses ou de nœuds ("braids"). La représentation *ci-contre* explique cela, avec une évolution temporelle des permutations d'anyons temporelle allant du bas vers le haut sachant que dans d'autres représentations, elle va de haut en bas[714].



Le schéma suivant précise un peu les choses[715]. On y apprend notamment que les portes quantiques topologiques nécessitent un long enchaînement de permutations anyoniques comme avec la porte CNOT présentée en bas du schéma. Le tout, en conservant bien les notions de superposition et d'intrication ! C'est **Alexei Kitaev**, à l'époque chercheur chez Microsoft, qui eut cette idée en 1997 d'utiliser des anyons pour des calculs quantiques.



D'un point de vue physique, les anyons sont des "quasi-particules", à savoir des modèles de représentation de particules qui décrivent l'état de nuages d'électrons autour d'atomes (pour faire simple). Les fermions de Majorana sont un type spécifique de quasi-particules.

---

[712] Voir Topological Quantum Computing par Torri Yearwood, janvier 2020 et A Short Introduction to Topological Quantum Computation par Ville Lahtinen et Jiannis K. Pachos, mai 2017 (44 pages).

[713] Voir Le spectre de Majorana - Des quasi-particules exotiques découvertes dans des nanostructures supraconductrices pourraient servir à construire un ordinateur quantique par Manuel Houzet (CEA), Julia Meyer (UGA) et Pascal Simon (LPS CNRS), dans Reflets de la Physique 61, 2018 (7 pages).

[714] Des qubits topologiques pourraient être aussi réalisés en architecture à base de photonique. Voir New photonic chip promises more robust quantum computers, septembre 2018, qui associe des chercheurs en Australie, en Italie et en Suisse.

[715] Le schéma est issu de Computing with Quantum Knots par Graham Collins, Scientific American, 2006 (8 pages).

Ils ont des comportements collectifs d'électrons dans des réseaux cristallins à très basse température[716].

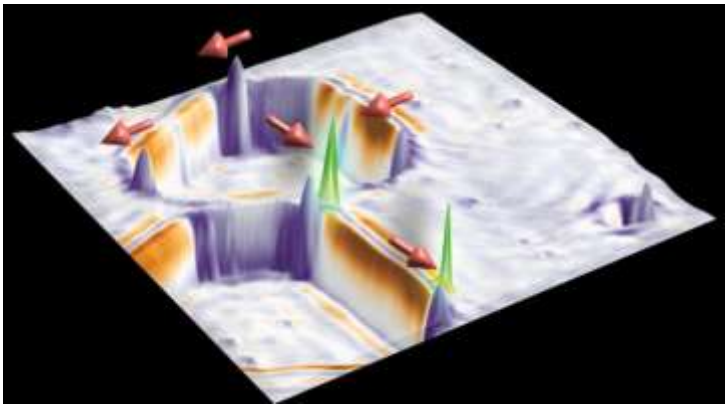
La complexité du sujet pourrait déclencher une véritable onde de choc dans l'enseignement de l'informatique car ces concepts associent mathématiques, physique et informatique à un niveau doctorat[717]. On est loin de l'Ecole 42 !

Pour comprendre le topologique et les fermions de Majorana, il faut se replonger dans le bestiaire de la physique des particules. Les fermions sont les particules de la matière et comprennent les leptons (électrons, neutrinos) et les baryons (protons, neutrons, à base de quarks) et qui composent les noyaux des atomes.

Les fermions de Majorana en sont un cas particulier qui correspondent à une sorte d'état de nuages d'électrons autour du noyau d'atomes et qui se manifestent aux deux bouts de fils supraconducteurs. Un débat court chez les physiciens sur l'existence même de ces fermions. Leo Kouwenhoven des Delft Lab (puis MSR) annonçait la détection de quasi-particules en 2012 à TU Delft[718].

Cette découverte était ensuite confirmée en 2016 au MIT. En 2018, un groupe de trois universités américaines UC Irvine, UCLA et Stanford aurait découvert de vrais fermions de Majorana[719].

En mai/juin 2019, des chercheurs allemands et autrichiens auraient réussi à créer des phénomènes topologiques assimilables à des fermions de Majorana dans deux dimensions, mais on est encore loin de leur usage dans un ordinateur quantique[720]. Il en va de même de chercheurs de Princeton qui publiaient en juin 2019 les résultats de travaux les ayant mené à contrôler l'état d'une quasi-particule[721].



En août 2019, des physiciens du NIST conduits par Nick Butch annonçaient la découverte par hasard de propriétés intéressantes du ditellurure d'uranium (UTe_2). Il serait supraconducteur à 1,7K avec la capacité de le faire via des paires de Cooper avec des spins identiques en plus de spins opposés, permettant d'avoir trois types de paires. Cela lui procurerait une rare capacité d'avoir une supraconductivité résistante aux flux magnétiques.

---

[716] L'explication, en français, la plus proche de la notion de compréhension humaine est ce bel article Le spectre de Majorana de Manuel Houzet, Julia Meyer et Pascal Simon dans Reflets de la Physique #61, 2018 (7 pages).

[717] C'est la thèse de Hugo de Garis dans Topological Quantum Computin The TQC Shock Wave and its Impact on University Computer Science Teaching, 2011 (29 pages).

[718] Certains résultats sont cependant sujets à caution. Le papier Quantized Majorana conductance par Leo Kouwenhoven et al, 2017 (26 pages) a été suivi d'une « expression of concern » des auteurs mettant en garde les lecteurs au sujet de la véracité des résultats publiés, ceux-ci n'étant pas reproductibles à cause d'un problème de calibrage des instruments de mesure. Il est possible que le papier doive être retiré.

[719] La source française de cette annonce Une particule théorique pour créer un ordinateur quantique impossible à hacker (2018) illustre au passage la difficulté de vulgariser le domaine. Les inexactitudes et approximations y sont énormes. En effet, le hacking d'ordinateur quantique n'est pas plus facile avec des fermions de Majorana qu'avec la totalité des autres technologies de qubits. Le hack, s'il a lieu, sera d'ailleurs toujours possible au niveau de l'indispensable ordinateur traditionnel qui pilote le processeur quantique.

[720] Voir Computing Faster With Quasi-Particles, mai 2019.

[721] Voir Mysterious Majorana Quasiparticle Is Now Closer To Being Controlled For Quantum Computing, juin 2019 qui fait référence à Observation of a Majorana zero mode in a topologically protected edge channel, de Ali Yazdani et al, Science, juin 2019 (12 pages).

Ce matériau aurait ainsi des propriétés topologiques dans ce cadre permettant de créer des qubits topologiques plus stables et moins sujets à la décohérence[722]. Des travaux voisins avaient été publiés par des chercheurs de la John Hopkins University en 2018 avec des qubits topologiques supraconducteurs réalisés en alliage de bismuth et de palladium[723].

L'actualité scientifique est continue autour de fermions de Majorana que l'on découvre, croit découvrir ou redécouvre selon les cas, sur de l'or[724], à la surface de nanofils supraconducteurs[725] ou dans des cristaux[726], sans compter d'autres publications pas évidentes à analyser[727], tout cela en 2020. C'est encore largement un champ de la physique fondamentale. Il est d'ailleurs l'objet de débats, certains physiciens puristes remettant régulièrement en question les découvertes de fermions de Majorana qui n'en seraient pas.

Nous avons vu que différents laboratoires de physique travaillent sur le sujet, notamment aux USA, en Chine, aux Pays-Bas, au Danemark et aussi en France. On y trouve notamment une équipe à l'IRIG du CEA à Grenoble (Manuel Houzet, Julia Meyer et Xavier Waintal), Hugue Pothier au CEA de Saclay et Pascal Simon au LPS d'Orsay.

Ils ne travaillent pas sur les fermions de Majorana mais sur la matière topologique au niveau fondamental et notamment sur les états d'Andreiv, les états liés et la physique des liens faibles, différents domaines qui restent à explorer dans ces lignes. Certains de ces chercheurs mènent des projets conjoints avec TU Delft.

qubits fermions de Majorana

avantages

- **qubits théoriquement très stables** et nécessitant peu de correction d'erreurs.
- **temps de cohérence long et rapidité des portes** permettant de traiter des algorithmes « profonds ».
- **scalabilité potentielle** des qubits, construits a priori avec des techniques voisines de celles qubits silicium.
- les recherches pourraient aboutir en utilisant des états topologiques de la matière différents des fermions de Majorana.

inconvénients

- on n'a **pas encore vu** la peau d'un qubit à base de fermion de Majorana.
- la **programmation de qubits topologique différente** des qubits universels classiques à bas niveau.
- **peu de laboratoires** impliqués dans cette voie.
- **aucune startup** ne s'est lancée sur ce créneau, Microsoft est le seul acteur privé.
- fonctionne à **basse température cryogénique** <20 mK comme les qubits supraconducteurs.

[722] Voir Newfound Superconductor Material Could Be the 'Silicon of Quantum Computers' Possible "topological superconductor" could overcome industry's problem of quantum decoherence, août 2019, qui fait référence à Nearly ferromagnetic spin-triplet superconductivity par Sheng Ran et al, 2019.

[723] Voir Observation of half-quantum flux in the unconventional superconductor β-Bi2Pd par Yufan Li & Al, octobre 2018 (12 pages).

[724] Voir Quantum Computing Breakthrough: First Sighting of Mysterious Majorana Fermion on Gold par Jennifer Chu, MIT, Indian Institute of Technology, University of California & Hong Kong University, 2020. Et Voir Signature of a pair of Majorana zero modes in superconducting gold surface states, par Sujit Manna et al, MIT, 2019 (35 pages).

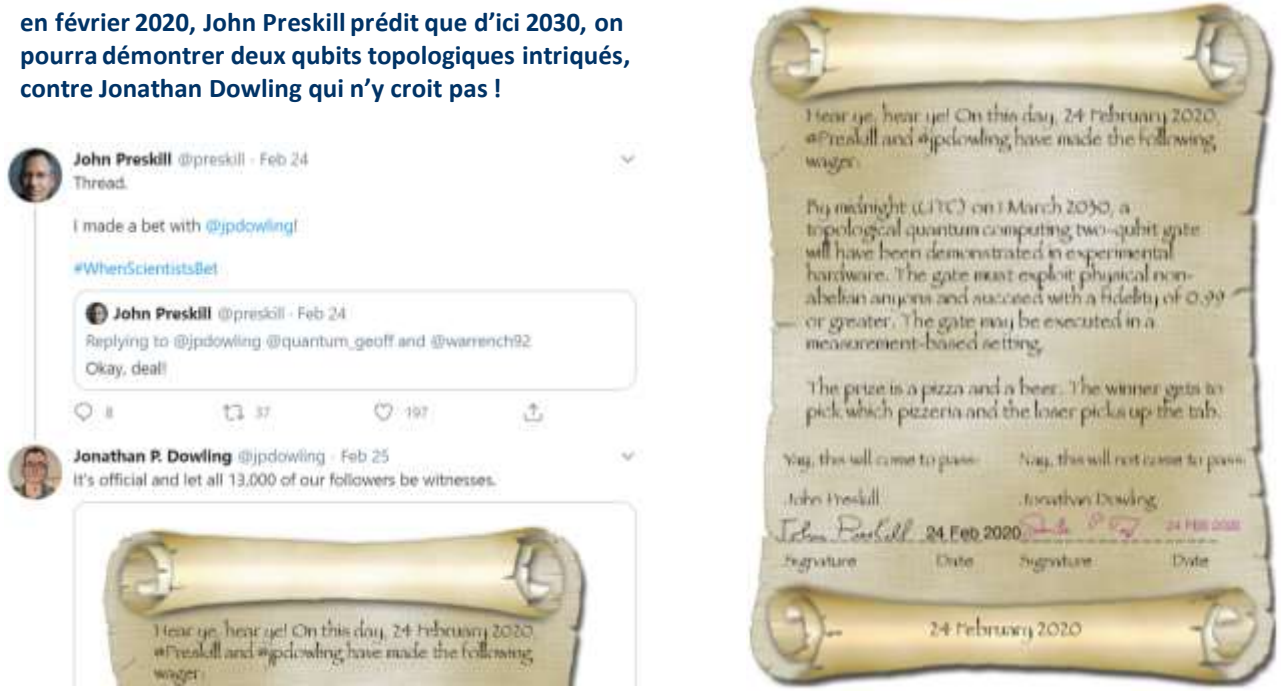
[725] Voir Alternative route to topological superconductivity Hub, avril 2020. Université de Copenhague en collaboration avec Microsoft. Fait référence à Flux-induced topological superconductivity in full-shell nanowires par S. Vaitiekėnas et al, mars 2020 (38 pages).

[726] Voir Building block for quantum computers more common than previously believed par Chanapa Tantibanchachai, Johns Hopkins University, avril 2020.

[727] Voir The observation of photon-assisted tunneling signatures in Majorana wires par Ingrid Fadelli, mai 2020, Quantum computers do the (instantaneous) twist par Chris Cesare, août 2020 sur un système de correction d'erreurs topologique et Fractional statistics of anyons in a two-dimensional conductor, C2N, avril 2020.

Avec cela en tête, voyons où en sont les deux acteurs principaux de ce domaine, Microsoft et Nokia. Leur investissement parallèle n'ayant rien à voir avec la mésaventure dans les smartphones qui a relié les deux marques il y a quelques années.

Les paris restent ouverts pour savoir si le quantique topologique verra le jour et sauvera Microsoft. En février 2020, **John Preskill** (père des notions de suprématies quantiques et de NISQ) prédisait que d'ici 2030, on pourra démontrer deux qubits topologiques intriqués, contre **Jonathan Dowling** (photonicien) qui de son côté n'y croit pas du tout ! L'objet de ce pari symbolique ? Une bonne bière avec une pizza. Manque de bol, Jonathan Dowling est décédé le 5 juin 2020 et ne pourra donc pas voir s'il a gagné son pari en 2030.



Microsoft Research planche sur le quantique topologique et les fermions de Majorana depuis pas mal n'années mais n'a pas encore de prototype à ce stade. Microsoft fait un pari de s'appuyer sur une particule virtuelle dont on n'a pas encore véritablement vérifié l'existence. C'est un pari très risqué, avec plein d'avantages stratégiques si cela fonctionne !

En effet, les qubits Majorana seraient bien plus fiables et générant moins d'erreurs (10^{-30}), avec comme implication, le fait que l'on pourrait se passer en partie des codes de correction d'erreurs utilisés avec les autres types de qubits comme les supraconducteurs ou au silicium[728].

[728] Voici quelques pistes pour en savoir plus : Microsoft prêt à bâtir un ordinateur quantique de Juliette Raynal, en 2016 !, A Software Design Architecture and Domain-Specific Language for Quantum Computing 2014 (14 pages), Quantum Computing at Microsoft (56 slides) et Quantum Computing Research at Microsoft (59 slides) de Dave Wecker et A short introduction to topological quantum computation de Ville Lahtinen et Jiannis Pachos, 2017, (43 pages). Et quelques vidéos : keynote de novembre 2017 avec notamment Leo Kouwenhoven (43 mn), conférence Build de mai 2018 sur Q# (1h15mn) et Majorana qubits de Xiao Hu, en mai 2017 (22 mn).

Médaille Fields en 1986 pour ses travaux sur la conjecture de Poincaré, **Michael Freedman** de l'Université de Santa Barbara rejoint Microsoft en 1997. Il démontre avec Alexei Kitaev la possibilité de faire du quantique avec une particule hypothétique, le fermion de Majorana, conceptualisé en 1937 par l'Italien Ettore Majorana à partir de la résolution d'équations mathématiques de Dirac[729]. Ce fermion est une particule étrange, dont la charge et l'énergie sont nulles et qui est sa propre antiparticule.

Freedman et Kitaev seront recrutés par Microsoft Research. Piloté par Michael Freedman, Microsoft Quantum Santa Barbara (Station Q) est installé sur le campus de l'Université de Santa Barbara en Californie d'où il vient. Le tout est complété par l'équipe de Leo Kouwenhoven de Delft Lab aux Pays-Bas et de Charles Marcus du Niels Bohr Institute qui rejoignent Microsoft Research. Microsoft valorise ainsi des résultats de la recherche européenne et américaine.

Ettore Majorana
1906-1938

fermions théorisés en 1937, particule virtuelle sans énergie ni charge qui est sa propre antiparticule

Michael Freedman et Alexei Kitaev
MSR

publient « Topological Quantum Computation » en 2002, jetant les bases de l'informatique quantique topologique

Leo Kouwenhoven
Delft Lab puis MSR

détection de quasi-particules en 2012 à TU Delft puis en 2016 au MIT

Charles M. Marcus
Niels Bohr Institute et MSR

mise au point des qubits à base de quasi-particules

Les fermions de Majorana sont en fait des comportements étranges d'électrons et de leur spin que l'on trouve aux deux bouts de fils supraconducteurs. Ils opèrent donc aussi à très basses températures, comme pour les qubits supraconducteurs et silicium, à environ 15-20 mK[730]. Vus de près, ces qubits sont des variantes sophistiquées de qubits supraconducteurs. Ces associations "topologiques" en mailles apportent une protection contre la décohérence des qubits car la forme des tresses importe peu tant que leur topologie est stable.

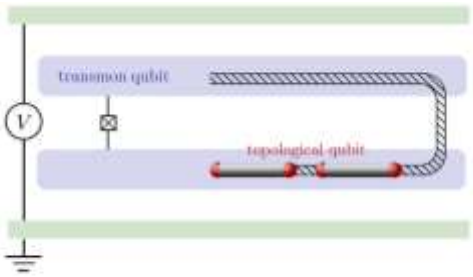


Fig. 6: *Read out of a parity qubit in a Cooper pair box. Two superconducting islands (blue), connected by a split Josephson junction (crosses) form the Cooper pair box. The topological Majorana qubit is formed by four Majorana fermions (red spheres), at the end points of two undepleted segments of a semiconductor nanowire (striped ribbon indicates the depleted region). A magnetic flux Φ enclosed by the Josephson junction controls the charge sensitivity of the Cooper pair box. To read out the topological qubit, two of the four Majorana fermions that encode the logical qubit are moved from one island to the other. Depending on the quasiparticle parity, the resonance frequency in a superconducting transmission line enclosing the Cooper pair box (green) is shifted upwards or downwards by the amount which is exponentially small in E_J/E_C.*

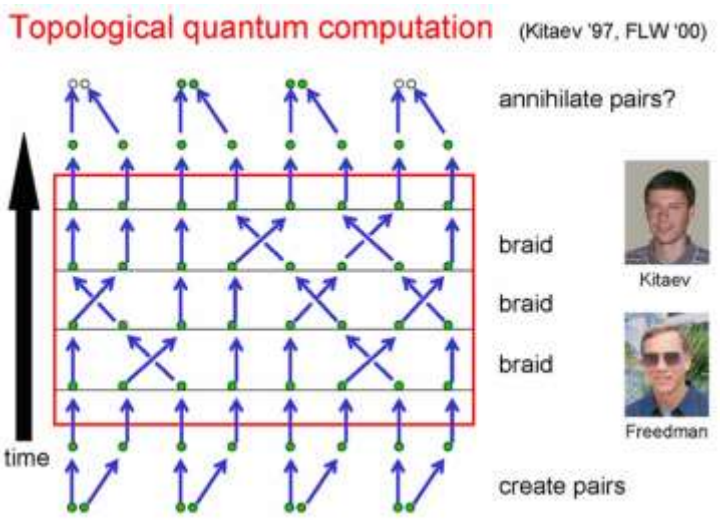
[729] Dans Topological Quantum Computation publié en 2002 et mis à jour en 2008 (12 pages).

[730] Source du schéma : Majorana Qubits de Fabian Hassler, 2014 (21 pages).

Microsoft annonçaient à la conférence Build de mai 2018 qu'ils sortiraient leur premier ordinateur quantique à base de fermions de Majorana en 2023, ce qui est un peu loin, surtout dans la mesure où ils ne précisent pas le nombre de qubits associés. Ils communiquent déjà de manière institutionnelle pour occuper le terrain[731].

En 2023, les prévisions de marché des ordinateurs quantiques sont autour de $1,9B, ce qui n'est pas grand-chose et est déjà pas mal compte-tenu de sa maturité actuelle[732].

Microsoft a évidemment aussi investi côté logiciels, d'abord avec sa plateforme Liquid, puis avec F# pour le scripting et avec le langage Q# servant à la programmation quantique, lancé fin 2017. L'une des contributrices de ces efforts est la chercheuse Krysta Svore qui vient de l'Université de Columbia. A noter que Microsoft a recruté en 2018 un certain **Helmut Katzgraber**, l'un des apôtres du recuit quantique façon D Wave ainsi que du MBQC (measurement based quantum computers)[733].



	Realizations	Lifetimes	Gate Speed
supraconducteurs	Topological (Majorana)	1 minute	Nanoseconds
supraconducteurs	Flux Qubit	/ 10^{10}	same
supraconducteurs	Charge Qubit	/ 10^{10}	same
supraconducteurs	Transmon	/ 10^{7}	same
	Ion Trap	/ 10^{2}	10^{3} slower

qubits plus stables
faible bruit de décohérence
peu d'erreurs
temps de decohérence long
rapidité des portes

rien démontré
prototype en cours de réalisation
algorithmes différents

NOKIA

Les Bell Labs de Nokia aux USA, situés à Murray Hill dans le New Jersey, travaillent aussi sur le topologique mais sont relativement discrets sur le sujet[734]. Nokia soutient aussi l'initiative Quopal de l'Université d'Oxford sur l'usage du quantique dans le machine learning.

Au passage, Nokia aime à rappeler que les algorithmes de Grover et Shor ont été découverts par leurs créateurs dans les Bell Labs. Et logiquement, Nokia planche aussi sur la cryptographie quantique, au moins au niveau de son transport sur fibres optiques comme en témoigne ce partenariat avec le Coréen SK Telecom de 2017.

Mais les nombreuses difficultés économiques de Nokia ne présagent rien de très enthousiasmant sur ces différentes recherches qui risquent bien de passer à la trappe des restructurations, si ce n'est pas déjà fait !

---

[731] Voir cette publicité vidéo : Introducing Quantum Impact (Ep. 0), février 2020 (4 minutes).

[732] Source du schéma : http://online.kitp.ucsb.edu/online/plecture/preskill/oh/140.html, par John Preskill.

[733] Voir Quantum Driven Classical Optimizations, août 2018 (vidéo de 28 mn).

[734] Voir Quantum computing using novel topological qubits at Nokia Bell Labs publié en 2017 qui décrit leur approche dans le topologique sachant qu'aucune roadmap n'est communiquée.

Ions piégés

Les ions piégés sont des atomes ionisés positivement qui sont piégés magnétiquement et/ou par des électrodes dans un espace confiné, et placés les uns à côté des autres. Les éléments utilisés sont généralement des métaux alcalins de la seconde colonne du tableau de Mendeleïev (dite « Group IIA » dans la notation de Mendeleev ou groupe 2 dans la notation moderne, avec le bérylium, le magnésium, le strontium, le baryum et surtout le calcium), puis comme l'ytterbium qui est une terre rare de la famille des lanthanides ou même le mercure, et enfin, plus rarement, les métaux du groupe IIB ou 12 (zinc, cadmium, mercure).

qubits ions piégés

avantages

- **ions parfaitement identiques** => pas besoin de calibrage.
- **bonne stabilité des qubits** avec faibles taux d'erreur.
- **long temps de cohérence** et ratio élevé entre temps de cohérence et durée des portes => supporte des algorihmes profonds en nombre de portes.
- **intrication** possible entre tous les qubits sur les architectures 1D.
- fonctionne à **température « clémente » de 4K à 10K** => cryogénie plus simple que pour les supraconducteurs.
- **intrication avec des photons** aisée pour des communications longue distance.

inconvénients

- pas évident à faire **scaler** au-delà d'une cinquantaine de qubits => mais architectures 2D prometteuses, notamment chez Honeywell.
- **calcul relativement lent** du fait de portes quantiques lentes => problème avec les algorithmes "profonds" comme celui de Shor.
- ions fonctionnant dans de l'**ultra-vide**… mais qui n'est pas difficile à obtenir.

La technologie des qubits à ions piégés a été imaginée dans les années 1950 par **Wolfgang Paul**, prix Nobel de physique en 1989. Les premiers à les tester, en 1995, furent **Juan Cirac** et **Peter Zoller** de l'Université d'Innsbruck en Autriche[735].

VOLUME 74, NUMBER 20 PHYSICAL REVIEW LETTERS 15 MAY 1995

Quantum Computations with Cold Trapped Ions

J. I. Cirac and P. Zoller*

Institut für Theoretische Physik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria

(Received 30 November 1994)

A quantum computer can be implemented with cold ions confined in a linear trap and interacting with laser beams. Quantum gates involving any pair, triplet, or subset of ions can be realized by coupling the ions through the collective quantized motion. In this system decoherence is negligible, and the measurement (readout of the quantum register) can be carried out with a high efficiency.

PACS numbers: 89.80.+h, 03.65.Bz, 32.80.Pj

Le principe général de ces qubits est le suivant [736]:

- Des **lasers** sont utilisés pour refroidir et stabiliser les ions, en exploitant notamment l'effet Doppler, mais un effet qui utilise des transitions énergétiques des atomes différentes de celles qui permettent de modifier l'état des qubits.
- Les **ions sont confinés** sous vide de différentes manières par un champ magnétique et/ou électrique. Ils sont placés dans une enceinte sous **ultra-vide**.
- L'**état quantique** du qubit correspond à deux niveaux d'énergie relativement stables de l'ion piégé.
- Les **portes quantiques à un qubit** sont activées par micro-ondes, par lasers ou par des dipôles magnétiques.

[735] Voir Trapped-Ion Quantum Computing: Progress and Challenges par Colin Bruzewicz et al du MIT, avril 2019 (56 pages). C'est une revue de l'état de l'art très bien documentée sur la technologie des ions piégés. Et l'article fondateur Quantum Computations with Cold Trapped Ions par Juan Cirac et Peter Zoller, 1995 (4 pages).

[736] Voir cette intéressante synthèse dans Introduction to Trapped-Ion Quantum Computing par Gabriel Mintzer du MIT, février 2020.

- Les **portes quantiques à deux qubits** utilisent des lasers avec des photons intriqués ou bien des électrodes. Ils peuvent notamment exploiter le phénomène des phonons qui relie les atomes entre eux par des vibrations qui se propagent de proche en proche, ce qui est valable pour les qubits alignés dans des pièges de Paul linéaires.
- La **mesure de l'état d'un qubit** utilise la captation de la fluorescence de la cavité avec un capteur CCD après excitation des ions par un laser. Les ions excités correspondant à l'état $|1\rangle$ sont visibles tandis que les ions non excités correspondant à l'état $|0\rangle$ ne le sont pas.

Une centaine d'équipes de recherche dans le monde travaillent sur des qubits à ions piégés dans quasiment tous les pays travaillant sur les technologies quantiques (Australie, Autriche, Canada, Chine, Danemark, Finlande, France, Allemagne, Inde, Israël, Japon, Pays-Bas, Singapour, Suisse, Royaume-Uni, USA). L'Autrichien Rainer Blatt de l'**Université d'Innsbruck** est un des pionniers de cette filière. Il créé un registre intriqué de 14 qubits adressables en 2011 et passait à 20 qubits adressables et individuellement contrôlables en 2018, à base d'ions calcium. Rainer Blatt a créé la startup **Alpine Quantum Technologies** (2017, Autriche) et y a caractérisé jusqu'à 10 qubits à ions piégés de très bonne qualité. La voie de la simulation quantique avec des ions piégés, mettant en œuvre des modèles d'Ising comme avec les D-Wave est aussi poursuivie par certains laboratoires comme à l'ETH Zurich ou à l'Université de Maryland et ailleurs aux USA[737].

Les ions piégés ont un temps de cohérence assez long, de plusieurs dizaines de secondes, mais c'est compensé par des *gate time* tout aussi longs en proportion. Le ratio entre temps de cohérence et gate time est cependant très bon, de 10^6 alors qu'il est de 10^3 pour les qubits supraconducteurs et d'environ 200 pour les qubits à base d'atomes froids.

Ils présentent l'avantage de générer un taux d'erreur assez faible avec jusqu'à 99,9999% de fidélité pour des portes à un qubit et 99,9% pour des portes à deux qubits (voir le tableau de synthèse *ci-dessous* qui illustre ces fidélités selon la méthode de gestion des portes quantiques et les ions utilisés). Cela permet d'exécuter en théorie des algorithmes « profonds » avec un grand nombre de portes quantiques et d'obtenir un bon volume quantique pour reprendre la terminologie d'IBM. Ce taux d'erreur augmente cependant avec l'accroissement du nombre de qubits, en tout cas dans les archictures 1D.

Type	Method	Fidelity	Time (μs)	Species	Ref.
1-qubit	Optical	0.99995	5	$^{40}Ca^+$	Bermudez 2017
	Raman	0.99993	7.5	$^{43}Ca^+$	Ballance 2016
	Raman	0.99996	2	$^{9}Be^+$	NIST 2016
	Raman	0.99	0.00005	$^{171}Yb^+$	Campbell 2010
	Raman	0.999	8	$^{88}Sr^+$	Knaulman 2011
	μwave	0.999999	12	$^{43}Ca^+$	Harty 2014
	μwave		0.0186	$^{25}Mg^+$	Ospelkaus 2011

Adapted from Bruzewicz et al.

Type	Method	Fidelity	Time (μs)	Species	Ref.
2-qubit	Optical	0.996	–	$^{40}Ca^+$	Erhard 2019
(1 sp.)	Optical	0.993	50	$^{40}Ca^+$	Benhelm 2008
	Raman	0.9991(6)	30	$^{9}Be^+$	NIST 2016
	Raman	0.999	100	$^{43}Ca^+$	Ballance 2016
	Raman	0.998	1.6	$^{43}Ca^+$	Schafer 2018
	Raman	0.60	0.5	$^{43}Ca^+$	Schafer 2018
	μwave	0.997	3250	$^{43}Ca^+$	Harty 2016
	μwave	0.985	2700	$^{171}Yb^+$	Weidt 2017
2-qubit	Ram./Ram.	0.998(6)	27.4	$^{40}Ca^+/^{43}Ca^+$	Ballance 2015
(2 sp.)	Ram./Ram.	0.979(1)	35	$^{9}Be^+/^{25}Mg^+$	Tan 2015

source des schémas : lecture 1 de 77 slides du cours d'Hélène Perrin à l'Université Paris 13 en quatre parties, février 2020.

En général, les qubits peuvent être tous intriqués les uns avec les autres grâce à l'usage de phonons[738] mais cela dépend de la manière dont ils sont répartis dans l'espace. Dans les technologies de qubits supraconducteurs, seuls les qubits voisins d'un qubit donné peuvent être intriqués, ce qui créé des contraintes dans la conception et/ou la compilation d'algorithmes quantiques.

Les qubits étant des atomes, ils sont identiques et ne nécessitent pas des réglages de calibrage comme les qubits supraconducteurs dont les caractéristiques physiques sont variables d'un qubit à l'autre.

---

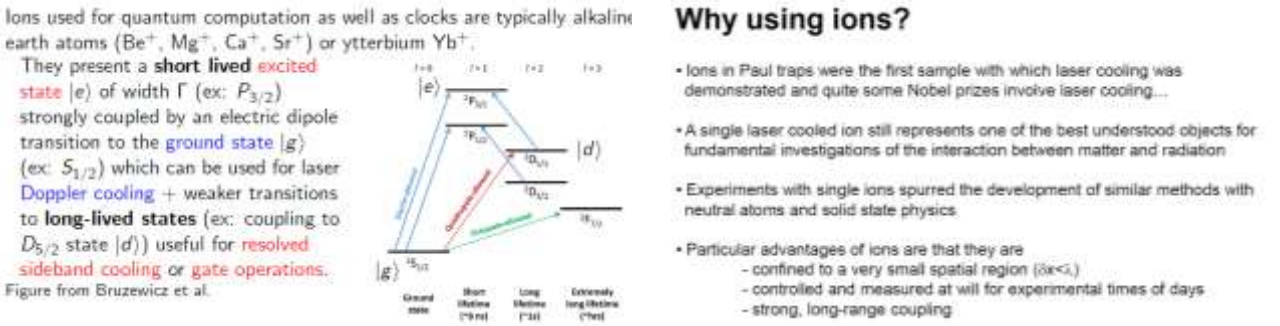
[737] Voir par exemple Digital Quantum Simulation with Trapped Ions par Kenny Choo et Tan Li Bing, 2016 (29 slides) et Programmable Quantum Simulations of Spin Systems with Trapped Ions par Christopher Monroe et al, 2019 (42 pages).

[738] Voir Benchmarking an 11-qubit quantum computer par Christopher Monroe et al, mars 2019 (8 pages).

Ces qubits sont censés opérer à température ambiante. En pratique, ce n'est pas vraiment le cas. Ils génèrent un effet gênant de montée en température, qui n'est pour l'instant pas totalement expliqué. Ceci requiert un refroidissement situé entre 4K et 10K[739]. L'intérêt d'un tel refroidissement est aussi d'améliorer les conditions de la mise sous ultra-vide des ions.

Les éléments utilisés pour les ions piégés sont le béryllium, le magnésium, le calcium, le strontium et l'ytterbium, les plus utilisés étant le calcium et l'ytterbium. Pourquoi utilise-t-on des ions et pourquoi s'appuie-t-on sur ces éléments ?

L'intérêt d'exploiter des ions est de permettre de les piéger magnétiquement ou avec des électrodes. On peut aussi les coupler à longue distance, de l'ordre de plusieurs dizaines de microns.



Les éléments utilisés ont plusieurs caractéristiques communes liées à leur configuration de couches d'électrons. Ils ont des niveaux d'excitation à partir de l'état de base (ground state) qui sont de courte durée et permettent leur usage pour le refroidissement des atomes par laser et effet Doppler. L'état énergétique de base correspondant au $|1\rangle$ et le niveau d'énergie correspondant à l'état $|0\rangle$ sont stables dans le temps, ce qui facilite les opérations de portes quantiques (détails *ci-dessus*)[740].

Il existe cinq grandes variantes d'usage de ces ions qui dépendent des transitions énergétiques utilisés pour gérer les deux états d'un qubit. À chacun de ces modes correspondent des fréquences de transition différentes qui sont utilisées pour modifier l'état des qubits :

- Les **qubits Zeeman** font appel à des ondes de quelques MHz avec un contrôle par champ magnétique. Ils y sont très sensibles mais permettent d'avoir des qubits avec un très faible taux d'erreur une fois ce champ bien contrôlé[741]. Ils sont plutôt utilisés en métrologie quantique car leur fréquence de contrôle est trop basse pour permettre un contrôle de précision de plusieurs qubits proches les uns des autres.
- Les **qubits à structure hyperfine** utilisent des micro-ondes de quelques GHz et des transitions Raman[742]. Cela s'applique aux ions dont le noyau a un spin non nul. Les autres cas concernent les ions à noyaux de spin nul, soit ceux dont le nombre de protons et de neutron sont tous les deux pairs. Cela explique pourquoi certains éléments comme le calcium sont parfois utilisés dans plusieurs de ces catégories, avec des isotopes différents comme le $^{40}Ca^+$ en qubits optiques et le $^{43}Ca^+$ en qubit de structure hyperfine[743]. Le nombre de neutrons dans ces ions modifie le spin du noyau des atomes et ses états d'énergie hyperfins.

---

[739] Voir Closed-cycle, low-vibration 4 K cryostat for ion traps and other applications par P. Micke et al, mai 2019 (15 pages) qui décrit un cryostat pour processeur à ions piégés, utilisant une tête pulsée.

[740] Source des schémas : lecture 1 de 77 slides du cours d'Hélène Perrin à l'Université Paris 13 en quatre parties, février 2020.

[741] Voir Comparing Zeeman qubits to hyperfine qubits in the context of the surface code: $^{174}Yb^+$ and $^{171}Yb^+$ par Natalie Brown, avril 2018 (7 pages).

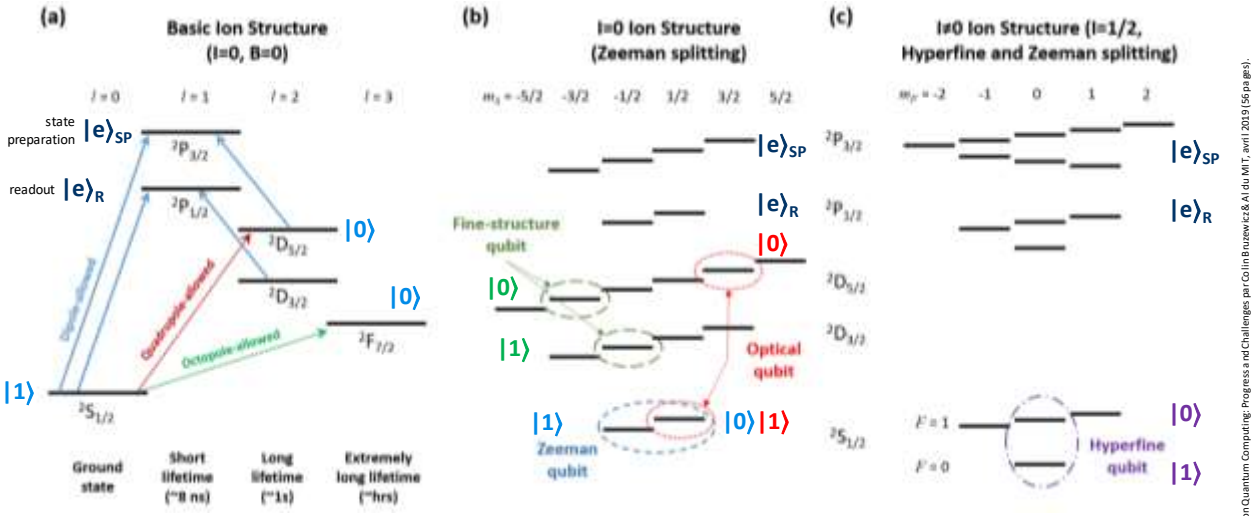
[742] Voir par exemple Controlling Qubits With Microwave Pulses Reduces Quantum Computer Error Rates, Increases Efficiency par Matt Swayne, 2020 qui fait référence à Robust and resource-efficient microwave near-field entangling 9Be+ gate par G. Zarantonello, novembre 2019 (6 pages).

[743] Schéma inspiré de : Quantum Computing with ions, F. Schmidt-Kaler, 2019 (40 slides).

- Les **qubits à structures fines** utilisent des ondes sous-millimétriques de quelques THz.
- Les **qubits optiques** utilisent des photons de quelques centaines de THz.
- Les **qubits Rydberg** utilisent des états énergétiques dits de Rydberg contrôlés par rayons ultra-violets de la catégorie VUV (vaccum ultra-violet) dans les longueurs d'onde de 122 nm[744].

Voici *ci-dessous* une explication de ces variantes basées sur les niveaux d'énergie des ions. Avec à gauche, une structure générique de niveaux d'énergie d'ions avec les transitions permettant le changement d'état du qubit et celles qui servent à préparer l'état du qubit ou à le lire.

Au milieu et à droite, les différentes transitions énergétiques utilisées pour définir les |0⟩ et |1⟩ du qubit. La hauteur entre le deux niveaux caractérise le niveau d'énergie qui sépare ces deux états. Plus il est grand, plus la fréquence utilisée pour modifier l'état du qubit est élevée, passant des ondes radio de quelques MHz aux ultra-violets extrêmes dans le cas des qubits Rydberg.



(a) **structure générique d'un ion piégé** :
- niveau énergétique de base $S_{1/2}$ = état |1⟩ du qubits.
- état |0⟩ excité en D (avec du Ca^+) ou F (avec de l'Yb^+) stable sur une durée longue ou très longue.
- quadrupole/octopole : type de système électrique de confinement des ions.
- états P de courte durée et utilisés par des lasers pour sa préparation ($|e\rangle_R$) et pour la mesure de son état ($|e\rangle_{SP}$).

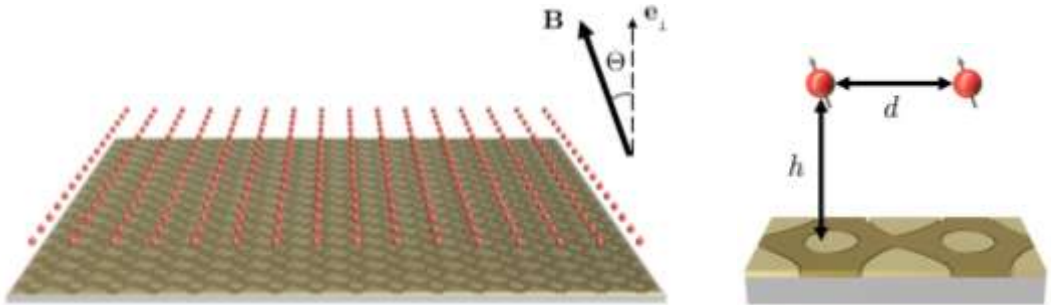
(b) **différents niveaux de base et excités**
- ces transitions entre |1⟩ et |0⟩ correspondent aux ions dont le noyau a un spin nul (cumul des moments magnétiques des neutrons et protons).
- plus l'écart vertical entre |1⟩ et |0⟩, plus le niveau d'énergie est élevé et la fréquence également, située entre quelques MHz (Zeeman), GHz (hyperfine), THz (fine), et 100s THz (optique).

(c) **autres niveaux de base et excités**
- ces transitions entre |1⟩ et |0⟩ correspondent aux ions dont le noyau a un spin non nul. D'où le fait qu'un même élément comme le calcium peut servir ici où dans le cas précédent, en fonction de l'isotope.

source schémas: Trapped-Ion Quantum Computing: Progress and Challenges par Colin Bruzewicz & Al du MIT, avril 2019 (56 pages).

La stabilisation dans l'espace des ions est réalisée de deux grandes manières avec des pièges à ions qui permettent de contrôler individuellement leur position :

- Par un **champ magnétique** et un **quadrupôle électrique** : ce sont les pièges de Penning (Penning traps, inventés en 1959). Ils sont notamment expérimentés à l'ETH Zurich et dans une version 2D qui présente l'intérêt d'être théoriquement scalable[745].



[744] Voir par exemple Speeding-up quantum computing using giant atomic ions par Stockholm University, avril 2020.

[745] Voir Scalable arrays of micro-Penning traps for quantum computing and simulation par S. Jain et al, avril 2020 (21 pages).

- Par un **champ électrique variable** : ce sont les pièges de Paul (Paul traps) du nom de Wolfgang Paul, prix Nobel de physique en 1989. Ces pièges sont soit linéaires en structure 1D (*ci-dessous* en (f)), soit mis à plat ce qui permet de créer des structures 2D. Ils sont les plus souvent utilisés. La version à plat correspond à la technique utilisée par Honeywell ainsi que chez IonQ.

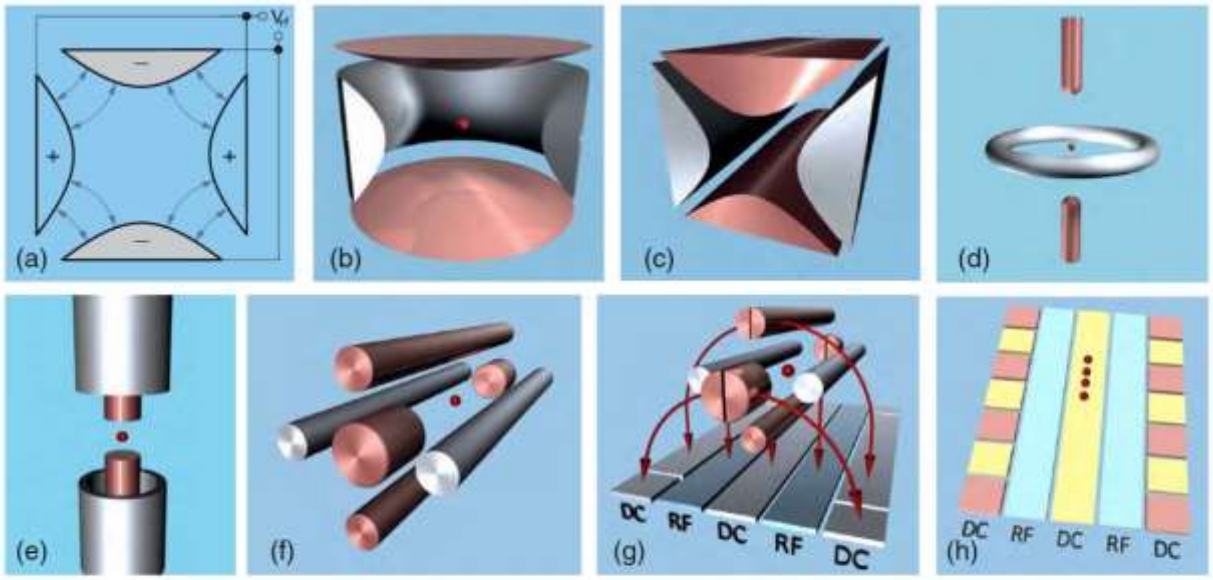


FIG. 2. (Reproduced from [68].) RF Paul trap geometries. (a) The basic concept of RF trapping, where quadrupolar fields oscillating at an RF frequency are produced using a set of (parabolic) electrodes. (b) The simplest cylindrically symmetric version of the basic RF trap. This is of the "ring and endcap" point-trap geometry. (c) The simplest translationally symmetric version of the basic RF trap. This will form a quadrupole mass filter and can be used to make a linear trap. (d,e) Topologically equivalent deformations of the geometry shown in (b). (f) Topologically equivalent deformations of the geometry shown in (c) with additional endcap electrodes added to form a four-rod, linear trap. (g) The four-rod trap in (f) may be deformed such that all electrodes reside in a single plane, forming a linear "surface-electrode trap." (h) A subset of the electrodes in a linear trap [a surface-electrode trap is depicted here, but segmentation may be applied to other linear trap geometries, such as that shown in (f)] may be segmented to allow trapping in multiple zones, along the axial direction.

Des lasers sont toujours utilisés et ils jouent plusieurs rôles : ils servent à refroidir les ions par effet Doppler et par « sideband cooling » pour ralentir les phonons (ce sont des vibrations inter-ions, sortes d'ondes de choc), pour initialiser l'état énergétique des qubits à |0⟩, pour réaliser des portes quantiques et enfin, pour lire l'état des qubits[746].

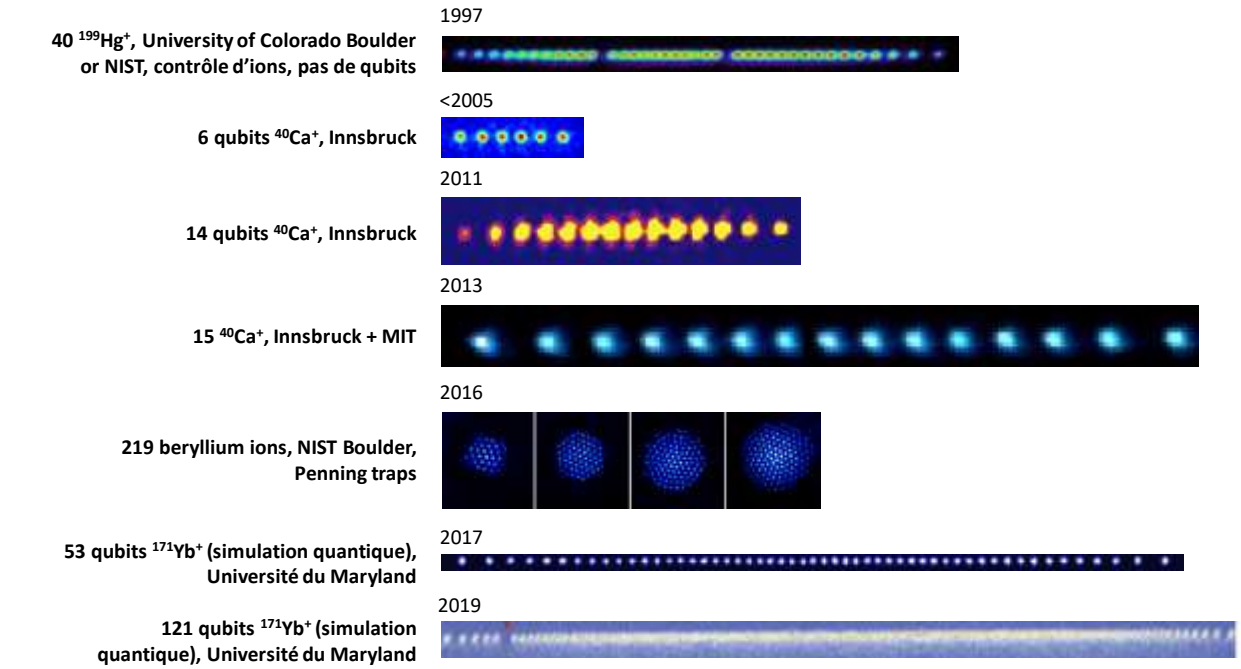
L'inconvénient principal est que la solution ne sera probablement pas facile à faire grandir en nombre de qubits confinés. Ne serait-ce que par le nombre de lasers à aligner pour leur contrôle et par l'espacement entre les ions alignés en rangs d'on-ions (facile…) qui est d'environ 2 à 5 µm. Enfin, la technique est difficile à miniaturiser à cause des systèmes de contrôles divers et à l'inexistence de lignes de production adaptées. Sauf lorsque les ions sont gérés par des électrodes comme le fait Honeywell. Nous allons examiner cette technologie prometteuse en détails un peu plus loin.

On n'est cependant pas à une exagération près, comme ces Autrichiens de l'Université d'Innsbruck et Suisses de l'ETH Zurich qui dans le projet **PIEDMONS** financé par l'Union Européenne (E2020) qui pensent rendre la technologie des ions piégés « portable », en oubliant le système de mise sous vide et le cryostat, nécessaires à leur fonctionnement[747]. Il ne suffit pas de miniaturiser le composant !

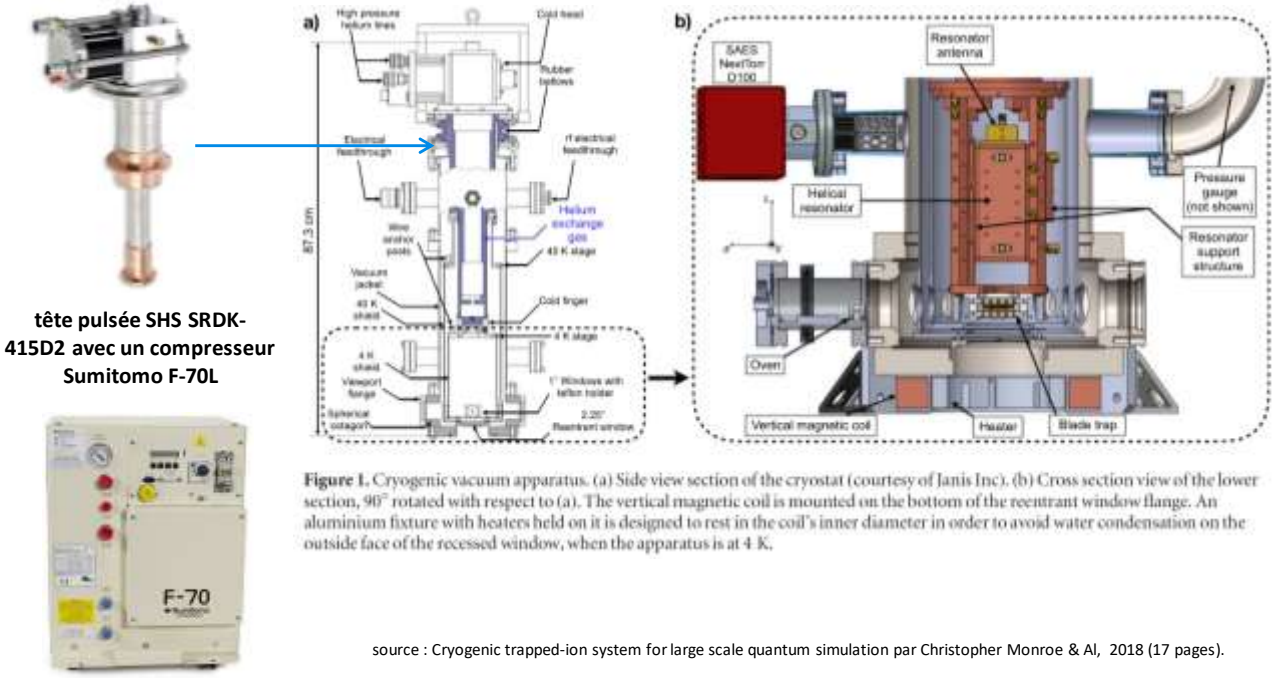
[746] Pour en savoir plus sur les détails d'activation des qubits à ions piégés, voir par exemple la présentation Quantum information processing with trapped ions de Christian Roos, 2012 (53 slides).

[747] Voir Quantum computers to become portable, août 2019.

Les ions piégés ont au moins deux autres utilités dans la périphérie du calcul quantique : la gestion de mémoires quantiques intermédiaires[748], et leur intégration dans des répéteurs quantiques pour des télécommunications quantiques sécurisées, notamment de clés quantiques via les protocoles de QKD.



Cela passe par des interactions entre ions piégés et photons, notamment via des cavités. On est déjà capable d'intriquer des ions piégés via une liaison photonique de plusieurs centaines de mètres (400 m à l'Université d'Innsbruck). Le tout permet d'envisager la création d'architectures de calcul distribuées[749].



tête pulsée SHS SRDK-415D2 avec un compresseur Sumitomo F-70L

Figure 1. Cryogenic vacuum apparatus. (a) Side view section of the cryostat (courtesy of Janis Inc). (b) Cross section view of the lower section, 90° rotated with respect to (a). The vertical magnetic coil is mounted on the bottom of the reentrant window flange. An aluminium fixture with heaters held on it is designed to rest in the coil's inner diameter in order to avoid water condensation on the outside face of the recessed window, when the apparatus is at 4 K.

source : Cryogenic trapped-ion system for large scale quantum simulation par Christopher Monroe & Al, 2018 (17 pages).

[748] Voir Single-qubit quantum memory exceeding 10-minute coherence time par Ye Wang (Chine), 2017 (6 pages).

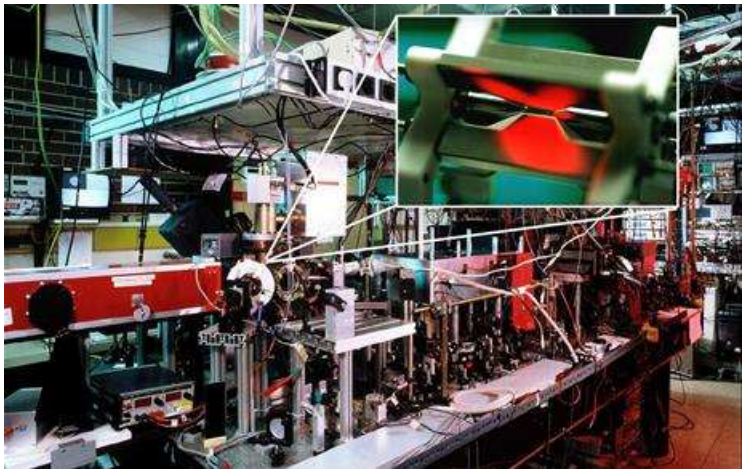
[749] Voir Large Scale Modular Quantum Computer Architecture with Atomic Memory and Photonic Interconnects par Christopher Monroe et al, 2014 (16 pages).

Les ions piégés sont explorés par les laboratoires de recherche[750] et par quelques acteurs du privé[751].

Le plus connu est celui de l'**Université de Maryland** où officie un grand spécialiste du sujet, Christopher Monroe. Sa spin-off **IonQ** est le principal acteur commercial de cette typologie de qubits. *Ci-dessus*, le cryostat fonctionnant à 4K qu'ils utilisent couramment pour piéger plus d'une centaine d'ions ytterbium[752]. Il exploite une tête pulsée SHS 4,2K et un compresseur Sumitomo[753].

En mai 2020, l'équipe d'**UCLA** de Wesley Campbell associée à l'UNSW annonçait avoir stabilisé des ions de baryum ($^{133}Ba^{+}$) pour en faire des qubits de qualité dans un piège linéaire[754]. La qualité de ces ions baryum est comparée à celle de qubits de 2014 avec une amélioration d'un facteur 10. Cette qualité n'est évaluée qu'avec l'indicateur SPAM qui mesure une fidélité sur un qubit après préparation, porte unitaire et mesure (SPAM = "state preparation and measurement"). Il manque une autre mesure : celle des portes quantiques à plusieurs qubits mettant en œuvre l'intrication, celle qui est la plus exigeante et générant les taux d'erreurs les plus élevés. Autant, celle-ci était évaluée par Honeywell en mars 2020, autant ici, elle ne l'est pas du tout. Bref, il reste encore du chemin à parcourir pour faire de ces qubits au baryum des objets comparables aux autres ions piégés déjà expérimentés.

Côté laboratoire, il faut aussi compter avec **l'IQOQI** (Autriche, cf. Rainer Blatt, un de leurs laboratoires *ci-contre*) et l'**IQST** (Allemagne), à l'origine d'un prototype de 20 qubits réalisé avec des ions calciums[755].



Il y a aussi l'Ion Quantum Technology Group de l'**University of West Sussex** (UK) qui travaille sur un prototype de 10 qubits et ambitionne de créer un ordinateur quantique à 1000 qubits à base de grappe de processeurs quantiques[756].

Cela a abouti à la création de la startup **Universal Quantum** (2019, UK). Il y a aussi la startup **Oxford Ionics** (2019, UK) qui est issue du Département de Physique de l'Université d'Oxford.

Le Flagship européen comprend le projet **AQTION** qui est piloté par l'Université d'Innsbruck et doté de 9,57M€. L'objectif est d'atteindre 50 qubits opérationnels pour préparer alors la suite, au-delà de 100 qubits, en adoptant notamment une architecture distribuée avec des liaisons photoniques. Y participent l'Université d'Oxford, l'ETZ Zurich, Fraunhofer IOF ainsi qu'Atos, probablement pour fournir des briques logicielles.

---

[750] On décomptait 98 laboratoires de recherche dans le monde travaillant sur les ions piégés en 2020. Voir ce tableau qui les liste tous dans List of Ion Trapping Groups, février 2020.

[751] Source de l'illustration : Quantum Computation with Trapped Ions de l'Université d'Innsbruck.

[752] Source de l'illustration : Cryogenic trapped-ion system for large scale quantum simulation par Christopher Monroe et al, 2018 (17 pages).

[753] Voir aussi la thèse Towards Cryogenic Scalable Quantum Computing with Trapped Ions de Matthias Brandl, 2016 (138 pages) qui documente très bien l'ingénierie d'ensemble d'un calculateur quantique à base d'ions piégés.

[754] Voir Physicists develop world's best quantum bits par Stuart Wolpert d'UCLA, mai 2020 qui fait référence à High-fidelity manipulation of a qubit enabled by a manufactured nucleus par Justin Christensen et al, mai 2020 (5 pages). Première précaution d'usage : identifier l'auteur de l'article. Il se trouve que c'est un certain Stuart Wolpert d'UCLA, en charge des relations médias de l'Université d'où viennent les travaux publiés. Il fait donc les RP du laboratoire et publie son article sur un site où c'est possible (Physorg).

[755] Ils sont coauteurs de Observation of Entangled States of a Fully Controlled 20-Qubit System, avril 2018 (20 pages).

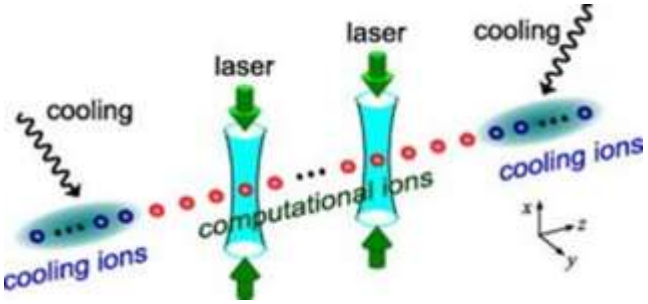
[756] Voir Blueprint for a microwave trapped ion quantum computer de Winfried Hensinger et al, 2017 (12 pages).

En France, divers laboratoires du CNRS travaillent sur des ions piégés, ainsi qu'une startup située en Bretagne, **NextGenQ**. Enfin, il faut ajouter l'Américain **Honeywell** dont nous allons détailler plus loin l'annonce de mars 2020.

IonQ (2016, USA, $84M) est une spin-off de l'Université de Maryland spécialisée dans la conception d'ordinateurs quantiques universels à base d'ions piégés, avec une trentaine de collaborateurs.

Cofondée par Christopher Monroe, un professeur de cette université qui en est le Chief Scientist[757], la startup a levé en tout $84M, dont une partie chez Google Ventures et Amazon, en 2019, chez Samsung Ventures et Microsoft, puis en 2020 chez Lockheed Martin et Bosch. Ils créaient en juin 2020 un advisory board comprenant David Wineland, Umesh Vazirani, Margaret Williams (ex Cray) et Kenneth Brown (Duke University).

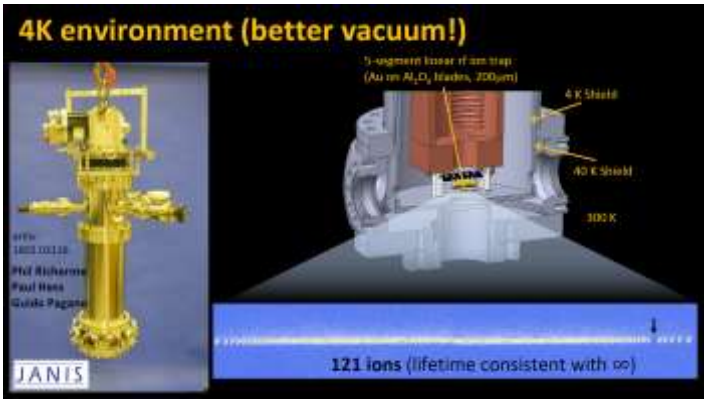
Les ions utilisés sont en d'ytterbium. Le record de début 2018 était de 53 qubits cohérents et intriqués mais pour de la simulation quantique, pas pour des qubits universels.



Fin 2018, IonQ annonçait avoir atteint 79 qubits associés à 160 qubits de stockage (utiles pour l'algorithme de Grover) mais avec une fidélité probablement moyenne[758].

Et on passait à 11 qubits caractérisés en 2019, à y perdre son latin et son quicksort. C'est lié au fait que les performances ne sont pas les mêmes selon le nombre de qubits assemblés[759].

L'Université de Maryland teste de son côté un dispositif à 121 qubits refroidi à 4K[760]. Ils anticipant d'atteindre rapidement un millier de qubits



Leurs portes quantiques auraient un taux de fidélité de 99,9% pour les portes à un qubit et de 99% pour les portes à deux qubits. La topologie du système permet de créer des portes arbitraires de deux à trois qubits reliant n'importe lequel des qubits alignés.

C'est dû aux couplages entre les ions qui exploitent des forces de Coulomb de longue portée, un peu comme lorsque dans un boulier le choc d'une bille d'un côté entraîne le mouvement de la bille à l'extrémité de l'autre côté.

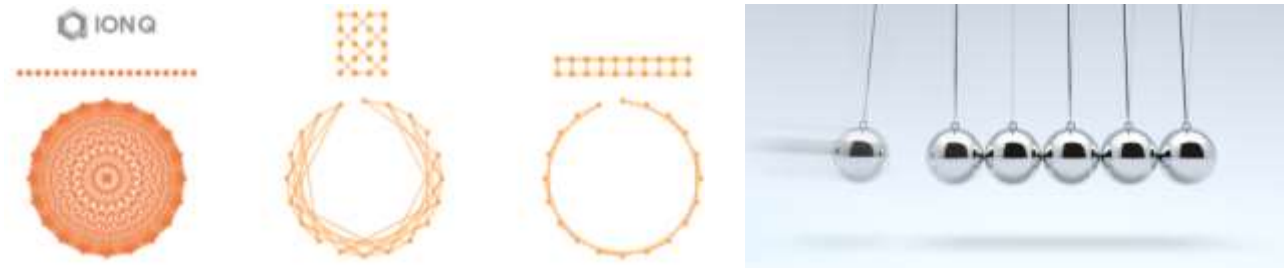
---

[757] Voir A Reconfigurable Quantum Computer par David Moehring, 2017 (20 slides).

[758] Voir IonQ Has the Most Powerful Quantum Computers With 79 Trapped Ion Qubits and 160 Stored Qubits de Brian Wang, décembre 2018.

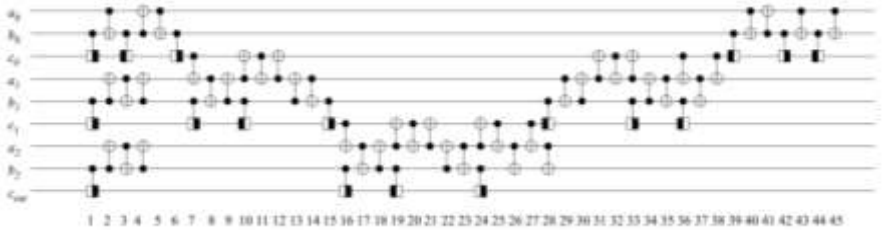
[759] Voir Benchmarking an 11-qubit quantum computer par K. Wright et al, novembre 2019.

[760] Source de l'illustration : Quantum Circuits and Simulation with Individual Atoms par Christopher Monroe, 2018 (36 slides). Ils utilisent des systèmes de cryogénie d'origine Janis.

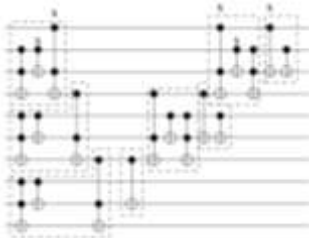


Cela permet d'optimiser les algorithmes quantiques pour minimiser le nombre de portes à exécuter comme l'illustre l'exemple *ci-contre*[761].

Ils proposent une offre logicielle de programmation en cloud. L'approche est aussi "full stack". Mais l'approche logicielle a l'air d'être très propriétaire.



version d'algorithme d'addition de 3 bits avec liaison des qubits uniquement adjacents les uns des autres



version du même algorithme avec liaison de tous les qubits entre eux

source : Fast Quantum Modular Exponentiation de Rodney Van Meter et Kohei Itoh, 2005 (12 pages)

En novembre 2019, **Microsoft** annonçait intégrer le support d'accélérateurs quantiques d'IonQ (en plus de ceux de **QCI** – en supraconducteurs - et **Honeywell** – en ions piégés) dans son offre en cloud Azure et avec ses outils de développement Q#, QDK et Visual Studio. Tout ceci a été mis à disposition des développeurs à partir de la fin du printemps 2020.

Enfin, début octobre 2020, IonQ annonçait avoir créé, à son tour, l'ordinateur quantique le plus puissant du monde avec 32 qubits et un volume quantique de 4 000 000, coiffant au poteau Honeywell et son volume quantique de 64 annoncé en juin 2020 et évoqué *ci-dessous*[762]. Le plus étonnant serait cette capacité à gérer un code de correction d'erreurs avec seulement 13 qubits physiques vs les 10 000 qubits physiques qui sont habituellement évoqués pour les qubits supraconducteurs. Ce système à 32 qubits est rendu disponible d'abord en bêta puis de manière commerciale aux clients des offres cloud quantiques d'Amazon (Braket) et Microsoft (Azure Quantum). Et notamment leurs partenaires logiciels 1QBit, Cambridge Quantum Computing, QC Ware et Zapata Computing. Tout ceci est à prendre avec des pincettes car ces prouesses ne sont encore pas documentées précisément avec des benchmarks.

Honeywell

En mars 2020, Honeywell annonçait avoir mis au point un ordinateur quantique qui serait le plus puissant du monde et doublerait la puissance par rapport au record précédent qui serait détenu par IBM[763].

L'annonce portait au départ sur un processeur quantique de quatre qubits à base d'ions piégés[764].

---

[761] Source : Fast Quantum Modular Exponentiation de Rodney Van Meter et Kohei Itoh, 2005 (12 pages).

[762] Voir IonQ Unveils World's Most Powerful Quantum Computer, IonQ, octobre 2020.

[763] Voir Honeywell Achieves Breakthrough That Will Enable The World's Most Powerful Quantum Computer et How Honeywell Made the Leap into Quantum Computing par Honeywell, mars 2020. Dans Honeywell a-t-il créé l'ordinateur quantique le plus puissant du monde ?, mars 2020, j'analyse en détail l'annonce, le texte intégré dans l'ebook en étant une version compactée.

Le doublement de la puissance était évalué par l'indicateur du volume quantique d'IBM. Comme la qualité des qubits d'Honeywell serait meilleure avec un faible taux d'erreurs, cela leur permettrait de faire mieux qu'IBM avec ses 28 qubits annoncés lors du CES 2020, d'un volume quantique de 32. Mais ils vendaient la peau de l'ours avant l'avoir vu !

Avec les 4 qubits démontrés, ils n'en étaient qu'à un volume quantique de 16. Le volume quantique de 64 était une promesse atteignable avec 6 qubits, annoncée pour la mi-2020. Elle a été atteinte comme prévu en juin 2020 malgré la grande pause du covid. Mais 4 ou 6 qubits, même de qualité, ne servent pas à grand-chose[765]. Il faut dépasser une cinquantaine de qubits pour pouvoir réaliser des calculs complètement inaccessibles aux supercalculateurs d'aujourd'hui.

La technologie utilisée est dénommée **Trapped-ion QCCD**, pour "quantum charge-coupled device". Elle exploite des ions à base d'ytterbium couplés à des ions au baryum servant au refroidissement de l'ensemble.

Cette technique a été conçue en 2002 par Christopher Monroe, David Wineland et Dave Kielpinski[766]. Honeywell fait état de la réutilisation de nombreux autres travaux issus d'autres laboratoires de recherche étalés entre 2008 et 2012.

Les ions sont générés à partir d'un jet d'atomes collimaté obtenu en chauffant une cible solide d'ytterbium. lls sont alors "touchés" par un laser, ce qui leur enlève un électron de la couche de valence de l'atome (la dernière). Il ne reste alors plus qu'un seul électron dans cette couche donnant lieu à un ion ayant une charge positive, Yb+.

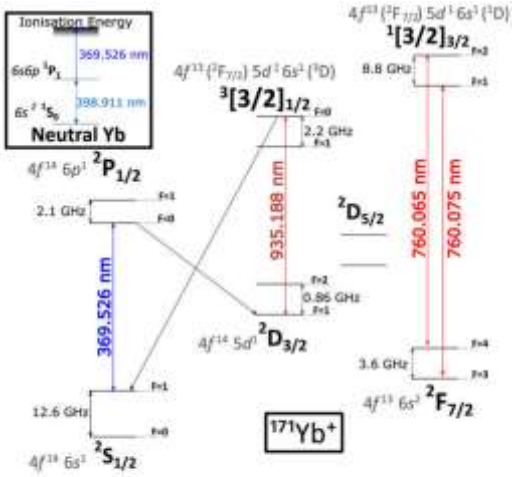


Figure 2: Partial term schemes showing the driven atomic transitions and the required laser wavelengths and microwave frequencies. The inset shows the transitions in neutral ytterbium used for photoionization. The main diagram shows the $^{171}Yb^{+}$ term scheme.

Le refroidissement laser de ces ions est bien maîtrisé grâce à leur schéma de niveaux d'énergie favorable. Grâce à leur charge électrique, il est possible de piéger et déplacer ces atomes à l'aide de potentiels électrostatiques et radiofréquence. Les autres éléments pouvant être utilisés pour créer des ions piégés sont le béryllium, le magnésium, le strontium et le calcium. L'ytterbium est aussi utilisé pour créer des mémoires quantiques, mais pas dans le cas présent.

L'état quantique des ions correspond à deux états énergétiques dits "hyperfins" dûs à l'interaction entre le moment magnétique du noyau et celui des électrons de l'ion. Ces niveaux hyperfins sont aussi utilisés dans les horloges atomiques au césium. La fréquence de transition entre les deux niveaux hyperfins de l'ytterbium est de 12,6 GHz[767].

---

[764] La performance est décrite en détail dans : Demonstration of the QCCD trapped-ion quantum computer architecture par J. M. Pino et al, 2020 (8 pages). On peut compléter cela par la présentation Shaping the future of quantum computing de Tony Uttley, le patron de l'équipe quantique d'Honeywell qui avait lieu lors de la conférence Q2B de QcWare en Californie en décembre 2019 (slides).

[765] Et il faut prendre de la distance avec la titraille de la presse sur le sujet comme dans Honeywell says it's got the fastest quantum computer on the planet For now... par Stephen Shankland dans C-Net, juin 2020.

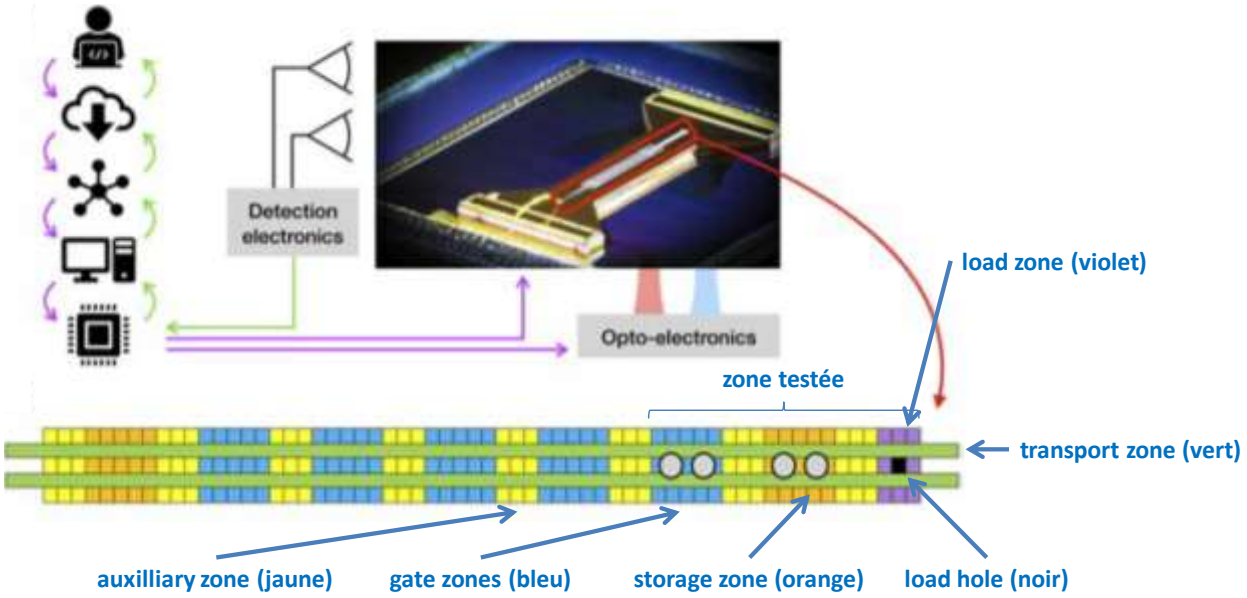
[766] Elle est décrite dans Architecture for a large-scale ion-trap, 2002 (4 pages).

[767] Voir Laser-cooled ytterbium ion microwave frequency standard de S. Mulholland et al, 2019 (16 pages).

Les états hyperfins de l'ion d'ytterbium se prêtent bien au calcul quantique car ils sont très stables, ce qui leur permet d'avoir un long temps de cohérence.

Les ions du processeur quantique d'Honeywell sont des **ions baladeurs**. C'est le premier cas de "flying qubits" qui ne sont pas à base de photons. D'habitude, les qubits à base d'électrons, d'atomes froids ou d'ions ne bougent pas (trop) là où on les installe. Cette idée avait été proposée en 2002 par Dave Wineland and co. Cela en serait la première réalisation complète et le résultat d'un gros travail d'ingénierie.

Leur système s'appuie sur un système classique qui prépare des atomes d'ytterbium, les ionise et les envoie dans un trou qui alimente le chipset. Il utilise ensuite une dizaine de zones de stockage et de tri des ions (en orange, jaune et bleu dans le schéma *ci-dessous*).



Les ions d'ytterbium sont confinés au-dessus d'un rail de trois rangées d'électrodes dont la tension variable permet d'en contrôler la position et de les déplacer latéralement. L'innovation de l'expérience de Honeywell est de réussir à démontrer des opérations logiques entre plusieurs qubits – ici, jusqu'à 4 – tout en les déplaçant à volonté entre des zones de stockage et des zones d'interaction pendant les opérations. Cette idée proposée en 2002 par David Wineland du NIST, a demandé 18 ans d'efforts continus pour aboutir.

Le système utilise 198 électrodes à courant continu pour le déplacement et le positionnement des ions ytterbium couplés à des ions de baryum. La puce exploite des pièges cryogéniques de surface ("cryogenic surface trap") qui permettent ainsi de réarranger dynamiquement le positionnement des couples d'ions ytterbium/baryum et de mettre en œuvre des portes quantiques exécutées en parallèle sur plusieurs zones du circuit.

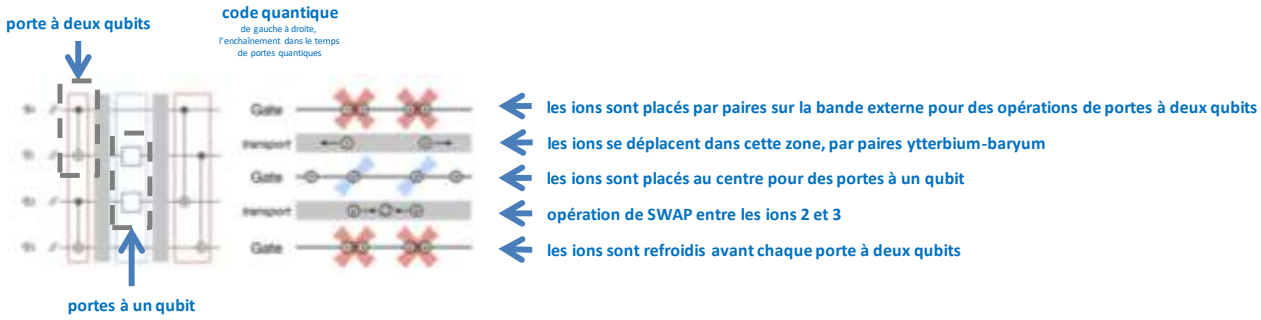
Les ions circulent sur la bande verte, permettant un déplacement arbitraire des ions le long de la bande. Une fois déplacés, ils sont recasés dans la bande du milieu pour subir une porte quantique à un qubit, ou dans les bandes latérales pour générer des portes quantiques à deux qubits, comme expliqué dans le schéma *ci-dessous*. L'une de ces opérations est une porte SWAP qui permet d'interchanger physiquement les ions.

L'inconvénient de la technique est la lenteur des portes quantiques dans les ions piégés, qui risque d'être ici encore plus marquée du fait du dispositif utilisé. Le temps de configuration des ions pour créer une porte quantique est de 3 à 5 ms ce qui n'est pas négligeable, surtout pour des algorithmes nécessitant d'enchaîner un grand nombre de portes quantiques.

Le système fonctionne à une température de 12,6K et avec une stabilité de température de 2mK qui évite de perturber les ions et leur état quantique superposé. Le refroidissement à l'hélium est complété par la technique du "sympathetic cooling" qui combine l'usage de l'effet Doppler et d'un refroidissement à effet Raman sur les ions de baryum qui sont voisins des ions ytterbium. L'interaction coulombienne entre les ions baryum permet de refroidir les ions ytterbium accolés aux ions baryum. Une opération de refroidissement des ions baryum a lieu avant chaque exécution de porte à deux qubits.

Le refroidissement par lasers des ions fonctionne à température ambiante et depuis plus de 30 ans. Comme de nombreux groupes de recherche, Honewyell refroidit le piège à ion (à 12,6K) pour minimiser l'effet d'échauffement anormal des ions, qui est un problème majeur des manipulations d'ions piégés et qui n'est d'ailleurs pas entièrement compris. Cet échauffement anormal est fortement réduit lorsque le piège est refroidi. C'est pour ça qu'ils le font ici.

Le système s'articule autour de briques de quatre qubits et utilise des **portes quantiques** à un et deux qubits qui sont activées par lasers, via l'effet Raman qui nécessite une paire de faisceaux. Les portes à un seul qubit sont activées par une paire de faisceaux Raman de 370,3 nm en polarisation circulaire. Le système permet de générer des portes X, Y et Z pour qui effectuent des rotations de quarts de tours et de demi-tours autour des trois axes de la sphère de Bloch qui représente l'état quantique d'un qubit. Ces rotations se font avec une très grande précision d'après Honeywell. Cela assure un taux d'erreur minimum pour des portes quantiques à un seul qubit.



Les portes à deux qubits utilisent deux paires de faisceaux laser additionnels qui agissent sur des paires d'atomes d'ytterbium qui ont été rapprochés l'un de l'autre par les électrodes de contrôle de positionnement du circuit. Deux ions sont ainsi déplacés par les électrodes dans le même puits de potentiel avant d'être couplés par laser. Les qubits peuvent alors être séparés et déplacés ailleurs pour interagir avec d'autres qubits.

La **lecture de l'état des ions** se fait avec un imageur classique qui détecte l'état énergétique des ions via leur fluorescence qui est activée par laser. Cet imageur est un "PMT array", c'est-à-dire un réseau linéaire de photomultiplicateurs (Photo-Multiplier Tube). Leur architecture permet une mesure de l'état des qubits en cours de traitement, sans perturber les qubits voisins. Cela permet de programmer l'ordinateur quantique avec une logique conditionnelle, avec des IF THEN ELSE comme en programmation classique.

Enfin, le système comprend un circuit électronique programmable FPGA pour le contrôle des qubits, à priori, hors de l'enceinte cryogénique.

La **performance de leurs qubits** semble correcte, mais pas forcément extraordinaire. Le taux d'erreur ne serait que de 2% après l'exécution d'une centaine de portes quantiques. Cela permettrait d'exécuter des algorithmes quantiques "profonds" avec un grand nombre d'enchaînements de portes quantiques. Cela se compare à une profondeur d'environ 20 portes quantiques exécutées avec les 53 qubits supraconducteurs du chipset Sycamore de Google. Il y aurait aussi un faible "cross talk" entre couples de qubits, à savoir que les qubits indépendants n'ont pas l'air d'interférer avec leurs voisins, sauf lorsqu'ils sont intriqués. Ce taux d'erreurs très bas est un record à ce jour.

Honeywell indique que son architecture serait scalable, en conservant ce faible taux d'erreurs. Ils n'ont à ce jour testé que quatre qubits ! Ils envisagent une approche de montée en puissance à trois étapes. Pour l'instant, ils utilisent une barre d'ions piégés "1D". Dans les deux étapes suivantes, ils passeraient à une barre en "2D" qui permettrait de déplacer les ions dans deux directions, permettant ainsi d'en accumuler un plus grand nombre et de les connecter avec leurs voisins dans deux dimensions. Cela prendra du temps de mettre cela au point.

Honeywell annonce ainsi que leur processeur sera 100 000 fois plus rapide d'ici 2025. Rapide comment ? Evalué avec le volume quantique d'IBM ou avec une autre méthode de mesure ? On ne sait pas. Par le passé, nombre d'annonces de ce genre ont été faites, comme John Martinis qui déclarait en 2017 scaler jusqu'à 72 qubits. Et ils en étaient à 53 en 2019. La scalabilité des processeurs quantiques est un des problèmes les plus complexes qui reste à régler.

Honeywell a démarré cet investissement dans le calcul quantique en 2016 mais en mode "stealth", sans communiquer autour. Cela se savait cependant car ils ont recruté des chercheurs issus de diverses universités américaines. Leur équipe rassemble aujourd'hui une centaine de personnes avec des physiciens, des ingénieurs et des développeurs. Ils viennent notamment du laboratoire du NIST de Boulder ainsi que de l'Université du Colorado. On y retrouve aussi des anciens de l'Université du Maryland et de l'équipe de Christopher Monroe (IonQ).

Au moment de l'annonce du 2 mars 2020, Honeywell évoquait plusieurs partenariats : avec **Microsoft**, pour l'intégration à terme des calculateurs quantiques d'Honeywell dans le cloud Azure, un investissement dans les startups **Cambridge Quantum Computing** (2014, UK, $22,4 levés en tout) et **Zapata Computing** (2017, USA, $64M). Startups qui développeront des outils logiciels pour les machines d'Honeywell. Et puis un partenariat avec **JPMorgan Chase** pour créer des algorithmes quantiques dans le secteur financier. En juin 2020, Honeywell annonçait que ses 6 qubits étaient bien opérationnels et disponibles dans le cloud soit directement chez eux, soit via Microsoft Azure Quantum Portal. En juillet, la disponibilité commerciale était enfin annoncée, sous la forme d'une offre payante en cloud dénommée System Model HØ. Pour accéder à 6 malheureux qubits, ce n'est pas très malin. Ils auraient dû proposer cela gratuitement comme le fait IBM jusqu'à 17 qubits.

Atomes froids

Les atomes froids (cold atoms) sont une autre forme atomique de qubits en plus des ions piégés. Eux-aussi sont piégés, mais pas exactement de la même manière. Comme ces atomes ne sont pas utilisés sous forme ionisée, on ne peut pas facilement les piéger avec des électrodes. On emploie pour cela des lasers envoyés dans plusieurs directions en exploitant la méthode de « l'optical tweezing » ou des pièges optiques[768]. C'est une variante de l'effet Doppler qui est utilisé pour refroidir des atomes. On peut aussi combiner cela avec des pièges magnétiques. Ces atomes sont cependant également contrôlés par magnétisme.

En pratique, les atomes froids utilisés se concentrent sur seulement quelques éléments comme le rubidium et le césium. Ils font partie de la première colonne du tableau des éléments avec un seul électron dans la couche de valence, comme l'hydrogène, le sodium et le lithium.

L'élément le plus souvent utilisé est le rubidium. C'est un métal alcalin qui présente des transitions énergétiques intéressantes qui correspondent à des longueurs d'ondes de lasers courants ainsi qu'à des micro-ondes faciles à générer, comprises entre 3 et 10 GHz. On peut gérer avec eux des transitions dites fermées qui permettent, avec des lasers, de faire transiter les atomes entre plusieurs états de manière cyclique et contrôlée. Qui plus est, les états sont stables suffisamment longtemps pour réaliser des calculs, soit de l'ordre de la centaine de microsecondes.

[768] Voir Quantum information processing with individual neutral atoms in optical tweezers par Philippe Grangier, (47 slides).

Les atomes froids sont aussi utilisés dans des états dits de Rydberg, qui correspondent à un niveau d'excitation énergétique très élevé. Dans les qubits à atomes froids, ces états énergétiques élevés servent à gérer l'intrication entre atomes et donc à la création de portes quantiques à plusieurs qubits. Ces états excités ont un niveau de stabilité assez bon, d'environ 100 µs. Il est plusieurs ordres de grandeur plus longs que les états excités classiques (hyperfins, utilisés pour les états des qubits). Cette stabilité équivaut en quelque sorte au temps de cohérence des qubits supraconducteurs.

On exploite aussi un l'effet du blocus de Rydberg ou *Rydberg blockade effect* en anglais. Il est lié au fait qu'un atome de Rydberg excité avec un niveau énergétique élevé (avec n>50-70, n étant le niveau énergétique quantique d'un électron autour du noyau d'un atome) va empêcher les atomes avoisinants d'atteindre ce niveau.

Lorsqu'ils sont excités, ces atomes se comportent comme des dipôles accentués, l'orbite des électrons de la couche de valence étant très inclinées comme illustré *ci-contre*[769]. Ils ont aussi une taille disproportionnée jusqu'à un micron (µm) de diamètre pour n=100 avec du ^{87}Ru. Ils sont proches de l'état d'ions[770]. Leurs caractéristiques électromagnétiques font réagir les atomes avec leurs voisins dont ils bloquent l'excitation au niveau de Rydberg dans un périmètre allant jusqu'à 20 µm, ce qui est énorme à l'échelle atomique.

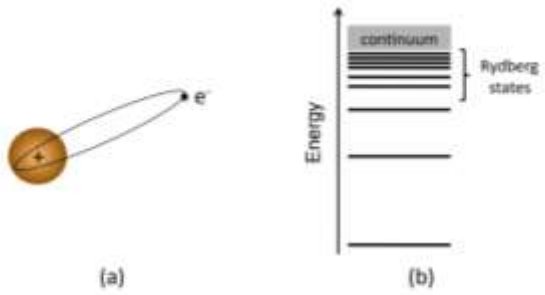


Figure 1: (a) Classical picture of an alkali Rydberg atom: the electron has an orbit far from the nucleus, which is screened by the electronic core. The resulting charge seen by the outer electron is therefore +e. When the outer electron has a low angular momentum, it penetrates the electronic core. (b) Quantum picture: Rydberg states are close to the ionization threshold. As a consequence, the energy spacing between Rydberg states decreases with increasing principal quantum numbers. Around $n = 50$, for alkali atoms, the frequencies of the transitions between nearby states is in the $10 - 100$ GHz range.

En dehors du calcul quantique, un atome de Rydberg activé peut être excité par laser pour générer des photons uniques bien isolés exploitables en optique non linéaire[771].

qubits à atomes froids

avantages

- **stabilité des atomes** utilisés.
- longs **temps de cohérence**.
- **atomes identiques**, contrôlables avec les mêmes fréquences de laser et micro-ondes.
- **réutilise le savoir faire des ions piégés** pour la mesure de l'état des qubits par fluorescence.
- fonctionne bien en **mode simulation.**
- une **startup française** à la pointe sur ce créneau : Pasqal.
- pas besoin de produire des **circuits intégrés**.
- fait appel à de l'**appareillage standard.**

inconvénients

- **taux d'erreurs des portes quantiques** correct mais pas "best in class".
- **cross-talk** entre qubits qui peuvent se perturber les uns les autres.
- **plus adapté à la simulation** qu'au calcul quantique universel.
- **optique et lasers** de contrôle qui ne scale pas facilement au-delà d'un millier de qubits avec l'état de l'art actuel.

[769] Source du schéma et explications détaillées Interacting Cold Rydberg Atoms: a Toy Many-Body System par Antoine Browaeys et Thierry Lahaye, 2013 (20 pages).

[770] Cette présentation de 52 slides datant de 2014 décrit bien l'histoire et la géométrie des atomes de Rydberg.

[771] Voir Observation of coherent many-body Rabi oscillations par Yaroslav Dudin et Alex Kuzmich de GeorgiaTech, 2012 (5 pages) ainsi que Nonlinear quantum optics mediated by Rydberg interactions par Sebastian Hofferberth et al, 2016 (26 pages).

Cela permet d'obtenir une autre source de photons uniques, en complément des quantum dots déjà évoqués au sujet des qubits photons. Le phénomène du blocus de Rydberg est aussi exploitable en cryptographie et télécommunications quantiques[772], en spectroscopie et dans les horloges atomiques.

Les atomes de Rydberg servent enfin à créer des mémoires quantiques[773]. Des états topologiques permettant de créer des systèmes de calcul à base de qubits plus fiables sont aussi étudiés[774].

Les qubits sont arrangés en matrice en 2D[775] ou en 3D dans l'espace[776]. Ils sont refroidis, contrôlés et positionnés par plusieurs lasers organisés en « pinces » de précision (« optical tweezers »). Un qubit peut reposer sur un seul atome ou sur un groupe d'atomes selon les méthodes employées. Les atomes sont préparés avec une source froide de quelques µK qui alimente ensuite une chambre sous vide où la prise de contrôle par les lasers a lieu[777].

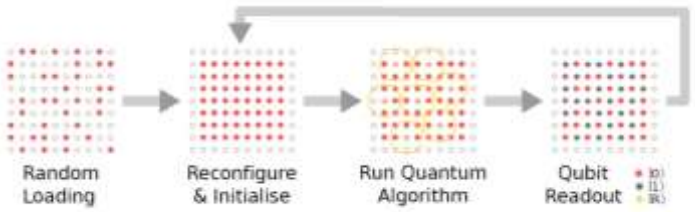


Figure 2. Schematic of a Rydberg array quantum computer. Atoms are initially loaded stochastically, followed by rearrangement to achieve a defect free qubit register. Coherent excitation to Rydberg states allows implementation of quantum algorithms exploiting long-range interactions to couple neighbouring qubits, followed by state-selective readout which is repeated many times to tomographically reconstruct the output state.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit fait appel en général à deux états hyperfins séparés par un niveau d'énergie de fréquence micro-onde pour définir le |0⟩ et le |1⟩ du qubit. Ce sont deux états énergétiques excités relativement stables au-dessus du ground state (état non excité) de l'atome.
- Les **portes quantiques à un qubit** sont activées par un mix de micro-ondes (de quelques GHz, compatibles avec les états hyperfins) et de pompage laser pour modifier l'état énergétique de l'atome froid entre son état de base et ses états hyperfins. Ces portes peuvent aussi faire appel à des transitions Raman pilotées par des lasers sur deux fréquences ou par une combinaison de l'effet Stark de décalage de raies spectrales sous l'effet d'un champ électrique et de micro-ondes. Les meilleures fidélités de portes à un qubit sont situées aux alentours de 99,6%[778] avec un objectif à terme d'atteindre un taux d'erreur de 10^{-4}. Heureusement, il il existe des systèmes optiques de multiplexage de rayons lasers permettant d'éviter d'avoir plus de lasers que de qubits.

---

[772] Voir sur le couplage avec des photons pour établir des liaisons distantes : Photon-Mediated Quantum Information Processing with Neutral Atoms in an Optical Cavity par Stephan Welte, 2019 (124 pages).

[773] Voir Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble par Julien Laurat et al, 2018 (6 pages) et Experimental realization of 105-qubit random access quantum memory par N. Jiang et al, 2019 (6 pages).

[774] Voir Topologically protected edge states in small Rydberg systems par Antoine Browaeys et al, 2018 (6 pages) et Observation of a symmetry protected topological phase of interacting bosons with Rydberg atoms par Antoine Browaeys, Thierry Lahaye et al, 2019 (20 pages). La simulation quantique à base d'atomes froids permet aussi de simuler la matière topologique. Voir Scientists unveil first quantum simulation of 3-D topological matter with ultracold atoms par la Hong Kong University of Science and Technology, juillet 2019.

[775] Voir la thèse Rydberg interactions in a defect-free array of single-atom quantum systems par Daniel Ohl de Mello, 2020 (147 pages) qui décrit la manière de remplir une matrice 2D d'une centaine d'atomes lourds.

[776] Voir Three-Dimensional Trapping of Individual Rydberg Atoms in Ponderomotive Bottle Beam Traps par Antoine Browaeys, Thierry Lahaye et al, 2019 (8 pages).

[777] Source du schéma : Rydberg atom quantum technologies par James Shaffer, 2019 (24 pages).

[778] Voir High-Fidelity Control, Detection, and Entanglement of Alkaline-Earth Rydberg Atoms par Ivaylo Madjarov, janvier 2020 (13 pages) qui utilize du strontium.

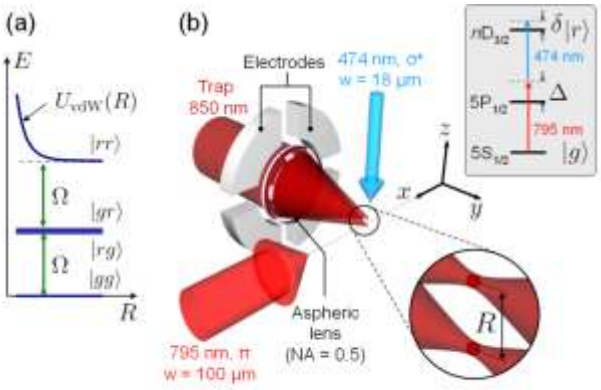
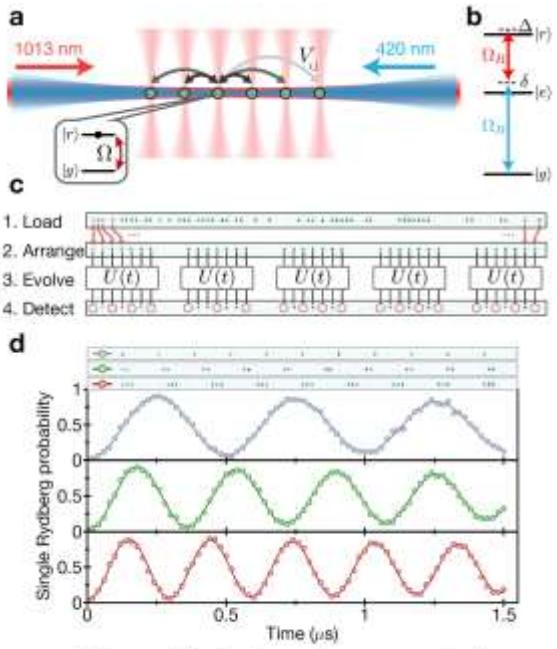


Illustration des combinaisons de lasers et d'électrodes utilisés pour contrôler l'état et la position des atomes froids

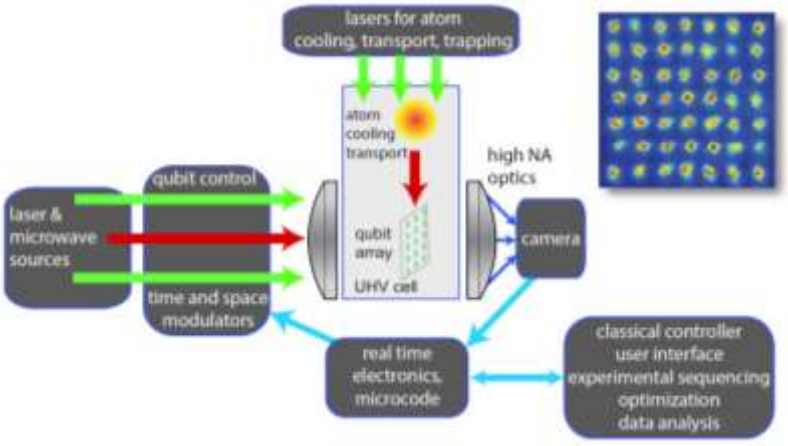
ci-dessus, liée à une porte quantique à deux qubits créée en 2013 et à droite, sur un simulateur quantique de 51 qubits créé en 2017 à Harvard et au MIT.

source : Direct Measurement of the van der Waals Interaction between Two Rydberg Atoms par Lucas Béguin, Antoine Browaeys & al, 2013 (5 pages).



source : Probing many-body dynamics on a 51-atom quantum simulator par Hannes Bernien, Mikhail Lukin & al, 2017 (24 pages).

- Les **portes quantiques à deux qubits** utilisent également des micro-ondes et lasers[779]. Elles sont appliquées sur les atomes dans leur état excité (dit de Rydberg) qui projette ses électrons de couche de valence dans une orbite haute. Pour le rubidium, il n'y a qu'un électron à gérer dans cette couche. Ces portes quantiques peuvent en pratique mettre en œuvre plus de deux qubits. A fidélité des portes à deux qubits était assez faible en 2016 avec un maximum de 75% avec du rubidium et de 81% en 2016 avec du césium. Elle était passée à un meilleur niveau de 97% en 2019[780]. La décohérence des qubits à base d'atomes froids a différentes origines : la photoionisation, l'émission spontanée de photons, des transitions induites par la radiation de corps noir, la stabilité des lasers de contrôle et du timing des impulsions lasers et la précision de contrôle des atomes dans l'espace[781].
- La **mesure de l'état d'un qubit** utilise une caméra CCD qui détecte la fluorescence des atomes avec une méthode voisine de celle qui est employée avec les ions piégés. *Ci-contre*, une description simplifiée d'un système de qubits à atomes froids avec les outils de contrôle à base de lasers et micro-ondes et de mesure des qubits par fluorescence et caméra[782].



[779] En août 2019, des chercheurs américains arrivaient à créer des portes quantiques à plusieurs qubits fidèles à 95% à base d'atomes froids. Voir Parallel implementation of high-fidelity multi-qubit gates with neutral atoms, par H. Levine et al, août 2019 (16 pages). Bases de portes à deux qubits dans Direct Measurement of the van der Waals Interaction between Two Rydberg Atoms, par Lucas Béguin, Antoine Browaeys et al, 2013 (5 pages).

[780] Selon Rydberg atom quantum technologies par James Shaffer, 2019 (24 pages), page 10.

[781] Source : Quantum Computing with Neutral Atoms, 2013 (42 slides).

[782] Pour en savoir plus, direction Quantum computing with atomic qubits and Rydberg interactions: Progress and challenges par Mark Saffman, 2016 (28 pages, d'où est extrait le schéma.

En général, les systèmes à base d'atomes froids fonctionnent à température de moins de 50 mK et sous ultra-vide. En pratique, c'est l'ultra-vide et le refroidissement des atomes qui assure cette thermalisation. Il n'est pas nécessaire d'utiliser des réfrigérateurs à dilution comme avec les qubits supraconducteurs et silicium. Le bilan thermique semble bien différent de celui des qubits supraconducteurs et mériterait d'être comparé.

Les laboratoires de recherche les plus actifs avec les qubits à base d'atome froids sont aux USA (Université du Wisconsin, du Colorado, Harvard, Caltech, GeorgiaTech), au Royaume Uni à l'Université de Cambridge, en Autriche à l'Université d'Innsbruck et celle de Vienne, l'Allemagne (Max-Planck-Institut für Quantenoptik, Université Libre de Berlin, Université de Stuttgart) et en France, en particulier au laboratoire Charles Fabry de l'Institut d'Optique à Palaiseau. C'est ce qui a abouti à la création de la startup française **Pasqal**, appuyée par les abondants travaux de recherche de ses cofondateurs Antoine Browaeys et Thierry Lahaye, actifs sur le sujet depuis une bonne dizaine d'années et sous le parrainage d'Alain Aspect qui s'intéresse au sujet depuis la fin des années 1980. D'autres startups sont positionnées sur les atomes froids : **Atom Computing** (2018, USA), **ColdQuanta** (USA) et **QuEra Computing** (2020, USA).

Enfin, le projet européen H2020 **AtomQT** couvre la recherche dans les atomes froids aussi bien côté qubits que métrologie. En France, il associe l'Institut d'Optique de Bordeaux (Philippe Bouyer) ainsi que le LPMMC de Grenoble.

Les premiers systèmes de qubits à base d'atomes froids sont pour l'instant plutôt des simulateurs et pas encore des calculateurs universels[783]. En 2017, l'équipe de Mikhail Lukin de l'Université d'**Harvard** et avec une équipe du **MIT** assemblait ainsi 51 atomes de rubidium[784].

Celle d'Antoine Browaeys de l'**Institut d'Optique** atteignait de son côté 72 atomes froids dans une structure 3D en 2018[785].

Photons

Nous avons fait le tour des qubits à base d'électrons (supraconducteurs, silicium, NV centers, fermions de Majorana) puis d'atomes (ions piégés et atomes froids). Il nous reste à traiter de la dernière catégorie de particules quantiques qui est utilisée dans le calcul quantique : les photons. Contrairement aux précédents, ils n'ont pas de masse et se déplacent à peu près à la vitesse de la lumière, modulo la nature des milieux physiques traversés.

Les photons sont utilisés pour créer des qubits exploitant la polarisation ou d'autres caractéristiques physiques comme la fréquence, l'amplitude ou la phase. C'est le vaste champ de l'optique linéaire et non linéaire. Il couvre à la fois la génération de qubits pour du calcul ou de la simulation quantiques mais aussi leur application dans les télécommunications et la cryptographie quantique que nous étudierons dans une autre partie de cet ebook. Les photons sont aussi utilisés en métrologie, notamment pour la mesure de précision du temps.

N'oublions pas que les photons sont les premiers « objets » quantiques avec lesquels on a pu mener des expériences d'intrication avec l'expérience d'Alain Aspect de 1982 !

---

[783] Voir Toward quantum simulation with Rydberg atoms par Thanh Long Nguyen, 2016 (182 pages), Quantum simulations with ultracold atoms in optical lattices, 2017 (8 pages), Tunable two-dimensional arrays of single Rydberg atoms for realizing quantum Ising models par Thierry Lahaye et Antoine Browaeys, 2017 (13 pages), Quantum read-out for cold atomic quantum simulators, par J. Eisert et al, 2018 (20 pages), Quantum critical behaviour at the many-body localization transition par Markus Greiner et al, 2018 (10 pages), Quantum Kibble-Zurek mechanism and critical dynamics on a programmable Rydberg simulator, Alexander Keesling et al, 2019 (16 pages) et Many-body physics with individually controlled Rydberg atoms, par Antoine Browaeys et Thierry Lahaye, 2020 (14 pages).

[784] Voir Quantum simulator with 51 qubits is largest ever, par Matt Reynolds, 2017 qui fait référence à Probing many-body dynamics on a 51-atom quantum simulator par Hannes Bernien, Mikhail Lukin et al, 2017 (24 pages).

[785] Voir Synthetic three-dimensional atomic structures assembled atom by atom par Daniel Barredo, Antoine Browaeys et al, 2018 (4 pages).

De nombreux laboratoires dans le monde sont investis dans ce champ. La photonique est à la fois une solution intéressante de création de qubits ainsi qu'une technologie transversale indispensable aux autres types de qubits car c'est la seule qui permette des communications longue distance entre qubits et entre unités de calcul quantiques.

qubits photons

avantages

- **qubits stables** avec un faible taux d'erreurs et pas de phénomène de décohérence.
- fonctionnement à **température ambiante** du traitement des qubits.
- **techniques de fabrication** courantes et maîtrisées (CMOS).
- **sources de photons** uniques et indistingables facilitant la création de portes quantiques à deux qubits.
- **technologie transversale incontournable,** notamment pour les communications inter-qubits longue distance et les télécommunications quantiques.

inconvénients

- technologie **pas encore scalable** en nombre de qubits.
- taux d'erreur élevé de la **lecture de l'état des qubits**, mais cela s'améliore.
- les photons ne peuvent **ni s'arrêter ni être stockés**. Ils peuvent juste être légèrement retardés.
- **besoin de refroidissement** des sources et détecteurs de photons, mais à des températures raisonnables nécessitant un équipement relativement léger.
- **suprématie quantique** de l'échantillonnage de bosons sans grande utilité à ce jour.

Les avantages de la photonique sont de permettre de gérer des qubits assez stables avec un taux d'erreurs très faible au niveau des portes quantiques, surtout au regard de celui des qubits supraconducteurs.

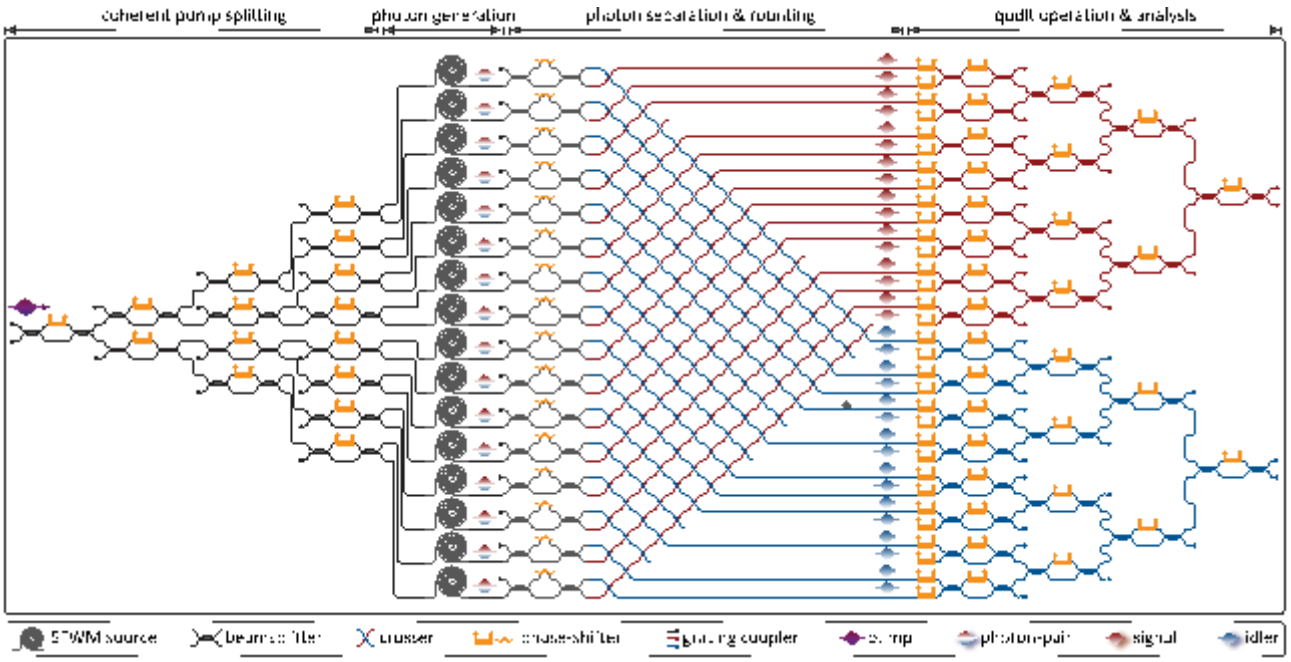
Ils fonctionnent aussi à température ambiante[786], n'impliquent pas des techniques de fabrication coûteuses au niveau nanoscopique et peuvent s'appuyer cependant sur des procédés de fabrication de composants CMOS courants[787].

Leur inconvénient réside dans la difficulté à assembler plus que quelques qubits tout du moins pour l'instant. Les détecteurs de l'état des photons en fin de calcul ne sont pas très fiables, avec un taux d'erreur compris entre 5% et 50%.

Les qubits photons exploitent des photons isolés, uniques et devant être indiscernable. On est capable aujourd'hui de générer des photons individuels sous forme de trains de photons bien espacés dans le temps et ayant les mêmes propriétés quantiques, comme ce que propose la startup française **Quandela** que nous aurons l'occasion de décrire en détail. Ces photons uniques sont détectables individuellement à la fin des traitements.

[786] Mais en général, leur source de lumière doit être refroidie à 10K et les détecteurs de photons en sortie à 2K.Au moins, on évite de descendre à moins de 1K ce qui permet d'utiliser des systèmes de cryogénie se contentant d'hélium 4 et ne nécessitant pas d'hélium 3 qui est plus rare. Ces systèmes de cryogénie sont miniaturisables et beaucoup moins d'énergie que les systèmes à dilution utilisés pour les qubits supraconducteur et silicium.

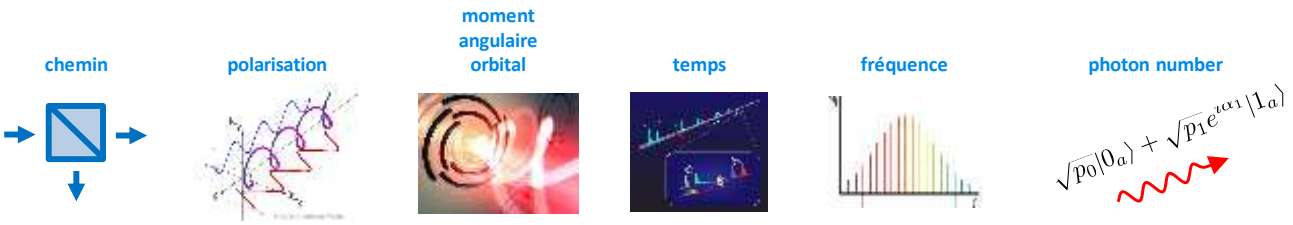
[787] Voir Photonic quantum information processing: A concise review par Sergei Slussarenkoa et Geoff Prydeb du Centre for Quantum Dynamics et du Centre for Quantum Computation and Communication Technology de l'Université Griffith de Brisbane en Australie (20 pages) qui décrit bien l'état de l'art des qubits photons. C'est la source du schéma. La bibliographie du document comprend 361 sources dont 7 qui mentionnent Pascale Senellart ! Voir aussi le plus ancien Why I am optimistic about the silicon-photonic route to quantum computing, de Terry Rudolph, le fondateur de PsiQuantum, publié en 2016 (14 pages).



Le principe général des systèmes de calcul quantique utilisant des qubits photons est le suivant :

- Les **sources de photons** sont des lasers, souvent couplés à des générateurs de trains de photons uniques et indiscernables comme ceux de Quandela[788]. Ils sont critiques pour générer simultanément un grand nombre de photons identiques qui vont alimenter en parallèle plusieurs qubits.
- L'**état quantique** du qubit est une propriété des photons utilisés. La plus courante est leur polarisation avec une base computationnelle assise sur la polarisation horizontale et verticale. D'autres paramètres des photons sont aussi explorés pour créer des qubits comme leur phase, leur amplitude, leur fréquence, leur chemin et leur moment angulaire orbital[789].

  Cela permet potentiellement de créer des qutrits ou des qudits qui gèrent donc plus que deux états superposés. Les photons sont des « flying qubits » car ils se déplacent dans l'espace et ne sont pas statiques ou quasi-statiques à l'échelle macroscopique contrairement à la plupart des autres types de qubits[790].

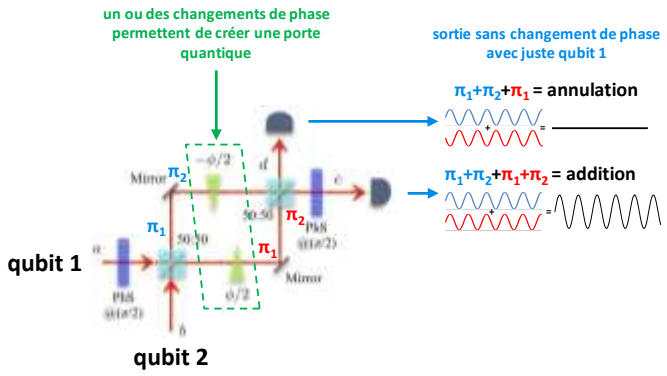


[788] Voir Near-ideal spontaneous photon sources in silicon quantum photonics par S. Paesani et al, 2020 (6 pages) qui décrit une source de photon unique à base d'un composant de photonique. C'est un projet de recherche anglo-italien.

[789] Cette multiplicité de paramètres permet d'ailleurs d'encoder non pas seulement des qubits mais aussi des qudits, avec un plus grand nombre d'états. Mais c'est assez complexe à gérer et, ne serait-ce que pour gérer des portes quantiques à deux qubits, on se contente de qubits au lieu d'exploiter des qudits. Source d'inspiration du schéma : Les débuts de l'ordinateur quantique : principes, promesses, réalisations et défis, de Pascale Senellart, janvier 2020 (98 slides). Voir aussi Forget qubits — scientists just built a quantum gate with qudits par Kristin Houser, juillet 2019 qui fait référence à High-dimensional optical quantum logic in large operational spaces par Poolad Imany et al, 2019 (10 pages).

[790] Les autres qubits sont « non volants » : les électrons dans une cavité (qui ne changent pas de cavité), les atomes froids (que l'on stabilise dans l'espace) et les ions piégés (qui eux peuvent bouger, mais dans un espace limité), les NV centers (les cavités ne bougent pas) et les circuits supraconducteurs (qui sont fixes dans l'espace même s'ils utilisent des paires d'élecrons de Cooper circulantes).

- Les **portes quantiques à un qubit** utilisent des circuits optiques simples, notamment des séparateurs de faisceaux, des lames d'ondes, des miroirs et miroirs semi-réfléchissants et des déphaseurs[791]. Par exemple, une porte de Hadamard (H) utilise un séparateur de faisceau ou une lame d'onde, une porte de Pauli X (bit flip) associe un séparateur de faisceau et une porte de Hadamard et une porte de Pauli Z (phase flip) utilise un déphaseur provoquant un changement de phase de 180° (π)[792].



interféromètre Mach-Zehnder (MZI)
fait interférer un faisceau lumineux ou un photon unique séparé en deux avec introduction d'un déphasage liés au nombre de réflexions sur les miroirs et faces avant de miroirs (les π)

Quantum Logic Gate	Unitary Matrix	Relation for MZI implementation	Elements
Beam Splitter(BS)			
50-50 Beam Splitter(B)			
Hadamard(H)		H=BZ	50-50 Beam splitter
Phase flip gate (Z)		Z=HH	π Phase shifter
Bit Flip gate (X)		X=HH	Beam Splitter, Balanced
T gate			π/4 phase shifter
S gate			Quarter wave plate
Pauli Y gate			
CNOT gate		(I⊗H)×K×(I⊗H)	Kerr Media(K) Balanced(B) Identity(I)

Quantum Logic Processor: A Mach Zehnder Interferometer based Approach, 2006 (19 pages).

portes quantiques MZI
on peut créer une porte quantique unitaire en introduisant un déphasage dans l'un des circuits, et créer une porte à deux qubits en utilisant deux entrées a et b et un déphasage. Le tableau ci-dessus indique la correspondance entre portes quantiques classiques et séquences de filtres et portes utilisés.

- Les **portes quantiques à deux qubits** sont difficiles à réaliser car il n'est pas évident de faire interagir des photons entre eux, en particulier si les photons ne sont pas indiscernables. Elles utilisent des circuits optiques à base de séparateurs de faisceaux ou d'interféromètres Mach-Zehnder à deux entrées intégrant des changements de phase sur les chemins optiques, s'appuyant sur la méthode KLM déjà citée en note de bas de page.

  Cela ne fonctionne pas bien dans les cas de figure où les photons sont inégaux comme ceux qui proviennent de lasers. A savoir, dans seulement quelques % des cas. Avec des photons indiscernables, les portes sont efficaces à plus de 95% car les photons peuvent interférer entre eux et s'additionner ou se soustraire. C'est la solution des sources de photons uniques stables et indiscernables comme celle qui est proposée par Quandela. Elle facilite les opérations d'interférométrie Mach-Zehnder.

  Ces sources présentent de plus l'intérêt d'être très brillantes, ce qui leur permet une démultiplication des photons en entrée et de traverser ensuite de nombreuses portes quantiques. Il existe aussi des solutions à base de cavités.

  La recherche s'active aussi sur la création de non-linéarités pour améliorer la fiabilité de ces portes quantiques[793]. Il faudrait idéalement disposer de cubes séparateurs non-linéaires[794].

---

[791] Cela s'appuie sur le schéma KLM proposé dans A scheme for efficient quantum computation with linear optics par Emanuel Knill, Raymond Laflamme et Gerard Milburn, 2001 (7 pages).

[792] Source du tableau à droite de l'illustration : Quantum Logic Processor: A Mach Zehnder Interferometer based Approach, par Angik Sarkar et Ajay Patwardhan 2006 (19 pages).

[793] Voir Quantum Computing With Graphene Plasmons, mai 2019 qui fait référence à Quantum computing with graphene plasmons d'Alonso Calafell et al, 2019. Il s'agit de la création de portes quantiques à deux qubits avec des structures non linéaires à base de graphène. Cela vient de l'Université de Vienne en Autriche et de laboratoires espagnols et serbes. Ainsi que Researchers see path to quantum computing at room temperature par Army Research Laboratory, mai 2020 qui fait référence à Controlled-Phase Gate Using Dynamically Coupled Cavities and Optical Nonlinearities par Mikkel Heuck, Kurt Jacobs et Dirk R. Englund, 2020 (5 pages).

[794] C'est une fonction réalisable avec le composant de génération de photons unique de Quandela, détourné de son usage originel. Voir aussi Researchers see path to quantum computing at room temperature, mai 2020 qui fait référence à Controlled-phase Gate using Dynamically Coupled Cavities and Optical Nonlinearities par Mikkel Heuck, septembre 2019 (5 pages) et porte sur une technique de portes quantiques optiques à cavités non linéaires.

- La **mesure de l'état d'un qubit** utilise des détecteurs de photons uniques qui captent aussi leur état quantique. Cette détection est encore imparfaite. Les détecteurs de photons les plus récents sont plus efficaces. Ces SNSPDs (Superconducting Nanowire Single-Photon Detectors) nécessitent un refroidissement situé entre 800 mK et 3K qui nécessite un système de réfrigération à dilution, heureusement, plus léger que celui des calculateurs quantiques supraconducteurs[795].

D'un point de vue physique, les composants s'appuient sur des briques connues dans la photonique en général : des sources de photons uniques et identiques, des guides de lumière, des lignes à retard optiques (fibres optiques ou cellules Pockels contrôlées par tension), des interféromètres Mach-Zehnder, des diviseurs de faisceaux (splitters, qui divisent un faisceau optique en deux faisceaux, en général identiques), des filtres biréfringents (qui possèdent deux indices de réfraction différents), des déphaseurs et des détecteurs de photons uniques[796].

guides de lumière
light guides
fibres optiques ou guides intégrés dans des composants à plat

lignes à retard optiques
optical delay line
alignent la phase de photons après passage par des chemins de longueur différente

diviseurs de faisceaux
splitters
divisent un faisceau optique en deux faisceaux en général identifiques

filtres biréfringents
birefringent filters
filtres avec deux indices de réfraction différents

polariseurs
conervent une seule polarité des photons entrants

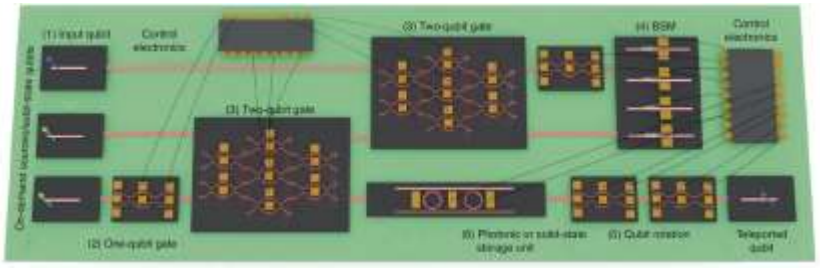
déphaseurs
modifie la polarisation (ou la phase) des photons
lames à retard
ou cellules Pockels

Pour mener des expériences, ces composants discrets et très abordables sont installés sur des tables optiques soigneusement calibrées de quelques mètres carrés avec plein d'instruments et des photons qui circulent en grande partie dans l'espace libre dans une pièce mise au noir. Heureusement, ces composants optiques sont miniaturisables sur des circuits intégrés semiconducteurs.

Cela fait partie du vaste champ de la nanophotonique qui mériterait son propre chapitre… pour la prochaine édition de cet ebook.

Les composants de nanophotonique sont gravés avec des densités comprises entre 220 nm et 3 µm[797].

Ces composants pourraient être assemblés de manière modulaire comme dans le schéma *ci-contre*[798]. Cela permet de mieux gérer l'hétérogénéité des procédés employés pour produire ces différents circuits.



Au bout du compte, un calculateur quantique va assembler trois composants clés : un générateur de photons uniques, des circuits en photonique intégrée et des détecteurs de photons uniques. Sachant que les premiers et les derniers sont intégrés avec un système de cryogénie pour fonctionner respectivement à environ 10K et 2K-4K[799].

---

[795] Voir The potential and challenges of timeresolved single-photon detection based on current-carrying superconducting nanowires par Hengbin Zhang et al, 2020 (19 pages)

[796] C'est bien expliqué dans la présentation Silicon photonic quantum computing de Syrus Ziai, PsiQuantum, 2018 (72 slides) ainsi que dans Large-scale quantum photonic circuits in silicon, 2016 (13 pages).

[797] Voir par exemple ces travaux de l'InPhyNi évoqués dans High-quality photonic entanglement based on a silicon chip par Dorian Oser, Sébastien Tanzilli et al, 2020 (9 pages).

[798] Voir Hybrid integrated quantum photonic circuits par Ali W. Elshaari et al, 2020 (14 pages).

[799] Source d'inspiration du schéma : Photonic quantum bits par Pascale Senellart, juin 2019 (31 slides) dans le slide 11.

Comme les photons ne restent pas en place et sont par nature circulants, nous sommes dans un rare cas où le diagramme d'un algorithme quantique correspond aussi à un schéma de circulation des qubits dans l'espace.

Les photons sont des « flying qubits » ou « qubits volants ». Ce sont les seuls ayant cette caractéristique. Les seuls autres qubits qui se déplacent dans l'espace à une échelle « macroscopique » sont certains types d'ions piégés, comme ceux d'Honeywell, qui sont guidés sur un circuit par des électrodes. Ils parcourent cependant de bien plus faibles distances que les photons.

Les portes quantiques sont programmées dynamiquement par le routage conditionnel des photons dans les circuits optiques. Ces circuits sont souvent gravés sur des composants CMOS (silicium) ou III/V (notamment en germanium).

Les pays les plus actifs dans le domaine semblent être la Chine, le Royaume Uni (notamment dans les Universités d'Oxford, de Bristol, de Cambridge et de Southhampton)[800], la France (C2N, LKB, …), en Italie[801], en Allemagne (notamment dans les Universités de Stuttgart et Paderborn), l'Autriche, l'Australie, le Japon mais les autres ne sont pas en reste avec bien entendu les USA. Ce sont d'ailleurs les « photoniciens » américains de la recherche et du secteur privé qui furent les plus actifs en 2018 dans leur lobbying pour déclencher ce qui est devenu le National Quantum Initiative Act. Il en a été de même en Europe pour le lancement du programme Flagship quantique la même année.

Les qubits photons sont la spécialité de quelques startups comme **PsiQuantum**, **Orca Computing**, **Tundra Systems Global**, **Quix, Quandela** (ces deux derniers travaillant ensembles) et **Xanadu**.

En photonique, le *litmus test* exploité pour l'atteindre est la simulation de l'**échantillonnage du boson** (« boson sampling »). La suprématie quantique de Google d'octobre 2019 avait d'ailleurs été atteinte avec un générateur de nombres aléatoires présentant des similitudes avec le boson sampling. L'un comme l'autre sont à la fois incompréhensibles pour le commun des mortels.

[800] Selon Quantum Age technological opportunities du gouvernement UK Office of Science en 2016 (64 pages).

[801] Fabio Sciarrino de l'Université La Sapienza de Rome, a réalisé en 2013 un échantillonnage de bosons avec une puce comprenant 13 ports en entrée et 13 ports en sortie, avec trois photons. Voir Efficient experimental validation of photonic boson sampling against the uniform distribution, 2013 (7 pages).

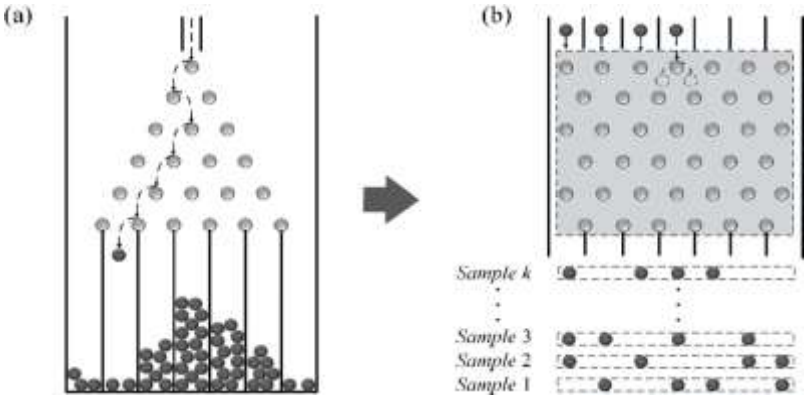
L'idée de l'échantillonnage du boson revient à **Scott Aaronson** et **Alex Arkhipov**, du MIT, dans un papier publié en 2010[802]. Ils avaient imaginé un exercice de style réalisable avec de l'optique linéaire qui serait impossible à simuler avec un calculateur traditionnel. Pour mémoire, un boson est une particule de spin entier par opposition aux fermions qui sont de spin demi-entiers, dont les photons[803].

L'échantillonnage de bosons est un exercice de style consistant à échantillonner les distributions de probabilités de répartition de photons identiques et indiscernables au travers d'un système à base d'interféromètres enchevêtrés et d'un système de mesure en sortie à base de détecteurs de photons uniques. Il est censé être réalisable avec du « calcul quantique » à base de photons et impossible à réaliser avec des calculateurs traditionnels à partir d'un certain seuil, ce qui génère un autre niveau de « suprématie quantique ».

La raison est qu'en mode classique, il est nécessaire pour réaliser cette simulation de faire des calculs matriciels extrêmement lourds : l'évaluation de permanents de matrices carrées[804]. On est dans la classe de problème « #P difficile » du zoo des théories de la complexité. Qui plus est, la vérification même du résultat obtenu ne peut même pas être réalisée par un ordinateur classique[805].

L'échantillonnage du boson est l'analogue quantique et photonique de la fameuse expérience de la planche de **Galton** où des billes traversent des rangées de clous de manière aléatoire et se retrouver à la fin dans des colonnes, avec une distribution gaussienne[806].

Cette expérience fait appel à des concepts de probabilité divers : convergence d'une loi binomiale de répartition vers une loi normale ou gaussienne, théorème de Moivre-Laplace, etc. Dans l'expérience à base de photons, ceux-ci sont injectés dans une série d'interféromètres les combinant avec leur voisin de manière aléatoire.



Par contre, la répartition à la fin ne suit pas une gaussienne. Et elle dépend des photons que l'on envoie au point de départ. C'est là que se trouvent les variables du problème à résoudre.

La pertinence de l'exercice de style de l'échantillonnage du boson est toujours sujette à caution. Elle vise à réaliser un phénomène physique avec des photons qui est difficile à simuler de manière classique[807].

---

[802] Voir The computational Complexity of Linear Optics par Alex Arkhipov et Scott Aaronson, 2010 (94 pages).

[803] En calcul quantique, on ne s'appuie que sur un seul type de boson : le photon. Les autres bosons sont des particules élémentaires comme les gluons ou le boson de Higgs que l'on n'observe que dans des accélérateurs de particules. On y trouve aussi des particules composites comme les paires de Cooper (double électron) à l'origine des courants supraconducteurs. Mais lorsque l'on parle d'échantillonnage du boson, il faut toujours entendre « photon ».

[804] Si vous voulez explorer la question, voir par exemple Lecture 3: Boson sampling par Fabio Sciarrino, Université de Rome, (63 slides) et Experimental boson sampling with integrated photonics du même auteur (33 slides) du même auteur qui décrit les techniques à base de laser de gravure de composants de photonique intégrés. Ainsi que Permanents and boson sampling par Stefan Scheel de l'Université de Rostock, 2018 (21 slides). Pour ce qui est de la définition de la notion de permanent dans Wikipedia, elle fait appel à des notions et notations d'algèbre linéaire qui ne sont même pas explicitées. Disons que le permanent d'une matrice est une variante de son déterminant ! Si la résolution classique de l'échantillonnage requiert le calcul de permanents de matrices, sa résolution par système d'optique linéaire ne permet pas pour autant de calculer des permanents de matrices.

[805] En 2018, une équipe chinoise réalisait une simulation numérique d'échantillonnage de bosons de 50 photons avec 320 000 processeurs du supercalculateur Tianhe-2. Voir A Benchmark Test of Boson Sampling on Tianhe-2 Supercomputer, 2018 (24 pages). Avec les 20 photons et 60 modes de l'expérience chinoise publiée en octobre 2019, un supercalculateur n'est plus en mesure de suivre.

[806] Source de l'illustration : Quantum Boson-Sampling Machine par Yong Liu et al, 2015.

La réalisation avec des photons ne relève cependant pas d'un calcul à proprement parler. Il n'y a même pas de véritable notion de qubits, de portes quantiques et de programmation, à part dans le choix des photons que l'on envoie dans le système. Les composants optiques utilisés sont tous passifs et statiques, sauf le générateur et les détecteurs de photons[808].

C'est une expérience de physique générant des interférences additives et soustractives et de la superposition d'états quantiques[809]. La difficulté de l'expérience repose surtout sur la complexité de la production de photons identiques. On est dans le registre du « simulateur quantique » plus que du calcul quantique.

Et à ce stade, personne n'a réussi à transformer (ou réduire) un algorithme utile en échantillonnage du boson. Cela pourrait cependant éventuellement déboucher sur des applications dans le chiffrement homomorphe et le blind computing[810].

Il existe aussi quelques algorithmes de simulation de vibrations moléculaires s'appuyant sur l'échantillonnage de bosons[811]. En 2020, une équipe chinoise menait une expérience voisine au boson sampling pour jouer à une variante du jeu de Go[812].

Les chercheurs chinois sont particulièrement actifs dans le domaine[813]. En juin 2019, le laboratoire d'Hefei annonçait avoir créé un processeur quantique photonique utilisant six photons avec trois degrés de liberté, donc, à base de qutrits (qubits à trois états)[814]. Les états des photons sont le chemin parcouru, la polarisation et le moment angulaire orbital. Avec un taux d'erreur de portes de 29%.

En octobre 2019, les chercheurs chinois passaient à 20 photons avec une expérience présentée comme atteignant la suprématie quantique, au même moment que l'annonce de Google Sycamore[815]. Dans cette expérience décrite dans le schéma *ci-dessous*, 20 photons sont indiscernables envoyés dans une série de splitters et aboutissent dans 60 détecteurs de photons. L'espace de Hilbert expérimenté en sortie se contentait de 14 détecteurs, avec une taille de $3,7*10^{14}$ soit 2^{48}. Avec les 60 détecteurs activés, il devrait pouvoir atteindre 60^{20} soit 2^{118}.

---

[807] Mais c'est une réalité valable pour la simulation de nombreux phénomènes physiques complexes, comme le repliement d'une protéine ou le fonctionnement d'une cellule vivante à ceci près que ces derniers restent du domaine du vivant et ne sont pas simulés dans une machine.

[808] Voir An introduction to boson-sampling par Jonathan Dowling et al, 2014 (13 pages) qui décrit bien les enjeux de réalisation de l'échantillonnage du boson.

[809] Voir l'animation Boson Sampling with Integrated Photonics, 2015 (3mn) qui décrit le cheminement des photons dans une expérience d'échantillonnage de boson ainsi que Photonic implementation of boson sampling: a review, Fabio Sciarrino, 2019 (14 pages) qui décrit dans le détail ce genre d'expérience. Malheureusement, la quantité de notions à maîtriser pour comprendre ce genre de papier est assez inabordable : espaces de Fock, permanents de matrices, opérateur unitaire de Haar, etc. Votre serviteur est largué !

[810] Vu dans Introduction to boson-sampling par Peter Rohde, 2014 (34 minutes) qui fait référence à A scheme for efficient quantum computation with linear optics par Emanuel Knill, Raymond Laflamme et Gerard Milburn, 2001 (7 pages) qui théorisait que le calcul quantique à base d'optique linéaire était plausible. On leur doit le schéma ou protocole KLM (leurs initiales), un modèle de programmation quantique à base d'optique linéaire (LOQC : linear optics quantum computing) qui présente l'inconvénient d'être très lourd en nombre de dispositifs matériels.

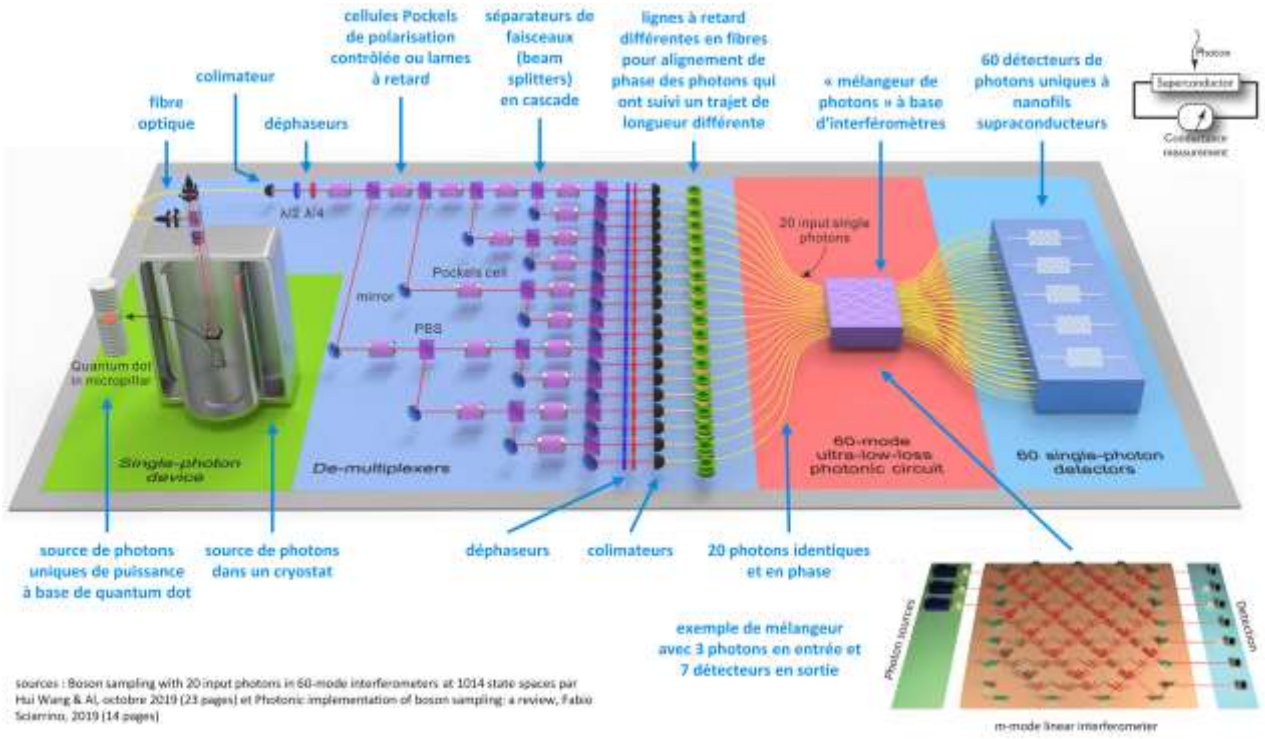
[811] Voir Boson sampling for molecular vibronic spectra par Joonsuk Huh, Alán Aspuru-Guzik et al, 2014 (7 pages) et Vibronic Boson Sampling: Generalized Gaussian Boson Sampling for Molecular Vibronic Spectra at Finite Temperature par Joonsuk Huh et al, 2017 (10 pages).

[812] Voir Quantum Go Machine par Lu-Feng Qiao et al, juillet 2020 (16 pages).

[813] Voir Des chercheurs chinois sur la voie du processeur quantique 'ultime' ?, de Bruno Cormier, septembre 2018 qui pointe sur Building Quantum Computers With Photons Silicon chip creates two-qubit processor de Neil Savage, septembre 2018 qui évoque la création d'un processeur quantique à deux qubits. L'article d'origine est Large-scale silicon quantum photonics implementing arbitrary two-qubit processing, septembre 2018 (23 pages). En fait, les chercheurs impliqués sont chinois, anglais et australiens.

[814] Voir 18-Qubit Entanglement with Six Photons' Three Degrees of Freedom de Xi-Lin Wang et al, juin 2019 (14 pages).

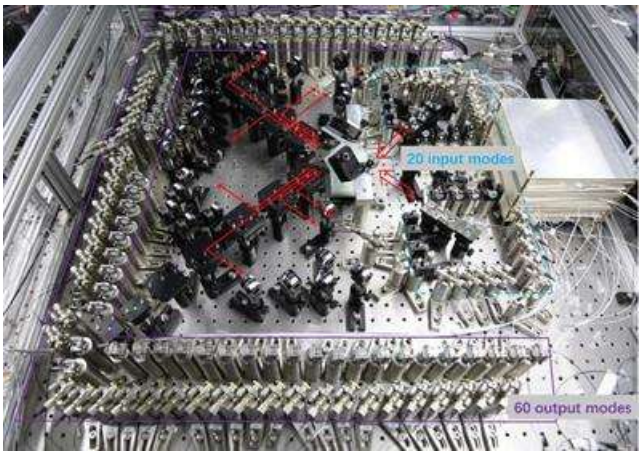
[815] Voir Boson sampling with 20 input photons in 60-mode interferometers at 10^{14} state spaces par Hui Wang et al, octobre 2019 (23 pages).



La dimension de l'espace de Hilbert d'un tel dispositif s'évalue avec la taille de l'espace de Fock de M modes occupés par N photons. Cela donnerait si j'ai bien compris un espace binomial $(\frac{M+N-1}{M})$ donc $(\frac{79}{60})$ qui est de taille égale à $\frac{79!}{60!*19!}$ (source). Mais j'ai bien du mal à raccommoder tous ces chiffres et ces concepts mathématiques abscons.

Les chercheurs chinois indiquent dans leur papier qu'ils pourraient utiliser plusieurs centaines de détecteurs en sortie et utiliser un double encodage des photons (polarisation et encodage spatial) pour démultiplier la puissance de leur système et le rendre ainsi apte à créer un système NISQ (noisy intermediate scale quantum computer), à ceci près que la capacité à le programmer ne semble pas évidente, ni ses usages.

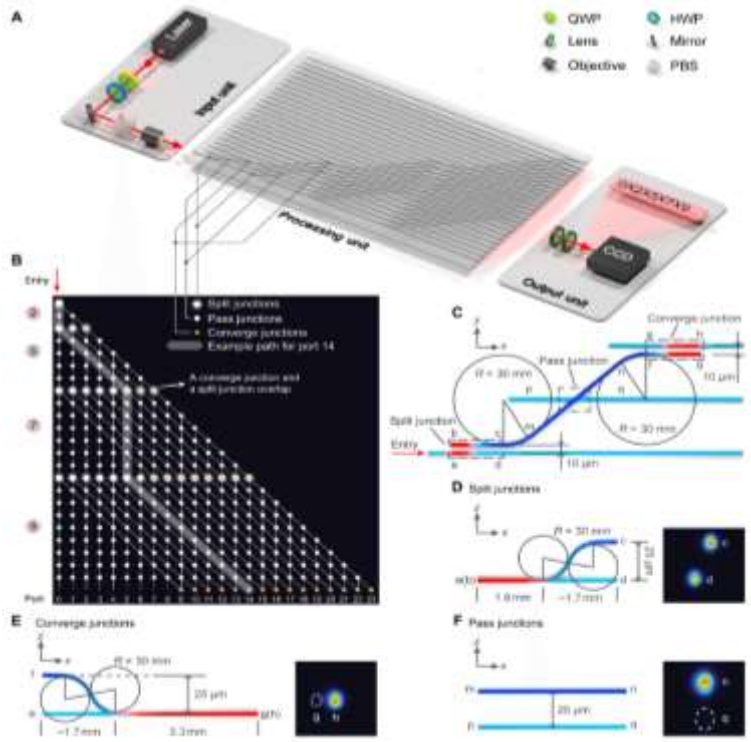
Cela représente le nombre de détecteurs de photons en arrivée à la puissance du nombre de photons en entrée. Les sources de photons identiques de qualité. Le record précédent était de 5 photons sur 16 modes et l'échantillonnage était vérifiable sur un ordinateur classique alors qu'avec ces 20 photons et 60 modes, ce n'est plus possible. Le générateur de photons était réalisé avec des quantum dots en arséniure de gallium et d'indium, placé dans un cryostat à 4K[816]. Le mélangeur de photons utilisait 396 séparateurs de faisceaux et 108 miroirs.

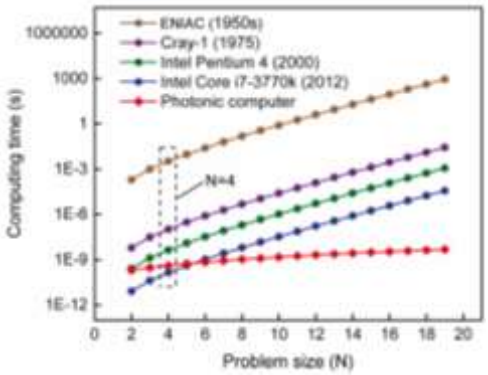


Pour que l'expérience fonctionne, il faut qu'un photon arrive en même temps dans toutes les entrées du mélangeur de photons. La probabilité correspondante est très faible. Ils utilisent des démultiplexeurs actifs avec des cellules de Pockels pour démultiplexer et diriger les photons.

[816] La source de photon proviendrait d'un laboratoire allemand situé à Wutzburg en Bavière. Elle s'inspire largement des travaux de référence dans le domaine de l'équipe de Pascale Senellart du CNRS C2N.

En 2020, d'autres chercheurs chinois ont utilisé un calculateur quantique optique à même de résoudre un problème utile, le problème de somme de sous-ensemble (subset-sum problem) qui est NP complet. Le système, *ci-dessous*, utilise un chipset bien plus miniaturisé que les expériences habituelles d'échantillonnage du boson.





sources : A scalable photonic computer solving the subset sum problem par Xiao-Yun Xu & Al, janvier 2020 (8 pages). Voir aussi Supplementary Materials for A scalable photonic computer solving the subset sum problem (7 pages).

Le problème consiste à déterminer à part d'un ensemble d'entiers signés s'il est possible d'en additionner un sous-ensemble pour obtenir un entier donné[817]. Le système utilise un laser comme source de photons. Le benchmark a été réalisé avec N=4 nombres entiers. Ils indiquent qu'en extrapolant, leur système battrait toutes les autres méthodes connues de résolution de ce genre de problème.

L'une des perspectives des qubits à base de photons consiste à contourner leurs défauts avec l'usage du MBQC et des *cluster states*, que nous avons déjà définis page 207. En effet, ceux-ci utilisent la mise en place d'un état intriqué entre tous les qubits puis une mesure de l'état progressive des autres. Cela évite la complexité des portes quantiques optiques difficiles à mettre en œuvre alors que l'on sait aujourd'hui créé un ensemble de photons bien intriqués.

Hewlett Packard Enterprise

HP fait de la recherche en informatique quantique dans son laboratoire de Bristol au Royaume-Uni. Cela couvre à la fois le calcul quantique, la cryptographie et les communications quantiques.

Ils ont investi dans leur projet "The Machine" qui est conceptuellement éloigné d'un ordinateur quantique universel et utilise un bus optique pour relier les différents composants de ce supercalculateur. Tout cela n'est pas bien clair ni bien avancé.

[817] Voir Photonic computer solves the subset sum problem, février 2020 qui fait référence à A scalable photonic computer solving the subset sum problem par Xiao-Yun Xu et al, janvier 2020 (8 pages). Voir aussi Supplementary Materials for A scalable photonic computer solving the subset sum problem (7 pages).

En partenariat avec HP, des scientifiques américains et japonais proposaient en 2008 la création d'un HPQC, High Performance Quantum Computer, avec des matrices 3D de qubits réalisés en optique linéaire contenant 7,5 milliards de qubits physiques permettant d'accumuler 2,5 millions de qubits logiques dans High performance quantum computing (7 pages). Ce projet n'a pas été suivi d'effets ! En fait, HPE a abandonné cette voie et s'en est expliqué en 2019. Ils préfèrent se focaliser sur les processeurs neuromorphiques et les memristors[818].

Leur spécialiste en photonique est **Ray Beausoleil**, basé dans la Silicon Valley. Il était spécialisé en photonique et NV centers et a abandonné cette piste, devenant un sceptique du calcul quantique. Un peu dans la lignée de Gil Kalai, il pense que les erreurs augmenteraient plus vite que l'augmentation du nombre de qubits. Pour faire bonne figure, HPE a tout de même investi dans **IonQ** en octobre 2019.

Alternatives au calcul quantique

Cette nouvelle partie introduite dans l'édition 2020 de cet ebook consolide un ensemble de technologies et sociétés qui proposent d'augmenter significativement la puissance de calcul de machines tout en ne s'appuyant pas sur les phénomènes quantiques de superposition et d'intrication.

Nous allons aborder tour à tour les supercalculateurs en général, le recuit numérique qui est une alternative au recuit quantique de D-Wave, le calcul réversible et adiabatique, les processeurs supraconducteurs, les ordinateurs probabilistes et les coprocesseurs optiques. Nombre de ces voies ont été explorées par de grands acteurs tels qu'IBM pour ls composants supraconducteurs ou par des startups et avec des hauts et des bas.

Certains comme MemComputing vont jusqu'à évoquer des accélérations exponentielles des capacités de calcul sur des architectures plus ou moins traditionnelles à base de composants CMOS classiques.

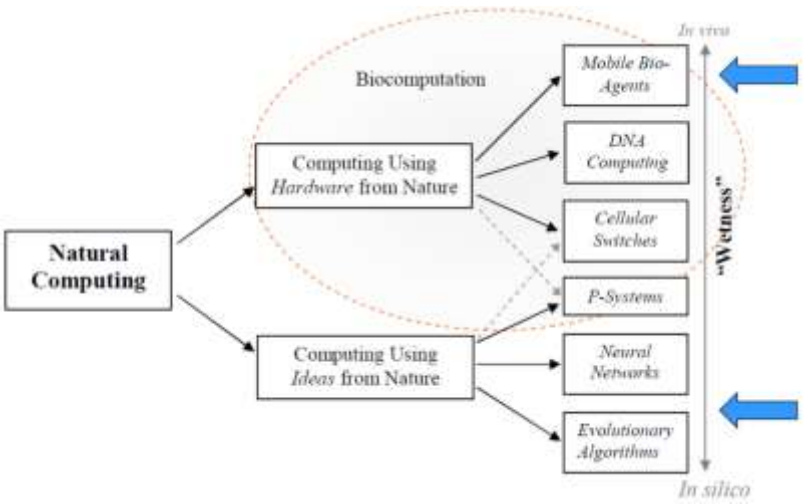
Au point de prouver implicitement que P=NP dans la théorie de la complexité, à savoir que la classe de problèmes qui peuvent être résolus en temps polynomial par rapport à leur taille est égale à celle des problèmes dont la vérification peut être réalisée en temps polynomial. Le consensus étant que P<>NP, c'est évidemment sujet à caution !

Une partie de ces technologies font partie de ce que l'on appelle l'**unconventional computing**, à savoir celles qui se différencient d'une manière ou d'une autre des technologies à base de machines de Turing et de l'architecture de Von Neumann à base d'unités de contrôle, de calcul, de registres et de mémoire qui sont la base des ordinateurs classiques d'aujourd'hui.

Je ne vais pas toutes les explorer car elles n'ont pas toutes des avantages pratiques voisins de ceux que le calcul quantique peut apporter.

[818] Voir Why HPE abandoned quantum computing research de Nicole Hemsoth, avril 2019.

C'est notamment le cas des différents domaines qui font partie du **natural computing** qui utilisent des éléments physiques issus de la nature ou sont bioinspirés par la nature[819].



Cela comprend les ordinateurs s'appuyant sur des composants biologiques, les p-systèmes ou ordinateurs à membrane, la spintronique et les processeurs neuromorphiques qui sont adaptés aux traitements de l'intelligence artificielle[820].

D'autres, comme le calcul supraconducteur, pourraient se rendre utile pour permettre aux calculateurs quantiques de « scaler ». On peut donc aussi évaluer ces différentes technologies sous l'angle de leur complémentarité, plus que de la concurrence, avec le calcul quantique.

Supercalculateurs

La suprématie quantique annoncée par Google en octobre 2019 faisait systématiquement référence à des comparaisons de puissance avec des supercalculateurs, en particulier avec l'**IBM Summit** installé au laboratoire d'Oak Ridge du Département de l'Energie US depuis 2018.

Ce genre de supercalculateur rentre dans le domaine du High Performance Computing que nous allons étudier rapidement ici pour le mettre en perspective par rapport au calcul quantique.

La notion de HPC n'a pas toujours été bien définie, ce d'autant plus qu'elle est une cible mouvante. La puissance d'un supercalculateur des années 1980 est maintenant disponible dans un simple serveur récent. On peut cependant partir des besoins applicatifs. Le HPC et les supercalculateurs font essentiellement de la simulation numérique et de l'analyse de données complexes. Ce sont des outils mis à disposition à la fois de chercheurs et de l'industrie pour leurs besoins de calculs les plus avancés.

Ils servent aux prévisions météo[821], aux simulations dans la chimie organique et inorganique, à la simulation pour l'aviation et l'automobile, à la simulation de l'arme nucléaire[822], dans la finance, de manière plus récente, dans le machine et le deep learning et, on a tendance à l'oublier, également pour générer des images de synthèse pour le cinéma. Les modèles mathématiques utilisés dans les supercalculateurs servent notamment à résoudre des équations aux dérivées partielles et à faire des simulations à N-corps.

---

[819] Source du schéma : Unconventional Computing: computation with networks biosimulation, and biological algorithms par Dan Nicolau, McGill University, 2019 (52 slides).

[820] Voir Unconventional Computation par Bruce MacLennan, de l'Université du Tennessee, qui est une référence du domaine, octobre 2019 (306 pages) ainsi que Unconventional Computing par Andrew Adamatzky et al, Springer, 2018 (698 pages).

[821] Comme pour IBM Weather Channel et son modèle de prévision GRAPH (Global Hi-Resolution Forecasting System) qui est précis à 3 km près. Il s'appuie sur un HPC, le Dyeus avec 76 nœuds de 4 GPU V100 et 2 CPU Power 9. Voir High Performance Computing for Numerical Weather Prediction at The Weather Company, an IBM Business par Todd Hutchinson et John Wong, 2019 (18 slides).

[822] C'est le rôle du supercalculateur du CEA-DAM de Bruyère le Chatel en Ile de France qui est alimenté en données provenant du laser Megajoule situé en Aquitaine.

Ces systèmes sont exigeants à plusieurs titres : en capacité de calcul, souvent évaluée en opérations sur des nombres flottants à la seconde, si possible en double précision (FLOPS), en capacité de stockage de données et surtout, dans la capacité à faire circuler ces données rapidement entre stockage, mémoire et processeurs. C'est d'ailleurs dans ces derniers domaines que les supercalculateurs se distinguent le plus des serveurs de commodité utilisés dans les data-centers.

Le tableau *ci-contre* décrit fort à propos le décalage de consommation d'énergie entre le calcul et les accès mémoire, qui sont de plus en plus couteux, plus la mémoire est éloignée du processeur. Le rapport va jusqu'à plus de 1 à 1000 ! Cela explique les tentatives de rapprochement de la mémoire des unités de calcul qui se développent de plus en plus.

Function	Energy in Picojoules
8-bit add	0.03
32-bit add	0.1
FP Multiply 16-bit	1.1
FP Multiply 32-bit	3.7
Register file access*	6
Control (per instruction, superscalar)	20-40
L1 cache access	10
L2 cache access	20
L3 cache access	100
Off-chip DRAM access	1,300-2,600

calculs

accès cache et mémoire

The End of Moores Law & Fater General Purpose Computing and a Road Forward John Hennessy 2019 (49 slides)

Historiquement, les supercalculateurs comme les **Cray**[823] s'appuyaient sur des processeurs vectoriels maison et des systèmes massivement parallèles propriétaires divers. Ces systèmes ont été balayés ces dix dernières années par des architectures à base de clusters utilisant des processeurs standards du marché de type CPU, complétés depuis quelques années par des GPU. Un cluster comprend plusieurs nœuds contenant chacun plusieurs CPU et/ou GPU, eux-mêmes multi-cœurs, et de l'interconnexion rapide entre ces nœuds, entre clusters, et un accès rapide au stockage des données, de plus en plus à base de SSDs, bien plus rapides que les disques durs.

Les clusters à base de processeurs standardisés correspondent maintenant à 85% des 500 plus grands supercalculateurs référencés dans le monde[824]. Les CPU proviennent le plus souvent d'Intel (Xeon), AMD (Opteron puis EPYC), IBM (Power9) alors que Nvidia domine le marché des accélérateurs avec ses GP-GPU (general purpose GPU), dont le célébrissime V100 de génération Volta lancé en 2017 et son successeur A100 Ampere annoncé en mai 2020.

C'est une forme de commoditisation du supercalculateur même si cela reste des architectures lourdes à déployer dans de grandes salles blanches. La valeur ajoutée s'est déplacée dans l'architecture d'interconnexion, de la mémoire et du stockage et bien entendu, du logiciel.

L'interconnexion dans les clusters utilise des technologies telles que le NVLink de Nvidia qui relie à grande vitesse GPU et CPU. Les clusters sont reliés entre eux par des liaisons multiples à 200 Gbits/s à fibre optique, provenant souvent de **Mellanox**, filiale de Nvidia depuis 2019. A plus grande échelle, HPE fait la promotion de l'architecture **Gen-Z** optimisée pour l'accès aux données dans les systèmes distribués "data-centric".

Les opérations sur supercalculateurs sont programmées avec différentes outils de développement. Citons par exemple **OpenFOAM**, un SDK open source qui sert à simuler la mécanique des fluides, les réactions chimiques, les transferts de chaleur, la mécanique des solides, l'électromagnétisme et aussi ka finance. Et puis aussi **LS-DYNA** pour la simulation de structure. Enfin, la bibliothèque de développement d'applications parallèles pour Fortran, C et C++ **OpenMP** est très couramment utilisée pour le calcul scientifique, tout comme **OpenACC**.

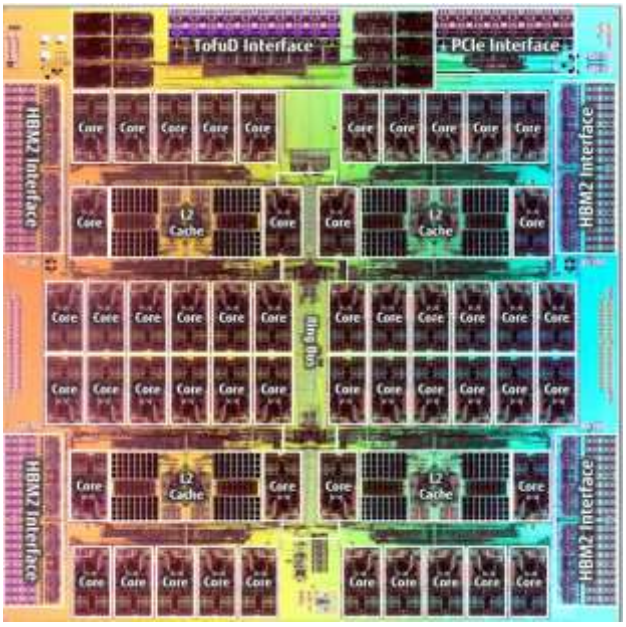
---

[823] Cray a été acquis par HPE en 2019.

[824] Le Top 500 s'appuie sur un benchmark standardisé, le HPL pour High Performance Linpack. Il sert à résoudre un jeu d'équations linéaires utilisant de l'élimination gaussienne exploitant des matrices denses et du calcul en nombre flottants. Voir https://www.top500.org/lists/top500/2019/11/.

N'oublions pas également qu'il existe nombre d'algorithmes d'optimisation basés sur des approximations acceptables d'un point de vue pratique, comme pour les problèmes du type de celui du voyageur du commerce.

Les Chinois et les Japonais développent leurs propres processeurs maison pour leurs supercalculateurs, histoire de limiter leur dépendance vis-à-vis des Américains, au moins pour les Chinois.



Au Japon, le supercalculateur **Fujitsu** Fugaku exploite des chipsets Fujitsu A64FX comprenant 52 cœurs arm et 32 Go de mémoire HBM2 délivrant une puissance nominale de 2,7 TFLOPS (layout du processeur *ci-dessous*). Le Fugaku qui n'est pas un poisson vénéneux fait un total de 415 PFLOPS en double précision avec 396 racks et 152 064 processeurs.

Son installation s'achevait en juin 2020 et permettait à Fujitsu de gagner la première place du podium des plus puissants supercalculateurs du monde devant les USA avec l'IBM Summit[825].

Le plus grand supercalculateur chinois est le **Sunway TaihuLight** du National Supercomputing Center de Wuxi. D'une capacité de 93 PFLOPS, il utilise 40 960 processeurs maison SW26010 à 256 cœurs 64-bit à architecture RISC (à jeu d'instruction simplifié). La Chine a déployé 40% des supercalculateurs du Top 500 mondial devant les USA avec 23%, mais seulement 6% du TOP50 pour 38% aux USA et 10% pour la France, qui est devant la Chine et derrière le Japon (à la mi-2019).

L'Europe a lancé de son côté le **EPI** (European Processor Initiative), un projet d'indépendance technologique côté processeur multi-cœurs destiné aux supercalculateurs. Il associe surtout les Allemands et les Français, notamment d'Atos.

L'effort est porté par la startup **SiPearl** portée par Philippe Notton. Il s'intègre dans le projet **EuroHPC** de création de supercalculateurs pré-exaflops et exaflops (dont un en Allemagne et un en France pour ce dernier cas). Le budget prévu est d'un milliard d'Euros réparti à moitié entre la Commission Européenne et les Etats.

[825] Voir Fujitsu and RIKEN Take First Place Worldwide in TOP500, HPCG, and HPL-AI with Supercomputer Fugaku, juin 2020 et Japanese Supercomputer Development and Hybrid Accelerated Supercomputing par Taisuke Boku, 2019 (59 slides); Supercomputer Fugaku, 2019 (13 slides) et The first "exascale" supercomputer Fugaku & beyond par Satoshi Mastuoka, août 2019 (80 slides).

En France, le supercalculateur **Jean Zay** déployé fin 2019 au GENCI pour le compte du CEA, du CNRS et d'Inria est équipé de 1300 GPU Nvidia V100 et de 3462 CPU Intel Xeon Cascade Lake. Il est refroidi par eau « chaude » (passant de 30°C à 42°C). Il était déployé dans le cadre du plan IA français annoncé en 2018. Il devrait voir sa puissance doubler en 2020.

Le centre de calcul GENCI doit héberger un calculateur quantique probablement d'origine **Pasqal** d'ici quelques années. Il sera intégré dans une architecture de calcul hybride.

Depuis l'avènement du cloud, les ressources de HPC et des supercalculateurs y sont maintenant proposées à la demande. D'ailleurs, il faut rappeler qu'un centre de calcul du cloud ne fournit pas forcément des ressources de HPC. Cela dépend de l'architecture des serveurs et des clusters et du packaging de l'offre de l'opérateur de cloud. Cette notion peut être associée à celle d'hyperscale qui couvre la capacité d'une infrastructure de cloud à s'adapter à l'augmentation en besoins de calcul du client.

Les applications de l'IA sont les plus récentes et nouvelles qui sont prises en charge par les supercalculateurs, ce d'autant plus qu'ils sont équipés de GPU qui contiennent des tenseurs permettant de gérer de manière efficace des opérations matricielles, très courantes dans les réseaux de neurones. En pratique cependant, les supercalculateurs continuent de faire en majorité des calculs de simulation qui ne relèvent pas du machine learning. Ce d'autant plus que les frameworks OpenMP et OpenACC sont portés sur les GPU Nvidia, ce qui facilite leur utilisation pour un tas d'applications scientifiques existantes.

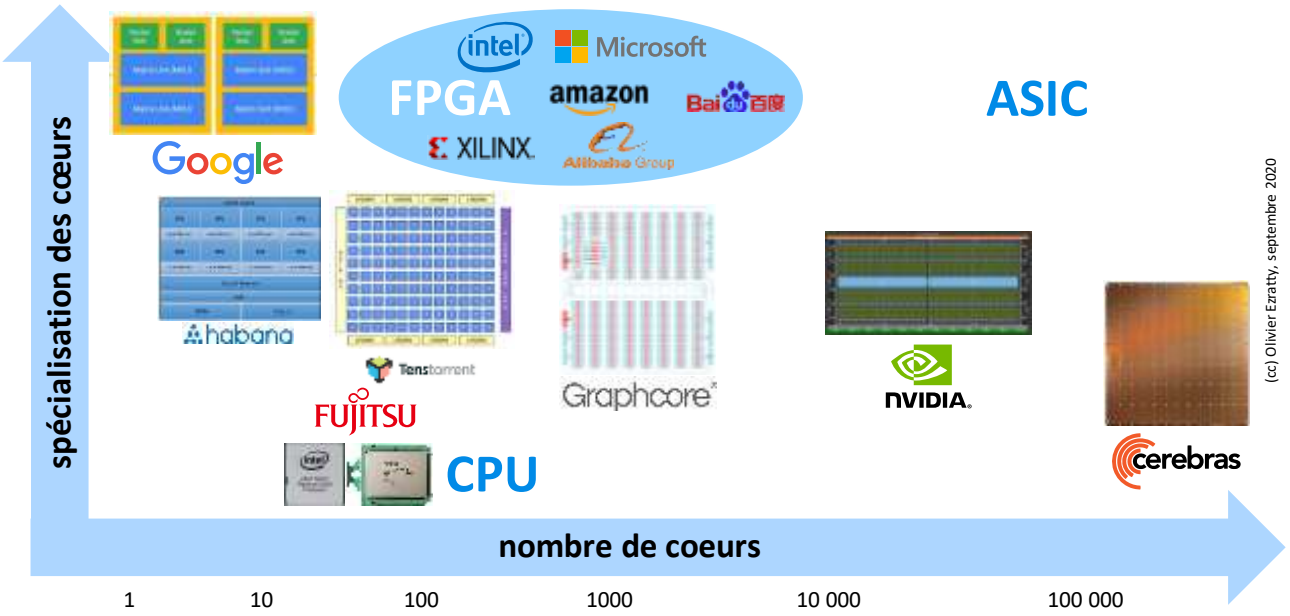
Le marché des processeurs adaptés à l'IA et au machine learning pullulent depuis quelques années et adoptent des approches très variées. On peut les représenter comme ci-dessous sur deux axes : d'un côté la spécialisation plus ou moins grande des cœurs et de l'autre le nombre de ces cœurs.

Les TPU de Google sont très spécialisés pour l'entraînement de réseaux de neurones, surtout les réseaux convolutifs de reconnaissance d'image. Les GPU de Nvidia contiennent des milliers de cœurs de calcul arithmétique classiques ainsi que des centaines de tenseurs pour le calcul matriciel ce qui en optimise la versatilité.

Le processeur le plus extrême est le **Cerebras** avec ses 400 000 cœurs. C'est un chipset de 21 cm de côté qui contient 1,2 trillions de transistors et 18 Go de mémoire cache intégrée. Il est déjà déployé dans deux serveurs de tests avec une et deux de ces « puces » et génère une très bonne performance dans l'entraînement de réseaux de neurones. Enfin, les FPGA sont des circuits programmables dynamiquement qui permettent de créer des circuits sur mesure à bon coût. Ils sont utilisés par certains opérateurs de cloud comme Microsoft (avec Brainwave) et les Chinois Alibaba et Baidu, pour la flexibilité que cela leur apporte.

Certains de ces acteurs développent leurs propres supercalculateurs. Google a créé ses TPU pods sur plusieurs générations pour ses data-centers. Chaque carte TPU contient quatre processeurs et totalise 420 TFLOPS et 128 Go de mémoire.

Leur Pod en comprend 320 et totalise 100 PFLOPS avec 32 To de mémoire HBM2. Nvidia intègre ses GPU A100 dans des SuperPods totalisant 140 serveurs DGX A100 et 1120 A100 et 4 Po de stockage, pour 700 PFLOPS. Mais attention, ces FLOPS ne sont pas forcément les mêmes que ceux qui servent à évaluer les supercalculateurs du TOP 500. La communication des fournisseurs est parfois trompeuse.

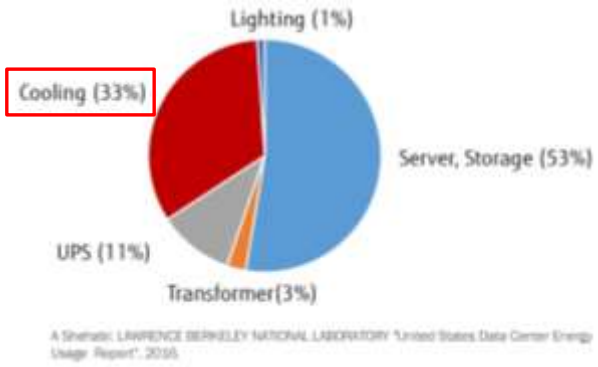


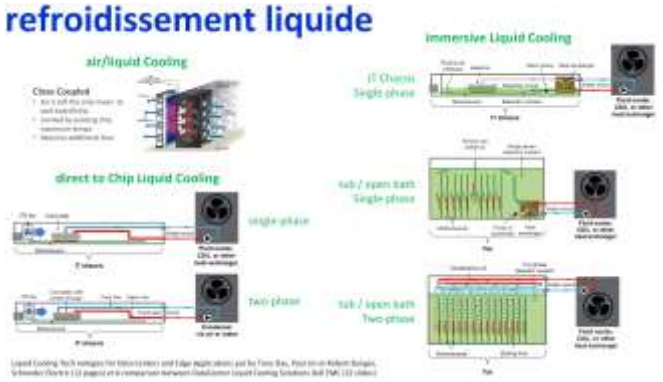
A la fois pour améliorer les performances et pour réduire la consommation énergétique, des pistes sont lancées pour rendre ces calculs plus efficaces : il y a l'**Approximate Computing** qui réduit la précision sans affecter les résultats, la **Quantification** (quantization) qui passe de calculs en nombre flottants à un calcul en nombres entiers pendant ou après l'entraînement, les **Binary Neuron Networks** qui sont encore plus simples et nous ramènent presque à l'ère des Perceptrons de 1957 et le **Sparse Computing** qui optimise le calcul matriciel en éliminant les valeurs nulles. Enfin et surtout, il y a l'intégration étroite entre la mémoire et les capacités de calcul. Ainsi, la startup française **UpMem** propose-t-elle des modules de mémoire DRAM qui intègrent des dizaines de cœurs RISC-V pour réaliser des calculs au sein même de la mémoire et accélérer d'un facteur 10 certains traitements, notamment pour les applications de « big data ». On peut aussi faire varier la fréquence d'horloge des cœurs lorsqu'ils attendent des données en provenance de la mémoire.

Les supercalculateurs sont assez voraces en énergie. Leurs processeurs de plus en plus intégrés consomment plusieurs centaines de Watts. Le tiers de la consommation en énergie électrique d'un data center est passe dans le refroidissement. Les racks de serveurs dégagent maintenant facilement plus de 10 kW.

C'en est au point où il faut maintenant privilégier le refroidissement liquide pour évacuer la chaleur des composants, en général avec de l'eau. Celui-ci procure un meilleur rendement effectif. Il est proche de 1,1 pour le Jean Zay.

Malgré les benchmarks de suprématie quantique qui défraient l'actualité, les supercalculateurs seront toujours pertinents. Les applications qui brassent de grandes quantités de données ne sont pas les plus appropriées pour le calcul quantique, même avec des zillions de qubits. En effet, le temps de chargement de l'information dans les qubits risque de devenir un énorme goulot d'étranglement car il repose sur de très longues séries de portes quantiques.





Les applications adaptées au calcul quantique sont plutôt frugales en données. Elles servent à résoudre des problèmes complexes de recherche de combinatoire ou de minimums énergétiques. Il est probable que nous aurons pendant longtemps des architectures hybrides associant des calculateurs ou supercalculateurs classiques et des accélérateurs quantiques. C'est l'approche retenue par les fournisseurs de supercalculateurs comme **Atos**.

Recuit numérique

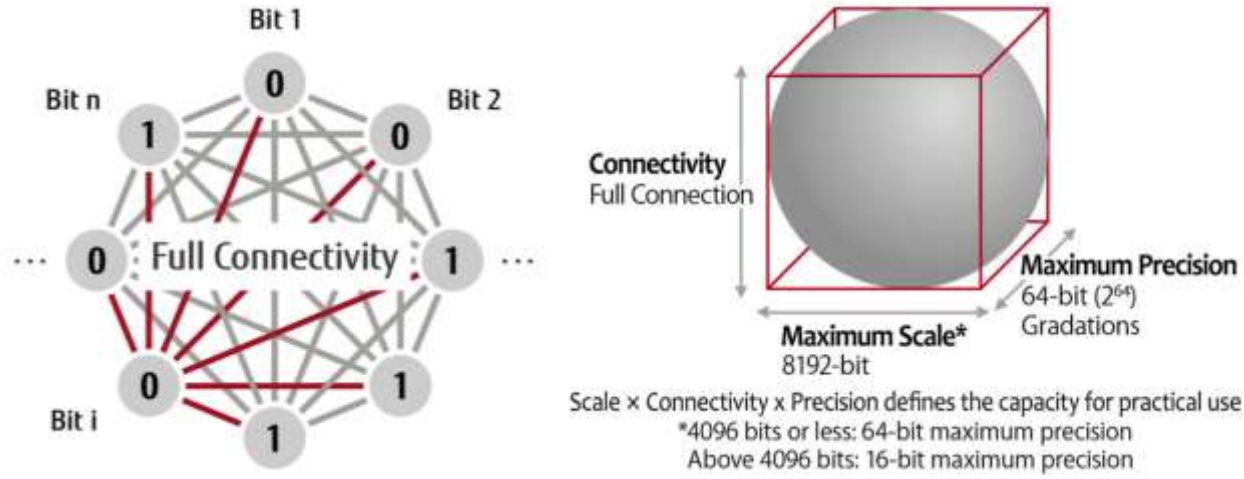
Le recuit numérique est une variante non quantique du recuit quantique utilisé dans les ordinateurs de D-Wave. Il présente l'avantage d'exploiter des technologies de production standard de composants, en CMOS. Le niveau d'accélération fourni au niveau du calcul n'est a priori pas exponentiel.

Fujitsu annonçait début juin 2018 un ordinateur à recuit digital fonctionnant à température ambiante. Fujitsu est un des leaders mondiaux du marché des supercalculateurs. Il était donc logique, comme pour le Français Atos, qu'ils explorent des moyens de continuer à faire monter en puissance leur offre. Fin mai 2018, le Japonais annonçait avoir mis au point un ordinateur utilisant le recuit digital à température ambiante.

Il scalerait bien mieux que ceux de D-Wave[826]. La technologie dénommée "Digital Annealer" est développée sur silicium en CMOS et en partenariat avec l'Université de Toronto. Elle serait déjà proposée dans le cloud. Elle sert à résoudre des problèmes d'optimisation et notamment à réaliser du criblage de molécules dans les biotechs.

Le "Digital Annealer" est un chipset dédié comportant 1 024 blocs de mise à jour de bits intégrant de la mémoire pour stocker leurs poids et avec une précision de 16 bits, des blocs logiques pour réaliser des inversion de valeurs, et les circuits de contrôle associés. Cela fait penser à des réseaux de neurones à base de memristors dans le principe. Comme pour les D-Wave, les problèmes sont chargés dans le système sous forme de matrices avec des biais dans les liaisons entre éléments et le système recherche un état d'énergie minimum pour résoudre le problème.

[826] Voir Fujitsu's CMOS Digital Annealer Produces Quantum Computer Speeds, 2018.



Son concepteur, **Hidetoshi Nishimori**, du Tokyo Institute of Technology, pense que Fujitsu arrivera à créer des solutions plus performantes que celles de D-Wave. Fujitsu annonçait en 2019 sa seconde génération des puces, dotées de 8192 blocs. Ils prévoient d'atteindre ensuite un million de blocs alors que la montée en puissance prévue de D-Wave est bien plus lente.

La partie logicielle est fournie par le Canadien **1QBit**, dans lequel ils ont investi. Le DAU doit être fourni sous forme de services dans le cloud. Ce système n'est cependant pas du tout quantique ! Il concurrence malgré tout directement D-Wave. Dans le même temps, Fujitsu collabore depuis avril 2020 avec la startup **Quantum Benchmarks** (Canada) sur les algorithmes quantiques et les codes de suppression d'erreurs, en s'appuyant sur un algorithme d'IA Fujitsu et sur leur expérience acquise avec leur recuit digital. Mais cela illustre peut-être le fait qu'ils s'intéressent tout de même au calcul quantique[827].

MemComputing, Inc.

On peut ranger la mystérieuse startup **MemComputing** (2016, USA) dans une catégorie voisine de l'offre de Fujitsu.

C'est une solution qui s'inspire du calcul à recuit quantique. Leur solution matérielle MemCPU Coprocessor place de la mémoire près d'unités de calcul dans des unités de traitement[828]. Mais ce n'est pas tout.

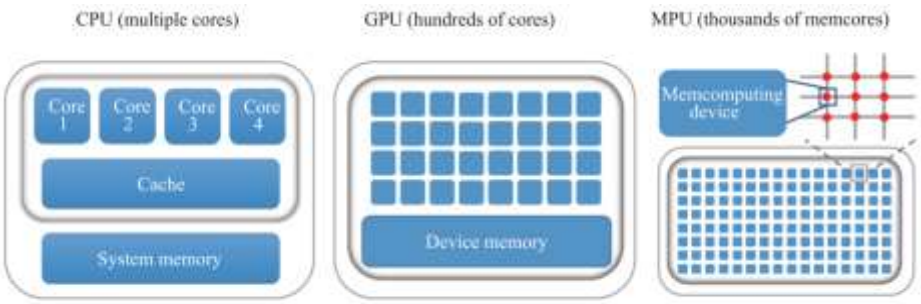
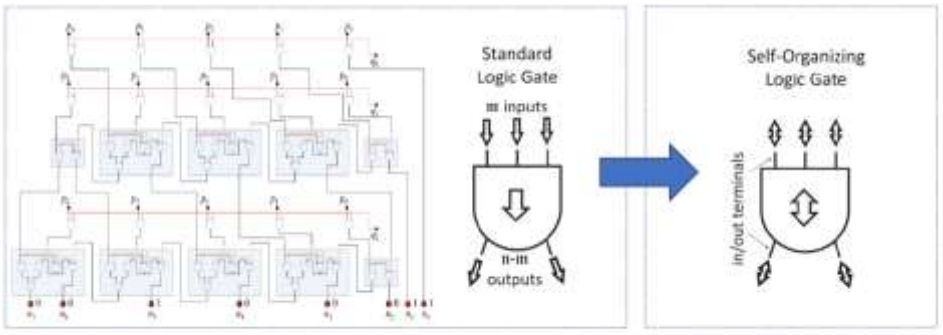


Figure 1 (Color online) Comparison of CPU, GPU, and MPU.

[827] Voir Fujitsu Laboratories and Quantum Benchmark Begin Joint Research on Algorithms with Error Suppression for Quantum Computing, avril 2020 et Voir Fujitsu Laboratories and Quantum Benchmark Begin Joint Research on Algorithms with Error Suppression for Quantum Computing par Fujitsu, mars 2020.

[828] Elle est décrite dans Memcomputing: fusion of memory and computing par Yi Li et al, 2017 (3 pages) d'où provient ce schéma.

Ces cellules de calcul qui ressemblent à des memristors auraient des entrées et sorties symétriques interconnectées aux cellules avoisinantes et elles gèrent exclusivement des nombres entiers. Pas de calcul en nombre flottants au programme !



A traditional Boolean circuit using logic Gate for prime factorization — Moving from traditional gates to terminal-agnostic gates

Elles permettraient de trouver automatiquement un équilibre complexe d'un système paramétré. C'est le principe des SOLGs (Self Organizing Logic Gates) du schéma *ci-dessus*[829].

La société a été créée par le serial entrepreneur **John Beane** et deux chercheurs en physique, **Massimiliano Di Ventra** et **Fabio Traversa** qui ont une belle bibliographie sur le sujet du « memory computing » dont ils sont à l'origine[830].

Leu architecture permettrait de résoudre diverses classes de problèmes NP-complets et NP-difficiles[831] en temps polynomial. Ils annoncent des gains de performance significatifs : quatre ordres de grandeur pour les applications de machine learning, donc une performance multipliée par 10 000 ! Les domaines d'applications annoncés comprennent la résolution de problèmes de planification et d'optimisation comme celui du voyageur de commerce, de combinatoire[832], de bioinformatique, d'entraînement de réseaux de neurones[833] et même de factorisation de nombres entiers[834], à chaque fois, avec un gain exponentiel de temps de calcul par rapport aux méthodes classiques.

Pour l'instant, leur solution est émulée dans des ordinateurs classiques et fournie sous forme de SDK opéré dans le cloud qu'ils ont conçu en partenariat avec **Canvass Labs** (2017, USA). Leur composant électronique n'est pas encore fabriqué, même à l'état de prototype, et il n'est d'ailleurs pas évident de déterminer s'il est possible de le fabriquer.

Ils ont notamment réussi à traiter des problèmes de type MIPLIB (Mixed Integer Programming Library) considérés comme intractables avec une réponse en 60 secondes sur un serveur tournant sous Linux et avoir même battu un D-Wave. Cela sert à trouver une combinaison de nombres entiers donnés pouvant générer zéro une fois additionnés (le « Subset Sum problem »). La startup arrive à obtenir un avantage d'échelle quantique avec l'émulation de son procédé sur des processeurs traditionnels. Ce qui revient à remettre en cause toutes les théories actuelles de la complexité. Bref, à en donner le tournis.

---

[829] Les SOLGs sont décrites dans le brevet Self-Organizing Logic Gates and Circuits and Complex Problem Solving With Self-Organizing Circuits, mars 2018 (37 pages).

[830] Voir Universal Memcomputing Machines, par Fabio Traversa et Max Di Ventra, 2014 (14 pages) et Perspective: Memcomputing: Leveraging memory and physics to compute efficiently, par Fabio Traversa et Massimilio Di Ventra, 2018 (16 pages).

[831] Voir Memcomputing NP-complete problems in polynomial time using polynomial resources and collective states, par Fabio Traversa, Massimilio Di Ventra et al, 2014 (10 pages) et Evidence of an exponential speed-up in the solution of hard optimization problems, Fabio Traversa et al, 2018. Enfin, voir cette Conférence de Massimiliano Di Ventra à Berkeley en 2016 (26 minutes).

[832] Voir Stress-testing memcomputing on hard combinatorial optimization problems par Fabio Traversa, Max Di Ventra et al, 2018 (6 pages).

[833] Voir Accelerating Deep Learning with Memcomputing par Haik Manukian, Fabio Traversa et Massimiliano Di Ventra, 2018 (8 pages).

[834] Voir Polynomial-time solution of prime factorization and NP-hard problems with digital memcomputing machines, par Fabio Traversa et Max Di Ventra, 2017 (22 pages).

En avril 2020, MemComputing annonçait mettre à disposition sa brique logicielle XPC (Xtreme Performance Computing) en cloud à disposition des chercheurs travaillant sur le Covid-19[835].

Alors, cette technologie est-elle tout bonnement révolutionnaire et pourrait-elle rendre caduque bon nombre d'efforts dans le calcul quantique ou il y a-t-il un ou plusieurs lézards ? Bien, il y en a plein. Comment initialiser le système pour qu'il soit proche d'un minimum global ? Quelle est leur capacité réelle à créer ces SOLGs dans des composants CMOS actuels ? Comment gérer le bruit du système qui pollue les calculs ? En fait, leur approche ne serait pas scalable d'après plusieurs spécialistes dont le renommé Scott Aaronson [836].

Calcul réversible et adiabatique

Depuis les années 1960, des chercheurs envisagent de réduire de plusieurs ordres de grandeur la consommation d'énergie des ordinateurs en s'appuyant sur le principe du calcul réversible adiabatique[837]. L'objectif est surtout énergétique et ne sert pas à accélérer la croissance des capacités de calcul, associée à l'application de la « la loi de Moore ». Dans certains cas, il est même antinomique avec cette loi, les principales techniques employées ayant comme conséquence un ralentissement du calcul.

Tout cela tient à la compréhension que l'on a depuis les années 1960 du lien entre le calcul et les processus thermodynamiques. Nous avons déjà évoqué **Rolf Landauer** et sa formulation en 1961 de l'équation selon laquelle le processus de traitement de l'information qui dissipe de l'énergie est celui de l'effacement de la mémoire[838]. L'information effacée est transformée en chaleur à l'extérieur de l'ordinateur, augmentant l'entropie de l'environnement.

Rolf Landauer estima que l'énergie dissipée était toujours supérieure à **kTln(2)** par bit effacé, k étant la constante de Boltzmann (1.38×10^{-23} J/K), T, la température en Kelvin et ln(2) le logarithme de 2 (environ 0,69315). A température ambiante, cela donne 0,017 eV. C'est la fameuse limite de Landauer[839].

Plus généralement, le principe de Landauer illustrait le lien entre les notions de réversibilité logique et physique du calcul. La première est liée à la capacité à déterminer les valeurs en entrée d'un calcul en fonction des valeurs en sortie.

---

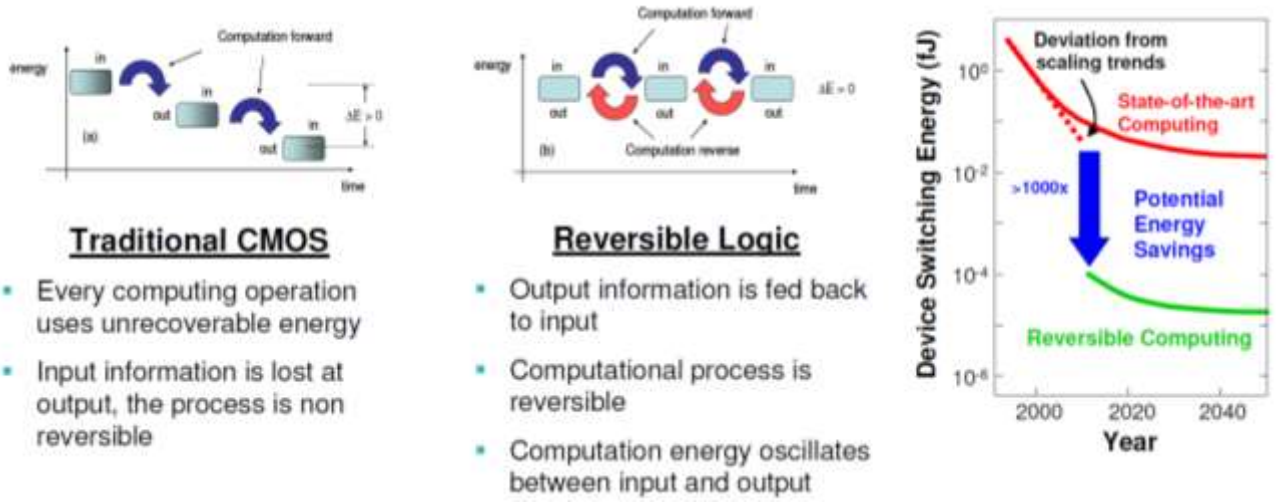
[835] Voir MemCPU XPC SaaS Platform available free for COVID-19 Research, 2020.

[836] Voir A Note on `Memcomputing NP-complete problems...' and (Strong) Church's Thesis par Ken Steiglitz, 2015 (2 pages) qui démontre rapidement que cela n'est pas possible. Il en va de même pour Memrefuting par Scott Aaronson en 2017 et pour A review of « Memcomputing NP-complete problems in polynomial time using polynomial resources » par Igor Markov, 2015 (3 pages).

[837] Pour rédiger cette partie, j'ai utilisé les nombreuses références de l'excellente présentation Reversible Adiabatic Classical Computation – an Overview par David Frank, 2014, IBM (46 slides) d'où provient l'illustration de cette page, ainsi que par The Future of Computing Depends on Making It Reversible par Michael P. Frank, 2017 et The Case for Reversible Computing par Michael P. Frank, 2018 (19 pages). Voir aussi Computers That Can Run Backwards par Peter Denning et Ted Lewis, 2017 ainsi que Theory of Reversible Computing par Kenichi Morita, 2017 (463 pages). J'ai aussi suivi un cours sur la thermodynamique quantique délivré en ligne entre avril et mai 2020 par Alexia Auffèves du CNRS Institut Néel.

[838] Voir Irreversibility and heat generation in the computing process, par Rolf Landauer, dans l'IBM Journal of Research & Development, 1961 (9 pages).

[839] La limite de Landauer a été vérifiée expérimentalement cinquante ans plus tard, en 2011, par une équipe de l'ENS Lyon dans le groupe de Sergio Ciliberto. Voir Experimental verification of Landauer's principle linking information and thermodynamics par Antoine Bérut et Al, 2011 (4 pages) et Information and thermodynamics: Experimental verification of Landauer's erasure principle par Antoine Bérut, Artyom Petrosyan et Sergio Ciliberto, ENS Lyon, 2015 (26 pages). D'autres expériences ont suivi pour valider cela, avec des mémoires magnétiques, comme Experimental test of Landauer's principle in single-bit operations on nanomagnetic memory bits par Jeongmin Hong et al, 2016 (6 pages). Le principe consiste à abaisser la barrière énergétique de transition d'état du bit lorsqu'une opération est nécessaire puis à la remonter ensuite pour préserver l'état du bit. Voir également l'expérience de Delft de 2018 dans Quantum Landauer erasure with a molecular nanomagnet par R. Gaudenzi et al, 2018 (7 pages).



La seconde porte sur le fait que le déroulement d'un processus physique à l'envers pourrait ne pas violer les lois de la physique, dont l'incontournable seconde loi de la thermodynamique selon laquelle l'entropie d'un système thermodynamique augmente toujours sauf si le processus est réversible.

Aujourd'hui, un composant CMOS dépense une énergie de 5000 eV pour effacer un bit, soit presque 300 000 fois plus que la limite de Landauer. On pourrait gagner un ordre de grandeur et descendre à 500 eV, mais cela ferait encore 30 000 fois plus que la limite de Landauer. Pour réduire la consommation d'énergie du calcul, pourquoi donc ne pas éviter d'effacer de l'information et, au passage, rendre tout calcul physiquement et logiquement réversible ?

Cela nécessiterait de revoir toute la logique actuelle du calcul qui repose à bas niveau sur des portes logiques irréversibles qui détruisent de l'information comme les portes NAND ou XOR qui génèrent un bit à partir de deux bits. Un autre chercheur d'IBM collègue de Rolf Landauer, **Charles Bennett**, imagina en 1973 une méthode de calcul permettant d'éviter cet effacement d'information dissipateur d'énergie sans pour autant nécessiter une mémoire infinie[840].

Il fut suivi par **Edward Fredkin** et **Tommaso Toffoli** qui, en 1978 et 1982, imaginèrent des portes logiques réversibles en s'inspirant d'un modèle physique métaphorique à base de boules de billard, le BBM pour billiard ball model[841].

Ces portes logiques ont autant de sorties que d'entrée et il est facile de comprendre pourquoi elles deviennent ainsi réversibles. Si leur modèle n'était pas pratiquement réalisable avec l'électronique de l'époque, leur concept fut cependant ensuite réutilisé dans les portes quantiques qui portent leur nom et que nous avons déjà traitées dans cet ebook.

Konstantin Likharev proposa en 1976, puis en 1982, de mettre en œuvre cette logique de calcul réversible en manipulant les niveaux d'énergie de jonctions supraconductrices Josephson[842], sous l'appellation de « quantrons paramétriques ». Cela devint en 1991 le « quantron flux parametron » (QFP), capable de fonctionner jusqu'à 10 GHz et développé par une équipe japonaise[843].

---

[840] Voir Logical reversibility of computation, Charles Bennett, IBM Journal of Research and Development, 1973 (8 pages). C'est le même Charles Bennett dont nous parlerons plus tard et qui est à l'origine des codes BB84 et des fondements de la QKD.

[841] Voir Conservative Logic, par Edward Fredkin et Tommaso Toffoli, International Journal of Theoretical Physics, 1982 (35 pages).

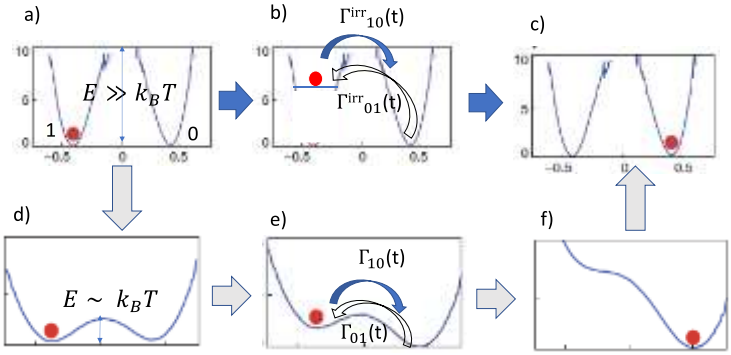
[842] Il raconte cela dans Josephson Digital Electronics in the Soviet Union, par Konstantin Likharev, 2012 (18 slides).

[843] Voir Quantum Flux Parametron : A Single QuantumFlux Device for Josephson Supercomputer par Mitsumi Hosoya et al, juin 1991.

Cela a abouti ensuite en 2003 à l'idée de **Vasili Semenov** d'exploiter des circuits nSQUID pour réaliser ces circuits, le n signifiant « negative » du fait d'une inductance négative qui relie deux SQUIDs du dispositif. Comme pour toute jonction Josephson, cela fonctionne sous température cryogénique[844].

Le calcul réversible est souvent associé au calcul adiabatique mais l'un pourrait fonctionner sans l'autre.

Le principe général du calcul adiabatique est illustré *ci-contre* : dans un calcul classique, la barrière énergétique est élevée pour modifier l'état d'un système entre a) et c). Dans un calcul quasi-adiabatique, un système physique abaisse la barrière de transition énergétique d'état (en d) pour le déclencher (en e) puis en f), en faisant remonter le niveau de la barrière à son état normal[845].



Le coût énergétique du traitement est ainsi abaissé en se rapprochant de la limite de Landauer. Le niveau élevé de la barrière hors calcul garantit la stabilité de l'information gérée en dehors de cette opération. L'abaissement de la barrière et sa remontée sont souvent gérées par un contrôle de tension trapézoïdal des transistors au lieu de ressembler à un signal carré.

Entre 1985 et 1993 furent imaginés des composants de calcul réversible ou partiellement réversible en CMOS et CCD. **Craig Lent** proposa ensuite en 1997 un système de calcul adiabatique à base de quantum-dots et d'automates cellulaires (QCA pour Quandum dots Cellular Automata) devant fonctionner jusqu'à 100 GHz[846].

Dans la même lignée, **Krishna Natarajan** suggéra en 2004 d'utiliser des MEMS (composants électro-micro-mécaniques) pour piloter le contrôle de tension trapézoïdal nécessaire à la création de composants CMOS adiabatiques avec une dissipation d'énergie très faible de 1 eV[847].

L'idée était poursuivie par une équipe du **CEA-Leti** et de **Delft** aux Pays Bas en 2017 puis de **Ralph Merkle** en 2019, avec des prototypes de circuits basés sur ce genre de technologie[848].

---

[844] Voir une explication du procédé dans Engineering and Measurement of nSQUID Circuits par Jie Ren, 2012 (26 slides). Les nSQUIDs sont des doubles SQUID reliés par une inductance négative. SQUID = Superconducting Quantum Interference Device, un système qui sert à mesurer avec précision le magnétisme des boucles supraconductrices à effet Josephson. Ces nSQUID étaient fabriqués par Hypres, dont nous reparlerons plusieurs fois.

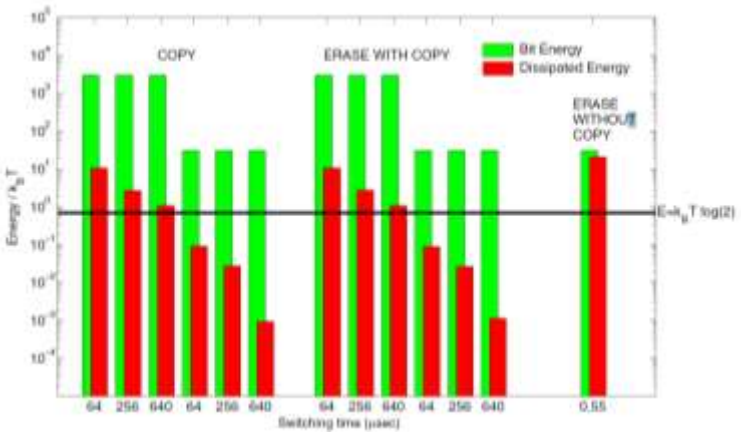
[845] Source : « Thermodynamics of computing, from classical to quantum » d'Alexia Auffèves, mai 2020 (11 pages), adapté de Experimental verification of Landauer's principle linking information and thermodynamics par Antoine Bérut et Al, 2011 (4 pages).

[846] Voir A Device Architecture for Computing with Quantum Dots par Craig Lent et Douglas Tougaw, 1997 (17 pages).

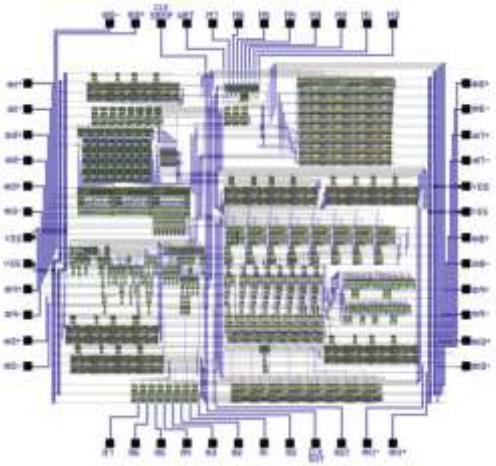
[847] Voir Driving Fully-Adiabatic Logic Circuits Using Custom High-Q MEMS Resonators par Krishna Natarajan et al, 2004 (7 pages).

[848] Voir Adiabatic capacitive logic: A paradigm for low-power logic par Gaël Pillonnet et al, du CEA-Leti, 2017 (5 pages) et Mechanical Computing Systems Using Only Links and Rotary Joints par Ralph Merkle et al, 2019 (34 pages).

En 2012, **Alexei Orlov** et al validaient expérimentalement la limite de Landauer et, surtout, la possibilité de la dépasser (par le bas) avec du calcul réversible, le tout avec quelques composants électroniques discrets classiques, des résistances et des capacités [849]. Leur expérience montrait qu'une copie de bit ou un effacement avec copie pouvait se faire avec une énergie inférieure à la limite de Landauer, au prix d'un ralentissement de l'opération.



Un effacement pur et simple consommait bien une énergie supérieure à la limite de Landauer. Le modèle était sauf ! Et tout cela fonctionnait à température ambiante. En 2019, la même équipe d'Alexei Orlov de l'Université Notre Dame dans l'Indiana produisait l'équivalent d'un micro-contrôleur 8 bits exploitant un sous-ensemble d'un jeu d'instruction MIPS de type RISC avec 5766 transistors dont 40% sont adiabatiques (*ci-contre*) [850]. Cela semble à ce jour être la réalisation la plus aboutie de processeur réversible adiabatique. Elle reste cependant expérimentale et très éloignée des besoins de l'industrie. Sa déclinaison industrielle pourrait avoir un intérêt pour créer des micro-contrôleurs d'objets connectés basse consommation dans un premier temps.



Cette technique de CMOS adiabatique requiert cependant un plus grand nombre de transistors. On remplace donc une consommation d'énergie par un composant plus grand, ce qui le rend plus cher à concevoir et à fabriquer que ses équivalents classiques.

La cause environnementale a récemment relancé l'intérêt pour le calcul réversible et adiabatique. Il est notamment promu par le groupe Computer Community Consortium de la **Computing Research Association** américaine avec un lead de chercheurs de l'équipe de Michael P. Frank du **Sandia National Labs**[851].

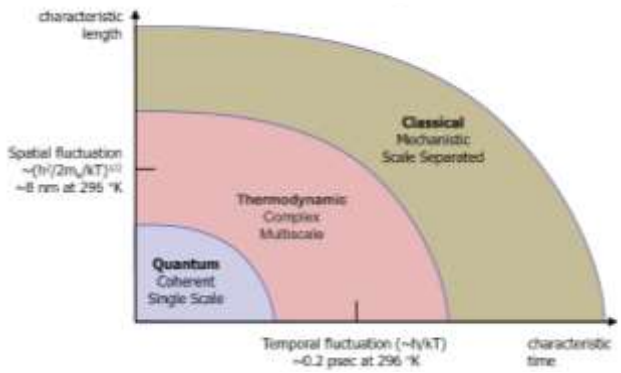
Ils le positionnent de manière intermédiaire entre le calcul classique et le calcul quantique mais sur des grandeurs pas forcément pertinentes au niveau des usages (dimension des composants et durée de fluctuation des états, voir le schéma *ci-dessous*). L'objet du manifesto est d'obtenir des crédits fédéraux US pour le financement de ces recherches. L'histoire n'est donc pas terminée !

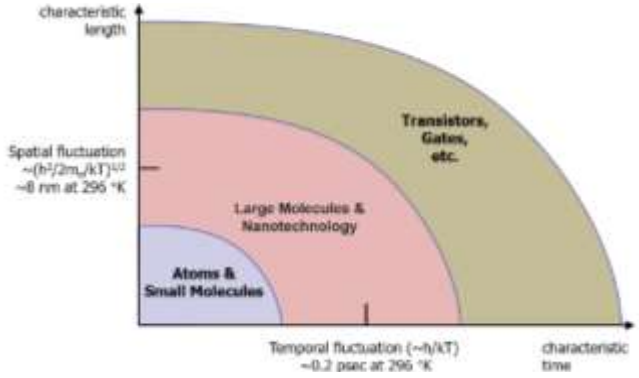
---

[849] Voir Experimental Test of Landauer's Principle at the Sub-kBT Level par Alexei Orlov, Craig Lent et al, 2012 (5 pages).

[850] Voir l'article « Experimental Tests of the Landauer Principle in Electron Circuits, and Quasi-Adiabatic Computing Systems » qui est intégré dans Energy Limits in Computation par Craig Lent, Alexei Orlov et al, 2019 (245 pages).

[851] Voir Thermodynamic Computing, Computer Community Consortium de la Computing Research Association, 2019 (36 pages). C'est un manifesto pour développer le calcul thermodynamiquement responsable inspiré par le biomimétisme. Le document résulte d'un workshop d'une quarantaine de participants, presque tous américains sauf un chercheur de Londres et un autre du Luxembourg, provenant d'universités et de quelques acteurs privés comme Google, Rigetti, HPE, Knowm (qui développe des circuits à base de memristors pour des applications d'IA, leur technologie kT-RAM) et Daptics (ex Protolife, créé par Norman Harry Packard (1954) et qui développe des algorithmes de simulation chimique).





Processeurs supraconducteurs

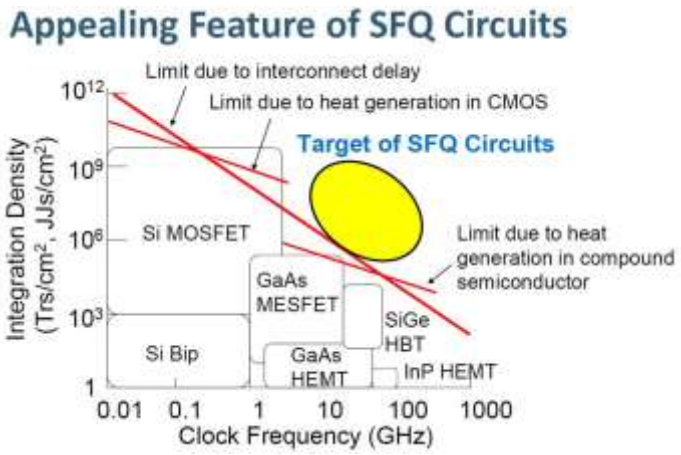
L'idée de créer des ordinateurs supraconducteurs capables de tirer parti de l'absence de résistance de composants à électroniques à basse température date du début des années 1960. Son histoire évolue parallèlement à celle du calcul réversible et adiabatique que nous venons de voir. Elle s'appuie en particulier sur la découverte de l'effet Josephson en 1962.

Cet effet Josephson sert, on l'a déjà vu en détails, à faire fonctionner les qubits supraconducteurs mais il est aussi potentiellement exploitable pour créer des transistors supraconducteurs qui ne vont pas faire appel aux mécanismes de la superposition et de l'intrication propres au calcul quantique.

Leurs bénéfices attendus sont une augmentation de la fréquence d'horloge des circuits et une baisse de la consommation d'énergie. Donc, dessert et fromage[852] ! En pratique le gain se situe plus du côté de la fréquence d'horloge que de la consommation d'énergie. Ainsi, dans un composant SFQ japonais réalisé en 2019, la fréquence d'horloge était de 32 GHz et la puissance de 2,5 TOPS par Watt, un peu plus du double du *best in-class* en composants CMOS classiques[853].

Plusieurs générations de composants supraconducteurs se sont succédées[854] :

- Des **SFQ** (Single Flux Quantum) de première génération, qui étaient limités à une fréquence d'horloge de 1 GHz et à 300 Mhz en pratique. Les études portant sur eux chez IBM avaient démarré dans les années 1960. Ils y avaient investi l'équivalent de $100M d'aujourd'hui, dans un programme qui était financé en partie par la NSA et qui a été abandonné en 1983[855]. Cela a cependant débouché indirectement sur les qubits supraconducteurs d'IBM qui sont aussi à base d'effet Josephson[856].



---

[852] Voir cette très intéressante présentation sur les composants supraconducteurs : Superconducting Microelectronics for Next-Generation Computing de Leonard Johnson, novembre 2018 (27 slides). Le gain en consommation d'énergie serait compris entre 10 et 1000. Le niveau d'intégration est pour l'instant faible, de l'ordre de 200 nm à comparer à 7 nm pour les processeurs les plus denses en CMOS. Mais il progresse régulièrement. Il existe même des pistes pour combiner transistors supraconducteurs, optoélectronique et réseaux de neurones. Voir Superconducting Optoelectronic Loop Neurons de Amir Jafari-Salim, 2018 (48 pages).

[853] Voir 29.3 A 48GHz 5.6mW Gate-Level-Pipelined Multiplier Using Single-Flux Quantum Logic par Ikki Nagaoka et al, 2019.

[854] Voir Single Flux Quantum (SFQ) Circuit Fabrication and Design: Status and Outlook, par V. Bolkhovsky et al, Lincoln Laboratory du MIT, 2016 (34 slides) ainsi que Cryogenic Electronic and Quantum Information Processing, 2018 (67 pages).

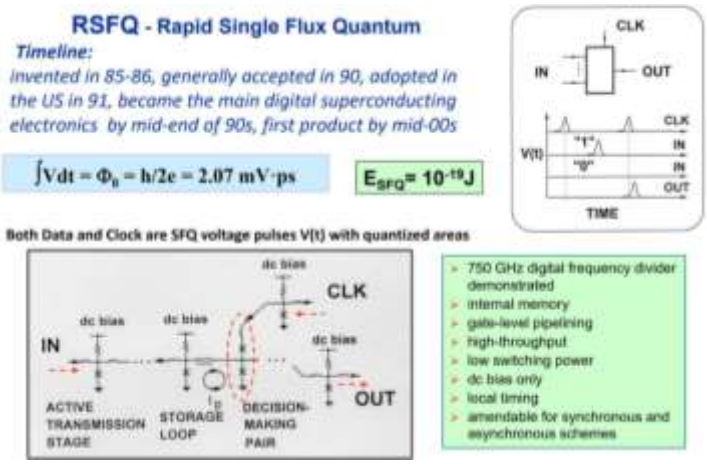
[855] Voir The Long Arm of Moore's Law: Microelectronics and American Science par Cyrus Mody, 2017 (299 pages), voir page 58.

[856] Source du schéma qui positionne les SFQ en termes de vitesse d'horloge et d'intégration par rapport aux composants traditionnels : Impact of Recent Advancement in Cryogenic Circuit Technology par Akira Fujimaki et Masamitsu Tanaka, 2017 (37 slides).

Il se trouve que les chipsets de qubits supraconducteurs de D-Wave comprennent des composants de type SFQ pour générer les signaux de contrôle des qubits et les lire (convertisseurs digital/analog et inverse, DAC et ADC)[857].

- Les **RSFQ** (Rapid Single Flux Quantum) inventés en Russie au milieu des années 1980 et réalisés à base de niobium et d'aluminium. Ils ont été adoptés aux USA en 1991 pour aboutir aux premiers composants finis au milieu des années 2000[858]. Ils présentent l'avantage de pouvoir opérer jusqu'à 750 GHz.

  On peut réaliser avec eux des ALU (Arithmetic Logic Units[859]) tournant à 20/30 GHz ainsi que des convertisseurs ADC (analog to digital) allant jusqu'à 40 GHz[860]. Dans la logique RSFQ, l'information binaire est gérée sous la forme d'états quantiques de flux de la jonction Josephson, qui est transférée sous forme de pulsations de tension[861]. La technologie ne fait pas appel à la superposition d'états comme dans les qubits supraconducteurs.



  Hypres développe des systèmes de réception radiofréquences qui utilisent deux composants supraconducteurs : des antennes à base de **SQUID** (Superconducting Quantum Interference Device) qui permettent de capter le magnétisme avec précision (inventés en 1964) et un chipset en RSFQ tournant à 30 GHz avec 11K JJ (jonctions Josephson) [862]!

- Les **AQFP** (Adiabatic Quantum Flux Parametron) qui comprennent deux boucles supraconductrices Josephson reliées entre elles par une inductance, ce qui rappelle le principe du nSQUID[863]. Le procédé est très efficace énergétiquement grâce à sa capacité à être réversible.
- Les **RQL** (Reciproqual Quantum Logic)[864], **eRSFQ** (Energy Efficient RSFQ) et **eSFQ** (Energy Efficient SFQ) qui sont des variantes des RSFQ qui sont plus efficaces énergétiquement grâce à l'absence de résistance de biais, remplacée par une inductance. C'est la voie choisie par Hypres et sa filiale SeeQC. Leurs SFQ associent des eRSFQ, dont ils sont à l'origine, et des eSFQ. Les RQL sont étudiés pour créer des mémoires supraconductrices.

---

[857] Voir Architectural considerations in the design of a superconducting quantum annealing processor, par P. I. Bunyk et al de D-Wave, 2014 (9 pages).

[858] Source : Single Flux Quantum Logic for Digital Applications par Oleg Mukhanov de SeeQC/Hypres, août 2019 (33 slides).

[859] Voir par exemple qBSA: Logic Design of a 32-bit Block-Skewed RSFQ Arithmetic Logic Unit, 2020 (3 pages).

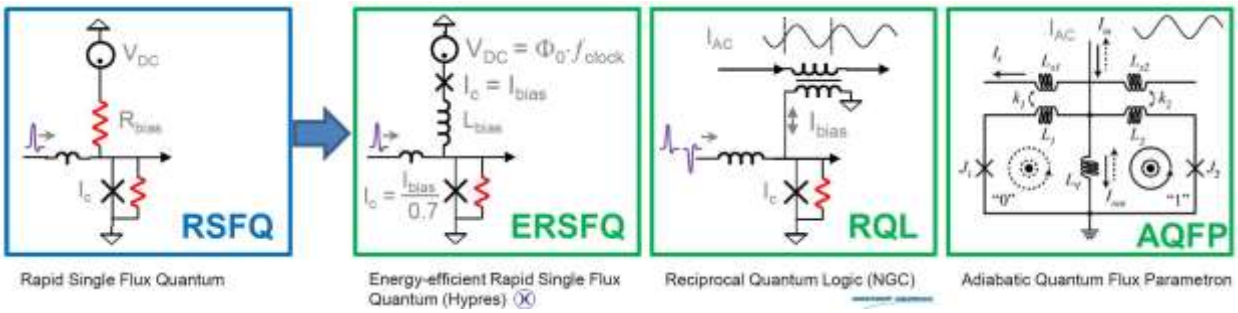
[860] Ce qui serait bien utile pour générer les micro-ondes de pilotage de qubits supraconducteurs et silicium.

[861] La gestion du temps dans la programmation de la logique doit en tenir compte. A ce sujet, voir A Computational Temporal Logic for Superconducting Accelerators par Georgios Tzimpragos et al, 2020 (14 pages).

[862] Voir Superconducting Quantum Arrays for Wideband Antennas and Low Noise Amplifiers par O. Mukhanov1 et al, 2014 (36 slides).

[863] Voir Adiabatic Quantum-FluxParametron: Towards Building Extremely Energy-Efficient Circuits and Systems, par Olivia Chen et al, 2018 (10 pages) et Design and Implementation of a Bitonic Sorter-Based DNN Using Adiabatic Superconducting Logic également par Olivia Chen et al, 2019 (24 slides).

[864] Voir Ultra-Low-Power Superconductor Logic par Quentin P. Herr et al, 2011 (7 pages).



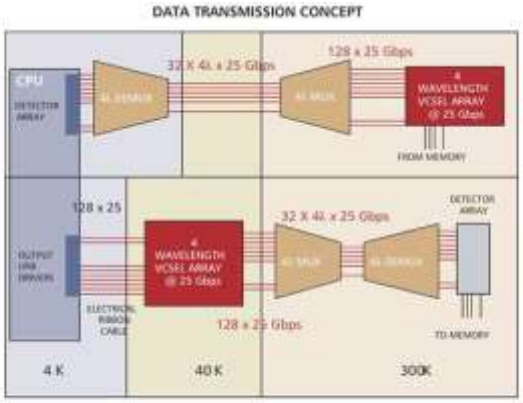
- Les **SFET** (Superconducting FET, Field Effect Transistors) qui appliquent un concept voisin des CMOS adiabatiques vus précédemment, mais avec un composant supraconducteur. Ces composants sont développés depuis les années 1980[865].

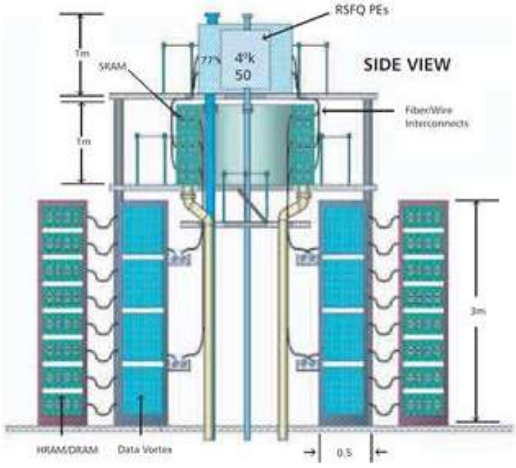
Il existe quelques autres variantes de composants supraconducteurs que je ne ferais que citer (SSV, SVJJ, STTJJ, S3JJ) car elles ne semblent pas courantes, sans compter la JMRAM pour la mémoire supraconductrice.

A ce jour, le record d'intégration de ce type de composant est de seulement 144 000 jonctions Josephson dans un chipset, réalisé en intégration 248 nm[866].

La **NSA** misait au milieu des années 2000 sur le RSFQ en y investissant $400M sur la période 2005-2010. Elle s'était donnée comme objectif de créer un processeur doté d'un million de portes logiques tournant à 50 GHz.

Le document de la NSA décrivant le projet est étonnamment très détaillé et tout autant instructif. On y découvre l'étendue des défis technologiques à relever[867]. Il y a notamment celui de la création de mémoires cryogéniques supraconductrices ou pas : hybride CMOS-jonction Josephson, SFQ ou monolithique RSFQ-MRAM. Puis la communication entre l'électronique cryogénisée et l'extérieur, a priori avec une bardée de fibres optiques à 25 Gbits/s que l'on ferait probablement monter aujourd'hui à 100 ou 200 Gbits/s mais avec la question de la modulation et de la démodulation du signal optique. Enfin, il faut dimensionner la cryogénie pour supporter un grand nombre de composants. Pour les tests, une simple tête pulsée suffit mais des installations plus imposantes sont envisagées pour la montée en puissance, comme dans l'illustration *ci-dessous* à droite.





[865] Voir Josephson Junction Field-effect Transistors for Boolean Logic Cryogenic Applications par Feng Wen, 2019 (7 pages). Voir aussi Superconducting silicon on insulator and silicide-based superconducting MOSFET for quantum technologies par Anaïs Francheteau, 2017 (153 pages).

[866] Voir Advanced Fabrication Processes for Superconducting Very Large Scale Integrated Circuits par Sergey K. Tolpygo, 2015 (43 slides).

[867] Voir NSA Superconducting Technology Assessment, 2005 (257 pages).

Le projet s'appuyait surtout sur la société **Hypres**, la seule société américaine entièrement dédiée à la création de composants supraconducteurs et dotée de sa propre fonderie depuis 1983. Ils fournissaient des composants radiofréquences à l'armée. Ils ont notamment développé un processeur 8 bits en RSFQ et 28 000 jonctions Josephson.

Il y a aussi **Northrop Grumman** avec sa fonderie située à Linthicum dans le Maryland. Enfin, étaient aussi impliquée l'Université Chalmers en Suède et divers laboratoires de recherche aux USA (JPL, Berkeley, Stony Brook) ainsi que le laboratoire de Boulder du NIST.

TABLE 2-2. SUPERCONDUCTOR RSFQ MICROPROCESSOR DESIGN PROJECTS

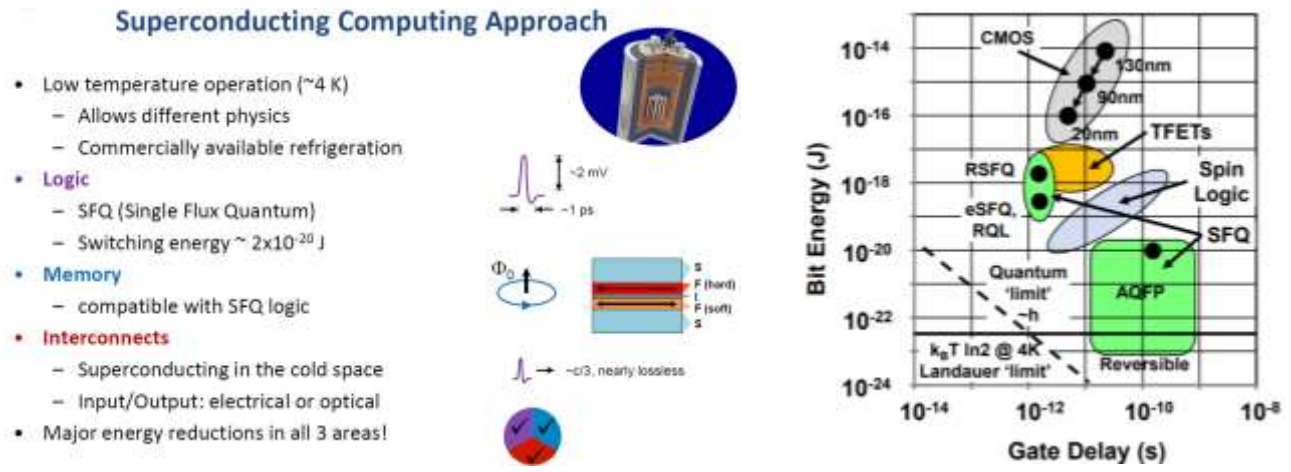
Time Frame	Project	Target Clock	Target CPU Performance (peak)	Architecture	Design Status
1997-1999	SPELL processor for the HTMT petaflops system (US)	50-60 GHz	~250 GFLOPS/CPU (est.)	64-bit RISC with dual-level multithreading (~120 instructions)	Feasibility study with no practical design
2000-2002	8-bit NUDX-1 microprocessor prototype (US)	20 GHz	40 billion 8-bit integer operations per second	Ultrapipelined, multi-ALU, multioperation synchronous long instruction word with bit-sliced organization (~ 25 instructions)	Designed, fabricated, operation not demonstrated
2002-2005	8-bit serial CORE1 microprocessor prototypes (Japan)	14-21 GHz 64-bit, 1 GHz system	250 million 8-bit integer operations per second	Non-pipelined, one serial 1-bit ALU, two 8-bit registers, very small memory (7 instructions)	Designed, fabricated, and demonstrated
2005-2015 (est.)	Vector processor for a petaflops system (Japan)	100 GHz	100 GFLOPS/CPU (target)	Traditional vector processor architecture	Proposal

TABLE 3.2-2. STATUS OF LOW-LATENCY CRYO-RAM CANDIDATES

Type/Lab	Access Time	Cycle Time	Power Dissipation	Density	Status
Hybrid JJ-CMOS (UC Berkeley)	500 ps for 64 kb	0.1 - 0.5 ns depending on architecture	12.4 mW read 10.7 mW write (Single cell writing)	64 kb in < 3x3 mm²	All parts simulated and tested at low speed
RSFQ decoder w/ latching drivers (ISTEC/SRL)	?	0.1 ns design goal	107 mW for 16 kb (Estimate)	16 kb in 2.5 cm² (Estimate*)	256b project completed (Small margins)
RSFQ decoder w/ latching drivers (NG)	?	2 ns	?	16 kb/cm² *	Partial testing of 1 kb block
SFQ RAM (HYPRES)	400 ps for 16 kb (Estimate)	100 ps for 16 kb (Estimate)	2 mW for 16 kb (Estimate)	16 kb/cm² *	Components of 4 kb block tested at low speed
SFQ ballistic RAM (Stony Brook University)	?	?	?	Potentially dense Requires refresh	Memory cell and decoder for 1 kb RAM designed
SFQ ballistic RAM (NG)	?	?	?	Potentially dense Requires refresh	SFQ pulse readout simulated
MRAM (4GK)	Comparable to hybrid CMOS	Comparable to hybrid CMOS	< 5mW at 20GHz (Estimate)	Comparable to DRAM (Estimate)	Room temperature MRAM in preproduction; Low temperature data sparse

*Densities of JJ memories are given for the technologies in use at the time of the cited work. Greater densities can be expected when a 20 kA/cm² process is used. The symbol ? signifies insufficient data.

L'agence **IARPA** a pris le relai avec le projet **Cryogenic Computing Complexity** (C3) lancé en 2014. Il impliquait IBM, Northrop Grumman, Raytheon et Hypres et devait se terminer en 2018[868].

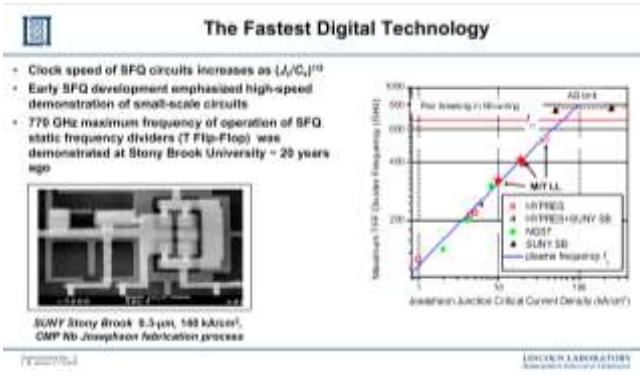


Ce projet s'intégrait à la **National Strategic Computing Initiative** (NSCI) lancée en 2015 par la Maison Blanche et qui portait sur le développement de supercalculateurs. Mais tout cela date de l'administration de Barack Obama et ne semble pas avoir été reconduit sous celle de Donald Trump[869]. Il est difficile de trouver ce qu'a donné ce projet en 2020.

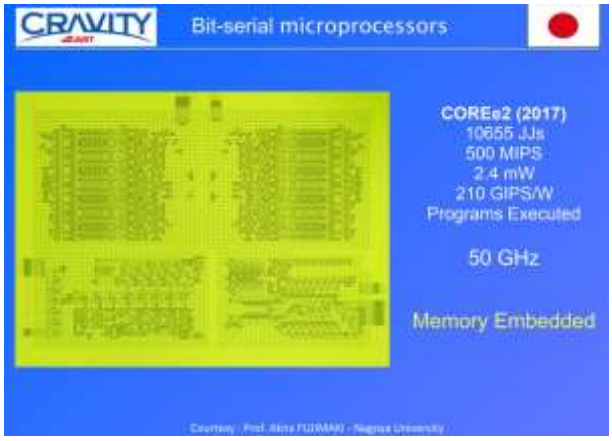
[868] Voir Superconducting Computing and the IARPA C3 Program par Scott Holmes, 2016 (57 slides) d'où vient le slide Supercomputing Computing Approach ainsi que le schema RSFQ/ERSFQ/RQL/AQFP d'une page précédente. L'ensemble des péesentations de la conférence C3 est ici.

[869] Le tableau qui suit comparant différents types de réalisations provient de Superconducting Computing par Pascal Febvre du CNRS, 2018 (56 slides). C'est aussi la source du slide sur Gravity Bit-Serial Microprocessors.

PROCESS	Current density (kA/cm²)	minimum area (μm²)	Maximum integration	Maximum frequency (GHz)
Hypres #03-10-45	0.03 1.0 4.5	~ 3.14	15,000	80 GHz RnIc=1.3mV @ 4.5 kA/cm²
Hypres #845/100/200	0.1 1 4.5 10 20 30	~ 0.4	10,000	200 GHz @ 30 kA/cm²
MIT Lincoln Lab SFQx	10 20 50	~ 0.06	~ 800,000	240 GHz RnIc=2.17 mV @50 kA/cm²
ADP2	10	1.0	1100 JJ/mm²	80 GHz
STP2	2.5 - 20	0.25 - 4.0	100 JJ/mm² - > 2,000 JJ/mm²	30 GHz - 150 GHz
NSTP	10	1.0	70,000	80 GHz
Fluxonics standard	1	12.5	100 JJ/mm²	40 GHz RnIc =0.256 mV
INRIM SNIS	up to 100	25	1,000 JJ/mm²	300 GHz RnIc >0.1mV - 0.7mV
NIST Nb/Nbx Si1-x/Nb	up to 110	?	70,000	300 GHz
INRIM SNIS 3D FIB	up to 100	0.1	10,000 JJ/mm²	300 GHz RnIc=0.1mV - 0.7mV



Hors USA, le **Japanese Superconducting Computing Program** ambitionnait en 2004 de créer un processeur tournant à 100 GHz générant 100 GLOPS en SFQ complété par 200 To de DRAM à 77K pour générer un système de 1,6 petaFLOPS comprenant 16384 processeurs. Le tout avec un cryostat consommant 12 MW et générant une puissance thermique de 18 kW à 4,2K. Il n'a pas encore vu le jour 15 ans plus tard[870]. En attendant, le supercalculateur IBM Summit qui utilise des processeurs traditionnels et des GPUs génère 200 petaFLOPS en consommant 13 MW. Alors, pourquoi se décarcasser ?



La **Chine** a annoncé en 2018 un plan à $145m de construction d'un ordinateur supraconducteur pour 2022. Ils avaient alors créé une puce avec 10000 jonctions Josephson. La **Russie** a aussi des ambitions dans le domaine[871].

En **France**, j'ai repéré que le laboratoire CMNE (Composants Micro Nano Electroniques) de l'IMEP-LaHC (Microélectronique, électromagnétisme, photonique, hyperfréquences) de l'UGA (Grenoble) travaillait dans ce domaine, sous la responsabilité de Pascal Febvre qui est basé sur le site de Chambéry.

Au final, cette filière des ordinateurs supraconducteurs est pour l'instant encore en suspens. Elle a souffert de l'avancée ininterrompue de la loi de Moore jusqu'à ces dernières années et aux difficultés de sa mise en œuvre pratique. Il n'est pas impossible que des synergies se développent entre le calcul quantique et cette branche un peu délaissée. Elles peuvent s'entre-aider comme on peut le voir avec les circuits supraconducteurs de pilotage de qubits supraconducteurs ou silicium. Sait-on, le calcul quantique fera peut-être renaître indirectement cette filière !

---

[870] Ils arrivaient à créer le CORE1α en 2003 à 4999 JJ (jonctions Josephson) et tournant à 15 GHz, le CORE1β en 2006 à 10955 JJ tournant à 25 GHz, le CORE1γ avec 22302 JJ également à 25 GHz, le CORE100 en 2015 à 3073 JJ et 100 GHz, le COREe2 en 2017 à 10655 JJ et 50 GHz avec une mémoire intégrée. Voir Impact of Recent Advancement in Cryogenic Circuit Technology par Akira Fujimaki et Masamitsu Tanaka, 2017 (37 slides). Cela continuait en 2019 avec un multiplieur 8 bits avec 20251 JJ tournant à 48 GHz et consommant 5,6 mW. Source : 29.3 A 48GHz 5.6mW Gate-Level-Pipelined Multiplier Using Single-Flux Quantum Logic par Ikki Nagaoka et al, 2019.

[871] Voir The Outlook for Superconducting Computers par R Colin Johnson, 2018.

Calcul probabiliste

Les processeurs probabilistes sont une autre sorte de processeurs exotiques. Ils utilisent des p-bits probabilistes qui peuvent fluctuer rapidement entre le 0 et le 1 avec un faible niveau d'énergie de transition. Ils sont censés permettre la résolution de problèmes dits « quantiques » sans s'appuyer sur des mécanismes quantiques. Les p-bits sont notamment réalisables avec des nano-aimants. Diverses applications sont envisagées comme la création de réseaux de neurones dits BSN (Binary Stochastic Neuron) et la résolution de problèmes d'optimisation voisins de ceux qui sont traités par le recuit quantique. Les accélérations obtenues ne sont pas qualifiées d'exponentielles.

Les travaux dans ce sens sont assez récents et proviennent de l'Université **Purdue** dans l'Indiana[872]. La startup française **HawAI.tech** basée à Grenoble est positionnée sur le même créneau et vise des applications dans le domaine de l'IA dans les systèmes embarqués exploitant des données de capteurs divers[873]. Leur roadmap doit mener à la création d'un ordinateur probabilistique complet d'ici 2024.

Processeurs optiques

De nombreux laboratoires de recherche et startups planchent sur la création de processeurs optiques qui ne sont pas à base de qubits. Certains cherchent à créer des réseaux de neurones optiques classiques, d'autres qui sont adaptés aux réseaux de neurones convolutifs ou aux neurones à impulsions, ces derniers se rapprochant le plus du fonctionnement du mode de fonctionnement du cerveau humain.

On compte surtout le **reservoir computing** qui est une catégorie spécifique de réseaux de neurones récurrents servant à traiter des séries temporelles (langage, finance, énergie, robotique)[874]. Leur particularité est d'utiliser des poids de neurones et des liaisons entre neurones fixés aléatoirement dans les réservoirs, le tout avec des fonctions d'activation non-linéaires de ces liaisons. Les centaines de neurones d'un réservoir sont alimentés par des données en entrées que les réservoirs mémorisent. La non-linéarité des fonctions d'activation rend évanescente cette mémoire.

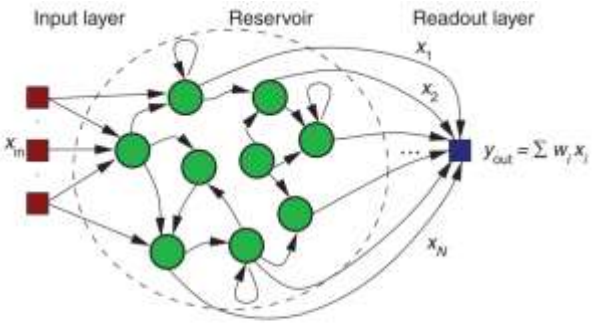


Figure 1: Standard layout of a reservoir computer, comprising an input layer (red), the reservoir (green) with randomized but fixed connections, and the linear readout layer (blue). Here, for simplicity a one-dimensional readout layer is drawn ($l = 1$).

Les paramètres d'entraînement de ces réseaux sont situés dans les poids des neurones qui relient les réservoirs aux données de sorties[875].

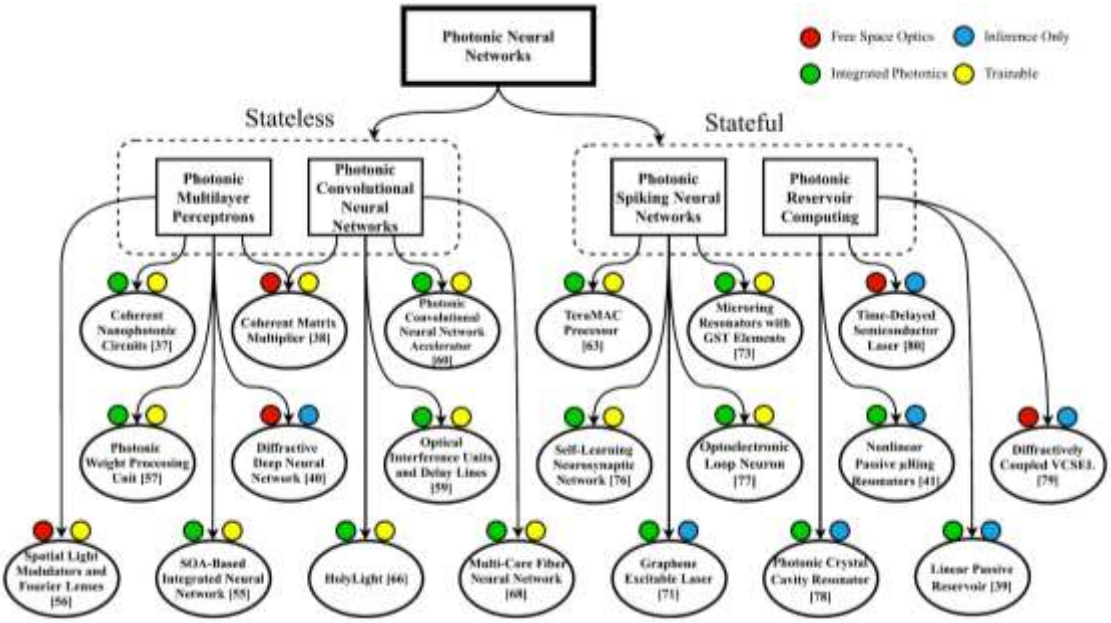
---

[872] Voir Integer factorization using stochastic magnetic tunnel junctions par William A. Borders et al, 2019, p-Bits for Probabilistic Spin Logic par Kerem Y. Camsari, 2019 (11 pages), Stochastic p-bits for Invertible Logic, Brian Sutton et al, 2017 (19 pages) et Ordinateur probabiliste : le nouveau compromis entre ordinateur classique et ordinateur quantique par Thomas Boisson, septembre 2019.

[873] Voir CONF@42 - 42AI - Bayes, IA et cookies, par Pierre Bessière, février 2018 (1h22mn) ainsi que la présentation Bayes from Cell to Chip également de Pierre Bessière, 2018 (33 slides).

[874] Le concept de reservoir computing date de 2007. Voir Toward optical signal processing using Photonic Reservoir Computing par Kristof Vandoorne et al, 2008 (11 pages). Il est aussi décrit dans Novel frontier of photonics for data processing—Photonic accelerator par Ken-ichi Kitayama, 2019 (25 pages) ainsi que dans cette belle présentation Introduction to Reservoir Computing par Helmut Hauser (282 slides). La notion est différente de celle de reservoir engineering que nous avons évoquée côté thermodynamique.

[875] La source du schéma est Advances in photonic reservoir computing par Guy Van der Sande et al, 2017 (16 pages) qui fait une excellente mise au point sur le reservoir computing à base d'optronique.



Il existe des projets de reservoir computing classiques, plutôt à base de memristors[876], cinq types de reservoir computing optiques et même des versions quantiques[877] ! Les différents types de réseaux de neurones optiques sont cartographiés *ci-dessus*[878].

Nous allons nous intéresser maintenant aux solutions qui s'appuient sur des procédés optiques utilisant de la diffraction d'images issues de puces DMD ou DLP illuminées par un laser et envoyées sur des structures diverses comme des matrices aléatoires ou des métamatériaux divers. Ils s'appuient souvent sur le principe de la transformée de Fourrier optique qui permet de décomposer une image 2D en fréquences spatiales elle-même représentée en 2D. Cette transformée est une image qui contient des points clés représentant des formes et répétitions dans les images analysées.

Cela peut notamment servir à réaliser des couches de convolution dans des réseaux de neurones convolutifs. Celles-ci servent habituellement à détecter la présence de formes dans une image, les formes étant représentées par des filtres. Ici, la transformée de Fourrier permet visiblement d'identifier automatiquement ces formes clés dans l'image. Ces systèmes captent le résultat avec un capteur CMOS en général de très haute résolution, largement supérieure à celle de la puce DLP ou DMD utilisée en amont. La diffraction réalise ainsi une projection dans un espace de plus grande dimension que l'image d'origine. Tout cela est soutenu par un corpus mathématique sérieux et ancien mais pas du tout évident à assimiler[879].

Ces différentes solutions en sont à leurs tous débuts. Elles n'ont pas l'air de concurrencer sérieusement le calcul quantique scalable, peut-être à part certains cas de Quantum Machine Learning. Elles permettent cependant d'accélérer certains calculs pour l'entraînement de réseaux de neurones complexes. Ces accélérations ont l'air d'être plutôt polynomiales et non pas exponentielles comme le permettront le calcul quantique. A ceci près qu'elles n'ont pas l'air d'être handicapées par des questions de bruit comme le sont les qubits.

---

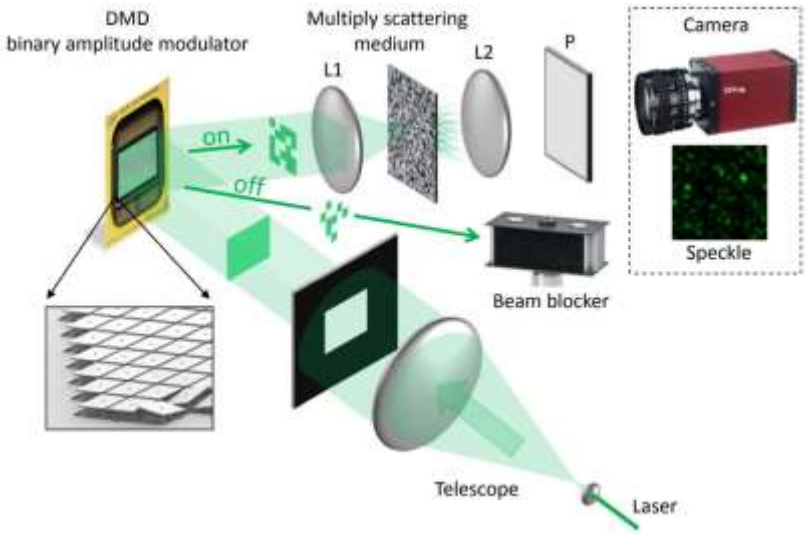
[876] Voir Memristors and Beyond: Recent Advances in Analog Computing par Nick Skuda, 2019 (12 slides).

[877] Voir Universal quantum reservoir computing par Sanjib Ghosh et al, de Singapour, 2020 (23 pages) ainsi que Integrated Nanophotonic Structures for Optical Computing par Laurent Larger et al, 2019 (50 slides).

[878] Source du schéma : Photonic Neural Networks: A Survey par Lorenzo de Marinis et al, 2019 (16 pages).

[879] Voir An optical Fourier transform coprocessor with direct phase determination par Alexander Macfaden et al, 2017 (8 pages) et Performing optical logic operations by a diffractive neural network par Chao Qian et al, 2020 (7 pages).

Lighton.io (2016, France, $3,7M) propose un coprocesseur optique dédié à l'accélération de l'entraînement de réseaux de neurones sur de gros volumes de données d'entraînement, comme des réseaux convolutifs. Le procédé est entièrement optique. Un laser émet un faisceau qui est agrandi pour éclairer une puce DLP à micro-miroirs. L'image générée traverse alors une matrice aléatoire (*scattering medium* dans l'illustration).

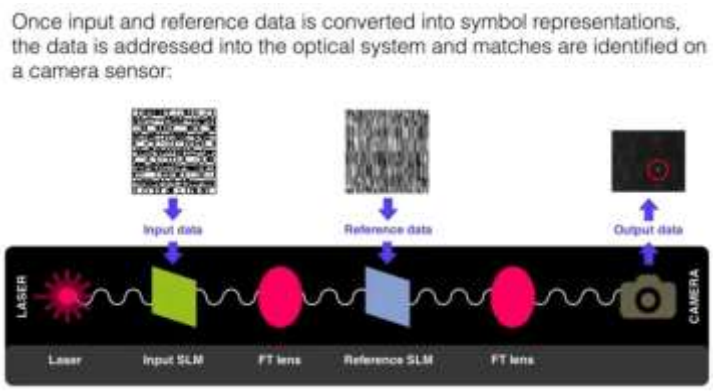


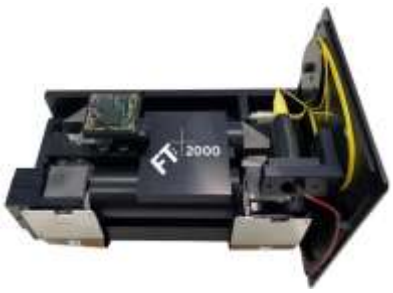
Elle atterrit alors dans un capteur CMOS monochrome[880]. Le capteur récupère le résultat des interférences générées par l'ensemble et un traitement mathématique permet d'en interpréter le résultat. Ce procédé permet de réduire la dimensionnalité d'un jeu de données complexes.

Le dispositif a été miniaturisé progressivement pendant la mise au point, tenant dans l'équivalent d'un serveur 2U à ce stade. La puissance du système vient en particulier de la résolution du DLP et du capteur CMOS, qui est de plusieurs millions de pixels.

Le tout est piloté à partir de bibliothèques Python développées avec TensorFlow. Les applications visées sont en premier lieu la génomique et l'Internet des objets.

Optalysys (2013, UK, $5,2M)[881] utilise un procédé voisin de celui de LightOn. Leur système FT:X 2000 est structuré autour de la réalisation de transformées de Fourier rapides optiques à base de diffraction. Le projet est issu de travaux de recherche de l'Université de Cambridge. Ils sont impliqués dans divers projets, l'un en génétique pour faire de l'alignement de séquences de génomes, GENESYS, mené avec le centre anglais **Earlham Institute**.





L'autre pour faire des prévisions météo avec le centre européen **ECMWF e**t un troisième pour la simulation de plasmas et de dynamique des fluides (pour la DARPA). Ils ont aussi réalisé un réseau convolutionnel début 2018 sur une base MNIST avec 60 000 lettres pour l'entraînement et 10 000 pour les tests. Mais avec un taux de réussite de seulement 70%. La startup a été fondée par Nick New, Robert Todd et Ananta Palani.

[880] Le procédé est décrit dans Random Projections through multiple optical scattering: Approximating kernels at the speed of light, 2015 (6 pages).

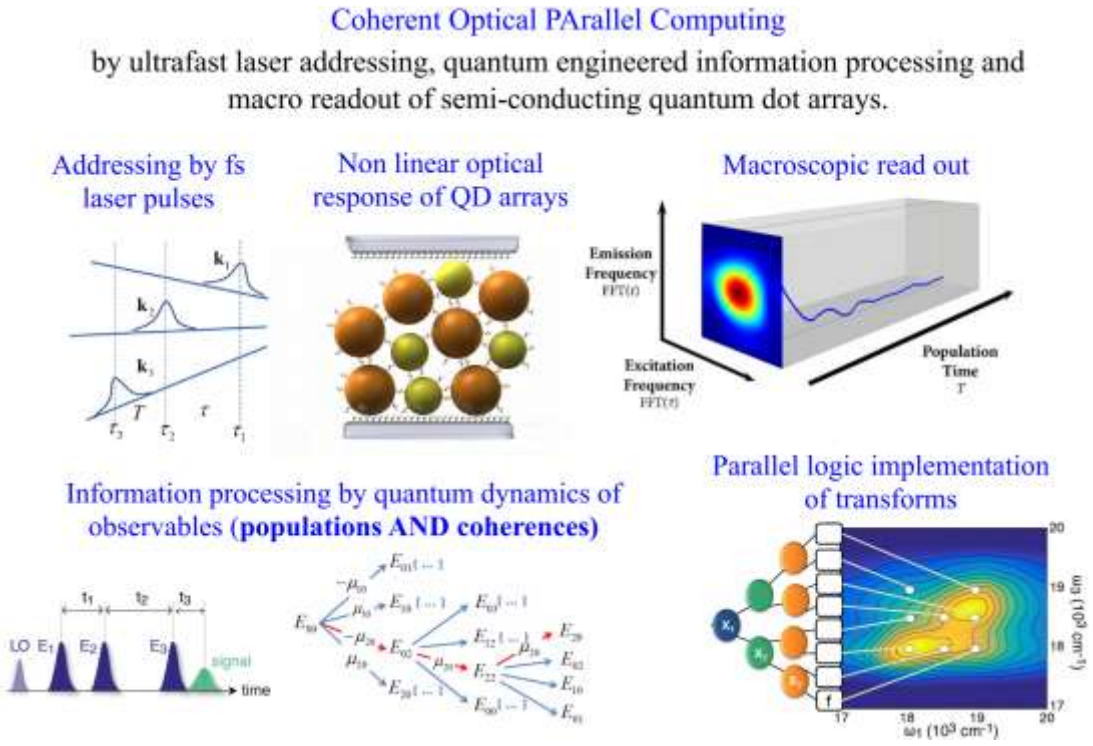
[881] Voir Optalysys - Revolutionary Optical Processing for HPC, septembre 2017 (23 mn).

Fathom Computing (2014, USA) utilise une architecture "électro-optique" capable d'entraîner des réseaux de neurones à mémoire (LSTM) et convolutionnels. Leur Light Processing Unit (LPU) serait capable de lire 90% des tests de la base d'écriture manuscrite MNIST, reprenant le même test que celui qui a été réalisé par Optalasys. Le système est adapté à l'algèbre linéaire et à la multiplication de matrices. Il leur reste à miniaturiser leur dispositif, ce qui selon eux devait prendre au moins deux ans, en 2018. La startup a été lancée par les frères William et Michael Andregg.

Luminous Computing (2018, USA, $9M) ambitionne de créer un composant optique ultra-performant qui remplacerait 3000 TPUs de Google ! Il exploiterait des lasers de plusieurs couleurs et des guides de lumière. Au vu des publications de leur CTO, Mitchell Nahmias, il semble qu'ils réalisent des neurones à impulsion optiques[882]. Ils permettent en effet de réaliser des calculs très rapidement, y compris en CMOS classique. Alors, en calcul optique, cela doit être plus rapide.

Toutes ces solutions issues de startups sont encore entre deux eaux. Elles ont démontré des capacités de calcul intéressantes à petite échelle sur des besoins ad-hoc. Reste à « scaler » et à les intégrer dans des solutions de calcul en général hybrides. Les efforts concernent alors à la fois le packaging des solutions pour pouvoir les intégrer dans des racks de serveurs standards, et les outils de développement. Sans développeurs, pas de logiciels ! Les phénomènes d'écosystèmes et de standardisation de facto du marché informatique font alors leur œuvre pour simplifier le marché.

Ajoutons-y le projet **Copac** financé par les programmes H2020 de l'Union Européenne. Il vise à créer une solution exotique de calcul quantique n'exploitant pas des qubits. Il ambitionne de permettre la résolution de problèmes d'analyse de données comme la simulation de systèmes complexes ou de machine learning. Le processeur aurait la capacité à évaluer toutes les variables d'une fonction logique en parallèle.



Le tout s'appuie sur une architecture à base de quantum dots excitables simultanément sur plusieurs fréquences par des lasers à large bande. La lecture des résultats est réalisée par spectroscopie 2D des quantum dots. La machine fonctionnerait à température ambiante. Le procédé mélange du calcul classique (pour l'évaluation des fonctions) et des méthodes quantiques (pour le faire simultanément sur plusieurs jeux de variables).

[882] Voir Progress in neuromorphic photonics par Thomas Ferreira de Lima, Mitchell Nahmias et al, 2017 (23 pages).

Le projet est mené avec les Universités de Liège (Françoise Remacle), Hébraïque de Jérusalem (Raphael Levine), Padoue, le CNR Institute for Physical and Chemical Processes de Bari, la société **KiloLambda** (2001, Israël) qui fabrique les quantum dots et le Français **ProBayes**, filiale de La Poste qui réalise le compilateur de la solution (Emmanuel Mazer et David Herrera-Marti)[883].

La grande incertitude sur ce projet, comme c'est souvent le cas, concerne sa scalabilité. Il dépend notamment de superposition de fréquences optiques. La documentation du projet ne décrit pas bien le domaine du possible en termes de classes de complexité de problèmes adressables.

[883] Voir Coherent Optical Parallel Computing, 2017. Le projet européen est financé jusqu'en 2021. Voir plus de détails dans Coherent Optical PArallel Computing Project Summary.

Startups et PME du calcul quantique

Après avoir fait le tour des solutions matérielles d'ordinateurs quantiques, voici un tour d'horizon très large et presque exhaustif des startups du calcul quantique dans le monde.

La cartographie est plus aisée que dans d'autres deep techs comme l'intelligence artificielle car elles ne sont pas encore très nombreuses. Il y en a plus de 260 à l'échelle mondiale. Dans cet inventaire, j'intègre cependant les grandes entreprises établies qui ne sont plus vraiment des startups ni des PME et, d'autre part, j'exclue les entreprises de conseil et de services qui n'ont pas et n'envisagent pas d'avoir de produits.

Cet écosystème a commencé à se structurer avant même que les ordinateurs quantiques fonctionnent à grande échelle. Il est fascinant de découvrir des startups qui font des paris à long terme, surtout dans le matériel. Les startups du logiciel s'appuient sur une infrastructure matérielle encore limitée mais réduisent souvent leurs risques en supportant également des architectures de calcul traditionnelles. Leurs clients sont de grandes entreprises, surtout américaines, qui font des tests d'algorithmes à petite échelle pour se faire la main sur la programmation quantique, souvent sur les machines de D-Wave. A ce jour, aucune application ne semble avoir été déployée en production. On est donc dans le champ de la recherche appliquée dans les entreprises clientes.

De leur côté, et nous les étudieront dans d'autres parties de cet ebook, les systèmes de cryptographie quantique sont opérationnels et correspondent à un marché bien à part, tout comme le marché fragmenté de la métrologie quantique.

Les startups identifiées ici sont surtout américaines et européennes. L'écosystème logiciel est à observer de prêt. Il se développera probablement de manière prononcée lorsque le matériel fonctionnera à plus grande échelle, notamment lors des calculateurs NISQ avec près d'une centaine de qubits seront disponibles[884].

Les enjeux de nombre de startups de ce domaine sont communs avec ceux des deep techs : comment développer de véritables produits avec des économies d'échelle, comment se développer rapidement à l'international, comme éviter de tomber dans les modèles trop orientés « services ». Et comment résister à ce que certains appellent déjà l'hiver quantique, une période de redoux de l'intérêt pour le sujet que certains anticipent à partir de 2020.

Dans le créneau des technologies dites habilitantes (sources de photons, cryostats, ultra vide, capteurs divers, électronique), les startups et PME concernées s'en sortent en touchant des marchés diversifiés, notamment ciblant plusieurs branches différentes de la recherche ou des applications militaires ou aérospatiales.

Investisseurs

Les premiers fonds d'investissements plus ou moins spécialisés dans les technologies quantiques ont déjà émergé avec notamment :

- **Quantonation**, un fonds d'amorçage français créé par Charles Beigbeder et géré par Christophe Jurczak, un physicien issu de l'Ecole Polytechnique et ancien thésard d'Alain Aspect. Ils ont déjà investi dans une dizaine de startups dont **LightOn** (France), **Spark Lasers** (France), qui propose des sources laser pas spécifiquement dédiées aux ordinateurs quantiques, **Pasqal** (France, atomes froids), **Quantum Benchmark** (Canada, logiciels), **Kets Quantum Security** (UK, composant QKD), **Orca Computing** (UK, matériel, calcul à base de photonique), **CryptoNext Security** (France, PQC), **Qunnect** (USA, répéteurs pour de la QKD), **Quandela** (France, source

[884] Voir Some Teams Go For NISQ-y Business. Some are NISQ-Averse par Doug Finke, février 2020.

de photons), **Qubit Pharma** (simulation moléculaire), **Qnami** (Suisse, métrologie à base de NV centers) et **QphoX** (Pays-Bas, interconnexion entre ordinateurs quantiques). Ils organisent des meetups et hackathons quantiques à Paris, la première édition ayant eu lieu en octobre 2018. C'est aujourd'hui le principal animateur de l'écosystème entrepreneurial quantique en France avec le **Lab Quantique**[885].

- **Quantum Valley Investments** (QVI), un fonds d'investissements canadien de $100M$, levés en 2013, dédié aux technologies quantiques. Leurs fondateurs avaient investi en 1984 dans Blackberry / RIM. Ils ne communiquent pas sur leurs investissements, à part dans ISARA Corporation, dont une part sont des spin-offs du laboratoire de recherche canadien Institute for Quantum Computing de l'Université de Waterloo dans l'Ontario.
- **Quantum Ventures** est une société d'investissement spécialisée dans le quantique lancée en 2016. Son "Quantum Revolution Fund" est géré à partir de Londres et de Suisse. Il ambitionne de réunir 100M€.
- **Quantum 1 Group** est un fonds d'investissement américain spécialisé dans les technologies quantiques depuis 2015.
- **Summer Capital** est un fonds d'investissement des Pays-Bas spécialisé dans les technologies quantiques, la data et la finance. Ils ont notamment investi dans QxBranch, Rigetti et Turing.
- **Quantum Wave Fund** créé par des Russes dans la Silicon Valley et ayant déjà investi dans les Suisses d'IDQ ainsi que dans l'Américain Nano-Meta Technologies. Leur fonds n'est pas 100% spécialisé dans le quantique. Ils investissent aussi dans la robotique, les drones, les capteurs et les objets connectés. D'après la Crunchbase, le fonds n'a pas l'air d'être très actif depuis 2016.
- **Parkwalk Advisors** est un fonds de deep techs britannique. En mars 2020, ils avaient investi à date dans trois startups des technologies quantiques : Phasecraft, Quantum Motion Technologies et Oxford Quantum Circuits. Ce fonds fait partie du groupe IP Group Plc depuis décembre 2016.
- **Machine Capital**, un fonds britannique focalisé sur le quantique et sur l'IA, qui a pour l'instant investi dans **QuantumX Incubator,** un incubateur de projets logiciels quantiques lancé conjointement avec la startup **Cambridge Quantum Computing**, qui est spécialisée dans le développement de logiciels quantiques, avec une incubation qui dure 20 semaines.
- **SpeedInvest** est un fonds d'investissement autrichien spécialisé dans les startups deep techs, qui s'investit entre autres dans les technologies quantiques. Ils investissent en amorçage avec des tours allant jusqu'à 1M€. Mais leur portefeuille n'a pas l'air de comprendre de startups du quantique (en mars 2020).

The Quantum Daily produisait début 2020 un inventaire des investisseurs dans les startups des technologies quantiques. En voici un extrait avec les investisseurs VCs généralistes et spécialisés.

[885] Voir Le pari fou du fonds français Quantonation, l'un des spécialistes mondiaux du quantique par François Manens, octobre 2019.

Il contient quelques erreurs comme Worldquant qui est positionné comme un investisseur spécialisé dans les technologies quantiques alors que c'est une société d'investissement généraliste crée en 2007. L'usage du mot quantum ou d'un bout de quantum n'est pas un gage de spécialité.

L'investissement dans les startups a commencé à décoller à l'échelle mondiale à partir de 2016[886].

Un inventaire des startups du secteur est disponible sur le site QuantumComputingReport. Il m'a permis d'identifier une majorité des startups citées dans cette partie. Certaines startups diffusent tellement peu d'informations à leur sujet que l'on peut se demander si elles ne sont pas des scams.

Ce manque de communication peut simplement provenir du fait que les créateurs peuvent être des chercheurs non férus de communication, qu'ils sont mal financés et que leurs projets ont des perspectives business trop lointaines et hasardeuses.

Une bonne part des startups citées ici ne sont pas encore sous la forme "pure" du modèle startupien, à savoir qu'elles sont loin d'avoir un modèle scalable. Ce sont souvent soit des TPE industrielles ciblant des marchés de niche à très faible volume, soit des startups où le risque scientifique et technologique est encore très élevé avant de pouvoir vendre quoi que ce soit. Et souvent, avec la combinaison des deux. Elles peuvent alors se financer avec de la recherche sous contrat pour de grandes entreprises ou des institutions publiques.

Dans la grande majorité des cas, je m'appuie sur les informations publiques disponibles sur Internet pour décrire ce que font ces startups. Sauf de rares cas que je signale, je n'ai pas d'information plus poussée. Une méthode d'investigation permet d'arriver à trouver ce que font ces startups : identifier leurs fondateurs, si ce sont des chercheurs, trouver leurs laboratoires d'origine et leurs publications scientifiques associées et consulter leur thèse de doctorat si elle est disponible. Enfin, rechercher d'éventuels brevets déposés par les startups. C'est du renseignement technologique sur « sources ouvertes ».

Nous allons donc maintenant faire le tour des startups du calcul quantique avec trois parties : les composants, les ordinateurs quantiques et les logiciels, comprenant les outils de développement.

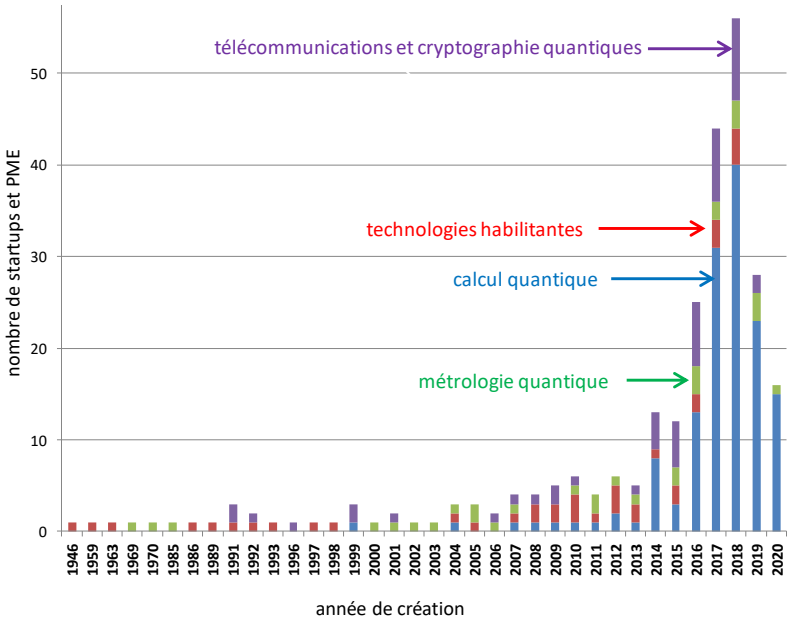
Ma cartographie ne comprend pas non plus les sociétés qui ont l'air de ne proposer que du service et du conseil dans l'informatique quantique, sans avoir de technologie en propre ou de produit[887]. Depuis la parution initiale de cet ebook, je continue de mettre à jour cette liste au fil de l'eau au gré des découvertes.

---

[886] Voir European Seed Investment: Quantum Applications, de Patrick Gilday, avril 2019.

[887] Voici quelques exemples de sociétés de conseil en vrac : **Q&I** (UK) aussi dénommée Qandi, **Quantum Phi** (UK). **RayCal** (UK) qui est un cabinet d'analystes dans les technologies quantiques, **Inside Quantum Technology** (2018, UK) créée par Lawrence Gasman avec l'aide de 3DR Holdings, **Qureca** (Espagne) dont le nom signifie Quantum Resources & Careers et qui fait de la formation, du recrutement, du business developpement et organise des événements, et aussi **Max Kelsen** (Australie). Aux USA, la société **StrategicQC** est aussi spécialisée dans le recrutement de talents dans les technologies quantiques.

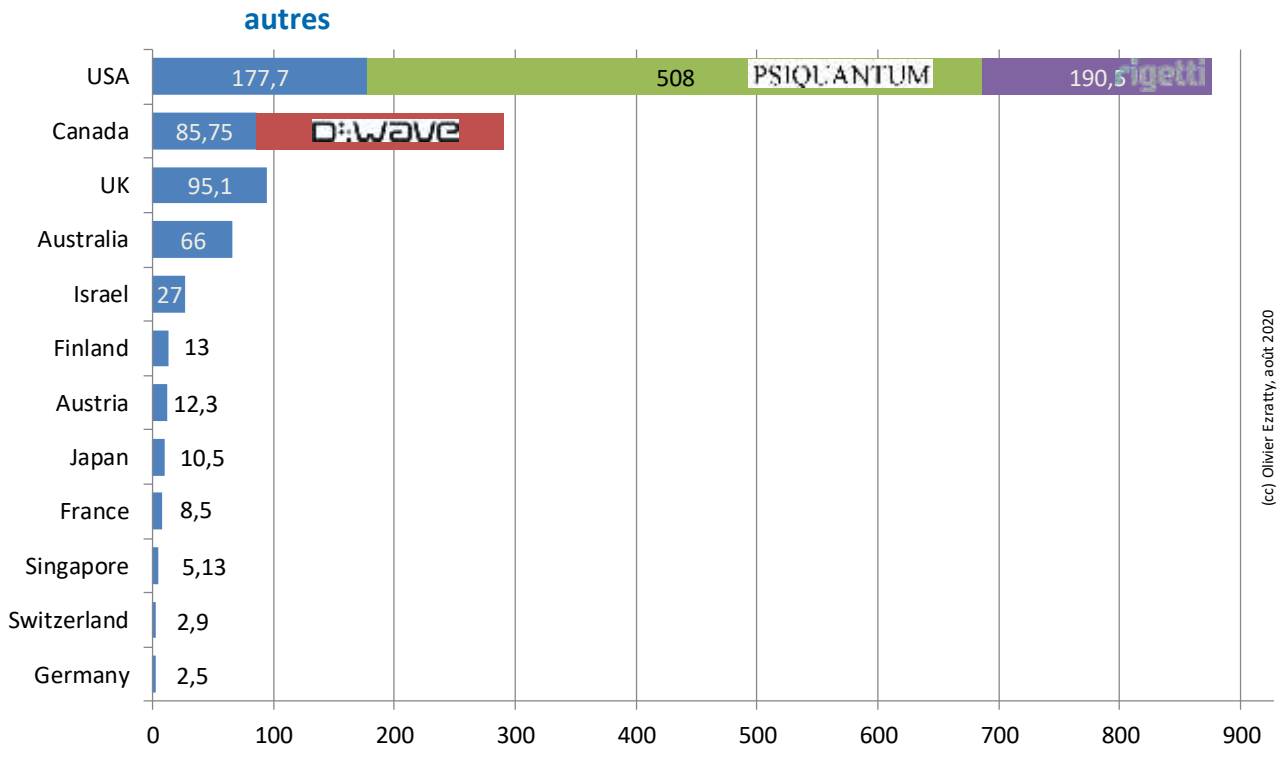
Pour ce qui est des données, voici quelques charts extraits de ma base de données de startups et PME. Le premier fournit une indication du nombre de création d'entreprises par année. Le second, une ventilation par pays.



Pays	Computing	Enabling	Sensing	Communication and security	Total
USA	40	12	13	9	74
Canada	27	2	1	6	36
UK	18	2	3	11	34
France	8	6	6	5	25
Germany	4	2	3	4	13
Switzerland	4	3	1	2	10
Japan	9				9
Australia	5		3	1	9
Netherlands	5	2			7
Spain	4	1		1	6
Singapore	4			1	5
China	1			3	4
Russia		1		3	4
India	1			2	3
Austria	2			1	3
Sweden	1	2			3
Israel	2			1	3
Estonia	2				2
Finland		2			2
Bulgaria	1			1	2
Denmark		2			2
Columbia	1				1
Italy			1		1
Norway	1				1
Hong-Kong	1				1
Luxembourg		1			1
Poland	1				1
Greece	1				1
EAU	1				1
Bielorussia	1				1
Total	145	38	31	51	265

source : compilation Olivier Ezratty, septembre 2020

Et dans ce troisième schéma, une ventilation différente par pays qui met en évidence les plus gros financements. On y voit, comme d'habitude, un écart de financement important entre l'Amérique du Nord et l'Europe. L'une des raisons est que les startups européennes ont été créées plus tardivement. L'autre est bien entendu un accès différent au capital. Le total du financeent des startups de l'Union Européenne est tout de même compris entre Israel et l'Australie ! Comme on dit à l'école, « peut mieux faire » !



Composants

Ces entreprises développent des composants physiques et technologies habilitantes qui peuvent jouer un rôle dans la construction d'ordinateurs quantiques. Le plus souvent, comme ce marché reste cantonné à la recherche, ces startups sont plus généralistes et visent des marchés plus larges que l'informatique quantique couvrant la recherche en physique en général voir des applications industrielles diverses.

Absolut System (2012, France) propose des cryostats dans des températures supérieures à 1,8K développés sur mesure pour des clients qui ne trouvent pas leur bonheur dans les produits génériques du marché.

La société crée par Alain Ravex, ancien chef du service des basses températures du CEA à Grenoble dans les années 1980/1990 puis consultant pour Air Liquide, cible un marché d'applications large dans la recherche et l'industrie, notamment pour la production d'azote liquide. Ils ont notamment le CEA-Leti, Thales et Air Liquide comme clients. Ils sont basés près de Grenoble. Ils ont créé AF-Cryo (2017), une filiale commune en Nouvelle-Zélande, avec Fabrum Solutions (2004) également basé en Nouvelle Zélande[888].

Anyon Systems (2014, Canada) est le genre de startup dont la communication semble être conçue pour déjouer toute tentative de comprendre ce qu'ils font avec précision.

Ainsi, sur leur site, on apprend qu'ils font du hardware et fourniraient des ordinateurs quantiques à qubits supraconducteurs clés en main. Sur LinkedIn, on découvre qu'ils développent en fait des calculateurs topologiques, ce qui est logique avec un tel nom de société, et qu'ils créent aussi bien du matériel que du logiciel.

[888] Voir Commercial Cryocoolers for use in HTS applications par Christopher Boyle, Hugh Reynolds, Julien Tanchon et Thierry Trollier, 2017 (29 slides).

Ailleurs, on apprend qu'ils ont développé un outil logiciel de conception et de simulation d'ordinateur quantique, leur Quantum Device Simulator (QDS) qui fait de la Quantum Electronic Design Automation. Celui-ci peut tourner sur des supercalculateurs. Ils avaient d'ailleurs fourni cette solution à l'équipe de John Martinis en 2017 pour leur conception d'un processeur à qubits supraconducteurs de 6 puis 20 qubits[889]. Leur logiciel servait surtout à prédire le niveau de cross-talks en qubits adjacents. La startup basée à Québec faisait 15 personnes en mai 2020. Et ils recrutent des ingénieurs et chercheurs dans la conception et même la fabrication de qubits supraconducteurs. Bref, cela a tout l'air d'être en fait un prestataire de services d'ingénierie pour des tiers. Ce d'autant plus qu'ils n'ont apparemment pas encore levé de fonds.

Atlantic Microwave (1989, USA) est une PME qui produit et commercialise des composants radio-fréquences et micro-ondes fonctionnant à température cryogénique.

Ils servent à contrôler les qubits supraconducteurs et silicium dans les cryostats. Cela comprend notamment des atténuateurs de micro-ondes, des filtres, des amplificateurs de micro-ondes et des tés de polarisation. C'est une filiale du groupe britannique ETL Systems, créé en 1984.

Aurea Technology (2010, France) est un équipementier en photonique qui propose notamment des générateurs de photons jumeaux et des détecteurs de photons uniques à base de diodes avalanche.

Ils fournissent aussi des lasers à impulsions picosecondes. La société est basée à Besançon.

AuroraQ (2017, Canada) est une société spécialisée dans la création de systèmes de communication avec des qubits supraconducteurs.

C'est complété par le logiciel QSPICE Design qui permet de concevoir des circuits quantiques supraconducteurs. Autant dire qu'il s'agit d'un marché ultra-niche[890].

Azur Light Systems (2010, France) développe des systèmes d'amplification laser à haute puissance dans l'infrarouge et le visible exploitant des fibres à base d'ytterbium et à faible dissipation thermique.

La société est basée à Pessac, près de Bordeaux.

bra-ket science (2017, USA) est une startup qui veut créer des systèmes de stockage d'information dans des qubits fonctionnant à température ambiante.

La société qui n'a que deux personnes est silencieuse sur sa technologie dont les brevets sont en cours de dépôt.

ColdQuanta (2007, USA, $6,8M) est une startup créée par Dana Anderson, maintenant son CTO, qui développe des solutions de refroidissement d'atomes froids à base de lasers. Elle est installée à Boulder dans le Colorado, à deux pas du laboratoire quantique du NIST.

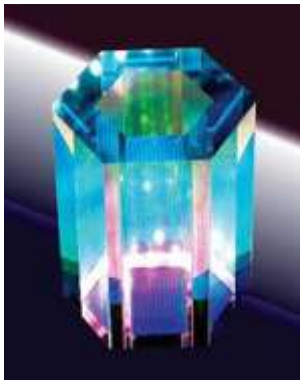
Ils présentent cela sous la forme du Quantum Core (*ci-dessous à gauche*), un guide de lumière qui permet de faire converger les rayons lasers pour contrôler les atomes froids qui sont généralement refroidis à moins de 50µK.

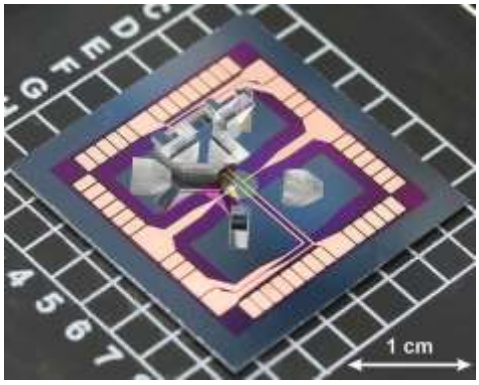
---

[889] Voir Google's 'supreme' 20-qubit quantum computer – Physics World par Tushna Commissariat, 2017.

[890] Voir The Geometry of a Quantum Circuit and its Impact on Electromagnetic Noise, 2018 (15 pages).

Il est notamment intégré dans le QuCAL, un générateur de condensats de Bose-Einstein complet ainsi que dans la Physics Station, un dispositif optique de contrôle d'atomes froids complet utilisable à des fins diverses. Les Atom Chips sont des puces intégrables dans ces systèmes comprenant l'optique miniaturisée de contrôle des atomes froids. La startup utilise ces technologies génériques pour créer des systèmes très variés, et avant tout pour de la métrologie quantique, notamment pour le géopositionnement en lieu et place du GPS, la microgravimétrie ou des horloges quantiques au césium. Ils proposent aussi des pompes à ultra-vide pour le contrôle d'atomes froids, dénommées RuBECi.





Leur approche du marché est très diversifiée, à se demander s'ils ont de véritables produits ou ne créent pas des solutions sur mesure pour de grands clients fédéraux américains. Ils ont notamment équipé la station spatiale ISS en instruments de mesure pour le compte de la NASA et du JPL. Ils ambitionnent aussi de créer un ordinateur quantique à base d'atomes froids, mais c'est probablement un peu plus complexe que de créer des outils de métrologie. Depuis mars 2019, son CEO est Bo Ewald qui était auparavant Président de D-Wave en charge des ventes internationales. Ils collaborent aussi avec IonQ pour la production de leurs ordinateurs quantiques à base d'ions piégés. La société est maintenant positionnée sur la création de processeurs quantiques complets à base d'atomes froids[891]. Ils obtenaient pour ce faire un financement de la DARPA en avril 2020 dans le cadre du programme ONISQ avec un projet collaboratif de $7,4M impliquant de nombreuses universités ainsi que Raytheon.

CryoConcept (2014[892], France) est un fournisseur de cryostats qui se différencie avec des systèmes générant un très faible niveau de vibrations via leur technologie UltraQuiet.

Nous en avons déjà parlé en détails dans la partie dédiée à la cryogénie. Ils font partie du groupe Air Liquide depuis juillet 2020.

Cryomech (2000, USA) est un fournisseur de composants qui rentrent dans la composition de cryostats et en particulier les systèmes de refroidissement à sec comprenant une tête pulsée et un compresseur qui sont intégrés dans les cryostats de la plupart des acteurs du marché comme BlueFors et CryoConcept.

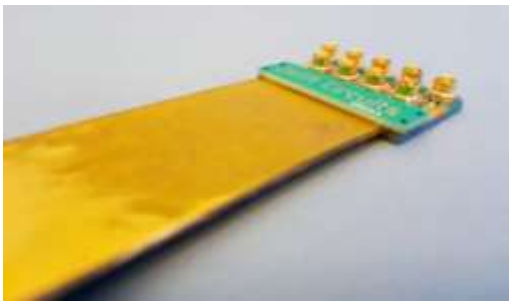
Ils constituent le premier étage des systèmes de réfrigération par dilution à sec pour descendre à une température de 4K, les autres étages étant un système de prérefroidissement et un système à dilution exploitant un mélange d'hélium 3 et 4 pour descendre à des températures inférieures à 20 mK.

---

[891] Voir ColdQuanta – Life in Quantum's Slow (and Cold) Lane Heats Up par John Russell, avril 2020 et le webinar Powering the Quantum Information Age avec Bo Ewald, avril 2020 (53 minutes).

[892] CryoConcept a en fait été créé en 2001 par transfert de technologie du CEA où Olivier Guia avait travaillé. La société a eu plusieurs propriétaires différents dont le Français Segula Technologies et l'Américain CryoMagnetics. Olivier Guia a repris l'activité de la société en 2014. Ils ont alors réintégré la R&D en interne et notamment récupéré la maîtrise technologique qui était au CEA.

Delft Circuits (2016, Pays-Bas) fournit des câbles et nappes souples servant à véhiculer les micro-ondes de contrôle des qubits supraconducteurs comme le CF3 (Cri/oFlex, *ci-contre*) et supportant des fréquences allant de 2 à 40 GHz. Ces câbles sont plus compacts et miniaturisés que la moyenne. Il semble qu'ils doivent cependant importer des conducteurs niobium-titane provenant du Japonais Coax-Co qui domine ce marché.



Element 6 (1946, Luxembourg) est une filiale du leader mondial de la production de diamants, De Beers Group, qui fabrique entre autres choses des diamants synthétiques utilisables dans les qubits à base de cavités de diamants, très utilisés en métrologie, notamment dans des magnétomètres quantiques.

High Precision Devices (1993, USA) développe des instruments cryogéniques adaptés aux ordinateurs quantiques supraconducteurs et notamment des capteurs. C'est de l'instrumentation de bas niveau très spécialisée.

Ils développent aussi des systèmes de cryogénie de type ADR (Adiabatic Demagnetization Refrigeration).

Intelline (2018, Canada) produit des systèmes de réfrigération cryogéniques sur mesure censés être plus abordables que ceux de ses concurrents.

Mais ils semblent viser d'autres marchés que la cryogénie d'ordinateurs quantiques, en tout cas à températures inférieures à 1K.

Intermodulation Products (2018, Suède) est une société issue de KTH, l'Institut Royal de Technologie suédois. Ils commercialisent Vivace, un générateur de micro-ondes dans la bande des 4GHz qui sert à piloter notamment des qubits supraconducteurs.

Kelvin Nanotechnology (2020, UK) est une société qui fabrique des composants miniaturisés utilisés dans les technologies quantiques. Ils produisent notamment des pièges à ions 3D, des dispositifs divers de photonique, des gravimètres en MEMS et des lasers.

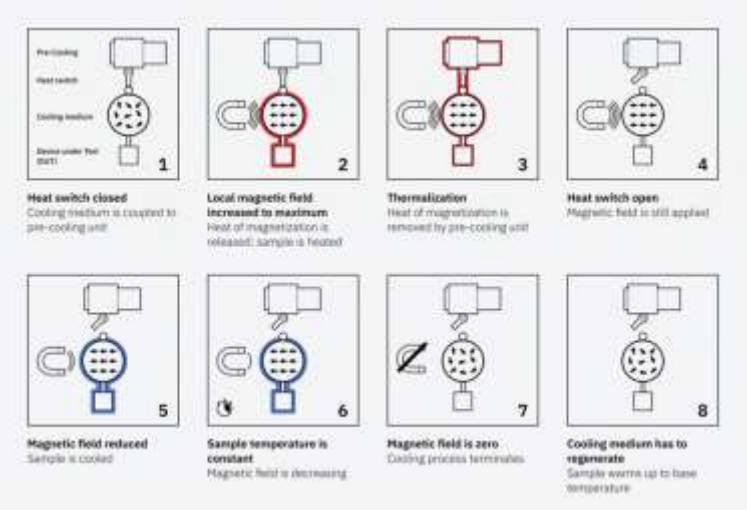
Ils sont basés au James Watt Nanofabrication Centre (JWNC) de Glasgow en Ecosse. C'est une société qui fournit les startups et PME fabless du secteur des technologies quantiques.

Kiutra (2017, Allemagne) développe un système de cryogénie à très basse température à base de magnétisme qui permet de se passer de l'hélium 3 utilisé dans les systèmes de cryogénie à dilution qui descendent jusqu'à 10 mK.

C'est une startup issue de la TUM (Technical University of Munich) lancée par Alexander Regnat. Elle a été financée en amorçage par APEX Ventures et des investisseurs allemands, sans que le montant soit connu.

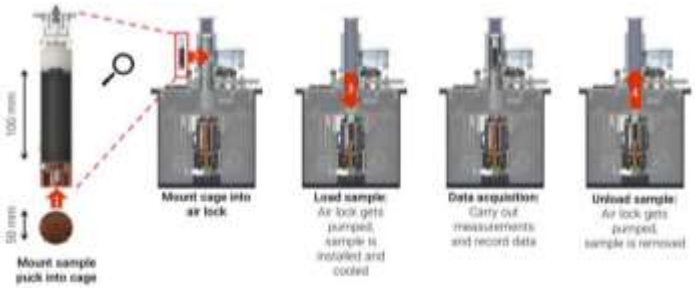
Leur gamme de cryostats descend à 100 mK (en mode pulsé) ou à 300 mK (en mode continu), ce qui est insuffisant pour refroidir des ordinateurs quantiques supraconducteurs à effet Josephson mais pourrait éventuellement convenir pour des chipsets silicium à spin d'électrons qui peuvent en théorie se contenter d'une température de 1K. Leur système utilise l'effet magnétocalorique qui a été découvert par étapes en 1881, 1917 puis démontré en 1933 pour atteindre une température de 250 mK.

Le procédé de Kiutra s'appuie d'abord sur cet effet classique aussi appelé la désaimantation adiabatique. Il consiste à magnétiser un matériau solide aux propriétés magnétocalorique. Cela le fait monter en température. Cet accroissement de température est évacué par un fluide caloporteur classique, qui n'est pas précisé. C'est peut-être de l'hélium 4 s'il s'agit de descendre à une température de moins de quelques Kelvins. Ensuite, l'aimantation est stoppée ce qui conduit le matériau à refroidir.



Pour lisser dans le temps et l'espace ce cycle de chauffe/refroidissement, ils combinent plusieurs unités de refroidissement avec ce qu'ils appellent le cADR (continuous Adiabatic Demagnetization Refrigeration)[893].

L'appareil proposé par Kiutra a l'air d'être surtout conçu pour refroidir des échantillons de taille réduite et ne semble pas encore adapté aux architectures habituelles des ordinateurs quantiques avec leurs étages de refroidissement empilés entre 4K en haut et 15 mK en bas.



Labber Quantum (2016, USA) développe des solutions logicielles de contrôle des qubits d'ordinateurs quantiques expérimentaux. Elles servent notamment à calibrer les qubits. La startup a été acquise par Keysight Technologies en mars 2020.

LakeDiamond (2015, Suisse, 2M€) produisait des diamants de synthèse pouvant être utilisés pour créer des qubits à base de lacunes dans les diamants ou dans des applications de métrologie.

Ils utilisent du dépôt sous vide avec la méthode CVD (Chemical Vapor Deposition). La société a fermé boutique en février 2020 après s'être financée via une ICO en 2018 (Initial Coin Offering, un mode de financement passant par une crypto-monnaie)[894].

[893] J'ai au passage découvert que cette technique était aussi explorée à l'Institut Polytechnique de Grenoble. Voir notamment la thèse La Réfrigération Magnétique : Conceptualisation, Caractérisation et Simulation de Morgan Almanza, 2015 (160 pages).

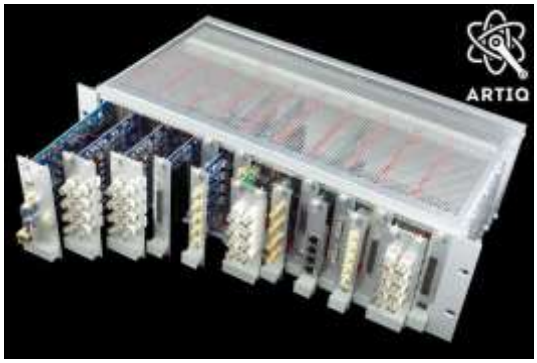
Low Noise Factory (2005, Suède) conçoit et produit des amplificateurs à faible bruit fonctionnant à températures ambiantes ou cryogéniques. Ils font partie du projet européen OpenSuperQ piloté par l'Université de Saarlandes en Allemagne, de création d'ordinateur quantique à base de qubits supraconducteurs.

Lumibird (1970, France) est un fournisseur de lasers. Anciennement Quantel et Keopsys, c'est une grande PME de plus de 800 collaborateurs et 110 M€ de CA dont 80% à l'export.

Marki Microwave (1991, USA) est un fournisseur de composants de contrôle de micro-ondes : amplificateurs, bias tees, coupleurs et filtres.

M-Labs (2007, Hong-Kong), anciennement dénommée Milkymist, travaille sur le projet ARTIQ (Advanced Real-Time Infrastructure for Quantum physics), un système qui associe le matériel et un système d'exploitation temps réel qui sert à contrôler le matériel d'ordinateurs quantiques à base d'ions piégés.

C'est un peu le pendant ions piégés de startups telles que l'israélienne Quantum Machines. Ils ont développé leur propre circuit FPGA pour ARTIQ, l'ensemble se programmant en Python.



Cette solution a été développée avec l'équipe Ion Storage Group du NIST aux USA qui travaille sur des qubits à ions piégés.

La société a été créée par un ingénieur français, Sébastien Bourdeauducq.

Nano-Meta Technologies (2010, USA) est une startup issue de l'Université de Perdue qui ambitionne de créer un système de stockage d'information quantique. C'est en fait un laboratoire de recherche privé.

Il commercialise des travaux associant photonique et nanomatériaux sous forme de propriété intellectuelle et dans des domaines variés tels qu'un système de nano-délivrance de médicaments ou des sources de photons individuelles à base de diamants dédiées à des systèmes de cryptographie quantique. Certains de ses composants innovants peuvent se retrouver dans des ordinateurs quantiques.

Photon Spot (2010, USA) développe des détecteurs de photons uniques à base de nanofils. Ils ont bénéficié de financements significatifs de la DARPA de $100K en 2014 et $1,5M en 2015.

[894] Voir LakeDiamond, des diamants à la faillite par Sébastien Ruche, février 2020.

Plassys Bestek (1987, France) est une PME qui fabrique des équipements de fabrication de composants sous vide. Ils sont leaders dans les équipements dédiés à la réalisation des jonctions Josephson et fournissent des laboratoires de recherches investis dans les qubits supraconducteurs (Yale, ETH Zurich, Rigetti, NTT, CEA Saclay).

Ils proposent aussi une machine de production de diamants artificiels utilisables dans les qubits ou systèmes de mesure à base de centres NV, le Diamond CVD Reactor SSDR150. Ils concurrencent à ce titre element 6 et (feu) Lake Diamond. La société fait environ 7M€ de CA.

Leurs machines de production dédiées aux technologies quantiques sont maintenant regroupées sous la marque Qutek Series. Rien que pour la fabrication de qubits supraconducteurs, ils proposent les MEB Systems, pour le dépôt de métal par faisceaux d'électrons (ceux-ci servent à vaporiser des atomes du métal que l'on cherche à déposer sur un substrat, le tout étant réalisé sous vide) et les MP Systems pour le dépôt par pulvérisation. Ils font aussi du dépôt d'indium par évaporation.




Photonic (2019, Canada) est une spin-off du Silicon Development Lab de l'Université Simon Fraser de Vancouver. Ils développent des qubits de photonique à base de silicium. Ils travaillent notamment sur les méthodes de conversion entre spins d'électrons et photons pour le transport d'informations quantiques entre qubits silicium.

Qontrol Systems (2016, UK) développe des composants de photonique dont des modules de lecture d'état d'appareils de photonique et des backplanes (cartes) sur lequelles on peut installer plusieurs de ces modules qui pilotent des dispositifs de photonique via une tension de 12V et lisent des signaux avec une précision de 18 bits. C'est de l'électronique de commande.

Oxford Instruments (1959, UK) est une entreprise britannique établie, cotée à Londres depuis 1999, qui est spécialisée dans l'instrumentation scientifique qui propose notamment des systèmes de cryogénie capables de descendre à 5 mK.

Ils fournissent aussi des caméras CCD servant de détecteur de l'état de qubits à base d'ions piégés, des microscopes électroniques, des systèmes de dépôt sous vide, des sources et caméras rayons-X ainsi que des spectrographes à résonance magnétique nucléaire. La société avait fait l'acquisition de VeriCold Technologies (Allemagne) en 2007 pour acquérir la maîtrise de têtes pulsées servant de premier étage de réfrigération de cryostats à sec.

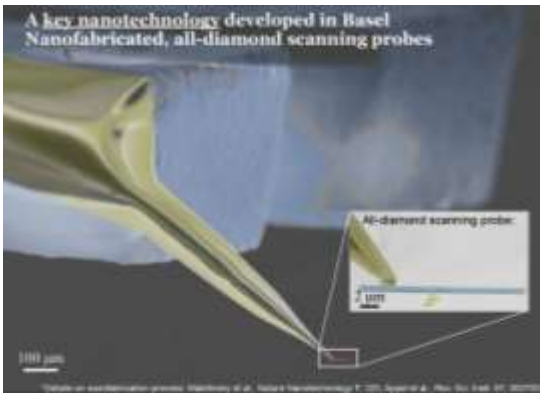
Qblox (2018, Pays-Bas) est une spin-off de QuTech qui développe de l'électronique de commande « scalable » de qubits supraconducteurs. On dirait des générateurs de micro-ondes somme toute assez classiques en apparence, les technologies les plus avancées consistant à générer ces micro-ondes dans des circuits fonctionnant à température très basse, 4K ou moins, et intégrés dans les cryostats.

La société se faisait curieusement distinguer au CES 2021 en étant nominée dans les awards de l'innovation du salon, ayant lieu, cause covid-19, entièrement en mode virtuel en janvier 2021.

Q-Lion (2019, Espagne) développe une solution de code de corrections d'erreurs pour qubits à ions piégés. La startup est issue du programme d'incubation Explorer de la Banque de Santander. Elle a été créée par Andrea Rodriguez Blanco, qui était encore en train de travailler sur une thèse en 2020.

Qnami (2017, Suisse, $2,9M) est une spin-off du laboratoire de recherche en métrologie quantique de l'Université de Bâle. Ils produisent notamment des diamants artificiels destinés à diverses applications de photonique.

Leur premier marché est pour l'instant celui de la métrologie quantique qui s'appuie sur leurs nanodiamants Quantilever MX comprenant des NV-centers (atome d'azote à côté d'une lacune de carbone). Ils proposent notamment une gamme de produits de microscopies confoncale comprenant le ProteusQ servant à analyser des matériaux ferromagnétiques. Le fonds d'investissement français Quantonation fait partie de ses investisseurs. Et l'un des cofondateurs et le CEO, Mathieu Munsch, est passé par l'ENS Grenoble INP Phelma et a travaillé au CEA de Grenoble.

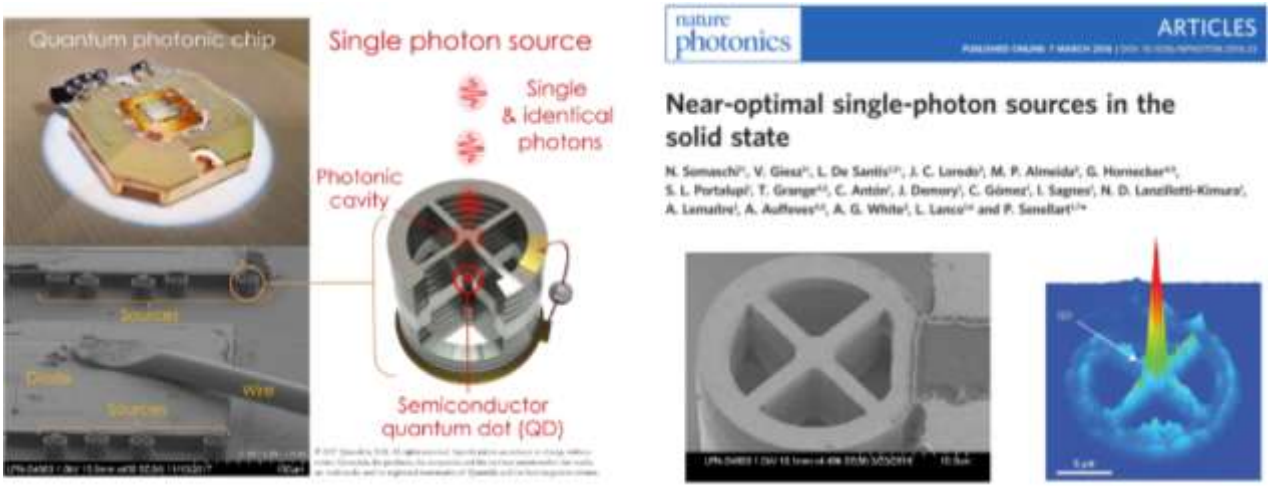


Quandela (2017, France, 1,5M€) est une startup basée à Massy dans le sud de l'Ile de France, qui est spécialisée dans la génération de sources de photons uniques et indiscernables à base de quantum dots destinées au monde de la recherche, des télécommunications et du calcul quantique.

L'équipe de quandela est composée de Valerian Giesz (CEO), ingénieur de l'Institut d'Optique avec un doctorat en photonique, Niccolo Somaschi (CTO), docteur de l'Université de Southampton et Pascale Senellart (CSO), directrice de recherche au C2N (CNRS, Université Paris-Saclay) dont la startup est issue. Ils ont aussi Alain Aspect, Andrew White et Eleni Diamanti dans leur advisory board. La startup était grand prix du concours i-Lab 2018 et comptait une dizaine de personnes en septembre 2020 et plusieurs clients à l'international, principalement en Europe et en Asie.

Avec un seul atome piégé, et forcé à émettre dans une direction donnée grâce à de l'électrodynamique quantique en cavité activée par un laser, ils arrivent à générer des trains de photons bien séparés dans le temps et de caractéristiques quantiques stables, de longueur d'onde 924 nm à 928 nm dans le proche infrarouge[895]. C'est un principe voisin de celui du laser, mais avec un seul atome activé et un seul photon émis à la fois.

Cela permet de générer des sources de photons uniques très brillantes qui peuvent ensuite être démultipliés pour créer des photons indiscernables exploitables dans des processeurs quantiques à photons ou diverses autres applications comme la cryptographie quantique[896].



La source de photons doit être refroidie dans une plage de température de 5K-10K, ce qui est réalisable avec des cryostats compacts de seulement quelques milliers d'Euros et utilisant de l'hélium 4, comme l'attoDRY800 d'**Attocube** (Allemagne).

Ces cryostats utilisent une tête pulsée, équivalente au premier étage du refroidissement des cryostats à dilution à sec que nous avons étudié sur les calculateurs quantiques à base de qubits supraconducteurs et silicium.

Comme nous l'avons vu dans la partie dédiée aux qubits photons, ces photons uniques sont particulièrement indiqués pour permettre de créer des portes quantiques de qubits de qualité.

L'équipe de Quandela illustre la qualité de ses photons uniques avec les données issues de deux expériences très connues des photoniciens. La première utilise une variante d'un autocorrélateur d'intensité **Hanbury Brown et Twiss** (HBT) qui permet de vérifier que les photons sont émis de manière bien régulière, comme un métronome[897].

---

[895] Voir Near optimal single-photon sources in the solid state, Niccolo Somachi, Valerian Giez, Pascale Senellart et al, 2016 (23 pages). Pascale Senellart décrit en detail la manière dont sont fabriqués les générateurs de photons de Quandela dans son intervention Quantum optics with artificial atoms dans une Rochester Lecture en juin 2018 (1h10mn). Les prestigieuses Rochester Lectures ont lieu une fois par an à Durham au Royaume-Uni. L'édition 2017 accueillait Peter Knight et celle de 2012, Alain Aspect.

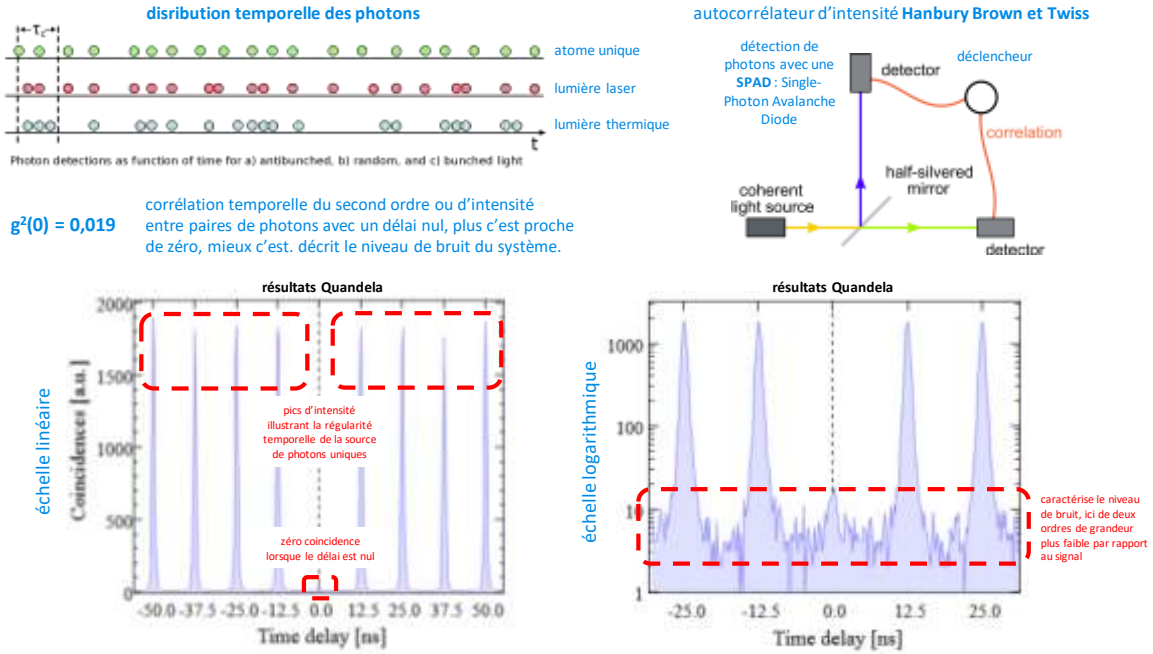
[896] Le procédé était amélioré dans le laboratoire de Pascale Senellart en 2020 pour générer des sources de photons encore plus brillantes et pures d'un point de vue spectral et polarisation grâce à une excitaton du quantum dot avec des phonons. Voir Efficient Source of Indistinguishable Single-Photons based on Phonon-Assisted Excitation par S. E. Thomas, Pascale Senellart et al, juillet 2020 (10 pages).

[897] Cette expérience créé à l'origine pour détecter la taille des étoiles a aussi permis de valider la nature corpusculaire des photons. L'expérience peut être facilement interprétée de manière intuitive : les photons traversent un miroir sans tain, qu'il traverse ou pas de manière aléatoire. Derrière ce miroir sont placés deux compteurs de photons, ici, avec des SPAD (diodes avalanches). Le système détecte les cas où un photon est détecté en même temps par les deux capteurs. Si les photons font le même chemin pour aller dans les deux détecteurs, il n'y aura pas de coïncidence puisque les photons émis sont envoyés en train bien ordonnancés et ne peuvent être que d'un côté ou de l'autre. Mais en ajoutant un retard entre le miroir et l'un des capteurs qui soit proportionnel à la période d'émission des photons, cela va créer de nombreuses occurrences avec des photons arrivant simultanément dans les deux capteurs. C'est ce que l'on voit dans les deux courbes, l'une d'entre elle étant avec une échelle linéaire de coïncidences (mesurée sur un laps de temps suffisant pour en capter des centaines) et une autre logarithmique qui permet de mieux caractériser le bruit du système.

C'est le phénomène de l'antibunching des photons, ou de leur dégroupement temporel alors que dans la lumière naturelle et celle des lasers, ils sont émis de manière aléatoire et sont souvent regroupés.

A partir d'un click de départ sur l'un des deux détecteurs de photons, ils analysent la répartition dans le temps de l'apparition des photons suivants. Cela donne les courbes *ci-dessous*. Le modèle idéal serait celui d'un pic haut de part et d'autre du centre. Les pics bas représentent le bruit du système.

La seconde expérience dite H.O.M. pour **Hong-Ou & Mandel** utilise un interféromètre Mach-Zehnder pour valider le fait que les photons émis sont bien identiques et impossibles à distinguer.



Le générateur de photons de Quandela était proposé jusqu'à présent avec la combinaison de deux produits packagés :

- Le **Qubit Control Single Unit** qui permet de filtrer complètement les photons uniques émis par les sources dans un cryostat attocube du laser utilisé pour l'excitation du quantum dot. Il est surtout composé de filtres accordés à l'énergie de la transition optique de l'émetteur.

- Le **QShaper** est un appareil plus compact qui génère des impulsions lasers femto/pico-secondes sur une fibre optique qui va ensuite alimenter le quantum dot du QCSU ci-dessus. Il est alimenté en entrée par le laser du client. Il sert à préparer le faisceau laser avec la bonne forme spatiale et temporelle. C'est un appareil constitué de filtres divers. Il est calibré pour bien alimenter les sources semiconductrices.

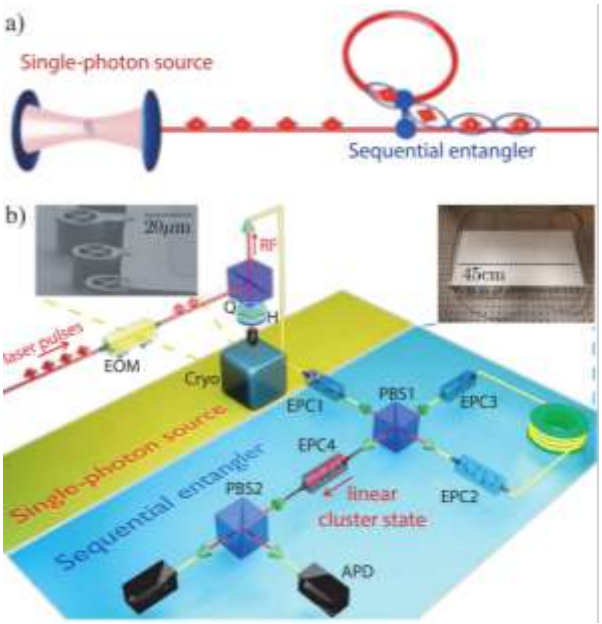
Quandela prépare pour la fin 2020 une version compacte et intégré de tout cet ensemble, qui tient dans un rack de datacenter. La fibre sera collée à la source de photons ce qui supprimera la partie mécanique du calibrage. La tête pulsée du cryostat 4K est aussi intégrée dans ce rack 3U, le compresseur étant à l'extérieur et refroidit par eau dans un premier temps. A terme, il sera intégré dans le rack et refroidi par air.

Le rack a été dessiné par Pentagram, le même designer anglais que celui auquel IBM a fait appel pour le Q System One lancé en janvier 2019. Il fait 1,75m de haut et 80 cm de largeur. Il empile tous les éléments : le QShaper, le nouveau QCF et un ordinateur de contrôle avec son clavier. Le tout consommera environ 5 à 6 kW. C'est le cryostat qui consomme le plus dans l'affaire.

La startup a été financée au départ par un prêt de l'accélérateur Wilco en 2017, puis par ses premières ventes. Elle vient de faire rentrer le fonds Quantonation dans son capital en 2020 en plus de Bpifrance.

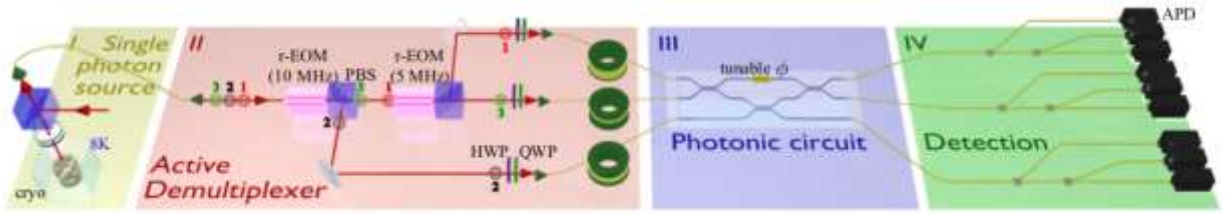
Quandela et le laboratoire du C2N collaborent avec des laboratoires de recherche dans le monde entier pour créer des plateformes de photonique avancée.

En 2020, ils publiaient avec une équipe de l'**Université Hébraïque de Jérusalem** un papier portant sur la création d'un « cluster state » de photons destiné à du calcul quantique (*ci-dessous*). Il s'agit d'utiliser un train de photons uniques pour les intriquer ensuite entre eux via une ligne à retard et les injecter dans un circuit de calcul basé sur la méthode du MBQC (measurement based quantum computing)[898].



En Europe, ils collaborent surtout avec l'équipe de **Fabio Sciarrino** en Italie, aux Pays Bas avec **Quix**, en Espagne avec l'**INL** et d'autres équipes en Autriche, au Royaume-Uni, en Slovaquie et en Israël. Ils font partie du projet FET européen PHOQUSING d'échantillonnage de bosons piloté par l'équipe de Fabio Sciarrino en Italie et financé à hauteur de 3,3M€.

En 2019, ils expérimentaient la source de photons de Quandela pour la démultiplexer en trois photons injectés ensuite dans un circuit intégré de photonique intégrant une porte quantique programmable. Le circuit de photonique était gravé précisément avec un laser femtoseconde[899].



Avec **QuiX**, sont impliqués dans un autre projet européen financé par un ERC pour créer un processeur quantique de machine learning, exploitant plusieurs sources Quandela.

Quantum Machines (2018, Israël, $23M) développe une couche de contrôle des qubits pour des ordinateurs quantiques supraconducteurs qui associe matériel et logiciel[900]. C'est une spin-off du laboratoire de recherche Braun Center for Submicron Research de l'Institut Weizmann.

[898] Voir Sequential generation of linear cluster states from a single photon emitter par D. Istrati et al, 2020 (14 pages).

[899] Voir Interfacing scalable photonic platforms: solid-state based multi-photon interference in a reconfigurable glass chip par Pascale Senellart et al, 2019 (7 pages).

[900] Voir The Story of the First Israeli Quantum Computing Startup, par Eliran Rubin, décembre 2018.

La startup annonçait une belle levée de fonds de $17,5M en mars 2020. Mi-2020, elle avait déjà une trentaine de collaborateurs.

Ils ont développé leur propre processeur classique de contrôle de qubits, un FPGA fonctionnant à température ambiante, qui génère les pulsations micro-ondes de contrôle des qubits et de la mesure de leurs états. Il supporterait aussi les qubits à NV centers, ions piégés et à atomes froids, qui utilisent des commandes différentes, notamment à base de lasers.

Ils ont déjà presque une dizaine de clients, dont l'ENS à Paris et la startup Alice&Bob. Et pour cause, Itamar Sivan, le cofondateur et CEO de la startup avait fait un Master à l'ENS entre 2009 et 2011 !

Leur processeur s'intègre dans leur « Quantum Orchestration Platform » qui associe aussi une couche logicielle[901] . En juin 2020, ils annonçaient la création du langage **QUA** qui est positionné comme un langage permettant de créer des algorithmes hybrides quantiques et classiques, de type VQE et QAOA qui ont besoin d'obtenir un feedback rapide entre les processeurs classiques et quantiques. C'est le language de programmation qui fonctionne avec tous types de qubits, supraconducteurs, silicium, atomes froids et ions piégés. Le compilateur tient ainsi compte des différences de mise en œuvre des qubits : leur connectivité, l'homogénéité ou hétérogénéité de leur couplage, les temps de cohérence, les taux d'erreurs, etc.

Quantum Opus (2013, USA) développe des détecteurs de photons uniques à base de nanofils supraconducteurs, les Opus One. La version compacte Opus Two est un boîtier 8U pour rack de data center, cryostat compris[902]. Cette société a aussi bénéficié de financements fédéraux US, dont $100K en 2015 et $1,5M en 2015 provenant de la DARPA puis $125K de la NASA en 2018. Elle équipe notamment l'expérience de gaussian boson sampling chinoise annoncé en décembre 2020.

Quantum Microwave (2016, USA) développe et produit des composants micro-ondes fonctionnant à température cryogénique pour les ordinateurs quantiques. Cela comprend des préamplificateurs, filtres, atténuateurs, coupleurs et multiplexeurs de fréquences.

On les retrouve surtout dans les ordinateurs à qubits supraconducteurs à effet Josephson (IBM, Google, Rigetti, D-Wave). Ils ne poussent cependant pas à la miniaturisation de ces composants comme le tente SeeQC.

Qubitekk (2012, USA) est un fournisseur de sources de photons et de photons intriqués utilisables dans le contexte de la cryptographie quantique (QKD). Cette technologie peut aussi servir pour gérer une partie de la communication entre qubits dans certains types d'ordinateurs quantiques.

Il concurrence dans une certaine mesure la startup française Quandela dont les sources de photons indiscernables semblent avoir un spectre d'applications plus large.

---

[901] Voir La société israélienne Quantum Machines lève 17,5 millions de dollars par Benjamin Terrasson, 2020, Quantum Machines raises $17.5M for its Quantum Orchestration Platform par Frederic Lardinois, mars 2020, Israel gets ready to join global quantum computing race par Amitai Ziv, décembre 2019 et The quantum computer is about to change the world. Three Israelis are leading the revolution par Oded Carmeli, février 2020.

[902] Voir Introduction to Quantum Opus and revolutionary superconducting detection systems (14 slides).

QuTech (2014, Pays-Bas) est la spin off "hardware quantique" de l'Université TU Delft. Elle collabore notamment avec Intel dans la mise au point de qubits supraconducteurs et avec Microsoft dans le quantique topologique.

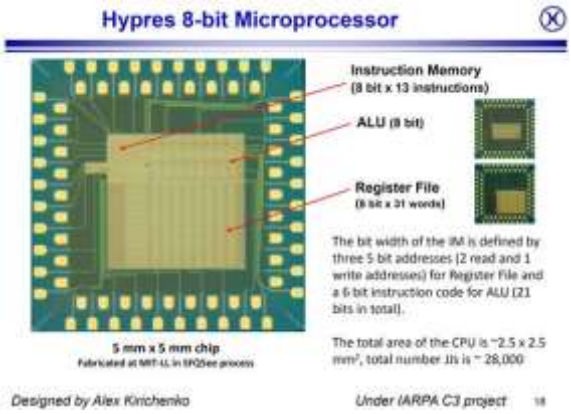
La société se positionne plutôt comme un laboratoire de recherche appliquée que comme une start-tup "produit". Elle développe cependant aussi des logiciels, comme la plateforme de développement **Quantum Inspire** qui permet notamment d'exécuter sur calculateurs classiques des algorithmes quantiques en mode émulation. Elle fournit une interface graphique de programmation dans le langage QASM. Le code peut ensuite être exécuté en mode émulation dans le cloud sur une machine classique, le supercalculateur national hollandais Cartesius, avec 5, 26 et 32 qubits, selon les formules choisies. Cartesius est équipé de milliers de CPU Intel Xeon et Xeon Phi et de quelques dizaines de GPU Nvidia Tesla K40m avec 130 To de mémoire délivrant 1,84 PFLOPS. L'équipement provient d'Atos-Bull. Quantum Inspire permet aussi d'accéder en mode cloud à des qubits de QuTech. L'ensemble a été lancé en avril 2020.

Scontel (2004, Russie) propose des détecteurs de photons uniques dans le visible et l'infrarouge (SSPD pour Superconducting Single Photon Detecting Systems). Ces détecteurs sont cryogénisés à 2,2K à l'hélium 4 avec un système à tête pulsée Sumitomo SRDK 101 accompagné d'un compresseur HC-4E réfrigéré par eau.

SeeQC (2017, USA, $11,8M) est une spin-off du groupe américain Hypres, spécialisée dans la création d'électronique supraconductrice et crée par John Levy, Matthew Hutchings et Oleg Mukhanov[903]. Sa maison mère Hypres (1983, USA, $50K) est déjà un spécialiste de longue date des circuits électroniques supraconducteurs.

Son nom signifie « Superconducting Energy Efficient Quantum Computing ». Elle se focalise dans la création de circuits de contrôle de qubits supraconducteurs eux-mêmes supraconducteurs dotés de mémoires à base de technologie spintronique (spin d'électrons). Leur chipset de contrôle est conçu pour être placé à l'étage 4K du cryostat. Il exploite des jonctions Josephson dans des circuits supraconducteurs SFQ.

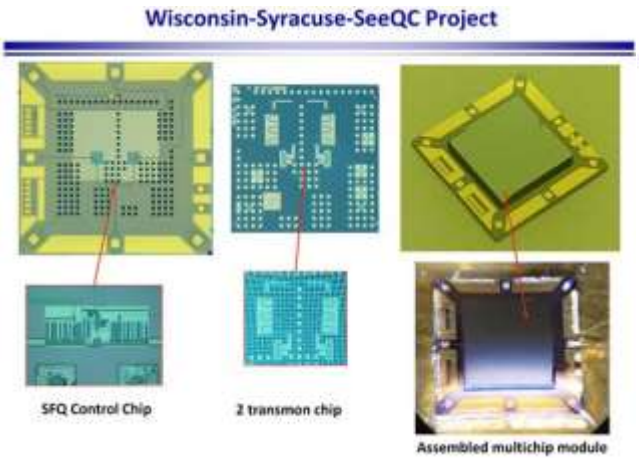
Dénommé Digital Quantum Management (DQM) System-on-a-Chip, le circuit comprend les générateurs de micro-ondes de pilotage des qubits (avec DAC, des convertisseurs de signaux numériques en analogiques) et de l'électronique de lecture de l'état des qubits (avec des ADC, convertisseurs des signaux de micro-ondes analogiques en versions numériques). C'est censé énormément simplifier la connectique interne de l'ordinateur, enlevant tous ces câbles supraconducteurs ainsi que les composants d'atténuation et d'amplification de micro-ondes[904].

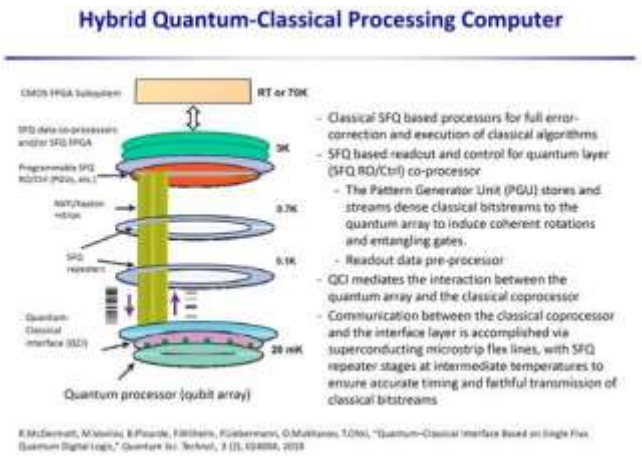


[903] En installant des bureaux à Milan et au Royaume-Uni, la startup a trouvé le moyen de récupérer des financements européens pour sa recherche. Ils collaborent sinon avec l'équipe de Robert McDermott de l'Université du Wisconsin et celle de Syracuse au nord de l'Etat de New York.

[904] J'ai trouvé des explications les concernant dans Single Flux Quantum Logic for Digital Applications par Oleg Mukhanov, août 2019 (33 slides) ainsi que dans Quantum–Classical Interface Based on Single Flux Quantum Digital Logic par Robert McDermott et al, 2017 (16 pages). Voir également Accurate Qubit Control with Single Flux Quantum Pulses par Robert McDermott et M.G. Vavilov, 2014 (10 pages) et Scalable Hardware-Efficient Qubit Control with Single Flux Quantum Pulse Sequences par Kangbo Li, Robert McDermott et Maxim G. Vavilov, 2019 (10 pages).

La société a en fait été financée dans le cadre du projet C3 de l'agence IARPA lancé en 2016. Comme nous l'avons vu dans la partie dédiée aux composants des ordinateurs quantiques et dans celle qui est dédiée au calcul supraconducteur classique, cette société a une position stratégique pour faciliter le développement d'ordinateurs quantiques scalable, notamment à base de qubits supraconducteurs. A surveiller donc de très près !

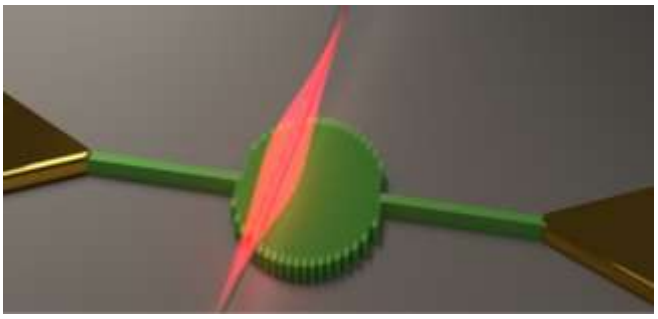


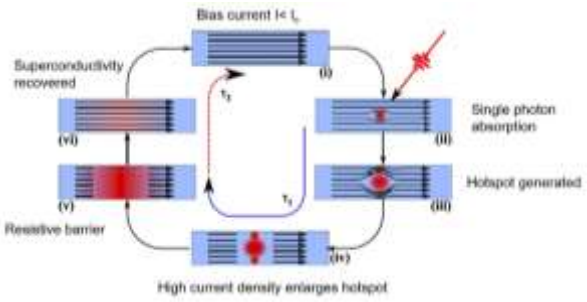


S-Fifteen Instruments (2017, Singapour) est une spin-off du fameux laboratoire CQT de Singapour et qui développe des systèmes de contrôle de qubits et des solutions de cryptographie quantique.

Single Quantum (2012, Pays-Bas) propose des détecteurs de photons uniques Qos, intégré dans un cryostat refroidi à l'hélium liquide à 2,5K. Leur capteur utilise la technique SNSPD (superconducting nanowire single photon detector) qui comprend un film mince de nanofils supraconducteurs en forme de serpentin aplati.

Ce dispositif permet de capter un photon unique issu d'une fibre optique. Les applications sont nombreuses et couvrent notamment le calcul quantique à base de photons, la métrologie ainsi que les télécommunications quantiques.





Sparrow Quantum (2016, Danemark) est une spin-off du laboratoire de recherche en photonique Niels Bohr. Comme Quandella et Qubitek, ils proposent des sources de photons uniques.

Stable Laser Systems (2009, USA) propose des lasers et des cavités Fabry-Perot utilisables notamment pour le confinement d'atomes froids. La startup lancée par Mark Notcutt est basée à Boulder dans le Colorado, l'un des centres névralgiques des technologies quantiques aux USA, près du NIST et de l'Université du Colorado. Son équipe comprend aussi Jan Hall, prix Nobel de physique en 2005 pour la découverte de l'effet qui porte son nom.

Toptica Photonics (1998, Allemagne) est un équipementier en photonique qui développe des sources laser couvrant une large gamme de fréquences allant de 190nm (UV) aux ondes TeraHertz et notamment des diodes lasers et des peignes de fréquences. Leurs lasers peuvent notamment servir à contrôler des ions piégés et des atomes froids[905].

La PME emploie plus de 300 personnes pour $82M de CA.

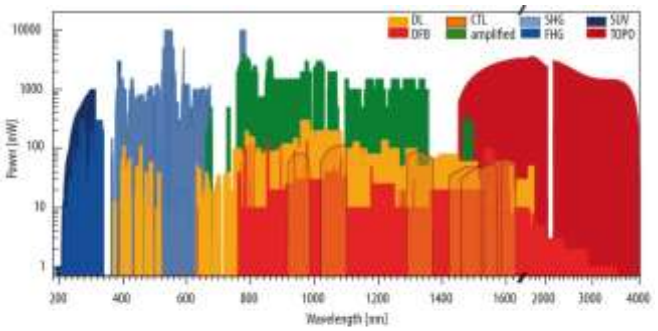


Fig 2. Each quantum system requires lasers with a specific combination of wavelengths and power levels. The broad wavelength coverage from 190 nm to 4 µm provided by Toptica's tunable diode lasers combined with reliable and convenient operation therefore enables many spectacular applications of quantum technologies. (Source: Toptica)

Vapor Cell Technologies (2020, USA) fournit des capsules d'atomes alkalins, principalement de rubidium, exploitables dans diverses solutions miniaturisées utilisant des atomes froids[906]. La société a été créée par Doug Bopp, un ancien chercheur du NIST de Boulder.

VLC Photonics (2011, Espagne) produit de l'appareillage de photonique et réalise de la conception en mode fabless de circuits intégrés de photonique. La société est impliquée dans des projets du Flagship européen.

C'est une spin-off de l'Université de Valence. La société a été créée par Iñigo Artundo, Pascual Muñoz, José Capmany et José David Domenech. Ils commercialisent aussi des rapports techniques à des prix allant de 4K€ à 5,4K€ la pièce.

Zurich Instruments (2008, Suisse, $112K) est un fabricant d'appareillage électronique de tests et de mesures. Ils proposent une gamme de produits adaptés à la création d'ordinateurs quantiques, en particulier de type supraconducteur à effet Josephson.

Leur offre s'articule autour de leur Quantum Computing Control System qui fait le pont entre les outils de pilotage logiciels de l'ordinateur quantique et l'instrumentation électronique associée.

Ce système comprend plusieurs composants : le PQSC (Programmable Quantum System Controller, *ci-dessous en haut à gauche*) qui sert à programmer et piloter l'ensemble des appareils.

---

[905] Voir The Control of Quantum States with Lasers dans Photonics View, 2019 (3 pages).

[906] Voir Chip-scale atomic devices par John Kitching, 2018 (39 pages) qui fait un très intéressant inventaire des composants de mesure utilisant cette technologie : magnétomètres, gyroscopes, horloges atomiques. Vous direz que cela devrait aller dans la rubrique métrologie et vous aurez raison.

Il est équipé d'un FPGA Xilinx UltraScale+ pilotable par le logiciel LabOne et via Python, C, MATLAB, LabVIEW et le framework .NET de Microsoft. Il peut gérer jusqu'à une centaine de qubits. Cela passe par le contrôle de jusqu'à 18 générateurs de micro-ondes HDAWG (High Density Arbitrary Waveform Generator, *ci-dessous plus bas en bleu*). Ils sont vendus 23K€ la pièce !

Ces générateurs créent des impulsions micro-ondes qui associent une forme d'onde (gaussienne ou autre, *ci-dessous* à droite) modulée par un signal à haute-fréquence, compris en général entre 5 et 10 GHz (résultat *ci-dessous* en bas à droite). Il peut contrôler 8 canaux. Ces micro-ondes sont envoyées sur les qubits pour les remettre à zéro ou activer des portes quantiques.

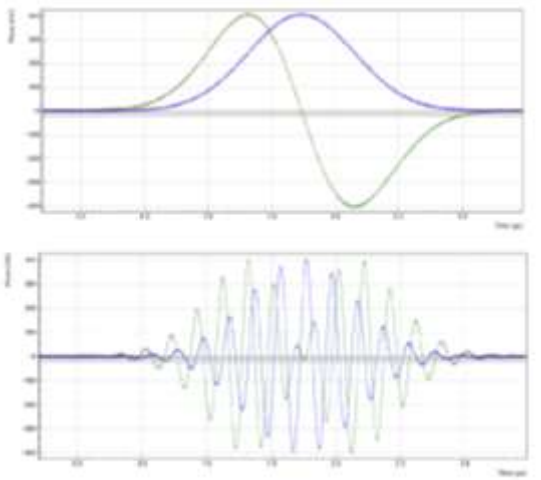


Figure 3.15. Dual-channel signal generated by the AWG and captured by the scope. The top figure shows two envelope waveforms played without modulation, the bottom figure shows the same envelope waveforms played with enabled modulation.

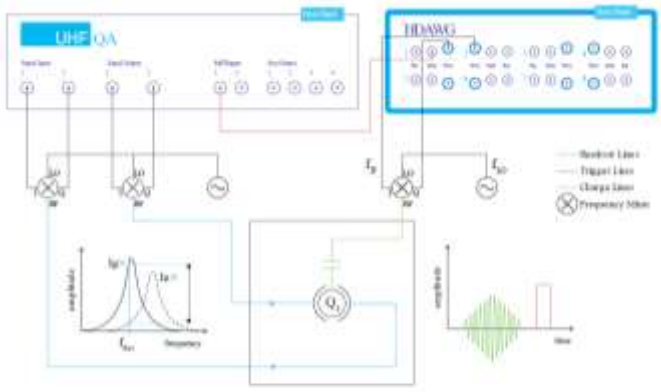


Figure 3.19. Experimental measurement setup and visualization of key signals. The element labeled as Q_i denotes a qubit dispersively coupled to a resonator.

Les portes quantiques à un qubit sont générées par l'envoi d'un paquet de micro-ondes modulé qui va modifier le niveau d'énergie du qubits et changer son état. Le tout est complété par l'UHFQA (Ultra-High Frequency Quantum Analyzer) qui peut analyser l'état de 10 qubits. Dans le schéma *ci-contre*, F_{LO} est la fréquence du signal micro-ondes à moduler, F_{IF} est la forme d'onde de modulation. Du côté de l'UHFQA, le système détecte la modification de modulation ou de phase du signal récupéré par le biais d'un résonateur associé au qubits.

Zyvex Labs (1997, USA) développe des solutions de production de composants à l'échelle atomique (APM : atomic precise manufacturing) qui peuvent servir à produire des composants utilisables dans le calcul quantique (comme le dépôt de dopants pour des qubits supraconducteurs et silicium) et dans la métrologie quantique.

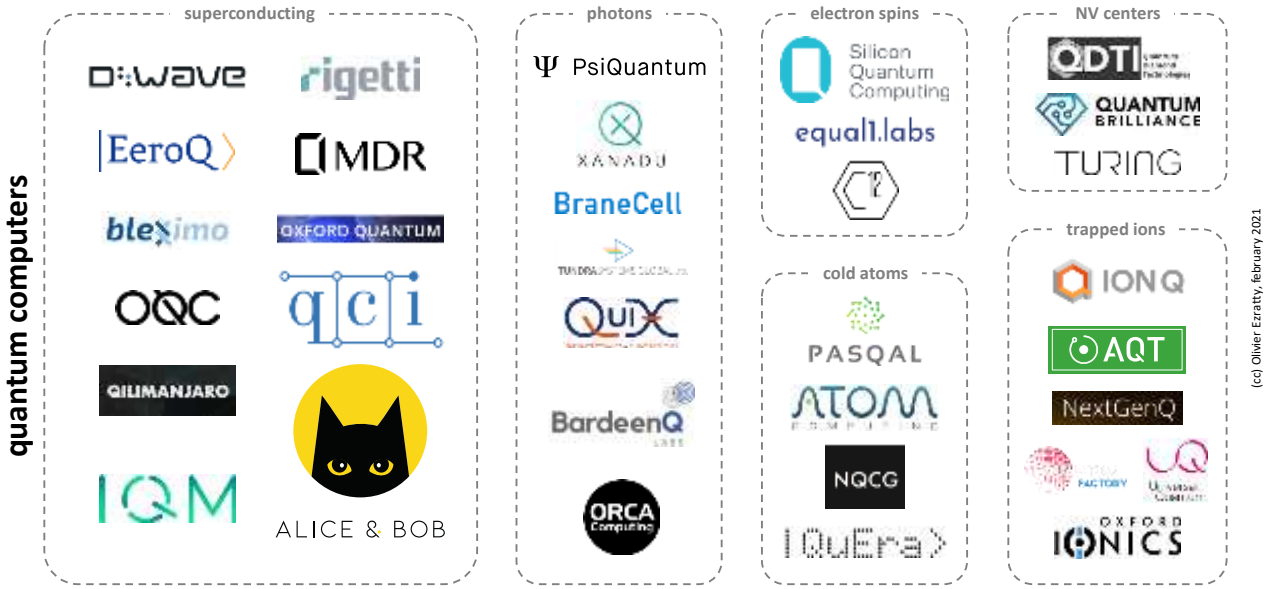
Ils ont été financés par des programmes de recherche SBIR par le NIST, la DARPA et le Département de l'Energie. La société a été créée par Jim Von Ehr.

Enfin, sans rentrer dans les détails, citons à nouveau **BlueFors Cryogenics** (Finlande), **Bruker** (USA) et **Janis** (USA) qui sont spécialisés dans la production de systèmes de cryogénie utilisés notamment pour les ordinateurs quantiques qui doivent fonctionner à de très basses températures, situées entre 10 et 20 mK.

Ordinateurs

Voici quelques PME et startups qui cherchent à créer des processeurs ou ordinateurs quantiques en plus de D-Wave, IonQ et Rigetti que nous avons déjà couverts en détail.

Très souvent, ces entreprises s'affichent comme étant "full stack", ce qui veut dire qu'elles ambitionnent de créer à la fois un ordinateur quantique et toute l'infrastructure logicielle qui l'accompagne. C'est souvent justifié pour les couches basses logicielles qui peuvent dépendre de l'architecture des qubits de l'ordinateur créé.



Pour les couches plus hautes, notamment au niveau des frameworks de développement, ce n'est pas forcément bien vu. Il vaudrait mieux se raccrocher aux frameworks qui commencent à s'imposer ou à ceux d'entre eux qui sont open source et multi-plateformes. Dans d'autres cas, les startups ici citées en sont au stade de la recherche appliquée pour créer un processeur quantique. Elles sont généralement loin d'avoir créé une infrastructure logicielle.

Alice&Bob (2020, France, 3,3M€) est une jeune startup crée par Théau Peronnin (ENS Lyon) et Raphaël Lescanne (ENS Paris) qui veut commercialiser une technologie de qubits plus fiables que l'état de l'art en allant jusqu'à promettre la création d'un ordinateur quantique complet d'ici 2024. Il s'agit d'une valorisation des thèses de doctorat de Théau et Raphaël (pas terminées en avril 2020) et de travaux associant notamment l'équipe Quantic de Mazyar Mirrahimi à l'Inria (où Raphaël Lescanne était doctorant et où travaille aussi Zaki Leghtas[907]), le CNRS et les ENS de Lyon et Paris.

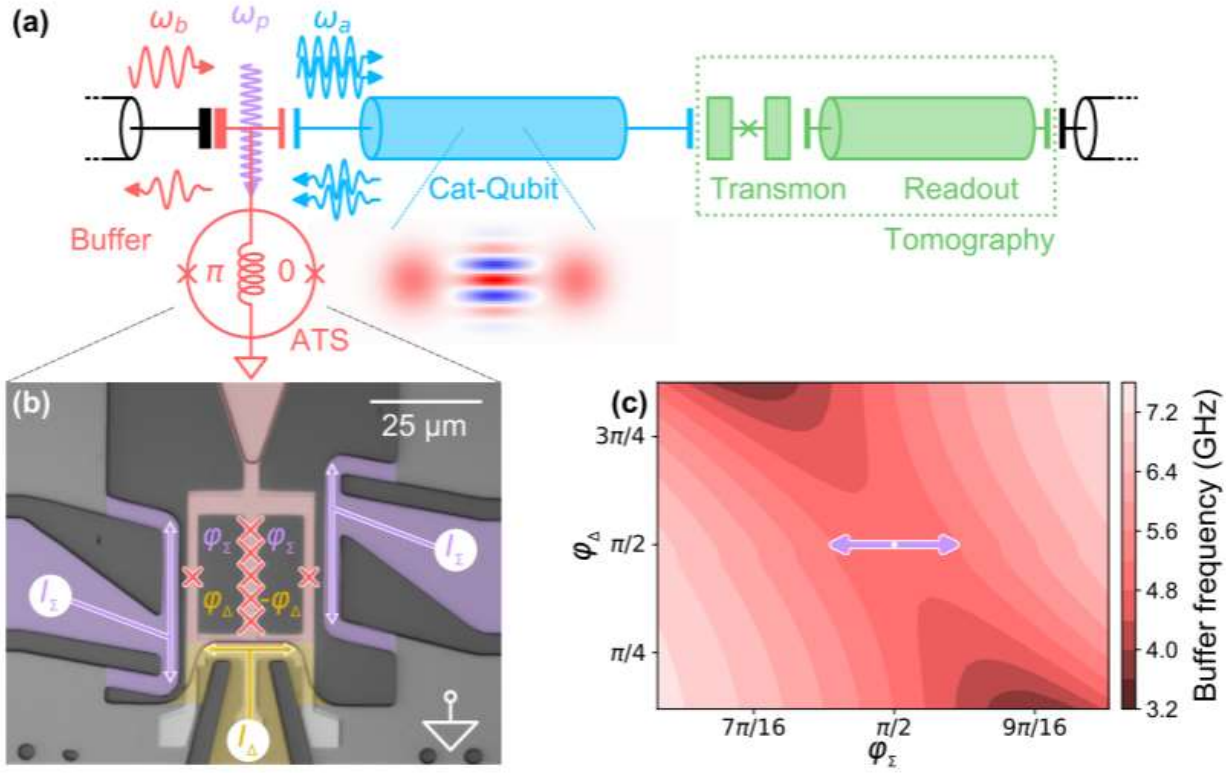
L'idée consiste à encoder coupler une cavité encodant des microondes de type « chat de Schrodinger » couplée à un qubit transmon pour leur lecture. Ces cat-qubits superposent des états quantiques opposés[908]. Ils forment des qubits qui s'auto-corrigent, pour l'instant au niveau des erreurs de flip. Il reste encore à corriger les erreurs de phase pour que cela devienne opérationnel.

[907] Qui a fait son post-doc dans l'équipe de Michel Devoret à Yale. Michel Devoret est la principale source d'inspiration du type de qubits exploité par Alice&Bob. Voir Dynamically protected cat-qubits: a new paradigm for universal quantum computation par Mazyar Mirrahimi, Zaki Leghtas et… Michel Devoret, 2013 (28 pages).

[908] Voir Exponential suppression of bit-flips in a qubit encoded in an oscillator de Raphaël Lescanne et al, juillet 2019 (18 pages) et Repetition Cat Qubits for Fault-Tolerant Quantum Computation par Jérémie Guillaud et Mazyar Mirrahimi, juillet 2019 (23 pages).

Ces qubits sont plus compliqués à fabriquer (cf schéma *ci-dessous*) mais il n'en faudrait qu'une trentaine pour créer un qubit logique, ce qui permettrait d'obtenir une architecture plus facilement scalable alors que dans les technologies actuelles d'IBM, Google ou Rigetti, il faudrait plus de 100 000 qubits physiques pour constituer un qubit logique. Qui plus est, leur système évite les effets du rayonnement de micro-ondes entre qubits adjacents qui perturbe leur cohérence.

Il leur reste aussi du travail pour créer un jeu de portes quantiques universelles. Ils travaillent sur une CNOT et devront ajouter une porte Toffoli à trois qubits. Ils créeront une porte d'Hadamard avec une porte Toffoli et une SWAP avec trois CNOT. Le tout va nécessiter un compilateur spécifique, qu'ils codéveloppent avec Atos.



Alpine Quantum Technologies ou **AQT** (2017, Autriche, $12,3M) est une spin-off de l'Université d'Innsbruck crée par Rainer Blatt. Peter Zoller et Thomas Monz et qui se focalise sur les systèmes de qubits à base d'ions piégés, le premier d'entre eux en étant l'un des pionniers.

Leur financement est pour l'instant d'origine publique, issu des équivalents autrichiens de notre Ministère de la Recherche et de l'ANR. Ils ont notamment évalué le taux d'erreurs de qubits en fonction de leur nombre. La fidélité des qubits est de 99,6% pour deux qubits et elle descend à 86% pour 10 qubit[909].

AQT pilote ses ions piégés par des micro-ondes sans faire appel à des lasers, ce qui simplifie le dispositif. Ils n'utilisent qu'un seul laser pour la photo-ionisation qui crée les ions au démarrage et un autre pour la mesure de l'état des qubits par fluorescence après les calculs.

[909] Voir Characterizing large-scale quantum computers via cycle benchmarking par Alexander Erhard et al, 2019 (13 pages).

Atom Computing (2018, USA) ambitionne de créer un ordinateur quantique à base d'atomes neutres contrôlés optiquement[910]. C'est un des concurrents de la startup française Pasqal.

La startup avait d'ailleurs été lancée après avoir analysé les résultats du laboratoire d'Antoine Browaeys de l'Institut d'Optique. Cela illustre la question du timing dans la bataille de la création de startups quantiques.

BardeenQ Labs (2019, USA) s'est lancé dans un projet que l'on peut qualifier d'assez futuriste compte-tenu de l'état de l'art actuel. Il s'agit de créer un système quantique embarqué pour véhicules autonomes avec de l'intelligence artificielle, un processeur quantique embarqué fonctionnant à température ambiante, de la mémoire quantique, des matériaux topologiques et des capteurs quantiques.

Rien que ça ! En fait, la société est une sorte d'incubateur qui héberge plusieurs startups.

Bleximo (2017, USA, $1,5M) veut développer des coprocesseurs quantiques adaptés à différents marchés dont les biotechs, les qASIC, à base de qubits supraconducteurs à effet Josephson.

Ils sont partenaires de Q-CTRL qui développe des logiciels quantiques de codes de correction d'erreur. La startup a été créée par Alexei Marchenkov et Richard Maydra, deux anciens de Rigetti. Il est très difficile de savoir ce qu'ils font exactement ni quelle technologie de qubits ils maîtrisent.

BraneCell (2015, Cambridge Massachusetts et Dusseldorf, $1,8M) est une startup lancée par Wassim Estephan et Christopher Papile (*ci-contre*). Elle développe un processeur quantique fonctionnant à température ambiante. Il s'agit en fait d'un système utilisant des atomes froids avec un procédé qui rappelle furieusement ce que fait la startup française Pasqal. L'idée est de permettre d'exécuter des programmes quantiques de manière décentralisée et pas dans des data centers[911] ! Ils ont déposé quelques brevets sur la question notamment le brevet USPTO 9607271 validé en mars 2017[912].

C12 Quantum Electronics (2019, France), anciennement CNT Nanotech, est une société lancée par Mathieu Desjardins et son frère jumeau Pierre. C'est un projet issu de l'ENS Paris devenu une startup en phase de création ayant Maud Vinet comme scientific advisor.

---

[910] Voici quelques éléments d'informations dans Neutral Atom Quantum Computing du Anderson Group Optical Physics ainsi que dans Quantum computing with neutral atoms, de David Weiss 2017 (7 pages).

[911] Leur communication est pour le moins cryptique, comme BraneCell Systems Presents Distributed Quantum Information Processing for Future Cities en avril 2018 et un partenariat annoncé avec le prestataire de services du gouvernement US, AST, en juillet 2018, dans AST and BraneCell Announce Their Partnership to Improve Critical Government Functions Through the Power of Quantum Computing. Ils ne fournissent aucune information technique ni de vulgarisation sur leur solution, sur le nombre de qubits et le taux d'erreurs. Ils visaient aussi une ICO qui aurait été la première du genre pour une startup de l'informatique quantique. Ils visent surtout à créer un système de communication sécurisé. Ils ciblent la finance, l'énergie, la santé, la chimie et le secteur public. Un Theranos du quantique ? Au minimum, on est en droit de douter.

[912] Voici la description du brevet : "*The subject matter relates to multiple parallel ensembles of early stage spherical pulses radiated through engineered arrays forming the foundation for quantized computer processors taking advantage of integer thermodynamics. The materials, architecture and methods for constructing micro- and/or nano-scale three-dimensional cellular arrays, cellular series logic gates, and signature logic form the basis of small- and large-scale apparatuses used to execute logic, data bases, memory, mathematics, artificial intelligence, prime factorization, optical routing and artificial thought tasks not otherwise replicated in electron-based circuits*".

Leur piste consiste à utiliser des nanotubes de carbone pour piéger les électrons utilisés dans des qubits CMOS. Cela permettrait d'améliorer leur isolation et leur temps de cohérence d'un facteur 100 atteignant une seconde. Ils se contrôleraient par couplage spin-photon. Les défis se situent au niveau des matériaux, du design, de l'électronique de contrôle, de la connectivité, de la topologie et des codes de correction d'erreurs. Les nanotubes sont intégrés au circuit mécaniquement à la fin du processus de fabrication. Les nanotubes de carbone proviennent de la société allemande Micromotive. La liaison entre deux qubits s'appuie sur des cavités à micro-ondes, exploitant le principe de la cQED (cavity Quantum Electrodynamic). Il subsiste évidemment de nombreux défis pour mettre au point ce genre de qubits mais la voie mérite d'être explorée.

Duality Quantum Photonics (2020, UK) est une startup basée à Bristol crée en février 2020 et dont l'activité n'est pas documentée en ligne. Son fondateur est Anthony Laing, du Département de Physique de l'Université de Bristol où il développait un simulateur quantique à base de photons en niobiate de lithium.

EeroQ (2017, USA) développe un processeur quantique qui serait plus-mieux que les autres, sans plus de précision autre que cela s'appuie sur des principes connus de la physique. La startup est fondée par Johannes Pollanen de l'Université du Michigan, Nick Farina et Faye Wattleton.

Elle a bénéficié de financements publics US (NSF) et privés. Leur site web n'indique pas grand-chose. La bio de Johannes Pollanen indique qu'il a mené des recherches dans les qubits supraconducteurs et bidimensionnels (silicium, graphène). Ils semblent utiliser un procédé d'immersion des qubits supraconducteurs dans de l'hélium liquide[913].

equal1.labs (2017, USA) développe en collaboration avec l'Université de Dublin un processeur quantique à spins d'électrons fonctionnant à 4K et fabriqués en technologie FD-SOI 22 nm chez Global Foundries.

Ils annoncent avoir développé un chipset de test de 422 qubits. Mais qui reste à tester et à mettre au point !

IonQ (2016, USA, $76M) est une startup issue du laboratoire de Christopher Monroe de l'Université du Maryland qui développe des ordinateurs quantiques à base d'ions piégés.

Ils sont déjà largement évoqués ailleurs dans ce document.

IQM (2018, Finlande, 26,5M€) est une startup qui développait initialement un système de réfrigération de chipsets supraconducteurs ou silicium à base d'envoi d'électrons (vidéo). Cela devait permettre d'agencer un plus grand nombre de qubits dans ce type d'ordinateurs quantiques.

Elle est issue du groupe Quantum Computing and Devices de l'Université d'Aalto et du centre de recherche VTT. Ils ont ouvert un laboratoire de développement en Allemagne en mars 2020.

Ils ont l'air d'être positionnés dans la création de processeurs quantiques hybrides analogiques/digitaux « Co-Design QC » que l'on pourrait caser dans la catégorie des simulateurs quantiques, toujours à partir de qubits supraconducteurs[914].

---

[913] Voir Integrating superfluids with superconducting qubit systems par Johannes Pollanen et al, 2019 (11 pages).

[914] Leur méthode est décrite dans Approximating the Quantum Approximate Optimisation Algorithm par David Headley et al, février 2020 (14 pages) et Improving the Performance of Deep Quantum Optimization Algorithms with Continuous Gate Sets par Nathan Lacroix, Alexandre Blais, Andreas Wallraff et al, mai 2020 (14 pages).

Ils seraient notamment adaptés à l'exécution d'algorithmes hybrides de type VQE (Variational Quantum Eigensolvers) et QAOA (Quantum Approximate Optimisation Algorithm). Ils communiquent sur le fait que leurs qubits sont actionnables plus rapidement avec une vitesse d'horloge plus rapide que les qubits supraconducteurs concurrents. Mais ils ne communiquent rien sur ce qu'ils font exactement et notamment sur le nombre et la qualité des qubits qu'ils réalisent en termes de bruit et de temps de cohérence. Il semblerait qu'ils en seraient à 2 qubits en 2020 et qu'ils visent 5 qubits d'ici 2021.

En juin 2020, ils recevaient un financement en capital de 15M€ de l'accélérateur EIC de la Commission Européenne complété d'un prêt de 2,5M€. Ils annonçaient aussi un partenariat avec Atos concernant l'acquisition d'un émulateur classique aQML de ce dernier pour leurs qubits supraconducteurs. Cette machine sert à la fois à simuler le fonctionnement des qubits de l'accélérateur quantique d'IQM et aussi à piloter ce dernier[915].

Le partenariat implique également le centre de calcul finlandais CSC qui fournit les ressources de calcul scientifique aux chercheurs du pays, un peu comme le fait le GENCI en France. Atos a aussi annoncé s'intéresser, sans exclusive, à la distribution d'un accélérateur quantique IQM.

MDR (2008, Japon, $2,3M), pour Machine learning and Dynamics Research est une énigmatique société japonaise qui ambitionne de créer son propre ordinateur quantique universel et de développer des algorithmes intégrant l'IA et la chimie. En attendant leur ordinateur, ils travaillent avec D-Wave. La startup a été créée par Yuichiro Minato et divers autres anciens de l'Université de Tokyo.

NextGenQ (2019, France) ambitionne de concevoir des ordinateurs quantiques à ions piégés qui seront intégrés dans une offre de « Blind Quantum Computing » permettant de les solliciter via le cloud tout en assurant la confidentialité des traitements et données soumis et sans passer par des liaisons physiquement protégées par de la QKD.

La société crée par Yann Allain à Rennes utilise une technologie de contrôle des qubits par micro-ondes voisine de celle d'AQT en Autriche et qu'il dénomme RF Qubit-ion. L'architecture est inspirée des travaux de l'Allemand Christof Wunderlich de l'Université Siegen et de son protocole Magic (Magnetic Gradient Induced Coupling)[916]. Les marchés visés sont classiques : la finance, la chimie, l'IA et la cybersécurité. Le projet est très ambitieux mais risque de manquer de moyens et de base scientifique solide[917].

Nordic Quantum Computing Group (NQCG) (2004, Norvège) fait de la R&D dans des domaines à la croisée des chemins entre l'IA et l'informatique quantique. Ils sont sur la piste du développement d'un simulateur quantique analogique.

[915] Voir Atos, le CSC et IQM s'associent pour accélérer la commercialisation de technologies quantiques européennes, juin 2020.

[916] Voir Quantum Computing using MAGIC with Trapped Atomic Ions par Christof Wunderlich et al, 2019.

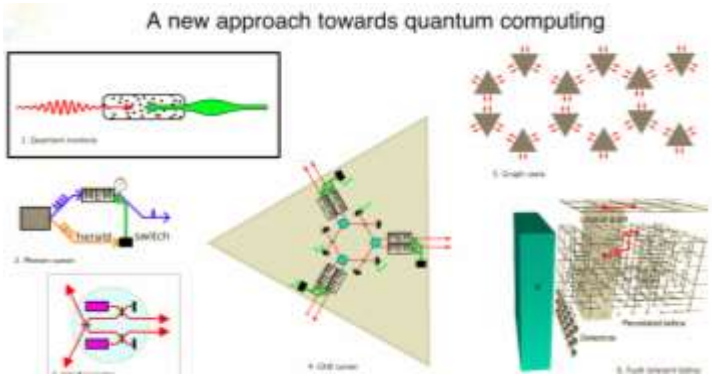
[917] Voir Comme en IA, il faut, peut-être, éviter le piège des "biais" concernant les technologies des ordinateurs quantiques à suivre : votre avis?, par Yann Allain, avril 2019. Voir aussi la conférence de Yann Allain de décembre 2019, Build you own Quantum Computer @ Home - 99% of discount - Hacker Style ! (55 minutes).

ORCA Computing (2019, UK, $3,7M dont une partie en financement public anglais) développe une plateforme de calcul quantique à base de photons et de mémoire photonique[918]. Ça parle de MBQC, une méthode de gestion du calcul quantique qui consiste à démarrer par créer un « cluster state » de qubits intriqués (ici des « GHZ states ») et de lire progressivement les états de qubits pour mener ses calculs progressivement.

Ils utilisent aussi des peignes de fréquences optiques et des variables continues.

La startup a été cofondée par Richard Murray (CEO, ancien responsable du programme quantique du Royaume Uni), Josh Nunn (CTO, ancien de l'Université d'Oxford) et Cristina Escoda (COO), une entrepreneuse avec un background dans la finance et les deep techs[919].

Leur roadmap prévoit de créer 3 qubits d'ici 2024 et des centaines de qubits en 2026.



Ils ont le fonds d'investissement français Quantonation parmi leurs investisseurs.

Oxford Quantum Circuits (2017, UK, $18M) a été lancée par Peter Leek, qui provient du Clarendon Laboratory Oxford. La startup est dirigée par Ilana Wisby. Elle veut produire des qubits supraconducteurs et lever les barrières identifiées qui empêchent ceux-ci de scaler en nombre.

Leur architecture comprendrait des qubits "planar" à grande cohérence avec un contrôle 3D miniaturisé des portes et de la lecture à base de résonateurs[920]. Ils sont associés à Cambridge Quantum Computing (CQC) qui développe un compilateur quantique dédié à leurs qubits. En avril 2020, OQC obtenait un financement de projet collaboratif du gouvernement britannique de £7M. Ils sont associés à SeeQC UK, Oxford Instruments, Kelvin Nanotechnology, l'Université de Glasgow et l'Université Royal Holloway de London. C'est donc un concurrent du Français Alice&Bob aussi bien que du finlandais IQM.

Oxford Ionics (2019, UK) est une spin-off du Département de Physique de l'Université d'Oxford qui développe un ordinateur quantique à base d'ions piégés et d'une électronique de contrôle à faible bruit.

Ils s'appelaient initialement Nqie Limited. La société a été créée par Thomas Harty et Christopher Ballance et comprend aussi Jochen Wolf, tous issus de l'Université d'Oxford.

Pasqal (2019, France) est la première startup de calcul quantique en France basée sur la filière du refroidissement d'atomes. Ils utilisent des atomes de rubidium confinés magnétiquement et refroidis par laser à effet Doppler pour atteindre le mK et avec une variante de l'effet Sisyphe atomique pour descendre à 30 µK[921], sans cryostat.

---

[918] Voir One-Way Quantum Computing in the Optical Frequency Comb, Nicolas C. Menicucci, Steven T. Flammia et Olivier Pfister, avril 2018 (4 pages).

[919] Voir quelques vagues détails sur leur approche dans Photonic quantum processors, Orca Computing, avril 2020 (27 slides).

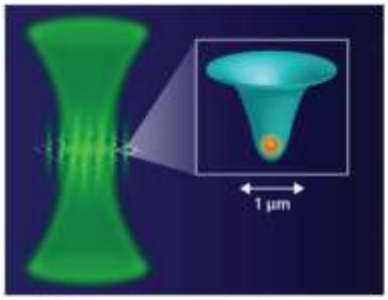
[920] Voir Surface acoustic wave resonators in the quantum regime, 2016 (40 slides).

[921] Cette méthode utilise aussi des lasers émettant des photons polarisés orthogonalement. La méthode a été inventée par Claude Cohen-Tannoudji qui a obtenu pour cela le prix Nobel de physique en 1997.

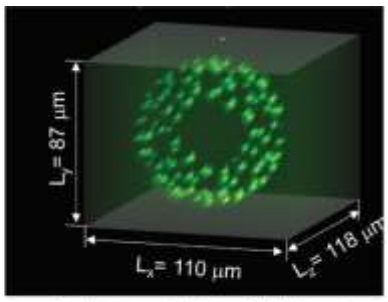
Les atomes sont piégés dans des matrices 2D ou des structures toriques 3D avec un espacement de quelques microns entre chacun d'entre eux. Ils sont gérés avec deux niveaux d'énergie. Les portes quantiques sont activées par laser pour contrôler l'état énergétique des atomes. L'intrication est provoquée par l'excitation des atomes dans l'état de Rydberg qui leur permet d'interagir avec d'autres atomes à longue distance[922].

La technologie permettrait d'atteindre rapidement une cinquantaine de qubits de qualité puis un millier d'ici 2023[923]. Ils arrivent déjà à contrôler une centaine d'atomes en laboratoire. Ils se positionnent dans un premier temps sur les PQS (Programmable Quantum Simulator, ou ordinateurs quantiques analogiques) puis ensuite sur les NISQ (Noisy Intermediate-Scale Quantum), des ordinateurs à portes quantiques universelles.

Côté performance et qualité des qubits, ils atteignent un temps de cohérence de 1 ms avec des portes de 1 µs (pour une CNOT), donc de quoi enquiller un millier de portes quantiques, hors codes de correction d'erreur. Le taux d'erreur des portes serait de 3% et le taux d'erreur de mesure de 1% ce qui est tout à fait raisonnable, tout du moins pour de la simulation quantique.

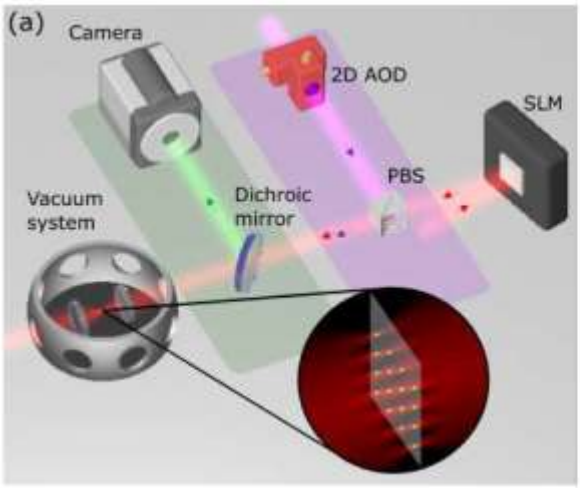


Single atoms are trapped in an energy potential pattern created by lasers



Each green dot is a Rubidium atom arranged within a torus

L'ordinateur tiendra à terme dans un rack de data center et fonctionnera à température ambiante et sous vide. Il s'appuie sur des composants standards et ne nécessite pas la création de chipsets spécifiques comme c'est le cas pour tous les autres types de qubits.



Le système de pilotage des qubits à base d'atomes froids comprend un modulateur spatial de lumière (Spatial Light Modulator, SLM, à base de cristaux liquides de type LCoS[924]) qui contrôle par la phase de la lumière transmise des atomes dans un plan de focale avec des micro-pièges optiques. Des tweezers ou pièges/pinces à laser de réarrangement des atomes sont contrôlés par l'AOD (Acousto-Optic laser beam Deflector) et ajoutés au faisceau issu du SLM par un filtre biréfringent. La lumière fluorescente émise par les atomes lors de la lecture est filtrée par un PBS (filtre séparateur polarisant) et lue par une caméra. Les atomes du système sont confinés dans un espace d'un mm^3.

---

[922] Voir Quantum Computing with Arrays of Atoms par Lucas Béguin et Adrien Signoles de Pasqal, avril 2020 qui détaille bien le fonctionnement des processeurs quantiques de la startup. Et leur livre blanc Quantum Compting with Neutral Atoms, juin 2020 (41 pages). On pourrait leur décerner la palme d'or de la documentation scientifique d'une startup quantique !

[923] Les atomes de Rydberg ont des usages insoupçonnés comme pour gérer de la musique aléatoire. Voir Quantum music to my ears, juin 2019. Cela change de la musique générée par du deep learning !

[924] Voir une description d'un SLM dans Spatial Light Modulators par Aurélie Jullien, 2020 (6 pages).

Ils développent leur propre environnement de programmation à bas niveau qui aura pour vocation à s'interfacer avec des langages de programmation à haut niveau du marché.

C'est un investissement « actif » du fonds Quantonation à savoir que Christophe Jurczak, le *general partner* du fonds, est le chairman de la startup. Alain Aspect en est conseil scientifique. L'équipe comprend trois fondateurs autour du CEO, Georges-Olivier Reymond.

En avril 2020, les startups **Pasqal** et **Muquans** annonçaient un partenariat qui était en gestation de longue date et pourtant sur l'usage de lasers de contrôle des atomes froids des seconds par le premier. A noter que Pasqal supporte le framework Cirq de Google.

En parallèle avec la mise au point des qubits, la startup a développé le support logiciel de plateformes de développement du marché comme **Cirq** et **TensorFlow Quantum** de Google ainsi que **Qiskit** d'IBM. En juillet 2020, c'était au tour de **Cambridge Quantum Computing** (CQC) d'annoncer leur support des qubits de Pasqal avec leur outil de développement t|ket⟩.

Ils développent des modèles de simulation quantique du magnétisme, pour la chimie et la découverte de molécules thérapeutiques ainsi que pour résoudre des problèmes d'optimisation (VQE, MaxCut pour le traitement de problèmes de graphes). Ils annonçaient en juin 2020 un partenariat avec la R&D d'EDF pour tester un algorithme d'optimisation de gestion de réseau pour la recharge de véhicules électriques, à base de QAOA (Quantum Approximate Optimization Algorithm).

Ψ PsiQuantum

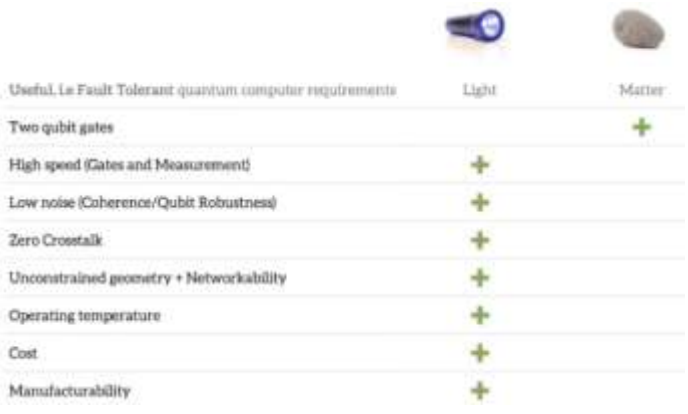
PsiQuantum (2016, USA/Europe, $508,5M) est une startup créé par Jeremy O'Brien, un ancien chercheur de Stanford et de l'Université de Bristol, qui veut créer un processeur quantique à base de photons en technologie silicium CMOS.

Il est accompagné de Pete Shadbolt (co-inventeur de l'algorithme VQE avec Jeremy O'Brien et Alán Aspuru-Guzik), Mark Thompson et Terry Rudolph. Ce dernier est le petit-fils d'Erwin Schrödinger, ce qui paraît-il peut aider lors des levées de fonds !

La société emploie déjà plus de 140 personnes, l'essentiel étant aux USA à Palo Alto mais une partie en remote un peu partout dans le monde, y compris une personne en France.

L'architecture de leur ordinateur quantique s'appuierait sur une variante du MBQC (Measurement Based Quantum Computing), elle-même une variante spécifique des ordinateurs à portes quantiques. Il s'agit d'une technique dénommée « ballistic quantum computing », à base de microclusters[925].

Et la photonique, *c'est mieux*, comme l'indique sans grande nuance le slide ci-dessous, extrait d'une présentation de Terry Rudolph de 2020[926]. Ils se sont donnés comme ambition de produire un processeur d'un million de qubits physiques générant 100 qubits logiques. La fabrication doit se faire dans la fab du Luther Forest Technology Campus de Global Foundries au nord de l'Etat de New York. Avec des cycles de production généralement assez lents de plusieurs mois.



[925] Voir Percolation thresholds for photonic quantum computing par Mihir Pant, 2017 (14 pages). Le processus est aussi documenté dans Towards practical linear optical quantum computing par Mercedes Gimeno-Segovia, 2015 (226 pages). C'est la dernière publication sur le procédé de PsiQuantum qui est depuis silencieux dessus. Ils ont cependant déposé plus de 100 brevets.

[926] Voir How to stop worrying and love the photon, par Terry Rudolph, mai 2020 (webinar 1h).

A ce jour, c'est la startup la mieux financée au monde dans le calcul quantique, même devant D-Wave. Originaire du Royaume-Uni, elle a dû pour ce faire déplacer une partie de son équipe aux USA[927]. Ils ont même Microsoft comme investisseurs ainsi que le fonds d'investissement de Pascal Cagni, C4 Ventures.

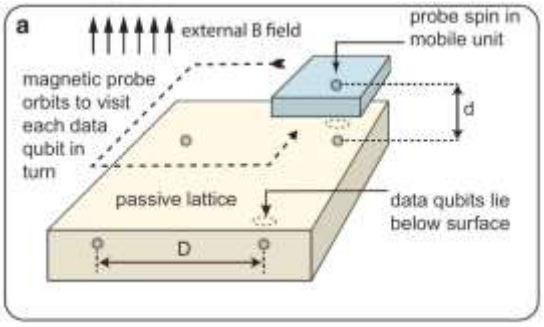
Quantum Brilliance (2019, Australie) développe un processeur quantique à base de NV centers devant opérer à température ambiante. Elle a été créée par des chercheurs de l'ANU (Australian National University), Andrew Horsley (CEO) et Marcus Doherty (CSO).

Ils en sont, comme tous, au développement d'un prototype de quelques qubits. Il est fort probable que cela devienne ensuite une startup de métrologie quantique, un débouché semble-t-il plus prometteur que le calcul quantique à base de NV centers. Le Pawsey Computing Center australien est partenaire de cette société pour y installer un calculateur quantique. Le jour où il sera opérationnel !

Quantum Motion Technologies (2017, UK, $9,7M) est une spin-off de l'Université d'Oxford qui ambitionne de créer une plateforme d'ordinateur quantique silicium permettant de créer des puces avec une grande densité de qubits. Ils ont bénéficié d'un financement d'amorçage non précisé du fonds britannique Parkwalk Advisors en 2017.

La startup cofondée par John Morton et Simon Benjamin souhaite industrialiser un procédé créé par l'équipe de Joe O'Gorman de l'Université d'Oxford consistant à séparer nettement des qubits silicium et à mesurer leur valeur en fin de calcul.

Cette mesure est réalisée avec une sonde magnétique déplacée mécaniquement en surface et faisant des mouvements « carrés » comme décrit dans le schéma suivant. C'est une structure guidée mécaniquement par un MEMS (micro-electro-mechanical device). Les qubits sont espacés de 400 nm (D) tandis que les sondes sont à 40 nm des qubits (d). Le tout est complété par un système de « surface code » associant plusieurs qubits physiques pour créer des qubits logiques.



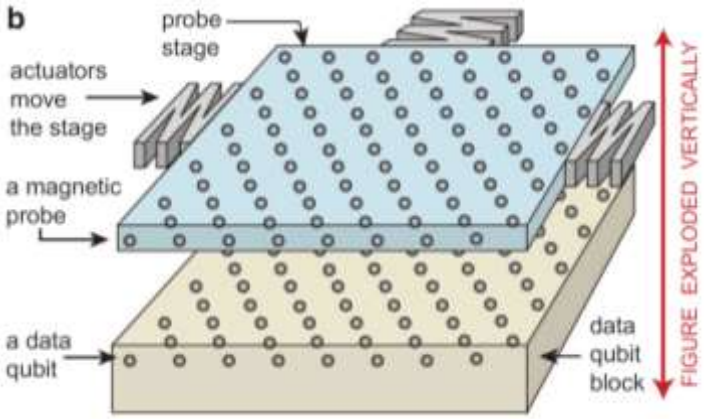


Figure 1. (a) The principle of the orbital probe parity measurement: a probe spin comes into proximity with four data qubits in turn during one cycle. (b) Simplified schematic of a scalable device showing that the probe layer and the data qubit layer both contain extended spin arrays (details of the their relative positions are shown in Figure 3). We depict the probe stage as mobile, whereas the data qubit stage is static, but in fact either may move; it is their relative motion that is key.

Ce système de sondes évite l'usage d'électronique de commande prenant de la place dans le circuit CMOS[928] et permet une meilleure séparation entre les qubits.

---

[927] Voir la présentation Measurement-based fault tolerance beyond foliation par Naomi Nickerson de PsiQuantum en septembre 2019 ainsi que Quantum Computing With Particles Of Light: A $215 Million Gamble, par Paul Smith-Goodson, avril 2020.

[928] Voir A silicon-based surface code quantum computer de Joe O'Gorman et al, 2015 (14 pages). Le papier est cosigné par John Motin et Simon Benjamin qui sont deux cofondateurs de la startup Quantum Motion Technologies.

Ils utilisent aussi un procédé de séparation des qubits de données avec des dots de médiation intermédiaires, limitant les effets de fuite[929]. Ce procédé est protégé par un brevet US validé et quatre brevets en cours de dépôt. Mais il semble que cette technologie ne soit finalement pas celle qu'ils ont retenue !

Leur roadmap consiste d'ici 2022 à produire des « small cells » de 5 qubits dans une structure qui pourrait alors être reproduite dans une matrice. Ils pensent ensuite pouvoir aboutir à la création d'un ordinateur quantique avec 100 qubits logiques d'ici 2029. C'est évidemment assez optimiste car la mise au point de ces qubits est complexe, notamment au niveau de leur intrication et de la maitrise du bruit pour limiter les taux d'erreurs.

Et la fabrication des composants ? Ils prévoient de la réaliser dans des fonderies classiques, notamment celle du laboratoire IMEC en Belgique qui est un peu l'analogue du CEA-Leti.

Ils n'ont pas encore décidé s'ils allaient jusqu'au bout de la création d'un ordinateur quantique. Ils sont une dizaine de personnes dans la startup et levaient £8M en mai 2020.

QCI (2015, USA, $18M) ou Quantum Circuits Inc est une spin-off de l'Université de Yale cofondée par Rob Schoelkopf, Luigi Frunzio et le français Michel Devoret (qui les a quittés en 2019 en raison de désaccords avec les autres fondateurs, un scénario classique des startups en tout genre).

Ils veulent créer des qubits supraconducteurs avec l'objectif, plus que courant dans le domaine, de résoudre les problèmes de bruit et de cohérence de cette technologie. Leur technologie est à base de qubits supraconducteurs transmon.

Leur originalité se situerait dans la méthode de gestion des corrections d'erreurs des qubits réduisant le besoin de redondances en nombre de qubits. Leur communication parle d'ordinateurs génériques faciles à reconfigurer selon les besoins.

Ce qui semble être une caractéristique commune des ordinateurs quantiques universels. Ils sont aussi à l'origine du framework **qbsolv**[930] qui fait partie de leur middleware et plateforme de développement **Mukai** lancé en janvier 2020. Il a l'air de supporter pour l'instant sur les ordinateurs à recuit quantique de D-Wave ainsi que les ordinateurs à recuit digital de Fujitsu et aussi les qubits supraconducteurs de Rigetti.

QuEra Computing (USA, 2020) développe un ordinateur quantique à base d'atomes froids. C'est un concurrent direct de la startup française Pasqal. La startup a été créée par des chercheurs de l'Université de Harvard et du MIT, qui sont toutes proches.

Avec notamment Nathan Gemelke, Alexei Bylinskii, Shengtao Wang ainsi que Mikhail D. Lukin qui est l'un de leurs conseillers scientifiques[931].

Quantum Factory (2018, Allemagne) veut commercialiser des ordinateurs quantiques à base d'ions piégés sous la forme de ressources dans le cloud.

---

[929] Voir A Silicon Surface Code Architecture Resilient Against Leakage Errors de Zhenyu Cai (Quantum Motion Technologies) et al, avril 2018 (19 pages).

[930] Voir QCI Qbsolv Delivers Strong Classical Performance for Quantum-Ready Formulation par Michael Booth et al, mai 2020 (7 pages).

[931] Voir notamment Parallel Implementation of High-Fidelity Multiqubit Gates with Neutral Atoms par Harry Levine et al, août 2019 (16 pages).

Quix Photonics (2019, Pays-Bas) développe un processeur quantique photonique utilisant des nitrures de silicium (SiN^4) comme guides d'ondes. C'est un projet issu de l'Université de Twente et du laboratoire AMOLF d'Amsterdam. La société est une filiale de la fab Lionix.

Silicon Quantum Computing ou **SQC** (2017, Australie, $66M) est une spinoff de l'University of New South Wales (UNSW) et de son laboratoire Centre of Excellence for Quantum Computation and Communication Technology (CQC2T).

Ils planchent sur une technologie CMOS proche de celle du CEA-Leti de Grenoble. A court terme, ils veulent sortir un circuit de 10 qubits d'ici 2022. La société a été créée par Michelle Simmons, une des rares femmes de l'écosystème entrepreneurial du quantique.

La société recrutait John Martinis, ex-Google- fin septembre 2020. On peut donc qualifier John de « transfuge » des qubits supraconducteurs. C'est une évolution plus que rare : voir un spécialiste d'un type de qubit tourner casaque pour s'attaquer à un autre type de qubit. Même si, au demeurant, il existe quelques points communs entre les qubits supraconducteurs et les qubits silicium. Le changement pour John Martinis n'est pas anodin puisqu'il va au passage déménager de Santa Barbara en Californie à Sydney en Australie. Deux lieux ayant en commun le Soleil et un beau cadre de vie !

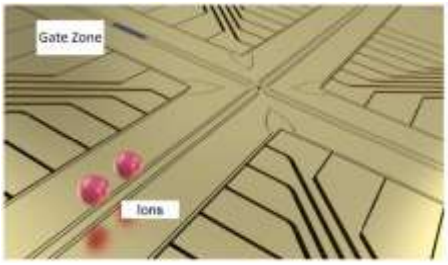
TundraSystems (2014, UK) développe un processeur quantique en optique linéaire fonctionnant à température ambiante. Difficile de savoir où ils en sont exactement. Ils ont l'air de vouloir créer un microprocesseur en photonique, et pas forcément, un ordinateur quantique avec des qubits utilisant l'optique linéaire.

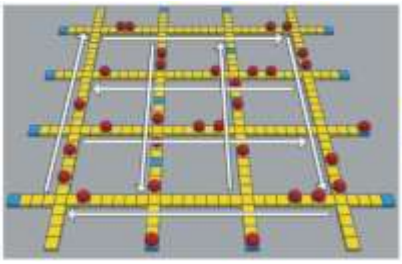
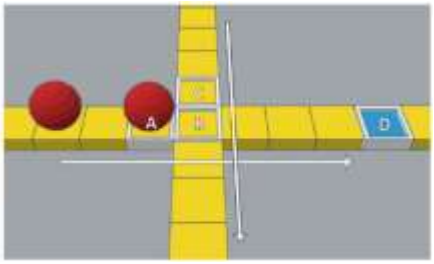
Leur Advisory Board comprend deux scientifiques chinois, Xinliang Zhang et Pochi Yeh qui sont spécialisés en optronique (site).

Turing Inc (2016, USA) est une startup qui ambitionne comme Rigetti de créer une offre matérielle et logicielle d'ordinateur quantique, à base de qubits utilisant des cavités de diamants (NV Centers) et fonctionnant à 4K, une température certes basse, mais gérable avec une cryogénie plus simple, à base d'hélium 4^{932}.

Ils développent aussi des systèmes de correction d'erreurs qu'ils commercialisent auprès d'autres spécialistes du secteur. Une manière de ne pas mettre tous ses œufs dans le même panier !

Universal Quantum (2018, UK, $4,5M) est une spin-off du Ion Quantum Technology Group de l'University of Sussex au Royaume-Uni dirigée par Winfried Hensinger. Ils développent un ordinateur quantique à ions piégés exploitant des micro-ondes transmises par des circuits électriques, et des champs magnétiques pour leur contrôle en lieu et place des encombrants et complexes lasers.



[932] Voir Turing Inc: Large Scale Universal Machines, 2017, qui détaille un peu cela.

Ils utilisent en fait des pièges de Penning qui sont bien connus. La vidéo qui présente la société donne l'impression qu'ils utilisent un procédé 2D voisin de celui d'Honeywell avec des ions qui peuvent se déplacer horizontalement sur des circuits contrôlés par des séries d'électrodes[933]. Le refroidissement nécessaire est de l'ordre de 70K, qui se contente d'azote liquide.

Ils sont tout de même besoin d'employer des lasers au moins pour le refroidissement par effet Doppler les ions pour leur préparation, puis pour la lecture de l'état des qubits qui combine une excitation laser et une lecture de la fluorescence générée avec un capteur CMOS ou CCD[934].

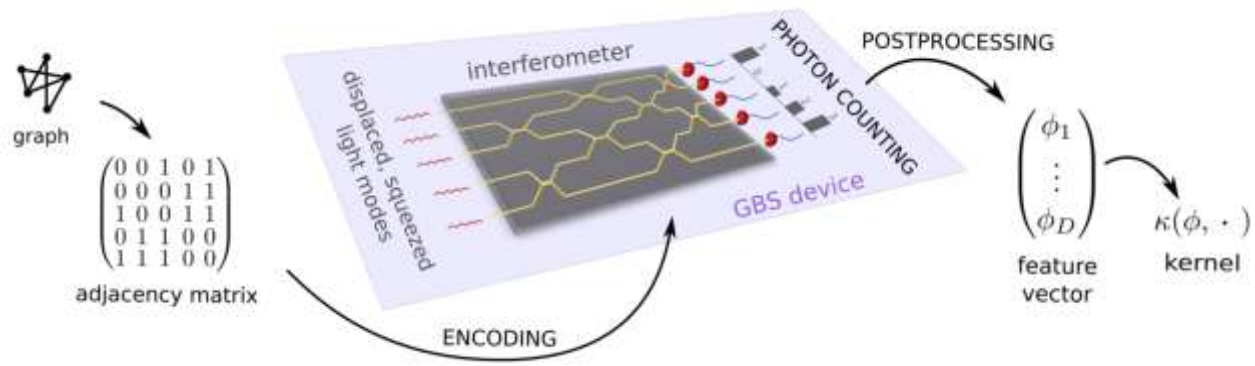
Xanadu (2016, Canada, $35,6M) est une startup créée par Christian Weedbrook, un chercheur prolifique passé entre autres par le MIT et l'Université de Toronto. La startup développe un ordinateur quantique à base de qubits photons qui doit fonctionner théoriquement à température ambiante.

C'est comme d'habitude une affirmation un peu exagérée car les générateurs et détecteurs de photons de ce genre de machine sont toujours cryogénisés. Le tout tient dans quelques racks.

Xanadu développe la plateforme logicielle qui va avec, dénommée Strawberry Fields et créée sans surprise en Python[935]. La plateforme comprend le langage Blackbird. Ils visent notamment le marché de la chimie, la théorie des graphes et le machine learning quantique. Tout cela est proposé en open source.

En septembre 2020, ils annonçaient mettre à disposition des développeurs une plateforme de tests en cloud de 8 et 12 qubits, devant évoluer jusqu'à 24 qubits. Mais sans préciser les caractéristiques précises des qubits utilisables, notamment en termes de fidélité. Leurs qubits sont des qumodes qui s'appuient sur des « squeezed states » utilisant un encodage de type "Continuous Variable"[936].

Leur principal domaine d'application est l'analyse de similarités entre graphes pour identifier ceux qui se ressemblent et/ou les séparer en plusieurs classes de similarité. Les méthodes classiques de résolution de ce genre de problème sont similaires au calcul d'un déterminant de matrices et non satisfaisantes[937].



[933] Le procédé de routage des ions est décrit dans Efficient Qubit Routing for a Globally Connected Trapped Ion Quantum Computer par Winfried Hensinger et al, février 2020 (13 pages). C'est l'origine de l'illustration utilisée dans ces lignes.

[934] Le procédé de contrôle des ions avec des pièges de Penning employé par Universal Quantum a l'air d'être décrit dans Microfabricated Ion Traps par Winfried Hensinger et al, 2011 (28 pages).

[935] Elle est documentée dans Strawberry Fields: A Software Platform for Photonic Quantum Computing, 2018 (25 pages).

[936] Leur procédé a l'air bien documenté dans The power of one qumode for quantum computation, 2016 (10 pages) avec un exemple de mise en œuvre dans Continuous-variable gate decomposition for the Bose-Hubbard model, 2018 (9 pages). Voir aussi Optical hybrid approaches to quantum information par Peter van Loock, 2010 (35 pages).

[937] Voir Measuring the similarity of graphs with a Gaussian Boson Sampler par Maria Schuld et al, 2019 (11 pages).

Logiciels et outils

Les startups de logiciels et d'outils de développement quantiques ne sont pas encore très nombreuses. Une bonne part d'entre elle travaille autour de D-Wave qui est le seul fournisseur d'ordinateurs quantiques commerciaux, même si ceux-ci ne sont pas des ordinateurs quantiques universels. Elles sont d'ailleurs souvent canadiennes, comme D-Wave.

D'autres adoptent des démarches logicielles hybrides associant une connaissance métier, les algorithmes associés et leur exécution sur des machines classiques et sur ordinateurs quantiques, des algorithmes hybrides classiques-quantiques ou encore des algorithmes dits « quantum inspired » qui fonctionnent sur ordinateurs classiques. Ces démarches sont indispensables pour pouvoir survivre. En effet, une startup ne peut pas être exclusivement dédiée au calcul quantique au risque de ne pouvoir vendre que des preuves de concepts à toute petite échelle qui ne peuvent généralement pas être déployés industriellement[938].

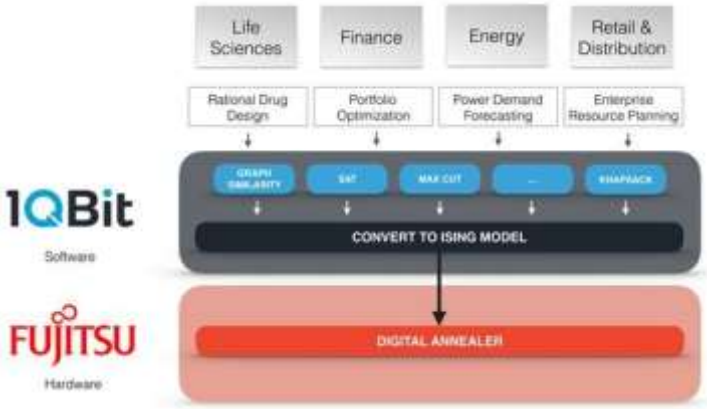
Il y a de véritables opportunités à se positionner sur ce marché naissant ! Vous remarquerez que cet inventaire ne comprend pas de startup chinoise. Ce n'est probablement pas par hasard. Cet écosystème est donc encore très jeune. Il évoluera en parallèle avec la mise au point d'ordinateurs quantiques commerciaux. La Chine n'est pas très versée dans le logiciel comparativement au matériel et elle semble avoir mis la priorité quantique sur la cybersécurité plus que sur le calcul quantique.

1QBit (2012, Canada, $35M) est un éditeur de logiciels quantiques multi-sectoriel. La société a été notamment financée par Fujitsu avec qui ils sont partenaires, ainsi qu'auprès d'Accenture et d'Allianz.

Ils sont comme il se doit également partenaires de D-Wave qui les met bien en avant dans son marketing. Ils ont développé des briques algorithmiques quantiques diverses de bas niveau qui sont indépendantes des architectures matérielles cibles. Cela comprend par exemple le traitement de graphes qu'ils appliquent dans un grand nombre de marché, via une activité de consulting.

[938] Ce principe de réalité est bien décrit dans The hard sell of quantum software par Jon Cartwright, 2019.

Ils couvrent notamment les marchés financiers, pour l'optimisation dynamique de portefeuille d'investissement[939] ou pour simplifier l'allocation de classes d'actifs dans un portefeuille. En plus d'être un partenaire historique de D-Wave, ils le sont aussi avec IBM. La startup a déjà une centaine de collaborateurs. Ils ont aussi comme clients Dow Chemical (chimie), Biogen (biotechs) et Allianz. Ils lançaient en avril 2020 le « Quantum Insights Network" un réseau d'une centaine d'experts et de contenus en calcul quantique.



1QBit Software running on Fujitsu Hardware – Source: Fujitsu

Adaptive Finance Technologies (2020, Canada) est une startup passé par le Creative Destruction Lab créée par Roman Lutsiv, Vlad Anisimov et Edward Tang qui développe des logiciels dans la finance pour l'investissement et la gestion du risque de crédit.

Ils s'appuient sur des méthodes classique et sur du quantum machine learning tournant sur des calculateurs D-Wave.

AIQTECH Inc (2018, Canada**)** est un spécialiste du machine learning qui explore les usages de la QML. Ils sont partenaires d'IBM Q Network.

Aliro Quantum (2018, USA, $2,7M) est une startup sortie du bois en septembre 2019 qui développe des briques logicielles permettant d'indiquer aux développeurs si des ressources cloud de calcul quantique sont disponibles pour réaliser des calculs plus rapidement que sur des processeurs traditionnels, notamment de type GPU.

La startup a été créée par Prineha Narang et Jim Ricotta. Bref, une sorte de « quantum cloud resources provisioning », qui se veut évidemment neutre du point de vue des technologies d'ordinateurs quantiques utilisées. Mais ce genre d'outil devrait être relié aux technologies de compilateurs qui savent tirer parti des caractéristiques spécifiques de chaque type d'ordinateur quantique.

ApexQubit (2018, Biélorussie) développe des solutions logicielles quantiques pour le secteur de la finance. Ils fonctionnent en mode projet.

A*Quantum (2018, Japon) est spécialisé dans le développement de solutions logicielles quantiques pour les ordinateurs à recuit quantique comme à ceux qui utilisent des portes quantiques universelles. Leur ambition est de créer des briques logicielles de haut niveau destinées à des utilisateurs.

[939] Voir Solving the Optimal Trading Trajectory Problem Using a Quantum Annealer, 2015 (13 pages).

Ankh.1 (2018, USA) a développé Anubis Cloud, une machine virtuelle dans le cloud pour les data scientists s'intégrant avec la solution open source Jupyter ainsi qu'avec les frameworks de machine learning Tensorflow et Keras.

AppliedQubit (2019, UK) se présente comme un éditeur de logiciels quantiques pour les entreprises.

Ils ciblent notamment les deux principaux marchés du moment : la finance et la simulation chimique en plus de problèmes génériques d'optimisation et d'analyses prédictives. Ils développent à la fois des solutions de calcul hybrides classique/quantique et de quantum machine learning.

Artiste-qb.net (2018, Canada) a un modèle d'activité voisin de celui de 1Qbit : ils développent des briques algorithmiques de niveaux intermédiaires qu'ils assemblent ensuite au gré des besoins de leurs clients.

Ils ont même déposé des brevets pour certaines méthodes. La startup a été créée par une équipe internationale comprenant notamment des chercheurs allemands.

Automatski (2014, USA) est une société de services établie d'abord à Londres, puis en Inde à Bengalore et récemment en Californie. Ils font de la recherche appliquée sous contrat de développement d'algorithmes quantiques sur toute forme d'ordinateur et de simulateur quantique. Ils ont notamment développé une solution logicielle permettant de simuler un grand nombre, non précisé, de qubits sur ordinateur classique. Ils développent des algorithmes en biochimie. Sur la forme, cette société est curieuse.

C'est une holding de sociétés de recherche qui tire dans tous les sens : informatique quantique, intelligence artificielle générale, robotique, blockchain, voyage spatial, guérison du cancer, etc, le tout associé à une mystique indienne[940].

Avanetix (2019, Allemagne) développe des algorithmes hybrides dédiés à la résolution de problèmes de *supply chain*. Ils associent des méthodes d'optimisation classiques, du machine learning et du calcul quantique.

Ils visent les marchés de l'automobile et de la logistique. L'avantage d'une approche hybride est que dans un premier temps, elle peut se contenter de méthodes classiques, tant que le calcul quantique n'est pas assez puissant pour y jouer un rôle. La startup est fondée et dirigée par la serial-entrepreneuse Naimah Schütter.

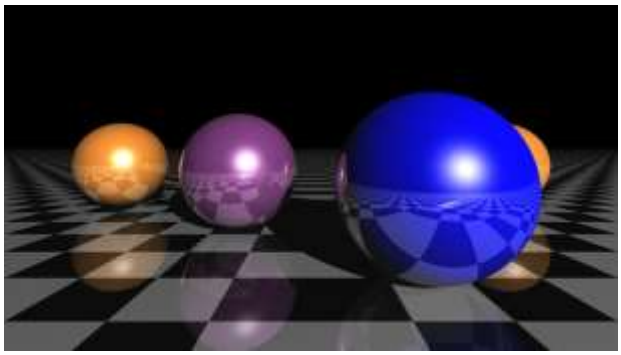
Beit.tech (2016, Pologne) est spécialisé dans le quantum machine learning. C'est surtout un projet de recherche financé par l'Union Européenne, couvrant la période 2017-2010. Le créateur Wojtek Burkot est un ancien de Google qui cherche même à rendre les D-Wave inutiles en créant des algorithmes d'optimisation de graphes complexes pouvant tourner sur ordinateurs traditionnels.

---

[940] Voici ce qu'indique leur site web : « *One of the earliest breakthroughs at Automatski Fundamental Research has been to (i) discover the working of the Human Mind and Brain, Consciousness and Soul, and explain Heaven, Hell, Rebirth, Consciousness etc. in a purely scientific non-religious or non-philosophical manner. And also (ii) to explain the Begining, Evolution and End of the Universe also explaining everything like Blackholes, Worm Holes, Space-Time, The Creation of Time, Particle-Wave Duality, Matter-Antimatter, Dark Matter, Dark Energy etc. without any contradictions in a single theory. In the next phases of Research, Automatski Fundamental Research made breathroughs in Science and Technology. From Robotics, to Artificial General Intelligence, NP Complete Problem Solutions, Quantum Computing and Quantum Simulations, Environment, Finance, Drug Research, Machine Learning, Operations Research, Chip Design, Computing, Mathematics, Algorithms, Automatic Theorem Proving, Drug Research, Space Travel etc. Our Mission is to Solve The Toughest Problems Facing Humanity and to Democratize and Guarantee the Health, Prosperity and the Survival of the Human Race.*".

Black Brane Systems (2016, Canada) est une startup focalisée dans le développement de solutions de machine learning quantiques. Ils sont très "stealth" à ce stade.

Boxcat (2017, Canada) développe des solutions de traitement de l'image et de vidéo à partir d'algorithmes quantiques. Ils visent les marchés des médias et de l'imagerie médicale. Leurs algorithmes sont hybrides et s'appuient sur les architectures matérielles disponibles du moment (D-Wave, IBM, Rigetti). La prouesse qu'ils présentent sur leur site est une image réalisée sur un D-Wave, qui aurait pu l'être avec les derniers GPU de Nvidia.



Cambridge Quantum Computing Limited (2015, UK, $50M) développe le système d'exploitation quantique **ti|ket>**[941] et divers algorithmes quantiques dont Arrow dans le machine learning. Ils sont comme nous l'avons vu plus haut partenaires d'**Oxford Quantum Circuits** qui travaille sur la partie hardware.

Et aussi d'IBM qui est un de leurs investisseurs depuis 2020. CQC est aussi actif dans la cryptographie post-quantique. En avril 2020, ils lançaient la version 0.5 de leur plateforme t|ket⟩ qui ajoutait le support d'Honeywell et de l'émulation via Q# de Microsoft. Ils ont notamment Total comme client.

ClassiQ (2020, Israël, $4M) est une jeune startup qui développe un outil de programmation quantique apportant un plus haut niveau d'abstraction que la programmation par portes quantiques classiques.

Tous les outils améliorant le niveau d'abstraction de la programmation quantique que j'ai pu découvrir continuent d'utiliser des portes quantiques, dont on attend de pouvoir juger sur pièces. La startup a été créée par Nir Minerbi (CEO), Amir Naveh (VP-R&D) et Yehuda Naveh (CTO, qui a passé 20 ans chez IBM Research à Haïfa, y compris dans le quantique, spécialiste de la matière condensée).

CogniFrame (2016, USA) est un éditeur de logiciel de plateforme d'analyse de données exploitant le machine learning. Ils développent aussi des algorithmes hybrides pour le secteur financier en s'appuyant sur les ordinateurs de D-Wave.

L'un de leurs premiers clients est la banque d'investissement américaine Alterna Savings. Les applications proposées sont classiques dans le domaine financier : évaluation de risque de crédit et optimisation de portefeuille d'investissements. Par contre, il est difficile d'identifier sur quels matériels ils s'appuient côté calcul quantique.

[941] Voir t|ket> : A Retargetable Compiler for NISQ Devices, avril 2020 (43 pages).

dividiti (2014, UK) développe des algorithmes quantiques notamment dans le machine learning et des méthodes hybrides. Leurs solutions sont open source. C'est donc un modèle de services, qui est plutôt la norme dans ce marché pour l'instant.

D Slit Technologies (2018, Japon) développe des solutions logicielles quantiques sur mesure pour créer des preuves de concept. Leur site web n'est pas très bavard sur leurs réalisations.

Elyah (2018, Japon/Dubaï) est une société qui développe des logiciels quantiques destinés "*à améliorer la vie des gens*". La société est constituée de deux personnes dont un certain Salman Al Jimeely basé à Dubai et une Américaine, Sydney Andrew, basée à Tokyo.

Entropica Labs (2018, Singapour, $1,8M[942]) est une startup dédiée à la création d'algorithmes quantiques (et non quantiques) pour les sciences du vivant et en particulier pour faire de la génomique, à base de quantum machine learning.

Avec à la clé, le développement plus rapide de thérapies, en partenariat avec les entreprises de pharmacie. La société a été créée par Tommaso Demarie, Ewan Munro, rejoint en 2018 par Joaquin Keller, un ancien chercheur d'Orange basé en France. Elle propose son Entropy Development Framework qui gère le workflow de logiciels quantiques.

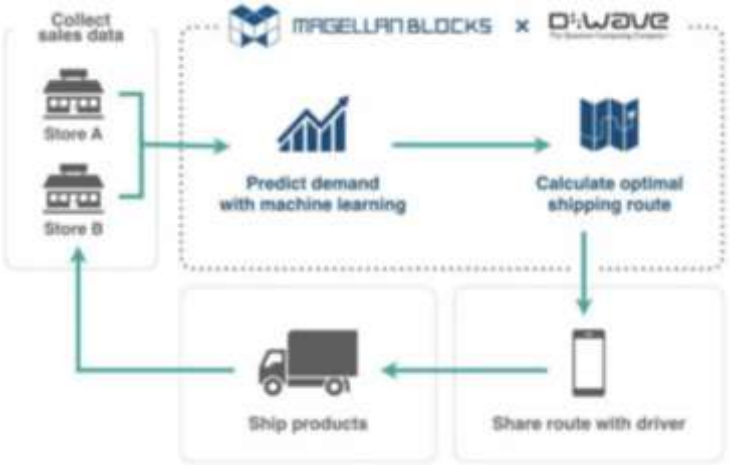
Everettian Technologies (2017, Canada) est une autre startup logicielle focalisée sur les usages du quantique dans le machine learning.

Grid (2009, Japon) est un spécialiste du deep learning et de l'apprentissage par renforcement avec leur plateforme ReNom.

Ils ont décliné cette bibliothèque avec une version quantique dénommée ReNomQ. Et ils sont partenaires d'IBM Q depuis septembre 2019. Par contre, leur IA ne leur a pas servi à trouver un nom facilement trouvable dans les moteurs de recherche.

Groovenauts (2012, Japon, $4,5M) a développé en 2016 un service en cloud dénommé Magellan Blocks qui sert à résoudre des problèmes d'optimisation complexes.

Ils exploitent des algorithmes hybrides associant du machine learning et des algorithmes quantiques. Ils s'appuient sur les ressources en cloud de D-Wave.



[942] Voir Singapore quantum computing startup Entropica Labs bags $1.8m in seed funding par Miguel Cordon, mai 2020.

Leurs premiers clients comprennent un retailer japonais qui optimise sa planification et Mitsubishi Estate qui optimise la collecte des déchets ménagers[943].

GTN Limited (2017, UK, $2,7M) développe un "Generative Tensorial Networks" pour faire du QML (quantum machine learning) afin de simuler, filtrer et faire des recherches de nouveaux traitements thérapeutiques.

Horizon Quantum Computing (2018, Singapour, $3,23m) créé des outils de développement quantiques[944]. Ils ambitionnent de compiler du code issu d'outils de développement classiques comme Matlab pour l'exécuter ensuite sur calculateurs quantiques, histoire de rendre le calcul quantique accessible à des développeurs traditionnels.

Bref, ils visent la démocratisation la plus large qui soit du développement de logiciels pour calculateurs quantiques. La startup a été lancée par Joe Fitzsimons et Si-Hui Tan, tous les deux passés par le centre de recherche CQT de Singapour lancé en 2007 et dirigé jusqu'en 2020 par Artur Ekert. Ils étaient environ une dizaine en avril 2020.

HQS Quantum Simulations (2018, Allemagne, 2,3M€) est une startup de Karlsruhe pilotée par Michael Marthaler qui développe des algorithmes quantiques dans le domaine de la simulation moléculaire organique et inorganique de molécules simples (méthane, émission de lumière dans des OLED, diffusion de molécules dans des liquides).

Ils ont annoncé en juillet 2018 un outil de portage open source de code ProjectQ (plateforme IBM) vers Cirq (plateforme Google). Ils ont déjà BASF et Bosch comme clients. Ils s'appelaient avant Heisenberg. En pratique, ils développent aussi des versions classiques de leurs algorithmes, tournant sur des datacenters ou supercalculateurs[945].

Innovatus Q (2018, Singapour) est une spin-off du Centre for Quantum Technologies de Singapour. Ils travaillent des des algorithmes quantiques hybrides à base d'ions piégés et de supraconducteurs.

Jij (2018, Japon, $1,9M) créé par des chercheurs du Tokyo Tech Institute of Technology développe des logiciels pour recuit quantique et notamment OpenJij, un framework open source pour l'implémentation de modèles d'Ising de modélisation d'interactions entre particules, construit sur les API QUBO de D-Wave. Ils sont notamment partenaires de Microsoft Azure.

JoS Quantum (2018, Allemagne) développe des solutions logicielles quantiques destinées aux services financiers et notamment dans la gestion de risques et la détection de fraudes. Ils font aussi de la recherche sous contrat.

Ketita Labs (2018, Estonie) développe des logiciels quantiques non précisés pour des ordinateurs NISQ, et pour cause, puisqu'il n'y a que cela à se mettre sous la dent. C'est une spin-off d'université.

---

[943] Voir Groovenauts and D-Wave collaborate on hybrid Quantum Computing, décembre 2019.

[944] Voir la présentation QSI Seminar: Dr Joe Fitzsimons, Horizon Quantum Computing, Abstracting Quantum Computation, avril 2020 (1h26).

[945] Voir HQS Quantum Simulations: How to survive a Quantum winter, par Richard Wordsworth, 2020.

Kuano (2020, UK) développe des solutions logicielles quantiques pour la conception de molécules et notamment pour l'inhibition d'enzymes qui sert aussi bien en pharmacie que pour créer des agents protecteurs dans l'agriculture.

Ils utilisent de l'émulation quantique et des algorithmes quantiques ainsi que du machine learning. La société a été créée par des transfuges de GTN, notamment leur CEO Vid Stojevic qui était le CTO de GTN.

Menten.ai (2018, Canada) développe des algorithmes hybrides associant machine learning et programmation quantique pour simuler la chimie organique et concevoir des enzymes, des peptides et des protéines.

Multiverse Computing (2017, Espagne) développe des logiciels quantiques et inspirés par le quantique pour la finance, avec de l'optimisation de portefeuilles, de l'analyse de risques et de la simulation de marchés. Ils annoncent être partenaires de Xanadu, Microsoft, Fujitsu, IBM, Rigetti, DWave et NTT. Ils sont l'une des rares startups internationales à avoir participé au Creative Destruction Lab de Toronto.

Ils utilisent aussi des techniques plus traditionnelles à base de machine learning et de recuit numérique (avec Fujitsu). Ils veulent commercialiser leurs solutions en mode SaaS.

NetraMark (2015, Canada) développe des solutions logicielles quantiques pour les industries pharmaceutiques pour définir des cibles thérapeutiques. Ils sont issus du programme Quantum Machine Learning du Creative Destruction Lab de Toronto.

Nord Quantique (2019, Canada) est une startup issue de l'Institut Quantique de l'Université de Sherbrooke au Québec qui travaille sur du calcul quantique, sans plus de précision à ce stade.

ODE L3C (2018, USA) est une ONG américaine qui s'investit dans la création d'algorithmes de simulation chimique. Elle ambitionne de résoudre des problèmes « NP difficiles » avec du calcul quantique, ce qui est loin d'être évident.

Cela ressemble plus à un prestataire de services qu'à un éditeur de logiciels. La société a été créée par une certaine Keeper Layne Sharkey.

Origin Quantum Computing (2017, Chine) est une startup basée à Hefei en Chine qui semble développer des algorithmes quantiques. Ils sont notamment à l'origine de l'un des records de simulation d'algorithme quantique de 64 qubits sur un supercalculateur[946].

Ils indiquent aussi développer leurs propres chipsets quantiques dont une version supraconductrice de 6 qubits (KF C6-130). Ils ont développé l'OriginQ Quantum AIO, un système de contrôle d'ordinateur quantique ainsi que le langage QRunes, l'architecture QPanda intégrant langage et compilateur et la machine virtuelle EmuWare. Côté applicative, ils ont notamment investi dans la simulation chimique. Ils font de tout et doivent légèrement survendre l'ensemble !

[946] Voir Researchers successfully simulate a 64-qubit circuit, juin 2018.

Opacity (2020, Australie) propose Quiver, un logiciel d'optimisation de code quantique compatible avec Qiskit d'IBM.

Il cartographie de manière analogique les erreurs du processeur à l'échelle globale et individuelle de chaque qubit, y compris les interactions parasites entre qubits. La solution est hardware-agnostique. Cela permet ensuite d'optimiser le code pour tenir compte de ce bruit dument cartographié. L'outil semble aussi bien dédié aux développeurs qu'aux concepteurs de calculateurs quantiques.

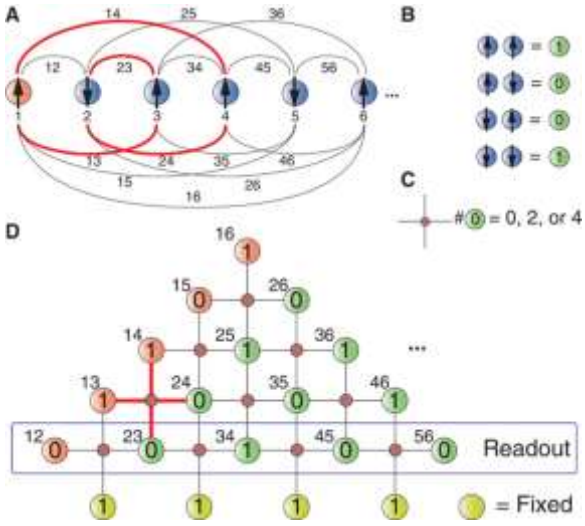
OTI Lumionics (2011, Canada, $5,7M) est une société spécialisée dans la conception de nouveaux matériaux et en particulier des LED et OLED. Ils ont développé des algorithmes quantiques et « inspirés par le quantique » de simulation moléculaire destinés à cet effet.

Cela leur permet notamment de prédire les propriétés des matériaux créés, de modéliser des relations chimiques et de déterminer des structures géométriques. Ils sont partenaires de Microsoft Azure (vidéo).

ParityQC (2020, Autriche) est une autre spin-off de l'Université d'Innsbruck crée par Wolfgang Lechner et Magdalena Hauser[947], le premier étant le scientifique et la seconde, à l'origine investisseuse dans le projet.

En août 2020, la société avait déjà une douzaine de collaborateurs. Ils développent des solutions logicielles de résolution de problèmes d'optimisation (QAOA, problèmes à N-corps, problèmes à contraintes) adaptées aux ordinateurs quantiques numériques et analogiques (qubits à portes universelles ou simulateurs quantiques).

Leur suite logicielle ParityOS optimise les paramètres logiciels de la solution ainsi que ceux du pilotage du matériel. Ils supportent une architecture dénommée LHZ, crée par Wolgang Lechner et des collègues autrichiens Philipp Hauke et Peter Zoller, qui est compatible avec les différentes plateformes quantiques matérielles dotées d'architectures 2D de connectivité entre qubits[948]. Son principe consiste à encoder un problème nécessitant des relations n-to-n entre qubits (tous à tous) pour l'exécuter sur une architecture physique où les qubits ne sont reliés qu'à leurs proches voisins comme c'est le cas dans la plupart des calculateurs quantiques, à l'exception de certains qui s'appuient sur des ions piégés.



Leur solution comprend aussi un système de corrections d'erreur maison[949].

[947] C'est la fille de Hermann Hauser, le cofondateur d'Arm devenu serial entrepreneur et investisseur dans les deep techs, dont Graphcore (UK).

[948] Cette architecture LHZ est documentée dans A quantum annealing architecture with all-to-all connectivity from local interactions par Wolfgang Lechner, Philipp Hauke et Peter Zoller, octobre 2015 (5 pages) pour les plateformes de qubits à portes universelles (source du schéma) et dans Rapid counter-diabatic sweeps in lattice gauge adiabatic quantum computing par Andreas Hartmann et Wolfgang Lechner, septembre 2019 (11 pages) pour le calcul à recuit quantique. Voir aussi Quantum Approximate Optimization with Parallelizable Gates par Wolfgang Lechner, 2018 (5 pages) qui décrit la mise en œuvre d'un algorithme d'optimisation QAOA avec des portes CNOT et à un qubit. A noter que leur architecture n'est pas adaptée aux calculateurs de D-Wave. Elle l'est par contre pour les simulateurs quantiques 2D comme ceux de Pasqal.

[949] Voir Error correction for encoded quantum annealing par Fernando Pastawski et John Preskill, 2015 (4 pages).

En août 2020, ils avaient un client établi mais non identifié. Ils étaient en discussion avec la startup Pasqal dont l'architecture de simulateur quantique à base d'atomes froids est adaptée à leur modèle.

Phase Space Computing (2017, Suède) est une spin-off de l'Université de Linköping qui développe des solutions de formation sur l'informatique quantique destinés à l'enseignement secondaire et supérieur.

PhaseCraft (2018, UK, $1M) est une société de logiciels quantiques issue de l'University College London et de l'Université de Bristol. Ils sont aussi partenaires de Google. Ils veulent exploiter le calcul quantique pour créer de meilleurs systèmes de collecte et de stockage de l'énergie (batteries, solaire PV, …).

PiDust (2019, Grèce) est une startup lancée par Vasilis Armaos, Paraskevas Deligiannis et Dimitris Badounas, des anciens de Cambridge, Stanford et de l'Université de Patras, qui développe des algorithmes quantiques dans le domaine de la chimie.

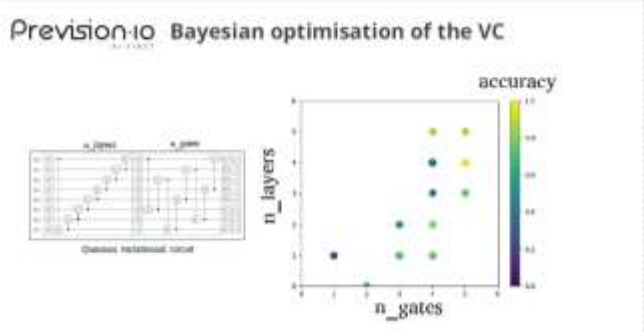
Pine.ly (2019, Canada) se positionne sur les logiciels d'aide à la création de matériaux innovants avec du calcul quantique. Ils visent notamment le recyclage des émissions de CO^2. La startup présente la particularité, rare, d'être créée par trois femmes, Nayer Hatefi, Shabnam Safaei et Rachelle Choueiri, toutes les trois scientifiques.

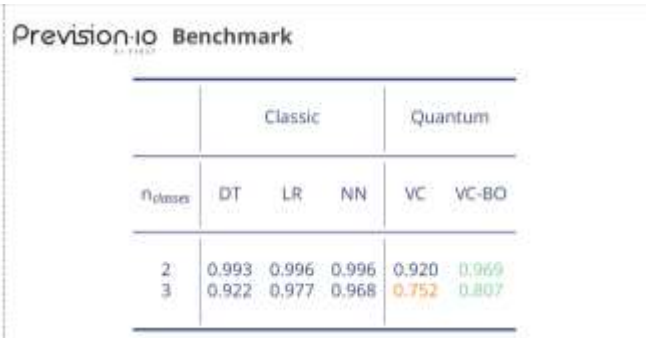
POLARISqb (2020, USA) est une startup qui veut utiliser le calcul quantique pour créer de nouvelles thérapies.

La startup a été créée par Shahar Keinan (CEO) et Bill Shipman (CTO). Ils sont notamment partenaires de Fujitsu, probablement pour utiliser leurs supercalculateurs classiques et leur calculateur à recuit numérique. Leur idée est d'utiliser des techniques de médecine personnalisée pour créer des thérapies ad-hoc. Shahar Keinan a obtenu un doctorat en chimie à l'Université Hébraïque de Jérusalem. Elle est spécialisée en chimie computationnelle. Reste maintenant à savoir ce qu'ils font réellement de quantique dans l'histoire.

Prevision.io (2016, France, 1,5M€) est une startup spécialisée dans le machine learning. Ils ont développé une plateforme qui automatise le choix de modèles de machine learning pour exploiter des données structurées.

Ils envisagent d'utiliser des algorithmes quantiques, notamment de QML (Quantum Machine Learning) pour compléter leur bibliothèque d'outils. Cela a du sens, d'autant plus que pour faire cela, la startup n'a pas besoin d'acquérir un ordinateur quantique ! On en trouve quelques-uns dans le cloud pour faire ses premiers tests sans compter les outils de simulation fonctionnant sur ordinateurs traditionnels ou supercalculateurs. Le quantique, ce sera surtout du cloud computing !





En mai 2019, le fondateur de la startup Nicolas Gaude, et un chercheur de la startup, Michel Nowak, PhD, présentaient les résultats de leur étude d'accélération quantique d'un algorithme de machine learning hybride, « Quantum Variational Circuits » sur un test de reconnaissance d'écriture du MNIST, le même que pour les débuts de réseaux de neurones convolutionnels de Yann LeCun en 1988. Le principe consiste à optimiser les hyperparamètres d'un réseau de neurones dans la partie quantique du calcul, couplé à une optimisation bayésienne fonctionnant de manière classique. C'est donc un algorithme quantique hybride.

Leur modèle illustrait l'intérêt d'une accélération quantique avec juste 20 qubits[950], simulés sur la bibliothèque de simulation quantique PennyLane de Xanadu. Ils estiment qu'un avantage quantique serait démontrable sur leur algorithme à partir de 28 qubits permettant de superposer l'équivalent d'un milliard d'hyperparamètres d'un réseau de neurones.

ProteinQure (2017, Canada) est une startup basée à Toronto qui utilise différentes technologies dont du calcul quantique pour créer et simuler de nouvelles thérapies "*in silico*". Ils utilisent des algorithmes quantiques pour simuler le repliement de protéines.

Ils développent aussi des algorithmes hybrides exploitant aussi des GPUs. Ils supportent différentes architectures matérielles dont les ordinateurs de D-Wave. Dans leurs expériences, ils arrivent à simuler des molécules avec 6 atomes dans des ordinateurs quantiques universels et atteignent 11 atomes avec les D-Wave. En pratique cependant, il semblerait qu'ils aient mis en veilleuse le calcul quantique et se concentreraient sur du machine learning classique en attendant.

QbitLogic (2014, USA, $1,5M) est une autre startup qui développe des applications de machine learning en quantique, sans plus de précision dans leur communication.

Q-Ctrl (2017, Australie) est une startup créée par Michael Biercuk, de l'Université de Sydney. Ils développent un firmware en cloud pour ordinateur quantique focalisé sur la gestion des codes de correction d'erreurs, Black Opal.

Ils ont aussi un outil de visualisation de l'effet de la modification de l'état des qubits par des portes quantiques… dans la sphère de Bloch. Ils sont notamment partenaires d'IBM. Ils interviennent aussi dans le champ de la métrologie quantique, à commencer par partenariat avec l'Australien **Advanced Navigation**, qui est spécialisé dans le géopositionnement.

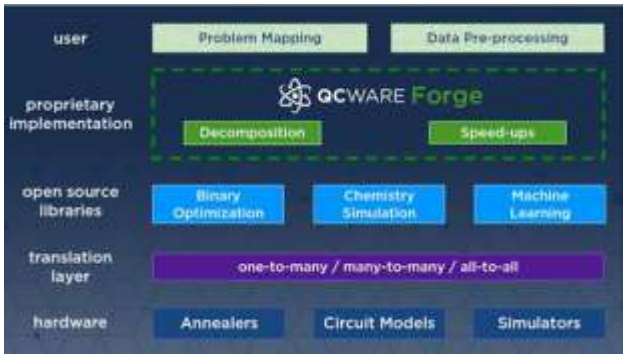
QC Ware (2014, USA, $14,7M) développe une plateforme de développement de logiciels quantiques en cloud. Ils créent des algorithmes quantiques et logiciels pour de grandes entreprises avec deux couches : leur plateforme propriétaire Forge et des bibliothèques open source pour l'optimisation, la simulation chimique et le machine learning.

Ils fournissent des outils pour charger plus rapidement en mémoire les données d'entraînement de modèles de machine learning. Ils ont aussi développé un algorithme de calcul de distance entre objets, pouvant servir à l'entraînement de modèles de machine learning supervisés (classification) et non supervisés (clustering).

Leurs premiers clients comprennent notamment **Equinor** pour de l'optimisation de prospection pétrolière, le Japonais **AISIN** pour des tests de certification de logiciels de boîtes de vitesse automatiques, **Airbus** pour de l'optimisation d'enveloppe de vol d'avions et **BMW** pour de l'optimisation de trajet de véhicules autonomes. Ils ciblent aussi le marché de la finance.

[950] Voir leur publication "One step towards quantum hyper parameter search", Michel Nowak et Nicolas Gaude (juin 2019).

Le tout supporte les ordinateurs quantiques à portes universelles (IBM, Rigetti), les ordinateurs à recuit quantique de D-Wave ainsi que les émulateurs logiciels (IBM, Google, Microsoft, Rigetti)[951].



Le groupe Airbus fait partie de leurs investisseurs. Ils ont reçu un financement public US de $1M via la NSF en 2017. La startup qui comprend déjà une vingtaine de personnes a été créée par Matt Johnson, qui a un background financier, et Kin-Joe Sham et Randy Correll qui ont l'air de s'être mis sur le tard dans l'informatique quantique. L'équipe comprend aussi Iordanis Kerenidis, qui est basé en France et est grand spécialiste du quantum machine learning. Il est en charge du développement international d'algorithmes. Le fameux Scott Aaronson est leur Chief Scientific Advisor.

Enfin, la startup organise une belle conférence annuelle sur l'informatique quantique, la **Q2B** dont la dernière édition avait lieu en décembre 2019 à San Jose en Californie[952].

QILIMANJARO

Qilimanjaro Quantum Hub (2018, Espagne) est une startup de Barcelone, donc plutôt Catalane ! Eux-aussi développent une plateforme logicielle quantique en cloud[953].

Ils veulent aussi développer leur propre ordinateur quantique adiabatique à base de qubits de flux. Ils prévoient aussi de se faire financer via une ICO, les tokens associés étant le QBIT, une crypto-monnaie d'usage de leurs ressources en cloud. Qui n'existent pas encore !

QINDOM

Qindom Inc. (2018, Canada, $2M) est une startup spécialisée dans le développement de logiciels de QML (quantum machine learning) sur ordinateurs quantiques D-Wave.

QRITHM

Qrithm (2018, USA) développe des algorithmes quantiques dans des domaines divers et plutôt disparates: machine learning, science des matériaux, cryptographie et finance.

Qu&Co

Qu&co (2016, Pays-Bas) développe des solutions logicielles quantiques sur mesure pour de grandes entreprises, accompagnés par des outils de benchmark.

Ils visent en particulier les applications de l'IA quantique ainsi que de la simulation chimique. Ils sont partenaires d'IBM et de Microsoft ainsi que de Schrodinger (USA).

QuantFi

QuantFi (2019, France/USA) est une jeune startup spécialisée dans la création de solutions logicielles quantiques pour la finance.

---

[951] Source des schémas : Enterprise Solutions for Quantum Computing par Yianni Gamvros, décembre 2019 (25 slides).

[952] Voir les supports de présentation et vidéos de la conférence Q2B de décembre 2019.

[953] Voir leur livre blanc : Qilimanjaro White paper (54 pages).

Elle a été créée par Paul Hiriart (Français, ex de Lehman Securities), Kevin Callaghan (un Américain ancien de la finance de New York) et Gabrielle Celani (une Américaine, sur la vente et le marketing). Ils sont accompagnés par Simon Perdrix dans le rôle de CTO (co-créateur du ZX Calculus, basé à Nancy) et de plusieurs chercheurs et développeurs. Ils visent la création d'algorithmes d'optimisation d'investissements ("goals based investment"), la détection de tendances, le pricing de dérivés et la gestion de risques. Ils ont rejoint en 2020 le réseau IBM Q dont ils exploitent les ressources en cloud, en liaison avec les équipes de Montpellier de ce dernier.

Quantopticon (2017, UK) développe des logiciels de modélisation et de simulation destinés à la conception de composants de photonique pour applications quantiques. C'est de l'outillage pour de la conception de nouveaux matériaux. Autant dire qu'ils sont positionnés sur un marché ultra-niche !

Quantum Benchmark Inc (2017, Canada) fournit une solution logicielle de code de correction d'erreurs pour ordinateurs quantiques universels et d'évaluation de ces erreurs. C'est donc en apparence un concurrent de l'Australien Q-Ctrl. Ils proposent aussi un système de validation de performance d'ordinateur quantique.

L'ensemble est intégré dans la suite True-Q, lancée en 2018, avec True-Q Design qui sert à évaluer le taux d'erreurs d'un ordinateur quantique et à en optimiser l'architecture et True-Q OS qui permet d'optimiser la précision des solutions logicielles.

Le marché visé est au départ celui des constructeurs d'ordinateurs quantiques et ceux qui les évaluent. A terme, cela sera celui des clients utilisateurs. A noter qu'ils ont déjà testé le framework Cirq de Google, ayant fait partie du programme de beta test de ce langage de Google et que ce dernier utilise leur solution. Ils sont aussi partenaires d'IBM.

Qsimulate (2018, USA) développe des solutions quantiques pour la simulation moléculaire dans la santé et la chimie. Ils sont partenaires d'Amazon Braket et de Google et travailleraient déjà avec Amgen. La société a été cofondée par Toru Shiozaki et Garnet Chan, tous les deux spécialisés en chimie.

Quacoon (2020, USA) développe des solutions logicielles associant IA et quantique.

Quantum Thought (2019, USA) développe des algorithmes quantiques ou quantum inspired pour les secteurs de la chimie, de l'IA et de la sécurité (QKD, PQC). Au vu de leur site web, il semble qu'il s'agisse surtout d'une société de service fonctionnant en mode projet. Leur CEO est Rebecca Krauthamer.

Quantumz.io (2019, Pologne) développe une solution logicielle d'émulation de calcul quantique fonctionnant sur GPU, la Quantum Simulator Platform (QSP). Ils développent aussi une solution de PQC (post-quantum cryptography) dénommée banax y compris des solutions matérielles pour la mettre en œuvre. Bref, deux activités sans grand rapport mais complémentaires.

Quantastica (2019, Estonie et Serbie) développe des outils logiciels d'algorithmes quantiques hybrides dont le Quantum Programming Studio, un environnement de développement web graphique pour créer des algorithmes quantiques exécutables sur ordinateurs quantiques ou sur émulateur, dont un émulateur qu'ils ont eux-mêmes développé.

Quantiq (2020, France) est une startup stealth crée par Alain Habra et Fabien Niel. Ils travaillent sur la création de solutions logicielles de diagnostic automatique, notamment dans la détection de pathologies avec l'analyse d'électrocardiogrammes.

Quantum Mads (2020, Espagne) est une jeune startup créée à Bilbao par Eriz Zárate et Alain Mateo Armas positionnée sur les marchés financiers. Elle propose quatre briques logicielles dont le dosage quantique/classique / hybride / quantum inspired n'est pas évident à identifier.

Avec Q-MADS, un framework d'analyse de stratégies d'investissements pour traders, Q-RETAIL, un framework pour la ba,qe de détail, Q-ALLOCATE, pour l'optimisation de l'allocation d'actifs et Q-CRYPTO, un framework de recherche de chemin optimum dans des graphes. Le tout s'appuie notamment sur l'algorithme d'algèbre linéaire HHL.

Quantopo LLC (2017, USA) est une société spécialisée dans les algorithmes de machine learning et . Ils se focalisent sur les biotechs et sur la supply chain et la logistique. Ils sont issus du Creative Destruction Lab. Mais n'ayant pas de site web actif, il n'est pas certain qu'ils existent encore.

Qubit Engineering (2018, USA) a été créée par des anciens de l'Université du Tennesse. Ils développent des algorithmes classiques et quantiques d'optimisation adaptés à la conception de turbines d'éoliennes et l'optimisation de leur emplacement. Ils sont partenaires de Microsoft Azure.

Qubitera (2018, USA) développe des solutions associant IA et quantique. N'a pu qu'à !

Qubit Pharmaceuticals (2020, France/USA) est une startup cofondée par Jean-Philip Piquemal, enseignant-chercheur CNRS de Sorbonne Université, spécialiste de longue date de la simulation de dynamique moléculaire qui modélise mathématiquement la mécanique quantique de molécules organiques.

Les cofondateurs de la startup sont basés à Austin et à la Washington University de Saint Louis. Ses algorithmes sont utilisés de longue date. Jean-Philip Piquemal est le coauteur de la bibliothèque de simulation moléculaire Tinker et de sa version Tinker-HP adaptée aux supercalculateurs. Elle exploite des systèmes massivement parallèles à base de CPU et des tenseurs des GPU Nvidia, le tout avec du calcul à haute précision. Ils exploitent notamment le calculateur Jean Zay du GENCI à Orsay ainsi que ceux du DoE aux USA. Ils ont été notamment impliqués dans le criblage de molécule pour la recherche de traitements du covid-19 par reciblage thérapeutique. Le reciblage est plus facile à simuler que la structure 3D de l'ensemble du covid-19 qui fait plus de 200 000 atomes ou la simulation du repliement de protéines. Et le calcul quantique dans tout cela ? Il pourrait servir à définir des paramètres optimisés pour la simulation classique, bref, dans le cadre d'algorithmes hybrides.

Ils pourront aussi exploiter des simulateurs quantiques à terme, comme ceux qui sont en train d'être mise au point avec des atomes froids chez Pasqal[954].

Le laboratoire de Jean-Philip Piquemal de Sorbonne Université a reçu un ERC de 9M€ pour le développement de solutions de simulation de systèmes organiques de plusieurs millions d'atomes[955]. Ils ont enfin accueilli le fonds d'investissement Quantonation dans leur capital en juin 2020[956].

QuDot (2018, USA) développe des logiciels de simulation de circuits quantiques sur ordinateurs traditionnels, le QuDot Net. Ils utilisent des techniques à base de réseaux bayésiens pour optimiser la représentation en mémoire des qubits.

QuLab (2017, USA) est une startup spécialisée dans les algorithmes quantiques pour la conception de molécules thérapeutiques.

QunaSys (2018, Japon) développe aussi des algorithmes quantiques pour la santé. Issue des université de Tokyo, Osaka et Kyoto, ils assurent aussi la maintenance du simulateur Qulacs développé à l'Université de Kyoto.

QuSoft (2014, Pays-Bas) est la spin-off de l'Université TU Delft spécialisée dans les algorithmes et logiciels quantiques. Comme sa sister-company QuTech, c'est plutôt un laboratoire privé de recherche appliquée qu'une startup.

Q^{x}Branch (2014, USA, $8,5M) a été créé par des anciens de Lockheed Martin. Elle propose des solutions, probablement sur mesure, pour les marchés de la finance, de l'assurance, de l'aérospatial et de la cybersécurité.

Basé à Washington DC, ils ont déjà des bureaux à Hong Kong, Londres et Adelaïde en Australie. Ils sont partenaires de D-Wave et d'IBM. La startup a été acquise par Rigetti (USA) en juillet 2019.

source : VC investment analysis Quantum Computing, Insead, 2018 (18 slides).

---

[954] Voir la présentation Computational Drug Design & Molecular Dynamics : an HPC perspective par Jean-Philip Piquemal, avril 2020 (28 slides).

[955] Voir Extreme-scale Mathematically-based Computational Chemistry (EMC2), 2020.

[956] Voir Qubit Pharmaceuticals closes a pre-seed round with Quantonation, Quantonation, juin 2020.

Rahko (2018, UK, £1,3M) est une société de développement de logiciels de quantum machine learning et de simulation chimique basée à Londres. Elle a été fondée par l'Allemand Leonard Wossnig. Ils font partie des premiers partenaires d'Amazon AWS pour l'usage de ressources quantiques en cloud, et le premier en Europe.

Ils annonçaient en mai 2020 travailler avec Merck sur des algorithmes « quantum inspired », donc sur des calculateurs classiques.

ReactiveQ (2018, Canada) dévelope des algorithmes quantique de simulation pour la conception de matériaux innovants comme des supraconducteurs à haute température, le tout sur calculateur quantique NISQ.

Riverlane (2016, UK, £3,3M) est une spin-off de l'Université de Cambridge qui fournit du service dans l'informatique quantique et développe de nouveaux algorithmes associant machine learning et le quantique dans le domaine de la chimie.

Ils développent avec dividiti Ltd (un one man shop créé par un certain Grigori Fursin), le Quantum Collective Knowledge, un SDK de benchmark de matériels et logiciels quantiques. Ils ont aussi développé ce qu'ils appellent un système d'exploitation quantique, Deltaflow.OS dedié aux calculateurs NISQ et qui optimise l'accès aux ressources matérielles de pilotage des qubits. Il était déployé à la mi 2020 sur plusieurs sites au Royaume-Uni.

RQuanTech (2018, Suisse) développe RTranscender, un outil à base de quantum machine learning pour la finance, la santé, l'automobile, la séismologie et la cybersécurité. Il supporte des transformées de Fourier, des opérations arithmétiques à base de qubits (additions, multiplications, divisions, exponentielles), de la factorisation, des log discrets etc.

Schrodinger (1990, USA, $193) est une entreprise de conception numérique de médicaments, principalement par criblage de molécules.

C'est un concurrent établi de Qubit Pharma (France) et travaille notamment avec Sanofi. La société est côté au NASDAQ. Ils se sont inévitablement intéressés au calcul quantique et ont pour ce faire démarré un partenariat avec Qu&Co.

Semicyber (2018, USA) développe des algorithmes dans différents domaines : analyses de données (non quantiques), quantiques et autres pour des applications « critiques » pour le secteur de la défense aux USA, et notamment l'US Air Force.

Ils sont donc probablement plus proches de la société de services que de la startup orientée produit. La startup est cofondée et dirigée par Kayla Farrow, une ingénieure spécialisée en création d'algorithmes et en traitement du signal.

Sigma-i Labs (2019, Japon, $3,7M) est une sorte de laboratoire privé issu du laboratoire de recherche en calcul à recuit quantique de l'Université Tohoku, basée à Sendai. Ils ont démarré en faisant du conseil autour de la création de logiciels pour les ordinateurs quantiques de D-Wave avec un qui ils ont signé en 2019 un partenariat pour mettre à disposition de leurs clients les ressources de D-Wave en cloud de leur offre Leap[957]. Et pas de logo de visible sur leur site web !

[957] Voir Sigma-i and D-Wave Announce Largest-Ever Quantum Cloud-Access Contract | D-Wave Systems, juillet 2019.

SolidState.AI (2017, Canada) développe des solutions de machine learning pour l'industrie couvrant l'amélioration de rendements, le calibrage de la production et la maintenance prédictive.

Le tout à partir d'algorithmes hybrides classiques/quantiques. Ils travaillent notamment avec Bosch, Applied Materials, Mercedez-Benz ainsi qu'avec D-Wave, Rigetti et IBM Q.

Spin Quantum Tech (2018, Colombie) développe des algorithmes quantiques dans le domaine de la cybersécurité qui combinent IA et quantique. Mais ils ne précisent pas du tout comment ils font cela. Ils ont l'air de faire de la PQC (post-quantum cryptography) qui exploite de nouveaux algorithmes de chiffrement.

Ils travaillent aussi sur de la simulation chimique, ce qui n'a rien à voir. Un syndrome de dispersion classique dans un marché émergent qui est de taille très limitée.

SHYN (2016, Bulgarie) développe des solutions de visualisation de données issues de calculs quantiques. Donc, du dataviz quantique ! Avec un cas d'usage consistant à détecter les fake news quantitatives. Elle a été cofinancée par le fonds Digital News Information Fund de Google qui est dédié à la presse. Ce fonds de 150M€ a distribué des financements de quelques centaines de milliers d'Euros à plus de 400 projets en Europe.

SoftwareQ (2017, Canada) propose des logiciels de développement pour le calcul quantique : compilateur, simulateur, optimisateurs.

La société a été cofondée par Michele Mosca et Vlad Gheorghiu de l'Institute of Quantum Computing canadien.

Solid State AI (2017, Canada) développe une plateforme logicielle quantique en cloud exploitant des algorithms hybrides adaptés aux besoins de l'industrie.

C'est une startup issue du programme Quantum Machine Learning du Creative Destruction Lab de Toronto.

Strangeworks (2018, USA, $4M) développe des logiciels quantiques. Comme de nombreux confrères, ils ciblent les marchés de l'aérospatial, de l'énergie, de la finance et de la santé. Ils sont à l'origine de la création d'un site de questions/réponses sur l'informatique quantique, Quantum Computing Stack Exchange.

Ils ont lancé en 2019 une bêta d'un environnement de développement multi-plateformes d'applications quantiques supportant les calculateurs quantiques ou émulateurs de Rigetti Computing (Forest), DWave (Leap), Microsoft (Q#), Google (Cirq) et IBM (Qiskit). Cet environnement a l'air de faciliter le travail collaboratif et le partage de résultats.

Stratum.ai (2018, Canada) développe un logiciel quantique dédié à un marché très pointu, l'optimisation de la prospection minière, notamment dans l'or.

Super.tech (2020, USA, $150K) est une startup lancée par Pranav Gokhale, Fred Chong et Teague Tomesh qui développe une stack logicielle dédiée au contrôle de systèmes de calcul quantiques allant d'une centaine à un millier de qubits.

La solution est issue du projet de recherche Practical-Scale Quantum Computation (EPiQC) financé par la NSF et associant cinq universités de la région de Chicago et du MIT et des stars telles que Peter Shor et Aram Harrow. Elle vise à créer une infrastructure logicielle adaptée au développement de solutions NISQ.

Terra Quantum AG (2019, Suisse, 10M€) développe des solutions logicielles quantiques dans tous les domaines : cryptographie, métrologie quantique, calcul quantique. Ils ont l'air d'être bien dispersés. C'est probablement plus une société de services que produit. Ils se positionnent modestement comme étant à même de construire « *l'écosystème quantique européen* »[958].

Tokyo Quantum Computing (2017, Tokyo) veut développer un logiciel de simulation d'ordinateur à recuit quantique.

Tradeteq (2016, UK, $6,3M) est une plateforme de trading financier qui s'appuie sur l'IA pour faire de l'évaluation de risque et de l'optimisation de portefeuille.

Ils ambitionnent de faire appel à du calcul quantique pour faire évoluer leurs méthodes. Ils annonçaient en avril 2020 travailler dans ce sens avec la Singapore Management University (SMU) et avec des algorithmes de réseaux de neurones quantiques.

Xofia (2019, USA) développe des solutions logicielles à base de quantum machine learning de classification. Ils veulent diffuser leurs logiciels en open source. Ils exploitent en cloud l'émulateur quantique de 40 qubits d'Atos, un serveur aQLM.

Zapata Computing (2017, USA, $64M) est une société de logiciels et services quantiques créée par des chercheurs de Harvard dont Christoper Savoie et le fameux Alán Aspuru-Guzik de l'Université de Toronto qui est spécialisé dans les applications du quantique dans la chimie. Ils sont notamment partenaires de Google et IBM.

Ils développaient à l'origine un système d'exploitation quantique complet devant jouer le rôle de plaque tournante entre algorithmes applicatifs et ordinateurs quantiques de tous types. En avril 2020, cela prenait la forme de la plateforme Orquestra, une plateforme de gestion de workflows d'applications quantiques programmés avec le langage maison Zapata Quantum Workflow Language (ZQWL) qui est compatible YAML[959], supportant diverses architectures matérielles de calcul quantique (NISQ, recuit quantique) et classique (émulateurs quantiques comme ceux d'Atos, supercalculateurs, serveurs en cloud). Elle propose des bibliothèques de code diverses supportant les langages de programmation quantiques Cirq (Google), Qiskit (IBM), PennyLane (Xanadu), PyQuil (Rigetti), Q# (Microsoft) et pyAQASM (Atos).

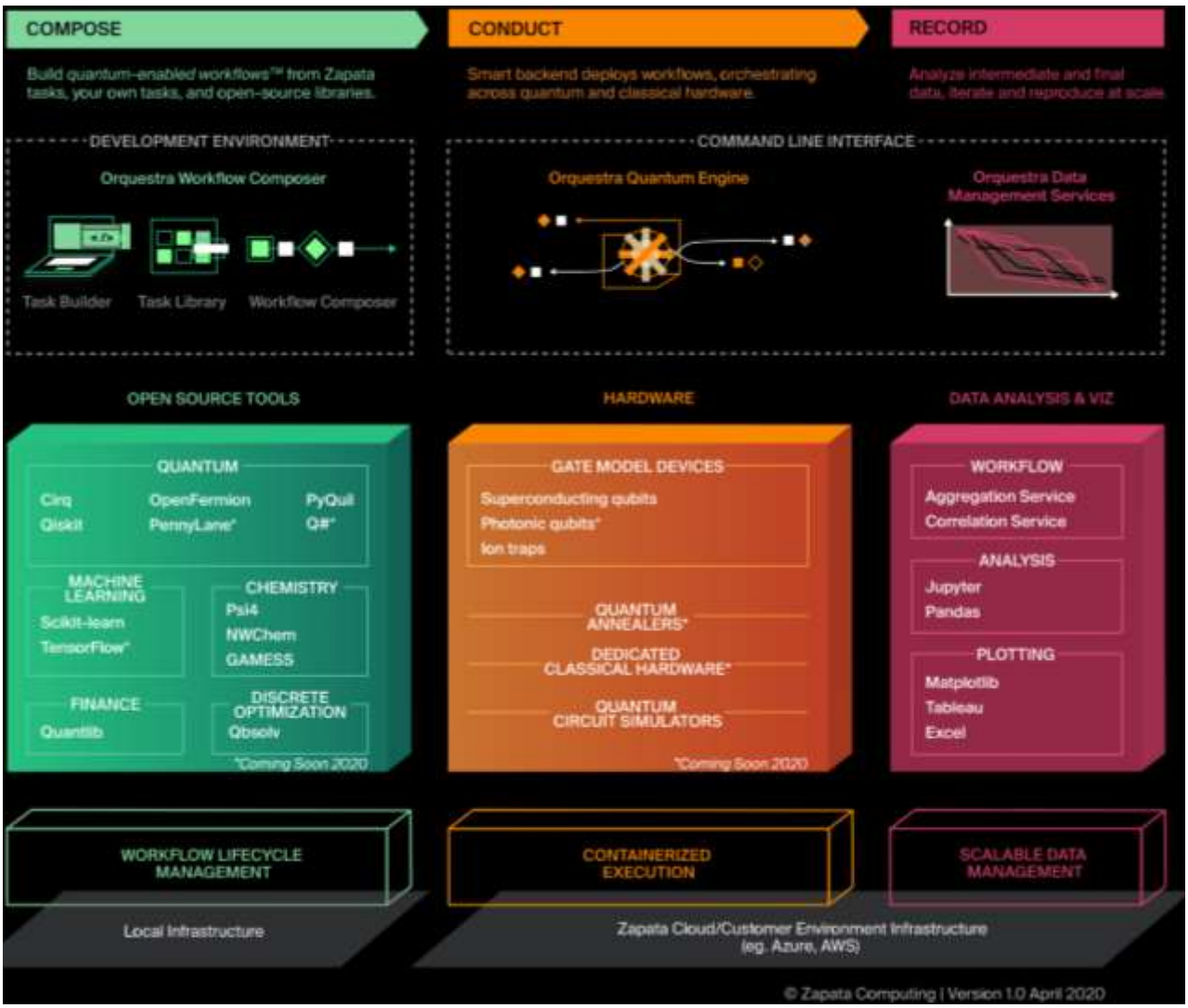
Orquestra comprend les outils de gestion de batchs de calcul. Le service Orquestra Data Correlation Service (ODCS) collecte les données des traitements dans une base MongoDB qui sont alors exportées sous forme de tableaux Excel, d'un notebook Jupyter ou pour le logiciel Tableau. Orquestra est en bêta depuis avril 2020 dans le cadre d'un Early Access Program.

A noter qu'Honeywell est rentré dans leur capital en mars 2020.

---

[958] Voir Terra Quantum secures EUR10m to build the European Quantum Ecosystem par James Dargan, avril 2020.

[959] YAML est un langage qui date de 2001. Il sert à créer des fichiers de configuration. Il est exploité de concert avec Python.



Voilà, ce petit tour est terminé. Si vous découvrez des startups du calcul quantique qui ne figurent pas dans cet inventaire ou disposez d'informations complémentaires sur celles qui sont citées, je suis preneur ! J'utiliserai vos informations pour actualiser cette liste au fil de l'eau[960].

[960] Voir This Startup Just Raised $21 Million To Bring Quantum Computing To Enterprise Applications, 2019.

Télécommunications et cryptographie

Les télécommunications quantiques reposent essentiellement sur la communication de photons et sur leur intrication. Leur champ est vaste mais, dans la pratique, il est aujourd'hui souvent réduit à celui de la cryptographie quantique. Cela tient au rythme de mise au point des technologies quantiques. Celles de la cryptographie sont déjà en cours de déploiement alors que les télécommunications quantiques associées aux calculateurs quantiques dépendent de l'avènement de ces derniers à grande échelle. Avènement qui pourrait attendre une décennie ou plus.

L'intérêt pour la cryptographie quantique comme post-quantique a été déclenché par la création de l'algorithme de Shor en 1994. Il permet théoriquement de factoriser rapidement des nombres entiers sur un calculateur quantique. Cet algorithme secoue le monde de la sécurité informatique depuis au moins une bonne quinzaine d'années. Il permettrait de casser les codes de nombre de systèmes de cryptographie à clés publiques qui sont couramment utilisés sur Internet. Cela reste encore hypothétique car les ordinateurs quantiques capables de l'exécuter ne sont pas encore au point. On ne dispose en effet pas encore d'u nombre suffisant de qubits de bonne qualité pour exécuter cet algorithme sur des nombres premiers de grande taille.

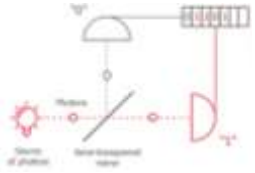
Lorsqu'ils sont au courant de la menace, les services de contre-espionnage, de renseignement et les entreprises de secteurs critiques s'en inquiètent cependant sérieusement. La menace de la factorisation quantique pèse même sur une partie du fonctionnement du Bitcoin et de la BlockChain. Même si la menace est lointaine, il faut s'y préparer dès maintenant du fait de l'inertie de cette préparation.

Avant donc même que la menace fantôme de Shor se matérialise concrètement, l'industrie de la cybersécurité s'est mise en ordre de bataille pour y faire face. Les marchés touchés en premier seront l'industrie informatique et des télécommunications en général qui vont devoir mettre à jour de nombreuses offres logicielles et matérielles, les banques, le secteur de l'énergie, la santé et les activités régaliennes des services publics.

Dans cette partie, nous allons décrire dans l'ordre :

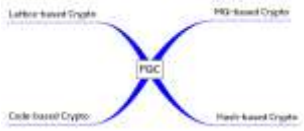
- Les principes de base de la **cryptographie** classique, notamment à clé publique, avec l'exemple des clés publiques RSA.
- La nature de la **menace** provenant de la factorisation de nombres entiers et les solutions de cryptographie concernées.
- Les **générateurs de nombres aléatoires quantiques**, compléments devenus indispensables des solutions de cryptographie de haut vol.
- Les systèmes à **clés quantiques** qui permettent de sécuriser la partie physique des communications pour l'usage de clés symétriques.
- La **cryptographie post-quantique** ou « quantum safe » qui sert à protéger la partie logique des communications cryptées dans le cas de l'usage de clés publiques. Ce sont des algorithmes utilisant du calcul classique, pas du calcul quantique.
- Les applications de **télécommunications quantiques** en dehors de celles qui sont liées à la cryptographie. Et en particulier celles qui permettront de créer des systèmes distribués de calcul quantique.
- Les **entreprises** de ces secteurs dans le monde, dans un marché qui comprend déjà de nombreux acteurs et en particulier des startups.

Le chiffrement et la cryptographie font appel à des notions mathématiques pas toujours évidentes et que je ne maîtrise pas du tout. Je vous partage donc ici ce que j'ai pu comprendre de ces sujets en les vulgarisant autant que possible.

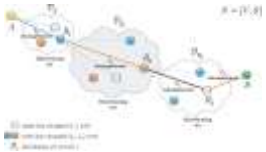


générateur quantique de clés aléatoires
assure la qualité des clés utilisés

clés quantiques QKD
protège les clés par liaison optique



cryptographie post-quantique
chiffrement résilient à l'algorithme de Shor



télécommunications quantiques
traitements quantiques distribués, relations calcul et capteurs quantiques

Cryptographie par clé publique

La cryptologie est la science des secrets. Elle permet la transmission d'informations sensibles entre un émetteur et un récepteur et de manière sure. La cryptologie comprend la cryptographie, qui sécurise l'information émise et la cryptanalyse qui cherche à la décrypter par attaque. Les puristes francophones parlent de chiffrement et de déchiffrement, lorsque l'on encode et décode l'information puis de décryptage, lorsqu'un attaquant décode les messages.

Dans le cas de la cryptographie asymétrique à clé publique, le chiffrement n'exploite que les clés publiques et le déchiffrement s'appuie sur les clés publiques et privées. Le décryptage exploite uniquement les clés publiques en cherchant à en déduire les clés privées par du calcul intensif plus ou moins accessible.

La cryptographie sécurise l'information transmise de plusieurs manières :

- Par la **confidentialité** : seul le destinataire peut récupérer la version non chiffrée de l'information transmise.
- Par l'**intégrité** : l'information n'a pas été modifiée pendant sa transmission.
- Par l'**authentification** : l'émetteur et le récepteur sont bien ceux qu'ils prétendent être.
- La **non-répudiation** : l'émetteur ne peut pas nier avoir transmis l'information chiffrée.
- Le **contrôle d'accès** : seules les personnes autorisées par l'émetteur et le récipiendaire peuvent accéder à l'information non chiffrée.

Avant les télécommunications informatiques, la confidentialité était assurée par la connaissance d'un secret commun entre émetteurs et récepteurs, les fameux codes de chiffrement et de déchiffrement, pouvant être la position des roues d'une machine **Enigma** allemande pendant la seconde guerre mondiale. Cela fonctionnait dans des environnements fermés comme pour les communications militaires ou entre ambassades et pays d'origine.

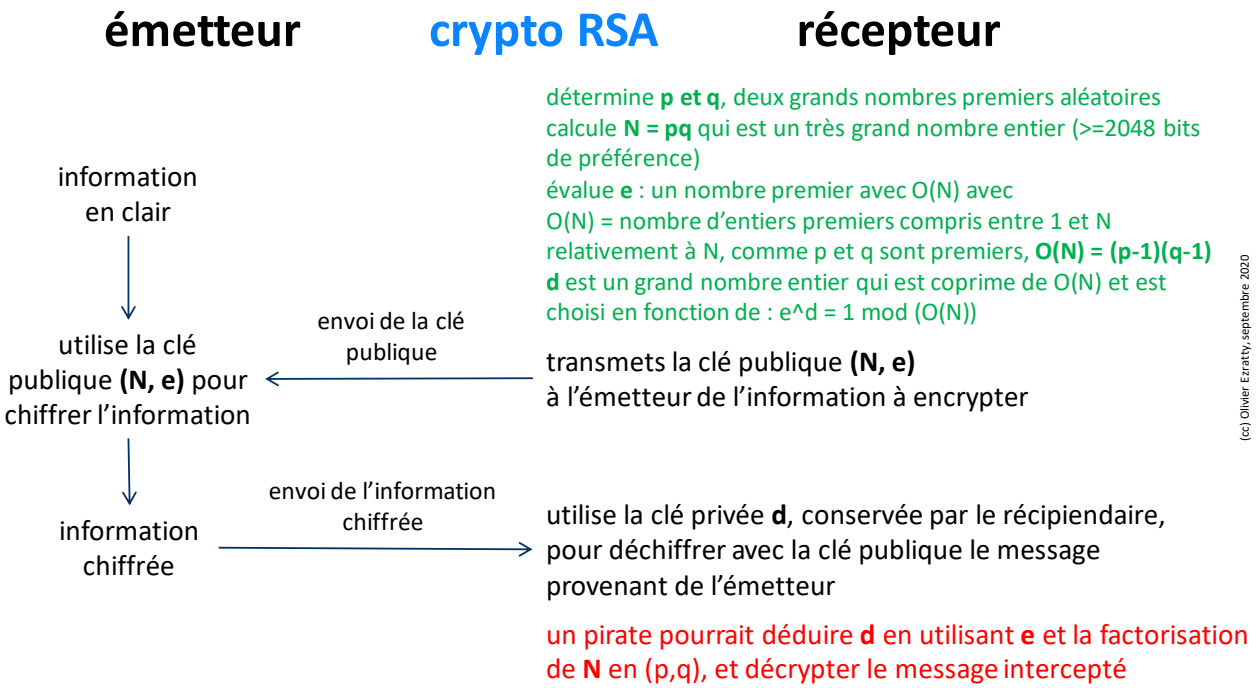
Avec les communications sur Internet, ce mode opératoire est inapplicable pour des applications grand public et pour les relations entre les entreprises en général. D'où les systèmes de cryptographie à clés publiques, notamment RSA, qui servent à un grand nombre d'échanges d'informations. Il subsiste des systèmes très protégés à base de clés privées et symétriques et qui sont principalement utilisés dans le cadre des applications régaliennes (armée, sécurité, renseignement) ainsi que dans divers autres cas (transferts de fichiers, chiffrage de mails, échanges serveur/client, dans les cartes à puces et terminaux de paiement associés).

La cryptographie asymétrique (à clés publique) est aussi exploitée pour l'établissement préalable de clés de chiffrement communes entre les utilisateurs de systèmes à clés privées, pour gérer l'intégrité des communications et pour l'authentification comme dans le protocole TLS sur Internet. Les informations sensibles sont alors chiffrées avec ces clés et un algorithme symétrique type AES. AES est ainsi utilisé pour chiffrer les communications dans Whatsapp, Messenger et Telegram. Ces applications utilisent souvent également de la cryptographie asymétrique pour l'authentification, les échanges de clés et la gestion de l'intégrité des communications.

Dans de très nombreux cas, les systèmes de cryptographie symétriques cohabitent avec des systèmes de cryptographie asymétriques (à clés publiques). Donc, lorsque vous communiquez sur Internet de manière sécurisée, ce sont plusieurs protocoles de sécurité complémentaires qui sont activés.

Dans les systèmes à clé publique, des clés différentes sont utilisées pour le chiffrement et le déchiffrement des informations transmises, de telle manière qu'il est très difficile (si ce n'est parfois impossible) de déduire la clé privée de déchiffrement à partir de la clé publique de chiffrement. C'est le récepteur du message qui envoie sa clé publique à l'émetteur, qui l'utilise à son tour pour chiffrer le message. Le récepteur utilise la clé privée qu'il a conservée pour déchiffrer le message reçu. Comme l'explique le schéma *ci-dessous*, la clé privée n'est jamais transmise. C'est ce que l'on appelle aussi une PKI, pour "Public Key Infrastructure".

L'algorithme **RSA** est le plus connu et le plus utilisé des systèmes de protection des transmissions d'information par clé publique sur Internet. Il a été créé en 1978 par **Ron Rivest** (1947, Américain), **Adi Shamir** (1952, Israélien) et **Leonard Adleman** (1945, Américain).



Vous n'avez pas forcément besoin de comprendre la tambouille interne que voici et qui explique comment les clés sont construites. Cela commence par la détermination de p et q, deux grands nombres premiers aléatoires, avec un "bon" générateur de nombres aléatoires. Nous verrons plus loin que la physique quantique permet de créer des générateurs de nombres vraiment aléatoires. On calcule N = pq qui est un très grand nombre entier. Une bonne clé RSA requiert d'avoir N stocké sur au moins 2048 bits sachant que la NSA recommande des clés de 3072 bits pour les applications critiques.

On évalue ensuite **e**, un nombre premier en exploitant O(N) qui égale le nombre d'entiers premiers compris entre 1 et N relativement à N, et qui, comme p et q sont premiers, égale (p-1)(q-1). d est un grand nombre entier qui est copremier de O(N) et est choisi en fonction de : e^d = 1 mod (O(N)). A la fin, on obtient une clé publique qui comprend les entiers N et e, et une clé privée qui comprend d. L'ensemble s'appuie sur la théorie des nombres et utilise notamment le petit théorème de Fermat et le théorème d'Euler qui permettent de créer deux clés distinctes et inverses l'une de l'autre.

La beauté du système permet à n'importe qui d'encrypter un message à partir de la clé publique, ce message n'étant déchiffrable que par celui qui dispose de la clé privée qui décompose la clé publique en primitives.

Un pirate pourrait décrypter l'information envoyée en exploitant e (le bout de la clé publique) et en factorisant N, l'autre bout de la clé publique, en entiers p et q, puis en déduire la clé privée d.

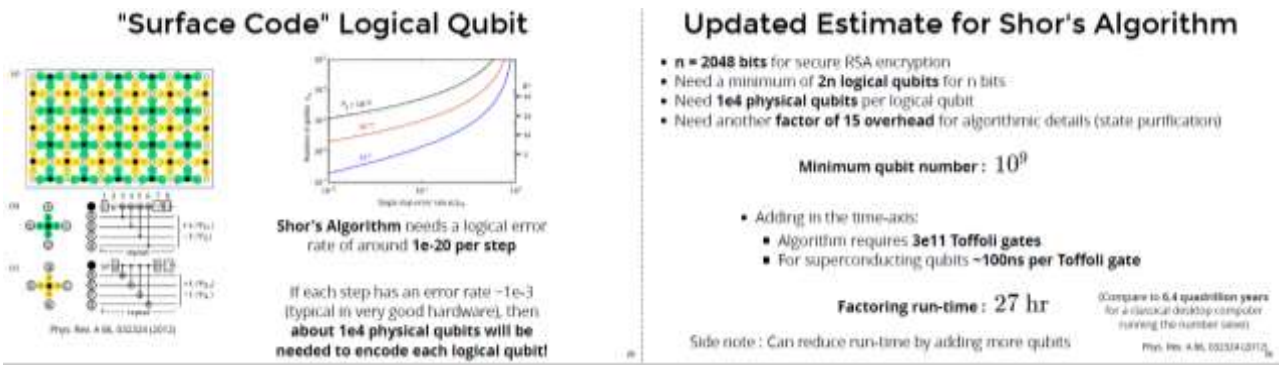
A ce jour, la factorisation de nombres premier demande une puissance machine traditionnelle qui croit à la vitesse de la racine carrée du nombre à factoriser. Le record de factorisation officiel de clé RSA est de 768 bits, réalisé en 2010. Cela n'inventorie visiblement pas les records non communiqués de la NSA.

Menace fantôme de Shor

Lorsque nous avons abordé les algorithmes quantiques, nous avons décrit celui de **Peter Shor**. C'est l'un des premiers algorithmes quantiques après celui de **Deutsch-Jozsa**. Il a provoqué un intérêt pour le calcul quantique alors que les chercheurs n'avaient pas encore réussi à créer un seul qubit contrôlable par une porte quantique à un qubit !

Il doit permettre de factoriser dans un temps raisonnable des nombres entiers, proportionnel à leur logarithme. C'est donc une factorisation en un temps linéaire en fonction du nombre de bits de la clé. Il se trouve que cela pourrait mettre à mal les systèmes de cryptographiques courants qui reposent sur la notion de clé publique[961].

Mais uniquement dans un futur relativement lointain ! En 2019, des chercheurs de Google publiaient un algorithme permettant de casser rapidement une clé RSA (de 2048 bits) et avec « seulement » 20 millions de qubits ayant un taux d'erreur de 0,1% et dans un calcul réalisé en 8 heures. C'est plus « acceptable » que le milliard de qubits indiqué dans le schéma *ci-dessous* à droite.



Les ordinateurs quantiques actuels ont un temps de cohérence bien court largement inférieur à la seconde, mais le compteur de la décohérence est remis à zéro après chaque code de correction d'erreur qui est utilisé dans l'algorithme[962]. A savoir que l'on va ainsi pouvoir s'affranchir de la limite du temps de cohérence généralement assez court, notamment pour les qubits supraconducteurs où il est situé aux alentours de 100 µs.

Il faut au minimum un nombre de qubits logiques qui égale le double de la taille de la clé utilisée +2, donc 4098 qubits pour casser une clé RSA de 2048 bits. Selon les technologies utilisées, il faudrait multiplier ce chiffre par 50 à 20 000 pour le nombre de qubits physiques.

---

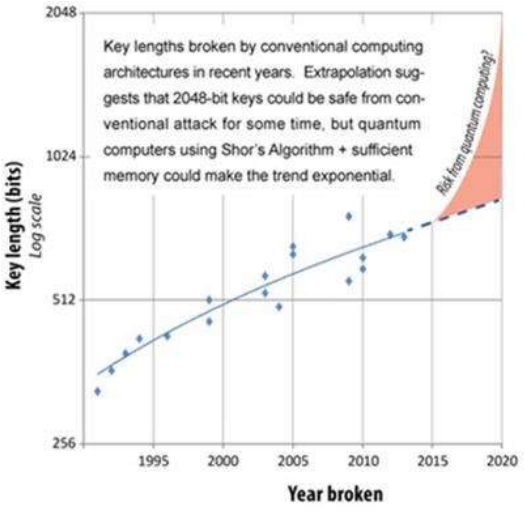
[961] Voir cette présentation qui décrit avec force détails le fonctionnement de l'algorithme de Shor : On Shor's algorithms, the various derivatives, their implementation and their applications par Martin Ekerå, 2019 (135 slides).

[962] Voir How a quantum computer could break 2048-bit RSA encryption in 8 hours et How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits de Craig Gidney et Martin Ekerå, 2019 (25 pages). Par contre, le titre de l'article Un ordinateur quantique casse le chiffrement RSA sur 2048 bits en 8 heures d'Arthur Vera (2019) est totalement faux. L'ordinateur en question n'existe pas encore !

Par ailleurs, comme nous l'avons vu dans la partie concernant l'algorithme de Shor, la transformée de Fourier quantique qui la sous-tend fait appel à des portes quantiques R à phase contrôlée dont la mise en œuvre est loin d'être évidente.

En effet, lorsque la phase en question fait un angle de 1/2048 fois un tour à 360° dans la sphère de Bloch d'un qubit, la rotation contrôlé de la phase peut être inférieure au taux d'erreur d'une porte quantique à deux qubits. Il faut donc parier sur la capacité des codes de correction d'erreur à traiter cela.

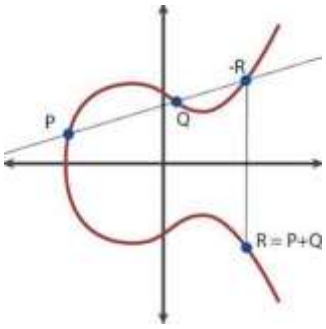
Une clé RSA de 762 bits proche du record de 2010 demanderait un ordinateur à recuit quantique du Canadien **D-Wave** avec 5,5 milliards de qubits, loin des 2048 existants[963]. Un D-Wave de 5893 qubits pourrait faire l'affaire si tous les qubits étaient couplables de manière arbitraire, ce qui n'est pas possible du fait de la conception en matrice 2D des chipsets de D-Wave, et de la plupart des qubits d'ailleurs. La menace de Shor est visualisée dans le temps dans ce schéma originaire de l'organisme de standardisation européen ETSI[964]. Elle s'appuie sur des prévisions très optimistes concernant les capacités des ordinateurs quantiques à exploiter l'algorithme de Shor. Il faudrait décaler vers le futur d'au moins 5 à 10 ans la partie orange du graphe.



L'algorithme de Shor appliqué au cassage de clés publiques RSA aurait un impact très large sur les usages d'Internet. On le retrouve en effet intégré dans les protocoles **TLS** et **SSL** qui protègent les sites web et les transferts de fichiers via **FTP**, dans le protocole **IPSEC** qui protège IP V4 dans le sous-protocole IKE, dans le protocole **SSH** d'accès à distance à une machine et dans le **PGP** qui est parfois utilisé pour chiffrer les emails.

La menace concernerait aussi la **signature électronique** de logiciels et donc leurs mises à jour automatiques, les **VPN** pour l'accès à distance aux réseaux d'entreprises protégés, la sécurisation des emails avec **S/MIME**, les systèmes de **paiement**, **DSA** (Digital Signature Algorithm, un protocole de signature électronique), les codes **Diffie-Hellman** (utilisés dans l'envoi de clés symétriques) ainsi que la cryptographie à courbes elliptiques **ECDH, ECDSA** et **3-DES**. Le protocole **Signal** utilisé dans Whatsapp serait aussi en ligne de mire. Une bonne part de la sécurité d'Internet est donc plus ou moins en ligne de mire.

ECC (Elliptic Curve Cryptography) est le premier algorithme à courbes elliptiques, créé en 1985 par Neal Koblitz et Victor Miller. Les variantes les plus courantes d'aujourd'hui sont **ECDH** (Elliptic-curve Diffie–Hellman) et **ECDSA** (Elliptic Curve Digital Signature Algorithm, lancé en 2005). Ces variantes ont été déployées à partir de 2005 et plus largement seulement à partir de 2015, donc 30 ans après la création du premier ECC ! Au passage, les courbes elliptiques ont permis à Andrew Wiles de démontrer le dernier théorème de Fermat en 1992, qui n'a pas de rapport avec la cryptographie.



[963] Selon High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311, de Nike Dattani, Xinhua Peng et Jiangfeng Du, juin 2017 (6 pages).

[964] Voir Quantum Safe Cryptography and Security, 2015 (64 pages).

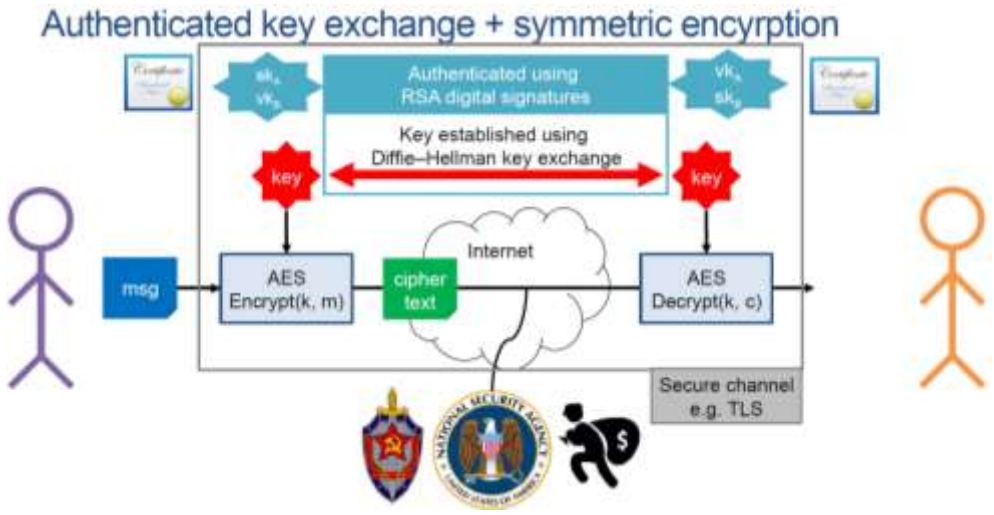
Je vous en passe les détails car je n'ai pas compris grand-chose aux explications que j'ai pu trouver[965]. Mais peu importe. L'un des intérêts des codes à base de courbes elliptiques est d'utiliser des clés publiques plus courtes qu'avec le chiffrement RSA.

Mais ces courbes elliptiques sont aussi cassables en quantique avec un temps raisonnable à cause de notre ami Peter Shor[966] et de la résolution du problème du logarithme discret (DLP : discrete logarithm problem)[967]. Qui plus est, une porte dérobée de l'ECDSA a été révélée par Edward Snowden en 2013, logée par la NSA dans son générateur de nombre aléatoire Dual EC DRBG. L'abandon de son usage était ensuite recommandé par le NIST en 2014 et la NSA en 2015 pour la transmission d'informations sensibles[968].

La seconde raison est que des communications sensibles d'aujourd'hui peuvent être stockées par des pirates privés ou d'Etats, conservées et exploitées bien plus tard, le jour où les ordinateurs quantiques seront à la hauteur. Nombre d'informations d'aujourd'hui auront de la valeur plus tard, qu'ils s'agisse de transactions financières, de communications privées diverses, de secrets industriels ou autres secrets d'Etats.

Le calcul quantique est une véritable épée de Damoclès dont la chute est difficile à prévoir et plutôt éloignée dans le temps d'au moins une bonne décennie. Au-delà d'un tel délai, il est quasiment impossible de faire des prévisions.

Michele Mosca a créé pour ce faire une inégalité qui porte son nom. Elle s'exprime sous la forme $D+T>G_c$, où D est la durée pendant laquelle les données d'aujourd'hui ayant circulé de manière chiffrée doivent être sécurisées, T, le temps nécessaire pour faire ma transition de ses systèmes de chiffrement vers des solutions résistantes au calcul quantique et G_c, le temps qu'il faudra pour que soient mis au point des ordinateurs quantiques capables de casser les clés publiques de systèmes actuels de chiffrement. D, c'est vous qui le spécifiez. T, vous pouvez le planifier en fonction de votre système d'information et de l'offre commerciale. Quant à G_c, il vous reste à l'évaluer au doigt mouillé car les estimations vont de 5-10 ans à… jamais !



source : Introduction to post-quantum cryptography and learning with errors, Douglas Stebila, 2018 (106 slides).

[965] Comme dans Elliptic curves cryptography and factorization (86 slides).

[966] Comme documenté dans Shor's discrete logarithm quantum algorithm for elliptic curves, de John Proos and Christof Zalka, 2003 (34 pages).

[967] Le problème du log discret consiste à trouver un entier k vérifiant a^k = b modulo p, a, b et p étant des entiers connus. Cela permet de casser les clés de courves élliptiques et Diffie-Hellman.

[968] Voir à ce sujet Elliptic Curve Cryptography and Government Backdoors de Ben Schwennesen, 2016 (20 pages).

Les systèmes de cryptographie symétriques ne sont pas concernés par l'algorithme de Shor. Il s'agit notamment du **Data Encryption Standard** (DES) qui utilise des clés de 64 bits ou plus et qui est dépassé, remplacé par l'**Advanced Encryption Standard** (AES) qui est un standard du gouvernement US depuis 2002, avec des clés privées allant de 128 à 256 bits.

Les clés sont partagées en amont des échanges et généralement elles-mêmes chiffrées avec l'algorithme **Diffie-Hellman**. Mais ce chiffrement Diffie-Hellman est à base de courbes elliptiques, qui est cassable par du calcul quantique avec l'algorithme de Shor. Le problème est la vulnérabilité de la majorité des systèmes de chiffrement à clés asymétriques et auxquels on fait appel pour partager des clefs symétriques.

A ce jour, les meilleurs algorithmes de cassage quantique des clés symétriques **AES** mettraient plus que l'ancienneté de l'Univers (13,8 milliards d'années) pour s'exécuter sur des clés de 128 bits. Avec l'AES-256 bits, on est donc des plus tranquille ! Ils reposent sur des mécanismes bien différents de la résolution de problèmes mathématiques des chiffrements à clés publiques.

Une fonction de hash convertit une donnée de taille arbitraire comme un fichier en un nombre de taille fixe. Cela permet de faire des recherches rapides pour comparer des fichiers. Elle peut par exemple servir à vérifier qu'un fichier n'a pas été altéré pendant sa transmission.

Les algorithmes SHA (Secure Hash Algorithms) sont des standards de fonctions de hachage qui consistent à remplacer une donnée de taille arbitraire par une clé de taille unique.

L'algorithme de hashage **SHA-1** résiste bien à l'algorithme de Shor, mais il a été cassé par d'autres méthodes et est donc jugé dépassé. C'est le **SHA-3** qui est le plus à jour et depuis 2015. L'algorithme SHA peut être cassé par l'algorithme de recherche de Grover, mais avec une grande quantité de qubits, au minimum 6000 qubits logiques pour les clés courantes[969]. Cela représente un ordre de grandeur voisin des besoins en qubits pour casser les clés RSA.

Une clé de hachage ou empreinte permet par exemple de vérifier l'intégrité d'un contenu comme un logiciel ou plus simplement, un mot de passe. Le problème étant de résister aux collisions, à savoir, aux méthodes permettant de trouver ou créer un objet dont l'empreinte serait celle dont on dispose, ce qui est bien différent que de retrouver l'objet (comme une image) d'origine à partir de son empreinte, qui est plutôt difficile.

		SHA-256	SHA3-256
Grover	T-count	1.27×10^{44}	2.71×10^{44}
	T-depth	3.76×10^{43}	2.31×10^{41}
	Logical qubits	2402	3200
	Surface code distance	43	44
	Physical qubits	1.39×10^{7}	1.94×10^{7}
Distilleries	Logical qubits per distillery	3600	3600
	Number of distilleries	1	294
	Surface code distances	{33, 13, 7}	{33, 13, 7}
	Physical qubits	5.54×10^{5}	1.63×10^{8}
Total	Logical qubits	$2^{12.6}$	2^{20}
	Surface code cycles	$2^{153.8}$	$2^{146.5}$
	Total cost	$2^{166.4}$	$2^{166.5}$

Table 3. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.

Le nombre de qubits nécessaires au cassage des clés dépend de la taille de la clé. SHA-1 et SHA-2 ont des tailles de clés faibles qui peuvent être récupérées en un temps considéré raisonnable avec l'algorithme quantique de recherche de **Grover** mais ce n'est pas le cas de SHA-3 qui exploite des clés plus grandes. C'est la même logique que pour AES.

Le schéma *ci-dessus* pointe du doigt les principaux algorithmes de chiffrement vulnérables ou pas aux algorithmes quantiques connus[970]. En gros, les systèmes de chiffrement courants à clés publics sont vulnérables. Seuls les systèmes de cryptographie post-quantiques sont résilients. Mais ils ne sont pas encore en production.

---

[969] D'après Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3, 2016 (21 pages), qui est aussi la source du tableau de cette page.

[970] Vu dans IDQ : Quantum-Safe Security elevance for Central Banks, 2018 (27 slides) et légèrement complété par quelques légendes.

Qu'en est-il du **Bitcoin**, des crypto-monnaies et de la **BlockChain** ? Voici une réponse résumée *ci-dessous*[971] avec pour commencer un bon inventaire des systèmes de cryptographie utilisés par usage.

En gros, la Blockchain s'appuie sur un patchwork d'algorithmes de cryptographie comprenant l'AES, RSA et SHA-3. Elle exploite un algorithme de hash pour s'assurer de l'intégrité de la chaine de confiance, et une signature numérique pour authentifier les nouvelles transactions qui s'ajoutent à la Blockchain de manière incrémentale. Dans le cas du Bitcoin, celui-ci utilise la crypto hash SHA-256 qui est résistante au quantique et une signature qui exploite des courbes elliptiques ECDSA qui elle ne l'est pas.

Table 3. Main Algorithms Types Used for Cryptography, and Uses For Smart Ledgers[19]

Type of Algorithm	General Use	Example Algorithms of This Type	Example Uses for Smart Ledgers
Symmetric	Secret communications	AES, DES, 3DES, RC4	Protection of resources stored on ledger
Public key	Secret communications (including key exchange) or digital signature	RSA, Diffie-Hellman, El Gamal, ECDSA	User authentication; signature of transactions, data or software
Hash	Generating fixed-length digest of arbitrary-length text	SHA-256, SHA-512, SHA-3	Ensuring authenticity of blockchain

Ethereum utilise un hash SHA-3 qui résiste au quantique et une signature ECDSA qui est vulnérable.

In fine, le calcul quantique ne permettra pas d'altérer la Blockchain ni la preuve de travail utilisée par le Bitcoin qui s'appuie sur l'usage répété de hash résistant au quantique. La vulnérabilité de la Blockchain se situe dans la signature qui s'appuie sur l'algorithme à courbes elliptiques ECDSA qui peut être cassée avec l'algorithme de Shor. Cela permettrait de se faire passer pour quelqu'un d'autre dans une transaction impliquant une Blockchain ou des Bitcoins.

Si une transaction Bitcoin était interceptée pour récupérer la signature ECDSA de l'émetteur, celle-ci pourrait être exploitée pour transférer des Bitcoins à partir du porte-monnaie de cet émetteur.

Des solutions de contournement pourront évidemment être créées d'ici la confirmation d'une menace quantique sur l'intégrité des transactions. Cela peut passer par le chiffrement en PQC des signatures utilisées par les blockchains[972].

---

[971] La réponse est fort bien documentée dans The Quantum Countdown Quantum Computing and The Future of Smart Ledger Encryption, de Long Finance, 2018 (60 pages).

[972] Voir Blockchained Post-Quantum Signatures, Chalkias Browny Hearnz, 2018 (8 pages).

On peut aussi d'emblée chiffrer les données circulant dans une Blockchain avec un algorithme résistant au calcul quantique comme AES-256, avec l'inconvénient qu'il est symétrique et nécessite donc que des clés soient échangées au préalable.

Il existe cependant déjà des parades. Un protocole utilisant un temps de validation plus long des transactions en Bitcoin permettrait de contourner l'usage de la factorisation d'entiers pour casser l'algorithme de signature électronique du Bitcoin, ECDSA[973]. Mais cela ne ferait qu'amplifier un défaut clé du Bitcoin en tant que monnaie : un rallongement des temps de transaction qui est déjà loin d'être temps réel !

On peut aussi citer le projet open source de Blockchain résistante aux sournoises attaques du quantique : Quantum Resistant Ledger. Il s'appuie sur le protocole de signature électronique XMSS (Extended Merkle Signature Scheme)[974].

Il existe aussi un risqué d'attaque au niveau du mining, cette fois-ci avec l'usage de l'algorithme de Grover. Mais là encore, des parades sont disponibles[975].

Le document de **Long Finance** d'où est extrait le tableau *ci-contre* résume tous ces risques sur les Smart Ledgers en séparant les transactions qui sont relativement protégées et celles qui s'appuient sur des signatures électroniques vulnérables qui ne le sont pas[976]. Il rappelle aussi que les échanges Internet sur lesquels s'appuient la Blockchain sont aussi vulnérables au hacking des protocoles SSL et TLS[977].

The Quantum Countdown
Quantum Computing And The Future Of Smart Ledger Encryption

Table 4. Risks to Blockchain Architectures from Quantum Computing

	Transactions	Data on Blockchain	Software on Blockchain
Read historical records without authorization	No (blockchains are intended to allow access to transaction information)	No, unless confidential and secured with vulnerable cryptography	No, unless confidential and secured with vulnerable cryptography
Alter historical records	No	No	May be able to run software without authorisation if signature used
Spoof ongoing records	Yes, possibly	Yes, possibly	Yes, possibly

Cette partie sur les menaces ne serait pas complète sans évoquer les désaccords qui règnent dans l'industrie et la recherche. Certains spécialistes de la cryptographie sont plutôt conservateurs et considèrent qu'il ne faut pas trop toucher à ce qui fonctionne bien.

Ils pensent que l'on en fait trop avec la menace de Shor. D'autres, comme le NIST aux USA, sont plus alarmistes et sont d'avis qu'il ne faut pas tarder à mettre à jour les systèmes de cryptographie les plus critiques[978].

---

[973] C'est documenté dans Committing to Quantum Resistance A Slow Defence for Bitcoin against a Fast Quantum Computing Attack, 2018 (18 pages).

[974] Voir aussi Blockchained Post-Quantum Signatures, Chalkias Browny Hearnz, 2018 (8 pages).

[975] Voir On the insecurity of quantum Bitcoin mining par Or Sattath, février 2019 (22 pages).

[976] Voir The Quantum Countdown Quantum Computing And The Future Of Smart Ledger Encryption, Long Finance, février 2018 (62 pages).

[977] Pour en savoir plus, voir aussi The quantum threat to payment systems de Michele Mosca de l'Université de Waterloo, 2017 (52 minutes). Mosca est une des références mondiales du domaine.

[978] Les analyses se chargent de relayer cette peur, comme dans Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity du Hudson Institute, un think tank conservateur US, mars 2019 (24 pages), Preparing Enterprises for the Quantum Computing Cybersecurity Threats de CSA, mai 2019 ou le Global Risk Report 2020 du World Economic Forum.

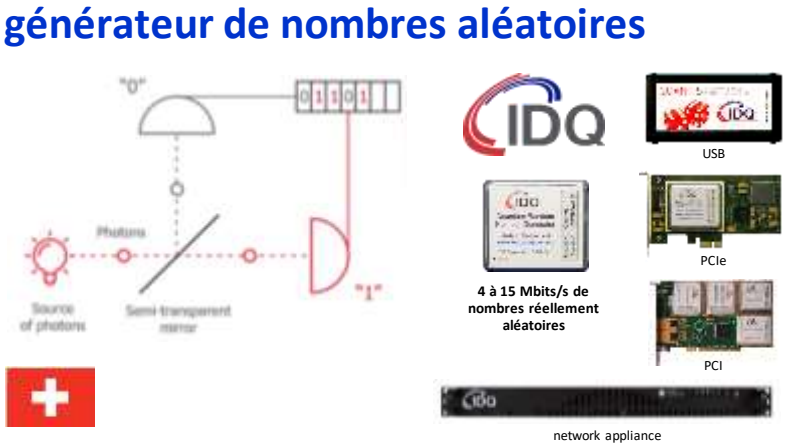
Génération de clés aléatoires quantiques

Nous allons maintenant passer à la description des trois briques de la cryptographie quantique avec pour commencer, la génération de clés aléatoires.

Les systèmes de cryptographie quantique et traditionnels sont tous alimentés par des générateurs de nombres aléatoires. Il en existe depuis des lustres. N'importe quel microprocesseur peut générer des nombres plus ou moins aléatoires. Le souci des cryptographes est de disposer de nombres véritablement aléatoires. A savoir des suites de 0 et de 1 sans répétitions avec une proportion de 0 et de 1 équilibrée. Comme le sont les décimales du nombre π ! Il faut de plus que la génération soit non déterministe et que l'on ne puisse pas la reproduire.

Une bonne part des générateurs de nombres aléatoires utilisés couramment sont pseudo-aléatoires et déterministes. Ce sont des **PRNG**, pour Pseudo-Random Number Generators. On introduit de l'aléatoire en utilisant comme paramètres de l'algorithme de génération des éléments variables comme l'heure à la milliseconde près, les coordonnées GPS, de l'agitation thermique ou d'autres informations de contexte.

Malheureusement, malgré ces variables d'initialisation, les algorithmes courants génèrent des périodes dans les nombres générés. La solution consiste à utiliser un processus physique réellement aléatoire dans la génération de nombres. L'un des processus connus consiste à mesurer le bruit d'origine thermique d'un composant électronique comme dans un amplificateur.



La méthode la plus aléatoire repose sur la physique quantique et en particulier sur un système conceptuellement assez simple reposant sur la mesure de photons uniques émis individuellement en série sur deux détecteurs après avoir traversé un miroir semi-transparent[979].

Elle permet de créer des nombres véritablement aléatoires de toute taille et assez rapidement, à raison d'un débit pouvant atteindre 1,5 Mbits aléatoires par seconde, voir même plusieurs dizaines de Gbits/s. Ils varient selon les processus utilisés. La technique est notamment maitrisée par IDQ ou ID Quantique, créée par le chercheur Nicolas Gisin et dans le giron de SK Telecom depuis 2018, ainsi que par exemple **MagiQ**, **cryptomathic**, **Crypta Labs** et **PicoQuant**.

Un générateur quantique optique de nombres aléatoire est rentré pour la première fois dans un produit grand public en 2020 sous la forme d'un chipset QRNG miniaturisé d'**ID Quantique** (filiale de SK Telecom) intégré dans une version spéciale du smartphone **Samsung** Galaxy A71 5G dénommée Galaxy A Quantum commercialisé par **SK Telecom** en Corée. A la clé, des … clés de chiffrement véritablement aléatoires. Cela ne changera probablement pas grand-chose à la sécurité des utilisateurs mais cela marquera les esprits.

[979] Voir Quantum Random Number Generators de Miguel Herrero-Collantes, 2016 (54 pages).

Il existe cependant encore des solutions de génération de nombres aléatoires non quantiques devant être tout aussi aléatoire, sachant que ceci est toujours sujet à caution[980].

Cryptographie quantique

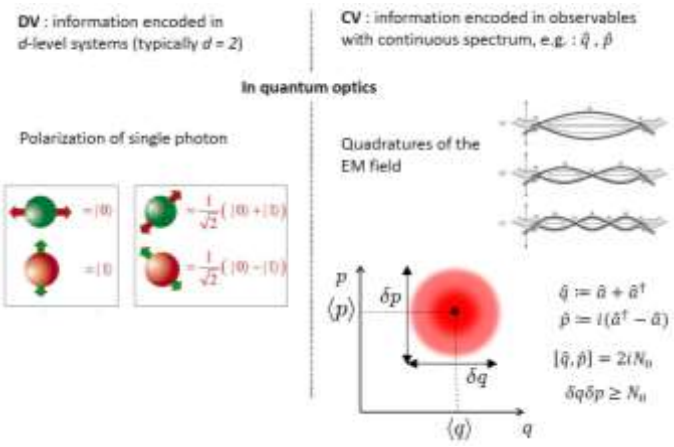
Le principe de base de la cryptographie quantique est celui de la QKD ou "quantum key distribution". Il consiste à permettre l'échange de clés de chiffrement, en général symétriques, par voie optique (fibre optique, liaison aérienne ou satellite) en s'appuyant sur un système de protection de sa transmission contre les intrusions.

Sa première mouture fut le protocole BB84 inventé par l'Américain **Charles Bennett** et le Canadien **Gilles Brassard** en 1984[981]. Ils sont les créateurs en 1982 de l'appellation de "cryptographie quantique"[982].

Principes de la QKD

Nous l'avions déjà évoqué dans une partie précédente : en 1992, un certain **Artur Ekert** né en 1961, Polonais et Anglais, rencontre le physicien français Alain Aspect en 1992 pour lui soumettre l'idée d'utiliser l'intrication quantique de photons qu'il a vérifié dans son expérience en 1982 pour l'envoi de clés quantiques inviolables. Alain Aspect trouve l'idée intéressante. Artur Ekert venait tout juste de créer en 1991 le protocole E91[983]. Artur Ekert avait perfectionné BB84 en utilisant l'intrication quantique et la non-localité, évitant la transmission explicite d'information de phase de photon pouvant être interceptée par un intrus. Ensuite, le protocole **BBM92** ajoutait aussi l'intrication au protocole BB84. L'idée a depuis fait son chemin. Elle est à l'origine de la création du champ entier de la cryptographie quantique qui est même sorti du domaine de l'expérimentation pour entrer dans la sphère industrielle. Il y a aussi le protocole CV-QKD pour "continuous variable"-QKD qui module à la fois la phase et l'amplitude du signal optique transmis.

Il permet notamment le multiplexage de plusieurs communications sur une même fibre optique et d'exploiter les infrastructures existantes des opérateurs télécoms. Philippe Grangier en est l'un des concepteurs, avec Frédéric Grosshans du CNRS-LIP6, en 2002. La CV-QKD complète la DV-QKD, nouvelle appellation de la première version de 1984, basée sur les propriétés de photons uniques et qui a besoin de refroidissement du côté des détecteurs de photons (illustration : Eleni Diamanti).



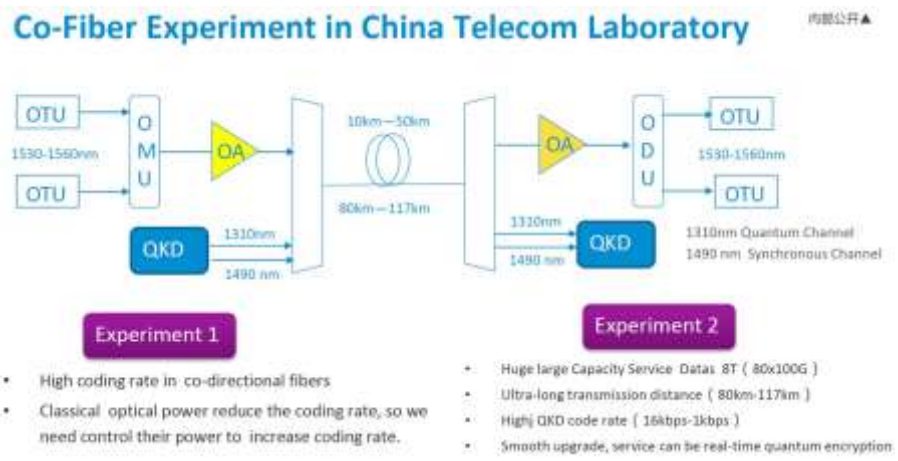
[980] Voir par exemple Scientists Develop 'Absolutely Unbreakable' Encryption Chip Using Chaos Theory par Davey Winder, 2019.

[981] Dans Quantum cryptography : public key distribution and coin tossing, 1984 (5 pages).

[982] Voici un apercu général de la QKD et de la PQC : The Impact of Quantum Computing on Present Cryptography, mars 2018 (10 pages).

[983] Et publié dans l'article Quantum Cryptography Based on Bell's Theorem (3 pages). Artur Ekert fait partie depuis 2016 du conseil scientifique d'Atos en compagnie d'Alain Aspect, Daniel Estève, Serge Haroche, Cédric Villani et David DiVincenzo.

L'intégration d'une QKD dans des fibres classiques de télécommunications passe par trois méthodes : par multiplexage de fréquence (WDM) avec une QKD sur 1310 et la data envoyée sur 1550 nm comme illustré *ci-contre*, par time sharing (TDM) ou par utilisation d'une fibre dédiée dans un fourreau (SDM)[984].



Les protocoles de QKD ont la particularité de permettre la détection de toute intrusion dans la chaine de transmission et d'indiquer que quelqu'un a tenté d'en lire le contenu ou si des perturbations sont intervenues "sur la ligne".

Dans le protocole BB84, cela repose sur l'envoi de l'information sur des photons avec quatre types de polarisations rectilignes : 0°, 45°, 90° et 135°. Leur lecture par un intrus va modifier la clé, en projetant leur polarisation à 0° ou 90°, ou 45°/135° selon les cas. Toute intrusion en lecture sera détectée à l'arrivée. Si le protocole détecte un intrus, il peut en tenir compte et bloquer la communication de l'information sensible parce que la clé d'encodage a été captée.

L'encodage d'une QKD par intrication est dit superdense (*superdense coding*) car on l'utilise pour envoyer deux bits sur un qubit transmis par voie optique entre deux points lorsqu'ils sont déjà reliés par un état intriqué de photons. C'est un protocole de communication imaginé par Charles Bennett et Stephen Weisner en 1992 et expérimenté en 1996 par Klaus Mattle, Harald Weinfurter, Paul Kwiat et Anton Zeilinger avec des paires de photons.

L'intrication initiale précédant l'envoi des deux bits dans le qubits permet d'éviter de violer le théorème d'Holevo, déjà cité plusieurs fois, selon lequel un jeu de qubits ne peut pas transporter plus d'information que le nombre équivalent de bits classiques.

De son côté, l'information chiffrée avec la clé transmise est habituellement envoyée sur un canal traditionnel[985]. Elle est elle-même souvent chiffrée comme avec le protocole SSL qui protège les relations entre votre navigateur et les sites web que vous visitez et qui supporte le protocole sécurisé https[986].

En pratique, la transmission de clé par QKD s'accompagne d'un système complexe de "distillation de clé" qui gère les imperfections de la communication avec des codes de correction d'erreurs classiques (qui n'ont rien à voir avec les codes de correction d'erreurs quantiques vus au niveau des qubits ailleurs dans ce document), une amplification de la confidentialité et un système d'authentification par clés privées déjà partagées par les correspondants, permettant d'éviter les attaques "*man in the middle*" de pirates qui se feraient passer pour l'un des interlocuteurs.

---

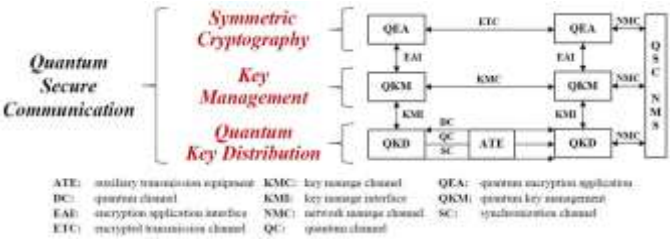
[984] Voir QKD Application: Coexistence QKD Networkand Optical Networking the same optical fiber network par JiDong Xu, juin 2019 (15 slides). C'est aussi décrit dans Quantum Encrypted Signals on Multiuser Optical Fiber Networks Simulation Analysis of Next Generation Services and Technologies de l'Anglais Rameez Asif, 2017 (6 pages) et Quantum experiments explore power of light for communications, computing par Elizabeth Rosenthal, janvier 2020.

[985] L'information classique peut d'ailleurs prendre un chemin très différent. Ainsi, une clé quantique peut être transmise par satellite et les données par voie terrestre sur fibre optique.

[986] C'est d'ailleurs une modification que j'ai mise en place dans le blog Opinions Libres fin juillet 2018. Cela ne change pas grand-chose dans la mesure où les lecteurs que vous êtes ne se connectent pas de manière sécurisée sur le site. Cela sécurise un peu mieux la connexion administrateur.

Les codes de correction d'erreurs et le reste du protocole génèrent des pertes en ligne d'environ 80% de la communication des clés quantiques[987].

La mise en œuvre d'une QKD combine un générateur de clés aléatoires quantiques comme ceux d'IDQ, un système de génération de clés logiques, puis une transmission de ces clés via la QKD. Elles vont circuler généralement sur fibre optique noire d'un opérateur télécom B2B[988].



Le signal est alors chiffré avec la clé logique qui a été préalablement envoyée via la QKD par le récipiendaire de l'information. Il est généralement transmis sur un canal traditionnel, pouvant passer aussi par fibre optique ou un autre support de communication physique. C'est bien documenté par l'ETSI[989]. A l'arrivée, on exploite un lecteur de clé quantique et le système de déchiffrement du signal arrivé par la voie classique.

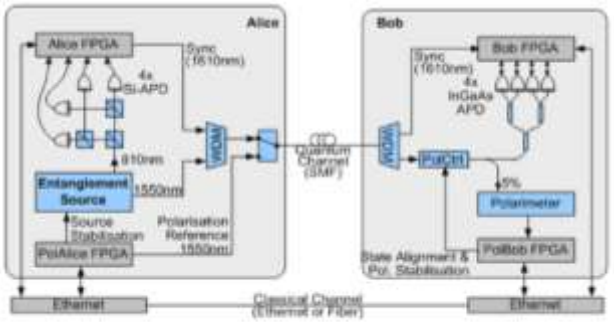


Figure 4.6: Schematic of an entanglement-based QKD system

Une QKD peut être utilisée pour transmettre des clés symétriques comme l'AES ainsi que des clés résistantes au déchiffrement par du calcul quantique (PQC), que nous verrons plus loin. Le débit des clés secrètes est une question importante et se chiffre actuellement au grand maximum en Mbits/s vs les Tbits/s des liaisons optiques des opérateurs. Le débit de transfert de clés quantiques peut être inférieur à celui des données transmises.

Il existe quelques autres variétés de protocoles de QKD au-delà des DV-QKD et CV-QKD déjà citées avec la HD-QKD (plusieurs bits d'encodage de clés par photon) et la MDI-QKD[990]. Je ne vais pas les détailler.

Expériences et déploiements

Les expériences symboliques de mise en œuvre de QKD se sont régulièrement succédées tant à l'air libre que sur fibres optiques.

Les démonstrations de QKD à l'air libre démarraient en 1996 aux USA sur 75m, puis sur 144 km pour relier les iles de La Palma et de Tenerife aux **Canaries** et menées par des Autrichiens en 2007 puis en 2010[991], et en 2019 en milieu urbain en Italie sur 145m[992].

---

[987] Selon l'excellent panorama de Sheila Cobourne de l'Université de Londres Quantum Key Distribution Protocols and Applications, 2011 (95 pages).

[988] Source du schéma : Development and evaluation of QKD-based secure communication in China par Wen-yu Zhao, juin 2019 (15 slides).

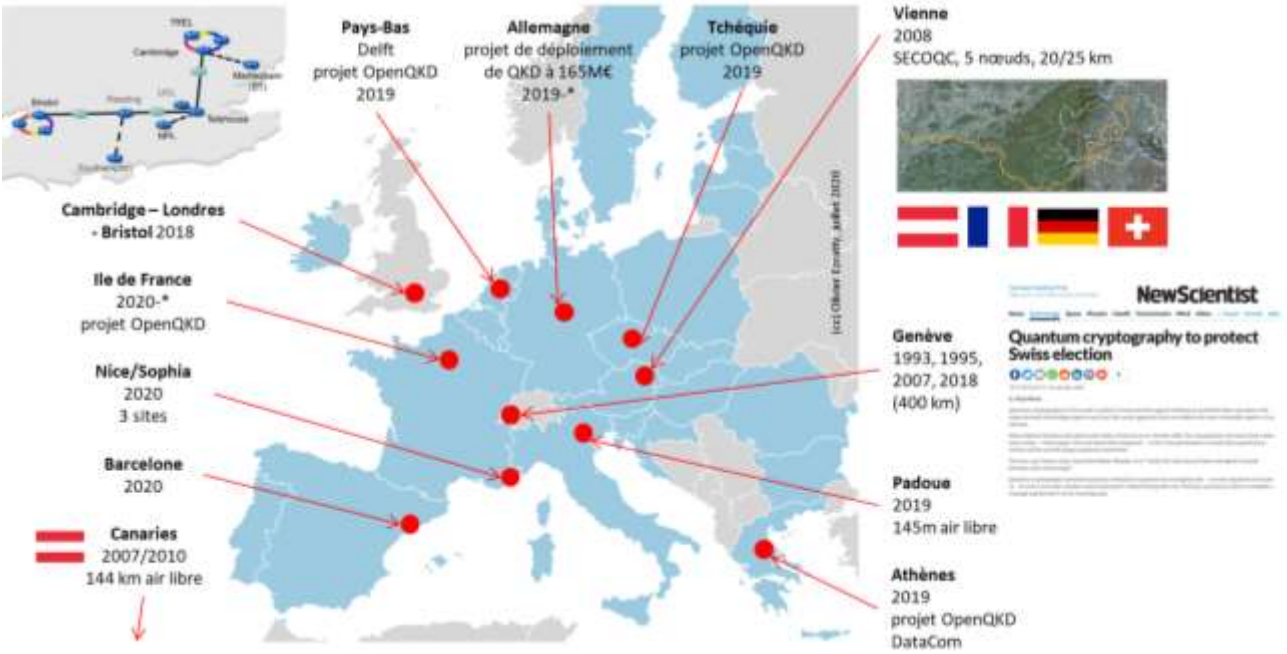
[989] Dans Quantum Key Distribution (QKD) Components and Internal Interfaces de l'ETSI, 2018 (47 pages) qui décrit les différentes techniques de QKD disponibles à ce jour et d'où le schéma de la page est issu. Il décrit aussi très bien les sources de photons utilisées dans la QKD ainsi que les paramètres quantitatifs et qualitatifs associés.

[990] Voir ce bon panorama sur la QKD et de ses enjeux techniques dans Practical challenges in quantum cryptography, d'Eleni Diamanti et al, 2016 (25 pages).

[991] Voir Second Generation QKD System over Commercial Fibers, 2016 (5 pages) et Feasibility of 300 km Quantum Key Distribution with Entangled States, 2010 (14 pages).

La portée de la transmission de QKD sur fibre s'est améliorée avec seulement 30 cm en 1989 (IBM avec Charles Bennett), 1100 m à l'Université de Genève en 1993, puis 23 km en 1995 avec le protocole BB84, le tout via une fibre optique. Le record début 2020 était de 509 km de transmission et sans répéteur, réalisé en Chine[993].

Une expérimentation a eu lieu à **Vienne** en 2008 dans le cadre du projet européen **SECOQC** (*SE*cure *CO*mmunication based on *Q*uantum *C*ryptography) lancé en 2004 et associant une quarantaine de laboratoires de recherche et d'entreprises privées, dont des laboratoires français, en exploitant une architecture "mesh"[994].



Cela a continué en Suisse avec **IDQ** pour relier entre elles des banques locales. Ils ont aussi mis en place en 2007 un système de décompte de votes d'élections s'appuyant sur une QKD. Si les machines à voter sont elles-mêmes sécurisées, cela peut avoir un intérêt.

En 2018, le Royaume Uni déployait son UK Quantum Communications hub entre Bristol, Londres, Cambridge et Ipswich[995].

En France, **Orange** annonçait en mai 2019 lancer les tests d'une communication protégée par QKD avec l'Université Côte d'Azur (UCA) qui en fournit la solution via le laboratoire InPhyNi.

Elle relie le campus Valrose et l'Inria de Sophia Antipolis avec un point d'accès sur le campus de la Plaine du Var IMREDD à Nice, le tout s'appuyant sur des fibres noires fournies par l'opérateur télécom[996]. Le réseau de test était opérationnel en mai 2020.

---

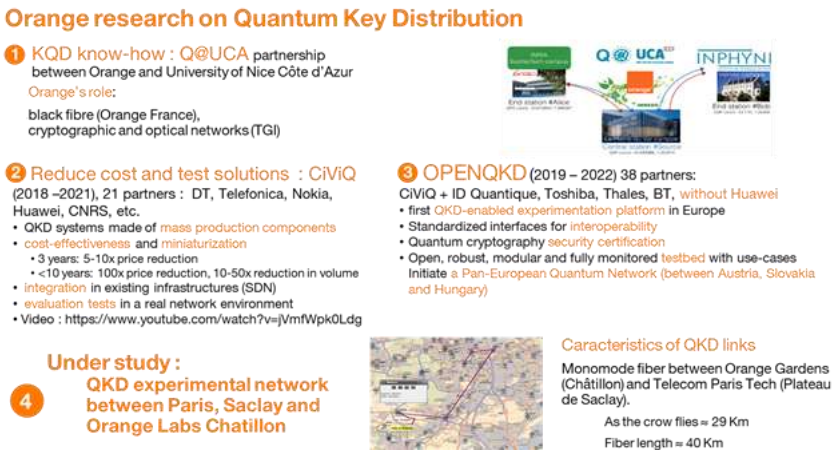
[992] Voir Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics par Matteo Schiavon et al, juillet 2019 (7 pages). La transmission de clé QKD en liaison aérienne de 145m avait lieu sur 1550 nm dans l'infrarouge qui est couramment utilisé dans les transmissions par fibre optique et donc compatible avec de nombreux équipements existants. Ils utilisaient un chipset en silicium qui faisait tout le boulot. Avec taux d'erreur de seulement 0,5% et un débit de 30 kbits/s. Leur QCosOne (« Quantum Communication for Space-One") utilisait des télescopes avec des optiques de 120 et 315 mm pour l'émission et la réception. Cela fonctionnait de jour, mais il y avait tout de même des problèmes en cas de turbulences et selon l'heure de la journée et les effets du soleil. La performance était meilleure en soirée. Ils utilisaient un triple encodage des photons : temporel, spatial et spectral.

[993] Voir Study achieves a new record fiber QKD transmission distance of over 509 km Ingrid Fadelli, mars 2020.

[994] Voir The SECOQC quantum key distribution network in Vienna par Romain Alléaume, Eleni Diamanti et al, 2016 (39 pages).

[995] Vue dans IDQ : Quantum-Safe Security elevance for Central Banks, 2018 (27 slides). Le réseau était étendu dans Cambridge en 2019 : voir Cambridge quantum network par J. F. Dynes et al, 2019 (8 pages).

Orange étudie notamment la fiabilisation des nœuds de confiance des réseaux optiques dans une telle configuration. L'opérateur cherche aussi à associer les solutions de QKD pour protéger les liaisons physiques et de PQC qui pourraient servir de méthode de chiffrement de données transmises en association avec une QKD.



Le consortium européen **OpenQKD** vise à expérimenter sur le continent un réseau de QKD terrestre. Il prépare le terrain pour le lancement de l'**EuroQCI** qui vise la mise en place opérationnelle d'un réseau de QKD européen à la fois terrestre et satellite[997]. Cela concerne en particulier la France, l'Allemagne, l'Autriche, l'Italie, l'Espagne, les Pays-Bas, la Grèce, la Suisse et la Pologne. Il implique notamment Thales Alenia Space pour la dimension satellitaire ainsi qu'Orange et Telecom Paris. Mellanox, filiale de Nvidia, est aussi impliqué. D'un point de vue pratique, il s'agit de déployer à l'échelle européenne un grand réseau expérimental de QKD interopérable et exploité par des applications dans différents domaines (santé, énergie, transports, finance, gouvernement, enseignement, etc). Le consortium entend aussi influencer la standardisation de la QKD. Et évidemment, dans la mesure du possible, de contribuer au développement de l'offre industrielle européenne en QKD et technologies associées.

En France, la zone de test sera la région parisienne et ses grands laboratoires de recherche avec l'Institut d'Optique, Telecom Paris, le LIP6 à Jussieu et les labs de Nokia à Villarceau. Le projet a bénéficié d'un financement européen Horizon 2020 de 15M€, indépendamment du Quantum Flagship.

Quittons l'Europe et passons aux USA. Les premières expériences y étaient menées à Boston par la **DARPA** entre 2004 et 2007. Un réseau QKD piloté par **Batelle** était testé dans l'Ohio en 2013[998]. Des tests avaient aussi été réalisés en 2015 au **MIT** pour relier entre eux deux sites distants de 43 km.

Un déploiement commercial de QKD sur un réseau de fibre optique inutilisé de 800 km reliant Boston à Washington DC est aussi en déploiement par **Quantum Xchange** et **Zayo**, pour connecter des sociétés financières de Wall Street avec leur backoffice dans le New Jersey. Il utilise des répéteurs sécurisés (« trusted node technology")[999].

---

[996] Voir Université Côte d'Azur et Orange collaborent pour la mise en place d'une expérimentation en matière de cryptographie quantique, mai 2019. Et pour les projets d'Orange en QKD en général : Orange et les technologies quantiques pour la sécurité des échanges de données, juin 2020.

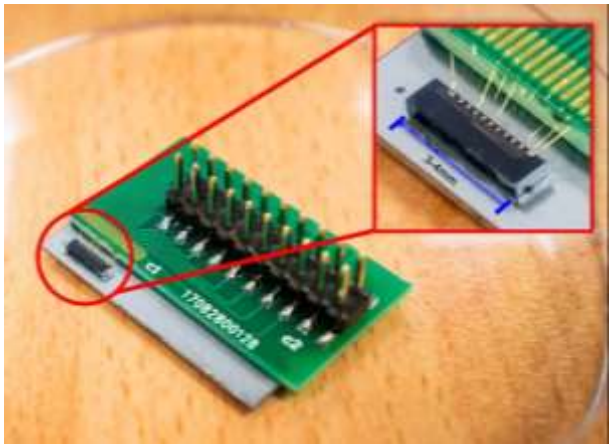
[997] Voir L'Europe se dote d'une infrastructure de télécommunications quantiques par Rémy Decourt, décembre 2019 et Nine more countries join initiative to explore quantum communication for Europe, décembre 2019.

[998] Voir Battelle Installs First Commercial Quantum Key Distribution Protected Network in U.S., 2013.

[999] Voir New plans aim to deploy the first US quantum network from Boston to Washington, DC, octobre 2018. Source du schéma: From MIT : Semiconductor Quantum Technologies for Communications and Computing, 2017, 32 slides).

Une installation de 85 km était aussi déployée à Chicago en 2019[1000]. En juillet 2020, le Département de l'Energie US annonçait élargir ce réseau de QKD pour relier tous ses sites des laboratoires de recherche[1001].

Au Japon, **Toshiba** annonçait en septembre 2018 une solution de QKD codéveloppée avec la Tohoku Medical Megabank Organization (ToMMo) de la l'Université de Tohoku avoir atteint un débit supérieur à 10 Mbits/s pendant un mois d'envoi de clés QKD.



L'un des enjeux du déploiement de la QKD est la miniaturisation de ses composants. Alors qu'il fallait au départ un rack complet de matériel pour les stations d'émission/réception de clés quantiques, on peut maintenant tout faire rentrer dans un composant de photonique de quelques mm de long. C'est ce qu'ont réalisé en 2019 des chercheurs de NTU à Singapour pour gérer de la CV-QKD à même de supporter des infrastructures de fibre existantes d'opérateurs télécoms[1002]. Mais la miniaturisation en question ne concerne ici que la partie photonique. Le circuit doit être complété par des composants électroniques classiques.

Le développement de tels composants de photonique intégrés sera aussi soutenu dans le cadre de projets européens Horizon Europe qui succéderont sur la période 2021-2027 aux projets Europe 2020.

Déploiements en Chine

Ce sont les Chinois qui se font le plus remarquer avec des démonstrations et projets destinés à marquer les esprits. Comme nombre de pays, la Chine investit dans les QKD pour des raisons de souveraineté et pour protéger ses communications sensibles. Un premier déploiement avait été réalisé en 2012 dans la zone d'Hefei pour relier diverses entités du gouvernement chinois[1003].

Il a eu ensuite la mise en place d'une liaison par fibre optique sécurisée par QKD entre Shanghaï et Beijing, faisant 2000 km. La ligne installée entre 2013 et 2016 a été déployé par la startup chinoise **QuantumCTek**. Le réseau comprend 32 répéteurs dont l'accès physique est sécurisé[1004]. En effet, l'atténuation du signal est trop forte au-delà d'une cinquantaine de km sur une fibre optique.

[1000] Voir Argonne and UChicago scientists take important step in developing national quantum internet par Louise Lerner, février 2020.

[1001] Voir Department of Energy (DOE) Unveils Blueprint for a U.S. Quantum Internet par Doug Finke, juillet 2020.

[1002] Voir Researchers create quantum chip 1,000 times smaller than current setups, octobre 2019 qui fait reference à An integrated silicon photonic chip platform for continuous-variable quantum key distribution par G. Zhang et al, décembre 2019 (5 pages).

[1003] Voir Unhackable Chinese Communication Network Launches Soon, de Rechelle Ann Fuertes, 2017.

[1004] Source : Security assessment and key management in a quantum key distribution network par Xiongfeng Ma, juin 2019 (21 slides).

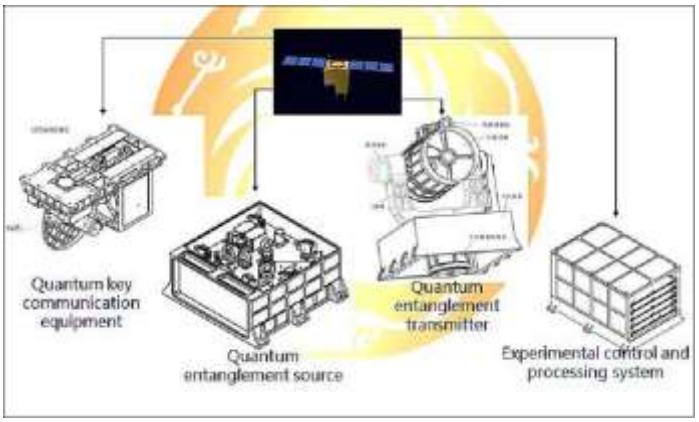
Les entités exploitant cette ligne sont des banques, des agences gouvernementales dont diverses agences de régulation du secteur financier. Le pays envisage aussi de protéger ses infrastructures de grid énergétique avec ce réseau[1005].

La Chine ne s'arrêtait pas là et lançait en 2017 un plan de déploiement de 33 000 km supplémentaires devant se dérouler jusqu'en 2025, le **National Quantum Secure Communication Backbone Network**.

Il avait démarré avec la création d'une liaison Hefei-Wuhan, et sans rapport avec le covid-19[1006]. Hefei est la ville où se situe le grand laboratoire quantique de Jian Wei-Pan.

QKD par satellite et avec drones

La seconde performance chinoise concerne l'usage du satellite **Micius** aussi dénommé **Mozi et QUESS** (Quantum Experiments at Space Scale) pour téléporter des états quantiques de photons par voie optique en 2017, à 1400 km de distance entre le satellite et la Terre, à 5100 m d'altitude dans la préfecture de Ngari dans le Tibet chinois[1007]. Le satellite pèse 640 kg et consomme 560W.



Mais cette expérience présentait des limites : elle permettait de gérer 5,9 millions de paires de photons intriqués par seconde, mais du fait des corrections d'erreurs, seulement une paire de photon utile était exploitable par seconde[1008].

Une communication de clé quantique QKD a ensuite été réalisée en utilisant un procédé différent, en 2018, entre la Chine et l'Autriche pour mener une vidéo-conférence sécurisée par cette clé (*ci-dessous*)[1009]. Pourquoi donc avec l'Autriche ? Parce que Jian-Wei Pan, le pape du quantique Chinois à l'origine de cette expérience a fait sa thèse de doctorat en Autriche sous la supervision d'Anton Zeilinger, qui pilotait la partie européenne de l'expérience !

[1005] Voir Application In Power Industry Promotes the Development of Quantum Cryptography Technology par Yonghe Guo, juin 2019 (13 slides).

[1006] Voir Towards large-scale quantum key distribution network and its applications par Hao Qin, 2019 (17 slides).

[1007] Les détails sont dans Ground-to-satellite quantum teleportation, 2017 (16 pages). Le principe a été décrit pour la première fois en 1993 dans Teleporting an Unknown Quantum State via Dual Classical and EPR Channels de Charles Bennett, Gilles Brassard (de Montréal), Claude Crépeau (un français de Normale Sup), Richard Jozsa, Asher Peres et William Wootters. Voir aussi Quantum Communication at 7,600km and Beyond de Chao-Yang Lu et Cheng-Zhi Peng, Jian-Wei Pan, novembre 2018.

[1008] Voir A step closer to secure global communication par Eleni Diamanti, Nature, juin 2020, qui décrit les conditions et limites pratiques de ces expériences de transmission de clés par satellite. Et en particulier la plus récente décrite dans Entanglement-based secure quantum cryptography over 1,120 kilometres par Juan Yin et al, Nature, juin 2020. L'expérience générait un débit d'envoi de clé pas vraiment phénoménal de 0,12 bits par secondes.

[1009] Des projets d'expériences ou expériences équivalents ont été lancés par des équipes européennes et françaises. Voir Quantum Photonics Technologies for Space, octobre 2018 (22 pages) et Nanobob CubeSat mission 2018 (31 pages). Cela fait aussi des émules au Royaume Uni où un projet expérimental de micro-satellites Cubesat est prévu pour couvrir le pays. Voir QUARC: Quantum Research Cubesat — A Constellation for Quantum Communication par Luca Mazzarella et al, 2020 (27 pages).

Début 2020, la Chine annonçait avoir miniaturisé sa station de réception terrestre pour la communication de clés quantiques avec le satellite Micius, passant de 10 tonnes à 80 kg. Le débit d'envoi des clés est réduit, passant de 40Kbits/s à 4-10Kbits/s. L'expérience avait lieu côté Terre à Jinan et Shanghai, donc semble-t-il au niveau de la mer[1010]. La Banque de Chine sécuriserait déjà des transactions par l'envoi de clés via le satellite Micius/Mozi Beijing et des provinces éloignées.

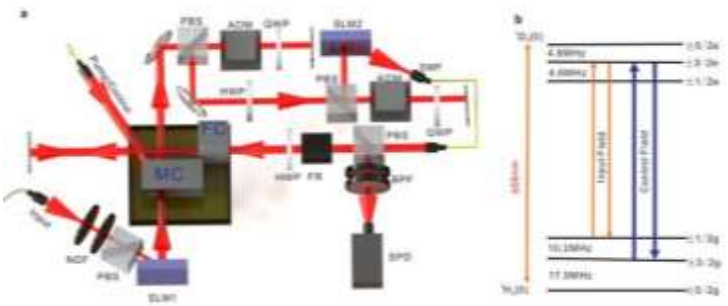
En juin 2019, des chercheurs chinois annonçaient avoir démontré la mise en œuvre de liaisons optiques QKD aériennes établies au sein d'un réseau de drones octocoptères de 35 kg espacés de 200 m pendant un vol de 40 mn à 100 m d'altitude[1011]. La charge utile gérant la communication quantique était de 11,8 kg. Elle reste miniaturisable, l'ambition des chinois étant de l'intégrer dans des drones grand-public. On imagine les impacts de cette technologie dans leur société de la surveillance continue des citoyens.

Répéteurs de QKD

Qu'en est-il donc des répéteurs, indispensables pour distribuer des clés quantiques sur de grandes distances, au-delà de 80 km [1012]? Des chercheurs chinois ont créé une connexion en fibre en QKD de 404 km sans répéteur[1013], mais à cette distance les taux d'erreurs sont tellement élevés que cela ne sert pas à grand-chose. Il existe des technologies de répéteurs quantiques pour fibres optiques à l'état de la recherche fondamentale mais avec quelques limitations[1014]. On en serait déjà à la troisième génération de ces répéteurs mais ils seraient déjà hackables[1015]. La recherche pour les fiabiliser est donc une priorité.

Ces répéteurs sont dotés de mémoire quantique pour répliquer l'état des photons à transmettre. C'est aussi l'objet de travaux de l'équipe de **Nicolas Gisin** de l'Université de Genève (et ID Quantique) accompagné d'une équipe du CNRS en France. Ils s'appuient sur une terre rare, l'ytterbium[1016].

Dans la même veine, des chercheurs du **Key Lab of Quantum Information** de l'Académie des Sciences chinoise publiaient en août 2018[1017] une étude sur la création de mémoires quantiques à base d'ions de terre rare (de praséodyme) dopés à trois degrés de liberté, pilotable par envoi de photons (schéma de l'expérience *ci-contre*).



Cette technique pourrait servir à la fois à la création de répéteurs pour des réseaux de QKD et pour créer des mémoires quantiques pour ordinateurs quantiques à base d'optique linéaire.

[1010] Voir China has developed the world's first mobile quantum satellite station par Donna Lu, janvier 2020..

[1011] Voir Drone-based all-weather entanglement distribution, Hua-Ying Liu et al, mai 2019 (16 pages) et World's First "Quantum Drone" for Impenetrable Air-to-Ground Data Links Takes Off de Charles Q. Choi, IEEE Spectrum.

[1012] Sachant que le record de distance de télécommunication quantique sans répéteurs est de 509 km comme nous l'avons déjà vu. Voir sinon Viewpoint: Record Distance for Quantum Cryptography de Marco Lucamarini, Toshiba & Cambridge, novembre 2018 et Recent progress on Measurement-Device-Independent (MDI) Quantum Key Distribution (QKD), Marco Lucamarini, 2018 (71 slides).

[1013] Documentée dans Measurement device independent quantum key distribution over 404 km optical fibre, 2016 (15 pages).

[1014] Voir Tutorial on quantum repeaters de Rodney Van Meter et Tracy Northup, 2019 (178 slides), Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, 2018 (5 pages) et An Information-Theoretic Framework for Quantum Repeaters de Roberto Ferrara, 2018 (144 pages).

[1015] Selon The network impact of hijacking a quantum repeater 2018 (23 pages).

[1016] Selon Ytterbium: The quantum memory of tomorrow, juillet 2018.

[1017] Voir Multiplexed storage and real-time manipulation based on a multiple-degree-of-freedom quantum memory, 2018 (9 pages).

En juillet 2019, des chercheurs chinois annonçaient enfin avoir réussi à expérimenter une technologie de répéteurs « photoniques » à base d'interféromètres à 12 photons et permettant de se passer de mémoire quantique. Cela les rend théoriquement très sécurisés[1018].

Mi-2019, d'autres chercheurs chinois présentaient une nouvelle prouesse : la téléportation de qutrits, permettant de transmettre quantiquement plus d'information par photons[1019]. Cela pourrait notamment servir à augmenter le débit de la transmission de clés en QKD. D'autres débouchés sont aussi envisageables dans des domaines très différents comme celui des radars quantiques qui sont évoqués page 526.

Sécurisation de la QKD

La sécurisation d'une chaîne dépend de ses maillons les plus faibles et ici, ce sont les émetteurs et les récepteurs avant même qu'ils n'échangent via une QKD. Par ailleurs, les QKD ne sont pas la panacée car elles dépendent d'une liaison point à point et pas d'une technique de routage permettant d'emprunter plusieurs chemins. Cela pourrait aboutir à une forme de déni de service par blocage de la communication physique employée[1020].

Attack	Target component	Tested system
Distinguishability of decoy states A. Huang et al., Phys. Rev. A **98**, 012330 (2018)	laser in Alice	3 research systems
Intersymbol interference K. Yoshino et al., poster at QCrypt (2016)	intensity modulator in Alice	research system
Laser damage V. Makarov et al., Phys. Rev. A **94**, 030302 (2016); A. Huang et al., poster at QCrypt (2018)	any	5 commercial & 1 research systems
Spatial efficiency mismatch M. Rau et al., IEEE J. Sel. Top. Quantum Electron. **21**, 6600905 (2015); S. Sajeed et al., Phys. Rev. A **91**, 062301 (2015)	receiver optics	2 research systems
Pulse energy calibration S. Sajeed et al., Phys. Rev. A **91**, 032326 (2015)	classical watchdog detector	ID Quantique
Trojan-horse I. Khan et al., presentation at QCrypt (2014)	phase modulator in Alice	SeQureNet
Trojan-horse N. Jain et al., New J. Phys. **18**, 123030 (2014); S. Sajeed et al., Sci. Rep. **7**, 8403 (2017)	phase modulator in Bob	ID Quantique
Detector saturation H. Qin, R. Kumar, R. Alleaume, Proc. SPIE 8899**0**N (2013)	homodyne detector	SeQureNet
Shot-noise calibration P. Jouguet, S. Kunz-Jacques, E. Diamanti, Phys. Rev. A **87**, 062313 (2013)	classical sync detector	SeQureNet
Wavelength-selected PNS M.-S. Jiang, S.-H. Sun, C.-Y. Li, L.-M. Liang, Phys. Rev. A **86**, 032310 (2012)	intensity modulator	(theory)
Multi-wavelength H.-W. Li et al., Phys. Rev. A **84**, 062308 (2011)	beamsplitter	research system
Deadtime H. Weier et al., New J. Phys. **13**, 073024 (2011)	single-photon detector	research system
Channel calibration N. Jain et al., Phys. Rev. Lett. **107**, 110501 (2011)	single-photon detector	ID Quantique
Faraday-mirror S.-H. Sun, M.-S. Jiang, L.-M. Liang, Phys. Rev. A **83**, 062331 (2011)	Faraday mirror	(theory)
Detector control I. Gerhardt et al., Nat. Commun. **2**, 349 (2011); L. Lydersen et al., Nat. Photonics **4**, 686 (2010)	single-photon detector	ID Quantique, MagiQ, research systems

Le schéma *ci-contre* inventorie tout un tas de vulnérabilités de la QKD, une partie ayant été comblée depuis[1021].

La cryptographie est fascinante pour la vitesse à laquelle des dispositifs de sécurité peuvent être cassés par des chercheurs avant même d'avoir été déployés en masse. Ainsi les QKD seraient vulnérables du fait d'une vulnérabilité d'implémentation associée au théorème de Bell qui peut être traitée avec des détecteurs de meilleure qualité[1022]. C'est une course sans fin !

QKD et Blockchain

Autre exemple, ce projet d'utiliser les QKD pour sécuriser une Blockchain. C'est évidemment délicat à déployer de bout en bout à grande échelle. En effet, les utilisateurs de Blockchain n'ont pas une liaison satellite en montagne ou une fibre sécurisée sous la main, ne serait-ce que lorsqu'ils sont mobiles. Mais soit.

C'est la proposition d'Evgeny Kiktenko du "Russian Quantum Center" de Moscou[1023], ainsi que de Del Rajan et Matt Visser de l'Université Victoria de Wellington en Nouvelle Zélande[1024].

[1018] Voir Scientists Firstly Realize All-photonic Quantum Repeater, juillet 2019 et Experimental quantum repeater without quantum memory de Zheng-Da Li et al, 2019.

[1019] Voir Qutrits experiments are a first in quantum teleportation, par Daniel Garisto dans Scientific American, août 2019, qui fait référence à Experimental multi-level quantum teleportation par Xiao-Min Hu et al, avril 2019 (12 pages) et Quantum teleportation in high dimensions par Yi-Han Luo, juin 2019 (23 pages).

[1020] Au sujet des vulnérabilités de la QKD et des méthodes pour les éviter, voir QKD Measurement Devices Independant Joshua Slater, 2014 (83 slides).

[1021] Voir Certification of cryptographic tools, par Vadim Makarov du Quantum Hacking Lab de Moscou, 2019 (15 slides).

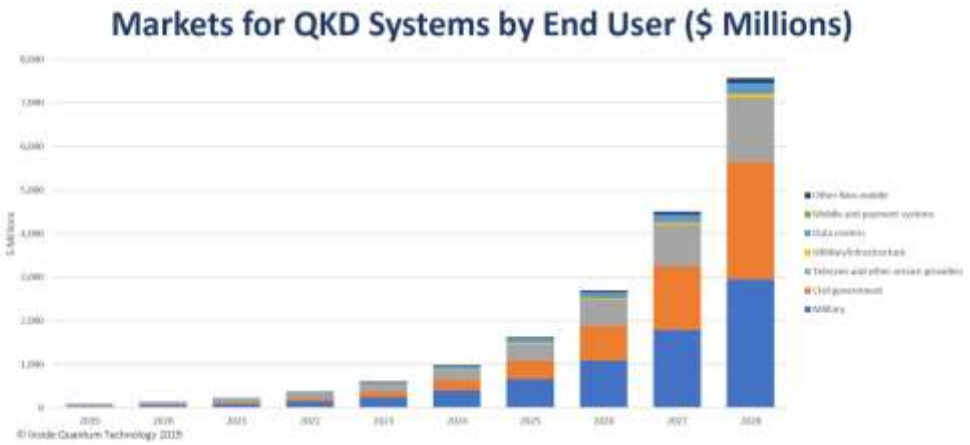
[1022] C'est comme documenté par Jonathan Jogenfors dans Breaking the Unbreakable Exploiting Loopholes in Bell's Theorem to Hack Quantum Cryptography, 2017 (254 pages).

[1023] Documenté dans First Quantum-Secured Blockchain Technology Tested in Moscow, juin 2017.

Au juste, pourquoi ne protège-t-on pas l'ensemble des données transmises avec le même principe que la QKD ? Ce qui s'y oppose semble être la limitation en débit du procédé.

Marché et standards

Qu'en est-il de la taille du marché de la QKD ? L'analyste **Inside Quantum Technology** (UK) en faisait une estimation avec un premier milliard de dollars atteint en 2024, puis une croissance exponentielle allant jusqu'à $7B en 2028[1025].



La Chine est aussi très active pour définir une batterie de standards de la QKD[1026]. L'ITU travaille aussi sur les standards de la QKD, mais la France n'y est pas vraiment représentée dans le board du groupe de travail[1027]. L'Europe est mieux représentée dans les travaux de standardisation menés à l'ISO, à l'IEEE, à l'ETSI et au CEN-CENELEC, le comité européen de normalisation en électronique et électrotechnique.

Cryptographie post-quantique

La protection physique de l'envoi de clés symétriques n'est pas facilement applicable de manière généralisée, ne serait-ce que parce qu'elle impose une liaison optique (directe ou par fibre optique) entre émetteurs et récepteurs. Ce qui, par exemple, ne fonctionne pas avec les liaisons radio comme avec les smartphones. Too bad !

L'objectif que se sont donnés les spécialistes est donc de créer et exploiter des systèmes capables de résister aux assauts des ordinateurs quantiques et en particulier aux algorithmes de Shor (factorisation d'entiers mais aussi logarithme discret) et de Grover (recherche brute) sans protection quantique de la liaison physique. Le décryptage de messages chiffrés - sans les clés privées - doit être un problème NP-Complet ou NP-Difficile pour résister aux assauts futurs du quantique.

La Post-Quantum Cryptography (PQC) est en quelque sorte concurrente de la Quantum Key Distribution (QKD) même si certains les jugent complémentaires. Et elle est certainement plus facile à déployer à grande échelle car elle est indépendante des infrastructures physiques utilisées pour les télécommunications. Mais on peut toutefois les combiner en envoyant des clés publiques de PQC via des liaisons physiques en QKD.

Les différents systèmes de PQC se distinguent par de nombreux paramètres et présentent des compromis différents entre taille de signature, vitesse de traitement pour le chiffrement et le déchiffrement et par la taille de la clé publique.

[1024] Dans Quantum Blockchain using entanglement in time, 2018 (5 pages).

[1025] Voir The Future of the Quantum Internet A Commercialization Perspective par Lawrence Gasman, juin 2019 (11 slides) ainsi que The Future of the Quantum Internet A Commercialization Perspective, par Lawrence Gasman d'Inside Quantum Technology, juin 2019 (11 slides). Vu dans l'ITU Workshop on Quantum Information Technology for Networks.

[1026] Voir Introduction of Quantum secured Communication Standardization in CCSA par Zhangchao Ma, juin 2019 (16 slides) et An overview of current quantum information technology (QIT) standardization par Wei Qi, juin 2019 (13 slides).

[1027] Voir ITU-T Focus Group on Quantum Information Technology for Networks (FG-QIT4N), 2019.

La chronologie mérite le détour pour sa dimension “long terme” [1028]:

- **1978** : le premier algorithme résistant aux ordinateurs quantiques est créé par l’Américain **Robert McEliece** (détails plus loin) avant même que Richard Feynman évoque l’idée de créer des ordinateurs quantiques.
- **2003** : Le terme de “post quantum cryptography” (PQC) est créé par l’Américain Daniel Bernstein[1029].
- **2006** : le premier workshop international **PQCrypto** se tient en mai en Belgique pour étudier les moyens de contourner les attaques d’ordinateurs quantiques à une époque où l’on peut à peine faire fonctionner deux qubits ensemble. Le programme consiste à trouver des successeurs aux algorithmes de cryptographie à clés publique RSA et ECC qui résistent au quantique[1030]. Le comité de programme de 12 personnes comprend trois français : Louis Goubin de Université de Versailles ainsi que Phong Nguyen et Christopher Wolf de l’ENS. Dès cette première édition, quatre des cinq piliers de la PQC sont établis avec la code-based crypto, les lattice codes, hash Lamport signature et multivariate cryptography. Les isogénies arriveront plus tard. Deux français interviennent pour proposer deux de ces quatre pistes : Nicolas Sendrier, de l’Inria, avec "Post-quantum code-based cryptography" et Jacques Stern de l’ENS avec "Post-quantum multivariate-quadratic public key schemes."[1031]. Ces workshops ont depuis lieu tous les uns à deux ans un peu partout dans le monde. L’édition 2013 avait eu lieu à Limoges.
- **2012** : le NIST (National Institute for Standards & Technologies), qui cumule les activités couverte par l’AFNOR et le LNE français, lançait ses premiers projets et une équipe sur la PQC.
- **2014** : l’**Union Européenne** lançait un appel à projets dans le cadre d’Horizon 2020 sur la PQC. Au même moment, l’ETSI qui est l’organisme européen de standardisation des télécoms, lançait aussi son groupe de travail sur la PQC.

[1028] Sachant que j’en ai extrait un bout dans Quantum cryptanalysis – the catastrophe we know and don’t know de Tanja Lange, une des spécialistes du sujet et chercheuse aux Pays Bas, 2017 (33 slides).

[1029] Daniel Bernstein est l’auteur avec Johannes Buchmann et Erik Dahmen de l’imposant ouvrage Post-Quantum Cryptography en 2009 (254 pages) qui pose bien les enjeux de la PQC.

[1030] Les actes sont ici : https://postquantum.cr.yp.to/pqcrypto2006record.pdf.

[1031] Source : Quantum Computing and Cryptography Today de Travis L. Swaim, University of Maryland University College (22 pages).

- **2015** : le NIST organisait son premier workshop sur la PQC. L'ETSI publiait un document de référence sur la PQC[1032]. La NSA se réveillait et déclarait que le passage à la PQC allait devenir une priorité[1033]. La NSA joue à chaque fois dans deux cours : elle veut se protéger et protéger les communications sensibles de l'Etat US avec de bons systèmes de chiffrement mais en même temps conserver des capacités à décrypter les communications commerciales standards et celles des autres pays. Cela repose sur la force brute de supercalculateurs géants et une forte asymétrie de moyens techniques. Cette asymétrie pourrait très bien disparaître avec les ordinateurs quantiques qui, sommes-toutes, seront peut-être bien plus abordables que les supercalculateurs géants. En 2015, le projet Européen PQCrypto coordonné par Tanja Lange est lancé[1034].
- **2016** : le NIST publie un rapport d'étape sur la PQC (15 pages) et une roadmap de standardisation associée. C'est aussi le lancement du programme d'Investissement d'Avenir RISQ (**R**egroupement de l'**I**ndustrie française pour la **S**écurité Post-**Q**uantique) qui comprend outre divers laboratoires (CEA, CNRS, INRIA, UMPC), des entreprises privées comme CryptoExperts, CS, Secure-IC et Thalès. Ils ont fait des soumissions de propositions de standards au NIST en 2017. RISQ est piloté par Secure-IC.
- **2017** : fin des soumissions de propositions de standardisation de PQC au NIST. Fin 2017, 69 candidats étaient acceptés parmi 82 candidats, principalement avec des réseaux euclidiens (lattice codes) et des codes de correction d'erreur (code based PQC). La même année avait lieu le 8eme workshop PQCrypto à Utrecht aux Pays-Bas.
- **2019** : 26 candidats étaient sélectionnés par le NIST en février pour passer à la seconde étape dont 17 candidats pour des solutions de chiffrement à base de clés publiques et 9 pour des signatures[1035].

  Parmi ces projets se trouvent trois projets où est impliqué Worldline, qui faisait partie jusqu'à 2019 du groupe Atos. L'Inria était de son côté impliquée dans 7 projets sur les 26 retenus[1036].

Second Round Candidates

BIKE	LEDAcrypt	Rainbow
Classic McEliece	LUOV	ROLLO
CRYSTALS-DILITHIUM	MQDSS	Round5
CRYSTALS-KYBER	NewHope	RQC
FALCON	NTRU	SABER
FrodoKEM	NTRU Prime	SIKE
GeMSS	NTS-KEM	SPHINCS+
HQC	Picnic	Three Bears
LAC	qTESLA	

- **2020** : résultats du troisième tour de sélection de candidats du NIST en juillet qui retient 15 candidats sur les 26 de la phase précédente. Cette sélection comprend 7 équipes finalistes pour cette étape et 8 équipes qui proposent des solutions de moins bonne qualité devant être encore évaluées. Le NIST prévoit d'organiser un quatrième tour de sélection d'ici 2021.
- **2022/2024** : publication prévue de drafts de standards de PQC par le NIST.

[1032] Voir Quantum Safe Cryptography and Security (64 pages).

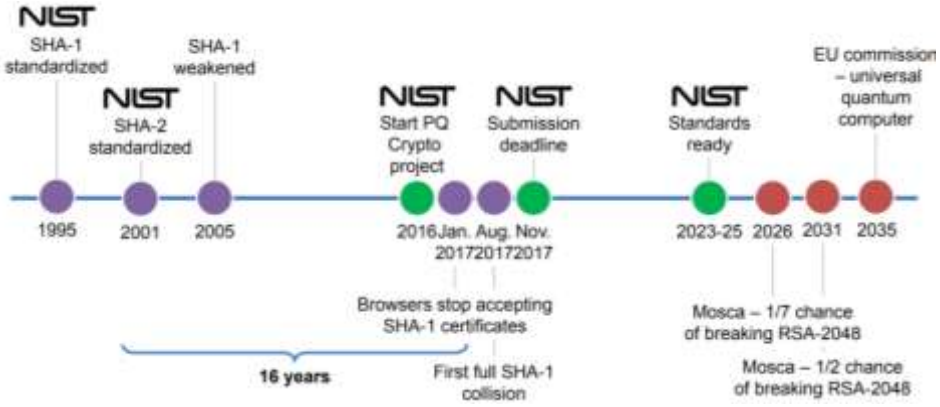
[1033] Voir Commercial national security algorithm suite and quantum computing FAQ IAD (11 pages).

[1034] Il est documenté dans Post-Quantum Cryptography for Long-Term Security (10 pages).

[1035] Voir NIST Post-Quantum Cryptography - A Hardware Evaluation Study, 2019 (16 pages) et Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process 2019 (27 pages) et Voir Recent Developments in Post Quantum Cryptography de Tsuyoshi Takagi, novembre 2018 (38 slides).

[1036] Voir Cryptographie post-quantique : forte présence d'Inria dans une compétition internationale, mai 2019. Ils sont gérés par quatre équipes : ARIC, SECRET, POLSYS et GRACE et dans quatre des catégories de systèmes de cryptographie PQC : réseaux euclidiens, isogénies, codes de correction d'erreur et systèmes polynomiaux multivariés.

- **2025** : échéance que s'est donné le NIST pour finaliser les standards de la PQC aux USA. Les déploiements de ces standards démarreront avec la commercialisation rapide de solutions logicielles supportant ces standards. Rapide pour la simple raison que les candidats sont souvent issus de consortiums comprenant des acteurs privés de cet écosystème. Certains ont déjà des tests en cours de leurs solutions.



source : Introduction to post-quantum cryptography and learning with errors, Douglas Stebila, 2018 (106 slides).

Les standards en lice de la PQC sont dans cinq catégories distinctes que voici. Je ne vais pas pouvoir les décrire convenablement dans leur dimension mathématique sauf pour la première catégorie[1037]. Nous évoquerons le cas de quelques startups qui s'attaquent à ce marché dans la dernière partie de cette rubrique sur la cryptographie.

Table 2 - Comparison on encryption schemes (RSA decryption = 1, size in bits, k security strength)

Algorithm	KeyGen (time compared to RSA decrypt)	Decryption (time compared to RSA decrypt)	Encryption (time compared to RSA decrypt)	PubKey (key size in bits to achieve 128 bits of security)	PrivateKey (key size in bits to achieve 128 bits of security)	Cipher text (size of resulting cipher text)	Time Scaling	Key Scaling
NTRU	5	0.05	0.05	4939	1398	4939	k^2	k
McEliece	2	0.5	0.01	1537536	64861	2860	k^2	k^2
Quasi-Cyclic MDPC McEliece	5	0.5	0.1	9857	19714	19714	k^2	k
RSA	50	1	0.01	3072	24.576	3072	k^3	k^2
DH	0.2	0.2	0.2	3072	3238	3072	k^3	k^2
ECDH	0.05	0.05	0.05	256	256	512	k^2	k

Note: in key scaling, the factor log k is omitted.

source : Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges, ETSI, 2015 (64 pages).

Mais les entreprises établies ne sont pas en reste. **Atos** et **Thalès** s'y intéressent en France. **IBM** annonçait en août 2019 un système d'archivage d'information sur banque magnétique qui intègre une cryptographie post-quantique[1038]. Ils utilisent un chiffrement à base de réseaux euclidiens. Comme il s'agit généralement de stockage long terme, il faut bien conserver le logiciel de déchiffrement sur la même durée pour éviter de se retrouver avec un tas de données non réutilisables.

[1037] Voir notamment de la vulgarisation du sujet dans A Guide to Post-Quantum Cryptography, par Ben Perez, octobre 2018.

[1038] Voir IBM's quantum-resistant magnetic tape storage is not actually snake oil, par Kevin Coldewey dans TechCrunch, août 2019.

IBM est aussi impliqué des trois des consortiums qui ont répondu à l'appel à proposition du NIST. **Kudelski Security** (Suisse) s'intéresse aussi à la PQC.

En France, l'**ANSSI** publiait en mai 2020 une note d'information où elle affichait une certaine réticente face à la QKD[1039]. Elle mettait en avant le fait qu'elle ne traite pas un problème courant, ne peut pas garantir une inviolabilité parfaite et nécessite des infrastructures dédiées optiques. Elle recommande plutôt de s'intéresser aux solutions à venir de cryptographie asymétrique de type PQC. Cela faisait suite à un mémo à teneur équivalente de leurs homologues britanniques du NCSC publié en avril 2020[1040].

Code-based cryptography (EN) ou codes linéaires aléatoires (FR)

Ce système de cryptographie inventé en 1978 par **Robert McEliece**, bien avant l'existence de la menace de l'algorithme de Shor, a résisté depuis à toutes les attaques de cryptanalyse, soit classiques soit conçues avec des algorithmes quantiques. C'est le plus ancien des codes PQC qui était même "PQC" avant l'heure. La méthode consiste à multiplier les données à encrypter représentées sous forme de vecteurs binaires par une matrice publique et statique avec plus de colonnes que de lignes, elle aussi binaire qui est un "*code de Goppa binaire"*.

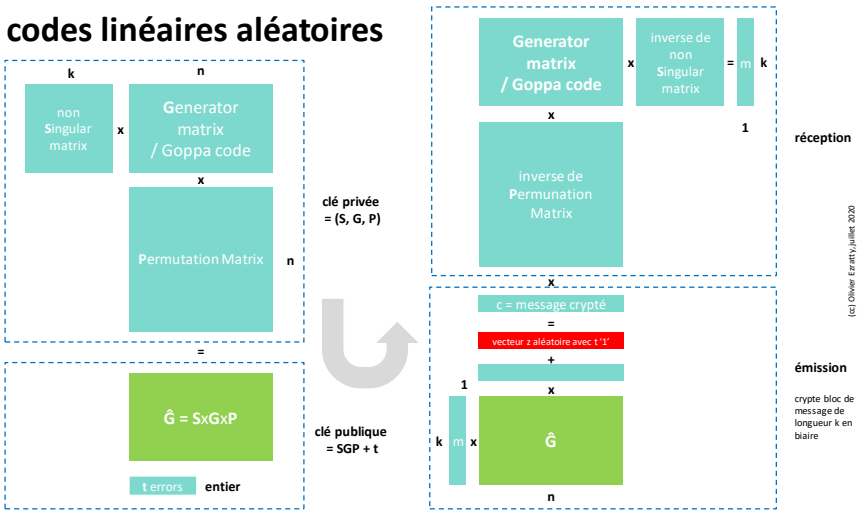
Allons donc. Cette multiplication génère un vecteur plus grand que le vecteur d'origine. On lui ajoute ensuite un vecteur binaire qui ajoute des erreurs aléatoires au résultat mais de nombre constant. Les spécialistes le décrivent comme un "*uniformly random word of weight t*" ce qui n'est pas bien clair pour le néophyte, et qui fournit un exemple de plus du manque de pédagogie de certains. En langage un peu plus naturel, il s'agit d'une série de bits aléatoire contenant un nombre fixe "t" de 1 que l'on appelle le poids de Hamming.

La clé publique envoyée par le récepteur à l'émetteur est la matrice et ce nombre d'erreurs t. Ce sont les composantes génératrices de la matrice qui constituent la clé privée. En effet, cette matrice est la multiplication de trois matrices dites SGP pour "non singular", "generator matrix / Goppa code" et "permutation matrix". Le décodage du message utilise des inverses de la matrice S et de la matrice P, et la matrice G.

[1039] Voir L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés ? par ANSSI, mai 2020 (6 pages).

[1040] Voir Quantum Security Technologies, NCSC, mars 2020 (4 pages) et une réponse circonstanciée dans Quantum safe cryptography - the big picture – Fact Based Insight par By David Shaw, 2020.

C'est assez alambiqué et j'ai essayé de représenter cela graphiquement dans le schéma *ci-contre*. La matrice G permet de supprimer les "t" erreurs introduites dans la phase de chiffrement. Elle est conçue pour cela au moment de la création des clés. Par contre, allez comprendre dans la phase d'émission l'effet mathématique de cette matrice de correction d'erreur au message à transmettre avant l'ajout de la dite erreur !



Ce système génère des clés publiques cent fois plus grande qu'avec RSA, de l'ordre de 80 Ko. Et si on veut réduire leur taille, cela génère des vulnérabilités. L'avantage est une bonne vitesse de chiffrement et de déchiffrement des messages. On peut même l'accélérer en utilisant un composant électronique dédié de type FPGA[1041].

Casser ce genre de chiffrement est un problème NP-Hard (NP-difficile) inaccessible au quantique à ce jour même si, pour résister au quantique, il faudrait une clé assez grande, de 1 Mo[1042].

Lattice-based cryptography (EN) ou réseaux euclidiens (FR)

La technique a été proposée par le Hongrois Miklos Ajtai, chercheur chez IBM, en 1996, mise en œuvre dans un système à base de clé publique en 2005 par Oded Regev avec son système LWE (Learning with errors) et améliorée depuis par de nombreux chercheurs.

La littérature sur le sujet est complètement inabordable pour les non spécialistes. Il n'est pas évident de comprendre le fonctionnement de cette méthode de chiffrement malgré l'élégance des schémas qui présentent la notion de réseau euclidien comme celui *ci-dessous*[1043]. En gros, c'est une matrice de points qui permet de repérer des points en fonction de leurs coordonnées selon un repère de vecteurs différents entre la clé publique et la clé privée.

Une erreur est ajoutée aux coordonnées générées avec le vecteur de la clé publique.

[1041] Comme vu dans Code-Based Cryptography for FPGAs de Ruben Niederhagen, 2018 (73 slides).

[1042] La résistance de cette méthode aux attaques est documentée dans Code-Based Cryptography de Tanja Lange, 2016 (38 slides). Pour en savoir plus, voir aussi Code Based Cryptography d'Alain Couvreur, 2018 (122 slides) et Some Notes on Code-Based Cryptography, une thèse de Carl Löndahl, 2014 (192 pages).

[1043] Source : On the Security of Lattice-Based Cryptography Against Lattice Reduction and Hybrid Attacks, de Thomas Wunderer, 2018 (188 pages).

Seuls les vecteurs de coordonnées de la clé privée permettent de retrouver la coordonnée de la valeur chiffrée. Bon, c'est ce que j'ai compris ! Initialement, elle souffrait de problèmes de performances mais des solutions efficaces sont apparues comme NTRU, créé en 1998 par Jeffrey Hoffstein, Jill Pipher et Joseph Silverman. L'avantage de la méthode est d'utiliser des clés publiques de petite taille. Son décryptage est un problème NP-complet inaccessible aux ordinateurs quantiques. Dans les inconvénients, c'est une méthode protégée par de nombreux brevets, donc propriétaire et potentiellement couteuse[1044].

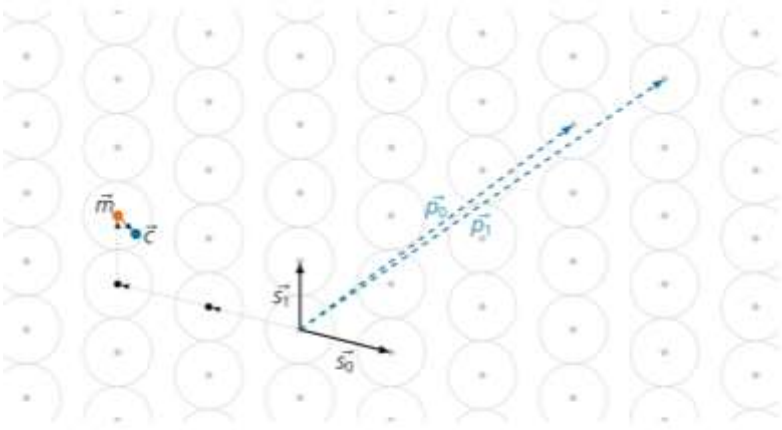


Figure 3.2: Example for lattice-based encryption in a two-dimensional lattice: The secret, well-formed base is $\{\vec{s_0}, \vec{s_1}\}$; the public, "scrambled" base is $\{\vec{p_0}, \vec{p_1}\}$. The sender uses $\{\vec{p_0}, \vec{p_1}\}$ to map the message to a lattice point $\vec{m}$ and adds an error vector to obtain the point $\vec{c}$. The point $\vec{c}$ is closer to $\vec{m}$ than to any other lattice point. Therefore, the receiver can use the well-formed secret base $\{\vec{s_0}, \vec{s_1}\}$ to easily recover $\vec{m}$ (dotted vectors); this is a hard computation for an attacker who only has the scrambled base $\{\vec{p_0}, \vec{p_1}\}$. For a secure scheme, the dimension of the lattice must be much higher than 2 as in this example.

C'est dans cette classe de méthodes que l'on peut ranger la solution de PQC **New Hope** (CECPQ1) qui a été testée en 2016 pendant quelques mois par **Google** dans Chrome et qui s'appuie sur Ring-LWE. Depuis 2019, ils sont passés à CECPQ2 qui comprend une variante du système d'échange de clés HRSS qui fait partie des soumissionnaires au concours du NIST[1045] et des sélectionnés de la dernière vague, dans le projet NTRU.

En France, une équipe du laboratoire de l'IRISA-EMSEC développe une solution de cryptographie à base de réseaux euclidiens.

Isogeny-based cryptography (EN) ou isogénie (FR)

Cette variante des courbes elliptiques est encore moins facile à appréhender que tout ce qui précède. En français, c'est un "*morphisme de groupe surjectif et de noyau fini entre deux courbes elliptiques*.". Fastoche ! Le système a été proposé en 2006 par Alexander Rostovtsev et Anton Stolbunov puis cassé par cryptoanalyse quantique par Andrew Childs, David Jao et Vladimir Soukharev. Ce qui a conduit David Jao et Luca de Feo (Inria) à proposer en 2011 l'utilisation de courbes "supersingulières" pour corriger cette faille[1046].

A noter le fait que l'éditeur de logiciels **Cloudflare** a sorti une solution de sécurité en open source s'appuyant sur les isogénies, CIRCL (Cloudflare Interoperable Reusable Cryptographic Library). Elle est publiée sur GitHub. Leur solution d'encapsulation de clés SIKE a été soumise au NIST dans son appel d'offre de solutions de cryptographie post-quantique.

[1044] Pour en savoir plus, voir la thèse Lattice-based cryptography : a practical implementation, de Michael Rose, 2011 (103 pages), Lattice-based Cryptography de Daniele Micciancio et Oded Regev, 2008 (33 pages) et le tantinet plus pédagogique mais tout de même incompréhensible Overview of Lattice based Cryptography from Geometric de Leo Ducas, 2017 (53 slides).

[1045] Voir Experimenting with Post-Quantum Cryptography, par Matt Braithwaite, juillet 2016. Puis Google starts CECPQ2, a new postquantum key exchange for TLS, janvier 2019.

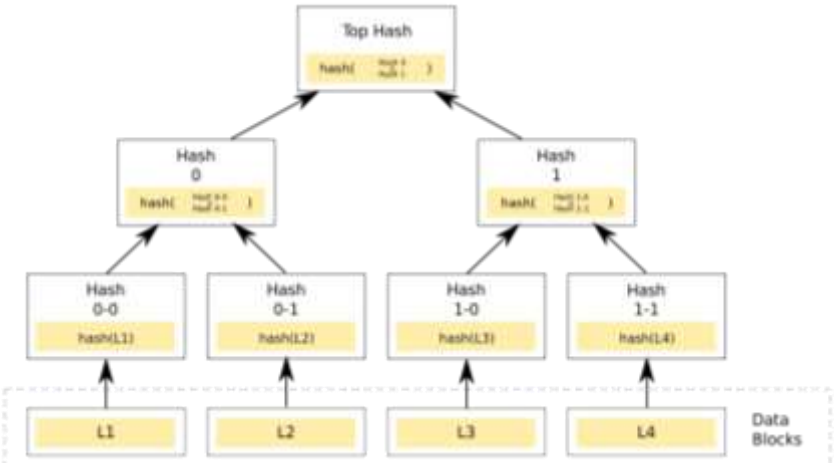
[1046] Pour en savoir plus si le cœur vous en dit, voir 20 years of isogeny-based cryptography de Luca De Feo, 2017 (84 slides), An introduction to supersingular isogeny-based cryptography, de Craig Costello (Microsoft Research), 2017 (78 slides), Isogeny Graphs in Cryptography de Luca De Feo, 2018 (73 slides) ou encore An introduction to isogeny-based crypto de Chloe Martindale, 2017 (78 slides).

Ils faisaient partie en janvier 2019 des 17 candidats finalistes pour les solutions de chiffrement à clés publiques ou de création de clés[1047].

Hash-based signatures (EN) ou arbres de hashage (FR)

Cette autre méthode de cryptographie post-quantique est aussi antérieure à la notion même d'ordinateur quantique imaginée par Richard Feynman en 1982, puisqu'elle repose sur les travaux de Leslie Lamport du SRI en 1979 et ses "signatures" à base de hash à usage unique.

La méthode a été ensuite améliorée en utilisant des arbres de hashage aussi appelé arbres de Merkle pour signer plusieurs messages.



source : Merkle Tree, Wikipedia.

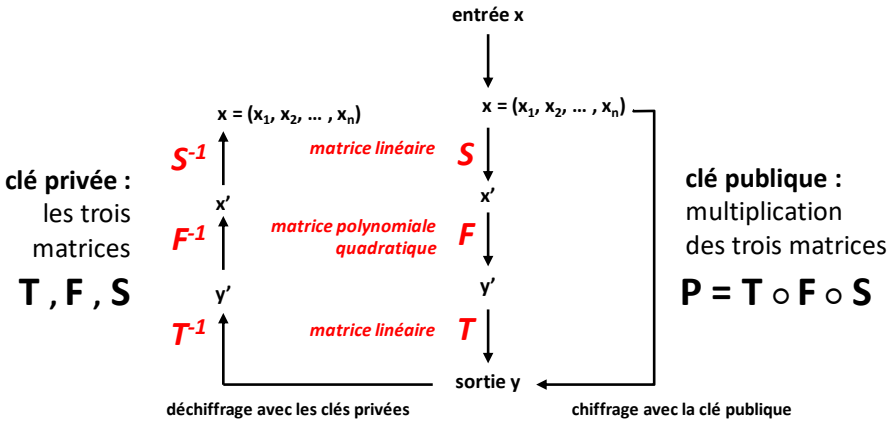
Le tout s'appuie sur des clés publiques de taille réduite, descendant à 1 kbits. Cette méthode est surtout utilisée pour de la signature électronique[1048].

Multivariate polynomial cryptography (EN) ou inversion de polynômes multivariés (FR)

Ce dernier groupe de méthodes fait penser aux codes de correction d'erreurs. La clé publique est une multiplication de plusieurs matrices dont deux sont linéaires et une quadratique (avec des valeurs au carré), les trois matrices séparées constituant la clé privée qui sert à reconstituer le message chiffré.

Le décryptage (donc, par des pirates) est un problème NP-Difficile, hors de portée des ordinateurs quantiques, sinon la méthode ne ferait pas partie de cet inventaire, pardi.

La méthode date de 2009 et a évidemment été ensuite déclinée sous plusieurs variantes.



Les clés publiques sont assez grandes, allant par exemple jusqu'à 130 Ko (avec la variante HFE-Boost)[1049]. Cette méthode de chiffrement est plutôt utilisée pour les signatures électroniques.

[1047] Voir Cloudflare wants to protect the internet from quantum computing, juin 2019 et Introducing CIRCL: An Advanced Cryptographic Library, juin 2019.

[1048] Pour en savoir plus si vous êtes un crack des maths et de la crypto, voir notamment Hash-based Signatures: An Outline for a New Standard (12 pages), Design and implementation of a post-quantum hash-based cryptographic signature scheme de Guillaume Endignoux, 2017 (102 pages) et SPHINCS: practical stateless hash-based signatures, 2015 (30 pages).

[1049] A noter la contribution de Jacques Stern de l'ENS "Post-quantum multivariate-quadratic public key schemes" lors de PQCRYPTO 2006.

En préparant cette partie, j'imaginais que l'on pouvait combiner de la QKD (protection physique de la distribution de clés) et de la PQC (protection logique du chiffrement contre le décryptage par ordinateur quantique). En fait, pas vraiment. La QKD est plutôt dédiée aux algorithmes à clés symétriques qui supposent une protection de la communication physique entre correspondants tandis que la PQC s'appuie sur des clés publiques qui n'ont donc pas besoin d'être protégées par QKD car leur interception (sans la QKD) ne servirait déjà à rien à des pirates.

On peut cependant combiner de la QKD pour l'échange de clés avec de la cryptographie post-quantique pour l'authentification et le chiffrement des données. La QKD a besoin d'authentification qui peut être assurée en amont par de la PQC. Par contre, la QKD peut être redondante avec de la PQC utilisée pour l'échange de clés[1050].

Cryptographie homomorphe quantique

La cryptographie homomorphe consiste à chiffrer des données qui peuvent ensuite traverser un traitement classique en mode chiffré et donner un résultat chiffré qui sera déchiffrable à la fin du traitement.

Dans le machine learning et le deep learning, ce mode de chiffrement permet de distribuer dans le cloud des traitements d'entraînement et d'inférence de modèles de machine learning sans que le piratage des données transmises permette de révéler le contenu de données qui alimentent le modèle.

L'inconvénient de cette méthode est qu'elle ne fonctionne pas avec tous les modèles de machine learning et qu'elle est très couteuse en temps machine pour le chiffrement et le déchiffrement des données.

Le chiffrement homomorphe quantique relève de la même démarche pour chiffrer des données qui vont alimenter un ordinateur quantique, dans le cloud, et déchiffrer ensuite le résultat des traitements. C'est l'un des outils qui permet de mettre en œuvre ce que l'on appelle le « blind computing » dans le cloud, où les serveurs ne peuvent pas comprendre et interpréter les données qu'ils traitent.

Divers algorithmes de chiffrement de programmes de contrôle de portes quantiques ont été proposés mais ne sont pas encore couramment utilisés[1051]. Une partie des clés peut être transmise de manière quantique à l'instar d'une QKD. C'est d'ailleurs l'une des conditions pour être sûr que la partie serveur ne puisse par interpréter les traitements qu'elle réalise[1052].

Chez les constructeurs d'ordinateurs quantiques, on considère qu'une suite de portes quantiques pilotant un processeur quantique est déjà difficile à interpréter dans l'absolu !

Télécommunications quantiques

Comme indiqué au début de cette longue partie, la cryptographie quantique à base de QKD n'est pas la seule application du champ des télécommunications quantiques[1053].

[1050] Pour en savoir plus sur la PQC, voir notamment Post-quantum cryptography – dealing with the fallout of physics success de Daniel Bernstein et Tanja Lange, 2017 (20 pages) et Le grand défi du post-quantique de Jean-Charles Faugère, 2018.

[1051] Voir Classical Homomorphic Encryption for Quantum Circuits, de Urmila Mahadev, 2018 (7 pages), Quantum Fully Homomorphic Encryption With Verification, 2017 (30 pages et slides, 28 slides), Quantum Homomorphic Encryption: A Survey, 2017 (11 pages) et Quantum homomorphic encryption for circuits of low T-gate complexity par Anne Broadbent et Stacey Jeffery, 2015 (35 pages).

[1052] Comme l'indique On the implausibility of classical client blind quantum computing de Scott Aaronson, Elham Kashefi et al, 2017 (43 pages).

[1053] Voir l'excellent Quantum internet: A vision for the road ahead par Stephanie Wehner et al, octobre 2018 (11 pages).

Nous l'avons déjà vu plus tôt dans cet ouvrage, les télécommunications quantiques n'ont pas pour objet de transmettre de l'information plus vite que la lumière[1054]. Cette limite peut cependant être contournée dans certains cas où l'information reste quantique de bout en bout de la chaîne et n'est pas lue de manière classique.

L'un des domaines d'applications est la création de réseaux quantiques reliant des « endpoints » eux-mêmes quantiques qui pourraient être des ordinateurs quantiques ou même des capteurs quantiques. Dans le premier cas, les liens entre ordinateurs quantiques permettraient de créer des architectures de calcul distribuées, à l'instar des architectures de calcul distribuées qui existent sur Internet, dans les data-centers et dans les supercalculateurs. A ceci près que si on pouvait créer de tels réseaux, l'emplacement physique des calculateurs serait moins important que dans les calculs classiques. En effet, le mécanisme de l'intrication utilisé pourrait s'affranchir des distances, tout du moins tant que l'on serait dans la portée des fibres optiques sans passer par des répéteurs.

Par ailleurs, un lien direct entre calculateurs quantiques et télécommunications quantiques présenterait d'énormes avantages en termes de sécurisation des traitements. Cela fait notamment partie du concept de « blind computing » sur lequel Elham Kashefi a beaucoup travaillé, en co-créant en 2009 le protocole BFK (pour Anne Broadbent / Joe Fitzsimons / Elham Kashefi) [1055].

Le principe consiste à préparer les traitements de manière quantique au point de départ et de l'envoyer par une liaison quantique par téléportation à l'ordinateur quantique à distance.

C'est un peu l'équivalent en quantique du chiffrage homomorphe utilisé dans le machine learning. Une manière de gérer la confidentialité des traitements est de partitionner le traitement sur plusieurs ordinateurs quantiques

La communication entre calculateurs quantiques n'est cependant pas une mince affaire. Il faudrait pouvoir en effet convertir l'état de qubits de ces machines en états quantiques de photons dans l'infrarouge pour les transmettre optiquement.

Or, mis à part le cas des calculateurs à base de photons, les qubits sont le plus souvent des états d'électrons ou d'atomes. D'où les nombreux efforts qui visent à permettre ces conversions[1056].

Dans les qubits supraconducteurs, on sait convertir l'état d'un qubit en micro-ondes. Mais celles-ci sont dans le domaine des 6-8 GHz, pas dans le domaine de l'infrarouge. Il faut donc les convertir d'une gamme de fréquence à l'autre tout en conservant l'état quantique combinant la bonne proportion des deux états de base du qubit. On peut aussi réaliser cette conversion avec des mécanismes opto-électro-mécaniques[1057].

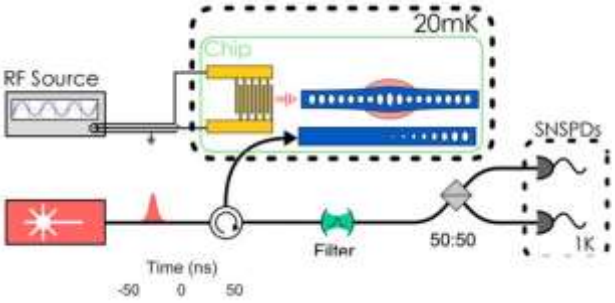
[1054] Voir No, We Still Can't Use Quantum Entanglement To Communicate Faster Than Light par Ethan Siegel, février 2020.

[1055] Voir Universal blind quantum computation de Anne Broadbent, Joseph Fitzsimons et Elham Kashefi, 2008 (20 pages) et la présentation associée (25 slides), Blind quantum computing can always be made verifiable de Tomoyuki Morimae, 2018 (5 pages), Experimental Blind Quantum Computing for a Classical Client, 2017 (5 pages) et Blind Quantum Computation de Charler Herder (5 pages).

[1056] Voir par exemple Milestone Experiment Proves Quantum Communication Really Is Faster, de Kevin Hartnett, Quanta Magazine, décembre 2018, qui fait référence à Experimental demonstration of quantum advantage for one-way communication complexity, de Niraj Kumar, Iordanis Kerenidis et Eleni Diamanti, décembre 2018 (12 pages) ainsi que One step closer to complex quantum teleportation de l'Université de Vienne, novembre 2018.

[1057] Voir aussi A quantum microwave-to-optical transducer par Thibaut Jacqmin du LKB, 2019 (17 slides) qui décrit des mécanismes opto-électro-mécaniques de conversion d'état de qubits supraconducteurs en photons transportables sur fibre optique.

C'est ce qu'ont réalisé expérimentalement des chercheurs de Delft fin 2018, à une température de 20 mK qui est voisine de celle des qubits supraconducteurs (schéma *ci-contre*)[1058].



Les ions piégés et les atomes froids sont contrôlés par des lasers, mais convertir leur état quantique en photon n'est pas une mince affaire non plus. Les qubits silicium utilisent le spin d'un ou de deux électrons. On fait alors des conversions spin-to-charge puis charge-to-photon.

Les recherches dans ces domaines progressent pas à pas, et pivotent essentiellement autour de la photonique et de l'interaction photons-matière[1059].

Deux autres domaines doivent progresser pour permettre le déploiement de réseaux de télécommunications quantiques : les répéteurs, les switchs[1060] et la mémoire quantique[1061].

Des chercheurs chinois ont réussi en 2019 à intriquer deux mémoires quantiques à base d'atomes de rubidium via des photons à une distance de 50 km[1062]. Ça avance !

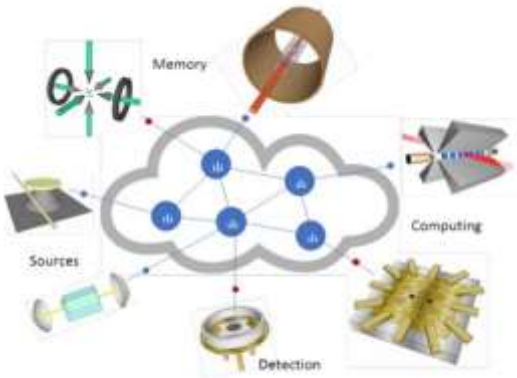


Fig. 11. Quantum internet.

D'autres applications des télécommunications quantiques sont à citer en plus du calcul distribué :

- La **transmission de données anonymes**. Elle permet à deux nœuds d'un réseau quantique de communique entre eux sans qu'il soit possible à l'un des nœuds d'identifier l'autre nœud. Les communications ne laissent pas de trace et ne sont donc pas auditables. Cela remplace les proxy d'anonymisation classiques. Cela peut servir de base à des traitements distribués, en couplant cela avec un chiffrage des données classiques ou quantique. C'est un moyen d'assurer l'anonymisation de la transmission de données comme des données de sondage ou de santé.
- Les **signatures électroniques quantiques** qui permettent d'authentifier des messages classiques. Elles sont transférables à des tiers, non répudiables et non forgeables.

[1058] Voir New horizons for connecting future quantum computers into a quantum network, octobre 2019 qui fait reference à Microwave-to-optics conversion using a mechanical oscillator in its quantum ground state par Moritz Forsch et al, 2019 (11 pages).

[1059] Voir par exemple First chip-to-chip quantum teleportation harnessing silicon photonic chip fabrication par l'Université de Bristol, décembre 2019 qui fait référence à Chip-to-chip quantum teleportation and multi-photon entanglement in silicon par Daniel Llewellyn et al, 2019 (48 pages). Et la version exagérée dans La première "téléportation quantique" entre deux puces informatiques a eu lieu par Valentin Cimino, décembre 2019.

[1060] Voir Development of Quantum InterConnects (QuICs) for Next-Generation Information Technologies par David Awschalom et al, 2019 (31 pages) et Quantum Switch for the Quantum Internet: Noiseless Communications Through Noisy Channels, 2020 (14 pages).

[1061] Voir ce panorama général de l'usage des mémoires quantiques dans les réseaux quantiques : Optical Quantum Memory and its Applications in Quantum Communication Systems par Lijun Ma et al du NIST, 2020 (13 pages). Le schéma de cette parge sur le Quantum Internet en est issu.

[1062] Voir Nouveau record : des chercheurs ont enchevêtré de la mémoire quantique sur plus de 50 kilomètres par Stéphanie Schmidt, février 2020. La prouesse vient du laboratoire de Jian-Wei Pan de Hefei en Chine. Cela fait référence à l'article publié dans Nature : Entanglement of two quantum memories via fibres over dozens of kilometres pa Jian-Wei Pan et al, février 2020 et auparavant sur Arxiv en mars 2019 : Entanglement of two quantum memories via metropolitan-scale fibers (19 pages).

- La **monnaie quantique** qui applique un concept de Stephen Wiesner (1942, Israélien) de 1970 mis en forme en 1983. Elle s'appuie sur des tokens d'intégrité vérifiable et qui ne peuvent être utilisés qu'une seule fois.

Startups et PMEs des télécommunications et de la cryptographie quantiques

Passons maintenant en revue les startups de ce vaste secteur d'activité de la cryptographie quantique et post-quantique, en essayant de bien décrire la nature de leur offre et de leur différenciation lorsque l'information est publiquement disponible ! Je n'ai conservé ici que les startups proposant des solutions technologies et pas intégré les sociétés de conseil et d'intégration.

Notons que du côté taille de marché, celui de la cryptographie quantique et post-quantique est pour l'instant modeste. Un rapport de 2017 l'évaluait à $2,5B d'ici 2022[1063].

Il devrait cependant monter en puissance à partir de cette période, après la finalisation de la standardisation par le NIST et par l'ETSI.

Hors startups, des offres commerciales de crytographie quantique et post-quantique sont aussi proposées ou sur le point d'être proposées par divers acteurs industriels tels que Batelle, Infineon, Raytheon, IBM, Cisco, Atos, Gemalto, Microsoft[1064], NEC, Toshiba, Huawei[1065], KT et Samsung.

AgilePQ (2014, USA) fournit une plateforme logicielle de sécurisation "post-quantum" de la communication entre objets connectés et le cloud, comme des drones.

[1063] Voir New CIR Report States Quantum Encryption Market To Reach $2.5 Billion Revenues By 2022: Mobile Systems Will Ultimately Dominate, 2017.

[1064] Voir le site de Microsoft qui décrit leur activité dans la PQC.

[1065] Voir Continuous-Variable Quantum Key Distribution with Gaussian Modulation, the Theory of Practical Implementations, 2018 (71 pages). L'équipe de Huawei qui planche sur la QKD est en partie située dans leur centre de recherché de Dusseldorf.

Il comprend AgilePQ C-code un bout de logiciel qui fonctionne sur les micro-contrôleurs d'objets connectés et consomme peu d'énergie et de l'autre, AgilePQ DEFEND, un système de génération de clé de taille adaptable. DEFEND génère des codes qui sont plus difficiles à casser que l'AES 256 et avec 429 ordres de grandeur de différence. Précisément, on passe d'un espace de clés de 10 puissance 77 à 8*10 puissance 506 (factorielle de 256)[1066]. Le système qui est breveté semble être une variante de codes linéaires aléatoires mais avec des clés de taille raisonnable.

Il a été soumis à la standardisation au NIST et s'interface avec les systèmes de contrôle et de supervision SCADA (Supervisory control and data acquisition). La société est partenaire de Microsoft Azure. Pour une startup, ses dirigeants et fondateurs n'ont pas l'air bien jeunes, mais ils ont de l'expérience !

Agnostiq (2018, Canada) est une startup issue de l'accélérateur Creative Destruction Lab de Toronto qui développe des solutions de cryptographie pour sécuriser les informations et traitement quantiques gérés via des ressources en cloud.

ArQit (2016, UK**)** développe une QKD distribuée dans le cloud avec une distribution de clé via des satellites en orbite basse, qui pourraient bien être remplacés par une infrastructure terrestre.

CAILabs (2013, France, 16,7M€) est une société basée à Rennes issue du LKB de l'ENS Paris qui commercialise de l'équipement en photonique et en particulier des systèmes de multiplexage multimode spatiaux pour fibres optiques supportant jusqu'à 45 nœuds.

C'est ce qui permet de démultiplier le débit des fibres optiques des réseaux des opérateurs télécoms. Ils ont notamment le Japonais KDDI comme client. La startup est dirigée par Jean-François Morizur (CEO) et Guillaume Labroille (CTO) avec Nicolas Treps du LKB comme conseiller scientifique.

Ciena (1992, USA) est un équipementier dans le domaine des télécommunications optiques. Ils intègrent les offres d'IDQ dans leurs solutions, et en particulier, leurs générateurs de clés aléatoires optiques.

Bien que n'ayant pas encore d'offre structurée de QKD, ils s'intéressent de près à sa standardisation. Ils participent notamment à la Quantum Alliance Initiative lancée en 2018 aux USA par le Hudson Institute, un think tank conservateur, qui œuvre dans ce sens et créé des propositions de standards pour la QKD et la QRNG (quantum random number generation).

Crypta Labs (2013, UK, $300K) développe des solutions de chiffrement post-quantiques adaptées aux objets connectés. Ils proposent notamment un générateur de nombres aléatoire quantique intégrable dans un mobile (comme IDQ). Ils travaillent de concert avec l'Université de Bristol.

Crypto4A Technologies (2016, Canada) propose une solution de chiffrement à base de génération de nombres aléatoires.

Elle comprend un serveur appliance de format 19 pouces QAOS de génération de nombre aléatoire entropique (en ne précisant pas la technologie employée) et un autre qui génère du chiffrement de type PQC, "quantum safe", le Q_xEdge Hardware Security Module (HSM). Le module de génération de PQC est dénommé QASM (Quantum Assured Security Module) qui fait doublon avec le langage de développement quantique du même nom.

[1066] Voir AgilePQ DEFEND Cryptographic Tests (11 pages).

Il s'appuie sur des signatures basées sur du hashage (HBS) quantum safe. Ces appliances sont équipés de quatre chipsets Intel Core i7, de 16 Go de mémoire et 256 Go de SSD et tournent sous une version durcie de Linux. Ils supportent les algorithmes certifiés par la NSA aux USA ("suite B") et les futurs standards de PQC du NIST.

CryptoExperts (2008, France) est une startup qui développe une offre de chiffrage homomorphe et de cryptographie post-quantique et qui propose aussi des services autour de ces technologies.

CryptoMathic (1986, Danemark) développe des générateurs de clés aléatoires quantiques.

CryptoNext Security (2019, France) est une startup qui développe une solution de cryptographie post-quantique fondée par Ludovic Perret (CEO, ex Inria) et Jean-Charles Faugères (CTO, ex LIP6 Sorbonne).

Ils ont notamment Philippe Duluc (Atos) et Denis Mercier (ex Otan) dans leur board. Leur solution logicielle est développée en langage C et en assembleur pour des questions de performance. Elle associe des polynômes multivariés et du hashage. Leur solution peut s'intégrer dans des schémas RSA/ECC par hybridation.

CryptoNext est aussi l'une des équipes françaises ayant soumis une proposition de PQC au NIST américain. Avec un bémol car le NIST demande à ce qu'il n'y ait pas de brevets sur les algorithmes qui seront retenus. Les processeurs de standardisation de la PQC passent en pratique par de nombreux organismes tels que l'ISO, ITU (X509), IETF (TLS) et ETSI (algorithmes). Leur PQC devrait s'intégrer dans la solution de blockchain CORDA de R3 qui est destinée aux banques. A noter que les Chinois organisent également un processus concurrent du NIST avec un calendrier de sélection plus rapide que celui du NIST. A noter qu'ils équipent les forces spéciales françaises avec leur PQC, s'exécutant sur des mobiles sécurisés tournant sous Android.

Crypto Quantique (2015, UK) est une startup qui propose une solution de cryptographie destinée à sécuriser la communication avec des objets connectés. Elle exploite un chipset qui est installé dans l'objet. C'est un « processeur quantique » en technologie silicium qui sert à générer une clé d'identification unique de l'objet, inclonable et inviolable. Il exploite probablement de la photonique avec un générateur de nombres aléatoires similaire aux technologies du Suisse IDQ.

Leur technologie s'appelle Quantum Driven Physically Unclonable Function (QD-PUF) mais ils n'expliquent rien sur son fonctionnement exact ni sur le modèle de chiffrement utilisé[1067]. La startup faisait partie de l'accélérateur de Thales à Station F dans la promotion démarrant en septembre 2018. Les fondateurs sont d'origine iranienne, italienne et grecque, un beau patchwork. Ils visent des marchés divers allant de l'automobile à la finance.

evolutionQ (2015, Canada) est une startup qui se distingue surtout par le pédigrée de son créateur, Michele Mosca, un spécialiste Italien de la cryptographie post-quantique.

[1067] Voir Physically Unclonable Functions: a Study on the State of the Art and Future Research Directions.de Roel Maes et Ingrid Verbauwhede (36 pages) et Quantum readout of Physical Unclonable Functions, de B. Skoric (21 pages).

C'est aussi le fondateur de l'Institut for Quantum Computing de l'Université de Waterloo au Canada. La société fait ce que l'on appelle du service outillé pour accompagner les entreprises dans l'adoption de cryptographie post-quantique et quantique. Cela commence par un produit d'évaluation du risque quantique ("Quantum Risk Assessment") qui comporte six phases, documentées dans A Methodology for Quantum Risk Assessment, publié en 2017. Est-ce vraiment un produit ? Cela ressemble surtout à une méthodologie à mettre en œuvre avec des consultants. Le reste est de la même crème avec des services d'intégration et de formation pour faire évoluer les systèmes de cryptographie de l'entreprise.

fragmentiX (Autriche) propose un système de gestion sécurisé du stockage de données qui utilise la technique de la fragmentation et de la distribution de données sur des supports physiques différents.

Le tout est fourni sous forme d'appliances. Les données distribuées sont évidemment chiffrées mais de manière classique. Ils utilisent une technologie qui provient de l'Austrian Institute of Technology. C'est une autre manière de créer une protection des données résistante à l'algorithme de Shor. Ce n'est pas la seule société positionnée sur ce créneau.

HaQien (2019, Inde) conçoit des solutions de cryptographie post-quantique (PQC). Mais ce n'est pas bien clair car ils semblent aussi utiliser un générateur de nombre aléatoires pour créer des clés classiques.

IDQ (ID Quantique) (2001, Suisse, $6,5M, acquise par SK Telecom en 2018 pour $65M) est l'une des plus anciennes sociétés du secteur, créée par le chercheur Suisse Nicolas Gisin, spécialiste de la photonique et de l'intrication quantique. La société propose une offre complète de générateurs de nombres aléatoires et de gestion de QKD.

Son générateur de nombres aléatoires Quantis, déjà décrit au début de cette partie, est complété par Cerberis, une solution de QKD pour protéger la circulation des clés de chiffrement en rack 6U et Centauris, une gamme de serveurs de chiffrement supportant des liaisons optiques de 100 GBits/s. Ce serveur à base de FPGA supporte pour l'instant des systèmes à base de courbes elliptiques ainsi que de l'AES-256, dans l'attente de la standardisation des protocoles de PQC (post-quantum-crypto)[1068].

La startup appartient depuis début 2018 au groupe coréen SKT Invest qui est la branche de Corporate Venture de **SK Telecom**. Le fonds a investi $65M dans la startup dans ce qui est pudiquement présenté comme un partenariat alors que c'est une prise de contrôle.

L'offre de QKD d'IDQ est notamment déployée en Corée pour protéger le backbone 5G de l'opérateur SK Telecom.

[1068] Dans L'arme anti-NSA de la France, sabordée en 2010 ?, de Guerric Poncet dans Le Point, 2013, est racontée l'histoire de SmartQuantum, une startup française spécialisée dans la QKD et fermée en 2010. Son créateur s'y plaint de l'influence néfaste de Thales qui aurait bloqué son développement. Neuf ans plus tard, le marché de la QKD ne fait que démarrer. Dans le meilleur des cas, SmartQuantum était juste un peu trop en avance de phase par rapport à la maturité de ce marché. Et ce n'est pas une société américaine qui est devenue leader, mais le Suisse IDQ.

Ils sont aussi partenaires de Toshiba à Cambridge ainsi que dans le projet OpenQKD. La société employait plus de 100 personnes en juin 2019.

InfiniQuant (2017, Allemagne) est une spin-off du Max Planck Institute for the Science of Light. Ils mettent au point une CV-QKD utilisable sur fibre optique et liaison satellite.

Cette technique utilise une modulation d'amplitude en plus d'une modulation de phase pour transmettre les clés quantiques. La startup travaille aussi sur un générateur de nombres aléatoire quantique, concurrent de ceux d'IDQ.

Infotecs (1991, Russie) est un spécialiste de la cybersécurité historiquement spécialisé dans la création de VPN.

Il développe une solution de PQC depuis 2016, avec une communication maladroite qui pourrait la faire passer pour de la QKD[1069]. Mais ils développent bien des solutions de QKD. En 2018, ils lançaient ainsi leur "ViPNet Quantum Phone", exploitant leur VPN ViPNet (ViPNet Client et ViPNet Connect) et une solution matérielle de QKD développée à l'Université de Moscou. Ce qu'ils appellent un "phone" est en fait un PC doté d'un boitier externe avec une liaison en fibre optique le connectant à un serveur de clé QKD[1070].

ISARA (2015, Canada, $1,6M de CA en 2017) développe des solutions logicielles de chiffrement post-quantiques et du conseil de mise en œuvre de PQC. Leur produit est la "ISARA Radiate Security Solution Suite" qui fournit des clés publiques et algorithmes de chiffrement non attaquables par des ordinateurs quantiques du futur.

Ils s'appuient visiblement sur des arbres de hashage et associent de la PQC (post-quantum crypto) et de la PKI (public-key infrastructure) traditionnelle[1071]. L'un de leurs investisseurs est le fonds Quantum Valley Investments, géré notamment par Mike Lazaridis, le cofondateur de Blackberry RIM. Ce dernier est une sorte de Xavier Niel canadien, ayant réinvesti sa fortune liée à Blackberry dans le développement de l'écosystème scientifique et entrepreneurial canadien, en particulier dans le quantique où il a investi en tout $450M (source).

KETS Quantum Security (2016, UK, £2M) développe un générateur de nombres aléatoire (QRNG = quantum random number generator) et un générateur de clé quantique QKD, le tout intégré dans une photonique miniaturisée dans un simple composant.

Le tout est combiné à une activité de conseil pour le déploiement des solutions. La société a été créée par des chercheurs en photonique de l'Université de Bristol. Ils ciblent les marchés financiers et du secteur public.

Ils prototypent des drones avec Airbus pour la mise en place de QKD dans des domaines militaires ou de sécurité publique, avec Airbus Defense. Leur chipset QKD peut aussi équiper des micro-satellites type Cubesat.

[1069] Voir Infotecs At The Forefront Of Quantum Cryptography, 2017.

[1070] Voir Infotecs has presented its ViPNet Quantum Phone, janvier 2018.

[1071] C'est documenté dans le livre blanc Enabling Quantum-Safe Migration with Crypto-Agile Certificates, 2018 (7 pages).

Magiq (1999, USA) est une startup qui s'était lancé initialement en 2003 dans la création d'un système de QKD. Depuis une dizaine d'année, cette société semble s'être repositionnée dans le service et pour la défense US. Ils ont développé l'Agile Interference Mitigation System (AIMS), un système de réduction d'interférences de communications électromagnétiques.

MtPellerin (2018, Suisse) est une startup spécialisée dans la gestion de crypto-assets via une application mobile dédiée (« Bridge Wallet »). Ils ont créé un coffre-fort sécurisé quantique avec IDQ, le « The Quantum Vault », qui s'appuie sur le générateur de nombres aléatoires et le système de QKD d'IDC.

NuCrypt (2003, USA) développe des technologies optiques pour les communications et la métrologie quantiques, notamment des sources de photons intriqués, des générateurs d'impulsions optiques, des détecteurs de photons uniques, des analyseurs de polarisation et des logiciels associés.

Nu Quantum (2018, UK) développe des solutions matérielles de sécurité quantique, probablement autour de la QKD. C'est une spin-off du Cavendish Lab de l'Université de Cambridge. Ils ont créé leur propre source de photons uniques, mais pas discernable comme celle de Quandela. La startup est cofondée et dirigée par l'Espagnole Carmen Palacios-Berraquero.

Origone (2014, UK) est une étrange startup basée au Royaume-Uni après avoir été située à Paris (jusqu'à sa liquidation en France en 2017) qui développe des solutions de cryptographie en s'appuyant notamment sur les ordinateurs de D-Wave. Elle vise notamment le marché de la défense ainsi que le ferroviaire. Leur activité de cryptographie quantique/post-quantique est une évolution d'une activité dans la cybersécurité classique.

PicoQuant (1996, Allemagne) est une PME de Berlin spécialisée en photonique et qui commercialise notamment des compteurs de photons ainsi que des lasers à diodes. Mais ils sont ici parce qu'ils proposent aussi un générateur de nombres aléatoire quantique, le PQRNG 150, avec un débit de 150 Mbits/s. Il est bien moins miniaturisé que le composant générateur de nombres aléatoires intégré dans le Galaxy 5G de Samsung annoncé en mai 2020.

Post-Quantum ou **PQ Solutions** (2009, UK, $10,4M) est une startup initialement créée sous l'appellation SRD Wireless qui avait créé la messagerie sécurisée PQ Chat utilisant les codes linéaires aléatoires inventés par Robert McEliece.

La société a été renommée en Post-Quantum ou PQ Solutions Limited en 2014. Ils proposent une ligne de produits de sécurisation intégrant des algorithmes de crypto post-quantique. L'un des cofondateurs Martin Tomlinson, a développé le préencodage Tomlinson-Harashima qui permet de corriger les interférences dans les signaux de télécommunications et divers codes de correction d'erreur. Leurs produits comprennent aussi notamment PQ Guard, un système de chiffrement post-quantique.

PQSecure Technologies (2017, USA) est un fournisseur de solutions de PQC à base d'isogénies. C'est une spin-off de l'Université de Floride Atlantique lancée par Reza Azarderakhsh. Leur algorithme SIKE fait partie des finalistes de l'appel à projet de PQC du NIST.

PQShield (2018, UK, $6,9M) est une spin-off de l'Université d'Oxford qui développe des solutions de PQC. Ils collaborent avec des équipes finalistes du concours de solutions de PQC lancé par le NIST. Ils ont développé un SoC (system on chip) vendu sous licence qui intègre leur PQC maison. Bosch est l'un de leurs premiers clients.

Qaisec (2019, Bulgarie) développe des solutions de cryptographie qui visent les secteurs de l'IA, de la finance et des télécommunications. Ils ont l'air de proposer dans un premier temps un service d'audit de sécurité puis des solutions de cryptographie qui utilisent des générateurs quantiques de nombres aléatoires pour les clés. Ils développent aussi une blockchain à base de PQC.

QEYnet (2016, Canada, $7M) développe un réseau de satellite de cryptographie quantique QKD. Le financement de la startup vient du gouvernement canadien.

QuantLR (2018, Israël) est un développeur de solutions de QKD qui ambitionne d'en abaisser de 90% le coût de déploiement via une solution logicielle fonctionnant sur du matériel de commodité non précisé.

QuantumCTek (2009, Chine) est un fournisseur de solution de cryptographie quantique de bout en bout : QKD, répéteurs de QKD, routeurs optiques. La société est issue du Hefei National Laboratory for Physical Science at Micro-scale (HFNL) et de l'University of Science and Technology of China (USTC).

Ils sont à l'origine de la création en 2014 du "Quantum-Safe Security Working Group" avec ID Quantique et Battelle, qui fait la promotion de la PQC. Ils ont comme nous l'avons vu plus haut déployé la liaison protégée par QKD de 2000 km reliant Shanghaï et Beijing. Ils réussissaient une belle IPO (introduction en bourse) en Chine en juillet 2020.

Qasky (2016, Chine) commercialise le produit de la recherche de l'académie chinoise des sciences. Les financements proviennent de Wuhu Construction and Investment Ltd et de l'Université des Sciences et de Technologie de Chine.

Ils proposent des solutions de crypto post-quantique, QKD et des composants de photonique. Leur nom est dérivé de CAS Key laboratory, CAS = Chine Academy of Sciences.

Qrate Quantum Communications (2015, Russie) propose le QRate Key Distributor, une solution de distribution de clés quantique QKD selon le protocole BB84 tenant dans un rack 4U et dotée d'une portée allant jusqu'à 100 km.

Ils commercialisent aussi un détecteur de photons uniques à diode avalanche (SPAD) opérant sur 1550 nm, un générateur de nombres aléatoires quantique.

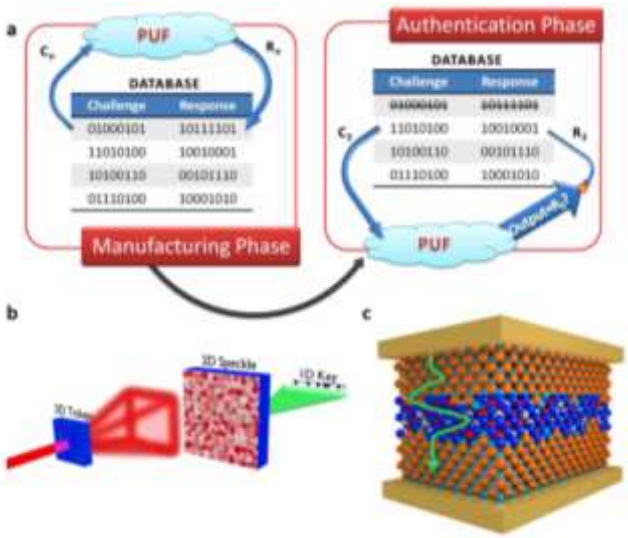
Qrypt (2017, USA) est une jeune startup de faisant de la PQC (post quantum crypto) créée par des anciens du gouvernement fédéral US, sans plus de précisions. Ils annonçaient en août 2018 utiliser sous licence le générateur de nombres aléatoire quantique à photons du laboratoire d'Oak Ridge du Département de l'Energie US.

QuantiCor Security (2017, Allemagne) développe des solutions de cryptographie post-quantique, notamment pour les applications de la Blockchain et pour les objets connectés, via les offres avec Quantum-Multisign et Quantum IDEncrypt. Ils communiquent très peu et très mal sur ce que proposent ces solutions. On sait juste qu'elles sont moins chères que les PKI classiques. Ils sont issus de TU Darmstadt. Ils visent notamment les marchés de la santé.

Quantropi (2018, Canada) propose un générateur logiciel de clés de chiffrement aléatoires à forte entropie. Cela permet de créer des solutions de chiffrement "quantum safe". La société se positionne en alternative aux solutions de QKD. Elle vise notamment les applications dans le secteur des objets connectés.

Quantum Base (2014, UK) propose différentes solutions quantiques d'authentification de produits comme le Q-ID Optical, une solution d'empreinte digitale "atomique" à lecture optique exploitant des fonctions physiques inclonables (PUFs - Physically Unclonable Functions) sous forme de tags physiques incopiables à l'échelle atomique[1072].

Le tag exploite une fine couche 2D de graphène qui contient des irrégularités uniques à l'échelle atomique et non clonables. Ces irrégularités seraient amplifiées par des phénomènes quantiques non précisés. Ces tags peuvent être de plus activités et désactivés dynamiquement. Le projet est issu de travaux de l'Université de Lancaster de Robert Young qui est le cofondateur de la startup. Le tout est intégré dans un générateur de nombres aléatoires maison (Q-RAND) à base de diode semiconductrice, intégrable dans un chipset (vidéo)[1073]. Ils proposent aussi le Q-ID Electronic, un générateur d'identifiant unique.



[1072] C'est documenté dans le brevet USPTO US10148435B2 Quantum Physical Unclonable Function déposé en 2015 (11 pages) et validé en 2018. Il évoque un composant semiconducteur à base d'arséniure de gallium, d'aluminium et d'antimoine qui génère une réponse spectrale aléatoire et différente d'un composant à l'autre. On retrouve la description du procédé dans Using Quantum Confinement to Uniquely Identify Devices, Robert Young et al, 2015 (8 pages).

[1073] Le procédé de *resonant tunnelling diode* (RTD) est documenté dans Resonant-Tunnelling Diodes as PUF Building Blocks, 2018 (6 pages).

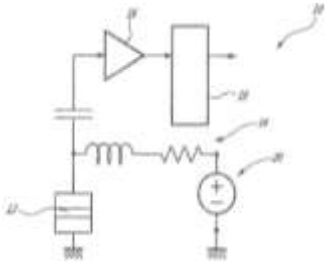
Quantum Impenetrable (2018, UK) est une startup écossaise qui développe un module de sécurité (HSM) exploitant un générateur de nombres aléatoire quantique et résistant aux algorithmes quantiques de cassage de clés.

Quantum Xchange (2016, USA) propose un réseau optique sécurisé par QKD aux USA, dénommé Phio Trusted Xchange. Ils sont partenaires de l'opérateur d'infrastructures télécoms Zayo Group dont ils exploitent leurs fibres noires et exploitent les solutions de QKD d'ID Quantique.

Ils ont commencé par déployer un réseau de QKD de 1000 km allant de Boston à Washington et passant par New York et le New Jersey[1074].

Quantum Numbers Corp (2007, Canada) est une startup qui développe un système de cryptographie qui repose sur un générateur quantique de nombres aléatoires et cible en particulier les usages mobiles. Elle communique surtout sur le dépôt d'un brevet associé.

On espère qu'il ne s'agira pas d'un « patent troller » en puissance ! La société a l'air de commercialiser sous licence sa technologie à des concepteurs de composants électroniques. Elle exploite des travaux de recherche du Département de Physique de l'Université de Sherbrooke au Québec. L'un des brevets porte sur la génération de nombre aléatoire en s'appuyant sur le bruit aléatoire généré par l'effet tunnel au travers d'une barrière de potentiel[1075]. La société est cotée en bourse au CVE (Canadian Venture Exchange).



QuBalt (2015, Allemagne) est une startup établie entre l'Allemagne et la Lettonie qui développe des solutions de cryptographie post-quantique (PQC) ainsi que sur des algorithmes quantiques.

Qubit Reset (2018, USA) développe des répéteurs quantiques pour des réseaux de QKD. La société a été créée par deux argentins basés à Miami. Elle ne figure pas dans la Crunchbase et ne semble pas avoir levé de fonds ce qui semble être un mauvais présage.

Quintessence Labs (2006, Australie) propose un générateur de nombres aléatoires quantiques et un système de QKD. Ils utilisent la technique CV-QKD qui permet d'utiliser des infrastructures de fibre optique existantes d'opérateurs télécoms à très haut débit.

[1074] Voir Quantum Xchange Breaks Final Barriers to Make Quantum Key Distribution (QKD) Commercially Viable with the Launch of Phio TX, septembre 2019.

[1075] J'ai retrouvé le PDF complet du brevet USPTO 10437559 sur le site https://www.pat2pdf.org/.

Qunnect (2017, USA) est une spin-off de la Stony Brook University de Long Island qui propose des composants permettant d'upgrader des installations télécom existantes avec de la QKD et de la PQC, dont des sources de photons.

Cela comprend une mémoire quantique fonctionnant à température ambiante pouvant servir à la mise en place de répéteurs de QKD (*ci-contre*). Le fonds Quantonation est un des investisseurs dans cette startup dirigée par Mehdi Namazi, Eden Figueroa, Noel Goddard et Mael Flament[1076].

QuNu Labs (2016, Inde) développe des solutions à base de QKD issues de L'Institut de Technologie de Madras. Ils proposent aussi leur propre générateur de nombres aléatoires quantique et planchent aussi sur la création d'une solution de QKD opérant sur du Li-Fi, le W-FI qui utilise les fréquences de la lumière visible.

QuSecure (2019, USA) développe une solution de blockchain sécurisée résiliente au calcul quantique. Il semble qu'ils développent aussi une Blockchain qui serait sécurisable via une QKD ainsi que des tests de sécurité de Blockchains. La startup fait aussi du conseil en cybersécurité et, notamment, des audits en vue du déploiement de PQC. Elle a été fondée par Rebecca Krauthamer, aussi à l'origine de la startup **Quantum Throught**, déjà citée.

Quside (2017, Espagne) propose un générateur de nombre aléatoire quantique. C'est une spin-off de l'ICFO, l'institut de photonique de Barcelone.

Ravel Technologies (2018, France) propose Ravel Homomorphic Encryption, une solution de chiffrement post-quantique et homomorphe. La société a été fondée par Mehdi Sabeg.

Secure-IC (2010, France) est le porteur du projet RISQ, de création d'une solution de crypto post-quantique française.

La société développe des solutions matérielles et logicielles de sécurité qui servent à évaluer la robustesse de solutions de sécurité. La société est issue de l'Institut Mines-Télécom.

SeQureNet (2008-2017, France) était une spin-off de Telecom ParisTech spécialisée dans la distribution de CV-QKD fonctionnant à longue distance (source).

Elle avait été financée dans le cadre du projet de recherche Européen SECOQC (secure communication based on quantum cryptography). La startup valorisait des travaux issus de l'équipe de Philippe Grangier de l'Institut d'Optique et du laboratoire Thales TRT à Palaiseau. La société a fermé boutique en 2017 ! Dommage. Elle avait été lancée un peu trop tôt par rapport à la maturité du marché.

Smarts Quanttelecom (1991, Russie) propose une solution de cryptographie quantique à base de CV-QKD qui exploite des fibres standards d'opérateurs télécoms.

[1076] En avril 2020, ils récupéraient un financement de $1,5M du Département de l'Energie US dans le cadre des programmes SBIR (Small Business Innovation Research awards). Voir Qunnect receives $1.5M award from the DoE - Swiss Quantum Hub, avril 2020. Cela leur permettra de tester leur équipement avec des opérateurs telecommunication spécialisés et à New York City.

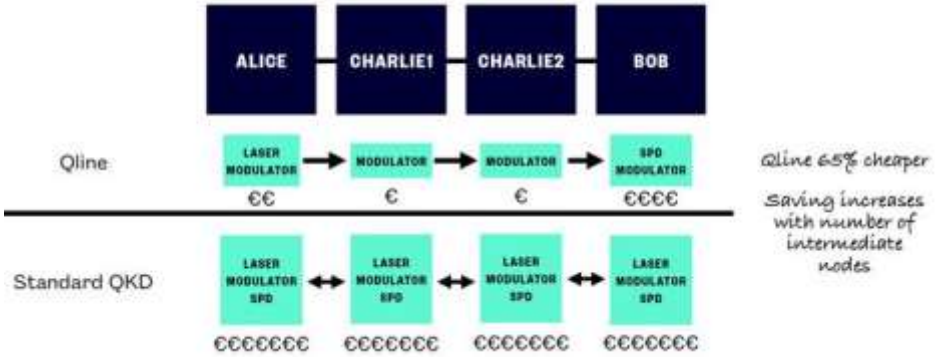
Smarts était jusqu'en 2015 un opérateur télécom mobile russe. C'est devenu depuis un opérateur de services télécoms avec une offre de liaisons télécoms sécurisés et de services de data-centers et cloud. Leur solution de QKD vient de Quanttelecom, une filiale de Smarts, développée conjointement avec l'Université ITMO de Saint Petersbourg.

SpeQtral Quantum Technologies (2017, Singapour), anciennement S-Fifteen Space Systems, est spécialisée dans la distribution de QKD par satellite. Ils valorisent des travaux de l'Université de Singapour dans la conception de pico-satellites de type CubeSat, pour la distribution de clés QKD.

Surrey Satellite Technology ou SSTL (UK) veut déployer un satellite de communication quantique à base de QKD et construit par Airbus Defense & Space. Le projet est mené en partenariat avec Eutelsat et l'ESA. Le lancement du satellite était planifié pour 2020.

VeriQloud (2017, France) est une startup créée par Elham Kashefi, et Marc Kaplan (France) et Joshua Nunn (UK). Elle est spécialisée dans la création de solutions logicielles quantiques adaptés aux télécommunications quantiques à la fois pour de la QKD et pour des traitements distribués.

Leur offre s'articule autour de la Qline, une solution logicielle qui permet de déployer un réseau quantique multi-points avec un coût plus faible en infrastructure matérielle. Avec cette architecture, les nœuds qui sont très chers peuvent être remplacés par de simples modulateurs qui sont bien plus abordables. Le fonctionnement repose sur une sorte de « time-sharing » de la ligne. Cela fait baisser l'addition matérielle d'environ deux tiers sur une installation type ci-dessous avec deux stations intermédiaires dans le réseau. Aux deux bouts de la ligne se trouve d'un côté un générateur de photons à base de laser et de modulateur et de l'autre, un détecteur de photons unique, la partie la plus chère de l'équipement qui va de 20K€ à 100K€.



La solution est déployable sur des réseaux faisant un total de 100 à 200 km. La première application est la distribution de clés quantiques QKD. Ils peuvent interopérer avec des réseaux QKD classiques. Sont visés dans un premier temps comme applications associées à la QKD le transfert de fichiers et la messagerie instantanée sécurisés. Le système peut aussi servir à générer des masques jetables[1077].

XT Quantech (2017, Chine) est spécialisé dans l'appareillage pour distribuer de la CV-QKD après s'être lancés initialement sur des solutions de DV-QKD.

[1077] Voir How to build quantum communication networks at a small scale par Marc Kaplan de VeriQloud, mai 2020.

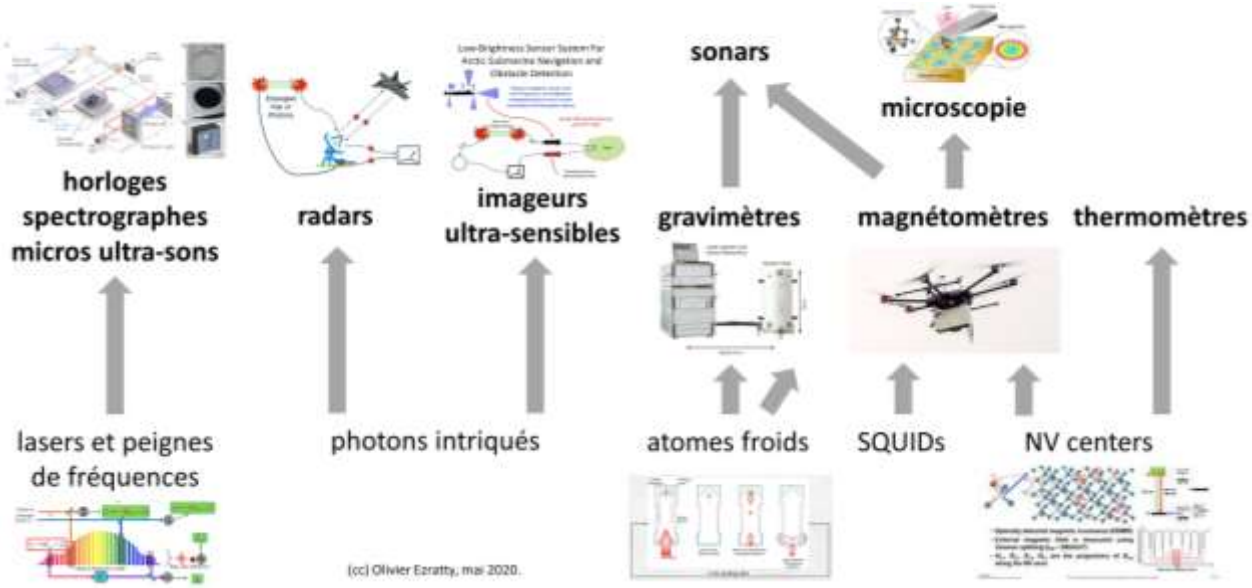
La CV-QKD s'impose car elle peut cohabiter dans les liaisons fibre des opérateurs télécoms. Ils proposent des *server appliances* pour des passerelles d'encodage et de décodage de clés QKD. Son nom complet est Shanghai Xuntai Information Technology Co.

ZY4 (2014, Canada) développe des solutions de cryptographie post-quantique basées sur leur concept maison du Shannon Event Horizon qui constituerait une nouvelle classe de PKI et de la génération de nombres aléatoires[1078].

[1078] Voir leur livre blanc Introducing the Shannon Event Horizon, 2019 (20 pages).

Métrologie quantique

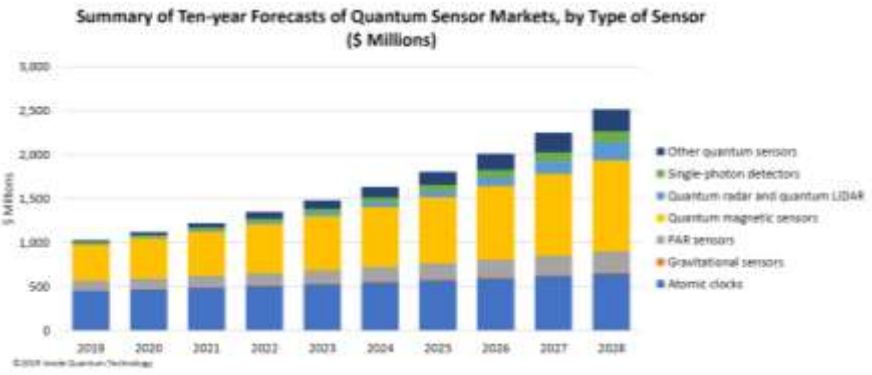
Nous allons rentrer ici dans le détail de la métrologie quantique. Il s'agit des différentes solutions de mesure de précision qui s'appuient sur des technologies quantiques de la seconde génération et qui permettent de dépasser les limites des mesures classiques. Elles permettent aussi très souvent de réaliser des mesures non invasives. Les principales mesures concernées sont celles du temps, de la gravité, du magnétisme et de la température. Les applications dérivées sont nombreuses dans les radars, les sonars, les microphones très haute sensibilité ou encore le domaine de l'imagerie en général et médicale en particulier.



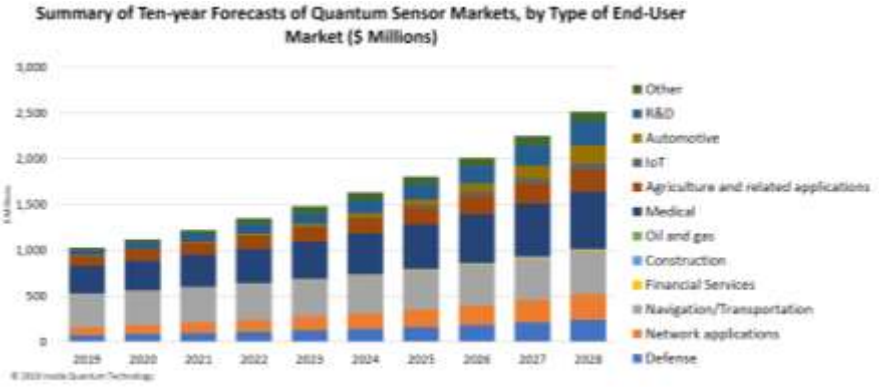
Certaines de ces technologies ont des points communs avec celles des qubits que nous avons déjà explorés en détail. C'est le cas en particulier des atomes froids et des NV centers. Pour les NV centers, le centre de gravité des usages penche d'ailleurs fortement du côté de la métrologie vs les qubits. Pour les atomes froids, c'est assez équilibré. Les magnétomètres de précision exploitent aussi bien des NV centers que des SQUIDs (Superconducting Quantum Interference Device), qui mesurent aussi le sens du courant dans les qubits supraconducteurs de type « flux » et sont utilisés en particulier par D-Wave dans ses ordinateurs à recuit quantique.

Une bonne part de ces technologies de mesure quantique font largement appel aux outils de la photonique, qu'elles soient directement à base de photons (lasers, peignes de fréquences, photons intriqués) ou exploitant des atomes froids et même des NV centers, dont on évalue l'état par mesure de leur fluorescence.

Ces technologies sont déjà exploitables commercialement et continuent de progresser régulièrement. C'est encore un marché de taille plus limitée, démarrant aujourd'hui à environ $1B pour en faire deux d'ici une dizaine d'années et à l'échelle mondiale, bien moins que pour le calcul et la cryptographie quantiques.



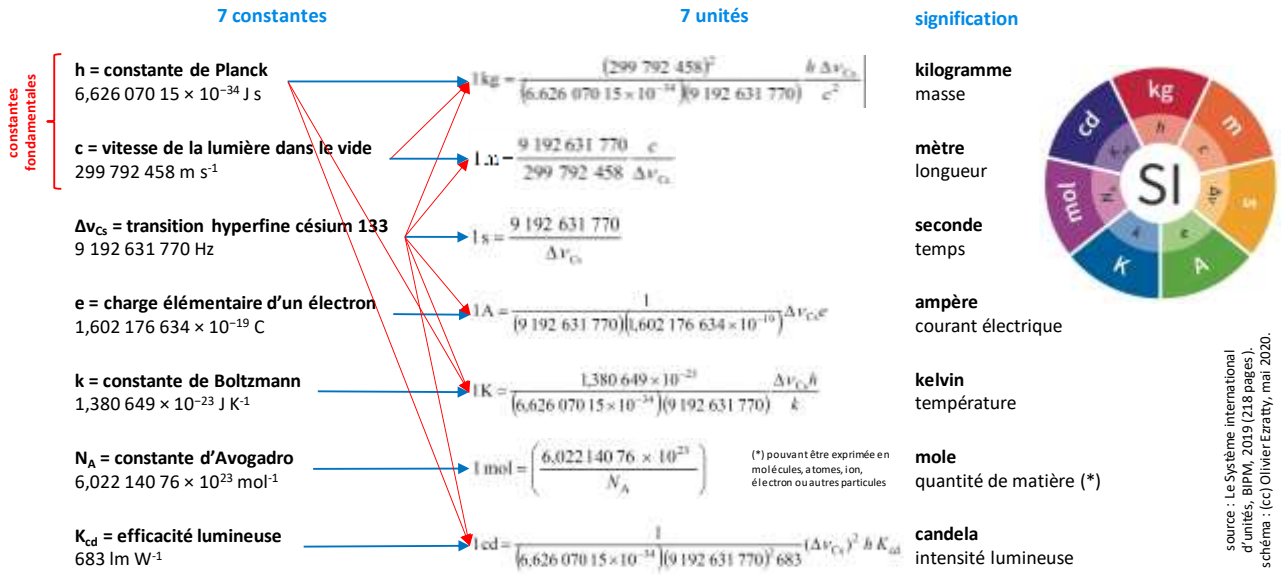
Ce marché est fragmenté en un grand nombre de sous-marchés que nous allons détailler dans cette partie[1079]. Les deux plus gros étant ceux des transports et de l'imagerie médicale. Mais ces prévisions ne veulent rien dire. Certains usages pourraient devenir grand public.



C'est le cas des GPS sans liaisons satellites faisant appel à des micro-magnétomètres et qui pourraient un jour équiper les véhicules autonomes.

On ne peut pas évoquer le thème de la métrologie sans faire référence au système international de mesure (SI). Celui-ci a été refondu après un vote à l'unanimité du traité du mètre de Versailles signé lors de la 26e Conférence Générale des Poids et Mesures (CGPM) de novembre 2018[1080]. Sa mise en application date du 20 mai 2019.

Le nouveau SI de 2019 modifie la définition du kilogramme, de l'ampère, du kelvin et de la mole. Il est construit autour de sept constantes figées : un nombre de transitions hyperfines du césium 133, la vitesse de la lumière dans le vide[1081], la constante de Planck, la charge élémentaire d'un électron, la constante de Bolzmann, le nombre ou constante d'Avogadro et l'efficacité lumineuse. De ces constantes sont dérivées les sept unités de base du système : le kilogramme, le mètre, la seconde[1082], l'ampère, le kelvin, la mole et le candela. Elles ne dépendent plus de matériaux qui pouvaient se dégrader dans le temps comme le kilogramme étalon conservé au BIPM à Saint-Cloud, ou du point triple de l'eau (gel) qui définissait le kelvin, et qui dépendait de sa composition isotopique.



[1079] Source des données : Quantum Sensors: Ten Year Market Projections par Lawrence Gasman, 2019 (7 slides).

[1080] Voir The International System of Units (SI), NIST, 2019 (13 pages) et Le Système international d'unités, BIPM, 2019 (218 pages).

[1081] La définition de la vitesse de la lumière à 299 792 458 m s^{-1} date de 1983.

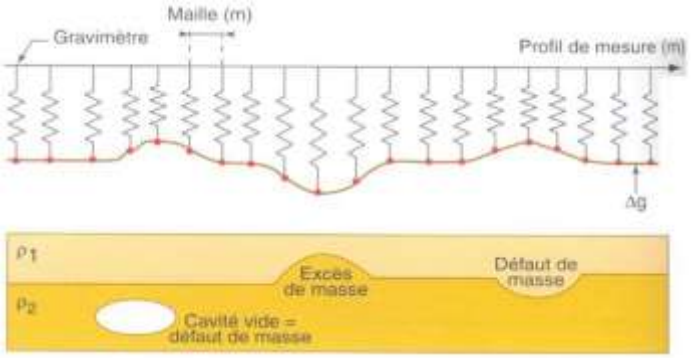
[1082] La seconde était définie à partir de la fréquence de transition hyperfine du césium 133 depuis la 13e CGPM de 1967. Auparavant, c'était une fraction de la journée solaire, qui n'était pas stable.

La mole était auparavant définie sur la base de 0,012 kg de carbone 12[1083]. Le mètre étalon qui est conservé aux Archives à Paris n'était déjà plus la référence depuis 1960. Toutes les autres unités de mesure comme le hertz, joule, coulomb, lumen ou le watt sont dérivées des constantes et unités de base. Ce système de mesure est dit « quantique » car il repose sur la mesure de phénomènes fondamentaux nous ramenant aux quanta, en particulier pour la définition de la seconde qui utilise des transitions énergétiques quantifiées dans l'atome de césium et celle du kilogramme qui fait appel à la constante de Planck, elle-même, un fondement de la physique quantique. De nombreux travaux de physique quantique reliés à ces évolutions du système international de mesure, notamment au NIST, ont un lien avec les dispositifs commerciaux qui sont évoqués dans cette partie.

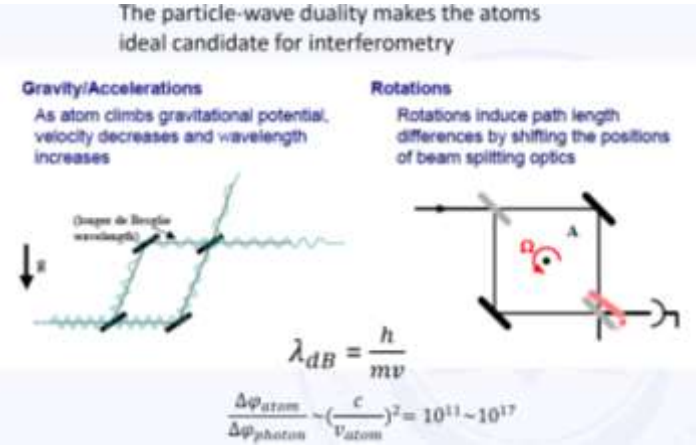
Gravimètres quantiques

Les gravimètres quantiques permettent de mesurer la gravité avec une très grande précision. C'est utile dans de nombreux scénarios : dans les détecteurs sismiques, pour la mesure et la définition du kilogramme de référence, pour la navigation autonome de précision complétant les GPS dans les avions, navires, sous-marins et drones, pour la cartographie de champ gravitationnel, pour la prospection de pétrole et de minerais et pour la détection d'ondes gravitationnelles en astronomie.

La mesure de la gravité est généralement réalisée avec des interféromètres d'atomes froids, tirant partie de la dualité onde-particules s'appliquant aussi aux atomes. La technique a été mise au point à partir de 1991 et perfectionnée depuis [1084] . En France, l'ONERA et le LNE-SYRTE ont été des pionniers dans le domaine, lançant des expérimentations en 2009 (projet GIRAFE) puis en 2014-2016 (GIRAFE2)[1085].



Le principe consiste à créer une source d'atomes froids en suspension, en général du rubidium, à préparer leur état avec des lasers, puis à les faire traverser un interféromètre et ensuite à analyser les résultats. Cela peut servir à la mesure de la gravité mais aussi d'accélérations et de rotations[1086]. La technique a été perfectionnée et rendue transportable par la PME française **Muquans** (2011), installée dans l'Institut d'Optique à Bordeaux. Ils valorisent des travaux conjoints avec le CNRS.



[1083] Avec le nouveau SI, un gramme de matière contient N_A multiplié par le nombre de nucléons (protons et neutrons) de l'élément considéré (atome, molécule). Cela vient du fait que dans un atome, la majorité du poids est dans le noyau. Les électrons ont une masse équivalente à 1/1836 fois celle d'un nucléon.

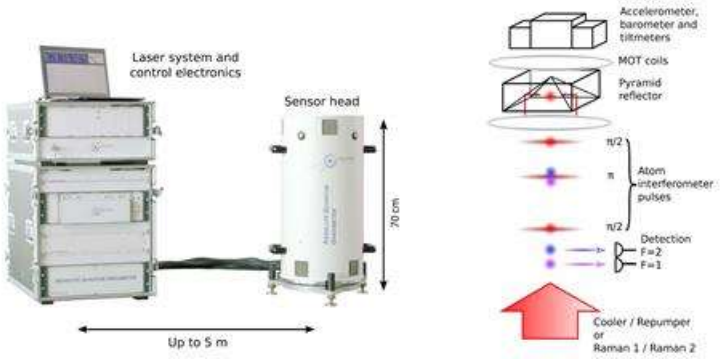
[1084] Voir Young s double-slit experiment with atoms : A simple atom interferometer, de O. Carnal, J. Mlynek, 1991 (6 pages) qui décrit une experience d'interférométrie de fentes de Young à base d'atomes d'hélium. Voir aussi Experimental gravitation and geophysics with matter wave sensors, LP2N, 2018 (234 slides).

[1085] Voir Applications « embarquées » de la gravimétrie atomique par N. Zahzam et al, avril 2019 (24 slides) et L'ONERA invente avec le SHOM la cartographie de pesanteur à précision "atomique", février 2016. Le SHOM est le Service Hydrographique et Océanographique de la Marine.

[1086] Source du schéma : Compact and Portable Atom Gravimeter de Shuai Chen, University of Science and Technology of China, juin 2019 (22 slides).

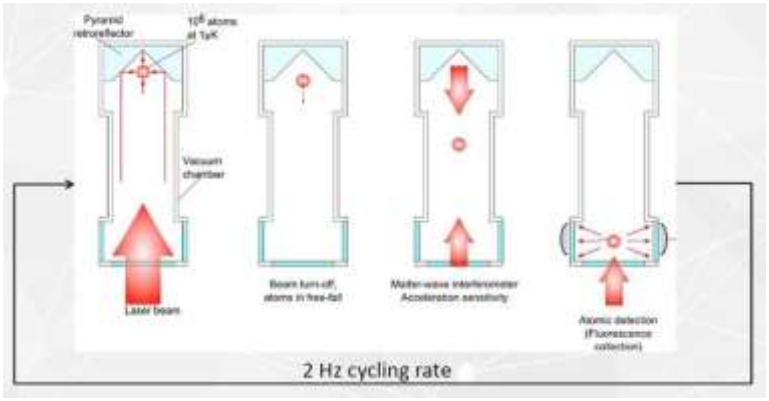
Leur gravimètre quantique cible par exemple la détection de cavités pour le BTP, la prospection pétrolière et la surveillance de volcans comme pour l'Etna en Italie[1087].

Le produit s'appelle « Absolute Quantum Gravimeter »[1088]. Ils utilisent un petit nuage d'une centaine d'atomes de rubidium refroidis à 1µK par lasers dans 6 directions et piégés magnétiquement sous vide. Ces atomes sont stimulés par des transitions de Raman à base de doubles photons avec des durées et polarisations différentes (π/2, −π, −π/2) [1089].



Le système mesure alors la chute gravitationnelle du nuage d'atome qui est différente selon la préparation des atomes.

Un système à base de fluorescence et de diodes mesure la vitesse de la chute et le fait dans la durée pour évaluer sa variation temporelle. Les diodes mesurent la proportion des atomes dans chaque sortie de l'interféromètre.



La source des atomes contient aussi un accéléromètre qui corrige en temps-réel la phase des lasers.

La maîtrise des atomes froids a d'autres applications[1090]. Ainsi, Muquans participe aux projets du projet flagship européen **Quantum Internet Alliance** pour créer un matériel d'extension de la portée des systèmes de QKD et avec la startup française **Pasqal** qui crée des processeurs quantiques à base d'atomes froids.

D'autres sociétés sont aussi positionnées dans ce marché :

[1087] La startup **Muquans** employait 29 personnes en mai 2019 et qui faisait 2,9M€ en 2018. Ils développent un gravimètre quantique qui sert par exemple à la détection de cavités pour le BTP, la prospection pétrolière et la surveillance de volcans comme pour l'Etna en Italie. Le produit s'appelle **Absolute Quantum Gravimeter**. Le système exploite des atomes froids (rubidium) éclairés et refroidis à 1 µK par laser dans 6 directions et piégés magnétiquement sous vide. Le système mesure avec une grande précision la chute gravitationnelle du nuage d'atome. Un système à base de fluorescence et de laser mesure la vitesse de la chute et le fait dans la durée pour évaluer sa variation temporelle. Ils participent aux projets du flasgship européen **Quantum Internet Alliance** pour créer un matériel d'extension de la portée des systèmes de QKD et **Pasquans** dans la simulation quantique à atomes froids. La société a été créée en 2011.

[1088] Le procédé de Muquans est documenté dans Gravity measurements below 10^{-9} g with a transportable absolute quantum gravimeter, 2018 (12 pages) et valorisé dans Digging Into Quantum Sensors par Stewart Wills dans Optics & Photonics, septembre 2019.

[1089] Le refroidissement Raman à double photon utilise deux lasers. Un premier excite les atomes pour les faire atteindre un état excité élevé et un autre désexcite l'atom pour le faire descendre à un état excité supérieur à l'état initial. C'est cette technique qui permet de descendre la température en-dessous du micro-Kelvin.

[1090] Voir Fifteen years of cold matter on the atom chip promise, realizations, and prospects par Mark Keil et al, 2019 (46 pages) qui fait un inventaire d'applications scientifiques des atomes froids.

Thales (France) développe des gravimètres à atomes froids miniaturisés conçus pour être embarqués. Le tout avec un composant « BEC on chip » pour « Bose Einstein condensate on chip » en collaboration avec le laboratoire Charles Fabry de l'Institut d'Optique (LCFIO). Les recherches sur le sujet ont démarré vers 2014 et ne semblent pas encore avoir débouché sur un produit[1091].

D'autres laboratoires planchent sur le même sujet, comme celui de l'Université Leibniz de Hannovre[1092]. **Aquark Technologies** (2020, UK) est une spin-off de l'Université de Southampton qui est sur le même créneau que Muquans. **AtomSensors** (2015, Italie) est une spin-off de l'Université de Florence qui développe aussi des capteurs quantiques à base d'atomes froids, et notamment des gravimètres. Ils fournissent aussi des sources laser pour de la spectroscopie et du refroidissement d'atomes par laser. Les Chinois sont aussi sur ce domaine, mais sans avoir été aussi loin dans la miniaturisation[1093].

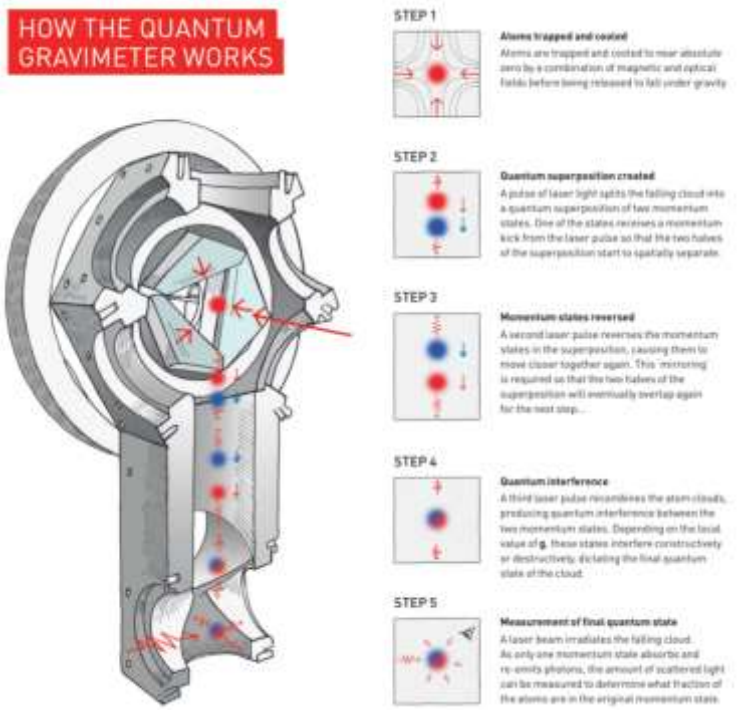
Teledyne e2v (UK, filiale de Teledyne US) vise la maintenance d'infrastructures avec la détection d'obstacles sous-terrains ou de cavités avant les travaux de BTP, la recherche d'énergies géothermiques et de réserves d'eaux souterraines. Ils sont aussi partie prenante de la création de **CASPA** (Cold Atom Space PAyload), un petit satellite de 14 kg rassemblant 6 CubeSat dans un volume de 30x20 x10cm, comprenant un gravimètre à atomes froids, qui serait le premier à fonctionner dans l'espace. Il doit être lancé par l'ESA en 2020.

[1091] Voir la thèse Vers un accéléromètre atomique sur puce de Matthieu Dupont-Nivet, 2016 (263 pages).

[1092] Voir Gravity measured using a Bose–Einstein condensate on a chip par Hamish Johnston, 2016 évoquant des travaux d'Ernst Rasel de l'Université Leibniz de Hannovre qui fait référence à Atom interferometry and its applications par S. Abend et al, 2020 (48 pages). Voir aussi Fifteen years of cold matter on the atom chip: promise, realizations, and prospects par Mark Keil et al, 2019 (46 pages).

[1093] Voir Compact and Portable Atom Gravimeter par Shuai Chen, 2019 (22 slides).

M Squared (2006, UK) a créé un gravimètre quantique à atomes froids utilisant un procédé voisin de celui de Muquans [1094], en partenariat avec l'Université de Birmingham et l'Imperial College de Londres. Le projet a été financé dans le cadre de l'initiative quantique du gouvernement UK lancée dès 2013. Le métier d'origine de la startup qui est basée en Ecosse est leur gamme de laser Sols-TiS couvrant le spectre de 200 nm à 4000 nm. Ces lasers sont utilisés dans l'industrie et dans des horloges optiques.



AOSense (2004, USA) qui créé des gyroscopes quantiques, un gravimètre quantique et des horloges optiques commerciaux.

Il fournit aussi de l'appareillage d'instrumentation pour la recherche dans ces domaines avec des générateurs d'atomes froids et des générateurs de peignes de fréquences lasers (voir la définition dans la partie suivante sur les horloges optiques). Ils collaborent avec IonQ pour leurs ordinateurs quantiques à base d'ions piégés.

Nomad Atomics (2018, Australie) développe des gravimètres et accéléromètres quantiques compacts à base d'atomes froids. La société a été lancée par Kyle Hardman, Christian Freier et Paul Wigley, respectivement chercheur et post-docs de l'Australian National University.

iXblue Photonics (2000, France) est la branche photonique de la société iXBlue, cette dernière étant spécialisée dans la conception et la fabrication de centrales inertielles et de sonars.

Elle est spécialisée dans la création de modulateurs optiques en niobiate de lithium, d'amplificateurs de micro-ondes et de contrôleurs de biais de modulateurs pour le pilotage d'interféromètres Mach-Zehnder. Leurs composants sont fabriqués sur leur site de Lannion en Bretagne. Ils sont en particulier impliqués avec le LP2N de Toulouse dans la création d'Ixatom, un capteur inertiel quantique à base d'atomes froids de rubidium[1095]. iXblue Photonics résulte de l'acquisition de deux sociétés : iXFiber en 2011, un spécialiste de composants optiques passifs (filtres à réseau de fibres de type FBG, Fiber Bragg Gratings). Puis Photline Technologies en 2013, une spin-off du laboratoire Femto-ST créé en 2000 à Besançon.

[1094] Source de l'illustration : M Squared quantum gravimetry (4 pages).

[1095] Voir iXAtom - LP2N and iXblue Cold Atoms joint laboratory.

Pour terminer, citons aussi une catégorie bien à part de microgravimètres : ceux du LIGO qui servent à évaluer les ondes gravitationnelles. Ils sont à base d'interféromètres optiques de très grande précision mais de taille incompatible avec tous les autres usages imaginables[1096].

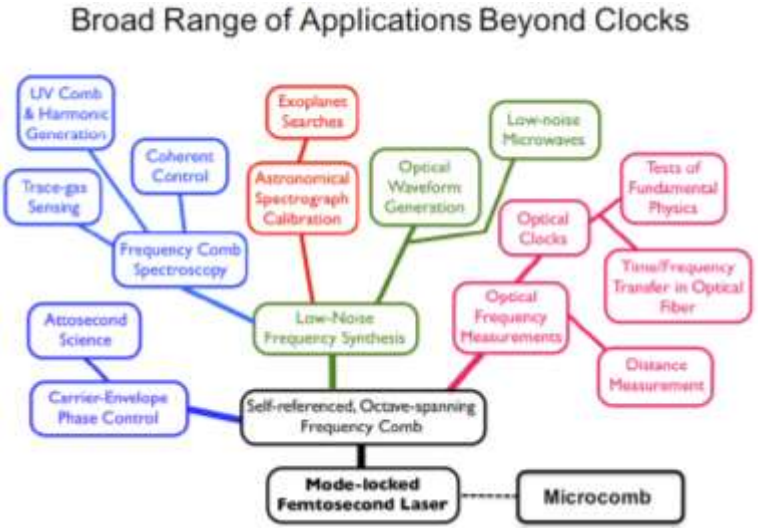
Horloges quantiques

La mesure du temps a régulièrement progressé depuis les premières horloges mécaniques entre le 14e et le 19e siècle. C'est entre deux guerres que sont apparues les horloges à quartz exploitant l'effet piézoélectrique démontré par Pierre et Jacques Curie en 1880. L'effet a une fréquence de 2^{15} Hz et on décompte le temps après application de diviseurs de fréquences. Le tout avec une dérive de quelques centaines de microsecondes par jour.

Les premières horloges atomiques au césium datent des années 1950. Elles ont une fréquence de l'ordre de 9 GHz et fournissent un étalon de fréquence de 10^{-13}. La seconde est définie, nous l'avons vu, depuis 1967 comme la durée de 9 192 631 770 périodes de la radiation correspondant à la transition entre les deux niveaux « hyperfins » de l'état électronique fondamental du césium 133.

La variante récente de ces horloges dite « fontaine » fonctionne à très basse température, avec un refroidissement laser amenant les atomes à 1 µK. C'est bien plus froid qu'un qubit supraconducteur qui se contente de 15 mK mais c'est plus simple à obtenir qu'avec un réfrigérateur à dilution. Un oscillateur de fréquence génère une transition entre deux niveaux d'énergie du césium. La fréquence est verrouillée avec une boucle d'asservissement.

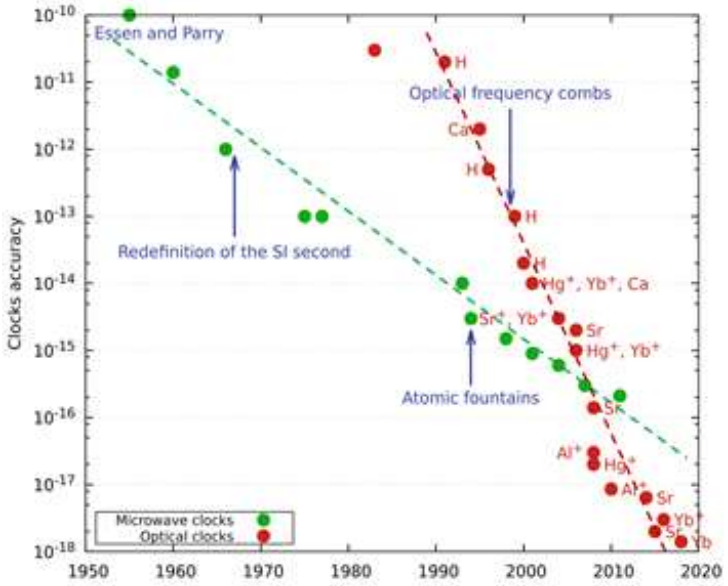
La mesure précise des fréquences a de nombreuses applications : la mesure du temps, la synchronisation d'appareils divers sur Internet, ne serait-ce que des serveurs ou instruments scientifiques, celle d'objets en mouvement pour mesurer leur position, l'astronomie (exoplanètes, ondes gravitationnelles[1097]), la spectroscopie de précision d'absorption ou d'émission, la gestion de transmissions par fibres optiques et la génération d'ondes radios de forme arbitraire.



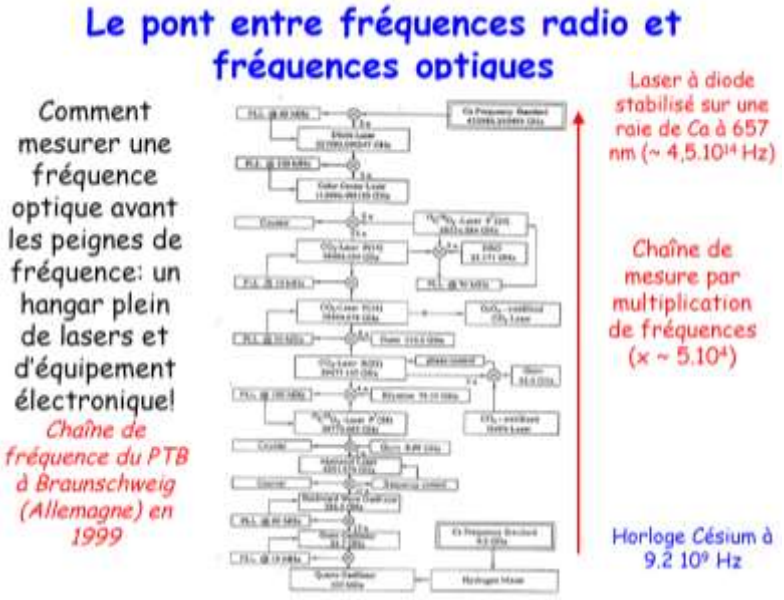
[1096] Voir Advanced LIGO Just Got More Advanced Thanks To An All-New Quantum Enhancement par Ethan Siegel, décembre 2019. Et une description de la technique du "quantum squeezing" qui est utilisée dans la dernière version du LIGO : NIST Team Supersizes 'Quantum Squeezing' to Measure Ultrasmall Motion, 2019.

[1097] Voir Atomic Clocks as Detectors of Gravitational Waves par Sergei Kopeikin, University of Missouri (43 slides). Qui est aussi la source du graphe sur l'évolution dans le temps de la precision des horloges. Mais Url morte.

Une meilleure précision est cependant nécessaire. Depuis une vingtaine d'année, elle est obtenue grâce à la mesure optique des fréquences et du temps. Pour cela, on a remplacé la mesure de vibrations atomiques par celle d'ondes lumineuses générées par des lasers et à 10^{15} Hz. Elle a permis de gagner une précision d'un facteur 10^5. Le principe a été démontré en 2000 pour générer une précision de l'ordre de la femtoseconde. Cela a valu le prix Nobel de Physique en 2005 à **Theodor Hänsch** (1941, Allemand) et **John Hall** (1934, Américain)[1098].



Les peignes de fréquences avaient été découverts avec les premiers lasers à mode bloqué par Logan Hargrove en 1964. Avant les peignes optiques, on utilisait des générateurs d'harmoniques de fréquences lumineuses avec une combinaison de plusieurs lasers dans des montages compliqués, comme *ci-contre*[1099]. Pour mesurer les fréquences élevées de la lumière, ces horloges utilisent des peignes de fréquences optiques (frequency combs) qui permettent de subdiviser des fréquences optiques (élevées) en fréquences micro-ondes (moins élevées) pour la mesure de fréquence et le décompte temporel.



Cette mesure exploite des lasers dits « à mode bloqué » qui génèrent des impulsions très courtes, pouvant descendre jusqu'à quelques femtosecondes, contrairement aux lasers continus.

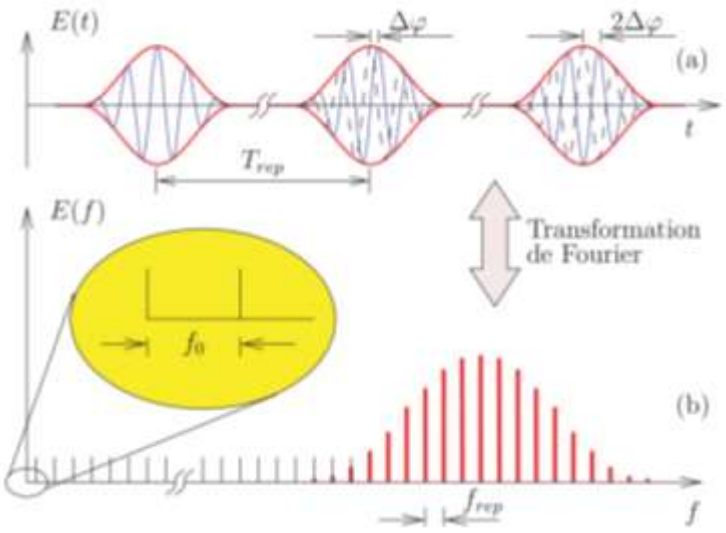
La décomposition en fréquence de ce genre de signal donne un peigne de fréquences en forme de gaussienne et dont chaque dent est espacée régulièrement d'une fréquence équivalente à celle de l'impulsion du laser. C'est lié au fait que la longueur de la cavité du laser est un multiple de la longueur des ondes électromagnétiques émises par le laser. Plus le multiple est grand, plus l'est la fréquence générée.

[1098] Voir Nobel Lecture: Defining and measuring optical frequencies de John Hall, 2006 (17 pages) et Des règles de lumière : les peignes de fréquence de Steven Cundiff, Jun Ye et John Hall dans Pour la Science, 2008 (8 pages). John Hall y raconte que les peignes de fréquence sont le croisement de quatre champs de recherche au départ indépendants : les lasers ultra-stables, les lasers à impulsions rapides, les matériaux optiques non linéaires et la spectroscopie laser de précision. A l'image de l'informatique quantique et de ses nombreuses sources scientifiques et technologiques. Source de l'illustration : Les horloges atomiques et leur impact en géodésie par Arnaud Landragin et al, 2019 (27 slides).

[1099] Source de l'illustration : Chaire de Physique Quantique-Cours 2014-2015, 5ème leçon - 7 Avril 2015, V. La passion de la précision et la mesure du temps de Serge Haroche, Collège de France (72 slides).

Le spectre de fréquence ressemble à une gaussienne. Son enveloppe est égale à l'enveloppe du spectre d'une impulsion isolée, qui est continue. La largeur du spectre de fréquence couvert peut être étroit, de quelques nm de longueur d'onde, ou couvrir tout le spectre visible, donc quelques centaines de nm.

Un calcul permet de déterminer les fréquences très élevées du peigne de fréquence (f_n). Il exploite plusieurs paramètres : la fréquence de référence f_{rep} des pulsations du laser qui est de l'ordre de 250 MHz à 1GHz, n, le nombre de fréquences détectées via spectroscopie (il peut y en avoir des centaines de milliers) et la phase d'émission du laser à mode bloqué qui s'ajoute à chaque impulsion et génère le décalage de fréquence f_0, que l'on évalue avec une méthode décrite plus loin et qui est aussi d'un ordre inférieur au GHz [1100].

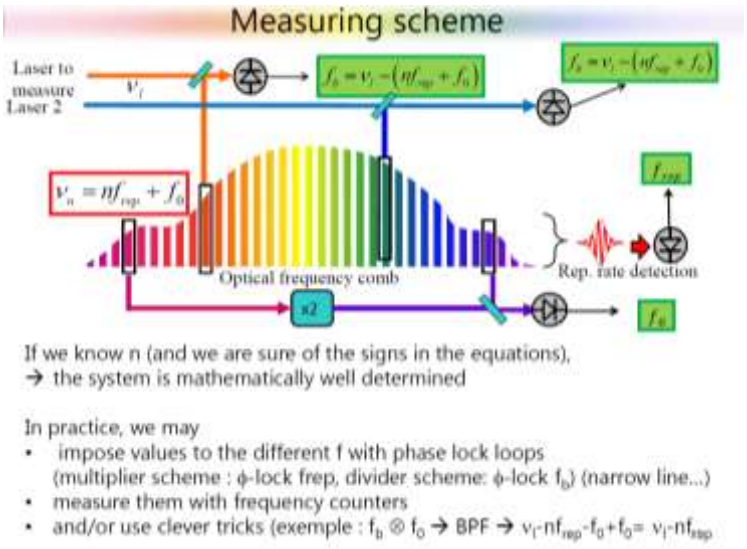


Grâce à la mesure de fréquences du domaine des ondes radio en MHz/GHz, on aboutit à la mesure de fréquences en dizaines et centaines de THz au Hz près. Le système agit ainsi comme un multiplicateur de fréquences. La mesure de fréquences lumineuses est impossible avec de l'électronique traditionnelle du fait des fréquences utilisées qui sont de plusieurs dizaines ou centaines de tera-Hertz. Ces peignes de fréquences étalonnés servent aussi à mesurer une différence de fréquences avec cet étalon [1101].

Le peigne de fréquences couvre une octave, soit d'une fréquence (n) jusqu'à son double (2n). L'évaluation de f_0 s'effectue en extrayant la fréquence f_n, et en la doublant avec un cristal. En additionnant cette fréquence doublée avec f_{2n}, on obtient un battement à la fréquence de f_0 [1102].

$$2(f_0 + n \times f_{rep}) - (f_0 + 2n \times f_{rep}) = f_0$$

C'est ce que l'on appelle la **détection hétérodyne**. Le peigne de fréquences devient une sorte de règle graduée qui est ensuite utilisée pour positionner une fréquence à mesurer par rapport à la règle.



[1100] Source de l'illustration : Impulsions lumineuses ultra-courtes pour la métrologie de fréquences, CNRS (6 pages).

[1101] Voir A la recherche d'une précision extrême les peignes de fréquences d'Alexandre Parriaux, 2016 (7 pages), Phase Coherent Vacuum-Ultraviolet to Radio Frequency Comparison with a Mode-Locked Laser de J. Reichert et al, 2005 (5 pages), Direct Link between Microwave and Optical Frequencies with a 300 THz Femtosecond Laser Comb de Scott Diddams et al, 2000 (4 pages), Fundamentals of frequency combs What they are and how they work de Scott Diddams (46 slides) et Optical frequency combs and optical frequency measurements de Yann Le Coq, 2014 (38 slides). Voir aussi les explications dans Chip-scale Optical Atomic Clocks and Integrated Photonics par Matthew Hummon, NIST, 2018 (35 slides).

[1102] Source du schéma : Optical frequency combs and optical frequency measurements de Yann Le Coq, 2014 (38 slides), slide 11.

Comment crée-t-on une horloge atomique optique avec tout cela ? Je n'ai pas encore compris[1103] !

La lecture des résultats de spectroscopie utilisant des peignes de fréquence peut utiliser des caméras CCD ou CMOS selon les fréquences utilisées dans ou autour du visible[1104]. La précision de cette mesure évolue avec l'usage de lasers utilisant une haute fréquence d'impulsion. Ils sont notamment à base de titane-saphir avec des impulsions de quelques femtosecondes (10^{-15} à 10^{-14} secondes).

A ce jour, le record de précision d'une horloge atomique utilisant de la spectroscopie est celle du **NIST.** Elle est bâtie avec un ion d'aluminium associé à un anion de magnésium. L'ion d'aluminium est excité par deux lasers à l'ytterbium. La mesure est réalisée par à l'aide d'une « quantum logic spectroscopy » qui fait elle-même appel aux peignes de fréquences vus plus haut[1105].

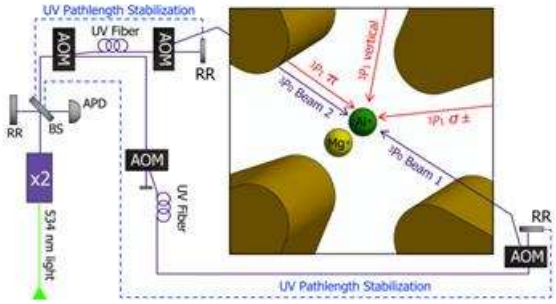
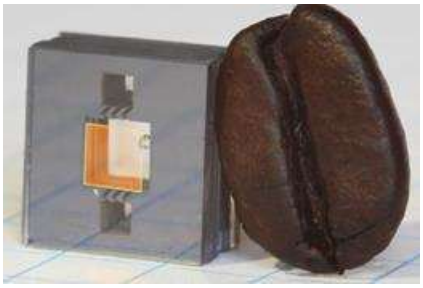


FIG. 1. Simplified schematic of the quantum-logic clock experimental setup. A frequency-quadrupled Yb-doped fiber laser is locked to the $^1S_0 \leftrightarrow {}^3P_0$ transition ($\lambda \simeq 267$ nm) by alternating the probe direction between two counterpropagating laser beams (shown in violet). An enlarged view of the trapping region is shown on the right. Three nominally orthogonal beams used for micromotion measurements are shown in red. Acousto-optic modulator (AOM), beam splitter (BS), retro-reflector (RR), frequency doubling stage (x2).

L'horloge atteint une précision de 10^{-18} seconde, soit une dérive d'une seconde sur 33 milliards d'années, ce qui représente 2,5 fois l'âge de l'Univers[1106]. Dans ce marché des horloges quantiques optiques, on trouve de nombreux laboratoires de recherche qui produisent leur propre appareillage.

Ce même NIST travaille sur une horloge atomique qui tiendrait dans un composant de la taille d'un grain de café, utilisant un double peigne de fréquences et un gaz de rubidium. L'ensemble ne consomme que 275 mW. C'est un projet cofinancé par la DARPA[1107]. Pour l'instant, la précision obtenue n'est pas encore satisfaisante pour une industrialisation.



L'un des projets du Quantum Flagship Européen, **iqClock** (Pays-Bas, 10M€), vise aussi à créer des horloges quantiques à très haute précision et portables. Le consortium rassemble six universités et six partenaires privés dont Teledyne EV (Américain), Toptica (Allemagne), NKT Photonics (Danmark), AckTar (Israël) et Chronos (UK).

Dans le privé, on compte notamment **Teledyne** avec une offre variée : Minac (horloge atomique au césium), T-CSAC (également au césium, intégrée dans une puce) et Synchronicity (à base d'ytterbium).

HyperLight Corp (2018, USA) développe des circuits intégrés de nanophotonique comme des peignes de fréquence ou des résonateurs.

[1103] C'est expliqué dans Optical Atomic Clocks, de Andrew Ludlow, Martin Boyd, Jun Ye, E. Peil et P.O. Schmidt, 2015 (65 pages) et Optical atomic clocks de N. Poli et al, 2014 (70 pages). Voir aussi Photonic integration of an optical atomic clock de Z. L. Newman et al, novembre 2018 (12 pages).

[1104] Voir Impulsions lumineuses ultra-courtes pour la métrologie de fréquences, CNRS (6 pages) et Peignes de fréquences femtosecondes : aux limites de la spectroscopie de Theodor Hänsch Nathalie Picqué, 2010 (8 pages).

[1105] Voir cette explication : Quantum Logic for Precision Spectroscopy par Piet Schmidt et al, 2009 (6 pages).

[1106] Voir $^{27}Al^+$ Quantum-Logic Clock with a Systematic Uncertainty below 10^{-18}, 2019 (6 pages).

[1107] Le projet est documenté dans Architecture for the photonic integration of an optical atomic clock, 2019 (6 pages).

Le tout doit pouvoir servir dans différents domaines et notamment en métrologie quantique. La startup est basée à Cambridge près de Boston.

Cryoclock (2016, Australie) développe des oscillateurs cryogéniques à base de saphir. La société a été cofondée par John Hartnett. Les applications couvrent notamment les processeurs quantiques à ions piégés et les horloges atomiques.

Orolia (2005, France) créé des horloges atomiques au césium, ou à base d'oscillateurs au rubidium. Ils visent surtout les machés de l'aérospatiale et fournissent le service Galileo GNSS.

Syrlinks (2011, France) développe notamment des horloges atomiques miniatures à base de MEMS et de césium qui sont destinées aux applications embarquées. Leur MMAC fait 40 x 35 x 22 mm et consomme moins de 0,3 W.

TMD (1969, UK) propose des amplificateurs de micro-ondes. Ils développent aussi des horloges atomiques ainsi que de l'instrumentation pour la manipulation d'atomes froids.

VectorAtomic (2018, USA) commercialise des horloges atomiques au rubidium destinées aux systèmes de navigation inertielle quantiques permettant de se passer de GPS.

Vescent Photonics (2002, USA) propose des générateurs de peignes de fréquences optiques exploitables dans des horloges atomiques. Ils maîtrisent aussi la technique à base de lasers pour le contrôle d'atomes froids. Ils sont basés dans le Colorado.

Rydberg Technologies (2015, USA) fournit des éprouvettes de césium ou de rubidium pour les solutions de métrologie à base d'atomes froids. Ils ont aussi en catalogue une sonde radio-fréquences à base d'atomes de Rydberg, un RFLS (Rydberg Field Measurement System). Leur technologie est aussi intégrée dans des récepteurs de radiofréquences AM et FM.

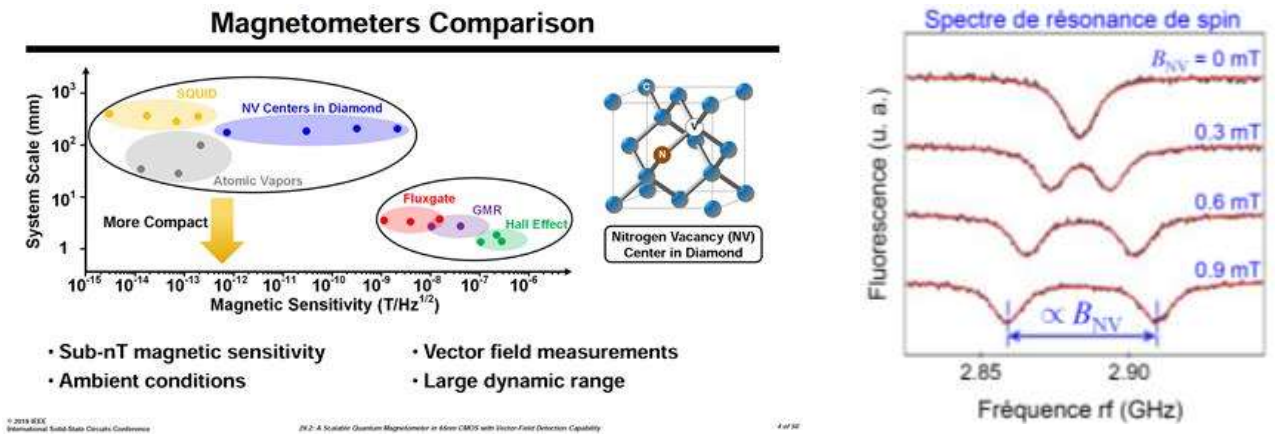
Enfin, citons aussi **Muquans** qui utilise aussi sa maîtrise des atomes froids pour proposer une horloge atomique les utilisant, la MuClock, conçue en partenariat avec le laboratoire LP2N de Toulouse et le LNE-SYRTE. Elle se positionne en alternative aux horloges atomiques au césium. L'instrument pèse 135 kg et consomme 200W.

Magnétomètres quantiques

Les magnétomètres quantiques servent à détecter les faibles variations ou niveaux de magnétisme et avec une grande précision spatiale. Les usages sont variés : pour la navigation, l'exploration de minerais, la détection de courant, la magnétocardiographie, la magnétoencéphalographie, l'orientation de drones et véhicules autonomes dans des tunnels, là où le GPS ne fonctionne pas[1108], les sonars, la détection d'objets métalliques mouvants comme des véhicules et l'imagerie cellulaire[1109].

[1108] Une solution de drones utilisant un GPS en tunnel est proposée par la startup **Hovering Solutions** (Espagne).

[1109] Voir Nitrogen-vacancy centers in diamond for nanoscale magnetic resonance imaging applications par Alberto Boretti et al, 2019 (24 pages).



Différentes techniques sont disponibles pour la magnétométrie de précision dont les atomes froids[1110], les SQUID (effet supraconducteur avec une jonction Josephson comme dans les qubits supraconducteurs[1111]) et les systèmes à base de cavités dans les diamants (NV-centers) dont nous avons vu qu'ils peuvent aussi servir de qubits, même si cette piste n'a pas l'air d'être sérieusement creusée en ce moment.

La mesure du magnétisme avec ces derniers utilise la variation du spectre de résonance du spin de la cavité de diamant, qui dépend du champ magnétique ambiant. On mesure la distance entre les deux impulsions lumineuses fluorescentes (Y) générées en fonction de la fréquence d'excitation électromagnétique utilisée (X)[1112]. La préparation des spins est réalisée avec un laser et sa modification avec des impulsions micro-ondes autour de 3 GHz.

La précision de la mesure du magnétisme atteint le pico-Tesla[1113] soit des milliards de fois moins que le magnétisme terrestre[1114]. Cette dernière technique NV-centers est apparue en 2009. Elle est notamment développée à Palaiseau chez **Thales**[1115]. Ils procurent une moins bonne précision que les atomes froids mais leur usage est plus pratique car l'instrument est plus facile à miniaturiser, même avec son petit système de cryogénie à azote liquide associé[1116].

Les magnétomètres à pointe utilisent un nano-cristal de diamant contenant une seule cavité et un atome d'azote, ce qui assure la précision de la mesure. La pointe peut être déplacée dans l'espace et servir à analyser le magnétisme d'un matériau en 2D[1117].

[1110] Voir la technique à base d'atomes de Rydberg décrite dans Quantum sensing using circular Rydberg states de Rémi Richaud, LKB, novembre 2018 (41 slides). Voir aussi la thèse Rubidium vapors in high magnetic fields de Stefano Scotto, novembre 2017 (168 pages).

[1111] Voir cette présentation des applications des SQUIDs : SQUID Fundamentals and Applications par Robin Cantor, 2017 (48 slides).

[1112] Après agrandissement optique, la fluorescente peut être analysée par un capteur d'image CCD.

[1113] Source de l'illustration : Centres NV du diamant : du matériau aux applications de Jean-François Roch, Collège de France, 2015 (52 slides).

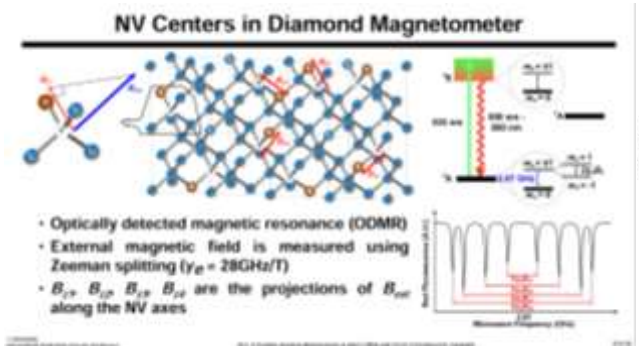
[1114] La précision de la magnétométrie à centres NV s'évalue avec une formule du type $1\mu T/\sqrt{Hz}$.

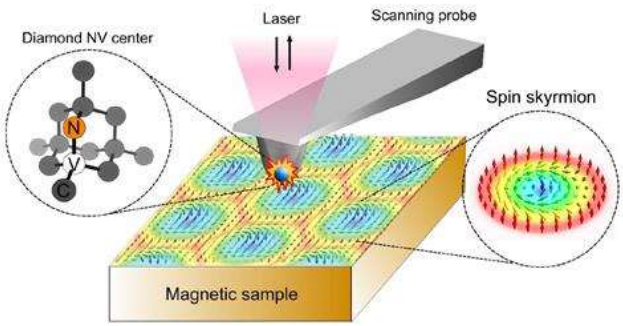
[1115] ASTERIQS (France, 9,7M€) ou "Advancing Science and Technology through diamond Quantum Sensing" est un projet du Quantum Flagship européen lancé en 2018 et mené par Thales qui devrait permettre de faire avancer les techniques de mesure de champs magnétiques, électriques, de température et de pression. Les applications sont nombreuses comme les capteurs de contrôle des batteries de véhicules, les capteurs haute résolution pour l'imagerie médicale nucléaire (RMN, résonance magnétique nucléaire). ou pour créer des analyseurs de spectre de radiofréquences. La startup suisse Qnami est impliquée dans le projet et fournit des diamants artificiels.

[1116] L'illustration provient de A Scalable Quantum Magnetometer in 65nm CMOS with Vector-Field Detection Capability par Mohamed Ibrahim du MIT 2019 (51 slides). Elle décrit un procédé de miniaturisation de magnétomètre quantique associant un circuit CMOS 65 nm fabriqué par TSMC et un système à base de NV-center en diamant.

[1117] Source de l'illustration : Probing and imaging nanoscale magnetism with scanning magnetometers based on diamond quantum defects, 2016 (35 slides).

Habituellement, les NV-centers sont utilisés en température cryogénique pour pouvoir fonctionner mais certains fonctionnent à température ambiante[1118].





Les laboratoires de Bristol, de l'Université d'Ulm en Allemagne et de Microsoft travaillent sur l'utilisation de techniques de NV Centers couplée à du machine learning et de méthodes d'inférence bayésiennes permettant de corriger le bruit constaté à plus haute température[1119].

QuSpin (2012, USA) développe un magnétomètre optique qui se positionne en alternative aux magnétomètres en centres NV.

Qubic (2019, Canada) est une startup issue de l'Institut Quantique de l'Université de Sherbrooke au Québec qui travaille sur de la métrologie quantique, sans plus de précision à ce stade.

SBQuantum (2019, Canada) aussi dénommée SBTech et Shine Bright Technologies développe des magnétomètres quantiques à base de NV centers. Ils ciblent notamment le marché automobile mais travaillent aussi sur l'intégration de leur technologie dans des satellites de type Cubesat[1120]. C'est une startup issue de l'Institut Quantique de l'Université de Sherbrooke du Québec.

La technique est dénommée « Optically Pumped Magnetometer (OPM) ». Ils ont même développé une version tri-axiale de leur système qui mesure le magnétisme en X, Y et X. La recherche sur ce produit a été financée par le NIH (National Health Institute, l'Inserm américain). Et pourquoi donc ? Parce que le produit est notamment utilisé pour faire de l'imagerie cérébrale dans le cadre de magnétoencéphalographie.

Qutools (2005, Allemagne) propose son magnétomètre quantique quNV, à base de NV-centers de diamants comme son nom l'indique. Il tient dans un rack 3U.

Toujours, en Allemagne, l'Université de Stuttgart travaille avec le Fraunhoffer Institute pour transférer la technologie de la magnétométrie à base de NV-centers dans le cadre du projet **QMag**[1121].

[1118] Voir CMOS-Integrated Diamond Nitrogen-Vacancy Quantum Sensor par Donggyu Kim et al, 2018 (7 pages).

[1119] Voir Magnetic-Field Learning Using a Single Electronic Spin in Diamond with One-Photon Readout at Room Temperature de Raffaele Santagati et al, 2018 (18 pages).

[1120] Voir Un magnétomètre quantique de Sherbrooke jusqu'en orbite, IciPremière, octobre 2019.

[1121] Voir Quantum Magnetometers for Industrial Applications, avril 2019.

Supracon (2001, Allemagne) fabrique des magnétomètres à base de SQUIDs (Superconducting Quantum Interference Devices). C'est une spin-off de l'Institut de Photonique Leibnitz de Iéna.

Great Lakes Crystal Technologies (2019, USA) est un fournisseur de diamants utilisables notamment dans les applications exploitant des NV centers, surtout en métrologie quantique à base de magnétomètres quantiques. C'est une spin-off de l'Université du Michigan et de Fraunhofer USA.

FieldLine Inc (2020, USA) développe des systèmes de métrologie magnétiques quantiques à base de NV centers notamment dans l'imagerie médicale du cerveau ainsi que pour le contrôle non destructif de matériaux.

Q-Sensorix (2019, USA) développe des gyroscopes à base de magnétomètres en NV centers, lancée par Alexey Akimov, Vladimir Shalaev et Yuri Lebedev qui sont comme leur nom l'indique d'origine russe. Ce sont des anciens de l'Université de Buffalo dans l'Etat de New York.

Twinleaf (2007, USA) développe des magnétomètres de précision à base de lasers à base de métaux alcalins. La société est dirigée par Elisabeth Foley, une spécialiste du domaine, ainsi que par Thomas Kornack (CSO), tous les deux des anciens de Princeton.

L'**Ivar Giæver Geomagnetic Laboratory** (IGGL) en Norvège utilise aussi des SQUIDs, pour détecter le magnétisme sous-terrain pour des applications de paléomagnétisme, pour mesurer la rémanence magnétique de roches anciennes. Utilisant des SQUIDs, leur magnétomètre doit être refroidi à 4K avec une tête pulsée dont nous avons étudié le principe dans la partie dédiée à la cryogénie des calculateurs quantiques de ce document[1122].

Thermomètres quantiques

La technique des NV centers a un autre usage : la mesure de la température avec une précision de quelques mK et avec une très grande résolution spatiale, le tout avec des capteurs miniaturisés. C'est à ce jour la technologie de mesure de température la plus performance sur ces différentes dimensions. Cela permet par exemple de déterminer la température au sein de cellules vivantes[1123].

[1122] Voir Instruments for Paleomagnetic Measurements WSGI (2G) Model 755 Superconducting Rock Magnetometer (SRM),

[1123] Voir Nanometre-scale thermometry in a living cell, 2013 (6 pages).

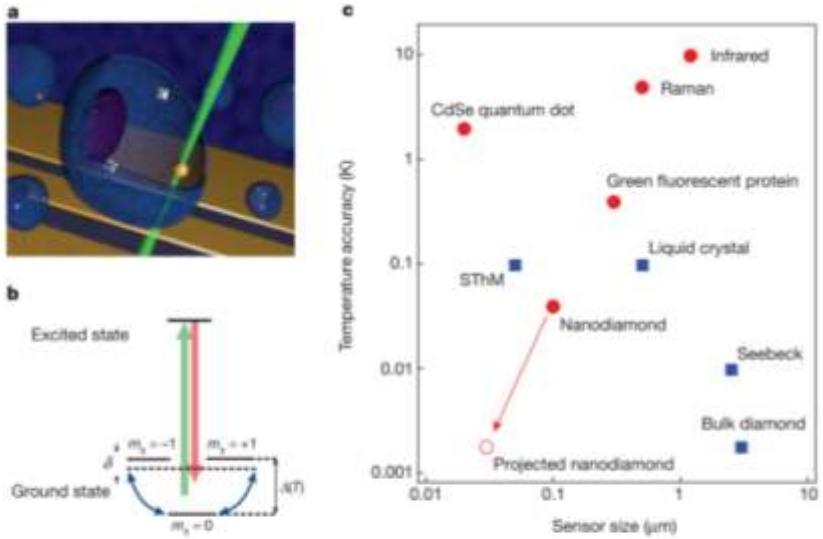
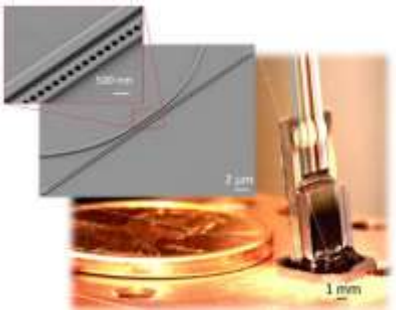


Figure 1 | Nitrogen–vacancy-based nanoscale thermometry. **a**, Schematic image depicting nanodiamonds (grey diamonds) and a gold nanoparticle (yellow sphere) within a living cell (central blue object; others are similar) with coplanar waveguide (yellow stripes) in the background. The controlled application of local heat is achieved by laser illumination of the gold nanoparticle, and nanoscale thermometry is achieved by precision spectroscopy of the nitrogen–vacancy spins in the nanodiamonds. **b**, Simplified nitrogen–vacancy level diagram showing a ground-state spin triplet and an excited state. At zero magnetic field, the $|\pm 1\rangle$ sublevels are split from the $|0\rangle$ state by a temperature-dependent zero field splitting $\mathcal{A}(T)$. Pulsed microwave radiation is applied (detuning, δ) to perform Ramsey-type spectroscopy. **c**, Comparison of sensor sizes and temperature accuracies for the nitrogen–vacancy quantum thermometer and other reported techniques. Red circles indicate methods that are biologically compatible. The open red circle indicates the ultimate expected accuracy for our measurement technique in solution (Methods).

Il existe aussi des solutions de mesure de température dans la matière biologique par fluorescence à base de quantum dots[1124].



En 2017, le NIST produisait un thermomètre quantique en photonique de taille très réduire et servant à mesurer optiquement la température à la surface de métaux. La photo ne montre cependant pas l'électronique de contrôle associée au capteur.

Southwest Sciences (1985, USA) développe notamment des capteurs de température optiques à base de NV centers utilisables dans les systèmes cryogéniques. La société a été fondée par Alan C. Stanton et Joel A. Silver.

Imagerie et microscopes

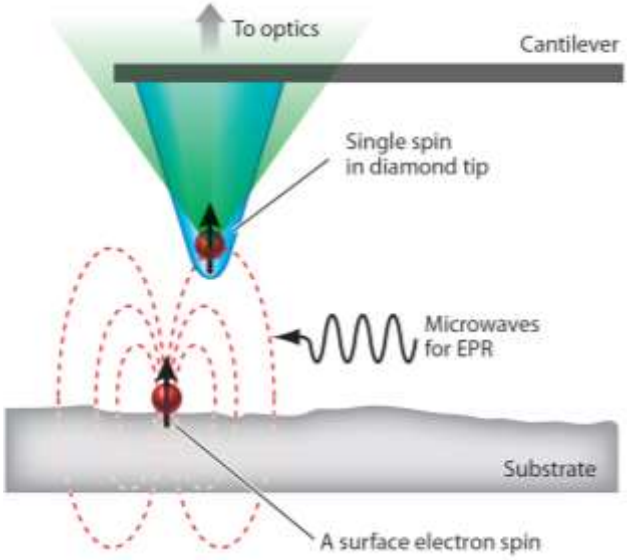
Des microscopes de nouvelle génération s'appuient sur des effets quantiques. Nous allons faire un tour du côté des microscopes utilisant des magnétomètres à base de NV-centers de diamants ou d'atomes froids, des mystérieux systèmes de « ghost imaging » qui font des photos d'objets avec un capteur à un seul pixel et autres capteurs quantiques originaux.

L'imagerie à base de NV-centers est l'un des axes du laboratoire **Max Planck Institute for Solid State Research** et du **Fraunhofer Institute** for Applied Solid State Physics (IAF) à Fribourg en Allemagne. Leurs microscopes servent à analyser des molécules organiques avec une excellente résolution spatiale.

Ils travaillent aussi sur des spectroscopes à spins d'électrons (ESR : electron spin resonance spectroscopy) à température cryogénique qui permettent d'examiner des atomes et des molécules au niveau du spin de leurs électrons. La technique est intégrée dans des microscopes à effet tunnel. Le spin des électrons des matériaux examinés est excité par un champ magnétique et des micro-ondes.

[1124] Voir Intracellular thermometry with fluorescent sensors for thermal biology par Kohki Okabe et al, 2018 (15 pages).

La technique des NV-centers permet d'examiner un disque dur avec une sonde dotée d'un seul NV-center (*ci-dessous*[1125] *et ci-contre*[1126]). Elle sert aussi à faire de la caractérisation (contrôle qualité) de circuits intégrés travaillant dans des fréquences millimétriques comme ceux de la 5G[1127]. D'autres encore travaillent sur la microscopie de cellules vivantes[1128]. Une application existe même pour qualifier les patients atteints de malaria, par l'analyse de nanocristaux de l'hémozoïne qui apparait dans les globules rouges affectés par le parasite de la maladie[1129]. Ces techniques sont utilisées dans la microscopie confocale. Celle-ci génère des images avec une très faible profondeur de champ d'environ 400 nm générant des sections optiques de l'échantillon à analyser.



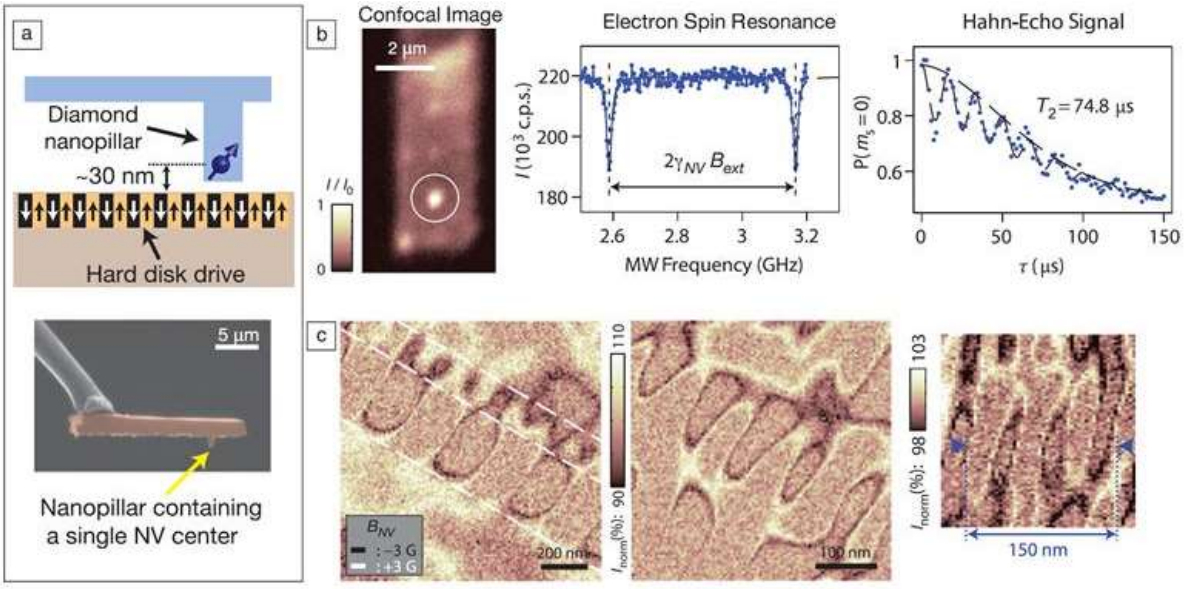


Figure 4. (a) Schematic of a monolithic diamond nanopillar probe (top) and representative SEM image of the nanopillar probe (bottom). (b) Characteristics of a nanopillar probe device. Confocal image of the device (left) clearly shows a localized fluorescence spot from a single NV center at the position of the nanopillar. Electron spin resonance (middle) was acquired with an enhanced fluorescence of 220,000 photons/sec. The coherence time of the measured Hahn-echo signal (right) is 74.8 μs, an order of magnitude longer than a typical Hahn-echo coherence time of commercial diamond nanocrystals (~5 μs). (c) Magnetic images of a hard disk drive acquired by the nanopillar probe. Alternating magnetic bits were imaged with varying sizes down to 25 nm (right), indicating the distance between a single NV center at the probe and the hard disk sample is roughly within 25 nm. Adapted with permission from Reference 19. © 2012 Nature Publishing Group.

[1125] Source de l'illustration : Solid-State Spin Quantum Computers (21 slides) et Optical far-field super-resolution microscopy using nitrogen vacancy center ensemble in bulk diamond, 2016 (5 pages) qui décrit une technique de microscopie avec une résolution descendant à 6 nm.

[1126] Source de l'illustration : Nitrogen-Vacancy Centers in Diamond: Nanoscale Sensors for Physics and Biology, 2014 (27 pages).

[1127] Voir Microwave Device Characterization Using a Widefield Diamond Microscope, 2018 (10 pages) qui implique notamment le LSPM de Paris.

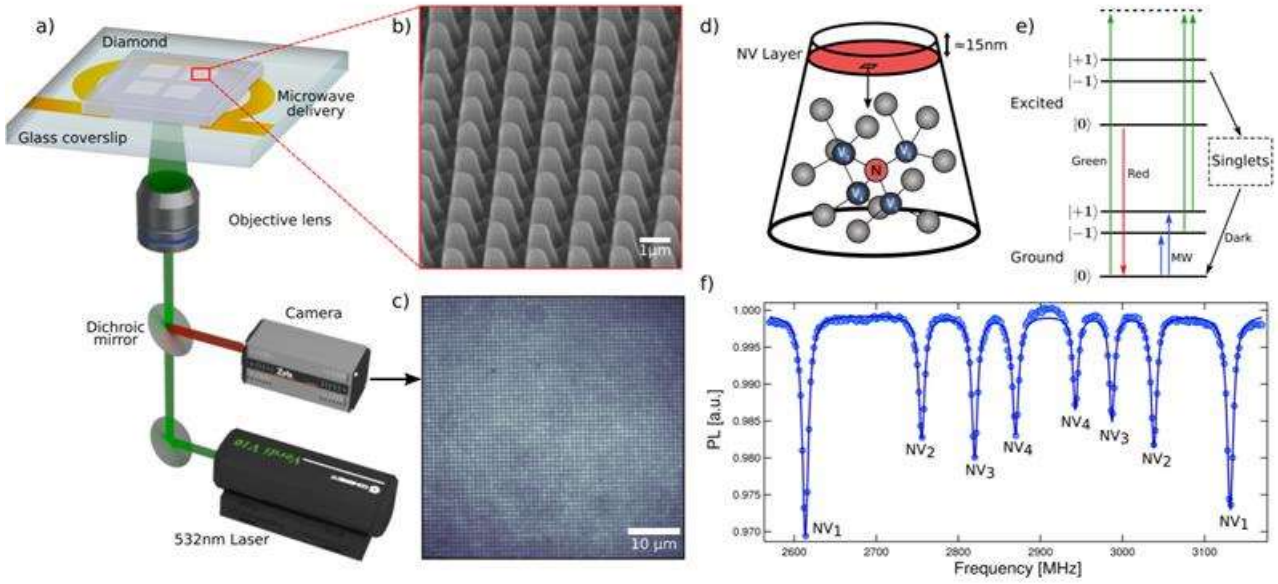
[1128] Voir A fluorescent nanodiamond foundation for quantum sensing in cells, 2018 (147 pages) qui évoque la microscopie de cellules vivantes.

[1129] Voir Diamond magnetic microscopy of malarial hemozoin nanocrystals d'Ilja Fescenko & A, septembre 2018 (17 pages),

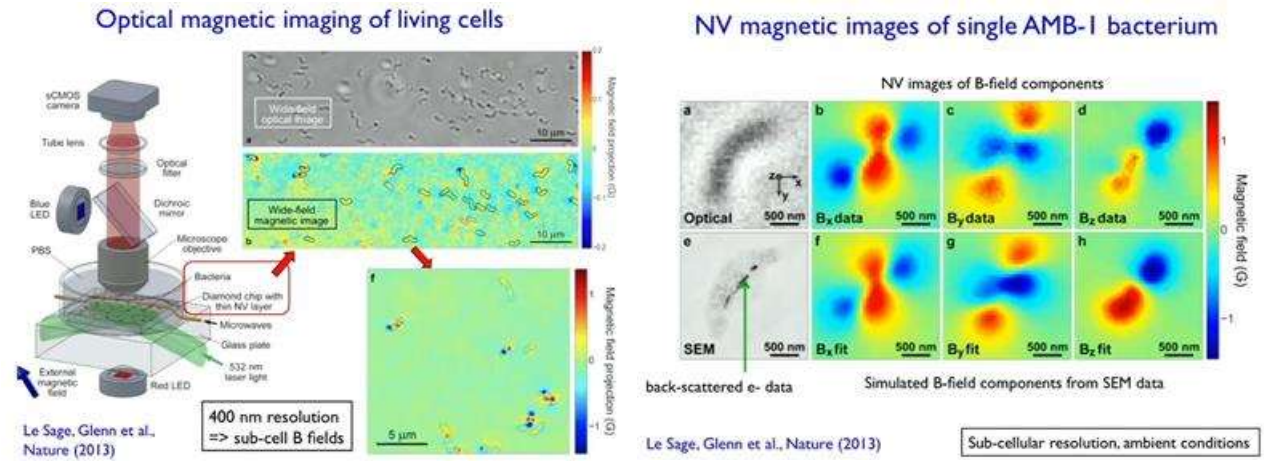
En modifiant la position du plan focal en profondeur, on réalise des séries d'images servant ensuite à générer sur ordinateur une vue en 3D de l'échantillon analysé. La source lumineuse est réfléchie ou obtenue par fluorescence en réaction à un rayon laser. Ce qui donne un microscope confocal à balayage laser, et, en anglais, un CLSM pour Confocal Laser Scanning Microscope.

Les NV-centers permettent aussi d'améliorer la précision des optiques adaptatives qui sont notamment utilisées en astronomie[1130].

D'autres techniques utilisant de l'interférométrie laser permettent d'examiner les molécules au niveau atomique dans leur milieu et non pas sous vide et dans un froid cryogénique[1131].



L'imagerie peut aussi exploiter une matrice de centres NV de petite taille qui procure une bien meilleure résolution que les systèmes d'imagerie à base de magnétomètres SQUIDs. Les deux exemples *ci-dessus* en montrent l'architecture[1132].



[1130] Voir Nanodiamonds enable adaptive-optics enhanced, super-resolution, two-photon excitation microscopy, 2019 (7 pages).

[1131] Voir An Entanglement-Enhanced Microscope de Takafumi Ono, Ryo Okamoto, Shigeki Takeuchi, 2014 (8 pages).

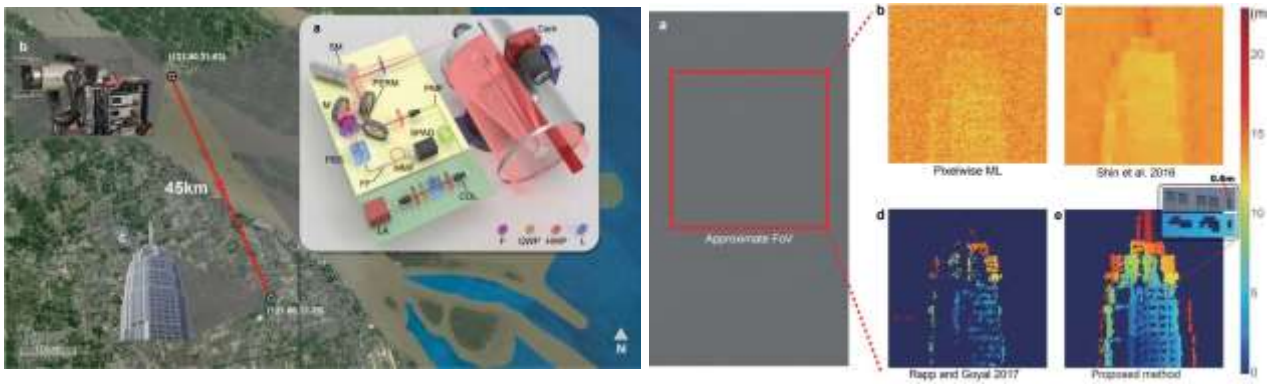
[1132] Voir Enhanced widefield quantum sensing with nitrogen-vacancy ensembles using diamond nanopillar arrays de D. J. McCloskey, 2019 (7 pages). Les matrices de centres NV expérimentées font 100 µm de côté. L'illustration provient d'autres travaux publiés en 2013, cités dans la conférence Magnetic imaging using NV-diamond: techniques & applications de Ronald Walsworth, 2015 (51 mn). Notamment Optical magnetic imaging of living cells, Le Sage et al, Nature, 2013 (11 pages).

Pour le second, il s'agissait d'étudier des bactéries qui contiennent de micro-éléments magnétiques. Dans d'autres cas, on peut utiliser des marqueurs magnétiques qui vont s'attacher aux cellules à détecter, typiquement en cancérologie.

Dans le Flagship Quantique européen, on compte **MetaboliQs** (Allemagne, 6,7M€), est un projet d'imagerie médicale cardiaque de résonance magnétique nucléaire à base de diamants. On détecte aussi la fibrillation atriale, une pathologie cardiaque courante, avec un magnétomètre atomique à base de rubidium[1133]. Un autre projet du Flagship, **PhoG** (Royaume Uni, 2,6M€) ou "Sub-Poissonian Photon Gun by Coherent Diffusive Photonics", ambitionne de créer de sources de lumières stables pour des applications diverses, notamment en métrologie quantique. Il implique aussi des chercheurs en Biélorussie, Allemagne et en Suisse.

Le laboratoire Chinois de Jian-Wei Pan a mis au point une caméra qui analyse la réflexion d'un photon unique par pixel sur l'objet à observer. Le tout est associé à des algorithmes qui filtrent le bruit. L'imagerie est réalisée dans l'infrarouge à 1550 nm et avec des photons polarisés. L'objectif ? Intégrer cette technologie dans des satellites d'observation[1134].

Autre application, celle de LIDARs à photons uniques. Elle sert à la détection du vent à distance à haute résolution. Elle est réalisée en Chine depuis 2014 et mise en pratique dans des radars transportables y compris dans des drones[1135].



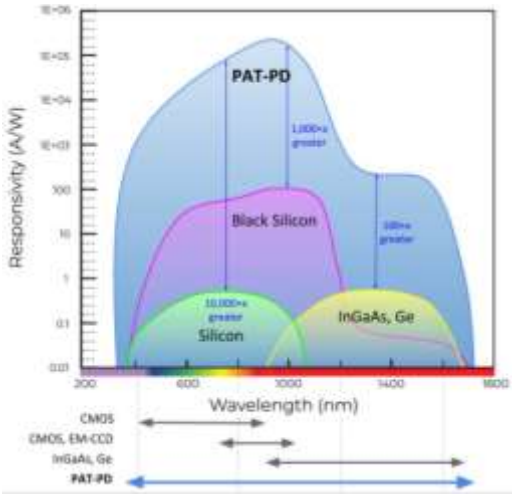
Dans le même ordre d'idée, **QLM Technology** (2017, UK) a développé une solution de magnétomètre quantique qui détecte les fuites de méthane dans les pipelines jusqu'à une distance de 100 mètres. Le système de mesure pesant quelques kg peut-être embarqué dans un drone de grande envergure volant à 50 km/h. Ils utilisent un laser qui éclaire un milieu gazeux d'opacité variable et un photodétecteur. **IDQ** est impliqué dans la création de la solution au niveau du LiDAR.

[1133] Voir New quantum technology could help diagnose and treat heart condition, mars 2020.

[1134] Voir A new camera can photograph you from 45 kilometers away, mai 2019 qui fait référence à Single-photon computational 3D imaging at 45 km par Zheng-Ping Li et al, avril 2019 (22 pages). Et la présentation Single Photon LiDAR par Feihu Xu, juin 2019 (25 slides).

[1135] Voir Single-Photon Lidar for atmospheric detection par Haiyun Xia et al, juin 2019 (22 slides).

Seedevices (2017, USA) développe un système d'imagerie quantique, le PAT-PD (Photon Assisted Tunneling- Photo Detector), qui dépasse les performances des imageurs CMOS traditionnels. Cet imageur contient des photosites utilisant l'effet tunnel capables de détecter des photons uniques et dans une large bande de longueurs d'ondes allant du proche infrarouge (1800 nm) à l'ultraviolet (jusqu'à l'UVA1, à 350 nm). Cela peut servir à voir dans le noir et pour de l'imagerie médicale (de vaisceaux sanguins dans l'infrarouge).



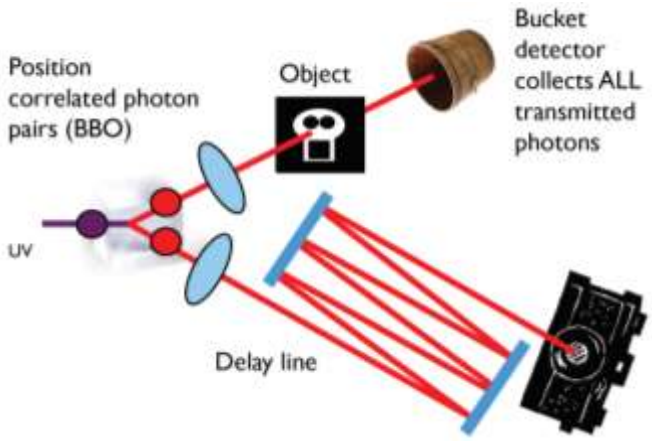
QDTI (2012, USA) est la seule startup connue s'étant initialement lancée dans la mise au point d'un ordinateur quantique à base de NV Centers. Créée par une équipe issue de l'Université d'Harvard, elle est basée logiquement à Boston.

La startup planche surtout sur des systèmes d'imagerie médicale utilisant aussi ces NV centers, avec la création de magnétomètres de précision associés à de l'IRM ainsi qu'à des tests immunologiques. La société n'a pas l'air d'être particulièrement active depuis 2016. La dernière actualité sur leur site date de juillet 2018.

Lucigem (2016, Australie) fabrique des nano-diamants fluorescents utilisables dans les différentes applications quantiques, en particulier pour de l'imagerie médicale. La société est issue de travaux réalisée dans la Macquarie University de Sydney.

Nvision Imaging (2015, Allemagne) développe une solution d'imagerie médicale IRM à base de NV centers.

L'imagerie quantique peut aussi faire appel à la curieuse technique du ghost imaging ou imagerie fantôme quantique. Elle existe sous de nombreuses déclinaisons. La première en date utilisait un générateur de photons infrarouges intriqués en 1995[1136]. Une moitié des photons éclaire l'objet et l'autre un capteur photo, en traversant une ligne à retard optique[1137]. Les photons qui éclairent l'objet sont intriqués avec ceux qui éclairent la caméra, ces derniers n'ayant pas vu l'objet ! L'image obtenue est très bruitée et nécessite un traitement idoine.



[1136] Voir Optical imaging by means of two-photon quantum entanglement, par Yanhua Shih et al, 1995 (4 pages), de l'Université de Maryland. Et Observation of two-photon 'ghost' interference and diffraction, Yanhua Shih, 1995 (4 pages).

[1137] An introduction to ghost imaging: quantum and classical par Miles Padgett et Robert Boyd, 2016 (10 pages) fait un bon tour d'horizon du sujet. Voir aussi Quantum Ghost Image Identification with Correlated Photon Pairs, 2010 (4 pages).

A quoi cela peut-il bien servir ? Principalement à analyser des objets avec un très faible nombre de photons pour éviter que ceux-ci modifient l'objet à analyser. Cela peut être intéressant en microbiologie[1138]. Visiblement, les objets analysés sont toujours de petite taille[1139].

D'autres techniques, non quantiques, utilisent un imageur couleur doté d'un seul pixel et exploitant 1300 éclairages structurés par seconde éclairant l'objet pendant quelques secondes.

Le capteur comprend quatre photodiodes positionnées à des endroits différents [1140]. Cela permet de générer une vue 3D de l'objet.

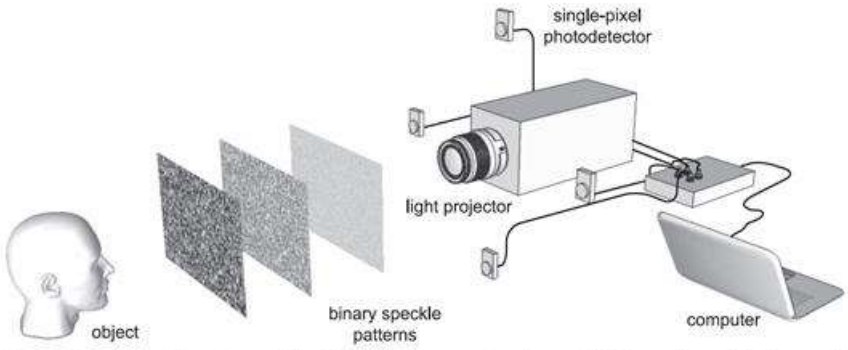
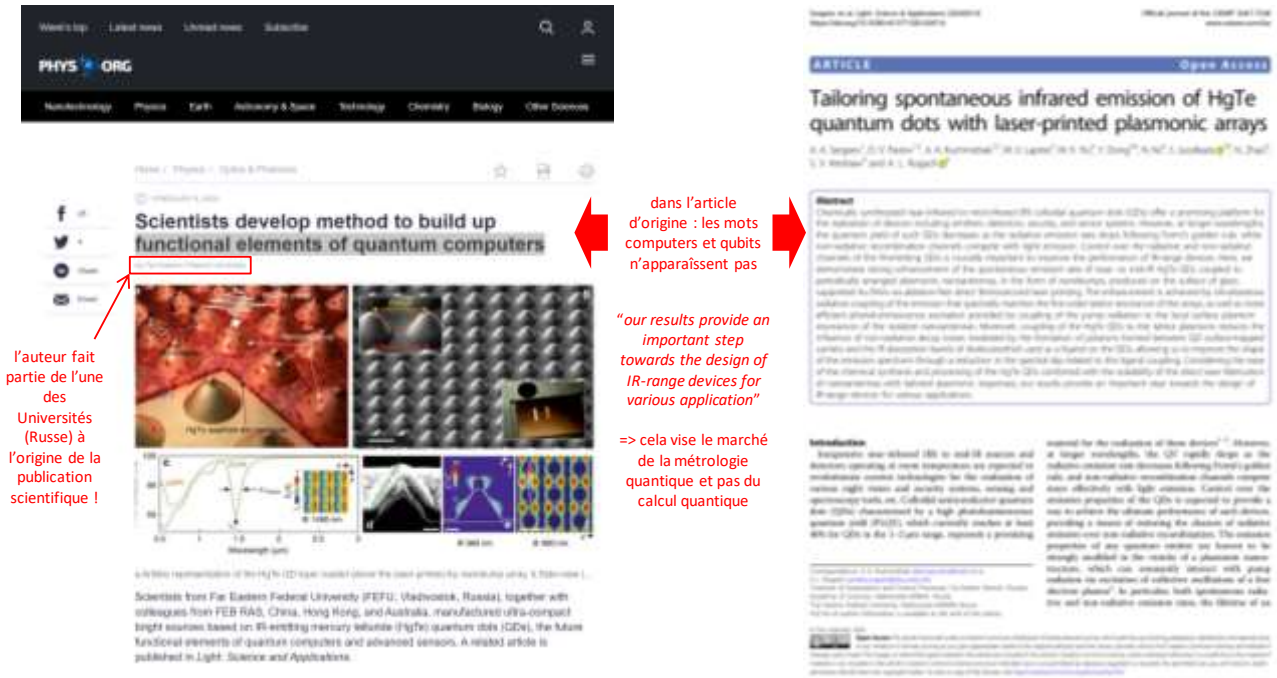


Fig. 1. Experimental setup used for 3D surface reconstructions. The light projector illuminates the object (head) with computer-generated random binary speckle patterns. The light reflected from the object is collected on four spatially separated single-pixel photodetectors. The signals from the photodetectors are measured and used to reconstruct a computational image for each photodetector.

Enfin, l'imagerie quantique peut s'appuyer également sur l'illumination de l'objet par micro-ondes intriquées, reprenant le principe du radar quantique que nous allons voir dans la partie suivante. Elle est intéressante pour analyser des objets à faible réflectivité, ce qui serait utile en imagerie médicale comme pour créer des radars courte-portée[1141].



[1138] Voir The Dawn of Quantum Biophotonics de Dmitri Voronine et al, 2016 (30 pages).

[1139] Voir ce panorama de nombreux méthodes de ghost imaging : The promise of quantum imaging de Robert Boyd, 2016 (53 slides).

[1140] Voir Fast full-color computational imaging with single-pixel detectors de Stephen Welsh et al, 2013 (7 pages). Vu aussi dans 3D Computational Imaging with Single-Pixel Detectors, 2013 (4 pages) qui étend cela à la capture d'objets en 3D grâce à quatre capteurs à un pixel. Le projecteur vidéo créé des patterns qui éclairent l'objet et alternent avec leur négatif. Voir enfin Imaging with a small number of photons, Peter Morris et al, 2014 (9 pages) et Quantum-inspired computational imaging, 2019 (9 pages).

[1141] Voir Experimental Microwave Quantum Illumination par S. Barzanjeh et al, août 2019.

Notons que le thème de l'imagerie quantique peut parfois prêter à confusion. Elle est énorme dans cette promotion d'un type particulier de quantum dot, confondu avec une technique d'ordinateur quantique (*ci-dessus*). Et là, ce n'est pas un problème de journaliste approximatif puisque l'article « fautif » provient du laboratoire à l'origine de la bévue de communication[1142].

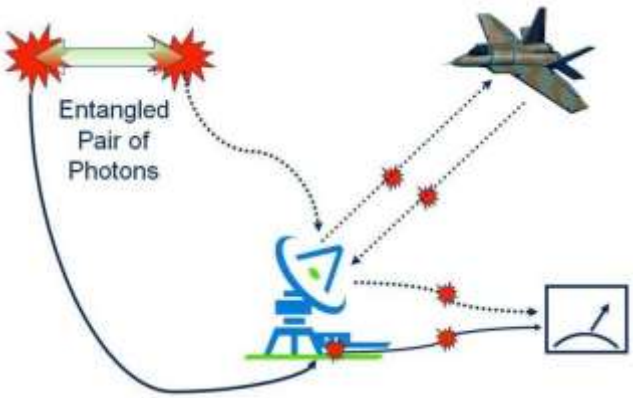
Radars quantiques

Les radars quantiques sont en train d'émerger lentement de la recherche. Ils s'appuient sur des photons dans le visible, et de trois manières différentes :

- Le radar émet des photons classiques dans le visible et reçoit le photon réfléchi par la cible. Cela ne fonctionne pas très bien à cause des nuages et du bruit lumineux environnant l'objet.
- Le radar émet des photons mais utilise des capteurs photo-sensibles quantiques pour améliorer sa performance. Cela ne fonctionne pas suffisamment mieux.
- Le radar prépare des paires de photons intriqués. L'un est envoyé vers la cible et réfléchi et l'autre reste dans le radar. Le photon réfléchi est comparé avec celui qui est resté sur place. Comme ils ont un passé commun, il est possible de faire le tri dans les photons reçus par le radar pour ne conserver que les photons réfléchis par la cible.

C'est en fait une variante de la troisième manière qui est étudiée. Elle consiste à convertir les photons envoyés vers la cible en onde radio, tout en préservant une partie de leur état quantique. Une conversion du même genre a lieu pour le photon resté dans le radar. Cela permet aux ondes radar de traverser les intempéries ce que les photons dans le visible ne peuvent pas faire.

Cette technique est censée améliorer la précision des radars traditionnels et d'améliorer sa résistance au bruit et au brouillage. Ce genre de radar pourrait en théorie détecter des avions furtifs, modulo le fait que leurs surfaces réfléchissantes planes réduisent leur signature radar quelle que soit la fréquence employée.



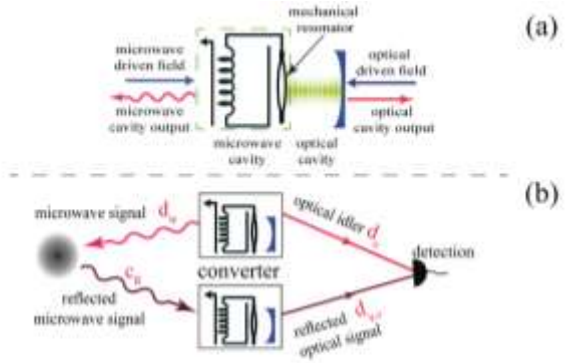


FIG. 1. (a) Schematic of the electro-opto-mechanical (EOM) converter in which driven microwave and optical cavities are coupled by a mechanical resonator. (b) Microwave-optical QI using EOM converters. The transmitter's EOM converter entangles microwave and optical fields. The receiver's EOM converter transforms the returning microwave field to the optical domain while performing a phase-conjugate operation.

[1142] Voir Scientists develop method to build up functional elements of quantum computers par la Far Eastern Federal University, février 2020, qui fait référence à Tailoring spontaneous infrared emission of HgTe quantum dots with laser-printed plasmonic arrays par A.A. Sergeev et al, 2020 (10 pages). Le quantum dot a l'air d'être plutôt adapté à de la vision nocturne qu'à du calcul quantique. Ce n'est pas une source de photons uniques. Et les mots « computer » et « qubit » sont absents dans l'article.

Autant dire néanmoins que cela intéresse beaucoup les Chinois qui travaillent d'arrache-pied dessus pour pouvoir détecter les avions furtifs américains comme les F-22 et B-2. Ils ont annoncé avoir testé leur premier radar quantique en 2016 qui passait à l'état de prototype en 2018, réalisé par la société gouvernementale **China Electronics Technology Group**[1143]. Sans que ses performances précises soient détaillées, au-delà d'une portée de 100 km.

D'autres laboratoires et entreprises mettent au point de tels radars, comme l'**Institute for Quantum Computing** de l'Université de Waterloo au Canada[1144]. C'est un projet financé par le Ministère de la Défense canadien pour $2,7M. Il y en a aussi en Autriche à l'Institute of Science and Technology de Klosterneuburg. Aux USA, **Lockheed Martin** est aussi investi dans ce domaine émergent.

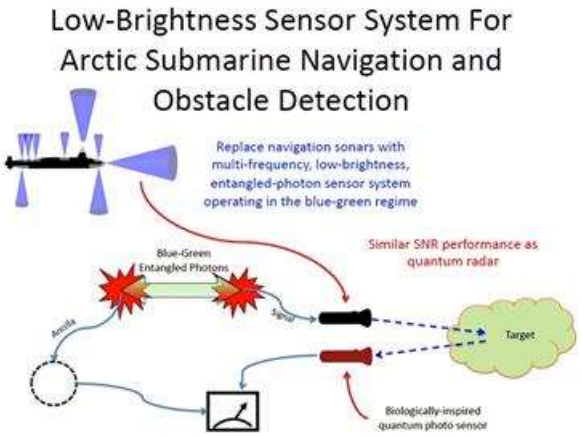
L'utilisation de photons intriqués permet aussi de résister efficacement aux systèmes de brouillage. Les premiers concepts ont vu le jour en 2015[1145].

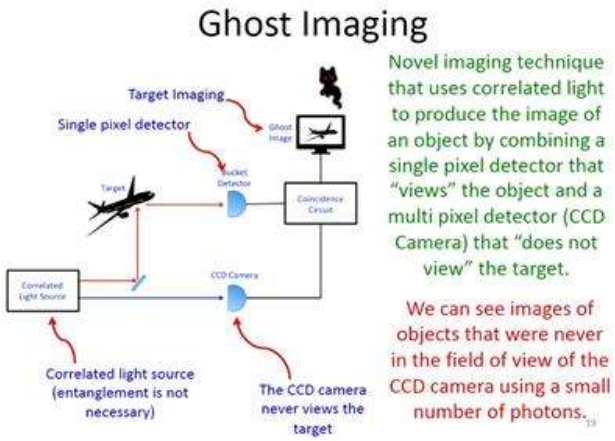
Elle pourrait être employée dans des LiDARs pour vérifier que les photons qui arrivent dedans correspondent bien à ceux qui ont été émis par ses lasers, échappant ainsi à un brouillage optique inopportun. Sans brouillage malintentionné, cela sera très utile lorsque de nombreux véhicules autonomes équipés de LiDARs devront cohabiter sur la route[1146].

Des spécialistes du sujet comme Marco Lanzagorta de l'US Naval Research Laboratory pensent que les satellites de QKD lancés par les Chinois comme Micius auraient des applications militaires de ce type[1147].

Dans un domaine voisin des radars, les sonars quantiques pourraient aussi émerger, si l'on peut dire. Ils utilisent des photons dans la zone bleue-verte du spectre visible et seraient utilisables pour la navigation dans l'océan arctique.

Ce serait en quelque sorte des LiDAR quantiques. Ces systèmes pourraient aussi mettre en œuvre une communication optique avec les sous-marins passant par satellite, histoire de remplacer les ondes radios qui pénètrent mal sous l'eau et sont exploitables pour des liaisons à très bas débit.





[1143] Voir China's claim of developing "quantum radar" for detecting stealth planes: beyond skepticism par Ashish Gupta, 2016 (4 pages) qui analyse cette information avec circonspection, sans pour autant affirmer clairement que les Chinois racontent des salads sur le sujet et The US and China are in a quantum arms race that will transform warfare, par Martin Giles, janvier 2019.

[1144] Voir Quantum radar will expose stealth aircraft, avril 2018.

[1145] Voir Focus: Quantum Mechanics Could Improve Radar, 2015, Microwave Quantum Illumination de Shabir Barzanjeh et al, 2015 (5 pages) qui est la source de l'illustration FIG 1, et Enhanced Sensitivity of Photodetection via Quantum Illumination par Seth Lloyd, 2018 (4 pages).

[1146] Cette approche est étudiée depuis au moins 2009. Voir Quantum Lidar – Remote Sensing at the Ultimate Limit, 2009 (97 pages).

[1147] Voir The Future of Quantum Sensing & Communications, par Marco Lanzagorta de l'US Naval Research Laboratory (USA), septembre 2018 (37 minutes). J'ai extrait deux illustrations de cette page de la vidéo de son intervention (sur les sonars et les caméras fantomes. Il est l'auteur du livre Quantum Radar qui a été traduit en chinois par la Chine, et officiellement en achetant les droits.

Autre technique envisagée, celle de la génération d'images fantômes, générée par un système couplant une caméra qui ne voit pas l'objet à capter et un capteur de pixel unique qui voit l'objet. Ce genre de technique peut s'appuyer sur l'intrication de photons dans le visible entre les deux capteurs.

D'un autre côté, il faudra peut-être un jour trouver des parades contre des revêtements « quantiques » qui permettent de supprimer ou réduire la signature infrarouge d'objets[1148].

Capteurs chimiques quantiques

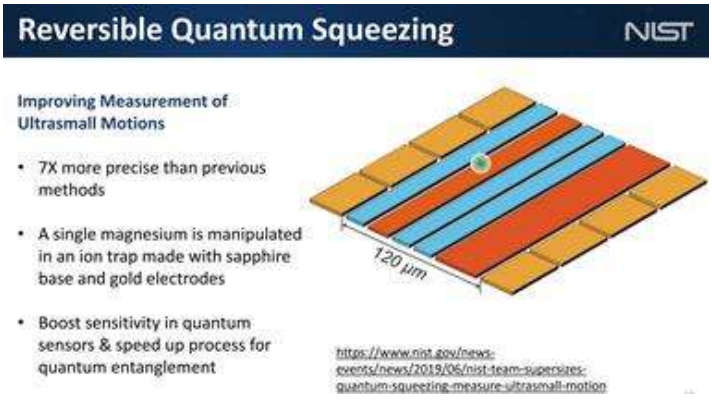
La métrologie quantique est aussi applicable dans les capteurs chimiques qui servent à analyser la composition chimique de matériaux et substances diverses. Elle est couramment employée avec des interféromètres optiques[1149].

Entanglement Technologies (2010, USA) est une spin-off de Stanford et Caltech qui propose le détecteur de gaz quantique AROMA (Autonomous Rugged Optical Multigas Analyzer) exploitant des lasers et des résonateurs optiques voisins de ceux qui ont servi à la détection des ondes gravitationnelles dans le LIGO, avec une technique de spectroscopie (CRDS : Cavity Ring-Down Spectroscopy, à ne pas confondre avec la CRDS inventée sous Michel Rocard). Il permet notamment de détecter les gaz dangereux dans l'industrie, notamment d'extraction des énergies fossiles. Ils ont été financés par EDF, via leur fonds Environmental Defense Fund.

NEMS et MEMS quantiques

Les nano ou macro-structures électromécaniques sont largement utilisées dans les objets connectés depuis longtemps, comme dans les accéléromètres. Ils utilisent de nombreux phénomènes quantiques, notamment à base de photonique, avec des résonateurs mécaniques dont le mouvement est analysé par des lasers et diodes.


At the heart of a new NIST portable pressure sensor is a dual cavity for laser measurements that is only 2.5 cm long.



[1148] Voir Camouflage made of quantum material could hide you from infrared cameras par Kayla Wiles, décembre 2019 qui fait reference à Temperature-independent thermal radiation par Alireza Shahsaf et al, septembre 2019 (17 pages).

[1149] Voir Quantum Optical Technologies for Metrology, Sensing, and Imaging de Jonathan Dowling, 2014 (20 slides) et 12 pages, Advanced Micro- and Nano-Gas Sensor Technology: A Review de Haleh Nazemi et al, 2019 (23 pages).

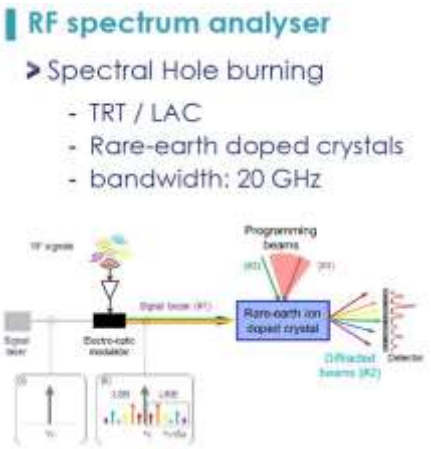
On les retrouve ainsi dans des capteurs de pression quantiques[1150] et des détecteurs de mouvements, tous deux issus du NIST (*ci-dessus*[1151]). D'autres capteurs servent à détecter la résistance électrique, la température, la masse et la force, le vide ou la tension[1152].

Citons enfin le projet Quantum Flagship européen **macQsimal** (Suisse, 10,2M€) ou "Miniature Atomic vapor-Cells Quantum devices for SensIng and Metrology AppLications", de création de capteurs quantiques visant le marché du pilotage des véhicules autonomes et pour l'imagerie médicale. Cela comprend la création d'horloges atomiques, de gyroscopes, de magnétomètres, de systèmes d'imagerie exploitant des micro-ondes et des champs électromagnétiques de l'ordre du tera-Hertz ainsi que des détecteurs de gaz. Bref, une approche assez généraliste. Elle repose sur l'usage de vapeur d'atomes froids intégrés dans des MEMS.

Radiofréquences

L'analyse de radiofréquences est un vieux sujet mais il progresse également grâce aux technologies quantiques associant souvent de l'optronique à des atomes froids.

Cela titille souvent le domaine de l'extrême comme ce récent capteur quantique à base d'atomes alcalins de Rydberg qui peut d'analyse le spectre radio de 1 kHz à 100 GHz[1153] ou cet autre capteur quantique capable d'analyser des ondes radio dans la bande du 1 THz, intermédiaire entre l'infrarouge et les micro-ondes, avec des applications potentielles dans la mesure d'épaisseur de couches minces de matériaux hétérogènes[1154].



Thales développe aussi des analyseurs de fréquences, avec une bande passante de 20 GHz à base de cristaux dopés aux terres rares[1155].

Tout cela mériterait sans doute d'être étudié plus en détail que dans ces quelques lignes !

[1150] Voir FLOC Takes Flight: First Portable Prototype of Photonic Pressure Sensor, février 2019.

[1151] Voir Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact, 2019 (39 slides).

[1152] Voir Quantum electro-mechanics: a new quantum technology par Konrad Lehnert du laboratoire JILA du NIST (47 slides) et From micro to nano-optomechanical systems: light interacting with mechanical resonators par Ivan Favero (45 slides).

[1153] Voir Scientists create quantum sensor that covers entire radio frequency spectrum par The Army Research Laboratory, mars 2020 et Quantum sensor for entire radio frequency spectrum, mars 2020 qui font référence à Assessment of Rydberg atoms for wideband electric field sensing par David H Meyer et al, janvier 2020 (16 pages).

[1154] Voir Researchers demonstrate first terahertz quantum sensing, mars 2020, qui fait référence à Terahertz quantum sensing par Mirco Kutas et al, 2020 (9 pages).

[1155] Voir Quantum technologies par Thierry Debuisschert, Thales Research & Technology, 2017 (4 slides). Lien mort !

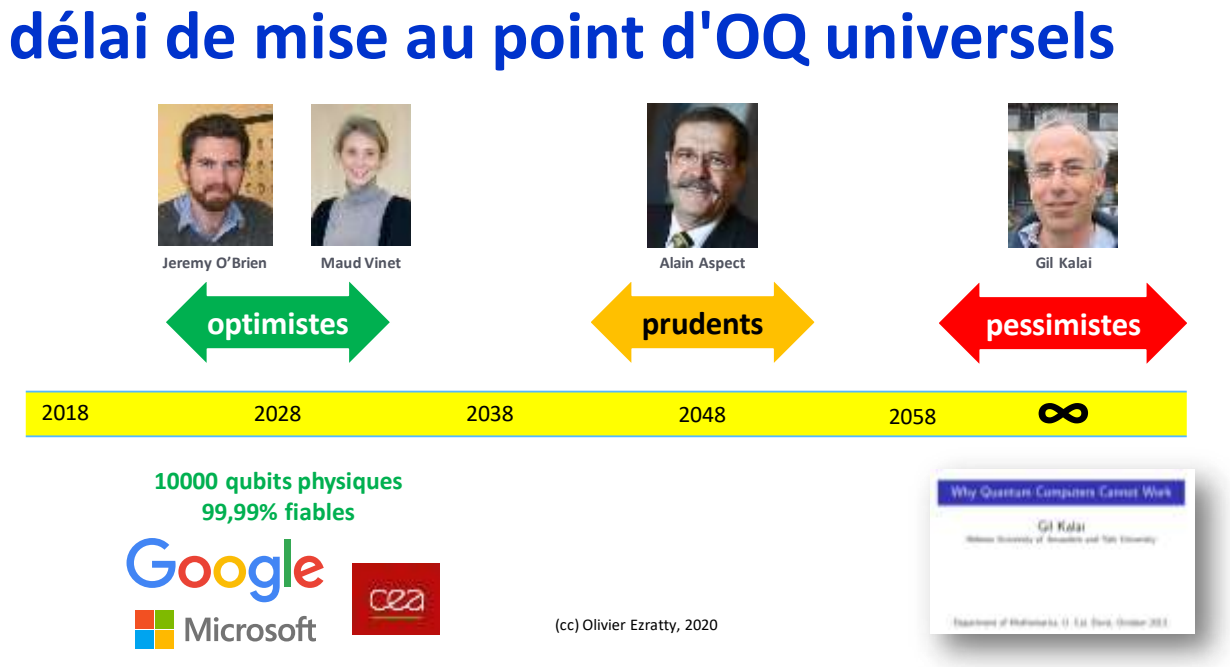
Technologies quantiques dans le monde

L'informatique quantique au sens large du terme est un secteur technologique stratégique à différents titres. Dans la cryptographie, il en va de la souveraineté avec l'enjeu de la protection des communications sensibles. Le calcul quantique est pour sa part porteur d'applications critiques qui vont étendre le champ du numérique au-delà de ce qui est faisable aujourd'hui, notamment dans le domaine de la santé, de l'environnement et de l'intelligence artificielle, prise dans une définition large.

En termes de maturité, la cryptographie quantique et post-quantique représentent des champs plus établis avec des acteurs économiques et des solutions commerciales, même si la standardisation de la cryptographie post-quantique n'est pas achevée. Elle comporte cependant moins d'inconnues scientifiques et d'ingénierie comparativement au calcul quantique scalable.

Le calcul quantique est moins mature. Si l'incertitude scientifique semble en partie levée pour ce qui est de la faisabilité des ordinateurs quantiques exploitables commercialement, les obstacles technologiques restent encore importants à surmonter pour y arriver, notamment l'épineuse question du bruit dans les qubits, de la correction d'erreurs quantiques et des technologies permettant d'augmenter de plusieurs ordres de grandeur le nombre de qubits physiques des calculateurs quantiques.

Les avis sont partagés sur la vitesse de la levée de ces incertitudes : elle va de quelques années pour certains comme chez Google ou Microsoft, à quelques décennies pour des scientifiques comme Alain Aspect, pour atteindre le "jamais" pour des chercheurs tels que l'Israélien Gil Kalai.



C'est donc un domaine à cheval entre l'incertitude scientifique et l'incertitude technologique. La recherche est pour l'instant issue essentiellement du secteur public dans les grands pays qui s'y investissent, puis de très grands acteurs du numérique qui ont de quoi faire plein de paris technologiques en parallèle (Google, Intel, Microsoft, IBM, Alibaba) puis de quelques startups plus ou moins bien financées ou avancées, essentiellement en Amérique du Nord (D-Wave, IonQ, Rigetti).

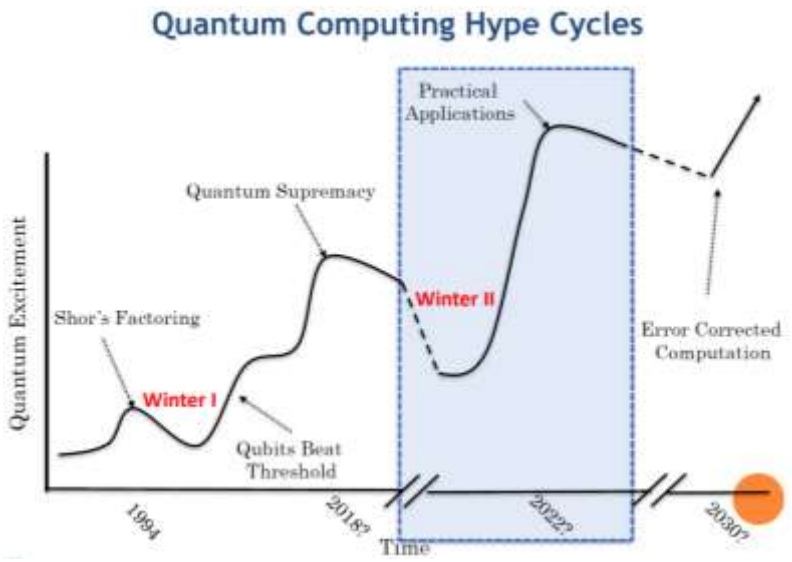
L'industrie des logiciels destinés aux ordinateurs quantiques est balbutiante. La majeure partie des "pure players" de ce secteur sont dédiés aux ordinateurs quantiques adiabatiques du Canadien D-Wave, tels que QxBranch et 1QBit qui sont respectivement Américains et Canadiens.

Les grands acteurs et startups qui planchent sur les calculateurs quantiques ont tous investi dans le logiciel, à commencer par les outils de développement d'algorithmes et d'applications quantiques.

Chacun ambitionne évidemment de créer des plateformes logicielles leaders. Certaines sont déjà disponibles dans le cloud, comme chez IBM. D'autres, tels le Français Atos et Microsoft proposent l'accès via le cloud à des simulateurs quantiques à base d'ordinateurs traditionnels.

Autre manière de voir les choses, celle de **Yuri Alexeev** de l'Argonne National Laboratory aux USA qui fait un parallèle entre l'histoire du calcul quantique et celle de l'intelligence artificielle et anticipe l'arrivée de deux hivers, le premier étant positionné en 2019/20 et le suivant vers 2030[1156].

Mais comme l'excitation sur un sujet est une fonction d'onde un peu floue et difficile à évaluer, cela ne veut pas dire grand-chose. On peut cependant anticiper au minimum un petit hiver concernant les startups du secteur. Celles du matériel mettront beaucoup de temps à livre des machines pratiquement utiles tandis que les startups logicielles n'auront pas un marché adressable bien grand faute de machine. Mais cela n'empêchera pas les laboratoires de recherche publics et les grandes entreprises de la tech de faire de la recherche fondamentale et appliquée.



Investissements mondiaux

Qu'en est-il des investissements mondiaux dans l'informatique quantique ? Une étude de McKinsey de 2015 faisait un tour d'horizon des investissements qui compilaient sans doute des budgets de recherche publique. Il y avait alors 1500 chercheurs dans le monde dotés d'un budget total de $1,5B. Même si ce nombre a dû augmenter depuis, il est très faible. Nous en étions en 2020 à l'état où l'informatique traditionnelle en était à la fin des années 1950 !

Les USA et la Chine y figuraient évidemment en tête. Mais la répartition de ces investissements, qui intègrent probablement aussi bien la cryptographie quantique que les calculateurs quantiques est intrigante pour les autres pays. La France y était en neuvième position, derrière l'Allemagne, le Royaume Uni, le Canada, le Japon la Suisse et l'Australie. Sachant que ces données ont dû évoluer depuis, avec, notamment, un accroissement significatif de l'effort de la recherche de la Chine.

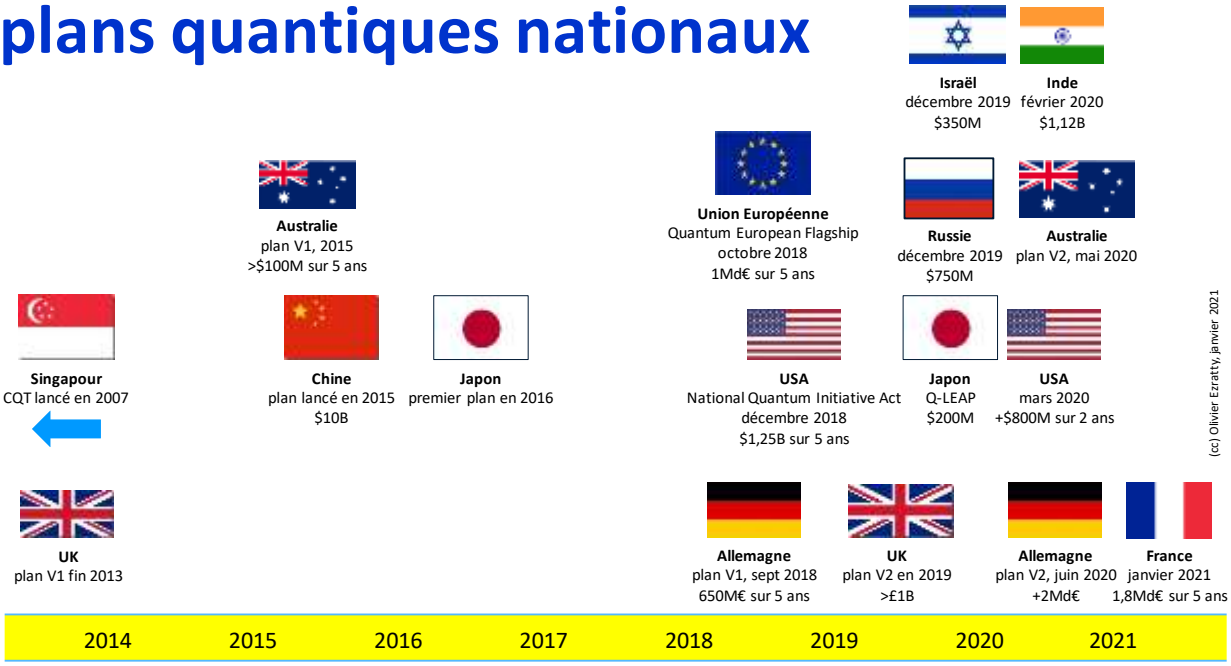
Une étude européenne produite en 2016 reprenait les mêmes chiffres en y ajoutant les effectifs. Avec donc 224 chercheurs en France à comparer à 1217 chercheurs aux USA, ce qui est un ratio tout à fait normal de 1 à 6. Mais le décompte du nombre de ces chercheurs relève de la logique floue, tant il est difficile de départager ceux qui font de la recherche dans la physique fondamentale et ceux qui mettent au point des qubits. Et surtout, ces chiffres commencent à dater.

Les technologies quantiques sont devenues un enjeu géopolitique, presque comme la dissuasion nucléaire[1157]. Les pouvoirs publics de ces différents pays se sont mobilisés de manière très différenciée sur le quantique.

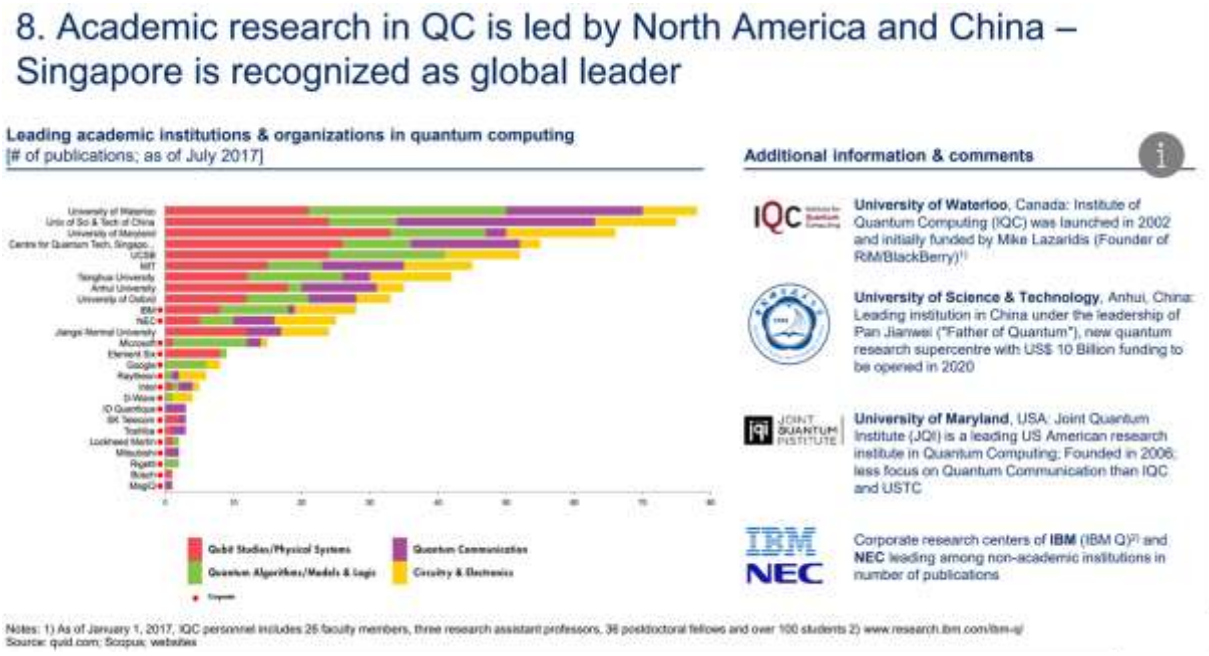
[1156] Voir Quantum Computing Trends par Yuri Alexeev, août 2019 (42 slides).

[1157] Voir à ce sujet Quantum, AI, and Geopolitics (3): Mapping The Race for Quantum Computing, par Hélène Lavoix, 2018.

La plupart des pays développés se sont mobilisés au niveau de leurs pouvoirs publics pour coordonner les efforts dans le quantique. Un pays faisait curieusement défaut dans ce panorama : la France. Elle s'est rattrapée depuis en lançant une mission parlementaire puis un plan quantique national pré-annoncé en septembre 2020 et annoncé par le Président de la République en janvier 2021.



Une évaluation des publications scientifiques dans l'informatique quantique est présentée dans une intéressante étude produite par des étudiants de l'Insead en 2018[1158]. On y découvre sans surprise que les USA, le Canada et la Chine sont les premiers pays à publier.



C'est l'effet de la masse. Mais la première Université est celle de Waterloo au Canada. Ce dernier pays est un véritable pionnier dans l'informatique quantique, et pas seulement grâce à D-Wave.

[1158] Voir VC investment analysis Quantum Computing, 2018 (18 slides).

De son côté, l'**IDA**, l'Institute for Defense Analysis, une organisation parapublique US qui gère trois fonds d'investissements financés par l'état fédéral faisait un bon tour d'horizon des domaines d'applications du quantique, y compris dans le petit marché de la métrologie quantique[1159].

On y trouve cet intéressant tableau qui classifie les principaux pays par dépense, publications scientifiques et dépôts de brevets, les données datant de 2016. La France y arrivait en 8e à 10e position selon les indicateurs. C'est un classement habituel. On a cependant plusieurs pays dont le PIB est inférieur à celui de la France qui arrivent devant elle : le Canada et l'Australie !

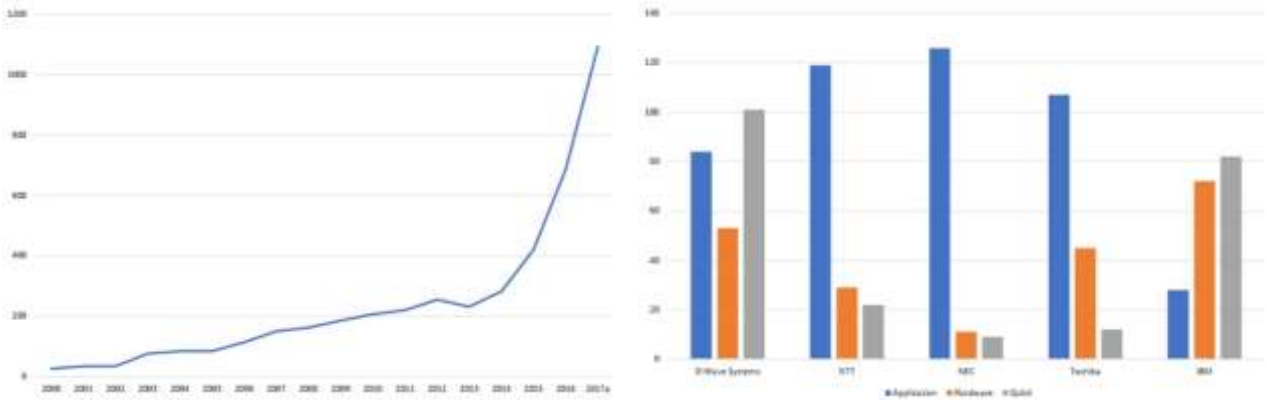
La Corée du Sud était devant la France en termes de dépôt de brevets, ce qui n'est pas une grande surprise au vu de la force de son industrie électronique, dominée par Samsung qui représente près du cinquième du PIB du pays. Une bonne partie des projets financés par les gouvernements de nombreux pays cités dans cette partie proviennent de ce document de l'IDA. La recherche dans le quantique est-elle juste une affaire de gros sous ? Pas seulement.

Table 5. World Ranking of Countries in Quantum Science and Technology

Country	World ranking based on spending	World ranking based on scientific publications	World ranking based on patent applications	Total world ranking
United States	1	2	1	1
China	2	1	2	2
Germany	3	3	6	3
United Kingdom	4	4	4	3
Japan	8	5	3	5
Canada	5	6	5	5
Australia	6	11	7	7
France	9	8	10	8
Italy	11	9	12	9
South Korea	17	10	8	10

Source: U.K. Government Office for Science (2016).

Il ne suffit pas d'aligner des milliards de dollars pour résoudre les problèmes de la matière condensée des qubits supraconducteurs. La réussite dans le quantique est aussi une question d'intégration de disciplines scientifiques nombreuses, puis de valorisation industrielle.



Du côté des brevets, leur dépôt dans les technologies quantiques connaît une croissance soutenue depuis 2014. Sans grande surprise, on découvre que D-Wave est le plus gros déposant de brevets, suivi d'IBM, NEC, NTT et Toshiba, ces derniers étant pourtant plutôt discrets sur le sujet[1160].

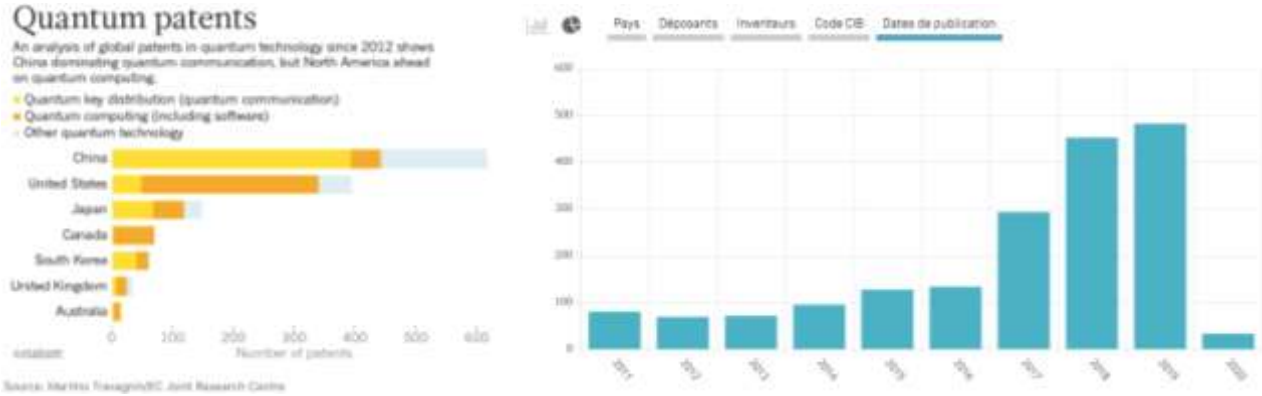
La France n'apparaît que très rarement dans les classements, sachant que ceux-ci sont toujours sujets à caution en fonction des critères de recherche réalisés dans les bases de brevets du WIPO, de l'USPTO ou de l'EPO, notamment par confusion entre le pays du déposant et le pays de dépôt des brevets[1161].

[1159] Voir Assessment of the Future Economic Impact of Quantum Information Science, 2017 (133 pages).

[1160] Voir Quantum Computing and Beyond: Can Patent Landscaping Predict the Future?, juillet 2018.

[1161] Voir Patent analysis of selected quantum technologies par Martino Travagnin, European Commission, 2019 (24 pages). Il s'appuie sur des recherches dans la base de l'EPO (European Patents Office) qui couvre bien les différentes branches des technologies quantiques. Le chart de cette page sur les « quantum patents » provient de Nature: "quantum gold rush" analysis, octobre 2019, et du même auteur. Une étude plus récente a été publiée par Michel Kurek, voir Paysage des brevets et publications sur les technologies quantiques, par Michel Kurek, juillet 2020.

En France, des gros déposants de brevets dans les technologies quantiques sont le CEA, Thales puis le CNRS[1162].



Les investissements importants des pays développés dans les technologies quantiques font craindre l'éventualité que la puissance de calcul puisse se retrouver concentrée dans les mains de quelques uns voir un seul, pays voire entreprise. Je n'y crois pas tout du moins dans une première phase de dévelopement de ces technologies. La connaissance sur le sujet est très distribuée comme le sont les technologies habilitantes et les matériaux stratégiques. Je situerai plutôt le risque de concentration dans une seconde phase de la maturation de ce marché, celle qui verra un marché au départ fragmenté avec de nombreux acteurs se concentrer par consolidation. Il le fera probablement pour des raisons plus macro-économiques que scientifiques ou technologiques par le biais des effets d'économie d'échelle et de plateformisation des offres. Cela explique pourquoi il faut avoir simultanément l'œil sur le matériel, les outils de développement et les applications logicielles du calcul quantique.

Une fois les principales hypothèques scientifiques et technologiques levées, le succès de chaque entreprise et pays dépendra de facteurs clés de succès classiques des écosystèmes technologiques : la vitesse d'exécution, la qualité des équipes, le niveau de financement, le marketing, la communication, la vente et la promotion de plateformes technologiques adoptées par un nombre maximum d'acteurs et à l'échelle mondiale. C'est là où il faudra adopter avec discernement des approches souverainistes associant un protectionnisme des acteurs clés tout en s'assurant d'une ouverture commerciale maximale sur le monde pour leur permettre d'atteindre des économies d'échelle.

Passons à une revue de détail pays par pays, continent par continent. A une exception près, l'Afrique, qui est peu investie sur le sujet, au moins en tant que producteur de technologies quantiques. Et côté utilisation, seule l'Afrique du Sud semble avoir commencé à s'y mettre[1163].

[1162] En faisant une recherche sur le site du WIPO sur l'URL https://patentscope.wipo.int/search/fr/search.jsf et avec la requête FP:(qubit* OR qbit* OR "quantum box*" OR ("entangled" NEAR "photon") OR "quantum key*" OR (quantum NEAR device*) OR "quantum bit*" OR "quantum comput*" OR "quantum simulat*" OR "quantum memor*" OR "quantum communicat*" OR "quantum sens*" OR ("quantum" AND "crypto*") OR "quantum error" OR "quantum process*" OR "quantum algo*" OR "quantum info*" OR "quantum error*" OR "QKD" OR "cold atom*" OR ("quantum" AND "key" AND "distribution") OR "Rydberg atom*"), on obtient 14581 résultats et le chart par année de cette page. En ajoutant AND PA:("commissariat" OR "centre nat" OR "INRIA" OR "SYRTE" OR "Thales" OR "ONERA"), on peut identifier 87 brevets d'origine française.

[1163] Voir Will Africa miss the next computational revolution? par Amira Abbas, avril 2020.

Amérique du Nord

Aux **USA**, la mobilisation apparente des pouvoirs publics est plus molle ou discrète, même si elle dépasse celle de l'Europe en quantité, ne serait-ce que du fait des investissements des grands acteurs du privé dans la recherche fondamentale ou de ceux de la NSA, qui sont probablement massifs, mais confidentiels.

La coordination de la recherche dans les différentes branches du quantique a démarré en octobre 2014. A l'époque où l'on s'intéressait aux sciences à la Maison Blanche, avec un véritable conseiller scientifique du Président, John Holdren, qui a traversé les deux mandats de Barack Obama[1164], celle-ci avait produit le rapport Advancing Quantum Information Science : National Challenges and Opportunities (juillet 2016, 23 pages) suivie d'une réunion de travail en octobre de la même année. Ce n'était pas un plan mais plutôt un inventaire de l'existant. Comme presque tous les pays, le découpage du quantique y est réalisé en quatre parties : la communication quantique, la métrologie quantique, le calcul quantique et les simulateurs quantiques, la distinction entre ces deux derniers étant subtile.

L'état fédéral finance des projets de recherche de startups avec des financements issus du programme SBIR, l'une des composantes du fameux Small Business Act. Cela concerne notamment **Axion Technologies** (2017, Canada) qui a créé un générateur de nombres aléatoires concurrent de ceux du Suisse IDQ.

Les laboratoires publics qui investissent dans l'informatique quantique traversent à peu près tout le complexe militaro-industriel fédéral avec de la recherche interne ou de la recherche externe subventionnée sur appels à projets ou des laboratoires conjoints établis avec des universités :

- La **DARPA** finance trois programmes dans le quantique, dans les communications quantiques à longue distance, dans la métrologie quantique appliquée à l'imagerie ainsi que dans le diagnostic de traumatismes neurologiques et le PTSD. Les financements vont à des projets menés par des Universités, startups et entreprises établies. En 2020, ils lançaient un challenge sur le calcul NISQ qui aboutit à la sélection de 7 équipes de recherches[1165].
- La **IARPA** (Intelligence Advanced Research Projects Agency) que nous avons déjà eu l'occasion de citer plusieurs fois finance des projets tiers sur les calculateurs et les algorithmes quantiques, notamment dans l'entrainement de réseaux de neurones, dans le test de circuits. Leur programme LogiQ vise à améliorer la qualité des qubits. L'IARPA finance également des programmes conduits par des entités tierces. C'est une petite agence qui emploie moins d'une centaine de personnes.
- La **NSA** investit beaucoup dans le quantique à la fois dans la course à la mise en œuvre de l'algorithme de Shor pour décrypter les communications protégées par clés publiques de type RSA et pour protéger les communications sensibles avec clés et cryptographie quantiques. Ses travaux ne sont évidemment pas publics. La NSA sous-traite également une partie de sa re-

[1164] Le remplaçant de John Holdren était nommé par Donald Trump après 18 mois de Présidence, un certain Kelvin Droegemeier, un météorologiste qui a même obtenu l'aval de son prédécesseur ce qui est plutôt rare dans cette Administration.

[1165] Voir DARPA Challenge May Boost Quantum Value of NISQ Devices par Matt Swayne, juin 2020. L'une des équipés sélectionnée comprend un certain Davide Venturelli qui avait fait ses études à l'Université de Grenoble.

cherche à des entreprises privées telles que Lockheed-Martin. Elle est aussi partie prenante d'un laboratoire conjoint avec le NIST et l'Université du Maryland, le QuICS, lancé en 2014 (voir plus loin les détails).

- L'**US Air Force** et son Quantum Communications qui est focalisé sur la cryptographie quantique (QKD). Un autre laboratoire fait de la recherche appliquée dans les qubits supraconducteurs et étudie l'application des algorithmes quantiques à ses besoins opérationnels.
- L'**Office of Naval Research** (ONR) travaille sur les usages des QKD pour la marine et sur l'exploitation d'algorithmes quantiques liés aux besoins opérationnels de la marine.
- L'**Army Research Office** a aussi son propre programme de recherche dans le quantique couvrant tout le spectre allant de la métrologie au calcul quantique en passant par la cryptographie et les communications quantiques.
- La **NASA** a créé en 2013 le Quantum Artificial Intelligence Laboratory (QuAIL) conjointement avec Google dans l'Ames Research Center à proximité du siège de ce dernier à Mountain Views pour explorer le champ des algorithmes quantiques, en particulier sur un ordinateur quantique adiabatique de D-Wave qu'ils ont installé à cette époque-là.
- Le **Los Alamos National Laboratory** (LANL) a un Quantum Institute (QI) lancé en 2002 qui investit aussi dans l'informatique et la cryptographie quantique. Ils financent notamment des recherches de l'UNSW en Australie ainsi que dans celle du Maryland. Ce laboratoire est financé par le Département de l'Energie (DoE). Ce dernier finance également le **Sandia National Laboratories** qui conduit aussi de la recherche appliquée tout azimut dans le quantique.
- La **NSF** finance des projets de recherche divers, un peu comme l'ANR en France[1166].

S'y ajoute le **Département de l'Energie** (DoE) avec ses nombreux laboratoires de recherche gros consommateurs de supercalculateurs comme eux d'Oak Ridge et Argonne.

Enfin, ajoutons à ce panorama le **NIST,** un institut de recherche fédéral qui dépend du Département du Commerce. Son rôle historique est celui de la métrologie, de la définition des poids et mesures. Ses travaux sur les horloges atomiques l'ont amené naturellement à s'intéresser aux technologies quantiques. Il est doté d'un budget annuel de $1,2B et emploie 3400 personnes installés sur deux campus, l'un à Boulder dans le Colorado et un autre dans le Maryland.

Plusieurs de ses groupes de recherche sont dédiés aux technologies quantiques avec le Quantum Processing Group pour le calcul quantique, un autre pour la spintronique, puis un pour la métrologie quantique et un autre pour l'électronique supraconductrice. Enfin, la Computer Security Division de l'Information Technology Laboratory (ITL) gère l'appel d'offre sur la standardisation de la PQC (Post-Quantum Cryptography) que nous avons déjà évoquée dans un chapitre dédié[1167].

[1166] Voir par exemple NSF Awards $2M For Research on Quantum Machine Learning With Photonics, septembre 2019 qui concerne l'Université de Maryland.

[1167] Voir ce tour d'horizon des activités scientifiques du NIST : Quantum Information Science & NIST - Advancing QIS Technologies for Economic Impact, 2019 (39 slides). Le NIST cumule les rôles en France de l'AFNOR pour la standardisation et du LNE pour la métrologie. L'AFNOR a un statut d'association, sous la tutelle de Bercy. C'est le pendant français de l'ISO. Elle emploie 1250 personnes avec un budget de 152M€. Le LNE (Laboratoire de Métrologie et d'Essai) s'occupe de la certification de produits pour leur mise sur le marché. C'est un EPIC rattaché à Bercy qui emploie 700 personnes.

Le NIST est aussi partie prenante et cofinanceur de trois laboratoires conjoints créés avec deux grandes universités situées chacune à proximité de ses propres campus dans le Colorado et le Maryland :

- Le **JQI** (Joint Quantum Institute) de l'Université du Maryland, créé en 2006. C'est un laboratoire de physique quantique fondamentale. C'est là où officie de longue date David Wineland, spécialiste du contrôle des ions par refroidissement laser, qui a obtenu le prix Nobel de physique en 2012 en même temps que Serge Haroche. C'est dans ce laboratoire qu'a germée la startup IonQ lancée en 2015 par Christopher Monroe. De nombreux ex de ce laboratoire ont aussi rejoint l'équipe quantique d'Honeywell à Denver. Ce laboratoire emploie 35 chercheurs permanents, 55 post-docs et 85 thésards avec un budget propre annuel de $6M complété de financements externes divers.
- Le **QuICS** (Joint Center for Quantum Information and Computer Science) de l'Université du Maryland (UMD) lancé en 2014 en partenariat avec la direction de la recherche de la NSA qui se focalise sur les architectures du calcul quantique, les algorithmes et les théories de la complexité en complément du JQI.
- Le **JILA** de l'Université du Colorado à Boulder, lancé en 1962 qui se focalise sur la métrologie. On y trouve deux prix Nobel : Eric Cornell (en 2001, pour ses travaux sur les condensats Bose-Einstein) et John Hall (en 2005, pour ses travaux sur les peignes laser).

Le NIST emploie un quatrième prix Nobel de physique, William Phillips pour ses travaux sur le refroidissement des atomes par laser en 1997, partagé avec Claude Cohen-Tannoudji.

En 2018, la communauté scientifique US s'inquiétait toutefois d'un risque de perte de leadership des USA sur le sujet. Vis à vis de l'Europe ? Non ! De la Chine qui investit massivement dans le quantique[1168].

La Chambre des Représentants US avait même organisé autour de ce sujet une audition en octobre 2017 (vidéo). Durant trois heures, on y voyait des élus interroger une brochette de scientifiques dont James Kurose de la NSF et John Stephen Binkley du Département de l'Energie, qui leur expliquaient les basiques des qubits et les enjeux de souveraineté associés. Les élus démocrates s'y inquiétèrent des coupes budgétaires proposées par l'administration Trump dans le financement de la recherche civile, au profit d'augmentations du budget de la défense et de réductions d'impôts.

In fine, le Congrès US a au contraire solidement augmenté les budgets de la recherche fédérale sur l'année fiscale 2018 (source), sachant que ceux-ci sont ensuite traditionnellement fléchés pour l'essentiel vers des organismes privés, notamment les laboratoires des grandes universités américaines. Avec +8,3% pour le NIH (santé), +3,9% pour la NSF (recherche généraliste), +15% pour la recherche au DoE (énergie), +7,9% pour les programmes scientifiques de la NASA et +26% pour le NIST qui gère les standards et travaille notamment sur la cryptographie quantique. C'est un des rares cas où le Congrès contrôlé par les Républicains s'est opposé à l'administration Trump. Ce mécanisme s'est reproduit l'année suivante et pourrait l'être encore en 2020.

La commission des sciences de la Chambre des Représentant introduisait le 26 juin 2018 le **National Quantum Initiative Act** (H.R. 6227, 25 pages) qui ambitionnait de sédimenter les objectifs, les responsabilités et les moyens publics autour du quantique.

[1168] Comme le soulignait cette note de l'Ambassade de France aux USA d'avril 2018.

Une proposition équivalente était déposée au Sénat le même jour. Ce projet n'est évidemment pas tombé du ciel. Il résultait d'une proposition, le National Quantum Initiative—Action Plan, préparée par des intervenants de la recherche publique et du privé (IBM, Google, Rigetti).

Une intense campagne de lobbying avait aussi été menée de front par plusieurs associations professionnelles[1169]. Il y a d'abord eu la **National Photonics Initiative**, une association professionnelle regroupant des physiciens en photonique et des industriels du secteur, accompagnés par le cabinet de lobbying **BGR Group**.

Cette association qui voulait faire de la photonique une priorité avait été lancée en 2012. Elle est sponsorisée par d'autres entités : The Optical Society (OSA), SPIE (The International Society for Optics and Photonics), American Physical Society, IEEE Photonics Society, ALIA Laser Institute of America et un tas d'autres associations professionnelles. Le lobbying avait été aussi poussé par **Jonathan Dowling** (1955-2020, Américain), professeur de physique de l'Université d'Etat de la Louisiane et spécialiste de la photonique[1170].

La **Quantum Industry Coalition** rassemble de son côté des industriel plus généralistes tels que Microsoft, Intel et Lockheed Martin ainsi que des startups[1171]. Cette coalition est accompagnée de son côté par le cabinet de lobbying KL Gates. C'est le 41e cabinet d'avocats dans le monde avec près de $1B de CA. Le directeur de la Quantum Industry Coalition est Paul Stimers, un partner de KL Gates[1172]. Il faudrait y ajouter la **Quantum Alliance Initiative** lancée en 2018 par le Hudson Institute, un think tank conservateur, qui créé des propositions de standards pour la QKD et la QRNG et milite bien évidemment pour le développement de ce secteur industriel aux USA.

Le **NIST** avait aussi créé avec **SRI International** (l'ancien laboratoire de valorisation industrielle de Stanford) le consortium **Quantum Economic Development Consortium** (QED-C) destiné à développer l'industrie quantique américaine dans les domaines de la communication et de la métrologie[1173]. Il est présidé par Joseph Broz qui est par ailleurs vice-président du SRI et par Celia Merzbacher, une lobbyiste de l'industrie des semiconducteurs qui avait travaillé à la Maison Blanche sous l'administration Bush 43. Bref, cela fait pas mal de monde de mobilisé autour du quantique !

Le Quantum National Initiative Act proposait d'allouer $1,275B sur cinq ans pour financer la R&D civile dans le quantique, répartis au Département de l'Energie ($625M), à la NSF ($250M) et au NIST qui est focalisé sur les questions de cryptographie ($400M). Lorsque l'on fait les comptes, cela faisait passer les investissements annuels de $200M à $255M, ce qui semble modeste, mais ce dernier montant n'intégrait pas les fonds alloués à la NSA et au Département de la Défense.

La loi proposait aussi la création d'un National Quantum Coordination Office au sein de l'Office of Science and Technology Policy. Il demandait au Président des USA de créer un plan à 10 ans sur le quantique, une première étape devant être un plan de cinq ans livrables un an après le vote de la loi.

[1169] Voir Quantum computing finds its lobbying voice par Aaron Gregg dans le Washington Post, juin 2018.

[1170] Voir Schrödinger's Killer App - Race to Build the World's First Quantum Computer par Jonathan P. Dowling, 2013 (445 pages) où il avertissait déjà du risque de voir la Chine prendre le dessus en calcul quantique à base de photons si les USA ne faisaient pas d'efforts dans le domaine : "*The future of the quantum Internet is in photons and the short circuiting of the development of optical quantum information processors in the United States means that the future quantum Internet will have 'Made in China' stamped all over it.*", page 173.

[1171] Voir leur site Quantum Industry Coalition.

[1172] Voir The US National Quantum Initiative par Paul Stimers, K&L Gates, octobre 2019 (6 pages).

[1173] Voir NIST Launches Consortium to Support Development of Quantum Industry, septembre 2018. Et plus de détails dans U.S. Consortium Pulls Ecosystem Into Quantum par Susan Rambo, août 2019. En juillet 2020, l'association regroupait 130 membres du secteur privé – grandes entreprises et startups - et une quarantaine de laboratoires d'Universités et du secteur public US.

Ce projet de loi a été poussé par des élus craignant que la Chine prenne le dessus sur le quantique, notamment dans la sécurité informatique[1174]. Les USA aiment se faire peur. Même si dans le domaine du quantique, les USA n'ont pas à rougir avec une densité de laboratoires de recherche publics et privés sans égal, de grands acteurs ont une capacité d'industrialisation à grande échelle que quasiment aucun pays ne peut concurrencer et leur marché intérieur qui reste le plus grand au monde pour les applications informatiques d'entreprise, là par où le quantique va démarrer.

Ce projet de loi de la Chambre des Représentants était voté en plénière le 13 septembre 2018[1175] puis par le Sénat en décembre 2018. La Maison Blanche avait publié en septembre 2018 un document qui reprenait les termes de la proposition du Congrès, dans le National Strategic Overview for Quantum Information Science. Ils insistaient notamment sur la recherche, sur la formation des scientifiques et sur la collaboration internationale.

Les montants demandés étaient approuvés par le Congrès et la Maison Blanche et Donald Trump signait cette loi le 21 décembre 2018 juste avant le shutdown[1176].

Au lieu de lui expliquer les arcanes de l'informatique quantique, il était probablement plus simple de mettre en avant les avancées de la Chine dans le domaine et le risque que cela fait peser sur les USA[1177]. Il est difficile de suivre à la trace l'usage qui a été fait de ces fonds sur l'année 2019, probablement distribués en partie, notamment à la NFS, via des appels à projets divers de leur programme **Quantum Leap**.

La NSF lançait en particulier en 2019 un appel à projet **Quantum Leap Challenge Institutes**, qui doit financer des instituts de recherche devant mener des projets interdisciplinaires pour faire avancer l'état de l'art dans les technologies quantiques (détails). Les QLCI devaient être sélectionnés d'ici fin 2021, probablement de laboratoires de recherche existants et pas nouvellement constitués. Leur format fait penser aux hubs du programme quantique du Royaume-Uni. Les sujets mis en avant sont les réseaux quantiques, le middleware logiciel quantique, les algorithmes et solutions pour la simulation quantique, la métrologie quantique, tout ce qui concerne le développement des compétences ainsi que la coordination de la recherche et le « community management ».

Trois hubs étaient sélectionnés dès juillet 2020 pour un total de $75M étalé sur cinq ans : un premier dédié à la métrologie quantique piloté par l'Université du Colorado, un second dédié au calcul quantique piloté par l'Université de l'Illinois - Urbana-Champaign et un troisième également sur le calcul quantique et plutôt côté logiciels piloté par l'Université de Berkeley (source). Ces trois hubs regroupent 16 institutions académiques, 8 laboratoires nationaux et 22 partenaires industriels.

La NSF lançait aussi en mars 2020 un **Quantum Algorithme Challenge** (source).

[1174] Voir How suspicions of spying threaten cross-border science par Patrick Howell O'Neill, décembre 2019 qui évoque les méthodes directes et indirectes utilisées par la Chine pour piller les travaux de recherche Européens et Américains dans le quantique et les exploiter aussi bien côté civil que militaire, comme les radars quantiques, les sonars quantiques et la QKD. Voici le lien pour récupérer l'étude de Quantum Dragon Strider évoquée dans l'article, novembre 2019 (22 pages). On peut indiquer un email bidon pour l'obtenir, le téléchargement ne passe pas par un mail. Elle évoque divers partenariats dans la recherche qui aident les Chinois à exploiter la recherche occidentale. Il s'appuie sur quelques exemples dont celui, très détaillé, de l'Université de Heidelberg en Allemagne. Sur ce même sujet, voir aussi China's top quantum scientist has ties to the country's defense companies, décembre 2019, Quantum USA Vs. Quantum China: The World's Most Important Technology Race par Moor Insights and Strategy, octobre 2019 et New Warnings Over China's Efforts in Quantum Computing par Sintia Radu, janvier 2020.

[1175] Voir SIA Welcomes House Passage of Quantum Computing Legislation, septembre 2018.

[1176] Voir President Trump has signed a $1.2 billon law to boost US quantum tech, par Martin Giles dans la MIT Technology Review, décembre 2018. Dans la signature dans le bureau oval, le Président est entouré de sa fille Ivanka Trump et par deux conseillers scientifiques de la Maison Blanche. Aucun représentant de l'écosystème de la recherche quantique ou du Congrès n'est présent. Le lendemain, 22 décembre 2018, démarrait le fameux « shutdown » du gouvernement qui dura 35 jours, provoqué par ce même Président.

[1177] Voir The Race to Develop the World's Best Quantum Tech de Jeremy Tsu dans IEEE Spectrum, décembre 2018, qui évoque le rapport Quantum Hegemony - China's Ambitions and the Challenge to U.S. Innovation Leadership du CNAS publié en septembre 2018 qui décrit la stratégie quantique de la Chine (52 pages). Voir aussi US intelligence community says quantum computing and AI pose an 'emerging threat' to national security de Zack Whittaker, décembre 2018.

De son côté, le DoE lançait un appel à projet pour attribuer 158 subventions totalisant $32M à 118 PME via le programme SBIR. Ils sont délivrés en deux phases, une première de $200K suivie d'une seconde, pour les meilleurs projets, de $1,1M, le tout s'étalant sur une période de deux ans et demi.

Le DoE annonçait aussi en août 2020 le financement de cinq centres de recherche en technologies quantiques tous pilotés par des laboratoires du DoE à raison de $300M provenant de ce dernier et le reste d'institutions concernées et du secteur privé (IBM, Microsoft, Intel, Lockheed Martin). La liste comprend **Q-NEXT** (Next Generation Quantum Science and Engineering Center) piloté par l'Argonne National Laboratory qui s'intéresse à l'industrialisation du harware quantique, **C²QA** (Co-design Center for Quantum Advantage) piloté par le Brookhaven National Laboratory et qui va se focaliser sur les moyens d'obtenir un avantage quantique dans les applications scienfiques, le **SQMS** (Superconducting Quantum Materials and Systems Center) piloté par le Fermi National Accelerator Laboratory qui va se concentre sur les qubits supraconducteurs, le **QSA** (Quantum Systems Accelerator Center) piloté par le Lawrence Berkeley National Laboratory qui va travailler sur le calcul quantique côté matériel et logiciel et enfin, le **QSC** (Quantum Science Center) piloté par l'Oak Ridge National Laboratory qui va s'intéresser aux questions de scalabilité du calcul quantique.

En décembre 2019 était créée l'alliance **Quantum Information Edge** (site) rassemblant des laboratoires de recherche Lawrence Berkeley National Laboratory et les Sandia Labs du Département de l'Energie, l'Université de Maryland, l'Université Duke (Caroline du Nord), l'Université du Colorado à Boulder, Harvard, Caltech, le MIT et l'Université du Nouveau Mexique[1178]. Pour une bonne part, les usual suspects de la recherche fondamentale dans le calcul quantique qui créent ainsi leur « hub virtuel » de coordination de la recherche dans ce domaine. Avec une focalisation sur la réduction des erreurs au niveau des qubits, les techniques d'interconnexions entre qubits et le développement de nouveaux algorithmes quantiques. De son côté, la NPI se lançait dans une nouvelle campagne de lobbying fin 2019 et début 2020 pour augmenter une nouvelle fois les crédits fédéraux alloués à la recherche dans les technologies quantiques[1179].

En février 2020, la Maison Blanche publiait une note du National Quantum Coordination Office recommandant le développement de réseaux quantiques[1180]. Et l'exécutif américain proposait en mars 2020 une nouvelle augmentation des budgets de la recherche dans le quantique sur les années 2020/2021[1181], à hauteur de $450M pour le Département de l'Energie, $330M pour la NSF et $80M pour le NIST. Cette augmentation allait de pair avec une augmentation de $1B pour l'intelligence artificielle[1182]. En août 2020, la Maison Blanche communiquait sur une augmentation de 30% des budgets quantiques et IA pour l'année fiscale 2021. Cela avait l'air redondant avec la communication de février et portait sur des montants légèrement supérieurs. Tout cela doit être validé par le Congrès, ce qui ne devrait pas trop poser de problèmes car ce sujet est plutôt bi-partisan. Toujours en août, la Maison Blanche annonçait la création d'un Advisory Committe pour le suivi de la National Quantum Initiative en liaison avec le Département de l'Energie qui est l'un des trois grands protagonistes de l'initiative avec la NSF et le NIST.

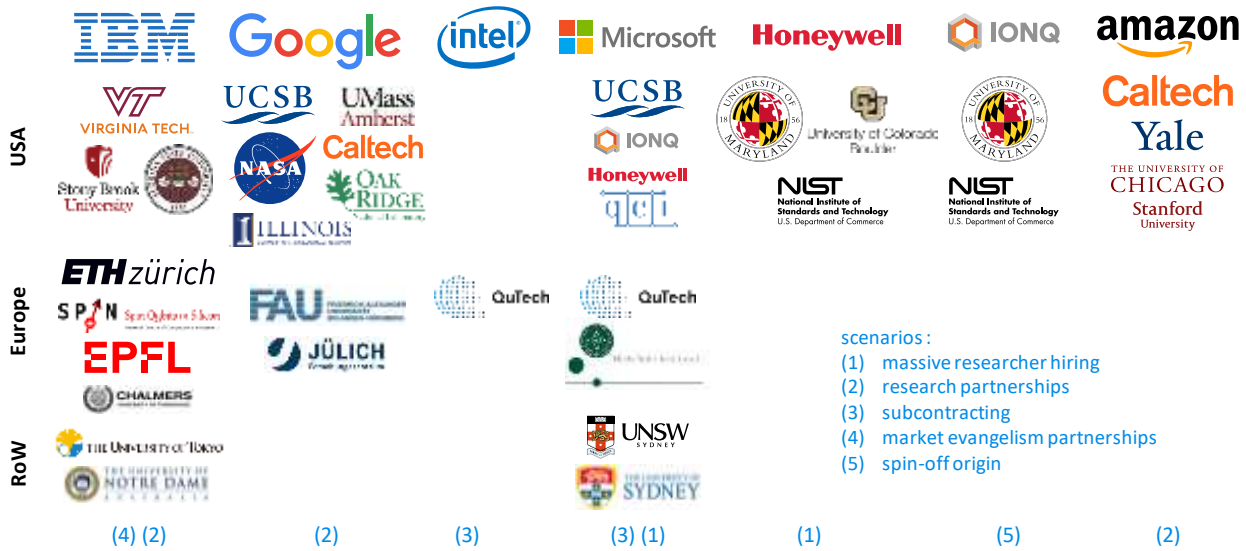
[1178] Voir US alliance for quantum computing par David Manners, 2019.

[1179] Voir NPI Brings Quantum Experts to Capitol Hill to Advocate for Additional NQI Funding, Jo Maney, mars 2020.

[1180] Voir A Stragegic Vision for America's Quantum Networks, Maison Blanche, février 2020 (4 pages).

[1181] Voir Why is Trump funding quantum computing research but cutting other science budgets? The national security implications of this technology may be exaggerated, par John Lindsay, mars 2020.

[1182] Voir White House reportedly aims to double AI research budget to $2B par Devin Coldewey dans TechCrunch, février 2020.



Rappelons enfin une réalité du marché faisant écho aux thèses de l'économiste **Maria Mazzucato** sur l'origine publique des innovations technologiques : les grands acteurs américains se sourcent à différents niveaux et un peu partout aux USA et dans le monde pour faire avancer leurs technologies quantiques. Le schéma *ci-dessus* en atteste bien. Et il manque sans-doute quelques laboratoires dans cet inventaire !

On peut faire un parallèle entre l'intelligence artificielle et l'informatique quantique pour ce qui concerne le Canada. Dans les deux cas, son influence du secteur est bien plus grande que le poids économique du pays, aussi bien au niveau de la recherche fondamentale que des entreprises. C'est notamment dû à un investissement constant et en avance de phase du gouvernement et des Universités dans la recherche et à un dynamisme entrepreneurial certain.

Le Canada a deux grandes stars quantiques dans la recherche avec **Gilles Brassard** de l'Université de Montréal qui est avec **Charles Bennett** d'IBM Research le coinventeur du protocole BB84 de QKD.

Le Canada se distingue par un fort investissement dans la recherche fondamentale dans l'informatique quantique, notamment avec plus de $1B d'investissements publics sur une décennie, répartis principalement dans trois institutions[1183] :

- L'Institut Quantique de l'**Université de Sherbrooke**, près de Montréal. On y trouve notamment Alexandre Blais, un spécialiste reconnu des qubits supraconducteurs. A noter leur programme de formation **QSciTech** en liaison avec leurs partenaires industriels et l'initiative Q2 pour encourager l'entrepreneuriat étudiant et leurs liens avec l'industrie. Plusieurs startups en sont sorties comme SBTech (métrologie), Nord Quantique (calcul quantique) et Quantic (métrologie).

[1183] Voir Quantum Canada, par Ben Sussman, Paul Corkum, Alexandre Blais, David Cory et Andrea Damascelli, février 2019 (6 pages) qui fait le point sur les investissements quantiques dans le pays.

- Le Quantum Matter Institute (QMI) de l'**University of British Columbia**, situé principalement à Vancouver.
- L'Institute for Quantum Computing de l'**Université de Waterloo**, proche de Toronto qui avait obtenu $120M en 2017 pour financer ses différents instituts de recherche dans le quantique, complétés par un financement australien de $53M provenant de l'UNSW, de l'opérateur Telstra et de la Commonwealth Bank of Australia. L'IQC fait à la fois de la recherche et de l'enseignement. Ils proposent des formations courtes d'une à deux semaines en été sur la cryptographie et le calcul quantiques. L'IQC est dirigé par Raymond Laflamme, un des pères de la QEC. Ils couvrent tous les pans des technologies quantiques avec une trentaine d'équipes de théoriciens et d'expérimentateurs une cinquantaine de post-docs et 125 thésards. Une douzaine de startups en sont sorties depuis 2002. L'IQC anime le Transformative Quantum Technologies (TQT), un programme de valorisation de la recherche financé sur sept ans à hauteur de $76M par le gouvernement canadien et son First Research Excellence Funds. Le TQT lançait en janvier 2020 la Quantum Alliance, une sorte de chapeau de l'IQC et du TQT pour les relier à leur écosystème canadien et international, notamment avec le tissu de startups quantiques.

D'autres laboratoires sont impliqués, comme dans l'**Université de Calgary** qui travaille sur les communications quantiques et a déployé un réseau expérimental de QKD de quelques dizaines de km. L'**Université d'Alberta** à Edmonton, au nord de Calgary, est également impliquée dans ces travaux[1184].

Du côté entrepreneurial, ils ont en tête de pont l'incontournable **D-Wave** ainsi que le spécialiste des logiciels quantiques, **1QBit**. Avec un total de 36 startups et PME du quantique, les positionnant en second au niveau mondial de ce point de vue-là.

Les financements privés notables comprennent surtout les donations de Michael Lazaridis, un des cofondateurs de RIM BlackBerry, avec $75M à l'**Institute for Quantum Computing** de l'Université de Waterloo et $128M en 1999 au **Perimeter Institute for Theoretical Physics** qui est aussi situé à Waterloo. Avec Doug Fregin, également cofondateur de RIM, ils ont également créé le **Quantum Valley Investment Fund** avec un financement total de $100M.

Notons aussi l'existence du **Creative Destruction Lab**, une structure d'accélération de startups deep techs avec une spécialité sur les technologies quantiques. Ils sont installés au Canada (Toronto, Montréal, Vancouver, Calgary, Halifax), aux USA (Atlanta) ainsi qu'à Oxford et Paris.

Ah, et puis, ils ont un premier ministre qui sait expliquer, depuis 2016, ce qu'est un qubit. C'est une prouesse qui a été bien remarquée à l'époque et qui reste encore rare. Mais aussi curieux que cela puisse paraître, le Canada n'a pas produit une véritable stratégie quantique nationale. Elle était encore en gestation en 2020.

[1184] Voir Quantum Communication Network Activities Across Canada par Barry Sanders et Daniel Oblak, juin 2019 (10 slides).

Royaume-Uni

Comme pour de nombreux pays d'Europe continentale, le Royaume-Uni a contribué aux avancées de la physique quantique depuis le 18e siècle avec quelques précurseurs et fondateurs, suivis d'une nouvelle génération dans la seconde moitié du 20e siècle : **Thomas Young** (1773-1829), **Ernest Rutherford** (1871-1937), **Joseph John Thomson** (1856-1940), **James Chadwick** (1891-1974), **Paul Dirac** (1902-1984), **Brian Josephson** (1940), **David Deutsch** (1953), **Andrew Steane** (1965) et encore plus récemment les créateurs du langage QML, **Thorsten Altenkirch** et **Jonathan Grattage**.

Sous l'impulsion du physicien spécialiste en photonique Sir **Peter Knight** (1947), le **Royaume-Uni** semble être le premier pays à s'être mobilisé sur les technologies quantiques au niveau d'un plan structuré, le **UK National Quantum Technologies Programme.**

Il était annoncé en novembre 2013 avec un premier financement de £270M étalé sur cinq ans[1185]. Ce plan représentait un financement bien plus important que pour les initiatives précédentes qui touchaient aux matériaux innovants ou à la robotique. Bien entendu, le plan ne partait pas de zéro et s'appuyait sur un existant avec une forte densité de laboratoires de recherche en physique quantique des universités.

Le plan était et reste coordonné par l'**EPSRC** (Engineering and Physical Sciences Research Council), un organisme non gouvernemental financé par les derniers publics et sous la supervision de l'exécutif. Le plan lancé pratiquement en 2014 associait l'EPSRC (où Lucy Martin et Liam Blackwell dirigent la branche des technologies quantiques), **Innovate UK** (leur équivalent de notre ANR pour le financement de la recherche fondamentale), le **Department for Business, Energy and Industrial Strategy** (leur équivalent de notre DGE à Bercy), le **NPL** (National Physical laboratory, où Peter Knight avait été Chief Science Advisor), le **CGHQ** (leur NSA) et **dstl** (leur équivalent de notre DGA).

De manière assez classique, le plan UK visait tous les domaines habituels du quantique : calcul, sécurité, métrologie avec un axe fort sur l'imagerie médicale. Les financements s'articulaient autour de celui de hubs thématiques regroupant des Universités et sélectionnés par appel à projets (£124m), de la formation, du transfert de technologie et de l'industrialisation[1186]. Dès le début, le plan affichait une volonté affirmée de créer du business et d'attirer des capitaux privés.

[1185] Voir The UK National Quantum Technologies Programme Current and Future Opportunities de Derek Gillespie, novembre 2014 (29 slides) et Delivering the National Strategy for Quantum Technologies (5 pages).

[1186] Source du schéma : UK national quantum technology programme, par Peter Knight et Ian Walmsley, octobre 2019 (10 pages).

Le plan initial prévoyait de valoriser les travaux de recherche dans des startups aussi rapidement que possible.

Quatre hubs quantiques couvrent les grands domaines des technologies quantiques et regroupent des équipes réparties sur le territoire dans une trentaine d'universités.

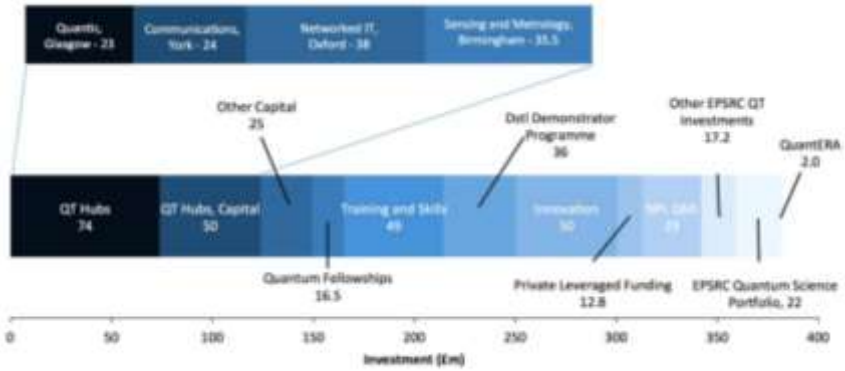


Figure 1. Representation of the funding allocated to the elements of the UK NQTP 2014–2019.

Tous les dirigeants des hubs sont des scientifiques du domaine, complétés par un "business development director " et un board de 8 personnes comprenant des industriels et notamment leurs CTO.

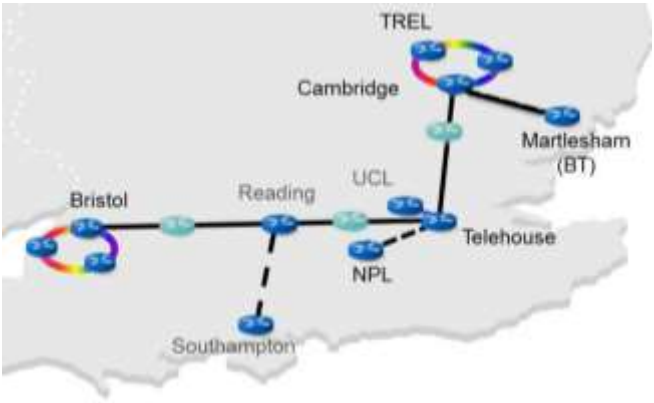
Le **UK Quantum Technology Hub Sensors and Timing** couvre les solutions de métrologie et de mesure du temps et associe les universités de Birmingham (lead, sous la direction de Kai Bongs), Glasgow, Nottingham, Southampton, Strathclyde et Sussex.

Le hub **Quantic** regroupe les universités de Glasgow (lead, sous la direction de Steve Beaumont), Bristol, Edinburgh, Heriot-Watt, Oxford et Strathclyde et s'intéresse à l'imagerie quantique. Ce qui nous fait deux hubs dans ledomaine de la métrologie quantique.

Le **Quantum Computing & Simulation Hub** regroupe 17 universités et est piloté par celle d'Oxford sous le lead d'Ian Walmsley. Il a pris la suite du hub NQIT (Networked Quantum Information Technologies) en 2019. Il se focalise sur les questions de calcul et de sécurité[1187].

Le **Quantum Communications Hub** associe une dizaine d'universités : Bristol, Cambridge, Glasgow, Heriot Watt, Kent, Oxford, Queen's Belfast, Sheffield, Strathclyde sous le pilotage de celle d'York, des entreprises comme Airbus, Toshiba, ID Quantique, Qunet, Kets, et des agences publiques.

Ils développent un réseau de communication quantique entre Bristol, Cambridge et Ipswich via l'infrastructure nationale de fibres noires du **UK National Dark Fibre Infrastructure Service** lancé par l'EPSRC (et qui relie aussi Southampton and UCL à Londres)[1188]. Cela n'empêchait pas l'agence de sécurité de l'état d'afficher son scepticisme sur la pertinence de QKD dans un livre blanc de quatre pages publié en avril 2020[1189].

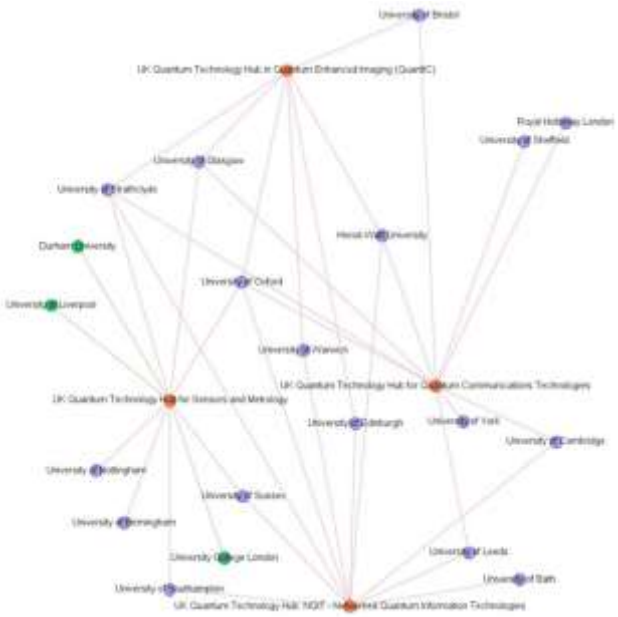


[1187] On y trouve notamment l'initiative QuOpaL (Quantum Optimisation and Machine Learning) qui est financée par Nokia et Lockheed Martin.

[1188] Source du schéma : The Quantum Communications Hub, 2016 (11 slides).

[1189] Voir Quantum Security Technologies, NCSC, mars 2020 (4 pages).

Ces hubs sont finalement très multipolaires, rassemblant des universités qui sont impliquées dans plusieurs hubs différents, selon la cartographie *ci-contre*[1190]. Le Royaume-Uni a bien eu de la suite dans les idées en gérant ce plan dans la durée. Un rapport d'étape était publié en 2015 par l'EPSRC et Innovate UK[1191] suivi d'un autre rapport intermédiaire le « Quantum Age-Blackett review » en 2016[1192]. Ce dernier recommandait de poursuivre l'investissement lancé en 2014 et notamment d'étendre l'effort à la partie algorithmique et logicielle en liaison notamment avec l'**Alan Turing Institute** et le **Heilbronn Institute for Mathematical Research** pour proposer des études de cas de problèmes de calcul à résoudre.



Suivait un rapport parlementaire publié en novembre 2018[1193] qui supportait la poursuite du plan, le lancement d'une seconde phase de £350m sur la période 2019-2024 et un peu de *fine tuning* sur la coordination entre les différents acteurs (les hubs, les centres d'innovation, les entreprises).

Le financement de la phase 2 devrait renouveler celui des hubs (£94m sur 5 ans), des projets d'industrialisation (£153m d'ISCF - Industrial Strategy Challenge Fund - sur 6 ans[1194]), de la formation (£25m sur 5 ans[1195]) et le lancement du centre national **NQCC** (National Quantum Computing Centre) pour le développement de solutions de calcul quantique, avec £93m sur 5 ans[1196].

Cela aboutissait en juin 2019 à l'annonce officielle de cette phase 2 suivant les recommandations de la Chambre des Communes[1197]. Avec les investissements prévus du secteur privé, le total des deux phases du plan quantique anglais était estimé à $1,227B.

Le gros de cette phase 2 est le NQCC qui est piloté par UKRI[1198], l'EPSRC et le STFC (Science and Technologies Facilities Council), une agence gouvernementale qui fait de la recherche en physique et en astronomie et gère les grands instruments scientifiques du pays (accélérateurs de particules, lasers, ingénierie spatiale, etc).

UK Research and Innovation

[1190] Source du schéma : UK national quantum technology programme, par Peter Knight et Ian Walmsley, octobre 2019 (10 pages).

[1191] Voir A roadmap for quantum technologies in the UK, 2015 (28 pages).

[1192] Voir The Quantum Age Technological Opportunities, 2016 (64 pages).

[1193] Voir Quantum technologies, House of Commons Science and Technology Committee, novembre 2018 (75 pages).

[1194] Le Strategy Challenge Fund organise des concours et appels à projets pour financer des projets de recherche et d'industrialisation, à l'image de ce que Bpifrance et la DGE font régulièrement en France (mais pas encore sur le quantique).

[1195] La formation doctorale au quantique n'est pas gérée dans les hubs mais dans des centres doctoraux comme le Quantum Engineering Centre for Doctoral Training de Bristol.

[1196] Voir Establishing the National Quantum Computing Centre (NQCC), août 2019 (64 slides).

[1197] Voir UK government invests $194M to commercialize quantum computing de Frederic Lardinois.

[1198] UKRI (UK Research and Innovation) est une organisation non gouvernementale autonome créée en avril 2018 qui gère un budget annuel de £7B et consolide sept anciens « research councils » dont l'EPSRC et le STFC, l'agence Innovate UK et Research England.

Ce centre doit produire des démonstrateurs de calcul quantique NISQ puis LSQ, développer des algorithmes et logiciels quantiques et leurs usages et bâtir une communauté d'utilisateurs autour. Le centre doit ouvrir d'ici l'été 2021 et devenir pleinement opérationnel en 2022. Il doit mettre en place une machine NISQ opérationnelle d'ici 2025. En 2020, les technologies privilégiées étaient celles des qubits supraconducteurs et à ions piégés. Le centre est dirigé par Michael Cuthbert de la société Oxford Instruments et Simon Benjamin, professeur de technologies quantiques de l'Université d'Oxford.

Le Royaume-Uni avait récupéré environ 14% des budgets de la première vague de projets du Flagship Quantique européen en octobre 2018. Malgré le Brexit, le pays continuera à en bénéficier, la collaboration avec l'Europe sur recherche survivant à ce dernier. Ainsi, le laboratoire d'UCL de John Morton est-il intégré dans le projet flagship sur les qubits silicium piloté par le CEA-Leti et attribué en mars 2020.

Du côté entrepreneurial, le Royaume-Uni a fait germer une trentaine de startups dans les technologies quantiques avec un bon équilibre par catégories. C'est le second pays dans le monde en nombre de startups, derrière les USA qui en ont une cinquantaine.

Mais le Royaume Uni est numéro un en financement de startups, si l'on considère que **PsiQuantum**, si l'on considère qu'il s'agit encore d'une startup du Royaume-Uni, une bonne part de la startup s'étant installée aux USA pour pouvoir se financer à hauteur de $230M, le record à ce jour de financement de startups dans les technologies quantiques, depuis D-Wave (1999, Canada, $205M).

A noter une initiative originale, celle de la société de gestion de propriété intellectuelle **IpGroup** qui lançait en août 2020 un fonds de £12m de financement de startups, ces dernières étant sélectionnées par l'agence indépendante **UKRI**. Les projets seront financés avec des montants compris entre £125k et £2m.

Les acteurs notables sont **Oxford Instruments** (cryogénie), **Oxford Quantum Circuits** (qubits supraconducteurs[1199]), **Quantum Motion Technologies** (qubits silicium), **Cambridge Quantum Computing** (système d'exploitation, logiciels, services), **TundraSystems** (qubits photoniques), **Orca Computing** (qubits photons) et **River Lane Research** (logiciels). Par contre, aucune grande entreprise du pays ne semble être particulièrement investie dans l'informatique quantique sauf peut-être dans les télécommunications.

[1199] Oxford Quantum Circuit obtenait un financement de Innovate UK en avril 2020 dans un consortium de quatre entreprises et deux universités. Voir Oxford Quantum Circuits-led consortium wins Grant to Boost Quantum Technologies in the UK par Quantum Analyst, avril 2020.

Europe continentale

La **Suisse** est aussi mobilisée sur le quantique, notamment à l'**Université ETH** de Zurich qui collabore d'ailleurs avec IBM et surtout autour de la cryptographie quantique, notamment avec sa startup **IDQ** qui est leader de la génération de nombres aléatoires utilisée dans la crypto quantique.

Le pays a publié un manifeste de promotion de ses efforts de recherche et industriels dans le quantique, Switzerland: At the Quantum Crossroads. Le **Swiss Quantum Hub** fédère de son côté l'écosystème suisse du quantique.

L'initiative **Quantum Science and Technology** (QIST) commune à l'ETH Zurich et l'Université de Bâle et qui associe aussi l'Université de Genève et l'EPFL de Lausanne comprend 34 enseignants et 300 étudiants. Elle a été financée à hauteur de $120M entre 2010 et 2017.

Elle couvre tous les domaines habituels du quantique avec, semble-t-il, un effort plus particulier dans les télécommunications quantiques.

A noter enfin la création en 2020 du **Swiss Quantum Investor Club** qui fait le lien entre les investisseurs et les entrepreneurs du quantique et organisent des événements à Genève, Lausanne et Zürich, et du **Swiss Quantum Hub**, un think tank et un accélérateur de startups dans le quantique, le tout complété par le Quantum Computing Garage, un hackathon permanent.

L'Allemagne est une terre de recherche fondamentale dense sur les technologies quantiques. Et elle s'appuie sur une l'histoire des nombreux fondateurs allemands de la physique quantique. Son réseau de centres de recherche n'a rien à envier à la complexité du système français.

Les principaux laboratoires de recherche impliqués de manière visible dans le quantique sont :

- Le **Max Planck-Institute for Quantum Optics** (MPQ) basé à Munich qui fait partie des 84 MPI et de leurs 24 000 personnes. Ils sont spécialisés notamment sur les qubits à base d'atomes froids. Ce MPI est associé à l'International Max Planck Research School aussi basé à Munich. Deux autres MPI sont dédiés aux technologies de l'information, mais ne semble pas investis dans le quantique.
- Les **Fraunhofer Institutes** qui font de la recherche appliquée et partenariale avec 72 instituts et 26 600 personnes. Ils comprennent trois instituts spécialisés dans le quantique : le Fraunhofer Institute for Applied Solid State Physics IAF à Fribourg, le Fraunhofer Institute for Applied Optics and Precision Engineering IOF à Iéna et le Fraunhofer Institute for Open Communication Systems FOKUS à Berlin.
- Le réseau des 19 centres de recherche **Helmholtz** qui font de la recherche fondamentale en réponse aux grands défis de société, avec un total de 40 000 personnes. Il comprend le laboratoire quantique de **Jülich Forschungszentrum** situé entre Aix-la-Chapelle et Cologne et piloté par

Kristel Michielsen[1200] ou travaille aussi Tommaso Callarco, qui coordonne le Quantum Flagship européen. Il est associé à l'Université d'Aix la Chapelle dans le **JARA Institute Quantum Information** (IQI). Le réseau Helmholz comprend aussi l'**Institute of Photonics and Quantum Electronics** du Karlsruhe Institute of Technology (KIT).

- La communauté des 91 **centres de recherche Leibniz** qui font de la recherche fondamentale comprend notamment l'Institute for Solid State and Materials Research de Dresden (IFW) qui planche sur la supraconductivité et le magnétisme, l'Institute of Photonic Technology (IPHT) à Iéna, le Max-Born-Institute for Nonlinear Optics and Short Pulse Spectroscopy (MBI) à Berlin, et le Paul Drude Institute for Solid State Electronics (PDI) également de Berlin.
- Le **Munich Center for Quantum Science and Technology** (MCQST) de Munich a été lancé en 2019. Il rassemble les centres de recherches quantiques de Munich : le MPQ, le Walther-Meißner-Institute for Low Temperature Research (WMI) et les deux grandes universités scientifiques de la ville : Ludwig-Maximilians-Universität München et Technical University of Munich (TUM). L'ensemble couvre toutes les technologies quantiques (simulation, calcul, communication, capteurs). Le tout avec un budget de 31M€ sur cinq ans et environ 55 chercheurs permanents.
- L'**Institute for Complex Quantum Systems** de l'Université d'Ulm entre Stuttgart et Munich.

S'y ajoutent le **PTB** qui est l'office fédéral de métrologie, équivalent du LNE français et le **BSI** qui est l'office fédéral pour la sécurité des technologies de l'information, équivalent de l'ANSSI française[1201].

[1200] Jülich Forschungszentrum est un peu l'équivalent du CEA en Allemagne. Il avait démarré en 1956 dans la recherche nucléaire. Il héberge aussi de nombreux supercalculateurs, à l'instar de la DAM du CEA à Bruyère le Chatel.

[1201] En **Allemagne**, l'agence fédérale qui protège les systèmes d'information homologue de l'ANSSI française publiait en mai 2018 le rapport Entwicklungsstand Quantencomputer (*état des lieux de l'informatique quantique*) qui faisait un point sur l'informatique quantique, focalisé notamment sur les questions de cybersécurité (231 pages, en anglais). Cet excellent document avait était créé par une demi-douzaine d'universitaires allemands faisant de la recherche à l'Université de Saarland à Sarrebruck et à l'Université de Floride à Boca Raton aux USA. Ce sont des physiciens spécialistes de la matière condensée et des qubits supraconducteurs, des mathématiciens et des spécialistes de la cybersécurité. C'est l'un des meilleurs tours d'horizon de cette époque de la recherche mondial en informatique quantique que j'ai pu consulter. Il faisait un inventaire étonnamment précis des efforts dans le domaine, notamment dans la recherche publique US.

Comme j'aime bien les schémas, en voici un qui consolide tout ce petit monde avec une certaine logique (*ci-dessus*).

En septembre 2018, le Ministère de la Recherche du gouvernement fédéral allemand annonçait un financement de 650M€ dans les technologies quantiques étalé sur quatre ans (2018 à 2022)[1202]. Comme tous les plans du genre, il finance des projets dans le calcul quantique, dans la communication quantique et dans la métrologie quantique. En septembre 2019, IBM annonçait rejoindre ce plan. IBM doit installer un ordinateur quantique en Allemagne qui sera exploitable pour les chercheurs dans le cloud. Il n'est pas certain que ce soit la meilleure approche pour développer une industrie allemande et européenne du quantique, tout du moins du côté du matériel.

En plus du financement générique de 650M€, le pays s'est lancé la création de deux réseaux de télécommunications à base de QKD :

- **QuNET** (165M€) qui utilise une QKD standard associée à des liaisons terrestres et satellites. Le projet associe plusieurs Fraunhofer Institutes dont le Heinrich Hertz Institute, HHI), le Max Planck Institute for the Physics of Light et le German Aerospace Center (DLR)[1203]. Le projet doit durer sept ans et vise à créer une infrastructure de protection des communications du gouvernement allemand. Cela doit aboutir à la création d'un réseau sécurisé européen. Le secteur privé est aussi impliqué avec Deutsche Telekom, ADVA Optical Networking et Tesat-Spacecom.
- **Q.Link.X** (14,8M€) pour la création d'un réseau terrestre en fibre optique et QKD et s'appuyant sur des répéteurs quantiques, géré par le Fraunhofer HHI[1204].

Ces deux projets sont financés par le Ministère de la Recherche fédéral allemand.

En juin 2020, le gouvernement allemand mettait les bouchées plus que doubles en annonçant un financement en apparence incrémental de 2Md€ pour son plan quantique comprenant notamment l'investissement dans deux ordinateurs quantiques[1205].

Du côté du secteur privé, l'Allemagne est située juste derrière la France avec une dizaine de startups dans le quantique dont **Avanetix** (algorithmes hybrides), **InfiniQuant** (cryptographie CV-QKD), **PicoQuant** (compteurs de photons), **Kiutra** (cryogénie magnétique), **HQS Quantum Simulations** (algorithmes), **JoS Quantum** (logiciels dans la finance), **Quantum Factory** (ions piégés dans le cloud), **QuantiCor Security, QuBalt** (tous deux dans la post-quantum cryptography) et **QuTools** (métrologie).

Les grandes entreprises industrielles du pays sont aussi nombreuses à s'intéresser aux applications quantiques et en particulier dans la chimie (**BASF**), la santé (**Merck**), les télécommunications (**Deutsche Telekom**) les composants et l'automobile (**Bosch**, **Daimler**).

[1202] Voir German Government Allocates 650M€ for quantum technologies, l'annonce du gouvernement allemand (en allemand) et le plan lui-même (51 pages).

[1203] Voir Germany's QuNET Receives €165 Million To Establish Quantum Communications Infrastructure, 2019, German ministry and research sector join forces to launch major quantum communications initiative, mai 2019 et German Aerospace Center In QuNET Working On Satellite-Based Quantum Communication, novembre 2019.

[1204] Voir Germany splashes further €15m in quantum networks R&D project, octobre 2018.

[1205] Voir Germany: 2 Billion euros for quantum technology, juin 2020.

Les **Pays-Bas** sont aussi actifs dans le quantique, principalement autour de l'Université de Delft (**TU Delft**). C'est de longue date un creuset historique de la recherche en physique quantique en Europe. Nous avons ainsi cité un grand nombre de grands noms dans les débuts de cet ebook : Hendrik Antoon Lorentz (1853-1928), Heike Kamerlingh Onnes (1853-1926), George Uhlenbeck (1900-1988), Hendrick Casimir (1909-2000), Samuel Goudsmit (1902-1978), Lieven Vandersypen (1972) et Stephanie Wehner (1977).

Le gouvernement lançait en 2015 un plan de création d'ordinateur quantique étalé sur 10 ans et doté de 135M€[1206]. L'investissement était fait dans **QuTech**, le centre de recherche quantique de TU Delft lancé en 2014 et dont le budget sur 10 ans est de 145M€[1207], la moitié provenant de l'Université TU Delft et l'autre de la NWO, l'agence de financement nationale qui a l'air d'être un équivalent de l'ANR française. Qutech occupe plus de 180 personnes en tout dont seulement 37% de Hollandais avec 25 chercheurs permanents.

QuTech est aussi associé à **Intel** et **Microsoft**. QuTech a reçu un financement de $50M en 2015 d'Intel dans le cadre d'un partenariat sur leurs qubits supraconducteurs. Microsoft est aussi partenaire de QuTech, ce depuis 2010, qu'ils ont d'ailleurs déplumé en embauchant Leo Kouwenhoven dans leur laboratoire de Microsoft Research qui est sur place et planche sur le quantique topologique et le fermion de Majorana en liaison avec une équipe de QuTech dédiée au même sujet. On peut dire que les Pays-Bas se positionnent aussi comme réservoir à cerveaux pour l'industrie quantique américaine. Dans la pratique, c'est à cela que mènent leurs investissements dans la recherche.

Les approches de recherche collaborative vont bon train, notamment dans l'optique de récupérer des financements européens. En octobre 2017, QuTech lançait un partenariat avec l'Institute of Photonic Sciences, l'Université d'Innsbruck en Autriche et le Paris Centre for Quantum Computer. QuTech est aussi partenaire de l'Université d'Aix la Chapelle dans le qubit CMOS. L'Université de Delft a aussi obtenu pour le volet européen du projet QuNET cité au sujet de l'Allemagne un ERC de 1,5M€ avec un lancement en novembre 2019 et une fin prévue pour octobre 2024[1208].

D'autres initiatives aux contours flous ont été lancées comme **Quantum Helix**, qui ambitionne d'être financée dans le cadre du programme flagship quantique européen et Horizon 2020. Un autre programme dénommé **Quantum Software Consortium** devant durer 10 ans à partir de 2017 a reçu 18,8M€ de financements publics du pays dans le cadre du Gravitation Program. Il associe divers laboratoires hollandais : **TU Delft**, **QuTech** (qui fait partie de cette dernière), **QuSoft** (laboratoire de recherche dédié aux logiciels quantiques, lancé par CWI, UvA et VU en 2015), **CWI** (*Centrum Wiskunde & Informatica*, l'équivalent hollandais de l'Inria français), l'**Université de Leiden**, **UvA** (Université d'Amsterdam) et **VU** (Université libre d'Amsterdam) pour mener de la recherche en logiciels quantiques et en cryptographie.

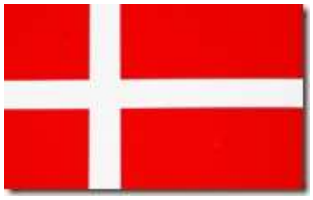
Sinon, côté entreprises, on compte notamment **Delft Circuits**, spécialisée dans la fabrication de circuits supraconducteurs, **Leiden Cryogenics** (un leader de cryostats haute puissance), **Qblox** (électronique de commande de qubits supraconducteurs), **Single Quantum** (détecteurs de photons uniques), **QuiX** (processeur photonique qui est notamment partenaire du Français Quandela, c'est

[1206] Voir l'état des lieux du plan national quantique des Pays-Bas dans National Agenda for Quantum Technologies, Quantum Delta Netherlands, septembre 2019 (51 pages).

[1207] Voir le rapport d'activité 2018 de QuTech (80 pages) ainsi qu'un rapport indépendant d'évaluation publié en 2019 et couvrant la période 2015-2018.

[1208] Voir A quantum network for distributed quantum computation, Cordis, 2019.

une filiale de Lionix, une fonderie notamment capable de produire des wafers de qubits silicium en nitrate sur SiO^2,), **Qu&Co** (logiciels quantiques), **QuSoft** (logiciels quantiques) et **ipCLock** (horloge quantique).



L'investissement de l'**Autriche** dans l'informatique quantique est concentré dans l'**IQOQI**, l'Institut für Quantenoptik und Quanteninformation d'Innsbruck et Vienne. Il se focalise en particulier dans la conception de qubits à base d'ions piégés. En est issue la startup **Alpine Quantum Technologies**, créée par Rainer Blatt de l'IQOQI, pour commercialiser des ordinateurs quantiques à ions piégés. Elle a bénéficié de financements publics à hauteur de 12,3M€. Elle concurrence la startup américaine **IonQ** issue de l'Université de Maryland qui est positionnée sur le même créneau des qubits à ions piégés, ainsi qu'**Honeywell**.

Le **VQC** (Vienna Center for Quantum Science and Technology) résulte d'un partenariat entre l'Université de Vienne, l'Université de Technologie de Vienne et l'Académie des Sciences d'Autriche. Il regroupe une masse critique d'une vingtaine de laboratoires de recherche en physique quantique.

L'Autriche est aussi investie dans la cryptographie quantique et associée avec la Chine, avec qui elle a mené des expériences d'envoi de clés quantiques par le satellite Micius pour mettre en place une communication vidéo sécurisée.

L'**IQOQI** collabore aussi avec le **Centre Spatial Universitaire de Grenoble** (CSUG) dans la mise au point d'un satellite de relai de clés quantiques de type CubeSat, similaire à celui de Singapour, dans le projet **Nanobob** (présentation, 13 slides).

La recherche dans le quantique au **Danemark** est organisée autour du Center for Quantum Devices (**QDev**) de l'Institut Niels Bohr de l'Université de Copenhague.

C'est un laboratoire de qualité focalisé notamment sur les qubits topologiques, avec son dirigeant Charles M. Marcus qui travaille aussi pour Microsoft Research dans cette filière conjointement avec les équipes de MSR de Leo Kouwenhoven aux Pays-Bas. QDev est un laboratoire de physiciens focalisé sur l'étude de la matière condensée, à savoir les couches basses physiques des qubits, comme on peut l'observer dans leurs publications.

L'équipe semble ne faire qu'une dizaine de personnes. Ils ne peuvent malheureusement pas s'appuyer ensuite sur des industriels danois ou européens pour envisager le transfert de leur recherche dans la production d'ordinateurs quantiques. C'est un problème français mais aussi européen !

Du côté de la **Suède**, il y a surtout le WACQT (Wallenberg Centre for Quantum Technology) qui fait partie de l'Université Chalmers de Gothenburg et est cofinancé par la fondation Wallenberg. Le WACQT a été financé dans le cadre d'un plan de 12 ans à hauteur de plus de $100M. Comme dans tous les pays, le centre cible toutes les branches des technologies quantiques (calcul, simulation, communications et métrologie). Ils sont notamment investis dans les qubits supraconducteurs ainsi que dans le calcul à qubits à variables continues à base de cavités électrodynamiques (QED). Le WACQT travaille aussi sur des qubits à atomes froids de Rydberg... du nom d'un physicien suédois ! Enfin, il a lancé une initiative « Women in WACQT » pour développer la diversité de genre dans les métiers du quantique.

L'**Espagne** a quelques cordes quantiques à son arc. Côté recherche, l'essentiel des efforts est concentré dans l'**ICFO** (Instituto de ciencias fotónicas) de Barcelone qui est surtout spécialisé en photonique. D'autres recherches dans le quantique sont menées au laboratoire Quantum Information and Computation (GIC-UB) de l'**Université de Barcelone** ainsi que dans le Grup d'Informació Quàntica (GIQ) de l'**Université Autonome de Barcelone**[1209].

Du côté du privé, ils ont une startup, **Qilimanjaro Quantum Hub** déjà citée, qui développe surtout une plateforme logicielle quantique en cloud, ainsi que **Entanglement Partners**, un prestataire de services qui arrive visiblement à vendre des prestations dans le domaine de la cybersécurité liées au quantique.

Ils animent sinon l'écosystème du pays, font de l'évangélisation et organisent des événements.

En 2017, la plateforme d'innovation ouverte **Open Trends** lançait **The Carrot Cake** pour encourager les projets dans le quantique. Ceci complète le think tank **Barcelona QBIT** lancé en 2015 ainsi que la **Quantum World Association** lancée au MWC 2017 qui associe la Suisse, le Canada, l'Australie et la Catalogne avec notamment les startups ID Quantique, evolutionQ, h-bar et Entanglement Partners. L'Espagne travaille en réseau, ayant compris que toute seule elle ne pourrait pas aller bien loin.

QUANTUM WORLD ASSOCIATION

QILIMANJARO

Entanglement Partners_ >

[1209] Voir Quantum Technologies in Catalonia, juillet 2019 (43 slides) qui décrit très bien l'écosystème quantique de cette région clé de l'Espagne.

La **Pologne** a notamment un Centre de recherche en physique quantique à Gdansk qui est focalisé sur la cryptographie quantique. Il a été lancé en 2007. L'Université de Varsovie est également très impliquée dans la recherche quantique.

Le National Science Centre polonais coordonne aussi le réseau de recherche international **QuantERA** lui-même financé par les budgets Europe 2020 de l'Union Européenne. Il fait cela en coordination avec l'ANR française. Les pays impliqués, outre ceux de l'Union Européenne sont la Suisse, Israël (Université Bar-Ilan) et la Turquie.

Une trentaine de projets de recherche avaient été financés après un appel à projets en 2017, certains s'étant ensuite retrouvés financés dans le Flagship quantique européen, comme SQUARE. Ce sont tous des projets de physique quantique (photonique, atomes froids, ...).

Le quantique est un domaine où l'**Union Européenne** se mobilise collectivement. Initié en 2016, un "flagship project" a germé en 2016 et était formellement lancé en 2018 pour financer de la recherche collaborative sur l'ensemble des pans de l'information quantique : métrologie, communications, calcul et simulation quantiques[1210].

Il est doté *en théorie* de 1 Md€ servant aux programmes de développement et de diffusion des technologies quantiques, étalés sur 10 ans. En théorie car les budgets n'ont pas été véritablement alloués à ce niveau par l'Union Européenne. Ils le sont par tranches étalées dans le temps.

Le flagship est surtout focalisé sur les couches physiques fondamentales de l'informatique quantique. Il est dommage qu'il ne prenne pas aussi bien en compte la dimension algorithmique et logicielle de l'informatique quantique qui est un domaine où l'Europe pourrait se distinguer. Il semblerait qu'il faille attendre pour cela les prochains appels d'offre du flagship.

Ce **Quantum Technologies Flagship** est un des trois "flagships" européens qui visent à placer l'Europe en tête de pont de ruptures technologiques majeures avec un fort investissement communautaire dans la recherche. Le ticket de base est de 1 milliard d'Euros, étalés sur plusieurs années. Les deux autres Flagship sont le "Human Brain Project" piloté par le Suisse Henri Markram et le projet Graphene dans les nanotechnologies.

[1210] Voir les motivations qui ont about it à ce Flagship : The Impact of quantum technologies on the EU's future policies: Part 1 Quantum Time, 2017 et Part 2.

La première phase du Flagship a été annoncée en octobre 2018. Elle comprend une première tranche de 132M€ alloués à 20 projets sélectionnés sur 140 candidats. Ce montant couvre trois années de besoins.

A terme 130 projets supplémentaires seront sélectionnés dans le cadre d'appels à projets complémentaires. Lancé par la Commission Européenne le 29 octobre 2018 à Vienne (vidéos), le programme couvre quatre secteurs : le calcul quantique, la simulation quantique, la communication quantique et la métrologie quantique. Cette répartition est assez habituelle et on la retrouve dans les plans de pays comme les USA ou la Chine[1211].

Parcourons la liste de ces projets financés dans cette première tranche. A chaque fois, j'indique le pays leader du projet et les montants européens accordés au projet. Ces projets impliquent en moyenne au minimum une demi-douzaine d'autres pays européens, voire limitrophes comme la Suisse et même Israël. Il n'est pas toujours facile d'obtenir la liste des parties impliquées dans les projets.

Cela commence avec trois projets côté liés au calcul quantique, probablement l'aspect le plus stratégique du plan et pourtant le moins bien représenté et financé :

- **OpenSuperQ** (Allemagne, 10,33M€) est un projet d'ordinateur quantique à base de supraconducteurs, piloté par l'Université de Saarlandes. Le projet associe également l'Espagne, la Suède, la Suisse et la Finlande et en tout 10 laboratoires de recherche. C'est une filière classique et la concurrence industrielle est rude avec Outre-Atlantique, au minimum, IBM, Google, Intel et Rigetti. L'ambition est de créer dans un premier temps un ordinateur quantique supraconducteur à 100 qubits. Pour mémoire, Rigetti pensait arriver à 128 qubits en 2019. Il semblerait que ce projet consiste surtout à créer un calculateur quantique disponible via le cloud, et focalisé sur des recherches en chimie. En étant mauvaise langue, c'est une sorte de Cloudwatt du quantique.

[1211] Voir le Dossier de Presse (28 pages), la liste complète des projets et L'Europe accélère l'industrialisation des technologies quantiques du 31 octobre 2018, dont le titre est quelque peu trompeur dans la mesure où la majorité des projets financés sont des projets de recherche et pas des projets d'industrialisation. Et puis aussi The quantum technologies roadmap: a European community view, octobre 2017 (25 pages) qui fait un point sur l'état de l'art en Europe et dans le monde. Voir aussi The EU Quantum Technology Flagship par Elisabeth Giacobino, 2018 (41 slides et vidéo).

- **AQTION** (Autriche, 9,57M€) est un projet d'ordinateurs quantiques à base d'ions piégés qui vise une capacité de 50 qubits. L'Autriche a un long historique sur le sujet et y est tout à fait légitime. Elle fait notamment face à IonQ, une startup issue de l'Université de Maryland aux USA. Atos participe à ce projet.
- **MicroQC** (Bulgarie, 2,36M€) pour la création d'un autre ordinateur quantique à base d'ions piégés. Ce projet de recherche est moins connu. Mais on sent l'approche européenne consistant à ne pas défavoriser les membres les plus récents de l'Union Européenne.

Nous avons ensuite quatre projets de simulateurs quantiques. Ces simulateurs sont des ordinateurs quantiques qui permettent de simuler des processus physiques quantiques. Ils sont utilisables en particulier pour simuler la physique des matériaux. On ne les programme pas comme les ordinateurs quantiques universels à portes quantiques de la catégorie précédente. Ces simulateurs sont pour l'instant des objets de recherche. Je n'ai pas encore identifié d'entreprise privée, établie ou startup, se lançant dans cette voie. C'est donc pour l'instant surtout une voie de recherche. Elle est cependant en train de passer doucement de la recherche fondamentale à la recherche appliquée, ne serait-ce que pour créer des algorithmes destinés aux applications cibles.

- **PASQuanS** (Allemagne, 9,25M€) est un projet de simulateur quantique à base d'ions piégés allant jusqu'à 1000 qubits. Il implique aussi le Royaume-Uni et Atos en France.
- **PhoQuS** (France, 3M€) est un projet de simulateur quantique également à base de photonique. Il est piloté par une équipe de chercheurs de PSL.
- **Qombs** (Italie, 9,3M€) est un projet de simulateur quantique à base de photonique.
- **SQUARE** (Allemagne, 2,99M€) est un projet de simulateur quantique à base d'ions de terres rares (rubidium, …). Il est piloté par l'Université de Karlsruhe et implique des laboratoires du Danemark, de Suède, Espagne et de France, comprenant Thales. Il semble qu'ils cherchent aussi à créer un processeur quantique à portes universelles.

Continuons avec les projets dans la communication quantique et la sécurisation des télécoms. On peut y constater une apparente redondance entre les projets financés qui sont tous positionnés sur la crypto quantique à base de clés symétriques et de QKD (Quantum Key Distribution, la technique d'envoi sécurisée de clés par voie optique). Curieusement, il n'y a rien sur la "cryptographie post-quantique" qui semble être plus prometteuse sur le marché de la cybersécurité. Elle ne rentre visiblement pas dans le cadre de ce Flagship puisque les techniques et algorithmes utilisés ne sont pas quantiques. Ils permettent de résister au décryptage de clés publiques classiques par des ordinateurs quantiques. Donc, exit.

- **Quantum Internet Alliance** (Pays-Bas, 10M€) (QIA) vise à déployer un réseau Internet protégé par clés quantiques (QKD) en mode réseau maillé et non seulement point à point. Les nœuds ou relais quantiques seront constitués de systèmes exploitant des atomes froids. Ils vont commencer par un réseau à trois ou quatre nœuds. Le projet est piloté par l'Université TU Delft. Le CNRS y participe et notamment Eleni Diamanti ainsi qu'Elham Kashefi et Iordanis Kerenidis. L'Université de la Sorbonne y participe également. On y trouve sinon des Suisses, des Allemands, des Danois et des Autrichiens (liste complète).
- **QRANGE** (Suisse, 3,87M€) est un projet d'amélioration des techniques de génération quantiques de nombres aléatoires. La startup suisse ID Quantique ne doit pas être loin derrière puisqu'elle est leader sur ce marché.
- **CiViQ** (Espagne, 9,9M€), ou Continuous Variable Quantum Communications, est un autre projet de sécurisation de télécommunications par fibre à base de QKD. Le projet comprend 21 parties prenantes couvrant le monde académique et industriel dont le CNRS, l'Institut Mines-Telecoms, Nokia Bell Labs France, Inria, Orange, ainsi que l'Israélien Mellanox qui est spécialisé dans les produits de communication très haut débit entre serveurs dans les data-centers ex-

ploitant l'architecture Infiniband. Il est probable qu'ils aient dans leurs cartons des produits exploitant des QKD.

- **Uniqorn** (Autriche, 9,9M€) est dans le même créneau et travaille sur un générateur de nombres aléatoires et un système de QKD. Il associe 17 organisations de 9 pays (Autriche, Pays-Bas, Italie). L'Israélien Mellanox est aussi de la partie.
- **S2QUIP** (Pays Bas, 3M€), Scalable Two-Dimensional Quantum Integrated Photonics, est un autre projet de communication sécurisée à base de QKD.
- **2D-SIPC** (Espagne, 2,9M€) est un projet de développement de composants de photo-électronique potentiellement exploitable pour créer des réseaux Internet sécurisés par clés quantiques (QKD).
- **QMICS** (Allemagne, 3M€) ou "Quantum Microwave Communication and Sensing" planche sur une technologie de création de réseau local à base de micro-ondes sur câble reliant des nœuds de réseaux supraconducteurs. Elle pourrait avoir des applications dans la communication entre processeurs de calcul quantique. Ils travaillent notamment sur la création de détecteurs de photons uniques.

Nous avons ensuite cinq projets en métrologie quantique déjà vus dans la rubrique sur la métrologie à partir de la page 506.

S'y ajoute aussi le projet **QFLAG** (Allemagne, 3,48M€) qui est la structure de pilotage et de coordination des projets du Flagship quantique européen. Il est curieux que la Commission Européenne présente ça comme un projet.

Et enfin, le projet **QLSI** attribué en mars 2020 de financement sur quatre ans de la recherche fondamentale dans les qubits silicium et qui est piloté par l'équipe de Grenoble sous la responsabilité de Maud Vinet du CEA-Leti. Ce projet est financé à hauteur de 14M€ répartis sur plusieurs laboratoires. Côté français sont aussi impliqués Atos, STMicroelectronics, SOITEC et le CNRS Institut Néel. Il implique aussi TU Delft, l'Université de Twente et TNO aux Pays-Bas, l'IMEC en Belgique, UCL et Quantum Motion au Royaume Uni, Infineon, RWTH Aachen, l'Université Konstanz, le Fraunhofer et l'IHP de Frankfort en Allemagne, l'Université de Copenhague et l'Université de Bâle.

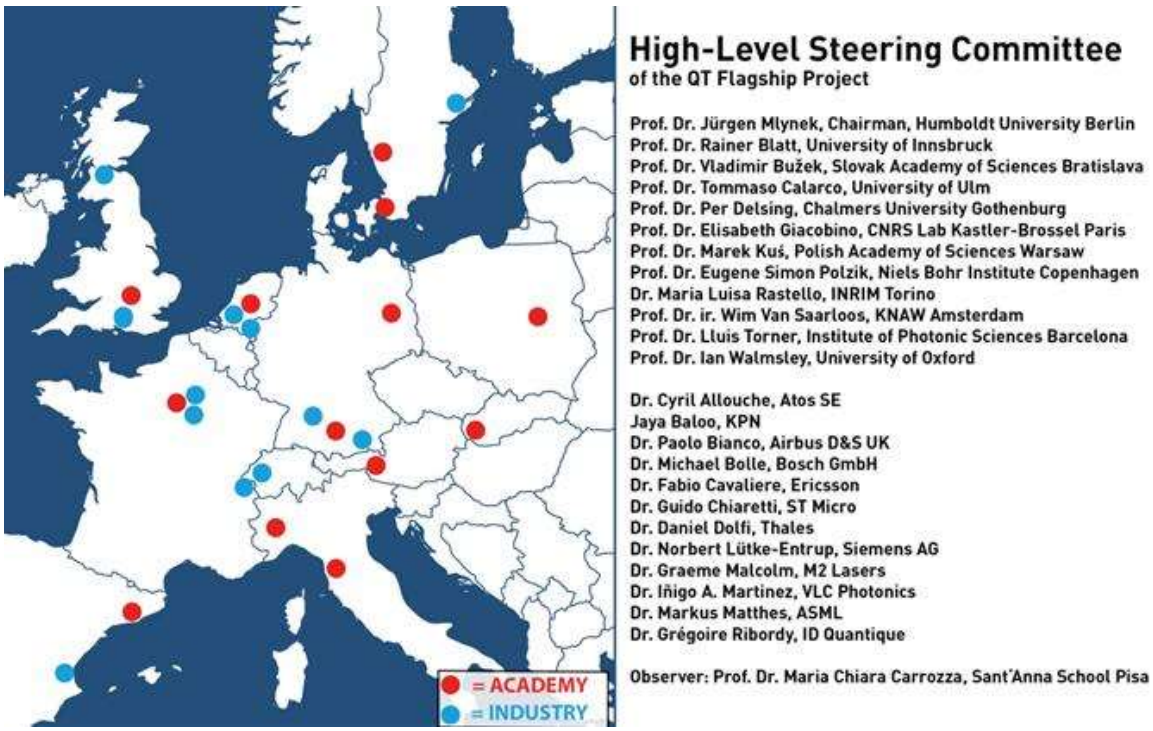
Pour comprendre la structure de ces projets avec leurs forces et faiblesses, il faut intégrer les conditions dans lesquels ils sont montés. La politique de la Commission Européenne consiste à gérer équilibre délicat entre les pays de l'Union, petits comme grands.

Les aides à la R&D favorisent aussi la recherche partenariale multi-partenaires et multi-pays. On se retrouve ainsi avec jusqu'à 20 partenaires et 9 pays impliqués dans ces différents projets. Les leaders des projets sont tous des laboratoires de recherche, en général publics. Il est difficile dans ces conditions d'identifier les voies d'industrialisation associées. Des pays externes à l'Union Européenne sont impliqués comme la Suisse, Israël, la Biélorussie, et bientôt, le Royaume Uni.

On note la forte prédominance de projets pilotés par des laboratoires de recherche allemands (5), suivis par les Pays-Bas (3), puis la France, l'Espagne et l'Autriche qui pilotent chacun 2 projets. Suivent l'Italie, le Royaume Uni et la Suisse qui pilotent chacun un seul projet.

La France est aussi impliquée dans nombre de ces projets mais sans en avoir le lead. En tout, les laboratoires du CNRS sont impliqués dans 13 des 19 projets scientifiques du Flagship[1212].

[1212] Voir New Strategic Research Agenda on Quantum technologies, février 2020 (114 pages) qui détaille l'état des lieux des projets du Quantum Flagship Européen.



source : Quantum Technology European Flagship, Jürgen Mlynek, décembre 2017 (28 slides).

On peut observer une certaine dispersion des efforts, que ce soit dans les simulateurs quantiques ou les systèmes de protection des télécommunications à base de clés quantiques (QKD). Ces projets ont un autre point commun : ils sont tous pilotés par des physiciens et concernent exclusivement le matériel. Il est très inquiétant de constater que ces projets ne comprennent pas d'efforts dans le logiciel, pour créer des algorithmes, des outils de développement et des solutions logicielles métier adaptées aux ordinateurs quantiques.

On peut espérer que de tels projets seront financés dans les phases suivantes de ce Flagship. Il en va de même de l'absence de projets de cryptographie post-quantique, même si cela peut s'expliquer comme nous l'avons déjà vu.

Dans le même temps, de nombreux industriels américains collaborent avec les laboratoires européens. Microsoft a recruté à l'Université de Delft des spécialistes du quantique, notamment dans les qubits topologiques. Intel a aussi chassé à Delft. Et IBM a une partie de ses équipes dans le quantique qui sont basées dans son laboratoire de recherche de Zurich, près de l'ETH Zurich qui abrite pas mal de spécialistes du quantique.

Nous avons ici la reproduction d'un scénario assez classique avec une excellence de recherche européenne qui se transforme en produits via les grands acteurs américains. Ceci dit, les grands acteurs américains exploitent aussi abondamment la recherche fondamentale issue de leur propre pays.

Ainsi, Google et IBM collaborent-ils avec l'Université de Santa Barbara en Californie. Le poids relatif de l'apport des laboratoires de recherche US vis à vis des laboratoires européens aux acteurs américains dépend des acteurs. Il semble plus faible pour Microsoft que pour Google et IBM.

Une note de l'ambassade de France[1213] mettait en évidence un point notable : l'**Allemagne** arriverait en troisième position mondiale en termes de publications scientifiques dans le secteur de l'informatique quantique, après les USA et la Chine et devant le Royaume Uni et le Japon. Cela ne se traduit visiblement pas en un écosystème entrepreneurial sur le domaine ni par une action particulière des grands acteurs du numérique du pays.

Sauf peut-être avec **Infineon**, la spin-off de semiconducteurs de Siemens qui s'intéresse à la cryptographie quantique. Ce syndrome est voisin en France avec une recherche assez active sur le sujet mais un côté plutôt atone du secteur privé, à l'exception notable d'Atos.

C'est lié au traditionnel différentiel entre recherche et entreprises. L'absence de grands acteurs du numérique en Europe à même de prendre le relai de la recherche est pénalisante. Qui plus est, le tissu de startups n'est pas assez bien financé et ne peut donc pas miser sur le long terme comme le fonds les homologues d'Amérique du Nord. D-Wave a été lancé en 1999, a produit son premier qubit en 2007, huit ans après et a commercialisé ses premiers ordinateurs quantiques vers 2012, donc 13 ans après sa création. Soit bien plus que la durée de vie moyenne d'un fonds d'investissement (à ne pas confondre avec celle des sociétés de gestion) !

L'Europe est par ailleurs assez active dans l'organisation de conférences scientifiques sur l'informatique quantique. Avec quelques exemples : la conférence QIP en janvier 2018 à l'Université de Delft aux Pays-Bas suivie de la conférence Quantum Europe 2018 des 17 et 18 mai 2018, également aux Pays-Bas. D'autres conférences de 2018 sur l'informatique quantique ont eu lieu ou vont avoir lieu en Suisse, au Portugal, en Espagne, en France, en Allemagne, en Autriche et même en Grèce. Parfois, la présence d'intervenants français y est négligeable, comme à Quantum Simulation & Computation de Bilbao en février 2018.

La recherché européenne est fédérée sous l'ombrelle de **QCN** (Quantum Community Network). La France y est représentée par Philippe Grangier et Sébastien Tanzilli. L'initiative est pilotée par Tommaso Callarco.

Citons aussi le projet de rechrche collaborative européen **EQUIPE** (Enable Quantum Information Processing in Europe) qui vise à faire avancer l'industrialisation de la création de solutions de calcul et de télécommunications quantiques pour l'industrie[1214].

[1213] Voir L'Informatique Quantique au Japon par Emma-Louise Scappaticci, novembre 2017 (27 pages).

[1214] Voir Simulation on / of various types of quantum computers de Kristel Michielsen (40 slides).

En juin 2020 était lancé le consortium **QuIC** (Quantum Industry Consortium), également piloté par Tommaso Calarco, avec Thomas Strohm de l'Institut Jülich de Munich et Monica Constantin de QCN Brussels. Le comble est que ce sont des chercheurs qui en sont à l'origine ! Les membres fondateurs sont des entreprises qui étaient impliquées dans au moins deux projets du Quantum Flagship Européen. On y retrouve bien logiquement Atos et Thales mais aussi Muquans et Airbus. Le consortium s'est doté d'un plan de travail fourni couvrant l'évaluation des besoins du marché, l'analyse de la chaîne de valeur des technologies quantiques, le développement de standards et réglementations, le partage de bonnes pratiques dans la protection de la propriété intellectuelle et l'évangélisation du marché, l'accès à des infrastructures, le liant entre startups et investisseurs, les questions de développement des compétences et la coordination avec les pouvoirs publics.

Enfin, en septembre 2020 était lancé le projet collaboratif européen **NEASQC** (NExt ApplicationS of Quantum Computing) destiné à développer des applications pratiques du NISQ (ordinateurs quantiques bruités, étape intermédiaire avant les ordinateurs quantiques scalable). C'est un projet H2020 qui rassemble des acteurs européens dont pas mal de français avec notamment Atos, Total, EDF, le laboratoire LORIA de l'Université de Lorraine, Astrazeneca, HQS Quantum Simulations, HSBC et l'Université de Leiden (Pays-Bas).

Russie

Terminons ce tour du continent européen avec la **Russie**. Elle n'est pas très visible dans la bataille industrielle qui se prépare autour de l'informatique quantique. Mais elle se réveille.

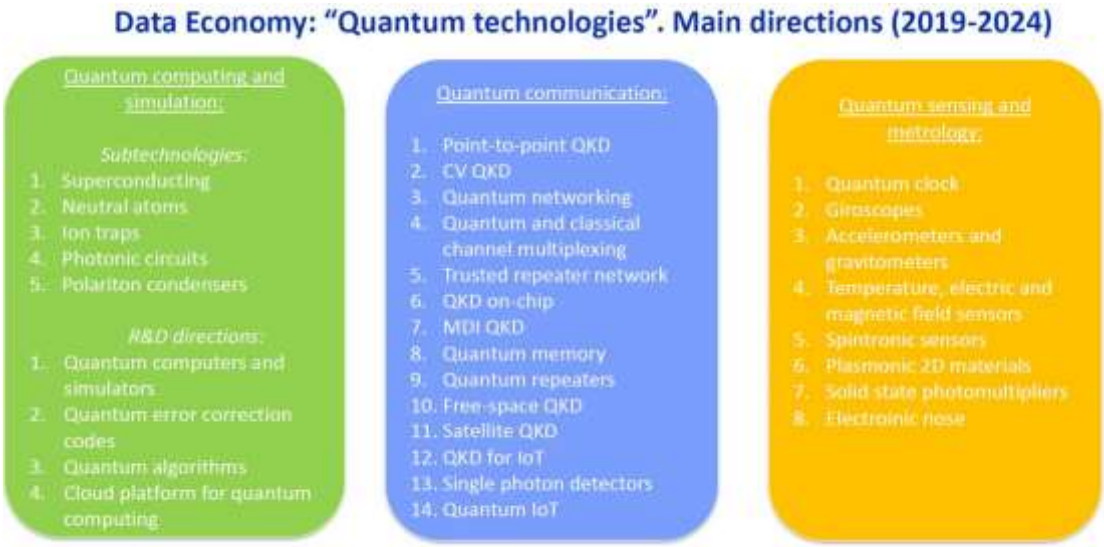
Le **Russian Quantum Center** était créé en 2010, un centre de recherche privé dédié aux différents domaines d'applications de l'informatique quantique, cryptographie quantique comprise comme il se doit. Il occuperait en tout environ 200 chercheurs.

Ses travaux couvrent de nombreuses branches de l'informatique quantique : les qubits supraconducteurs, à base d'ions piégés, de photons et de cavités de diamants. Il ne manque que le silicium ! Ils travaillent aussi dans le domaine de la métrologie quantique. Ils ont notamment développé leur propre solution de QKD et un détecteur de photon unique. Mais à ce jour, ils n'ont rien communiqué sur des avancées côté qubits. Ils collaborent avec de nombreux organismes de recherche internationaux aux USA (MIT), Canada (Université de Calgary), Allemagne (Max Planck Institute for Quantum Optics), UK (Université de Bath), etc[1215].

L'**ITMO University** de Saint-Petersbourgh comprend aussi un laboratoire de recherche en QKD tout comme le **Kazan Quantum Center** qui a déployé une QKD sur un réseau de 160 km à Kazan. Le pays prévoit de plus le lancement de satellite de communication de clé quantique QKD en 2023. Quelques autres laboratoires sont investis dans les technologies quantiques comme le **NTI Center for Quantum Communications** de l'université MISiS et le **NTI Technologies Centre** de l'Université de Moscou.

[1215] Ces informations proviennent de Evaluation Report of Russian Quantum Center, 2017 (7 pages). Voir aussi Quantum technologies in Russia, octobre 2019 (9 pages).

En décembre 2019, la Russie annonçait son propre plan d'attaque des technologies quantiques, qui semblait très focalisé sur les applications militaires, de renseignement et de cryptanalyse[1216]. Ce plan est financé à hauteur de $790M sur cinq ans. Mais en pratique, il couvre presque tous les domaines des technologies quantiques comme le montre l'inventaire *ci-dessous*[1217].



Source: roadmap draft "Data Economy: Quantum technologies", 2019

Le pays a tout naturellement fait germer quelques entreprises dans la cryptographie quantique, ne serait-ce que pour des raisons de souveraineté pour ce pays qui tient à sa position dans le monde, face à la Chine, aux USA autant que face à l'Europe[1218]. A vrai dire, ils n'ont qu'une startup dans le domaine, **Qrate Quantum Communications**, les autres étant des entreprises établies de plus longue date, comme **Infotecs**, **Scontel** et **Smarts QuantTelecom**.

Proche et Moyen-Orient

Israël est un pays qui était jusqu'en 2019 relativement discret sur le quantique, à part Gil Kalai de l'Université Hébraïque de Jérusalem qui affiche depuis 2013 un scepticisme bien ancré sur le devenir des ordinateurs quantiques. Ils ont une startup de visible dans le domaine, **Quantum Machines**.

Après une étude réalisée en 2017 par Uri Sivan (Technion) sur l'état des forces dans les technologies quantiques du pays, une première initiative de financement de la recherche quantique avait était lancée en 2018 par le gouvernement du pays et dotée de 75M€ sur un nombre d'années non précisé. Ce financement devait aller surtout au Technion, l'Université de Haïfa au nord du pays, qui veut concevoir son propre ordinateur quantique et avait par ailleurs bénéficié d'une donation de $50M.

[1216] Voir Russia joins race to make quantum dreams a reality par Quirin Schiermeier, décembre 2019.

[1217] Source : Quantum communication in Russia: status and perspective par Vladimir Egorov, 2019 (22 slides).

[1218] Voici quelques éléments sur cet écosystème : Quantum communication in Russia: status and perspective par Vladimir Egorov, 2019 (22 slides).

Ce Quantum Information Processing lab travaille sur de nombreuses pistes, presque trop avec des qubits à résonance magnétique nucléaire, en photonique et en silicium. Il est possible que la proximité d'un laboratoire de recherche d'Intel explique cette dernière piste même si elle semble être très récente dans ce laboratoire.

La recherche quantique est aussi au programme du Quantum Information Science Center de l'Université Hébraïque de Jérusalem créé en 2013 et qui est focalisé sur la communication quantique sécurisée (QKD). Il est financé à hauteur de $2M par le Ministère de la Défense. Ils travaillent aussi sur la création de portes quantiques servant à échanger des états de qubits entre processeurs quantiques. Le QISC comprend une équipe d'une vingtaine de chercheurs.

L'Université de Nanotechnologies de Bar-Ilan situé à Ramat Gan près de Tel Aviv dispose de son propre laboratoire quantique, le Quantum Entanglement in Science and Technology (QUEST), lancé en 2017 et visiblement investi dans la physique quantique à bas niveau et surtout, la communication quantique.

En juillet 2019, la **Ben-Gurion University of the Negev** (BGU) annonçait un partenariat avec le Ministère de la Défense israélien sur le quantique, sans préciser les applications visées. La startup **Accubeat** qui produit des horloges atomiques quantiques au rubidium est issue de cette université.

Il semblerait aussi que le laboratoire de R&D de Google de Tel Aviv comprenne des chercheurs dans le calcul quantique.

Enfin, en décembre 2019, un panel de spécialistes missionné par le gouvernement faisait une proposition de plan d'investissement de $350M étalés sur 6 ans dans les technologies quantiques[1219]. En quelques mois seulement, le gouvernement aurait approuvé ces propositions. Le plan est assez classique avec un investissement dans le capital humain (recrutement d'enseignants et lancement de formations), financement de la recherche et de bourses, attractivité de chercheurs étrangers et accès à des ressources en cloud pour les laboratoires de recherche. Du côté des filières, l'accent est mis sur les matériels et composants du calcul quantique, sur les télécommunications et la cryptographie quantiques ainsi que sur la métrologie quantique, en particulier dans ses applications militaires. Bref, comme partout, sur toutes les branches des technologies quantiques. Le plan est coordonné par l'ancienne Chief Scientist du Ministère de l'Industrie entre 1996-2000, Orna Berry.

Comme aux USA, ce plan a vu le jour grâce à une campagne de lobbying bien orchestrée puisque l'on voit souvent intervenir dans les médias israéliens sur le plan quantique un certain David Malits, qui est le CEO de DM Communications, une société de gestion de relations publiques[1220].

Israël n'est pas le seul pays du proche et du moyen orient qui semble investi dans la recherche quantique. L'**Iran** est aussi de la partie avec au moins deux laboratoires de recherche, l'**Université de Sharif** qui travaille sur la physique quantique en partenariat avec le Canada et le **Quantronics Lab** de l'Université Technologique d'Iran qui est dédié à la communication quantique (QKD)[1221]. Le pays organise même sa conférence sur l'informatique quantique, l'**IICQI**, ce depuis 2007[1222].

[1219] Voir Israel joins the quantum club par Uri Berkovitz, décembre 2019 et Israel joins the race to become a quantum superpower par Anna Ahronheim et Maayan Hoffman, Jerusalem Post, décembre 2019.

[1220] Voir par exemple Israeli Government To Allocate $350 Million For Quantum Computing par Analytics India Magazine, décembre 2019.

[1221] Source : Iranian research in quantum information and computation, juin 2016.

[1222] Voir http://iicqi.sharif.edu/.

Asie-Pacifique

L'**Australie** est un pays qui s'investit aussi dans le quantique à différents niveaux.

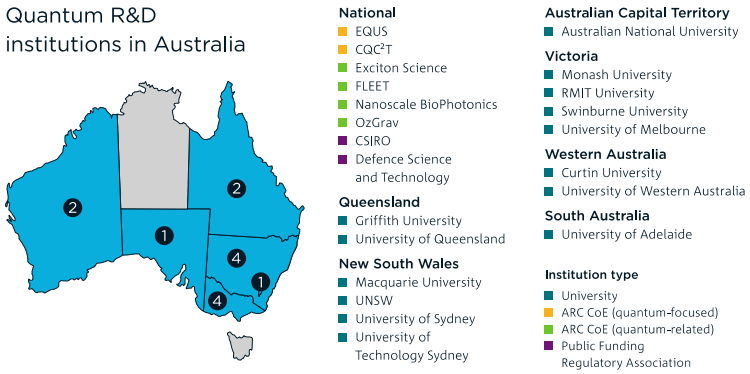
Le plan National Innovation and Science Agenda annoncé en 2015 comprenait 24 initiatives et $820M de financement sur 4 ans dont $19M sont alloués au Center for Quantum Computation and Communication Technology (CQCCT) sur 5 ans dans l'informatique quantique. Le pays est aussi prolixe en projets partenariaux public-privé et associant l'Australie à d'autres pays[1223].

Côté militaire, un fonds d'investissement du Ministère de la Défense, l'**Australian Next Generation Technologies Fund** allouait $730M à 9 domaines dont un sur le quantique[1224]. Il faut ici comme ailleurs lire entre les lignes : ces fonds étaient alloués sur 10 ans à partir de 2016. Supposons qu'ils soient distribués équitablement entre les 9 initiatives, cela nous fait $8M de fonds additionnels par an sur le quantique pour des usages militaires, métrologie compris. Vu comme cela, c'est toujours moins impressionnant !

En 2017, l'UNSW (Université de Nouvelle Galle), la Commonwealth Bank of Australia et l'opérateur télécom Telstra financaient à hauteur de $52M les efforts de création d'un processeur quantique à qubits silicium. On pourrait espérer qu'Orange fasse la même chose en France avec le CEA et/ou une startup !

En février 2019 était créé à l'UNSW le **CQC2T** (Centre of Excellence in Quantum Computation and Communication Technology) dirigé par Michelle Simmons. L'objectif est toujours de créer un ordinateur quantique à base de qubits silicium. Avec un financement fédéral de $33,7M. Il rassemblerait une communauté de 200 chercheurs.

Côté partenariats internationaux, le pays est associé avec l'Université de Singapour pour la création de satellites de télécommunication quantique. L'Université de Sydney fait partie d'un consortium international intégré dans le programme **LogiQ** de l'IARPA US. Enfin, le **Centre for Quantum Computation** de l'UNSW[1225] avait initié un partenariat avec le CEA-Leti pour la recherche appliquée de qubits silicium[1226].



[1223] Voir Charting the Australian quantum landscape, février 2019 (5 pages).

[1224] Voir Next Generation Technologies Fund, 2016.

[1225] Début 2019, le CQC de l'UNSW obtenait un financement additionnel de $33M à l'occasion de son lancement officiel. Voir Federal govt funnels $33.7 million towards UNSW's quantum research par Matt Johnston, févier 2019.

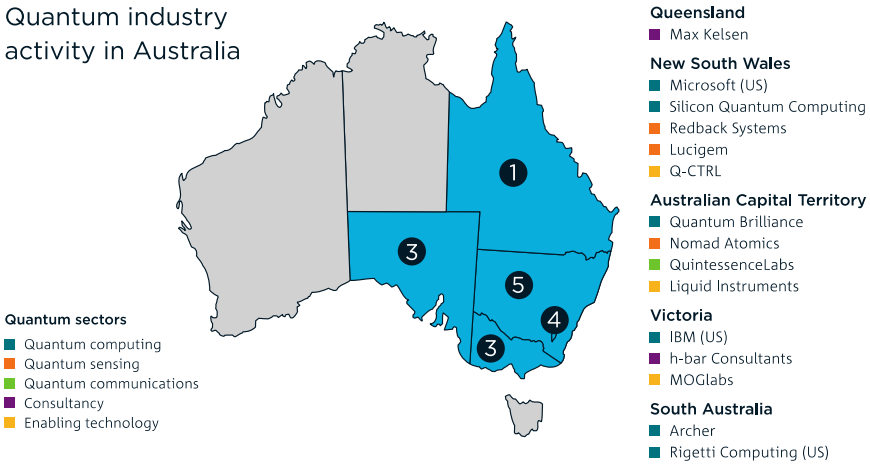
[1226] Il avait même été signé en mai 2018 en présence d'Emmanuel Macron et du Premier Ministre australien Malcolm Turnbull. Ce partenariat associe aussi la société **Silicon Quantum Computing** (SQC) issue de l'UNSW, créée par **Michelle Simmons**, et dont les actionnaires comprennent le gouvernement australien ainsi que l'opérateur Telstra. Il porte sur le développement de technologies quantiques CMOS. Il associe enfin Andrew Dzurak, un physicien de l'UNSW spécialisé dans les qubits silicium. Ceci étant dit, ce partenariat semble être à ce stade une déclaration de bonnes intentions, notamment concernant la partie industrialisation. La question des brevets n'est notamment pas entièrement tranchée. En 2020, il semblait en rade.

Le pays comprend aussi **EQUS** (Arc Center of Excellence for Engineered Quantum Systems), un centre national de recherche en métrologie quantique. Il est notamment partenaire avec Microsoft, Moglabs et Lockheed Martin.

Du côté entrepreneurial, on compte trois startups dans le domaine des technologies quantiques avec **QuintessenceLabs** (clés optiques QKD), **QxBranch** (logiciels et conseil, une startup américaine avec un bureau en Australie, acquise par Rigetti en juillet 2019) et **Silicon Quantum Computing** (qubits silicium) que nous venions de citer.

En mai 2020, le gouvernement du pays décidait de mettre de l'ordre dans sa stratégie quantique avec la publication d'un plan par CSIRO, leur CNRS[1227]. Ils ambitionnent d'en faire une industrie de $4B créant 16 000 emplois d'ici 2040 sur un total prévisionnel mondial de $86B. La répartition prévue est $2,5B et 10 000 emplois pour le calcul, $900M et 3000 emplois pour la métrologie et $800K et 3000 emplois pour les télécommunications. Les moyens ? Définir une stratégie coordonnée, financer la recherche et la création d'entreprises, former les talents et créer une chaîne de valeur industrielle cohérente.

A noter un point relativement nouveau dans un tel plan voisin de ce qui avait pas mal préoccupé la mission Villani sur l'intelligence artificielle entre 2017 et 2018 : explorer les questions d'éthiques, sociales et environnementales qui pourraient être soulevées par les technologies quantiques. Le sujet monte en importance depuis 2020.



Ils se posent comme dans le plan français la question de la chaîne d'approvisionnement des composants et matériaux clés des technologies quantiques.

Côté entreprises et startups, ils en ont quelques-unes réaprties dans cette carte. Ils mettent en avant Microsoft et IBM. Soit. Rigetti parce-que ces derniers ont acquis la startup locale QxBranch. Et quelques autres startups, dont pas mal spécialisées autour du diamant.

Passons à l'Asie en démarrant avec le **Japon**. Le pays se distingue par une recherche fondamentale très active et orientée long terme[1228] et par l'initialisation de deux vagues technologiques clés du calcul quantique.

[1227] Voir Growing Australia's Quantum Technology Industry par CSIRO, mai 2020 (56 pages) et Australia could lose its quantum computing lead, CSIRO warns par John Davidson, mai 2020.

[1228] Une note de l'ambassade de France au Japon de fin 2017 faisant le point de l'informatique quantique au Japon (27 pages) illustrait un investissement de long terme du pays dans l'exploration de l'informatique quantique, dans la lignée de leurs efforts dans les supercalculateurs, pilotés notamment par Fujitsu. On y trouve aussi un bel historique de la contribution des scientifiques japonais aux progrès de la physique quantique aux débuts du 20e siècle.

Il y a d'un côté, la création des premiers qubits supraconducteurs en 1999 par **Yasunobu Nakamura**, **Jaw Shen Tsai** (tous les deux alors chez NEC) en liaison avec Yuri Pashkin (Université de Lancaster, UK) puis celle du principe du recuit quantique par **Hidetoshi Nishimori** en 1998[1229].

Cela a cependant un arrière-goût amer, que l'on connait aussi parfois en France, dans la mesure où les acteurs économiques qui tirent leur épingle du jeu dans ces deux créneaux sont nord-américains, avec IBM, Google et Rigetti (USA) pour les qubits supraconducteurs et D-Wave (Canada) pour le recuit quantique.

La recherche publique japonaise est pilotée par plusieurs agences indépendantes rattachées à différents ministères qui financent des laboratoires publics, ceux des Universités[1230] et de la recherche partenariale avec les entreprises [1231] :

- **JST** (Japan Science and Technology Agency) financée par le ministère de la recherche et qui finance des projets de recherche orientés deep techs et fait aussi la promotion des sciences auprès du grand public et de la collaboration scientifique internationale. On dirait qu'il s'agit d'un mélange de l'ANR et d'Universcience. En 2016, la JST lançait un projet de Yasunobu Nakamura de « Macroscopic Quantum Machines » permettant d'assembler 100 qubits supraconducteurs.
- **RIKEN** (Institute of Physical and Chemical Research) également financée par le ministère de la recherche (MEXT). Avec environ 3000 chercheurs en tout. Il comprend un laboratoire de physique quantique théorique, piloté par Franco Nori et un autre en photonique, dirigé par Katsumi Midorikawa. Ils travaillent notamment sur les qubits silicium.
- **NICT** (National Institute of Information and Communication Technologies) qui correspond à l'ancienne branche de recherche de France Télécom maintenant dans les Orange Labs, comprend le Quantum ICT Advanced Development Center qui est notamment spécialisé en cryptographie quantique. L'institut réalisait en juillet 2017 une démonstration de télécommunication quantique exploitant un microsatellite qui rappelle l'expérience chinoise avec le satellite Micius réalisée la même année.
- **NII** (National Institute of Informatics) est l'équivalent de l'Inria. Mais il ne comprend qu'une centaine de chercheurs. Il se focalise sur la recherche en informatique quantique théorique mais planche aussi sur des qubits supraconducteurs et silicium.

  Le JFLI (Japanese-French Laboratory for Informatics) créé en 2009 est basé à Tokyo et hébergé à la fois au NII et à l'Université de Tokyo. Il associe des chercheurs des Universités de Tokyo, de Keio, du NII avec ceux du CNRS, de Sorbonne Université (LIP6), de l'Inria et de l'Université Paris-Sud. Cette équipe pluridisciplinaire va de la physique fondamentale à l'algorithmique et étudie la faisabilité du calcul quantique à grande échelle tout comme la cryptographie quantique. Le laboratoire est codirigé par **Kae Nemoto**, du NII, l'une des rares femmes de tout ce panorama. Depuis début 2020 y travaille Damian Markham du CNRS LIP6.
- **NEDO** (New Energy and Industrial Technology Development Organization) qui est rattachée au ministère de l'économie et de l'industrie, le METI. Il fait penser à la branche énergie du CEA. Il est particulièrement investi dans la recherche en recuit quantique avec un projet s'étalant de 2018 à 2022 doté de $4,5M par an.

[1229] Voir Quantum annealing in the transverse Ising model par Tadashi Kadowaki et Hidetoshi Nishimori, 1998 (9 pages) et Quantum Annealing by Hidetoshi Nishimori où il explique les fondements du recuit quantique, utilisé par D-Wave.

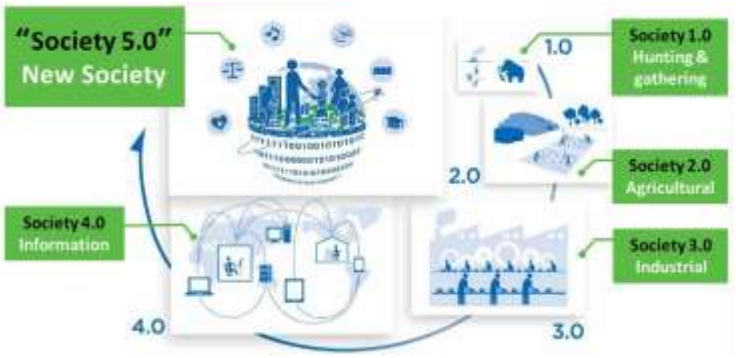
[1230] Les laboratoires les plus actifs dans le quantique se trouvent dans les universités de Tokyo, de Kyoto, Tohoku, Osaka, Nagoya, Keio, Tsukuka et Hokkaido.

[1231] Voir Activities on Quantum Information Technology in Japan par Akihisa Tomita, juin 2019 (19 slides). C'est la source du schéma dans les pages qui suivent.

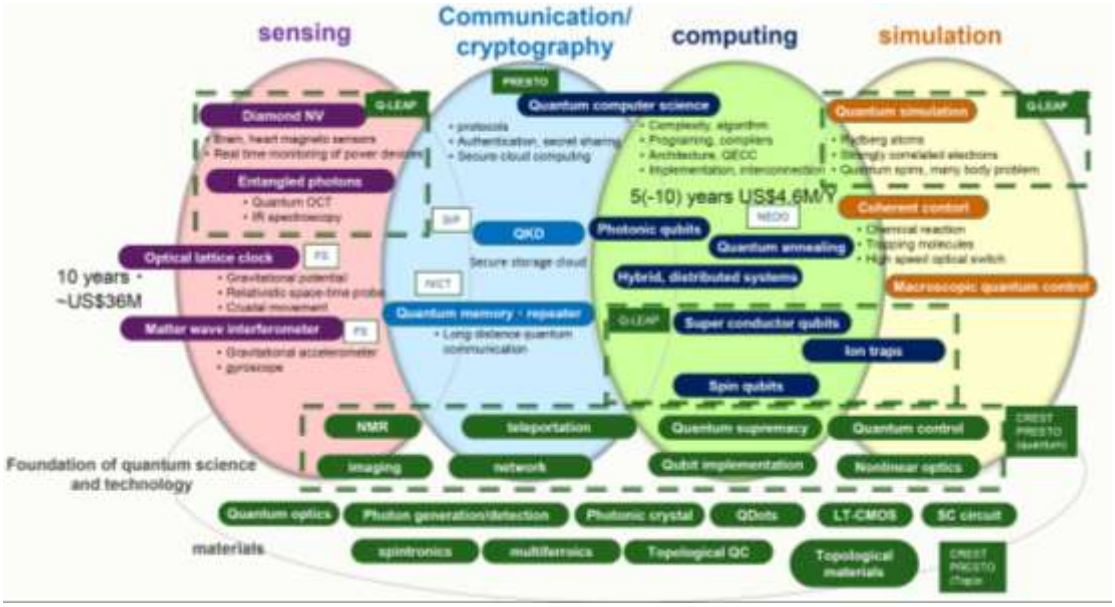
- **AIST** (National Institute of Advanced Industrial Science and Technology) également financées par le METI. Il emploie environ 2300 chercheurs en tout. Plusieurs laboratoires ont l'air dédiés aux sciences des nanomatériaux. On y trouve aussi un groupe de recherche sur la mesure de precision qui semble être l'équivalent du NIST américain et du LNE français.
- **QST (**National Institutes for Quantum and Radiological Science and Technology**)** étaient lancés en avril 2016 dotés de $487M de budget annuel. Ce montant impressionnant n'est pas alloué exclusivement aux technologies quantiques. Il couvre surtout le vaste secteur de la métrologie quantique et en particulier celui de l'imagerie médicale.

Le gouvernement japonais avait lancé diverses initiatives dans le quantique comme **PRESTO** (depuis 2016) ou le programme transversal **CREST** (aussi depuis 2016) ainsi que les projets **ERATO** en 1981 (Exploratory Research for Advanced Technology). Les initiatives quantiques du pays s'inscrivent en ce moment dans leur cinquième plan pour les sciences et technologies, s'étalant entre 2016 et 2022.

De manière typiquement japonaise, ce plan est relié à un objectif sociétal « Society 5.0 » visant à rapprocher le cyberespace et l'espace physique pour résoudre les problèmes sociaux de la société et créer une société centrée sur l'humain[1232]. Le tout avec de l'IA, des capteurs quantiques et de la cybersécurité. Si un politique français s'avançait de la sorte, il se ferait karchériser sur le champ !



Mais le projet *flagship* **Q-LEAP** lancé fin 2019 par le Ministère de la Recherche (MEXT) semble le plus ambitieux et vise à rattraper aussi bien la Chine que les USA, même si une alliance avec les USA semble aussi à l'ordre du jour[1233].



[1232] Voir Outline of the Fifth Science and Technology Basic Plan (2 pages).

[1233] Voir Japan plots 20-year race to quantum computers, chasing US and China par Noriaki Koshikawa, novembre 2019, Japan plots 20-year race to quantum computers, chasing US and China, par Noriaki Koshikawa, novembre 2019, Land of the Rising Qubit: Japan's Quantum Computing Landscape par James Dargan, décembre 2019, et Japan, U.S. unite to counter China in quantum computer race, décembre 2019.

La roadmap s'étale jusqu'à 2039 et il est doté de $200M sur la première période de 10 ans. Le programme cible le calcul quantique, la métrologie quantique et les lasers de nouvelle génération. On y trouve des projets pour créer des qubits un peut tout azimut : supraconducteurs, atomes froids, ions piégés et en silicium. Ce « Flagship » se déroulera jusqu'en 2027. Chaque projet a un directeur et est évalué par un comité d'experts.

Voici quelques chercheurs qui ont l'air de compter au Japon en plus de ceux qui sont cités ci-dessus[1234] :

Akira Furusawa de l'Université de Tokyo effectue des recherches en photonique et a l'ambition de créer une solution de calcul quantique à grande échelle avec des qubits à base de photons.

Yoshihisa Yamamoto (1950), un ancien de Stanford et directeur du laboratoire de physique et d'informatique de NTT, qui a œuvré dans un très grand nombre de domaines en photonique, en QKD ainsi que sur les quantum dots silicium. Il serait très influent au Japon sur les choix technologiques du pays[1235]. Il est le pilote du projet QIP (Quantum Information Project), l'un des projets du programme de recherche national FIRST sélectionné en 2009 et qui couvrait toutes les branches des applications du quantique (source).

Kohei Itoh de l'Université de Keio gère le projet Q-LEAP depuis 2018 qui planche sur des procédés d'assemblage de différents isotopes de silicium dans des composants CMOS ainsi que sur de la magnétométrie quantique à base de NV center (vidéo). Il est aussi partenaire du Q Lab d'IBM à Tokyo.

Yasuhiko Arakawa (1952) de l'Université de Tokyo qui est spécialisé dans la physique des semiconducteurs et de l'optoélectronique qui est à l'origine de nouveaux procédés d'exploitation des quantum dots en métrologie.

Yasuobu Nakamura (1968) qui est spécialisé dans les qubits supraconducteurs et officie au RCAST (Research Center for Advanced Science and Technology) de l'Université de Tokyo et dans le CEMS (Center for Emergent Matter Science) de RIKEN[1236].

François Le Gall (1959) est un chercheur Français installé à l'Université de Kyoto qui est spécialisé en théorie de l'informatique quantique, mathématiques, algorithmes quantiques et cryptographie. Il s'intéresse aussi au calcul quantique distribué (vidéo). Il est installé au Japon depuis plus de 20 ans.

Masahito Hayashi de l'Université de Nagoya est à l'origine un mathématicien, devenu spécialiste de l'informatique quantique théorique. Il a notamment coordonné le projet ERATO sur l'informatique quantique théorique.

Masahiro Kitagawa de l'Université d'Osaka est spécialisé dans la métrologie quantique à base de spin de noyaux d'atomes dans la résonance magnétique nucléaire avec des applications notables dans l'imagerie médicale.

Mio Murao qui a créé et dirige le Quantum Information Group de l'Université de Tokyo qui porte son nom (Murao Group). Cette chercheuse est spécialisée dans le calcul quantique distribué, en algorithmes de simulation de systèmes quantiques, en protocoles de télécommunications quantiques et en algorithmes quantiques. Et elle s'exprime très bien en anglais ce qui lui a permis de servir de passerelle avec la recherche aux USA (vidéo).

[1234] Source : Q2B 2019 - International Government Panel, décembre 2019.

[1235] Il est notamment le coauteur de la note d'information Quantum information science and technology in Japan, février 2019 (8 pages).

[1236] Voir sa présentation de l'état de l'art du calcul quantique Development of quantum hardware towards fault fault-tolerant quantum computing par Yasunobu Nakamura (19 slides).

Nobuyuki Imoto de l'Université d'Osaka University pilote de la recherche en cryptographie et télécommunications quantiques.

Masahide Sasaki du NICT pilote une bonne part des efforts en cryptographie quantique du Japon. Il a notamment contribué au projet SOTA de communication de clé quantique avec un satellite[1237].

Passons au secteur privé. Les startups japonaises sont plutôt spécialisées dans les logiciels et en particulier dans les logiciels pour le calcul à recuit quantique sur machines D-Wave. Nous avons ainsi **A*Quantum** (2018, logiciel pour recuit quantique), **D Slit Technologies** (2018, logiciels), **Groovenauts** (2012, logiciel pour recuit quantique), **Jij** (2018, framework pour recuit quantique), **MDR** (2008, simulation chimique), **QunaSys** (2018, santé), **Sigma-I** (2019, logiciels pour recuit quantique) et **Tokyo Quantum Computing** (2017, logiciels pour recuit quantique).

A noter que le fonds d'investissements de **Softbank** abondé par de l'argent de la famille Saoud et doté de $100B doit aussi investir tout azimut dans le quantique (source). Cependant, trois ans après son annonce, le fonds n'a pas l'air d'avoir une seule participation dans les technologies quantiques. Il faut toujours se méfier des effets d'annonce ! Entre temps, ils ont perdu des milliards de dollars avec Wework !

Dans le privé, les grands groupes industriels japonais sont surtout focalisés sur les télécommunications et la cryptographie quantiques, un peu comme en Chine et en Corée du Sud, ainsi que sur le calcul à base de recuit quantique ou non quantique.

Hitachi a aussi un laboratoire de recherche situé à l'Université de Cambridge (UK) qui planche sur les clés quantiques, l'informatique quantique et la création de composants SQUID pour qubits supraconducteurs.

En 2017, l'opérateur télécom **NTT** lançait un prototype de réseau de neurones quantique (QNN) à base de photonique, en collaboration avec le **National Institute of Informatics** et l'**Université de Tokyo**. Il était disponible sur le cloud sur qnncloud.com (vidéo) mais le service a été arrêté en mars 2019[1238].

Toshiba Corporation s'est lancé dans la cryptographie quantique dès 2003. Ils travaillent dessus avec le Quantum Information Group (QIG) à l'Université de Cambridge, UK. Ils ont réalisé une première démonstration de communication quantique en 2014, en envoyant 878 Gbits/s de données sécurisées sur une fibre de 45 km entre deux zones de la région de Tokyo sur une durée cumulée de 34 jours, à raison de 300 kbits/s. Ils poursuivaient les expériences en 2019 et avec British Telecom au Royaume-Uni[1239].

NTT entretient quatre laboratoires de recherche appliquée dans le quantique, focalisés dans les télécommunications et la cryptographie quantiques, le tout avec une quarantaine de chercheurs[1240].

NTT a aussi déployé un réseau de communication quantique QKD avec Toshiba, NEC et le NICT à Tokyo avec trois nœuds distants de 11 et 45 km[1241].

[1237] Voir QKD from a microsatellite: the SOTA experience, octobre 2018 (10 pages).

[1238] Voir Japan launches its first quantum computer de Walter Sim, novembre 2017.

[1239] Voir Performance Limits for Quantum Key Distribution Networks par Andrew Shields, juin 2019 (16 slides).

[1240] Cela amène d'ailleurs à une inflation galopante des salaires pour les talents les plus pointus, un peu comme dans la Silicon Valley. Voir NTT offers researchers $1 million salaries in bid to lure top talent in cryptography, quantum computing, novembre 2019.

[1241] Voir Tokyo QKD Network and its application to distributed storage network par Masahiro Takeoka, juin 2019 (22 slides).

Ils travaillent aussi dans la filière des qubits CMOS à quantum dots. En novembre 2017, ils annonçaient mettre au point avec l'Université de Tokyo et le NII le QNNcloud, un ordinateur quantique utilisant l'optique linéaire (photons) mis en service dans le cloud pour simuler des réseaux de neurones avec une boucle optique alimentée par des impulsions laser (vidéo)[1242].

Il serait très peu consommateur d'énergie, de l'ordre de 1 kW. C'est en fait plutôt un concurrent de D-Wave. QNNcloud est un projet financé dans le cadre du programme d'innovation ImPACT et en partenariat avec le National Institute of Informatics (NII), l'Université de Stanford, celles de Tokyo, Osaka et Tohoku. Le projet avait démarré en 2011.

Enfin, plusieurs projets de calcul d'optimisation par recuit non quantique sur composants CMOS ont été lancés. Il y a celui de **Fujitsu** dont nous avons déjà longuement parlé mais aussi le projet NEDO piloté par Masanao Yamaoka et Masato Hayashi chez **Hitachi**[1243] en partenariat avec les laboratoires de l'AIST, RIKEN et NEDO (New Energy and Industrial Technology Development Organization, équivalent de la branche énergie du CEA).

Et puis le projet de **NEC** dans le recuit quantique piloté par **Yuichi Nakamura** en liaison avec l'Université Waseda, celles de Yokohama et de Kyoto, l'AIST et Titech (Tokyo Institute of Technology). Il s'agit en fait pour eux d'optimiser la partie classique du recuit avec des processeurs vectoriels de NEC. La partie quantique a l'air d'être gérée sur des machines de D-Wave. NEC est aussi versé dans les clés quantiques (QKD).

IBM annonçait fin 2019 l'ouverture d'un Q Lab à Tokyo en partenariat avec l'Université de Tokyo. L'investissement d'IBM au Japon suit un modèle déjà inauguré en France à Montpellier en 2018, en Allemagne en septembre 2019 et au Canada avec l'Institut Quantique en juin 2020 : un partenariat avec une Université, des investissements en formation et surtout, un investissement technico-marketing pour évangéliser le quantique chez les grands clients[1244].

Citons enfin **Recruit Communications Ltd** (1960), une grande société de $16B de CA spécialisée dans les RH, la communication et le marketing qui s'est distinguée en lançant en 2017 un partenariat avec D-Wave pour développer des solutions à base de recuit quantique pour l'optimisation opérationnelle du marketing, de la communication et de la publicité. Ils ont notamment développé la bibliothèque open source PyQUBO qui simplifie le développement d'applications logicielles de recuit quantique[1245]. Encore D-Wave, qui a décidément le vent en poupe au Japon !

[1242] Le procédé qui ne s'appuie pas sur la notion de qubits est décrit dans Universal Quantum Computing with Measurement-Induced Continuous-Variable, 2017 (5 pages).

[1243] Voir CMOS Annealing Machine – developed through multi-disciplinary cooperation, novembre 2018, Overview of CMOS Annealing Machines par Masanao Yamaoka, Hitachi, (4 pages) et Voir A 2 x 30k-Spin Multi-Chip Scalable CMOS Annealing Processor Based on a Processing- In-Memory Approach for Solving Large-Scale Combinatorial Optimization Problems, novembre 2019.

[1244] Voir IBM Takes Its Quantum Computer to Japan to Launch Country-Wide Quantum Initiative par Anthony Annunziata, décembre 2019. En partenariat avec l'Université de Tokyo et IBM and the University of Tokyo Launch Quantum Computing Initiative for Japan par IBM, 2019. En août 2020, IBM enjolivait un peu ce partenariat en annonçant la création d'un consortium pour l'adoption des technologies quantiques au Japon. Voir IBM lance un consortium mondial dédié à l'innovation quantique par Chris Duckett, août 2020 qui fait référence à une annonce qui ne concerne en fait que le Japon : IBM and the University of Tokyo Unveil the Quantum Innovation Initiative Consortium to Accelerate Japan's Quantum Research and Development Leadership par IBM, août 2020.

[1245] Voir Recruit Communications and D-Wave Collaborate to Apply Quantum Computing to Marketing, Advertising, and Communications Optimization, mai 2017.

En **Corée du Sud,** l'opérateur télécom **SK Telecom** investit dans les télécommunications quantiques[1246]. Ils sont partenaires de la Florida Atlantic University. Ils ont aussi investi en 2016 dans la startup suisse ID Quantique.

SK Telecom est également partenaire depuis 2017 avec Nokia dans le domaine des QKD tout comme avec Deutsche Telekom avec qui ils ont établi une "Quantum Alliance" pour créer des télécommunications sécurisées. SK Telecom a déployé un réseau de QKD dans le backbone de son réseau 4K dans la ville de Sejong sur deux liaisons de respectivement 38 et 50 km[1247].

De son côté, **Samsung** investit aussi dans les QKD et la cryptographie quantiques. Ils intégraient un générateur quantique de nombres aléatoires dans une version dédiée d'un smartphone Galaxy pour le marché coréen en avril 2020, le tout avec un composant provenant d'IQ Quantique, la startup suisse acquise par SK Telecom en 2018.

Le petit état de **Singapour** est connu pour son dynamisme économique et entrepreneurial. Au sein de l'Université de Singapour, la recherche dans le quantique est consolidée depuis décembre 2007 dans le **Center for Quantum Technologies** (CQT) avec un financement d'environ $15M annuels[1248].

Il est comme c'est souvent le cas investi à la fois dans le calcul quantique (atomes froids dans le groupe de Berge Englert, photons et supraconducteurs dans le groupe de Dimitris Angelakis, ions piégés), la cryptographie quantique (groupe de Kwek Leong Chuan) et la métrologie quantique (notamment des horloges atomiques dans le groupe de Murray Barrett).

Le CQT était dirigé depuis sa création et jusqu'à juillet 2020 par Artur Ekert. Il regroupe une vingtaine d'équipes représentant 22 chercheurs permanents, 60 research fellows et 60 thésards, couvrant les quatre habituels domaines des technologies quantiques. Cela représente un total de 300 personnes en tout.

Sur les 22 responsables de recherche, environ le quart sont des singapouriens ayant généralement fait une thèse à l'étranger. Singapour fait en sorte d'attirer des étrangers de talents et à faire en sorte qu'ils s'installent dans la durée dans ce pays de cinq millions d'habitants.

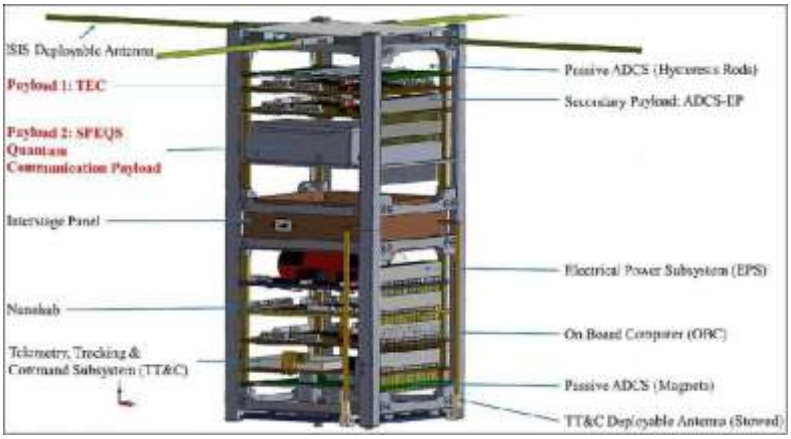
[1246] Voir SK Telecom Continues to Protect its 5G Network with Quantum Cryptography Technologies, march 2019.

[1247] Voir Quantum Safe Communication – Preparing for the Next Era par Dong-Hi Sim, juin 2019 (21 slides).

[1248] Artur Ekert raconte qu'il avait été persuadé en 2000 de rejoindre Singapour par Tony Tan, qui était à l'époque ministre de la défense du pays. Il l'avait rencontré dans une conférence où son discours visionnaire, pour un politique, l'avait impressionné. Tony Tan a prise en charge en 2005 le fonds souverain Singapore Investment Corporation puis la Singapore's National Research Foundation. Il était à l'origine de la stratégie d'investissement ciblée dans des domaines pointus de la recherche, que l'on qualifie aujourd'hui de deep tech. Ce Tony Tan est ensuite devenu le président de Singapour entre 2011 et jusqu'à 2017. Le CQT a été lancé en 2006. L'histoire est racontée dans l'ouvrage 50 years of science in Singapore pages 362 à 387, février 2017. Son credo personnel : pour réussir, il faut attirer dans l'ordre les bonnes personnes, les idées originales puis les financements. Trop souvent, cela arrive trop par le financement.

Six startups sont sorties du CQT avec **Entropica Labs** (algorithmes quantiques), **Horizon Quantum Computing** (logiciels), **Innovatus Q** (algorithmes hybrides), **S-Fifteen Instruments** (cryptographie quantique) et **SpeQtral** (QKD satellite).

Singapour est notamment associé à la Chine voisine. Singapour a lancé en 2015 son nano-satellite Galassia-2U, créé par le CQT et servant à expérimenter des communications quantiques cryptées via QKD. Galassia est intégré dans un format CubeSat à deux unités (deux cubes l'un sur l'autre, cf *ci-contre*). Il ne fait que 3,4 Kg au total. Il a été lancé avec 5 autres satellites dont le satellite de télécommunications TeLEOS-1 (400 kg) fin 2015 par un lanceur indien.



source : https://directory.eoportal.org/web/eoportal/satellite-missions/g/galassia

La durée de vie de ce genre de satellite est de six mois[1249]. Ces expériences ont mené, visiblement, à la création de la startup S-Fifteen Space Systems. Mais, il reste à trouver des solutions pour que ces satellites durent plus longtemps sur leur orbite basse et ne contribuent pas encore plus à poubelliser l'espace autour de la Terre. Auparavant, le CQT avait eu l'occasion de tester involontairement l'envoi d'un satellite (ComX-2) dans une fusée ayant explosé en 2014 après le décollage. Non sans humour, il explique que ComX-2 n'a pas survécu à l'expérience[1250]. Mais ils ont récupéré un ComX-2 après un autre lancement raté. Ces initiatives sont dues à Alexander Ling, principal investigator du CQT.

Le CQT est aussi associé depuis 2016 au laboratoire lancé par l'opérateur télécom **Singtel** et la **National University of Singapore** pour le déploiement de QKD sur fibres optiques avec des répéteurs.

Toujours dans le domaine de la QKD, fin 2019, une équipe de la **Nanyang Technological University** (NTU) mettait au point un chipset de 3 mm de côté capable d'intégrer une CV-QKD, un système de chiffrement à base de clé quantique à variable continue[1251]. Ce n'est pas sans rappeler ce que souhaite faire la startup anglaise Kets Quantum Security.

Côté partenariats internationaux, citons aussi l'association d'une responsable de groupe de recherche du CQT en charge de l'étude du bruit et des codes de correction d'erreurs, **Hui Khoon Ng**, avec **Alexia Auffèves** du CNRS Institut Néel et Atos sur l'évaluation de la thermodynamique du calcul quantique. Le CQT accueille plusieurs chercheurs venant de France dont **Miklos Santha** (CNRS). **Christian Miniatura** travaille de son côté à l'université NTU.

[1249] Voir Quantum Tech demos on CubeSat nanosatellites (41 slides).

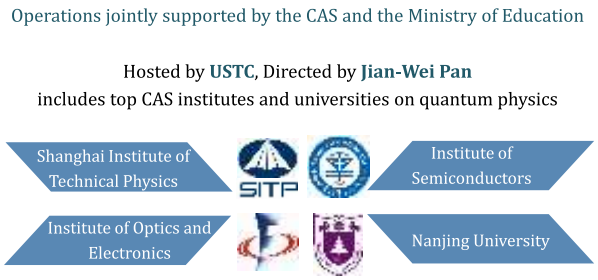
[1250] Dans Extreme Environmental Testing of a Rugged Correlated Photon Source, 2015 (2 pages).

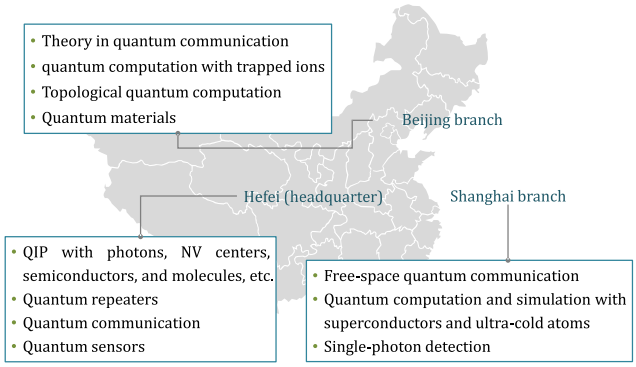
[1251] Voir Quantum chip 1,000 times smaller than current setups, novembre 2019.

Comme dans pas mal de secteurs technologiques, la **Chine** affirme haut et fort ses ambitions et sa puissance dans le secteur du quantique. Elle s'est aussi lancée dans des efforts tout azimut, touchant la cryptographie, les télécommunications, la simulation et le calcul quantiques[1252].

De même qu'au Royaume-Uni, cet investissement a été pris en main assez tôt par l'exécutif et dès 2013 avec l'implication de Xi Jinping, le président Chinois, lors d'une visite du laboratoire d'Anhui, portant surtout sur la cryptographie quantique, associée à une session de formation. Dès 2015, Xi Jinping intégrait la communication quantique dans les priorités scientifiques du pays. L'informatique quantique était intégrée de son côté dans les priorités du 13ième plan couvrant la période 2016-2020. C'est l'avantage d'avoir un gouvernement constitué en majorité de politiques ayant une formation initiale scientifique.

Les montants investis dans le quantique étaient respectivement de $160M dans le 11e plan couvrant la période 2006-2010, de $800M dans le 12e plan couvrant 2011-2016 et de $320M dans le 13e plan démarrant en 2016, complétés par $640M de financement des régions[1253]. Plus tard, le gouvernement chinois a communiqué sur un montant de $34B correspondant cependant à plusieurs priorités scientifiques comprenant le quantique. En pratique, cela représentait entre $2B et $3B étalés entre 2016 et 2020. Mais c'est déjà conséquent.





Ces investissements sont répartis principalement sur trois villes : Beijing, Shanghai et Hefei, à 500 km à l'Ouest de Shanghai. Ils sont spécialisés respectivement sur les communications quantiques, le calcul à base d'ions piégés, le calcul à base de qubits topologiques et les matériaux quantiques pour Beijing, le calcul en qubits silicium, NV centers et photons, les communications et la métrologie quantiques pour Hefei et enfin, la communication, le calcul en qubits supraconducteurs et à atomes froids et la détection de photons pour Shanghai.

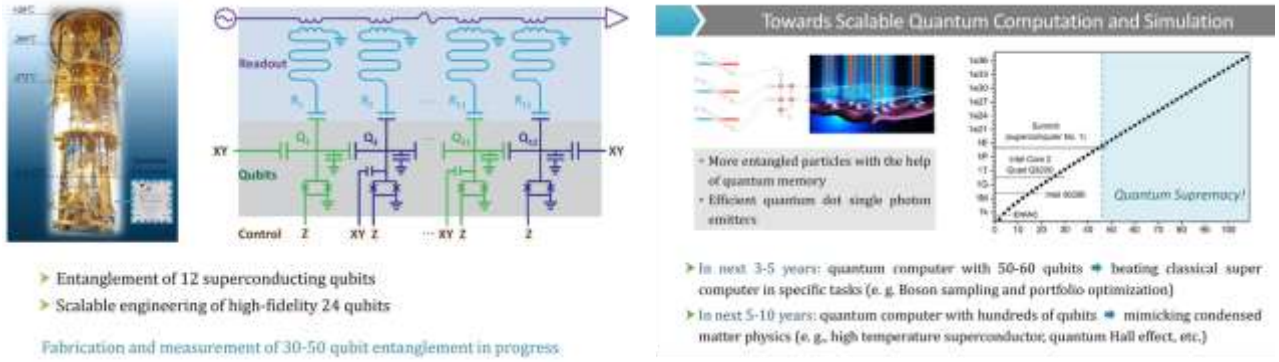
[1252] Voir Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership CNAS, 2018 (52 pages) et le plus récent Quantum information technology development in China par Yuao Chen, juin 2019 (25 slides).

[1253] La roadmap quantique datant de 2016 est disponible dans "Quantum Leap: The Strategic Implications of Quantum Technologies de Elsa Kania" et John Costello (part 1 and part 2). Voir aussi Chinese QC Funding de Xiaobo Zhu, 2017 (35 slides).

Le plan chinois est coordonné par l'**USTC** (University of Science and Technology of China) de l'Académie des Sciences Chinoises (CAS) et sous le leadership de Jian-Wei Pan,[1254]. Le projet le plus ambitieux est le centre de recherche à $10B ouvert en 2020, le **NLQIS (**National Laboratory for Quantum Information Sciences) d'Hefei,. Ce laboratoire est focalisé sur l'informatique et la métrologie quantiques, pour des applications militaires et civiles.

Côté calcul quantique, les laboratoires Chinois testent toutes les filières imaginables de qubits et annoncent régulièrement des prouesses technologiques. Ils semblent être plutôt en avance en qubits photons comme nous l'avons vu au sujet de l'échantillonnage du boson dans la rubrique des qubits photons mais pas vraiment dans les autres branches. Sachant que pour réaliser la prouesse de l'échantillonnage de bosons avec une source de photons uniques, ils n'hésitaient pas à copier la technologie de source de photons du français Quandela.

En 2017, le laboratoire d'Hefei annonçait la réalisation d'un système de test de 10 qubits supraconducteurs intriqués en aluminium et saphir[1255]. Le taux d'erreurs serait élevé, à 0,9% pour les portes à deux qubits. L'équipe de Jian-Wei Pan prévoit de créer un ordinateur quantique universel de 50 qubits supraconducteurs d'ici 2023 ! Et il pense qu'il faudra attendre 30 à 50 ans pour qu'un ordinateur quantique universel soit disponible.



En août 2018 était annoncée une prouesse avec deux qubits manipulant des photons, fabriqués en technologie silicium[1256]. La nouveauté résidait dans l'exploitation de portes quantiques opérant sur ces deux qubits.

Contrairement à la couverture presse qui s'enthousiasmait sur la question[1257], il faut raison garder. Il est difficile d'intriquer correctement ces qubits à grande échelle et leurs taux d'erreurs sont largement supérieurs à 1% alors qu'il faudrait être situé entre 0,001% et 0,1% pour que cela soit intéressant.

[1254] Voir The man turning China into a quantum superpower, de Martin Giles dans MIT Technology Review, décembre 2018.

[1255] Voir 10-qubit entanglement and parallel logic operations with a superconducting circuit par Chao Song et al, 2017 (16 pages).

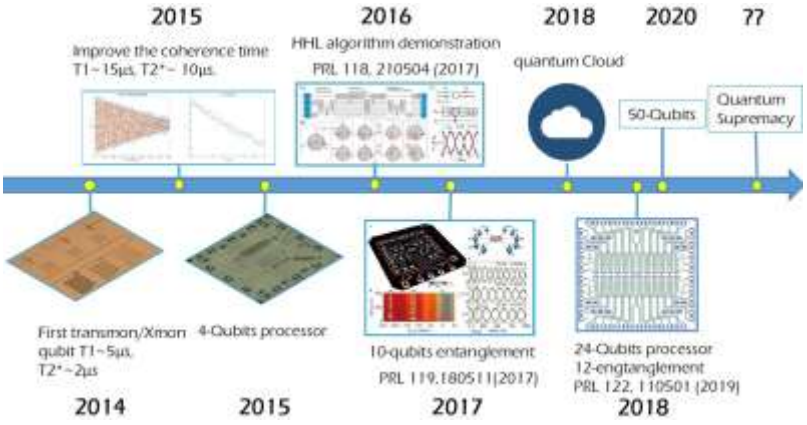
[1256] Voir Large-scale silicon quantum photonics implementing arbitrary two-qubit processing, août 2018 (7 pages).

[1257] Par exemple, dans Des chercheurs chinois sur la voie du processeur quantique 'ultime' ? Effectivement ça sent bon ! de Bruno Cormier dans Tom's Hardware.

Ce projet conduit par plusieurs laboratoires de recherche chinois a été mené en partenariat avec le laboratoire de photonique de Jeremy O'Brien à l'Université de Bristol et un laboratoire australien à Brisbane.

Des partenariats public-privé ont été établis comme celui d'**Alibaba** qui a investi 1 Md$ dans l'USTC de Jian-Wei Pan pour lancer en 2015 l'Alibaba Quantum Computing Laboratory à Shanghai, qui s'intéresse à la cryptographie quantique et au calcul quantique. La crypto quantique pourrait servir à sécuriser certaines transactions de commerce en ligne et de liaisons entre data centers. Alibaba lançait même en janvier 2018 la mise en ligne dans le cloud d'un ordinateur quantique de 11 qubits développé par l'USTC.

Cela faisait suite au lancement d'un simulateur quantique à base d'ordinateurs traditionnels de 22 qubits fin 2017. Cette offre de tests d'algorithmes quantiques dans le cloud est très similaire à celle que propose IBM depuis 2016.



Ils en étaient à 24 qubits supraconducteurs en 2019 avec le projet d'en supporter 50 en 2020. Leurs fidélité est de 99,9% sur les portes à un qubit et 99,5% sur des portes CZ à deux qubits ce qui est très correct[1258].

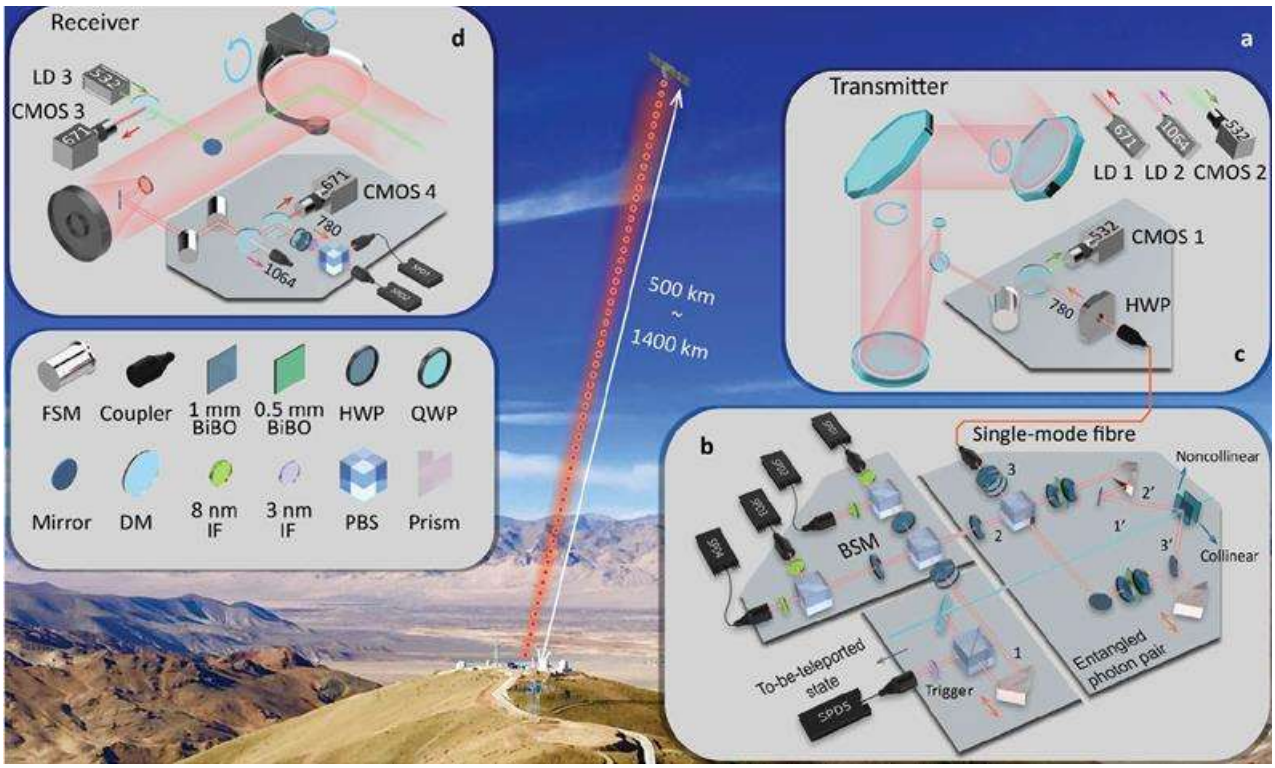
Leur durée T1, qui définit le temps de cohérence des qubits est de 40 µs, équivalent à ce qu'obtient IBM avec son Q System One à 20 qubits.

Dans l'ensemble, le niveau scientifique chinois est de bonne facture. Ils améliorent le plus souvent des technologies développées dans les pays occidentaux et ne sont pas à l'origine de nombreuses idées nouvelles. Par contre, leurs moyens illimités leur permettent de créer des expériences (boson sampling) ou déploiement (fibres en QKD) de grande ampleur.

La Chine ne semble pas avoir d'influence dans le monde académique sur la partie algorithmique et programmation. Aucun outil de développement ou framework de développement d'application quantique n'est proposé au monde par la Chine. Il ne faut jamais oublier le rôle stratégique du logiciel et des plateformes dans les batailles économiques du numérique ! J'ai l'impression que l'Histoire se répète en Chine de ce côté-là.

Par contre, la Chine est en avance du côté de la cryptographie quantique, au moins au niveau du livre des records. Cela commence avec une expérience record d'intrication de photons à longue distance menée mi 2017.

[1258] Source : Superconducting Quantum Computing par Xiaobo Zhu, juin 2019 (53 slides).



La téléportation d'un photon dupliqué était réalisée à 5100 m d'altitude à Ngari au Tibet vers le satellite Micius qui orbite à 500 km d'altitude, et à une distance maximale de 1400 km. Les photons émis provenaient d'un laser opérant dans l'ultraviolet.

Ce genre d'expérience avait déjà été faite sur Terre avec des distance allant jusqu'à 100 km correspondant à la longueur maximale d'une fibre optique sans répéteur[1259]. Elle permet notamment d'envoyer des clés quantiques protégées contre les interceptions.

L'expérience a été renouvelée début 2018 avec l'organisation d'une vidéoconférence entre la Chine et l'Autriche utilisant une clé quantique envoyée toutes les minutes[1260]. La Chine prévoit en fait de lancer d'ici 2030 une nuée de satellites en orbite basse dédiée à l'envoi de clés quantiques en reprenant ce processus. Enfin, une liaison en fibre optique protégée par clé quantique de 2000 km a été déployée entre Shanghaï et Beijing. En tout cas, on voit que la Chine prend très au sérieux cette histoire de sécurisation des communications.

S'ils mettent le paquet sur la QKD pour la gestion de clés symétriques, il semble qu'ils investissent aussi en cryptographie post-quantique mais de manière un peu plus discrète.

Du côté des entreprises, on peut citer l'implication de **ZTE** et de nombreux opérateurs et industriels des télécoms dans le déploiement de réseaux de fibres sécurisés par QKD (**China Telecom, China Cable, China Comservice, China Unicom**) ainsi que différentes banques qui y font appel.

Baidu s'est lancé en 2018 dans le calcul quantique avec son **Institute for Quantum Computing** qui est déployé dans leur Technology Park à Beijing avec une dizaine de personnes en septembre 2019. Il est dirigé par Runyao Duan, un spécialiste de la théorie de l'information quantique, avec Artur Ekert comme board member. Pour l'instant, ils travaillent sur les stacks logicielles, sans ambitionner de construire leur propre ordinateur quantique.

[1259] Voir la source du schéma et détails de l'expérience.

[1260] Voir Real-world intercontinental quantum communications enabled by the Micius satellite, USTC, janvier 2018.

Ils ont aussi une offre d'émulation quantique proposée dans leurs ressources en cloud[1261].

Tencent a également lancé en 2018 de son côté un Quantum Lab, dirigé par Shengyu Zhang et basé à Shenzhen. Ils envisagent de proposer des ressources de calcul quantique dans le cloud. Le laboratoire publie des travaux dans les algorithmes de simulation et de machine learning quantique.

Les startups chinoises ne sont pas très nombreuses à ce stade, l'une des raisons étant que les laboratoires de recherche publique sont bien financés et sont moins incités à créer des entreprises. On compte notamment **QuantumCTek** et **Qasky Science** qui sont spécialisées dans la cryptographie quantique. Les deux dernières ont rejoint avec le Suisse ID Quantique et l'Américain Battelle le **Quantum-Safe Security Working Group**, qui fédère l'industrie de la cryptographie quantique. La Chine met donc le paquet sur le quantique dans toutes ses dimensions, mais surtout dans la cryptographie quantique !

Taiwan est très en pointe dans les semiconducteurs avec TSMC, le leader de la fab CMOS et le seul avec Samsung qui est capable de descendre à un niveau d'intégration de 7 nm et bientôt 5 nm. Il est aussi toujours très présent dans le marché des composants pour PC.

C'est notamment le cas avec les cartes mères (MSI, Asus, Gigabyte) et la fabrication de PCs (Quanta, …). Il était logique dans ces conditions que le pays s'intéresse au calcul quantique. Il semble cependant ne pas avoir encore lancé de plan formel.

On peut identifier des initiatives dans la formation d'étudiants[1262] et avec une conférence organisée en septembre 2019[1263]. Ils ont une PME dénommée **Quantum Design** qui fournit des instruments de mesure mais n'a pas l'air d'exploiter des technologies de la seconde révolution quantique[1264].

Enfin, IBM a pris pieds dans le pays pour l'aider à adopter les technologies quantiques. Je traduis cela par « aider à utiliser l'offre d'IBM pour développer des logiciels quantiques ».

Début 2020, l'**Inde** lançait à son tour un plan d'investissement dans les technologies quantiques, le NMQTA (National Mission on Quantum Technologies & Applications). Ce plan est bien financé en proportion du PIB du pays, à hauteur de $1,12B étalés sur 5 ans, au même niveau que le Quantum Initiative Act américain de 2018 ou du Flagship Européen lancé la même année[1265]. Comme dans tous les pays, le plan couvre le calcul quantique, les télécommunications quantiques et la métrologie quantique.

[1261] Voir Introduction to Baidu Quantum Program par Shuming Cheng, juin 2019 (9 slides). Ils proposent notamment la bibliothèque Paddle Quantum, diffusée sur GitHub, qui supporte de la QML de réseaux de neurones, de la chimie quantique et des outils d'optimisation. Le tout en émulation quantique sur data-centers classiques.

[1262] Voir Quantum tech summer program in Taiwan a success par Taiwan News, juillet 2019.

[1263] Voir Quantum Computer: Envision the New Era of Computing, une conférence en septembre 2019.

[1264] Voir Quantum Design Taiwan.

[1265] Voir India finally commits to quantum computing, promises $1.12B investment par Ivan Mehta, février 2020.

Ironiquement, les CEO d'IBM, Google et Microsoft sont tous… indiens (Arvind Krishna, Sundar Pichai et Satya Nadella) !

Quelles stratégies industrielles ?

Le marché potentiel de l'informatique quantique est et restera probablement assez longtemps un marché de niche. Les prévisions des analystes qui sont d'habitude tout feu tout flamme sur les marchés émergents comme sur l'Internet des objets sont assez prudents, et à juste titre, sur la taille de ce marché. Il serait de $553M en 2023 selon MarketsandMarkets, une prévision datant d'aout 2017.

Il serait de $1,9B en 2023 selon CIR et de $2,64B en 2022 selon Market Research Future, une prévision datant de 2018. Homeland Security Research voit plus large avec $8,45B en 2024 (en 2018), intégrant produits et services, auxquels s'additionneraient $2,24B de financements publics.

Une étude de Morgan Stanley de 2017 évalue la taille du marché de l'informatique quantique à plus de $10B en 2028 tout en la comparant au marché de l'informatique grand public ($590B, en y intégrant les PC, les smartphones et les tablettes) et d'entreprise ($185B). Les marchés visés mis en avant sont souvent celui des transports, de la défense et de la lutte contre le cybercriminalité. Ces prévisions intègrent parfois le marché de la cryptographie quantique. Par comparaison, le marché des supercalculateurs était situé aux alentours de $5B à $6B en 2017. En juillet 2018, ABI Research évaluait pour sa part le marché du quantique à $15B d'ici 2028.

Le marché de l'informatique quantique est en fait bien moins mature et prêt à être lancé que celui de la cryptographie quantique. L'ordinateur quantique est incertain et assez éloigné dans le temps. Cela explique l'investissement de presque tous les pays en parallèle dans l'informatique quantique, la cryptographie quantique et la métrologie quantique, cette dernière ayant un marché cible très professionnel et limité.

Les Etats sont motivés à investir sur le quantique pour des raisons stratégiques : à la fois dans l'idée de pouvoir décrypter les télécommunications existantes ou passées dans le cadre de l'activité de leurs services de renseignement (Direction Technique de la DGSE en France, NSA aux USA, GCHQ au Royaume-Uni…) et de protéger les leurs via de la cryptographie quantique ou post-quantique. Le quantique est donc, plus que presque toute autre technologie numérique, un outil de souveraineté stratégique des états[1266].

Les partenariats dans l'informatique quantique sont de nature différente : entre laboratoires de recherche intra-pays (comme dans l'initiative Quantum Silicon Grenoble), inter-pays (comme le CEA-Leti et USNW, ou les Chinois avec les Australiens et les Britanniques), puis entre la recherche publique et le privé au sein du même pays (CEA et Atos) ou entre pays différents (Intel avec Qutech). La raison d'être de tous ces partenariats est identifiable : l'informatique quantique est un sujet scientifique complexe qui ne peut pas être maitrisé par un seul laboratoire ou une seule entreprise. La collaboration est nécessaire pour rassembler des talents de spécialités différentes, entre la physique de la matière condensée, les technologies de capteurs et de contrôle, l'optronique, la cryogénie, la production de semiconducteurs, l'algorithmie et le développement logiciel.

Au-delà de cet aspect stratégique se posent des questions sur la vitesse à laquelle le secteur privé pourrait et devrait prendre le relai de la recherche fondamentale publique. C'est un enjeu technologique au long cours qui relève d'un risque presque aussi grand que le risque et l'incertitude scientifique. Quel serait le meilleur timing de l'investissement privé et la capacité de le faire avec une incertitude technologique très forte ? Il existe quelques "best practices" comme ID Quantique, lancé en Suisse par le chercheur Nicolas Gisin.

[1266] Voir la tribune Europe : des clés pour la souveraineté par Thierry Breton, août 2020. Il y cite trois piliers de cette souveraineté : la puissance de calcul, la maîtrise des données et la connectivité sécurisée. Les technologies quantiques ont un rôle clé à jouer dans le premier et le troisième ! Les moyens cités d'obtenir cette souveraineté sont cependant classiques et portent sur le financement public de la R&D. On sait que c'est clairement insuffisant.

Malgré la belle dynamique autour des deep techs que l'on sent en Europe et en France, ce type de financement semble pour l'instant accessible uniquement en Amérique du Nord. Il nous faut inventer des modèles entrepreneuriaux et de financement permettant de conduire des aventures au long cours dans le secteur privé, à l'image de la longue histoire de D-Wave.

Comme d'habitude, nombre de pays se demandent comment encourager la création de startups par des chercheurs ou l'exploitation de leurs travaux par des entrepreneurs qui ne sont pas des chercheurs. A part Atos qui s'est déjà engagé sur le quantique, quelles autres entreprises établies et orientée "produits" pourraient se lancer sur le quantique ? On pense au complexe militaro-industriel avec des entreprises comme Thalès. Le quantique est peut-être le seul endroit où un "CloudWatt" aurait eu du sens avec un financement public/privé, voir même une approche transnationale européenne.

La situation actuelle met en lumière une autre déficience française : l'absence d'un office scientifique rattaché à l'exécutif comme il en existe aux USA ou en Israël. Lorsque l'exécutif a besoin de lumières pour comprendre les enjeux scientifiques du moment, vers qui se tourne-t-il ? Comme on l'a vu sur l'intelligence artificielle, il doit lui-même jouer le rôle d'intégrateur et enquêter auprès de centaines de personnalités et organisations représentatives.

C'est long, séquentiel, souvent biaisé et réalisé de manière ponctuelle alors que cela devrait être une tâche permanente et centralisée quelque part et piloté par une personnalité reconnue par la communauté scientifique. Ce n'est cependant pas le rôle d'une Académie comme celle des sciences ou celle des technologies.

Ainsi, aux USA, l'Académie des Sciences est une organisation privée distincte de l'Office Scientifique et Technologique du Président (OSTP) établi par le Congrès en 1976. L'OSTP s'appuie sur le National Science and Technology Council, créé sous la Présidence Clinton en 1993.

Enfin, nous avons aussi l'opportunité de créer un écosystème logiciel avec des outils de modélisation, de développement et des applicatifs métiers. La cartographie des acteurs privés de l'informatique quantique que j'ai compilée à partir de sources diverses est encore éparse. Une industrie nouvelle va probablement émerger de l'informatique quantique, même si elle sera plus modeste en taille que le marché de l'informatique d'entreprise actuel. L'un des enjeux clés me semble être celui de la création d'applications "grand public" du quantique.

A savoir, des applications qui pourraient générer des économies d'échelle et permettre à ce marché de dépasser le cadre d'un marché étroit dédié à la recherche et à quelques applications b2b.

Nous avons aussi besoin de mathématiciens et d'une nouvelle génération de développeurs qui vont devoir tout apprendre ou réapprendre pour créer et utiliser des algorithmes quantiques.

Il faudra se bouger si l'on veut éviter de se voir une fois de plus dominés par des acteurs américains, canadiens si ce n'est chinois. Le syndrome de la dominance des GAFA peut se reproduire facilement dans le quantique si l'on n'y prend gare. Si la France annonçait la couleur sur le sujet, il vaudrait mieux que cela se fasse très rapidement. Pas dans 5 ans avec un "plan de rattrapage" comme l'est le Rapport Villani pour ce qui est de l'intelligence artificielle.

Technologies quantiques en France

Dans le benchmark mondial, la France se distingue d'une manière encore plus radicale que dans l'intelligence artificielle. Nous avons une recherche de qualité mais pas encore assez de transformation de sa production en initiatives entrepreneuriales même si nous avons vu que le nombre de startups quantiques en France était déjà respectable.

Les stars françaises de la physique quantique sont Alain Aspect et Serge Haroche, le premier ayant invalidé les inégalités de Bell en 1982 et vérifié le principe de non localité de quantum intriqués, un élément clé servant notamment à la cryptographie quantique. Prix Nobel de physiques en 2012, Serge Haroche est pionnier de l'électrodynamique quantique en cavité et sur l'interaction entre les photons d'une cavité supraconductrice et des atomes de Rydberg qui traversent la cavité[1267]. Ancien thésard d'Alain Aspect, Philipe Grangier est un spécialiste mondial de la cryptographie quantique. Comme d'habitude, les cerveaux brillants ne manquent pas.

Michel Devoret est en quelque sorte le "Yann LeCun" du quantique, à savoir qu'il travaille maintenant à l'Université de Yale aux USA (vs l'Université de New York) et dans la startup qu'il a cofondée aux USA puis quittée en 2019, QCI. Mais nuance, il n'est pas (encore) dans un GAFA !

Nombre de laboratoires de recherche planchent sur les différentes briques du quantique, que ce soit au CEA à Saclay (supraconducteurs) et à Grenoble (CMOS), au CNRS ou à l'Inria, au Laboratoire Circuits Quantiques Hybrides de l'ENS Ulm, dans le Quantum Circuit Group de l'ENS Lyon et dans plein de régions, notamment à Toulouse, Montpellier, Bordeaux (LaBRI), Nancy et Grenoble, en plus de l'Ile de France.

[1267] Voir ses cours de physique quantique au Collège de France entre 2001 et 2015. En photonique, sur le contrôle d'atomes froids, sur les questions de décohérence, etc.

Du côté des entreprises, nous avons quelques acteurs des couches basses physiques **CryoConcept** et **MyCryoFirm** et leurs systèmes de cryogénie, **Quandela** avec ses sources de photons uniques utilisables dans des ordinateurs quantiques à base de photons ou dans les télécommunications et la cryptographie quantiques et **Pasqal** et son projet de simulateur analogique. La startup **Prevision.io** est de son côté en train d'évaluer l'intérêt des algorithmes quantiques à intégrer dans sa boîte à outils d'algorithmes de machine learning.

Seul **Atos** sort du lot. Leur stratégie lancée en 2016 consiste à se préparer à devenir un intégrateur d'accélérateurs quantiques en prenant le problème "par le haut", par le logiciel, avec une focalisation sur les applications b2b et industrielles du quantique et enfin, en privilégiant le calcul hybride, qui associe le calcul sur des supercalculateurs et sur calculateurs quantiques. Ils développent des compétences dans les algorithmes et la programmation de calculateurs quantiques, notamment avec le langage aQASM qui peut fonctionner sur tout ordinateur quantique présent ou futur. A terme, on peut espérer qu'ils prendront une part dans les offres de calcul quantique en cloud qui pourraient bien dominer le marché.

Cela semble avoir porté ses fruits avec la création d'une mission d'étude parlementaire commanditée officiellement par le Premier Ministre en mars/avril 2019 et confiée à la députée LREM **Paula Forteza**[1268] qui était déjà très engagée autour des sujets numériques. Elle y était accompagnée par **Iordanis Kerenidis** (chercheur au CNRS, spécialisé dans le quantum machine learning, et chez QCWare) et **Jean-Paul Herteman** (ancien PDG de Safran). J'ai été auditionné en avril 2019 pour évoquer les questions relatives à l'écosystème du quantique et aux enjeux stratégiques du secteur.

La mission parlementaire terminait ses auditions en juin 2019 et remettait son rapport le 9 janvier 2020 à l'Assemblée Nationale. Le gouvernement concoctait ensuite un plan quantique national reprenant tout ou partie des propositions de la mission parlementaire. Le covid et la lenteur du remaniement ministériel de juin/juillet 2020 lui ont fait prendre du retard. Il devait être annoncé avant la fin 2020.

Recherche

De nombreux laboratoires de recherche français sont actifs dans les différentes branches du quantique, principalement autour du CEA, du CNRS et de l'Inria. Une bonne part de ces laboratoires de recherche sont des UMR, Unités Mixtes de Recherche, qui associent le CNRS et des laboratoires d'Universités, grandes écoles ou d'un autre organisme national de recherche. Ces laboratoires quantiques sont fédérés par le **GDR IQFA**[1269] fondé par Jean-Philippe Poizat dans les années 2000 puis repris depuis 2010 par Sébastien Tanzilli de l'InPhyNi (Nice). Il est complété par le **GDR MecaQ** qui fédère la recherche en métrologie quantique.

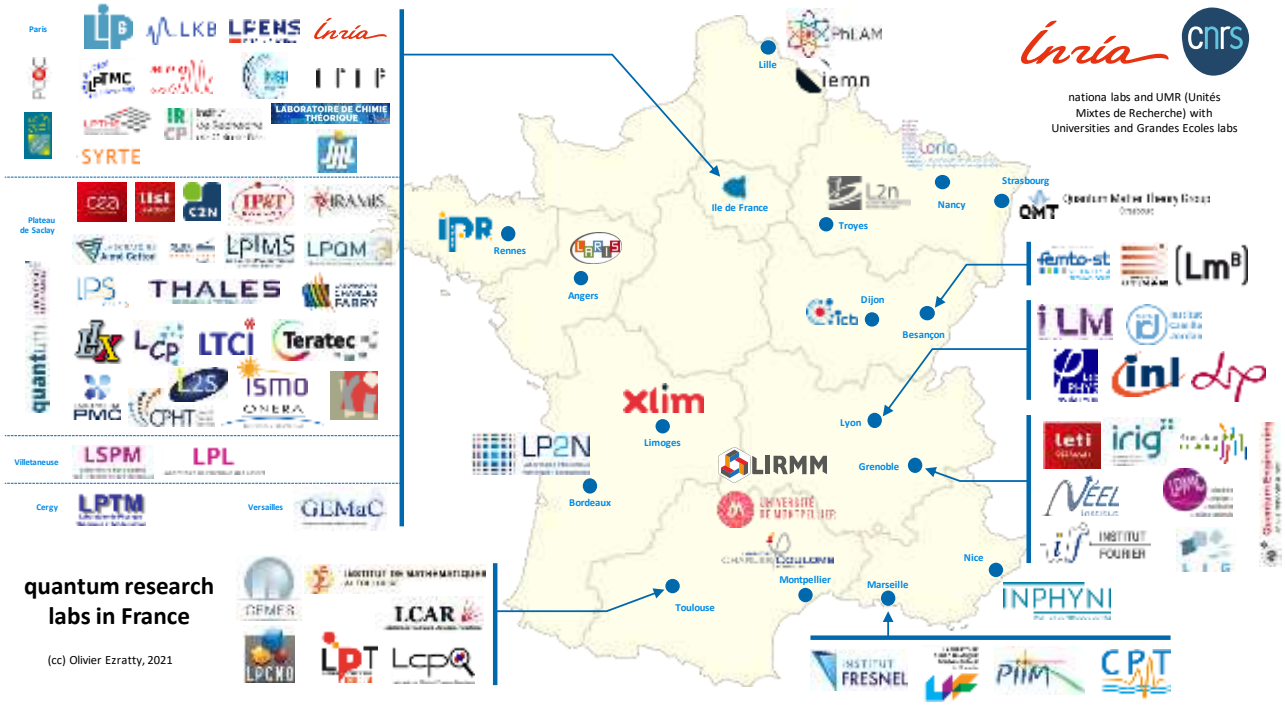
Les deux plus grands pôles de recherche sont en Ile de France et à Grenoble, mais d'autres métropoles sont actives comme Toulouse, Montpellier, Marseille, Besançon et Lille. Et encore, cet inventaire est probablement incomplet. Il comprend les laboratoires de recherche publics qui travaillent de près ou de loin sur le quantique en consolidant diverses listes et cartographies du secteur[1270].

[1268] Voir le communiqué de Paula Forteza : Technologies quantiques : un tournant numérique majeur à ne pas manquer pour la France ?, 10 avril 2019.

[1269] Un GDR est un Groupement de Recherche qui coordonne la recherche nationale dans un domaine scientifique donné. Son rôle est surtout d'animer la communauté des chercheurs du domaine, notamment via des colloques, mais aussi de coordonner les axes de recherche. Voir Les Groupements de Recherche, novembre 2018.

[1270] J'ai pour cela consulté les sites web de ces laboratoires et les domaines de recherche qu'ils y présentent, plus, lorsqu'elles étaient faciles à trouver, les publications scientifiques des chercheurs de ces laboratoires.

Ces laboratoires changent parfois de nom ou se regroupent. Il est donc possible qu'une partie de cet inventaire soit caduque. La majorité de ces laboratoires opèrent dans le champ de la physique fondamentale avec de nombreuses redondances apparentes et très peu sont engagés dans la recherche pratique sur la création de qubits.



Mais ces recherches fondamentales peuvent à terme y servir. Je les cite dès lors qu'ils font de la recherche fondamentale dans la physique quantique qui pourrait avoir un intérêt de près ou de loin avec le calcul ou les télécommunications quantiques. Les laboratoires français explorent en parallèle de nombreuses pistes de qubits : les supraconducteurs, la photonique, les atomes froids, les spins d'électrons et même les ions piégés et les fermions de Majorana. J'ai par contre trouvé très peu de laboratoires directement impliqués dans la recherche en algorithmie quantique parmi les dizaines de laboratoires spécialisés en mathématiques.

Avec les restrictions budgétaires endémiques du secteur, les chercheurs du secteur public ont appris à se financer en soumettant et défendant leurs projets pour obtenir des financements publics et privés[1271]. L'étape suivante, franchie par certains, consiste à passer à la création de startups avec ses codes et coutumes. Statutairement et d'un point de vue pratique, elle est plus encouragée au CEA et à l'Inria qu'elle ne l'est au CNRS. Mais nombre de startups sont tout de même issues du CNRS ou d'UMR du CNRS dans les technologies quantiques, comme Quandela ou Pasqal. Sur les 19 startups du quantique en France en mars 2020, 7 sont issues du CNRS, deux d'Inria, deux des ENS et une du CEA. Et dans l'édition 2020 du **concours iLab** du Ministère de la Recherche, trois chercheurs/entrepreneurs du quantique faisaient partie des dix grands Prix : Théo Peronnin (Alice&Bob), Ludovic Perret (CryptoNext) et Georges Reymond (Pasqal).

Si l'on évalue la recherche française quantique de manière traditionnelle avec ses publications scientifiques et ses brevets, le pays se positionne habituellement entre la 8e et la 10e position mondiale, les premiers étant les USA, la Chine et le Canada. C'est un classement que l'on retrouve dans de nombreuses disciplines scientifiques.

[1271] Certains obtiennent des ERC Grants (European Research Council) : les Synergy Grants pour quelques poignées d'équipes (jusqu'à 14M€ su 6 ans), et plus souvent des Starting (jeunes chercheurs, jusqu'à 1,5M€), Consolidators (chercheurs expérimentés, jusqu'à 2M€) et des Advanced (chercheurs émérites, jusqu'à 2,5M€ étalés sur 5 ans). Puis des financements FET Européens, des financements via le Flagship Européen quantique, ou enfin par des appels à projets divers à l'échelon national (ANR).

Le monde de la recherche publique recèle quelques différences de générations. En moyenne, certains anciens comme Serge Haroche sont plutôt sceptiques et prudents sur le calcul quantique tandis que les jeunes chercheurs sont plus optimistes et à l'affût de nouvelles approches. D'autres comme Alain Aspect font le pont entre les deux.

Certains comme ce dernier ou Julien Bobroff, Philippe Chomaz[1272] et Etienne Klein s'investissent à fond dans la vulgarisation destinée à un public aussi large que possible, un point de passage obligé pour se faire connaître et faire rayonner la discipline. Le CEA s'y est même mis en créant un jeu pédagogique, le Prisonnier Quantique[1273].

Ile de France

L'Ile de France concentre une bonne moitié des laboratoires de recherche du pays consacrés au quantique aussi bien côté création de qubits que dans le domaine des algorithmes, et des télécommunications et de la cryptographie quantique et post-quantique.

Commençons par les laboratoires qui sont situés dans Paris intra-muros.

Les efforts de l'**Inria** en région parisienne sont concentrés dans l'équipe Quantic (Quantum Information Circuits) de Pierre Rouchon, Mazyar Mirrahimi, Zaki Leghtas et Alain Sarlette qui est conjointe entre le CNRS, l'ENS et l'école des Mines de Paris.

Elle travaille sur les modèles mathématiques des qubits supraconducteurs, sur des codes de correction d'erreur, sur la preuve de la supériorité d'algorithmes quantiques ainsi que sur les questions de cryptographie[1274]. Il faut y ajouter l'équipe Secret, devenue Cosmiq en 2020, basée à Paris et dirigée par Anne Canteaut, qui travaille sur les algorithmes de cryptographie ainsi que l'équipe Cascade de David Pointcheval qui travaille dans la cryptographie et donc la PQC.

Le **LIP6** (Laboratoire d'Informatique de la Sorbonne) est situé à Jussieu. On y trouve plusieurs spécialistes reconnus de la cryptographie et des télécommunications quantiques (QKD) : Eleni Diamanti et Elham Kashefi. Eleni a obtenu un ERC Synergy Grand européen pour ses travaux dans le projet QUSCO (Quantum Superiority with Coherent State). Elham Kashefi est cofondatrice de la startup Veriqloud. Ils travaillent aussi sur le calcul quantique vérifié, sur le calcul quantique multipartite sécurisé et sur les caractéristiques qui permettent d'obtenir des avantages quantiques.

Le **LPENS** (Laboratoire de Physique de l'Ecole Normale Supérieure) résulte de la fusion début 2019 de plusieurs laboratoires de recherche en physique de l'ENS Paris, dont le **LPA** (Laboratoire Pierre Aigrain) qui est spécialisé en nanotechnologies et en photonique.

Ils planchent sur de nombreuses nanotechnologies servant à la création de qubits et au tranport d'informations quantiques : films minces supraconducteurs, circuits supraconducteurs et micro-ondes pour leur contrôle, gaz bidimensionnels d'électrons de très haute mobilité, boîtes quantiques semiconductrices, qubits à base de nanotubes de carbone. L'équipe de Taki Kontos est à l'origine de la création de nanotubes de carbone servant de pièges à électrons potentiellement utilisables dans des qubits à spin d'électron, ce qui a mené à la création de la startup C12, déjà citée.

[1272] Voir la vidéo du TEDx Versailles Grand Parc de Philippe Chomaz en 2019.

[1273] Voir Le CEA présente Le Prisonnier quantique, un jeu vidéo inédit d'aventure au cœur des sciences et des technologies, juin 2019. Je jeu doit être publié à l'automne 2019 lors de la fête de la science.

[1274] C'est précisé dans leur plan stratégique scientifique 2018-2022, 2018 (93 pages), pages 47 et 48.

Leurs travaux dans les qubits supraconducteurs visent à les protéger contre les erreurs avec un plus faible nombre de qubits physiques intégrables dans un qubit logique en 1D au lieu d'être en 2D comme avec les surface codes classiques. Les codes de correction d'erreurs Cat-Qubit fonctionneraient avec seulement 9 qubits physiques et apporteraient un gain exponentiel dans la suppression des erreurs. Ils permettent aussi de se passer de la "magic state distillation", une technique complexe de codes de correction d'erreurs.

Ces travaux sont pilotés par une équipe mixte associant l'ENS, Inria (l'incontournable Mazyar Mirrahimi) et l'Ecole des Mines de Paris[1275]. C'est la base du procédé de la startup Alice&Bob qui en résulte et a été lancée début 2020.

Le **LKB** (Laboratoire Kastler Brossel) est un autre laboratoire de l'ENS Paris où travaille notamment le prix Nobel Serge Haroche. Ils sont focalisés sur l'information et l'optique quantique, les interactions entre matière et lumière, la simulation quantique et de la métrologie de précision avec des atomes de Rydberg (du rubidium) piégés magnétiquement dans des cavités optiques et excités par laser, qui est à l'origine de la startup Pasqal.

Thibault Jacqmin y travaille sur la génération de photons micro-ondes avec des NEMS. Traduction : NEMS = MEMS mais au lieu de l'échelle micro, c'est de l'échelle nanoscopique. Ce sont des dispositifs nano-mécaniques tels que ceux que l'on trouve dans les nombreux capteurs qui équipent nos smartphones. Pourquoi générer des micro-ondes de cette manière ? C'est probablement pour permettre le contrôle de qubits de types divers, notamment supraconducteurs, avec des dispositifs miniaturisés. On y trouve aussi Christophe Salomon, qui est notamment spécialisé dans les atomes froids et la mesure du temps ainsi que Nicolas Treps et Valentina Parigi, spécialisés en photonique.

L'Ecole Normale Supérieur héberge aussi un **Laboratoire de Physique** (LPENS) qui planche sur de la physique quantique fondamentale et notamment sur la matière quantique topologique (Erwann Bocquillon) ainsi que sur les qubits supraconducteurs (Takis Kontos et Zaki Leghtas) et la photonique (Gwendal Fève).

L'IRIF (Institut de Recherche en Informatique Fondamentale) est une UMR associant le CNRS et l'Université Paris Diderot.

Elle héberge notamment deux équipes de l'Inria. Au CNRS, l'IRIF est rattaché à l'INS2I (Institut National des Sciences de l'Information et de leurs Interactions) et à l'INSMI (Institut National des Sciences Mathématiques et de leurs Interactions). Le laboratoire travaille dans le calcul quantique, la cryptographie et les communications. On y trouve l'équipe de Iordanis Kerenidis qui travaille notamment sur les algorithmes quantiques, en particulier dans le machine learning.

Le laboratoire **MPQ** (Matériaux et Physique Quantique) de l'Université Paris Diderot s'intéresse notamment à la technique des ions piégés dans les groupes Quantum Physics and Devices (QUAD) et QITE (Quantum Information and Technologies). Mais aussi à la génération de paires de photons intriquées (Sara Ducci).

Le **LPTHE** (Laboratoire de Physique Théorique et Hautes Energies) de l'Université Paris Sorbonne travaille dans la matière condensée et la physique statistique avec des applications dans les qubits supraconducteurs.

[1275] Voir à ce sujet Repetition cat-qubits: fault-tolerant quantum computation with highly reduced overhead, de Jérémie Guillaud et Mazyar Mirrahimi, avril 2019 (22 pages).

L'**INSP** (Institut des Nanosciences de Paris) de l'Université Paris-Sorbonne est un laboratoire généraliste sur les nanosciences. Ils travaillent notamment dans différentes branches de la photonique, sur les NV centers de diamants, sur le spin et le magnétisme et sur le développement de composants de photonique en matériaux semi-conducteurs de type III-V.

L'**IRCP** (Institut de Recherche de Chimie Paris) associé à l'Ecole Nationale Supérieure de Chimie ParisTech fait de la recherche dans les matériaux innovants.

Au sein de l'école, Philippe Goldner travaille sur la création de qubits à base de nano-cristaux dopés par ions de terres rares comme l'europium ou l'erbium, et est impliqué dans le projet SQUARE du Quantum Flagship européen, coordonné par le Karlsruhe Institute of Technology et impliquant aussi Thales. Le laboratoire est aussi impliqué dans le projet ASTERIQS qui planche sur les qubits à base de NV centers dans les diamants.

Le **LPEM** (Laboratoire de Physique et d'Etude des Matériaux) de l'ESPCI et de l'UMPC travaille notamment dans la supraconductivité ainsi que sur les fermions de Majorana.

Le **LPTMC** (Laboratoire de Physique Théorique de la Matière Condensée) de l'Université Paris-Sorbonne (Jussieu) n'a pas l'air d'être impliqué dans la physique quantique en relation avec l'informatique quantique. Néanmoins, ils s'intéressent à la simulation du vivant, qui est une des applications clés, à long terme, du calcul quantique.

SYRTE (Laboratoire Systèmes de Référence Temps-Espace) situé à l'Observatoire de Paris travaille dans le domaine de la métrologie quantique, notamment la gravitométrie, les gyroscopes quantiques et sur la mesure du temps dans des horloges atomiques et optiques. Ils sont partenaires du NIST aux USA.

Le **Laboratoire Jacques Louis Lions** (LJLL) est une UMR spécialisée en mathématiques appliquées de l'UPMC, de l'Université Paris Diderot et du CNRS. Il planche sur l'analyse, la modélisation et le calcul scientifique haute performance de phénomènes représentés par des équations aux dérivées partielles. On y trouve notamment Mario Sigalotti et Ugo Boscain qui sont notamment spécialisés dans le contrôle de systèmes quantiques et font aussi partie d'Inria.

Le **Laboratoire de Chimie Théorique** de Sorbonne Université est dirigé par Jean-Philip Piquemal (cofondateur de Qubit Pharma) et s'intéresse à la chimie computationnelle, y compris quantique.

Notons qu'en septembre 2020 était inauguré le **Quantum Innovation Center Sorbonne** (QICS), une structure de recherche collaborative associant le LIP6, le LKB de l'ENS et Inria.

Le **plateau de Saclay** comprend une densité de laboratoires encore plus forte que dans Paris intra-muros. Ils sont situés aussi bien du côté Ouest de la N118 avec l'Université d'Orsay et ses nombreux laboratoires, le CEA de Saclay, l'école d'ingénieurs CentraleSupelec et l'ENS ex-Cachan, puis du côté Est avec l'Ecole Polytechnique et ses écoles d'application, en particulier l'Institut d'Optique ainsi que le CEA List.

Au **CEA**, l'équipe Quantronics de Daniel Estève dans le laboratoire Iramis de Saclay planche depuis près de 20 ans sur les qubits supraconducteurs. Le laboratoire de Daniel Estève comprend une quinzaine de personnes.

Son homologue à l'Université de Yale aux USA en comprend une trentaine. Selon lui, il ne suffit pas d'aligner en parallèle plus de chercheurs pour accélérer la recherche dans ce domaine !

Christian Gamrat fait de son côté partie du CEA List dans la branche CEA Tech et planche sur les outils de développement et algorithmes quantiques.

L'**IphT** (Institut de Physique Théorique de Saclay) associe le CEA et le CNRS. Ils planchent sur la physique de la matière condensée, dont les supraconducteurs à haute température, et sur les fermions de Majorana. Mais leur principal centre d'intérêt a l'air d'être surtout l'astrophysique.

Le **LAC** (Laboratoire Aimé Cotton) de l'Université Paris-Sud (Orsay) est situé à l'ENS Cachan. Il travaille aussi sur les atomes froids et les interactions entre atomes et lumière.

Ils créent notamment des qubits en combinant un ion optiquement actif d'erbium et un spin nucléaire d'yttrium.

Le **C2N** (Centre des Nanosciences et des Nanotechnologies) de l'Université Paris-Sud est un autre laboratoire de photonique quantique. On y trouve notamment Jacqueline Bloch et Pascale Senellart, toutes deux médailles d'argent du CNRS, cette dernière étant à l'origine de la startup Quandela. Ils travaillent notamment sur le couplage lumière-matière dans les semiconducteurs. On y trouve aussi notamment des équipes en électronique quantique (Frédéric Pierre).

Le **LPS** (Laboratoire de Physique des Solides) de l'Université Parisud travaille sur le magnétisme, les supraconducteurs à jonctions Josephson, la thermodynamique, la spintronique supraconductrice et la dynamique quantique. Ils développent aussi des codes de dynamique quantique et semi-classique et de contrôle quantique avec des applications en information quantique.

Le **LPTMS** (Laboratoire de Phyique Théorique et de Modèles Statistiques) de l'Université Parisud a plusieurs cordes à son arc dans la physique quantique sans que le lien avec le calcul quantique soit immédiatement décelable.

Le **LCP** (Laboratoire de Chimie Parisud) travaille les supraconducteurs et sur la dynamique et contrôle d'ions piégés par impulsions laser. Ils développent des modèles de calcul hybrides de chimie quantique (quantiques+traditionnels) mettant en œuvre la MCTDH (Multi-configuration time-dependent Hartree) qui permet de résoudre l'équation de Schrödinger pour la simulation d'interactions entre atomes dans des molécules.

Au programme : physique de la matière condensée, modélisation de systèmes classiques et quantiques via la physique statistique, chaos quantique, théorie des nombres et chaos quantique, aspects théoriques de l'information quantique; atomes froids, systèmes intégrables quantiques, groupes quantiques, etc.

Le **LTCI** (Laboratoire Traitement et Communication de l'Information) de TelecomParistech est un laboratoire industriel fonctionnant avec des partenariats avec le privé et via des chaires. Son équipe « Information Quantique et Applications » (IQA) est spécialisée dans les aspects théoriques et expérimentaux des communications quantiques.

Ils développent des protocoles de cryptographie quantique hybrides à base de CV-QKD compatibles avec les réseaux de fibres des opérateurs télécoms ainsi que des répéteurs de QKD. Ils sont contributeur, membre fondateur et rapporteur à l'ETSI QKD-ISG sur le processeur de standardisation de QKD. L'équipe est pilotée par Isabelle Zaquine et on y trouve notamment Romain Alléaume.

L'**ISMO** (Institut des Sciences Moléculaires d'Orsay) est de l'Université Parisud travaille sur la dynamique quantique, les interactions entre particules lourdes et électrons à basse température, le couplage lumière/matière et sur les logiciels de simulation de la physique quantique.

Le **CPht** (Centre de Physique Théorique de Polytechnique) est spécialisé entre autres choses dans la physique de la matière condensée. Mais pas au point de créer des qubits supraconducteurs ! On y trouve notamment le groupe de Karyn Le Hur qui est spécialisée dans la physique de la matière condensée.

Le **Laboratoire Charles Fabry** de l'Institut d'Optique est spécialisé dans les lasers et l'optique quantique. On y trouve Alain Aspect (bien qu'il ait dépassé l'âge de la retraite), Philippe Grangier (notamment spécialisé dans la CV-QKD) ainsi qu'Antoine Browaeys, cofondateur de la startup Pasqal et ses qubits à atomes froids contrôlés par lasers.

Le **LIX** (Laboratoire d'Informatique de l'Ecole Polytechnique) est notamment actif dans les algorithmes de cryptographie post-quantique.

Le **PMC** (Laboratoire de Physique de la Matière Condensée) est un autre laboratoire de l'école Polytechnique. Ils travaillent notamment sur la dynamique de spin dans les semi-conducteurs et les couches minces magnétiques.

Le **L2S** (Laboratoire Signaux et Systèmes) de CentraleSupelec est actif dans la recherche en systèmes quantiques. On y trouve notamment l'enseignant-chercheur Zeno Toffano qui s'intéresse en particulier à la mesure des états quantiques et aux valeurs propres (eigenvalues).

Le **LPQM** (Laboratoire de Photonique Quantique et Moléculaire) associe l'ENS Paris Saclay et l'école CentraleSupelec. Leurs domaines sont la cohérence et les corrélations quantiques.

Le **LRI** (Laboratoire de Recherche en Informatique) situé à CentraleSupélec est géré par Benoît Valiron qui y fait de l'enseignement et de la recherche en calcul quantique, un domaine encore assez peu enseigné dans les grandes écoles d'ingénieurs.

Thales RT (Thales Research and Technology) fait de la R&D pour créer des solutions de métrologie quantique industrialisées. Ils ont notamment développé une expertise dans les NV centers de diamants.

L'**Onera** étudie l'optique quantique sur son site de Palaiseau. C'est à ce titre qu'il coordonne le projet ASTERIQS du Flagship Quantique Européen, "Advancing Science and Technology through diamond Quantum Sensing".

Ils ont aussi des équipes de chercheurs en photonique, dans les matériaux semi-conducteurs dits III-V (gallium, …) avec une unité de fabrication de prototypes située dans leurs locaux à Palaiseau, dans la métrologie (gravimètre, horloge atomique, accéléromètre) et dans la QKD.

Passons à d'autres parties de l'Ile de France : Cergy-Pontoise, Villetaneuse et Versailles.

Le **LPTM** (Laboratoire de Physique Théorique et Modélisation) de l'Université de Cergy-Pontoise s'intéresse aux atomes froids, en liaison avec l'Institut Francilien de Recherche sur les Atomes Froids (IFRAF).

Ils étudient aussi le graphène, le transport quantique électronique, les phases topologiques et l'intrication.

Le **LSPM** (Laboratoire des Sciences des Procédés et des Matériaux) de l'Université Paris 13 à Villetaneuse travaille sur les procédés de fabrication de NV centers de diamants, de nanotubes de carbone et de graphène et sur les applications associées.

Le **LPL** (Laboratoire de Physique des Lasers) de l'Université Paris 13 à Villetaneuse travaille dans la photonique et les atomes froids, leurs pièges et sur la métrologie quantique. C'est le laboratoire d'Hélène Perrin, déjà citée, qui en est Directrice Adjointe.

Le **GEMaC** (Groupe d'Etude de la Matière Condensée) de Versailles travaille aussi dans le domaine des diamants et du graphène, sur l'électronique de spin et le magnétisme. On y trouve aussi de la QKD et de la mémoire quantique photonique. .

Du côté des approches de recherche collaboratives en Ile de France…

Le GDR[1276] **IQFA** (Quantum Engineering, from Fundamental Aspects) regroupe une cinquantaine de laboratoires de recherché en physique quantique ainsi qu'en informatique quantique. D'un point de vue pratique, ce genre de groupe se matérialise sous la forme de congrès de chercheurs et d'une coordination nationale de la recherche dans son domaine.

[1276] Groupement de recherche, entité de recherche collaborative qui agrège plusieurs laboratoires de recherche.

L'Initiative de Projet Stratégique **IQUPS** (Ingénierie Quantique à l'Université Paris-Saclay) est répartie sur plusieurs sites de l'Université Paris-Saclay aussi bien côté Palaiseau/X que côté Orsay. Elle regroupe une dizaine d'UMR (Unités mixtes de recherche) associant outre le CNRS, le CEA, l'Institut Mines Télécom et l'Ecole Polytechnique situées dans la zone Est du plateau de Saclay. Lancée en 2017, elle vise à coordonner les efforts d'ingénierie en informatique quantique. Il ne semble pas, néanmoins, qu'ils aient choisi une voie spécifique de qubits entre les supraconducteurs, les spins d'électrons et la photonique.

Lancé en 2014, le groupe **Paris Center for Quantum Computing** (PCQC) associe plusieurs dizaines de chercheurs franciliens issus de divers laboratoires, dont Philippe Grangier. Le **CNRS** a regroupé informellement ses efforts avec le groupe de travail Informatique Quantique qui travaille plutôt sur la dimension algorithmique.

On peut aussi signaler l'initiative du pôle de compétences en calcul haute performance **Teratec** (basé à Bruyère le Chatel, près de la Direction des Affaires Militaires du CEA) autour du quantique[1277].

Elle vise à développer des algorithmes quantiques, des méthodes de développement hybrides, des cas d'usage, et d'informer, former et animer une communauté.

Ils bénéficient d'un simulateur QLM d'Atos installé au CRTT (Centre de Calcul, Recherche et Technologie) du CEA à Bruyères-le-Châtel.

Enfin, le **SIRTEQ** (Science et Ingénierie en Région Ile de France pour les Technologies Quantiques) est une communauté qui groupe les laboratoires de recherche de l'Ile de France qui sont focalisés sur les technologies de communications quantiques.

Selon eux, il y a en Ile-de-France 650 chercheurs dans le quantique en tout (physique, algorithmes, télécommunications, cryptographie) répartis dans 100 équipes de 30 laboratoires de recherche.

Grenoble

L'écosystème quantique de Grenoble est dense, bien organisé et très focalisé sur la création de qubits à base de spins d'électron mais aussi en supraconducteurs, le tout avec de bonnes compétences en photonique. C'est probablement l'endroit où la coordination entre les équipes de recherche fonctionne le mieux, notamment en intégrant les étapes clés de l'industrialisation.

La recherche quantique à Grenoble est pilotée par différentes branches du CEA (Leti en nanoélectronique, qui fait partie de la DRT – direction de la recherche technologique - et IRIG en physique, qui fait partie de la DRF – direction de la recherche fondamentale), du CNRS (dans l'Institut Néel) et du LPMMC et notamment par deux équipes mixtes CNRS et CEA : NPSC (NanoPhysique et Semi Conducteurs) qui planche sur de la métrologie quantique, de la photonique quantique, de la thermodynamique quantique et des fondements de la mécanique quantique et Quanteca, créé en 2019, qui concerne toutes sortes de qubits statiques (CMOS, supraconducteurs, etc).

[1277] Teratec fédère plusieurs acteurs privés et publics du calcul haute performance dont Atos, le CEA, le CERFACS (Centre Européen de Recherche et de Formation Avancée en Calcul Scientifique), Dassault-Aviation, EDF, l'IFPEN, le PCQC (Paris Centre for Quantum Computing), Total et l'Université de Reims.

Le **CEA-Leti** (Laboratoire d'électronique et de technologie de l'information) de Grenoble est le laboratoire de micro et nanoélectronique du CEA. Il est notamment à l'origine de la technologie de wafer SOI qui a donné lieu à la création de SOITEC. Le Leti est focalisé sur l'ingénierie de qubits à spins d'électrons CMOS. Le projet est coordonné par Maud Vinet et fédère les efforts de plusieurs laboratoires du CEA et du CNRS.

L'**IRIG** (Institut de Recherche Interdisciplinaire de Grenoble) est un peu le pendant de l'Institut Néel du côté de la recherche fondamentale au CEA et en amont de ce que le Leti peut ensuite étudier côté ingénierie et fabrication. Il comprend notamment le Laboratoire PHotonique ELectronique et Ingénierie QuantiqueS qui travaille sur la physique de la matière condensée.

L'**Institut Néel**[1278], lancé en 2007, est un laboratoire du CNRS spécialisé notamment dans la physique de la matière condensée et disposant d'une masse critique de chercheurs dans le quantique. Il est situé sur la presque-île de Grenoble à deux pas du CEA-Leti. Ses chercheurs y explorent les pistes des qubits à spin d'électrons, supraconducteurs et en photonique.

On y trouve notamment Alexia Auffèves, Tristan Meunier et Franck Balestro. Une de ses unités de recherche est spécialisée en cryonégie avec notamment Henri Godfrin. Ils développent aussi de l'instrumentation spatiale.

Le **LPMMC** (physique de la matière condensée) de l'Université Grenoble Alpes est une UMR du CNRS tournée vers la physique théorique de la matière condensée et la physique quantique, les interactions quantiques à N-corps, la supraconductivité et la superfluidité, et sur l'évolution temporelle de systèmes quantique sous l'effet de champs magnétiques et électriques.

L'**IJF** (Institut Joseph Fourier) de l'Université de Grenoble travaille sur la dynamique quantique et en particulier sur les questions de décohérence et de bruit quantique thermique.

Le **LIG** (Laboratoire d'Informatique de Grenoble) s'intéresse aux algorithmes quantiques en général. On y trouve notamment le chercheur Mehdi Mhalla qui se penche sur la résolution quantique de problèmes de graphes.

[1278] L'institut tire son nom de **Louis Néel** (1904–2000, Français), un physician d'origine Lyonnaise devenu prix Nobel de Physique en 1970 pour ses études sur le magnétisme et la découverte de l'antiferromagnétisme. Il est à l'origine de la création du Polygone Scientifique de Grenoble qui regroupe de nombreux instituts de recherche et d'entreprises dans la presque-île entre l'Isère et le Drac. Le lieu accueillait le premier site du CEA hors région parisienne en 1956, lancé par Louis Néel. Le CNRS y prenait pied en 1962 et en 1967 était créé le CEA-Leti. Ce dernier est l'un des plus grands laboratoires civils au monde en recherche appliquée en nanoélectronique et nanotechnologies. Le polygone scientifique de Grenoble accueille également plusieurs organisations de recherch internationales, l'Institut Laue–Langevin, l'European Synchrotron Radiation Facility et l'une des branches de l'European Molecular Biology Laboratory. En 2005 était créé le CEA-Liten, une branche de la DRT spécialisée dans les énergies nouvelles (solaire photovoltaïque, batteries, piles à combustible, gestion complète du cycle du carbone, gestion d'énergies mixtes, matériaux innovants). En 2006 était lancé Minatec, un lieu de développement commercial de nanotechnologies complété ensuite par le pôle de compétivité Minalogic. En 2012 était lance le centre de recherché Clinatec, fondé par Alim-Louis Benabid, qui est à l'origine du premier exosquelette complet destiné à des tétraplégiques.

L'école d'ingénieurs en informatique **Ensimag** a lancé en 2019 un partenariat avec IBM qui est devenu parrain de la promotion 2021, avec en tête l'idée de former les élèves à la programmation quantique sur la plateforme IBM Q / Qiskit.

La recherche en ordinateur quantique à Grenoble est actuellement structurée autour de trois initiatives : **QuEnG**, **QuantECA** et **QuCube** qui ne sont d'ailleurs pas du même niveau.

Quantum Engineering
Univ. Grenoble Alpes

QuEnG (Quantum Engineering Grenoble) est un écosystème qui va du philosophe à l'industriel. C'est une initiative chapeau trans-laboratoire, trans-disciplinaire et trans-sectorielle. Elle s'attaque à la réalisation de qubits en CMOS et électrons piégés. Les équipes travaillent en physique sur de nombreuses autres filières : en photonique, sur des qubits supraconducteurs, à spins d'électrons et à base d'aimants moléculaires. Ces branches sont complémentaires. Ainsi, la photonique peut permettre la création de liens entre processeurs quantiques pour distribuer les traitements.

Le travail sur les capteurs joue un rôle pour mesurer l'état des qubits, quels qu'ils soient. Ils creusent aussi les questions de thermodynamique. Alexia Auffèves, de l'Institut Néel du CNRS, en est une grande spécialiste et assure la coordination de QuEng depuis sa création en 2017. Ils s'intéressent aux capteurs, aux codes de correction d'erreurs et aux algorithmes quantiques, notamment en partenariat avec Atos. Des équipes font aussi le lien entre physique quantique et philosophie avec Vincent Lam. L'initiative comprend aussi la formation d'ingénieurs en physique et en calcul quantique avec des cursus divers dont un projet avec l'Ensimag, la grande école d'informatique de Grenoble. Ils sont aussi partenaires d'IBM.

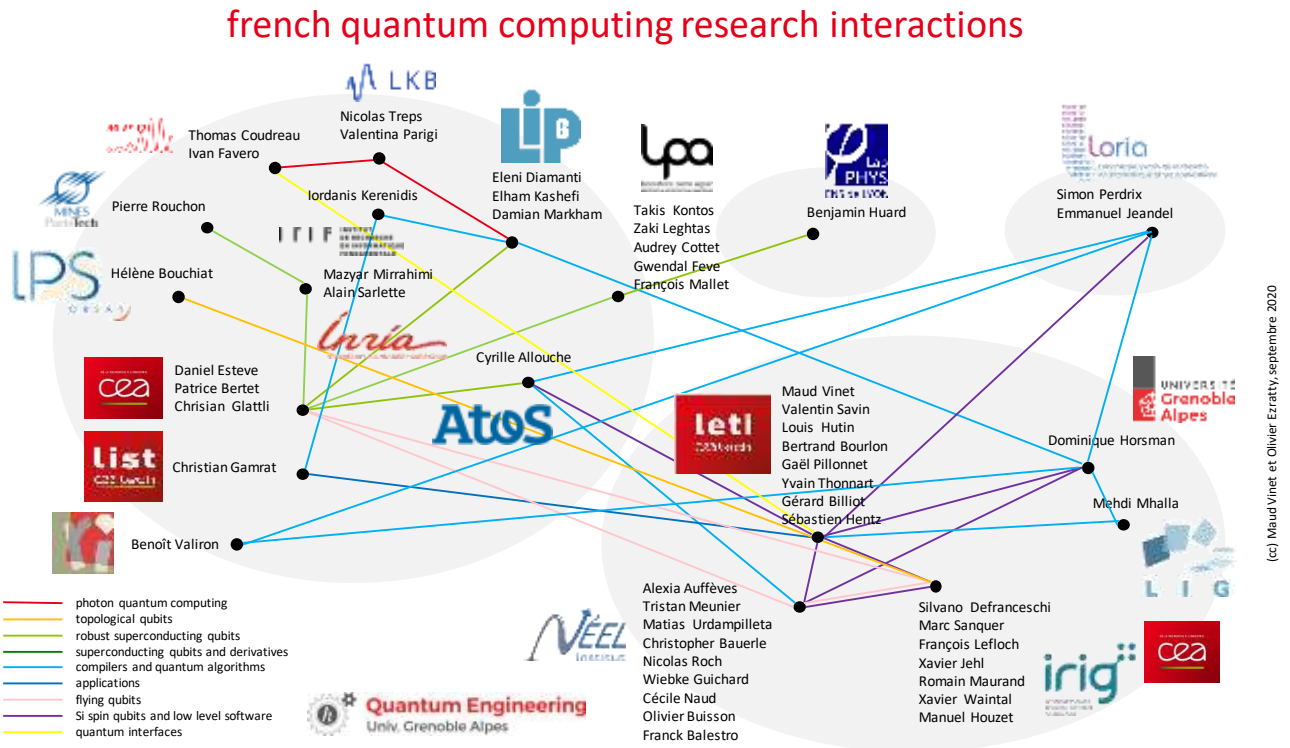
QuEnG est une initiative financée initialement par l'IDEX (Initiative d'Excellence) des Programmes d'Investissements d'Avenir (PIA) de l'UGA (Université Grenoble-Alpes) avec 1,7M€ complétés par un financement européen FP7 de 1,9M€ couvrant notamment des bourses de thésards. QuEnG regroupe une centaine de chercheurs en sciences fondamentales. S'y ajoutent ce qu'ils appellent des avantages en nature avec l'accès aux salles blanches du CNRS, du CEA-Leti, de SOITEC à Bernin et de STMicroelectronics à Crolles près de Grenoble qui permettent la fabrication de nombreux composants critiques : wafers SOI (silicon on insulators), prototypes de composants et industrialisation de leur fabrication.

QuantECA ou Quantum Electronic Circuits Alps est une initiative qui se situe au-dessous de QuEnG et couvre la partie intégration à grande échelle de qubits dans des puces. Elle regroupe le CEA-Leti, le département de physique de l'IRIG (ancien INAC, Interdisciplinary Research Institute of Grenoble, qui fait partie du CEA) et l'Institut Néel du CNRS. Leur champ d'action est la création de circuits de qubits stables, scalables et bien intriqués. Ils planchent aussi sur les technologies de stockage et de transport de l'information quantique. Ils s'appuient sur trois branches technologiques (supra-conducteurs/optique/spin d'électron spin). Ils maîtrisent en particulier une technologie unique au monde : l'optomécanique intégrée dans des circuits CMOS. Le CMOS est une partie de l'effort. C'est au sein de Quanteca que se situe l'équipe de Maud Vinet, Tristan Meunier et Silvano De Franceschi qui ont obtenu un financement ERC Synergy Grant pour le projet QuQube.

QuCube est l'initiative qui a récupéré le financement ERC Synergy Grant de 14M€ fin 2018. Son objectif est de créer un ordinateur quantique avec plus de 100 qubits d'ici moins de 10 ans en technologie CMOS / spin d'électron. Les qubits auront une taille de 100 nm avec la possibilité à terme d'en intégrer des millions dans un chipset. L'une des technologies clés à miniaturiser sont les briques de conversion du spin des électrons piégés en charge électrique.

Les capteurs associés sont placés dans une couche qui est située en-dessous des qubits. Les éléments de contrôle des qubits (initialisation, portes quantiques) sont placés au-dessus des qubits.

Et voici comment sont reliés les divers laboratoires de recherche en France autour du pôle de Grenoble. Ce visuel est dérivé d'un schéma de Maud Vinet du CEA-Leti.



Lyon

La recherche à Lyon est bien équilibrée entre la partie physique et la partie mathématique et logicielle du quantique.

Le **Laboratoire de Physique de l'ENS Lyon** est focalisé sur l'étude de la matière condensée et de l'information contenue dans les dispositifs quantiques, à son amplification, à leur fluctuation, à la thermodynamique de l'informatique quantique, à la mesure quantique et à l'optique quantique. On y trouve notamment le Quantum Circuit Group de Benjamin Huard qui travaille sur les qubits supraconducteurs et leurs codes de correction d'erreurs. Il a été notamment rejoint par Audrey Bienfait en 2019, en provenance d'une thèse réalisée au CEA-SPEC de Saclay. C'est aussi là que Théau Peronnin finalisait sa thèse en 2020 tout en créant la startup Alice&Bob avec Raphaël Lescanne, qui est aussi passé par ce laboratoire.

L'**INL** (Institut des Nanotechnologies de Lyon) est situé à Centrale Lyon (Ecully). Ils planchent sur les semiconducteurs et la photonique. Ils disposent d'une plateforme technologique de prototypage de composants, notamment en photonique.

L'**iLM** (Institut Lumière Matière) de Lyon est spécialisé comme son nom l'indique en photonique. Je n'ai par contre pas trouvé de liens directs avec le calcul quantique.

L'**Institut Camille Jordan** de Lyon est un laboratoire de recherche en mathématiques qui travaille notamment sur les probabilités quantiques. Il est distribué sur plusieurs sites : Villeurbanne, Saint-Étienne et sur le campus de Centrale Lyon à Écully.

Le **LIP** (Laboratoire de l'Informatique du Parallélisme) de l'ENS Lyon associe le CNRS, l'Inria et l'Université Claude Bernard Lyon 1. Son équipe MC2 travaille sur l'informatique théorique et la théorie de la complexité. On y trouve notamment Omar Fawzi, médaille de bronze 2019 du CNRS et spécialiste de la théorie de l'information quantique. Il mène ses travaux dans l'équipe MC2 du LIP.

Occitanie

La recherche quantique à Toulouse est très centrée sur la physique de base et assez éloignée de l'informatique quantique à l'exception du **LPTT**. On trouve sinon deux laboratoires à Montpellier dont un est associé à IBM.

Le **CEMES** (Centre d'Élaboration de Matériaux et d'Etudes Structurales) de Toulouse est spécialisé en physique et en optronique. Il s'intéresse au couplage lumière-matière à l'échelle et la création de capteurs plutôt orientés vers les objets connectés que les applications quantiques.

Le **LCAR** (Laboratoire Collisions Agrégats Réactivité) de l'Université Paul Sabatier de Toulouse travaille notamment sur les atomes de Rydberg mais sans aller jusqu'à créer des qubits basés dessus. C'est dans l'équipe de Juliette Billy et David Guéry-Odelin.

Le **LPCNO** (Laboratoire de Physique et Chimie des Nano-objets) de l'INSA Toulouse est spécialisé en photonique et électronique quantique. Ils étudient les spins d'électrons et de noyaux, les quasi-particules et les quantum dots. Ils visent des applications dans l'informatique quantique. Leurs recherches visent aussi des applications dans le secteur de la santé.

L'**IMT** (Institut de Mathématiques de Toulouse) de l'Université de Toulouse étudie la physique statistique et quantique. On y trouve notamment Clément Pellegrini qui étudie la théorie de l'information quantique et la mesure d'états quantiques.

Le **LPTT** (Laboratoire de Physique Théorique de Toulouse) travaille sur les supraconducteurs et les boucles SQUID à effet Josephson. Petite particularité, ils sont impliqués dans le projet Quantware qui a été cofinancé entre autres par la NSA !

Le **LCPQ** (Laboratoire de Chimie et Physique Quantiques) de l'Université Paul Sabatier de Toulouse développe des codes généralistes de chimie quantique, contribuant aux efforts de simulation moléculaire.

Le **L2C** (Laboratoire Charles Coulomb) de l'Université de Montpellier planche sur la métrologie quantique, la dynamique de spin et le graphène, avec des applications dans la microscopie magnétique.

L'Université de Montpellier est partenaire d'IBM dans la mise en place d'un laboratoire commun sur le quantique qui vise en fait à évangéliser les clients sur les principes généraux et les outils de la plateforme quantique IBM Q.

Le **LIRMM** (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier) se penche notamment sur la création d'algorithmes quantiques. Il collabore avec Total dans ce sens. Y officie notamment Aida Todri-Sanial qui y est Directrice de Recherche et travaille notammentsur la création d'algorithmes quantiques de routage de circuits dans les circuits intégrés.

Sud

On trouve aussi quelques laboratoires de physique quantique à Marseille dont trois ont un lien direct avec les besoins de l'informatique quantique. Et un laboratoire à Nice.

L'**Institut Fresnel** de Marseille fait de la photonique, donc, inévitablement, peut contribuer aux avancée dans la gestion de qubits à base de photons ainsi que dans la cryptographie quantique à base de QKD.

Le **CPT** des Universités de Marseille et de Toulon travaille sur la dynamique quantique et la diffusion d'ondes dans les fibres optiques et guides de lumières, à l'électrodynamique quantique. Ils sont partenaires de diverses universités étrangères : Aalborg University (Danemark), Pontificia Universidad Catolica de Chile, Karlsruhe Institute of Technology (Allemagne), Kyoto Institute of Technology et le Moscow Institute of Physics and Technology.

Le laboratoire **PIMM** (Physique des interactions Ioniques et Moléculaires) de l'Université de Marseille fait de la recherche dans les plasmas, plus en lien avec le projet de fusion nucléaire ITER qu'avec l'informatique quantique.

Le **Laboratoire d'Informatique Fondamentale** de Marseille s'intéresse notamment au calcul quantique. Leur projet Discrete Time Quantum Simulator a été lancé en 2018. Ils travaillent sur les Quantum Walks et le Quantum Cellular Automata qui a l'air de s'apparenter au MBQC.

INPHYNI (Institut de Physique de Nice) de l'Université Nice Côte d'Azur s'intéresse aux atomes froids, au transport d'ondes, aux interactions entre lumière et atomes. Il déploie un réseau de test de QKD entre Nice en Sophia-Antipolis depuis 2019 en partenariat avec Orange. Le laboratoire quantique est dirigé par Sébastien Tanzilli.

Bourgogne Franche-Comté

Besançon héberge trois laboratoires dans le quantique et Dijon un quatrième.

Le **LmB** (Laboratoire de Mathématiques de Besançon) de l'Université Bourgogne Franche-Comté étudie les groupes quantiques et les probabilités.

L'Institut **UTINAM** (Univers Transport Interfaces Nanostructures Atmosphère et environnement, Molécules) de l'Université de Besançon étudie notamment les phénomènes de décohérence quantique dans des problèmes de contrôle, de diagnostic, de traitement et de transport de l'information quantique. Cela relève plutôt du champ de la métrologie.

Femto-St est un Institut de recherche à Besançon focalisé sur les nanosciences, l'optique et l'optoélectronique. Ils planchent notamment sur les télécommunications optiques, sur l'optique non linéaire et sur l'imagerie quantique.

Le laboratoire **Icb** (Interdisciplinaire Carnot de Bourgogne) de l'Université de Bourgogne, basé à Dijon comprend une équipe étudiant la dynamique quantique et non-linéaire (DQNL).

Grand Est

La région comprend trois laboratoires sur le quantique situés à Strasbourg, Nancy et Troyes.

Le **Quantum Matter Theory Group** de l'Université de Strasbourg fait de la physique de la matière condensée et travaille aussi sur les interactions entre lumière et matière, notamment avec des atomes de Rydberg.

Le **L2n** (Lumière Nanomatériaux Nanotechnologies) de l'Université de Technologie de Troyes travaille dans l'optoélectronique et les sources de photons.

Le **Loria** (Laboratoire lorrain de recherche en informatique et ses applications) est basé à Nancy. Deux enseignants-chercheurs s'y intéressent au calcul quantique et aux algorithmes : Simon Perdrix et Emmanuel Jeandel. Le premier est l'un des principaux contributeurs aux travaux sur le ZX-Calculus qui accompagne le développement d'algorithmes dans les architectures MBQC.

Ils pilotent le projet **SoftQPro**, en association avec le CEA et Atos, qui s'étale entre 2017 et 2020 et vise à optimiser les programmes quantiques. Visiblement, beaucoup avec le ZX-calculus.

Ailleurs en France

Et pour terminer, voici quelques laboratoires de physique touchant au quantique situés dans d'autres régions, à Rennes, Lille, Bordeaux et Limoges mais sans lien direct apparent avec l'informatique quantique.

L'**IPR** (Institut de Physique de Rennes) est rattaché à l'Université de Rennes. Ils s'intéressent à la dynamique quantique, l'évolution des états quantiques dans le temps.

Le **LARIS** (Laboratoire Angevin de Recherche en Ingénierie des Systèmes) basé à Angers traite de sujets informatiques divers. En son sein, François Chapeau-Blondeau et Etienne Belin s'intéressent à l'impact du bruit sur les algorithmes quantiques.

Le **PhLAM** (Laboratoire de Physique des Lasers Atomes et Molécules) de Lille s'intéresse à la photonique et aux atomes froids.

L'**IEMN** (Institute of Electronics, Microelectronics and Nanotechnology) est un laboratoire situé sur quatre sites à Lille, Villeneuve d'Ascq et Valencienne. Ils sont notamment spécialisés dans la conception de nanostructures quantiques.

Le **LP2N** (Laboratoire Photonique, Numérique et Nanosciences) de l'Institut d'Optique de Bordeaux fait de la recherche en photonique et en métrologie à base d'atomes froids (microgravitométrie). C'est de là qu'a émergé la startup Muquans.

Le **XLIM** (Limoges) fait entre autres choses de la photonique. Ils sont notamment partenaires avec Thales TRT. Ils travaillent notamment sur des applications en métrologie des polaritons, en particulier les SPR (Surface Plasmon Resonance).

Collaborations internationales

Les partenariats internationaux sont très courants dans la recherche. Nombre de travaux de chercheurs français sont réalisés avec des chercheurs d'autres pays, notamment des USA, du Royaume-Uni, d'Autriche, Pays-Bas et Allemagne, Japon et Singapour (notamment avec des unités mixtes internationales du CNRS). Il suffit de consulter la littérature scientifique pour se rendre compte de l'intensité de cette coopération.

Le CEA avait lancé en 2018 un partenariat avec l'**UNSW** australienne et la startup Silicon Quantum Computing (SQC) pour créer des processeurs quantiques silicium. Il s'agissait en fait d'étudier l'opportunité de créer un partenariat. Mais les négociations n'ont pas abouties.

Le CEA-Leti est partenaire de l'**Imec**, son homologue en Belgique, basé à Louvain avec 1600 chercheurs, couvrant l'IA et le calcul quantique.[1279] Comme le CEA-Leti à Grenoble, ils disposent d'une salle blanche pour de la gravure jusqu'en 28 nm et sur wafers de 30 cm et une autre sur wafers de 20 cm pour des MEMS.

Le **Centre Spatial Universitaire de Grenoble** collabore depuis 2017 avec l'**IQOQI** autrichien sur l'envoi de clés quantiques par satellite dans le projet Nanobob.

L'**ANR** avait clôt en février 2018 un appel à projets de recherche, lancé dans le cadre d'un partenariat de recherche avec le Japon (CREST).

Et il existe une autre collaboration internationale sur le quantique associant la France, les Pays-Bas (QuSoft) et la Lettonie. Cet inventaire est très incomplet car les collaborations internationales sont innombrables.

Enseignement supérieur

L'enseignement supérieur autour du quantique est structuré sur divers parcours :

- Les bases de la physique quantique sont enseignées en **classes préparatoires scientifiques**. Equations de Maxwell et de Schrödinger sont au programme. Ce sont les bases des bases.

[1279] Voir Partners Double-Team AI & Quantum Computing, de Mathew Dirjish, novembre 2018.

- Les cursus de **licences et masters** en physique ont des spécialités en physique quantique. C'est notamment le cas à l'Université Côte d'Azur, Sorbonne Université, Paris Diderot, à l'Université Paris Saclay en partenariat avec CentraleSupelec, à l'Université Paul Sabatier de Toulouse en partenariat avec l'INSA, à l'UGA de Grenoble, à l'Université de Lorraine, à l'Université de Montpellier en partenariat avec IBM. En règle générale la physique quantique est bien plus enseignée que l'informatique quantique.
- Les **écoles d'ingénieurs** commencent à mettre en place des spécialités ou options en physique et en informatique quantique. C'est notamment le cas à l'Ecole Polytechnique[1280], l'ENS Ulm, à l'ENS Paris Saclay, l'ENS Lyon, CentraleSupelec, Télécom Paristech, ISAE-Sup Aero, INSA de Lyon[1281], INSA de Toulouse, CPE Lyon, Epitech Lyon, à l'ISEN, Supinfo et à l'ECE.
- Il est ensuite possible de faire un **doctorat et un post-doc** dans les Universités, les écoles d'ingénieurs et dans les nombreux laboratoires de recherche inventoriés dans la partie précédente.

L'un des grands enjeux est de créer des cursus d'ingénierie de systèmes pour créer de véritables machines qui fonctionnent de bout en bout. Cela nécessite de décloisonner les disciplines et de rapprocher les physiciens des ingénieurs. Les technologies mises en jeu sont variées et incluent la photonique et les lasers, l'électronique analogique et numérique, notamment avec les micro-ondes, la thermodynamique, la mécanique des fluides, l'ingénierie de production de composants diverses et enfin, la conception de systèmes complets.

Ensuite, dans les domaines purement mathématiques et logiciels entrent en jeu des disciplines très importantes pour pouvoir créer des solutions quantiques de bout en bout : les théories de la complexité pour la conception d'algorithmes efficaces et la création d'algorithmes quantiques. S'y ajoute le champ de la cryptographie post-quantique.

Enfin, la création des applications métiers demande des compétences à la croisée des chemins entre celle du dessus et des compétences sectorielles, souvent elles-mêmes scientifiques comme dans les sciences du vivant (chimie organique, repliement des protéines, photosynthèse, …), les sciences des matériaux (comme dans la chimie des batteries au niveau des cathodes et anodes) ou d'autres branches comme les calculs de risques dans la finance ou les problèmes d'optimisation dans la logistique et les transports. C'est là que grandiront le plus les besoins en compétences au gré de l'augmentation de la puissance de calcul des ordinateurs quantiques. On en trouve déjà dans les premières grandes entreprises françaises qui se sont emparée du quantique, en particulier chez Total, EDF, Airbus et BNP où des dizaines d'ingénieurs et chercheurs sont déjà actifs autour des applications des technologies quantiques.

Du côté des métiers à proprement parler, on peut citer :

- Les **physiciens de la physique fondamentale** (physique du solide, de la matière condensée, interaction lumière-matière, optique quantique) qui associent approches théoriques et expérimentales pour comprendre des phénomènes à bas niveau. Côté calcul quantique, l'augmentation du nombre de qubits et de portes logiques ne pourra se faire que grâce à de nouveaux sauts conceptuels.
- Les **chercheurs en technologies quantiques** qui transforment les découvertes fondamentales en premières preuves de concept en laboratoire. Ces équipes de recherche combinent des chercheurs en physiques, des chercheurs en technologies et ingénierie.

[1280] Signalons à ce sujet la création du groupe QuantX d'anciens de l'école Polytechnique actifs dans l'écosystème quantique. On y trouve notamment les incontournables Christophe Jurczak (Quantonation) et Pascale Senellart (CNRS, Quandela). L'association est présidée par Elvira Shishenina, une brillante chercheuse en algorithmie quantique qui travaille chez Total. Voir QuantX : les polytechniciens et le quantique par Elvira Shishenina, Alexandre Krajenbrink, et Christophe Jurczak, juin 2020.

[1281] Avec deux modules électifs pour les étudiants de cinquième année avec 64h de cours, 32h pour la théorie du calcul quantique et 32h pour la programmation.

- Des **ingénieurs de conception** qui créent des sous-ensembles techniques d'ordinateurs quantiques jusqu'à des produits finis complets. Ils font essentiellement le "D" de la "R&D" en s'appuyant sur le R des physiciens.
- Des **ingénieurs de recherche**, qui participent au développement des nouveaux matériaux et nouvelles technologies dans les centrales RENATECH comme le C2N à Palaiseau ou dans la salle blanche de Thales TRT, ou des ingénieurs procédés qui conçoivent les processus de fabrication de ces systèmes de circuits intégrés supportant les qubits au CEA-Leti.
- Des **techniciens** pour la fabrication de certains composants et/ou pour le déploiement de technologies comme la cryptographie quantique dans l'univers des télécoms. Mais seulement une fois que cette technologie sera déployée à l'échelle industrielle, probablement par des opérateurs de télécommunication généralistes ou spécialisés.
- Des **développeurs d'outils de développement** qui doivent être associés aux chercheurs et ingénieurs précédents. En effet, pour l'instant, la conception de ces outils doit encore tenir compte des spécificités physiques des calculateurs/accélérateurs quantiques.
- Des **développeurs d'applications**, qui seront de plus en plus nombreux au gré de l'augmentation de la puissance de calcul des ordinateurs quantiques.
- Des **chefs de projets** qui gèrent des projets associant ces différents métiers.

Comme dans de nombreuses disciplines, les chercheurs et ingénieurs doivent de plus en plus être polyvalents. Les équipes doivent s'articuler autour d'une forte interdisciplinarité et transversalité. Elles ont besoin de "polyglottes technologiques" qui relient tous ces métiers et toutes ces compétences. Les physiciens devront notamment s'intéresser de plus en plus à l'ingénierie et les ingénieurs à la physique. Dans le quantique, les deux sont étroitement associés (évitons les jeux de mots habituels…).

Enfin, lorsque l'on arrive au "business" avec des produits qui peuvent être commercialisés, il faut ajouter tout le mixte des compétences habituelles de la vente de technologies : du marketing produit, du marketing opérationnel, du lancement de partenariats, de la création d'écosystèmes et surtout, de la vente pure et simple en mode B2B.

S'y ajoutent les compétences génériques de la création de startups dans l'univers des deep techs (organisation, business planning, recrutement, financements, etc). Il faut compléter cela par des conseils en propriété industrielle qui doivent se coltiner les spécificités du vocabulaire du quantique ainsi que des contributeurs aux divers processus de standardisation qui ne manqueront pas d'émerger.

Le mix des compétences évoquées va évoluer au gré de la maturation des technologies quantiques. Elle est de niveau différent selon le domaine.

Les produits de la métrologie quantique commencent à être commercialisés, comme les gravimètres de Muquans et sur un marché pour l'instant de niche mais qui pourrait devenir un marché de volume comme l'envisage Thales dans les capteurs de position.

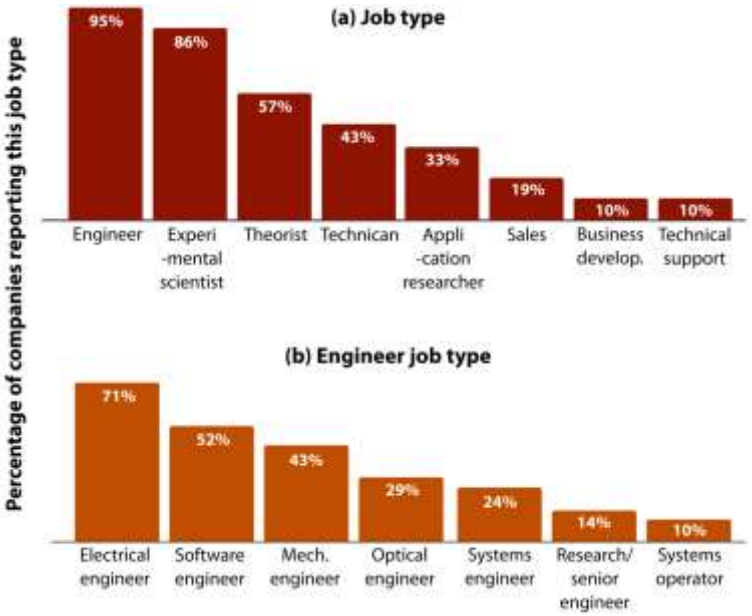
De nombreux autres capteurs quantiques sont en développement à base de cavités de diamants, de lumière quantique ou de résonateurs optomécaniques qui arriveront sur le marché dans la décennie qui vient.

Les systèmes de cryptographie quantiques sont en phase expérimentale terrain et pourraient être déployés à plus grande échelle dans la décennie qui vient. Les communications quantiques dont l'objectif est de conduire à des réseaux de communications quantiques se développeront dans un second temps, combinant réseau fibré et satellite, avec relais quantiques. C'est un domaine complémentaire du développement des ordinateurs quantiques qui seront mis en réseau grâce à ces nouveaux moyens de communication.

Enfin, le calcul et la simulation quantiques vont évoluer progressivement et voir leur champ applicatif s'élargir au gré de l'augmentation du nombre de qubits de qualité disponibles dans les calculateurs quantiques.

Ce sera un processus d'innovation continu. Il passera par différentes étapes transitoires comme le NISQ ("noisy intermediate-scale quantum") qui décrit les ordinateurs quantiques actuels et des 10 prochaines années qui utilisent des qubits "bruités" imparfaits.

Avant que l'on puisse utiliser des qubits en très grande quantité, au-delà de 100, bruités et intégrant des systèmes de corrections d'erreurs.



voici un inventaire américain des métiers et compétences d'ingénieurs dans les technologies quantiques[1282]

Comme c'est le cas dans l'informatique traditionnelle, le poids du logiciel est amené à terme à devenir dominant dans les besoins en compétences. Cela explique pourquoi nombre de publications insistent sur le besoin en développeurs d'applications quantiques. C'est ce sur quoi "évangélisent" les grands acteurs que sont IBM, Google et Microsoft, sans compter D-Wave, Rigetti ou IonQ[1283].

Néanmoins, parallèlement au développement du marché logiciel, une phase intermédiaire demandera beaucoup de compétences en ingénierie et dans les différentes branches du quantique. C'est la voie indispensable de l'industrialisation des ordinateurs quantiques, tout du moins si la France veut avoir sa part du gâteau dans ces marchés de l'offre et pas seulement dans l'usage des technologies quantiques.

Pour s'organiser, il faudra coordonner la création de cursus complémentaires, d'assurer une volumétrie en phase avec des besoins, et en avance de phase. Dans certains cas, des formations pourront être mutualisées entre plusieurs établissements supérieurs (grandes écoles, universités), surtout lorsque les compétences d'enseignement sont rares.

La formation dans l'enseignement supérieur public devra introduire les sciences et technologies quantiques le plus en amont possible des cursus aux niveaux licence et master. Il faudra aussi y créer des masters en ingénierie quantique, rapprochant le monde de la recherche et de l'ingénierie.

L'offre de formation dépendra de plusieurs paramètres : des financements de postes d'enseignants chercheurs ou d'enseignants, de la création de vocations, de la capacité à les attirer les enseignants et les étudiants, d'où qu'ils viennent. Cela passera par le développement de l'attractivité de l'offre en France. Il faudra pour la partie fondamentale générer autant de doctorants que possible pour les formations scientifiques et développer les thèses CIFRE avec les industriels. Et côté ingénierie, l'offre de formations devra être en phase avec la capacité de l'industrie à proposer de stages de longue durée.

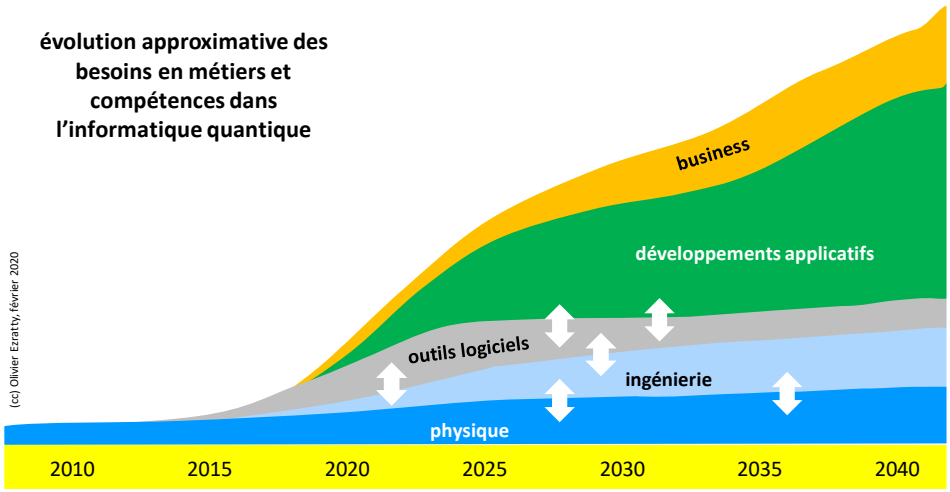
[1282] Source : Preparing for the quantum revolution -- what is the role of higher education? par Michael F. J. Fox, Benjamin M. Zwickl et H. J. Lewandowski, 2020 (23 pages).

[1283] Voir ainsi : Quantum Computing Demands a Whole New Kind of Programmer par Edd Gent, mai 2017 (un peu en avance de phase), The Hitchhiking Cat's Guide to Getting a Job in Quantum Computing par Jay Gambetta, octobre 2019, Building Quantum Skills With Tools For Developers, Researchers and Educators, IBM Research, septembre 2019 et Some useful skills for quantum computing par Chris Granada, janvier 2020, qui insiste aussi sur les compétences mathématiques et logicielles.

Ces stages seront probablement proposés par des entreprises et startups aussi bien françaises qu'étrangères. Des entreprises qui seront donc naturellement intégrées dans les hubs quantiques.

Les chaires industrielles jouent un rôle de passerelle entre les grandes entreprises, la recherche et l'enseignement supérieur. Atos en a créé une sur le quantique conjointement avec le CEA en 2018. Dénommée Nasniq ("Nouvelle architecture de spins nucléaires pour l'information quantique"), elle est portée par Daniel Estève du CEA-Saclay et couvre à la fois des aspects physiques (qubits supraconducteurs) et logiciels (programmation hybride). IBM a créé de son côté une chaire avec l'ESIEE Paris qui porte sur l'IA et les analytics qui aura accès aux outils de calcul quantique d'IBM.

La formation continue pourra comprendre des cursus aussi bien scientifiques et technologiques (physique quantique, communications quantiques, algorithmes et logiciels quantiques) que stratégiques (compréhension des enjeux, connaissance des acteurs, économie du secteur, bonne pratiques).



Elle peut ou pourra être délivrée par des organisations privées comme Capgemini Institut (où je délivre des séminaires de sensibilisation sur le sujet), par des organismes d'enseignement supérieur ainsi que via des cours en ligne proposés à différents endroits (Coursera, …).

Alain Aspect propose même un MOOC sur l'optique quantique en deux parties à l'Ecole Polytechnique. On trouve des Mooc chez Udemy. On peut évidemment en dénicher un bon nombre aux USA (Stanford, MIT, Coursera, …). Enfin, les pionniers des technologies quantiques des grandes entreprises françaises (Atos, Thales, Total, EDF, Airbus, BNP, …) pourront faire intervenir leurs cadres et chercheurs dans l'enseignement supérieur comme dans la formation continue.

L'auto-formation permet aux passionnés de découvrir par eux-mêmes ces sciences et technologies mais elle n'est pas autosuffisante comme c'est parfois le cas dans l'intelligence artificielle.

Elle doit être complétée par un accompagnement pédagogique de qualité, ne serait-ce que pour faire et corriger des exercices. Pour ce qui est de la partie logicielle, cela changera peut-être le jour où les outils de développement auront un plus haut niveau d'abstraction que ceux d'aujourd'hui.

Les événements scientifiques organisés par les hubs quantiques, les laboratoires de recherche et les entreprises servent à faciliter la transdisciplinarité des chercheurs et des ingénieurs. Il peut s'agir de colloques interdisciplinaires, de conférences thématiques ou d'ateliers.

L'un des bons exemples est la conférence du 27 novembre 2019 organisée par le C2N du CNRS et l'équipe mixte Thalès/CNRS pour croiser informatique quantique et processeurs neuromorphiques. Ce sont des mises en bouche qui doivent s'accompagner ensuite de formation et de temps pour approfondir les sujets découverts.

Il faudra aussi faire en sorte d'attirer autant de femmes que d'hommes dans ces cursus, au risque sinon, de voir se développer comme dans l'IA un secteur entier bien trop masculin. Sans compter l'augmentation de la diversité des origines sociales des étudiants qui reste un moyen de promotion républicain clé, malgré son déclin actuel.

En amont de tous ces cursus, la création de vocations chez les jeunes est indispensable. L'équipe de Paula Forteza avait fort à propos lancé une initiative dans ce sens avec une mini-exposition de vulgarisation du quantique à la Cité des Sciences en octobre/novembre 2019. Avec Fanny Bouton et Tara Mestman (15 ans), je suis intervenu chez Magic Makers en septembre 2019 devant une vingtaine de lycéennes (ci-dessus), puis le 29 février 2020 dans l'événement Startup4Teens et enfin le 7 mars 2020 dans le programme de #laTechpourtoutes à l'Ecole 42. Des actions à démultiplier si possible en région !

La fête de la science annuelle et les journées portes ouvertes des laboratoires de recherche peuvent aussi y contribuer. C'est un travail de longue haleine comme l'est la création de vocations dans les sciences en général et dans les métiers scientifiques et techniques du numérique en particulier.

Startups

Les startups quantiques françaises sont les quatrièmes dans le monde en nombre. Elles sont plutôt spécialisées dans les composants (**CryoConcept** pour la cryogénie, **Muquans** pour la métrologie, **Quandela** pour les sources de photons). Nous avons côté qubits trois startups avec **Alice&Bob** (qubits supraconducteurs à faible taux d'erreurs) **C12** (nanotubes de graphène), **Pasqal** (atomes froids) et **NextGenQ** (ions piégés).

Côté logiciels, **Prevision.io** s'intéresse à l'intégration d'algorithmes quantiques dans son offre d'automatisation de recherche d'algorithmes de machine learning dans le cloud. On compte aussi **Qubit Pharma** (simulation moléculaire et criblage) et **QuantFi** (dans la finance).

Enfin, du côté de la cryptographie quantique et post-quantique, nous avons principalement **CryptoNext**, **CryptoExperts** et **Veriqloud**.

Investisseurs et accompagnement

Concernant les investisseurs, en plus de **Bpifrance**, il y a surtout le fonds d'investissement **Quantonation**, déjà cité, et qui joue un rôle clé dans l'animation de l'écosystème quantique en France.

Citons également le **Deep Tech Founders** qui forme des entrepreneurs/chercheurs dans les deep techs. C'est un programme international créé par l'équipe de Hello Tomorrow. Ils sont à l'origine de la création d'une structure d'accompagnement de l'écosystème quantique en partenariat avec Quantonation et Bpifrance, le **Lab Quantique**. Sa structure a été officialisée en avril 2020.

Le Lab Quantique se positionne comme un think tank pour le développement des talents, notamment à la croisée des chemins entre la science et l'entrepreneuriat. D'un point de vue pratique, le Lab Quantique organise des rencontres régulières rassemblant surtout des entrepreneurs des technologies quantiques, de France et de l'étranger. Ces rencontres avaient lieu sous la forme de visioconférences sur Zoom pendant la période du confinement du virus covid-19 en 2020. Il se donne comme objectifs de densifier le maillage entre acteurs industriels, startups et académiques, d'établir des passerelles avec l'international, de lancer un programme d'accélération des startups du quantique et d'organiser une grande conférence annuelle de haut niveau associent toutes les parties prenantes de l'écosystème, ainsi qu'un Prix International (attractivité des talents)[1284].

Entreprises

Parmi les grands comptes français ayant publiquement annoncé s'intéresser à l'informatique quantique, on peut citer **Airbus** qui, depuis 2015, étudie diverses domaines d'applications aussi bien côté cryptographie que côté calcul quantiques. Les banques sont aussi intéressées, au moins sur la partie crypto quantique, comme à la **Société Générale** ! D'autres industriels font de la veille active sur le quantique, comme **Total**, **EDF** et la **BNP**.

[1284] Voir Pour un écosystème de l'informatique quantique par Christophe Jurczak et Jean-Christophe Gougeon, 2020.

De son côté, **Thales** est très actif comme nous l'avons déjà vu du côté de la métrologie quantique ainsi que dans la cryogénie des systèmes embarqués. **Air Liquide** compte pour sa part être un acteur clé des technologies habilitantes, notamment dans la cryogénie.

C'est **Atos** qui est l'acteur industriel le plus actif en France sur le calcul quantique. Nous avions déjà eu l'occasion de décrire leur offre logicielle quantique.

Ils ont notamment développé un émulateur quantique sur serveurs à base Intel, la Atos Quantum Learning Machine (aQLM). Lancé en septembre 2017, l'émulateur quantique aQML est un calculateur classique notamment adopté par le centre de recherches américain d'Oak Ridge du Département de l'Energie, qui teste de nombreux types de supercalculateurs. Il est aussi installé au CEA, à l'Université de Reims et depuis juillet 2018, dans le département de recherche en cybersécurité de l'Université de Sciences Appliquées de Haute-Autriche à Hagenberg. Il a été vendu en février 2019 au Centre des installations scientifiques et technologiques (STFC) Hartree du Royaume-Uni ainsi qu'en août 2019, au C-DAC (Centre for Development of Advanced Computing) en Inde qui créait par la même occasion un Quantum Computing Experience Center[1285] et en 2020 au Japon ainsi qu'en Finlande au CSC IT Center for Science Kvasi dans le cadre d'une collaboration avec la startup IQM. Atos travaille aussi avec Total pour développer des solutions quantiques destinées à identifier de nouveaux matériaux et molécules de la transition énergétique. Ils s'appuient sur Centre d'Excellence en Programmation Parallèle (CEPP) d'Atos qui est installé au centre de calcul GENCI à Orsay.

En juin 2020, Atos lançait le QLM E, une nouvelle version de cet émulateur intégrant de 2 à 32 GPUs Nvidia V100, et multipliant la puissance par 12 par rapport à la version initiale qui était équipée uniquement de processeur Intel.

C'était complété début juillet 2020 par l'annonce d'une solution logicielle d'émulation du calcul à recuit quantique, donc de code destiné aux D-Wave, compatible avec les machines aQML.

Ils annonçaient en 2020 qu'ils lanceraient un accélérateur quantique NISQ d'ici 2023, sans préciser la technologie de qubits utilisée. Ils ménagent leurs options côté matériel en observant ce qui se fait dans l'ensemble des filières du quantique. Ils examinent plusieurs pistes comme les supraconducteurs (avec IQM), les ions piégés (avec l'Université d'Innsbruck), les atomes froids (avec la startup française Pasqal) et à plus long terme les qubits silicium (avec le CEA-Leti).

En mai 2018, Atos et le CEA lançaient une chaire industrielle sur l'informatique quantique, cofinancée par l'ANR. Dirigée par Daniel Estève du CEA Saclay, elle est baptisée **Nasniq** pour "Nouvelle architecture de spins nucléaires pour l'information quantique". Donc, avec un axe porté sur un type spécifique de qubit. Par contre, l'annonce de cette chaire évoque des recherches pour faire "*face à l'explosion des données entraînée par le Big Data et l'Internet des Objets*". Pourquoi pas, mais l'informatique quantique ne semble pas vraiment adaptée à court et à moyen terme à l'exploitation de très gros volumes de données. On est dans la complexité algorithmique plutôt que dans le traitement de gros volumes de données, tout du moins compte-tenu de l'état de l'art des algorithmes et architectures quantiques.

Ils participent notamment aux projets du Flagship Européen **AQTION** (accélérateur quantique) et **PASQuanS** (simulateur analogique quantique). Atos s'intéresse aussi à la cryptographie post-quantique.

[1285] Voir Atos et C-DAC signent un accord de coopération pour accélérer le développement de l'informatique quantique et exascale et l'Intelligence Artificielle en Inde, août 2019.

Atos est aussi très impliqué dans le projet EuroHPC dont fait partie l'**European Processor Initiative**, cette initiative de développement d'un processeur adapté à la fois aux besoins des supercalculateurs et à ceux de l'embarqué comme dans les véhicules autonomes. Ce dernier projet est piloté par Philippe Notton d'Atos (jusqu'en juin 2019) en étroite collaboration avec de nombreuses institutions et entreprises allemandes. L'axe Franco-Allemand est stratégique pour Atos, notamment du fait que Siemens est un de leurs principaux actionnaires depuis l'acquisition de trois filiales de ce dernier entre 2011 et 2017 (Siemens IT Solutions and Services, Unity et Convergence Creators)[1286].

La bataille du quantique va rapidement devenir une bataille de plateformes logicielles. L'un des enjeux d'Atos est donc de pousser ses outils de développement auprès d'un maximum de développeurs, décrits dans la partie idoine de cette série.

En mai 2019, Atos faisait une marche en avant dans cette bataille de plateforme en lançant myQLM, une offre d'outils de programmation quantique destinée aux chercheurs, étudiants et développeurs. C'est un environnement de développement en Python permettant de simuler des programmes quantiques sur son propre ordinateur. La programmation est réalisée en aQASM (Atos Quantum Assembly Language) et pyAQSM. Pour accéder à un nombre de qubits dépassant les capacités courantes des PC, soit au-delà d'une vingtaine de qubits, les développeurs peuvent exécuter leur code sur un simulateur Atos Quantum Learning Machine dans le cloud, mais de manière payante. Atos envisage de permettre le partage de pratiques, bibliothèques et codes d'applications quantiques. Atos propose également un des traducteurs open source de codes myQLM vers d'autres environnements de programmation quantique. En septembre 2020, cette offre logicielle devenait gratuite.

Dans cette lignée, Atos lançait en juillet 2020 le programme d'accélération **Scaler**, destiné aux startups et PME pour leur permettre d'adopter des technologies de calcul haute puissance et d'émulation de code quantique. Cela couvre aussi les solutions de sécurité et de décarbonation.

Atos s'est doté d'un conseil scientifique de compétition avec Cédric Villani, Alain Aspect, Serge Haroche, Daniel Estève, David DiVincenzo (IBM) et Artur Ekert (inventeur des clés quantiques QKD). C'est un très beau panel. Malheureusement entièrement masculin !

Toujours pour ce qui est de la France, signalons le lancement en décembre 2018 par **IBM** d'un laboratoire quantique (IBM Q Hub) à Montpellier en partenariat avec l'Université de Montpellier et avec le soutien de la Région Occitanie. Ce laboratoire dénommé QuantUM (facile à Googleizer…), c'est surtout un centre d'expertise technique pour évangéliser le marché. L'Université de Montpellier serait très active dans les communications quantiques, les capteurs et la simulation.

Conférences

Diverses conférences internationales sur l'informatique quantique ont lieu en France, soit de manière permanente, soit de manière passagère.

C'est le cas de l'**ICoQC** (International Conference on Quantum Computing) qui se tenait à l'ENS à Paris en novembre 2018[1287].

Pour mobiliser l'écosystème, **Bpifrance** organisait la **Conférence QCB** (Quantum Computing Business) le 20 juin 2019 à Paris avec un beau line-up d'intervenants dont Alain Aspect, Cédric Villani, le CEO de D-Wave, des représentants d'IBM, Rigetti, etc ainsi que les grands chercheurs et entrepreneurs français du quantique comme Maud Vinet (CEA-Leti) et Pascale Senellart (Quandela), le tout avec l'intervention de Cédric O, Antoine Petit (Président du CNRS) et Thierry Breton (Atos). L'édition suivante était planifiée le 4 novembre 2020.

[1286] En juillet 2018, Atos faisait aussi l'acquisition de Syntel pour $3,4B aux USA, un prestataire de services spécialisé dans le développement et le déploiement d'applications dans le cloud faisant $923M de CA avec 22 500 collaborateurs créé en 1980 par des Indo-Américains. Cela ne semble pas avoir de rapport avec le quantique.

[1287] Voir https://icoqc.sciencesconf.org/.

Le **CEA-Leti** organisait le 28 juin 2019 un workshop quantique à l'occasion des Leti Innovation Days (programme). Il regroupait un excellent panel de chercheurs dans la discipline, issus de nombreux laboratoires de recherche français[1288]. L'édition suivante est prévue en juin 2021, covid-19 oblige.

Des colloques scientifiques sont sinon organisés par les différents groupements comme le **PCQC** et le **GDR IFQA**, par exemple le 10e colloque de ce dernier qui avait lieu à Paris en novembre 2019 (lien). L'édition suivante est planifiée début décembre 2020 à Grenoble.

Plan quantique national

La mission parlementaire lancée en avril 2019, pilotée par Paula Forteza avec Iordanis Kerenidis (directeur de recherche au CNRS) et Jean-Paul Herteman (ex CEO de Safran) avait terminé ses auditions à la fin du printemps 2019.

Elle a remis son rapport « Quantique : le virage technologique que la France ne ratera pas » lors d'une réunion à l'Assemblée Nationale le 9 janvier 2020, avec les interventions des Ministres concernés : Bruno Lemaire (économie, en vidéo), Florence Parly (armées), Frédérique Vidéo (recherche et enseignement supérieur) et Cédric O (numérique)[1289]. Le rapport faisait une cinquantaine de propositions dont 37 étaient rendues publiques. S'en est suivi un travail d'un bon gros semestre pour la finalisation de la feuille de route de l'Etat qui devait mettre au noir des propositions et un budget opérationnels avec les parties prenantes, principalement les grands organismes nationaux de recherche (CNRS, CEA, Inria mais aussi Onera, LNE et CNES), la DGE, la DGA, le Ministère de l'Enseignement Supérieur et de la Recherche, l'ANR et Bpifrance.

Les cabinets ministériels ont ensuite réalisé les arbitrages budgétaires pour que ce plan à cinq ans puisse être annoncé aux alentours de septembre 2020.

Les ambitions affichées par le plan et par la feuille de route pourraient tourner autour des thématiques suivantes, s'inspirant du rapport parlementaire :

- **Le calcul quantique tolérant aux pannes (LSQ)**. Il s'agira d'ordinateurs quantiques disposant de milliers si ce n'est de millions de qubits exploitant des codes de correction d'erreur. En imaginant réaliser cela avec la filière des qubits silicium qui est la spécialité de Grenoble associant les laboratoires du CEA, du CNRS (surtout l'Institut Néel) et l'UGA.
- **Le calcul quantique de type NISQ**, une étape intermédiaire avant la précédente pouvant notamment s'appuyer sur la prometteuse architecture à base d'atomes froids de la startup Pasqal.
- **Les logiciels métiers**. Cela revient à créer une filière logicielle métiers et verticale sur le calcul quantique en visant la chimie, la pharmacie, les matériaux avancés, la logistique et l'apprentissage en IA.
- **Les technologies habilitantes**. Cela couvre notamment les cryostats, le contrôle du vide, les lasers et autres sources de photons, le câblage et l'électronique de contrôle des qubits. L'idée est d'éviter de se trouver bloqué par des embargos à l'export d'autres pays.

[1288] J'en ai fait un compte-rendu dans Vers une stratégie industrielle de l'informatique quantique ?, juin 2019.

[1289] Voir la conférence du 9 janvier 2020 : "Quantique : le virage technologique que la France ne ratera pas" - remise du rapport (09/01/2020) (2h33mn) et le rapport (68 pages). Et le compte-rendu que j'en avais fait alors que j'étais au CES de Las Vegas au même moment : Les ambitions de la France dans le quantique par Olivier Ezratty, janvier 2020.

- **La métrologie quantique**, notamment à base de NV Centers. C'est notamment une activité de Thales avec ses micro-magnétomètres quantiques[1290].
- **La cryptographie** qui couvre aussi bien la QKD que la PQC. Sans compter la filière plus générale des télécommunications quantiques.

Le Rapport parlementaire contenait quelques recommandations de haut niveau qui pourraient être également reprises dans le plan finalisé :

- **Créer une infrastructure de pointe pour la recherche et l'industrie**. Il s'agira semble-t-il d'un ajout de processeurs quantiques aux supercalculateurs du GENCI opéré par le CNRS à Orsay.
- **Un programme de soutien au développement technologique** couvrant un spectre large allant d'un soutien à la recherche fondamentale, à la recherche appliquée et à la valorisation, selon le degré de maturité des technologies. Les outils de financement peuvent prendre la forme d'appels à projets habituels de l'ANR, des concours d'Innovation, des Programmes Prioritaires de Recherche, des Programmes de Maturation Technologiques associant des acteurs privés, des Programmes de Développement Industriels, des Grands Défis et des bourses de thèses[1291].
- **Un environnement d'innovation efficace**. Il s'agissait de bien construire et développer les écosystèmes d'innovation et surtout les formations supérieures pour créer le pool de compétences dont les laboratoires de recherche et les entreprises auront besoin. Le Rapport préconisait le soutien des hubs quantiques qui étaient alors déjà créés à Saclay[1292] et Grenoble[1293], celui de Paris ayant vu le jour en mai 2020. En avril 2020, Bpifrance lançait avec Quantonation Le Lab Quantique qui est positionné sur l'aval de l'innovation du côté des startups et des entreprises.
- **Le développement des usages**. Il pourrait être structuré autour d'un programme financé par le PIA4 (programme d'investissements d'avenir).
- **Une stratégie de sécurité économique adaptée**. Cela a abouti à une décision de Bruno Lemaire du 9 janvier de placer les technologies quantiques dans la liste des technologies sous surveillance en cas de souhait de prise de contrôle d'entreprises françaises du secteur par des acteurs étrangers. Cela passe aussi par différents aspects du plan visant à développer ou consolider les filières françaises de technologies habilitantes clés, déjà citées.
- **Une gouvernance efficace**. C'est-à-dire, pouvoir financer ces initiatives, startups comprises, sur le long terme, et de mettre en place un groupe de coordination de l'ensemble. Affaire à suivre.

Du côté budgétaire, le plan final s'étalera sur cinq ans avec un apport public situé aux alentours du milliard d'Euros et faisant partie du plan de relance annoncé par le Premier Ministre le 3 septembre 2020 et un apport du privé et des financements européens évalué autour de 800M€. Cela fait un montant total honorable. Plus des trois quarts de ces investissements seraient véritablement incrémentaux par rapport à l'existant.

[1290] Voir Pourquoi Thalès ne jure que par le quantique par Paul Loubière, novembre 2019.

[1291] Le tout en piochant dans le PIA4, la quatrième mouture des programmes d'investissements d'avenir. Voir Un nouveau programme d'investissements d'avenir début 2020, décembre 2019.

[1292] Voir Création de Quantum, le Centre des Sciences et Technologies Quantiques de l'Université Paris Saclay, décembre 2019.

[1293] Voir le site de QuEng, le hub quantique de Grenoble.

Ce plan pourrait donc être homothétique avec celui de l'Allemagne (2Md€ sur 5 ans, semble-t-il véritablement incrémental) et les investissements du Royaume-Uni (plus de 1Md€ depuis 2013) sans compter ceux des USA (environ $2B d'incrémental sur 5 ans).

Ce plan quantique s'intègre dans un plan de relance, dénommé pacte productif avant la crise du covid-19. Ce dernier s'articulait autour d'une dizaine de marchés prioritaires proposés au Conseil National de l'Innovation (Bercy) par le rapporteur Benoit Potier (CEO d'Air Liquide) [1294]. Ces 10 marchés comprenaient 3 sur la santé, 2 sur l'agriculture, un sur les matériaux composites, un sur l'hydrogène, un sur la cybersécurité et un sur les technologies quantiques. Il se trouve que le plan quantique était le plus aboutit !

La crise du covid-19 a renforcé l'**enjeu de souveraineté** du plan quantique. Emmanuel Macron déclarait déjà que les technologies numériques étaient devenues un véritable enjeu de souveraineté, lors d'un discours auprès de France Digitale le 17 septembre 2019 à l'Elysée. Emmanuel Macron renforçait ce point lors d'un discours à l'Ecole de Guerre le 7 février 2020[1295]. Les technologies quantiques sont éminemment duales (avec usages civils et militaires) et l'autonomie stratégique les concernant est encore possible, ce qui est malheureusement plus délicat pour de nombreuses technologies numériques existantes.

L'autre attendu naturel d'un tel plan est sa **dimension européenne**. La recherche et les entreprises françaises sont déjà bien impliquées dans les projets du Quantum Flagship lancé en 2018 par l'Union Européenne. On peut bien entendu rêver de créer un Concorde ou, mieux, d'un Airbus du quantique. Pour ce faire, il faut être en position de force, disposer d'un capital humain et technologique à la hauteur, et surtout d'acteurs privés dynamiques. Avec Atos et Thales, la France n'est pas trop à plaindre du côté de ses grands acteurs technologiques du numérique par rapport au reste de l'Europe[1296].

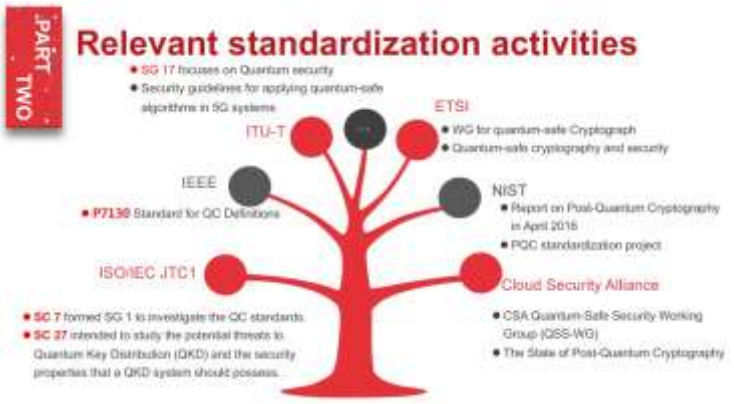
A noter que début 2020, l'**AFNOR** lançait d'ailleurs un processus de normalisation autour des technologies quantiques et en particulier autour du calcul quantique. Cela concernerait dans un premier temps la terminologie (histoire par exemple de trancher nettement sur la différence entre simulation et émulation quantiques), sur les méthodes de benchmarking et sur les questions d'interopérabilité. Les entrepries devaient donner un avis avant le 20 mars 2020. Il est probable que tout cela dure un peu plus longtemps que prévu.

[1294] Voir Remise du rapport du collège d'experts présidé par Benoît Potier "Faire de la France une économie de rupture technologique", février 2020 (116 pages).

[1295] Voir Macron : l'IA, la physique quantique et la 5G au cœur du « discours nucléaire » par Guerric Poncet dans Le Point, février 2020.

[1296] Voir le Rapport France Digitale Quantique, prêts pour le grand saut réalisé par Wavestone, octobre 2019 (23 pages). Au menu des propositions : souveraineté, collaborations européennes, encourager les investissements, développer les compétences, expérimenter, etc.

Cela doit s'intégrer dans les travaux du même domaine lancés par l'ISO., notamment dans le groupe ISO/IEC JTC 1/SG 2, JTC 1 qui avait lancé un groupe d'étude sur le calcul quantique en 2018. Ses membres initiaux sont l'Australie, le Canada, la Chine, l'Allemagne, l'Irlande, le Japon, la Corée, le Royaume-Uni et les USA. La France y est représentée par Frédéric Solbès de l'AFNOR[1297].



On peut rapidement tomber dans le pessimisme ambiant sur ce genre de plan[1298]. Nombre des plans technologiques du passé ont lamentablement échoué. Ils arrivaient trop tard, n'avaient pas de relais solides dans le privé et souvent, arrosaient de financement des projets voués à l'échec, les plus patents ayant été le plan Quaero de moteur de recherche lancé en 2005, le plan de cloud souverain lancé en 2010 et le plan objets connectés de 2014. Très souvent, on part péremptoirement du principe que l'excellence de nos chercheurs et ingénieurs doit nous octroyer une belle place au soleil dans la compétition internationale. Si cette excellence est utile, elle est largement insuffisante. Tout d'abord, elle est loin d'être exclusive. Ensuite, la réussite économique est une affaire de culture, de vélocité de création d'entreprises, de capacité à créer des produits, à les vendre, à les marketer et rapidement à l'échelle mondiale.

Dans des marchés de niche très spécialisés comme ceux des technologies quantiques, ce débat n'a pas encore vraiment lieu. Les décideurs de l'Etat se demandaient si on ne les baladait pas, notamment sur les perspectives du calcul quantique. Le paradoxe de la situation est que cette grande incertitude scientifique et technologique sur l'avènement d'ordinateurs quantiques scalables est en fait une chance. Elle laisse la porte ouverte à des réussites françaises basées sur cette excellence technologique. Si le risque n'était que marché, comme dans les services en ligne, la messe serait quasiment déjà dite.

En amont des questions de marketing, de commercialisation et d'export, de nombreuses planètes devront être alignées pour réussir dans les technologies quantiques. La première est le développement des compétences. La seconde est La capacité à gérer l'interdisciplinarité du secteur et à créer une véritable discipline d'ingénierie quantique dans les laboratoires de recherche appliquée et les entreprises.

La troisième est dans les logiciels quantiques qu'il faudra rapidement développer et au niveau des outils et plateformes que des applications métiers. L'Histoire n'est en tout cas pas encore écrite et elle sera relativement lente à émerger.

[1297] Vu dans ISO/IEC JTC 1 Quantum Computing Standardization Progress par Hong Yang, 2019 (22 slides).

[1298] En voici un exemple, pas forcément bien documenté : Physique quantique : comment la France est en train de perdre l'avance qu'elle avait par Jocelin Morisson, octobre 2019. Et un point plus neutre : L'écosystème français de l'informatique quantique : ses atouts, ses faiblesses par Sylvain Rolland, octobre 2019.

Entreprises

Cet ouvrage est destiné à un large public intéressé par le sujet de l'informatique quantique. Il comprend en particulier les entreprises qui peuvent se demander quoi faire devant un tel déluge d'informations, de complexité et d'incertitudes. Et cela s'ajoute aux autres vagues technologiques à assimiler comme l'intelligence artificielle, la Blockchain, les objets connectés et la 5G sans compter les déploiements d'applications dans le cloud qui sont loin d'être achevés.

La vague de l'informatique quantique a ceci de particulier qu'elle est encore plus imprédictible et difficile à saisir que les autres vagues du numérique. Et pourtant, elle mérite bien l'attention des entreprises, en particulier dans certains secteurs clés comme la finance, la santé, les transports et tout ce qui relève du régalien.

Je propose une approche relativement simple et somme toute assez classique que voici, en une douzaine de points, certains provenant de l'expérience de grandes entreprises françaises.

Veille technologique

- Comprendre la **dimension technologique** des ordinateurs quantiques et des questions de cryptographie associées. La lecture de cet ouvrage peut aider. De nombreux autres supports de vulgarisation sont disponibles en formats texte[1299] et vidéo[1300].
- Apprendre à **décoder les annonces** des laboratoires de recherche et fournisseurs. Je fournis quelques exemples dans cet ebook, au sujet notamment du fait que le calcul quantique n'est pas une solution miracle qui peut accélérer tous les traitements informatiques. De même, ce n'est pas une voie naturelle pour les applications de big data.
- Comprendre ce que l'on peut faire avec les **algorithmes quantiques** en consultant les parties de cet ebook sur les algorithmes et les applications métiers classées par marché vertical. Si votre marché n'y est pas, cela ne veut pas forcément dire que vous n'êtes pas concerné.
- Participer aux **événements de l'écosystème** comme les meetups de Quantonation, la conférence QCB de Bpifrance ou les conférences organisées par les chercheurs (CNRS, CEA-Leti, LIP6, PCQC, etc).
- En plus de cet ebook, vous pouvez exploiter une version simplifiée sous la forme du **livre blanc du CIGREF** publié début 2020[1301].

[1299] Voir par exemple Pédagogie sur l'informatique quantique : L'ordinateur quantique : tout comprendre en partant de zéro, décembre 2016 qui est assez bien fait.

[1300] J'assure de mon côté une formation de découverte de l'informatique quantique d'une journée qui est proposée dans le catalogue de Capgemini Institut. Voir le synopsis et les dates.

[1301] Ce livre blanc a été concocté par Frédéric Lau « Informatique quantique – Comprendre le quantum computing pour se préparer à l'inattendu », février 2020 (40 pages). Il est mieux documenté que nombre de livres blancs de cabinets d'analystes comme Quantum Computing : A technology for the future already present, PwC, 2019 (22 pages) qui est vraiment très sommaire.

Analyse des besoins

- Identifier les **problèmes de nature exponentielle** dans le portefeuille applicatif de l'entreprise. C'est une question à laquelle les développeurs et les data scientists peuvent répondre. Ce sont par exemple les problèmes d'optimisation complexe impliquant l'orchestration de nombreuses ressources.
- Créer une **communauté interne** d'ingénieurs et spécialistes métiers autour des technologies quantiques comme l'ont par exemple fait Airbus et la BNP.
- Lancer une cartographie de l'usage de **protocoles de sécurité** menacés par les ordinateurs quantiques à une échéance imprécise. Quelles sont les données du présent dont le piratage dans le futur pourrait poser un problème de confidentialité à l'entreprise ? Si les données du présent ont de la valeur dans plus de 5 ans, il faut commencer à s'inquiéter et s'intéresser à la QKD et à la PQC.
- Impliquer les **RSSI** dans les processus de standardisation de nouvelles clés publiques résilientes au quantique (post-quantum cryptography). Une entreprise seule n'imposera pas un standard de cryptographie post-quantique mais les grandes entreprises ont chacune un rôle d'influence dans leur marché vertical.

Formation

- Former **quelques développeurs** à la programmation quantique. Cela peut se faire en laissant les gens intéressés par le sujet y consacrer du temps par leurs propres moyens. L'information et les outils sont disponibles en ligne comme chez IBM ou Microsoft. Les outils open source en cloud sont déjà là. Les plus jeunes seront probablement ceux qui s'adapteront le mieux aux méthodes de programmation du calcul quantique qu'il est difficile d'assimiler lorsque l'on a été formatté à la programmation classique[1302].
- Comprendre les liens entre le **calcul quantique et l'intelligence artificielle**. Le « quantum machine learning » est une nouvelle sous-discipline de l'algorithmie quantique qui mérite d'être explorée et comprise.

Evaluation

- Tester **quelques algorithmes** dans le cloud avec des ordinateurs quantiques universels (IBM, Rigetti) ou à recuit quantique (D-Wave) ou avec des émulateurs à base de supercalculateurs (Atos, IBM, Microsoft, Google). Les études de cas disponibles sont évoquées dans cet ebook dans la partie sur les algorithmes et sur les applications par marchés.
- Ne pas hésiter à tester des algorithmes sur les **ordinateurs à recuit quantique** de D-Wave malgré leur relative mauvaise image chez les puristes du calculateur quantique universel. C'est autour de cette société que les premiers éditeurs de logiciels quantiques comme le Canadien 1Qbit gravitent. Les algorithmes quantiques pour ces ordinateurs sont adaptés à la résolution de problèmes d'optimisation complexes et représentent une bonne part de ce que peut apporter le calcul quantique, que ce soit en biologie ou dans la finance pour ne prendre que deux exemples.

Bravo, vous avez ainsi économisé une étude de McKinsey ou du BCG !

[1302] Petite publicité : je propose une journée de séminaire de découverte de l'informatique quantique, notamment chez CapGemini Institut. Voir l'agenda et le programme.

Société

Nous allons ici quitter les mathématiques, les algorithmes, les logiciels et la physique pour nous intéresser aux liens entre le quantique et la société. Ceux qui avaient du mal à digérer les éléments scientifiques de l'histoire vont pouvoir respirer !

Nous sommes encore aux tous débuts de l'Histoire. Ce qui va suivre est un mélange d'observations et d'interpolations. Comme toute vague technologique du numérique, celle du quantique touchera la société et les industries à plusieurs niveaux dont certains peuvent être anticipés.

Je vais tour à tour, m'intéresser à l'ambition humaine associée au quantique, au rôle de la science-fiction dans la contruction de l'imaginaire quantique, de la philosophie de la physique quantique, à la manière dont les religions et le spirituel s'approprient le quantique, à l'éthique des usages du calcul quantique, à l'éducation et la formation à l'informatique quantique, au rôle des femmes dans le secteur et au marketing du quantique par les fournisseurs.

Ambition humaine

L'informatique quantique est facilement présentée au grand public comme apportant une capacité de calcul défiant l'entendement allant au-delà de ce tout ce que l'on faisait jusqu'à présent. L'informatique quantique serait donc le moyen de détourner ou de provoquer la prolongation de l'application empirique de la loi de Moore. Elle permettrait d'entretenir l'exponentialité éternelle des technologies. Cela peut donner l'impression qu'avec l'informatique quantique, l'Homme va disposer d'un outil lui apportant une puissance infinie et un contrôle total de l'information, dans la lignée de nombreux mythes construits autour de l'intelligence artificielle et de sa destinée ultime, l'intelligence artificielle générale (AGI). En 2018, le physicien et auteur futuriste américain **Michio Kaku** prévoyait que les calculateurs quantiques seront les ordinateurs ultimes capables de dépasser l'intelligence humaine[1303]. C'est reparti de plus belle dans le n-importe-quoi-isme !

L'intelligence artificielle et l'informatique quantique semblent ne pas avoir de bornes. Elles illustrent cette volonté de puissance et d'omniscience de l'Homme, de modeler la matière si ce n'est les esprits et de disposer d'une capacité à prévoir le futur, quasiment à le rendre déterministe. A tel point que ce serait l'abandon du libre arbitre[1304].

A elle toute-seule, la physique quantique a généré son lot de questionnements et de certitudes sur la nature du monde. L'indéterminisme de la mesure de l'état des quantums est devenu celui de la vie. L'intrication quantique a fait germer des explications pseudo-scientifiques de la télékinésie et de la transmission de pensée. Nous verrons dans la partie suivante comment la médecine quantique mélange le nano et le macro de manière quelque peu cavalière.

[1303] Voir The World's Most Disruptive Technology (That No One Is Talking About), Part II. par Ian Connett, 2018.

[1304] Comme le laisse entendre cet article de The Atlantic de juin 2018, dont le titre n'a d'ailleurs pas un grand rapport avec le contenu !

La nature mécanique ou pas de la conscience est en jeu. Pour l'**épiphénoménisme** (définition), notre conscience est le résultat de phénomènes physiques dans notre corps et notre cerveau mais sans effets physiques externes directs. Le comportement est le résultat de l'action du cerveau sur les muscles.

Pour le **mystérianisme**, la compréhension de la conscience est hors de portée de l'Homme. Comme la conscience dépend à bas niveau de phénomènes quantiques qui régissent a-minima les relations entre atomes des molécules de notre cerveau, certains en déduisent un peu rapidement que l'informatique quantique permettrait à l'IA de devenir générale comme dans ce débat ! Mais ce ne sont à ce stade que des élucubrations.

Là-dessus, des projets ambitieux comme le **Human Brain Project** européen piloté par le Suisse Henri Markram visent à simuler dans un ordinateur le comportement du cerveau et donc à en comprendre le fonctionnement de bout en bout, même si ce n'est pas envisageable de le faire à une échelle ne serait-ce que moléculaire. Dans une autre veine, la capacité des ordinateurs quantiques de simuler des phénomènes quantiques a aussi entretenu l'idée que nous étions des objets d'une grande simulation. Une idée qui fait fi des contraintes de dimensionnement des traitements à réaliser.

Une exploration des arcanes du calcul quantique et des théories de la complexité permet de remettre les pieds sur Terre. Les théories de la complexité décrivent diverses limites à la nature des problèmes qui peuvent être résolus avec l'informatique quantique. La toute-puissance calculatoire n'existe pas encore. On sera toujours obligé d'utiliser diverses formes de réductionnisme pour simuler le monde, à savoir qu'on ne pourra le faire correctement qu'à des échelles "macro" et pas "micro" ou "nano" pour des questions d'ordre de grandeur de calcul. Un peu comme on prédit la météo grâce à la méthode des éléments finis applicable à de grandes portions de ciel et pas au niveau de chaque molécule d'eau.

Les limites du possible seront sans cesse repoussées mais elles subsisteront. Tout comme celles de la compréhension du monde qui se heurtent aux limites temporelles et spatiales de l'Univers. On ne pourra probablement pas savoir ce qui se passait avant le big bang ni évaluer l'existence de multivers[1305]. Etant non vérifiables, ces interprétations du monde ne peuvent rester que des spéculations et pas devenir de véritables sciences. De même, nos moyens physiques ne permettront probablement jamais de simuler notre monde in-extenso.

La physique quantique introduit aussi beaucoup de chaos et de l'aléatoire dans le biologique qu'aucun ordinateur ne pourra jamais entièrement simuler et contrôler. Finalement, cette citation de Scott Aaronson résume bien d'ailleurs la quête du calcul quantique. Celle-ci serait justifiée par la volonté de contrer ceux qui disent que c'est impossible. Le reste étant la cerise sur le gâteau[1306]. C'est évidemment un trait d'humour à prendre au second degré !

"For me, the single most important application of a quantum computer is disproving the people who said it's impossible. The rest is just icing on the cake"
Scott Aaronson

source : A tale of quantum computers de Alexandru Gheorghiu (131 slides)

[1305] Voir Les limites de la connaissance en physique par François Vannucci, juin 2020.

[1306] La citation provient de A tale of quantum computers de Alexandru Gheorghiu (131 slides, slide 31). Pour en savoir plus sur ces débats, voir notamment Quantum Darwinism, Decoherence, and the Randomness of Quantum Jumps de Wojciech Zurek, 2014 (8 pages), The Combination Problem for Panpsychism de David Chalmers (37 pages) et Why Philosophers Should Care About Computational Complexity de Scott Aaronson (59 pages) ?

Science-fiction

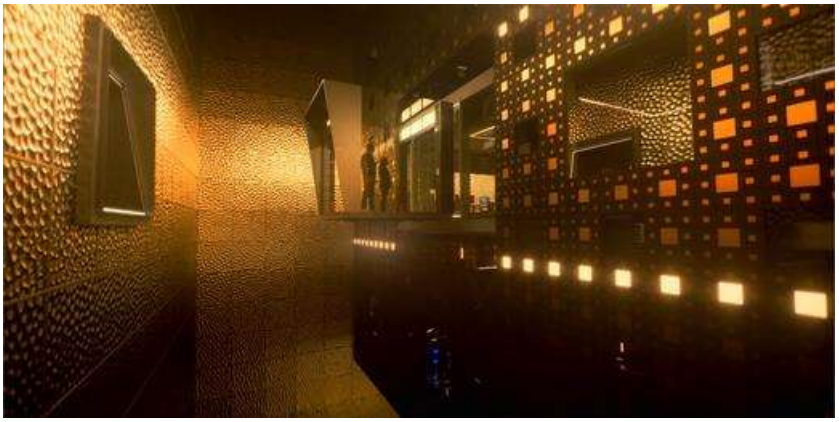
La science-fiction et surtout la production cinématographique et télévisuelles ont été de grandes source d'inspirations et aussi de délires sur le potentiel des technologies quantiques. Ils ont créé un imaginaire fait de téléportation (**Star Trek**), de vitesse supraluminique (**Star Trek**, **Star Wars**), d'intrications diverses et de miniaturisation (comme dans **Ant Man**[1307]), de la superposition d'états (**Coherence**), de mondes parallèles ou multiverses (**Fringe**, **Spiderman**) ou de remontées dans le temps (**Interstellar**).

Dans certains cas, le terme quantum est utilisé sans rapport scientifique avec la physique quantique, comme dans le James Bond **Quantum of Solace** de 2013 qui signifie approximativement « une once de consolation » proche en pratique de zéro.

Ou alors, il joue le rôle du « MacGuffin », popularisé par le réalisateur **Alfred Hitchcock**, le bidule que les protagonistes vont chercher d'un bout à l'autre du film sans que l'on sache vraiment ce qu'il contient. C'est le cas de la malette du film **Ronin**. On en retrouve un dans le film **Hard Kill** avec Bruce Willis lancé en février 2020. Des méchants cherchent à récupérer « le code » qui permettra d'activer une « quantum AI », mais ses contours sont bien flous. On sait juste qu'elle pourrait éventuellement faire des choses « en bien » tout comme hacker un avion de ligne pour le faire s'écraser. Bref, c'est une banale solution « duale » civile et militaire. Les balles vont pleuvoir jusqu'à la mort du méchant sans que l'on sache vraiment de quoi il s'agit. Donc, aucune prétention scientifique !

Il existe cependant un petit guide de 11 pages pour expliquer la physique quantique aux scénaristes[1308]! Il contient quelques rudiments de langage exploitables pour la création de scripts. Cela ne casse pas trois briques. Les scénaristes habituels n'hésitent pas à jouer hors des clous, comme **Christopher Nolan** avec sa vision très élastique de la flèche du temps dans Interstellar ou Tenet.

Plus récemment, en mars 2020, la mini-série TV **Devs** en huit épisodes était la première à être articulée autour des prouesses d'un ordinateur quantique capable de reconstruire le passé jusqu'à la crucifixion du Christ et de prévoir le futur partout sur Terre. Et en images ! N'y allons pas par quatre chemins : cette prouesse n'est pas réalisable[1309].



[1307] Voir 'Ant-Man' science adviser explains the real-life physics behind the film par Denise Chow, juillet 2018, qui explique les liens entre la physique quantique et le scenario du dernier Ant Man. Bon, sachant qu'il n'y en a pas pour agrandir ou miniaturiser un personnage.

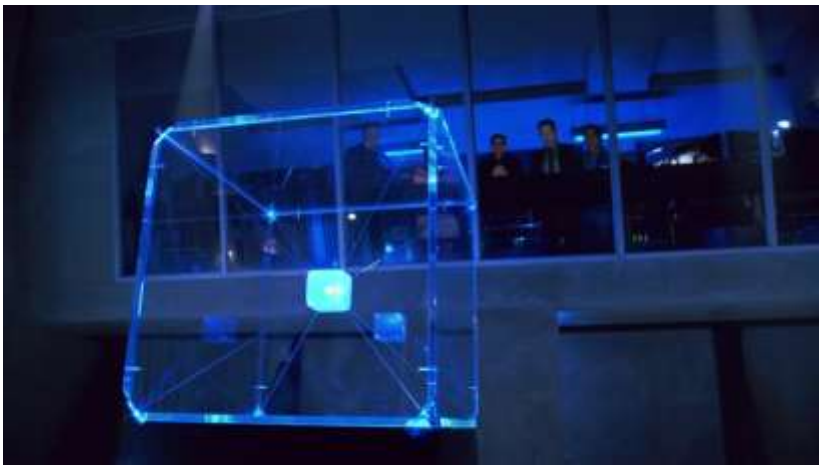
[1308] Voir The Sci-Fi Writer's Guide to Quantum Physics par Radha Pyari Sandhir, 2019 (11 pages).

[1309] L'ordinateur quantique stylisé comprend un chandelier allongé qui ressemble à ceux des ordinateurs quantiques d'IBM et de Google. Il n'est connecté à rien du tout par le haut, mais ce n'est pas grave ! L'ensemble est enfermé dans un énorme cube suspendu et isolé magnétiquement. Voir cette belle analyse de la série : « Devs » d'Alex Garland : un thriller quantique dans la Silicon Valley par Romane Mugnier dans Usbek&Rica, mai 2020.

Avec les technologies d'aujourd'hui, mais aussi avec celles de demain. C'est un problème de niveau de complexité. Même en supposant que le fonctionnement de l'Univers est totalement déterministe, il est impossible de capter la position précise de toutes les particules dans l'espace pour déterminer leur passé et leur futur.

D'ailleurs, cela se heurte à l'un des principes clés de la physique quantique : le principe d'indétermination d'Heisenberg qui veut que l'on ne puisse pas capter avec précision la position et la vitesse d'une particule élémentaire. A partir de là, tout tombe à l'eau pour modéliser et simuler le monde avec précision !

En 2015, l'épisode 11 de la saison 2 de **Scorpions** mettait en scène un ordinateur quantique fait de lasers et d'un grand cube en plexiglass et capable d'injecter un ransomware dans la banque fédérale des USA, avec seulement 4 qubits ! En voilà une belle performance ! Les héros hackent l'ordinateur habillé de tenue de cosmonaute en réorientant le rayon d'un des lasers vers le cube lumineux.



Ces rêves de science-fiction sont très éloignés de la science d'aujourd'hui et probablement de demain. Leur bénéfice est de créer des vocations. Rêver permet d'innover. Même lorsqu'un jeune découvre que la science ne permet pas de réaliser les scénarios de ces fictions, ils peuvent découvrir le champ infini des applications de la physique quantique.

L'usage de la physique quantique dans les films d'Hollywood peut aussi servir à faire passer d'autres messages. Ils peuvent comme souvent agiter le potentiel d'une menace externe contre laquelle l'Amérique pourrait se mobiliser. Il ne serait pas étonnant que l'on voie émerger des fictions où la menace quantique vient de Chine. Ces films illustrent souvent le mythe du héros qui peut traverser les épreuves, illustration à la fois du chacun pour soi et d'une alternative aux pouvoirs centraux des gouvernements[1310].

Dans les romans, la fiction peut avoir aussi des vertus pédagogiques. C'est dans une certaine mesure le cas de **La clé de Salomon**, un roman du portugais José Rodrigues Dos Santos paru en 2015. Dans une affaire mêlant espionnage et informatique quantique, le héros passe son temps à faire des cours de physique quantique aux autres protagonistes de l'histoire. Cela fait passer les messages de manière didactique et sans trop écorcher la science.

[1310] Voir Quantum Computing, Hollywood and geopolitics par Jean-Michel Valentin, mars 2019. L'auteur est un français spécialiste des études stratégiques, de la sociologie de la défense et de la stratégie américaine. L'article s'appuie beaucoup sur le film Mortal Engines (2018) dont le scénario ne met en valeur le quantique que de manière indirecte, avec une guerre quantique passée qui a ravagé la planète.

Philosophie de la physique quantique

La philosophie est une démarche de réflexion critique et de questionnement sur le monde, la connaissance et l'existence humaines. Elle crée un ciment entre tous ces éléments. Par les bouleversements qu'elle a apportés dans la compréhension du monde au niveau microscopique[1311], la découverte de la physique quantique aux débuts du 20e siècle a créé une véritable onde de choc philosophique. Elle remettait en question des notions clés comme les notions de réalité et d'observation.

La science a toujours été étroitement liée à la philosophie. Ce n'est pas par hasard si un doctorat est un « PhD », ou doctorat en philosophie, que ce soit dans les sciences humaines ou les sciences dites dures ou exactes, et qui ne sont d'ailleurs ni l'une ni l'autre en pratique. Les grands physiciens et mathématiciens du 19e et des débuts du 20e siècle étaient aussi des philosophes, ce qui est moins courant maintenant, du fait d'un processus d'accélération de la spécialisation et du rangement des métiers dans des cases.

Les créateurs de la physique quantique questionnaient sans cesse l'impact et le sens de leurs découvertes. **Niels Bohr** était aussi à la fois physicien et philosophe, influencé notamment par **Søren Kierkegaard** (1813-1855, Danois). **Erwin Schrödinger** était même plus philosophe que physicien. Il avait étudié la philosophie occidentale et indienne avant de créer la fameuse fonction d'onde qui porte son nom et reste l'une des bases de la physique quantique non relativiste[1312]. Assistant de Niels Bohr, **Werner Heisenberg** avait aussi beaucoup investi de son temps dans la philosophie et ses travaux autour de la modélisation mathématique de la physique quantique et de la fameuse indétermination s'y prêtaient bien.

Les débats qui agitaient les physiciens de la mécanique quantique prenaient souvent autant la forme de joutes philosophiques que de débats physiques ou mathématiques, ce d'autant plus que les fondateurs de la physique quantique n'étaient pas des expérimentateurs et étaient plutôt des théoriciens[1313]. L'Histoire a d'ailleurs bien moins retenu le nom de ces derniers[1314].

[1311] En pratique, ces bouleversements se manifestent surtout à l'échelle nanoscopique, celle des atomes et de leurs constituantes, les noyaux et les électrons. Les effets quantiques son cependant également observables à l'échelle de grands groupes de particules pouvant être microscopiques, comme c'est le cas avec de grandes molécules et leur dualité onde-particule, dans les condensats de Bose-Einstein ou les courants supraconducteurs. Sachant dans tout cela que la frontière entre physique quantique et physique classique a régulièrement évolué depuis un siècle.

[1312] Michel Bitbol indique que dans l'épilogue de « What is life ? Mind and matter », Erwin Schrödinger se demandait si la conscience était singulière ou plurielle. Si la conscience n'est qu'éprouvée au singulier, son extension à une conscience globale comme celle de l'Univers n'est qu'une extrapolation risquée et difficile à prouver expérimentalement. La thèse d'une conscience de l'Univers est défendue par certains scientifiques. Voir par exemple Is the universe conscious? It seems impossible until you do the maths par Michael Brooks, avril 2020 qui fait référence aux travaux de mathématiciens allemands qui tentent de définir mathématiquement la notion de conscience, leur permettant de l'appliquer ensuite à l'univers dans son ensemble. Les détails sont dans The mathematical structure of integrated information theory par Johannes Kleiner et Sean Tull, 2020 (22 pages). C'est froid et abstrait !

[1313] Un ouvrage récent en atteste : Fantaisies quantiques - dans les coulisses des grandes découvertes du xxe siècle par Catherine d'Oultremont et Marina Solvay, 464 pages (2020), qui raconte notamment les dessous de la fameuse conférence Solvay de 1927. C'est en fait une très belle histoire de la mécanique quantique qui dresse des portraits touchants de ses différents protagonistes de la première moitié du XXe siècle.

La physique quantique génère des débats sans fin depuis ses débuts car son formalisme est difficilement associable aux principes de réalité habituellement applicables en physique classique. Dans la physique newtonienne, la notion d'état avec position et mouvement d'un objet et les lois d'évolution de ces propriétés permettent la prévision des phénomènes comme le mouvement des planètes. Ces évolutions sont parfaitement observables et déterministes.

En physique quantique, l'instrument de prédiction est une fonction d'onde probabiliste difficile à appréhender.

Elle est couplée à tout un tas de notions nouvelles qui n'ont pas d'équivalents dans le monde macroscopique et classique : la quantification de l'énergie, la dualité onde et corpuscule qui s'applique aussi bien à la matière (électrons, atomes) qu'aux photons (qui ont un moment cinétique), l'influence de la mesure sur les grandeurs à mesurer[1315], l'indétermination de la mesure et la notion de hasard. Werner Heisenberg affirmait même en 1927 que la mécanique quantique établissait l'échec final de la causalité !

La connaissance du présent ne permettait plus de prédire le futur à partir de l'application des lois de la physique, ce d'autant plus que la connaissance du présent avec précision est aussi impossible[1316].

On en vient à débattre de la relation entre données à mesurer, mesure et observateur. Est-ce qu'une véritable mesure serait celle qui ne modifie pas du tout la grandeur à mesurer, une prouesse quasiment inaccessible dans l'infiniment petit ? En fait, la mécanique quantique est contextuelle, la mesure dépendant de son contexte, ce qui n'enlève rien à son objectivité[1317]. Là-dessus s'ajoutent la superposition des états, l'intrication et la notion de non-localité, ces deux dernières ayant été vérifiées expérimentalement assez tardivement, en 1982[1318].

Le formalisme mathématique de la physique quantique des années 1900 à 1935 n'était pas déconnecté du monde physique observable. Il permettait d'expliquer des phénomènes étudiés de manière expérimentale comme le rayonnement du corps noir, les interférences des fentes de Young ou encore les raies spectrales d'excitation d'atomes dans de très nombreuses conditions.

Nous avons vu à quel point elles étaient importantes dans la photonique, avec les NV centers, les ions piégés et les atomes froids. Le spin des électrons expliquait les niveaux d'énergie hyperfins d'atomes observés en 1922 dans l'expérience de Stern-Gerlach[1319].

[1314] Nous en avons cité un bon nombre au début de cet ebook comme Johann Balmer, Theodore Lyman, Friedrich Paschen, James Chadwick, Arthur Holly Compton, George Paget Thomson, Clinton Davisson et Lester Germer. Les noms de ces physiciens expérimentalistes ne sonnent généralement pas aux oreilles du grand public généraliste et scientifique alors qu'il a bien plus souvent entendu parler de Planck (avec sa constante plus qu'avec le corps noir), Einstein (pour la relativité plus que pour l'effet photoélectrique), Bohr (pour son modèle de l'atome), Schrödinger (grâce à son chat plus qu'à son équation) et Heisenberg (pour son principe d'indétermination, couramment appelé d'incertitude).

[1315] Cela n'est pas valable que dans la physique quantique et l'infiniment petit. Cela fonctionne régulièrement à l'échelle macro, comme dans n'importe quel sondage aux questions biaisées par exemple.

[1316] "*In the strong formulation of the causal law, 'If we know the present with exactitude, we can predict the future,' it is not the conclusion, but rather the premise that is false. We cannot know, as a matter of principle, the present in all its details.*" vu dans One Thing Is Certain: Heisenberg's Uncertainty Principle Is Not Dead, par Ava Furuta dans Scientific American, 2012.

[1317] Cette approche est contestée par l'interprétation quantique bayésienne (QBism pour Quantum Bayesianism) promue à partir de 2002 par Carlton Caves, Christopher Fuchs, Rüdiger Schack puis David Mermin. Voir notamment QBism The Future of Quantum Physics par Hans Christian von Baeyer, 2016 (268 pages).

[1318] Ecouter à ce sujet Philosophie de la physique quantique avec Michel Bitbol, sur France Culture, avril 2017 (55 minutes). Il est l'auteur de l'ouvrage de référence Mécanique quantique, une introduction philosophique, 2008 (474 pages). Entendre aussi Michel Bitbol, Thibaut Gress et Katia Kanban - Physique quantique et philosophie de la conscience, 2017 (2h12), Michel Bitbol Science et Métaphysique Le Cas de la Théorie Quantique, 2019 (1h51) et Michel Bitbol – Bohr's Complementary and Kant's Epistemology, 2014 (59 minutes).

[1319] Celle-ci faisait passer un faisceau d'atomes d'argents chauffés au travers d'un champ magnétique non homogène, ce qui générait deux tâches distinctes sur un écran.

La chimie quantique relativiste issue des équations de Paul Dirac expliquait des décalages spectraux de transitions impliquant des électrons de couche basse d'atomes lourds se déplaçant à des vitesses relativistes. La liste est longue.

Si la physique quantique expliquait des mesures expérimentales, reliant bien le réel observé et la théorie, elle était cependant insuffisante pour produire une représentation unanimement acceptée de la réalité. Elle s'inscrit dans une histoire des sciences qui a décrit la matière étape par étape, par poupées russes imbriquées. Les atomes étaient au départ des entités abstraites, théoriques avant d'être incarnées et décrites avec précision et ensuite, observées directement comme on le fait maintenant avec les microscopes électroniques ou la microscopie cryogénique (Cryo-EM). L'existence même des atomes faisait débat à la fin du XIX^{e} siècle opposant Ludwig Boltzmann qui y croyait et Wilhelm Ostwald ainsi que Ernst Mach qui s'y opposaient.

On a ensuite découvert les protons et les neutrons. On a décortiqué ces derniers en quarks et gluons avec les accélérateurs de particules, à croire que le monde réel n'est qu'une fractale sans fin. Les obstacles à sa compréhension pourraient être simplement liés à l'énorme quantité d'énergie qu'il faut injecter dans les accélérateurs de particules et qui va croissante, plus les particules sont élémentaires.

La philosophie de la physique quantique se focalise essentiellement sur les interprétations multiples possibles des mêmes théories. Elles posent toutes des questions voisines comme : la réalité existe-t-elle indépendamment de l'observateur ? Quelle est la signification physique de l'onde dans la dualité onde-corpuscule notamment pour ce qui est des électrons ? Est-ce une onde réelle de nature indéterminée ou bien un simple modèle mathématique statistique et probabiliste incomplet dans sa capacité à décrire la réalité physique [1320]?

Plusieurs interprétations de la physique quantique ont ainsi vu le jour pour tenter d'expliquer cela :

- L'interprétation dite de **Copenhague**, essentiellement ondulatoire et probabiliste et pour qui la mécanique quantique décrit ce que nous pouvons connaître de la réalité mais pas la réalité en elle-même qui n'est pas accessible ni n'a de sens. Elle adopte l'approche positiviste selon laquelle on s'en tient aux observations, lois et phénomènes, sans chercher à connaître leur nature intrinsèque. Elle était le versant « Bohrien » du débat historique entre Niels Bohr et Albert Einstein, s'étalant principalement entre 1927 (la fameuse conférence Solay de Bruxelles) et 1935 (le paradoxe EPR). Adoptée par Werner Heisenberg, Max Born, Wolgang Pauli, Paul Dirac ainsi que par Louis de Broglie, c'est l'interprétation classique et dominante de la physique quantique qui est encore majoritairement enseignée. Elle se satisfait d'un modèle essentiellement mathématique et probabiliste qui ne cherche pas à décrire physiquement l'intégralité du monde réel. Il existe d'ailleurs des sous-courants dans la branche de Copenhague, notamment autour des théories ouvertes et fermées qui avaient opposé Heisenberg et Dirac à partir de 1929.

[1320] Ces différentes interprétations peuvent être évaluées selon les critères de scientificité de Karl Popper (1902-1994, Autrichien/Anglais), selon lesquels une théorie est scientifique si elle est réfutable par des expériences cruciales et donnant des résultats précis. Sachant que l'on ne peut pas démontrer qu'une théorie est inréfutable. Une théorie scientifique éprouvée est donc toujours entre deux eaux, à l'état de théorie corroborée par les faits, jusqu'à la preuve du contraire. L'histoire de la physique a cependant démontré que les théories « sérieuses » du passé étaient surtout remises en cause par l'élargissement de leur perspective et de leur contexte : avec de grandes masses et de grandes vitesses (pour la relativité) et dans le microscopique (pour la physique quantique). Dans leurs contextes initiaux, elles restaient parfaitement valables. J'aime bien l'exemple très actuel de la recherche de matière noire qui représenterait 85% de celle de l'Univers. Son existence n'est pas encore démontrée expérimentalement mais supputée par l'application des lois de la gravité et de la relativité appliquées à la cohésion des galaxies. On peut la réfuter ou la vérifier partiellement actuellement d'au moins trois manières : en découvrant des particules élémentaires associées à la matière noire (des détecteurs… quantiques sont construits dans ce sens, et n'ont pour l'instant rien donné), en modifiant à la marge les lois de la relativité générale comme cherche à le faire l'Israélien Morchedai Milgrom, ou en découvrant de la matière cachée comme la poussière des galaxies qui pourrait expliquer toute ou partie de leur cohésion sans faire appel à de la matière noire. La croyance en Dieu et de nombreux domaines de la métaphysique ne font pas partie des sciences car ils ne sont ni démontrables ni réfutables. Voir à ce sujet l'intéressant débat entre André Comte-Sponville et Jean Staune dans André Comte-Sponville - Jean Staune : la science va-t-elle réfuter l'athéisme ?, juin 2007, où quelques allusions sont faites à la physique quantique.

- L'interprétation de **David Bohm** (1917-1992, Américain puis Brésilien et Britannique) qui proposa en 1952 une version déterministe de la mécanique quantique, dite « théorie De Broglie – Bohm ». Elle s'inspirait d'idées promues initialement - mais rapidement abandonnées - par le physicien français et reprenait l'idée de l'existence de variables cachées, évoquée par Albert Einstein lors des années 1930, et sous la forme « d'ondes pilotes »[1321]. L'existence de variables cachées a pris du plomb dans l'aile en 1982 avec la fameuse expérience d'Alain Aspect. Mais les promoteurs de la théorie Bohmienne sont toujours très actifs, y compris en France.
- L'interprétation de la fonction d'onde de l'Univers d'**Hugh Everett** (1930-1982, Américain), proposée en 1957 et complétée par Bryce DeWitt en 1970 pour devenir l'interprétation des mondes multiples ou des multivers dans un article publié dans Physics Today[1322]. Elle est dite réaliste. Pour l'interprétation d'Everett, l'Univers est une énorme fonction d'onde avec un grand nombre de paramètres. Elle ne s'écrase jamais et le monde est déterministe. Elle suffit à décrire la réalité. L'interprétation de DeWitt transforme les probabilités quantiques en mondes parallèles qui existeraient simultanément. Mais comme il est impossible de vérifier qu'il existe des mondes parallèles, la théorie n'est pas réfutable à ce stade. On est donc loin d'une interprétation étayable expérimentalement[1323]. Cette théorie a aussi été promue par David Deutsch, aussi connu pour l'algorithme quantique qui porte son nom, avec celui de Richard Josza.

  De quoi, en tout cas, alimenter nombre de rêves de la science-fiction et aussi de mysticisme forcené, tout étant lié à tout et réciproquement, notamment les âmes et consciences[1324].

caractéristique	interprétation orthodoxe	interprétation bohmienne	interprétation everettienne
entités composant le monde	systèmes quantiques avec objets macroscopiques	fonction d'onde et positions des particules	fonction d'onde avec mondes quasi-classiques
déterminisme	indéterministe	déterministe	déterministe
interprétation des probabilités	objective	épistémique	objective
objet des prédictions de la théorie	résultats de mesures (toute observable)	positions des particules	paris des agents
localité	non-locale	non-locale	locale
formulation mathématique de la théorie	éq. de Schrödinger, postulat de projection et règle de probabilité	éq. de Schrödinger et équation guidante	éq. de Schrödinger

- On peut y ajouter la théorie dite **GRW** pour Ghirardi–Rimini–Weber, publiée en 1986, qui propose une formulation différente de l'équation de Schrödinger avec une réduction spontanée de la fonction d'onde qui ne soit pas simplement liée à la notion de mesure.

En complément, l'ontologie[1325] ou **modèle CSM** proposée par Alexia Auffèves et Philippe Grangier à partir de 2014, vise la réconciliation entre l'interprétation de Copenhague et les modèles réalistes[1326].

[1321] L'approche Bohmienne est bien vulgarisée dans Quantum Physics Without Quantum Philosophy par Detlef Dürr, Sheldon Goldstein et Nino Zanghì, 2013 (304 pages).

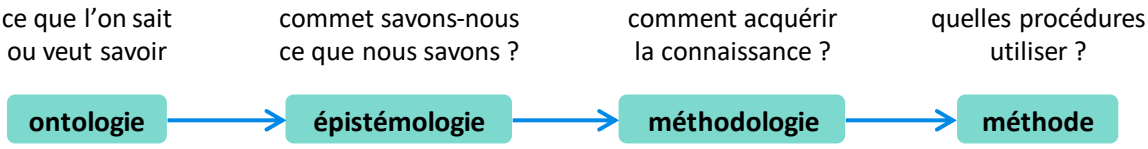
[1322] Voir Quantum mechanics and reality par Bryce S. DeWitt, 1970 (6 pages) ainsi que The Many-Worlds Interpretation of Quantum Mechanics par Bryce DeWitt et Neill Graham, 1973 (146 pages) qui contient "The theory of the universal wave function" par Hugh Everett, 1957. L'interprétation de DeWitt est aussi dénommée EWG pour Everett-Wheeler-Graham. John Wheeler était superviseur de la thèse de High Everett et Neill Graham, un étudiant de DeWitt. Vu dans Everett's pure wave mechanics and the notion of worlds par Jeffrey A. Barrett, 2011 (27 pages).

[1323] Voir Making Sense of the Many Worlds Interpretation par Stephen Boughn, 2018 (36 pages) qui démonte un peu le modèle des univers parallèles, notamment en termes de dimensionnement. En faisant le calcul sur le nombre de bifurcations de l'Univers depuis sa naissance, et en prenant le temps de Planck comme base, on aboutit à un nombre de mondes parallèles qui dépasse l'entendement et toutes les analogies imaginables. Quant au chat de Schrödinger, le chat mort et le chat vivant cohabitent dans deux mondes parallèles et l'affaire est réglée !

[1324] Source du schéma, l'excellente thèse La pluralité des interprétations d'une théorie scientifique : le cas de la mécanique quantique par Thomas Boyer-Kassem, 2011 (289 pages).

[1325] L'ontologie traite de ce qui est, des types et des structures d'objets, des propriétés, des événements, des processus et des relations dans tous les domaines de la réalité. Elle précède l'épistémologie qui couvre la manière d'obtenir des connaissances valides.

Les états quantiques sont attribués à un système et à un contexte, en prenant comme exemples les différentes modèles de mesure de la polarisation de photons (à 0/90° et 45°/135°) et de spins d'électrons (angle différent du magnétisme) mais en minimisant l'appel aux mathématiques dans l'argumentation. Le modèle CSM vise à pacifier quelque peu ces débats anciens. Alain Aspect juge que cette interprétation est très proche de celle de l'Ecole de Copenhague.



Parmi les physiciens ayant contribué au champ de la philosophie de la physique quantique, nous avons notamment **Pascual Jordan** (1902-1980, Allemand) sur sa théorie du libre arbitre selon laquelle on n'est pas plus libre en agissant au hasard ou de manière déterminée, cassant l'idée que le non déterminisme quantique serait une preuve du libre arbitre humain, **Henri Stapp** (1928, Américain) qui a travaillé sur la conscience et qui pense qu'elle régit le monde et la réalité et qu'elle ne peut s'expliquer que par la physique quantique[1327], **Roger Penrose** (1931, Anglais) qui considère que la conscience résulte de la réduction du paquet d'ondes et **Elizabeth Rauscher** [1328](1931-2019, Américaine), une physicienne qui s'intéressa d'abord à la philosophie puis versa ensuite dans la parapsychologie.

A contrario, **Steven Weinberg** (1933, Américain), prix Nobel de Physique en 1979 pour ses travaux sur l'unification des forces faibles et électromagnétiques, est d'avis que la philosophie ne sert pas à grand-chose d'autre dans la physique quantique que de se garder des erreurs d'autres philosophes[1329]. Ce point de vue était partagé par **Stephen Hawking** (1942-2018, Anglais).

En France, en plus du trio du modèle CSM, nous avons notamment **Michel Bitbol**, déjà cité avec de nombreuses ressources, biophysicien à l'origine et philosophe des sciences, intéressé notamment par la question de la conscience, **Etienne Klein**, ingénieur et physicien à l'origine, qui s'est spécialisé dans la philosophie des sciences au CEA, ainsi qu'**Alexei Grinbaum** et **Vincent Bontemps** qui font tous deux partie du laboratoire LARSIM d'Etienne Klein.

[1326] Elle résulte de la création avec Nayla Farouki du CEA d'un groupe dédié aux fondements de la mécanique quantique à Grenoble. Elles forment en 2013 un groupe avec Philippe Grangier qui défendait depuis longtemps l'objectivité contextuelle. Voir l'entretien l'Alexia Auffèves avec Loïc Mangin dans Pour la Science, Les promesses du Monde Quantique, octobre-décembre 2016. Résumé : « *C'est le premier postulat que nous posons dans notre nouvelle façon d'envisager la réalité et que nous nommons Contexte, Système, Modalité (csm). Exprimé autrement, il signifie qu'en mécanique quantique, l'état d'un système ne dépend pas que du système lui-même, mais aussi du contexte. Pour bien distinguer ces états qui caractérisent système et contexte des états classiques qui ne dépendent que du système, nous les avons baptisé « modalités ». Ces modalités sont des réponses certaines, prédictibles et répétées à des questions posées dans un contexte donné. Ce premier postulat est en fait une reformulation des idées de Bohr en termes ontologiques.* ».

[1327] Voir Mind, Matter and Quantum Mechanics par Henry P. Stapp, 2009 (303 pages). C'est le genre d'ouvrage qui émet des hypothèses non vérifiables qui deviennent alors paroles d'évangiles pour les charlatans de la médecine quantique dont nous parlons dans la dense rubrique dédiée aux fumisteries quantiques. Et pourtant, le propos de base n'a rien d'extraordinaire : la chimie du cerveau s'appuie comme toute chimie sur de nombreuses facettes de la physique quantique. Cela devient compliqué lorsque l'hypothèse est émise d'une mise en œuvre de l'intrication dans la conscience. La médecine quantique sort du jeu scientifique lorsqu'elle prétend que l'on peut contrôler ces mécanismes à partir de la simple volonté, sans compter l'action sur les autres organes (malades de préférence) du corps humain.

[1328] Elizabeth Rauscher est coauteur avec Richard Amoroso de l'ouvrage The Holographic Anthropic Universe, 2009 (510 pages). Ils y évoquent un modèle de création d'ordinateur quantique scalable dénommé « Universal Quantum Computing » qu'il est difficile d'appréhender entre véritable science et crackpot science et qui s'appuie sur une théorie dénommée « Unified Field Mechanics » difficile à évaluer. Le propos est détaillé dans Brief Primer on the Fundaments of Quantum Computing de Richard L Amoroso, 2017 (140 pages). Richard Amoroso est Directeur du Noetic Advanced Studies Institute à Oakland en Californie. La noétique s'intéresse entre autres aux liens entre les états quantiques et la conscience. Et cela dépasse nettement le cadre de la science avec Pragmatic Proof of God (Part I & Part II), 2017 par Richard L. Amoroso (34 et 13 pages).

[1329] Voir le chapitre "Against Philosophy" dans "Dreams of a Final Theory", 1994, Steven Weinberg, qui est contredit dans Physics Needs Philosophy / Philosophy Needs Physics, par Carlo Rovelli, 2018. Pour ce dernier, affirmer que la science n'a pas besoin de philosophie consiste à faire… de la philosophie des sciences ! Voir aussi The Trouble with Quantum Mechanics, 2016.

La physique quantique pose d'autres questions physico-philosophiques comme le vide total existe-t-il ? En effet, la physique quantique décrit l'énergie du vide, qui serait toujours traversé par des particules réelles et virtuelles diverses. D'un point de vue pratique, il est donc difficile de créer un espace vide qui ne soit pas du tout traversé par des ondes électromagnétiques ou particules de toutes sortes. Si donc le rien n'existe pas, qu'il y avait-il avant le big bang ? Et ne parlons pas de la nature du temps qui fait encore débat.

L'approche philosophique courante de la physique quantique m'a un peu désarçonné. La majorité des ouvrages de cette discipline sont bourrés de mathématiques et de physique. Ils doivent battre des records de ce point de vue-là par rapport à n'importe quel autre sujet couvert par le champ de la philosophie. Et surtout, ils abordent peu les sciences humaines à proprement parler.

Quelles sont les conséquences humaines de ces différentes interprétations de la physique quantique ? Existe-t-il d'autres questions philosophiques que ces questions d'interprétation sur le réalisme applicable à bas niveau ? Il y aurait fort à faire en la matière. Les notions d'incertitude et d'indéterminisme débouchent immanquablement sur la notion de libre arbitre et de destin (vue par Pascual Jordan). La focalisation philosophique quantique sur l'échelle microscopie et nanoscopique de la physique pourrait aussi relever d'une forme de réductionnisme empêchant d'adopter une vision grand angle de son impact sociétal.

L'extension du champ scientifique est-elle infinie ? Quelles sont les limites du savoir humain qui cherche à tout expliquer et interpréter sur le fonctionnement de l'Univers ?

Qu'est-ce qui lui échappe et pourquoi ? Quels liens peut-on faire avec l'humilité dont l'Homme devrait se prévaloir[1330] ? Quelles sont les limites structurelles à sa curiosité insatiable ? En fait, je ne fais que reformuler la notion même de métaphysique kantienne, c'est-à-dire, la « *science des limites de la raison humaine*".

La question philosophique porte ainsi sur la notion de faisable et d'infaisable et de son évolution dans le temps, une perspective apportée par l'histoire et la philosophie des sciences. Quelles sont les limites de l'ingéniosité humaine ? Qu'est-ce qui est surhumain ? Pourra-t-on se téléporter ? Pourra-t-on se déplacer plus vite que la lumière ? Pourra-t-on créer des ordinateurs quantiques ultra fiables et *scalables* ? Les théories et classes de la complexité, évoquées dans cet ouvrage, devraient aussi servir de base à ces réflexions.

Comment étendre l'interprétation de la physique quantique à la métaphore du calcul quantique qui est complexe en son sein, mais simple lors de la mesure ? Pourra-t-l'utiliser pour simuler le vivant et le créer in silico ? Ce qui posera alors des questions sur le pouvoir de l'Homme sur la nature et sur les responsabilités associées. Nous verrons aussi resurgir les débats sur le scientisme, la « *société dirigée par la science* » ainsi que sur le solutionnisme technologique qui pourrait avoir réponse à tous les problèmes notamment environnementaux et dans la santé, permettant de ne pas les traiter convenablement dans l'urgence nécessaire.

Ces questions se posent de plus en plus dans une période où la précaution prévaut sur tout, où l'on craint des dérapages technologiques dans presque tous les domaines (le nucléaire, les OGM, les engrais, les vaccins, l'intelligence artificielle et la 5G), où la notion même de progrès scientifique n'est plus acquise et où sévit le relativisme cognitif ne permettant plus de distinguer le sérieux du farfelu, entraînant une défiance collective dans les sciences. Nous allons justement étudier dans la partie suivante une question qui fait partie du champ de la philosophie, la question de l'éthique du calcul quantique.

[1330] La physique quantique est une belle école d'humilité autant pour les profanes que pour les spécialistes. Comme le disait Richard Feynman, on ne peut jamais l'assimiler complètement ni expliquer et interpréter tous les phénomènes qu'elle décrit, notamment l'intrication à longue distance.

Ces questions sont-elles véritablement spécifiques à la physique et au calcul quantique ? Ne sont-elles pas récurrentes dès qu'une nouvelle technologie majeure voit le jour ? Peut-être, mais ces questions méritent toutefois d'être posées, comme celles qu'ont posé l'émergence des usages courants de l'intelligence artificielle depuis 2012.

Les interprétations de la physique quantique sont en tout cas là pour nous rappeler qu'en toute matière, il nous faut multiplier les angles de vue des problèmes pour mieux les analyser. C'est évidemment très chargé de leçons d'un point de vue métaphorique.

Je m'interroge sur toutes ces questions en observant que, faute d'être traitées, elles ont tendance à devenir le champ de l'ésotérisme et du charlatanisme comme nous le verrons dans une partie suivante dédiée aux fumisteries quantiques.

C'est un peu comme si la philosophie de la physique quantique en était restée au stade de la recherche fondamentale sans passer à l'étape de la recherche appliquée. En quelque sorte, elle est en phase avec le niveau de maturité marché des technologies de la seconde révolution quantique. Gageons que plus les usages prolifèreront, plus cette philosophie appliquée se développera et permettra d'écrire un nouveau chapitre de cette histoire passionnante des sciences.

Ethique des usages du calcul quantique

L'éthique des usages de l'intelligence artificielle est devenue en 2018 un véritable sujet politique. C'était très apparent dans le **Rapport de la Mission Villani sur l'intelligence artificielle** de mars 2018 ainsi que dans un rapport de la Chambre des Lords au même moment et sur le même sujet au Royaume-Uni. Il mettait en avant le besoin de s'assurer, au minimum moralement mais si possible pratiquement, que les solutions à base d'IA respectaient la société et évitait notamment de générer ou de perpétuer des discriminations du fait des données utilisées. D'où deux sujets saillants comme l'explicabilité des algorithmes et les limites de la manipulation de nos émotions, notamment via des robots plus ou moins humanoïdes.

La difficulté à expliquer le fonctionnement de certains algorithmes de deep learning a été quelque peu montée en épingle. S'il est vrai que le fonctionnement de réseaux de neurones multicouches est quelque peu abstrait pour le commun des mortels, il l'est tout autant pour quasiment n'importe quel logiciel, avec ou sans IA, qui peut affecter notre vie courante. Mais on l'a un peu oublié. Lorsqu'un logiciel du groupe Visa vous refuse votre paiement de carte bancaire à l'étranger, on ne vous explique quasiment jamais le pourquoi du comment. Les techniques bayésiennes de détection de fraude ne sont pas documentées pour le grand public. Et elles ne relèvent pas de l'intelligence artificielle !

Le calcul quantique risque d'amplifier cette quête d'explicabilité. Elle est encore moins évidente à assouvir avec les algorithmes quantiques dont nous avons pu voir qu'ils suivaient une logique que peu de développeurs d'aujourd'hui peuvent appréhender. Les algorithmes quantiques risquent bien d'être encore plus compliqués et moins compréhensibles que ceux de l'IA d'aujourd'hui. Ce d'autant plus que lors de leurs opérations, on ne peut pas en observer le fonctionnement et les états quantiques intermédiaires. On ne mesure que le résultat « classique » à la fin des opérations. Qui plus est, à partir d'une cinquantaine de qubits, il devient impossible d'émuler un algorithme sur un calculateur classique.

Leurs biais éventuels ne viendront pas forcément des données qui les alimentent car, pour un temps certain, les calculateurs quantiques n'exploiteront pas de gros volumes de données. On pourra donc parler au sens propre du terme de biais des algorithmes alors que lorsqu'on évoque ce terme au sujet de l'IA, on évoque en fait beaucoup plus le biais des données qui alimentent les algorithmes que le biais de ces derniers.

Mais on jugera au cas par cas. Selon que les applications du calcul quantique gèrent la circulation automobile, la gestion de la distribution d'énergie, la création de nouvelles molécules en chimie ou biologie ou aident la NSA à décrypter les communications privées, les enjeux ne seront pas les mêmes.

Une question éthique émergera sans doute devant les autres. Elle sera associée à un pan entier des applications du calcul quantique : la simulation de la dynamique de molécules organiques. Elle sera probablement limitée aux débuts à la simulation de molécules relativement simples. La simulation du repliement de protéines complexes est une hypothèse qui n'est pas encore validée. Dans un futur hypothétique lointain, on saura peut-être simuler l'assemblage d'un ribosome.

L'une des grandes avancées dans l'explicabilité des algorithmes quantiques vient de la chercheuse **Urmila Mahadev** dont les travaux étalés entre 2012 et 2018 ont permis de créer une méthode de vérification des traitements d'ordinateurs quantiques. Elle était postdoc à Berkeley et soutenue par Scott Aaronson et Umesh Vazirani, deux éminences de la recherche en algorithmie quantique.

Ses travaux visent à permettre de prouver qu'un ordinateur quantique a bien réalisé les traitements qu'on lui a demandés de faire. Elle montre qu'un ordinateur classique couplé à un ordinateur quantique simple peut vérifier de manière polynomiale les résultats d'un ordinateur quantique[1331]. La méthode exploite une technique de cryptographie post-quantique que le vérifieur ne peut pas casser (LWE : Learning With Errors). Les LWE font partie de la classe des Lattice-based cryptography (EN) ou réseaux euclidiens (FR)[1332].

Lorsque l'on simulera ce fonctionnement pour ensuite l'altérer, par exemple pour créer de nouvelles thérapies, le rejet des OGM ou des vaccins sembleront être de lointains soubresauts du passé. De nouvelles peurs se construiront et les scientifiques devront redoubler d'efforts pour éviter qu'elles se propagent. Ces peurs irrationnelles vont d'ailleurs émerger du fait d'exagérations sur les capacités des ordinateurs quantiques. On entend déjà parler de "robots quantiques", ce qui ne veut rien dire, mais peut impressionner et titiller l'imaginaire.


MOTHERBOARD

Quantum Robots Will Do Your Job Better Than You Can

Quantum computing will be powerful enough to create artificial intelligence that can learn and react in real time.

International Business Times

Technology

Quantum Robotics will Create Artificial Intelligence 'Capable of Creativity'

By Anthony Cuthbertson

October 9, 2014 11:46 BST

[1331] Voir une description de la méthode en langage presque natural dans Graduate Student Solves Quantum Verification Problem, octobre 2018 et deux publications de référence : Classical Verification of Quantum Computations, septembre 2018 (53 pages) et Interactive Proofs For Quantum Computations, avril 2017 (75 pages).

[1332] Voir cette présentation décrivant le protocole LWE : An Introduction to the Learning with Errors Problem in 3 Hours (76 slides).

L'exemple *ci-dessus* est éloquent de ce point de vue-là avec deux titres tapageurs dans la presse US en 2014[1333] qui ne font, en pratique, que relayer une publication scientifique assez banale, Quantum speedup for active learning agents (15 pages) décrivant des algorithmes quantiques pour l'exécution de réseaux d'agents servant à la robotique apportant un gain de performance dit "quadratique", donc… pas exponentiel, donc, pas extraordinaire. On n'a pas fini d'en voir passer de cette couleur ! Il faudra à chaque fois décoder et prendre du recul.

Une bonne approche pour la communauté scientifique quantique consisterait à préempter ces peurs en les analysant le plus en amont et en les désamorçant si possible, histoire de ne pas se trouver dans une situation qui bloquerait le progrès scientifique et de l'innovation utile à la société du fait de ces peurs irrationnelles.

Religions et mysticisme

Depuis quelques millénaires, l'espèce humaine a pris l'habitude de consacrer un culte à une ou plusieurs puissances divines supérieures de nature imprécise, mais expliquant tout et le reste.

L'Homme a probablement commencé à attribuer cette puissance aux phénomènes naturels qu'il ne pouvait pas expliquer comme le Soleil ou les étoiles. L'Homme est ensuite passé de systèmes de dieux multiples à un Dieu unique tout puissant. En quelque sorte, les religions monothéistes ont réalisé avant l'heure la théorie de l'unification tant recherchée par les physiciens. Cette Histoire est racontée avec recul par **Yuval Harari** dans Sapiens et avec cynisme par **Richard Dawkins** dans The God Delusion.

Pour certains scientifiques ou croyants en un au-delà, la physique quantique renouvèle les velléités d'expliquer le fonctionnement de l'Univers par une puissance divine. Elle donne l'impression de se fournir une explication scientifique ultime du tout, de Dieu, et de sa capacité à tout contrôler et superviser[1334].

La fonction quantique la plus souvent mise en avant est l'intrication. Elle permet d'envisager l'existence d'un être suprême qui, grâce à ce phénomène physique, peut contrôler toutes les particules de l'Univers et à distance. Elle expliquerait aussi des phénomènes étranges de synchronicité. La dualité onde-particule permet aussi d'imaginer ou expliquer plein de scénarios magiques comme la guérison à distance, la télékinésie ou la télépathie[1335].

Certains des protagonistes de ces théories sont eux-mêmes des scientifiques de la physique quantique.

L'un des plus connus est **David Bohm** (1917-1992) qui se rapprocha du spiritualisme indien à partir des années 1960… au même moment que les Beatles ! Il était convaincu que les lois de l'Univers étaient gouvernées par un esprit[1336]. Il est l'un des initiateurs des théories de la **cognition quantique**, un champ des théories cognitives qui s'appuie sur le formalisme mathématique de la mécanique quantique, et en s'appuyant sur des analogies.

[1333] Voir article 1 et article 2.

[1334] Voir à ce sujet la fiche Wikipedia qui décrit succinctement le mysticisme quantique.

[1335] On trouve un bon inventaire de ces différents débats dans The Quantum God An Investigation of the Image of God from Quantum Science, 2015 (81 pages) qui évoque notamment la notion de conscience de l'Univers. Voir aussi le presque parodique Rien n'est solide « Tout est énergie ».

[1336] Voir à ce sujet Lifework of David Bohm - River of Truth de Will Keepin, 2016 (22 pages).

La littérature sur cette question est parfois édifiante comme Google's Quantum Computer May Point People to God, qui date de 2013. Selon l'auteur (anonyme), un ordinateur quantique parfait pourrait tenter de simuler l'apparition de la vie sur Terre et démontrer par l'absurde qu'elle ne serait pas possible sans une intervention divine. Mais qui dit que le résultat ne serait pas le contraire ? L'informatique quantique permettrait d'invalider les théories classiques de l'évolution.

Ils ne précisent pas le nombre de zillions de qubits intriqués dont il faudrait disposer pour étayer cela. Bien entendu, car ils n'ont aucune idée des algorithmes à utiliser. C'est de la fumette !

Tout cela relève de la religion-science-fiction et peut générer des débats enflammés avec des interlocuteurs qui ne seront jamais sur la même longueur d'onde, les uns adoptant une démarche scientifique classique et les autres, relevant du mysticisme et d'une approche plus émotionnelle. Quoi qu'il arrive, cela sera un débat de sourds.

Culture générale

L'informatique quantique va faire perdurer et amplifier un paysage commun avec celui de l'intelligence artificielle : un gouffre entre ceux qui comprennent et ceux qui utilisent et une pénurie de compétences. Le premier va intervenir assez rapidement tandis que la seconde se manifestera avec un délai plus long.

L'informatique quantique est définitivement un monde de spécialistes, et il est encore plus abscons que nombre d'autres domaines liés au numérique. Aujourd'hui, ce monde est équilibré entre spécialistes de la physique de la matière condensée et des algorithmes et logiciels quantiques[1337].

En extrapolant un peu et en s'inspirant de l'Histoire de l'informatique, on peut anticiper que la partie logicielle prendra progressivement le dessus lorsque le calcul quantique deviendra monnaie courante, surtout s'il débouche sur des applications dans l'ensemble des secteurs de l'industrie.

Dans l'économie numérique d'aujourd'hui, il y a bien plus de spécialistes du logiciel que des semiconducteurs. Les économies d'échelle sont en fait bien plus grandes avec ces derniers entre producteurs et utilisateurs. Le quantique n'y échappera probablement pas, même si dans un premier temps, le marché des ordinateurs quantiques ne sera pas un marché de volume.

A court terme, le besoin est grand de vulgariser le domaine et de sortir de son jargon technique. La lecture d'une bonne partie de cet ebook en a probablement rebuté quelques-uns de ce point de vue-là. Ma démarche n'est certainement pas très grand public. Il faut procéder pas à pas. Il faut déjà commencer avec les habitués du numérique et du développement logiciel. S'ils peuvent appréhender les enjeux de l'informatique quantique, cela sera déjà un bon pas de fait. Ensuite, il faudra élargir progressivement l'audience.

[1337] Voir Eleven risks of marrying a quantum information scientist par Nicole Yunger Halpern, 2020. Un inventaire second degré mais réaliste de la vie d'une scientifique du quantique aux USA.

La prochaine étape est celle de la formation et de la vulgarisation auprès des décideurs d'entreprises et aussi institutionnels. Elle deviendra d'autant plus importante que l'effet de mode va commencer à décoller, du fait des annonces tonitruantes qui ne manqueront pas d'arriver, notamment de la part des grands acteurs du secteur, et surtout Américains et Chinois. De ce point de vue-là, les acteurs européens du quantique devront aussi investir sur le terrain pour ne pas se laisser dépasser par les acteurs Américains puis Chinois.

Nous ferons aussi face à une pénurie de spécialistes et au manque de diversité chez ces spécialistes. Ce monde est déjà très masculin, avec peu de femmes chez les scientifiques du secteur, dans la lignée de l'informatique et de l'intelligence artificielle. Cette pénurie pourrait être encore plus forte qu'avec l'intelligence artificielle[1338].

La spécialité est encore trop masculine en l'état. Je l'ai constaté en faisant le tour des stars du secteur côté scientifique comme entrepreneurial. Malgré tout, nous avons pu voir dans l'inventaire des scientifiques du quantique que l'on peut identifier des dizaines de femmes dans cette discipline qui peuvent servir de *role models*.

Il y a encore peu de startups crées par des femmes dans l'inventaire que j'ai pu en faire à part Silicon Quantum Computing (SQC, Australie), créée par la chercheuse **Michelle Simmons**, Quandela, cofondée par **Pascale Senellart** et VeriQloud cofondée par **Elham Kashefi**. L'inventaire des startups réalisé dans cet ebook fait heureusement ressortir quelques autres entrepreneuses dans le monde entier.

Le langage qui est utilisé autour du quantique est très masculin dans la forme[1339]. C'est un langage où l'on évoque les notions de supériorité (supremacy) et d'auxiliaires (ancillae), le premier faisant écho à une autorité supérieure, et à l'actuelle "white supremacy" issue de l'Apartheid Sud-Africain et qui remue la sphère politique US. La seconde notion reprend la notion de "servante femme" en latin, d'esclavage et de ségrégation raciale, alors que le terme technique a été inventé en 1995. Ce sont de petites choses symboliques mais qui mériteraient d'être corrigées. On ne veut pas d'Handmaid's Tale dans le quantique ! La solution consiste à parler d'avantage quantique (« quantum advantage ») même si le sens est légèrement différent de celui de la suprématie quantique.

Qu'en est-il enfin du futur de l'emploi lié au quantique, question que se pose Sophia Chen dans Wired en juin 2018 ? C'est difficile à évaluer car on raisonne sur plusieurs décennies et sur des usages pas encore bien détourés. Il y aura comme avec l'IA, ceux qui savent et les autres, ceux qui codent et ceux qui exécutent ou utilisent, ceux qui créent la richesse et ceux dont l'emploi est menacé.


WIRED

SOPHIA CHEN SCIENCE 08.06.18 08:00 AM

QUANTUM COMPUTING WILL CREATE JOBS. BUT WHICH ONES?

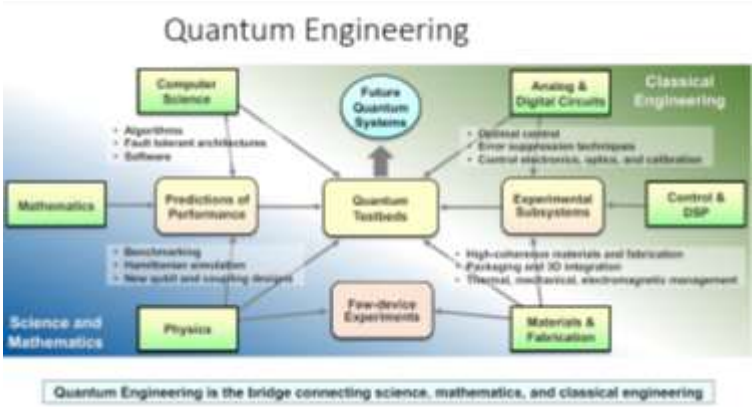
Mais le calcul quantique ne génère pour l'instant pas de menaces spécifiques sur l'emploi car il permettra de faire des choses que l'Homme ne sait de toutes manières pas réaliser de manière traditionnelle aujourd'hui. Il n'y a pas de logique de remplacement, tout au plus d'optimisation comme pour les applications basées sur l'optimisation de graphes comme ceux du "voyageur du commerce".

[1338] La pénurie de compétences qui démarre dans le quantique est bien décrite dans The Next Tech Talent Shortage: Quantum Computing Researchers, octobre 2018.

[1339] Comme le relève très bien **Karoline Wiesner** de l'Université de Bristol dans son succinct The careless use of language in quantum information, 2017 (2 pages).

Il faudra en tout cas préparer de nouvelles générations d'ingénieurs dans un grand nombre de disciplines et en particulier dans celles des mathématiques et de la création de logiciels quantiques.

Du côté du matériel, on aura aussi besoin d'ingénieurs spécialisés et généralistes. L'ingénierie quantique fait appel à de nombreuses disciplines complémentaires[1340].



Avec l'IA, c'est un nouveau défi pour l'enseignement supérieur qui se prépare[1341]. Très peu d'écoles d'ingénieurs proposent des cours sur l'informatique quantique en France. Les premiers sont apparus à CentraleSupelec (Benoît Valiron, Zeno Toffano, Thomas Antoni), à Télécom Paris (Romain Alléaume), à l'Ecole Polytechnique (Alain Aspect, Silke Biermann, Pascale Senellart) ainsi qu'à l'ESGI à Paris (Alain Lioret), à l'ECE et à l'INSA Lyon. D'autres doivent exister dans d'autres écoles d'ingénieurs et universités, qui restent à inventorier.

Marketing des technologies quantiques

Dernier point à évoquer, celui du rôle du marketing de l'offre. Comme je l'ai traité dans une série de 2014 sur les Propagandes de l'innovation, le marketing des fournisseurs et des analystes est celui qui fera le plus de bruit dans le domaine du quantique.

Nous allons être noyés sous une propagande innovationnelle qui brouillera le message. Les scientifiques du domaine ne reconnaitront plus leurs créations.

[1340] Le schéma provient de la présentation Introduction to Quantum Computing par William Oliver du MIT à la Q2B de décembre 2019.

[1341] Voir à ce sujet A la recherche des métiers quantiques de Fabien Goubet dans le journal suisse Le Temps, août 2018.

Les articles de vulgarisation sur le calcul quantique vont continuer à démarrer les explications sur les qubits avec leur état superposé 0 et 1 et s'arrêter là [1342]!

Le propre du marketing et de la communication sera d'embellir la mariée et de simplifier les faits par exagérations. Cela va commencer avec la notion de suprématie quantique qui sera valorisée à tort et à travers. On retiendra l'expression mais pas les détails de l'explication.

Dans certains cas, des offres accoleront le label "quantique" à des produits qui n'ont rien de quantique. C'est par exemple le cas des pico-serveurs en cloud distribués par la startup française R136.fr. L'enquête de Science et Avenir sur cette entreprise montre bien qu'il n'y a pas que le quantique qui y soit louche.

On voit déjà apparaître des analyses à l'emporte-pièce sur les usages du calcul quantique dans le big data, alors que ce n'est pas le premier domaine concerné. Cela se retrouve dans Informatique quantique et Big Data : une révolution pour l'analyse de données en août 2018.

Cet article est assez imprécis voire à côté de la plaque sur quelques points, et c'est un grand classique : *"Les ordinateurs quantiques ... peuvent être utilisés pour trouver des nombres premiers très larges. Il serait donc possible d'appliquer cette technologie au domaine de la cryptographie pour créer des systèmes de cybersécurité plus résistants."* alors que les ordinateurs quantiques permettent de factoriser des nombres entiers très grands en nombres premiers, mais les systèmes de cybersécurité plus résistants ne passent pas forcément par l'ordinateur quantique !

Ils s'appuient sur des clés quantiques QKD pour les systèmes à clés privées ou sur de la cryptographie post-quantique pour les systèmes à clés publiques, et sans passer par des ordinateurs quantiques.

Quant à l'exploitation en mémoire de grosses bases de données, elle nécessiterait un très grand nombre de qubits qui est difficile à obtenir, et qui plus est, de la mémoire quantique nécessaire pour exécuter le fameux algorithme de recherche de Grover et qui n'est pas du tout au point. Cela arrivera bien un jour, mais assez lointain.

Autre exemple de dérive, cette fois-ci dans un cabinet de conseil, avec cette infographie du **BCG** erronée à 80% qui fait la promotion du calcul quantique dans les industries pharmaceutiques[1343] (*ci-dessous*).

A force de grossir le trait, cela en devient absurde. Ainsi, en va-t-il lorsqu'ils évoquent la capacité d'un ordinateur quantique à résoudre une « *infinité de problèmes simultanément* » ! Tout d'abord, il ne s'agit pas d'infinité mais d'exponentialité et ensuite, la superposition dans un registre quantique n'est pas celle de problèmes mais d'états. Et cela ne permet de résoudre un seul problème à la fois. La nuance est peut-être sémantique et subtile mais importante.

Autre délire, celui de l'estimation du marché de l'informatique quantique dans les industries pharmaceutiques aux USA. Il est estimé entre $15B à $30B sans précision de date alors que l'ordre de grandeur de la dépense en informatique de l'ensemble du secteur de la santé aux USA serait de $53B aux USA en 2018 [1344]!

Enfin, nous avons une courbe d'adoption des ordinateurs quantiques dans les entreprises selon le niveau de complexité des problèmes à résoudre, avant même qu'ils ne soient disponibles, surtout pour ceux qui ciblent les problèmes les plus complexes !

[1342] Je vais plus loin que cela dans cet ebook mais ai conscience qu'il peut contenir des erreurs factuelles, interprétations erronées ou exagérations. Par contre, je les corrige au fil de l'eau lorsque je les découvre ou que l'on me les signale !

[1343] Source : https://www.bcg.com/publications/2018/qubits-are-coming-infographic.aspx.

[1344] Source : https://www.ranosys.com/blog/industry/healthcare/healthcare-technology-trends-predictions-for-2018/.

Ce graphe parle d'adoption bien avant que les ordinateurs quantiques correspondants ne soient disponibles !

"quantum computing solves an infinite number of problems simultaneously" est une simplification outrancière de l'apport de la superposition d'états dans des registres de qubits. Il n'y a d'ailleurs pas d'infinité dans le quantique.

Là, OK. Les ordinateurs quantiques vont en effet se propager par vagues avec des capacités croissantes. Un grand classique.

20% d'accélération du temps de développement de nouveaux traitements et doublement du nombre d'agréments de mise sur le marché. Estimation faite au doigt mouillé ?

Ce montant de $15B à $30B d'informatique quantique dans la pharma est absurde. La dépense IT du secteur santé serait de $53B aux USA en 2018 !

Erreur classique : le quantique n'est pas adapté au "big data" contrairement à une idée répandue.

source : https://www.bcg.com/publications/2018/qubits-are-coming-infographic.aspx
commentaires d'Olivier Ezratty, septembre 2018.

Et pourtant, je suis le premier des convaincus des bénéfices du calcul quantique dans les applications de pharmacie et notamment de simulation du comportement de molécules organiques ! Ces exagérations à l'emporte-pièce sont délirantes et me rappellent celles qui portaient sur les objets connectés il y a quelques années[1345].

Dans la même veine, les **transistors quantiques** évoqués dans cette présentation de Movimento Group pour les véhicules autonomes de 2030, relèvent d'une méconnaissance de l'état de l'art du calcul quantique, de sa vitesse de progression et de la nature physique des qubits (source). Sachant que les transistors font depuis leur création appel à des phénomènes quantiques ! C'est donc une exagération relativement sage !

Autre phénomène qui est amené à devenir récurent, la propension des médias à se mélanger les pinceaux dans la couverture de l'actualité sur les technologies quantiques. Nous en avons un excellent exemple dans Avec l'IA, l'informatique quantique pourrait faire progresser l'IoT par Elina S. dans Objets Connectés en mai 2020 qui reprend Quantum technologies identified as a major trend for 2020 publié par IDQ en février 2020. Elle fait un lien entre le marché du quantique et celui des objets connectés alors qu'il n'y en avait pas dans l'article d'origine qui évoquait une dizaine de tendances dans les technologies, le quantique n'en étant qu'une. Avec une envolée lyrique qui mérite son pesant de cacahuètes : « *Il est absolument crucial que des tests d'utilisabilité soient effectués sur tous les produits quantiques et IoT pour s'assurer qu'ils sont accessibles et faciles à utiliser. C'est le meilleur moyen de résoudre les problèmes réels des utilisateurs.* ».

[1345] Voir La grande intox des objets connectés, août 2015.

Fumisteries quantiques

L'un des sujets les plus fascinants de l'impact grand public de la physique quantique est la manière dont certains s'emparent de la thématique pour l'intégrer dans des approches scientifiques alternatives, généralement douteuses. Le vaste cadre de la "médecine quantique" est un courant de pensées et de pratiques assez cohérent de ce point de vue-là, nous allons le voir. Il a engendré la prolifération de gourous en tout genre et d'escroqueries volontaires ou involontaires à base de machines miracles de détection d'ondes électromagnétiques et de rétablissement de l'équilibre corporel. C'est au mieux un sous-ensemble de la vaste industrie de l'effet placebo !

D'autres domaines se sont emparés de la physique quantique et bien avant que l'informatique quantique devienne un sujet visible : le management et le marketing sans compter la politique[1346]. La physique quantique y est essentiellement employée comme une source d'inspirations par analogies. Mais la gouroutisation de ces secteurs est aussi assez courante, reliant entre eux des courants de pensée tournant beaucoup autour de la pensée magique.

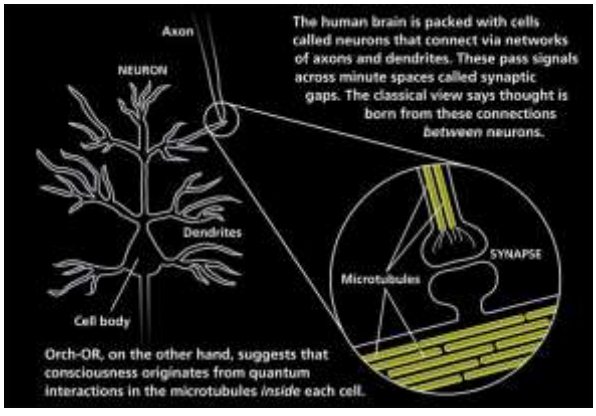
Biologie quantique

Le point de départ de la médecine quantique est pourtant scientifiquement pertinent et intéressant. Certains phénomènes biologiques s'expliquent bien à bas niveau par la physique quantique.

Pour n'en citer que quelques exemples, c'est évidemment le cas de la **photosynthèse** dans les plantes, qui fait jouer l'effet photoélectrique transformant un photon en déplacement d'électron, entraînant la génération de glucose, servant au stockage de l'énergie. Il en va de même dans le fonctionnement des **cônes et bâtonnets dans la rétine** qui captent la lumière. Les **rayons UV-B** participent à la synthèse des précurseurs de la Vitamine D3 dans la peau (source).

La physique quantique explique aussi la **captation du magnétisme terrestre** dans le cerveau de nombreux oiseaux via une protéine spéciale appelée cryptochrome. Il semblerait que ce mécanisme fasse appel à la capacité de la protéine à détecter des variations magnétiques grâce à l'intrication quantique d'électrons (source).

Des scientifiques de renom cherchent aussi à expliquer l'origine de la conscience par la physique quantique. Plusieurs grandes écoles de pensée sont reliées entre elles : la **théorie Orch-OR**, celle de la dimension **holographique de l'ADN** et celle des **biophotons**. Et puis, il faut ajouter tous les travaux autour de la **mémoire et de la structure de l'eau**.

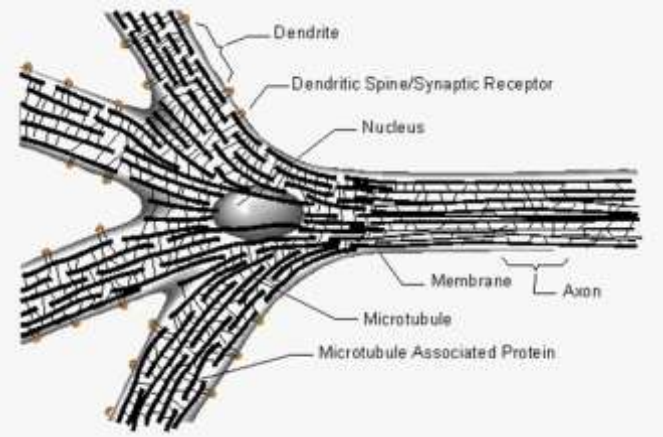


Aucun de ces travaux n'a obtenu l'assentiment d'une majorité de scientifiques mais ils méritent tout de même un petit examen. Ne serait-ce que pour comprendre comment ils sont rapidement dévoyés.

[1346] Le concept de politique quantique est encore balbutiant, même du côté du fumage de moquette. J'ai trouvé un peu de littérature de chercheurs en économie et en sciences sociales sur le sujet, mais ils ne mènent pas bien loin. Voir par exemple Quantum like modelling of the non-separability of voters' preferences in the US political system de PolinaKhrennikova, Université de Leicester (13 pages) cherche à modéliser les choix des électeurs américains et l'intrication ou pas du choix du candidat à la présidentiel et des candidats aux élections pour le Congrès montrant que celui-ci peut se découpler sous certaines conditions. Et Quantum Politics: New Methodological Perspective de Asghar Kazemi, 2011 (15 pages) fait un lien avec la théorie du chaos et l'effet papillon. Le papier a été écrit juste après les révolutions arabes de l'année. Voir aussi ce petit essai qui se contente d'exploiter l'analogie de la superposition : Politique. Cantique du quantique par Mikael Cabon, 2020. Voir aussi Schrodinger's Cat and World History: The Many Worlds Interpretation of Alternative Facts par Tom Banks qui utilise la thèse des mondes multiples de Bryce DeWitt pour expliquer l'élection de Donald Trump en 2016 par un effet tunnel géant.

Théorie Orch-OR

Selon **Roger Penrose** (Anglais, 1931) et **Stuart Hameroff** (Américain, 1947), la conscience serait logée et gérée par les microtubules, ces structures fibreuses complexes qui constituent avec les filaments d'actine et les filaments intermédiaires la structure des cellules, dénommée cytosquelette, et dans le cas des neurones, celle des dendrites, synapses et axones[1347]. Ils ont proposé en 1996 le modèle **Orch-OR** (Orchestrated Objective Reduction) selon lequel ces microtubules étaient des systèmes quantiques cohérents expliquant la conscience.



Pour eux, la conscience est gérée dans les neurones dans ces microtubules et non pas par leurs interconnexions via les couples dendrites/synapses. D'ailleurs, ils parlent de conscience, mais la question se pose sur la mémoire elle-même que l'on ne sait pas encore loger avec précision dans les structures neuronales du cerveau.

En 2011, Roger Penrose et Stuart Hameroff ont même avancé que ces microtubules seraient des nano-ordinateurs quantiques capables de gérer des qubits et des calculs associés[1348]. Si c'était vrai, la puissance de cet ordinateur en nombre de qubits serait incommensurable car un neurone comprend environ 100 millions de tubules, le cerveau 86 milliards de neurones et plus de 600 trillions de liaisons entre neurones ! Ces théories ne précisent évidemment pas comment fonctionnerait l'intrication entre ces qubits à cette échelle.

Ironiquement, l'impact indirect de ce dimensionnement gargantuesque serait de repousser encore plus loin dans le temps une éventuelle singularité, moment où un ordinateur atteindrait la capacité de calcul d'un cerveau humain en puissance de calcul brute[1349]. Mais on à affaire ici à un autre courant de pensée, promu notamment par **Ray Kurzweil**.

La théorie Orch-OR a connu un regain d'intérêt en 2014 avec la découverte de vibrations quantiques dans les microtubules par un certain **Anirban Bandyopadhyay** du National Institute for Materials Science au Japon[1350].

[1347] Source de l'illustration : Notre cerveau est-il un ordinateur quantique ?, de Laurent Sacco, avril 2018.

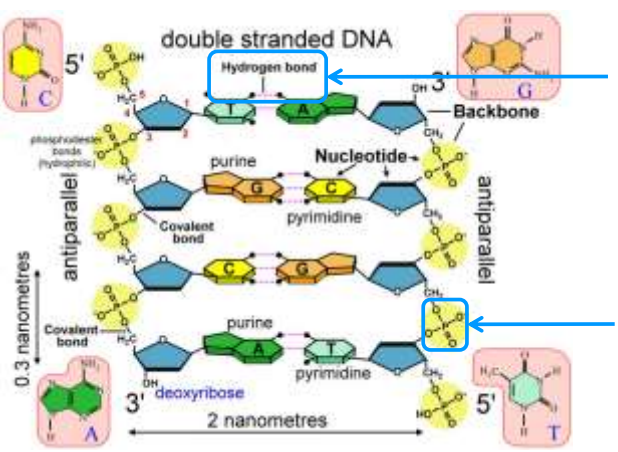
[1348] D'autres théories pensent que l'intrication quantique fonctionne également ailleurs dans le cerveau, au niveau des atomes de phosphore associés à du calcium. Cela permettrait la création de liaisons quantiques entre neurones. Voir Un nouveau spin dans le cerveau quantique de Jacqueline Charpentier, 2016. Le papier fait référence à Quantum Cognition: The possibility of processing with nuclear spins in the brain de Matthew Fisher, 2015 (8 pages). Comme l'indique l'article, cela pose des questions mais ne fournit pas de réponses ! Donc, toute interprétation un peu rapide sur le « cerveau quantique » est à prendre avec des pincettes.

[1349] Voir Consciousness in the Universe Neuroscience, Quantum Space-Time Geometry and Orch OR Theory de Roger Penrose, 2011, 50 pages). Tout cela est documenté dans Orchestrated Objective Reduction of Quantum Coherence in Brain Microtubules: The "Orch OR" Model for Consciousness, 1996 (28 pages) ainsi que dans Consciousness, Microtubules, & 'Orch OR' A 'Space-time Odyssey' de Stuart Hameroff, 2013 (28 pages), Are Microtubules the Brain of the Neuron de Jon Lieff, 2015 et vulgarisé dans The strange link between the human mind and quantum de Philipp Ball, 2017. Roger Penrose a collaboré avec Stephen Hawking sur les singularités gravitationnelles et sur l'émission de radiation par les trous noirs. Ce dernier avait développé une théorie cosmologique associant la théorie de la relativité et la physique quantique.

[1350] La découverte est contestée par Matti Pitkanen dans New Results about Microtubules as Quantum Systems, 2014 (18 pages).

Mais tout cela n'explique rien. La conscience est un phénomène « macro ». Vouloir expliquer un phénomène « macro » par un unique processus « nanoscopique » n'a pas de sens car il évacue complètement toute la hiérarchie biologique entre les deux et les autres mécanismes nanoscopiques du système nerveux : les neurones eux-mêmes, les neurotransmetteurs, les synapses et dendrites, le noyau des neurones, les cellules gliales régulatrices du cerveau, et à plus grande échelle, les sens et l'organisation macro du cerveau.

On peut par exemple expliquer une bonne partie du fonctionnement du vivant via les liaisons faibles hydrogène-hydrogène (quantiques, bien entendu) qui relient les deux brins de l'ADN, ou les liaisons oxygène-phosphore, dans l'ADN et l'ARN, qui sont fortes et peuvent ainsi expliquer la cohésion de ces molécules fondamentales du vivant.



la **liaison hydrogène-hydrogène** entre nucléotides est de faible énergie et explique indirectement comment l'ADN peut être répliqué et générer de l'ARN messager

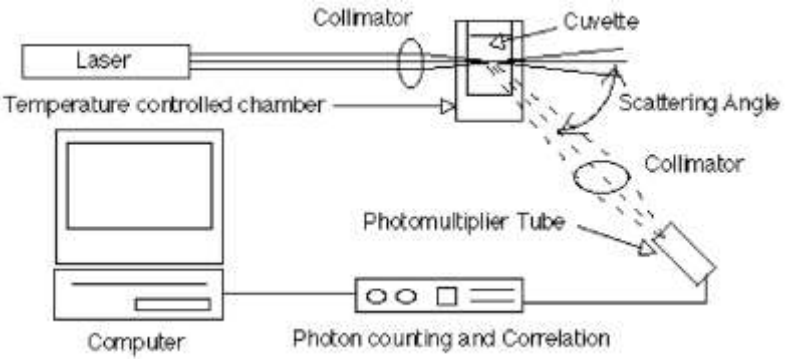
la **liaison phosphore-oxygène** est à plus haut niveau d'énergie et explique la cohésion des brins d'ADN (et d'ARN) dans le sens de la longueur, celle qui porte le code de la vie, servant ensuite à générer des protéines dans les cellules

source illustration : http://universe-review.ca/F11-monocell08.htm

C'est cependant bien insuffisant pour expliquer la conscience ou le fonctionnement du cœur et des reins. On pourrait aussi facilement bâtir une théorie pour gogos associant la conscience aux électrons tant qu'on y est. Bien oui, sans électrons, pas de chimie et pas de conscience ! Et leur fonctionnement est bien complexe. Ils expliquent les liaisons chimiques entre atomes. Leur fonctionnement est ce qu'il y a de plus quantique, avec la dualité ondes-particules. Mais heureusement, personne ne s'est encore aventuré dans ce genre d'explication.

Bref, vouloir expliquer la conscience par la nature éventuellement quantique d'une structure particulière des neurones relève du réductionnisme le plus simpliste qui soit, faisant fi de toutes les autres connaissances disponibles... ou indisponibles.

L'ADN aurait aussi une fonction quantique. Un curieux papier d'origine Russe, Allemande et Anglaise décrit des phénomènes quantiques et de non localité dans l'ADN, vérifiés dans une fameuse expérience à base de diffraction de lumière laser (*ci-contre*)[1351]. L'onde ADN bio-numérique (20 pages) explique que l'ADN est en fait un hologramme, qui interagit avec son environnement avec des radiations lasers.



Via l'intrication quantique, les chromosomes de plusieurs cellules interagiraient entre eux via ces radiations. Le Russe de l'histoire et leader de ces travaux est un certain **Peter Gariaev**, créateur de la notion de BioHologrammes au sein de son **Wave Genetics Institute** à Moscou[1352].

[1351] Voir DNA as Basis for Quantum Biocomputer 2011 (22 pages),

[1352] L'Histoire de la thématique est explorée dans Quantum BioHolography A Review of the Field from 1973-2002, de Richard Alan Miller, Iona Miller et Burt Webb (23 pages) mais sans que ces textes puissent permettre de s'en faire une idée de la validité scientifique.

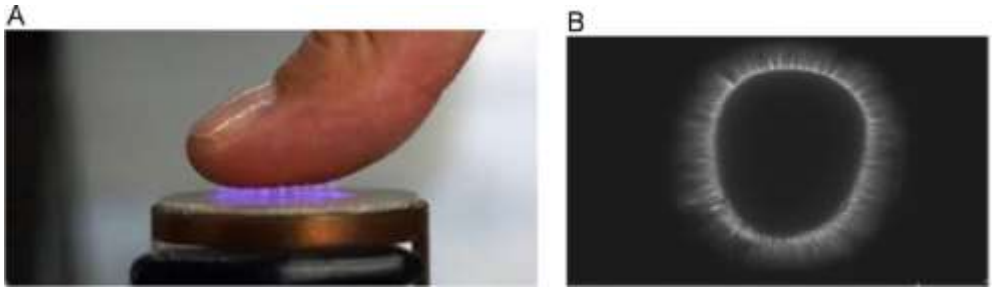
Biophotons

Autre école "alternative", celle des **biophotons**. Ce sont les faibles émissions de lumière dans le visible générées par les êtres vivants. Elles ont été découvertes en 1922 par le Russe **Alexander Gurwitsch**. La théorie des biophotons a été perfectionnée par l'Allemand **Fritz Albert Popp** et complète à bas niveau celle de l'ADN hologramme.

Elle décrit l'émission de photons par les molécules comme l'ADN, mais aussi celle qui est liée au métabolisme énergétique des cellules comme la transformation des molécules d'ADP en ATP dans les mitochondries des cellules. Les biophotons seraient des émissions d'ultra-violet et de lumière visible, à des niveaux bien plus faibles que l'émission d'infrarouge moyen qui intervient autour des 12 microns de longueur d'onde. On pourrait détecter jusqu'à quelques centaines de photons par centimètre carré d'organe analysé, souvent, au niveau de la peau.

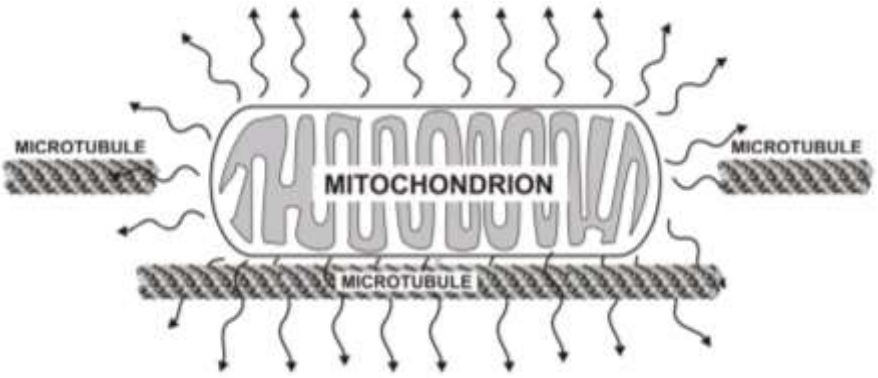
Ces biophotons seraient aussi une lumière cohérente – faite de photons de même fréquence - qui constituerait la composante clé d'une forme de communication inter-cellulaire[1353]. Je me demande comment fonctionne cette communication : à quelle portée, du fait de l'atténuation évidente de la diffusion des photons et avec quel ciblage (direction, orientation).

Selon Fritz Albert Popp, les aliments crus émettraient plus de biophotons que les aliments cuits, et les végétaux crus bios cinq fois plus que les végétaux cultivés traditionnellement. Conclusion : mangez du cru et du bio ! Voilà aussi de quoi faire regretter à l'Homme préhistorique d'avoir découvert le feu !



En tout cas, la détection de biophotons sur les 10 doigts de la main permettrait de détecter des pathologies cardiaques[1354]. Le scanner **ClearView** utilisé exploite un procédé curieux : il envoie une impulsion à haute tension qui créé un champ électromagnétique autour du doigt qui amplifie les biophotons qui sont émis. Cela excite les molécules dans l'air, créant un plasma entre le capteur et le doigt (*ci-dessus à gauche*) qui ionise l'air, générant l'émission d'UV et de lumière visible. C'est l'**effet Kirlian**, découvert par le Russe Semyon Kirlian en 1939.

C'est l'ionisation qui est captée par la caméra (*ci-dessus à droite*). Le logiciel analyse la forme générée et la compare à une base de pathologies. J'ai bien du mal à faire le lien entre la bioluminescence et ce procédé !



Et quid des récepteurs de ces biophotons ?

[1353] Comme décrit dans Photonic Communications and Information Encoding in Biological Systems de S.N. Mayburov, 2012 (10 pages) et vulgarisé dans Biophoton Communication: Can Cells Talk Using Light?, 2012 dans la MIT Technology Review.

[1354] Selon Detecting presence of cardiovascular disease through mitochondria respiration as depicted through biophotonic emission par Nancy Rizzo, 2015 (11 pages).

Eh bien, les microtubules des neurones, pardi [1355]! De quoi boucler la boucle. Dans les raccourcis proposés, selon Popp : "*la matière ne serait que de la lumière condensée*"[1356]. Ah, et puis, les biophotons seraient une manière d'expliquer le chi. David Muehsam évoque de nombreux effets biologiques des biophotons, qui seraient notamment impliqués dans la régulation de la sécrétion de neurotransmetteurs (pour des rats) mais sans que la distinction entre corrélation et causalité soit visiblement faite dans les publications associées[1357].

Les biophotons sont aussi promus par la société **Coramp Solutions** et par Georges Vieilledent. Elle exploite l'effet Kirlian dans ses appareils pour détecter les « effets de couronne ». Leur analyseur de biophotons sert à détecter des lymphomes. Cette société propose aussi un appareil d'électrophysiologie qui permettrait de traiter la maladie de Lyme qui se transmet par voie bactérienne et génère des infections cutanées.

Les acquis scientifiques établis, comme ceux qui sont encore sujets à caution, indiquent bien que le vivant dépend de la physique quantique à l'échelle subatomique voire moléculaire. Et il faut un sacré bagage scientifique et du temps pour évaluer ces différentes théories et comparer le pour et le contre.

Mais de là à utiliser tout cela pour vendre des guérisons miracles par le contrôle du corps par la conscience ! Les praticiens de la médecine quantique sont ainsi très souvent des psychosomaticiens exploitant le mysticisme et la méthode Coué pour générer, dans le meilleur des cas, un bon effet placebo qui peut fonctionner sur certaines pathologies légères. Quand bien même ils justifient leurs méthodes sur les travaux contestés de chercheurs tels que Roger Penrose et Stuart Hameroff, déjà cités, mais aussi Karl Pribram et Henry Stapp, qui veulent expliquer la conscience humaine par des phénomènes quantiques intervenant à bas niveau dans le cerveau qui expliqueraient aussi une soi-disante immortalité[1358].

La fiche Quantum Mind de Wikipedia relate les évolutions de cette branche et les critiques associées. Elle souligne surtout le fait que rien ne permet d'appliquer d'éventuels phénomènes quantiques comme l'intrication à l'échelle de structures macroscopiques moléculaires ou cellulaires dans le cerveau.

Cette intrication est encore moins justifiable pour relier à longue distance le cerveau à la "*conscience globale holographique de l'Univers*" promue par **Karl Pribram** et **Paola Zizzi**[1359]. Au même titre, cela n'a pas forcément de sens de relier esprit et matière comme ondes et particules et leur fameuse dualité. Cela mène sinon à des absurdités qui expliquent des phénomènes psychiques de synchronicité par l'effondrement de la fonction d'onde de la conscience, une explication aussi absurde que l'expérience de pensée du chat de Schrödinger[1360]. Même si les théories de Penrose et Hameroff étaient vérifiées, le raccourci serait un peu trop rapide, passant une fois encore très abusivement du nano-phénomène au macro-phénomène !

[1355] C'est ce qui ressort de l'article Emission of Mitochondrial Biophotons and their Effect on Electrical Activity of Membrane via Microtubules, 2010 (22 pages, schéma *de cette page*).

[1356] Voir à ce sujet Introduction de la conscience dans la matière de la physique quantique à la biologie (18 pages) de Jacqueline Bousquet, une ancienne chercheuse du CNRS décédée en 2013.

[1357] Voir The Energy That Heals Part II: Biophoton Emissions and The Body of Light, David Muehsam, avril 2018.

[1358] Voir Des physiciens apportent la preuve que l'âme est immortelle et qu'elle subsiste après la mort, sur InfoChrétienne, novembre 2016.

[1359] Dans Consciousness and Logic in a Quantum-Computing Universe, 2006 (25 pages).

[1360] Voir Mécanique quantique et psychisme, de Giuliana Galli Carminati et François Martin, 2007 (32 pages).

L'autre méthode couramment proposée relève de l'utilisation d'ondes électromagnétiques diverses, dont les fameuses et fumeuses **ondes scalaires**. L'idée consiste à les exploiter pour rétablir des équilibres d'organes déséquilibrés, exploitant la dualité ondes-particules et la capacité à rétablir le niveau énergétique de base de… on ne sait pas trop. Surtout dans la mesure où les ondes proposées sont faiblement ciblées[1361].

Il est notable, par contre, que peu de spécialistes scientifiques de la médecine quantique n'évoquent les capacités des futurs calculateurs quantiques pour simuler le fonctionnement de molécules organiques et créer de nouvelles thérapies. C'est explicable car les applications connues du calcul quantique dans la santé font partie de la médecine allopathique traditionnelle qu'ils cherchent à éviter ou tout du moins à compléter.

J'en ai cependant trouvé une vague trace chez le Finlandais **Matti Pitkanen** qui, dans le cadre de ses travaux sur la TGD (Topological Geometrodynamics), propose une théorie unifiée de la physique, et émet l'idée de créer des ordinateurs quantiques à base d'ADN[1362]. Il pense que l'ADN communique "avec l'Univers".

Il s'appuie aussi sur les expériences de Luc Montagnier sur l'ADN. Matti Pitkanen fournit les bases de théories très spéculatives sur la conscience supposée de l'Univers[1363]. Ses théories d'unification de la physique sont tellement complexes qu'elles sont impossibles à comprendre, et, éventuellement, à valider par l'expérience ou à réfuter.

Mémoire de l'eau

Le dernier domaine à la frontière ténue entre la science et le charlatanisme est celui de l'eau. Il met en scène un modèle de pensée voisin de la théorie **Orch-OR** de Penrose consistant à vouloir tout expliquer de la vie à partir de quelques phénomènes physiques isolés et de niveau microscopique. On y retrouve pêle-mêle le phénomène de la **mémoire de l'eau**, son explication par l'**électromagnétisme**, et des théories parallèles sur la **structuration de l'eau**.

L'un des points de départ de tout cela sont les travaux sur la mémoire de l'eau de **Jacques Benveniste**. Ce spécialiste de l'immunologie et des allergies et directeur d'un laboratoire de recherche de l'Inserm à Clamart mène alors des expériences permettant de conclure que « *l'eau pourrait conserver un souvenir, une empreinte, de substances qui y ont transité* ». Accompagné de chercheurs israéliens, italiens et canadiens, il publie dans Nature en 1988 un article qui fera date mais sera vite contesté[1364]. Il y décrit une série d'expériences qui montre l'efficacité de l'anti-IgE provoquant la perte de granules contenant de l'histamine par un type de globules blancs, les cellules basophiles, ceci, même lorsque cet anti-IgE est dilué à répétition au point qu'aucune molécule de celui-ci ne peut se retrouver dans la solution.

[1361] Voir à ce sujet L'enjeu actuel du quantique par Jean-Michel Vaysse, 2016 (12 pages) qui positionne cette branche de la médecine quantique en faisant notamment référence à de nombreux travaux de chercheurs russes.

[1362] Dans Quantum Mind, Magnetic Body, and Biological Body, Matti Pitkanen, août 2018 (186 pages).

[1363] Dans TGD Universe as a conscious hologram, publié en février 2018 (612 pages).

[1364] Voir Human basophil degranulation triggered by very dilute antiserum against IgE, Jacques Benveniste et al, juin 1988 (3 pages) et Ma vérité sur la mémoire de l'eau par Jacques Venveniste, 2005 (122 pages) avec une préface de Brian Josephson, le prix Nobel, celui de l'effet qui porte son nom et est utilisé dans les qubits supraconducteurs ! Dans cet ouvrage publié après sa mort en 2004, Jacques Benveniste y raconte ses expériences, ses relations tumultueuses avec les mandarins de la médecine sur plusieurs décennies, l'histoire de la publication de son fameux article dans Nature en 1988 et d'autres expériences menées pendant les années 1990 et début 2000.

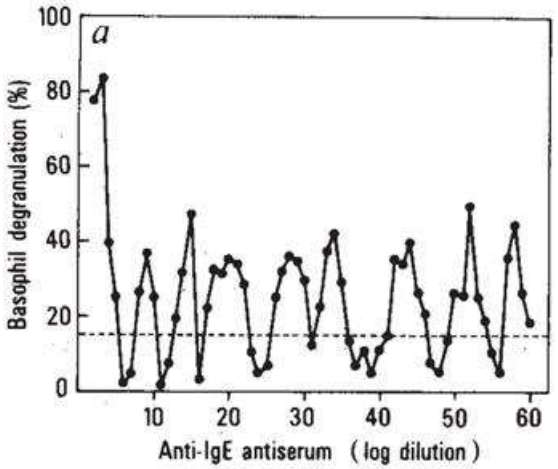
Pour que cela fonctionne, les solutions doivent être secouées vigoureusement après chaque dilution. C'est le principe de la dynamisation[1365] !

Dans l'article, il émet l'hypothèse que le phénomène s'expliquerait par la création de réseaux structurés dans l'eau ou par des champs électriques ou magnétiques persistants. Ils constitueraient une « mémoire de l'eau » qui a vu passer l'allergène dans le passé et en reproduirait les effets sur les cellules basophiles.

> Therefore we propose that none of the starting molecules is present in the dilutions beyond the Avogadro limit and that specific information must have been transmitted during the dilution/shaking process. Water could act as a 'template' for the molecule, for example by an infinite hydrogen-bonded network[12], or electric and magnetic fields[13,14]. At present we can only speculate on the nature of the specific activity present in the highly diluted solutions. We can affirm that (1) this activity was established under stringent experimental conditions, such as

A la clé, l'explication potentielle des effets supposés de l'homéopathie à haute dilution ! Les promoteurs de cette médecine empirique inventée par **Samuel Hahnemann** autour de 1810 dans l'ouvrage « Organon, de l'art de guérir » pensaient avoir enfin trouvé leur caution scientifique.

Les protocoles de tests et d'évaluation étaient entachés de nombreuses lacunes. Les solutions n'étaient pas analysées par spectrographie pour en déduire leur composition moléculaire[1366]. Seule une électrophorèse était utilisée qui permettait de détecter la présence d'ions[1367]. La présence d'histamine résultant de la libération des granules des basophiles n'avait pas évaluée[1368]. On s'est rendu compte dans d'autres expériences qu'il n'y en avait pas ! Qui plus est, le phénomène présentait un caractère cyclique d'une période de 8 dilutions (*ci-contre*), au gré des dilutions successives, mais en étant déphasé de quatre dilutions d'une expérience à l'autre. Sans qu'aucune explication ne soit fournie sur ce phénomène cyclique[1369].



La théorie électromagnétique qui expliquerait le phénomène est son autre talon d'Achille. Elle est faiblement substantiée. Ces ondes ne sont pas caractérisées, véritablement mesurées ni leur source expliquée. L'histoire de Jacques Benveniste est celle d'un expérimentateur curieux manquant cependant de bases dans des disciplines adjacentes autour de l'électromagnétisme. Il a toutefois creusé la piste des champs électromagnétiques à longue portée, inspiré par les travaux des physiciens italiens spécialisés dans l'électrodynamique quantique, **Giuliano Preparata** (1942-2000) et **Emilio Del Giudice** (1940-2014).

[1365] Il fonctionne aussi à l'envers ! Voir De l'eau en vrac dans les magasins pour remplacer les bouteilles en plastique par Helen Herault|, juillet 2020, qui fait allusion à l'offre d'H_2Origin qui filre l'eau et la regénère grâce à des hautes fréquences ! Et pourquoi donc ? Parce que la structure des molécules d'eau serait altérée lors de son transport !

[1366] De la spectrométrie Raman sera utilisée dans d'autres expériences, bien plus tard à partir de 2007, sur diverses souches homéopathiques.

[1367] Aux fortes dilutions, l'électrophorèse montrait qu'il n'y avait plus de molécule anti-IgG dans le principe actif.

[1368] Les expériences sur la mémoire de l'eau sont critiquées dans La fumeuse mémoire de l'eau par Henri Broch, un auteur spécialiste de zététique et pourfendeur des fausses sciences. Ce texte est un gros chapitre de son ouvrage Au cœur de l'extraordinaire (10e édition 2015). Il souligne que l'évaluation de la dégranulation était évaluée par la mesure du niveau de coloration des cellules basophiles. Avec deux niveaux mélangés : celui des cellules dégranulées et celui des cellules non dégranulées. Sans pour autant que les variations de couleur soient pour autant directement associables à la dégranulation. On pourrait ajouter dans l'étonnement le fait que ce genre d'expérience n'ait été réalisé que sur une réaction précise, sans que ses effets puissent être généricisé à d'autres réactions biologiques. La non reproductibilité d'une expérience dans d'autres contextes doit être une grosse source de doute scientifique.

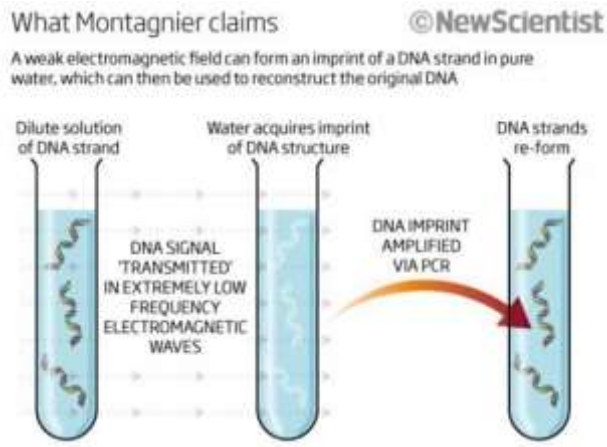
[1369] Ironiquement, le procédé utilisé n'empêche pas les réactions allergiques comme le prévoit l'homéopathie qui veut soigner le mal par le mal, mais à faible dose. Ici l'anti-IgE provoque la production d'histamine et ne l'empêche pas.

Il monte ainsi en 1990 une expérience avec le Laboratoire central du magnétisme du CNRS à Meudon qui montre que l'activité de la solution diluée est modifiée par son exposition prolongée à un champ magnétique. Mais ici, l'expérience porte sur des cœurs d'animaux, avec un appareillage électrique inventé par **Oskar Langendorff** (1853-1908).

Dans une autre expérience réalisée sur plusieurs années, il utilise aussi un amplificateur utilisant une carte son d'un micro-ordinateur pour transmettre les propriétés d'une solution à un autre liquide neutre. Cela aboutit au concept de « biologie numérique »[1370].

Après le décès de Jacques Benveniste en 2004, ses travaux sont repris par **Luc Montagnier**. Ce dernier est à l'origine du premier traitement contre le SIDA et prix Nobel de médecine en 2008. Il décrit des ondes de basse fréquence (7 Hz) qui seraient émises par les brins d'ADN. Il monte une expérience dans laquelle les ondes de molécules d'ADN sont transmises grâce à une bobine alimentée à 7 Hz à de l'eau pure dans une autre éprouvette. Une PCR est alors utilisée pour régénérer de l'ADN dans cette éprouvette (processus de démultiplication d'ADN, "réaction en chaîne par polymérase"). Et une électrophorèse sur gel est utilisée pour décoder l'ADN répliqué. Dans l'expérience, cet ADN correspond exactement à l'ADN de départ.

Son code aurait donc été transmis par onde électromagnétique [1371]. Mais problème, la documentation ne précise pas quel ADN a été utilisé comme amorce pour la PCR !



En effet, une PCR ne part pas de zéro et de nucléotides, mais utilise des brins d'ADN les répliquer[1372]. Les travaux de Luc Montagnier ont un lien de parenté avec ceux de l'Italien **Emilio Del Giudice**, encore lui, sur la structure de l'eau liquide[1373].

Cela ne vous surprendra pas d'apprendre que ce genre de découverte est plutôt controversée chez les spécialistes[1374]. Et la publication de Luc Montagnier n'a pas été faite dans une revue à comité d'auteurs. Mais il continue de publier, avec des équipes internationales, et sur des recherches intéressantes expliquant par la théorie quantique des champs le fonctionnement de la polymérase de l'ADN[1375].

[1370] Cette histoire est bien racontée dans L'âme des molécules, une histoire de la mémoire de l'eau par Francis Beauvais, 2007 (626 pages). L'auteur a été un des expérimentateurs de Jacques Benveniste.

[1371] Voir les explications dans La téléportation quantique de l'ADN, 2011 et dans l'article de Luc Montagnier DNA waves and water de janvier 2010 (10 pages). Montagnier et la téléportation quantique de l'ADN de Vincent Verschoore, janvier 2011, est la source de l'illustration.

[1372] Ce problème de PCR est relevé dans The Nobel disease meets DNA teleportation and homeopathy, janvier 2011.

[1373] Voir Illuminating Water and Life de Mae-Wan Ho, 2014 (18 pages) qui décrit les théories d'Emilio Del Giudice, qui est décédé cette même année.

[1374] Voir Luc Montagnier and the Nobel Disease par David Gorski, juin 2012.

[1375] Voir L'étonnante propriété de l'eau comme instrument de communication par Bernard Dugué, juin 2018 qui fait référence à Water Bridging Dynamics of Polymerase Chain Reaction in the Gauge Theory Paradigm of Quantum Fields par Luc Montagnier et al, 2018 (18 pages).

La relation entre l'eau et la physique quantique fait d'autres émules[1376]. Ci-devant **Marc Henry**, professeur de chimie moléculaire à l'Université de Strasbourg qui s'en est fait une spécialité[1377]. Il en connaît un rayon sur l'eau, de manière aussi bien documentée scientifiquement sur certains aspects qu'obsessionnelle par d'autres. Il cherche à expliquer tous les mécanismes de la vie par le biais du fonctionnement de la molécule d'eau. Il véhicule l'idée selon laquelle l'eau véhicule et transmet des tombeaux d'informations avec des analogies informatiques.

Il nous parle aussi d'exformation, à savoir d'information abandonnée par la conscience et qui se trouve dans le vide. C'est la variante « eau » des microtubulines de Roger Penrose ! Cela expliquerait l'omniprésence de l'eau dans les cellules (99% des molécules du corps en quantité) et fournirait au passage une base théorique à l'homéopathie. Pour lui, le vide quantique serait la source de toute matière et de toute énergie et expliquerait le rôle de l'eau comme vecteur d'information biologique. Il explique que dans le vide, l'ADN se détruit et qu'il lui faut de l'eau pour rester entier. Oui, mais en oubliant que l'ADN se conserve aussi dans l'éthanol ! Un détail, certes.

Enfin, il est membre d'honneur de l'association **Natur'Eau Quant**, une association militant pour « *une approche quantique de la nature utilisant l'eau comme vecteur d'information* ». Et tenez-vous bien, elle promeut « *la diffusion d'un mode de pensée basé sur la physique quantique des champs auprès de personnes utilisant l'eau, l'alimentation biologique ou biodynamique vivante, la naturopathie, les remèdes naturels, la musique, l'art pictural, le jeûne, les techniques de développement du soi, les états modifiés de conscience à des fins thérapeutiques en relation avec tout organisme vivant, et de manière plus large, toute personne développant des alternatives de vie écologique amenant à l'autosuffisance dans le respect total de l'environnement* ». En anglais, on appelle cela de la *crackpottery*.

J'ai découvert d'autres zones d'ombres entre des pratiques scientifiques à la limite de l'acceptable et la charlatanerie la plus totale. Nous en avons un exemple avec le site de **BeBooda.fr**[1378] qui véhicule en l'exagérant tout le discours sur l'eau quantique. Cela commence avec des recommandations anodines sur la consommation d'eaux minérales qu'ils recommandent d'éviter, pour promouvoir des compléments minéraux de la marque **Quinton**. Cela se gâte lorsque la présentation propose de restructurer l'eau parce que l'eau contient une mémoire qui emprisonne les ondes. Il y est même dit que « *Quand on filtre l'eau pour la rendre plus pure et fluide, on réveille sa mémoire et les fréquences d'émission correspondant aux polluants qu'elle contenait (germes, métaux lourds, ...)* » en s'appuyant sur les travaux de Luc Montagnier.

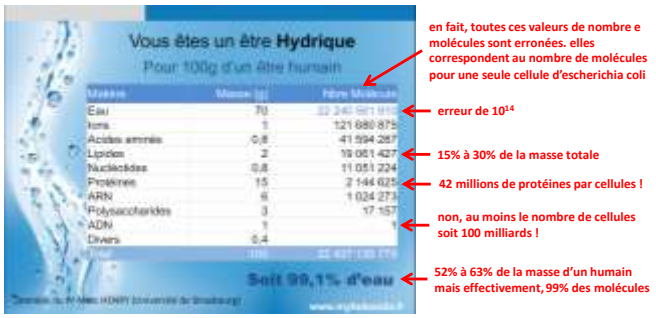
[1376] Hypothèses quantiques de mécanisme d'action des hautes dilutions homéopathiques, est une thèse de docteur en pharmacie de Mathieu Palluel, 2017 (252 pages). Sa première partie est une histoire assez bien fournie de l'homéopathie. Elle couvre aussi l'épisode des expériences de Jacques Benveniste et Luc Montagnier. La partie quantique démarre page 181 et est assez faible. On sent que le thésard n'était pas un physicien. Il fait un contre-sens sur l'équation de Schrödinger page 189. Il abuse un peu de la théorie quantique des champs et de l'électrodynamique quantique qui ne s'appliquent pas vraiment à l'eau à température ambiante. Page 201, le document indique que les molécules d'eau ont un diamètre approximatif de 3 nm alors qu'il est de 0,27 nm. Ça parle aussi page 221 du prix Nobel de « Serge Laroche » au lieu de Haroche. Bref, le document a mal été revu par les personnes qui ont validé la thèse. Et qui n'étaient d'ailleurs pas du tout calées en physique quantique.

[1377] Voir son ouvrage L'eau et la physique quantique par Marc Henry, 2016 (396 pages) et un extrait de 21 pages. Voir aussi ses conférences : L'information et l'eau par Marc Henry (53 mn), Pr Marc Henry - Approche Quantique de l'Eau. Forum à la rencontre de l'eau, novembre 2018 (2h) et Structure quantique cohérente et incohérente de l'eau liquide, 2011 (14 slides). Voir aussi L'homéopathie possède-t-elle des bases scientifiques ? (11 pages), L'Eau, la Terre, et les Hommes (11 pages), Eau et électromagnétisme le point de vue de la science, 2015 (1h57) où l'on entend que l'homéopathie dématérialise le médicament et où l'on apprend qu'il se passe quelque chose lorsque le curé bénit l'eau bénite, Eau, musique et physique quantique - Marc Henry, 2015 (7 mn) où il explique comment on utilise la physique quantique pour transformer une séquence d'ADN en morceau de musique. Il se présente aussi ou est présenté comme professeur de mécanique quantique, comme dans Scientificité de l'Homéopathie : l'avis du Professeur en physique quantique Marc Henry, février 2020.

[1378] Voir Les bienfaits de l'Eau, BeBooda, 2018 (36 slides).

On y découvre une citation d'un prix Nobel de Chimie, **Albert Szent-Györgyi** (1893-1986) selon laquelle « *La structure moléculaire de l'Eau est l'essence de toute vie* ». Renseignement pris, ce monsieur était prix Nobel de physiologie et de médecine, en 1937 pour sa découverte de la vitamine C. Il a bien produit des écrits sur la structure de l'eau, mais plutôt dans les cellules que dans les bouteilles d'eau[1379]. L'entourloupe scientifique est en partie là : si l'eau joue bien un rôle de structuration autour de molécules organiques dans les cellules, elle ne se structure probablement pas autant lorsqu'elle est dans des volumes plus macros, même associée à des minéraux et à des impuretés diverses.

L'eau formerait des clusters de molécules d'eau bien organisés qui capteraient et émettraient des ondes électromagnétiques. Et cette mémoire est évaluée à 1 Go par goutte d'eau, reprenant les thèses de Marc Henry. Certains slides comprennent des erreurs monumentales sur le nombre de molécules dans le corps, se trompant dans les légendes, confondant 100 g de corps humain et une bactérie (*ci-contre*).



Ces slides sont édifiants, mettant en valeur en les exagérant des travaux, contestés, montés en épingle ou difficiles à vérifier, de scientifiques, souvent japonais ou russes. On y découvre les travaux du russe **Konstantin Korotkov** et son expérience qui aurait démontré que l'eau sur laquelle on projetait des émotions négatives voyait son niveau énergétique baisser et réciproquement[1380]. Ce Korotkov est le créateur de l'IUMAB (International Union of Medical and Applied Bioelectrography)[1381], un organisme qui promeut l'usage d'appareils de bioélectrographie qui ne servent à rien.

Suivent les bienfaits du MRA (Magnetic Resonance Analyzer) de **Mazaru Emoto** (1943-2014). Il avait mené des expériences d'analyse de l'impact des émotions sur la structure de l'eau. Des expériences jamais reproduites de manière indépendante comme il se doit[1382].

[1379] Voir Biology and Pathology of Water, Albert Szent-Györgyi, 1971 (11 pages).

[1380] Voir The First Korotkov Intention Experiment, par Konstantin Korotkov, janvier 2018 ainsi que The Intention Experiment on H2O, 2007 (18 pages) qui avait reproduit ses expériences aux USA.

[1381] Il est aussi l'auteur de The Emerging Science of Water: Water Science in the XXIst Century par Vladimir Voeikov et Konstantin Korotkov, 2018 (253 pages), ouvrage ou courant de pensée qui ont certainement influencé les travaux de Marc Henry, à moins que cela ne soit le contraire.

[1382] C'est bien expliqué dans The pseudoscience of creating beautiful (or ugly) water par William Reville, 2011. Voir aussi le site Structure-altered water nonsense qui fait un bon inventaire d'offres commerciales d'eau structure aux USA. La mise en page style 1995 dessert le site mais l'inventaire des solutions est édifiant.

OK, les émotions peuvent générer des ondes infrarouges et des gaz pouvant être exhalés, produisant à leur tour une infime réaction sur de l'eau exposée[1383]. Cela permet de vendre au gogo une eau structurée concentrée qui permet de préparer de l'eau distillée, l'**Indigo Water** (*ci-contre*, source). En voici la description : « *A geometrically perfect water with the "Message" your body is waiting to receive. Dr. Emoto's Indigo Water contains eight ounces of highly charged hexagonally structured concentrate. By mixing one ounce of concentrate with one gallon of distilled water, you are creating eight gallons of structured water from this 8 ounce Indigo water. This is about a one month supply of structured water*". Pour $35. Ca ne précise pas si c'est de l'eau à boire ou pour la douche !

Le délire continue avec l'eau structurée de l'Américain **Rustum Roy**. L'eau structurée serait un antibiotique : « *une molécule d'eau structurée dans 100 millions de molécules d'eau potable peut détruire tous les germes présents dans une plaie. L'armée Américaine a utilisé cette eau en Irak et en Afghanistan. Obama utilise de l'eau structurée pour se laver les mains* ». Vérification faite, le seul exemple trouvable est celui de la guérison d'une plaie au pied et c'est de l'eau associée à de l'argent[1384]. Et comment restructurer l'eau dites-donc ? Simple : en la chauffant, avec des vortex, des champs magnétiques, de la musique, la force de la pensée, des « fréquences » ou des minéraux !

Le concept des vortex provient de l'astronome **Nicolaï Kosyrev** (1905-1983) qui avait découvert le volcanisme lunaire et du biologiste **Rupert Sheldrake** (1942), devenu expert en télépathie. Cela aboutit aux vortexeurs Voda de **Vodaflor** qui génèrent des tourbillons dans l'eau pour la structurer avec des modèles allant de 936€ à 3300€ selon le débit de structuration d'eau désiré.

Plus récemment, le discours autour des bienfaits de l'eau dans l'homéopathie s'est renouvelé avec l'intégration de l'électrodynamique quantique comme élément d'explication. Ça tombe bien, comme quasiment personne ne peut y comprendre quelque chose, sauf les physiciens de ce domaine qui vont immanquablement hausser les épaules, l'histoire peut continuer de se propager sans contre-expertise[1385]. Sans compter l'absence de protocoles expérimentaux permettant de vérifier quoi que ce soit. On est en pleine fausse science, car pas réfutable [1386]!

Pour conclure cette partie avant de passer aux plus belles escroqueries de la pseudo-médecine quantique, rappelons que la frontière est ténue entre la science à bas niveau et son interprétation à haut niveau, surtout lorsqu'elle est ensuite exploitée par des entrepreneurs sans scrupules.

[1383] Voir The experiments of Masaru Emoto with emotional imprinting of water, 2018 (11 pages).

[1384] Dans Ultradilute Ag-Aquasols with extraordinary bactericidal properties : the role of the system Ag-O-H2O, 2006 (13 pages). Rustum Roy est aussi l'auteur de The Structure Of Liquid Water; Novel Insights From Materials Research; Potential Relevance To Homeopathy, par Rustum Roy, 2009 (33 pages).

[1385] Voir Explaining Homeopathy With Quantum Electrodynamics par Antonio Manzalini et Bruno Galeazzi, 2018.

[1386] Heureusement, quelques scientifiques prennent le temps de démonter ces balivernes comme L'homéopathie confrontée à la physique par Alain Bonnier, 2014 (34 pages) qui démonte l'homéopathie de manière très didactique en s'appuyant notamment sur la constante de Planck.

Et nous n'avons pas fini d'en trouver de la même veine. Récemment, on a pu découvrir un comportement quantique étranger de l'eau dans des nanotubes de carbone[1387], des phénomènes de supraconductivité dans le cerveau[1388], un antibiotique qui se comporte comme une onde[1389] ou des élucubrations sur la cognition quantique[1390]. Cela alimentera sans doute de nouvelles vagues de mysticisme quantique !

Médecine quantique

Comme le souligne la maigre fiche Wikipedia sur la médecine quantique, cette discipline utilise abusivement le jargon de la physique quantique pour noyer le poisson et faire avaler des couleuvres à des gens qui sont prêts à tout pour trouver des remèdes à certaines pathologies que la médecine traditionnelle, bien ou mal exercée, ne peut pas traiter[1391].

Je crains fort qu'avec le bruit médiatique que l'informatique quantique va générer, on assiste à une recrudescence de la visibilité de la médecine quantique, en plus de l'effet Streisand limité qui sera généré par cet article. Le phénomène a déjà une bonne dizaine d'années d'ancienneté[1392].

Méthode de détection de fausses sciences

Les méthodes utilisées pour promouvoir de fausses sciences quantiques dans la santé (et en général d'ailleurs) sont assez facilement détectables pour l'esprit éveillé avec[1393] :

- Un **propos scientifique** associant un peu rapidement sciences humaines et biologie et faisant des raccourcis très rapides et approximatifs sur la physique quantique[1394].
- Quand ils existent, les **tests sont réalisés avec des échantillons trop faibles** pour être statistiquement représentatifs. Le propos associe souvent un bon nombre d'anecdotes ponctuelles non vérifiables. Les guérisons miraculeuses constatées à Lourdes sont même mieux documentées et d'ailleurs, aussi probables que celles qui interviennent en milieu hospitalier (source), à savoir comprises entre 1/350 000 et 1/100 000 cas.
- Nombre de spécialistes proposent la vente de **matériels de guérison divers**, assez chers, qui ne sont pas des dispositifs médicaux remboursés, et dont l'efficacité relève visiblement aussi de l'effet placebo[1395].
- Les solutions ciblent en priorité des **personnes vulnérables** (malades, séniors, etc).

[1387] Voir Evidence of a new quantum state of nano-confined water par G. F. Reiter et al, 2011 (5 pages).

[1388] Voir Possible superconductivity in brain par P. Mikheenko, 2018 (10 pages).

[1389] Voir Biologie quantique : un antibiotique se comporte comme une onde de matière par Laurent Sacco, avril 2020.

[1390] Voir What is quantum cognition? Physics theory could predict human behavior par Nicoletta Lanese, janvier 2020.

[1391] Ces méthodes sont aussi bien décrites dans Quantox - Mésusages idéologiques de la mécanique quantique" de Richard Monvoisin, paru en 2013. Voir aussi Sept idées fausses sur la physique quantique, de Julien Bobroff dans TheConversation, mars 2019.

[1392] Des conférences sur le sujet de la médecine quantique ont été organisées, surtout entre 2011 et 2013, comme le Congrès Quantique Planète 2012 de Reims avec un large panel d'intervenants dont le fameux cancérologue Henri Joyeux connu pour ses positions contre les vaccins, notamment celui de l'hépatite B. Le Programme de l'édition 2013 est aussi consultable, avec un grand nombre de praticiens du monde de la santé qui se sont convertis à la médecine quantique et autres médecines alternatives. Voir aussi Dr Jean-Louis Garillon : La médecine quantique rend visible l'invisible par Isabelle Fontaine, novembre 2017 et la vidéo Dr Jean Louis Garillon Partie 1 : Qu'est-ce que la Médecine Quantique ?, 2013 (5 minutes 40s).

[1393] Ces différentes méthodes sont décrites avec humour par l'Institut Supérieur de Charlatologie et son générateur automatique d'argumentaire ! Voir aussi cette mise en abîme de ces méthodes dans Monoxyde de dihydrogène – FAQ.

[1394] Exemple avec L'Univers Quantique, un autre livret gratuit de 26 pages de mybebooda (surtout slides 20 avec un baratin sur l'ADN et les photons, et qui cite un certain Wladimir Popenon alors qu'il s'agit de Vladimir Poponin et de son expérience d'ADN fantôme). Un charabia limite manipulateur.

[1395] La brochure du 2e Congrès International des thérapies quantiques de Lyon en 2011 contient une très belle brochette d'exposants de ces appareils pour gogos. Parfois, c'est plus léger techniquement comme ce jeu de cartes de conscience quantique proposé par Richard Gandon aux voyants professionnels.

- Le **côté vague des pathologies couvertes**. Certaines relèvent de la gestion de la douleur ou de ce qui peut être traité par effet placebo, comme la psychonomie[1396]. D'autres ciblent pêle-mêle toutes les grandes pathologies du moment : maladies chroniques, cancers et dans certains cas, même les maladies neurodégénératives.
- Des **CV à rallonge** avec des diplômes impressionnants et des cautions scientifiques à prendre avec des pincettes pour une bonne part des spécialistes de la médecine quantique. Il existerait même des "usines à diplômes" aux USA, où l'on peut à bon compte s'acheter un titre de docteur en médecine ou autre discipline de pacotille. Un peu comme dans feu l'Université Trump.
- Des **publications scientifiques** rares et quand elles existent, tout aussi rarement réalisées dans des revues avec validation par des pairs, sachant que cette validation n'est déjà pas suffisante pour être un gage de sérieux. Cela devient donc des publications "privées".
- Quelques **théories du complot** sur les agissements du lobby des sociétés de pharmacies et autres professionnels de santé prêts à tout pour empêcher des solutions alternatives d'émerger.

Il n'empêche que l'on trouvera des commentaires positifs des lecteurs de ces livres qui montrent que le marché des gogos est un marché florissant. Il s'inscrit dans un contexte de perte de confiance dans les politiques, dans les médias et dans les sciences et du développement de nombreuses théories du complot, alimentées par la fluidité d'Internet et des réseaux sociaux.

Certaines de ces pratiques sont dénoncées dans des sites spécialisés tels que Psiram qui est lui-même d'origine douteuse ou tout du moins pas documentée. Il a son propre anti-site, Antispiram visiblement lancé par l'un des praticiens mis en cause, Christian Daniel Assoun et qui a obtenu par décision de justice en 2016 leur déréférencement sur Google pour la page le concernant, mais pas une modification de son contenu qui est toujours en ligne[1397].

Ouvrages de prosélytisme de la médecine quantique

Passons en revue quelques-uns des thèses et des ouvrages de référence qui font la promotion de cette curieuse médecine quantique.

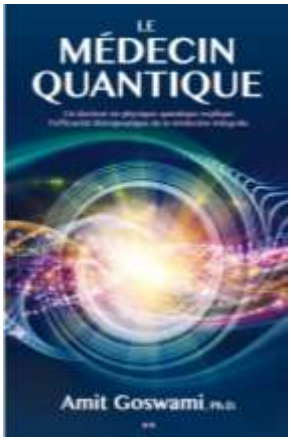
Le corps quantique, de Deepak Chopra (2009), ex-endocrinologue. L'auteur est issu du filon de la méditation transcendantale et devenu praticien ayurvédique, la médecine traditionnelle indienne. Selon lui, la pensée quantique explique certains cas de guérisons psychosomatiques qui ressemblaient à de l'auto-guérison. L'auteur est une star du domaine, surtout en Inde et aux USA, avec une prose vendue au total à plus de 10 millions d'exemplaires et une fortune personnelle estimée à plus de $80M (source). Le Corps Quantique semble être la traduction en français de *Quantum Healing* paru en 1988. Le contenu de ses ouvrages est faiblement scientifique, surtout lorsqu'il évoque les notions de quantique, qui sont souvent plus métaphoriques que physiques.

J'ai visionné à ce sujet l'éclairant débat entre Deepak Chopra et Richard Dawkins (Mexique, 2013, 1h13) qui met en avant la difficulté de réconcilier l'approche émotionnelle et symbolique de Chopra avec l'approche rationaliste et scientifique de Dawkins. Le débat porte à un moment sur l'intelligence supposée de l'Univers qui existe selon Chopra et à tous les niveaux, des particules élémentaires à l'Univers tout entier. Alors que cela n'a pas de sens pour Dawkins au-delà des êtres biologiques dotés d'un cerveau, ou d'ordinateurs l'imitant.

[1396] Qui est une fausse science de plus associant l'esprit et le corps.

[1397] La médecine quantique est aussi dénoncée dans Vers une critique de la raison quantique: les approches transcendantales en mécanique quantique de Patricia Kauark-Leite, 2010 (509 pages) ainsi que dans La médecine quantique, révolution scientifique ou arnaque? de Coline Vasquez et Bruno Lus, dans Slate en décembre 2017.

C'est un débat homothétique avec le lien entre la conscience et les pathologies que la conscience contrôlerait ou ne contrôle pas forcément. L'autre partie intéressante de ce débat concerne la notion de saut quantique sur l'apparition du langage ou certaines évolutions biologiques qui sont une vue de l'esprit pour Richard Dawkins. Ce dernier dénonce même "l'obscurantisme délibéré" de Chopra. Pour Richard Dawkins, la conscience s'explique ou s'expliquera par les neurosciences et sûrement pas par le galimatias de la méta-conscience de Deepak Chopra.



Le médecin quantique d'Amit Goswami (2013) est dans la même veine que les théories de Deepak Chopra. L'auteur est un enseignant en physique indo-américain qui a exercé dans l'Oregon entre 1968 et 1997, mais en physique nucléaire. Il se définit comme un activiste quantique qui a même sa propre Université Quantique qui semble être à la santé ce qu'était la Trump University aux business schools. Selon lui, l'activisme quantique par la conscience peut sauver la civilisation. Il démontre aussi scientifiquement (!) l'existence de Dieu en reprenant des thèses de Deepak Chopra sur la conscience de l'Univers. Dans son ouvrage qui est la traduction en français d'un livre paru la première fois en 2004, il explique l'efficacité thérapeutique de la "médecine intégrale" qui associe la médecine allopathique et les médecines plus ou moins douces, alternatives et traditionnelles, surtout indiennes mais aussi chinoises.

Le contenu scientifique de l'ensemble tient sur un timbre-poste. Ca parle de causalité descendante du quantique et de la conscience sur la matière, un propos qui associe les pathologies d'un organe du corps humain à l'effondrement quantique de ses fonctions provoqué par la conscience. L'ouvrage cherche à expliquer les effets et préceptes de médecines orientales (chakras, réincarnation, médecine ayurvédique, acuponcture) par de la physique quantique de café du commerce[1398].

En voici quelques morceaux choisis avec les "*champs morphogénétiques du corps vital*", "*quand l'esprit crée la maladie, il arrive que la guérison soit impossible à réaliser sur le plan de l'esprit. On doit alors faire un saut quantique jusqu'au supramental pour guérir*" ou "*l'effondrement quantique est aussi fondamentalement non local. Par conséquent, la non-localité de la guérison, comme dans la guérison par la prière, trouve une explication limpide dans le cadre de la pensée quantique.*". Donc, avec de l'intrication quantique, on peut relier tout à tout et tout expliquer. Ce n'est pas bien compliqué à comprendre !

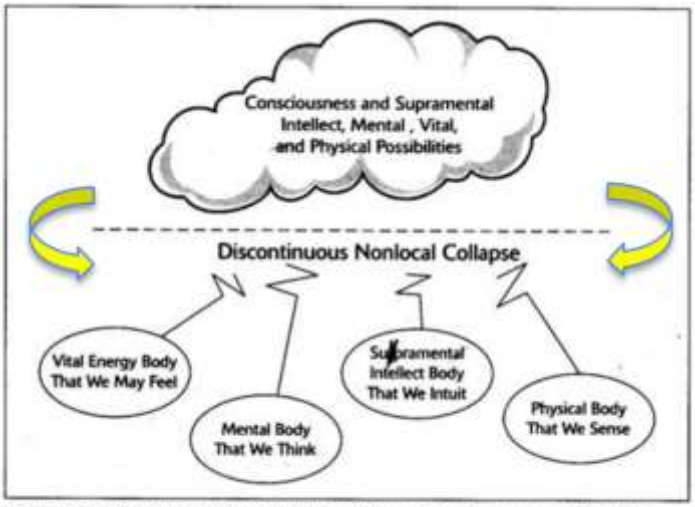


FIGURE 1-5. Quantum psychophysical parallelism. Consciousness mediates for physical, vital, mental, and supramental domains of quantum possibilities functioning in parallel.

D'autres que lui ont une vision légèrement plus scientifique de la nature quantique de la conscience, comme Ervin Laszlo même si ce dernier s'appuie un peu abusivement sur l'intrication quantique dans ses explications[1399].

[1398] Source de l'illustration : Messengers and Messages—then, now, and yet to come (15 pages).

[1399] Dans Why Your Brain Is A Quantum Computer, 2010. Cette thèse est en partie déconstruite dans The Myth of Quantum Consciousness, 2002 (19 pages), même si c'est un écrit antérieur.

Amit Goswami évoque des guérisons à distance par la prière en faisant référence à une expérience du physicien **Randolph Byrd** réalisée en 1988. La représentation statistique y était très faible avec 6 guérisons sur 26 malades, de pathologies cardiaques pas bien précisées. Il a été en fait démontré que les prières n'avaient pas d'effets à grande échelle[1400].

Il cite aussi l'expérience du Mexicain **Jacobo Grinberg-Zylberbaum** de télépathie[1401]. Il s'agissait de la mesure d'ondes EEG sur un participant pour évaluer l'impact sur lui d'un éclair de lumière arrivant sur l'un des participants, les deux étant dans des cages de Faraday. L'expérience a été répétée plus tard entre 2000 et 2004 en s'appuyant sur de l'IRM[1402].

Petit détail technique : il n'y a pas de transmission d'ondes radio entre les participants qui sont dans des cages de Faraday, pas de photon non plus, ni de particules ayant une histoire commune dans le cerveau des participants.

Donc, a minima, l'explication quantique sauce "expérience d'intrication d'Alain Aspect" est douteuse.

La santé, applications quantiques 2012 est un ouvrage collectif avec une douzaine de contributeurs, coordonné par Lara Lellouche, présidente de l'ARTTIQ (Association de Recherche sur les Technologies et techniques Informationnelles Intégrées et Quantiques), qu'elle a fondée en 2009 et dont le site n'a pas été mis à jour depuis 2011.

L'ouvrage reprend les communications d'un colloque organisé par ses soins en 2011 et sponsorisé par Glycan, la société de Christian Daniel Assoun dont nous parlerons plus loin.

Les contributeurs sont des adeptes internationaux de médecines alternatives, ce qui permet de faire un bon petit tour de diverses charlataneries quantiques.

- **Christian Agrapart** propose des traitements de chromatothérapie, à savoir l'usage de rayonnements colorés à des fins thérapeutiques, ciblés organe par organe, avec délivrance par transmission oculaire, par acupuncture sur les zones malades ou par exposition directe sur la peau. Au menu, les engelures et brûlures sont traitées avec du rouge et de l'orange ("*L'orange neutralise l'excès de chaleur en appelant localement de l'énergie froide.*"). Le vert assécherait les pieds restés trop longtemps dans l'eau (une pathologie bien connue) et le pourpre traiterait la frigidité. Heureusement, ces techniques ne prétendent pas guérir les infarctus, les maladies neurodégénératives, les diabètes ou les cancers. Cela a en tout cas toutes les couleurs de la fausse science selon Sébastien Point (source, 2015). Mais bon, cela pourrait peut-être marcher dans certaines circonstances.
- **Olivier Abossolo** est un anesthésiste qui fait la promotion de la médecine intégrative dans le cadre de chirurgie orthopédique. Il réduit le stress d'opérations avec des médecines douces diverses : surtout de l'aromathérapie, de l'homéopathie, des champs photoniques pulsés et magnéto-infrarouge laser.

  Cela permettrait la réduction de prises d'antalgiques. Il est surtout le promoteur en France des bains de pieds dans l'eau salée et électrisée de l'Anglais Pura Détox dont une variante fonctionne à l'ozone et aux infrarouges. Il fournit des huiles essentielles de son cru pour agrémenter ces bains de pieds. Au minimum, cela doit bien détendre.

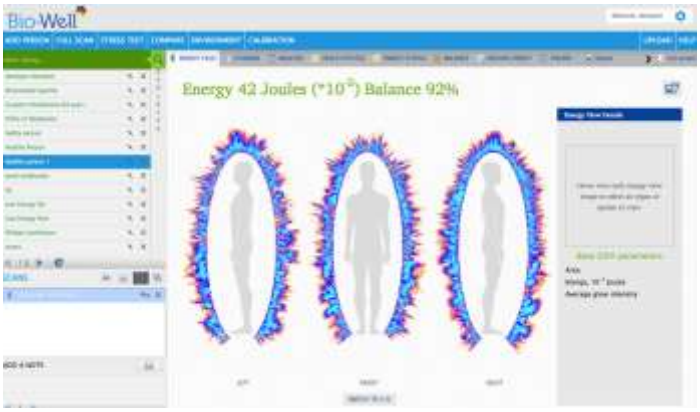
[1400] Voir Studies on intercessory prayer, Wikipedia.

[1401] Documentée dans The Einstein-Podolsky-Rosen Paradox in the Brain: The Transferred Potential, 1994 (7 pages).

[1402] Voir les détails et les résultats.

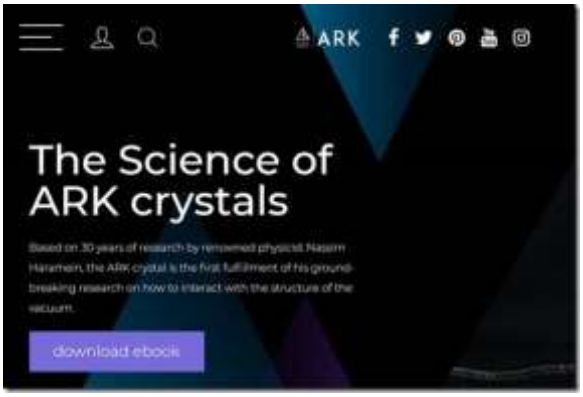
- **James Oschman** promeut un concept sur l'énergie vitale, à base de courants électriques. Il invente la notion des cellules périneurales du cerveau, qui ne sont visiblement que les cellules gliales qui entourent les neurones, mais avec un autre nom et qui génèrent de l'énergie qui va jusqu'aux mains.
- **Nadine Schuster** fait de la psycho-neuro-immunologie opérant sur les états d'oscillation des cellules. On raccroche vite lorsque l'on voit comment elle relie la physique quantique au vivant : "*physique qui MESURE les photons par « paquets », c'est-à-dire les grains de lumière (ou quanta) intervenant dans TOUS les processus du vivant en tant que porteurs des informations qui l'organisent. Quand un photon frappe un atome de métal (en biophysique et en biochimie également), il chasse un électron d'une orbite à l'autre, d'un niveau d'énergie à l'autre en provoquant un rayonnement : on pourrait dire que la VIE « est » ce jaillissement permanent de lumières au sein même du corps humain*". Elle en oublie que le quantique ne concerne pas que les photons et que la photosynthèse fonctionne mieux sur les plantes que sur l'Homme ! Sa médecine "*répare les déséquilibres oscillatoires des cellules afin de ramener l'ordre, qu'on appelle néguentropie (la néguentropie est la transformation de l'antimatière en énergie), au sein du tissu vivant.*". C'est bien la première fois que j'entends parler du rôle de l'antimatière dans la biologie humaine. Elle affirme que "*les maladies auto-immunes sont en fait des processus d'autodestruction liés au manque d'amour",* une technique de manipulation qui permet d'éloigner les adeptes de leur propre entourage. La page de présentation de ses recherches est un panaché détonnant où elle fait notamment la promotion des systèmes à base d'ondes scalaires, que nous étudierons plus loin. Son activité est liée à IVI "Invitation à la Vie Intense", citée aussi plus loin.
- **Ravi Roy** est un Indien adepte de la médecine holistique séphirotique, qui utilise l'arbre séfirotique de la Kabbale (tradition ésotérique juive) comme support de méthode d'examen, de diagnostic, de traitement, applicable à toutes les disciplines médicales. Il utilise aussi l'astrologie appliquée à la médecine. Il n'y a rien de quantique ni de fantastique dans tout cela.
- **Christine Fageot** pratique le Feng Shui et son texte n'évoque rien de quantique du tout du tout[1403].
- **Luc Bodin** parle de l'homme créateur de l'Univers, du pouvoir de la pensée sur le corps, de magnétisme et de médecine énergétique. L'onde peut se transformer en matière et réciproquement. Allez vous soignez avec ça !
- **Kiran Schmidt** est un Allemand qui fait de la "médecine informationnelle". Lui aussi fait la promotion de machines bizarres qui sont censée guérir de tout, notamment sous la marque **Inergetix**, qui n'a pas ou plus de site web.
- **Audun Myjska** parle aussi de médecine intégrée, qui fait l'association entre allopathie et médecines douces dans la lignée des méthodes d'Amit Goswami.
- **Konstantin Korotkov** est un Russe qui fait la promotion des caméras DGV Bio Well, des systèmes de détection d'aura autour des malades qui matérialiserait les chakras, via l'analyse de la "décharge gazeuse". Même pas de biophotons dans l'histoire ! Son texte est un amalgame de l'Histoire de l'Humanité et de la médecine, mais avec rien de quantique.

[1403] Le Feng Shui est référencé couramment comme une pseudo-science. Des descriptions extensives de la notion de pseudo-science sont fournies par Rory Coker dans Distinguishing Science and Pseudoscience, publié en 2011 ainsi que dans Seven Warning Signs of Bogus Science de Robert Park, publié en 2003. Le Feng Shui est décrit de manière critique comme un bric à brac ésotérique incohérent dans Alternative Medicine An Alternative Magical Mystery Tour de Steven Ranson, 2012 (129 pages, pages 72 à 77).



- **Nassim Haramein** parle de l'énergie de la création et aussi de la mémoire de l'eau, qui est comme il se doit quantique. C'est le cas du faux scientifique passé au spiritualisme qui se met à commercialiser des produits fantaisistes via sa Renonance Science Foundation. Le point de départ ? Des travaux, en apparence sérieux, sur sa théorie des champs unifiés, un vieux Graal de la physique fondamentale[1404]. Les sites web qui relaient les travaux d'Haramein sont tous du champ de l'ésotérisme comme Medium-Guérisseur. On peut prendre du recul lorsque l'on apprend que ce scientifique pense avoir découvert une source d'énergie infinie. A vrai dire, aucun des travaux de ce "scientifique" n'a été validé par ses pairs.

  Ce gourou commercialise les ARK crystals, des cristaux magiques qui guérissent ou améliorent la performance des sportifs. Ils publient même une étude portant sur l'amélioration de la performance d'athlètes. Une méthode en double aveugle avec effet placébo pour une moitié des testés. L'étude en question portait sur seulement 10 athlètes, 5 hommes et 5 femmes, avec des progrès d'environ 10%, donc situés dans la marge d'erreur de l'échantillon. Qui a réalisé l'étude ?



  Le laboratoire Energy Medicine Research Institute, visiblement versée dans les études sur des produits fantaisistes comme les placébos de LifeWave commercialisés dans un modèle pyramidal à la Tupperware. Ces cristaux permettraient aussi d'accélérer la croissance des plantes ! Les prix vont de 277€ à 1850€ (pour la version en boucles d'oreilles). Ceci s'inscrit dans une tendance de la vente de cristaux magiques qui date d'il y a quelques années et où l'offre est pléthorique[1405].

- **Vlady Sténanovich** est un Serbe qui veut aller dans le sens de la vie ce qui est plutôt sympa pour un médecin. Il parle d'émetteur d'ondes vives et de l'art du Chi. C'est le fondateur de "l'Ecole de la Voie Intérieure" en 1988, semble-t-il répertoriée comme une secte en 1995 en France.
- **Rav Michaël Laitman** est un Biélorusse qui promeut la force motrice de la nature et est aussi féru de la Kabbale.

[1404] Sa liste de publications scientifiques concerne les neutrons et des protons. Une partie des articles ont été publiés dans la revue NeuroQuantology qui n'est pas jugée sérieuse et dont le comité de relecture ne comprend aucun scientifique en physique quantique ou en neurosciences. Ce procédé de publication est connu et existe dans d'autres domaines comme en médecine. Voir à ce sujet Être juge et partie, ou comment contrôler une revue scientifique par Yves Gingras et Mahdi Khelfaoui dans The Conversation, juin 2020.

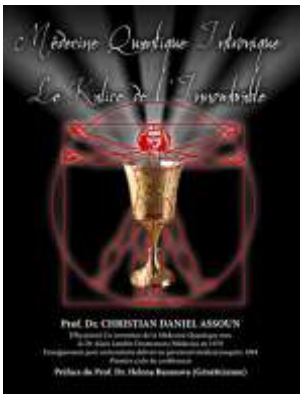
[1405] Voir Dark crystals: the brutal reality behind a booming wellness craze par Tess McCLure dans The Guardian, septembre 2019, A Cynic's Search for the Truth About Healing Crystals par Katherine Gillespie dans Vice, septembre 2017 et The Sickening Business of Wellness par Yvette d'Entremont, décembre 2016.

- **Claude Lagarde** décrit l'énergétique des cellules et des réactions catalytiques diverses, de maintien du gradient sodium/potassium dans les cellules, notamment nerveuses ainsi que du rôle des oligoéléments. C'est la partie en apparence la plus sérieuse et la plus longue du livre. Le gars est le créateur du laboratoire **Nutergia**, spécialiste de la nutrition cellulaire active, en gros, de compléments alimentaires.

Voilà une sacrée équipée pour s'occuper de votre santé !

La guérison quantique de Frank J. Kinslow (2012) reprend si ce n'est singe les mêmes théories d'Amit Goswami sur la guérison par la conscience. Il introduit la notion de "Quantum Entrainment", une méthode "*scientifique, rapide et efficace, qui permet de diminuer la douleur et de favoriser la guérison*". En quelques mots, il s'agit de faire envoyer par votre conscience des ondes vibratoires à vos organes pour les guérir. Par le jeu des interférences, elles vont annuler le mal. Encore un coup à la sauce du chat de Schrödinger avec application de la mécanique quantique du pico (particules élémentaires) au macro (les organes). Il s'adresse surtout aux douleurs physiques et émotionnelles. C'est une variante de la méditation. Pour le traitement de l'hypothyroïdie, il faudra éviter !

Ce genre d'ouvrage a la particularité d'être toujours très vague sur la notion de pathologie traitée, surtout si un appareil pseudo-médical est en jeu comme c'est ici le cas. Même si le "Quantum Entrainment" est censé fonctionner à distance[1406].



Médecine Quantique Intronique du Suisse Christian Daniel Assoun traite de la biologie quantique. C'est une forme de traité d'épigénétique décrivant la mémoire de l'ADN par la mécanique quantique. Selon lui, "*L'EAU est le premier liquide quantique : son état actuel est liquide alors* [que] *son état devrait être gazeux !".* Hum hum. Il met en avant les "*lois radiatives à l'ADN*-" correspondant aux thèses évoquées en début d'article. Ce livre décrit la présence d'un troisième caténaire d'ADN sous forme de plasma physique (hydrogène)[1407].Il y indique que son "*travail porte actuellement sur les parties INTRONIQUES qui représentent 95% de notre ADN et classées injustement de silencieuses ou voire inutiles.".*

Intronique au sens des "introns" de l'ADN, la partie des gênes qui est transcrite en ARN lors de l'expression des gênes, mais éliminée lors de l'épissage qui permet de générer un ARN mature qui sera ensuite utilisé dans les ribosomes pour fabriquer des protéines. A vrai dire, les introns ne représentent que 25% de l'ADN humain.

Le reste, environ 73%, correspond à des séquences effectivement non codantes de l'ADN de nos chromosomes, mais dont le rôle dans les processus de régulation des gênes se révèle progressivement avec la recherche. Les exons, la partie codante des gênes représente 1,5% de l'ADN humain (source).

Christian Daniel Assoun pense que l'ADN pourrait se renforcer avec "*l'aide de nouveaux éléments tétravalents tels que le Germanium ou le Silicium (propriétés optoquantiques reverses).*". Pourquoi le germanium et le silicium ? Car ils sont dans la même colonne du tableau de Mendeleïev que le carbone avec quatre électrons libres. Voilà une bonne idée pour créer de la vie extra-terrestre. Pourquoi donc la vie sur Terre n'a-t-elle pas utilisé le silicium qui est aussi abondant que le carbone ?

[1406] Si vous adhérez, l'auteur organise des séminaires en France sur sa méthode et la version anglaise de son ouvrage est téléchargeable ici.

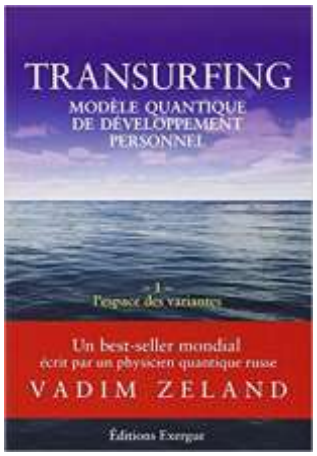
[1407] C'est aussi documenté dans Le 3ème Brin (ou 3ème Caténaire) de l'ADN ou DNA du même auteur et qui date de 2011/2012.

L'une des raisons est que l'oxyde de silicium (SiO_2) est inerte et solide tandis que les oxydes de carbone (CO, CO_2) sont gazeux donc, plus facilement recombinables avec d'autres atomes et molécules. Enfin, le carbone est plus abondant que le silicium sur la surface de la Terre. Par contre, le SiO_2 est très utile dans les chipsets quantiques CMOS du CEA-Leti (procédé SOI et FD-SOI) !

Christian Daniel Assoun est aussi le fondateur de **Glycan Group**, en 1996. La société commercialise du silicium organique pour différents usages et notamment comme complément alimentaire. Leur filiale Glycan Pharma a été radiée du registre du commerce en 2012. La société est en concurrence avec Silicium Espana, une société liée à Loic Le Ribault, décédé en 2007, lui aussi passionné de silicium organique. Les deux sociétés ont connu un différend juridique en 2011, sur l'usage de la marque G5.

Enfin, Christian Daniel Assoun est aussi président du comité scientifique du Collège Francophone de médecine quantique et alternative lancé en 2015.

Deux autres ouvrages reprennent des thèses composites des précédents : **Transurfing, modèle quantique de développement personnel** de Vadim Zeland pour qui « *Quand les paramètres de l'énergie mentale changent, l'organisme se déplace vers une autre ligne de vie.* » et **Médecine, le grand tournant vers la médecine quantique** de Simone Brousse. En France, un certain Olivier Masselot propose du coaching et de la formation et des conférences de transurfing (exemple). Il existe même une Quantum University pour enseigner toutes ces charlatanneries.



Il y a mieux puisque vous pouvez aussi gérer votre cheval avec des soins quantiques. Une conférence était même organisée sur le sujet en 2017 sans qu'il soit possible de savoir si l'expérience avait été répétée.

Il existe aussi de la **permaculture quantique** si vous jardinez qui recycle un bon nombre des élucubrations citées dans ces dernières pages.

J'attends avec une impatience fébrile l'arroseur quantique de Gardena qui évite de tirer les tuyaux dans le jardin !

Générateurs d'ondes scalaires

Le top du top de l'escroquerie de la médecine quantique sont les **générateurs d'ondes scalaires**[1408]. Le procédé est décrit dans Les ondes scalaires, 2014, dans Alternative Santé par un certain Docteur Hervé Janecek.

[1408] Voir la fiche sur les ondes scalaires du site Psiram ainsi que Ondes et croyances paranormales par Henri Brugère, 2009. Cela permet de prendre du recul sur cette interview d'un vétérinaire faisant la promotion des ondes scalaires :Voir Interview du Dr Hervé Janecek - Les Ondes Scalaires, la lumière qui nourrit et qui guérit ! | Bio Infos Santé, 2018. Le tableau intégré dans l'article comparant les ondes électromagnétiques aux ondes scalaires vont son pesant de cacahuètes ! Notamment avec les neutrinos ! Voir aussi Ondes scalaires : qu'est-ce que c'est ?, du site Quant-essence. Il décrit les CEF (Correcteurs d'Etat Fonctionnels) conçus par le russe **Sergeï Koltsov**.

Ça commence très mal avec le préliminaire qui dit que *"Des chercheurs de l'Université du Pirée avancent que notre métabolisme de base nécessite quelques 12 000 calories à fournir chaque jour, dont un quart au maximum proviendrait des aliments solides ; un autre quart serait tiré - grâce à nos mitochondries - **de l'hydrogène de l'eau bue** ! Et enfin 50% de nos besoins énergétiques seraient fournis par la **lumière cosmique touchant la terre** !* [NDLR : celle du Soleil ?] *Certaines personnes seraient même capables de se passer de nourriture physique et de ne **se nourrir que d'air, d'eau et de lumière** !"*.

On aimerait bien voir la tête de ces personnes ! Le malheureux auteur de ces inepties a loupé toutes ses classes de biologie moléculaire et ne connait visiblement pas le cycle de Krebs qui décrit le métabolisme énergétique des cellules à base de glucoses ! Pourtant, c'est un docteur ! Au passage, il est bien entendu impossible de trouver des traces web des travaux de ces chercheurs du Pirée !

Dès qu'on a lu cela, le pipomètre n'est plus dans un état superposé. Il explose en "Alerte Rouge" ! C'est confirmé avec Les ondes scalaires, la médecine de demain. Tout cela est déjà bien entendu déjà référencé comme faisant partie des pseudo-sciences (Wikipedia, RationalWiki). Concrètement, il s'agit d'ondes électromagnétiques associant une onde à polarisation horizontale et une autre à polarisation verticale de même fréquence mais déphasée de 90° ou d'un quart de longueur d'onde. Il n'est pas impossible que ces ondes aient un effet sur les tissus biologiques mais il n'est pas véritablement qualifié.

Les ondes scalaires ont été promues initialement par un certain **Thomas Bearden** aux USA ainsi que par le Russe **Sergeï Koltsov** avec ses Correcteurs d'Etat Fonctionnel (CEF[1409]). Bearden explique cela dans une interview de 1991 ! Il avait aussi inventé un **MEG** (Motionless Electromagnetic Generator) capable d'extraire l'énergie libre du vide et donc, de générer plus d'énergie qu'il en consommait.

Produit qui n'a bien entendu jamais été commercialisé et qui rappelle les théories **synergétiques** du professeur Vallée des années 1970. Les ondes scalaires permettraient aussi de traiter le diabète (I ou II ?), les calculs rénaux, la maladie de Parkinson, les infarctus, l'arthrose, le cancer et aussi le vieillissement. N'a pu qu'à ! Pour ce qui est des calculs rénaux, il vaudrait mieux faire appel à des ultrasons.

Quant au diabète type I, lié à la destruction auto-immune des cellules bêta des îlots de Langherans dans le pancréas, on ne voit pas comment des ondes, quelle que soit leur nature, ramèneraient des cellules mortes à la vie.

La solution proposée ? Des générateurs d'ondes scalaires comme le SWD de l'Allemand **INDEL** à 8820€ qui est distribué en France par la société **Cytobiotech** depuis 2013. Vu son prix, il cible les professionnels dans une sorte de modèle de Ponzi. Ce générateur produit un champ d'ondes scalaires d'une tension de 2V. Il comprend aussi un accessoire de modulation par la musique destiné aux cabinets de thérapie et aux centres de bien-être. On en trouve aussi chez **QuWave**, qui ne sera pas intégré dans les startups du calcul quantique.

[1409] Voir cette vidéo Correcteurs d'Etat Fonctionnel (CEF) - Plaques de Koltsov, 2014 (55 minutes) qui est un bon condensé de n'importequoiisme scientifique.

Il y a aussi l'**EPFX-SCIO Biofeedback** du Professeur William Nelson qui combine les thérapies globales et la physique quantique avancée (*ci-dessus*). Le dispositif scanne le corps sur 10 400 fréquences différentes pour détecter les pathologies. Il rééquilibre ensuite l'énergie du corps avec un biofeedback quantique. Le joujou propose 200 thérapies de biofeedback avec le plus grand logiciel de santé du monde (qui pourtant n'a pas été développé par Donald Trump ni par SAP) intégrant les philosophies occidentales et orientales[1410]. Ce dispositif est proposé en France pour faire de la médecine prédictive par la thérapeute quantique **Jacqueline Jacques**.

Elle forme les profanes à l'usage de l'EPFX-SCIO qui comprend un boîtier diffuseur d'ondes, relié au patient par des capteurs attachés à ses chevilles, poignets et crâne. On pourrait presque faire à la fois un EEG et un ECG avec ! Le tout n'a d'effet que placebo.

Une autre société vend un produit équivalent, **Physioquanta** lancée en 2005 et avec 1700 machines vendues à ce jour et 4M€ de CA en 2016. Le **Physioscan** «*repère et corrige les déséquilibres énergétiques*», l'Oligoscan, «*évalue en un instant minéraux, oligoéléments, stress oxydatif et métaux lourd*[1411]*s*» et le Milta, «*associe de façon synergique des émetteur lasers, des diodes infrarouges et des diodes RVB, fonctionnant dans un tunnel magnétique*».

Le descriptif des bienfaits du Physioscan sont à géométrie variable. Il est proposé par certains naturopathes pour faire un bilan de santé "quantique". Son descriptif met alors une fois encore tous les voyants au rouge, mais différemment : *« Issu de la recherche spatiale russe, le Physioscan permet d'écouter les fréquences émises par chaque cellule, tissu ou organe et de repérer les dysfonctionnements. Analyse rapide du niveau énergétique des différents organes afin d'évaluer la fonction de chacun ainsi que l'état de santé globale de l'individu. Détermination du terrain de l'organisme. Estimation de la meilleure action à poser afin d'éviter une dégradation de la santé. Correction des déséquilibres énergétiques grâce à la Méta-thérapie et à la ré-information* ». La sémantique utilisée se situe au top de l'échelle exponentielle du pipotron.

Le produit est vendu par **Santévie** sous l'appellation Biospect. « *Avec son scanner volumétrique, le Biospect effectue son analyse informationnelle dans les profondeurs des tissus jusqu'à l'ADN.* » C'est un « *Scanner volumétrique de l'organe à l'ADN* ». Voilà une invention extraordinaire permettant de faire du séquençage de l'ADN à distance, Illumina n'a qu'à bien se tenir. Bien entendu (présentation) !

J'ai trouvé une explication sur "la recherche spatiale russe" (source). Elle emploie une technique d'amalgame énorme : "*Les Russes ont été les premiers à travailler sur la physique ultra-corpusculaire ou quantique pour laquelle Nikolaï G. Bassov et Alexandre M. Prokhorov ont reçu le Prix Nobel en 1964 au sujet de la découverte du maser (précurseur du laser). Leurs progrès fulgurants sont dus à leurs découvertes faites pour la conquête spatiale*".

[1410] Voir How one man's invention is part of a growing worlwide scam that snares the desperate ill.

[1411] Voir sa fiche gratinée dans le site Psiram qui lutte contre les fausses sciences.

Ces chercheurs ont bien contribué à la découverte des masers et lasers mais aucunement à des applications ésotériques comme celle du Physioscan. On peut trouver un peu plus de littérature sur les guérisseurs russes. Cela ajoute une règle de plus à notre détecteur de pipeau : plus c'est loin, plus c'est louche car c'est plus difficile à vérifier !

Le Physioscan existe aussi dans un modèle perfectionné, le **Quantascan** de Quantaform (source 1 et source 2). Ce genre d'outil serait proposé par des dizaines de naturopathes en France[1412]. S'il s'agit de gérer des troubles bénins, pourquoi pas, mais lorsqu'ils sont proposés pour traiter des pathologies graves (cancers, maladies cardiovasculaires), cela devient un exercice illégal de la médecine, et surtout… c'est dangereux.

Ainsi, au sujet du Quantascan, on peut lire : "*Le traitement mis en œuvre par le Quantascan ne remplace pas un traitement médical prescrit par le médecin, mais il permet de vérifier l'efficacité de celui-ci et de le compléter le cas échéant. Ses domaines d'application sont aussi nombreux que les spécialités médicales (cardiologie, pneumologie, traumatologie, gastro-entérologie, gynécologie, urologie, stomatologie, dermatologie, ophtalmologie, neurologie, rhumatologie, ...), et de nombreuses statistiques médicales viennent confirmer l'efficacité des traitements et valider les résultats obtenus*". Les statistiques médicales sont-elles disponibles ? Difficile à trouver !

Heureusement, certains médias font leur travail. C'est le cas de Coline Vazquez et Bruno Lus dans La médecine quantique, révolution scientifique ou arnaque? publié en décembre 2017 sur Slate. Il fait état d'une décision de l'Agence Française de Sécurité Sanitaire qui interdisait en 2009 la publicité mensongère sur le Physioscan et produits voisins (source). Ce qui n'empêche visiblement pas de nombreux sites de continuer à contourner cette interdiction.

Des tests "scientifiques" sont parfois évoqués sur les sites de produits relevant de fausses sciences. On peut y détecter quelques entourloupes mais ce n'est pas toujours évident. La plus classique est celle de la corrélation entre deux phénomènes, qui n'induit pas forcément une causalité. La seconde est une explication alambiquée d'un phénomène. La dernière, dans la santé, relève de la difficulté à faire la part des choses entre un remède sans effets et l'effet placebo. Enfin, il existe de nombreuses erreurs méthodologiques dans les tests pouvant avoir été effectués, comme l'usage de tous petits échantillons qui n'ont donc aucune valeur statistique. Et par des laboratoires pas forcément recommandables.

Médaillons quantiques

Un panaché de ces méthodes est proposé avec le "médaillon quantique" phénoménal de Osenslife qui permet de traiter plein de bobos. Il avait été découvert fortuitement dans le magazine Séniors-Actuels par Fanny Bouton. C'est le genre de revue qui publie facilement des articles et des publi-rédactionnels à la véracité scientifique plus que douteuse. Lisez si vous le pouvez le texte ci-dessous, c'est édifiant ! Il a l'air de reposer sur le principe des CEF (ou Functional State Correctors) de Sergeï Koltsov.

[1412] Les naturopathes se sont emparés de la médecine quantique depuis des années. Voir par exemple **Drouot Production** qui propose une formation « Outils et pratiques de l'évolution de la conscience » dans un programme de formation sur les thérapies quantiques et vibratoires. **L'Espace Tellura** propose en Suisse des formations sur les bioénergies et la conscience élargie, l''offre du Psycho_Bio_Énergéticien **Frédéric Dreyfus** qui vous aide à trouver le point Zéro dit "point de convergence" pour réinitialiser votre ADN quantique et celle d'harmonisation quantique Alteralliah de **Marie-Claude Palau-Reault**. Tout ça est à pleurer ! Voir cette bonne mise en perspective dans La médecine quantique, révolution scientifique ou arnaque? par Coline Vazquez, 2017.

On y découvre que « *L'une des théories de thérapie quantique veut qu'autour de chacun d'entre nous il y ait 4 plans émettant un rayonnement qui interagit avec tous les êtres vivants. Ces plans sont le sens, le plan ondulatoire, l'énergie et la matière. Il forme le flux de vie. Le travail du thérapeute selon ces plans sera de rétablir leur harmonie chez le patient afin de ressusciter le flux de vie* ».

Les deux pages suivantes contiennent une publicité sur le médaillon évoqué dans les deux pages précédentes de rédactionnel. Le site du fournisseur contient un dossier scientifique censé donner confiance. Si c'est scientifique, c'est que cela doit être sérieux ! Il est basé sur le retour d'expérience de 4500 clients et fait appel à quatre laboratoires d'analyse scientifiques indépendants. Seulement voilà, aucun des tests présenté ne concerne 4500 personnes !

Le premier test concerne le développement de bactéries dans des verres. Il a été réalisé en 2017 par le Laboratoire Berthet Bernard, situé en Haute-Savoie, spécialisé dans les analyses agroalimentaires. Le fondateur est un pharmacien spécialisé en nutrithérapies. Sa bio datant de 2009 est raccord avec ce que fait Osenslife. Elle évoque l'énergétique humaine et la notion de corps éthérique qui imprègne les corps matériels. Le tout relié à la présence de bactéries dans le corps. Il y a comme qui dirait un biais cognitif dans le laboratoire !

Le test réalisé concerne la culture de la bactérie commune Escherichia coli, présentée comme pathogène alors qu'elle occupe la flore intestinale et que seules certaines variantes sont pathogènes. Une autre bactérie est testée, la lactobacillus plantarum, qui ne tolère que de faibles concentrations en oxygène. Elle se développe avec du sucre. Ces deux bactéries sont anaérobies, à savoir qu'elles n'ont pas besoin d'oxygène pour se développer. Le test indique « *19 à 28 % de moins de bactéries dans le récipient où le disque Osens a été posé... ce qui est absolument remarquable !* ».

L'explication donnée ? « *Le disque OSENS est un dispositif de «traitement quantique comprenant une imbrication d'ondes de formes primordiales. Son créateur allègue que celles-ci modifient notamment les propriétés de l'eau et la «revitalise» en plaçant le disque sur un verre d'eau.* ». Il faudrait donc creuser le protocole expérimental pour trouver le lièvre.

On y retrouve un problème classique qui rappelle les travers du machine learning : l'expérience trouve une corrélation entre le fait qu'un disque soit posé sur le verre et la croissance des bactéries. Cela ne fournit cependant en aucune façon une causalité sur les caractéristiques du disque et sûrement pas ses propriétés quantiques. On peut imaginer d'autres explications : un nombre d'expériences insuffisant, des réactions chimiques avec les composés métalliques du médaillon (qui ne sont évidemment pas indiqués) et le fait qu'il bloque l'entrée d'oxygène et l'azote dans le verre, même si les bactéries testées sont anaérobies.

De simples réactions chimiques n'auraient en tout cas aucune origine "quantique" magique. Et cela ne prouve évidemment pas que le médaillon serait capable de détruire les mauvaises bactéries du système digestif à distance. Bref, cela ne prouve aucun effet thérapeutique du médaillon.

Un second test a été réalisé par le Laboratoire **Emitech** qui est spécialisé dans les tests électromagnétiques. Il mesure le taux d'absorption des ondes DAS sur un corps exposé à un smartphone protégé par le médaillon Osens. Que trouve le test ? Que le médaillon ne réduit les ondes des smartphones que de 2,7%. Bon, c'est peut-être normal puisque le médaillon est placé au milieu du smartphone testé (un Galaxy). En général, les antennes sont sur les bords des smartphones, pas au milieu ! Et le test n'était réalisé qu'en 2G et 3G. Il montre juste que le médaillon n'est pas un anti-ondes. On est bien avancés ! Cela n'en prouve pas les effets ! C'est juste le test d'une négation !

Un troisième test montre une réduction de l'agglutination des cellules sanguines, toujours en utilisant le médaillon avec son smartphone. Le test est réalisé dans un laboratoire de l'Ile Maurice et sur un échantillon de seulement quatre personnes. Il n'a donc aucune validité statistique ! Et le sang testé est récupéré sur le doigt.

En parcourant ces trois tests, on est en droit de douter de leur véracité. Mais il faut se les palucher et disposer d'un minimum de bagage scientifique et de sens critique pour prendre du recul. Le gogo de base se fera facilement avoir !

Ces médaillons pour smartphone sont devenus monnaie courante depuis plusieurs années et ciblent une autre phobie, celles des ondes et de la 5G[1413]. C'est le cas des médaillons Quantum Shield de **Quantum Science** (sur Amazon et Alibaba). On en trouve aussi sous forme de clés USB **5G BioShield** qui contiennent un « *catalyseur holographique quantique* »**.**

C'est évidemment un énorme bullshit quantique de la première espèce. C'est accompagné d'une justification scientifique qui ne vaut pas tripette[1414]. La FTC américaine dénonce ces produits comme étant de vulgaires scams[1415].

Dans le domaine des appareils quantiques farfelus, terminons avec le **Quantum 5 Ozone Generator** utilisant la technologie Neos Technology de l'américain **Longevity Resources** (sources). Il utilise une électrode en quartz. C'est censé aider à purifier l'air ambiant d'intérieur. Il y a un inconvénient majeur : l'ozone peut aussi être toxique pour le corps humain et générer des problèmes respiratoires. Il peut aussi altérer la santé des plantes.

Il y a aussi des cas où la pseudo-médecine quantique vire au quasi-auto-parodique comme dans cette notion de plancher neuroquantique qui a l'air d'appartenir à la catégorie du Gorafi[1416].

[1413] Voi le vidéoblog Deus ex Silicium qui dénonce des arnaques équivalentes comme les patches anti-ondes de Fazup (qui ne sont pas présentés comme étant quantiques) ou l'oscillateur Magnétique de Décompensation de CEM-VIVANT.

[1414] Voir "Aton" True Cell, Atom and Particle Concept par Ilija Lakicevic, 2019 (8 pages).

[1415] Voir Cell Phone Radiation Scams, 2011.

[1416] Voir la vidéo Je construis un plancher neuroquantique, avril 2020.

Bref, la médecine quantique émergera peut-être un jour au gré des découvertes scientifiques, mais celle qui est proposée aujourd'hui relève pour l'instant essentiellement du charlatanisme. Elles ont l'avantage de générer au minimum un effet placebo pour les utilisateurs et de remplir le porte-monnaie de leurs promoteurs. Sauf que cela peut être dangereux si l'effet placebo est utilisé en lieu et place d'un traitement traditionnel incontournable pour rester en vie.

Je ne jetterai pas pour autant aux orties toutes les techniques et approches évoquées dans ce texte. Dans le tas, il y en a peut-être qui ont du sens, même s'il manque encore à la fois un corpus scientifique et des preuves plus solides pour les étayer.

Une fausse science se détecte cependant assez facilement lorsqu'elle est promue avec un jargon ésotérique ou décalé par rapport au champ scientifique classique du produit (onde, matière, vibrations, vortex). Le détecter peut nécessiter de disposer d'une culture scientifique généraliste et parfois spécialisée dans le domaine. Le discours va exploiter des mots qui ne signifient rien comme "l'énergie", "les vibrations", ou "les ondes", sans plus de précisions, par les gourous qui les relaient, sans avoir compris leurs sous-jacents scientifiques et leurs nuances.

Management quantique

Le management quantique est une nouvelle pratique en vogue qui cherche à s'inspirer des principes généraux de la mécanique quantique. Ses praticiens sont fréquemment des adeptes de sciences plus ou moins occultes qui se sont reconvertis pour attaquer des marchés d'entreprises plus solvables que celui des gogos du grand public.

Solvable mais pas moins crédule, malheureusement. La vulnérabilité de cadres et dirigeants éduqués, y compris BAC+5 ou plus, aux thèses les plus farfelues est toujours déconcertante.

J'ai ainsi dégotté le coaching quantique d'un certain Olivier Honsperger (vidéo, 2016) qui mélange allègrement mécanique quantique, épigénétique et modifications des gênes par l'action de la pensée pour prodiguer ses conseils aux entreprises. On n'est pas loin de Deepak Chopra. Alors, Etes-vous prêts pour le management quantique ?. A vrai dire, il n'y a pas le feu au lac. Ne vous lancez pas tête baissée dans l'organisation d'un offsite Métaplan quantique dédié au travail d'équipe et au leadership dans un Chateauform de circonstance. Sauf si vous avez le budget pour et de bonnes activités extra-scolaires prévues au programme.

Mais si vous y tenez vraiment, vous pourrez aussi faire appel aux services de Muguette Bruneau, hypno-thérapeute après avoir été spécialiste de la défiscalisation. Son site Management Quantique fait la promotion d'un management qui « humanise la performance ». Personne ne sera contre car peu de managers sont opposés à toute forme d'humanisation, même d'un tableau Excel ou d'un reporting Salesforce.

La description de l'approche fera évidemment s'esclaffer les spécialistes de la mécanique quantique : *« Le Management Quantique s'inspire des dernières découvertes en matière de neurosciences. La mécanique quantique nous explique que tout existe déjà et donc que le champ des possibles est infini. […] La théorie des cordes* [qu'elle se garde bien d'expliquer] *affirme que tout ce qui compose l'univers est fait d'infimes parties VIBRANTES et qu'elles nous informent en permanence* [via son smartphone ou la fibre ?]*. Nous sommes donc entourés d'informations. Mais savons-nous les décrypter ? A partir de ces observations, le management quantique nous apprend à développer notre sens de l'observation, nos ressentis afin de percevoir un maximum d'informations* ». Nous avons droit à une théorie du non-déterminisme et de la force de la volonté. Le management quantique serait la capacité à remettre en question nos perceptions. Donc, en ayant de l'empathie. Tout ça pour ça !

Pour autant, on peut en effet identifier de nombreuses analogies entre la physique quantique et le management au sens large du terme. J'ai repris pour cela les principales bases de la mécanique quantique et les ai appliquées à la vie en entreprise. Toute ressemblance avec une situation vécue serait totalement fortuite ou voulue, comme vous le souhaitez.

La **quantification** veut que certaines valeurs physiques ne puissent être que très précises, discontinues et pas arbitraires. Comme le niveau d'énergie d'un atome d'hydrogène ou le spin d'un électron.

Après tout, un salarié n'est qu'une case dans un tableur. Il est là un jour et hop, il disparaît le lendemain. La gestion des effectifs est en effet quantique. L'effectif d'une entreprise à un moment précis est un entier. Mais si on en fait la moyenne sur une période en tenant compte des départs en cours de période, des temps partiels, des CDD, des contrats d'apprentissage, des sous-traitants et des gens dont on n'est pas sûr de leur activité réelle, ce n'est plus un entier mais un nombre de FTEs (full time employees) ou ETPs (équivalents temps plein) qui est au minimum l'addition de fractions. Heureusement, ce n'est jamais un nombre complexe et on échappe aux espaces de Hilbert pour les représenter. Ouf !

La quantification se manifeste aussi dans le *sand bagging* qui veut qu'un manager commercial va transmettre ses objectifs au niveau du dessous en ajoutant une marge de sécurité « quantique ». Le dernier maillon de la chaîne, le malheureux commercial de base, va récupérer un objectif plus grand que celui de toutes les couches de management du dessus.

Seules certaines strates de management ont cette latitude. Pour les spécialistes, il devient un atome de Rydberg : on l'excite avec un très haut niveau d'énergie. Ce système est conçu pour que le commercial de base n'atteigne pas son objectif et soit pénalisé côté bonus contrairement à celui des managers au-dessus. Surtout si on souhaite le virer. Ceci n'est qu'une fiction bien entendu !

Le jugement sur les individus est aussi sujet à la quantification. Une personne est souvent smart ou sympa ou alors, c'est un abruti total. Les jugements sont rarement nuancés, entre les deux. Pourtant, en application puriste de la physique quantique, ce jugement devrait être une fonction d'onde plus vague (genre « il est un peu c… sur les bords, mais pas toujours »). Avec la physique quantique, la vie est une grande gaussienne !

La **superposition d'états** a très couramment lieu à cause des smartphones et autres laptops grâce à qui les collaborateurs sont à la fois au travail et dans leur vie personnelle toute la journée. Elle peut se manifester également dans la conformité aux règlements qui est à géométrie variable dans nombre d'entreprises. Et puis bien entendu, dans l'application des valeurs définies à coup de slides Powerpoint rabâchés par les dirigeants ou la DRH.

La superposition des états se manifeste aussi dans l'évaluation des *leads* qui sont *closés* ou pas dans un *pipe* commercial. On leur attribue généralement un taux de *closing* qui est un pourcentage jusqu'au moment où l'on sait si le deal est perdu ou gagné, ce qui relève de l'écrasement de la fonction d'onde de Schrödinger sur un état de base (perdu ou gagné). Cet écrasement peut aussi intervenir si un élément extérieur intervient et génère une décohérence de l'état du lead. Par exemple, un concurrent qui rafle l'affaire au nez et à la barbe du commercial, fort marri de cette mésaventure. Son manager lui en fera porter l'intégralité de la responsabilité, ce qui constitue une autre forme d'écrasement. Ce genre d'analogie quantique ne vous aidera cependant pas à améliorer votre taux de closing de pipe commercial.

Le principe d'**indétermination** d'Heisenberg s'applique ainsi à la mesure de la satisfaction des collaborateurs, où l'outil de mesure influe toujours sur la grandeur à mesurer ! C'est vrai dans l'infiniment petit ainsi que dans les questions posées dans les sondages d'opinion qui sont souvent orientées, aussi bien en politique que pour évaluer la satisfaction des collaborateurs d'une entreprise. Et on navigue allègrement entre le béni-ouiouisme et le courage de s'exprimer, qui dépend de l'anonymat et de l'existence de champs de commentaires en texte libre qui permettent d'ajouter un peu de logique floue. Le top du top de l'insupportable ? Ces popups Internet où le choix donné est "OK" ou "Plus tard".

Plus généralement, la mesure de n'importe quel paramètre dans une entreprise, notamment lors d'un audit, va probablement aboutir à modifier les grandeurs mesurées (élagage d'effectif, mutation de manager, modification de processus).

La définition d'origine du principe d'indétermination d'Heisenberg est que l'on ne peut pas mesurer avec précision la position et la vitesse d'une particule dans l'infiniment petit, du fait notamment de sa grande rapidité de mouvement. L'analogie dans les affaires serait l'observation d'une startup en pleine croissance : le temps que l'on comprenne où elle en est à un moment donné, elle a déjà changé de situation (de siège, d'effectif, de CEO, de chiffre d'affaires, un petit pivot, etc). C'est la raison pour laquelle il faut une énergie infinie pour créer une base de startups à jour sur un pays ou au niveau du monde entier.

Dans un autre cadre, l'immobilisme dans l'entreprise est facilement associable à la constante de planque.

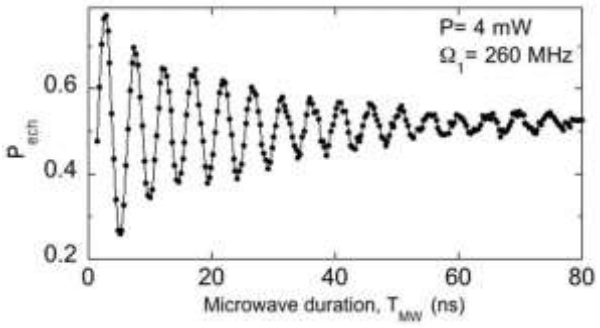
La **réduction d'états** rejoint l'histoire de la quantification des états lorsque l'on mesure le chiffre d'affaire en fin de trimestre. Là, on est bien obligé de fournir des chiffres et de ne pas s'appuyer sur la logique floue des taux de closing. Ne serait-ce que pour déterminer les bonus des commerciaux. Dans le cas de la superposition travail/vie personnelle, seule une observation de l'écran va permettre d'en savoir plus. Elle génère souvent un écrasement de la fonction d'onde de Schrödinger sur l'état « travail », sauf pour les jmenfoutistes.

Sinon, Bill Gates affirmait haut et fort en 1997 que les “mauvaises nouvelles devaient circuler vite dans les entreprises efficaces” (“bad news should travel fast”). Mais pas trop tout de même. L’écrasement de la fonction d’onde de Schrödinger s’applique très bien à la situation, lorsque les collaborateurs et managers pleutres s’écrasent en pareille situation, de peur des retombées négatives. Ou alors, au contraire, lorsqu’un salarié prend son courage à deux mains et dénonce l’insupportable, jusqu’à parfois devenir un lanceur d’alertes.

La **dualité onde-particule** se manifeste avec de vrais gens dans les entreprises qui travaillent sur des projets concurrents et s’annihilent allègrement. C’est le phénomène d’interférences lié à la forme d’onde des projets ! Il y a aussi les managers grandes gueules face à leurs équipes (donc, à l’état de particules solides) qui se transforment en lavettes face à leur propre management (donc, à l’état d’ondes flasques).

Cette dualité comportementale se manifeste aussi souvent chez les managers irascibles qui deviennent des moutons dociles une fois chez eux, ou qui n’arrivent pas à éduquer convenablement leurs enfants.

Et le Chief Happiness Officer de la startup branchée, il peut être quantique [1417]? Il doit en tout cas lutter contre un phénomène universel : un bon nombre de passions s’estompent rapidement avec le temps comme l’amplitude d’une **oscillation de Rabi**, qui est couramment observée en mécanique quantique et dans les qubits supraconducteurs (*ci-contre*). Un bon leader est en phase avec ses équipes.



Il émet des ondes qui entrent en résonance avec elles, un peu comme dans l’algorithme de tri quantique de Grover. L’effet Doppler permet aussi de stopper un projet foireux avec de la lumière, par exemple, via une fuite bien gérée dans les médias.

L’**intrication** quantique s’applique aux startups qui sont intégrées dans les programmes d’innovation ouverte des grandes entreprises. Tout va bien jusqu’à l’apparition de la **décohérence** des objectifs entre la startup et la grande entreprise ! Je fais un produit et tu veux un projet-service, j'ai besoin de rapidité et tu es trop lent à la détente, etc !

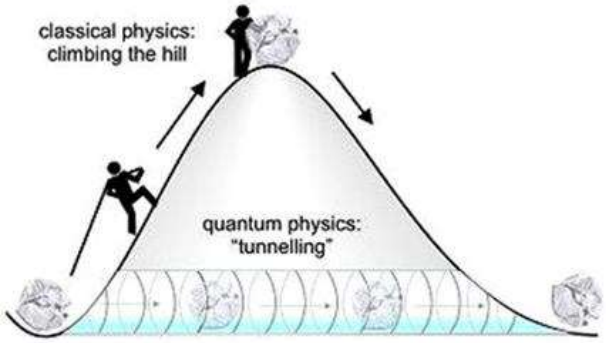
L’intrication se produit également dans le phénomène couramment dénommé radio-moquette, couplé à la téléportation des rumeurs plus rapidement que la lumière. On sait aussi que le temps de cohérence des qubits est lié à leur bonne isolation physique, magnétique, sous vide, et, souvent à très basse température, histoire d’éviter toute perturbation externe. Tout le contraire des open spaces des entreprises où l’on entasse les collaborateurs ! On a longtemps prétendu que cela améliorait le travail en équipe alors que cela servait principalement à réduire les coûts immobiliers !

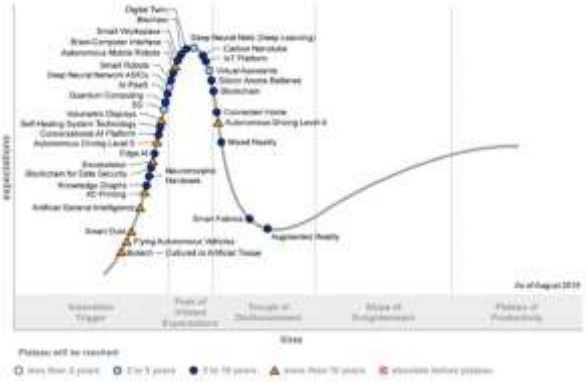
Le **théorème de non clonage** quantique qui dit qu’il est impossible de cloner à l’identique l’état d’un qubit ou d’un quantum a une application dans la vie des entreprises avec tous ces gens que l’on croit irremplaçables jusqu’au jour où ils s’en vont. Le théorème s’applique notamment lorsque le manager qui s’en va n’est pas remplacé et dont on répartit ensuite le rôle sur plusieurs managers en place. Et comme le veut l’adage, les cimetières sont pleins de gens irremplaçables ! Le théorème s'applique aussi aux entrepreneurs à succès qui ont du mal à répliquer un succès dans un domaine à un autre secteur d’activité.

[1417] Voir l’excellente parodie du rôle dans la vidéo USI 2019 - "Depuis deux ans, je conquiers le bonheur" | Confessions Digitales.

L’**effet tunnel** permet de faire passer des vessies pour des lanternes et gérer les bases du changement. Cela consiste à présenter une situation future mirifique en faisant oublier les difficultés pour y arriver. L’effet tunnel s’appelle la méthode Coué dans la vie courante. Le principe pourrait d’ailleurs être adopté par le Gartner Group avec ses fameuses courbes de cycle d’adoption de l’innovation (« hype cycle »), certaines technologies ne passant pas forcément par la vallée de la mort, comme ce fut le cas pour les smartphones.

Il faut dire qu’ils ont bénéficié du champ de déformation de la réalité d’un certain Steve Jobs, autre grand adepte de la mécanique quantique managériale. Imbuvable avec ses collaborateurs directs mais admiré quoi qu’il arrive !





Dans le plus fumeux, on peut trouver une analogie entre la **supraconductivité** et la réunionite aiguë dans les entreprises. Les salariés et cadres sont conditionnés pour être des bosons à spin pairs donc assemblables dans une salle de réunion, comme des photons ou comme des paires d’électrons dites de Cooper qui se manifestent dans la supraconductivité, alors que s’ils étaient des bosons à spin demi-entier comme des électrons libres classiques, on ne pourrait pas facilement les mettre au même endroit. On pourrait prolonger le raisonnement avec le remplissage des open spaces.

Il vaut mieux que les salariés proches les uns des autres soient compatibles donc appairables comme dans des paires de Cooper. Libre à vous de passer ensuite, par effet tunnel, de l’état de boson à celui de bozo, très cher à Guy Kawasaki.

La supraconductivité organisationnelle permet d’ailleurs d’éviter la résistance au changement. Vous congelez les collaborateurs et leur résistance au changement disparaît. Ce qui est un peu paradoxal car une fois congelé, on est solide comme un roc, et la décongélation n’est pas évidente.

Si on reprend les principes de la pseudo-médecine quantique de Deepak Chopra, une entreprise est dans un état superposé entre celui de leader en bonne santé et de société en perte de vitesse. La force du leadership devrait théoriquement permettre d’écraser la fonction d’onde de l’état quantique de l’entreprise dans l’état leader en bonne santé. Dans la vraie vie, cet écrasement est délicat à réaliser. Les processus qui amènent l’entreprise à se trouver en situation de déclin sont le plus souvent irréversibles et liés à l’environnement, aux concurrents et aux clients qui eux, n’ont pas attendu pour s’adapter.

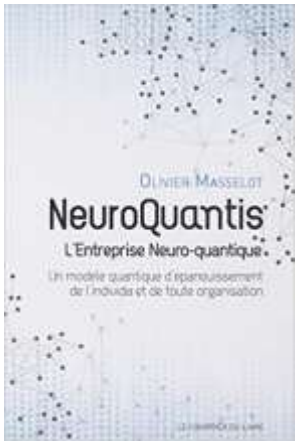
La vie des entreprises n’est pas une porte quantique réversible ! Essayez par exemple de transformer Nokia en leader des smartphones sous Android ou Technicolor en Samsung !

Le **calcul quantique à portes universelles** a une belle analogie dans la vie des entreprises avec la gestion des appels d’offre comme ceux qui portent sur les agences de communication. Les réponses des agences candidates sont des états superposés de registre quantique. Elles subissent un processus d’évaluation simultané, comme dans le calcul quantique. A la fin, un seul état (offre) ressort : le gagnant.

Mais dans le calcul, il peut y avoir un peu de mélange des états quantiques affectant le résultat. Traduction : les éléments de certaines réponses vont se retrouver comme par magie dans la réponse du gagnant. Là encore, peut-être via le fameux effet tunnel. En plein, le même processus s'applique aux projets open source bénéficiant d'un grand nombre de contributeurs.

Enfin, citons cet autre principe universel, la **téléportation quantique** de la bêtise humaine auprès de larges pans de l'entreprise ou de la population. Elle est tellement rapide que cela ne peut être que la seule explication plausible !

Toutes ces analogies créent des nœuds dans le cerveau et sont parfois amusantes. Elles ne servent pas à grand-chose pour améliorer le management. Elles sont plutôt utiles pour rappeler l'absurdité de certaines pratiques managériales dans les entreprises et leurs contradictions éternelles. En positivant un peu, même si sa dimension scientifique est plus que sujette à caution, la parodie est finalement une intéressante forme de pédagogie !



La gourourisation du coaching a en fait démarré bien avant la vague de l'informatique quantique, dès le début des années 2010 voire même avant. Le modèle de vente le plus classique consiste à publier un ouvrage de promotion d'une méthode en exploitant quelques vagues analogies entre une méthode existante et des rudiments de physique quantique à côté desquels la partie qui précèdent sur le management quantique me vaudrait une thèse de doctorat ! C'est le cas de **NeuroQuantis** qui fait de la formation de sa méthode de coaching dans un ouvrage du même nom[1418].

Une méthode équivalente est proposée par la société **QuantumLifeCoaching** qui se propose de vous former comme coach de l'entreprise neuro-quantique[1419].

Elle propose la même méthode baratinesque : « *Le coaching quantique est une pratique relativement récente qui se base sur des principes de physique quantique. Cette approche nouvelle du coaching permet de prendre conscience de toutes les formes d'énergie cachées dans le subconscient collectif et individuel* » à des coaches qui n'auront aucune notion de ce qu'est la physique quantique. Je n'ai rien contre les coaches. Mais ceux-là n'ont rien de quantique, je vous l'assure !

Ces méthodes de coaching sont aussi mises en sauce sous l'appellation de **systémie quantique** et de **communication quantique**. Elles sont notamment proposées par une certaine Agathe Bourasset selon qui « *L'être humain est composé d'une somme de fréquences vibratoires plus ou moins denses, et qui interagissent constamment sur des plans non-verbaux. En pratiquant la Communication Quantique vous posez la convention que les vibrations se transforment sous forme de mots et de phrases. Dans certaines traditions, on parle de communication « de cœur à cœur, d'âme à âme », avec les différents plans de l'être. C'est l'ouverture d'un espace où vous accédez en direct à l'information juste, pour la comprendre, puis évoluer en conscience !* » (vidéo d'entretien et vidéo de présentation). Aurélie Surmely et Agathe Lecointre pratiquent cette communication quantique en reprenant les méthodes d'Agathe Bourasset. Elle permet de « *dissoudre des blocages relationnels, de découvrir de nouvelles possibilités pour résoudre un conflit, de fluidifier l'information par la mise en mouvement* ». Même topo avec Nancy Miquel.

[1418] Voir NeuroQuantis, l'Entreprise Neuro-quantique, un modèle quantique d'épanouissement de l'individu et de toute organisation, par Olivier Masselot, 2012. Cet auteur est aussi le traducteur en français de l'ouvrage Transurfing du Russe Vadim Zeland, aussi en 2012. Le tout est un gloubi-boulga de recommandations basées sur la maîtrise de ses émotions, particulièrement les émotions positives, pour atteindre ses objectifs.

[1419] Voir Créer une activité de coaching neuro quantique par QuantumLifeCoaching, non daté.

Les thérapeutes quantiques prolifèrent depuis des années. Vous avez par exemple Yves Borgers qui propose la méthode du Quantum-Touch consistant à élever le taux vibratoire pour activer l'auto-guérison, ce qui rappelle les méthodes de Deepak Chopra. Cette méthode est pratiquée en France par une trentaine de praticiens dont 17 à Paris (source). Sachant que les autres thérapies proposées sur ce site n'ont pas l'air toutes bien plus sérieuses que les méthodes labellisées quantiques.

Vous avez aussi une modèle quantique d'évolution personnelle en coaching holistique proposé en Suisse par Danielle Brault International.

Comme le veut l'adage des adeptes de ces méthodes, si elles fonctionnent, on ne va pas les empêcher de faire rêver les gens.

Marketing quantique

Cette grille de lecture sur le management et la vente est adoptée sérieusement par quelques rares adeptes du marketing quantique. Ainsi, le site Quantum-Marketing est lié à la société GetQuanty dont l'offre logicielle est une solution de scoring prédictif B2B[1420], donc, de la gestion de leads[1421]. Le fondateur, Hervé Gonay, que j'ai rencontré, ne prétend pas faire de la physique quantique mais cherche à s'en inspirer.

Il m'a fait découvrir le groupe de chercheurs du Quantum Interaction qui se sont réunis dans leur 8ième congrès en 2018 à Nice et dont les interventions sont disponibles sur Youtube. Il a même co-écrit un papier de recherche avec Ariane Lambert Mongiliansky (PSE) qui travaille avec Michel Bitboll (CNRS, ENS Lyon) et Bob Coecke (Oxford), lui-même co-auteur de Picturing Quantum Processes.

Ces chercheurs bâtissent des modèles inspirés de la physique quantique dans des domaines variés tels que l'économie, la recherche d'information et la dynamique des organisations. Ça a l'air plus sérieux que les fumisteries évoquées dans ces pages. La frontière entre sciences humaines et fumisteries reste cependant très ténue.

[1420] Voir la vidéo sur « le marketing quantique expliqué à mon boss » par Hervé Gonay.

[1421] Le problème ? Des marketeurs sans formation scientifique qui s'emmêlent les paluches dans l'histoire du quantique : « C'est Albert Einstein qui, le premier, a affirmé qu'une particule de lumière pouvait à la fois se comporter comme un objet (un corpuscule) et comme une onde. Il l'a démontré par la logique, puis cette réalité a été prouvée par l'expérimentation (expérience des deux fentes de Thomas Young [en fait, l'expérience des fentes de Young date de 1806 et le texte d'Einstein de 1905]). Plus tard, le français Louis de Broglie a émis l'hypothèse, vérifiée ensuite, que les électrons, qui sont au cœur de la matière, possédaient la même dualité. C'est pourquoi on parle de superposition [le lien entre dualité et superposition est un peu rapide] : toute particule se situe dans plusieurs états à la fois. De plus, ce n'est qu'au moment où on l'observe que la particule « choisit » d'être soit un corpuscule, soit une onde [la superposition n'est pas entre un état « particule » et un état « onde »]. On parle alors de « réduction de la fonction d'onde »… ».

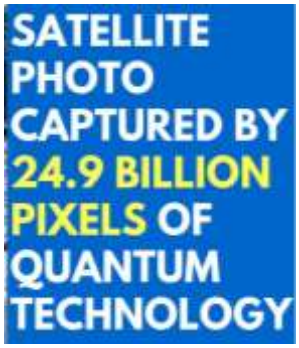
Dans Innovation quantique, ou cantique de l'innovation, un certain Philippe Cartau recommande de ne pas trop mesurer ses actions lorsque l'on innove en mode startup, ce qui fera naturellement s'étranger les adeptes du growth hacking, ce dernier reposant sur la mesure constante de la performance du mix marketing. Quel monde paradoxal !

Autres fumisteries

La physique quantique donne lieu à d'autres propagations de théories ou affirmations fumeuses, malgré le fait qu'elles s'appuient parfois sur des travaux de recherche sérieux. Le biais de ces exagérations vient souvent d'extrapolations abusives de phénomènes constatables à une échelle nanoscopique à la vie macroscopique.

En Chine, nous avons par exemple vu apparaître une soi-disante **caméra quantique satellite** servant à réaliser des panoramas haute-résolution. La vue présentée est celle de Shanghaï avec 195 milliards de pixels.

En y regardant de près, les images ont été captées en haut d'un gratte-ciel – il n'en manque pas à Shanghaï - et pas par satellite et par des caméras haute résolution classiques qui n'ont rien de plus quantique que le très classique effet photo-électrique. Ce dernier permet à un capteur photo CMOS de transformer des photons en courant électrique. L'information est totalement bidon et ne servait qu'à générer du buzz.



Malheureusement, nombre de médias ont mordu à l'hameçon dans le monde entier sans douter de la chose[1422].

Une PME française **What-Innove** de l'Est de la France et spécialisée dans les énergies renouvelables ambitionne de son côté de créer un moteur captant l'énergie du vide. Le fonctionnement ? Un fourre-tout improbable qui associe un générateur de champ quantique, la création de photons issu de l'énergie du vide exploitant l'effet Casimir (mais pas avec des plaques parallèles comme dans l'expérience éponyme), la combinaison du magnétodynamisme et de l'espace-temps, des supraconducteurs fonctionnant à température et pression ambiante (qui leur vaudrait un prix Nobel si cela fonctionnait…), et de la néguentropie. Pour y arriver, il ne faudrait que 2,7M€ de financements ! C'est censé résulter d'une dizaine d'années de recherche fondamentale à IUTT de Troyes et dans le laboratoire du créateur. Autant dire que c'est plutôt difficile à prendre au sérieux.

[1422] Voir 60 seconds over sinoland: quantum satellite camera used to do movable, panoramic photos of Shanghaï, décembre 2018 (vidéo) et Truth Behind Viral 24.9 Billion Pixel Image Taken By Chinese "Quantum Satellite" par Anmol Sachdeva, décembre 2018 et le site Bigpixel pour consulter la vue.

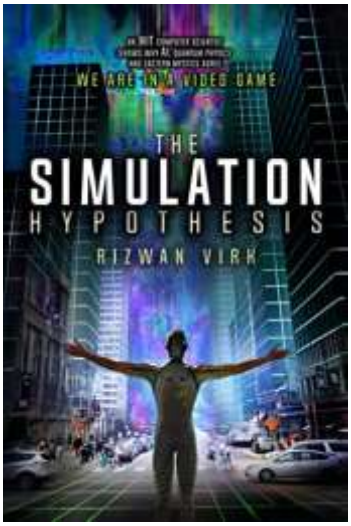
Vous avez aussi droit à un beau **réfrigérateur quantique** (« Quantum Cooler ») de Chillout Systems qui n'a de quantique que le nom. Il utilise un compresseur classique compact[1423].

D'autres cas de figure extrapolent à l'échelle macro des phénomènes quantiques observés à une échelle nano. C'est le cas de l'**inversion du temps** avec du calcul quantique, une vision de l'esprit qui est liée à la nature réversible des portes quantiques mais ne signifie aucunement que l'on peut revenir en arrière sur l'échelle du temps dans la pratique macroscopique[1424].

Nous avons aussi des théories tout aussi fumeuses visant à **prédire le futur** grâce au calcul quantique. S'il est vrai que le calcul quantique permet d'évaluer toutes les solutions d'un problème complexe, il est réduit à des problèmes simples au vu de la complexité de la vie macroscopique, quand bien même celle-ci pourrait être déterministe[1425].

L'étape suivante consiste à considérer que nous vivons en fait dans une **simulation**.

C'est la théorie évoquée dans The Simulation Hypothesis de Rizwan Virh. Comme cela peut arriver en pareil cas, l'auteur survend son parcours personnel en se présentant comme un MIT Computer Scientist alors que c'est plutôt un entrepreneur dans le jeu vidéo plutôt habitué aux ouvrages sur l'entrepreneuriat que sur les sciences. Ce genre de scénario de la simulation équivaut à la croyance en une sorte de Dieu omnipotent qui contrôle tout ou qui a créé l'outil de simulation en question. La question peut d'ailleurs être déclinée récursivement : si ce créateur a développé un outil de simulation, qui a créé son univers et celui-ci n'est-il pas également une simulation ? Les lois de la physique que l'Homme découvre petit à petit permettent de décrire le comportement de la matière et des ondes. Plus on avance, plus elles permettent d'imaginer un monde déterministe gouverné par ces lois. Mais cela ne signifie pas que ces lois soient gouvernées par un système qui les contrôle.



Autre cas de figure qui devrait inspirer la plus grande prudence, celui de cette curieuse société **Precog Technologies** qui prétend proposer des solutions de téléportation, de voyage dans le temps et de systèmes anti-gravitation. La totale ! La société a été créée pour valoriser la propriété intellectuelle d'un certaine Anisse Zerouta qui est décrite dans un papier scientifique douteux[1426].

Un autre olibrius, de **Qaunta QB** (d'Afrique du Sud) pense avoir aussi trouvé la pierre philosophale et l'architecture de qubits qui fait tout ce qu'il faut et avec un miraculeux 0% d'erreurs[1427].

[1423] Voir Chillout Systems Quantum Cooler. Il est vendu $2199.

[1424] Voir Des physiciens ont réussi à "inverser" la flèche du temps grâce à un ordinateur quantique de Stéphanie Schmidt, mars 2019, qui fait référence à Arrow of time and its reversal on the IBM quantum computer, de G. B. Lesovik et al, 2018 (14 pages). Voir aussi L'ordinateur quantique d'IBM viole-t-il le second principe de la thermodynamique ?, 2019.

[1425] Voir Des scientifiques construisent une machine permettant de voir tous les futurs possibles de manière simultanée de Jonathan Paiano, avril 2019 et Interfering trajectories in experimental quantum-enhanced stochastic simulation de Farzad Ghafari et al, 2019 (7 pages).

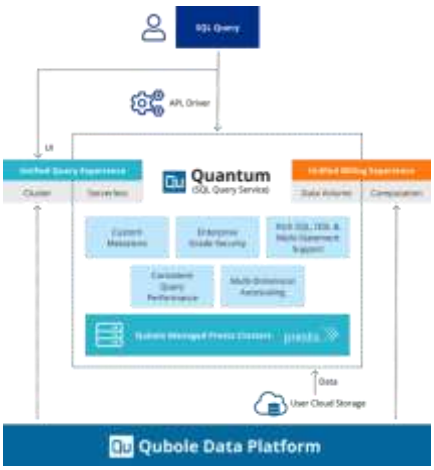
[1426] Voir The Seed Theory: Unifying and replacing quantum physics and general relativity with "state physics" d'Anisse Zerouta, 2017 (28 pages) qui développe une théorie de mondes parallèles et qui n'a pas du tout l'air de remplir les critères d'une publication scientifique digne de ce nom. Anisse Zerouta est un gérant d'entreprises à Paris né en 1973, d'abord avec Elysee Communication (2008-2011) puis avec Avenir Optique, un opticien (2011-*), des sociétés n'ayant qu'un salarié, son fondateur (source). Créé en septembre 2018, Precogtec aurait un CTO, un certain François Bissege, qui possède un doctorat en sociologie (source) et un autre salarié, Julien Darivel, qui possède un DUT et a travaillé chez PSA. C'est du bizarre !

[1427] Voir I made the Quantum Breakthrough, juin 2019.

On a aussi vu apparaître le premier scam quantique en 2018 avec ce faux article du Guardian faisant état d'un projet d'ordinateur quantique pour la finance d'Elon Musk[1428]. L'œil exercé dans l'informatique quantique détecte rapidement qu'il s'agit d'un montage, comme cette série d'ordinateurs quantiques **QuantumAI** qui ne sont que des D-Wave dont le logo a été photoshoppé.

Second point, l'article serait issu du Guardian… mais pas l'url ! L'article cite un nombre de scientifiques de laboratoires de recherche du monde entier, mais ayant tous un nom russe. L'article pointe sur le service en ligne de **QuantumAI** qui serait capable de boursicoter pour dépouiller les riches et redistribuer l'argent aux plus pauvres. Le site ose tout, comme indiquer que la startup a comme advisors Jeff Bezos et Bill Gates et comme partenaires IBM, Microsoft et OpenAI.

Il en existe un autre, dénommé **Quantum Code**. Evidemment, fuyez ! C'est en fait un scam destiné à détrousser les utilisateurs de leurs économies mais de manière indirecte. Le site propose de créer un compte en fournissant ses coordonnées. Celles-ci sont alors revendues à des sociétés peu scrupuleuses de produits financiers louches qui exploitent ainsi des leads de prospects faciles à berner[1429].



[1428] Voir Elon Musk to Step Back From Tesla And SpaceX, Jumps on Qm Computing Financial Tech (non daté).

[1429] Voir QuantumAI review – is Quantum-aix.com a scam?, juin 2019.

On peut aussi citer **Qubole** qui lançait son serveur SQL Quantum, qui n'a rien de quantique[1430]. Le processeur **Samsung** Quantum 8K lancé en 2018 n'était pas non plus particulièrement quantique à part via ses transistors CMOS classiques. Le quantique risque de laver plus blanc que blanc, comme cette lessive "Quantum Max" de la marque **Finish** du groupe Reckitt Benckiser !

Sinon, **Quantum Corp** (USA) ne fait rien de quantique et gère du stockage sur bandes magnétiques. Il en va de même de **Quantum Entanglement Entertainment** (Canada) qui comme son nom l'indique est dans le marché des contenus. **Quantum Surgical** (France) fait des robots de chirurgie pour le cancer du foie et qui n'ont rien de quantique. Et l'executive MBA **Quantic** n'a de quantique que le nom.

Dans les produits grand public, la nomenclature quantique est enfin utilisée dans des rouleaux de PQ américains **Quantum** ainsi que dans le vin rouge Quantum de **Beringer**, une marque de la Napa Valley en Californie.

Nous n'avons donc pas fini de voir le quantique mis à toutes les sauces et dans toutes les couleurs !

[1430] Voir Qubole launches Quantum, its serverless database engine de Frederic Lardinois, juin 2019.

Conclusion

La production la troisième édition de cet ebook m'a pris bien plus de temps que pour lancer la première en 2018. Le confinement lié au covid-19 y est pour quelque chose puisque j'ai consacré presque tout le temps qui n'était pas en webcall à cet ouvrage, pendant cinq mois. Cela m'a permis d'approfondir le sujet dans toutes ses dimensions, à la fois, scientifiques, technologiques, économiques, politiques et sociétales. L'image est plus nette mais ce n'est pas encore l'hyperrésolution. C'est le propre des technologies quantiques que de conserver leur part de mystère, surtout lorsque l'on n'en est pas un véritable spécialiste.

Depuis septembre, j'ai passé aussi beaucoup de temps à côtoyer chercheuses et chercheurs et à mieux comprendre leur façon de travailler, leurs cycles, leur ambitions, leurs difficultés. J'étais « embedded ».

Les technologies quantiques symbolisent parfaitement l'univers de l'innovation et de l'entrepreneuriat extrême : il est plein d'incertitudes, de risques et d'échecs. Il y a du "test & learn", du croisement de sciences, le besoin d'investir très en amont de la réussite économique avec un rôle critique des Etats, les seuls à même de voir loin, à plus de 10 ans. Nombreuses sont les voies parallèles d'exploration du possible qui ont été lancées par les chercheurs et les entrepreneurs. Seuls quelques-uns réussiront comme le veut la loi du genre. Une industrie nouvelle est en train d'émerger de tout cela.

Pour rédiger cet ouvrage, j'ai téléchargé et compulsé plus de 1500 documents librement disponibles sur Internet, visualisé des dizaines d'heures de conférences et de cours sur YouTube, et rencontré des dizaines de chercheurs et entrepreneurs.

Il me faut remercier plusieurs personnes de talent ici. Tout d'abord **Fanny Bouton**, avec qui nous avons démarré cette aventure du quantique en 2018 à commencer par la conférence Le quantique, c'est fantastique du Web2day, délivrée le 14 juin 2018.



Cette conférence de Nantes, les suivantes et cet ebook tirent parti de rencontres ou d'échanges avec une belle brochette de spécialistes du secteur qu'il nous faut remercier : **Alain Aspect** (X, SupOptique), **Daniel Estève** (CEA-DRF), **Christian Gamrat** (CEA-LIST), **Maud Vinet** (CEA-Leti à Grenoble), **Tristan Meunier** (CNRS Grenoble), **Alexei Tchelnokov** (CEA Grenoble), **Laurent Fulbert** (CEA-Leti Grenoble), **Cyrille Allouche** et **Philippe Duluc** (Atos), **Bernard Ourghanlian** et **David Rousset** (Microsoft), **Pat Gumann** (IBM), **Etienne Klein** (CEA), **Christophe Jurczak** et **Zoé Amblard** (Quantonation), **Nicolas Gaude** (Prevision.io) et **Françoise Gruson** (Société Générale).





Nous avons depuis pu rencontrer encore plus de chercheurs dans le quantique tels que **Philippe Grangier** (Institut d'Optique), **Elham Kashefi** (LIP6 et Veriqloud), **Marc Kaplan** (Veriqloud), **Pascale Senellart** (C2N et Quandela), **Franck Balestro** et **Alexia Auffèves** (CNRS Institut Néel), **Mathieu Desjardins** (LNA et CNT Technologies devenu C12), **Jacqueline Bloch** (C2N) et **Iordanis Kerenidis** (CNRS). Nous avons aussi pu rencontrer **Cédric Villani** à plusieurs reprises pour discuter du sujet. J'ai aussi animé un débat avec **Heike Riel** (IBM) et **Massimo Russo** (BCG) en mars 2019 dans l'événement Hello Tomorrow. Lors de la conférence QCB de juin 2019, bis repetita avec **Vern Brownell**, le CEO de D-Wave.

Cela s'est poursuivi pour cette troisième édition côté recherche avec de rencontres pour l'essentiel zoomifiées avec **Alain Aspect** (Institut d'Optique), **Artur Ekert** (CQT Singapour), **Patrice Bertet** (CEA SPEC), **Xavier Waintal** (CEA IRIG), **Yvain Thonnart** (CEA LIST), **Rob Whitney** (LPMMC Grenoble), **Damian Markham** (CNRS LIP6 et JFLI à Tokyo), **Pascale Senellart** (C2N) et **Maud Vinet** (CEA-Leti) et côté entrepreneuriat avec **Bruno Desruelle** (Muquans), **Georges-Olivier Raymond** et **Antoine Browaeys** (Pasqal), **Théau Perronnin** et **Raphaël Lascanne** (Alice&Bob) ainsi que **Matthieu Desjardins** (C12), **Jeremy O'Brien** (PsiQuantum), **Magdalena Hauser** et **Wolfgang Lechner** (ParityQC) et **Roger MKinley** (UKRI).

Il y a eu ces innombrables discussions avec **Jean-Christophe Gougeon** de Bpifrance, **Neil Abroug** de la DGE, qui était rapporteur de la mission Forteza et coordinateur de la task force qui lui a succédé ainsi que **Charles Beigbeder** et **Christophe Jurczak** de Quantonation. Je dois aussi citer les nombreux échanges sur le plan quantique a**vec Cédric O** et son cabinet. Il a cru au sujet et en est devenu le moteur au sein du gouvernement.

La première édition de 2018 a bénéficié des relectures attentives de **Godefroy Troude**, jouant le candide sur le sujet et de **Zoé Amblard** pour la partie cryptographie.

La seconde édition, de 2019, a bénéficié de l'apport de **Peter Eid** (élève-ingénieur à CentraleSupelec), **Valérian Giesz** (CEO Quandela) pour la partie dédiée à la cryptographie, d'**Alexia Auffèves** (CNRS, Institut Néel), notamment sur l'écosystème de recherche français et sur les questions de thermodynamique, de **Nicolas Gaude** (CEO de Prevision.io) pour la partie algorithmes quantiques, d'**Harold Ollivier** (LIP6) pour l'introduction et de **Maud Vinet** (CEA-Leti) pour les parties CMOS/electron spins.

Cette troisième édition de 2020 a bénéficié de la relecture transversale de **Michel Kurek, Bruno Fedrici** et **Peter Eid**, de la contribution de **Pierre Perrot** de CryoConcept pour la partie cryogénie, de celle de **Neil Abroug** sur le fonctionnement de la recherche, les classes de complexité et les plans industriels, de **Valérian Giesz** de Quandela sur les parties consacrées à la photonique, d'**Alexia Auffèves** pour les parties sur la cryogénie, sur l'énergie, sur le fonctionnement de la recherche et sur la philosophie quantique, de **Marco Fellous-Asiani** pour la correction d'erreurs, la cryogénie et l'énergie, d'**Elham Kashefi** sur le MBQC, de **Maxime Richard** sur les polaritons et d'**Eleni Diamanti** pour la partie sur les télécommunications et la cryptographie quantiques[1431].

A plusieurs, on est toujours meilleurs !

[1431] Je n'ai cependant pas eu suffisamment de relecteurs pour couvrir toutes les parties de l'ouvrage. Il est difficile de fact-checker un ouvrage de cette taille. Je corrige cependant tous mes ouvrages au fil de l'eau après leur publication lorsque l'on me signale des erreurs. Donc, si vous détectez des erreurs, surtout scientifiques, n'hésitez pas à me les signaler. Je les corrigerai au fil de l'eau.

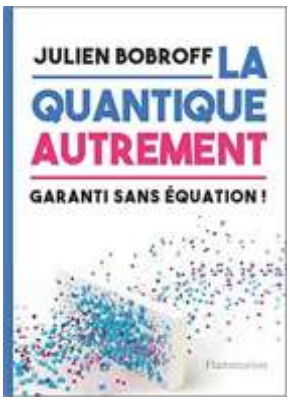
Bibliographie

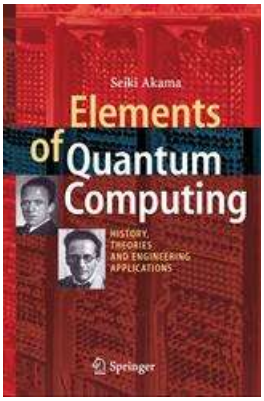
Voici un peu en vrac quelques ouvrages généralistes et autres sources d'informations sur les technologies quantiques que j'ai pu consulter ou découvrir pour préparer et mettre à jour cet ebook.

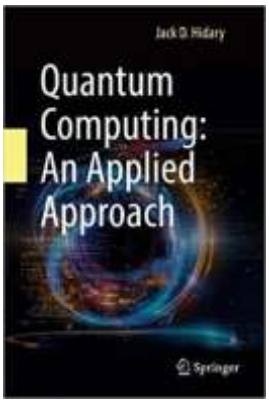
Livres et ebooks

Les ouvrages cités ici sont majoritairement téléchargeables gratuitement.

Mon grand Mécano quantique de Julien Bobroff, un ouvrage de vulgarisation de la mécanique quantique qui s'appuie sur l'approche expérimentale. Il y décrit notamment la supraconductivité, l'effet tunnel, l'IRM et les lasers. Le même auteur a publié La quantique autrement - garanti sans équation ! en 2020. On trouve de nombreuses conférences de l'auteur sur YouTube où il se focalise surtout sur l'effet supraconducteur (vidéo, 1h54) et une autre de mars 2020 où il évoque la suprématie quantique de Google (vidéo, 1h37). Voir aussi le site de vulgarisation de la physique La Physique Autrement.







Quantum Computation and Quantum Information de Nielsen et Chuang, 2010 (10e édition, 704 pages) est la référence incontournable sur les bases de l'informatique quantique. Le livre répond à de nombreuses questions clés sur le sujet, en particulier sur les modèles mathématiques de l'algèbre linéaire utilisés dans le calcul quantique.

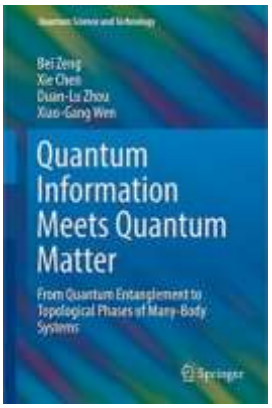
Elements of Quantum Computing de Seiki Akama (133 pages) et qui est à la fois concis, précis et assez complet sur les recoins de la mécanique et de l'informatique quantiques, avec qui plus est une bonne vision historique.

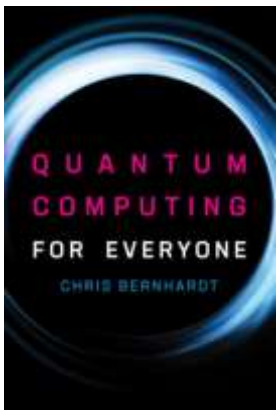
Quantum Computing : An Applied Approach (2019, 379 pages), un ouvrage assez complet qui couvre les algorithmes quantiques, leurs fondements mathématiques. Il décrit succinctement les différentes architectures d'ordinateurs quantiques.

La seconde révolution quantique trouve déjà de nombreuses applications de Xavier Bouju, 2019, un bon travail de vulgarisation.

Quantum Information Meets Quantum Matter de Bei Zeng, Xie Chen, Duan-Lu Zhou et Xiao-Gang Wen. Il est disponible dans une version de février 2018 sur Arxiv en téléchargement libre (373 pages).

Informatique quantique - de la physique quantique à la programmation quantique en Q# de Benoit Prieur, 2019 (244 pages). Il démarre par les principes généraux de la physique quantique. La partie sur les ordinateurs quantiques eux-mêmes est assez maigre et n'explore que quelques technologies (supraconducteurs et RMN, qui est peu utilisée). Le reste est dédié à l'apprentissage de la programmation en Q#, le langage de programmation quantique de Microsoft.





Principles of Quantum Computation and Information, A Comprehensive Textbook de Giuliano Benenti, Giulio Casati, Davide Rossini et Giuliano Strini, décembre 2018 (598 pages).

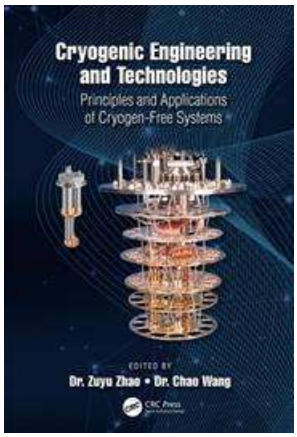
Quantum Computing for Everyone de Chris Bernhardt, 2019 (216 pages) qui décrit les bases du calcul quantique à commencer par les incontournables qubits, les portes quantiques, les accélérations apportées par les algorithmes quantiques et les grandes composantes d'un calculateur quantique.

L'avantage quantique, enjeux industriels et formation, septembre 2019 (56 pages), un document de qualité créé par la Fondation Mines-Télécom. Il couvre tous les aspects du quantique, du calcul aux télécommunications en passant par la métrologie. Il est certainement plus digeste que cet ebook mais ne décrit pas trop l'ingénierie des ordinateurs quantique comme je le fais dans cet ebook.

Quantum Internet, un magazine de 60 pages présentant les différentes facettes de l'informatique quantique, édité par TU Delft (2019).

Quantum computing de Joseph Gruska (1999, 390 pages), une autre base assez complète couvrant tous les aspects du calcul et de la communication quantiques.

Unconventional Computation de Bruce MacLennan, Université du Tennessee, octobre 2019 (304 pages) qui traite des questions énergétiques du calcul (réversible, non réversible) et de différentes méthodes alternatives de calcul dont le calcul quantique et le calcul moléculaire.



An Introduction to Quantum Computing de Phillip Kaye, Raymond Laflamme et Michele Mosca, 2007 (284 pages) qui commence par quelques fondements mathématiques de la physique et du calcul quantique. Par des auteurs de référence comme Raymond Laflamme (Canada) qui est un des pères des codes de correction d'erreurs.

Cryogenic Engineering and Technologies par Zuyu Zhao et Chao Wang, octobre 2019 (386 pages) est un ouvrage de référence sur les questions de cryogénie dont il donne un historique très fourni et bien documenté. On y trouve un excellent chapitre sur les cryostats à dilution à sec utilisés dans les ordinateurs quantiques. Cela m'a aidé à préparer la partie de cet ebook sur la cryogénie en complément d'un entretien avec l'équipe de la startup française CryoConcept et celles de l'Institut Néel de Grenoble.

Notes de cours sur la Mécanique quantique de Frédéric Faure, 2015 (397 pages) qui m'a fourni quelques pistes pour relier la mécanique quantique à son formalisme mathématique et notamment pour expliquer l'équation de Born.

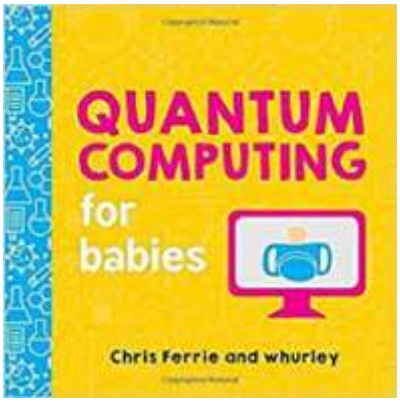
Introduction to quantum computing algorithms d'Arthur Pittenberger, 2001 (152 pages) qui décrit les algorithmes quantiques classiques avec une bonne partie dédiée aux codes de correction d'erreurs.

Vocabulaire d'optique, CNRS, 2019 (310 pages) est un dictionnaire de traduction anglais/français du vocabulaire de l'optique, donc de l'optique quantique au passage.

Bandes dessinées

Quantum Computing for Babies par Chris Ferrie et William Hurley, avril 2018 qui s'adresse plutôt aux enfants voire aux grands enfants. L'ouvrage vulgarise les grands concepts de la physique et du calcul quantique de manière très imagée. Il vient d'un enseignant en informatique quantique de l'Université de Technologie de Sydney et du fondateur de la startup américaine Strangeworks.

Le Mystère du monde quantique de Thibault Damour et Mathieu Burniat est une bande dessinée destinée à un large public et qui explique les principes de base de la mécanique quantique et leur origine historique.



Présentations

Voici quelques conférences et supports de présentations plutôt bien réalisés pour vulgariser l'informatique quantique.

Les débuts de l'ordinateur quantique : principes, promesses, réalisations et défis, une excellente conférence de **Pascale Senellart** (C2N) qui couvre bien la partie physique du calcul quantique, janvier 2020 (vidéo de 90 mn et 98 slides). Elle ouvre tout un tas de portes à explorer ensuite pour creuser.

Quantum computing, un cours d'**Hélène Perrin** à l'Université Paris 13 en quatre parties, février 2020 (lecture 1 de 77 slides sur les ions piégés, lecture 2 de 36 slides sur les qubits supraconducteurs, lecture 3 de 39 slides sur les qubits silicium, moléculaires et NV Centers, lecture 4 de 75 slides sur les atomes froids). Cela demande un bon background en physique pour être pigé de bout en bout. Les références fournies permettent de creuser les sujets abordés.

La conférence Introduction à la physique quantique de l'astrophysicien **Roland Lehoucq** donnée à l'Ecole Polytechnique en juin 2018 (1h16). Il est aussi l'auteur du très intéressant Faire des sciences avec Star Wars en 2015 (83 pages).

Trois conférences d'**Etienne Klein** du CEA sur la physique quantique à la Cité des Sciences de Paris, datant de 2007 et qui sont remarquables de pédagogie (cours 1, cours 2, cours 3) et durent en tout près de cinq heures ainsi que Comprenons nous vraiment la mécanique quantique de **Franck Laloë** (1940, France), (45 pages) et qui semble dater d'il y a au moins une quinzaine d'années au vu de sa bibliographie mais qui met au clair de nombreux débats scientifiques au sujet de la physique quantique.

Quantum computing Overview par **Sunil Dixit**, septembre 2018 (94 slides) est une présentation de Northrop Grumman qui fait un tour assez large du calcul quantique et des modèles mathématiques sous-jacents.

A pedestrian introduction to quantum computing par **Jérome Milan**, Ecole Polytechnique, 2010 (55 slides) qui explique de manière bien illustrée les grands principes du calcul quantique et en particulier de l'algorithme de Grover.

Le Quantum Computing for High Energy Physics workshop du CERN en novembre 2018 avec les supports de présentation et vidéos et les interventions intéressantes de différents acteurs du calcul quantique dont Intel que l'on ne voit pas souvent. Le contenu spécifique est peut-être dépassé par les principes de base restent valables.

Quantum computing for the determined par Michael Nielsen, une série de 22 vidéos sur le calcul quantique, 2011, accompagnées d'un long texte d'explications.

Conférences

Il existe de très nombreuses conférences sur les différentes branches scientifiques des technologies quantiques.

Dans les conférences plus généralistes, on peut citer la **QCB** organisée par Bpifrance à Paris (juin 2019 et novembre 2020), la **Q2B** de QcWare organisée en Californie en décembre chaque année, la **QT Digital Week** anglaise en juin (qui avait lieu sous la forme de webinar en 2020) ainsi que l'**European Quantum Technologies Conference** à Dublin en novembre-décembre 2021. Il va sans dire que toutes les conférences du genre ont l'ambition d'être internationales, ne serait-ce que parce que la compétence est répartie dans le monde entier et que de nombreuses équipes de chercheurs travaillent en mode partenarial avec des équipes d'autres pays.

Articles

L'ordinateur quantique : tout comprendre en partant de zéro, de Vincent Rollet, Institut Pandore, 2016.

Ordinateur : les promesses de l'aube quantique de Julien Bourdet, CNRS, 2019.

Introduction to Quantum computing, une thèse de Suau Adrien, 2018 (64 pages).

Le numéro spécial de **Pour la Science** de juin 2020 "La nouvelle révolution quantique" avec des articles d'Alain Aspect, Etienne Klein, Carlo Rovelli, Antoine Tilloy, Tristan Meunier et Pascale Senellart pour les contributeurs français (première page des articles).

Formations

Les cours de Berkeley de 2013 : Quantum Mechanics and Quantum Computation sur YouTube.

Les vidéos du cours d'informatique quantique de Stanford.

Le cours Quantum Computing Fundamentals proposé par le MIT.

Une formation en ligne sur la programmation quantique proposée par Brillant en partenariat avec Microsoft.

Le cours QSIT (FS 2016) de l'ETZ Zurich avec ses slides et notes de lecture.

Quantum Computing as a High School Module, un cursus d'enseignement avec exercices sur les basiques de la physique quantique destine à étudiants des élèves de niveau BAC.

Sites web

Toutestquantique, un site français de vulgarisation sur la physique quantique.

The Quantum Daily, un site d'actualité sur le quantique créé par Ethan Hansen, qui diffuse aussi un podcast mensuel.

AzoQuantum, un site d'information sur l'actualité scientifique quantique.

Quantum – the open journal for quantum science, un site d'actualités scientifiques sur la mécanique quantique.

Quantiki, un site d'information sur l'informatique quantique.

Quantum Info qui liste notamment l'agenda des événements mondiaux sur le quantique.

Qosf : site qui inventorie des guides et formations pour les développeurs d'applications quantiques.

Les newsletters de Nathan Shammah du RIKEN (Japon).

Quantum Journal, the open journal for quantum science, qui référence des publications scientifiques sur le quantique, généralement disponibles sur Arxiv.

Quantum-show, de la société Anabole est un site de vulgarisation qui propose des représentations graphiques, sonores et interactives des états de chacun des qbits mobilisés dans les algorithmes quantiques. Ils permettent de réfléchir d'un point de vue philosophique à l'interprétation de ce qu'est une superposition de "vrai" et de "faux". Il s'agit d'une revisite des origines de l'informatique à l'aune du calcul quantique.

Podcasts

Les podcasts Quantum que j'enregistre régulièrement depuis septembre 2019 avec Fanny Bouton. Ils sont disponibles sur toutes les plateformes audio (Spotify, iTunes, Deezer, …) ainsi que sur YouTube en version vidéo.

Ils sont complétés par les entretiens de **Decode Quantum** que nous enregistrons depuis mars 2020 avec les acteurs de l'écosystème quantique (chercheurs, startups, investisseurs, entreprises, etc) en partenariat avec Frenchweb. Les premiers épisodes faisaient intervenir Pascale Senellart, Alexia Auffèves, Maud Vinet, Eleni Diamanti, Elham Kashefi, Théau Peronnin et Raphaël Lescanne d'Alice&Bob, Christophe Jurczak de Quantonation et Jean-Christophe Gougeon de Bpifrance, Georges-Olivier Reymond et Antoine Browaeys de Pasqal ainsi qu'Alain Aspect.

Rapports

Les notes de l'OPECST sur les technologies quantiques : Les technologies quantiques : introduction et enjeux, mars 2019 (7 pages), Technologies quantiques : l'ordinateur quantique, juillet 2019 (6 pages) et Technologies quantiques : la programmation quantique, juillet 2019 (5 pages).

The Next Decade in Quantum Computing and How to Play, de Philipp Gerbert et Frank Ruess, BCG, novembre 2018 (30 pages) fait un panorama bien documenté de l'état de l'art de l'informatique quantique et positionne clairement les différents acteurs du marché.

Inside Quantum Technology, une société d'analystes dédiée aux technologies quantiques qui propose des rapports payants sur le sujet.

Divers

La présentation Designing and Presenting a Science Poster, Jonathan Carter, Berkeley (20 slides) qui est destinée aux chercheurs, pour les aider à bien concevoir un poster de presentation de projet de recherche.

Glossaire

A quoi sert un glossaire ? Il permet de s'y retrouver dans une terminologie nouvelle et de revenir sur certains concepts pas évidents. Pour l'auteur, c'est un bon checkpoint de compréhension et de capacité à vulgariser des concepts scientifiques et technologiques pas évidents. Mais détrompez-vous, je suis très loin d'avoir tout compris !

137 : constante que l'on retrouve pour comparer différentes grandeurs équivalentes dans la physique quantique. Il se trouve que 1/137 est une valeur qui correspond approximativement à la constante de structure fine, un ratio que l'on retrouve à plusieurs endroits dans la physique quantique et qui compare des données de même dimension. C'est par exemple le ratio entre la vitesse d'un électron de la couche basse d'un atome d'hydrogène et la vitesse de la lumière ou la probabilité d'émission sur l'absorption d'un photon pour un électron. 137 est un peu le 42 de la physique quantique. Wolfgang Pauli est mort des suites d'une opération d'un cancer du pancréas, alors que sa chambre d'hôpital avait le numéro 137.

Adiabatique : méthode de calcul quantique utilisée notamment dans les ordinateurs à recuit quantique de D-Wave. On détermine d'abord un hamiltonien complexe dont l'état fondamental décrit une solution du problème étudié. On prépare ensuite un système possédant un hamiltonien plus simple, que l'on initialise dans son état fondamental. On fait alors évoluer adiabatiquement cet hamiltonien vers le hamiltonien complexe qu'on a déterminé ; d'après le théorème adiabatique, le système reste dans l'état fondamental, et son état final décrit une solution du problème envisagé.

Algèbre linéaire : branche des mathématiques qui est utilisée dans le calcul quantique. Elle s'appuie sur la manipulation de vecteurs et de matrices. En particulier, l'état d'un qubit est représenté par un vecteur dans un espace à trois dimensions et dont la norme est égale à 1. Les opérations sur un qubit consistent à faire tourner ce vecteur dans la sphère de Bloch qui le représente. Ces rotations correspondent à des opérations d'algèbre linéaire sur le vecteur à deux dimensions qui représente l'état du vecteur. Ce sont des multiplications des vecteurs d'états par des matrices symétriques.

Algorithme : méthode de résolution de problème qui est faite d'une suite finie d'opérations ou d'instructions. Le mot vient du nom du mathématicien perse du IX^{e} siècle, Al-Khwârizmî.

Algorithme quantique hybride : algorithme qui associe des traitements classiques dans des ordinateurs traditionnels et des traitements réalisés sur ordinateurs quantiques, là où ils sont nécessaires.

Anyons : type de particule élémentaire que l'on trouve dans les systèmes de deux dimensions. C'est une généralisation du concept de bosons et de fermions. Les anyons ont des comportements statistiques intermédiaires entre les deux types de particules élémentaires. Ce sont en fait des particules virtuelles qui vivent en deux dimensions spatiales et sont généralement à base d'électrons ou de manques d'électrons se déplaçant dans des structures 2D métalliques supraconductrices. Les anyons sont un type particulier de quasi-particules. Le tout est utilisé dans les ordinateurs quantiques topologiques et le serait en particulier dans les ordinateurs à base des hypothétiques fermions de Majorana étudiés chez Microsoft.

Arxiv : site de l'Université Cornell qui permet aux chercheurs de publier des articles scientifiques avant leur publication par des revues à comités d'auteur comme Nature, Science ou Physical Review. Il peut se passer jusqu'à 9 mois entre une publication d'article sur Arxiv et dans une revue à comité d'auteurs. Dans ce dernier cas, l'article aura éventuellement évolué. L'intérêt d'Arxiv dans la recherche documentaire est que les publications y sont ouvertes et gratuites alors que la plupart des revues à comité d'auteurs sont payantes. L'inconvénient est que les articles ne sont pas forcément validés et qu'il faut prendre des pincettes dans leur évaluation. A noter que dans une publication de chercheur, il y a souvent plusieurs auteurs, jusqu'à plusieurs dizaines. Le premier auteur est généralement le thésard qui a réalisé une bonne partie du travail, notamment expérimental. Ceux du milieu sont des contributeurs qui l'ont aidé. Le dernier des auteurs est le directeur de thèse, le chef de groupe ou le directeur de laboratoire qui a encadré de près ou de loin le projet. En France, si c'est un directeur/une directrice de recherche, il/elle a probablement significativement contribué à la rédaction de l'article.

Atomes : le plus petit élément constitutif de la matière et qui manifeste des propriétés chimiques. Il comprend un noyau, avec un ou des protons chargés positivement et un ou des neutrons de charge neutre, autour duquel gravitent des électrons chargés négativement. Dans un atome neutre, le nombre d'électrons est égal au nombre de protons. Autrement, l'atome est chargé négativement ou positivement, et forme un ion. Le nombre de protons détermine la nature de l'atome dans le tableau périodique des éléments de Mendeleïev. Un atome avec un proton est de l'hydrogène, avec deux protons, c'est de l'hélium, etc. L'uranium a 92 protons. Le noyau représente l'essentiel de la masse de l'atome. Les isotopes d'un élément correspondent à des variations du nombre de neutrons dans un atome. En général, le nombre de neutrons d'un élément est équivalent à celui des protons. Les électrons sont répartis par couches dont le nombre dépend du nombre atomique. Elles sont numérotées de 1 à 7. Chaque couche peut contenir au maximum $2*n^2$ électrons, n étant le numéro de la couche (donc 2, 8, 18, 32, 50, 72 et 98). Ce modèle a été élaboré par Niels Bohr entre 1909 et 1913. Les propriétés chimiques de l'élément dépendent du nombre d'électron de la dernière couche que l'on appelle la couche de valence. Si ce nombre est $2*n^2$, l'atome sera inerte et ne se combinera pas chimiquement avec d'autres atomes. Le carbone a trois couches

d'électrons, la dernière en ayant 4 ce qui lui permet de se combiner à d'autres atomes comme l'hydrogène (1 couche, 1 électron) ou l'oxygène (6 électrons en dernière couche).

Atomes froids : atomes refroidis à très basse température, en général avec des techniques utilisant des lasers et l'effet Doppler. Ils sont utilisés dans certains types d'ordinateurs quantiques dits… à atomes froids. Les atomes utilisés sont des atomes neutres (pas ionisés) et assez souvent, le rubidium, un métal alcalin.

Avantage quantique : intervient lorsqu'un ordinateur quantique exécute un traitement plus rapidement que son équivalent optimum adapté à un supercalculateur. Cet avantage peut être décliné sur un autre aspect que la durée du calcul. Ainsi, un avantage énergétique quantique porte sur la consommation d'énergie en lieu et place du temps de calcul.

Baryon : classe des particules élémentaires de premier niveau des noyaux des atomes. Elle contient les protons et les neutrons.

Base computationnelle : dénomination des états de base des qubits qui sont mesurables par projection d'états. Cela correspond aux 0 et 1 des qubits, ou avec plus de valeurs possibles pour des qutrits (3) et qudits (au-delà de 3). Cette base utilise des états physiques ou des combinaisons d'états physiques d'état des qubits physique. Cela peut-être la phase de photons, le niveau d'énergie de courants supraconducteurs, l'orientation de spin d'un électron ou encore l'état d'énergie d'un atome froid ou d'un ion piégé. En anglais : computational basis ou bien aussi standard basis.

Bell (inégalités) : le théorème de Bell de 1964 prouve qu'aucune théorie de variable cachée - imaginée par Einstein en 1935 - ne peut reproduire les phénomènes de la mécanique quantique. Les inégalités de Bell sont les relations que doivent respecter les mesures sur des états intriqués quantiques dans l'hypothèse d'une théorie déterministe locale à variables cachées. L'expérience démontre que les inégalités de Bell sont systématiquement violées, forçant à renoncer à une des trois hypothèses suivantes sur lesquelles sont fondées les inégalités de Bell. La première est le principe de localité selon lequel deux objets distants ne peuvent avoir une influence instantanée l'un sur l'autre, ce qui revient à dire qu'un signal ne peut se propager à une vitesse plus grande que celle de la lumière dans le vide. La seconde est la causalité selon laquelle l'état des particules quantique est déterminé uniquement par leur expérience, c'est-à-dire leur état initial et l'ensemble des influences reçues dans le passé. La troisième est le réalisme qui signifie que les particules individuelles sont des entités qui possèdent des propriétés propres, véhiculées avec elles (source).

Blind Quantum Computing : technique de répartition des traitements quantiques dans des processeurs quantiques à distance et sécurisant la confidentialité des traitements.

Bloch (sphère) : modèle géométrique de représentation de l'état d'un qubit avec un vecteur dans une sphère de rayon 1. L'état au repos du qubits est un vecteur 0 dirigé vers le haut et l'état excité est un vecteur 1 dirigé vers le bas. Un vecteur d'état intermédiaire est défini par son amplitude et sa phase, en ligne avec la dualité onde-particule des qubits.

Born (règle) : modèle qui décrit la relation entre la probabilité des états quantiques d'un quantum. La somme de la probabilité de chaque état au carré égale 1 sachant que chaque probabilité se décrit avec un nombre complexe traduisant l'amplitude et la phase de chaque état possible du quantum. On retrouve ce modèle dans la représentation géométrique de la sphère de Bloch.

Boson : particules au comportement grégaire, qui peuvent s'accumuler en nombre arbitrairement grand et dans le même état. On y trouve les photons et les objets composites de spin entier comme les atomes d'hydrogène, de lithium-7, de rubidium-87, de carbone, de silicium dans des structures cristallines (source : Jean Dalibard). Ces particules échappent au principe d'exclusion de Pauli. Elles ont une fonction d'onde symétrique.

Boson (simulation) : résolution d'un problème de physique quantique avec du calcul quantique ou un simulateur quantique analogique.

Bose-Einstein (condensat) : état de la matière de gaz de bosons à très faible densité refroidi à une température voisine du zero absolu (-273,15°C) lors duquel une grande partie des bosons sont dans l'état énergétique quantique le plus bas possible et manifestent des propriétés particulières comme des interférences. Un cas particulier est celui de l'hélium superfluide, découvert en 1938, et qui, à très basse température, n'a plus de viscosité, à savoir qu'il peut se déplacer sans dissiper d'énergie. Ces condensats ont été imaginés et théorisés le chercheur indien Satyendra Nath Bose puis Albert Einstein en 1924 et leur existence démontrée par l'expérience en 1995 par Wolfgang Ketterle, Eric Cornell et Carl Wieman qui obtinrent pour cela le prix Nobel de physique en 2001. Dans l'informatique quantique, ce domaine a un lien avec le champ des qubits à base d'atomes froids et supraconducteurs.

BQP (classe de problème) : classe de complexité des problèmes qui peuvent être traités par des algorithmes quantiques. Signifie « bounded-error quantum polynomial time ». C'est la classe des problèmes qui peuvent être résolus en temps polynomial par rapport à la taille du problème avec une probabilité d'obtenir une erreur ne dépassant pas le tier des résultats. Cette classe est comprise entre la classe P (problèmes qui peuvent être résolus en temps polynomial sur machine classique) et NP (problèmes dont on peut vérifier une solution en temps polynomial sur une machine classique).

Bra-ket (notation) : modèle de notation décrivant l'état d'un quantum et d'un qubit sous la forme $\langle\phi|\psi\rangle$. Elle a été créée par Paul Dirac en 1939. La partie droite est le vecteur complexe en colonne qui décrit l'état quantique. La partie gauche est un vecteur ligne qui est la transposée de la partie droite.

Cavités Fabry-Pérot : appareillage utilisé dans les lasers qui associe deux miroirs parallèles dont l'un est semi-réfléchissant. C'est ce qui contribue à générer l'effet laser

dans la cavité. La longueur de la cavité est généralement un multiple de la longueur d'onde du laser, en tout cas si l'on cherche à émettre une lumière cohérente avec des photons ayant tous la même phase. Le nom de la cavité vient de Charles Fabry (1867-1945) et Alfred Pérot (1963-1925).

Chandelier : nom souvent donné au système situé à l'intérieur du cryostat d'un ordinateur quantique à base notamment de qubits supraconducteurs ou silicium. Il est constitué de plusieurs étages faits de disque en cuivre recouverts d'or. Ces disques sont traversés par de nombreux câbles coaxiaux qui servent à piloter les qubits et à lire leur état. C'est complété par divers composants électroniques : filtres, atténuateurs et amplificateurs des micro-ondes qui circulent dans ces fils, capteurs divers, et échangeurs thermiques refroidissant les disques en cuivre qui à leur tour refroidissent les éléments qui sont posés dessus.

Chromodynamique quantique : décrit l'interaction forte, l'une des quatre forces fondamentales, qui régit les interactions entre les quarks et les gluons et la cohésion des noyaux des atomes. Pourquoi « chromo » ? Parce que l'on décrit les états des particules élémentaires avec des codes de couleur : bleue, verte et rouge pour les particules puis antibleue, antiverte et antirouge pour les antiparticules. Cette théorie s'appuie sur la théorie quantique des champs. Cette partie de la physique quantique n'est pas utilisée dans le cadre de la création de qubits. Elle l'est pour la physique des particules élémentaires et est vérifiée dans les grands accélérateurs de particules comme le LHC du CERN à Genève.

Clé privée : clé utilisée dans les systèmes de chiffrement à clé privée. Les clés sont échangées au préalable par les parties avec un algorithme de chiffrement, souvent des hash ou des algorithmes Diffie-Helfmann.

Clé publique : système de chiffrement qui passe par l'envoi d'une clé publique à un interlocuteur qui va l'utiliser pour chiffrer un message envoyé dans l'autre sens. Les éléments ayant permis de créer cette clé publique sont utilisés pour le déchiffrement du message envoyé. Il est normalement impossible ou très difficile de décomposer la clé publique pour retrouver les éléments qui ont permis de la créer.

Clifford (groupe) : groupe de portes quantiques unitaires qui sont simulables facilement et en temps polynomial sur ordinateurs classiques selon le théorème de Gottesman-Knill. Une porte de Clifford est une porte quantique qui peut être décomposée en portes du groupe de Clifford. Il suffit d'avoir une porte réalisant une rotation sur l'axe X et une autre sur l'axe Z pour créer un jeu de portes de Clifford complet. Elles doivent être complétées d'au moins une porte à deux qubits comme une CNOT. Ces portes réalisent des quarts de tours ou des demi-tours dans la sphère de Bloch. Pour créer un jeu de portes universelles capable de créer toute transformation unitaire, il faut ajouter au moins une porte hors groupe de Clifford comme une porte T qui réalise un huitième de tour dans la sphère de Bloch.

Cluster state : base de départ d'un calcul MBQC (Measurement Based Quantum Computing) avec une grille de qubits intriqués.

CMOS : technique de fabrication courante de semiconducteurs utilisée pour produire des processeurs et de la mémoire, et qui est réutilisée pour créer des qubits manipulant des spins d'électrons.

Codes de correction d'erreurs : décrit à la fois les méthodes logiques et architectures physiques permettant de contourner les erreurs générées par le bruit dans le calcul quantique universel et une variante de cryptographie post-quantique.

Cognition quantique : modèle descriptif du fonctionnement de la connaissance humaine (langage, prise de décision, mémoire, conceptualisation, jugement, perception) qui s'appuie sur le formalisme mathématique de la mécanique quantique, en procédant principalement par analogie, sans passer par des explications physiques ou de quantification des neuro-sciences, qui eux relèvent du champ « quantum mind » issu des travaux de Roger Penrose. Voir la fiche Wikipedia associée. Il n'y a pas de startups dans cette catégorie !

Cohérence : état permettant la superposition d'états dans un objet quantique et l'intrication entre plusieurs objets quantiques. Cette cohérence se dégrade progressivement naturellement et se termine au bout d'un certain temps pour les qubits (le temps de cohérence) et lors de la mesure de l'état d'un qubit.

Complexité (théorie) : branche de l'informatique théorique et des mathématiques qui joue un rôle important dans le calcul quantique pour évaluer sa performance par rapport au calcul traditionnel sur machine de Turing/Neumann. Elle définit des classes de problèmes par niveau de complexité, en termes de temps de calcul voire d'espace mémoire nécessaire, avec, notamment, des problèmes qui sont résolus en temps polynomial par rapport à leur complexité (classe P) et dont les résultats sont vérifiables en temps polynomial (classe NP). Les méthodes de résolutions de ces problèmes relèvent le plus souvent de la force brute consistant à naviguer dans un espace de plus en plus grand de combinatoires à évaluer en fonction de la taille du problème à résoudre.

Concatenated codes : décrit l'application récursive de codes de correction d'erreur où dans un code de correction d'erreur, un qubit physique est remplacé par un qubit logique, et ainsi de suite.

Continuous variables quantum computing (CV) : type d'ordinateur quantique qui utilise des qubits dont la valeur est continue et non binaire. Utilisée dans deux types d'ordinateurs quantiques : les simulateurs quantiques analogiques (notamment à base d'atomes froids) et les ordinateurs à recuit quantiques de D-Wave.

Corps noir : corps qui est en équilibre thermique avec le rayonnement qu'il émet. Cela peut être l'intérieur d'un four où une étoile. C'est en étudiant le rayonnement du corps noir et sa fréquence en fonction de la température du corps que Max Planck a découvert l'existence des quanta en 1900.

Courbes elliptiques : type de cryptographie à clés publiques qui est potentiellement cassée par les algorithmes quantiques. Elliptic-curve cryptography (ECC) en anglais. L'un de ses avantages est de nécessiter des clés de petite taille, environ trois fois plus petites en nombre de bits que les clés publiques RSA.

Cryogénie : technique de refroidissement. La cryogénie à très basse température est utilisée dans une bonne partie des ordinateurs quantiques, tous ceux qui sont à base d'électrons ou d'atomes froids. Les températures requises pour stabiliser des qubits et réduire leur taux d'erreur sont très proches du zéro absolu : entre 5 et 20 mK. Les systèmes les plus utilisés sont des réfrigérateurs à dilution qui exploitent de l'hélium 3 et de l'hélium 4. La cryogénie est aussi utilisée pour les systèmes de lecture de qubits à base de photons.

Décohérence : marque la fin de la cohérence d'un objet quantique ou d'un qubit. Elle est notamment provoquée par les interactions entre ces derniers et leur environnement. On utilise souvent indifféremment l'expression temps de cohérence (temps pendant lequel les qubits sont en état de superposition et d'intrication avec d'autres qubits) ou de décohérence (temps au bout duquel cette superposition et l'intrication se terminent), ce qui revient au même.

Deutsch-Jozsa (algorithme) : algorithme quantique crée en 1992 par David Deutsch et Richard Jozsa servant à vérifier si une fonction donnée est équilibrée ou non, à savoir, si elle renvoie toujours 0 ou 1, ou des 0 et 1 à proportion égale. L'alternative entre l'équilibre (autant de 0 que de 1) ou non (que des 0 ou des 1 en sortie) est le postulat de départ. Le gain de performance par rapport à des algorithmes classiques est exponentiel. Dans le cas de N qubits, il faudrait évaluer la fonction sur au moins la moitié des valeurs d'entrée possible, soit 2 puissance N-1 +1. Malheureusement, cet algorithme ne sert pas à grand-chose.

DFT (Density Functional Theory) : modèle mathématique servant à décrire la structure de molécules au repos en fonction des interactions inter-atomiques. Utilisé dans le calcul haute performance ainsi que dans le calcul quantique pour la simulation chimique.

Distillation : technique utilisée dans la gestion de codes de correction d'erreurs à base de magic states. Elle consiste à combiner plusieurs qubits de type magic state pour en alimenter d'autres avec un taux d'erreur plus faible.

Doppler (effet) : décalage du spectre électromagnétique sous l'effet de la vitesse d'éloignement ou de rapprochement de la source par rapport à l'observateur. Si la source s'éloigne de l'observateur, la lumière est décalée vers le rouge (redshift), dans le cas contraire, vers le bleu. Cet effet est notamment utilisé dans la technique de refroidissement des atomes par laser dans les températures cryogéniques. Il consiste à éclairer des atomes qui sont en mouvement du fait de la température avec une fréquence qui est juste en-dessous du niveau d'absorption des atomes en question. Ceux qui se déplacent vers la lumière vont absorber le photon ce qui réduira leur énergie cinétique. Ceux qui se déplacent dans l'autre direction ne les absorberont pas car la fréquence apparente du photon sera trop faible pour changer l'état énergétique des atomes. Cette technique permet de refroidir des atomes jusqu'à en-dessous du mK (milli-Kelvin).

Dualité onde particule : propriété de particules élémentaires ayant une masse comme les électrons, les neutrons ou les atomes de se comporter à la fois comme des particules avec une masse et des ondes pouvant générer des interférences. On le vérifie avec la fameuse expérience des fentes de Young qui mettent en évidence ces interférences.

D-Wave : société canadienne concevant des ordinateurs quantiques à recuit quantique. Ils n'ont pas la même puissance que les ordinateurs quantiques à portes universelles à nombre égal de portes. Mais ces derniers sont actuellement situés entre 50 et 100 portes tandis que la génération actuelle des D-Wave comprend 2048 qubits.

Ecrasement de la fonction d'onde de Schrödinger : petit nom donné à la fin de la cohérence d'un qubit (état superposé) qui est notamment généré par la mesure de son état qui le rabat à l'une de ses valeurs de base (0 ou 1). Cet écrasement peut aussi intervenir au terme de la durée de cohérence. Celui-ci est provoqué par l'interaction avec le qubit et son environnement.

Effet tunnel : propriété d'un objet quantique de franchir une barrière de potentiel (ou d'énergie) même si son énergie est inférieure à l'énergie minimale requise pour franchir cette barrière. Cet effet est utilisé dans les ordinateurs recuit quantique de D-Wave pour déterminer rapidement un minimum énergétique d'un système complexe (« hamiltonien »).

Eigenstate : voilà un concept quantique que les physiciens ont bien du mal à vulgariser de manière non récursive. L'explication en anglais est « *quantum state whose wave function is an eigenfunction of the linear operator that corresponds with an observable*." Ce qui nous fait une belle jambe puisque cela oblige à comprendre la définition de quatre autres notions. En vaguement clair, cela correspond à l'utilisation de repères orthonormés de description de l'état d'un quantum.

Electrodynamique quantique : branche de la physique quantique, ou QED en anglais (Quantum Electro-Dynamic) est « *une théorie physique ayant pour but de concilier l'électromagnétisme avec la mécanique quantique en utilisant un formalisme lagrangien relativiste. Selon cette théorie, les charges électriques interagissent par échange de photons* » (Wikipedia). C'est la base de la théorie quantique des champs qui s'applique à toutes les particules élémentaires.

Electron : particule élémentaire que l'on trouve notamment dans les atomes, en orbite autour du noyau. D'après le modèle de Bohr élaboré en 1913, il existe un nombre fini d'orbites d'électrons autour du noyau des atomes. Le déplacement des électrons d'une orbite à l'autre correspond à l'absorption ou l'émission d'un photon. Les électrons sont souvent utilisés dans les qubits, notamment sous forme d'électrons piégés dans des semi-conducteurs et dont on contrôle le spin. L'électron est « élémentaire » car il n'est pas composé de sous-particules, contrairement aux neutrons et aux protons qui sont composés de quarks.

Emulateur quantique : système logiciel et/ou matériel utilisant un ordinateur classique servant à exécuter un logiciel destiné à un ordinateur quantique. Cela permet de faire des tests de programmes quantiques sans disposer d'ordinateur quantique. La vitesse d'exécution est moins bonne que sur un calculateur quantique, surtout dès que l'on dépasse quelques dizaines de qubits. Et au-delà d'une cinquantaine de qubits, la capacité des machines classiques est insuffisante pour réaliser ce genre d'émulation. Il ne faut pas confondre l'émulation avec la simulation quantique. Cette dernière simule des phénomènes de physique quantique avec un ordinateur quantique analogique.

Equations linéaires : opérations mathématiques relevant de l'algèbre linéaire. Dans le cas du calcul quantique, il s'agit de multiplications de matrices de nombres complexes.

ERC Grants : European Research Council grants. Un financement de projets de recherché européen avec plusieurs niveaux dont le top est le Synergy Grant qui finance des « moonshots » dans la recherche européenne associant au moins deux laboratoires de recherche. 14M€ est le financement maximum d'un tel projet avec 10M€ de financement de base et 4M€ qui peuvent notamment financer des investissements lourds où l'accès à de grosses infrastructures.

Erreurs : gros sujet de préoccupation dans le fonctionnement des ordinateurs quantiques. Les opérations sur les qubits : portes à un ou plusieurs qubits puis mesure de leur état génère des erreurs qu'il faut chercher à minimiser. Les taux d'erreurs sont en 2019 compris entre 0,4% et 4% pour les portes quantiques. Lorsque l'on enchaine plusieurs portes quantiques, les taux de résultats corrects (1-% d'erreur) se multiplient au point de tout fausser. On évite cela soit en réduisant le taux d'erreurs, soit en utilisant des algorithmes de faible profondeur (faible nombre de portes) soit avec des systèmes de code de correction d'erreurs.

Espace de Fock : objet mathématique d'algèbre qui sert à décrire l'état quantique d'un ensemble de particules identiques dont le nombre est variable ou inconnu. C'est un espace de Hilbert constitué de la somme des produits tensoriels des espaces de Hilbert pour les particules qui composent l'ensemble.

Fermions : particules au comportement individualiste. Deux particules de ce type ne peuvent pas être dans le même état au même endroit. Cela comprend les électrons, les quarks, les objets composites de spin demi-entier. Par exemple les atomes de deutérium, de lithium-6, de potassium-40 (source : Jean Dalibard). Par opposition, les bosons de spin entier comme les photons et certains atomes peuvent s'accumuler dans le même état.

Fermion de Majorana : quasi-particule à base d'électrons dans des matériaux supraconducteurs qui pourrait servir à gérer des qubits fiables dans le cadre de ce que l'on appelle le calcul topologique. Cette particule virtuelle a été imaginée par Ettore Majorana en 1937. C'est sur elle que Microsoft compter créer un ordinateur quantique sachant que l'existence de la quasi-particule n'a pas été véritablement démontrée.

Flying qubits : qubits pouvant se déplacer, à contrario des stationary qubits qui ne bougent pas. Ce sont en général des photons.

Friedkin (porte) : porte quantique qui opère sur trois qubits. Elle intervertit l'état du second et du troisième qubit si le premier qubits est à la valeur 1. Aussi dénommée porte CSWAP (conditionnal SWAP).

FTQC : Fault-Tolerant Quantum Computer. Ordinateur quantique résistant aux erreurs. A priori, avec un très grand nombre de qubits et des codes de correction d'erreurs.

GHZ : veut dire autre chose que giga Hertz en informatique quantique ! Il s'agit d'un état superposé Greenberger-Horne-Zeilinger à trois qubits qui permet de démontrer l'inexistence de variables cachées dans l'intrication quantique d'au moins trois particules et avec un nombre fini de mesures. La notion date de 1989 et sa validation expérimentale de 1999.

Grover (algorithme) : algorithme quantique de recherche d'un élément dans un tableau non indexé.

Hadamard (porte) : porte permettant de générer un état superposé entre 0 et 1 dans un qubit.

Hamiltonien : équations servant à décrire l'énergie totale et potentielle d'un système de particules élémentaires. L'équation de Schrödinger décrit l'évolution dans le temps d'un hamiltonien d'une particule élémentaire. Ce concept est notamment utilisé dans les ordinateurs à recuit quantique de D-Wave. « Préparer un Hamiltonien » dans ce genre d'ordinateur revient à mettre en place une matrice de qubits reliés entre eux par des potentiels et qui va rechercher un minimum énergétique aboutissant à un hamiltonien équilibré correspondant à la solution du problème à résoudre. C'est l'explication la plus simple que j'ai trouvée à ce concept qui nécessite sinon de solides bases mathématiques.

Hélium 3 : isotope rare de l'hélium qui est utilisé dans les systèmes cryogénie d'ordinateurs quantiques pour générer des températures inférieures à 1K. Il est généralement produit à partir de tritium dans des centrales nucléaires spécialisées, notamment celle de Savannah River du Département de l'Energie aux USA.

Heisenberg (principe d'indétermination) : principe fondamental de la mécanique quantique qui postule qu'il existe une limite inférieure à la précision avec laquelle on peut connaître deux paramètres indépendants relatif à un même objet comme sa vitesse et sa position ou l'énergie émise et la durée d'émission.

Hélium 4 : isotope commun de l'hélium qui est également utilisé dans les systèmes de cryogénie. Il est aussi superfluide à très basse température (moins de 2K).

Hilbert (espace) : espace vectoriel de nombres réels ou complexes muni d'un produit scalaire euclidien ou hermitien, qui sert à mesurer des distances et des angles et de définir une orthogonalité. C'est une extension à n dimensions du concept d'espace euclidien à trois dimensions. En mécanique quantique, l'état d'un quantum est représenté par un vecteur dans un espace de Hilbert à autant de dimensions que le nombre d'états de base (ou obser-

vables) de ce quantum. Il s'agit d'espaces géométriques qui servent notamment à mesurer des longueurs et des angles, de faire des projections sur des dimensions et de définir l'orthogonalité entre vecteurs.

HPQC : High Performance Quantum Computing, analogue quantique du HPC (High Performance Computing). Il s'agit pour l'instant de modèles théoriques de mainframes quantiques comprenant des matrices géantes de qubits pouvant être partitionnées pour un usage partagé par plusieurs utilisateurs. Voir High Performance Quantum Computing, 2011 (7 pages).

Hydrodynamique quantique : étudie les effets hydrodynamiques de systèmes quantiques tels que les éléments superfluides (hélium à très basse température) ou les polaritons et les fluides de lumière associés.

Intrication : liaison entre deux quantums qui sont reliés entre eux de telle sorte qu'une modification de l'un entraîne celle de l'autre. Ce processus est utilisé pour relier des qubits entre eux par des portes quantiques à deux ou trois qubits dans les ordinateurs quantiques. Il l'est également dans les systèmes de cryptographie et de télécommunications quantiques à base de photons intriqués, exploités dans les QKD. Mais attention, l'intrication est étroitement associée au côté aléatoire de la mesure de l'état des objets quantiques intriqués. Leur mesure est corrélée mais elle est aléatoire. L'intrication ne permet pas de définir une information à un point A et de l'intriquer avec B. Par contre, on peut s'appuyer sur une intrication pour téléporter l'état d'un qubit d'un point A à un point B. Comme cela nécessite l'emploi de deux canaux d'informations bits classiques en plus du canal optique de l'intrication, l'information sur le qubit ne peut pas être transmise plus vite que la lumière.

Ion : atome non neutre, qui a une charge électrique positive ou négative. Elle est négative si son nombre d'électrons dépasse celui des protons (anions) et positive dans le cas contraire (cations).

Ion piégé : ce sont des ions utilisés dans certains types d'ordinateurs quantiques. Ils sont généralement piégés magnétiquement ou électriquement et on contrôle leur état avec des lasers.

IonQ : startup américaine issue de l'Université de Maryland et à l'origine des premiers ordinateurs quantiques commerciaux à ions piégés. Leur record annoncé fin 2019 était de 79 ions piégés.

Ising (modèle) : problème de physique statistique qui peut être simulé et résolu à l'aide d'algorithmes quantiques, en particulier sur ordinateurs à recuit quantique. Il modélise les interactions entre particules à deux états.

Josephson (effet) : effet supraconducteur utilisé dans les qubits de d'ordinateurs quantiques dits à supraconducteurs comme ceux d'IBM et Google.

Ket : vecteur à deux dimensions en nombres complexes qui définit l'état d'un qubit.

Laser : source de lumière cohérente inventée en 1960 et utilisée dans de nombreux domaines comme les lecteurs de CD et DVD, les communications par fibre optique, en chirurgie, ophtalmologie et odontologie. On les retrouve aussi souvent dans l'informatique quantique pour contrôler des atomes froids ou gérer des qubits à base de photons ainsi que dans la cryptographie quantique (QKD & co). Laser signifie Light Amplification by Stimulated Emission of Radiation ». C'est une source de lumière cohérente, à savoir qu'elle est constituée de photons de même polarisation, phase et longueur d'onde, qui sont émis dans une même direction. L'amplification utilise un processus d'émission stimulée dans un milieu actif amplificateur fait de solide, fibre, liquide, gaz ou semiconducteur qui est placé au centre d'une cavité optique résonante avec d'un côté, un miroir réfléchissant et de l'autre un miroir semi-réfléchissant qui permet de faire sortir le faisceau lumineux. La fréquence et la puissance du rayonnement lumineux dépendent de nombreux paramètres. L'énergie provient d'un système d'excitation ou de pompage : laser primaire, diode laser, lampe flash ou décharge électrique.

Localité (principe) : principe selon lequel des objets distants ne peuvent avoir une influence directe l'un sur l'autre. Un objet ne peut être influencé que par son environnement immédiat. Ce principe issu de la relativité restreinte d'Albert Einstein est remis en question par la mécanique quantique, la non localité et l'intrication quantique observées expérimentalement depuis au moins 1982 avec des photons, dans le cadre de la fameuse expérience d'Alain Aspect (avec Philippe Grangier et Jean Dalibard).

Log discret (problème) : problème mathématique consistant à trouver un log entier d'un nombre. Est utilisé dans la résolution de problèmes de cryptographie à l'aide d'algorithmes quantiques. Peter Shor a créé un algorithme dit « dlog » capable de résoudre des problèmes de logarithmes discrets.

LSQC : Large Scale Quantum Computing appelé aussi FTQC pour fault tolerant quantum computing. Catégorie d'ordinateurs quantiques futurs à tolérance de pannes. Ceux-ci reposeront sur l'usage de nombreux qubits physiques assemblés en qubits logiques présentant, vu du logiciel, un très faible taux d'erreurs.

Magic states : qubits utilisés dans une méthode de gestion de codes de correction d'erreurs dénommée magic states distillation. Difficile d'en dire plus tellement c'est compliqué !

Matrice : objet mathématique fait de lignes et de colonnes de valeurs.

Matrice densité : objet mathématique en forme de matrice carrée servant à définir aussi bien des états mixtes que des états purs de systèmes à un ou plusieurs objets quantiques. Il est notamment indispensable pour décrire la richesse des données comprises dans un système intriqué de qubits. La diagonale de la matrice décrit les probabilités des états de la base computationnelle du registre quantique (les combinaisons de 0 et de 1) et les probabilités de corrélation entre ces états (hors de la diagonale).

MBQC ou MQCM : Measurement Based Quantum Computing, méthode de calcul quantique inventée en 2001 par Robert Raussendorf et Hans Briegel qui utilise un nombre élevé de qubits intriqués dans des grilles à deux dimensions et dans lequelles des lectures d'état de

qubits sont réalisées pour modifier la structure de la grille. Ces mesures servent aussi à guider l'algorithme.

Médecine quantique : en général, fausse science et charlatanerie qui s'appuie sur une interprétation totalement fantaisiste de la mécanique quantique.

Mélasse optique : gaz d'atomes neutres froids dont la force de cohésion est de type visqueux.

MINLP : Mixed Integer Non Linear programming, classe de problèmes complexes qui peuvent être potentiellement résolus avec des algorithmes quantiques. Il s'agit de trouver le ou les minimums de fonctions non linéaires et sous contraintes qui visent à respecter des fonctions non linéaires. Les variables de l'équation sont une combinaison de nombres entiers et de nombres flottants. Les applications sont nombreuses dans tous les cas où l'on cherche à optimiser une fonction sous contraintes (distribution d'énergie, décollage optimum d'un avion, optimisation de portefeuille financier, minimiser le risque dans une assurance ou dans le crédit, etc).

Mixed state : état de quantums qui représentent l'association statistique de deux états purs. Ce genre d'état qui s'oppose à un état pur (pure state) qui est représenté par un vecteur complexe à deux dimensions. Un état mixte est représenté par une matrice densité.

NISQ : Noisy Intermediate-Scale Quantum, dénomination des calculateurs quantiques actuels et à venir dans un futur proche, qui sont de taille intermédiaire en nombre de qubits (quelques dizaines à centaines) et sujets à un bruit quantique qui en limite les capacités. Cette appellation a été créée par le chercheur américain John Preskill.

Noms de chercheurs : les conventions de nommage des chercheurs dans les publications scientifiques donnent du fil à retordre à nombre d'observateurs dont je fais partie. Ils ne comprennent que les initiales de prénoms, créant parfois de situations ubuesques avec des homonymes dans ces conditions (exemple). Visiblement, ce système antédiluvien semble difficile à réformer. Seule explication valable : le besoin de recourcir la liste interminable de contributeurs des articles. Mais aussi, de nombreuses variations culturelles dans la manière de dénommer une personne. Lorsque je cite ces articles, j'utilise la convention « et al » en ne citant que le premier auteur ou celui ou celle qui est connu(e) pour être le principal contributeur. Et j'enlève le middle name des scientifiques américains au passage ! « et al » est la compression du latin et alii ou et aliae qui veut dire « et tous les autres ».

Nombre complexe : ensemble des nombres complexes créé comme extension de l'ensemble des nombres réels, contenant en particulier un nombre imaginaire noté i tel que $i^2 = -1$. Tout nombre complexe peut s'écrire sous la forme a + i b où a et b sont des nombres réels. Ces nombres servent notamment à décrire l'état d'un qubit.

Non localité : principe permettant à un objet (quantique) d'influencer l'état d'un autre objet (quantique) à distance, celle-ci pouvant être très grande. Contredit le principe de localité qui veut d'un objet ne puisse influencer qu'un autre objet qu'à proximité. L'intrication quantique de photons à de grandes distances vérifie la non localité.

Non clonage (théorème) : interdit la copie à l'identique de l'état d'un quantum. Il a comme conséquence qu'il est impossible de copier l'état d'un qubits pour l'exploiter indépendamment de son original. Toute copie détruit l'original. !

Notation de Dirac : voir bra-ket.

NP (classe de problème) : classe de problèmes dont la solution est vérifiable dans un tems polynomial relativement à la taille du problème. Comprend notamment les problèmes dits exponentiels ou intractables, dont le temps de la résolution est exponentiel par rapport à leur taille. Un ordinateur quantique permet de résoudre une partie des problèmes NP.

NP-complet (classe de problème) : problème de décision dont il est possible de vérifier une solution en temps polynomial et pour qui tous les problèmes de la classe NP se ramènent à celui-ci via une réduction polynomiale. Cela signifie que le problème est au moins aussi difficile que tous les autres problèmes de la classe NP. Les problèmes du voyageur de commerce et du remplissage du sac à dos sont des problèmes NP Complet. Le concept date de 1971 et provient de Stephen Cook.

NP-difficile (classe de problème) : problème vers lequel on peut ramener tout problème de la classe NP par une réduction polynomiale. S'il est également dans la classe NP, on dit que c'est un problème NP-complet. Si $P \neq NP$, alors, les problèmes NP-difficile ne peuvent pas être résolus en temps polynomial.

Observable : équivalent en mécanique quantique d'une grandeur physique en mécanique classique, comme la position, la quantité de mouvement, le spin ou l'énergie. Pour un qubit d'ordinateur quantique, un observable est l'un des deux états de base, au repos ou excité (0 ou 1) du qubit.

Opération unitaire : opération sur un vecteur qui préserve sa longueur. Dans le cas des qubits dont le vecteur a toujours une longueur de 1, les portes quantiques unitaires appliquent dessus une transformation qui préserve cette longueur. Dans la représentation des qubits dans la sphère de Bloch, l'opération fait tourner le vecteur représentant l'état du qubit dans cette sphère.

Optique linéaire : champ de la mécanique quantique qui manipule des photons en s'appuyant sur leurs propriétés classiques : polarisation, phase ou fréquence.

Optique non linéaire : domaine de l'optique où les propriétés optiques de matériaux dépendent de l'amplitude lumineuse et conduire à l'apparition de nouvelles fréquences. La non linéarité qualifie la réponse d'un milieu à une excitation en général assez énergétique provenant de champs intenses, issus principalement de lasers, en particulier les lasers à impulsions femtosecondes. En pareil cas, la réponse d'un matériau à la somme de deux champs électromagnétiques n'est pas égale à la somme de de la réponse à chaque champ individuel. L'optique non linéaire permet notamment de gérer des portes quantiques à deux photons. Elle sert aussi à générer des fréquences lumineuses variées avec plus de latitude, comme pour créer des lasers émettant une lumière blanche.

P (classe de problème) : problème qui peut être résolu en temps polynomial par rapport à sa taille, sur une machine de Turing déterministe.

Paire de Cooper : paires d'électrons qui se combinent pour faire circuler le courant électrique dans les matériaux supraconducteurs, en général à très basse température, et sans opposer de résistance. Les paires de Cooper ont un spin entier car elles cumulent deux électrons ayant un spin de ½.

Pauli (principe d'exclusion) : postule que deux particules de type fermion ne peuvent se trouver dans le même état quantique. Deux électrons ou deux neutrons ne peuvent se trouver au même endroit avec le même niveau d'énergie. Si une force extérieure comme la gravitation les oblige à se trouver au même endroit, ils ne pourront pas avoir la même énergie c'est-à-dire la même vitesse. Si un ensemble de fermions doit se trouver dans un même lieu, ils vont devoir adopter des vitesses toutes différentes.

Permanent : objet mathématique utilisé pour décrire la complexité du calcul classique d'un échantillonnage de boson. Il est très complexe à évaluer de manière classique qui exploite un sigma de multiplication de matrices permettant d'illustrer la combinatoire des combinaisons de photons interférant les uns avec les autres dans un ensemble d'interféromètres.

Phase : situation instantanée d'une grandeur qui varie cycliquement, en physique et en mécanique des ondes. On parle surtout de déphasage d'une onde par rapport à une onde de référence. Le déphasage entre deux ondes s'exprime comme un angle (en radians, degrés ou tours, en considérant un tour comme une période), comme un temps (à comparer avec la période de l'onde) ou comme une distance (à comparer avec la longueur d'onde).

Phase Estimation Algorithm (PEA) : un des premiers algorithmes de simulation de la structure électronique de molécules sur ordinateur quantique. Mais il requiert des temps de cohérence assez longs que les ordinateurs quantiques à porte universelle ne sont pas encore en mesure de fournir. L'algorithme est « concurrencé » par le Variational Quantum Eigensolver (VQE), un algorithme hybride qui fonctionne avec un nombre de portes quantiques plus faible.

Phonon : ondulations d'atomes dans des phénomènes nanoscopiques. Ils se manifestent notamment dans la supraconductivité en suivant et accompagnant le mouvement des électrons arrangés en paires de Cooper ainsi que pour relier entre eux par portes quantiques des ions piégés.

Photon : quantum d'énergie associé aux ondes électromagnétiques allant des ondes radio (ondes longues, fréquences peu élevées) jusqu'aux rayons gamma (ondes très courtes, fréquences très élevées) en passant par la lumière visible. Depuis 1926, c'est une particule de lumière élémentaire. Sa masse est nulle. Son spin est 1 et il fait donc à ce titre partie des bosons, à savoir qu'ils peuvent s'accumuler au même endroit dans le même état contrairement aux fermions. Les photons sont notamment générés lors de changements d'états énergétiques d'atomes et, plus précisément, de niveau d'orbite d'électrons tournant autour des noyaux d'atomes.

Physique de la matière condensée : branche de la physique qui étudie les propriétés macroscopiques de la matière (solides, liquides, verres, polymères) et dans les systèmes où le nombre de constituants est grand et les interactions entre eux sont fortes. Les physiciens de la matière condensée cherchent à comprendre les comportements de ces phases en utilisant les lois de la physique (mécanique quantique, électromagnétisme et physique statistique). Ce champ est historiquement limité aux systèmes qui peuvent être étudiés en laboratoire. En pratique, cette science s'intéresse surtout aux phases supraconductrices à basse température, aux phases ferromagnétique, antiferromagnétique et ferrimagnétique des spins dans des réseaux cristallins d'atomes, les verres de spins, liquide de spins, ainsi que le condensat de Bose-Einstein. Les physiciens qui travaillent sur les qubits supraconducteurs font partie de cette discipline.

Polaritons : quasi-particules quantiques du domaine des interactions fortes entre lumière et matière. Ils résultent du couplage entre des photons et une onde de polarisation électrique qui se manifeste en particulier dans des plasmons (oscillations d'électrons libres dans des métaux), des phonons (oscillations d'atomes, en particulier dans des structures cristallines) et des excitons (paires d'électrons-trous d'électrons générées par des photons dans des semi-conducteurs).

Pompage optique : technique qui sert à modifier les états des atomes en augmentant leur niveau d'énergie à l'aide de photons polarisés. Elle a valu le prix Nobel de physique en 1966 au Français Alfred Kastler, qui l'avait inventé en 1950. La technique est utilisée dans la photonique et notamment dans les lasers et la métrologie quantique. Le pompage optique passe par trois à quatre niveaux d'énergie des atomes (E_0, E_1, E_2, E_3). Le pompage fait passer un atome de son niveau fondamental E_0 au niveau E_3. Une relaxation (mécanique) ramène l'atome de l'état E_3 en E_2. Dans les lasers, cela permet de générer une inversion de population entre les états E_1 et E_2, pour faire en sorte qu'il y ait plus d'atomes dans l'état E_2 que dans l'état E_1. L'émission spontanée et stimulée de photons d'énergie E_2- E_1 peut alors avoir lieu. L'atome au niveau E_1 repasse ensuite au niveau E_0 par relaxation.

Portes quantiques : opérations de manipulations de l'état de qubits qui agissent sur un ou plusieurs qubits. Les portes à plusieurs qubits (Toffoli, Friedkin, …) qui exploitent le principe de l'intrication quantique. Les opérations de portes quantiques sont générées par des actions physiques sur les qubits qui dépendent de leur nature. Pour les qubits supraconducteurs, il s'agit d'envoi de microondes entre 5 et 10 GHz via des conducteurs électriques. Pour les ions piégés, ce sont des opérations pilotées par des lasers. Pour des qubits CMOS, ce sont des tensions électriques. Pour les qubits reposant sur des particules à masse (électrons, ions, atomes froids), les portes quantiques agissent sur les qubits mais ceux-ci ne bougent pas. Pour des qubits à base de photons, ceux-ci circulent et traversent des portes quantiques qui modifient leur état (phase, fréquence, ou autre).

Portes quantiques universelles : se dit de jeux de portes quantiques à partir desquelles toutes les autres portes quantiques peuvent être reproduites.

PCQC : Paris Center for Quantum Computing, communauté de chercheurs en informatique quantique de la région parisienne. C'est une fédération de recherche associant le CNRS, l'Université Paris Diderot, l'UMPC, Telecom Paristech, le CEA, l'Institut d'Optique et l'Université Paris-Sud (Orsay/Saclay).

PQC : Post Quantum Cryptography, cryptographie résistante aux algorithmes conçus pour les ordinateurs quantiques. Elle repose sur l'usage de clés publiques qui ne sont pas décomposables avec des ordinateurs classiques ou des ordinateurs quantiques. C'est lié au fait qu'il s'agit d'un problème « NP difficile ».

PQS : Programmable Quantum Simulator, ou ordinateurs quantiques analogiques.

Pure state : se dit d'un état d'un quantum ou d'un qubit qui est défini par un vecteur de norme 1 dans la sphère de Bloch. Par opposition, un mixed state est un état combinant plusieurs états purs de quantum ou qubits. Ils s'additionnent avec des probabilités classiques dont la somme fait 1 (et pas la somme au carré comme pour la superposition d'états). Cet état est bien représenté par une matrice densité et c'est un point qui est à l'intérieur de la sphère de Bloch. En pratique, les qubits utilisés dans le calcul quantique avec des registres quantiques et des portes quantiques restent à l'état pur. Par contre, la mesure de l'état d'un qubit intriqué avec un autre qubit va transformer son état de pur en mixte. Je n'ai pas encore compris si le calcul quantique manipulait des mixed states pendant les calculs et l'application de portes quantiques à des qubits.

QFHE : Quantum Fully Homomorphic Encryption. Méthode de chiffrement quantique de l'information permettant de réaliser des traitements sur des données chiffrées.

QFT : Quantum Fourier Transform. Variation quantique de la transformée de Fourier. La transformée de Fourier classique permet de décomposer un signal (comme en audio) en fréquences (ou spectre de fréquences). La QFT fait cela sur une suite de nombres entiers et détermine sa plus grande fréquence observable.

QIP : Quantum Information Processing, appellation parfois utilisée pour décrire le calcul quantique.

QKD : Quantum Key Distribution, protocole de sécurisation d'envoi de clés symétriques via une liaison optique qui s'appuie sur l'intrication quantique (fibre ou satellite). Ces clés sont inviolables ou tout du moins, une interception de la clé est détectable. Malgré tout, il existe des failles qui se situent aux extrémités de la connexion et aussi au niveau des répéteurs qu'il faut utiliser si les liaisons sont longues de plusieurs centaines de km.

QMA : Quentin Merlin Arthur, classe de problèmes qui est vérifiable en temps polynomial sur un ordinateur quantique avec une probabilité supérieure aux 2/3. C'est l'analogue quantique de la classe de complexité "traditionnelle" NP. QML : Quantum Machine Learning. Branche des algorithmes quantique qui sert au machine learning.

QRNG : Quantum Random Number Generator, les générateurs de nombres aléatoires optiques utilisés en cryptographie quantique, comme ceux du Suisse IDF.

Quantum Variational Circuits : type d'algorithme quantique servant à faire du machine learning.

Quantum Physical Unclonable Functions (QPUF) : identifieurs physiques d'objets de nature quantique et inclonables.

Quasi-particules : phénomène correspondant au comportement de particules élémentaires interagissant avec leur environnement. C'est le cas d'électrons circulant dans des semiconducteurs et dont le mouvement est perturbé par leur interaction avec les autres électrons et noyaux de la structure. Ils se comportent comme des électrons ayant une masse différente. En pratique, les quasiparticules sont des modèles mathématiques permettant de décrire de manière simplifiée le fonctionnement de particules élémentaires dans des structures solides. On les retrouve dans les anyons et les ordinateurs quantiques topologiques.

Qubit ou **qubit physique** : unité d'information élémentaire de l'informatique quantique dans les ordinateurs quantiques. Elle stocke un état quantique associant deux états distincts d'une particule ou d'un système quantique à base de plusieurs particules (spin d'électron, état superconducteur d'un groupe d'électron, niveau d'énergie d'un atome ou d'un ion piégé, polarisation ou autre propriété d'un photon). Sa représentation mathématique est un vecteur comprenant deux nombres complexes.

Qubit logique : assemblage de qubits physiques mettant en oeuvre un dispositif matériel ou logiciel de correction d'erreur.Vu du développeur de logiciel, il présente le comportement d'un qubit physique dont la fidélité serait meilleure que celle de ces derniers. La fidélité des qubits logiques dépend notamment du nombre de qubits physiques qu'ils contiennent, de la qualité des codes de correction d'erreur et de la stabilité de la fidélité avec l'augmentation du nombre de qubits.

Qudit : est une forme générique de qubit qui a d états quantiques possibles au lieu de deux. L'approche est rarement utilisée, en tout cas dans des ordinateurs quantiques hors des laboratoires de recherche.

Qutrit : c'est une forme de qubit qui au lieu d'avoir deux états quantiques possibles, en a trois. C'est un cas particulier des qudits.

Rabi (oscillation) : oscillations entre états d'un système à deux niveaux excité à une fréquence proche de sa résonance. Ce phénomène est observé entre deux états de spin dans la résonance magnétique nucléaire ainsi que lorsqu'un champ électrique agit sur les transitions d'un état électronique d'un système à un autre pour un atome ou

une molécule. La courbe décrivant l'oscillation ressemble à une sinusoïdale qui s'atténue dans le temps. Isidor Isaac Rabi est un physicien américain d'origine hongroise (1898-1988) prix Nobel de physique en 1944. On retrouve les oscillations de Rabi un peu partout et notamment dans le fonctionnement des qubits supraconducteurs.

Recuit quantique : procédé de calcul quantique utilisé dans les ordinateurs quantiques de D-Wave. Voir hamiltonien et D-Wave.

Réduction d'état : conséquence de la mesure de l'état d'un quantum ou d'un qubit, qui modifie cet état (superposé) en un état stable (non superposé). Pour un qubit, c'est l'un des deux états de base : excité ou non excité, phase horizontale ou verticale pour un photon, spin haut ou bas pour un électron, état excité pour un ion ou un atome froid, etc.

Réfrigérateur à dilution : nom donné aux cryostats de la plupart des ordinateurs quantiques qui sont utilisés pour refroidir la puce de calcul quantique à moins de 20 mK. La dilution est liée au fait que ces systèmes utilisent un mix de deux isotopes de l'hélium : le 3 et le 4, qui sont dilués l'un dans l'autre dans la boucle de réfrigération, les deux isotopes ayant des propriétés légèrement différentes. Un cryostat à l'hélium 4 ne descend qu'à 4K, un cryostat à l'hélium 3 descend à 300mK tandis qu'un cryostat utilisant les deux descend jusqu'à 10 mK. A noter que la variante la plus courante est le réfrigérateur à dilution « à sec » par opposition à « humide ». Cette version utilise une moins grande quantité d'hélium et laisse plus de place dans le « chandelier » pour y caser l'appareillage électronique et quantique.

Registre : ensemble de bits ou de qubits.

Réseaux euclidiens : classe d'algorithmes utilisés dans la cryptographie post-quantique (PQC).

Reservoir computing : catégorie spécifique de réseaux de neurones récurrents servant à traiter des séries temporelles (langage, finance, énergie, robo-tique). Leur particularité est d'utiliser des poids de neurones et des liaisons entre neurones fixés aléatoirement dans les réservoirs, le tout avec des fonctions d'activation non-linéaires de ces liaisons.

Reservoir engineering : ensemble de techniques de gestion des qubits qui passe par leur interaction avec un « bain thermique quantique» (quantum bath) pour réduire la consommation énergétique, réduire la durée de la mesure de l'état du qubit et permettre une mesure non destructive et réversible de cet état (« Quantum non-demolition" ou QND).

Rigetti : startup US créant des ordinateurs quantiques supraconducteurs.

RSA : système de chiffrement à clés publiques s'appuyant sur la difficulté à factoriser une clé publique constituée à partir de la multiplication de deux nombres premiers de très grande taille. Cette factorisation est possible avec l'algorithme quantique de Peter Shor. Cependant, elle nécessite un très grand nombre de qubits pour casser les clés RSA les plus courantes à 1024 ou 2048 bits. Pour les clés 2048 bits, il faudrait disposer aux dernières nouvelles de 20 millions de qubits avec une fidélité de plus de 99,9% que l'on n'obtient pas encore aujourd'hui.

Rydberg (atomes) : état excité d'un atome possédant un ou plusieurs électrons et dont le nombre quantique principal n (indice de la couche d'électrons dans l'atome qui est un entier compris entre 1 et le nombre de couches d'électrons dans l'atome) est très élevé. Ces atomes sont généralement de grande taille, proportionnelle à n^2, et avec des interactions inter-atomiques très fortes. Ces interactions permettent l'intrication de sous-ensembles atomiques voire d'atomes uniques. Ces atomes ont été utilisés par l'équipe de Serge Haroche pour détecter de manière non destructive la présence d'un photon dans une cavité, et ainsi étudier la décohérence quantique. Mais l'hydrogène peut aussi être un atome de Rydberg s'il est excité avec de hauts niveaux d'énergie, faisant passer son électron à une couche quantique de nombre élevé.

SAT : classe de problème de logique ou problème de satisfaisabilité booléenne, de logique d'ordre 0. C'est un problème de décision, qui, étant donné une formule de logique propositionnelle, détermine s'il existe une assignation des variables propositionnelles qui rend la formule vraie. Comme lorsque l'on cherche des variables booléennes x, y et z qui satisfont l'équation $(x \vee y \vee z) \wedge (\bar{\mathbf{x}} \vee \bar{\mathbf{y}}) \wedge (\bar{\mathbf{x}} \vee y \vee z)$, $\wedge$ voulant dire « et », et $\vee$ « ou » et $\bar{\mathbf{x}}$ étant la négation de x. Le problème devient très complexe si le nombre N de variable devient très élevé car pour tester leur combinatoire avec la force brute, il faudra tester 2^N combinaisons. Ce problème a été mis en lumière par le théorème de Cook selon lequel le problème SAT est NP-complet. Le problème SAT a aussi de nombreuses applications notamment en satisfaction de contraintes, planification classique, vérification de modèles, diagnostic, jusqu'au configurateur d'un PC ou de son système d'exploitation : on se ramène à des formules propositionnelles et on utilise un solveur SAT (Wikipedia et ici).

Schrödinger (équation, fonction d'onde) : décrit l'évolution dans le temps et l'espace de l'état ondulatoire d'un quantum, à savoir les probabilités de trouver le quantum à un endroit donné et moment donné dans le temps.

Seconde révolution quantique : couvre les avancées dans la mécanique quantique depuis les années 1990, où l'on a commencé à contrôler les propriétés quantiques de quantums individuels, au niveau de photons (polarisation, …), d'électrons (spin) et d'atomes. Elle couvre notamment les usages du quantique en cryptographie et télécommunications. L'appellation a été créée simultanément en 2003 par Alain Aspect, Jonathan Dowling et Gerard Milburn.

Shor (algorithme) : algorithme de factorisation quantique de nombres entiers inventé par Peter Shor en 1994. Il permettrait en théorie de casser des clés publiques RSA en les décomposant en nombres premiers.

Silicium 28 : isotope de silicium permettant de créer des wafers de silicium adaptés à la création de qubits en silicium. Le silicium 28 a un spin nul qui n'influe pas sur le spin des électrons piégés servant à gérer les qubits. Il est purifié en Russie et peut être ensuite déposé en couche mince en phase gazeuse sur du silicium classique.

Simulateur quantique : nom donné aux ordinateurs quantiques analogiques qui sont capables de simuler la mécanique quantique et de résoudre des problèmes associés, en particulier dans la physique des matériaux. Par abus de langage, l'appellation est utilisée pour les supercalculateurs capables d'exécuter par simulation numérique des algorithmes quantiques. Dans ce cas, il est préférable d'utiliser l'appellation d'émulateur quantique.

SIRTEQ : réseau de chercheurs en technologies quantiques, veut dire Science et Ingénierie en Région Ile de France pour les Technologies Quantiques. Il regroupe plus de 100 équipes de chercheurs et 728 chercheurs répartis dans 32 laboratoires. Il couvre les quatre pans habituels du quantique : calcul, simulation, télécommunications/cryptographie et métrologie.

SPAM : State Preparation And Measurement, soit préparation d'état et mesure, une suite d'opération après laquelle on mesure la fidélité de qubits. Cette fidélité traduit celle d'une séquence d'initialisation, de l'application de portes quantiques unitaires et de la mesure de l'état d'un qubit.

Spectre électromagnétique : ensemble des rayonnements électromagnétiques allant des plus grandes ondes radio jusqu'aux rayons X et gamma. La lumière visible n'est qu'une toute petite partie située au milieu de ce spectre.

Sphère de Bloch : modèle de représentation géométrique de l'état d'un qubit utilisant des coordonnées polaires avec deux angles, l'un indiquant l'amplitude du quantum et l'autre sa phase. Permet d'incarner la dualité onde-particule des objets quantiques servant à créer les qubits.

Spin : état d'une particule décrivant sa rotation sur elle-même ou un moment magnétique. S'applique aux électrons, aux neutrons et aux atomes. Le spin de particules composites est l'addition du spin de ses composantes. Un proton et un neutron ont un spin de ½. Un électron a un spin de +1/2 ou -1/2.

Spintronique : ensemble des technologies qui s'appuient sur la manipulation du spin des électrons. On la retrouve dans les memristors ainsi que dans les disques durs utilisant la magnétorésistance géante (GMR en anglais). Cette dernière a été découverte par Albert Fert (France) et Peter Grünberg (Allemagne) indépendamment et la même année, en 1988. Cela leur a permis d'obtenir le Prix Nobel de physique en 2007.

SQUID : Superconducting Quantum Interference Device, un magnétomètre qui mesure le sens du courant dans un qubit supraconducteur. Il est notamment utilisé par D-Wave.

Stabilizer gates : portes quantiques qui sont utilisées dans des systèmes de correction d'erreur : CNOT, H (Hadamard) et P (phase).

State vector : vecteur d'état représentant un état pur d'un quantum et d'un qubit. On le retrouve sous la forme d'un vecteur de norme 1 dans la sphère de Bloch qui matérialise physiquement l'état d'un qubit en état superposé.

Stationary qubits : qubits stationnaires (ou statiques), qui ne bougent pas dans un circuit. C'est le cas des qubits supraconducteurs, à base d'ions piégés, de spin d'électron et dérivés. S'opposent aux flying qubits qui se déplacent, comme les photons.

Superdense coding : l'encodage superdense coding est utilisé pour envoyer deux bits sur un qubit transmis par voie optique entre deux points lorsqu'ils sont déjà reliés par une paire de photons intriqués. C'est un protocole de communication imaginé par Charles Bennett et Stephen Weisner en 1992 et expérimenté en 1996 par Klaus Mattle, Harald Weinfurter, Paul Kwiat et Anton Zeilinger. L'intrication initiale précédant l'envoi des deux bits dans le qubits permet d'éviter de violer le théorème d'Holevo selon lequel un jeu de qubits ne peut pas transporter plus d'information que le nombre équivalent de bits classiques.

Superposition : propriété de quantum et des qubits d'être capable d'être dans plusieurs états en même temps. Un peu comme si la matière vibrait à très haute fréquence. Cela s'explique par la nature ondulatoire de la matière à l'échelle nanoscopique.

Supraconductivité : capacité de la matière à permettre de conduire l'électricité sans résistance. Elle se manifeste généralement à basse température. Les qubits de certains types, notamment à base d'électrons, sont refroidis à très basse température pour permettre cet effet, soit au niveau des qubits pour les qubits supraconducteurs, soit pour les dispositifs et câbles de lecture de l'état des qubits. A noter le faux ami : en anglais, on ne dit pas supra, mais superconductivity.

Suprématie quantique : qualifie une situation où un ordinateur quantique peut réaliser un calcul qui est inaccessible aux meilleurs supercalculateurs du moment en un temps humainement raisonnable. Le différentiel de temps de calcul entre le calcul quantique et le calcul classique doit être de plusieurs ordres de grandeur ou dépasser la durée d'une vie humaine. La suprématie peut concerner un calcul utile ou pas. Ainsi, la suprématie quantique revendiquée par Google en octobre 2019 concerne-t-elle un algorithme de génération et de vérification de nombres aléatoires qui n'a pas d'intérêt pratique. Un autre débat porte sur le bien-fondé de cette appellation de supremacy qui écho au thème polémique de la « white supremacy ». L'expression a été créée par John Preskill en 2011.

SWAP : porte quantique qui interverti l'état de deux qubits.

T1 : indication du temps de cohérence de qubits, qui indique la fin de cohérence des qubits liée à une perte d'amplitude (« energy relaxation »).

T2 : indication de temps de cohérence au bout duquel intervient un déphasage, à savoir une rotation autour de l'axe z dans la sphère de Bloch de l'état des qubits.

Téléportation quantique : technique consistant à envoyer l'état d'un quantum à un autre quantum et à distance. C'est généralement réalisé avec des photons qui ont été au préalable intriqués et qui ont souvent une source commune. Cela a plein d'usages comme en cryptographie quantique (QKD) mais ne peut pas servir pour autant à transmettre de l'information classique. Le théorème de non clonage dit aussi que l'état d'un quantum téléporté disparait de la source après téléportation.

Tenseur : en algèbre multilinéaire et en géométrie différentielle, un tenseur désigne un objet très général, dont la valeur s'exprime dans un espace vectoriel. En calcul quantique, les tenseurs sont utilisés pour décrire l'état de registre de qubits. Un qubit est représenté par un vecteur de 2 nombres complexes. Un registre de N qubits est représenté par 2^N nombres complexes qui résulte du produit tensoriel de N vecteurs à 2 nombres complexes. En quelque sorte, le produit tensoriel représente l'espace combinatoire des valeurs que peut prendre une combinaison de qubits.

Topologique : le calcul quantique topologique repose sur la notion d'anyons qui sont des "quasi-particules" intégrées dans des systèmes à deux dimensions. Les anyons sont des structures physiques asymétriques et à deux dimensions dont la symétrie peut être modifiée. Cela permet d'appliquer des principes de topologie avec des ensembles de permutations successives appliquées aux couples d'anyons qui se trouvent à proximité dans des circuits. Les algorithmes associés s'appuient sur les concepts d'organisations topologiques de tresses ou de nœuds ("braids"). Il existe une équivalence algorithmique entre le calcul avec des qubits à portes universelle et les qubits topologiques.

Toffoli (porte) : aussi appelée CCNOT, est porte quantique opérant sur trois qubits qui modifie la valeur du troisième qubit si celle des deux premiers est à 1.

UHV : Ultra High Vacuum, l'ultra-vide qui est nécessaire pour faire fonctionner certains types de qubits. Cela concerne surtout les atomes froids et les ions piégés. Les qubits supraconducteurs sont intégrés dans un cryostat sous vide qui n'a pas besoin d'ultra-vide.

Unconventional Computing : méthodes informatiques qui ne relèvent pas des principes de calcul classiques des machines de Turing et de Von Neuman. Couvre les outils et méthodes non traditionnels dont font partie les ordinateurs quantiques, mais pas que. Cela comprend aussi notamment les ordinateurs moléculaires et les processeurs neuromorphiques.

UMR : Unité Mixte de Recherche, laboratoire conjoint entre le CNRS et une autre entité, comme une Université, une Grande Ecole ou un autre laboratoire de recherche publique comme l'Inria ou le CEA.

UQCM : ou Universal Quantum Cloning Machine, le modèle le plus classique d'organisation et de programmation des ordinateurs quantiques à base de portes quantiques universelles.

VQE (Variational Quantum Eigensolver) : algorithme quantique hybride utilisé dans la simulation chimique créé en 2013. Son principal contributeur est Alan Aspuru-Guzik, un chercheur qui fait partie de la startup Zapata Computing.

X : porte quantique à un qubit qui inverse son amplitude, passe de $|0\rangle$ à $|1\rangle$ ou de $|1\rangle$ à $|0\rangle$ pour ce qui est des états de base.

Y : porte quantique à un qubit qui réalise une rotation de 180° autour de l'axe Y dans la sphère de Bloch.

Z : porte quantique à un qubit qui applique un changement de signe sur la composante β du vecteur du qubit, soit une inversion de phase et une rotation de 180° par rapport à l'axe Z.

ZX calculus : langage graphique utilisé pour visualiser dans la programmation quantique les notions d'intrication, la complémentarité, la causalité et leurs interactions. Il peut notamment servir au calcul par la mesure (Measurement Based Quantum Computing ou MBQC), à la création de codes de corrections d'erreurs et à l'optimisation de programmes quantiques dans des compilateurs grâce à sa théorie équationnelle et aux déformations topologiques de graphes. Ses principaux contributeurs sont des chercheurs français comme Simon Perdrix.

Historique des révisions

Cet ebook fait partie d'une série d'ouvrages avec « Les usages de l'intelligence artificielle » ou le « Guide des startups » qui se bonifie avec le temps avec des révisions successives. La première édition date de septembre 2018, la seconde de septembre 2019 et celle-ci de septembre 2020.

Cet historique permet de retrouver les principales modifications du texte d'une version à l'autre. Ce ne sont que les principales car en général, je modifie quasiment le texte de toutes les pages dans de tels ouvrages.

Version et date	Modifications
1.0 (332 pages) 29 septembre 2018	Première version du document publiée sur https://www.oezratty.net/wordpress/2018/ebook-pour-comprendre-informatique-quantique/ et consolidant 18 articles publiés entre mai et septembre 2018.
1.1 (338 pages) 4 novembre 2018	Ajouts des startups Bleximo, GTN, Intelline, LakeDiamond et Qindom, des travaux d'Urmila Mahadev sur l'explicabilité des algorithmes quantiques, de l'annonce de l'ERC Synergy Grant de 14M€ aux équipes de Grenoble autour de Maud Vinet du CEA-Leti et de diverses autres actualités scientifiques.
1.1 (342 pages) 7 novembre 2018	Ajout des détails de la première tranche du Flagship Européen et du dernier plan quantique du gouvernement allemand.
1.2 (342 pages) 10 novembre 2018	Ajout de quelques détails au sujet du plan scientifique de l'INRIA.
1.3 (342 pages) 25 novembre 2018	Ajout de la startup Quantum Machines.
2.0 (504 pages) 20 septembre 2019	Intégration de la version haute résolution des illustrations. Ajout d'Emmy Noether dans les créateurs de la physique quantique, de Chien Shiung Wu dans les physiciens de l'informatique quantique et d'un grand nombre d'autres scientifiques dans le panorama historique du quantique. Plus un topo sur le démon de Maxwell. Ajout d'une rubrique sur les supraconducteurs et sur la superfluidité et d'informations au sujet des transistors supraconducteurs pour supercalculateurs. Modification de l'organisation du document sur les parties ordinateur quantique et acteurs du marché. Nouvelle grande partie détaillée sur la métrologie quantique. Nouvelle explication de la représentation de l'état des quantums et de la sphère de Bloch. Notion de qudits et de qutrits. Plus de détails sur la suprématie quantique, l'avantage quantique et sur l'émulation quantique sur supercalculateurs. Compléments sur la cryogénie et sur la mémoire quantique. Nouvelle rubrique sur les algorithmes hybrides, sur la certification des algorithmes quantiques et sur la mise au point de logiciels quantiques et aussi sur la téléportation de qubits. Ajout de NEEXP dans les classes de complexité quantiques.

2.0 (suite)	Ajout du blind computing et du chiffrement homomorphe quantique. Ajout du MBQC (dans les classes d'ordinateurs quantiques) et du ZX calculus (méthode de programmation). Ajout de eQASM dans les outils de développement. Le point sur IBM Q System One. Ajout de MemComputing. Ajout du projet européen Mos-quito. Ajout de startups dans le calcul quantique : Mentai.ai, Pasqal, Stratum.ai, A*Quantum, Ankh.1, AppliedQubit, Automatski, Boxcat, D SLit Technologies, Elyah, Equal1.labs, JoS Quantum, Ketita Labs, Kiutra, Labber Quantum, M-Labs, Multiverse Computing, NetraMark, Nu Quantum, PhaseCraft, Plassys Bestek, QEYnet, Qirithm, Quantastica, QuantiCor Security, Quantopo, Quantum Factory, Quantum Impenetrable, Quantum Xchange, QuBalt, Qubit Reset, QuDot, Quix, QuLab, QunaSys, Rahko, Shyn, SoftwareQ, Solid State AI, SpeQtral, Universal Quantum, Xofia, ZY4. Graphe de répartition par pays et dans le temps des startups quantiques. Ajout de CryptoNext, Crypto Quantique, Ravel Technologies et VeriQloud dans les startups de la cryptographie quantique. Ajout de la Pologne dans les pays de l'Europe du quantique. Cartographie des laboratoires de recherche quantiques en France. Nouvelles fumisteries quantiques dont le premier scam quantique financier, QuantumAI, et sur le management quantique. Création d'un glossaire et d'une bibliographie.
3.0 (682 pages) 7 septembre 2020	Ajout d'un topo sur les équations de Maxwell, sur la fonction d'onde de Schrödinger, au sujet de Paul Dirac et de la mécanique quantique relativiste et de ses implications dans la chimie quantique relativiste et dans la physique des particules, au sujet de Wolfgang Pauli et de la découverte du spin de l'électron. Ajout de Hendrik Antoon Lorentz et Linus Pauling dans les précurseurs. Nouvelle rubrique sur la recherche en général et ses codes. Ajout d'Andrea Morello, Andrew Dzurak, Christophe Salomon, David Wineland, Fabio Sciarrino, Patrice Bertet, Sébastien Tanzilli et Virginia d'Auria dans les chercheurs en physique ainsi que de Dorit Aharonov et Zaki Leghtas dans les chercheurs en algorithmie. Explications détaillées du fonctionnement des masers et des lasers et leurs liens avec la physique quantique. Une nouvelle partie sur les polaritons et une autre, Extreme quantum, sur les autres théories de la physique quantique, notamment la théorie quantique des champs et les différentes théories d'unification de la physique. Je tranche sans trancher le débat sur « la quantique » ou « le quantique ». Compléments sur l'algèbre linéaire : nablas, laplaciens, déterminants, permanents, et les notions de non-linéarités utilisées dans les technologies quantiques. Nouvelle rédaction et nombreux compléments sur les jeux de portes quantiques universels (groupe de Clifford, théorème de Solovay-Kitaev), les codes de correction d'erreurs, sur l'ingénierie de la cryogénie, sur les composants électroniques des calculateurs quantiques ainsi que sur le measurement based quantum computing. Nouveau schéma d'explication de l'algorithme de téléportation. Ajout d'une rubrique sur les offres de cloud quantique, intégrant celles d'Amazon et de Microsoft. Approfondissement scientifique et révision complète de toutes les parties sur les technologies de qubits et les acteurs du marché correspondants. Compléments au sujet d'IBM et de leur volume quantique ainsi que sur Google et leur suprématie quantique.

3.0 (suite)	Regroupement des technologies alternatives au calcul quantique dans un chapitre dédié, avec Fujitsu, MemComputing, Hawai, sur les ordinateurs supraconducteurs, le calcul réversible et adiabatique, les processeurs statistiques et les supercalculateurs. Ajout de startups dans le calcul quantique et technologies habilitantes : Alice&Bob, AIQTech, Atlantic Microwave, Avanetix, Azur Light Systems, BardeenQ Labs, ClassiQ, Groovenauts, Jji, Juano, Kelvin Technology, Low Noise Factory, Lumibird, Marki Microwave, ODE L3C, MyCryoFirm, Nord Quantique, ORCA Computing, OTILumionics, Oxford Ionics, Opacity, ParityQC, Photonic, QuantFi, Quantum Microwave, Qsimulate, Quantopticon, Quantum Mads, Quantum Thought, Quantumz.io, Qubit Engineering, QuEra, Qontrol Systems, ReactiveQ, RQuanTech, Semicyber, Scontel, SHYN, SolidState.AI, Spin Quantum Tech, StrangeWorks, Super.tech, Terra Quantum, Toptica Photonics, Tradeteq, Zurich Instruments et Zyvex Labs. Plus de détails sur les startups Kiutra et SeeQC ainsi que Plassys Bestek. Ajout de startups dans les télécommunications et la sécurité : Agnostiq, CAIlabs, Crypto4A Technologies, Fragmentix, HaQuien, Infotecs, MtPellerin, NuCrypt, PQSHield, PQSecure Technologies, Qrate, QuantLR, Quantum Base, Quantropi, QuSecure, Smarts, XT Quantech. Ajout d'entreprises dans la métrologie : Aquark Technologies, CryoLock, Entanglement Technologies, FieldLine Inc, Great Lakes Crystal Technologies, HyperLight Corp, iXblue, Lucigem, Nomad Atomics, Nvision Imaging, Orolia, Qubic, QuSpin, Q-Sensorix, Rydberg Technologies, SBQuantum, Seedevices, Southwest Sciences, Stable Laser Systems, Supracon, Syrlinks, TMD, Twinleaf, Vapor Cell Technologies, VectorAtomic et Vescent Photonics. Mise à jour de la partie sur la métrologie avec ajout de NEMS/MEMS et de la mesure de radiofréquences. Topo sur le Quantum Hype Cycle et l'hiver quantique. Mises à jour sur les investissements dans les technologies quantiques dans le monde avec en particulier : USA (dont des détails sur le rôle du NIST), Chine, Canada, UK, Allemagne, Israël, Allemagne, Pays Bas, Australie, Japon et Singapour. Ajout de la Suède, de l'Inde et de Taiwan. Nouvelles rubriques sur l'influence de la science-fiction et sur la philosophie de la physique quantique. Ajouts divers sur les fausses sciences du quantique. Mise à jour et structuration de la bibliographie. Compléments dans le glossaire : nombre 137, Arxiv, cavités Fabry-Pérot, chandeliers, DFT, électrodynamique quantique, émulateur quantique, concatenated codes, ERC, hydrodynamique quantique, permanents, espaces de Fock, polaritons, QPUF, réfrigérateurs quantiques, reservoir computing, reservoir engineering, SPAM, spintronique, SWAP, T1, T2, UHV, unconventional Computing, portes (de Pauli) X, Y et Z.
3.1 (682 pages) 16 septembre 2020	Quelques compléments sur l'algèbre linéaire. Ajout d'informations sur l'annonce de la roadmap détaillée d'IBM publiée le 15 septembre 2020 par Jay Gambetta, sur celle de 4 qubits silicium intriqués réalisés par TU Delft également en septembre 2020.
3.2 (682 pages) 22 septembre 2020	Corrections au sujet de la sphère de Bloch, ajout de la notion de phase globale et du fait que alpha peut être complexe. Modification des schémas associés.

3.3 (682 pages) 1ier octobre 2020	Mention de l'étonnant recrutement de John Martinis par la startup SQC en Australie. Mise à jour dans l'inventaire des laboratoires de recherche français avec le LPENS qui a digéré le LPA début 2019.
3.4 (682 pages) 3 octobre 2020	Ajout dans les qubits à ions piégés de l'annonce d'IonQ sur l'ordinateur quantique le plus puissant du monde (du jour) avec 32 qubits de très bonne qualité. Ajout de l'annonce de la génération Advantage de calculateur à recuit quantique de D-Wave.
3.5 (682 pages) 22 novembre 2020	Corrections et mises à jour au sujet du volume quantique et de ses deux versions (2017 et 2019) dans la partie concernant IBM dans les qubits supraconducteurs. Ajout de LSQC dans le glossaire.
3.6 (684 pages) 24 novembre 2020	Enrichissement des schémas explicatifs des basiques de la physique quantique.
3.7 (684 pages) 28 mars 2021	Corrections sur les aspects probabilistes de la mesure quantique et quelques autres aspects des basiques de la physique quantique. Correction du schéma sur les classes de portes quantiques.
3.8 (684 pages) 5 avril 2021	Corrections diverses sur l'algèbre linéaire et autres erreurs mathématiques. Mise à jour de schémas liés à la sphère de Bloch. Corrigé le nom de David DiVincenzo (le premier n manquait à certains endroits).
3.9 (684 pages) 24 avril 2021	Corrections diverses. Harmonisation de l'usage des termes émulateurs vs simulateur quantique.
4.0 (684 pages) 1ier juillet 2021	Correction au sujet de la position du germanium dans le tableau des éléments.
4.1 (684 pages) 6 juillet 2021	Correction dans le glossaire sur le groupe des portes de Clifford et le dlog de Shor.

⟨ Aage Niels Bohr | Abner Shimony | Adi Shamir | Akira Furusawa | Alain Aspect | Alain Ravex | Alain Sarlette | Alan Aspuru-Guzik | Alastair Abbot | Albert Einstein | Alberto Bramati | Alexander Holevo | Alexander Prokhorov | Alexandre Blais | Alexandre Zagoskin | Alexei Bylinskii | Alexei Grinbaum | Alexei Kitaev | Alexia Auffèves | Alfred Kastler | Alfred Pérot | Alonzo Church | Amir Naveh | André Luiz Barbosa | Andrea Morello | Andrea Rodriguez Blanco | Andreas Wallraf | Andrew Cross | Andrew Horsley | Andrew S. Dzurak | Andrew Steane | Andrew White | Anne Canteaut | Anne Matsuura | Antoine Browaeys | Anton Zeilinger | Aram Harrow | Arieh Warshel | Arthur Holly Compton | Arthur Leonard Schawlow | Artur Ekert | Astrid Lambrecht | Audrey Bienfait | Axel Becke | Benjamin Huard | Benoît Valiron | Bettina Heim | Bob Wiens | Boris Podolsky | Brian Josephson | Bruno Desruelles | Bryce DeWitt | Carlo Rovelli | Chad Rigetti | Charles Bennett | Charles Fabry | Charles Hard Townes | Charles Hermite | Chien Shiung Wu | Christiaan Huygens | Christian Weedbrook | Christine Silberhorn | Christophe Jurczak | Christophe Solomon | Christophe Vuillot | Christopher Monroe | Christopher Papile | Claude Cohen Tannoudji | Claude Weisbuch | Clinton Davisson | Cornelis Dorsman | Cristian Calude | Cristina Escoda | Cyril Allouche | Daniel Estève | Daniel Gottesman | Dave Wecker | David Deutsch | David DiVincenzo | David Gosset | David Hilbert | David Wineland | Dennis Dieks | Dieter Zeh | Don Coppersmith | Don Misener | Dorit Aharonov | Douglas James Scalapino | Earle Hesse Kennard | Ed Sperling | Edward Farhi | Edward Fredkin | Edward Tang | Elena Calude | Eleni Diamanti | Elham Kashefi | Elisabeth Giacobino | Emanuel Knill | Emmy Noether | Enrico Fermi | Ernest Rutherford | Ernst Ising | Erwin Schrödinger | Etienne Klein | Ettore Majorana | Ewin Tang | Fabio Sciarrino | Faye Wattleton | Felix Bloch | Francesca Ferlaino | Franck Balestro | Francois Le Gall | Frédéric Grosshans | Freeman John Dyson | Friedrich Hund | Friedrich Paschen | Geordie Rose | George Uhlenbeck | Georges Paget Thomson | Georges Zweig | Georges-Olivier Reymond | Gerard Milburn | Gerrit Jan Flim | Gil Kalai | Gilles Brassard | Gilles Holst | Giorgio Frossati | Gordon Baym | Gordon Gould | Guang-Can Guo | Haig Farris | Hans Albrecht Bethe | Hantaro Nagaoka | Harald Fritzsch | Hartmut Neven | Heike Kamerlingh Onnes | Heinrich Hertz | Hélène Bouchiat | Hélène Perrin | Hendrik Anthony Kramers | Hendrik Casimir | Hendrik Lorentz | Henri Poincaré | Hermann Minkosvki | Hugh Everett | Hui Khoon Ng | Ilana Wisby | Iñigo Artundo | Iordanis Kerenidis | Issac Newton | Itamar Sivan | Jacqueline Bloch | Jacques Salomon Hadamard | Jacquiline Romero | James Chadwick | James Clerck Maxwell | Jason Alicea | Jay Gambetta | Jean Dalibard | Jean Michel Raymond | Jean-Michel Gérard | Jean-Philippe Piquemal | Jei Wei Pan | Jelena Vučković | Jelena Vucokic | Jeremy O'Brien | Johannes van der Walls | Joe O'Gorman | Johann Balmer | Johannes Pollanen | Johannes Rydberg | John Bardeen | John Clauser | John Frank Allen | John Hall | John Levy | John Martinis | John Morton | John Preskill | John Rowell | John Smolin | John Stewart Bell | John Von Neumann | John Watrous | John Wheeler | Jonathan Dowling | Jonathan Koomey | José Capmany | José David Domenech | Joseph John Thomson | Josh Nunn | Juan Cirac | Julian Schwinger | Julien Bobroff | Jürgen Mlynek | Kenneth Appel | Kenneth Regan | Kevin Young | Kirill Tolpygo | Kohei Itoh | Kristel Michielsen | Kun Huang | Kurt Gödel | Le Si Dang | Lee Smolin | Léon Brillouin | Leonard Adleman | Lester Germer | Lev Bishop | Lev Landau | Lieven Vandersypen | Linus Pauling | Llewellyn Thomas | Loïc Henriet | Louis Cauchy | Louis de Broglie | Lu Jeu Sham | Ludwig Botzmann | Luigi Frunzio | Magdalena Hauser | Marcus Doherty | Marcus Huber | Marie-Anne Bouchiat | Martin Karplus | Masahide Sasaki | Masahiro Kitagawa | Masahito Hayashi | Mathieu Munsch | Matthew Hutchings | Matthias Troyer | Matthieu Desjardins | Maud Vinet | Max Born | Max Planck | Maxime Richard | Mazyar Mirrahimi | Michael Ben-Or | Michael Frank | Michael Freedman | Michael Horne | Michael Levitt | Michael Nielsen | Michel Brune | Michel Devoret | Michelle Simmons | Mikhail Dyakonov | Mikhail Lukin | Mio Murao | Murray Gell-Mann | Nathan Gemelke | Nathan Rosen | Nathanaël Cottet | Niccolo Somaschi | Nick Farina | Nicolas Gaude | Nicolas Gisin | Nicolas Roch | Niels Henrik Abel | Nikolay Basov | Nir Minerbi | Nobuyuki Imoto | Oleg Mukhanov | Olivier Carnal | Pascale Senellart | Pascual Jordan | Pascual Muñoz | Patrice Bertet | Paul Benioff | Paul Dirac | Paul Hiriart | Perola Milman | Pete Shadbolt | Peter Higgs | Peter Knight | Peter Leek | Peter Shor | Peter Zoller | Philipp Lenard | Philippe Duluc | Philippe Grangier | Pierre Hohenberg | Pierre Rouchon | Pieter Zeeman | Pranav Gokhale | Pyotr Kapitsa | Qingfeng Wang | Rainer Blatt | Raphaël Lescanne | Raymond Laflamme | Rebecca Krauthamer | René Descartes | Richard Feynman | Richard Holt | Richard Karp | Richard Murray | Rob Schoelkopf | Rob Whitney | Robert Andrews Milikan | Robert Dennard | Robert König | Robert McDermott | Robert Rausseendorf | Robin Blume-Kohout | Roland Gähler | Roman Lutsiv | Ron Rivest | Ryan Babbush | Samuel Goudsmit | Sara Ducci | Sarah Sheldon | Satyendranath Bose | Scott Aaronson | Sébastien Tanzilli | Serge Haroche | Sergey Bravyi | Seth Lloyd | Shengtao Wang | Shi Yaoyun | Silvano de Franceschi | Simon Benjamin | Simon Perdrix | Sophia Economou | Stefanie Barz | Stephanie Wehner | Steve Lamoreaux | Tauqir Abdullah | Terry Rudolph | Théau Peronnin | Theodor Hänsch | Theodore Lyman | Theodore Maiman | Thibault Jacqmin | Thierry Lahaye | Thomas Monz | Thomas Young | Tommaso Callarco | Tommaso Toffoli | Tracy Northrup | Travis Humble | Tristan Meunier | Umesh Virkumar Vazirani | Valerian Giesz | Vasilis Armaos | Vincent Bouchiat | Virginia D'Auria | Vlad Anisimov | Vladan Vuletic | Vladimir Fock | Walter Brattain | Walter Kohn | Walther Meissner | Walther Nernst | Wassim Estephan | Werner Heisenberg | William Rowan Hamilton | William Shockley | William Wootters | Willis Eugene Lamb | Winfried Hensinger | Wojciech Zurek | Wolfgang Haken | Wolfgang Lechner | Wolfgang Paul | Wolfgang Pauli | Xavier Waintal | Yakov Frenkel | Yann Allain | Yasuhiko Arakawa | Yasunobu Nakamura | Yasuobu Nakamura | Yehuda Naveh | Yoshihisa Yamamoto | Yuichiro Minato | Yuri Alexeev | Yuri Manin | Zaki Leghtas ⟩