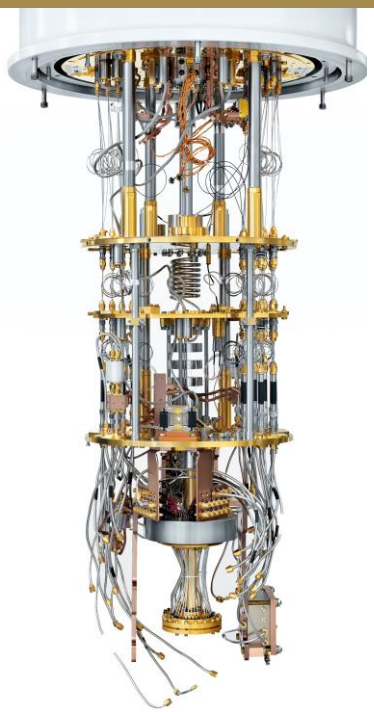
KUREK Michel

michel.kurek@neuf.fr

Mars 2021



TECHNOLOGIES QUANTIQUES
VERS LA SECONDE REVOLUTION

Mots clés : Ordinateur quantique, Communication quantique, Capteurs, Qubit, Superposition, Intrication

Executive summary

Centenaire, la physique quantique a permis des inventions majeures tels le laser ou le transistor, élément de base de nos ordinateurs et smartphones et, par conséquent, de notre civilisation de l'information et de la télécommunication. Désormais, une seconde révolution est en cours, celle de l'information quantique dont l'unité n'est plus le bit mais le bit quantique - dit qubit.

Le monde quantique est un univers particulier, celui des particules atomiques et subatomiques, où règnent les probabilités et les concepts de superposition, de non-clonage et d'intrigante intrication. Les progrès parallèles et continus de la recherche et de la technologie ont permis de valider et d'exploiter ces phénomènes, et de développer notre capacité à manipuler des objets quantiques individuels (atomes, électrons, photons) pour y stocker, traiter et lire des qubits.

Ces progrès ont conduit à l'émergence d'une nouvelle génération d'appareils, dont certains, déjà commercialisés, pourraient révolutionner des domaines aussi variés que la métrologie, les télécommunications et l'informatique, tant ils surpasseraient les performances des technologies existantes.

En métrologie, l'extrême sensibilité des objets quantiques aux influences externes les rend idéaux pour la réalisation de mesures de grandeurs physiques à haute précision, mais certains dispositifs devront être miniaturisés.

Les télécommunications cryptées sont dès aujourd'hui sous la menace d'un futur ordinateur quantique dont la puissance de calcul exponentielle pourrait casser les cryptosystèmes actuellement utilisés, mais l'intrication et l'impossibilité de cloner les qubits apporteraient une solution quantique… à la menace quantique

Enfin, en exploitant les superposition et intrication de qubits, les ordinateurs quantiques pourraient effectuer des calculs totalement inaccessibles aux supercalculateurs classiques, ce qui profiterait à de nombreuses industries (chimie, énergie, transport…). Cependant, les qubits actuels sont trop bruités et les erreurs de calculs trop nombreuses. Des protocoles de correction sont proposés mais ils nécessiteront l'intégration d'un grand nombre de qubits de meilleure qualité si bien que les ressources nécessaires pour les mettre en place vont bien au-delà des capacités de la technologie existante. En attendant, des solutions matérielles et algorithmiques, adaptables à la situation actuelle, sont explorées pour démontrer un réel *avantage quantique* sur un cas d'usage pratique.

Page de couverture : Les puces d'ordinateurs quantiques doivent être encapsulées dans un environnement cryogénique (Photo/Justin Fantl, Rigetti Computing)

Contents

Préambule

L'objectif de ce document est de dresser un état de l'art des nouvelles technologies quantiques potentiellement disruptives pour de nombreux secteurs économiques. Son ambition est d'éveiller l'intérêt, et nourrir la curiosité de ses lecteurs sur un sujet d'actualité de prime abord complexe. Sur le fond et la forme, j'ai voulu un discours clair étayé de nombreuses références (~200) et illustrations(~110).

Sa conception est le résultat d'un parcours initiatique de 6 mois qui m'a permis d'être en contact avec un certain nombre de praticiens du domaine, scientifiques (Eleni Diamanti, Pascale Senellart, Alexia Auffèves, Elham Kashefi, Bruno Fedrici, Christophe Jurzcak -VC), industriels (Philippe Duluc -ATOS, Elvira Shishena -TOTAL), fondateurs de startups (Pasqal, Cryptonext, Alice& Bob), consultants (Jean-François Bobier -BCG, Olivier Ezratty -aussi auteur de l'excellent ebook[144]), tous membres d'un écosystème en pleine effervescence.

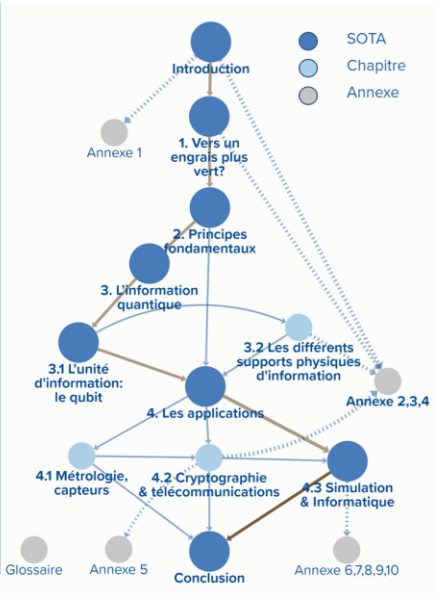
J'ai eu la chance de débuter ma démarche avant le confinement en assistant à quelques séminaires: à la Cité des Sciences ou chez BPI... Ce fut l'occasion d'y rencontrer physiquement quelques-unes des personnes citées.

Mon chemin fut ensuite marqué par la rédaction d'un rapport bilingue de 50 pages, synthétisant mon étude détaillée des paysages des brevets, publications et investissements dans le quantique. Cette étape d'analyse était, selon moi, un préalable indispensable à la rédaction du corpus principal du SOTA. Au final, ce travail m'a permis de m'immerger dans l'écosystème du quantique, en publiant, avec l'accord de Nicolas Mottis, et sous le mentoring du Lab Quantique et de QuantX (Alumni Polytechnique), le « Rapport Kurek ». A ce jour, les publications *medium* et *linkedin* mentionnant ce rapport cumulent plus de 10 000 vues. Point d'orgue, j'ai eu le plaisir de le présenter le 13 octobre dernier lors d'un meetup organisé par le Lab Quantique devant la « communauté quantique » internationale.

C'est après avoir assisté à plus de 20 webinars organisés par différents acteurs de la scène quantique: IBM, Microsoft, Le Lab Quantique, Digital Week et, analysé près de 500 références (publications scientifiques, livres, articles de presse, sites web), que je me suis lancé dans la rédaction du document principal. Au final, le document est dense, et je vous propose une sélection de quelques chapitres traitant de **l'informatique quantique** comme éléments de mon SOTA. Les autres technologies quantiques ont été couvertes à parts égales (physique des qubits, applications dans les domaines de la métrologie, des télécommunications) afin de proposer une vision globale dans une seconde lecture. Pour ce faire, chacune des parties peut être lue indépendamment, même si certaines informations se capitalisent tout au long du document.

Chapitre	SOTA	Le réaliste	Le geek	philosophe	Le pressé	Le fan
Introduction (2p)	✓	✓	✓	✓	✓	✓
1. Vers un engrais plus vert ? (3p)	✓	✓	✓	✓	✓	✓
2. Principes fondamentaux (4p)	✓	✓	✓	✓		✓
3. L'information quantique (0p)	✓	+	+			✓
3.1 L'unité d'information: le qubit (4p)	✓	+	+			✓
3.2 Supports physiques du qubit (11p)	+	+	+			✓
4. Les applications (2p)	✓	✓	✓	✓		✓
4.1 Métrologie, capteurs (10p)	+	✓	+			✓
4.2 Cryptographie & communications (18p)	+	✓	✓			✓
4.3 Simulation & Informatique (32p)	✓	✓	✓			✓
Conclusion (3p)	✓	✓	✓	✓	✓	✓
Annexe 1 (4p)	+	✓				✓
Annexe 2, 3 ,4 (57p)	+	✓				✓
Annexe 5 (3p)	+	✓	✓			✓
Annexe 6, 7, 8, 9, 10 (19p)	+	✓	✓			✓
Glossaire	+	+	+	+		+

\+ Optionnel



Introduction

La physique quantique traite du comportement des objets physiques au niveau microscopique (molécules, atomes, électrons, photons…). Elle est l'une des théories les plus fructueuses en termes de compréhension de notre Univers. Son développement initial pendant la première moitié du XX^{ème} siècle a été par ailleurs une aventure humaine et scientifique des plus extraordinaires[1].

Initiée en 1900 par Planck sous le nom de théorie des quantas, c'est principalement au cours des années 1920[1] que Bohr, Schrödinger, Heisenberg, de Broglie, Einstein et une poignée d'autres physiciens[2] mirent sur pied cette nouvelle théorie dotée de règles et d'un formalisme mathématique particuliers après avoir constaté que les lois de la physique classique peinaient à décrire le comportement des particules. Cette théorie s'est avérée efficace pour cerner les phénomènes à l'œuvre à l'échelle corpusculaire.

Loin des lois classiques, la physique quantique repose sur quelques concepts parfois peu intuitifs : le principe de **quantification** (les grandeurs physiques, telle l'énergie, ne sont pas de nature continue et ne peuvent prendre qu'un ensemble de valeurs discrètes appelées « *quanta* »), les principes de **dualité onde-corpuscule, d'indétermination,** de **superposition** et d'**intrication** qui laissent une place prépondérante aux probabilités, pour ne citer que les principaux.

Cette physique a non seulement, complètement modifié notre conception du monde en nous permettant de comprendre certaines propriétés de la matière, de la lumière et de leurs interactions, mais aussi révolutionné nos vies quotidiennes au XXème siècle. Le principe des quanta est, à titre d'exemple, à l'origine de nombre d'applications technologiques : horloge atomique, GPS[3], RMN et IRM[4], LASER[5], semi-conducteurs[6]. Ces derniers sont au cœur des outils issus des technologies de l'information et de la communication, autant dire de notre société.

Mais l'histoire ne s'arrête pas là. Depuis 1960, les progrès parallèles et continus de la recherche[7] et de la technologie[8] (souvent récompensés par l'attribution de prix Nobel[9]) ont permis de valider et d'exploiter les principes de superposition et d'intrication, d'appréhender de nouveaux phénomènes, et de développer notre capacité à **manipuler des objets quantiques individuels** (atomes, ions, électrons, photons) **pour y stocker, traiter et mesurer de l'information**.

Si cette capacité de contrôle des systèmes quantiques individuels fut l'objet même du prix Nobel de Serge Haroche en 2012, elle ressortait déjà remarquablement des expériences menées en 1980-82 par Alain Aspect qui réussit à établir un résultat irréfutable conduisant à la validation du phénomène d'intrication grâce à des paires de photons convenablement préparés, alors même que les lasers ne pouvaient mettre en action que des milliards de milliards de telles particules.

---

[1] ANNEXE 1 (Figure 2): Chronologie des travaux marquants sur la première moitié du XX^{ème} siècle.

[2] ANNEXE 1 (Figure 1): Photo du congrès SOLVAY (Bruxelles, 1927) réunissant plusieurs physiciens à l'origine de la physique quantique.

[3] La précision des GPS (Global Positioning System) est liée à leurs synchronisations régulières sur des horloges atomiques pour déterminer la position des sondes spatiales en mesurant le temps qu'un signal envoyé met pour faire un aller-retour. Créées dès les années 1960, les **horloges atomiques** utilisent un phénomène quantique, l'immuabilité des fréquences de transitions d'états de certains atomes (Cesium 133)[2].

[4] La spectroscopie RMN (résonance magnétique nucléaire) consiste à soumettre un corps chimique à une onde électromagnétique variable et à un champ magnétique constant. À une fréquence particulière (résonance), certains noyaux du corps chimique vont être le siège d'une transition énergétique qui peut être détectée par une sonde. L'imagerie par résonance magnétique (IRM) est une application de la RMN dans le domaine du diagnostic médical (Wikipedia).

[5] Les lasers, développés à partir des années 1960, utilisent le principe de quantification de la matière (dans les atomes, les électrons se répartissent sur des niveaux discrets d'énergie, le passage entre les niveaux se fait par absorption et émission de photons).

[6] La compréhension des matériaux conducteurs, semi-conducteurs et isolants, est de nature quantique. Diodes, transistors, cellules photovoltaïques, circuits intégrés sont issus des propriétés quantiques des matériaux semi-conducteurs.

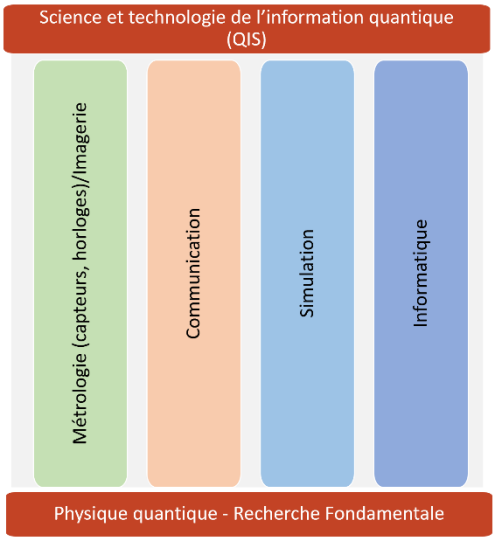
[7] ANNEXE 3 : Etude scientométrique des publications en physique quantique

[8] ANNEXE 2 : Etude du paysage des brevets issus de la recherche en Physique Quantique.

[9] ANNEXE 1 : Tableau et statistiques des Prix Nobel de Physique.

Il est aujourd'hui légitime de penser que depuis le début du XXI^{ème} siècle, nous entamons une **deuxième révolution technologique quantique liée à l'information** et initiée par le pivot entre la recherche fondamentale et l'industrialisation des technologies de manipulation et de contrôle des objets quantiques individuels, technologies qui n'avaient pu être exploitées lors de la 1ère révolution.

Cette seconde révolution se cristallise autour de quatre domaines d'application : la métrologie, les communications, la simulation et l'informatique. Dans leurs déclinaisons quantiques, ces technologies sont loin d'être matures, même si elles utilisent des outils éprouvés issus de la 1ère révolution tels que les lasers. Cependant, comme l'explique Clayton Christensen[3], la maturité n'est pas nécessaire pour imposer une innovation si celle-ci apporte déjà un avantage compétitif décisif. A ce titre les bénéfices potentiels de ces technologies sont importants puisqu'elles devraient nous permettre d'augmenter de manière exponentielle nos puissances de calcul, de sécuriser nos communications et de mesurer des grandeurs physiques avec des précisions sans précédent, ce qui pourrait être disruptif pour un grand nombre de marchés finaux, de la recherche pharmaceutique aux télécommunications en passant par la cybersécurité.



Dans ce cadre, il n'est pas étonnant de constater l'intérêt grandissant aussi bien de la part des industriels que des gouvernements pour qui ces technologies sont à la fois des enjeux, des perturbateurs et des arbitres des équilibres stratégiques[10].

L'objectif de cette étude est de dresser un panorama sous forme d'état de l'art des technologies de la seconde révolution quantique en y présentant les principes, les mises en œuvre, les challenges et les verrous potentiels.

Nous commençons par introduire dans le premier chapitre un exemple concret d'application des nouvelles technologies quantiques au monde de la chimie. Le chapitre suivant expose les principes de base de la physique quantique communs aux différents domaines, puis nous abordons dans la troisième partie les supports physiques principalement utilisés dans la mise en œuvre des technologies quantiques, objets de la quatrième partie.

Si cette ultime section conclut le corpus principal de notre analyse, nous invitons les lecteurs, qui le souhaitent, à prendre connaissances des différentes annexes, en particulier les annexes 2, 3 et 4, synthèses d'un travail de recherche sur les paysages des publications, des brevets et des investissements privés et publics dans ces domaines.

[10] ANNEXE 4 : Paysage mondial des investissements publics et privés

1. Vers un engrais plus vert

Cela s'agite du côté des corpuscules. Depuis 2015, le nombre d'articles académiques traitant d'avancées dans le domaine des technologies quantiques est en croissance annuelle moyenne de 10%/an[11] tandis que celui des brevets augmente fortement de 27%/an[12].

Au cours de ces dernières années, plusieurs nations ont lancé des plans d'investissements conséquents pour le développement des technologies quantiques[13]. Le secteur privé n'est pas en reste avec la création de centaines de startups et des investissements importants d'une dizaine de géants de l'IT[13]. En octobre 2019, Google annonce dans un article de la revue Nature [4] avoir atteint la « suprématie quantique »[14] avec son **processeur quantique Sycamore** et fait immédiatement réagir IBM[15].

Pendant la rédaction même de ce document, plusieurs revues scientifiques[16] grand public ou généralistes[17] ont publié des numéros spéciaux ou articles de fond sur le sujet. Ainsi, le hors-série de la revue *Pour la science* de mai 2020, titrait-il: "*La nouvelle révolution quantique…va changer notre monde* !" (Figure 1), faisant références aux nouvelles technologies quantiques.

Comment pourraient-elle changer le monde ? Pour esquisser un début de réponse, nous avons choisi un exemple tiré du domaine de la chimie industrielle, le procédé **Haber-Bosch**.

Pourquoi la Chimie ? Parce que ce secteur pourrait bien être un des premiers champs d'application[7] des technologies quantiques grâce, en particulier, aux ordinateurs et simulateurs quantiques potentiellement capables d'aider à la compréhension des propriétés des molécules et de simuler des réactions chimiques. Le secteur de la chimie n'est pas une exception, bien d'autres secteurs et cas d'usages potentiels seront mentionnés par la suite …après tout, nous parlons de Révolution.

L'azote est nécessaire à la vie et au développement de tous les êtres vivants et en particulier des plantes, car il entre dans la composition des acides nucléiques, des protéines, etc. Le procédé Haber-Bosch, mis au point au tout début du XXème siècle, permet de fixer l'azote atmosphérique sous forme d'ammoniac, lequel permet à son tour la synthèse de différents explosifs et engrais azotés. A ce titre, il est probablement le plus important procédé industriel jamais mis au point durant le siècle dernier[8] puisque

Figure 1: Pour la science, HS N°107

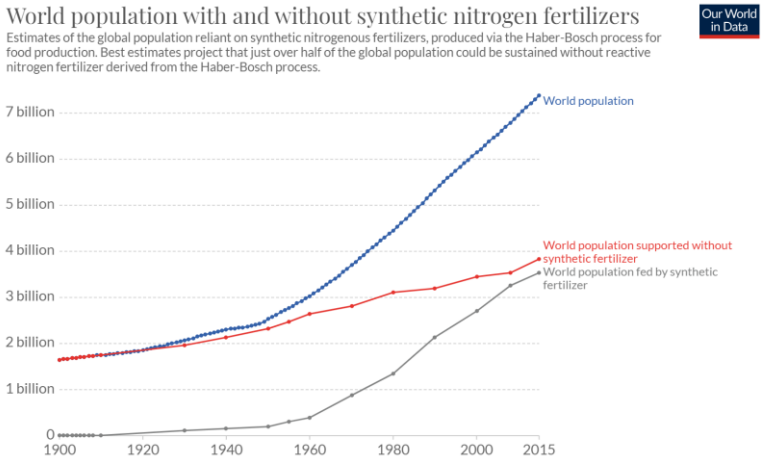


*Figure 2: Part de la population nourrie grâce aux engrais azotés (Source: **https://ourworldindata.org/how-many-people-does-synthetic-fertilizer-feed**)*

[11] ANNEXE 3 : Etude scientométrique des publications en physique quantique.
[12] ANNEXE 2 : Etude du paysage des brevets issus de la recherche en physique quantique.
[13] ANNEXE 4 : Paysage mondial des investissements publics et privés.
[14] John Preskil propose en 2012 dans [5] le terme "suprématie quantique" pour décrire le point où un ordinateur quantique pourraient résoudre un problème, quel qu'il soit, que les ordinateurs classiques ne pourraient pas résoudre.
[15] IBM :*"Because the original meaning of the term - quantum supremacy -, as proposed by John Preskill in 2012, was to describe the point where quantum computers can do things that classical computers can't, this threshold has not been met."*[6]
[16] Par ex. « Pour la Science », « La nouvelle révolution quantique…va changer notre monde ! » Hors-Série 107, mai 2020.
[17] Revue l'éléphant N°31, Juillet 2020 https://lelephant-larevue.fr/thematiques/ce-que-va-changer-lordinateur-quantique/

les engrais synthétiques permettent de nos jours de nourrir la moitié des huit milliards d'habitants de la Terre (voir [9] et figure 2)

Pour fonctionner la transformation Haber-Bosch du diazote (N_2) en ammoniac (NH_3) nécessite beaucoup d'hydrogène et une catalyse à température et pression élevée (~500°C, 100 bars voir figure 3). Elle est largement tributaire de l'utilisation de combustibles fossiles. Ainsi, est-elle réputée consommer 2% de l'énergie mondiale[10] et contribuer significativement aux émissions de gaz à effet de serre en libérant 1,44% du CO_2 mondial[11].

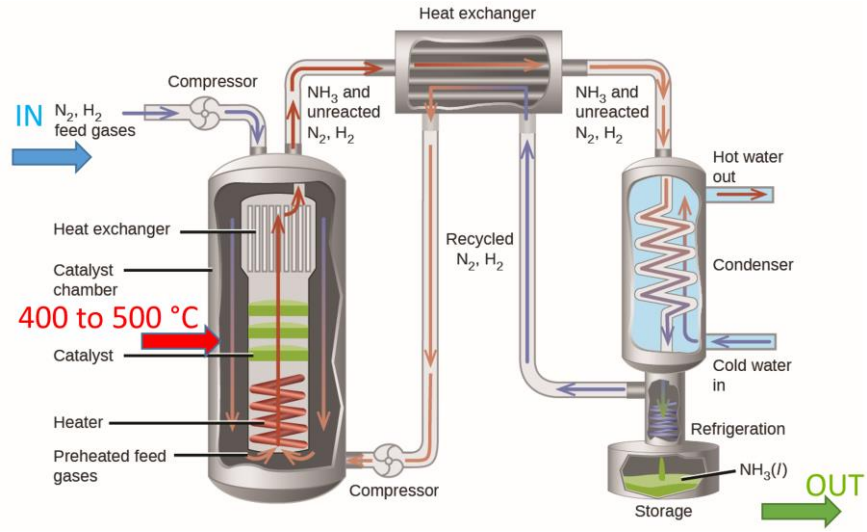


Figure 3: Schéma du procédé Haber-Bosch (Source: https://www.inspirationchemistry.com)

Pourtant un processus équivalent de fixation de l'azote existe dans la nature dans des conditions de température et de pression normales (Figure 4). Utilisé par certaines plantes, il met en action des bactéries contenant un complexe enzymatique[18], **la nitrogénase**, capable de catalyser la transformation de l'azote en ion ammonium NH_4^+, assimilable par les plantes (Figure 5).

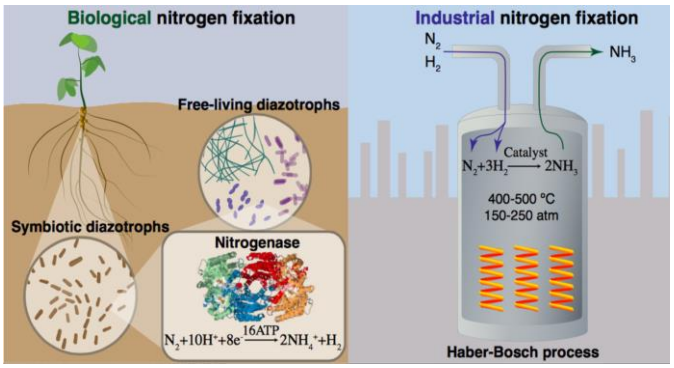


Figure 4: Processus biologique et industriel de fixation de l'azote

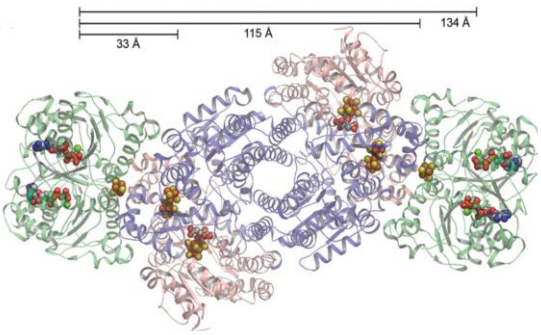


Figure 5: Complexe nitrogénase

Ce processus naturel est mystérieux. Il est certes lent, mais pouvoir l'imiter prodiguerait d'énormes bénéfices environnementaux. Il serait alors possible de créer des engrais synthétiques « verts ».

Une solution serait de modéliser grâce à un simulateur numérique classique (supercalculateur ou HPC[19]) le site actif de la nitrogénase, appelé FeMoco (Fe_7MoS_9C), qui dans la nature interagit avec l'azote. Malheureusement, ces ordinateurs ne sont pas assez puissants pour ce type de problèmes. En effet, la

[18] Une enzyme est une protéine dotée de propriétés catalytiques accélérant ou orientant une réaction chimique dans un sens. Les enzymes peuvent agir seules ou regroupées en complexe.

[19] HPC : *High-performance computing* désigne les ordinateurs à haute performance utilisés pour du calcul intensif.

simulation du comportement d'une molécule dépend d'équations de la physique quantique certes connues, mais dont la résolution devient rapidement trop complexe, lorsque la molécule comporte trop d'atomes interagissant les uns avec les autres (on parle de problèmes à N corps).

De tels cas sont illustrés sur la figure 6. La modélisation d'une molécule de caféine ($C_8H_{10}N_3O_2$) nécessiterait 10^{48} bits (à valeur « 0 » ou « 1 » classique) mais seulement 160 « bits quantiques » (ou qubits[20]), celle d'une molécule de pénicilline 10^{86} bits (soit plus que le nombre d'atomes dans l'univers[21]) mais seulement 286 qubits.

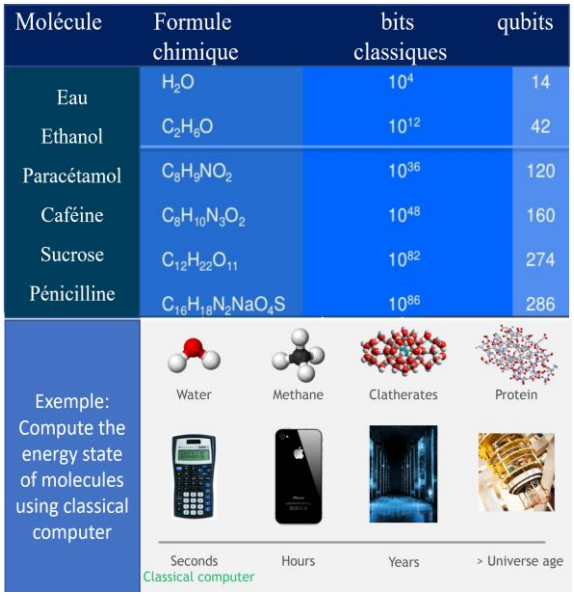


Figure 6: Comparaison du nombre de bits et qubits pour modéliser des molécules et du temps de calcul d'état énergétique (Source: d'après IBM, BCG)

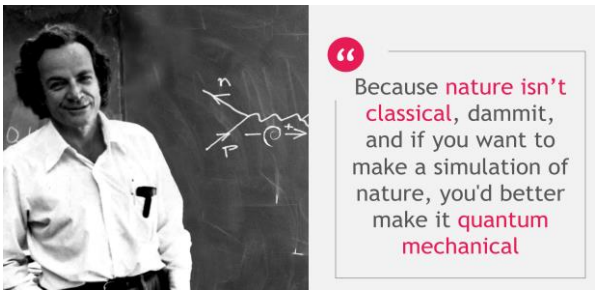
Le temps nécessaire pour calculer l'état énergétique d'une protéine serait supérieur à l'âge de l'univers tandis que la modélisation utilisant un simulateur quantique, à la puissance de calcul exponentielle dont nous parlerons ultérieurement, serait par contre totalement envisageable.

Dans une étude publiée fin août 2020 dans la revue Science[12], l'équipe de Google AI Quantum a cherché à accélérer les techniques actuelles de simulation de la chimie quantique. Les chercheurs ont utilisé quelques-uns des 53 qubits de Sycamore, pour effectuer la plus grande simulation chimique réalisée sur un ordinateur quantique à ce jour en modélisant l'isomérisation du diimide (composé inorganique : H_2N_2) et les énergies de liaison de chaînes d'atomes d'hydrogène. Ces simulations sont encore en retrait de ce qui est réalisable sur des serveurs HPC. Cependant, le CEO de la compagnie estime que la résolution par un ordinateur quantique, du défi posé par le procédé Haber Bosch, sera possible d'ici une décennie [13].

Cette démonstration récente de Google, même modeste, ainsi que l'optimisation hypothétique de la fabrication des engrais agricoles, exposée dans ce chapitre, ne sont que des exemples parmi tant d'autres des apports possibles des technologies quantiques. Ces dernières portent en elles-mêmes la promesse du dépassement des limites technologiques courantes. L'idée n'est pas nouvelle, car dès 1981, Richard Feynman avait formulé ces termes mémorables:

« La nature n'est pas classique, bon sang, et si vous voulez simuler la nature, il faudra bien utiliser la mécanique quantique, et je vous assure que c'est un problème merveilleux, car il a l'air loin d'être simple »[14].

Malgré la complexité sous-jacente, certains principes de la mécanique quantique peuvent s'appréhender simplement. C'est l'objet du chapitre suivant. Les lecteurs familiers avec le sujet, ou ceux, désireux d'aborder directement la partie applicative et l'état de l'art de différents cas d'usage, pourront s'y référer ultérieurement.



[20] Unité d'information quantique que nous détaillerons dans la section 3.1.
[21] Ce qui ne signifie pas grand-chose mais permet de marquer les esprits.

2. Principes fondamentaux de la physique quantique : quelques clés

La théorie de la physique quantique fournit un formalisme mathématique permettant de décrire le comportement du monde physique à très petite échelle, celle des corpuscules: électrons, atomes neutres ou ionisés[22], photons[23]. Au-delà du modèle mathématique, les comportements observés ont permis de définir un certain nombre de principes physiques dont nous avons extrait une liste de concepts clés qui seront repris par la suite, notamment lors de la description du fonctionnement des qubits et de leurs diverses techniques de mise en œuvre[24].

2.1. La quantification

L'observation des systèmes physiques à l'échelle atomique ou subatomique montre que les grandeurs physiques aussi appelées observables[25] (énergie, champs de force, quantité de mouvement) ne sont pas des valeurs continues mais discrètes. Un quantum représente alors la plus petite mesure indivisible d'une quantité physique. Les effets de la quantification les plus connus sont la polarisation linéaire des photons (horizontale / verticale), ainsi que les spins[26] et niveaux d'énergie des électrons au sein des atomes. Pour rappel, l'énergie d'un électron ne peut prendre que certaines valeurs bien précises si bien que si l'on imaginait un électron monter/descendre en énergie comme il gravirait/descendrait un escalier, il passerait brusquement d'une marche à l'autre sans pouvoir s'arrêter au milieu.

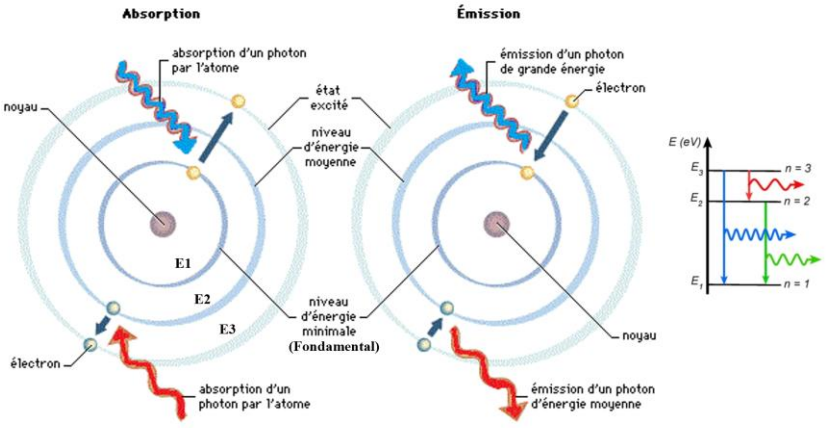


Figure 7: Niveaux d'énergie discret d'un atome, absorption et émission de photons (Source: d'après http://light.physics.auth.gr/enc/wavelength_en.html)

La figure 7 (gauche) présente les cas d'électrons absorbant l'énergie de photons de différentes longueurs d'ondes (donc d'énergie) et changeant d'orbite. L'énergie d'une lumière monochromatique bleue (fournie par exemple par un laser) est supérieure à celle d'une lumière rouge ce qui induit un changement supérieur du niveau d'énergie dans l'atome (E1→E3). Inversement, pour retomber à un niveau énergétique inférieur, l'électron libère son surplus d'énergie sous la forme d'un photon (Figure 7 - droite). Ce phénomène d'émission lumineuse postérieure à une excitation est à l'origine de la phosphorescence

[22] Chargés électriquement par excès (ion négatif) ou absence (ion positif) d'un ou plusieurs électrons.
[23] Sans que cela ne se limite à ces entités puisque la taille maximale des objets quantiques est toujours un sujet de recherche
[24] Le lecteur familier avec le sujet ou désireux d'aborder la partie applicative pourra se rendre directement au chapitre 3 et revenir, si besoin, sur ces principes fondamentaux. Il pourra aussi se référer au glossaire proposé en annexe 11.
[25] Dans le vocabulaire de la physique quantique.
[26] Le spin est une propriété interne d'une particule tout comme la masse ou la charge électrique. Il peut être schématiquement lié au moment cinétique (ou angulaire) et magnétique de la particule et être orienté vers le haut ou vers le bas.

et de la fluorescence de la matière. Nous verrons que le phénomène de fluorescence est utilisé pour mesurer l'état quantique de particules dans certaines technologies quantiques (e.g. ions piégés).

2.2. La dualité onde-corpuscule

Un objet quantique possédant à la fois des propriétés de particule (vitesse, position) et d'onde (fréquence, amplitude, phase) est à ce titre susceptible d'interférer comme une onde classique. L'expérience des fentes de Young (Figure 8) est une des manipulations[27] illustrant cette propriété propre aux phénomènes ondulatoires.

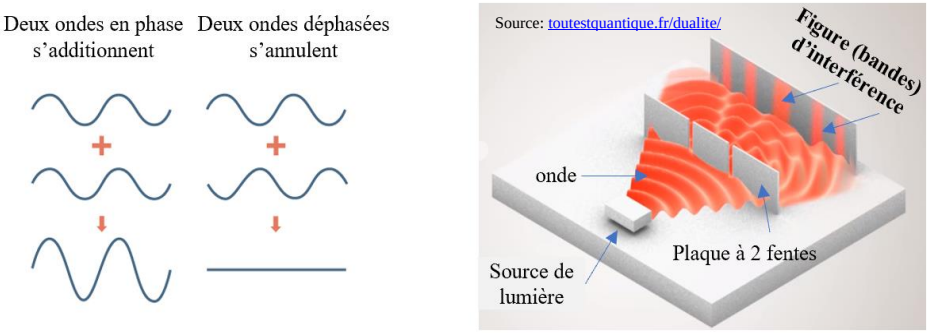


Figure 8: Expérience des fentes de Young à partir d'une source lumineuse (photons) (Source: toutestquantique.fr/dualite)

Une onde lumineuse passant à travers deux fines fentes verticales se divise en deux ondes qui, suivant des chemins différents, se déphasent et interfèrent pour former, sur un écran placé en aval, une figure d'interférence constituée d'une alternance de bandes verticales brillantes et sombres correspondant respectivement aux interférences constructives (addition) et destructives (soustraction)[28]. Dans une expérience complémentaire, la même figure d'interférence se reconstruit progressivement lorsque les photons sont envoyés un par un successivement en très grand nombre.

Des bandes d'interférence identiques s'observent si l'on remplace les photons par des électrons[15], des atomes ou même des molécules de grandes tailles, inorganiques ou organiques comme l'ont prouvé des expériences récentes portant sur le fullerène composé de 70 atomes de carbone[16], des molécules de 58 et 114 atomes[17], ou encore des molécules organiques de polypeptides constitués de 15 acides aminés[29] [18].

Les photons peuvent aussi se comporter comme des particules. Ainsi, lorsqu'ils atteignent un atome, ils peuvent lui transmettre un moment cinétique comme s'ils avaient une masse. Ce phénomène permet par exemple de ralentir des atomes ou même depuis peu des molécules [19] en mouvement, ce qui revient à limiter leur agitation et à les refroidir (température record obtenue de 50nK[20]). Au final, ce sont toutes ces observations qui ont permis de valider la complémentarité onde/corpuscule.

2.3. Le principe d'indétermination de Heisenberg

Selon cette relation fondamentale énoncée en 1927 par Heisenberg [21], il est impossible de connaître simultanément la position et la vitesse d'un objet quantique ou de tout autre couple de grandeurs complémentaires de celui-ci. De manière plus générale, l'acquisition d'information sur une grandeur quantique implique nécessairement la perte d'information sur d'autres. Ce principe, en rupture avec la physique classique remplace la notion de trajectoire par une probabilité de présence d'un objet quantique. Tout objet quantique possède donc une **fonction d'onde** calculée à l'aide de l'équation de Schrödinger. Mathématiquement la fonction d'onde correspond à une amplitude de probabilité et permet

[27] Nous rencontrerons aussi plus loin l'interféromètre optique de Mach-Zehnder
[28] Le contrôle des interférences quantiques est à la base de puissant algorithmes d'informatique quantique
[29] N.D.A. : L'ADN serait-il quantique …?

de calculer la probabilité de trouver la particule à une position donnée. Lorsqu'une mesure est effectuée sur l'objet, la fonction d'onde s'effondre et la mesure sera cohérente avec la densité de probabilité préalablement définie par la fonction d'onde.

2.4. La superposition

Un système quantique peut exister dans plusieurs états à la fois, appelé superposition d'états. La fonction d'onde pour un tel état de superposition peut être décrite comme une combinaison linéaire des fonctions d'ondes des états contributeurs, avec des coefficients complexes[30] (α et β dans le cas de la figure 9). Ces coefficients décrivent l'amplitude de probabilité (la somme de leur module au carré doit valoir 1) et les phases relatives entre les états de base. Notons que bien plus grandes que des corpuscules, des molécules composées de 2000 atomes ont pu aussi être mises en état de superposition l'an dernier[22].

Figure 9:Illustration du concept de superposition à partir d'une pièce[31]. Une pièce a en principe deux états possibles au repos (pile noté |0⟩ ou face |1⟩) alors que, dans un jeu de pile ou face quantique, elle peut tout aussi bien être simultanément sur le côté pile et face (imaginer une pièce en rotation sur sa tranche)

Le principe de superposition est particulièrement puissant. Il est au centre des développements actuels dans les domaines des communications et de l'informatique quantique où il **permet de paralléliser les calculs** et permettrait un gain de temps exponentiel dans la résolution de certains problèmes par rapport à l'informatique classique. Attention cependant, l'état de superposition est aussi fragile car sensible aux interactions indésirées.

2.5. La cohérence quantique

La cohérence est la capacité qu'a un système quantique à conserver dans le temps un état quantique comme la superposition. De petites interactions du système, par nature très sensible, avec son environnement peut provoquer sa décohérence (la destruction de son état quantique). Un objet macro, comme l'illustre l'expérience du chat de Schrödinger[32] n'est pas quantique car il *décohére* au contact de l'extérieur. La cohérence est nécessaire pour que les phénomènes quantiques tels que l'interférence, la superposition et l'intrication soient possibles. Formellement, c'est lorsque l'état d'un système quantique peut être décrit comme une combinaison linéaire d'états de base du système que l'on parle d'état cohérent. **Allonger le temps de cohérence quantique est la problématique majeure** dans de nombreuses applications des technologies quantiques**,** en particulier **pour l'informatique quantique.**

[30] Dans le cadre du calcul quantique, le fait que les coefficients (poids) soient complexes est fondamental car les algorithmes quantiques (suite de portes logiques quantiques) visent à créer des interférences entre du positif et du négatif (interférences constructives et destructives) et ainsi progressivement placer dans une superposition tout le poids sur l'état qui est solution du problème en utilisant beaucoup moins d'opérations qu'un processeur conventionnel.

[31] Edition spéciale d'une pièce de 10 Euros éditée en 2008 en Allemagne pour les 150 ans de la naissance de Max Planck (précurseur de la théorie des quanta suite à son étude du rayonnement du corps noir).

[32] Expérience de pensée proposée en 1935 par Erwin Schrödinger qui voulait illustrer les paradoxes de la physique quantique à l'échelle humaine. Un chat, être vivant macroscopique, se trouvait néanmoins soumis aux étranges principes du monde microscopique de la physique quantique. Au final, le chat n'est pas un objet quantique et le paradoxe est levé.

2.6. La mesure

Nous pouvons connaitre de manière objective le monde qui nous entoure en le mesurant mais toute mesure d'une observable d'un système quantique le change fondamentalement. **La mesure réduit l'information probabiliste à un état classique bien défini**. Le système est laissé dans un état correspondant à la valeur mesurée. Ceci est communément appelé « effondrement de la fonction d'onde » ou « réduction du paquet d'onde ».

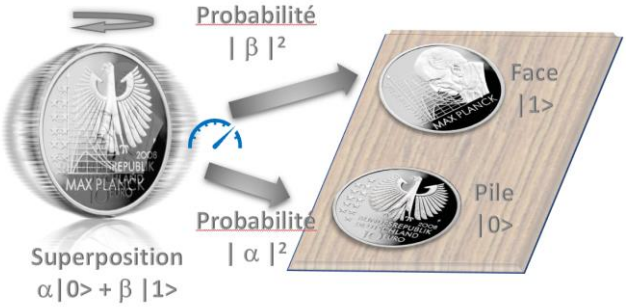


Figure 10: La mesure détruit l'état quantique et donne un résultat qui est associé à sa probabilité d'apparaître

Connexe au principe d'indétermination de Heisenberg et celui de la mesure, le théorème de **non-clonage**[23] est un résultat de la physique quantique qui interdit la copie à l'identique d'un état quantique inconnu et arbitraire. Il est fondamental dans le cadre des technologies de communications sécurisées.

2.7. L'intrication

Il n'existe pas d'équivalent en physique classique mais ce concept n'est pas sans rappeler celui de corrélation probabiliste. L'intrication correspond à la situation où les états quantiques de plusieurs objets quantiques dépendent instantanément les uns des autres même si les objets sont très éloignés entre eux. Cette intrication peut résulter d'un phénomène naturel (collision) ou d'une manipulation humaine. Ainsi, deux objets intriqués O_1 et O_2, même séparés, ne sont pas indépendants, et $\{O_1+O_2\}$ doit être considéré comme un système unique. Par exemple, une modification d'état sur l'un des objets, comme celle induite par une mesure, entraine un changement chez l'autre de manière immédiate. Formellement cela s'exprime par le fait que la fonction d'onde du système constitué par les objets intriqués ne peut pas s'écrire comme le produit mathématique des fonctions d'onde de chacun des objets. L'intrication permet de communiquer, d'échanger de l'information, de manière sécurisée, et à distance. Elle joue aussi un rôle majeur en informatique quantique.

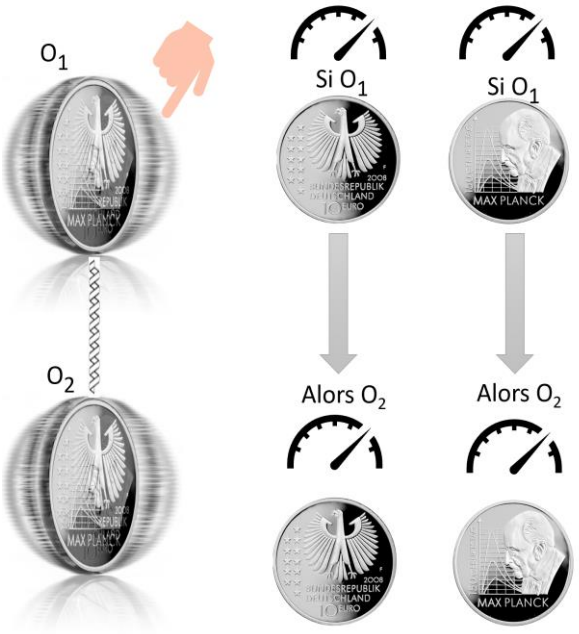


Figure 11: L'intrication : deux objets intriqués O_1 et O_2 ne sont pas indépendants même séparés

Il n'est pas de notre propos ici d'exposer tous les phénomènes et lois de la physique quantique. Nous retiendrons que le probabilisme y a remplacé le déterminisme de la physique classique, que les premiers principes énoncés dans cette section (quanta, dualité, indétermination) ont conduit à la première révolution quantique, et permis de comprendre des effets et des propriétés remarquables de la matière ou de la lumière (effets photoélectrique, laser, tunnel, supraconduction, RMN…). Par la suite, la vérification expérimentale des concepts de superposition et d'intrication, associée depuis la fin du XXème siècle aux progrès techniques qui permettent d'utiliser les corpuscules quantiques comme support d'information, conduisent à la seconde révolution en introduisant un changement de paradigme dans notre capacité à traiter de l'information[33]. Nous pouvons la préparer, la stocker, la manipuler et la véhiculer dans des objets quantiques. C'est l'objet du chapitre suivant.

[33] Au sens de la théorie de l'information de Shannon https://fr.wikipedia.org/wiki/Théorie_de_l'information

3. L'information quantique : bit quantique et support physique

L'objectif de cette section est double, d'abord introduire la notion de qubit qui représente la plus petite unité de stockage d'information quantique, puis dresser un inventaire sous forme d'état de l'art des dispositifs physiques permettant de la manipuler.

3.1. L'unité d'information : le qubit

La brique élémentaire d'information du monde numérique classique est le bit qui peut prendre deux valeurs : 0 ou 1. Dans l'informatique traditionnelle cela correspond généralement à la création, au traitement et à la mesure d'une charge électrique (0 Volt/5 Volts) qui exprime le passage, possible ou pas, du courant à l'aide de transistors[34] qui possèdent ces deux états passant (1) et bloquant (0). La lecture d'un bit est déterministe à savoir que si on la répète plusieurs fois on obtiendra toujours le même résultat.

Dans la théorie de l'information quantique, l'unité de base de stockage est le **qubit**[35], qui désigne l'état quantique d'un objet physique quantique (atome, électron, photon…) ayant deux états de base possibles[36], notés généralement **|0⟩** et **|1⟩** respectivement selon la notation de Dirac **|.⟩.** Bits comme qubits peuvent être regroupés dans des ensembles nommés registres. La figure 12 liste certains des éléments de comparaison bits vs. qubits qui seront abordés dans la section suivante.

	Bits: 0 ou 1 	**Qubits : |0⟩ et |1⟩** 
Etats	2 états possibles exclusifs	2 états possibles simultanés
Initialisation	0 ou 1	Généralement |0⟩
Codage interne	Un chiffre binaire : 0 ou 1	Vecteur à deux dimensions, un nombre flottant et un nombre complexe **[α,β]**
Modification	Portes logiques*	Portes quantiques*
Lecture	0 ou 1, déterministe	0 ou 1, probabiliste
	REGISTRE DE n BITS	REGISTRE DE n QUBITS
Nombre de combinaisons codées	2^n états possibles **mais 1 seul à la fois** peut être traité par ex si n=3 : 101	2^n états possibles **simultanément,** par ex si n=3: 000,001,010 011,100,101,110,111
Traitement pour parcourir tous les états	Séquentiel: 2^n appels séquentiels	Parallèle: 1 seul appel
Lecture	n bits	n bits : à la lecture d'un qubit, on ne récupère que 0 ou 1 et donc une seule combinaison des 0 et 1 des qubits du registre

* Dans la terminologie propre à l'informatique classique ou des ordinateurs à circuit quantique, mais traitement équivalent en métrologie

Figure 12: Quelques éléments de comparaison entre bits classiques et qubits

3.1.1. Propriétés quantique du qubit

La représentation des qubits nous permet de retrouver les principes fondamentaux de la physique quantique exposés dans la section précédente :

[34] Le nombre de transistors dans les processeurs actuels est de l'ordre du milliard, e.g. l'EPYC Rome Zen2 du fabricant AMD, gravé en 7nm a près de 40 milliards de transistors (Source: https://www.tomshardware.fr/)

[35] L'appellation qubit, pour « **qu**antum **bit** », est apparue en 1995 dans un article de Benjamin Schumacher publié dans la revue Physical Review A (réf : [24]).

[36] Au-delà des 2 états possibles d'un qubit, des plateformes quantiques peuvent aussi être construites à partir de **qutrits** (3 états quantiques possibles), de **ququarts** (4 états) et plus génériquement, de **qudits** (avec *d* états quantiques possibles). Ces alternatives ne sont pas courantes pour l'instant même si théoriquement individuellement plus puissantes qu'un qubit.

- La superposition (§2.4) permet à un qubit d'encoder plusieurs informations en parallèle, l'état du qubit est une combinaison linéaire des états $|0\rangle$ et $|1\rangle$ (dans une proportion définie par deux nombres et une représentation mathématique et géométrique dont nous parlerons ensuite). **C'est la superposition des états codés qui apporte la puissance de représentation et de traitement de l'information quantique**. Un registre de 2 qubits permet de représenter ou traiter l'équivalent de 4 bits, 3 qubits l'équivalent de 8 bits, n qubits équivalent à 2^n bits[37]. Ainsi, un registre quantique de 10 qubits peut traiter simultanément $2^{10} = 1024$ états, et en corollaire, rajouter 10 qubits multiplie la performance d'un facteur 1000, qui équivaut à 15 ans d'évolution de machines conventionnelles selon la loi de Moore[38].

  Pour être encore plus concret, la séquence du génome humain contient au minimum 1,5 Gb de données soit environ 2^{34} bits, de sorte que 34 qubits suffiraient pour contenir une représentation de la séquence complète[26]. Un corps humain entier de 100 milliards de cellules, pourrait contenir 150 zétaoctets, soit environ 2^{80} bits, donc 80 qubits suffiraient. Les capacités de représentation permises par l'information quantique augmentent donc en théorie exponentiellement avec le nombre de qubits. Elles permettraient par exemple, aux processeurs quantiques, de paralléliser et d'effectuer certains types de calcul physiquement inaccessibles au plus puissant des supercalculateurs. Nous reviendrons sur ce point au §4.3 dédiée à l'informatique quantique.

- L'intrication (§2.7) permet de faire interagir différents qubits entre eux pour les synchroniser, souvent de manière contingente, mais sans pouvoir ni lire, ni modifier indépendamment, ni copier leurs contenus. Elle est mise en œuvre par différents procédés physiques (par exemple des impulsion lasers envoyées sur les qubits à intriquer) correspondant dans le domaine informatique à des portes logiques quantiques. Elle est l'outil de base utilisé dans les développements des télécommunications quantiques sécurisées et, en métrologie pour certains capteurs spécialisés. En informatique quantique, **l'intrication** permet la mise en œuvre de puissants **opérateurs logiques** (binaires).

- La dualité onde-corpuscule (§2.2) permet d'interagir avec les qubits ou de les faire interagir entre eux par interférences dans le cadre d'instruments de mesures ou d'algorithmes en informatique quantique. Exploiter des interférences de qubits est ainsi l'un des moyens de générer le résultat d'un calcul quantique en le faisant ressortir de l'ensemble des valeurs possibles, superposées dans les états d'un registre. Cette dualité onde-corpuscule explique aussi pourquoi le formalisme mathématique de la physique quantique repose sur des vecteurs qui, tout comme les ondes, peuvent s'additionner ou se soustraire, comme nous allons le voir maintenant.

3.1.2. Représentation mathématique et géométrique d'un qubit

Mathématiquement, l'état d'un qubit est une superposition linéaire de deux états $|0\rangle$ et $|1\rangle$ qui peut se représenter de différentes façons équivalentes: linéaire, vectorielle, géométrique (voir Figure 13 et par exemple le fascicule [27] pour plus de détails). La représentation vectorielle permet d'utiliser pleinement

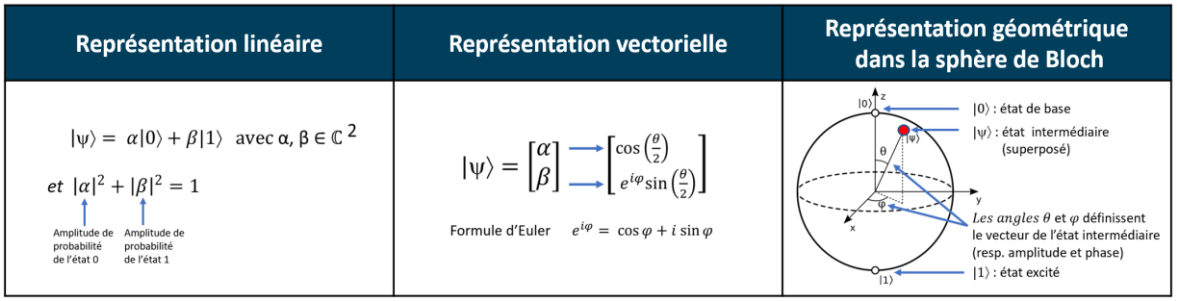


Figure 13: Différentes représentation d'un qubit

[37] Ajouter un qubit à un registre quantique double la puissance du système.
[38] En 1965, Gordon Moore (Intel) énonçait ce qu'on appelle aujourd'hui *la loi de Moore*[25] : la densité des transistors (nb de transistors/mm^2) pourrait doubler tous les 24 mois, ce qui entrainerait le doublement de la puissance de calcul des ordinateurs. Cette conjoncture s'est avérée remarquablement exacte, même si, elle a été révisée à la baisse depuis, avec un doublement tous les 18 mois (1.5 ans). La finesse de gravure des wafers a continuellement diminué mais atteindrait un seuil bas proche de la largeur de quelques atomes seulement. Le calcul pour 15 ans d'évolution de la loi de Moore donne: $2^{(15/1.5)} = 2^{10} \sim 1000$.

le formalisme mathématique de la physique quantique qui fait largement appel à **l'algèbre linéaire**[39]. L'état quantique d'un qubit se représente par un vecteur d'un espace appelé espace de Hilbert. Géométriquement, il peut être représenté par un point sur la surface d'une sphère nommée la **sphère de Bloch**, de rayon 1 (point rouge $|\psi\rangle$ en figure 13). Le pôle nord de la sphère porte généralement l'état de base $|0\rangle$ (*ground state*) et le sud l'état excité $|1\rangle$ (*excited state*). Entre les deux se trouvent une infinité de points possibles pouvant représenter chacun l'état d'un qubit. Suivant qu'il est plutôt dans l'hémisphère nord ou sud, un qubit peut être plus ou moins 0 et 1, et ceci dans une proportion qui dépend de sa latitude (angle θ). La lecture d'un qubit revient à projeter le point le représentant sur l'axe Z (nord-sud) et renvoie un nombre 0 ou 1 déterministe. . Après lecture, l'état quantique, **probabiliste**, est perdu.

De nombreuses opérations appliquées sur des qubits peuvent être décrites avec précision par cette analogie géométrique. L'annexe 6 présente différents opérateurs (portes quantiques) appliquées dans le traitement de qubits en les illustrant sur la sphère de Bloch. Les ordinateurs quantiques universels, dont nous reparlerons §4.3, utilisent des algorithmes quantiques souvent représentés par des circuits quantiques (à l'instar des circuits électroniques classiques) composés de la séquence des opérations (portes) appliquées au(x) registre(s) de qubits.

3.1.3. La gestion des erreurs des qubits (bruit et décohérence quantique)

Objets de la seconde révolution quantique, les technologies mises en œuvre pour créer un état quantique (initialiser l'information quantique), la traiter, la stocker ou la transmettre font encore l'objet de nombreuses recherches et sont contraintes par le fait qu'un état quantique est fragile, car sensible aux interactions avec son environnement. Les qubits tendent à perdre très rapidement leurs propriétés quantiques. Or, un traitement de l'information quantique n'est efficace que si la décohérence et les erreurs sont marginales.

Si la décohérence intervient avant la fin d'une communication, de l'exécution d'un algorithme ou d'une mesure physique, les résultats seront inutilisables. Nous reviendrons sur ce sujet crucial dans le chapitre consacré à l'informatique quantique (§4.3). Il convenait toutefois de le mentionner avant d'aborder la section suivante traitant des différents types de systèmes physiques aujourd'hui envisagés pour coder l'information d'un qubit. Toutes ces plateformes ne sont pas égales en termes d'erreurs et de cohérence quantique.

3.2. Différents supports physiques d'information

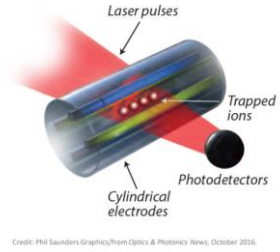
Nous avons vu précédemment que la puissance de représentation de l'information quantique tenait à la superposition, qui permet à un qubit d'encoder plusieurs informations en parallèle, à l'intrication qui fait interagir les qubits entre eux et à la dualité onde-corpuscule qui, grâce au phénomène d'interférence, permet d'effectuer des mesures précises, ou de faire converger rapidement un calcul informatique. Mais, l'information quantique est fragile par nature. Elle peut être rapidement polluée ou même disparaitre. Les qubits sont donc notoirement difficiles à créer et à entretenir, mais la recherche est très active[40] pour trouver les meilleurs solutions technologiques (temps de cohérence, sensibilité, passage à l'échelle…).

Différents supports physiques susceptibles d'héberger l'information quantique sont d'ailleurs actuellement développés en parallèle. Chacun présente des avantages et des inconvénients mais aussi des niveaux de maturité différents. La figure 15 synthétise les sept principaux types de plateformes physiques, lesquelles peuvent se regrouper en trois grandes classes suivant la nature du corpuscule utilisé pour coder le qubit: atome, électron, photon.

Parmi toutes les solutions existantes seuls les photons peuvent voyager et transporter de l'information sur de grandes distances. On les appelle les « flying qubits ». Les autres qubits sont généralement stationnaires, ou *emprisonnés* dans un espace infinitésimal. L'initialisation du qubit, l'application des portes logiques, ou la mesure s'effectuent en un lieu unique bien déterminé (i.e. le qubit est fixe). C'est une différence avec l'informatique classique où le bit est un signal électrique (5V) qui circule à travers les portes logiques (transistors), qui elles sont fixes.

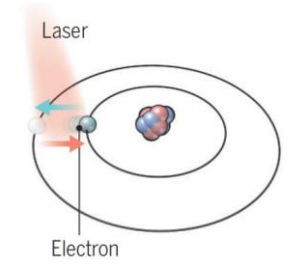
[39] Calcul matriciel, valeurs et vecteurs propres sont omniprésents.
[40] Voir nos analyses sur les publications et brevets proposée en annexe 2 & 3.

3.2.1. *Les ions piégés*



Credit: Phil Saunders Graphics/from Optics & Photonics News, October 2016.

C'est aujourd'hui l'une des deux technologies les plus avancées avec celle des supraconducteurs (§3.2.3). Elle permit de construire le premier qubit en 1995[28]. Elle utilise des ions[41] maintenus dans une cavité sous vide par un champ électrique et refroidis par laser[42]. Dans la plupart des implémentations, les ions sont alignés dans la cavité (voir la récente revue sur le sujet [29]).



From Science News Feature, "Scientists are close to building a quantum computer that can beat a conventional one" by Gabriel Popkin, Illustration by Chris Bickel/Science. Reprinted with permission from AAAS.

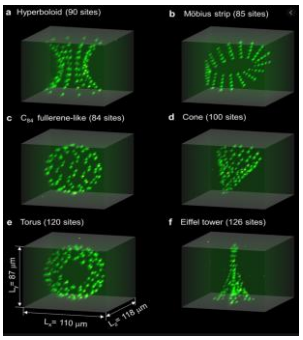
Il existe cinq grandes variantes[29] d'usage de ces ions qui dépendent des transitions énergétiques (des électrons de la bande de valence) choisies pour coder les deux états d'un qubit : qubits Zeeman, qubits à structure hyperfine, à structures fines, les qubits optiques et les qubits Rydberg[30]. À chacune de ces modalités correspondent des fréquences de transition différentes (Mhz, GHz, THz). Suivant la variante utilisée **les états quantiques sont contrôlés** et modifiés **par micro-ondes**, ou **impulsions lasers**. La lecture de l'état des qubit se fait par captation de la fluorescence des ions. D'autres caractéristiques sont détaillées dans le tableau de la figure 15.

Pour une application en informatique, les ions piégés ont un temps de cohérence assez long, de plusieurs dizaines de secondes, qui compense la lenteur des portes logiques qui leur sont appliquées[31]. Le ratio entre temps de cohérence et application d'une porte est cependant très bon (= 10^6) alors qu'il est de 10^3 pour les qubits supraconducteurs (voir §3.2.3) et d'environ 200 pour les qubits d'atomes froids (§3.2.2).

Récemment Honeywell a proposé une nouvelle architecture utilisant des ions, toujours piégés, mais sur une surface 2D (QCCD - Q*uantum Charge-Coupled Device*[32]). Ces ions peuvent être convoyés individuellement d'un point à un autre du circuit pour y recevoir un traitement, tel que la création d'un état intriqué avec un autre ion. C'est un cas rare de "*flying qubits*" qui ne soient pas des photons.

Pour terminer notre analyse, la figure 16 résume les avantages et inconvénients de cette technologie qui s'avère très intéressante car les qubits produits, bien isolés, sont de très bonne qualité mais le passage à l'échelle avec un système proposant une centaine de qubits (première taille désirée) pourrait être compliqué.

3.2.2. *Les atomes froids*



Alors que les atomes froids[42] sont utilisés depuis plusieurs années en métrologie pour mesurer par exemple la gravité par interférométrie (§4.1), c'est une technologie plus récente pour les ordinateurs quantiques avec un principe de fonctionnement qui présente de nombreuses similitudes avec la mise en œuvre des ions piégés.

Une récente étude publiée par des chercheurs de la startup française Pasqal détaille cette technologie[33]. Les atomes neutres sont retenus sous vide dans des champs magnétiques ou des réseaux optiques de faisceaux laser (pinces optiques ou *optical tweezers*).

[41] Les ions utilisés ici sont des atomes auquel on a enlevé un ou plusieurs électrons et qui sont donc chargés positivement. On privilégie les ions (calcium, béryllium, magnésium, strontium) qui ne contiennent plus qu'un seul électron sur leur couche périphérique de manière à bénéficier d'un schéma de niveaux d'énergie favorable pour lequel les techniques de refroidissement et manipulation par laser sont bien maitrisées. Les deux niveaux d'énergie sélectionnés pour former les états de base du qubit sont des niveaux d'états dits "hyperfins" dus à l'interaction dans l'ion entre les moments magnétiques (spin) du noyau et des électrons. Les états hyperfins de l'ion d'ytterbium sont bien adaptés à l'informatique quantique car ils sont particulièrement stables, ce qui leur permet d'avoir une longue durée de cohérence.

[42] Le refroidissement d'atomes par laser est une technique qui permet de refroidir un gaz atomique, jusqu'à des températures de l'ordre du mK par réduction de la vitesse d'agitation des atomes pris sous le « feu des photons» (qui leur communiquent une force de recul) (Wikipedia).

Les pinces laser permettent d'agencer les atomes dans des structures 2D ou même 3D, répliquant par exemple des configurations cristallines. En raison de cette capacité naturelle à imiter certains systèmes quantiques, ils sont depuis longtemps considérés comme une plateforme de pointe pour la simulation quantique analogique dont nous parlerons au §4.3. De récentes démonstrations d'applications de portes logiques sur des qubits d'atomes froids ont stimulé la recherche pour leur mise en œuvre dans des ordinateurs quantiques à portes.

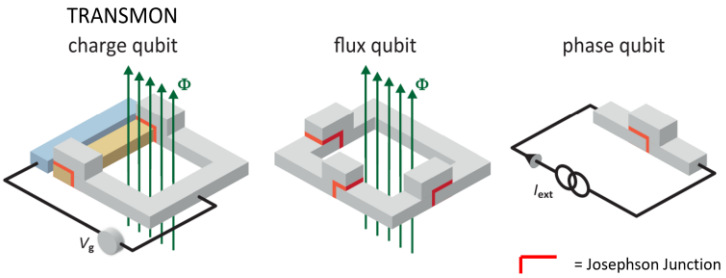
Le refroidissement des atomes par laser réduit la contribution du bruit pendant les opérations de calcul tandis que des impulsions laser ou micro-ondes sont à nouveau utilisées pour manipuler les états quantiques des qubits. Les atomes froids sont aussi utilisés dans des états dits de Rydberg, qui correspondent 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. En dehors du calcul quantique, un atome de Rydberg, excité par un laser, peut être utilisé pour générer des photons uniques bien isolés exploitables en optique [34], mais aussi servir en cryptographie et télécommunications quantiques[35], et métrologie (horloges atomiques, spectroscopie[36], [37]).

La figure 16 résume les forces et faiblesses de cette technologie qui partagent de nombreux points avec les ions piégés. Elle pourrait néanmoins permettre une densité de qubits nettement plus élevée dans un seul piège.

3.2.3. Les qubits supraconducteurs

Les qubits supraconducteurs[43] sont actuellement, avec les ions piégés, les qubits les plus avancés mais surtout les plus utilisés. Ils ont la particularité de ne pas être liés à l'information contenue dans un corpuscule unique, tel un atome ou un électron, comme dans les autres technologies de qubit, mais dans des paires d'électrons dites de Cooper, responsables de la supraconductivité. On parle parfois d' « atomes artificiels »[44] avec des niveaux d'énergie contrôlables mais ils sont bien sûr beaucoup plus gros, en termes de taille, qu'un atome.

Il existe plusieurs types de qubits supraconducteurs (cf. les revues récentes [38], [39]) ; tous utilisent les propriétés physiques d'une ou plusieurs jonctions dites de « Josephson »[45] au sein d'une boucle supraconductrice. Mais, ils diffèrent dans la manière d'encoder l'information quantique avec deux états bien distincts. La figure 14 illustre les trois variantes principales d'utilisation des jonctions Josephson au sein d'une boucle supraconductrice pour la construction d'un qubit supraconducteur : qubit de charge - aussi nommée **transmon**, qubit de **flux** et qubit de phase.



Source : Materials in superconducting quantum bits William D. Oliverand Paul B. Welander

Figure 14: Les trois types de qubits supraconducteurs

[43] Un matériau supraconducteur n'offre aucune résistance électrique à la circulation d'un courant et ne dissipe pas d'énergie. Ces propriétés n'apparaissent qu'à très basse température (de l'ordre de -271,3° C soit 1,8 K).
[44] Les qubits sont définis par les états d'énergie d'électrons liés à de petits dispositifs microscopiques et non à un atome.
[45] L'effet Josephson désigne l'apparition d'un courant entre 2 couches supraconductrices séparées par un matériau non-supraconducteur (isolant ou conducteur). La physique quantique établit **l'effet tunnel** entre ces 2 couches, à savoir qu'un électron a la capacité de franchir la barrière de potentiel induite même si son énergie est inférieure à l'énergie minimale nécessaire pour franchir cette barrière (jonction de Josephson). Une telle jonction peut être assimilée à la fente utilisée dans les expériences de diffraction/interférence sur les ondes, dont nous avons déjà parlé.

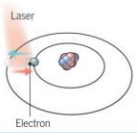
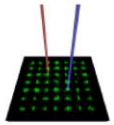
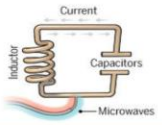
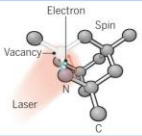
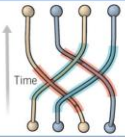
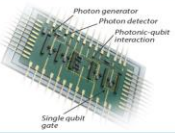
	Atomes		Electrons				Photons
Les illustrations sont pour la plupart extraites de "From Science News Feature, "Scientists are close to building a quantum computer that can beat a conventional one", Gabriel Popkin, 2016. Illustration by Chris Bickel/Science							
Technologie de qubit	**Ions piégés**	**Atomes froids**	**Supraconducteurs**	**Silicium (+quantum dot)**	**Impureté diamant (NV center)**	**Fermion de Majorana (topologique)**	**Photons**
Domaine d'application	métrologie, informatique, communication (répéteur, couplage avec photon)	métrologie, informatique, communication (couplage avec photon)	métrologie, informatique	métrologie, informatique	métrologie, communication, informatique	informatique	métrologie, communication, informatique
Nature des qubits	ions piégés électromagnétiquement	atomes piégés par des pinces laser	boucle/circuit supraconducteur	électrons piégés dans un semi-conducteur	électrons d'une cavité de diamant près d'un atome d'azote	quasi-particules, paires d'anyons, dans des nano-fils supraconducteurs	photons circulants dans des guides d'onde
États quantiques des qubits	niveau d'énergie de l'ion piégé	niveau d'énergie de l'atome	3 types: qubit de phase, de charge a.k.a transmon (niveau du courant) et de flux (sens du courant)	spin d'électron	niveau d'énergie des électrons du centre NV	sens de l'anyon	1 -propriété du photon (polarité ou autre)
Portes quantiques	laser ou micro-ondes	micro-ondes, lasers, états de Rygberg des atomes	micro-ondes>4Ghz et effet Josephson, magnétique	micro-ondes > 20 GHz	micro-ondes	inversion 2D d'anyons (tresse de nanofil)	interféromètre de Mach-Zehnder
Mesure d'état	laser + fluorescence	laser + fluorescence	Magnétomètre (SQUID), résonateur micro-onde	conversion spins vers charge	laser + fluorescence	fusion d'anyons	capteur de photons uniques
Caractéristiques techniques actuelles pour une application dans le domaine de l'ordinateur quantique							
Nb de qubits intriqués	11 qubits (IonQ)	51 qubits (simulations)	53 qubits (IBM et Google)	2 qubits (UNSW)	10 qubits (QDTI)	n.d.	20 qubits (Chine)
Tailles qubits	1mm²	atomes	100µm²	100nm²		n.d.	
Fidélité porte logique unitaire	99.999% [a]	>99% [c]	99.6-99.8% [e]	98% (→ 99.99% [g])	92% (→ 99.99% [h])	target: ~100%	98% (→ 99.99% [j])
Fidélité lecture	99.7%	97%	96%	98%	93%	n.d.	>50%
Durée porte	100µs		20-300ns	~5µs	~60s [i]	n.d.	1ns
Temps de cohérence	~600s [b]	100µs [d]	~100µs [f]	1-10s (→ 30s [g])		target: 100s	
Cryogénie	300K mais performances meilleures à 4-10K	15mK	15mK	100mK-1K	300K	15mK	300K mais générateur et lecteur en cryostat
Maturité (TRL) et potentiel de « Scale up » pour ordinateur quantique	5 Extensibilité : relativement difficile	4 Extensibilité : difficile	5 Extensibilité : relativement facile	3 Extensibilité : pas facile aujourd'hui mais bonne	3 Extensibilité : relativement difficile	1 Extensibilité : trop tôt pour se prononcer	3 Extensibilité : difficile

Figure 15: Caractéristiques des principales plateformes de qubits (Source: recherche documentaire diverse, O. Ezratty [144])

[a] C. D. Bruzewicz, J. Chiaverini, R. McConnell, et J. M. Sage, « Trapped-Ion Quantum Computing: Progress and Challenges », *Applied Physics Reviews*, vol. 6, nº 2, p. 021314, juin 2019
[b] Y. Wang *et al.*, « Single-qubit quantum memory exceeding ten-minute coherence time », *Nature Photonics*, vol. 11, nº 10, Art. nº 10, oct. 2017
[c] M. Saffman, « Quantum computing with atomic qubits and Rydberg interactions: progress and challenges », *J. Phys. B: At. Mol. Opt. Phys.*, vol. 49, nº 20, p. 202001, oct. 2016
[d] C. Sheng *et al.*, « High-Fidelity Single-Qubit Gates on Neutral Atoms in a Two-Dimensional Magic-Intensity Optical Dipole Trap Array », *Phys. Rev. Lett.*, vol. 121, nº 24, p. 240501, déc. 2018
[e] F. Arute *et al.*, « Quantum supremacy using a programmable superconducting processor », *Nature*, vol. 574, nº 7779, p. 505-510, oct. 2019
[f] M. Kjaergaard *et al.*, « Superconducting Qubits: Current State of Play », *Annual Review of Condensed Matter Physics*, vol. 11, nº 1, p. 369-395, 2020
[g] J. T. Muhonen *et al.*, « Storing quantum information for 30 seconds in a nanoelectronic device », *Nature Nanotechnology*, vol. 9, nº 12, Art. nº 12, déc. 2014
[h] X. Rong *et al.*, « Experimental fault-tolerant universal quantum gates with solid-state spins under ambient conditions », *Nature Communications*, vol. 6, nº 1, Art. nº 1, nov. 2015
[i] C. E. Bradley *et al.*, « A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute », *Phys. Rev. X*, vol. 9, nº 3, p. 031045, sept. 2019
[j] H. Wang *et al.*, « Boson Sampling with 20 Input Photons and a 60-Mode Interferometer in a 10^{14}-Dimensional Hilbert Space », *Phys. Rev. Lett.*, vol. 123, nº 25, p. 250503, déc. 2019

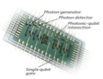
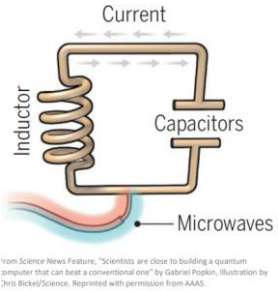
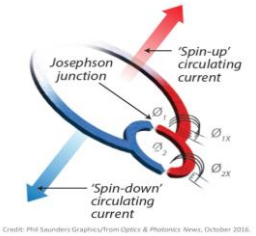
QUBIT	AVANTAGES/OPPORTUNITES	INCONVENIENTS/CHALLENGES
 IONS PIÉGÉS	• Taux de fidélité élevé des portes quantiques • Cohérence longue et ratio (temps de cohérence) / (durée des portes) élevé => algorithmes profonds • Intrication possible entre tous les qubits sur les architectures 1D et potentiellement 2D: Honeywell • Froid cryogénique extrême n'est pas nécessaire; le refroidissement par laser suffit (4-10K)→ plus simple que pour supraconducteurs • Interface avec des photons possible pour communications quantiques sur longue distance, entre ordinateurs quantiques et futur internet quantique • Les ions sont identiques => peu de calibrage	• Calcul relativement lent du fait des portes quantiques (mais contrebalancé par la durée de vie élevée du qubit=> ratio élevé) • Passage à l'échelle au-delà de 50 qubits sera difficile dans une architecture 1D, mais piste 2D prometteuse • Nécessité de chambres ultravides et d'un alignement précis des lasers ce qui peut être pénalisant pour le passage à l échelle • Leur dimension ($1mm^2$) peut aussi être un obstacle pour le passage à l'échelle
 ATOMES FROIDS	• Stabilité des atomes utilisés, agencés en 2D ou 3D • Taux de fidélité correct des portes logiques (mais pas le meilleur) + temps de cohérence des qubits longue • Atomes identiques et contrôlables avec les mêmes fréquences (laser & micro-onde) • Interface photonique possible (communication) • Réutilise les technologies éprouvées des ions piégés pour la mesure des états par fluorescence • Fonctionne bien en mode simulation analogique • Industrie française à la pointe: CEA, Pasqal • Utilisation d'appareillage standard • Fortes synergies avec métrologie et horloges quantiques	• Taux d'erreurs de lecture des états quantiques • Cross-talk entre qubits qui peuvent se perturber les uns les autres (comme les supraconducteurs) • Plus adapté à la simulation (analogique) qu'au calcul quantique universel => pourrait être remplacé par un ordinateur quantique générique (tolérant aux erreurs) dans le futur • Complexité des systèmes de lasers de contrôle physique (position) et logique (porte) des qubits => pénalisant pour le passage à l'échelle (nombre, calibration)
 SUPRACONDUCTEUR	• Fidélité et rapidité des portes élevées • Choix technologique privilégié par la recherche publique et privée (IBM, Google…) • Avancées majeures (53 bits), suprématie quantique • Offre commerciale existante • Progrès constants dans la réduction du bruit • Maitrise des technologies habilitantes : lithographie, cryostat, câblage, amplificateurs, logique, capteurs • Technologie déployable en 2D et adaptée aux techniques de correction d'erreur (surface code)=> passage à l'échelle	• Temps de cohérence des qubits modeste (~100µs) (mais effet atténué par la vitesse des portes) • Niveau de bruit dans les qubits • Technologie la plus exigeante en cryogénie (<20mK) nécessitant des réfrigérateurs à dilution • Complexité du câblage et de l'électronique pour le contrôle des qubits • Qubits hétérogènes à la fabrication => calibrage des contrôleurs (micro-ondes) • Couplage limité entre qubits proches dans des structures 2D (cross-talk potentiel) • Taille des qubits et miniaturisation délicate, « footprint » important
 SPIN SILICIUM	• Scalabilité: potentiel pour créer des processeurs avec des millions de qubits, grâce à leur taille $100nm^2$ • Fonctionne avec 1K (bien plus facile que 20mK) • Architectures 2D et intégration de « surface code » correcteur d'erreur possible • Technologie de fabrication du silicium inégalée par rapport à celle des autres qubits • Couplage possible des qubits avec des fibres optiques pour de la communication inter qubits longue distance • Vitesse d'exécution des portes quantiques	• Intrication de seulement 2 qubits réalisée à ce jour • Fidélité des portes binaires (2 qubits) moyennes (98%) • Variabilité des qubits nécessitant un réglage des fréquences micro-ondes d'activation (comme pour les qubits supraconducteurs) • Purification isotopique du silicium naturel nécessaire pour améliorer le qubit
 CENTRE NV	• Temps de cohérence intéressant même à T° ambiante, et qui s'améliore encore avec le froid cryogénique (4K) • Interconnexions photoniques pour communication • Peut servir à créer de la mémoire quantique auxiliaire à d'autres types de qubits • Synergies dans les utilisations des centres NV en métrologie, communication et informatique • Utilisation possible du spin atomique adjacent à la cavité	• Fidélité des portes quantiques faible • Complexité des systèmes lasers nécessaires pour le contrôle et la lecture • Fabrication des impuretés d'azote difficile, qui peut endommager le cristal et compromettre la fidélité des lasers de contrôle => pas facilement scalable • Difficulté à fabriquer des qubits identiques
 TOPOLOGIQUE	• Qubits théoriquement très stables et nécessitant peu de correction d'erreurs car intégrée dans le matériel • Potentiellement temps de cohérence long et rapidité des portes permettant de traiter des algorithmes profonds • Scalabilité des qubits construits a priori avec des techniques voisines de celles des qubits silicium (nanotechnologie)	• Aucun prototype n'a encore été construit • Qubits basés sur des nanostructures fabriquées et donc sujets à variabilité. • Fonctionnement probable à T° cryogénique <20mK comme les qubits supraconducteurs • Commence en retard par rapport aux autres qubits
 PHOTON	• Qubits stables: faible taux d'erreurs, et pas de décohérence (dans l'espace) • La plupart des opérations réalisables à T° ambiante • Techniques de fabrication courantes et maitrisées (semiconducteur CMOS) • Sources de photons uniques, indistingables faciliteraient la création de portes à deux qubits, fidèles et rapides • Technologie transversale incontournable: communications quantiques, métrologie	• Nombre de qubits encore limités, portes binaires conventionnelles difficiles à mettre en oeuvre • Taux d'erreur de lecture encore élevé, décohérence dans la fibre 150µs mais en amélioration • Les photons ne peuvent ni s'arrêter ni être stockés. Ils peuvent juste être légèrement retardés. • Les technologies de détections sensibles, telles que le SNSPD nécessitent un froid cryogéniques (~2K)

Figure 16: Avantages/Inconvénients de différentes technologies de qubit (Source: recherche documentaire dont [144])

La variante la plus employée est le *transmon* développé à l'Université de Yale en 2007 [47]. Les transmons utilisent une paire d'électrons liés[46] (paire de Cooper), qui couplée à un résonateur micro-onde[47] induit un léger changement de fréquence suivant l'état du qubit et permet ainsi la mesure de celui-ci. L'état du qubit en lui-même correspond à des niveaux de passage de courant à travers la jonction Josephson de la boucle supraconductrice. Les qubits sont contrôlés par des signaux électriques micro-ondes et basses fréquences. La durée des impulsions micro-ondes détermine les opérations quantiques qui sont effectuées.



Les états des *qubits de flux* correspondent au sens de circulation du courant supraconducteur dans sa boucle. La mesure de l'état d'un tel qubit utilise un SQUID[48] qui est un magnétomètre utilisant lui-même une (ou deux) jonction(s) Josephson et que l'on retrouvera plus loin dans la section consacrée à la métrologie. Les *qubits de phase* utilisent quant à eux deux niveaux d'énergie de courant dans une jonction Josephson. Ils sont en phase exploratoire dans quelques laboratoires comme ceux du NIST[49] aux USA.



A ce jour IBM, Google, Intel (transmon), Rigetti, D-Wave (flux) développent ou même commercialisent des ordinateurs construits sur cette technologie de qubits.

Les principales caractéristiques techniques sont reprises sur la figure 15, tandis qu'avantages et inconvénients sont présentés figure 16. Pour des applications dans le domaine de l'informatique, ces qubits sont extrêmement rapides (temps d'application des portes) mais leur temps de cohérence est très moyen et le taux d'erreurs encore élevé[50].

Le fait de pouvoir s'appuyer sur les connaissances existantes et la base de fabrication de l'industrie des semi-conducteurs « classiques » est une opportunité pour le passage à l'échelle et le développement de processeurs quantiques ayant un plus grand nombre de qubits. Les challenges principaux tiennent au fait que ces systèmes nécessitent des réfrigérateurs à dilution pour maintenir les états de supraconduction (15mK – voir figure 17) et que les procédés de fabrication actuels ne garantissent pas l'exacte similitude de chacune des boucles créées (qubit) ce qui a un impact sur le temps de cohérence et les erreurs.

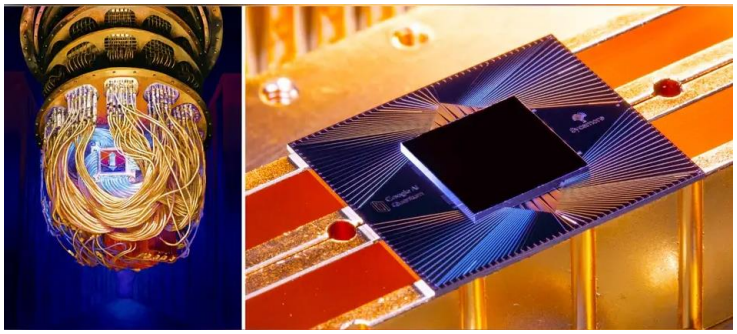


Figure 17: Processeur Google Sycomore (droite) et son cryostat (gauche) (Source: Google)

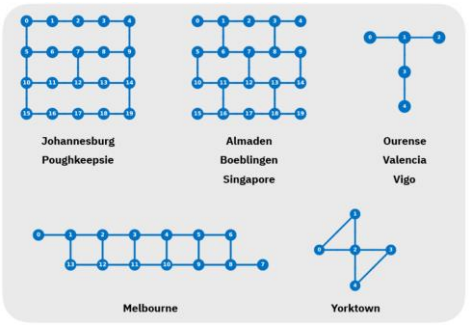


Figure 18: Connectivité des qubits d'une famille d'ordinateurs quantiques d'IBM (Source: IBM)

Enfin la connectivité entre les différents qubits pour faire de l'intrication est limitée (Figure 18), ce qui restreint le type d'algorithme qui peut y fonctionner.

---

[46] Deux électrons peuvent s'apparier dans un métal à très basse température malgré leur charge négative identique. Ce phénomène, où la force de répulsion ne semble plus œuvrer, est à l'origine de la supraconductivité (Nobel 1972).

[47] Un résonateur (ou cavité) micro-onde est une cavité à l'intérieur de laquelle une onde (ici dans la gamme des micro-ondes i.e. ~2,5GHz) entre en résonance avec les parois.

[48] Superconducting Quantum Interference Device

[49] Le National Institute of Standards and Technology est une agence du département du Commerce des États-Unis dont le but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie (Wiki).

[50] Pour préserver l'espace, nous ne détaillons pas les nouvelles conceptions de qubits qui pourraient ouvrir la voie à des durées de vie plus longues, par exemple Transmons 3D, Fluxonium, Zero-Pi.

3.2.4. Les qubits semiconducteurs (Spin Silicium)

Les qubits à base de silicium[51] (Si) constituent une voie d'exploration récente mais prometteuse car elle permettrait d'utiliser des processus de fabrication existants pour les composants CMOS[52] standards. Intel est le principal acteur impliqué, tandis qu'en France des équipes du CEA-Leti en collaboration avec l'Institut Néel du CNRS travaillent sur le sujet.

Cette technologie vise à utiliser le spin de l'électron, qui est l'archétype du système quantique à deux niveaux, alors que la particule est enfermée dans un puit de potentiel. Le silicium[53] est un substrat idéal pour confiner les électrons. Il y a trois principales catégories de qubits Silicium (voir figure 19 et [49]): ceux à base d'impuretés de phosphore[54] (dopage négatif), les boites (quantum dot) à base de métal-oxyde-semiconducteur (MOS) et celles utilisant des structures hétérogènes de Si coincé entre deux barrières de SiGe[55].

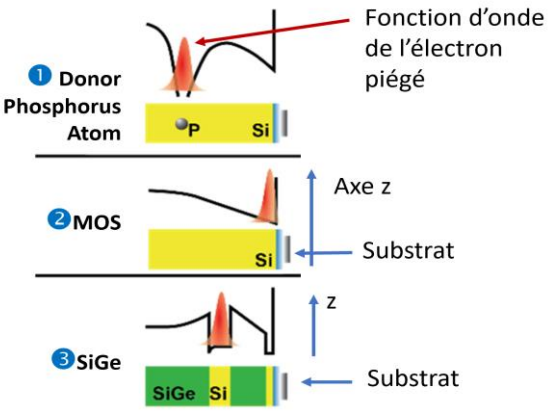
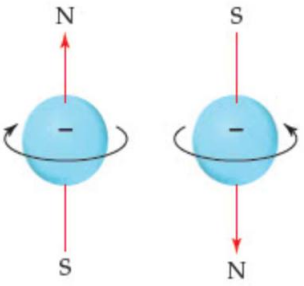


Figure 19: Les trois principaux types de qubits silicium: bande d'énergie (ligne noire), fonction d'onde de l'électron (rouge) et substrats en dessous (Source: d'après M. S. Carroll et Al. Silicon Qubit)

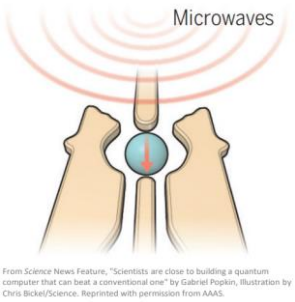
L'objectif des trois méthodes est de piéger un électron de conduction dans la direction z (perpendiculaire au substrat) par un dispositif physique (d'où le terme puit/boite ou point) et d'utiliser le spin de cet électron pour encoder l'information.

Comme dans le cas des qubits supraconducteurs, le contrôle des qubits et l'application des portes logiques quantiques s'effectuent par l'envoi de micro-ondes et la lecture des états de spin par un procédé de conversion spin-to-charge. Comme pour les qubits supraconducteurs, il arrive que l'on parle d'« atome artificiel ».



En termes de refroidissement, des avancées très récentes[50], [51] permettent d'envisager des température de fonctionnement de 1K, ce qui reste bien sûr très froid mais qui est technologiquement beaucoup plus simple que maintenir 15mK comme pour les qubits supraconducteurs.

Comme on peut le voir sur la figure 15, les débuts sont modestes. En 2020, le nombre de qubits à base de silicium se limite à 2 avec une fidélité supérieure à 98% pour toutes les opérations. Par contre, les temps de manipulations (lectures ou applications de portes) sont rapides (avantages et inconvénients sont résumés dans le tableau de la figure 16). Les qubits de spin ont des dimensions de l'ordre de 100nm^2 et se prêtent donc à une forte densité et miniaturisation. Pour le passage à l'échelle, ils bénéficieraient des infrastructures des semiconducteurs existantes (e.g. : lithographie) mais la nécessité d'avoir un environnement cryogénisé et une protection renforcée de l'état quantique des qubits sensibles au magnétisme serait une contrainte.



[51] D'autres matériaux semiconducteurs sont également étudié comme l'Arséniure de gallium (GaAs)[48].
[52] Le CMOS (Complementary Metal Oxide Semiconductor) est la principale technologie utilisée pour produire des processeurs dans le monde : CPU, GPU, chipsets pour smartphones et outils électroniques spécialisés(Intel, AMD, Nvidia, Qualcomm...).
[53] Pour rappel, le principe du dopage des semi-conducteurs est d'ajouter des impuretés en petites quantités au silicium afin de modifier ses propriétés de conductivité.
[54] Le phosphore est un dopant qui va donner un électron et créer un semi-conducteur de type n (négatif).
[55] SiGe : Silicium + Germanium

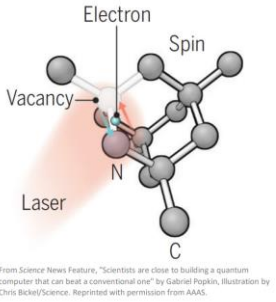
3.2.5. Les impuretés dans le diamant (centre Azote-lacune, NV center)

Les diamants sont des bijoux éternels qui symbolisent, dans certaines circonstances, l'engagement et la pureté. Leur utilisation dans le domaine des technologies quantiques peut du coup surprendre, d'autant plus que c'est un défaut spécifique de la structure cristalline d'atomes de carbone, composant du diamant, qui est alors exploité.

Ce que l'on entend par défaut ou impureté désigne le remplacement dans le réseau cristallin d'un atome de carbone par un atome d'azote (*Nitrogen : N*) et d'un autre atome de carbone adjacent par un vide sans atome, ce qui crée une cavité ou lacune (*Vacancy : V*), d'où leur nom usuel de *NV center*. Les diamants destinés à cet usage sont créés artificiellement. Ils ont une couleur particulière si bien que l'on rencontre parfois le terme « *color center* » dans la littérature scientifique. Ils sont la plupart du temps déposés sur des couches de substrat à plat[52].

Les travaux sur les diamants NV se sont longtemps concentrés sur leurs applications dans le domaine des capteurs et des communications quantiques. La technologie des capteurs à base de centre NV est l'une des technologies de capteurs quantiques les plus prometteuses[53]. Le matériau est inoffensif et peut être utilisé en imagerie du magnétisme de cellules vivantes[54]. Dans les télécommunications, leur couplage possible avec des photons est un sujet de recherche actuel[55].

Cette technologie présente plusieurs avantages liés à ses performances (résolution des mesures, sensibilité, temps de cohérence) et à sa facilité de mise en œuvre (température/pression ambiante) ce qui au final sied bien aussi au domaine de l'informatique. Ainsi, son utilisation pour créer des qubits est étudiée par des startups comme QDTI et laboratoires comme Delft aux Pays-Bas, ou Hefei en chine [44].



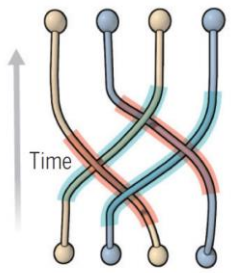
From *Science* News Feature, "Scientists are close to building a quantum computer that can beat a conventional one" by Gabriel Popkin, Illustration by Chris Bickel/Science. Reprinted with permission from AAAS.

Pour les qubits, la technologie repose sur le contrôle du spin d'électrons piégés dans les cavités et est souvent aussi appelé « atome artificiel » comme deux des technologies déjà décrites précédemment. Les spins des électrons piégés et des noyaux de carbone voisins peuvent être contrôlés par une combinaison de micro-ondes et de champs magnétiques. La mesure de l'état des qubits se fait par la captation de la fluorescence de la cavité lorsqu'elle est éclairée par un laser comme c'est aussi le cas pour les ions piégés.

Lafigure 16 résume les avantages et inconvénients de cette technologie encore peu utilisée dans la construction d'ordinateurs car, si elle peut en théorie être opérée à température ambiante, l'intrication et la production fiable de qubits identiques sont problématiques. Enfin, il convient de noter que l'exploitation d'autres défauts du diamant comme le Silicon Vacancy (SiV Center) est à l'étude et constitueraient une alternative intéressante aux centres NV[56].

3.2.6. Les qubits topologiques

La technologie des qubits topologiques exposée ici n'est envisagée que pour le développement d'ordinateurs quantiques. Elle ne semble pas transposable aux autres domaines d'application des technologies quantiques. Elle est certainement la moins développée (TRL[56] 1) de notre liste et complexe à appréhender.



From *Science* News Feature, "Scientists are close to building a quantum computer that can beat a conventional one" by Gabriel Popkin, Illustration by Chris Bickel/Science. Reprinted with permission from AAAS.

Le développement d'architectures topologiques repose sur une approche permettant de construire des qubits qui pourraient vraisemblablement atteindre des taux d'erreurs intrinsèques extrêmement faibles, de sorte que la mise en œuvre d'un système de correction d'erreurs ne serait pas nécessaire (contrairement aux autres plateformes de qubits présentées jusqu'à présent - voir §4.3).

[56] L'échelle TRL (technology readiness level) évalue le niveau, allant de 1 à 9, de maturité d'une technologie.

Dans cette technologie, l'état quantique est encodé dans des « quasiparticules » évoluant sur un plan en 2D appelé des anyons[57] (e.g. le fermion de Majorana [59]). Ces anyons modélisent des grands nuages d'électrons autour d'atomes. L'état quantique codé ne dépend donc pas d'un électron individuel mais d'un large groupe ce qui garantit sa stabilité. Les anyons créés peuvent ensuite être canalisés à travers des nanofils supraconducteurs qui peuvent s'entrecroiser. Les portes quantiques sont implémentées par les différentes tresses que les particules suivent dans le temps [60].

Les verrous technologiques sont encore nombreux avant que tout cela ne fonctionne. Toutefois les promesses d'un taux de fidélité très élevé (opérations quantiques, mesures), et d'un temps de cohérence très long intéressent des entreprises comme Microsoft et Nokia, ainsi que plusieurs laboratoires universitaires dans le monde. Corollairement, les taux d'erreurs devant être très faibles, seul un petit nombre de qubits physiques serait nécessaire pour avoir un ordinateur quantique utilisable (Figure 16).

3.2.7. Les photons

La photonique est une science et une industrie à part entière, transversale à beaucoup de domaines scientifiques et technologiques. Au-delà des lasers, produits de la première révolution quantique[58], les applications exploitant les principes de superposition ou d'intrication commencent à émerger lentement de la recherche, c'est la photonique quantique.

A la différence des supports de qubits mentionnés précédemment qui exploitaient un encodage de l'information sur des atomes ionisés ou neutres, ou des électrons (qubits supraconducteurs, silicium, NV center, topologique), la photonique quantique s'appuie sur les photons, corpuscules de la lumière, sans masse et qui se déplacent à des vitesses proches de celle de la lumière sur des puces optiques, guides d'onde, fibres ou en espace libre.

Un photon offre de nombreux degrés de liberté pour encoder de l'information (sa fréquence/couleur, sa polarisation, son amplitude, sa phase…) sachant que combiner plusieurs codages est possible.

Les domaines d'applications de la photonique quantique sont multiples. Par exemple, en métrologie nous aborderons §4.1.5 le thème des radars quantiques dont le principe consiste en la préparation d'une paire de photons intriqués dans le radar, suivi de l'envoi d'un des photons vers la cible tandis que l'autre est conservé sur place. Lorsqu'un photon est reçu par le radar, il est possible de tester s'il est intriqué avec celui resté sur place, et de déterminer alors s'il a été réfléchi, ou pas, par la cible

Dans le domaine des télécommunications, l'état quantique des photons et leur l'intrication potentielle, utilisés comme support de l'information, sont les clés de la sécurisation des communications sur de longues distances (voir §4.2).

La mise en œuvre technologique de la photonique quantique implique des détecteurs performants pour la métrologie et les télécommunications mais aussi le développement de sources de photons uniques et indiscernables[59]. Ainsi, la startup française Quandela, co-fondée par Pascale Senellart, propose-t-elle un générateur capable d'envoyer des séries de photons individuels régulièrement espacés dans le temps et possédant les mêmes propriétés quantiques.

Avec ces outils, la photonique quantique devient une technologie prometteuse pour le calcul quantique. L'état quantique le plus couramment utilisé est celui de leur polarisation (horizontale ou verticale) mais combiner plusieurs codages permettrait d'aller au-delà des qubits traditionnels à deux états de base, et d'augmenter encore la puissance de calcul/codage (ex: création de *qudits* [61], [62]).

[57] Voir les travaux publiés par l'équipe française qui a relevé la première signature expérimentale [57] suivi d'une publication de chercheurs de Microsoft [58].
[58] Les lasers sont largement utilisés dans la manipulation des autres variété de qubits -. la 1ère révolution sert à la 2nde révolution.
[59] Des photons indiscernables sont des photons qui ne peuvent être différenciés les uns des autres, par exemple par rapport à leur fréquence. Ce concept est en lien direct avec la physique quantique, où les photons n'ont pas de trajectoire bien définie qui permettrait de les distinguer (Wikipedia).

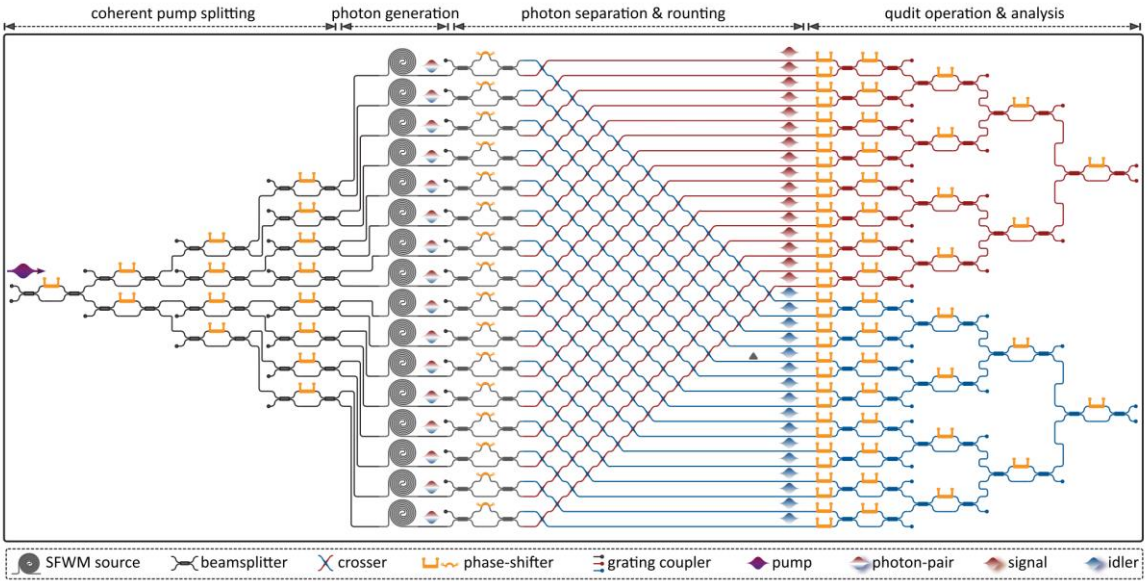


FIG. 2. A circuit diagram of the multidimensional silicon quantum photonic circuit. Reprinted with permission from Wang *et al.*, Science **360**, 285–291 (2018). Copyright 2018 AAAS. The device monolithically integrates 16 photon-pair sources, 93 thermo-optical phase shifters, 122 multimode interferometer beamsplitters, 256 waveguide crossers, and 64 optical grating couplers. A photon pair is generated by SFWM in superposition across 16 optical modes, producing a tunable multidimensional bipartite entangled state. The two photons, signal and idler, are separated by an array of asymmetric Mach–Zehnder-Interferometer (MZI) filters and routed by a network of crossers, allowing the local manipulation of the state by linear optical circuits. Triangular networks of MZIs perform arbitrary local projective measurements. The photons are coupled off the chip into fibers by means of grating couplers, and are detected by two SNSPDs. See Ref. 204 for details.

Figure 20: Schéma d'un circuit photonique quantique
(Source: Diagramme et légende de "Photonic quantum information processing : a consive review », Slussarenko, Pryde, 2019)

Concernant les portes logiques quantiques, la manipulation des photons individuels pour les opérations unaires se fait par des éléments optiques usuels[60] (miroirs, séparateurs de faisceaux, déphaseurs...).

La mise en place d'opération portant sur deux qubits (e.g. pour intrication) est plus complexe car les photons interagissent peu avec leur environnement. Des interféromètres Mach-Zehnder[61] sont souvent utilisés mais la fidélité des opérations n'y est bonne qu'avec des sources de photons uniques de grande qualité.

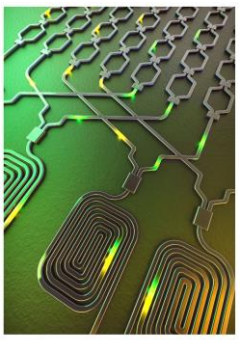


Image: Xiaogang Qiang/University of Bristol

Une autre solution explorée récemment est l'utilisation de nanostructure en forme de cavité [65]. Pour finir, la lecture de l'état quantique du qubit utilise des détecteurs de photons uniques. La détection est encore imparfaite, néanmoins des technologies récentes ont amélioré les résultats (SNSPD[62] utilisé aussi pour la détection des photons[66] dans les technologies de télécommunications quantiques [67]). La figure 20 illustre ce que peut être un circuit de calcul utilisant des qubits photoniques [68].

Les photons sont des « flying qubits » ou « qubits volants ». Ils se déplacent et sont par conséquent parfaits pour les télécommunications. Ils sont les seuls qubits à offrir une interface naturelle pour la mise en réseau de calculateurs quantiques, point que nous développerons au chapitre 4 (section §4.2).

Comme précédemment, la figure 16 résume les principaux avantages et inconvénients de cette technologie. Les qubits photoniques sont assez stables (peu de décohérence). Ils permettraient de réaliser des circuits fonctionnant à température ambiante (les SNSPD nécessitent par contre de la cryogénie) et de s'appuyer pour une mise à l'échelle, qui resterait toutefois délicate, sur le savoir-faire des nanotechnologies optiques classiques et les infrastructures courantes utilisées pour les processeurs silicium.

[60] On parle de la proposition ou schéma de KLM du nom des auteurs[63] qui ont proposé en 2001 une approche permettant d'éviter d'utiliser de l'optique non-linéaire pour la construction d'un ordinateur quantique.
[61] Le livre « Le Monde Quantique » de Michel Le Bellac [64] fournit une explication clair de l'interféromètre Mach-Zehnder.
[62] Superconducting nanowire single-photon detectors.

3.2.8. *Autres qubits*

D'autres approches exotiques ont été testées par le passé ou sont en cours d'étude. Nous pouvons citer le cas particulier de la résonance magnétique nucléaire (RMN) qui utilise les propriétés des spins d'atomes dans des molécules (à l'état liquide ou cristallin). L'application du principe n'a pas donné de résultats probants pour le codage de qubits. Cependant, la technologie reste bien sûr très efficace dans le domaine des capteurs et de l'imagerie médicale en particulier.

Par ailleurs, plus prospectif, certains groupes de chercheurs étudient l'encodage et la manipulation d'informations sur des électrons piégés dans de l'hélium liquide [69], [70].

3.2.9. *Maturité des technologies*

Les technologies que nous avons abordées, ont des niveaux de maturité très différents (Figure 21). Aucune n'est aboutie. Chacune a ses avantages, ses inconvénients et peut bénéficier d'opportunités ou se confronter à des challenges (Figure 16).

Ces différentes approches sont nécessaires. Il est possible qu'une ou plusieurs portent leurs fruits. On ne sait prédire à ce stade car les technologies évoluent vite. Il est d'ailleurs probable que selon les applications plusieurs soient utilisées comme c'est déjà le cas aujourd'hui.

Les qubits supraconducteurs et les ions piégés sont à ce jour les plus avancés technologiquement. Mais ces derniers, tout comme les qubits photoniques et les centres NV pourraient avoir du mal à être déclinés en un grand nombre de qubits et à proposer des modalités de contrôle et d'utilisation performantes lors du passage à l'échelle

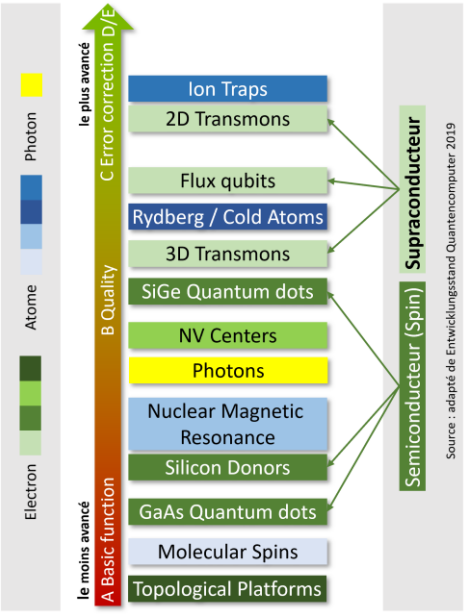


Figure 21: Maturité des technologies de qubits – par grande famille (Source: d'après Entwicklungsstand Quantencomputer,2019)

Ainsi, **le passage à l'échelle n'est pas lié** à la seule performance individuelle des qubits ou à leur **nombre (pourtant paramètre clé)**. La variabilité dans la qualité de fabrication de certains types de qubits, et la capacité à en contrôler et à en faire interagir un grand nombre simultanément seront primordiales pour les performances globales du système. Le succès d'une technologie, particulièrement dans le cadre d'une application en informatique quantique, sera lié à sa capacité à répondre aux critères principaux que nous avons résumés figure 22 :

Stabilité des qubits

Elle s'évalue par plusieurs métriques notamment la durée de cohérence. Si l'on rapporte cette durée au temps d'activation des portes logiques quantiques et au taux d'erreur, elle détermine le nombre maximal de portes que l'on peut enchaîner dans un algorithme (appelé « profondeur » de l'algorithme).

Température de fonctionnement

des qubits et de l'électronique associée. Il est fréquent d'avoir des qubit censés fonctionner à T° ambiante mais pour lesquels certains autres équipements (e.g. détecteurs de photons) doivent être cryogénisés à 15mK ou à 1K (ce qui est un moindre mal car refroidir à 1K est plus simple qu'à 15mK).

Taux de fidélité (niveau d'erreurs) des qubits

Il se mesure lorsqu'on applique des portes quantiques unaires (1 qubit en entrée) ou binaire (2 qubits). L'erreur de mesure en fin de calcul est également à considérer. Cela ouvre la question épineuse d'un benchmarking normalisé. Il faut au moins 99%, idéalement 99,9%+.

Niveau de miniaturisation

La taille physique des qubits et de leur entourage technique («empreinte au sol», nombre de câbles,…) conditionne la capacité à en augmenter le nombre. Les qubits à spin d'électrons (semiconducteurs) sont à leur avantage sur cet aspect.

Capacité d'intrication

La possibilité de connecter, d'intriquer les qubits à grande échelle sans être limité aux qubits voisins les plus proches (relation 1:1 ou n:n) est un gage de puissance qui permet dans le cadre des ordinateurs quantiques de ne pas se limiter à des algorithmes spécifiques simples.

Processus de fabrication

Il dépend de nombreux paramètres dont la variabilité de la qualité de fabrication de certains types de qubits (centre NV) et la possibilité d'employer des savoir-faire/ infrastructures existants (qubit semiconducteur). Certaines technologies nécessitent de créer des circuits spécialisés ad-hoc (e.g. ce n'est pas le cas pour les atomes froids).

Figure 22: Indicateurs clés pour l'évaluation et le suivi des technologies de qubits

3.2.10. Les technologies de qubits par acteurs

Les domaines d'applications des technologies quantiques sont nombreux et le potentiel disruptif probable pour certains secteurs. Nous en parlerons dans le chapitre 4. De nombreuses organisations s'attachent à faire progresser la recherche tandis que des acteurs économiques variés ont déjà choisi d'investir dans ces technologies. Nos analyses (annexes 2, 3, 4) prouvent que l'accélération de l'intérêt des mondes académiques, économiques et industriels pour ces technologies est bien réelle que ce soit en termes de publications scientifiques, de brevets, ou d'investissements capitalistiques et que les gouvernements sont eux-mêmes prêts à des investissements très conséquents.

Compte tenu de la diversité des technologies et des acteurs, il nous a semblé éclairant de faire le lien entre les deux. La figure 23 illustre notre recherche[63]. Les intervenants qu'ils soient entreprises établies, startups ou laboratoires universitaires peuvent travailler sur plusieurs technologies .Cette liste n'est pas exhaustive et évolue rapidement. Un inventaire plus complet est proposé à la fin de l'annexe 4[64].

Il est à présent temps de passer à la description des principaux domaines d'applications.

[63] La liste fait apparaitre la catégorie « Adiabatic/Annealing » qui regroupe des types particuliers de processeurs/calculateurs quantiques adaptés à la résolution de problèmes d'optimisation complexes et utilisant pour la plupart les technologies de qubits supraconducteurs (§4.3.2.2).
[64] Nous y avons recensé près de 300 sociétés, sans prétention d'exhaustivité.

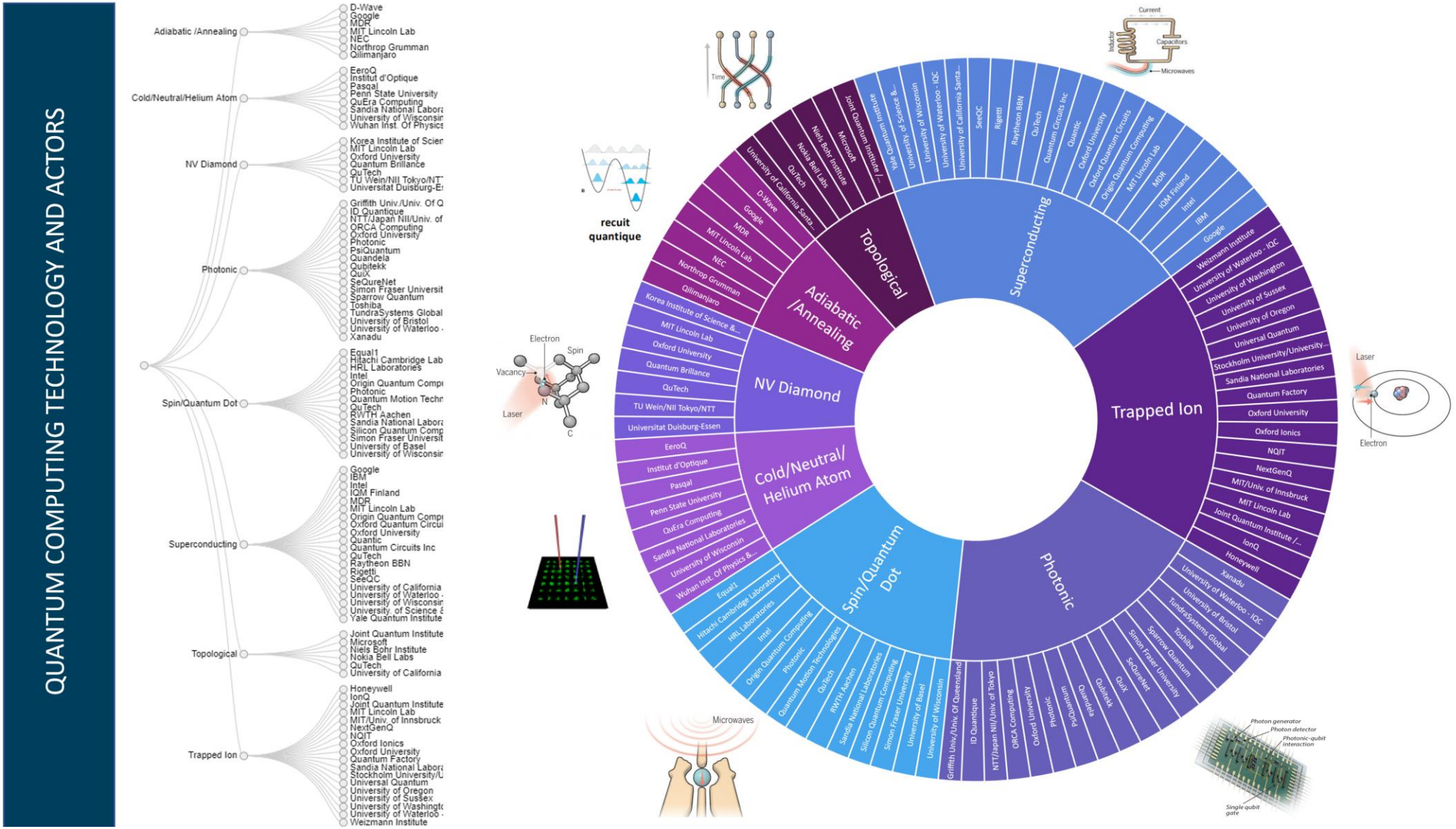


Figure 23:Intérêts des différentes organisations (géants de l'IT, startups, universités...) pour les différentes technologies de qubits
(Source : d'après les données de www.quantumcomputingreport.com)

4. Les applications

Dépassant la simple exploitation du principe de quantification, cœur de la 1ère révolution quantique, les progrès majeurs réalisés dans la capacité de détecter et manipuler individuellement des objets quantiques initient ce l'on considère comme la 2nde révolution, tant le champ des applications peut être étendu comme nous le verrons dans ce chapitre.

En raison de cet énorme potentiel, des initiatives et des investissements stratégiques de grande envergure sont mis en place par les gouvernements et les entreprises du monde entier (voir annexe 4) afin de tirer parti des bénéfices scientifiques, technologiques, économiques et sociétaux pour des secteurs aussi divers que l'énergie, la chimie, les transports, les télécommunications, la médecine...

Les roadmaps de la plupart des programmes d'investissements nationaux ou transnationaux comme le Quantum Flagship de l'Union Européenne[71] visent à inclure tous les aspects des technologies quantiques en les divisant en trois grands domaines d'intérêt (énumérés ❶,❷,❸ figure 24) reposant sur un socle commune de science fondamentale.

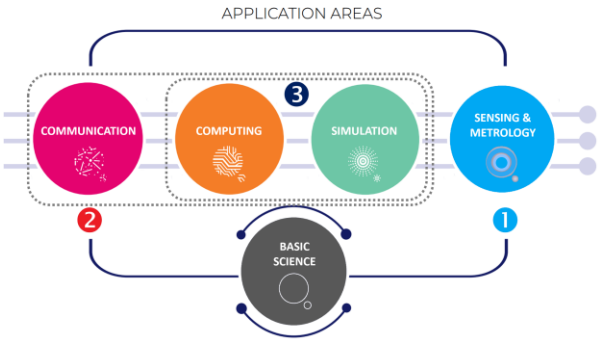


Figure 24: Domaines d'application (Source: European Quantum Flagship)

				Secteurs d'activité**				
Domaine		**Principe**	**Applications***	**Télécom**	**Médecine**	**Pétrole**	**Finance**	**Transport**
❶ Métrologie capteurs, horloges		• La métrologie regroupe les applications reliées au domaine des **capteurs**, de la mesure du temps et d'autres quantités physiques et de **l'imagerie** • La grande sensibilité des systèmes quantiques aux perturbations externes est exploitée pour améliorer les performances des mesures de quantités physiques	Gravimètre Accéléromètre Magnétomètre Géolocalisation Horloge atomique	Horloge atomique pour synchronisation de serveurs réseaux	Imagerie cérébrale améliorée	Imagerie du sous-sol	Horodatage des transactions	Navigation GPS Navigation sans GPS LiDAR quantique
❷ Communication cryptographie		• Les photons individuels ou intriqués sont utilisés pour transmettre des données de manière sécurisée • Les technologies quantiques permettent de générer des clés de **cryptage** réellement aléatoires et de détecter toute interception de messages • De nouveaux algorithmes et protocoles sont développés pour contrer les risques potentiels liés aux nouvelles possibilités de décodage des ordinateurs quantiques	Communication sécurisée point-à-point Communication longues distances Génération de nombres aléatoires (QRNG) Distribution de clés de cryptage publique (QKD)	Cryptographie Internet quantique	Protection des données patients	Protection des infrastructures	Sécurisation des transactions	Protection des véhicules autonomes
❸ Simulation & calcul	Simulation analogique& digitale	• Les systèmes quantiques sont utilisés pour **reproduire** le comportement d'autres **systèmes quantiques** moins accessibles	Conception de nouveaux produits chimiques (engrais, médicaments), et matériaux		Découverte matériaux, molécules			Simulation des matériaux pour batterie
	Calcul ordinateur	• Utilisation des principes quantiques (qubit, superposition, intrication) pour augmenter la **puissance de calcul** d'un ordinateur	Résolution de problèmes d'optimisation combinatoire Intelligence artificielle	Optimisations des réseaux	Découverte médicaments	Analyse des emplacements de forage Optimisation des réseaux de distributions	Gestion de portefeuille	Optimisation du trafic

Figure 25: Technologies quantiques, principes et exemples d'applications

Nous avons retenu cette classification et le tableau précédent (Figure 25) détaille les grands principes et quelques exemples d'applications métiers que nous allons détailler dans les sections suivantes.

Notons par ailleurs que le socle commun est constitué, d'une part des principes et du formalisme mathématique, rigoureux et complexe de la théorie quantique, et d'autre part des technologies de contrôle de l'information quantique contenue dans les corpuscules. Ainsi des progrès de la base commune en lien avec un domaine d'application spécifique peuvent naturellement bénéficier à d'autres domaines, tout comme, transversalement, une avancée directe dans un domaine particulier pourrait être transposable dans un autre. Ces éléments particuliers concourent au fait que les technologies quantiques pourraient se développer à un rythme soutenu. La figure 26 propose un agenda indicatif, non exhaustif que nous aurons l'occasion de détailler dans les différentes sections de ce chapitre.

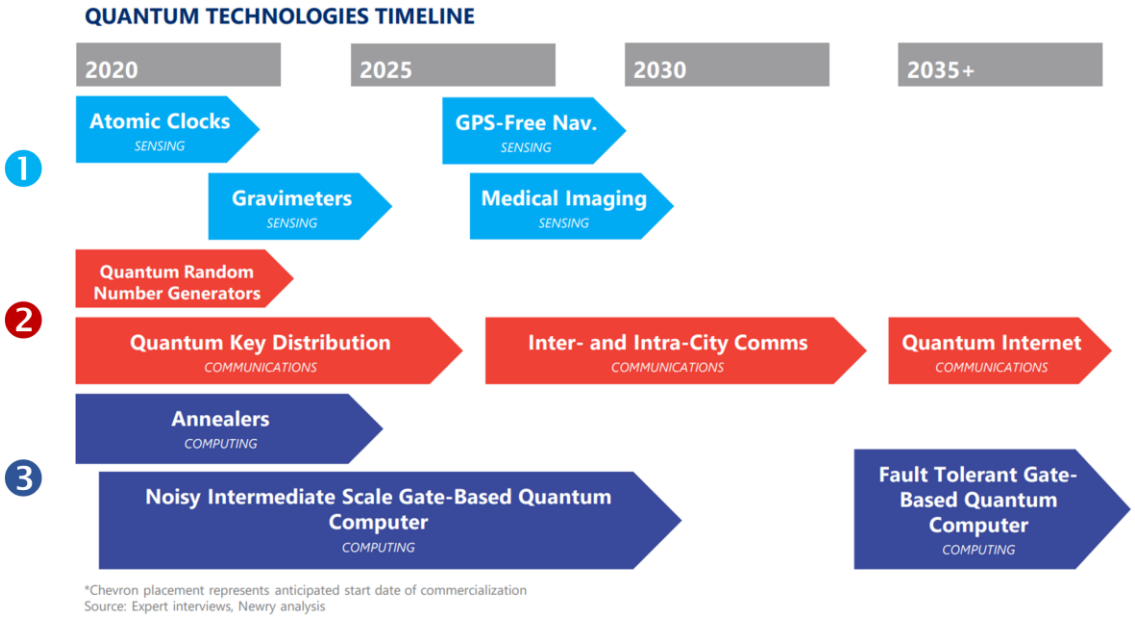


Figure 26: Calendrier prospectif du déploiement commercial des technologies quantiques (Source: [72])

4.1. Métrologie, capteurs et imagerie quantique

Le premier domaine d'application de la physique quantique, et du traitement de l'information quantique, est celui de la métrologie et des capteurs au sens large. Si l'informatique quantique recueille une grande partie de l'attention des médias généralistes, la plupart des experts estiment que les instruments de métrologie (capteurs) et horloges quantiques connaîtront un succès commercial rapide si tout en étant plus performants que les technologies classiques des critères de coûts et d'encombrement sont atteints (objectifs SWaP-C)[65].

Employant certains des supports quantiques physiques décrits dans le §3.2, les capteurs quantiques tirent parti de l'extrême sensibilité des états quantiques en exploitant les principes de superposition et d'intrication pour obtenir des performances plus élevées que celles des capteurs conventionnels. Ainsi sont-ils à même de révéler les infimes variations de l'environnement, telles que changements de température, de pression, d'accélération, de champs électromagnétiques. Sensibles et précis ils amélioreront la navigation (avec ou sans GPS[66]), la synchronisation des réseaux, les relevés géologiques, le LiDAR, l'imagerie médicale même à l'échelle de l'ADN, etc…

[65] SWaP-C : Le terme anglais SWaP-C (Size, Weight, Power and Cost) est souvent employé dans ce contexte pour faire référence à un objectif d'optimisation de la taille, du poids, de la puissance et du coût d'un appareillage.
[66] La navigation sans GPS permet de continuer ses déplacements malgré la présence de bâtiments hauts, de souterrains ou de brouillage du signal. C'est un domaine qui intéresse particulièrement les militaires.

Dans les faits, certains types de capteurs quantiques, tels que les horloges atomiques et les interféromètres à atomes froids[67] sont déjà commercialisés et surpassent les dispositifs traditionnels.

Les travaux se poursuivent au sein de laboratoires, de startups ou de départements R&D pour proposer de nouveaux produits, et rendre les existants plus petits et plus robustes. Résultant d'interviews d'experts de ce domaine [72], un calendrier potentiel d'arrivée sur le marché est proposé à la Figure 27.

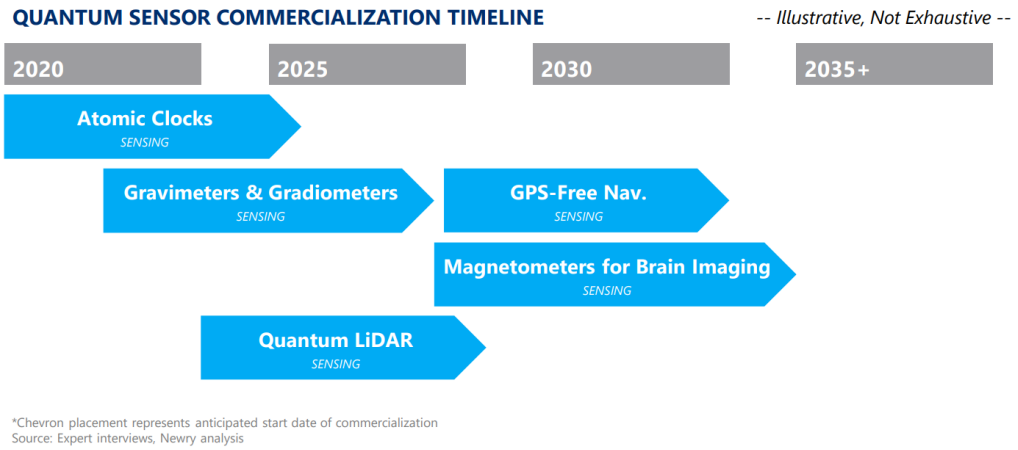


Figure 27: Calendrier de déploiement prospectif indicatif des technologies de métrologie et capteurs (Source: [72])

Métrologie, capteurs et imagerie quantique emploient de multiples approches technologiques, communes, pour la plupart, aux autres « domaines du quantique ». Ne pouvant être exhaustif, nous proposons dans la suite une sélection d'applications et, pour chacune, l'état de l'art des technologies employées.

4.1.1. Horloge atomique

La mesure précise du temps est un élément essentiel non seulement pour la recherche fondamentale ou appliquée (e.g. recherche de la matière noire dans l'univers), mais aussi pour les technologies utilisées dans les réseaux de communication et les systèmes de navigation GPS/GNSS.

Les horloges atomiques sont l'exemple le plus établi de la technologie quantique, puisque c'est une fréquence caractéristique des atomes de césium 133 (^{133}Cs) qui sert de définition de la seconde dans le Système International. Ainsi depuis 1967, la seconde est définie[68] 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* ».

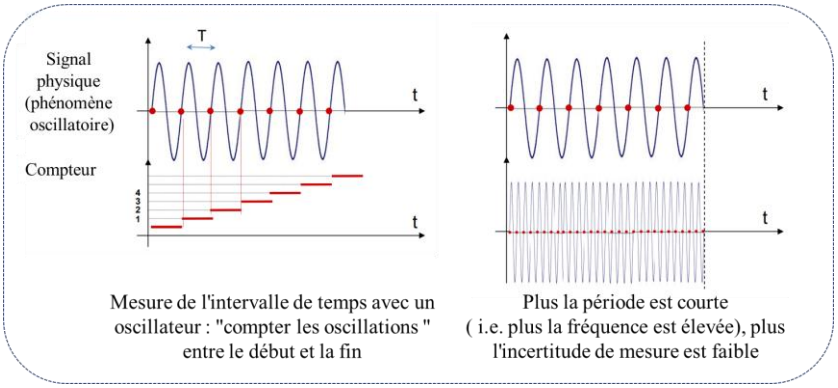


Figure 28: La mesure du temps nécessite un phénomène physique oscillatoire

[67] Muquans & AOSense par exemple.
[68] https://www.bipm.org/metrologie/time-frequency/units.html

Cette définition de la seconde fait référence à un phénomène physique oscillatoire (périodique), tout comme le battement du balancier d'un métronome (Figure 28). Plus la fréquence de l'oscillateur est élevée, plus la mesure du temps sera précise (Figure 29).

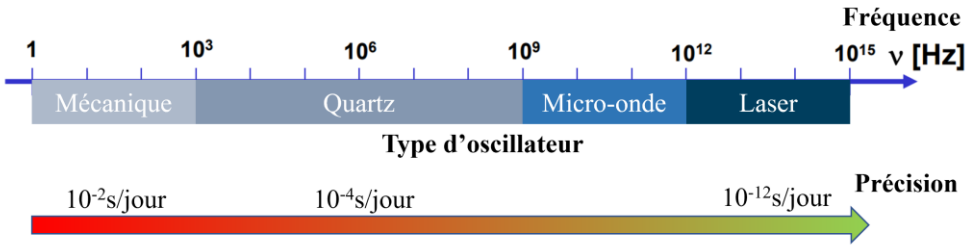


Figure 29: Précision des horloges en fonction de la fréquence des oscillateurs

Les horloges atomiques utilisent les structures hyperfines[69] de certains atomes (Ca, Sr, Yb…) comme référence de fréquence à partir de laquelle elles dérivent un étalon de temps. La fréquence élevée de ces transitions atomiques permet alors une synchronisation à très haute résolution. Le développement de la technologie des peignes de fréquence (honorée d'un prix Nobel en 2005), dans laquelle des lasers émettent un rayonnement caractérisé par une série de fréquences régulièrement espacées, a permis de mesurer des intervalles de temps et des fréquences lumineuses avec une précision inégalée[70].

Par ailleurs, à la différence des cristaux de quartz, tous les atomes d'un isotope[71] d'élément chimique donné sont identiques. Ainsi, tant que les atomes sont correctement isolés des influences extérieures, des horloges atomiques séparées, basées sur le même isotope, doivent avoir des décomptes (tops) constants et identiques. Le taux de dérive est minimal (10^{-18} voir [73]). Dans les dix dernières années, la technologie des horloges à réseau optique[74] qui confine les atomes utilisés au sein d'un maillage de rayon laser a surpassé la précision des premières générations d'horloges atomique et des fontaines atomiques[72] (Figure 30).

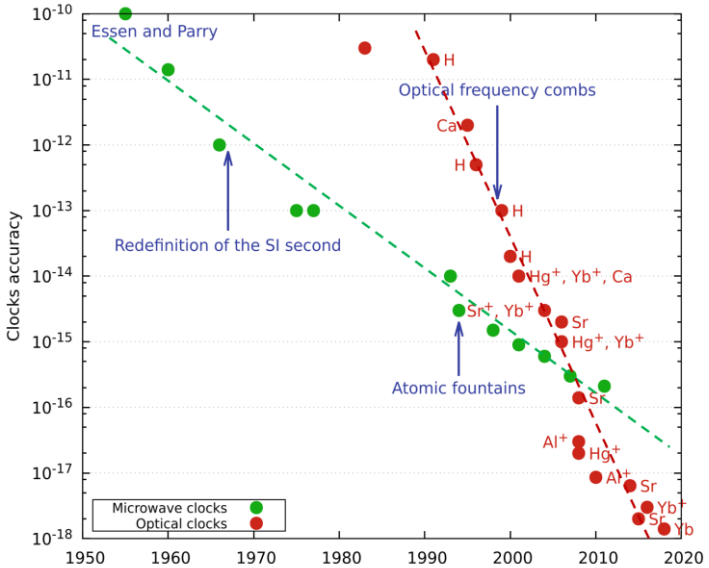


Figure 30 : Evolution de l'incertitude des horloges micro-onde (type césium) vs optiques (Source: P. Delva, Relativistic geodesy, 2019)

[69] La structure hyperfine d'un niveau d'énergie dans un atome consiste en une séparation de ce niveau en états d'énergie très proches (Wikipedia). Ce phénomène s'explique essentiellement par l'interaction entre deux dipôles magnétiques : celui résultant du spin du noyau, et celui lié au spin de l'électron.

[70] https://www.pourlascience.fr/sd/physique/des-regles-de-lumiere-les-peignes-de-frequence-3495.php/

[71] Sont qualifiés d'isotopes les différents types d'atomes d'un même élément chimique qui se distinguent seulement par leur nombre de neutrons présents dans le noyau. Les isotopes d'un même élément gardent en effet le même nombre de protons et d'électrons.

[72] Les fontaines atomiques exploitent les techniques de refroidissement d'atomes par laser, ce qui permet un gain en performance de plusieurs ordres de grandeur par rapport aux horloges conventionnelles à jet thermique : leur stabilité de fréquence relative atteint quelques 10^{-14} à une seconde et leur exactitude quelques 10^{-16}
(Source:https://syrte.obspm.fr/spip/science/references-micro-ondes-et-echelles-de-temps/activites-138)

Au-delà de la précision, d'autres objectifs peuvent motiver la recherche. Aux USA, le NIST[73] travaille sur une horloge qui s'intégrerait dans un composant de la taille d'un grain de café ne consommant que 275 mW[74](Figure 31). Co-financé par la DARPA, le projet bénéficie des avancées en photonique sur puce de silicium pour la réduction de taille, de complexité et de coût des composants. Pour l'instant, la précision obtenue n'est pas encore satisfaisante pour une industrialisation[75].

Les objectifs de très haute précision et portabilité sont aussi au cœur des projets de l'un des consortiums du Quantum Flagship Européen : iqclock[75].

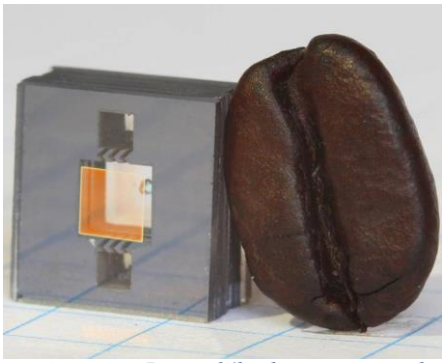


Figure 31: Projet d''horloge atomique de la taille d'un grain de café par le NIST & la DARPA (Source: M.T.Hummon/NIST)

Aujourd'hui les horloges atomiques ont un impact sociétal très important en permettant d'établir et de maintenir synchrones toutes les échelles de temps définies à travers le monde. De nombreuses applications peuvent bénéficier des améliorations de performance apportées par des horloges plus précises[76]. Citons par exemple :

- GPS : La mesure précise du temps est essentielle pour des systèmes de positionnement global car elle permet de calculer avec précision la distance entre les satellites et un récepteur au sol.
- Synchronisation de réseau IT/ Horodatage : La synchronisation et l'horodatage (*timestamping*) précis sont essentiels pour le bon fonctionnement dans un réseau, qu'il s'agisse d'un réseau électrique, de télécommunications, ou de transactions boursières.
- Recherche fondamentale : La Recherche sur la matière noire et d'autres expériences de science fondamentale (LIGO) peuvent bénéficier d'une précision accrue.

4.1.2. Capteur de gravité (gravimètre, gradiomètre), accéléromètre et gyromètre quantique

Selon les lois de la physique quantique, les atomes peuvent se comporter de façon ondulatoire (dualité onde-corpuscule) et donc générer des figures d'interférence lorsque deux ondes de la matière atomique voyagent sur des chemins différents et se rencontrent ensuite (Figure 32).

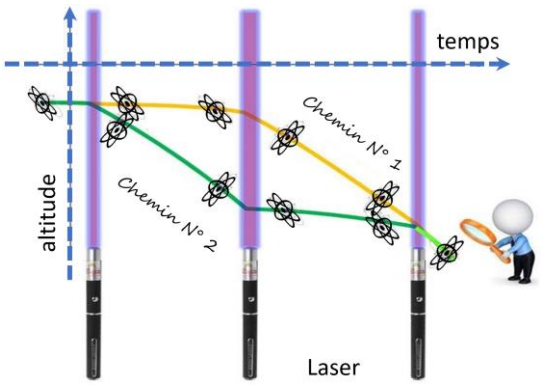


Figure 32: Principe du capteur de gravité à atome froid (Source: Bresson et al, les atomes froids, 2018)

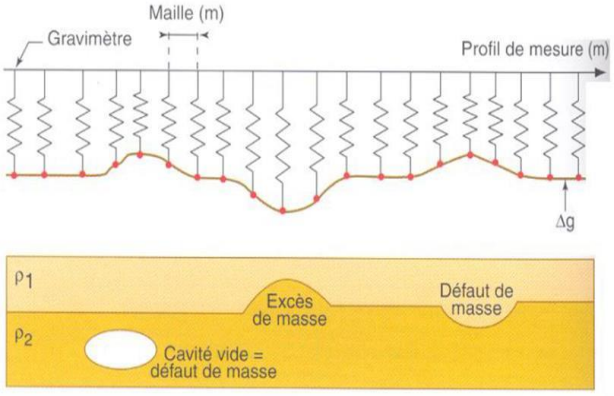


Figure 33: Principe du mesure de gravité

[73] Le National Institute of Standards and Technology est une agence du département du Commerce des États-Unis dont le but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie (Wiki).
[74] A comparer avec l'horloge atomique MuClock vendue par Muquans qui consomme 200W et pèse 135kg.
[75] "Integrated quantum clock", constitué de 6 universités et 6 partenaires industriels :https://www.iqclock.eu/

Cette propriété sert à construire des interféromètres atomiques qui exploitent la sensibilité de la superposition quantique et qui sont par exemple capables de dresser très précisément la carte d'un sous-sol (Figure 33), ou de mesurer des accélérations.

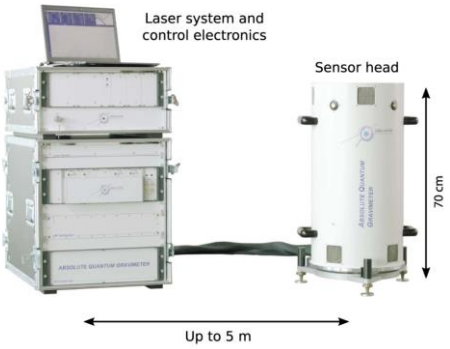


Figure 34: "Absolute Quantum Gravimeter"

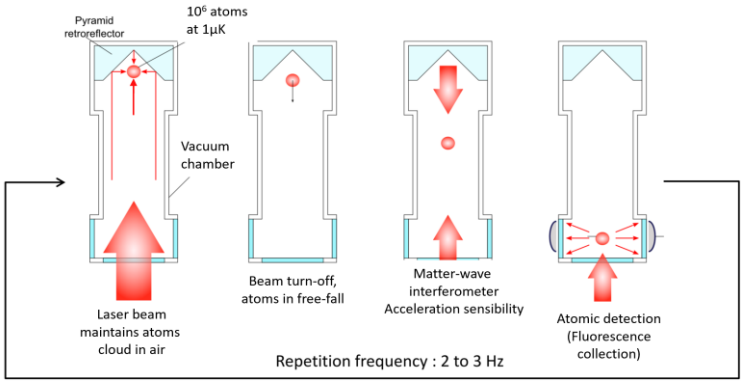


Figure 35: Principe opérationnel d'un gravimètre à atomes froids (Source: Muquans, eost.unistra.fr/uploads/media/G2_Desruelle_01.pdf)

Le procédé consiste à créer une source d'atomes froids en suspension (généralement du rubidium : Rb), dont on prépare l'état à l'aide de lasers, puis à les faire tomber dans le vide en traversant un interféromètre dont les résultats sont ensuite évalués (Figure 35). L'analyse des figures d'interférence par la mesure de déphasage des ondes superposées permet d'estimer avec une grande précision des grandeurs comme la gravité, l'inertie ou la rotation, qui peuvent être ensuite utilisées dans des appareils de navigation inertielle, de stabilisation ou de mesure.

Cette technologie est mature et déjà commercialisée par des sociétés comme Muquans (Figure 34). La précision de la mesure de gravité absolue est de l'ordre de 10^{-9}g [77], et celle d'un gradient de gravité 10^{-10} (gradiomètre).

Certains capteurs utilisent un phénomène particulier (condensats de Bose-Einstein) qui exploite des états quantiques d'intrication pour détecter avec précision des champs proches des surfaces [78]. Cette technologie est aussi une voie explorée depuis plusieurs années[79] pour la miniaturisation d'accéléromètres atomiques sur puce (*« BEC on chip » Bose-Einstein Condensate on chip*) par exemple chez Thalès.

Les domaines d'utilisation des capteurs de gravité sont variés :

- Observation de la Terre/ Recherche sur le climat : Les satellites équipés d'un gravimètre peuvent être utilisés pour mesurer la gravité à travers différentes régions de la terre (masse de glace, niveau d'eau) pour alimenter les modèles climatiques et ou permettre d'anticiper des catastrophes naturelles (sismologie, volcanologie).

- BTP/Génie civil : Des gradiomètres atomiques peuvent permettre de mieux identifier les conduites, les cavités non référencées sur les sites de chantiers ce qui améliore la précision et la sécurité des travaux.

- Exploration géophysique, minière, pétrolière, aquifère : tout objet ou cavité ayant une densité inférieure à celle de son environnement aura une force de gravité locale plus faible. Les gravimètres quantiques peuvent mesurer et cartographier ces dynamiques pour guider l'exploration des ressources naturelles.

- Navigation sans GNSS/GPS : Les accéléromètres et gyroscopes quantiques sont extrêmement précis. Ils pourraient être une alternative : i) pour la navigation dans des environnements où l'accès aux satellites de guidage est impossible (bâtiment, tunnel…), ii) dans des applications susceptibles d'être victimes d'un brouillage ou d'une usurpation du GPS.

4.1.3. Magnétomètre quantique

Les magnétomètres mesurent le champ magnétique. Leurs déclinaisons quantiques sont utilisées pour mesurer des niveaux absolus ou de petites variations du magnétisme avec une grande précision spatiale. Les cas d'usage sont variés : la métrologie (analyse des défauts dans des circuits électroniques, microfissures), l'imagerie médicale ou biologique (magnétoencéphalographie ou MEG, magnétocardiographie ou MCG (Figure 37), bactéries (Figure 36), cellules individuelles [80]), la navigation (e.g. aviation [81]) incluant l'orientation de drones dans des tunnels où les GPS ne fonctionnent pas (Figure 38), la détection de courant et d'objets métalliques mobiles, l'exploration de minerais…

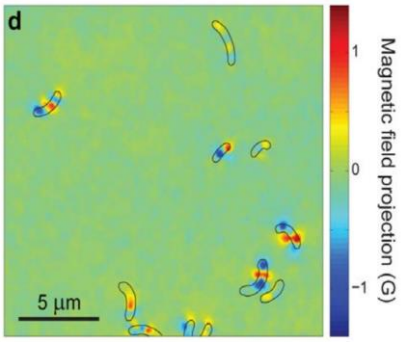


Figure 36: Imagerie magnétique de bactéries (Source: D. Le Sage, et al., Nature 2013)

Figure 37: Appareil de magnétocardiographie

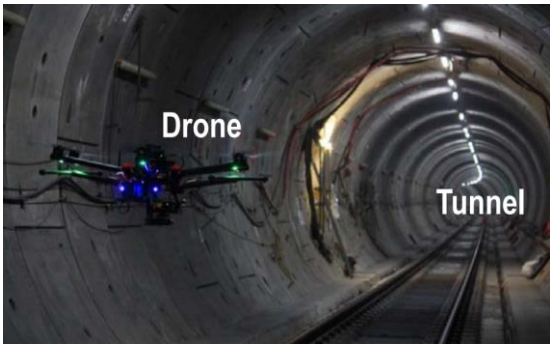


Figure 38: Orientation d'un drone dans un tunnel (Source: HoveringSolutions)

Trois axes techniques sont possibles pour le développement de magnétomètres quantiques :

- Les **atomes froids** sont, pour rappel, des atomes refroidis à très basse température, en général avec des techniques utilisant des lasers et l'effet Doppler. Ils sont également exploités pour construire les qubits à atomes froids utilisés en informatique quantique (§3.2.2). Les magnétomètres à atomes froids isolent une vapeur d'atomes (par exemple, de Rubidium) dans une chambre à vide. Un faisceau laser est appliqué pour orienter les spins des électrons de valence de tous les atomes dans la même direction. Tout champ magnétique externe provoque une oscillation des spins dans un mouvement appelé précession. La précession entraîne une modification de la lumière laser, qui peut être mesurée pour déterminer l'intensité du champ magnétique externe.

- Les **SQUID** (Superconducting QUantum Interference Device) sont utilisés pour mesurer des champs magnétiques très faibles. Nécessitant une température cryogénique, ils sont généralement constitués de deux jonctions Josephson (aussi utilisées dans les qubits supraconducteurs voir §3.2.3) montées en parallèle dans une boucle supraconductrice. Les variations du flux magnétique externe sont converties par le SQUID en des variations de signal électrique mesurées aux bornes de la boucle (Figure 39).

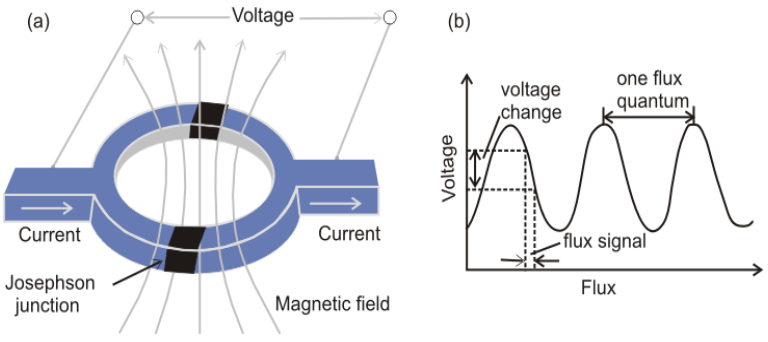


Figure 39: Schéma de principe des magnétomètres SQUID

- Les **centres azote-lacune** (ou **centre NV**), aussi utilisés comme support de qubit en informatique quantique (§3.2.5), sont des défauts présents dans la structure d'un diamant artificiel dans laquelle un atome de carbone a été remplacé par un atome d'azote et à proximité duquel se situe une lacune d'atome de carbone. Une telle structure possède des propriétés de photoluminescence et de spin qui la rendent attractive pour un grand nombre d'applications[82].

  Le fonctionnement des magnétomètres à centre NV reposent sur le comportement de ces spins lorsqu'ils sont soumis à un champ magnétique extérieur. La fluorescence varie elle-même en fonction de l'état des spins, ainsi l'intensité du champ magnétique peut être déterminée en mesurant la variance de la fluorescence. Les centres NV sont également sensibles à d'autres influences externes. Par exemple, ils peuvent être utilisés pour mesurer un champ électrique, ou une température.

  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 à une échelle nanométrique. La pointe peut être déplacée dans l'espace et servir à analyser le magnétisme d'un matériau en 2D. Habituellement, les centres NV sont utilisés en température cryogénique pour pouvoir fonctionner mais certains fonctionnent à température ambiante.

  La figure 40 illustre les produits commercialisés par la startup suisse Qnami qui propose une gamme de produits utilisant ce type de magnétomètre servant à analyser des matériaux ferromagnétiques.

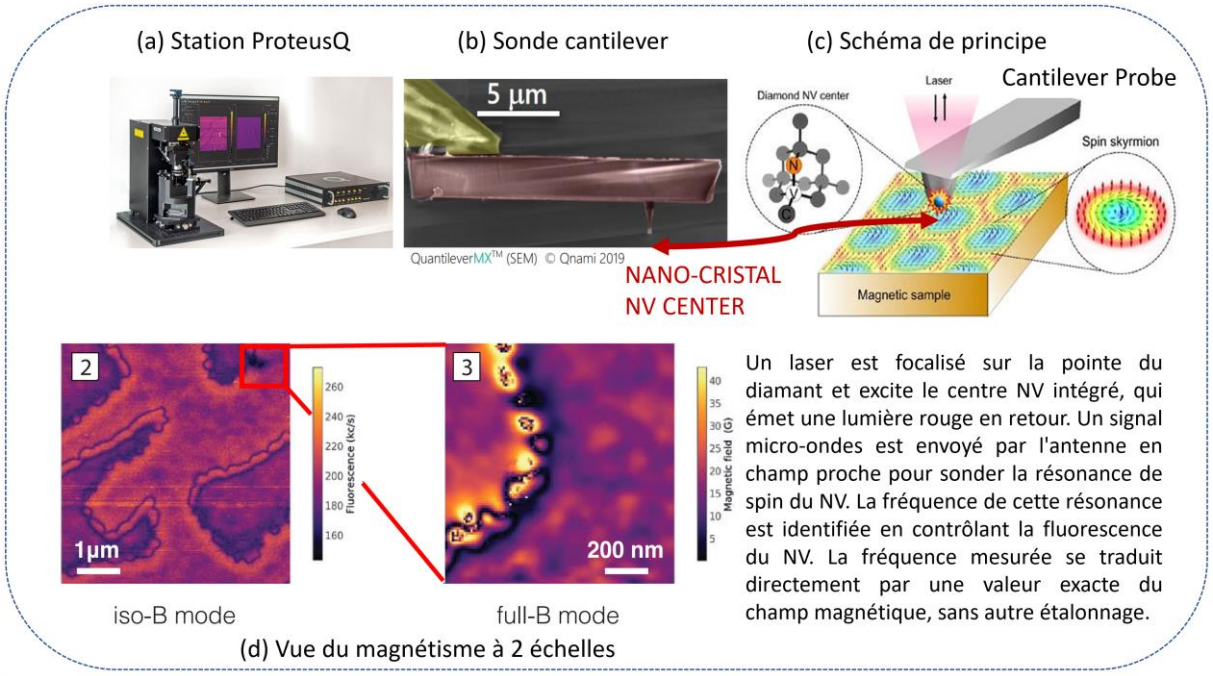


Figure 40: Matériel de la startup Qnami (a) Station ProteusQ intégrant un magnétomètre à centre NV (b) Sonde cantilever disposant d'un diamant à centre NV unique en sa pointe (c) Schéma de principe (d) Vues d'un matériau ferromagnétique aux échelles 1µm et 200 nm (Source: (a)(b)(d) https://qnami.ch/ (c) http://komag.org/2016summer/dhlee.pdf)

Pour terminer ce paragraphe sur les magnétomètres, il est intéressant de comparer sur la figure 41 les performances des trois technologies de magnétomètres quantiques à celles des technologies conventionnelles. La supériorité des systèmes quantiques est notoire mais leur taille supérieure. Comme dans le cas des autres familles de capteurs, la miniaturisation et l'intégration sont un objectif de la recherche actuelle.

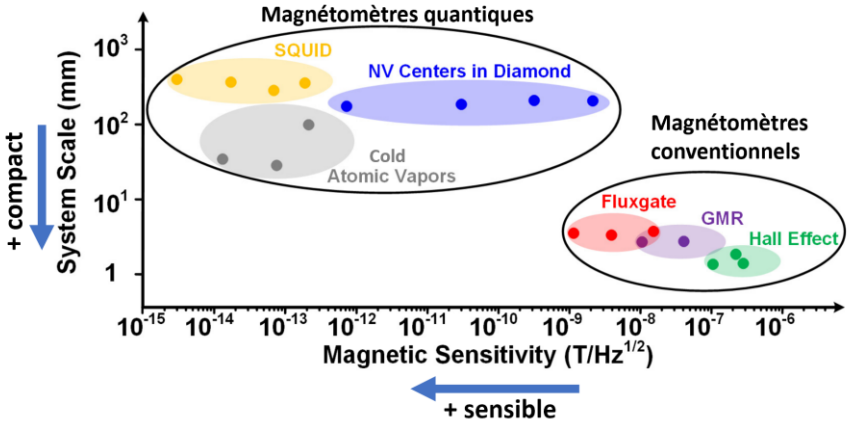


Figure 41: Performance comparée des principales techniques de magnétométrie conventionnelles et quantiques (Source: https://hangroup.mit.edu/wp-content/uploads/2019/03/ISSCC2019_29.2_Published.pdf)

Les magnétomètres quantiques, en particulier ceux à base de centres NV, sont à un stade plus précoce de maturité que les horloges atomiques et les gravimètres à atomes froids décrits précédemment. Par ailleurs, la fabrication homogène de centres NV reste un défi, et des améliorations supplémentaires de la sensibilité sont nécessaires pour de nombreuses applications.

4.1.4. Thermomètre quantique

Les centres NV, qubits décidément polyvalents, sont particulièrement performants pour la mesure de température. Les capteurs miniaturisés offrent une précision de l'ordre du milli-Kelvin ainsi qu'une très grande résolution spatiale (Figure 42). C'est une technologie, biologiquement compatible, qui permet par exemple de déterminer la température au sein de cellules vivantes [83].

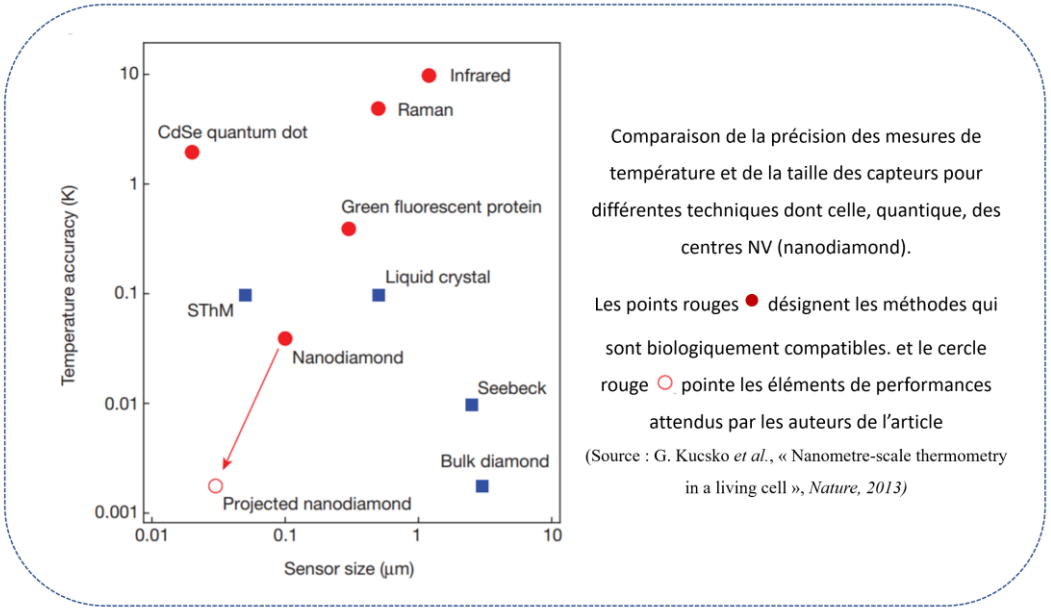


Figure 42: Précision de température et taille de capteurs comparées pour différentes techniques (Source: [82])

S'agissant de la mesure de température dans la matière biologique par fluorescence, d'autres technologies peuvent être employées, par exemple, celle des quantum dots[76][84]. Et pour un environnement à température cryogénique, un dispositif de type SQUID, déposé à la pointe d'une sonde nanométrique, permet d'atteindre une grande précision spatiale et thermique adaptée à l'étude des systèmes quantiques[85] refroidis à très basse température.

[76] Le quantum dot est une nanostructure de semi-conducteurs dans laquelle des électrons peuvent être confinés spatialement.

Publiée cette année, citons enfin l'étude[86] qui décrit l'utilisation d'un thermomètre photonique offrant une résolution de 0.25mK sur une plage de température allant de 10°C à 90°C. C'est ici un phénomène d'interférence quantique particulier qui est exploité. La thermométrie photonique fait également l'objet d'un projet mené par le NIST [87]. L'emploi de capteurs photoniques se révèlerait être une solution de mesure peu coûteuse, légère, portable, résistante aux interférences électromagnétique et multi-usage (utilisable aussi pour des mesures de pression et de vide).

4.1.5. LiDAR/RADAR quantique

Le LiDAR (Light Detection And Ranging) est une technique de mesure à distance fondée sur l'analyse des propriétés d'un faisceau de lumière renvoyé vers son émetteur. À la différence du radar qui emploie des ondes radio (ou du sonar qui utilise des ondes acoustiques), le LiDAR utilise de la lumière (visible, infrarouge ou ultraviolet) dont la source est quasiment toujours issue d'un laser[77].

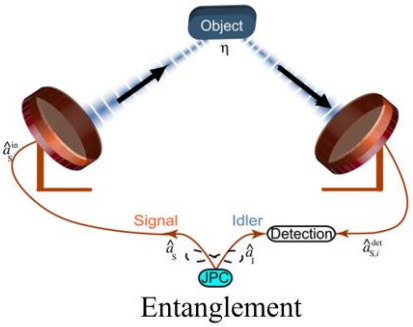


Figure 43: Implémentation d'un radar quantique (Source: Barzanjeh et al, « Microwave quantum illumination using a digital receiver », 2020)

Le LiDAR quantique peut utiliser des détecteurs à photon unique ou, dans certains cas, des photons intriqués qui permettent alors aux systèmes de fonctionner dans des conditions de visibilité réduite.

Le radar quantique a également fait l'objet de théories[88] ou été simulé [89][78] et serait en développement[79]. Ce système consiste à faire rebondir sur un objet la moitié d'une série de paires de photons intriqués, puis à les comparer lorsqu'ils reviennent à ceux qui sont restés en attente. Cette méthode permet de distinguer le rayonnement des photons intriqués des autres sources de bruit afin de repérer, par exemple, des avions furtifs[90]. Elle est aussi désignée dans la littérature par le terme *illumination quantique* [91].

Figure 44: Réalisation de LiDARs quantiques (Source: Single-Photon Lidar for atmospheric detection, Haiyun Xia et al, 2019)

Les applications du LiDAR concernent tout ce qui peut avoir trait à des mesures dans l'atmosphère (détection de la pollution de l'air, mesure du vent et efficacité des éoliennes, météorologie (pluie, gel…) et utilisation en agriculture). L'emploi dans des véhicules autonomes est à plus long terme, tandis que l'imagerie pour la détection des fuites de gaz plus proche[80]. Déjà existants, des LiDARs embarquables dans des drones servent à la détection précise du vent (Figure 44). Par ailleurs, une équipe chinoise de chercheurs a communiqué en 2019 sur une démonstration d'imagerie 3D longue distance (45km), par l'utilisation d'une caméra LiDAR à photon unique et, d'algorithmes de traitement optimisés [92].

L'usage potentiel du RADAR quantique dans le secteur de la Défense rend l'information rare, et sa commercialisation ne se fera certainement qu'à long terme.

4.1.6. Imagerie quantique

L'imagerie quantique est un autre domaine où peuvent s'exprimer les propriétés des états non-classiques de la lumière pour permettre une amélioration des performances (e.g. la résolution). En quelques mots, les exemples incluent la technique des images fantômes qui améliore le rapport signal/bruit pour les applications dans un environnement bruité (faible intensité du signal à mesurer), la microscopie

[77] https://fr.wikipedia.org/wiki?curid=299490
[78] Les auteurs parlent d'illumination quantique, terme désignant les radars quantiques utilisant des photons intriqués, ici sur des longueurs d'ondes dans la gamme des micro-ondes
[79] https://www.popularmechanics.com/military/research/a22996/china-quantum-stealth-radar/
[80] https://www.qlmtec.com/#technology

multiphotons, la tomographie par cohérence optique, l'interférométrie quantique, la lithographie quantique…chacune faisant appel à des mécanismes quantiques comme l'intrication de qubits.

L'activité commerciale autour de l'imagerie quantique est plus limitée que celle des autres secteurs de la métrologie quantique, mais elle pourrait tout à fait trouver des applications de niche dans les prochaines années.

4.1.7. Les challenges et progrès à venir

Comme nous venons de le voir, le portefeuille d'applications dans le domaine de la métrologie et des capteurs quantiques est diversifié. L'apport du quantique et les progrès à venir seront spécifiques à chaque application, car les avantages en termes de performances et de coûts devront être démontrés par rapport aux techniques conventionnelles particulières.

Si l'on devait donner des étapes-clés communes, ce serait (a) une **intégration plus poussée** des systèmes quantiques (par exemple sur puce) qui constituerait une avancée notable pour faciliter (b) la mise au point de dispositifs de taille, de poids, de puissance et de coût réduits (**SWaP-C**) ; (c) **l'amélioration de la stabilité** des mesures.

Concernant les points (a) et (b), citons la démarche du NIST nommée « NIST On A Chip »(NOAC)[81] qui dans le domaine spécifique de la métrologie et des capteurs vise à développer des dispositifs quantiques très précis, ultra-compacts (puce voire plus petits), peu coûteux et à faible consommation énergétique, pour l'industrie et les particuliers.

L'aspect coût légitime la priorité donnée à l'utilisation de la photonique ou de technologies à base de silicium, dont les procédés de fabrication, déjà utilisés, sont bien connus (circuits intégrés, MEMS[82]). Neuf domaines d'applications sont pour l'instant concernés (Figure 45).

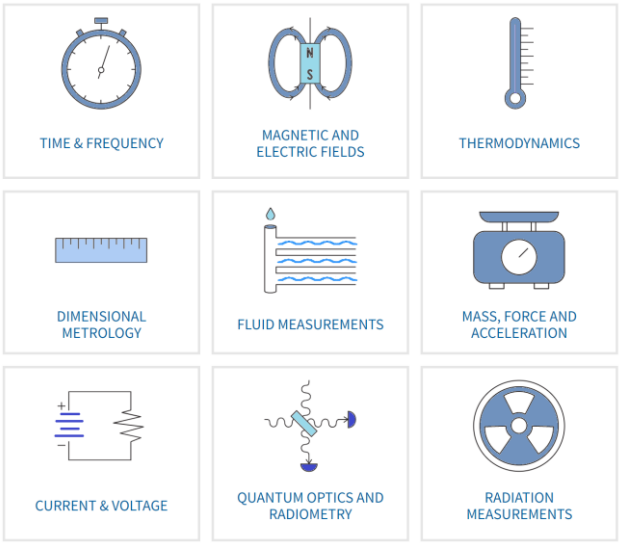


Figure 45: Les 9 domaines d'application du projet NOAC (Source: https://www.nist.gov/noac)

Sur le point (c) mentionnons que la stabilité des mesures ou l'instabilité n'est pas un point d'attention spécifique à la métrologie car elle découle directement de la fragilité des états quantiques (décohérence), du bruit[83], des erreurs… qui touchent donc aussi bien l'informatique que les communications quantiques, domaine que nous développons dans le chapitre suivant.

[81] https://www.nist.gov/noac
[82] Systèmes micro-électromécaniques.
[83] Le bruit quantique affectant la mesure impose une limite sur la précision maximale accessible à partir d'états quantiques classiques: la **limite quantique standard** (**SQL**). La métrologie quantique cherche à utiliser les caractéristiques propres à la mécanique quantique pour la dépasser et se rapprocher le plus possible de la limite ultime, physiquement non franchissable, appelée **limite de Heisenberg**. Pour cela les scientifiques font appel à des "astuces quantiques" telles que la compression (de spin , de la lumière) et l'intrication (Source: [93])

4.2. Cryptographie et télécommunications quantiques

La société moderne s'alimente de l'échange d'informations à grande échelle. La sécurisation des données sensibles dans le monde entier devient un impératif de plus en plus incontournable. La boîte à outils mathématiques, aujourd'hui largement utilisée pour cette tâche, peut être complétée par l'application des principes de la physique quantique.

Les photons - parfaitement adaptés à la transmission d'informations quantiques via des fibres optiques ou l'espace libre - combinés aux propriétés de la mesure d'observables ou de l'intrication sont le fondement d'un champ d'application majeur des technologies quantiques : les **télécommunications quantiques.** L'un des objectifs principaux de celles-ci est le développement de réseaux protégés de la menace potentielle et paradoxale que représente, à terme, l'exploitation de la puissance de calcul d'un ordinateur quantique[84] à des fins malicieuses[85].

Au-delà de la protection de l'information aujourd'hui stockée ou transitant sur les réseaux, les télécommunications quantiques pourront jouer un rôle important dans la protection des réseaux 5G en cours de déploiement. Le nombre d'appareils et de capteurs s'y connectant[94], et par là même la quantité de données sensibles circulant, devraient augmenter de façon spectaculaire[86].

Le domaine des télécommunications quantiques combine essentiellement deux objectifs. Le premier relève de la modification des techniques traditionnelles et/ou de l'utilisation des technologies quantiques pour assurer la transmission sécurisée des informations classiques (suite de bits « 0 » ou « 1 »). Il s'agit essentiellement ici de développer des techniques de cryptographie résistantes (PQC, QKD, QRNG) aux attaques d'un ordinateur quantique[84] capable de mettre en œuvre de puissants algorithmes de décryptage. C'est aujourd'hui l'axe le plus avancé puisque des solutions commerciales existent depuis plusieurs années. Le deuxième objectif est, dans un avenir plus lointain, la transmission d'informations quantiques, généralement dans le cadre d'une informatique quantiques distribuée au sein d'un réseau de plusieurs calculateurs quantiques, dont l'avènement, possible à grande échelle à long terme, conditionnera peut-être même la création d'un internet quantique (Figure 46).

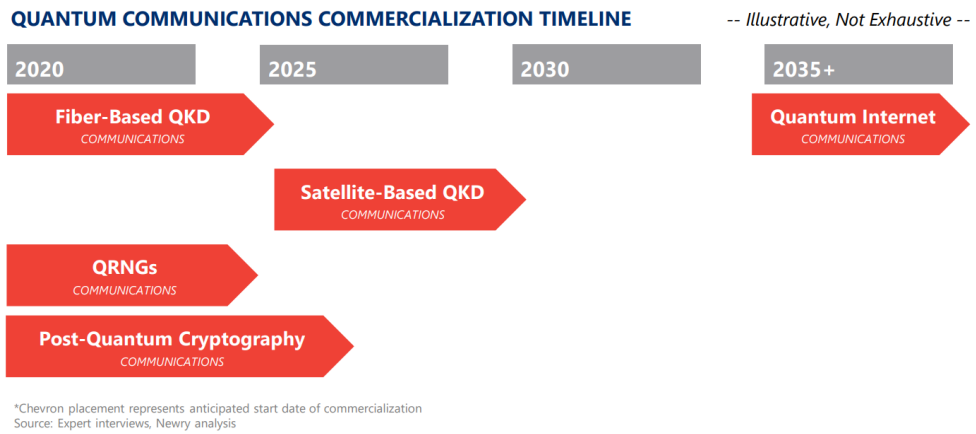


Figure 46: Calendrier indicatif pour le déploiement des technologies de communications quantiques (Source: [72])

Du point de vue des systèmes, les deux concepts se chevauchent et font largement appel à des dispositifs physiques. Nous abordons ce chapitre en précisant la nature de la menace quantique pour la cybersécurité puis détaillerons les nouveaux outils cryptographiques (tant conventionnels que quantiques) dont le déploiement permettrait d'atténuer le risque: i) la cryptographie post-quantique (PQC[87]), conventionnelle, qui fait appel à de nouveaux modèles mathématiques de chiffrage,

[84] Dans le futur, des avancées d'autres technologies ou dans l'algorithmie pourraient aussi conduire à des calculateurs exponentiellement plus rapides que ceux existants aujourd'hui
[85] E.g. pour casser les clés chiffrant les informations circulant sur les réseaux de communications traditionnels (RSA…)
[86] Gartner estime que le nombre total de bases de terminaux 5G IoT installées serait de 48,6 millions en 2023 [95].
[87] Post-Quantum Cryptography

ii) les protocoles physiques de cryptographie quantique, avec en particulier la distribution quantique de clés (QKD[88]). Nous terminerons par les applications liées à un futur web quantique capable de distribuer des états quantiques telles que l'intrication, et de connecter des appareils quantiques distants.

4.2.1. La cryptographie et la menace quantique

La **cryptologie** est étymologiquement la science du secret. Son objectif est de protéger de manière sûre de l'information sensible, qu'elle soit stockée, ou transmise sous forme de message entre un émetteur et un récepteur. La cryptologie se scinde en deux sous-domaines : la **cryptographie**, qui sécurise les informations transmises et la **cryptanalyse** qui cherche à les décrypter par analyse ou attaque.

La cryptographie comprend elle-même deux familles de techniques[89] (ou cryptosystèmes) : la **cryptographie symétrique** ou **à clé secrète**, et **la cryptographie asymétrique** ou **à clé publique**. La différence fondamentale qui distingue la cryptographie symétrique de l'asymétrique est que la première permet le cryptage et le décryptage du message avec la même clé secrète, tandis que la seconde utilise la clé publique pour le chiffrement et une clé privée pour le déchiffrement[90]. Ici, une condition indispensable pour que l'information soit protégée est qu'il soit *calculatoirement très difficile*[91] *(*dans l'idéal *impossible)* de déchiffrer à l'aide de la seule clé publique, en particulier de reconstituer la clé privée à partir de la clé publique, c'est-à-dire que les moyens de calcul disponibles et les méthodes connues au moment de l'échange (et le temps pendant lequel le secret doit être conservé) ne le permettent pas. C'est le concept de fonctions mathématiques à sens unique qui est exploité aujourd'hui dans ces protocoles de clés publiques largement usités dans la sécurisation des systèmes d'échange d'informations. Le problème de factorisation de grands nombres entiers en nombres premiers est ainsi utilisé par l'algorithme RSA[92] tandis que celui du logarithme discret est utilisé pour l'échange de clés Diffie-Hellman (ECDH) et la cryptographie sur les courbes elliptiques(ECC[92]).

L'intérêt pour la cryptographie quantique et post-quantique (PQC) a débuté par la publication en 1994 de l'algorithme[93] de Peter Shor [97]. Les codes secrets, inviolables, ne le seraient plus. Un futur ordinateur quantique capable de mettre en œuvre l'algorithme de Shor pourrait factoriser les nombres entiers ou résoudre les problèmes de logarithme discret exponentiellement plus rapidement qu'un ordinateur classique[98], rendant caduques les protocoles utilisant ces problèmes supposés jusqu'alors *intractables*. Les communications Internet, qui font aujourd'hui largement appel au protocole RSA[94] conjointement aux protocoles ECC, ECDH[95], AES (système symétrique à clé privée) [99], sont en danger, tout comme le sont donc les transactions bancaires, le e-commerce, les données de santé, etc…

Depuis le travail séminal de P. Shor, de nombreuses études ont cherché à quantifier le temps de calcul nécessaire à un ordinateur quantique pour atteindre cet objectif malveillant. Le tableau de la figure 47 résume les *meilleurs performances actuelles supposées*. Il est important à ce stade de préciser qu'aucun ordinateur quantique ayant les caractéristiques demandées n'existe aujourd'hui. En particulier, comme on peut le voir, le nombre de qubits physiques nécessaires est de l'ordre de plusieurs millions tandis qu'à ce jour les ordinateurs quantiques de Google et IBM n'en proposent qu'une cinquantaine. Nous reviendrons sur ce point dans la section suivante.

Ce sont essentiellement les systèmes de cryptage asymétrique (ECC, RSA) qui sont menacés par un ordinateur quantique programmé avec l'algorithme de Shor. En effet, si pour renforcer la sécurité d'un

[88] Quantum Key Distribution.
[89] Le *hashing* utilisé pour les signatures numériques ou les codes d'authentification ne seront pas abordées ici.
[90] P. Guillot, *La cryptologie - L'art des codes secrets*, Librairie Eyrolles [96].
[91] C'est le concept lié à l'anglicisme « intractabilité » (Source wikipedia)
[92] Le chiffrement RSA a été créé en 1977 et ECC en 1985 (Source: wikipedia)
[93] Avant même que les chercheurs aient été capables de créer un qubit contrôlable, des mathématiciens ou physiciens comme D. Deutsch, R. Jozsa, P. Shor ou L. Grover ont conçu des algorithmes quantiques et ainsi attiré l'attention sur le sujet (leurs fonctionnements sont décrits dans le livre de référence de Nielsen & Chuang[70]) ou en annexes 8 et 9 pour les deux derniers.
[94] En 2018, 85,2% des certificats sécurisant des échanges web ont utilisé le protocole RSA-2048 : notary.icsi.berkeley.edu
[95] Échange de clé Diffie-Hellman basé sur les courbes elliptiques (courbes de degré 3 ayant certaines propriétés mathématiques)

système privé symétrique comme l'AES il suffit d'augmenter la longueur de la clé[96], ceci n'est pas une mesure suffisamment dissuasive pour les cryptosystèmes asymétriques en usage aujourd'hui.

Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required[a]	Time Required to Break System[b]	Quantum-Resilient Replacement Strategies
AES-GCM	Symmetric encryption	128	128	Grover's algorithm	2,953	4.61×10^6	2.61×10^{12} years	
		192	192		4,449	1.68×10^7	1.97×10^{22} years	
		256	256		6,681	3.36×10^7	2.29×10^{32} years	
RSA	Asymmetric encryption	1024	80	Shor's algorithm	2,05	8.05×10^6	3.58 hours	Move to NIST-selected PQC algorithm when available
		2048	112		4,098	8.56×10^6	28.63 hours	
		4096	128		8,194	1.12×10^7	229 hours	
ECC Discrete-log problem ECDH	Asymmetric encryption	256	128	Shor's algorithm	2,33	8.56×10^6	10.5 hours	Move to NIST-selected PQC algorithm when available
		384	192		3,484	9.05×10^6	37.67 hours	
		521	256		4,719	1.13×10^6	55 hours	
SHA256	Bitcoin mining	N/A	72	Grover's Algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iterations	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from password-based authentication

[a]: Estimations approximatives. Le nombre de qubits physiques requis dépend de plusieurs hypothèses, notamment de l'architecture sous-jacente et des taux d'erreur. Les hypothèses considérées ici comprennent un réseau bidimensionnel (2D) de qubits avec des interactions possibles avec les voisins les plus proches, un taux d'erreur effectif de 10^{-5}, et la mise en œuvre d'un algorithme de correction d'erreur (code de surface) utilisant les qubits physiques pour créer les qubits logiques

[b]: Estimations approximatives se basant sur un ordinateur quantique utilisant des portes logiques quantiques fonctionnant à une fréquence de 5 MHz

Figure 47: Estimations de la résilience quantique des cryptosystèmes actuels, sous diverses hypothèses de paramètres de sécurité, taux d'erreurs et de codes correcteurs d'erreurs (Source: Quantum Computing: Progress and Prospects (2019)[98])

Il faudrait moins de 4 heures pour casser la clé d'une communication RSA-1024. Moins de 29 heures et 9 millions de qubits seraient nécessaires pour briser un code RSA-2048 bits, référence aujourd'hui en matière de sécurité. Plus inquiétant encore, Gidney&Ekera[100] ont publié en 2019 une étude, selon laquelle factoriser des entiers RSA-2048 ne prendrait que 8 heures en utilisant 20 millions de qubits physiques.

4.2.2. L'horizon de la menace quantique et l'inégalité de Mosca

Reprécisons qu'un ordinateur quantique capable de telles prouesses n'existe pas. L'évaluation du calendrier de la menace pour la cybersécurité est difficile en raison des obstacles scientifiques et techniques liés à la construction d'un ordinateur quantique fonctionnel. Une fourchette de 7 à 20 ans a été suggérée pour un tel ordinateur, par exemple dans [98], [101] tandis qu'une étude de 2019, recueillant l'opinion de 22 experts[102], indique comme on peut le voir sur la figure 48 : i) qu'une majorité (20 sur 22) s'accorde sur une chance faible mais non négligeable dans les 5 ans (~1-5%), ii) mais que le risque est significatif dans les 10 ans (~5-30%).

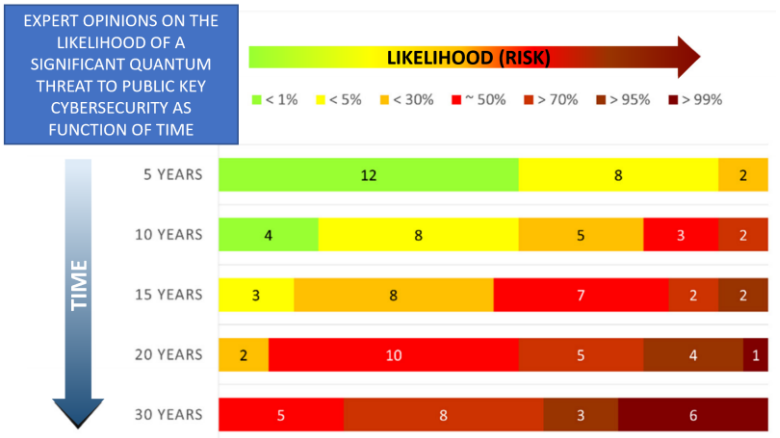


Figure 48: Opinions d'experts sur la chronologie de la menace pour la cybersécurité (Source: Global Risk Institute, https://globalriskinstitute.org/publications/quantum-threat-timeline/

[96] L'algorithme quantique de recherche (par « force brute ») de Grover, utilisable pour décrypter des messages chiffrés par clé symétrique ne génère, par rapport à une méthode traditionnelle, qu'une accélération quadratique (temps de calcul augmente en $\sqrt{N}$, au lieu de N) et non pas exponentielle (log(N) au lieu de N) comme celui de Shor, applicable aux clés asymétriques.

Des scénarios plus courts sont également possibles: i) des programmes majeurs lancés par certaines nations (cf. Annexe 4) pourraient peut-être réduire ce délai à 5 ou 7 ans, ii) des schémas alternatifs basés sur des dispositifs quantiques spéciaux ou des avancées majeures pourraient bouleverser ces estimations.

Si un tel ordinateur n'existe pas aujourd'hui, il n'en reste pas moins que cette menace future s'applique déjà aujourd'hui aux données interceptées et stockées[97] en vue d'un décryptage futur. Ainsi, même si une tierce-partie hostile ne disposait d'un ordinateur quantique qu'en 2030, mais qu'elle intercepte et stocke aujourd'hui des données dont la durée de confidentialité est de 10 ans ou plus, elle serait en mesure de décrypter les informations à ce moment-là.

Par ailleurs, le passage à une cryptographie résistante à une attaque quantique est un défi en soi, car il nécessite l'établissement de normes, le développement et le déploiement de solutions matérielles et logicielles, avec en particulier la migration des systèmes existants... ce qui prendra du temps.

Comme l'a formulé en 2015 Michele Mosca, chercheur et entrepreneur réputé[105], l'urgence pour une organisation spécifique (entreprise, gouvernement,…) d'achever la transition de leurs systèmes vers une cryptographie « quantum-safe » repose sur une inégalité utilisant trois paramètres simples :

- **La durée de vie des données (X):** le nombre d'années pendant lesquelles les données doivent être protégées (10 ans , 20 ans ou 50 ans),
- **la durée de migration (Y)**: le nombre d'années nécessaires pour migrer le système vers une solution « quantum-safe »,
- **le calendrier de la menace (Z)**: le nombre d'années avant qu'un ordinateur quantique universel suffisamment puissant ne soit disponible,

Si X+Y > Z, alors il y a urgence à agir comme cela est illustré sur la figure 49.

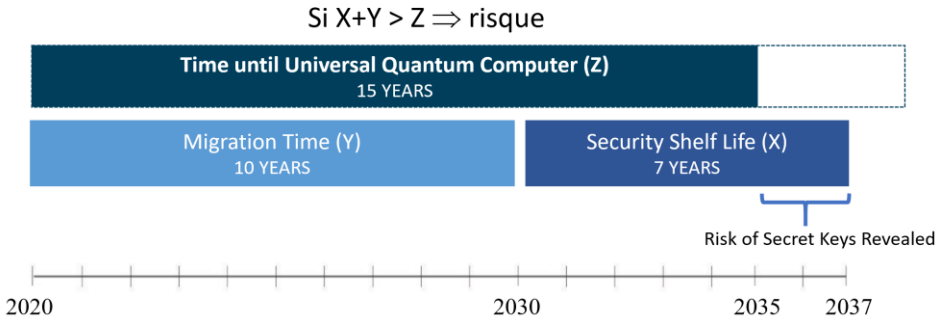


Figure 49 : Modèle de Mosca - illustration d'un calendrier défavorable
(Source: Quantum Computing: Progress and Prospects. 2018.)

Dans les faits, alors que nous sommes probablement à une décennie ou plus d'un ordinateur quantique capable de casser le standard RSA-2048, Recherche et Industrie travaillent activement sur de nouvelles solutions pour résister aux attaques de l'informatique quantique. Certaines applications sont disponibles et certains utilisateurs finaux migrent déjà aujourd'hui vers des solutions « quantum safe ». Deux approches complémentaires sont privilégiées : i) la **cryptographie post-quantique** (PQC) qui offre des solutions logiciels basées sur de nouveaux modèles mathématiques sans faire appel au quantique ; ii) la **distribution quantiques de clés (QKD)**, faisant appel à du matériel physique qui commence à être disponible mais pour lequel des développements sont toujours en cours.

[97] Au-delà des révélations de Snowden sur le stockage des informations provenant d'internet par la NSA (par ex : https://fr.wikipedia.org/wiki/Révélations_d'Edward_Snowden, des nations comme le Kazakhstan sont réputées intercepter tout le trafic sécurisé d'internet (https) [103], [104] ou au moins dans leur pays.

4.2.3. La cryptographie post-quantique

La cryptographie conventionnelle basée sur les mathématiques n'est pas sans défense face à l'informatique quantique. Depuis 2006[98], l'objectif que se sont donnés les spécialistes, avec la cryptographie post-quantique (aussi appelée **PQC** ou cryptographie « **quantum safe** »), est de développer des solutions logicielles alternatives capables de résister aux assauts des ordinateurs quantiques (e.g. algorithmes de Shor et de Grover). **Ces protocoles algorithmiques sont purement basés sur de nouveaux modèles mathématiques et n'intègrent aucun système de physique quantique.** Ils remplaceraient donc par exemple les modèles mathématiques utilisés dans les protocoles RSA pour sécuriser l'échange de clés.

La figure 50 résume les 5 approches les plus robustes proposées par les spécialistes de PQC. On peut y rajouter les codes symétriques standards (type AES) dont la sécurité peut être renforcée en augmentant la taille de clés. Le NIST[99] a lancé en 2016 un programme de formalisation et de standardisation des protocoles PQC qui a donné lieu à un concours international débuté en 2017 avec initialement 69 algorithmes candidats présentés par des organisations de 25 pays répartis sur les 6 continents. En juillet 2020, le NIST a annoncé avoir terminé l'analyse des 26 algorithmes[100] retenus pour le deuxième tour en janvier 2019. Le troisième round débute ainsi avec 7 finalistes et 8 substituts[101] et devrait durer de 12 à 18 mois. Il débouchera sur la publication d'un draft de recommandations en 2022 et une formalisation des normes en 2024.

CRYPTOSYSTEMES PQC

Codes linéaires aléatoires (code-based) Cryptage et signature	Le code McEliece est un exemple d'algorithme existant depuis 40 ans et dont la communauté a donc pu éprouver la robustesse. Ce système génère des clés publiques cent fois plus grandes que pour un code RSA standard (~ 80 Ko), mais le chiffrement et le déchiffrement des messages peuvent se faire rapidement. Le déchiffrement est inaccessible au quantique à ce jour même si, pour lui résister, il faudrait une clé beaucoup plus grande ~1 Mo.
Arbres de hashage (hash-based) Signature	Comme pour les codes linéaires aléatoires, les premiers travaux sont antérieurs à l'apparition de la menace quantique. Ces algorithmes sont essentiellement utilisés pour la signature des messages. Bien connus de la communauté, les arbres de Merkle ont l'avantage de fonctionner avec des clés relativement petites mais présentent quelques défauts qu'une nouvelle approche alternative nommée SPHINCS vise à corriger au prix toutefois de besoins plus élevées (taille clés et calculs).
Réseaux euclidiens (lattice-based) Cryptage et signature	Il s'agit d'une famille d'approches, mathématiquement très complexes, basées sur la difficulté de résoudre le problème du plus court vecteur dans les treillis. Les principaux algorithmes candidats portent des noms évocateurs tels que New Hope ou Frodo. L'avantage de ces méthodes est d'utiliser des clés publiques de petites tailles mais elles ont par contre l'inconvénient d'être souvent protégés par des brevets et donc potentiellement couteuses à l'emploi.
Inversion de polynôme multivarié (multivariate) Cryptage et signature	Les méthodes sont ici liées à la difficulté de résoudre des systèmes d'équations. De nombreuses propositions de ce type ont été brisées avec succès, ce qui a permis d'avoir une grande expérience dans l'étude de ces problèmes. Le MQDSS est un nouveau candidat. D'autres variantes telles que HFEBoost ont été utilisées dans des essais sur le terrain avec l'armée française. Les clés publiques sont assez grandes (~130Ko).
Isogénies (isogeny–based) Cryptage	Mathématiquement très complexes, les isogénies sont une version renforcée des codes actuels utilisant les courbes elliptiques comme le protocole ECDH couramment employé. Avec l'utilisation de courbes « super-singulières » la méthode serait résistante au quantique. Les clés sont de petites tailles, mais les calculs sont coûteux ce qui pourrait être un problème pour le déploiement et l'emploi pour des objets connectés (IoT).
Cryptage par clés symétrique (symetric) Cryptage et authentification	Au final le cryptage par clé symétrique (type AES) est peu impacté par la menace potentielle de décryptage par un ordinateur quantique pour peu que les clés soient i)longues (dans l'idéal au moins de la longueur du message à coder), ii) choisies réellement aléatoirement et iii) changées à chaque message. Dans ce cas le système assurerait une sécurité inconditionnelle (chiffre de Vernam / masque jetable).

Figure 50: Familles de codes PQC réputées résister aux assauts quantiques

[98] PQCrypto, premier workshop international se tient alors en Belgique pour étudier les moyens de contourner les assauts potentiels d'ordinateurs quantiques à une époque où l'on sait à peine faire fonctionner deux qubits ensemble.
[99] Le National Institute of Standards and Technology est une agence du département du Commerce des États-Unis dont le but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie (Wiki).
[100] https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round
[101] Listes des 7 finalistes et 8 suppléants : https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement

Notons que si la procédure du NIST pouvait être considérée comme globale, une initiative chinoise, visant elle aussi à définir des normes pour la PQC, a été lancée en 2018 par l'association chinoise de recherche cryptologique (CACR). Son calendrier est plus agressif puisque les résultats ont déjà été annoncés[102], toutefois son périmètre d'application est moins ambitieux que celui du NIST.

Chacun des protocoles PQC évoqués a ses avantages et ses inconvénients. D'autres facteurs sont susceptibles de compliquer ou modifier la définition des normes futures :

- d'une manière générale la taille des clés et signatures utilisées sera significativement supérieure aux standards conventionnels actuels
- l'utilisation de ces protocoles sur des objets connectés pourrait être problématique (mémoire, énergie, batterie),
- certaines des méthodes sont propriétaires, protégées par des brevets, donc potentiellement coûteuses à l'usage,
- il n'y pas de garantie qu'un protocole aujourd'hui jugé comme résistant à des assauts quantiques ou conventionnels ne le reste dans le futur,
- les nouvelles méthodes pourraient être sensibles à des attaques de type « déni de service » i.e. par saturation de la mémoire des appareils alors qu'ils tentent de traiter des clés PQC.

Considérons à présent l'emploi des technologies quantiques proprement dites, dans la sécurisation des communications.

4.2.4. La cryptographie quantique : distribution quantique de clés (QKD)

Les techniques de cryptographie quantique, utilisant le matériel[103] de la physique quantique, fournissent une approche complémentaire à la PQC pour la sécurité des communications. Elles assurent une inviolabilité théorique des communications en permettant à deux parties d'échanger d'abord une clé de cryptage puis ensuite des informations chiffrées par cette clé.

Généralement, les systèmes sous-jacents reposent sur des générateurs quantiques de nombres aléatoires (QRNG) pour la génération de clés secrètes et sur des protocoles de distribution quantique de ces clés (QKD) pour leur transmission sécurisée, tous deux résultant de la seconde révolution quantique (Figure 51).

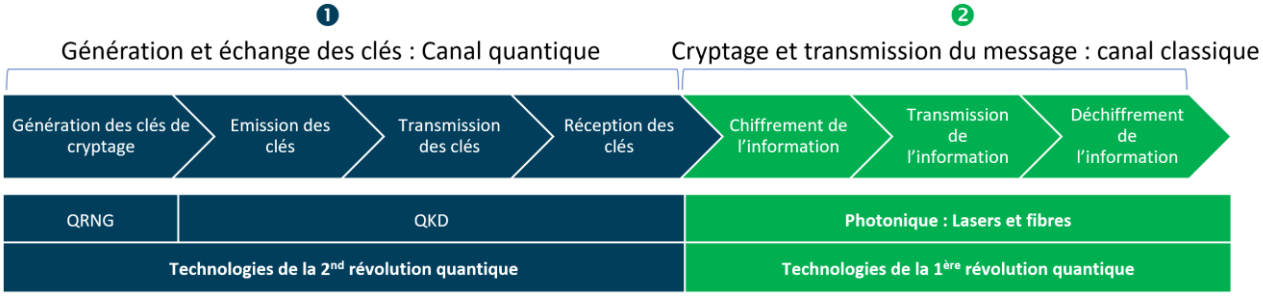


Figure 51: Technologies quantiques et communications cryptées

Une fois les clés distribuées, la suite des protocoles s'apparente à celle des cryptosystèmes symétriques à clés secrètes classiques.

4.2.4.1. Générateur quantique de nombres aléatoires (QRNG)

La génération de séquences de bits ou nombres véritablement aléatoires, est fondamentale pour de nombreuses applications scientifiques et techniques, comme par exemple pour les simulations

[102] https://www.cacrnet.org.cn/site/content/854.html
[103] Au sens propre et figuré, s'agissant d'une part des lois de la physique quantique et aussi d'appareils mettant en œuvre la manipulation d'objets ou vecteurs quantiques (photons, électrons, …)

numériques. Dans de nombreux cas, des algorithmes de génération pseudo-aléatoire, mais déterministes, sont employés pour produire des suites de nombres semblant suffisamment désordonnés pour que l'on puisse penser, sans un examen rigoureux, qu'ils ont été tirés au hasard. Cela n'est toutefois pas suffisant pour de nombreuses applications comme pour la sécurisation de l'information et la cryptographie. Les clés de cryptage générées par ces suites, qui ne sont pas vraiment aléatoires, offrent une certaine vulnérabilité à la cryptanalyse et aux attaques malveillantes.

Au lieu d'algorithmes mathématiques, l'emploi de processus physique stochastique, et en particulier de processus quantique permet d'assurer un caractère aléatoire parfait nécessaire à la fiabilité des algorithmes de sécurité[106]. C'est le principe des générateurs quantiques de nombres aléatoires (QRNG[104]).

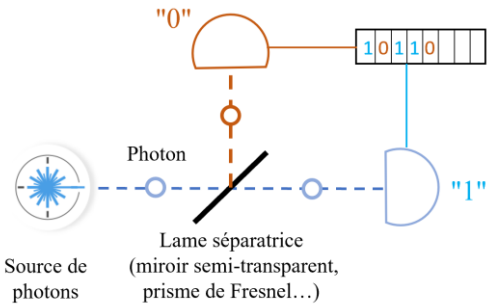


Figure 52: Exemple d'architecture de QRNG

L'archétype du QRNG (voir par exemple [107],[108]) implique l'envoi d'un train de photons uniques sur une lame séparatrice (miroir semi-transparent) suivi de deux détecteurs associés aux valeurs binaires 0 et 1 (Figure 52). L'origine du caractère aléatoire est clairement identifiée par le fait que chaque photon envoyé est réfléchi ou traverse la lame séparatrice.

D'autres réalisations s'appuient sur les temps d'arrivée de photons [109] ou leur comptage [110]. Des technologies exploitant le bruit quantique des lasers[105] ou les fluctuations quantiques du vide[106] permettent d'atteindre des taux de génération allant jusqu'à plusieurs dizaines de GHz [106], [111].

Des nombres aléatoires sont même générés à partir de la caméra d'un smartphone [112] par comptage de photons. Ce dispositif optique a d'ailleurs débouché pour la première fois en 2020 dans un produit grand public sous la forme d'un chipset QRNG miniaturisé (Figure 53) d'ID Quantique[107] intégré dans une version spécifique du smartphone Samsung Galaxy [113]. IDQ propose également des solutions de QRNG sous divers autres formats (Figure 53).

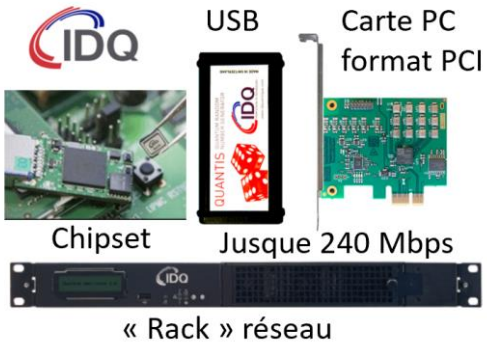


Figure 53: Offre QRNG IDQ (port USB, PCI) (Source ; ID Quantique)

D'autres sociétés plus récentes, telles que MagiQ Technology (USA), Quintessence Labs (Australie), Quside (Espagne), Qutools (Allemagne)[108] ont aussi lancé la commercialisation de ce type de générateurs quantiques.

Si, comme nous allons le voir dans la section suivante les protocoles QKD font largement usage des QRNG, la production de véritables nombres aléatoires est aussi utile pour nombre de cryptosystèmes classiques et, comme nous l'avons signalé, différents domaines applicatifs (simulation, jeux, IoT).

4.2.4.2. Les systèmes/protocoles QKD

Les systèmes de distribution quantique de clé ou QKD (*Quantum Key Distribution*) sont à la base de la cryptographie et de la communication quantique. Ils visent à permettre l'échange de clés de chiffrement,

[104] Quantum Random Numbers Generator.
[105] Le bruit incontrôlable d'une source laser.
[106] Le vide n'est pas une entité physique inerte mais, il est au contraire animé d'un mouvement chaotique permanent.
[107] IDQ, ancienne startup suisse maintenant filiale de SK Telecom, opérateur mobile coréen.
[108] Sites: www.idquantique.com, www.magiqtech.com, www.quintessencelabs.com, www.quside.com, www.qutools.com.

en général symétriques, générées par des dispositifs QRNG, via des infrastructures physiques reposant principalement sur les technologies de photonique quantique[109] et en s'appuyant sur des protocoles[110] assurant la protection de la transmission des clés secrètes contre les intrusions. Ces protocoles offrent une sécurité garantie par les lois de la physique (principe d'indétermination de Heisenberg[21] et théorème de non-clonage[23]) plutôt que par un algorithme mathématique.

Comme l'illustre la figure 54[114], les systèmes de QKD utilisent généralement deux canaux de communication qui permettent à un émetteur, Alice, et un récepteur, Bob, de convenir d'une clé secrète commune puis de communiquer des informations classiques chiffrées par cette clé.

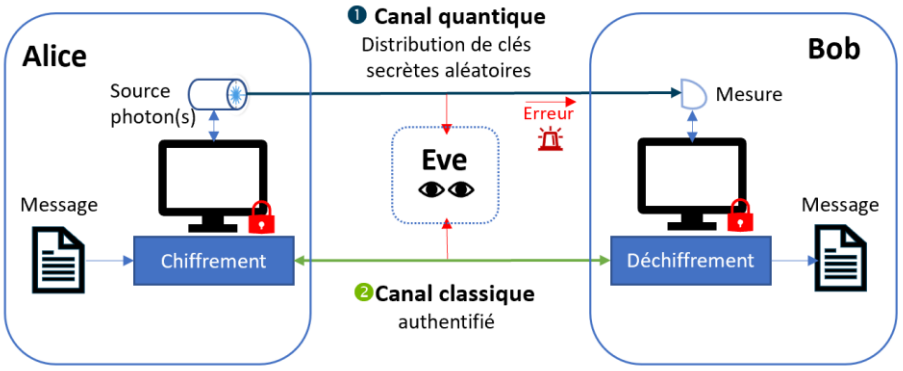


Figure 54: Principe des systèmes de QKD (source : d'après [114])

Un canal quantique est utilisé pour la transmission des signaux quantiques tandis qu'un canal public authentifié est utilisé pour l'échange d'informations durant la procédure préliminaire de détermination de la clé, puis ensuite, pour les échanges de messages chiffrés entre les deux parties.

Si un espion potentiel, traditionnellement appelée Eve, veut intercepter l'échange de clé en tentant d'obtenir de l'information sur l'état quantique des photons de lumière (supports physiques naturels des informations dans la communication quantique) cela les perturbera inévitablement à cause des lois de la physique quantique, et révèlera sa présence en engendrant des erreurs dans la corrélation des données partagées par Alice et Bob. Dans ce cas un nouvel échange de clé peut être initié.

Protocoles QKD Catégorisation par usage ou non de l'intrication d'une paire (ou plus) de photons / Catégorisation par la dimension de l'espace de codage		Discrete Variable QKD (DV QKD)	Continuous Variable QKD (CV QKD)
		Les états quantiques pour le codage sont discrets. Ce sont des qubits. Par exemple la direction de polarisation du ou des photons porteurs de l'information est utilisée pour distinguer les états.	*Les états quantiques utilisés pour la représentation des informations sont continus et à dimension infinie, contrairement au DVQKD. Ce peut être par exemple à la fois la phase et l'amplitude du signal optique transmis.*
Prepare & Measure QKD (PM QKD)	*Les protocoles QKD de type "Prepare & Measure" tirent parti de la propriété de la mesure quantique selon laquelle la mesure d'une observable fait tomber la fonction d'onde probabiliste dans un état discret déterministe.*	**BB84** – 1984 par C.H. Bennett et G. Brassard B92 – 1992 par C.H. Bennet Six-State Protocol – 1998 par D. Bru SARG04 – 2004 par V. Scarani et al DPS – 2002 par Inoue et al COW – 2005 par Stucki et al	GMSSP (Gaussian-modulated squeezed state protocol) - 2001 par N.J. Cerf et al.
Entanglement-Based (EB QKD)	*L'information quantique est véhiculée par une paire de photons intriqués. Selon la propriété d'intrication une mesure sur un des photons de la paire donne immédiatement l'information sur l'état de l'autre photon.*	**E91** – 1991 par Artur Ekert **BBM92** – 1992 par C.H. Bennett et al.	GG02 (Coherent state balanced homodyne detection protocol) –2002 par F.Grosshans et P. Grangier

Figure 55: Catégories des protocoles principaux de QKD (liste de protocoles NON EXHAUSTIVE)

[109] i.e. utilisation de photons transmis par voie optique : fibre optique, liaison aérienne ou satellitaire
[110] Règles et contraintes encadrant la communication en particulier la détection des intrusions

Lorsque les deux parties, Alice et Bob, ont pu convenir d'une clé secrète commune, et confirmer qu'un espion n'est pas présent, ils peuvent utiliser cette clé dans un algorithme de cryptage symétrique[111] classique, pour crypter et décrypter des données confidentielles.

Divers protocoles, tant conceptuels que pratiques, et approches matérielles ont été élaborés pour mettre en œuvre ces principes[116]. Nous pouvons diviser ces différentes approches en deux grandes catégories selon les propriétés quantiques qu'elles exploitent (Figure 55).

Si l'on considère la dimension de l'espace de codage comme critère discriminant, la plupart des protocoles QKD peuvent être classés dans la catégorie « **Discrete variable** » QKD (**DV QKD**) ou « **Continuous Variable** » QKD (**CV QKD**) suivant qu'ils font usage des photons avec un codage discret (type qubit) ou continu (phase, amplitude).

Par ailleurs, l'utilisation de photons uniques vs intriqués (jumeaux) est un second critère de classification utile. Ainsi à tous les **protocoles** de type **Préparation & Mesure (PM QKD)**, où Alice envoie des impulsions codées à Bob qui décode en suivant un protocole spécifique, s'ajoutent les **protocoles utilisant l'intrication** (**EB QKD**) dans lesquels les deux parties reçoivent les photons d'un état intriqué et exécutent des mesures appropriées[114].

La figure 55 liste quelques-uns des protocoles connus. Les plus courants appartiennent à la catégorie DV QKD. Le plus ancien est le protocole BB84 (PM QKD) créé en 1984 par C. Bennett et G. Brassard dont le fonctionnement est détaillé à l'annexe 5 (Figure 56). L'utilisation de l'intrication, apport ultérieur, a donné naissance aux protocoles E91 et BBM92 (EB QKD).

Cette liste n'est pas exhaustive. Une autre variété de protocoles, non exposée ici, permet par exemple d'établir des communications bilatérales (à l'initiative d'Alice ou Bob). Si la communication quantique assure une inviolabilité théorique des transmissions, elle impose de fortes contraintes d'usage qu'il s'agit de résoudre, si bien que régulièrement des améliorations ou de nouveaux protocoles émanent de la communauté scientifique dans ce sens.

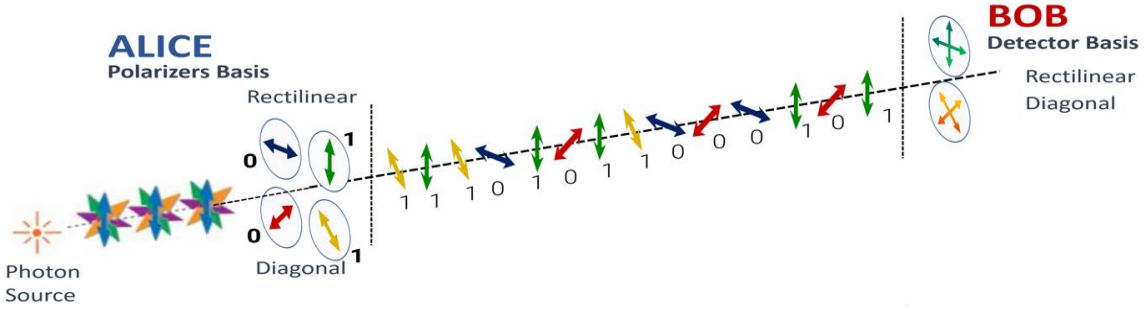


Figure 56: Protocole BB84 : Alice envoie une clé aléatoire brute sur le canal quantique à Bob (voir annexe 5)

La figure 57 résume les principaux avantages, inconvénients et barrières technologiques liés aux communications quantiques par distribution quantique de clé.

On peut y relever, par exemple, que trouver une parade à la vulnérabilité matérielle, préoccupation récurrente dans ce domaine, est l'un des axes importants de la recherche actuelle. Celle-ci a permis la création d'une nouvelle famille de protocoles dits *Device Independent* : **DI QKD** [117] et **MDI QKD** (Measurement Device Independent)[118].

Ces nouveaux systèmes exploitent les propriétés statistiques de l'intrication quantique pour garantir une sécurité maximale des communications en résolvant les scénarios où la sécurité des protocoles QKD est

[111] Comme nous l'avons vu dans la section 4.2.1 les cryptosystèmes symétriques (type AES) sont robustes. Dans certaines conditions (clés aléatoires, renouvelées à chaque message et de taille équivalente à celle du message) ils sont même réputés inviolables comme l'a prouvé Claude Shannon en 1949 [115].

remise en question par des dispositifs quantiques imparfaits, ou dans lesquels on ne peut avoir confiance car potentiellement malicieusement « préparés » (piratage)[119]. Si Eve modifie délibérément la source de photons ou les dispositifs de mesure, Alice et Bob parviendront toujours à déceler sa présence.

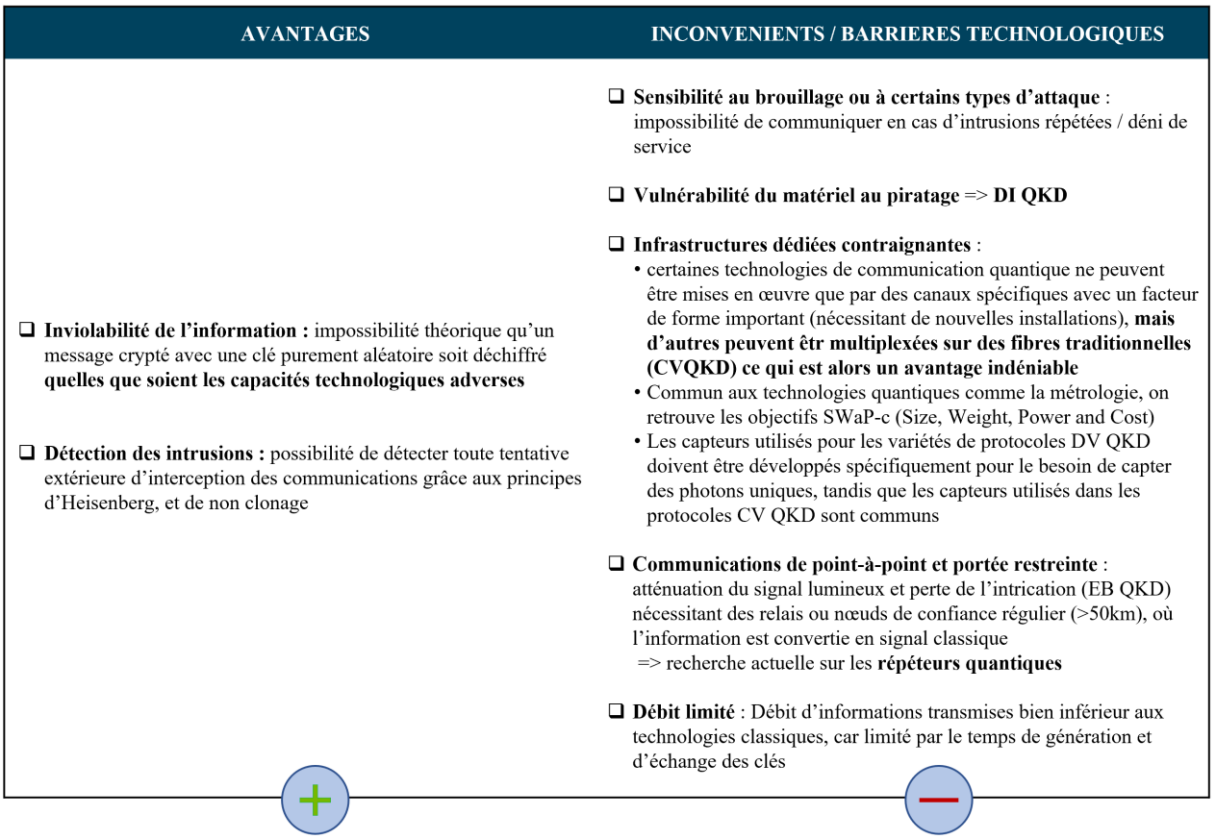


Figure 57: Avantages et inconvénients des communications quantiques (QKD)

Autres points mentionnés dans la figure 57, **l'augmentation des débits de génération de clés** et **l'allongement des distances** (qui entraine pour l'instant des pertes de signal dans les fibres optiques ou à l'air libre) pour les communications point-à-point **sont également deux enjeux majeurs** détaillés dans la section suivante. Nous y traitons des implémentations pratiques dans le domaine des communications QKD longues distances filaires et satellitaires (notamment chinoises voir annexe 2 -§ 3.4),. Au final, la correction des défauts et la levée des barrières technologiques conditionneront l'adoption plus importante par la sphère industrielle[112] des protocoles les plus performants.

4.2.4.3. Les implémentations pratiques de la QKD

La mise en œuvre pratique des protocoles QKD peut utiliser des liaisons par fibre optique ou en espace libre (aériennes ou satellitaires). La performance des liaisons point-à-point est évaluée par la distance à laquelle les clés secrètes peuvent être distribuées et par le débit de génération de ces clés. Le but ultime est de fournir un niveau de sécurité maximale, résistant aux attaques les plus courantes, avec un débit et une distance de communication qui sont compatibles avec des usages pratiques[114]. La Chine se fait particulièrement remarquer avec des projets destinés à frapper les esprits. Comme nombre de pays (voir annexe 2 & 4), elle investit dans les communications QKD pour des raisons de souveraineté et pour protéger ses communications sensibles, telles celles qui interviennent dans la gestion de son réseau électrique[113]. Un premier déploiement avait été réalisé dès 2012 dans la zone d'Hefei pour relier diverses entités du gouvernement chinois [120].

[112] Plusieurs solutions de PM QKD sont aujourd'hui commercialisées (par ex ID Quantique et MagiqTech déjà cités), ce qui n'est pas encore le cas pour la variété de protocoles CV QKD et DI QKD.
[113] Voir les expériences effectuées par le gestionnaire du réseau électrique chinois SGCC (annexe 2, §3.4, p.105)

Globalement quelques expériences récentes ont fourni des performances qu'il est intéressant de citer. Elles concrétisent l'état de l'art dans le domaine des liaisons QKD fibrées, aériennes ou satellitaires et les barrières actuelles que constituent i) la distance et ii) le débit.

i) Le défi de la distance

Dans le cadre d'un protocole **PM QKD**[114], une implémentation en laboratoire a été démontrée sur environ **400 km** dans une **fibre optique** à faibles pertes[121]. Mais le record semble être de **509 km** (sans répéteur) réalisé en Chine en mars 2020 avec le protocole *Twin-Field QKD*[115] [122]. En espace libre, la **communication satellite / sol** [123] utilisant un protocole PM QKD la plus longue a été réalisée, aussi en Chine, sur plus de **1 200 km**.

Les meilleures performances des protocoles **EB QKD** (utilisant des photons intriqués e.g. BBM92) sont, quant à elles, de ~100/150 km dans de la fibre optique [124], [125] et **1 203 km** [126] par satellite.

En pratique les communications QKD commerciales, transitant sur des réseaux de fibre optique hors laboratoire ou conditions expérimentales optimisées, sont bien plus limitées en distance. Il y a là une première barrière physique qui concerne la distance maximale de communication qui peut être atteinte sur des canaux de fibre optique.

L'atténuation de la lumière à la longueur d'onde des télécommunications (1 550 nm) étant de l'ordre de 0,2 dB/km[114], les pertes engendrées par la propagation dans le canal limitent la portée des liens QKD à ~50/100km. Au-delà, les taux de générations de clé finissent par devenir beaucoup trop bas (Figure 58) et il n'est pas possible de simplement amplifier le signal comme en télécommunication classique en raison du théorème de non-clonage.

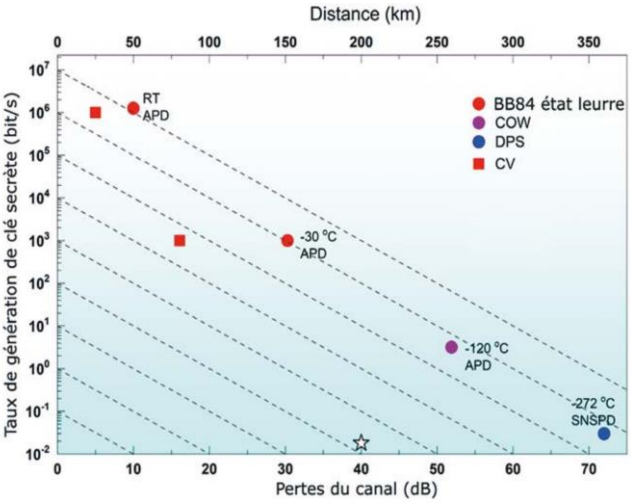


Figure 58: Relation entre la distance, perte de signal et taux de génération de clé pour différentes implémentations QKD (Source: « La cryptographie quantique », E. Diamanti, 2018)

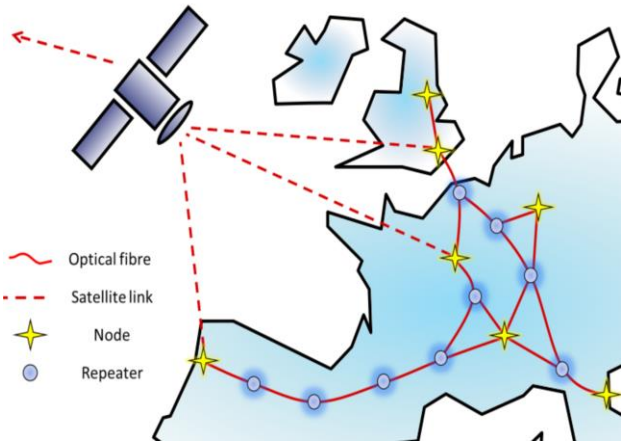


Figure 59: A quoi ressemblerait un premier réseau de communication quantique ? (Source: http://www.qcall-itn.eu/2019/08/15/solid-state-crystals-for-quantum-repeaters/)

Pour arriver à concevoir un réseau de communication quantique comme celui illustré sur la figure 59, il faudra surmonter cette limitation de distance. Il existe diverses solutions aux degrés de maturité et sécurité différents : (a) les **nœuds de confiance**, (b) les **répéteurs quantiques** de signal qui permettent de fractionner les distances à parcourir, (c) les **satellites** dont la portée intrinsèque est supérieure.

[114] Où pour rappel il est possible pour Alice de préparer des états quantiques de photons, de les envoyer à Bob, qui les mesure, les traite puis convient en retour, à l'aide d'une communication classique standard avec Alice, d'une clé commune secrète.
[115] Faisant intervenir deux lasers à disposition d'Alice et Bob respectivement.

(a) Les nœuds de confiance

Certaines implémentations de type PM QKD utilisent des nœuds classiques pour répéter/amplifier le signal. L'utilisation de ces répéteurs conventionnels fait perdre l'état quantique de l'information transmise (leur inefficacité serait encore plus grande avec les protocoles à intrication EB QKD). Des clés QKD sont alors établies séparément pour chaque tronçon de ligne . Les nœuds sont généralement appelés nœuds de confiance (*trusted nodes*) car ils exigent une sécurité à chaque lien pour garantir que les informations n'y soient pas compromises.

Certains affirment qu'il ne s'agit là que d'une solution à court terme, car il est difficile d'envisager la construction de bunkers gardés par des bataillons de l'armée tous les 50 km[116]. D'autres pensent que cela pourrait être une approche pratique pour certaines applications si les coûts des boîtiers émetteur/récepteur QKD diminuent.

Néanmoins, les réseaux quantiques à nœuds de confiance ont déjà fait leurs preuves. C'est sur cette architecture que la Chine a installé une liaison par fibre sécurisée entre Shanghai et Pékin, faisant 2000 km (Figure 60). Déployée entre 2013 et 2016 par la startup chinoise QuantumCTek, la ligne comprend 32 répéteurs classiques dont l'accès physique est sécurisé[117] et constituera une des artères terrestres du futur réseau quantique chinois de 35 000 km planifié à l'horizon de 2025[118].

(b) Les répéteurs quantiques

De nombreux groupes de recherche travaillent au développement de répéteurs quantiques capables d'étendre des informations d'intrications de proche en proche afin de créer un lien plus large. Une approche courante envisage de stocker, manipuler et réémettre des qubits sans perturber leur état quantique (e.g. [129], [130]).

Le stockage de l'information quantique nécessite un transfert direct et réversible (interface), sans mesure vers un système matériel ou **mémoire quantique**, dont le registre est constitué de qubits basés sur l'état quantique d'une particule de matière (§3.2). Les télécommunications quantiques utilisent, quant à elles,

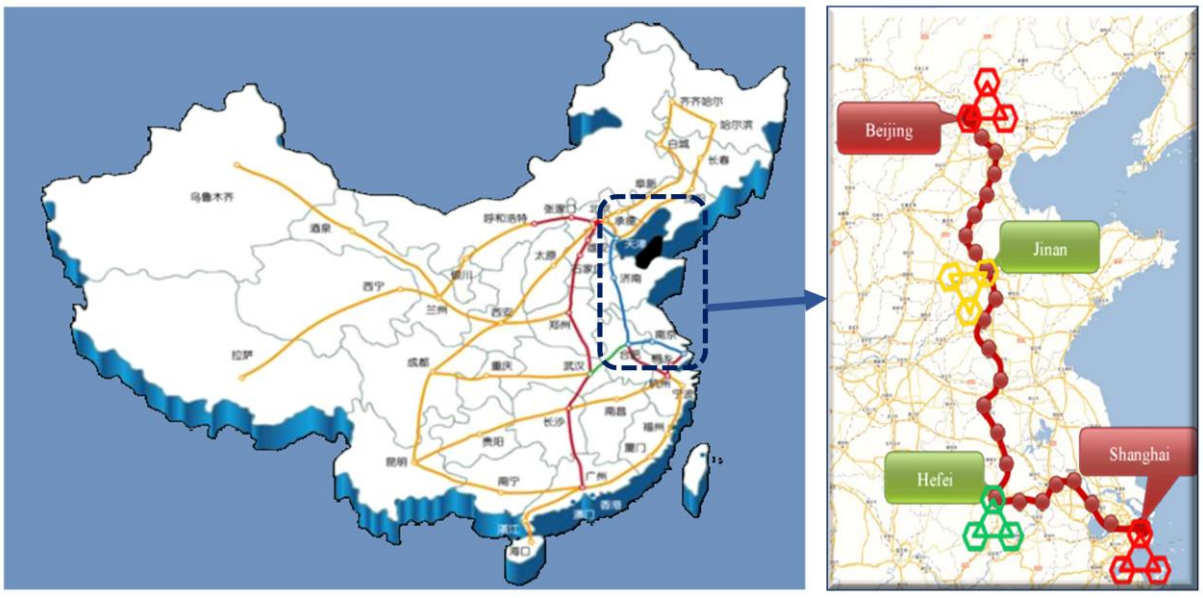


Figure 60: A droite : Liaison QKD fibre optique 1200km Shanghai-Pékin, 32 nœuds de confiance
A gauche : réseau quantique chinois de 35000 km planifié pour 2025
(Source: d'après présentation de Xiongfeng Ma[117])

[116] Dans leur version chinoise, ils seraient dans des bunkers gardés par un bataillon d'armée (Source : [127]).
[117] Voir [128] et www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Xiongfeng_Ma_Presentation.pdf
[118] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hao_Qin_Presentation.pdf

des qubits photoniques et les interfaces utilisées seraient donc de type lumière/matière. Les centres NV dans le diamant[45] décrits au chapitre 3.2.5. sont particulièrement étudiés dans ce cadre-là.

Notons qu'en juillet 2019, des chercheurs chinois annonçaient avoir expérimenté une technologie de répéteurs *photoniques* à base d'interféromètres à 12 photons permettant de se passer de mémoire quantique. Cela les rendrait théoriquement très sécurisés [131].

Un véritable répéteur quantique permet la sécurisation de bout en bout en utilisant le principe d'intrication quantique, et celui de **téléportation quantique** pour la transmission de qubits.

La téléportation quantique [132] désigne un protocole de communication par lequel des informations quantiques peuvent être transmises d'un endroit à un autre à l'aide d'une communication classique et d'une intrication préalablement partagée entre un émetteur et un récepteur (Figure 61).

Fondamentalement, la téléportation quantique transfère l'état quantique d'une particule à une autre, identique, et efface en même temps l'état de l'original. Contrairement à ce que le nom suggère, il ne s'agit donc pas d'un transfert d'énergie ou de matière. Le terme de téléportation quantique est utilisé pour souligner le fait que le processus est destructif: après la téléportation, la première particule ne sera plus dans son état initial[119].

Au final, cependant, il faudra probablement plusieurs années avant qu'un répéteur quantique ne soit commercialisé.

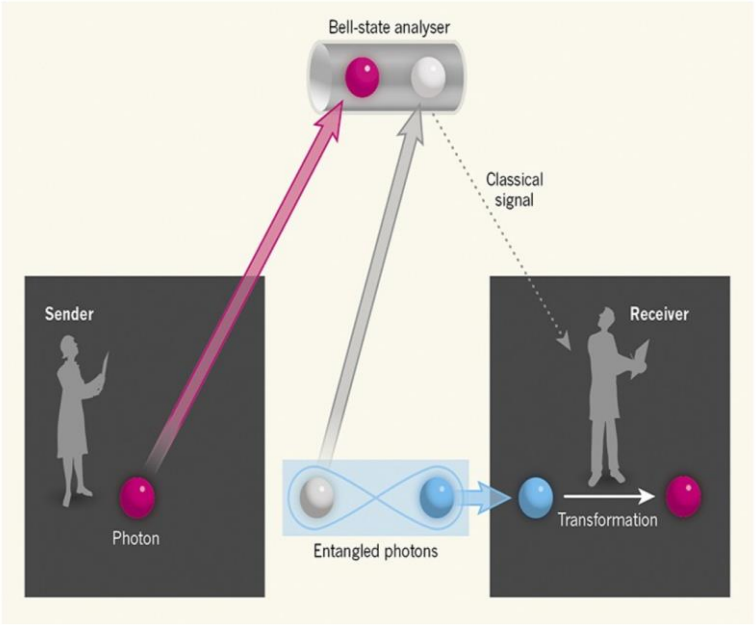


Figure 1 | Quantum teleportation. Twenty years ago, Boschi *et al.*[1] and Bouwmeester *et al.*[2] showed that the quantum state of a photon can be teleported from a sender to a distant receiver. The technique uses a pair of photons that are entangled, which means that their properties are strongly correlated. One of the entangled photons (blue) is given to the receiver — in principle, in advance of the quantum-teleportation process. The sender then prepares a photon in an unknown quantum state (pink) and combines this photon with the second entangled photon (grey) in a device called a Bell-state analyser. This device performs a joint measurement of the quantum states of the two photons and sends the result to the receiver as a classical (non-quantum) signal. Finally, the receiver uses this information to transform their photon, recreating the quantum state of sender's photon.

Figure 61: Illustration du principe de téléportation extrait de l'article publié en 2017 dans Nature pour fêter les 20 ans de l'idée (Source: N. Gisin, « Quantum-teleportation experiments turn 20 »)

(c) Les satellites et liaisons optiques en espace libre

L'utilisation de satellites ou de plateformes aériennes (drones compris), servant de relais quantiques, est une approche alternative et complémentaire permettant de s'affranchir des pertes inhérentes aux canaux terrestres, puisque les effets des pertes et fluctuations dues à l'atmosphère sont limités à son épaisseur d'environ 10 kilomètres[114][120]. La lumière peut ensuite se propager sans modification vers des satellites en orbite basse ou géostationnaires[134]. Un autre avantage est que la communication optique aérienne peut utiliser une gamme de longueurs d'onde plus large que celle des fibres optiques, qui doivent fonctionner dans la bande des télécommunications[133].

Le principe d'utilisation de satellites en orbite basse pour distribuer des clés sécurisées a déjà été expérimenté suite au lancement en Chine, en 2016 du premier satellite QKD Micius[121]. Quelques

[119] Source : Wikipedia
[120] Les pertes dues à la propagation dans l'air sont liées quadratiquement (racine carrée) à la distance tandis qu'elles sont exponentielles dans la fibre optique, puis nulle au-delà des 10km de l'atmosphère[133].
[121] Aussi appelé Mozi, dans le cadre du programme QUEST (Source : https://fr.wikipedia.org/wiki/QUESS).

semaines après, il permit la mise en place d'une liaison vidéo intercontinentale cryptée entre la Chine et l'Autriche[134]. Le principe de fonctionnement est illustré sur la Figure 62. Le satellite vole sur une orbite héliosynchrone à une altitude de 500 km. Une paire de photons intriqués est générée à bord du satellite et envoyée par deux liaisons vers deux stations optiques au sol (Figure 62). La technologie est actuellement limitée à de faibles débits de transmission et à un fonctionnement nocturne, mais son développement est en cours.

Ainsi en juin 2020, une équipe chinoise a réalisé avec Micius une implémentation complète de la QKD à longue distance (1120km)[135].

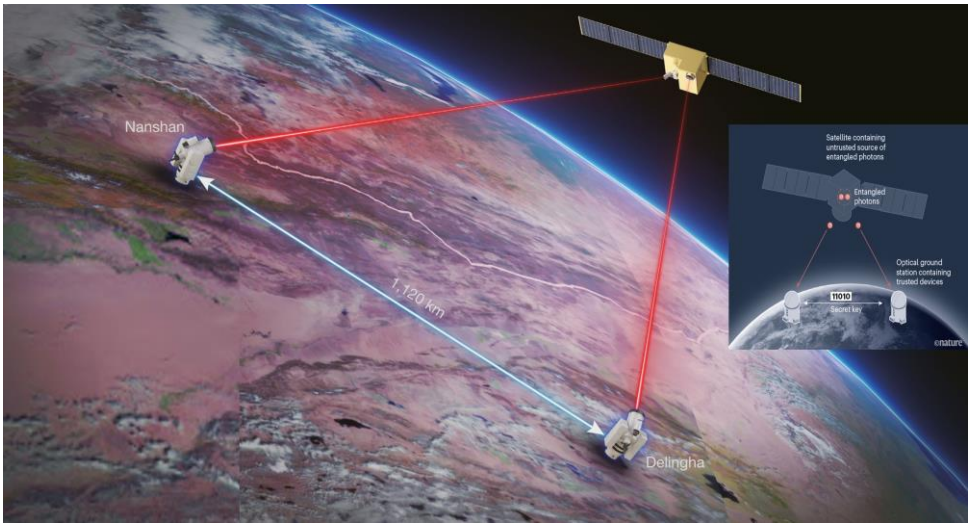


Figure 62: Principe de communication par distribution quantique de clés sécurisées (QKD) point-à-point sur longue distance par le satellite chinois Micius (Source: J. Yin et al., Entanglement-based secure quantum cryptography over 1,120 km)

Elle fait suite à celle effectuée en 2017, par la même équipe, et qui avait débouché sur des débits bien trop faibles pour être utilisables[126]. Pour remédier à ce problème, les scientifiques ont mis en œuvre des améliorations technologiques majeures : installation au sol de télescopes à haut rendement, optimisation des équipements le long du chemin optique, des optiques de suivi, des systèmes de synchronisation satellite/sol et de traitement des signaux. Ils ont ainsi pu quadrupler l'efficacité de la liaison par rapport à l'expérience précédente et, par conséquent, produire des taux d'erreurs suffisamment bas pour qu'une clé puisse être générée et exploitée. Pour finir, ils se sont aussi attachés à augmenter la sécurité des stations au sol.

Si cette démonstration peut être considérée comme la plus avancée à ce jour, de nombreuses faiblesses devront être corrigées pour que ces résultats puissent vraiment être utilisés opérationnellement. Ainsi, à 0,12kbits/s, le débit d'envoi des clés reste très limité. En outre, l'expérience a été réalisée la nuit, sur une fréquence de signal incompatible avec celle utilisée dans les réseaux de fibres optiques qui servent de relais terrestres et enfin, dans une configuration où les deux stations au sol étaient visibles simultanément par le satellite [136].

Sur ce dernier point, l'utilisation de satellites sur des orbites plus élevées que celle de Micius serait nécessaire, il est intéressant de citer, à l'opposé, les approches visant une couverture plus locale par l'utilisation d'un réseau de drones. En juin 2019, des chercheurs chinois annonçaient avoir établi des liaisons optiques QKD aériennes au sein d'un réseau de drones espacés de 200 m à 100 m d'altitude [137].

Notons pour terminer que si la Chine se démarque par l'avancée de ses travaux, d'autres recherches à travers le monde sont en cours comme l'illustre la figure 63. En Europe, par exemple, le consortium

européen de cybersécurité par satellite QUARTZ[122] (ESA) coordonne plusieurs projets tandis qu'ArQit, start-up anglaise travaille à la construction du premier système QKD satellitaire commercial (SaaS)[123].

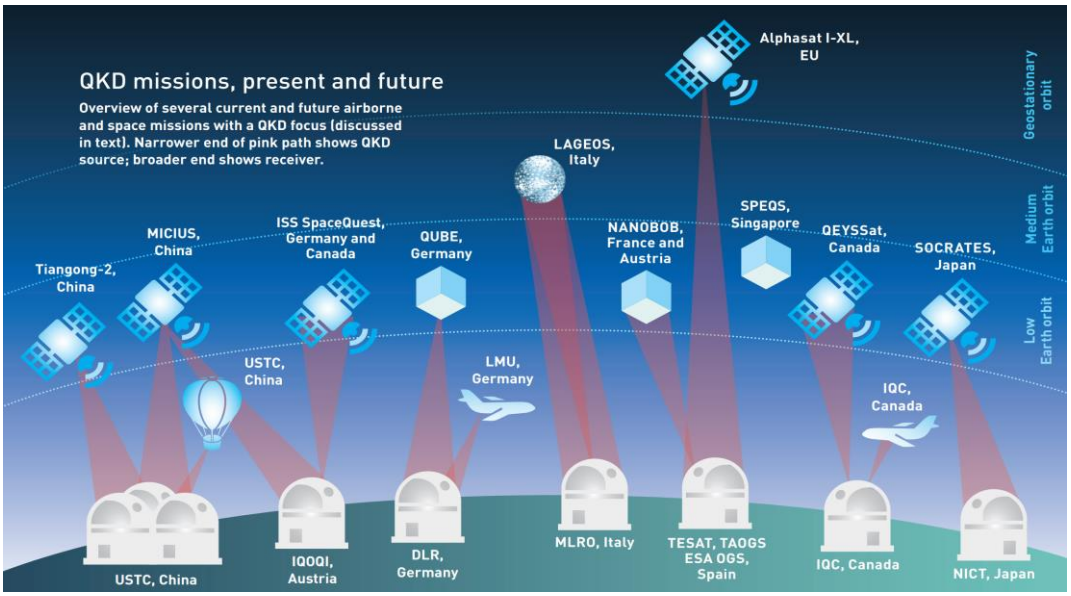


Figure 63: Aperçu de plusieurs projets de QKD aériennes et spatiales actuelles et futures (Source: I. Khan, B. Heim, A. Neuzner, et C. Marquardt, « Satellite-Based QKD »)

ii) Le défi du débit

Comme nous l'avons déjà évoqué, une barrière à franchir pour des systèmes QKD concerne le taux maximal de génération de clés secrètes possible, lorsqu'en particulier les canaux de communication utilisés sont bruités, ce qui est toujours le cas en pratique. Actuellement, il existe encore une forte disparité entre les débits de communications optiques classiques (> 100Gbits/s) et la QKD (~10Mbit/s)[114]. Ces débits sont suffisants pour de la transmission vidéo, mais pas s'il s'agit de chiffrer de grands volumes de données avec des systèmes cryptographiques dont la taille des clés serait augmentée.

Comme l'illustre la dernière démonstration (2020) de Micius, l'optimisation des composants sur tout le trajet optique permet de nettes améliorations. Cela concerne en particulier les **sources de photons** (lasers de faible puissance, à photon unique ou de photons jumeaux intriqués) et **les détecteurs de photons.** Les performances de ces derniers déterminent largement le débit de génération des clés.

DV QKD: nécessite du matériel spécifique donc coût > matériel CV QKD	
Photodiode à avalanche (APD)	+ peu coûteux
Nanofil supraconducteur (SNSPD)	+ meilleures performances que APD (x4) (efficacité de détection, taux de comptage, temps mort) - cryogénie nécessaire - coûteux
CV QKD : matériel commun, utilisé en communication optique classique et compatible avec les réseaux de communication conventionnels	
Détecteur homodyne (diode PIN) / hétérodyne	+ coût, + compatibilité réseaux conventionnels - augmenter la bande passante tout en gardant un bruit faible

Figure 64: Forces, faiblesses et points à développer pour l'amélioration des débits et l'intégration opérationnelle de différents type de capteurs (Source: d'après « La cryptographie quantique » Eleni Diamanti, 2018)

[122] https://www.ses.com/fr/press-release/lesa-et-un-consortium-dirige-par-ses-developpent-des-solutions-de-cybersecurite
[123] https://www.arqit.io/

Les différents protocoles QKD (discret/variable) et leurs applications conditionneront le choix des détecteurs en fonction de différents arbitrages (efficacité, taux de comptage en obscurité[124], cryogénie nécessaire ou pas, coût, …). Certains de ces éléments sont précisés sur la figure 64.

iii) Autres défis

Au-delà des limites de performances déjà exposées, un autre défi majeur à relever pour les années à venir sera le développement de dispositifs dont la complexité, les coûts, et la consommation d'énergie seront réduits, à l'instar des objectifs SWaP-C[125] mentionnés pour la métrologie et les capteurs. Sur ce point, l'intégration photonique (sur silicium ou phosphate d'indium) offrirait un niveau de miniaturisation élevé et permettrait une production de masse à bas coût[138].

Déjà commercialisée pour des communications par fibre optique, l'offre QKD satellitaire devrait se développer dans les prochaines années. La PQC et la distribution quantique de clés sécurisées seraient ainsi les premiers outils disponibles pour la sécurisation des communications. A plus long terme (15 à 20 ans) le développement d'un réseau quantique plus global conduisant à un internet quantique pourrait émerger (Figure 46). Nous en décrivons à présent les contours.

4.2.4.4. Vers un internet quantique

Internet a eu un impact radical sur notre monde. L'objectif d'une version quantique serait de fournir une technologie radicalement nouvelle, mais complémentaire au web classique, permettant une communication quantique ultra-sécurisée (transmission de qubits) entre deux lieux distants quelconques sur Terre.

En assurant une sécurité inconditionnelle (*perfect secrecy*) des communications, grâce à l'application des technologies QKD utilisant l'intrication et la téléportation, l'internet quantique permettrait de mettre en œuvre d'autres applications telles que :

- Les réseaux distribués de capteurs quantiques.
- Le **Blind Quantum Computing**, protocole qui permettrait à un client ne disposant pas d'ordinateurs quantiques, de déléguer son informatique quantique à un serveur quantique distant (QaaS) tout en assurant que ses informations privées seront protégées du serveur de calcul si celui-ci n'est pas fiable[139].
- Le **calcul quantique distribué** dans lequel un cluster d'ordinateurs quantiques, n'ayant chacun qu'un petit nombre de qubits, serait exponentiellement plus puissant.

Comme ce fut le cas pour la naissance de l'internet classique, il est impossible à ce stade de prévoir toutes les applications qui émergeront.

Des développements supplémentaires seront nécessaires pour progresser sur la voie d'un web quantique. L'article « Quantum internet: A vision for the road ahead » [140] dont nous reproduisons une illustration sur la figure 65 précise les étapes importantes. On y retrouve par exemple, les mémoires quantiques qui utilisées dans des répéteurs quantiques, seraient aussi nécessaires pour établir des services de type QaaS (informatique quantique sur le cloud), de sorte que deux utilisateurs pourront obtenir et stocker des qubits intriqués puis les utiliser pour se téléporter, l'un l'autre, des informations quantiques.

[124] Comptage de photons incidents alors qu'il n'y en a pas (noir).
[125] SWaP-C : Size, Weight, and Power - Cost

Des nœuds terminaux pour la préparation, la mesure, le stockage et la manipulation des qubits seront également nécessaires pour l'informatique quantique distribuée et les réseaux de capteurs quantiques. Ces nœuds terminaux peuvent être constitués de simples dispositifs photoniques ou de petits ordinateurs quantiques.

Au-delà du matériel, l'aspect logiciel est également primordial. Il faudra développer différentes couches logiciels telles que les couches réseaux gérant les protocoles de communications quantiques (similaire à ce qui existe aujourd'hui pour le protocole TCP/IP[126] dans le monde Internet classique).

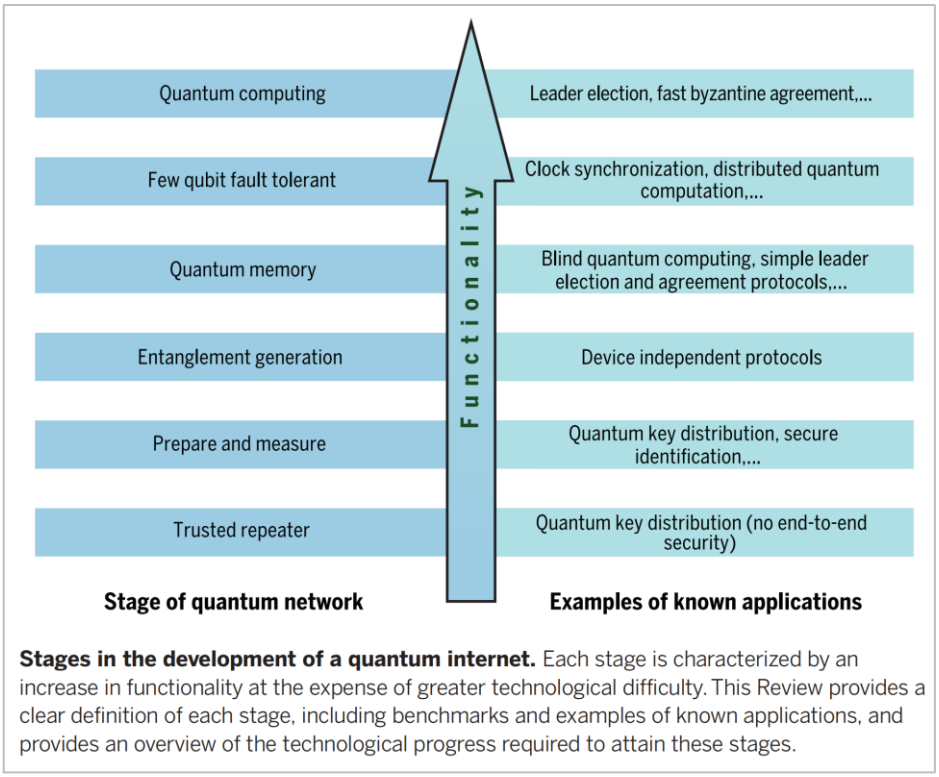


Figure 65: Fonctionnalités nécessaires pour la réalisation d'un internet quantique (Source: S. Wehner, "Quantum internet: A vision for the road ahead", Science, 2018)

Des progrès graduels sont réalisés aujourd'hui, mais de nombreux experts estiment qu'il faudra au moins une autre décennie voire deux pour développer un tel réseau longue distance. Mais dès aujourd'hui, des feuilles de route nationales ou régionales se mettent en place. Si la Chine parait en avance (Figure 60), l'Europe a créé en 2018 la Quantum Internet Alliance pour développer une stratégie Internet Quantique. L'an dernier, l'un des projets de la QIA a démontré l'intrication entre un qubit photonique et un qubit ion piégé, donc entre la lumière et la matière, sur une distance de 50 km [141].

Il y a quelques jours le ministère de l'Énergie américain a dévoilé son plan décennal pour développer un Internet quantique national qui pourrait fonctionner sur les réseaux actuels de fibres optiques du pays[127]. Dans un premier temps, ce réseau ne sera qu'un projet de recherche gouvernemental mais il laisse tout de même entrevoir un avenir où nous surferons peut-être sur un Web quantique.

[126] Transmission Control Protocol/Internet Protocol (TCP/IP)
[127] https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet

4.2.5. Les challenges et progrès à venir

Comme développés dans la section précédente, les défis principaux dans le domaine des télécommunications quantiques sont liés principalement aux importantes contraintes de déploiement de la QKD, en particulier à la capacité de communiquer via les canaux quantiques (a) sur des **distances plus importantes**, ce qui nécessitera (b) le développement de **répéteurs quantiques**. Par ailleurs (c) les **taux de génération de clés** devront être largement améliorés (débit).

Au niveau des États, il n'y a pas consensus sur le type de solution à adopter face à la menace future de l'ordinateur quantique. Alors que la Chine investit massivement dans son projet de réseau quantique, l'agence française de la Sécurité des Systèmes d'information (ANSSI) publiait en mai 2020 une note d'information[128] où elle affichait une certaine réticence vis-à-vis de la QKD et recommandait de plutôt privilégier des cryptosystèmes de type PQC. Ce qui est souvent mis en avant est le ratio (coûts+contraintes)/bénéfices défavorable.

Avis de l'ANSSI

Les garanties de sécurité apportées en principe par la QKD le sont aux au prix de contraintes d'emploi lourdes qui réduisent la portée des services offerts et compromettent le niveau de sécurité qui peut être atteint en pratique, en particulier dans les scénarios où les communications transitent par un réseau de liens QKD connectés entre eux. Si l'emploi de QKD sur des liaisons point à point peut malgré tout être envisagé comme une mesure complémentaire aux moyens cryptographiques classiques dans une logique de défense en profondeur, les dépenses qu'un tel choix occasionne ne doivent pas être faites au détriment de la lutte contre les menaces actuelles sur les systèmes d'information.

Son homologue britannique, le NCSC, avait lui-même exprimé son scepticisme[129] en mars 2020 en mettant en avant essentiellement les risques autour de l'authentification[130] . Les débats sont ouverts. Alors que **le choix des solutions dépendra** probablement **de l'application**, la plupart des experts en cryptographie s'accordent à dire qu'**une approche hybride *clé publique PQC + QKD*** devrait être utilisée **pour les applications les plus sensibles**. Ces clés hybrides combinent les avantages de la complexité calculatoire et les promesses de sécurité des lois de la physique.

[128] L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés ?, ANSSI
[129] Quantum Security Technologies, NCSC
[130] En cryptographie, prouver de qui provient un message et qu'il n'a pas été altéré lors de son transit.

4.3. Simulation et informatique

Lorsque l'on entend aujourd'hui parler de l'informatique quantique c'est bien souvent pour évoquer la promesse de sa capacité à résoudre des problèmes que les ordinateurs traditionnels ne peuvent pas et ne pourront peut-être jamais traiter convenablement.

La raison fondamentale en est le parallélisme inhérent des systèmes quantiques (voir §3.1). Un registre quantique de dimension N peut contenir 2^N nombres simultanément tandis qu'un registre classique n'en contient qu'un seul. Quand on fait une opération sur un registre quantique, les calculs sont menés sur l'ensemble des nombres conjointement alors que pour son analogue classique, ils ne portent que sur un seul nombre.

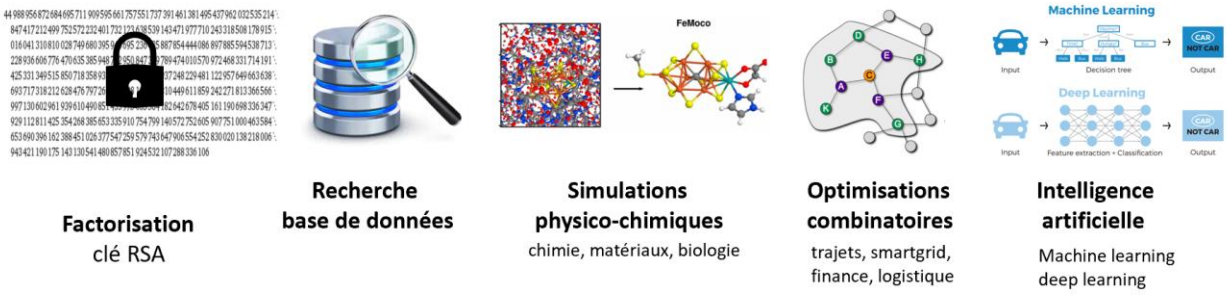


Figure 66: Quelques problèmes potentiellement visés par l'informatique et la simulation quantique

Dès lors, dans la mesure où nous pouvons l'exploiter efficacement, l'ordinateur quantique pourrait surpasser l'ordinateur classique dans la résolution de problèmes dont la complexité augmente exponentiellement avec la quantité des données à traiter[131]: optimisation combinatoire, simulation numérique moléculaire, cryptanalyse, IA (Figure 66).

Le calendrier est d'autant plus incertain (Figure 67) qu'il existe plusieurs types d'ordinateurs quantiques et différentes plateformes physiques (qubits) potentielles aux maturités technologiques diverses (voir §3.2.9). Les ordinateurs à recuit quantique, bien que spécialisés sur des cas d'usages limités, sont déjà

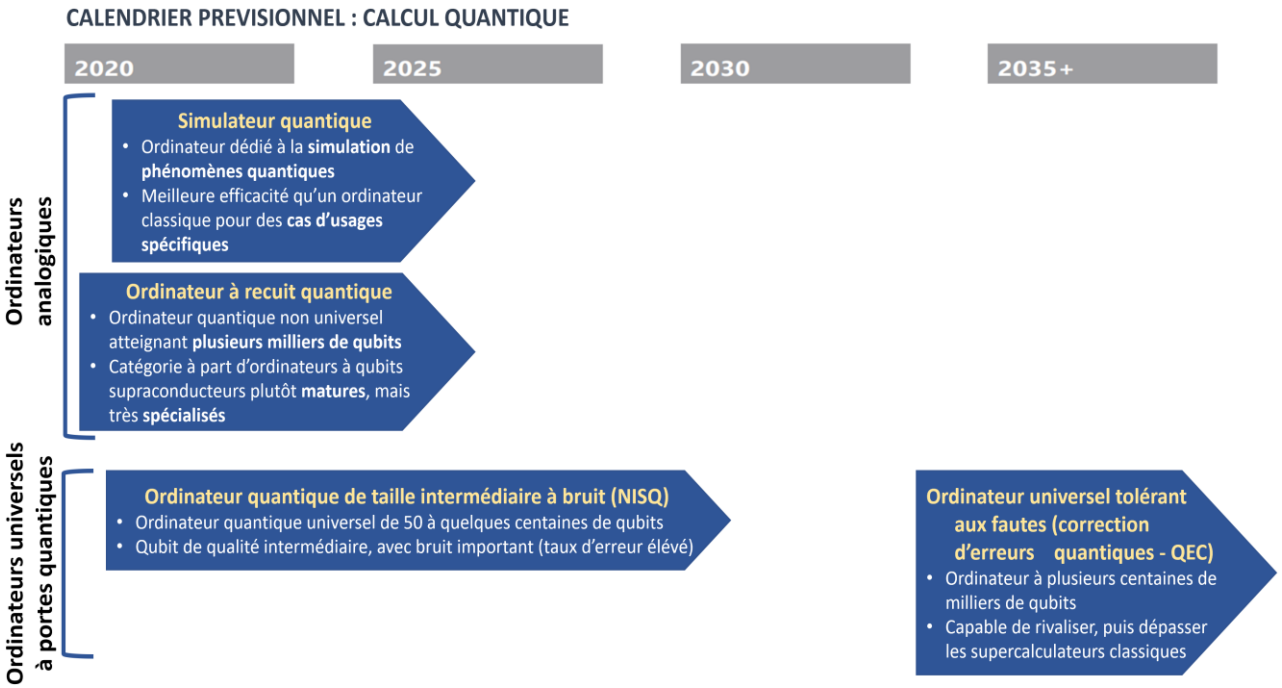


Figure 67: Catégories d'ordinateurs quantiques et horizons de deploiement commercial associés (adapté de la figure 26)

[131] Syndrome parfois désigné sous le terme de malédiction (ou fléau) de la dimension (Wikipedia)

commercialisés par la firme canadienne D-Wave[132] et les ordinateurs universels à correction d'erreurs quantiques seraient disponibles d'ici 10 ou 15 ans d'après les experts. D'ici là , nous vivrons à l'ère des ordinateurs NISQ[133] dont nous parlerons plus tard.

L'objectif de ce chapitre n'est pas de couvrir en profondeur l'ensemble, trop vaste, des sujets technologiques, logiciels et applicatifs liés aux ordinateurs quantiques. Nous nous limiterons à quelques éléments représentatifs de l'état de l'art pour chacun d'entre eux.

Si nous débutons la première section en nous intéressant aux ordinateurs conventionnels, c'est pour nous amener au constat que des barrières technologiques et physiques se rapprochent inexorablement, ce qui pourrait limiter leur développement futur. Les alternatives technologiques offertes par les différentes catégories d'ordinateurs quantiques seront ensuite exposées dans la deuxième section. Sans entrer dans le détail des implémentations physiques, en grande partie couvertes dans le chapitre traitant des qubits (§3), nous nous arrêterons sur la définition du cahier des charges qu'un ordinateur quantique doit respecter et les verrous actuels, ce qui nous permettra d'entamer la quatrième section consacrée aux erreurs quantiques, principales faiblesses des processeurs quantiques à ce jour. La dernière section détaillera les applications et types d'algorithmes envisagés.

Nous n'aborderons pas dans ce document les aspects logiciels de développement et de contrôle. Certaines informations sont toutefois disponibles à l'annexe 8.

4.3.1. Limites des ordinateurs conventionnels

Jusqu'à présent les technologies des supercalculateurs et du calcul haute performance (HPC[134]), pris dans la course à l'exascale[135], ont permis de répondre à certaines problématiques complexes au prix de coûts et consommations électriques très élevés[136] mais les paradigmes de nombreux problèmes analytiques ou d'optimisation leur restent inaccessibles tandis que l'accroissement des performances brutes s'essouffle depuis 2017 (Figure 68).

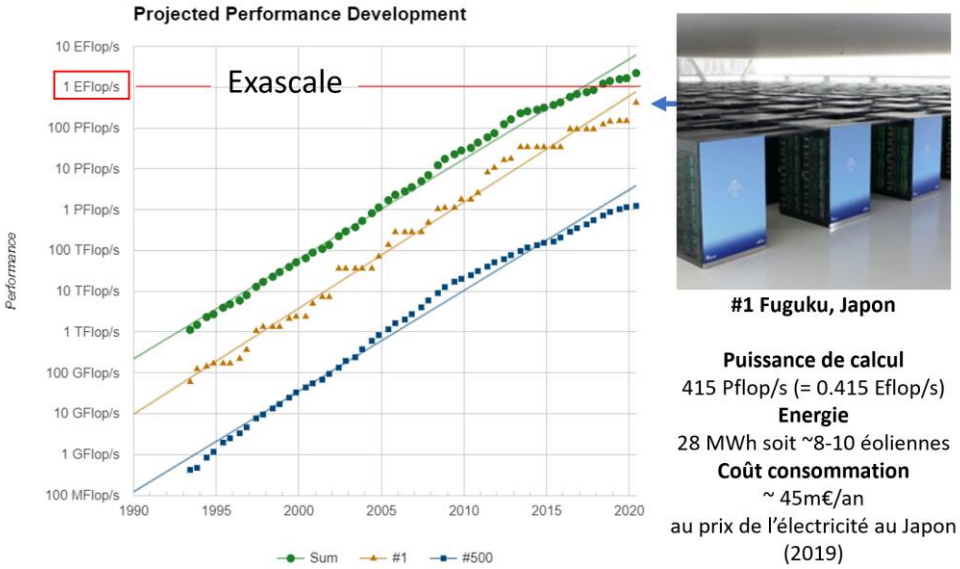


Figure 68: Evolution sur 30 ans du top500 des supercalculateurs #1 (orange), #500 et cumul des puissances de calculs (échelle log) (Source: https://www.top500.org/statistics)

[132] https://www.dwavesys.com/
[133] Noisy Intermediate-Scale Quantum (NISQ)
[134] High-Performance Computing
[135] Les supercalculateurs exaflopiques sont des superordinateurs fonctionnant selon une architecture massivement parallèle avec une puissance de calcul de ~10^{18} flops (1 exaflop = 1 milliard de milliards d'opérations en virgule flottante par seconde).
[136] Ainsi la consommation du supercalculateur japonais Fuguku, le plus puissant à ce jour, est de 28MWh, soit une facture estimée à 45m€/an au prix local de l'électricité. Le projet, lui-même a couté 1 milliard USD$.

Le ralentissement de la **loi de Moore** (voire sa fin[137]) est souvent mentionné comme une des raisons qui justifierait le développement de solutions alternatives aux technologies conventionnelles (puces de Silicium/Chipset CMOS). Dans sa version la plus récente, elle stipulait que la densité des transistors (nombre de transistors/mm^2) et, par conséquent la puissance de calcul des ordinateurs classiques, pourrait doubler tous les 18 mois. Mais si les finesses de gravure des chipsets ont régulièrement diminué, elles pourraient atteindre un palier en raison d'une combinaison de contraintes technologiques, physiques et de facteurs économiques [142]. Comme on peut le voir sur la figure 69, les performances des processeurs individuels n'ont augmenté que de 3.5%/an depuis 2015 selon le benchmark SpecINT.

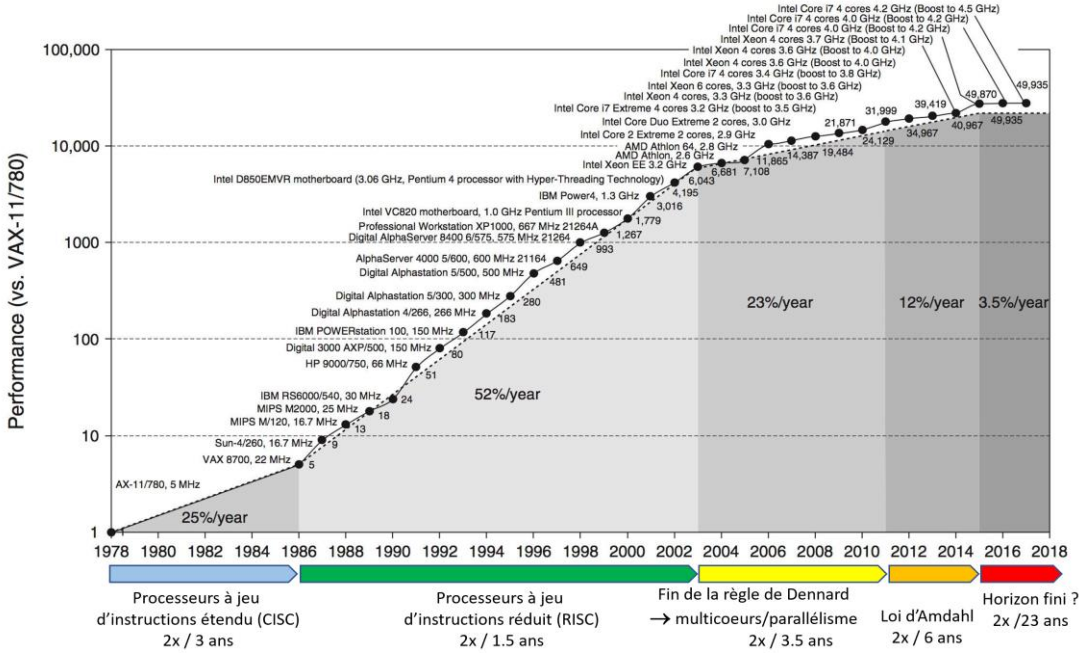


Figure 69: Croissance des performances des (uni)processeurs sur 40 ans selon le benchmark SpecINT (Source: « Computer architecture: a quantitative approach », Hennessy & Patterson, 2018)

Dans les faits, la densification des transistors avait aussi causé la rupture vers 2004, d'une autre règle, celle de **Dennard,** qui stipulait que lorsque l'on augmentait la densité des transistors, on pouvait stabiliser la puissance consommée par unité de surface des chipsets[142]. Les fuites de courant dans les transistors devinrent importantes et la consommation électrique explosa, tout comme la chaleur dégagée, ce qui eut aussi pour conséquence la limitation de la vitesse des horloges cadençant la vitesse des opérations des chipsets (Figure 71).

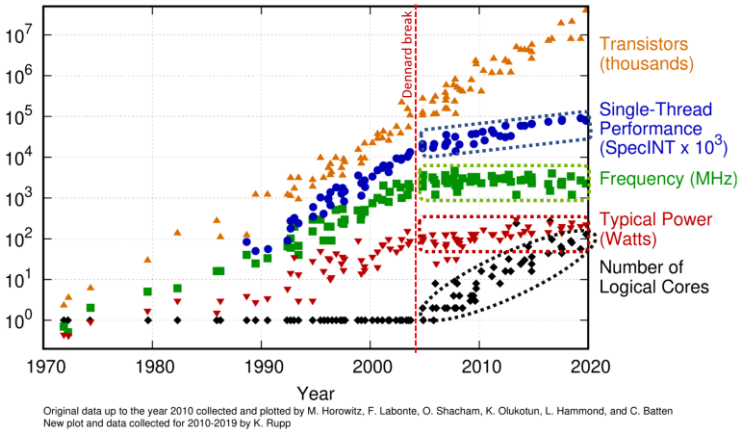


Figure 71: 48 années d'évolution des microprocesseurs (1971-2019) (Source: d'après K. Rupp)

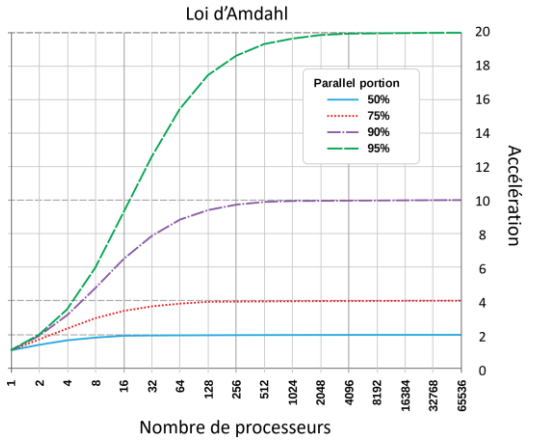


Figure 70: Loi d'Amdahl, limitant les capacités du multicoeur et de la parallélisation(Source: Wikipedia)

[137] Il s'agit plutôt d'un déclin progressif.

Dès lors, les constructeurs ont misé sur les architectures multicoeurs 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 formalise l'accélération maximale d'un système de calculs parallèles (Figure 70).

Cette liste n'est pas exhaustive. Il y a aujourd'hui d'autres contraintes potentiellement limitantes, comme celles liées aux procédés de fabrication eux-mêmes, telle la photolithographie utilisée pour la gravure des wafers de silicium. Au final, retenons que si l'on peut s'attendre à ce que les fabricants produisent encore quelques générations de processeurs plus avancées, l'époque où l'on pouvait compter sur des puces plus performantes et moins coûteuses tous les 18 mois est révolue. Attention, cela ne sonne pas le glas du progrès de l'informatique pour autant.

Un rapport récent du MIT[143] explique que l'industrie a des possibilités pour améliorer les performances de calcul grâce à de meilleurs algorithmes et logiciels, ainsi que des architectures de processeurs spécialisées (tels que GPU, FPGA, NPU[138]qui pourraient déboucher sur des puces 3D). Par ailleurs, il n'est pas exclu qu'une percée technologique majeure, telle qu'une nouvelle conception de transistor, puisse repousser certaines des limites exposées ici pour la technologie des puces de silicium.

L'informatique quantique, voie exploratoire parallèle au même titre que d'autres technologies non conventionnelles[139], permettra de passer outre les diverses limitations des processeurs CMOS actuels pour certaines tâches. Il convient de noter ici que : i) **les ordinateurs quantiques ne sont pas destinés à remplacer la technologie classique** (ils doivent plutôt être considérés comme des accélérateurs spécialisés, à l'instar encore des GPU, FPGA, NPU actuels qui fonctionnent dans les centres de calcul pour accélérer des applications ou des sous-processus spécifiques) ; ii) **il n'existe pas un type unique d'ordinateur quantique** et un certain nombre de critères sont à considérer lors de la conception de tels ordinateurs comme va être détaillé à présent.

4.3.2. Grandes catégories d'ordinateurs quantiques

Suivant les critères choisis pour les distinguer, il existe de trois à six catégories d'ordinateurs et simulateurs quantiques. Pour notre part, nous retiendrons la représentation illustrée figure 72 dans laquelle deux classes principales se distinguent : les ordinateurs/simulateurs quantiques analogiques et les ordinateurs quantiques numériques à base de portes logiques quantiques (ou circuits quantiques).

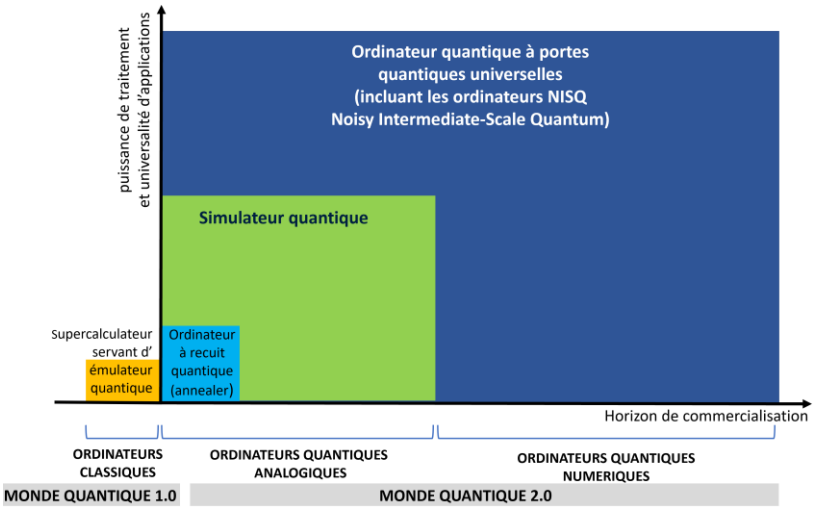


Figure 72: Grandes familles d'ordinateurs/simulateurs quantiques, puissance et horizon de commercialisation

[138] GPU: Graphics Processing Unit / FPGA: Field Programmable Gate Array / NPU: Neural Processing Unit

[139] L'informatique non conventionnelle désigne un large éventail de méthodes nouvelles ou inhabituelles pour le calcul et le traitement de l'information utilisant par exemple des dispositifs mécaniques, optiques, chimiques, biologiques, ou encore physiques comme ceux mis en œuvre dans l'informatique quantique.

Avant de les détailler, donnons quelques éléments sur les émulateurs quantiques qui utilisent des ordinateurs traditionnels et des logiciels spécifiques pour simuler des qubits.

4.3.2.1. Émulateurs quantiques

Les **émulateurs quantiques** sont utilisés pour simuler l'exécution d'algorithmes quantiques sur des ordinateurs traditionnels, allant de simples portables à des supercalculateurs, selon le nombre de qubits à simuler[140]. Ils transposent ces algorithmes, qubits et portes quantiques, en bits et portes logiques classiques. Il est ainsi possible de tester des algorithmes quantiques sans avoir d'ordinateurs quantiques, ce qui peut être utile puisque ceux-ci sont encore rares. Cela reste néanmoins très consommateur en mémoire et beaucoup plus lent[144].

Figure 73: Emulateur QLM d'Atos

Pour l'heure, les supercalculateurs peuvent simuler 40 à 50 qubits. Ainsi, la QLM d'Atos (Quantum Learning Machine)[141] est une plateforme logicielle qui permet de simuler le fonctionnement d'un processeur quantique comptant jusqu'à 41 qubits sur un supercalculateur conventionnel (Figure 73). Entièrement paramétrable, elle permet de définir les caractéristiques techniques spécifiques de chaque technologie de qubits (temps de cohérence, temps d'activation des portes logiques…) et leurs taux de fiabilité actuelle. En juin 2020, l'entreprise a lancé une nouvelle version[145] de son émulateur, baptisée QLM-E, annoncée 12 fois plus puissante que son prédécesseur, sans préciser toutefois pour l'instant le nombre de qubits simulables.

Des records sont régulièrement battus pour dépasser le seuil de 50 qubits (voir les performances des émulateurs logiciels présentées à la figure 78, p.66), mais alors avec un faible nombre de portes quantiques (i.e. transcrivant de petits algorithmes) ou des méthodes visant à diminuer la dimensionalité de certains problèmes spécifiques[146].

Une simulation naïve d'un ordinateur quantique nécessite beaucoup de puissance du côté de la mémoire, pour stocker 2^N états d'un registre quantique de N qubits, et dans une moindre mesure, du côté des traitements associés qui font usage du calcul matriciel à grande échelle. Il faudrait 16 Pétaoctets (Po) de mémoire pour simuler complètement 50 qubits en précision *double-flottant*[142, 143].

Après cette brève incursion dans l'univers des ordinateurs classiques (le *monde quantique 1.0* des circuits intégrés et CMOS), revenons à présent à la *version 2.0* proposée par les ordinateurs quantiques.

4.3.2.2. Simulateurs ou ordinateurs quantiques analogiques

La simulation de la dynamique des systèmes quantiques est l'application la plus naturelle et la plus évidente des ordinateurs quantiques. Ce fut la motivation première de Richard Feynman, pionnier de l'informatique quantique dès 1981[14]. Les simulateurs quantiques pourraient surpasser de manière exponentielle les ordinateurs classiques lorsqu'ils simulent un système avec de nombreux degrés de liberté quantique comme ce peut être le cas par exemple pour des problèmes de physique, de chimie ou de science des matériaux. L'idée de Feynman était que ces simulations devraient être réalisables plus rapidement par un ordinateur qui exploiterait lui-même les particularités de la physique quantique pour augmenter sa puissance de calcul.

---

[140] Nous avons recensé 146 logiciels de simulations écrits en 19 langages : https://www.quantiki.org/wiki/list-qc-simulators
[141] https://atos.net/fr/solutions/quantum-learning-machine
[142] Dans sa représentation mathématique (c.f. §3.1.2) un qubit est caractérisé par deux nombres qui en précision double flottant occupent 8 octets en mémoire chacun. Le compte est alors de $2x8x2^{50}$ octets = $16x2^{50} \sim 16x10^{15}$ = 16 Po.
[143] Fugaku, supercalculateur top#1 depuis juin 2020 a environ 5Po de mémoire vive.

L'objectif général de la simulation d'un système quantique est de déterminer sa structure ou son comportement, compte tenu de la connaissance de ses composants et de l'environnement dans lequel il se trouve. En général, ces simulations nécessitent la connaissance de *l'hamiltonien* (opérateur énergétique) décrivant tous les éléments et interactions du système.

Les ordinateurs quantiques analogiques incluent la famille des **ordinateurs adiabatiques** ou **à recuit quantique (annealer)** dont le seul acteur commercial est l'entreprise canadienne D-Wave (Figure 74) et les **simulateurs quantiques analogiques** à usage plus général**.** Ces deux variétés d'ordinateurs manipulent directement les interactions entre les qubits[144] physiques, plutôt que de décomposer les actions en opérations de porte plus abstraites comme c'est le cas pour les ordinateurs quantiques numériques.

Figure 74: Ordinateur (Annealer) D-Wave (Source : D-Wave)

Les **ordinateurs quantiques à recuit quantique (annealer)** utilisent des processeurs quantiques constitués de plusieurs milliers de qubits[145], avec leurs deux états $|0\rangle$ et $|1\rangle$. Ils sont pour l'instant de qualité moyenne en matière de durée de cohérence[146]. Ces processeurs ne sont adaptés qu'à une petite partie des algorithmes quantiques existants (essentiellement des problèmes d'optimisation). Pour ces algorithmes éligibles, la puissance de calcul serait supérieure à celle offerte par des supercalculateur mais cela reste controversé[147].

Le recuit est une méthode de programmation qui existe en informatique classique. Elle s'inspire d'un procédé utilisé dans la métallurgie dans lequel des cycles alternés de chauffage (recuit) et de refroidissement lent minimisent l'énergie du matériau. Cette méthode a été transposée en optimisation pour trouver l'extremum d'une fonction.

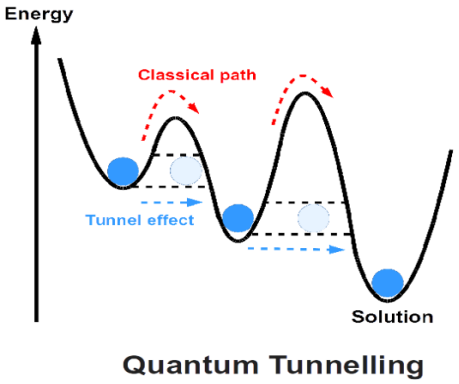


Figure 75: Recuit thermique vs. quantique (Source : https://medium.com//

Le recuit quantique est plus efficace que le recuit thermique. En effet, si l'on représente un problème d'optimisation comme un paysage de pics et de vallées dont la meilleure solution correspond au point le plus bas de la vallée la plus profonde du paysage (Figure 75), le recuit classique (ordinateur classique) devra essayer chaque vallée avant de pouvoir confirmer qu'il a trouvé la plus basse représentant la solution optimale (ce qui peut prendre énormément de temps). Le recuit quantique permet de trouver la solution optimale dans un délai plus court car il peut contourner ces pics en exploitant l'effet tunnel[147].

Le problème que l'on souhaite résoudre est modélisé au sein d'un réseau de qubits interconnectés (*lattice*). La structure est initialisée dans un état à priori proche de la solution. L'ordinateur va alors la faire converger lentement, de façon adiabatique (sans échange de chaleur), vers la solution du problème posé (Figure 76). Les problématiques abordées correspondent à la recherche d'un minimum d'énergie dans un système comme pour la simulation de la dynamique d'une molécule ou l'optimisation de la distance d'un trajet complexe (problème du voyageur de commerce).

[144] Le terme « qubit » pourrait être considéré comme un abus de langage dans le cas des simulateurs quantiques analogiques.
[145] D-Wave a annoncé récemment un nouveau processeur possédant 5000 qubits (le précédent en avait 2000).
[146] L'erreur quantique n'est pas en soi ici un problème pour les systèmes quantiques modélisés car ils sont eux-mêmes bruités.
[147] L'effet tunnel désigne la propriété que possède un objet quantique de franchir une barrière de potentiel même si son énergie est inférieure à l'énergie minimale requise pour franchir cette barrière. C'est un effet purement quantique, qui ne peut pas s'expliquer par la mécanique classique (Source : Wikipedia).

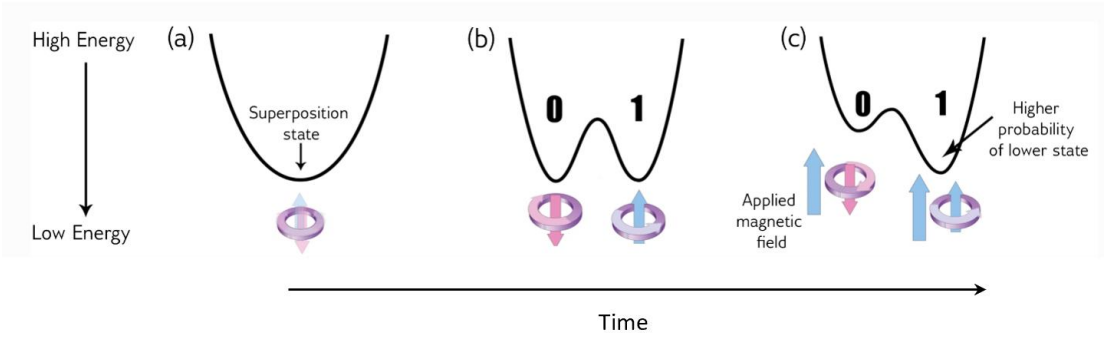


Figure 76: La physique du recuit quantique peut être visualisée par un diagramme énergétique (Source: D-Wave)

Les **simulateurs quantiques analogiques,** quant à eux, tentent d'établir un analogue physique du phénomène quantique à la base du problème étudié. 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 sujets à recherche dans des laboratoires (Figure 78). La technologie la plus utilisée est celle des atomes froids contrôlés par lasers, aussi exploitable, comme nous l'avons vu au §3.2.2, pour la création d'ordinateurs quantiques universels utilisant des circuits quantiques constitués de qubits et de portes logiques quantiques.

Si les simulateurs quantiques exploitent ainsi les mêmes technologies que les ordinateurs quantiques universels abordés dans la prochaine section, ils n'utilisent pas les mêmes propriétés de qubit, de correction d'erreurs, ou de portes quantiques. Leurs heuristiques de recherches sont moins généralistes que celles des systèmes « universels ». Elles ne permettent par exemple de bénéficier des phénomènes d'interférences[148] mis en œuvre par certaines portes logiques spécialisées.

4.3.2.3. Ordinateurs quantiques universels à portes logiques (et tolérance de fautes)

Figure 77: « Salle des machines » d'IBM contenant des ordinateurs à portes quantiques accessibles sur le Cloud (IBM Q Experience)

Construire un ordinateur quantique n'est pas facile. Une ingénierie de pointe est nécessaire pour maintenir le système isolé de son environnement en lui permettant de fonctionner dans un régime quantique pur, mais tout en ayant un contrôle actif et précis des processus. Un dispositif idéal aurait des qubits stables et durables. Il serait tolérant aux fautes grâce à des dispositifs de **correction d'erreurs (QEC** ou **QECC)** et offrirait un ensemble complet de portes quantiques (§3.1.2 et annexe 6), toutes fonctionnant à grande vitesse et avec une grande fidélité. Il serait alors possible d'y exécuter tous les algorithmes quantiques existants et futurs avec une vitesse optimale par rapport aux supercalculateurs et aux ordinateurs quantiques adiabatiques[144]. Il serait enfin facile d'augmenter dynamiquement le nombre de qubits disponibles pour les calculs jusqu'à atteindre plusieurs millions de qubits physiques ce qui lui permettrait de résoudre une grande variété de problèmes. Ces ordinateurs sont désignés par les termes : ***Large-Scale Quantum Computers*** **LSQC** ou ***Fault-Tolerant Quantum Computer*** **FTQC**.

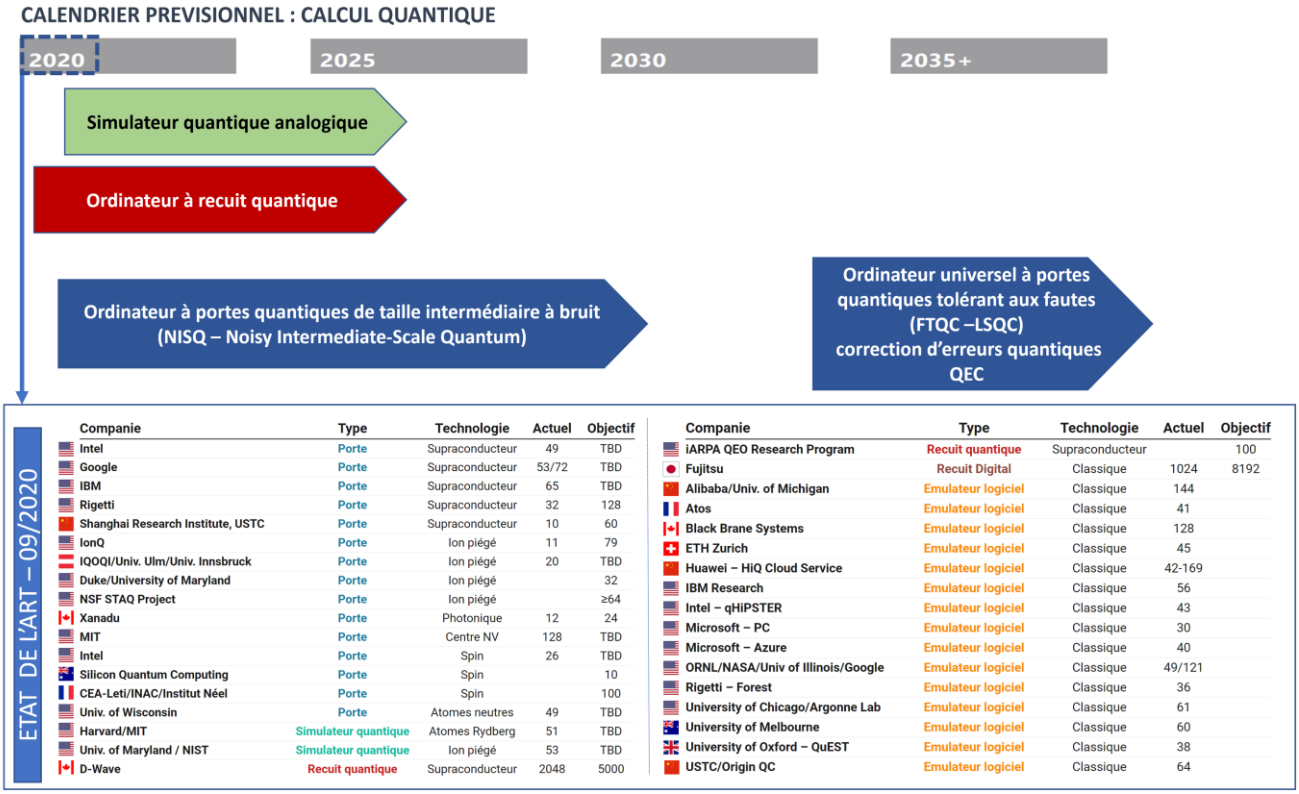
Aujourd'hui, la réalité est différente (Figure 77). Les processeurs quantiques à portes, sont limités à une cinquantaine de qubits. Le niveau de bruit quantique des qubits limite l'efficacité des calculs et rend nécessaire ce qui n'est pas encore disponible: la multiplication des qubits et l'enchaînement des portes quantiques afin de gérer les codes de correction d'erreurs quantiques (QECC).

[148] La capacité de faire interférer des informations quantiques (ou fonction d'ondes) de façon constructive ou destructive est à la base de nombreux algorithmes quantiques proposés pour les ordinateurs quantiques de type NISQ et universels.

En attendant que la qualité des qubits ne s'améliore, ce qui permettrait de concevoir des processeurs plus puissants, nous devons nous contenter de qubits de qualité intermédiaire. Nous sommes rentrés dans l'ère des ordinateurs **NISQ (Noisy Intermediate-Scale Quantum)**. Cette sous-catégorie d'*ordinateurs quantiques universels de génération intermédiaire* a été introduite par John P. Preskill, fin 2017 [148]. Elle désigne les ordinateurs quantiques universels existants, et à venir dans un futur proche, disposant de cinquante à quelques centaines de qubits physiques sans correction d'erreurs fiable. S'ils n'ont pas la précision suffisante pour révolutionner le monde, ils permettront de démontrer que les technologies employées et les algorithmes sont valides, et qu'en les faisant interagir avec un système informatique traditionnel, des applications concrètes pourront émerger, voire que certaines tâches allant au-delà des capacités des ordinateurs classiques pourraient être réalisées.

Pour compléter notre inventaire, signalons qu'il existe quelques autres types d'ordinateurs quantiques que nous ne développerons pas plus avant ici : les **ordinateurs quantiques à variables continues**[144]**,** les **Measurement Based Quantum Computers (MBQC)**[144], et les **ordinateurs topologiques** (§3.2.6).

Pour terminer, la figure 78 nous resitue dans le contexte, d'une part du calendrier prévisionnel déjà présenté et, d'autre part, de l'état de l'art du nombre de qubits aujourd'hui disponibles par familles d'ordinateurs[149] au niveau international pour quelques startups, industriels ou laboratoires de recherche. L'ère de l'ordinateur NISQ débute tandis que des simulations sur des simulateurs quantiques analogiques sont d'ores et déjà possibles, 10 à 15 ans nous sépareraient de l'ordinateur quantique universel.



Companie	Type	Technologie	Actuel	Objectif
Intel	Porte	Supraconducteur	49	TBD
Google	Porte	Supraconducteur	53/72	TBD
IBM	Porte	Supraconducteur	65	TBD
Rigetti	Porte	Supraconducteur	32	128
Shanghai Research Institute, USTC	Porte	Supraconducteur	10	60
IonQ	Porte	Ion piégé	11	79
IQOQI/Univ. Ulm/Univ. Innsbruck	Porte	Ion piégé	20	TBD
Duke/University of Maryland	Porte	Ion piégé		32
NSF STAQ Project	Porte	Ion piégé		≥64
Xanadu	Porte	Photonique	12	24
MIT	Porte	Centre NV	128	TBD
Intel	Porte	Spin	26	TBD
Silicon Quantum Computing	Porte	Spin		10
CEA-Leti/INAC/Institut Néel	Porte	Spin		100
Univ. of Wisconsin	Porte	Atomes neutres	49	TBD
Harvard/MIT	Simulateur quantique	Atomes Rydberg	51	TBD
Univ. of Maryland / NIST	Simulateur quantique	Ion piégé	53	TBD
D-Wave	Recuit quantique	Supraconducteur	2048	5000

Companie	Type	Technologie	Actuel	Objectif
iARPA QEO Research Program	Recuit quantique	Supraconducteur		100
Fujitsu	Recuit Digital	Classique	1024	8192
Alibaba/Univ. of Michigan	Emulateur logiciel	Classique	144	
Atos	Emulateur logiciel	Classique	41	
Black Brane Systems	Emulateur logiciel	Classique	128	
ETH Zurich	Emulateur logiciel	Classique	45	
Huawei – HiQ Cloud Service	Emulateur logiciel	Classique	42-169	
IBM Research	Emulateur logiciel	Classique	56	
Intel – qHiPSTER	Emulateur logiciel	Classique	43	
Microsoft – PC	Emulateur logiciel	Classique	30	
Microsoft – Azure	Emulateur logiciel	Classique	40	
ORNL/NASA/Univ of Illinois/Google	Emulateur logiciel	Classique	49/121	
Rigetti – Forest	Emulateur logiciel	Classique	36	
University of Chicago/Argonne Lab	Emulateur logiciel	Classique	61	
University of Melbourne	Emulateur logiciel	Classique	60	
University of Oxford – QuEST	Emulateur logiciel	Classique	38	
USTC/Origin QC	Emulateur logiciel	Classique	64	

Figure 78: Calendrier et nombre de qubits par famille d'ordinateurs quantiques (à portes -bleu, simulateurs -vert, à recuit -rouge + émulateurs) (Source des données : https://quantumcomputingreport.com/)

Pour bien appréhender le chemin qu'il reste à parcourir, il faut comprendre que le nombre de qubits équipant un calculateur quantique est loin d'être le seul critère à prendre en compte lorsqu'il s'agit d'évaluer ses performances. De plus, toutes les technologies de qubits ne se valent pas. Nous abordons à présent ces différents points.

[149] Ce tableau fait apparaître Fujitsu, qui depuis 2018 propose un ordinateur (classique) à recuit digital fonctionnant à température ambiante. Ce « digital annealer » est développé sur silicium en CMOS, technologie classique.

4.3.3. Ordinateurs quantiques, les barrières technologiques du hardware

Lors de l'évaluation de la conception d'un nouvel ordinateur quantique, il est utile de disposer d'une liste des exigences connues auxquelles il doit répondre. En 2000, David DiVincenzo proposait cinq critères, connus sous le nom des « **critères de DiVincenzo** », définissant les caractéristiques techniques minimales d'un ordinateur quantique universel[149]. Le système doit ainsi proposer [144]:

1. Des **qubits bien caractérisés et évolutifs** : un processeur quantique utilise des qubits qui exploitent des corpuscules élémentaires pouvant avoir deux états distincts mesurables. On en connait bien les propriétés et le comportement physique. Le système est évolutif au sens où il doit pouvoir **passer à l'échelle** en fonctionnant avec un grand nombre de qubits (*scalability*),

2. Des **qubits initialisables** : il doit être possible d'initialiser les qubits, en général à la valeur $|0\rangle$ souvent appelée état fondamental (ou *ground state*) renvoyant à un état de plus basse énergie pour une particule élémentaire support physique d'un qubit , par exemple un électron (on notera $|000\ldots0\rangle$ pour l'initialisation d'un registre de qubits),

3. Des **durées de cohérence bien supérieures aux durées d'activation des portes quantiques** : les durées des états de cohérence[150] et d'intrication[151] des qubits doivent être bien plus longues que celles requises pour les opérations effectuées par les portes logiques quantiques. C'est à cette condition que l'on peut appliquer un algorithme composé d'un enchainement long de portes sur des qubits avant qu'ils ne perdent l'information qu'ils portent. La différence d'ordre de grandeur[152] doit être de 3 ou 4[98], ce qui permettrait l'exécution en séquence de centaines voire de milliers de portes en considérant que cette quantité intégrera à terme les longues séries de portes utilisées dans les procédés de correction d'erreurs (voir §4.3.4 p.70). En dehors de la qualité intrinsèque des qubits, tout le dispositif physique doit préserver la cohérence quantique en isolant le système pendant le temps nécessaire au calcul.

4. Un ensemble de **portes logiques quantiques universelles**[153] : toutes les portes quantiques applicables aux qubits, peuvent être reproduites grâce à une base minimale de portes logiques quantiques dites universelles. Il faut au minimum 2 portes [149] i) une porte unaire comme la porte X[154] ; ii) une porte binaire comme la porte CNOT[155] (voir annexe 6). L'ensemble des portes universelles exploité dans un processeur quantique dépend de l'architecture physique des qubits et n'est donc pas le même d'une technologie à l'autre.

5. **L'état final de chaque qubit individuel doit pouvoir être mesuré** lorsque le calcul est terminé. Pratiquement cette mesure ne doit pas affecter l'état des autres qubits du système et il faudrait idéalement avoir une erreur de mesure inférieure à 1% voire 0,1%[98]. L'observation d'un système quantique est probabiliste: elle fournit en moyenne le résultat attendu, lequel peut varier à chaque exécution d'un algorithme (Figure 79). Il peut donc être nécessaire de recommencer le calcul un certain nombre de fois, ce nombre étant d'autant plus grand que le taux d'erreurs de mesure est élevé [149].

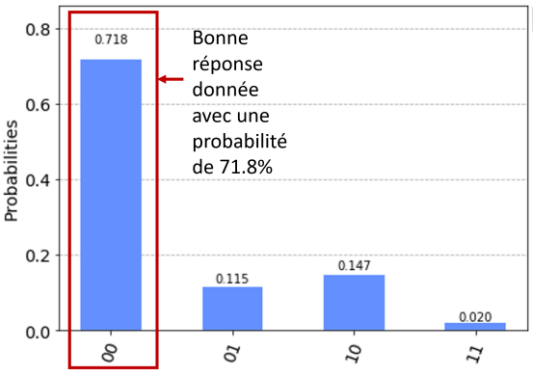


Figure 79: Histogramme des résultats donnés par un algorithme quantique après sur 1 024 exécutions, la réponse $|00\rangle$ a été donnée 735 fois (71.8%).

[150] Superposition d'états.
[151] Liens entre qubits ayant interagis via des portes quantiques à deux entrées (portes binaires).
[152] Soit des ratios de 1 pour 1 000 , ou 1 pour 10 000.
[153] Un ensemble de portes quantiques universelles est un ensemble de portes pour lesquelles toute opération possible sur un ordinateur quantique peut être réduite, c'est-à-dire que toute autre opération unitaire peut être exprimée comme une séquence finie de portes à partir de l'ensemble (Wikipedia)
[154] Unaire : agissant sur un seul qubit.
[155] Binaire : agissant sur deux qubits. La porte CNOT est l'équivalent quantique de la porte classique XOR (Annexe 6).

Pour compléter sa check-list, DiVincenzo a ajouté deux items supplémentaires qui ont tout leur sens dans le contexte des télécommunications entre différents dispositifs quantiques [144]:

6. Le système doit être capable de **convertir des qubits statiques en qubits volants (photons) et vice-versa**.

7. Le système doit être capable **de transmettre de manière fiable des qubits volants entre deux localisations spécifiques**.

Ces deux conditions spécifiques recouvrent donc les applications de la physique quantique aux télécommunications quantiques développées au §4.2 : cryptographie (QKD), architectures distribuées de calculateurs quantiques et protocole de *blind quantum computing* permettant de distribuer des traitements en protégeant leur confidentialité.

Dans la pratique, les critères principaux de DiVincenzo, même s'ils semblent basiques, sont loin d'être simples à satisfaire et aujourd'hui aucun ordinateur quantique n'y répond totalement. Du point de vue opérationnel, pour qualifier une technologie cette checklist est souvent complétée par un certain nombre de métriques et d'éléments qualitatifs déjà présentés §3.2.9 (figure 22, p. 27) dont nous rappelons ici les principaux points (extraits de [144]**)**:

- Le **nombre de qubits** qui conditionne la puissance de calcul,
- La **stabilité des qubits** qui s'évalue par des métriques liées au temps de cohérence des qubits,
- La **fidélité** des qubits déterminée par leur taux d'erreurs suite à l'application des portes logiques quantiques, ou à la lecture de leur état,
- Les **temps d'activation** des portes quantiques et de la lecture de l'état des qubits qui conditionnent la complexité possible (lorsqu'elle est rapportée au temps de cohérence) et le temps d'exécution des algorithmes,
- La capacité **d'intriquer/connecter les qubits** peut déterminer la rapidité d'exécution d' algorithmes quantiques. Plus la connectivité est grande, plus l'exécution d'un algorithme sera rapide,
- La **température de fonctionnement** des processeurs et de leur appareillage qui est très dépendante du type de qubits. Si l'idéal serait d'avoir un ordinateur fonctionnant à température ambiante, la plupart des technologies de qubit utilisées nécessitent de la cryogénie (de 10-15mK à quelques K),
- La **consommation totale d'énergie** de l'ensembles des composants de l'ordinateur (qui resterait largement à l'avantage des ordinateurs quantiques même en cas de besoin cryogénique par rapport aux supercalculateurs [150]),

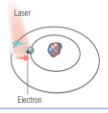
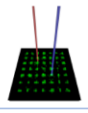
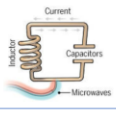
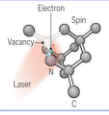
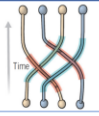
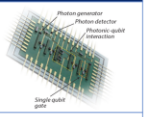
	Atomes		Electrons				Photons
Les illustrations sont pour la plupart extraites de "From Science News Feature, "Scientists are close to building a quantum computer that can beat a conventional one", Gabriel Popkin, 2016. Illustration by Chris Bickel/Science							
Technologie de qubit	**Ions piégés**	**Atomes froids**	**Supraconducteurs**	**Silicium (+quantum dot)**	**Impureté diamant (NV center)**	**Fermion de Majorana (topologique)**	**Photons**
Domaine d'application	métrologie, informatique, communication (répéteur, couplage avec photon)	métrologie, informatique, communication (couplage avec photon)	métrologie, informatique	métrologie, informatique	métrologie, communication, informatique	informatique	métrologie, communication, informatique
Nature des qubits	ions piégés électromagnétiquement	atomes piégés par des pinces laser	boucle/circuit supraconducteur	électrons piégés dans un semi-conducteur	électrons d'une cavité de diamant près d'un atome d'azote	quasi-particules, paires d'anyons, dans des nano-fils supraconducteurs	photons circulants dans des guides d'onde
États quantiques des qubits	niveau d'énergie de l'ion piégé	niveau d'énergie de l'atome	3 types: qubit de phase, de charge a.k.a transmon (niveau du courant) et de flux (sens du courant)	spin d'électron	niveau d'énergie des électrons du centre NV	sens de l'anyon	1 -propriété du photon (polarité ou autre)
Maturité (TRL) et potentiel de « Scale up » pour ordinateur quantique	**5** Extensibilité : relativement difficile	**4** Extensibilité : difficile	**5** Extensibilité : relativement facile	**3** Extensibilité : pas facile aujourd'hui mais bonne	**3** Extensibilité : relativement difficile	**1** Extensibilité : trop tôt pour se prononcer	**3** Extensibilité : difficile

Figure 80: Principales technologies de qubits: extrait de la figure 15 p.20

- La capacité de **miniaturisation** des qubits et des supports peut déterminer le nombre maximum possible de qubits pour une technologie donnée,
- Enfin, liées aux processus de fabrication, la **variabilité de la qualité** dans la production des qubits et la capacité à employer des **infrastructures existantes**.

Notons que le benchmarking impartial de ces métriques est en soi une problématique émergente, qui devrait donner lieu à la création d'une nouvelle discipline, et gageons que les tableaux de bord y intégreront également des éléments de comparaison ordinateurs quantiques / supercalculateurs[151].

Nous avons décrit chapitre §3.2 la plupart des systèmes physiques pouvant être utilisés pour construire un processeur quantique : ions piégés, atomes froids, supraconducteurs, semiconducteurs, centre NV, photons, qubits topologiques (Figure 80).

Comme nous l'avons vu, le niveau de maturité (TRL[156]) des technologies est très différent allant de 1(qubits topologiques) à 5 pour les ions piégés et supraconducteurs (Figure 80, ou Figure 21, p.27 plus détaillée). Néanmoins, pour la majorité d'entre elles, les **deux principaux défis** rencontrés à ce jour sont liés au critère N°3 de DiVincenzo (cf. différentes métriques, p.20&21, Figure 15,Figure 16):

i) **la décohérence** des qubits qui leur fait perdre leur état quantique de superposition ou d'intrication lorsqu'ils interagissent avec l'environnement,

ii) **les taux d'erreurs non négligeables** générés lorsque l'on opère sur les qubits avec des portes quantiques ainsi que lors de la lecture de leur état, ou dans une moindre mesure au moment de leur initialisation.

Les systèmes quantiques sont particulièrement sensibles aux interférences externes. Le bruit (vibration, température) peut faire s'effondrer l'état quantique d'un qubit avant qu'un calcul ne soit terminé, ce qui

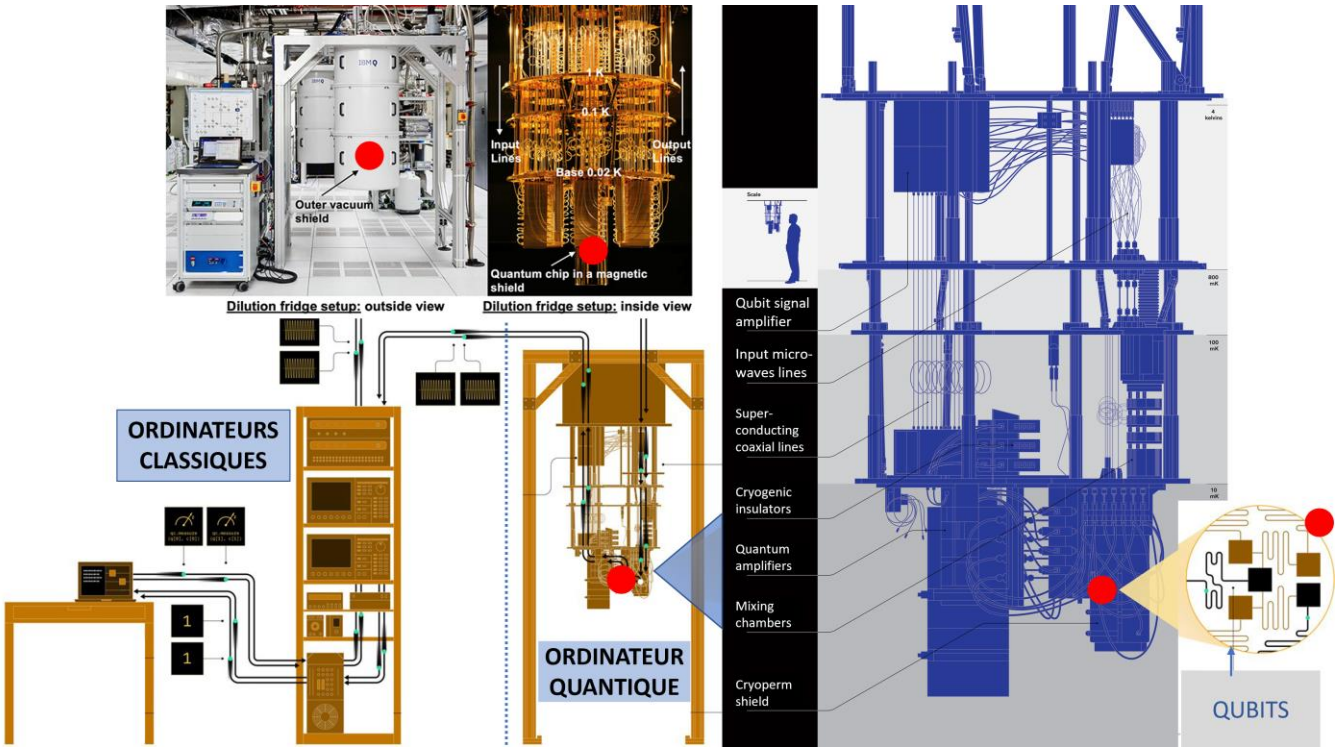


Figure 81: Éléments d'un ordinateur quantique d'IBM, montrant le contrôle et la mesure de bout en bout de qubits supraconducteurs. La température passe de 4 K en haut du réfrigérateur de dilution/chandelier (à droite) à seulement 15mK en bas où est situé le processeur hébergeant les qubits (point rouge) (Source: d'après photo et croquis IBM)

[156] L'échelle TRL (Technology Readiness Level) évalue le niveau de maturité d'une technologie sur une échelle allant de 1 à 9 avec 1 = observation du principe de base et 9 = système réel démontré en environnement opérationnel (Source: Wikipedia).

explique pourquoi beaucoup de ces plateformes nécessitent des appareillages de cryogénie et de vide pour isoler les qubits comme la figure 81 en illustre les dessous.

Les chercheurs s'efforcent d'atténuer les taux d'erreurs en explorant des pistes d'améliorations ou d'innovations tant matérielles que logicielles (qualité des qubits, technologies de contrôle, algorithmes). Le domaine de la correction des erreurs quantiques (QECC ou QEC[157]), objet de la prochaine section, offre des solutions de plus en plus matures. Mais c'est aussi une discipline qui évolue rapidement, et l'innovation dans ce domaine devrait contribuer tout autant à la future roadmap de l'informatique quantique que les innovations matérielles.

4.3.4. Correction des erreurs

Nous avons illustré la section précédente d'une photo d'ordinateur quantique. Considérons à présent la figure 82 : une partition musicale ? Bien étranges notes…et pourtant nous allons parler de haute-fidélité.

Ce diagramme est en fait une *partition (*ou *circuit*) *quantique* représentant un programme ou algorithme quantique. Les quatre lignes horizontales symbolisent un registre à 4 qubits. Les « notes » sont en fait des portes quantiques (opérations) qui sont successivement appliquées sur 1, 2, 3 ou 4 qubits. La partition se lit de gauche à droite et il y a ici une petite trentaine de portes.

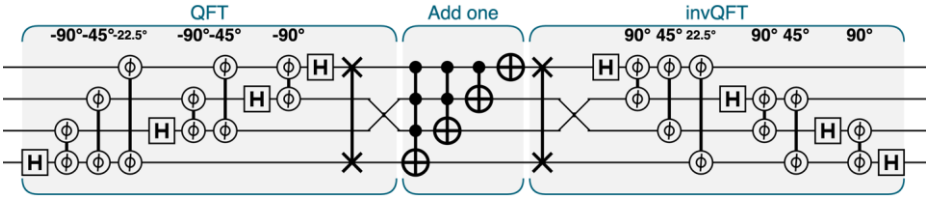


Figure 82: Partition quantique: les 4 lignes horizontales représentent 4 qubits auxquels est appliquée une succession de 28 portes quantiques, suivant une chronologie se lisant de gauche à droite (Source: Eric Johnston et al., « Programming Quantum Computers », Editions O'Reilly)

Les ordinateurs quantiques à portes actuels sont limités à quelques dizaines de qubits physiques (Figure 78) et la fiabilité de leurs calculs, matérialisés par l'application de portes quantiques à des qubits, est limitée. Ils font beaucoup trop d'erreurs pour offrir leur pleine puissance. Ces erreurs sont générées par des interactions entre les qubits et leur environnement.

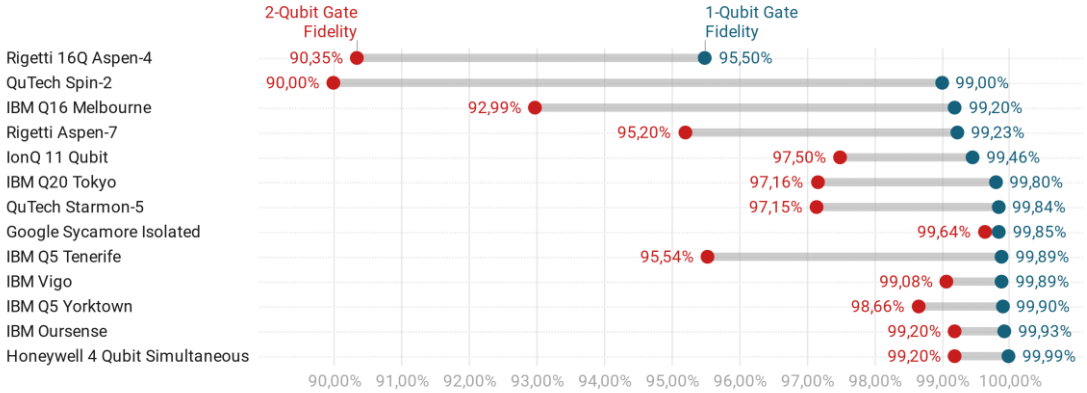


Figure 83: Taux de fidélité des portes quantiques unaires (1-Qubit gate en bleu) et binaires (2-Qubit gate en rouge) pour quelques ordinateurs quantiques existants (Données de https://quantumcomputingreport.com/qubit-quality/)

La figure 83 recense les taux de fidélité[158] de portes unaires et binaires d'une sélection d'ordinateurs quantiques existants. La fidélité des portes binaires est bien plus faible que celle des portes unaires. C'est aussi le cas pour la lecture (non présentée ici). Il faut donc toujours porter une attention particulière au taux de fidélité des portes binaires, lesquelles permettent de créer des états d'intrication, source d'une bonne partie de la puissance du calcul quantique.

[157] Quantum Error Correction (Code).
[158] Défini comme 100% moins le taux d'erreurs en question : porte 1 qubit, 2 qubits, lecture.

Quelle que soit la plateforme physique utilisée[159] et les problèmes de décohérence associés, les erreurs sont générées lors des manipulations physiques (par lasers, micro-ondes…) correspondant à l'application des opérations quantiques sur les qubits. Elles se cumulent lorsque l'on enchaîne plusieurs portes quantiques et une lecture finale. Elles deviennent prohibitives dès que l'on exécute trop de portes d'affilée. Un algorithme de seulement 20 opérations sur 53 qubits a moins de 1 chance sur 10 000 de donner le bon résultat[160]. Par ailleurs, notons que les premiers processeurs quantiques font 10^{19} fois plus d'erreurs[160] que les ordinateurs traditionnels (Figure 84).

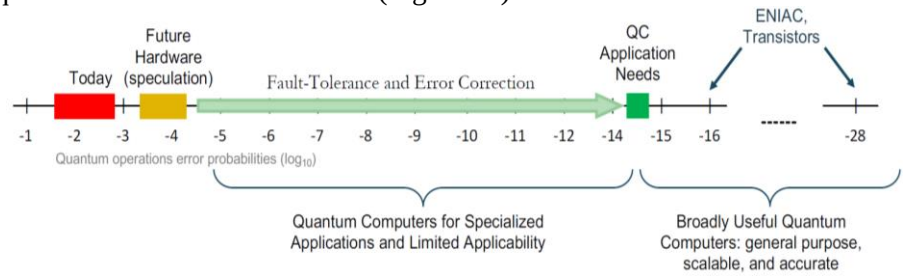


Figure 84: Décalage entre les valeurs des taux d'erreurs actuels et l'idéal pour une application de calcul sans correction d'erreurs (échelle log base 10 : -2 ← 10^{-2} … -28←10^{-28})
(Source: How about quantum computing? , De Jong)

Pour surpasser les supercalculateurs classiques, il est généralement admis qu'un ordinateur quantique devrait comporter 50 à 60 qubits parfaits, capables de réaliser des millions d'opérations sans erreur (e.g figure 85) mais pour cela le taux d'erreurs devrait être diminué de 12 ordres de grandeur par rapport à l'actuel (carré vert - Figure 84), ce qui est aujourd'hui hors de portée des physiciens qui, s'ils progressent régulièrement, ne grapillent qu'1 ou 2 ordres de grandeur[161]. C'est ici que les codes correcteurs d'erreurs quantiques (QECC ou QEC) se positionnent (orange et vert clair - Figure 84).

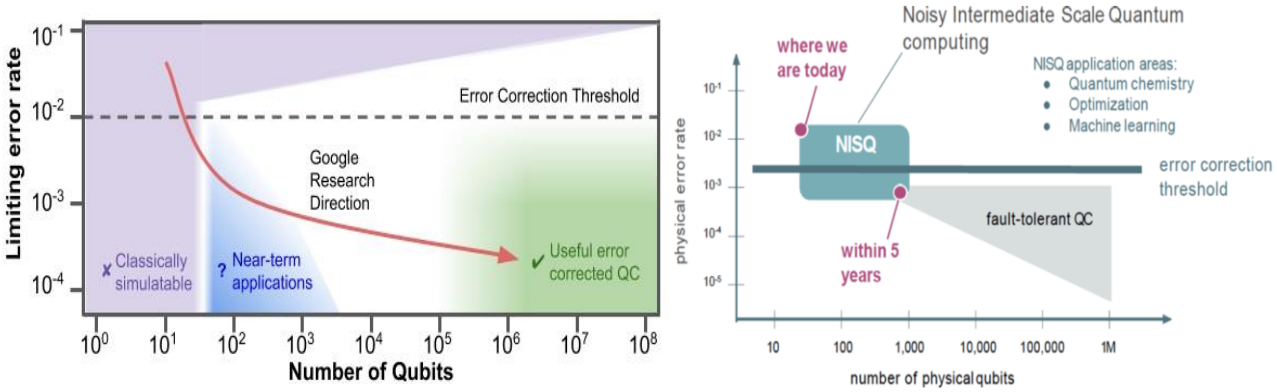


Figure 85: Graphiques conceptuels illustrant la relation entre le taux d'erreurs et le nombre de qubits. A gauche, le seuil d'environ 50-60 qubits et le taux d'erreurs de 1% voire 0,1% délimitent les zones des ordinateurs NISQ (bleu) puis universels (vert) inatteignables aux ordinateurs classiques (violet) (Source: Google). A droite, l'ordinateur universel aura plusieurs centaines de milliers voire des millions de qubits physiques (Source: [148])

Signalons, tout de même, qu'en attendant la mise en place future de tels systèmes, la solution explorée dans le cadre des ordinateurs NISQ, trop contraints par leur ressource, est de créer des algorithmes eux-mêmes tolérants aux erreurs. Ils sont souvent hybrides, faisant travailler en synergie ordinateurs classiques et quantiques. Nous en reparlerons dans la suite de ce chapitre.

Le domaine des QECC est particulièrement actif au niveau de la recherche. Ainsi, le nombre de publications est-il dense (voir par exemple [152],[153],[154]). Nous ne pourrons ici qu'effleurer ce sujet complexe à travers la présentation de quelques principes de bases.

[159] A l'exception peut-être des qubits topologiques mais qui sont encore à l'état de concept.
[160] Données communiquées lors d'un webinar de la Startup Alice&Bob visant à construire un ordinateur quantique utilisant des états particuliers d'atomes froids reconnus pour leur stabilité.
[161] Il est en théorie possible de ralentir le processus de décohérence d'un système quantique si on connait son environnement et sait le mesurer ou le manipuler, mais il n'y a pas de méthodes universelles pour protéger un système de qubits des effets perturbations d'un environnement arbitraire.

4.3.4.1. Types d'erreurs

L'interaction des qubits avec leur environnement immédiat engendre trois principaux types d'erreurs[144] :

i) Les **erreurs de flip,** comme illustré figure 86 sur la sphère de Bloch (§3.1.2), sont des erreurs d'amplitude où le vecteur représentant le qubit passerait d'un hémisphère vers l'autre, en l'occurrence souvent de |1⟩ vers |0⟩. C'est le seul type d'erreur commun avec l'informatique classique où un bit 1 peut devenir 0 suite à une erreur de transmission par exemple, On associe parfois à ce phénomène inexorable, même sans interactions manifestes des qubits, un temps moyen noté T1.

ii) Les **erreurs de phase (déphasage)** sont des rotations sur l'équateur (Figure 87), on mentionne parfois dans les métriques le temps de déphasage moyen T2. Notons que i) et ii) peuvent se combiner,

iii) Les **erreurs de fuite** (leakage errors) surviennent lorsque le qubit dérive et se stabilise dans un état énergétique autre que le |0⟩ ou le |1⟩ de base. Cela peut arriver, par exemple, lorsqu'un qubit se place dans un état |2⟩, niveau d'énergie, que l'on cherche normalement à éviter sur certaines plateformes physiques.

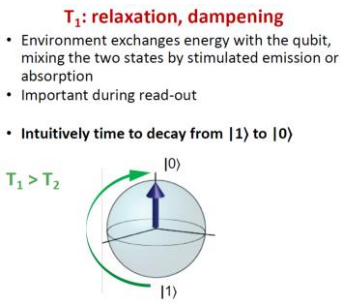


Figure 86: Types d'erreurs (Source: How about quantum computing?, De Jong)

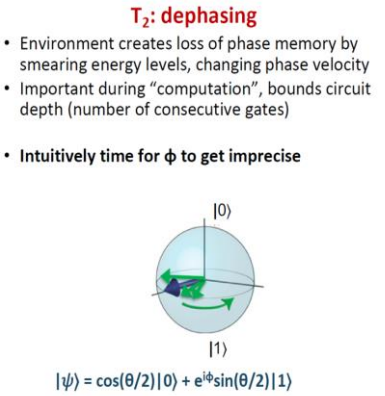


Figure 87: Erreur de phase (Source: How about quantum computing?, De Jong)

Les causes de ces erreurs sont multiples : erreur de calibrage des instruments de contrôles[162] des qubits (laser, micro-onde), bruits d'origine thermique, ou électromagnétique, radioactivité, etc...

Les problèmes de calibrage sont souvent à l'origine des erreurs de ***crosstalk (diaphonie)*** qui affectent la plupart des ordinateurs quantiques disposant de plus d'un qubit. Le *crosstalk* désigne l'effet d'une action souhaitée et effectuée sur un ou plusieurs qubits (e.g. opération d'une porte quantique) qui affecte involontairement un ou plusieurs autres qubits (et générant une des erreurs mentionnées précédemment). Il peut être particulièrement préjudiciable aux méthodes de corrections d'erreurs abordées à présent.

4.3.4.2. Correction des erreurs quantiques (QEC – *Quantum Error Correction*)

En informatique conventionnelle, lorsque l'on souhaite limiter les erreurs, par exemple pour la transmission d'un message constitué de bits, une solution consiste à envoyer plusieurs copies du même bit (**encodage**) de sorte qu'en cas d'erreur sur une des copies, il soit possible de la détecter (on parle de **détection de syndrome**) puis par un système de décision à la majorité de la **corriger** (Figure 88).

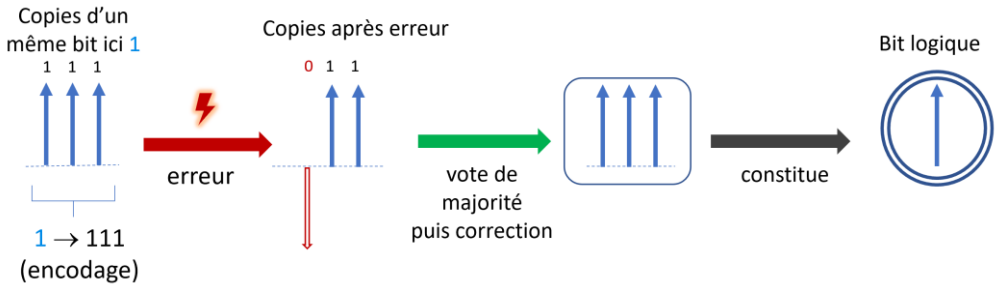


Figure 88: Système de correction de bit par répétition

[162] Le calibrage des instruments de contrôle consiste, entre autres, aux réglages précis des dispositifs utilisés pour opérer sur les états des qubits. Cela correspond, par exemple, aux réglages fins des fréquences micro-ondes, directions des lasers ou tout autre dispositif utilisé lors des manipulations des qubits ; initialisation des états, application des portes quantiques, mesures.

Les méthodes de correction des erreurs quantiques (appelées codes de correction et désignées sous le sigle **QECC** pour *Quantum Error-Correcting Codes*) reposent sur le même principe de redondance d'information.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \xrightarrow{encodage} \quad |\psi\rangle_L = \alpha|000\rangle + \beta|111\rangle$$

Toutefois son implémentation est très différente puisque les lois quantiques interdisent la copie d'un qubit[163]. La réplication se fait alors grâce aux propriétés de l'intrication quantique appliquée à un nombre de qubits physiques variable suivant les codes. **Plusieurs qubits physiques sont** donc **utilisés pour constituer** in fine **un seul qubit,** dit **logique**, capable de traiter parfaitement l'information ou le calcul.

i) Familles de codes

Il existe huit familles de codes de correction d'erreurs (Figure 89). Les plus documentés sont les codes stabilisateurs (*stabilizer codes*) qui détectent et corrigent les erreurs de flip et/ou de phase, et dont les protocoles les plus connus font intervenir trois[164], cinq (Bennett[155] & Laflamme[156]), sept (Steane[157] - assez usité) ou neuf qubits (Shor[158]).

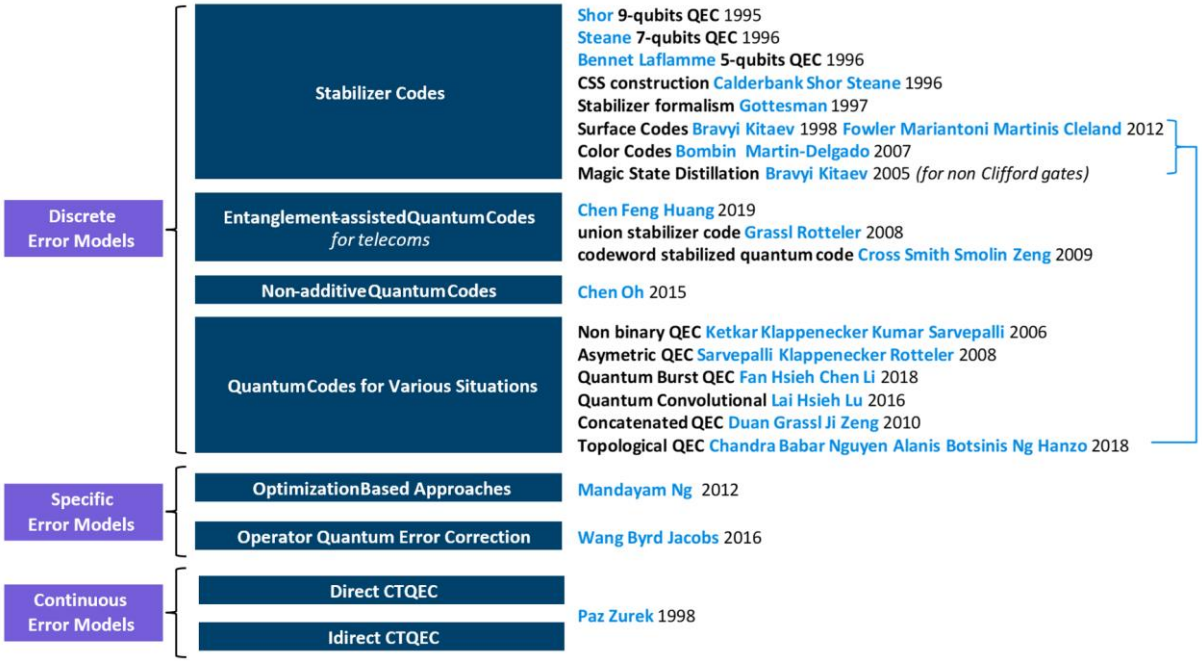


Figure 89: Famille de QECC (Sources : [144], [153])

Ces codes répliquent par intrication plusieurs fois les qubits de calcul pour leur appliquer les mêmes opérations en parallèle puis comparent les résultats en sortie des algorithmes pour ne conserver que les résultats les plus statistiquement significatifs.

Comme on ne doit pas lire la valeur des qubits de calcul, le protocole utilise des qubits auxiliaires qui servent à détecter des syndromes d'erreurs sans affecter les qubits principaux. C'est la redondance de l'information sur plusieurs qubits qui permet à la mesure de syndromes de ne pas détériorer l'information du système.

[163] L'information d'un qubit est en fait sa fonction d'onde, qui ne peut ni être clonée, ni mesurée sans être perturbée.
[164] Trois qubits sont peu utiles dans la pratique du calcul quantique car ils ne permettent de ne corriger que les erreurs de flip.

ii) Principe général de fonctionnement

Le schéma de figure 90 illustre le principe de fonctionnement de six étapes[144] d'un code de correction d'erreurs classique :

❶ **Préparation**: le qubit à corriger $|\psi\rangle$ va d'abord être répliqué par intrication sur plusieurs qubits auxiliaires (ici deux) pour créer un qubit logique $|\psi\rangle_L$.

❷ **Traitement** : un traitement, potentiellement source d'erreurs, s'effectue. Cela peut être un calcul ou une transmission de télécommunication du qubit.

❸ **Détection d'erreurs** : évaluation d'un syndrome en exploitant des qubits auxiliaires.

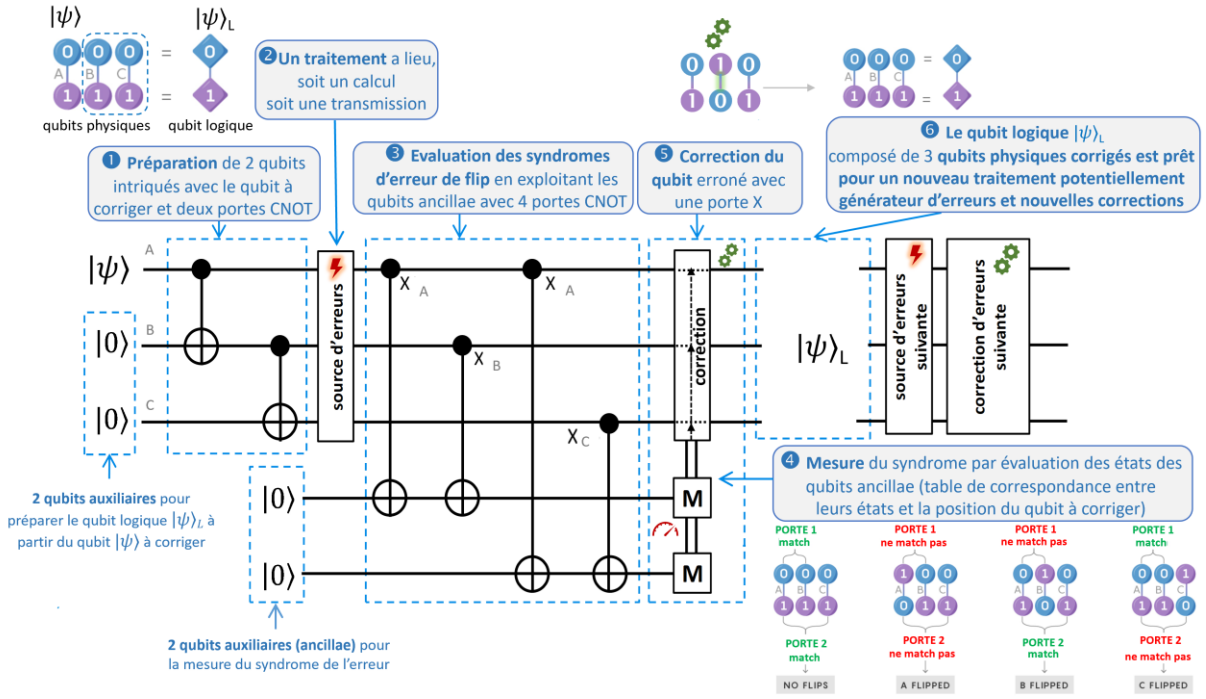


Figure 90: Code de correction d'erreurs de flip à trois qubits - les 6 étapes (Source : d'après [152], [144])

❹ **Mesure du syndrome d'erreur** : l'état de ces qubits auxiliaires est mesuré pour devenir des bits 0 ou 1 classiques. Combinés, ces bits donnent un code auquel correspond l'indice du qubit physique à corriger.

Résultats des mesures des qubits auxiliaires	Conséquence
00	Pas d'erreur
01	Erreur de flip sur le qubit C
10	Erreur de flip sur le qubit B
11	Erreur de flip sur le qubit A

❺ **Correction d'erreurs** : la mesure permet de déclencher la correction du qubit erroné avec une porte logique déterminée par le type d'erreurs corrigées (e.g. porte X pour une correction de flip).

❻ **Consolidation** : l'ensemble des qubits corrigés est conservé pour passer à une nouvelle opération à corriger : calcul (i.e. de nouvelles portes quantiques), transmission.

Les codes de correction d'erreurs ne peuvent pas corriger plusieurs erreurs en même temps. Enfin si la majorité des portes peut être contrôlée par ces QECC, certaines portes (e.g. « porte T », voir annexe 6), nécessaires car garantissant l'universalité de l'ensemble des portes quantiques (critère N°4 de DiVincenzo) imposent des codes de correction d'erreurs complémentaires spécifiques comme le ***magic state distillation***, que nous ne détaillerons pas ici.

iii) Les codes de surface (*surface codes*)

Ces dernières années se sont aussi développées des familles de protocoles utilisant des codes topologiques[165] comme les ***surface codes***[159] et les ***color codes***. Les codes de surface sont une famille de QECC bien adaptée aux technologies où les qubits peuvent être agencés de manière à être bien connectés à leurs plus proches voisins. La structure la plus souvent envisagée est celle d'un maillage de qubits en 2D, mais une structure 3D serait possible.

Dans la perspective future d'un ordinateur quantique universel (FTQC/LSQC), les codes de surface sont actuellement les codes de correction d'erreurs les plus étudiés par la communauté, en raison de leurs seuils de tolérance aux erreurs élevés et de leur dépendance aux seules mesures des voisins les plus proches[160].

À l'image du code de correction présenté précédemment, les surface codes font largement usage de qubits auxiliaires pour ne pas perturber le système quantique. Chaque code de cette famille possède des stabilisateurs (du système quantique) qui sont définis dans l'ensemble de manière équivalente, mais qui diffèrent par le traitement appliqué aux extrémités (bords) du maillage de qubits.

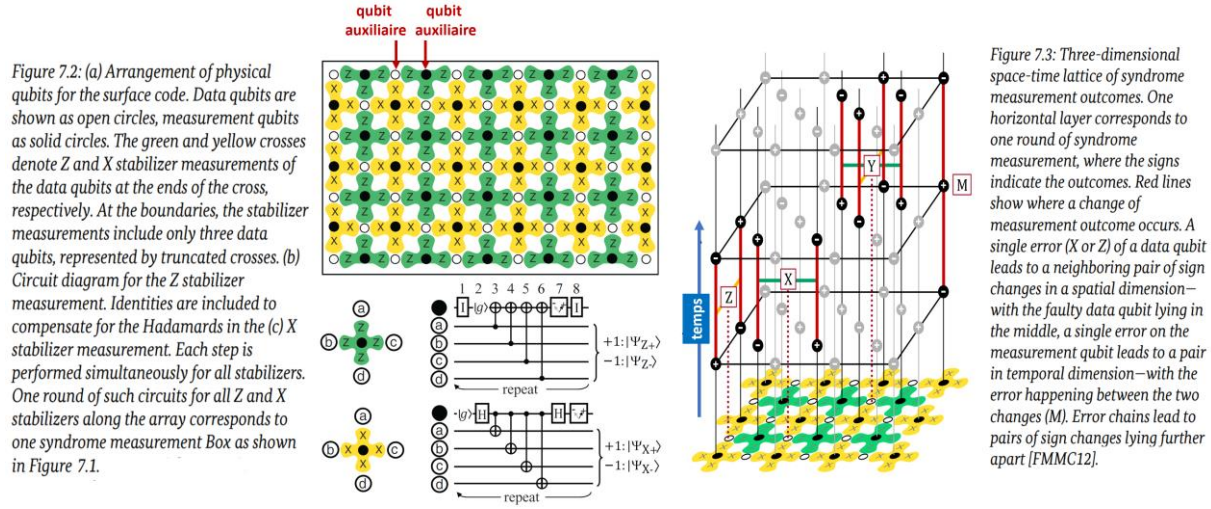


Figure 7.2: (a) Arrangement of physical qubits for the surface code. Data qubits are shown as open circles, measurement qubits as solid circles. The green and yellow crosses denote Z and X stabilizer measurements of the data qubits at the ends of the cross, respectively. At the boundaries, the stabilizer measurements include only three data qubits, represented by truncated crosses. (b) Circuit diagram for the Z stabilizer measurement. Identities are included to compensate for the Hadamards in the (c) X stabilizer measurement. Each step is performed simultaneously for all stabilizers. One round of such circuits for all Z and X stabilizers along the array corresponds to one syndrome measurement Box as shown in Figure 7.1.

Figure 7.3: Three-dimensional space-time lattice of syndrome measurement outcomes. One horizontal layer corresponds to one round of syndrome measurement, where the signs indicate the outcomes. Red lines show where a change of measurement outcome occurs. A single error (X or Z) of a data qubit leads to a neighboring pair of sign changes in a spatial dimension—with the faulty data qubit lying in the middle, a single error on the measurement qubit leads to a pair in temporal dimension—with the error happening between the two changes (M). Error chains lead to pairs of sign changes lying further apart [FMMC12].

Figure 91: Surface code - arrangement des qubits de calcul (rond blanc) et auxiliaires (rond noir) ainsi que des portes constituant les opérateurs stabilisateurs en croix (gauche) - séquence temporelle de la mesure de syndrome (droite) (Source: [158])

Les stabilisateurs sont des ensembles d'opérateurs (constitués de portes logiques : portes Z (verts) et porte X (jaunes) ici placées en croix, sauf sur les bords – figure 91) dont on peut mesurer et contrôler les états simultanément sans perturber le système. Ils utilisent des qubits auxiliaires (en noir).

Les stabilisateurs font l'objet d'un formalisme mathématique qui ne sera pas abordé ici. Ils sont très importants pour préserver les états quantiques. En mesurant de manière répétée un système quantique à l'aide d'un ensemble complet de stabilisateurs, le système est forcé à rester dans un état propre[166] simultané et unique de tous les stabilisateurs. On peut mesurer les stabilisateurs sans perturber le système. Lorsque les résultats des mesures changent, cela correspond à une ou plusieurs erreurs de qubit, et l'état quantique du système peut être corrigé.

Les codes de surface partagent les caractéristiques communes suivantes :

- Plus tolérants que d'autres codes, ils fonctionnent pour des qubits physiques et portes ayant des taux d'erreurs allant jusqu'au seuil de 1% (10^{-2}). L'objectif est de construire des qubits logiques, ayant quant à eux des taux d'erreurs inférieurs d'environ dix ordres de grandeur (e.g. 10^{-12} - Figure 84).

[165] Sans lien avec les qubits topologiques. Le terme fait référence à l'agencement des qubits sous forme d'un quadrillage 2D.
[166] Au sens mathématique et physique du terme, comprenons le ici comme un état d'équilibre.

- Dans le treillis 2D, les seules interactions requises sont entre qubits « voisins ». La distance de voisinage à prendre en compte lors de la mesure est un sujet de recherche (Figure 92), sachant qu'en théorie au moins 5 qubits sont nécessaires pour pouvoir corriger à la fois les erreurs de flip et de phase. Par ailleurs, plus on contrôle une surface étendue, plus le nombre de qubits nécessaires est faible pour un taux d'erreurs cible[167] fixé[38].

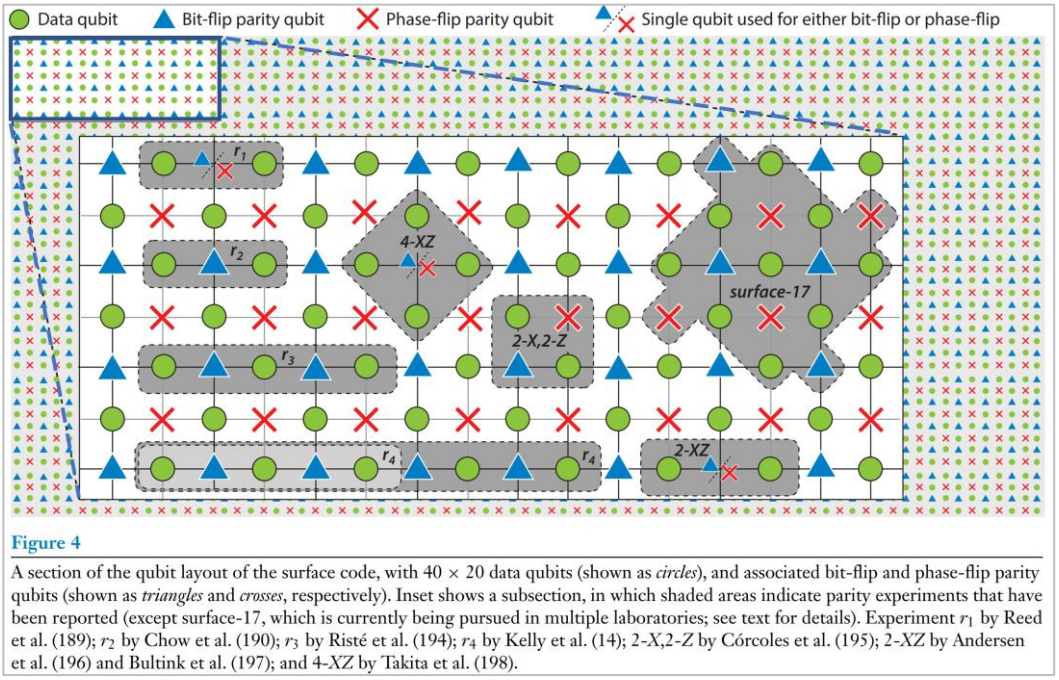


Figure 4

A section of the qubit layout of the surface code, with 40 × 20 data qubits (shown as *circles*), and associated bit-flip and phase-flip parity qubits (shown as *triangles* and *crosses*, respectively). Inset shows a subsection, in which shaded areas indicate parity experiments that have been reported (except surface-17, which is currently being pursued in multiple laboratories; see text for details). Experiment r_1 by Reed et al. (189); r_2 by Chow et al. (190); r_3 by Risté et al. (194); r_4 by Kelly et al. (14); 2-*X*,2-*Z* by Córcoles et al. (195); 2-*XZ* by Andersen et al. (196) and Bultink et al. (197); and 4-*XZ* by Takita et al. (198).

Figure 92: Surface code : diverses expérimentations portant sur des géométries de mesures différentes (Source:[38])

- Les surface codes permettent de corriger les erreurs de flip (Porte X) et de phase (Porte Z), toutefois de récentes propositions permettraient la correction des erreurs de fuite (leakage errors)[161].
- La majorité des portes quantiques peut être corrigée, bien qu'il manque la Porte T ou celle de Toffoli pour constituer un ensemble universel de portes quantiques,
- L'une ou l'autre des portes manquantes peut être rétablie par la technique du *magic state distillation*, mais nécessite des qubits auxiliaires supplémentaires, ce qui est généralement considéré comme un goulot d'étranglement possible pour les futurs calculs fonctionnels[162].
- Pour être suffisamment efficaces, les codes de surface nécessitent un plus grand nombre de qubits physiques par qubit logique ce qui pourra créer des contraintes de conception puisque les qubits doivent être reliés à leurs voisins immédiats dans une structure 2D.

  En matière de métrique, suivant les sources académiques, on trouve des rapports allant de 100 à 10 000 qubits physiques par qubit logique. Dans une étude récente[100], les chercheurs ont démontré (théoriquement) qu'en appliquant l'algorithme de Shor avec 20 millions de qubits physiques ils pourraient casser une clé RSA de 2 048 bits en 8 heures (Figure 93) alors qu'il faut en théorie 4 098 qubits logiques(Annexe 7). Ce qui donne un ratio 1 pour 5 000.

	Physical assumptions				Approach		Estimated costs		
Historical cost estimate at $n = 2048$	Physical gate error rate	Cycle time (microseconds)	Reaction time (microseconds)	Physical connectivity	Distillation strategy	Execution strategy	Physical qubits (millions)	Expected runtime (days)	Expected volume (megaqubitdays)
Fowler et al. 2012 [9]	0.1%	1	0.1	planar	1200 T	single threaded	1000	1.1	1100
O'Gorman et al. 2017 [18]	0.1%	10	1	arbitrary	block CCZ	single threaded	230	3.7	850
Gheorghiu et al. 2019 [19]	0.1%	0.2	0.1	planar	1100 T	single threaded	170	1	170
(ours) 2019 (1 factory)	0.1%	1	10	planar	1 CCZ	serial distillation	16	6	90
(ours) 2019 (1 thread)	0.1%	1	10	planar	14 CCZ	single threaded	19	0.36	6.6
(ours) 2019 (parallel)	**0.1%**	**1**	**10**	**planar**	**28 CCZ**	**double threaded**	**20**	**0.31**	**5.9**

Figure 93: 20 millions de qubits physiques pour exécuter l'algorithme de factorisation de Shor sur une clé RSA 2048 (le nombre nécessaire de qubits logiques étant de 4098) (Source : [100])

[167] Du qubit logique.

Les codes de surface présentent des inconvénients, notamment la nécessité d'utiliser des *magic states* et un nombre important de qubits physiques. Pour essayer de faire mieux, diverses variantes sont en cours de développement. Un exemple notable est une autre famille de codes topologiques connue sous le nom de color codes[163] mais il existe bien d'autres pistes actuellement explorées.

iv) Perspectives sur les QECC

Les codes de correction d'erreurs (QECC), en introduisant redondance, qubits auxiliaires, enchainements de portes quantiques et mesures supplémentaires, peuvent être du coup, eux-mêmes, générateurs de nouvelles erreurs. Il est d'ailleurs probable que, passé un certain nombre de qubits physiques, le taux d'erreurs des qubits logiques constitués ne diminue plus.

La plupart des QECC ne corrigent pas toutes les erreurs, ne serait-ce que, lorsque plusieurs surviennent au même moment. Pour tirer profit des avantages de différents types de codes, il serait possible de créer un QECC concaténant différents codes correcteurs, lesquels seraient appliqués récursivement[164] jusqu'à atteindre le taux d'erreurs souhaité. Au-delà du bénéfice direct lié à la diminution attendue du taux d'erreurs, un des avantages collatéraux des QECC est de rallonger la durée de cohérence des qubits puisque chaque correction revient à en réinitialiser les temps de cohérence T1 (flip) et T2 (phase). Cela permettra de faire fonctionner des algorithmes contenant plus de portes (dits plus profonds).

Il existe un champ exploratoire connexe assez large visant à mettre en place des mécanismes de correction d'erreurs bas niveau, i.e. au sein même des qubits. Outre les qubits topologiques étudiés entre autres par Microsoft[168], la technologie de *cat-qubits* développée par la startup française Alice & Bob[169] semble prometteuse. La société a ainsi l'ambition de commercialiser, d'ici 2024, un ordinateur quantique utilisant une technologie de qubits supraconducteurs plus fiables que l'état de l'art. Le codage de l'information quantique y est différent et les qubits seraient capables de se stabiliser et de s'auto-réguler eux-mêmes.

La nature des supports physiques des qubits est variée, allant des ions piégés aux qubits topologiques en passant par les qubits supraconducteurs. Chacune des technologies étudiées présente des forces et des faiblesses qui prennent plus ou moins d'importance, quand il s'agit d'envisager le passage à l'échelle pour l'ordinateur quantique universel (LSQC/FTQC). En dehors des technologies prospectives mentionnées dans le paragraphe précédent, il est certain que la voie vers ce futur ordinateur passera par l'intégration de QECC performants adaptés aux technologies qui se démarqueront.

Il est aussi important de réaliser que le nombre exact de qubits requis dépend d'une combinaison complexe entre i) les spécifications matérielles supposées de chacune des technologies (fidélité, interconnectivité, portes prises en charge) et ii) les capacités des QECC compatibles avec cette technologie. Chaque protocole a ses propres caractéristiques (taille de la cellule logique, nombre de qubits requis, vitesse de traitement). Pour l'ordinateur quantique universel, la grande majorité des qubits physiques requis provient des besoins de la correction d'erreurs, et non des applications ou algorithmes quantiques sous-jacents.

4.3.5. Familles d'algorithmes et applications

Le calcul numérique acquiert une place prépondérante dans notre société avec des besoins de plus en plus importants qui imposent aux acteurs du secteur une course à la puissance effrénée comme nous pouvons le constater dans l'évolution du secteur des supercalculateurs (Figure 68 p.60). Sans revenir sur les limites possibles des technologies traditionnelles et les avantages théoriques des calculateurs quantiques (§4.3.1) on peut comprendre que le champ d'application de l'informatique quantique serait très large. Il faut rester toutefois prudent et ne pas tomber dans une surenchère technologique.

[168] Dont le degré de maturité technologique est très bas (TRL=1).
[169] https://www.linkedin.com/company/alice-bob/about/

Le nombre d'algorithmes quantiques, destinés à tirer parti des simulateurs et ordinateurs quantiques, n'est pas très important à ce jour. Le site Quantum Algorithm Zoo en recense une soixantaine de classes[170] à partir des publications scientifiques afférentes. Ce nombre modeste n'a rien d'étonnant puisque cela ne fait qu'une trentaine d'années que les premiers ont été publiés, dix ans avant que les premiers ordinateurs quantiques n'apparaissent !

Leur étalonnage face aux algorithmes traditionnels, eux-mêmes en constante évolution, n'est pas facile et l'avantage quantique pas toujours évident à démontrer, même si sur le papier, leur capacité à diminuer la complexité[171] des problèmes auxquels ils s'attaquent est démontrée. La comparaison peut être d'autant plus délicate que le paysage évolue rapidement avec d'un côté des **algorithmes inspirés par le quantique (*quantum inspired*)** mais destinés à des ordinateurs classiques qui continuent à bien se développer [165], et de l'autre le fait que les recherches sur les algorithmes quantiques et le *hardware* se font maintenant en parallèle.

Du point de vue des applications, il est donc essentiel de comprendre au cas par cas : « quels types d'algorithmes quantiques pourraient être utilisés ? » et « pour une application donnée, quelle est l'ampleur de l'avantage procuré par l'utilisation d'un algorithme / ordinateur quantique par rapport à un algorithme / ordinateur traditionnel? ».

A cet instant, deux situations peuvent alors se rencontrer :

i) il existe déjà des algorithmes exploitables sur un ordinateur quantique actuel et susceptibles de délivrer un avantage moyennant juste des mises au point. Dans ce cas, les acteurs de différents secteurs économiques peuvent tester la solution quantique sur des problèmes réels (Total, BMW, Airbus, BBVA, JP Morgan).

ii) il n'existe pas d'algorithmes ou leur mise au point est contingente à l'amélioration simultanée du matériel (e.g. plus de qubits, taux d'erreurs plus faible…). On est ici sur de l'exploratoire. Le secteur du logiciel quantique y est très actif, certaines entreprises développant même des logiciels avant que le matériel ne soit disponible.

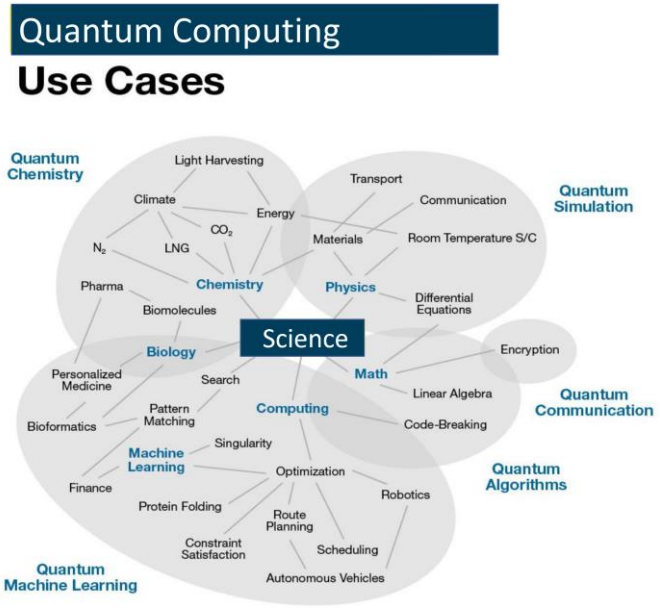


Figure 94: Domaines et cas d'usage de l'informatique quantique (Source: d'après P. Schadbolt & J O'Brien)

Passons à présent rapidement en revue quelques-uns des éléments du schéma présenté figure 94 et pour lesquels l'informatique quantique devrait être particulièrement bien adaptée.

4.3.5.1. Factorisation des grands nombres - Cryptographie

Comme nous l'avons détaillé dans la partie de ce document dédiée aux télécommunications quantiques (§4.2) les ordinateurs quantiques sont théoriquement capables d'exploiter l'algorithme de Shor (sujet de l'annexe 7) pour craquer les méthodes courantes de cryptographie à clé publique. Conçu pour la première fois en 1994, soit une dizaine d'années après que les ordinateurs quantiques aient été proposés, l'algorithme de Shor a révélé une nouvelle approche de la factorisation des grands nombres et a ravivé

[170] Au 23 septembre 2020 : 420 algorithmes, beaucoup similaires, regroupés en 60 classes.
[171] A dessein nous n'avons pas abordé dans ce document la théorie de la complexité qui, en informatique, étudie formellement la quantité de ressources (temps, espace mémoire…) dont a besoin un algorithme pour résoudre un problème algorithmique. Il s'agit donc d'étudier la difficulté intrinsèque des problèmes, de les organiser par classes de complexité et d'étudier les relations entre les classes de complexité (Wikipedia).

l'intérêt pour le développement de cryptosystèmes *quantum-safe* (PQC) ou quantiques (QKD) capables de lui résister.

4.3.5.2. Recherche dans une bases de données

L'algorithme quantique de Grover[166] permet d'effectuer une recherche précise dans des bases de données non triées (e.g. trouver à partir d'un numéro de téléphone, le nom associé dans un annuaire). Il s'avère utile pour tout algorithme nécessitant une telle recherche heuristique ou exhaustive. Ses applications sont donc multiples. Ainsi, peut-il être utilisé en cryptanalyse comme l'algorithme de Shor, (§ 4.2.3 p.45). Il permettrait un gain quadratique[172] du temps de calcul (annexe 9 pour plus de détails).

4.3.5.3. Simulation

Les simulations quantiques[173], à la base de l'idée originelle d'ordinateur quantique articulée par le physicien Richard Feynman[14] en 1981, sont l'une des applications les plus prometteuses de l'informatique quantique, particulièrement dans le domaine de la chimie et de la science des matériaux où règnent les lois de la physique quantique. Feynman disait en substance : « *Quoi de mieux qu'un système quantique [que l'on peut contrôler] pour simuler un autre système quantique ?* »

La simulation informatique désigne l'exécution d'un programme informatique sur un ordinateur pour simuler un phénomène physique. Elle conduit à la description du résultat de ce phénomène, comme s'il s'était réellement produit[174].

Depuis des décennies, les simulations traditionnelles élargissent notre compréhension des systèmes quantiques. Mais si les équations modélisant les phénomènes étudiés sont connues, et l'usage de supercalculateurs de plus en plus fréquent, il faut souvent recourir à des simplifications car la complexité de résolution croît exponentiellement avec le nombre d'éléments du système. L'imprécision limite en fin de compte la fiabilité ou la portée des résultats en les rendant parfois inapplicables à la réalité.

Parmi les problèmes classiques, citons les systèmes à plusieurs corps[175] (astres, particules), ou bien

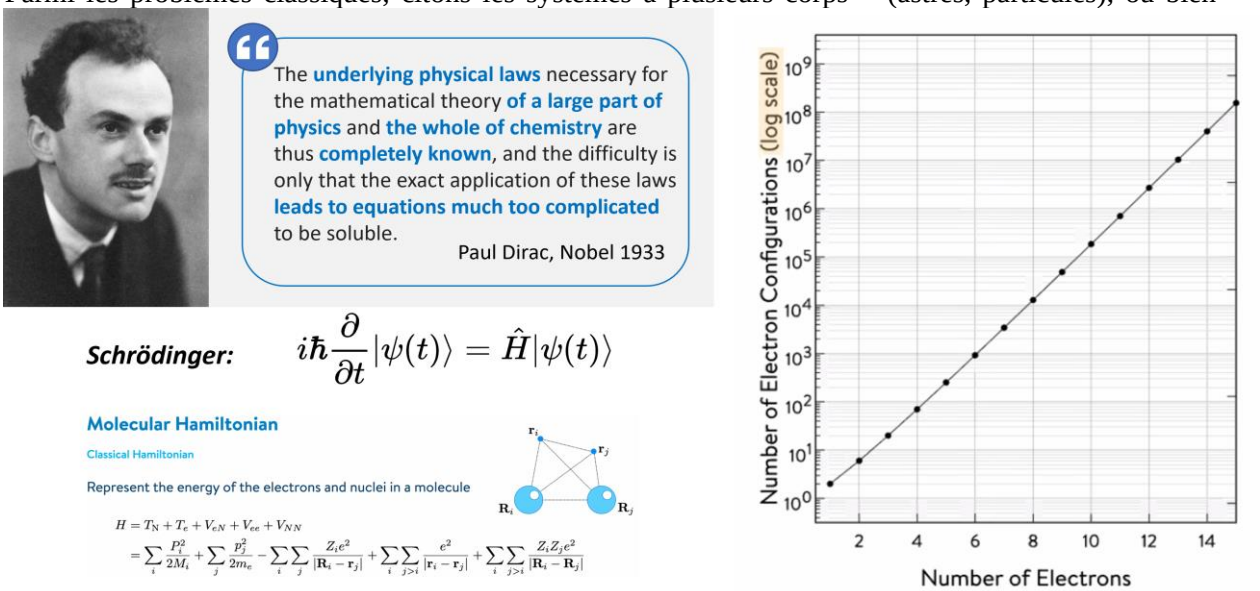


Figure 95: Citation Paul Dirac. Equation de Schrödinger, Hamiltonien et croissance exponentielle du nombre de configurations électroniques possibles en fonction du nombre d'électrons du système étudié (échelle log – Source: 1Qbit)

[172] Lorsque N, le nombre d'éléments de la base de données, augmente, le temps de calcul n'augmente qu'en $\sqrt{N}$, au lieu de N.
[173] Ne pas confondre les simulateurs quantiques avec les émulateurs quantiques (§4.3.2.1)
[174] Source: Wikipedia
[175] En physique newtonienne, le problème à plusieurs corps (ou n-corps) consiste à résoudre les équations du mouvement de Newton de n-corps interagissant gravitationnellement (e.g. des astres). Le terme peut être étendu à des systèmes dans lesquels interagissent n-éléments (e.g. des particules) soumis à différents types de forces.

l'équation de Schrödinger qui reste analytiquement insoluble pour les systèmes à plus d'un électron, où le nombre de configurations augmente exponentiellement[167] (Figure 95).

A l'inverse, les simulations quantiques permettraient d'étudier avec précision ces systèmes quantiques difficiles à expérimenter en laboratoire et impossibles à modéliser avec un supercalculateur.

Appliquées à la chimie, elles permettraient de mieux comprendre et concevoir les réactions chimiques, allant de la transformation de l'azote en ammoniac comme base de la production d'engrais (voir le procédé de Haber Bosch présenté au §1[168]), à la conception de produits pharmaceutiques[169], [170] en passant par l'optimisation de la photosynthèse en vue d'améliorer la capture du CO_2 ou la production de carburant synthétique[171].

De la même façon, des problèmes en science des matériaux pourraient être abordés beaucoup plus efficacement comme la recherche de matériaux augmentant les rendements des cellules solaires[172] ou l'efficacité des batteries. Cela pourrait aussi aider à répondre à des questions non résolues telle que la supraconductivité à haute température[173].

Les industries automobile et pharmaceutique explorent déjà les possibilités offertes par les ordinateurs quantiques pour la simulation chimique en vue de la conception moléculaire de nouveaux matériaux et médicaments. Par exemple, Volkswagen teste l'ordinateur quantique commercialisé par D-Wave (de type annealer, §4.3.2.2) pour simuler différentes options de matériaux pour les batteries des véhicules électriques[174] ; les premiers résultats sont pour l'instant en demi-teintes[175]. La R&D BMW[176] travaille également sur les matériaux de batteries avec l'objectif à long terme de pouvoir simuler des matériaux pertinents avec une précision égale à celle de l'expérimentation. Selon eux, les points clés à retenir à ce jour sont :

- Les simulateurs et ordinateurs NISQ sont encore trop limités pour les problèmes chimiques liés à l'industrie en raison principalement des taux d'erreurs actuels trop élevés.
- Néanmoins, c'est un sujet plus que jamais d'actualité pour la R&D, tant sur la partie algorithmique que matérielle. L'objectif est d'augmenter la capacité, la fiabilité, et la précision de résolution des systèmes employés pour pouvoir les basculer à l'échelle industrielle sur des problèmes réels.
- Les futurs ordinateurs quantiques universels, tolérants aux erreurs, apporteront des bénéfices majeurs.

Des entreprises pharmaceutiques, telle Biogen, évaluent l'utilité des ordinateurs quantiques pour leur processus de découverte de médicaments [176]. Il faut dire que ce secteur est particulièrement touché par l'augmentation des coûts de production de nouveaux médicaments comme en atteste la loi empirique d'Eroom (Figure 96) selon laquelle la découverte de médicaments coûte environ le double tous les 9 ans[177]. Cette loi est en contraste avec la loi de Moore selon laquelle la puissance de calcul informatique double tous les 18 mois pour un coût équivalent[177]. Le changement de paradigme qu'apporteraient de nouvelles méthodes de simulations de chimie quantique, pourrait aider à améliorer la situation.

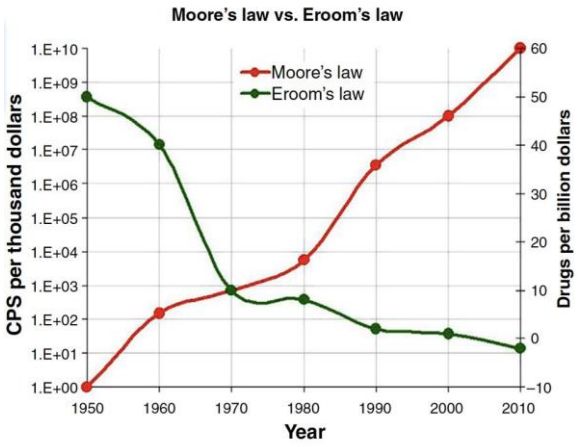


Figure 96: Loi d'Eroom vs loi de Moore (Source: Forbes)

[176] Showcase BWM, Quantum Tech Digital Week, 16 June 2020.
[177] Mettre un nouveau médicament sur le marché coute de 1 à 4 mds USD$ et prend de 10 à 15 ans (Source: Forbes [177])

La simulation quantique ne se cantonne pas à la simulation de systèmes physico-chimiques. Elle peut également être avantageusement utilisée pour la simulation de modèles ou **scénarios** sur des marchés finaux aussi variés que les sciences de la vie, la distribution et la logistique. Dans le secteur bancaire et financier, où des problèmes de simulation se retrouvent à chaque étape du cycle de vie du client, la puissance calculatoire de la simulation quantique pourrait ainsi améliorer l'évaluation des risques ou encore la détermination de prix d'instruments financiers complexes[178].

Plusieurs algorithmes de simulation quantique ont déjà été proposés et testés sur des ordinateurs quantiques[169]. **Un axe de recherche prometteur est celui des approches hybrides quantique/classique** dans lesquelles certains calculs sont sous-traités sur des ordinateurs classiques. Par exemple, la simulation d'un système quantique nécessite la préparation de l'opérateur Hamiltonien *H* correspondant à l'énergie totale du système et caractérisant son évolution dans le temps (par l'équation de Schrödinger - Figure 95). Certains éléments liés à l'Hamiltonien peuvent être précalculés sur un ordinateur classique et ensuite chargés sur l'ordinateur quantique en tant que paramètres. Réciproquement, un ordinateur quantique est utilisé pour accélérer les parties critiques des simulations.

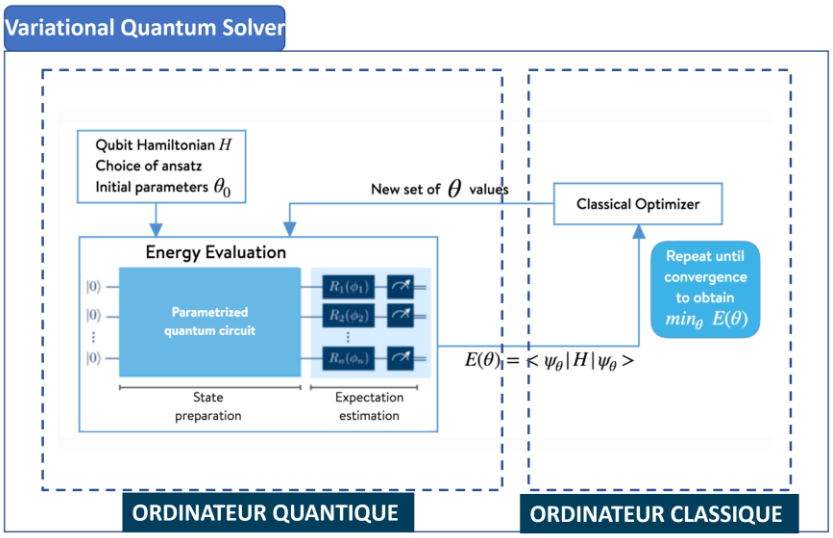


Figure 97:Algorithme VQE de la classe des algorithmes hybrides et utilisant une méthode variationnelle (Source: d'après 1QBit)

Les propriétés de l'état fondamental[178] d'un système quantique, tel son niveau d'énergie (minimum énergétique), sont généralement obtenues à l'aide de méthodes dites variationnelles à l'instar de l'algorithme hybride **VQE** (**Variational Quantum Eigensolver**[179], [180]), qui converge, par itérations successives, vers le résultat recherché (Figure 97). Ces méthodes sont particulièrement adaptées aux ordinateurs quantiques existants aujourd'hui (technologie NISQ) pour peu que le nombre d'étapes du calcul ne soit pas trop grand (les erreurs se cumulant au fur et à mesure du processus). Par contre, compte tenu du nombre et de la qualité des qubits disponibles sur les plateformes existantes (ou à venir dans un futur proche), il est encore difficile de dire si elles permettront de surpasser les algorithmes classiques qui trouvent des solutions approximatives aux mêmes problèmes[148].

Les algorithmes de simulation atomistique ou moléculaire devraient fonctionner le plus efficacement sur un ordinateur quantique universel (qubits & portes avec tolérance aux fautes). En attendant donc d'avoir un tel ordinateur, disposant de cinquante à quelques centaines de qubits logiques, les recherches s'effectuent sur des ordinateurs à recuit quantique (D-Wave) voire dans des simulateurs quantiques analogiques qui sont assez adaptés aux problèmes de détermination des niveaux d'énergie minimale de systèmes quantiques simples. Pour clore cette section, la figure 98 illustre l'augmentation conséquente du nombre de qubits nécessaires pour simuler le fonctionnement de la protéine MRC2 présente chez les mitochondries[181], donnant ainsi une idée des défis à venir dans le domaine de la chimie quantique.

[178] En physique quantique, connaitre les états fondamentaux d'un système, états quantiques de plus basse énergie, est primordial.

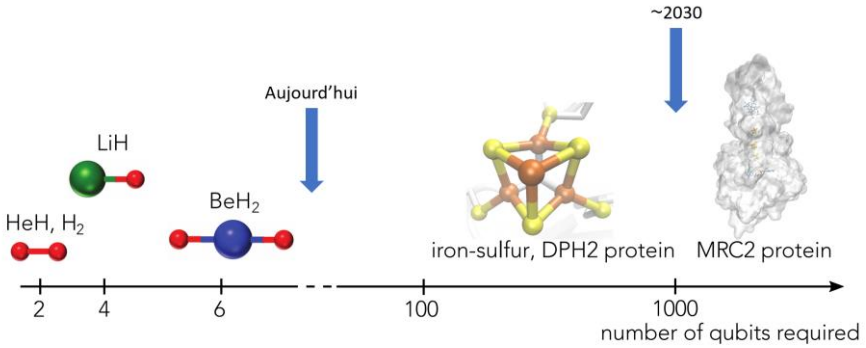


Figure 98: Qubits logiques nécessaires à la chimie quantique (Source:[181])

4.3.5.4. Optimisation

Les ordinateurs quantiques peuvent en théorie résoudre plus efficacement les problèmes d'optimisation, dont l'objectif est de trouver l'optimum d'une fonction. L'optimisation numérique est une brique de base de nombreux modèles de simulation et du machine learning (objet de la section suivante).

Par sa rapidité et sa capacité de calcul exponentielle, le processeur quantique peut évaluer de nombreuses solutions potentielles et trouver l'optimum recherché. Ces problématiques concernent un large éventail de secteurs industriels, allant de la santé ou la chimie (simulation, configuration de molécules), à la planification des processus de fabrication, ou l'optimisation des chaînes d'approvisionnement en passant par la finance (optimisation de portefeuilles).

Les principaux problèmes d'optimisations visés appartiennent à la catégorie des problèmes combinatoires dits **NP-complets**[179], pour lesquels **il n'y a pas de meilleure heuristique que de tester toutes les possibilités**, mais où il est facile de vérifier la validité d'une solution.

Les temps d'exécution nécessaires aux algorithmes de résolution de ces problèmes varient de manière exponentielle avec la taille des données en entrée et peuvent être très longs sur des machines conventionnelles. Les algorithmes quantiques pourraient les réduire significativement. Les problèmes NP-complets du « sac à dos »[180] ou du « **voyageur de commerce**[181]» sont deux archétypes illustrant bien cette classe de complexité (Figure 99).

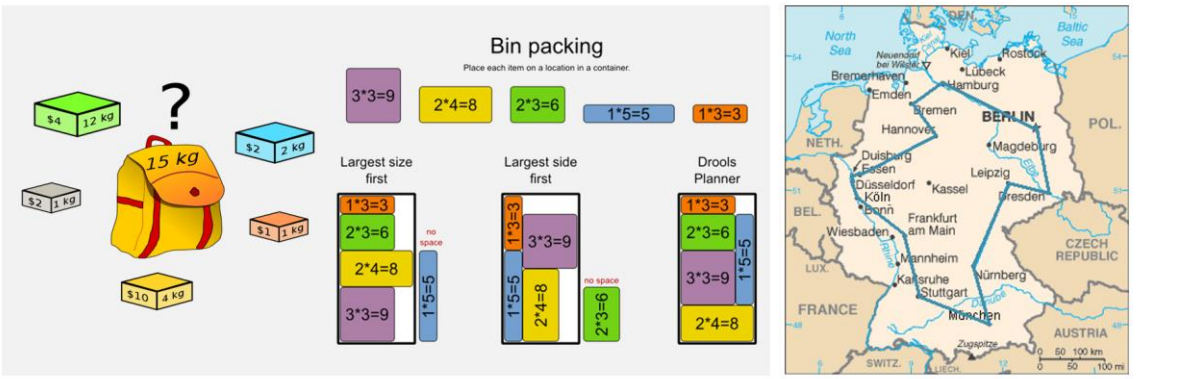


Figure 99: Deux problèmes NP-complets : le sac à dos dont il faut maximiser le contenu et le voyageur de commerce (Source: Wikipedia, stackoverflow.com, Wikipedia)

[179] Nous n'aborderons pas dans ce document la définition de l'ensemble des **classes de complexité** de la théorie informatique.
[180] Le problème est ici de remplir un sac à dos de manière optimale avec un jeu d'objets ayant chacun un poids et une valeur , pour maximiser la valeur et sans dépasser un poids maximum.
[181] Aussi appelé problème du commis voyageur.

Le défi du voyageur de commerce consiste à trouver le trajet le plus court d'un commis voyageur dont la mission est de visiter une liste de villes en y passant une et une seule fois. Ce type de combinatoire se retrouve dans de nombreuses applications comme dans la distribution d'électricité sur une grille électrique où la production est décentralisée (photovoltaïque, centrale, éolien…), et la consommation variable suivant la saison, l'heure de la journée, l'endroit[182]. Des tests de résolutions par un ordinateur quantique sont aussi en cours dans d'autres secteurs. BMW[182] a étudié par exemple l'optimisation des mouvements des robots en charge de la pose des joints d'étanchéité PVC sur ses véhicules et travaille sur un projet d'optimisation de l'offre de mobilité à la demande − affectation des véhicules à la commande d'un passager (Figure 100). Airbus a lancé un concours portant sur la capacité des ordinateurs quantiques à résoudre des problèmes d'intérêt pratique aussi variés que l'évaluation de la trajectoire ascendante la plus économique en carburant, ou l'optimisation du chargement des avions[183].

Figure 100: Portefeuille de projets BMW en "optimisation quantique" (Source: BMW)

D'autres entreprises évaluent également les possibilités offertes par l'ordinateur à recuit quantique de D-Wave (même s'il ne peut résoudre toutes les problématiques qu'un ordinateur quantique universel pourrait adresser, il présente l'avantage d'être déjà commercialisé). En 2019, ce fabricant totalisait 150+ applications dont la moitié concernait de l'optimisation[184](Volkswagen, pour l'optimisation des flux de trafic routier ; British Telecom, pour l'optimisation de leur réseau cellulaire…).

Il faut néanmoins noter que si un problème d'optimisation numérique ou combinatoire peut être retranscrit dans un ordinateur à recuit quantique, la possibilité d'amélioration des performances par rapport à un algorithme classique n'est pas acquise (voir la conclusion de certains PoC de BMW[182] : « *Quantum Annealer: No performance nor accuracy benefit, difficulty fitting problem, both currently and in the future* »).

4.3.5.5. Machine learning

L'Intelligence Artificielle n'est pas une discipline nouvelle mais ses techniques spécifiques d'apprentissage automatique (ou *Machine Learning - ML*) ont connu ces dernières années un regain d'intérêt grâce principalement à la combinaison de deux facteurs: l'augmentation du volume et de la variété des données disponibles (*Big Data*) et, la croissance exponentielle des puissances de calcul. Les techniques de ML sont devenues de puissants outils pour trouver des *patterns* dans des données toujours plus abondantes.

Afin d'identifier ces patterns, les algorithmes de *machine learning* font souvent appel à des routines d'algèbre linéaire standard telles que l'inversion de matrice ou la décomposition des valeurs propres. Par exemple, un modèle **SVM**[185], l'une des approches d'apprentissage machine traditionnelles les plus efficaces pour la

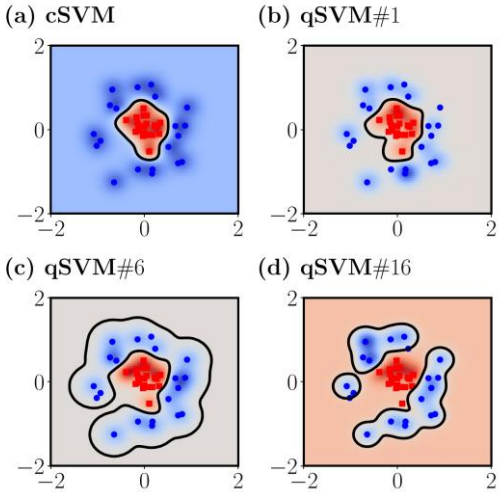


Figure 101: Problème de classification : bleu/rouge SVM Classique (cSVM) comparé à des SVM "quantiques" (qSVM) selon différents paramètres sur un Annealer D-Wave (Source: Willsch et al. 2020)

[182] Showcase BWM, Quantum Tech Digital Week, 16 June 2020
[183] https://www.airbus.com/newsroom/press-releases/2019/01
[184] https://www.dwavesys.com
[185] Les *Support Vector Machines* (machines à vecteurs supports) sont un ensemble de techniques d'apprentissage supervisé destinées à résoudre des problèmes de classification et de régression (Wikipedia).

classification, peut être transformé en un système d'équations linéaires, puis être résolu en utilisant une inversion de matrice. Le formalisme mathématique utilisé dans le traitement de l'information quantique fait lui-même largement appel aux mêmes outils d'algèbre linéaire[186] : vecteurs, matrices, vecteurs propres…

De cette boîte à outils mathématiques commune a récemment germé l'idée d'utiliser l'informatique quantique pour améliorer les performances des algorithmes du ML [183] qui pourraient souffrir de la « malédiction de la dimension »[187] et devenir coûteux en temps de calcul.

En 2019, IBM et le MIT ont collaboré pour évaluer l'avantage de l'utilisation des ordinateurs quantiques pour la classification (type SVM)[184] mais la démonstration, encourageante, n'utilisait que 2 qubits. En 2020, Willsch et al.[185] introduisent une méthode d'entrainement des SVM sur l'ordinateur à recuit quantique de D-Wave et étudient ses performances par rapport à un modèle SVM traditionnel. Leurs résultats montreraient que l'ensemble des classifieurs produits par le recuit quantique est une alternative réaliste et utile au classifieur traditionnel (Figure 101).

Parallèlement aux travaux menés sur les modèles SVM, d'autres algorithmes quantiques utilisables en ML ont été créés ces dernières années: PCA, HHL, circuits quantiques variationnels (VQE, QAOA[186]), algorithmes de recommandation[187], QCNN[188]… Ils couvrent la palette des méthodes classiques du ML mais parfois aussi, les réseaux de neurones du Deep Learning. Ils sont regroupés sous le nom de **QML** pour ***Quantum Machine Learning***.

L'annexe 9 regroupe quelques détails supplémentaires sur leur fonctionnement. Ils exploitent tous les principes quantiques de superposition d'états, d'intrication, et d'interférences contrôlées entre qubits.

A l'instar de l'IA et du ML classique, le champ d'application du QML serait très vaste. Néanmoins, même si elles sont prometteuses, **les versions quantiques sont encore limitées par la puissance et la fiabilité des machines quantiques actuelles**. De plus, la mise en œuvre opérationnelle du QML nécessitera la résolution d'un certain nombre de points [189]:

- Les données d'entraînement des modèles de ML sont de type classiques (images, textes, sons, données quantitatives ou qualitatives). Ces **jeux de données volumineux doivent être** traduits et **chargés dans la machine quantique** ce qui peut prendre du temps et nécessiter la gestion de mémoires quantiques (QRAM), qui ne sont pas encore opérationnelles. Il existe toutefois des pistes alternatives prometteuses explorées par exemple par la startup QCWare (Data Loader)[188].

- Un réseau de neurones classique utilise des **fonctions d'activation non-linéaires** comme les sigmoïdes[189] ou redresseurs (ReLu)[190]. Répliquer le fonctionnement de ces neurones sur une machine quantique est difficile car les **portes logiques quantiques appliquent toutes des opérations linéaires**. Des solutions ont été proposées [191] pour créer des neurones quantiques mais qui ne fonctionnent qu'en *feed-forward*. La solution proposée par I. Kerenidis[188], utilisant des registres mémoire, QRAM, permettrait de faire de la *back-propagation*.

- Un modèle de QML serait plus robuste (i.e. il généraliserait mieux sur des données non connues) s'il pouvait bénéficier des erreurs quantiques lors des traitements plutôt que d'en être tributaire.

---

[186] Voir les représentations vectorielles des qubits au §3.1.2 et matricielles des portes logiques quantiques en annexe 6.
[187] La *malédiction* (ou *fléau de la dimension*) désigne divers phénomènes qui ont lieu lorsque l'on cherche à analyser ou organiser des données dans des espaces de grande dimension. Lorsque le nombre de dimensions augmente, le volume de l'espace croît rapidement si bien que [lorsque l'on y place les données] elles se retrouvent « isolées » et deviennent éparses. Cela est problématique pour les méthodes nécessitant un nombre significatif de données pour être valides, les rendant alors peu efficaces voire inopérantes(Wikipedia).
[188] Meetup Le Lab Quantique https://lelabquantique.com/llq-11/, 3 juin 2020
[189] C'est grâce à la non-linéarité des fonctions d'activation qu'un réseau neuronal à 2 couches peut être considéré comme un approximateur de fonction universel (Source : Wikipedia, [190])
[190] *Rectified Linear Unit* Wikipedia

- Le modèle de QML doit prouver qu'il apporte un **véritable gain en temps de calcul** par rapport aux processeurs les plus avancés d'aujourd'hui.

- A l'instar des modèles de ML classiques, les développeurs de modèles QML devront prendre en compte les demandes croissantes en matière **d'interprétabilité** et explicabilité des résultats dans certains secteurs d'applications (e.g. Finance).

4.3.5.6. Synthèse des applications

Les figure 102 et figure 103 résument les principales familles d'algorithmes, cas d'usage et secteurs industriels. Avec des cas pratiques nombreux, les applications de l'informatique quantique sont prometteuses. Mais elles sont encore pour beaucoup à l'état prospectif, tout comme les algorithmes quantiques proposés jusqu'à présent, puisque s'il existe bien un certain nombre d'ordinateurs quantiques ils ne sont pas encore assez puissants et fiables pour les exécuter. L'annexe 10 est utile pour illustrer les délais dans lesquels un grand fabricant (IBM) estime que des applications à différents cas d'usages clairement identifiés seront possibles.

Algorithm Family	Main Uses	Example
Chemical Simulation Computational calculation of molecular interactions and properties	Molecular design	Engineer chemicals or materials for given purposes
Scenario Simulation Imitating representation of something to study potential outcomes	Risk	Impact of volatility on an outcome
	Pricing	Evaluate asset values for trades
	Market	Monitor economic system impacts
Optimization To make something as perfect as possible towards a goal	Routing	Transport from origin to destination
	Supply-Chain	Steps to deliver something to customers
	Portfolio	Best product combination for an objective
	Operations	Increase productivity boosting resources
AI, Machine Learning Find relations in data and build assumptions around them	Prediction	Anticipate future events from historic data
	Classification	Divide an end result into different categories
	Patterns	Discovery of regularities or anomalies in data

Figure 102: Famille d'algorithmes et exemple de cas d'usage (Source: d'après IBM Roadmap, 2019)

	Chemicals and Petroleum	Distribution and Logistics	Financial Services	Health Care and Life Sciences	Manufacturing
Chemical Simulation	Chemical product design Surfactants, catalysts			Drug discovery Protein structure predictions	Materials discovery Quantum chemistry
Scenario Simulation		Disruption management	Derivatives pricing Investment risk analysis	Disease risk prediction	
Optimization	Feedstock to product Oil shipping / trucking Refining processes	Distribution supply chain Network optimization Vehicle routing	Portfolio management Transaction settlement	Medical / drug supply chain	Fabrication optimization Manufacturing supply chain Process planning
AI, Machine Learning	Drilling locations Seismic imaging	Consumer offer recommender Freight forecasting Irregular behaviors (ops)	Finance offer recommender Credit / asset scoring Irregular behaviors (fraud)	Accelerate diagnosis Genomic analysis Clinical trial enhancements	Quality control Structural design & fluid dynamics

Figure 103:Différents cas d'usage par familles d'algorithmes et secteurs industriels (Source: d'après IBM Roadmap, 2019)

Il est fort probable que les ordinateurs quantiques fonctionneront dans une architecture hybride avec l'informatique classique, dans la plupart des cas. Ce type d'alliance est d'une certaine façon déjà bien en place, puisque le contrôle des machines quantiques est assuré par un ordinateur classique, ne serait-ce que pour déclencher les portes quantiques d'un algorithme au bon moment, de manière séquentielle (Figure 104).

Pour optimiser le temps de calcul, un modèle de fonctionnement hybride serait idéal, les qubits se chargeant de calculs complexes paramétrés par un processeur classique. Comme pour l'exemple des algorithmes variationnels, des recherches sont toujours en cours pour identifier la gamme de problèmes pour lesquels l'informatique quantique pourrait réellement apporter un avantage.

Les développements de l'informatique quantique influencent aussi l'informatique traditionnelle[192][191]. Il y a une sorte de « coopétition » dans laquelle les créateurs d'algorithmes classiques s'inspirent de méthodes quantiques, ou améliorent indépendamment leur processus pour tirer leurs performances vers le haut. Les cibles quantiques et classiques sont mouvantes.

Il est très peu probable que les ordinateurs quantiques remplacent complètement les ordinateurs classiques dans un avenir prévisible. A l'image de GPU ou FGPA, les ordinateurs quantiques seront plus susceptibles d'être des machines spécialisées appliquées à des problématiques spécifiques qu'ils seront les seuls à pouvoir résoudre.

Bien sûr, les tests réalisés sur des machines quantiques actuelles (NISQ) au nombre restreint de qubits ne sont pas vains, ils permettent de valider des principes, concepts, schémas d'algorithme ou pistes de recherche. Une démonstration expérimentale de la **suprématie quantique (**Figure 105**)** nécessiterait au moins une centaine de qubits. Mais si ce défi majeur est relevé, il est fort probable que cela initiera un cercle vertueux de recherche, d'industrialisation, et de commercialisation.

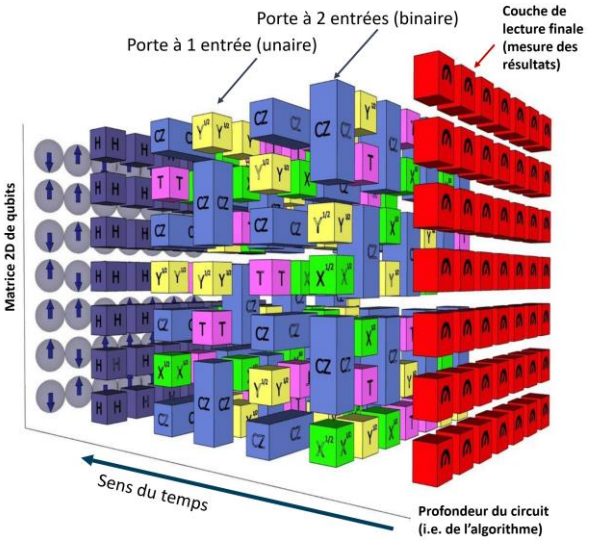


Figure 104: Algorithme quantique appliqué à un registre 2D de qubits. C'est un ordinateur classique qui contrôle l'exécution d'un tel circuit : application des portes et mesures finales (Source: d'après Google)

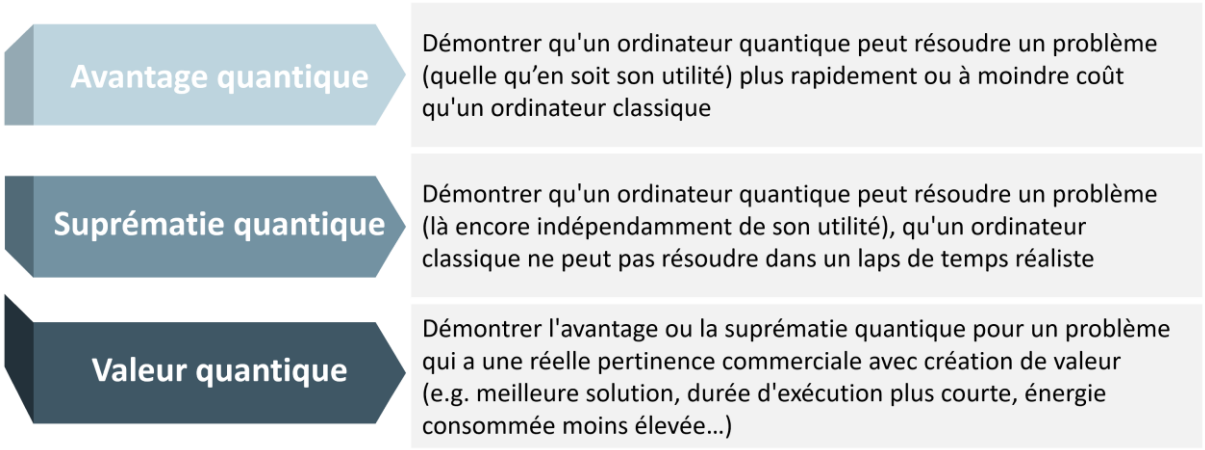


Figure 105: Avantage, suprématie, et valeur quantique

4.3.6. Bilan Energétique

L'une des motivations de l'informatique quantique est de pouvoir accélérer les calculs et traiter à terme des problèmes inaccessibles aux ordinateurs traditionnels en bénéficiant de la puissance de calcul exponentielle des processeurs quantiques. Suivant les problématiques visées, les machines et les algorithmes quantiques utilisés, l'avantage en temps de calcul sera plus ou moins manifeste[192]. Mais s'il y a un critère sur lequel les ordinateurs quantiques vont surpasser largement les supercalculateurs c'est celui de **l'efficacité énergétique** ce qui participera sans ambiguïté à ce qu'on nomme l'**avantage quantique**.

[191] Ainsi, l'informaticienne Ewin Tang a-t-elle proposé un algorithme de Machine Learning destiné aux ordinateurs classiques en s'inspirant d'une proposition d'algorithme quantique faite par Iordanis Kerenidis (voir annexe 9, §,1 p.167).
[192] Ne serait-ce que par le niveau d'accélération des algorithmes quantiques : allant d'un gain quadratique (Grover) à exponentiel (Shor).

4.3.6.1. Quelques ordres de grandeur

Comme on peut le voir sur la figure 106 la consommation des plus grands supercalculateurs est de l'ordre du mégawatt (MW). Depuis juin 2020, le supercalculateur le plus puissant en matière de calcul est le Fugaku construit par Fujitsu. Sa capacité de calcul s'élève à 514 GFlop/s tandis que sa puissance électrique est de 28MW. Son emprise au sol est de 1 920 m2, son poids de 700 tonnes environ[193].

Un ordinateur quantique commercial comme le D-Wave pèse environ 2 tonnes, sa surface au sol[193] est d'environ 10 m2. Le facteur de forme est donc largement à l'avantage du quantique.

La puissance électrique d'un ordinateur quantique est raisonnable. Elle est de l'ordre du kW soit 3 à 4 ordres de grandeur inférieurs à celle des plus grands supercalculateurs. Un D-Wave consomme ainsi 25kW[194] dont 16kW[195] sont liés au système de cryogénie nécessaire au fonctionnement des qubits supraconducteurs de ce processeur (15 mK).

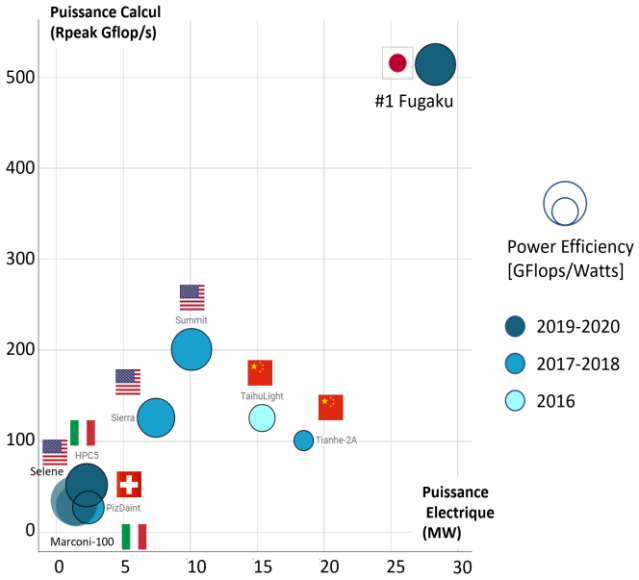


Figure 106: Puissance de calcul et consommation des supercalculateurs TOP10 (Source des données: Top500)

Des chercheurs ont comparé les consommations électriques lors de la résolution d'un même problème par d'un côté, deux supercalculateurs différents (dont le SUMMIT classé encore N°1 à l'époque de l'étude), et de l'autre, un ordinateur quantique de type NISQ. La puissance électrique et le temps de résolution étant à l'avantage de l'ordinateur quantique, les résultats de consommation totale ont été encore plus contrastés avec au final 5 à 6 ordres de grandeur d'écart en faveur du NISQ[150]. Cet ordre de grandeur parait tout de même optimiste puisqu'il faut considérer qu'un calcul mené sur un ordinateur quantique est répété de nombreuses fois car les résultats sont probabilistes. Ainsi, IBM exécute les algorithmes 1024 fois avant de moyenner les résultats. Cette répétition affecte donc de 3 ordres de grandeur le temps et l'énergie dans les comparaisons.

4.3.6.2. Réversibilité / Irréversibilité des calculs

Le paradigme utilisé en informatique quantique est celui de la **réversibilité** des calculs. Ce concept est au cœur même de la thermodynamique et de la théorie de l'information. La réversibilité d'un calcul est

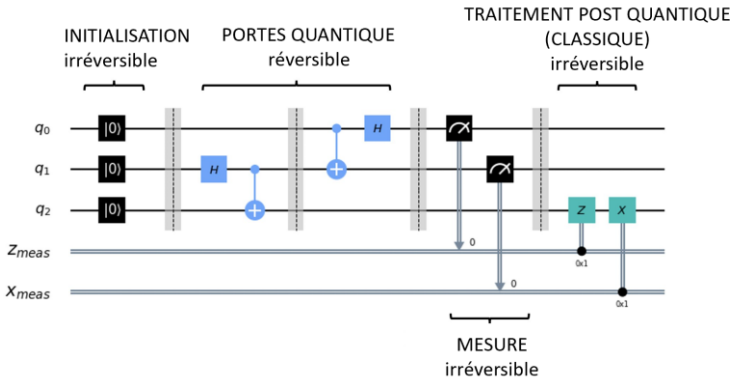


Figure 107: Phases de réversibilité et irréversibilité dans calcul quantique

[193] L'ordinateur D-Wave 2000Q est un cube d'environ 3m de côté (Source: D-Wave 2000Q)

liée au fait de pouvoir revenir en arrière après une opération. Les portes logiques quantiques sont toutes réversibles (voir annexe 6). Cela se matérialise par le fait qu'elles ont autant d'entrées, que de sorties, et qu'il n'y a donc pas d'information détruite après l'application d'une porte sur un qubit. A contrario, les portes logiques classiques sont pour la plupart irréversibles. Selon les lois de la thermodynamique, l'irréversibilité d'un calcul entraine une dissipation d'énergie (i.e. dépense). Dans le calcul quantique, seules l'initiation des qubits et la lecture (mesure) de leurs états sont irréversibles, puisque dans ce dernier cas on perd l'état quantique au profit d'une valeur déterministe (Figure 107).

4.3.6.3. Inventaire énergétique

Si l'informatique quantique est réversible, de nombreuses opérations qui l'entourent ne le sont pas, ce qui pose le problème de la consommation d'énergie par qubit. Les éléments les plus consommateurs d'un ordinateur quantique sont les appareils de cryogénie et de contrôle des qubits (laser, micro-onde). Un inventaire plus précis de la consommation des différents éléments de l'infrastructure est proposé ci-dessous :

- **La cryogénie** : comme nous l'avons vu dans le chapitre précédent (§3.2 p. 20), les niveaux de refroidissement nécessaire aux diverses plateformes physiques de qubits sont différents tout autant donc que les besoins énergétiques :
  - Température ambiante : air conditionné,
  - 77 K:Azote liquide,
  - 4 K: Helium (He) liquide,
  - 1 K: Isotope ^{3}He liquide
  - ~15 mK : Mélange isotopes ^{3}He-^{4}He

  La **consommation électrique due à la cryogénie** pour des qubits supraconducteurs (15mK) est de l'ordre de **16kW** selon D-Wave[195]. Ce chiffre doit également correspondre aux ordinateurs d'IBM et Google qui utilisent la même technologie de qubits. La consommation est moindre pour des températures supérieures.

- **L'électronique de contrôle (lasers et micro-ondes)**. La consommation est très variable suivant la technologie de qubits et leur nombre. Elle est de l'ordre de quelques kW pour les plateformes existantes.

- **Pompe à vide** : le vide ou l'ultra vide nécessaire aux différentes technologies impose l'utilisation de pompe à vide dont les moteurs consomme 600 W maximum[194].

- **L'informatique (classique) de contrôle** : comme nous l'avons déjà évoqué précédemment , ce sont des ordinateurs classiques qui gèrent l'enchainement des portes et des mesures appliquées aux qubits et la consommation est de l'ordre du kW

Au final, si l'ordre de grandeur d'une vingtaine de kW semble tout à fait raisonnable pour les premiers ordinateurs actuels de type NISQ, il faudra bien sûr voir à long terme quel(s) type(s) de technologies de qubits prévaudra(ont) dans le futur, mais aussi quels codes de correction d'erreurs seront employés puisque pour ce critère le ratio du nombre de qubits physiques par qubit logique varie de plusieurs ordres de grandeur suivant les estimations (de 10^3 à 10^5), comme nous l'avons vu au §4.3.4.

Au final, si l'ordre de grandeur d'une vingtaine de kW semble tout à fait raisonnable pour les premiers ordinateurs actuels de type NISQ, qu'en sera-t-il à long terme ? Quels type(s) de technologie(s) de qubits prévaudront à l'avenir? Quel code de correction d'erreur sera employé étant donné que les estimations du rapport du nombre de qubits physiques par qubit logique varie de plusieurs ordres de grandeur selon les protocoles (de 10^3 à 10^5 – cf. §4.3.4) ?

[194] https://www.edwardsvacuum.com/

4.3.7. Les challenges et progrès à venir

La simulation et l'informatique quantique sont à une période charnière de leur développement. Les simulateurs quantiques devraient pouvoir jouer un rôle essentiel dans l'exploration et la compréhension des systèmes quantiques où de nombreuses particules sont en interaction ainsi que dans la résolution de problèmes d'optimisation hors de portée des ordinateurs classiques. A long terme, peut-être 10 ans, des simulations quantiques menées à grande échelle devraient être possibles pour répondre à des questions clés en physique, science des matériaux et chimie quantique.

D'ici là, il faudra continuer à faire l'inventaire des modèles difficiles à simuler d'une manière classique, mais néanmoins, intéressants et importants d'un point de vue physique, puis essayer de les implémenter sur un simulateur quantique.

Toutefois, une fois arrivé à un stade intermédiaire, l'un des principaux défis consistera à être capable de déterminer si le simulateur a correctement effectué la simulation quantique puisqu'il n'y aura plus moyen de comparer les résultats avec celui d'un simulateur classique, le problème étant alors hors de sa portée (**problème de la vérification**).

Ce moment n'est pas si éloigné. En attestent les simulations menées l'an dernier par Google, qui avaient conduit la firme de Mountain View à revendiquer la suprématie quantique. Ce point est illustré figure 108. Les simulations de Google y sont indiquées par des cercles et des étoiles rouges (les étoiles identifiant, selon Google, des cas de suprématie). On peut constater que : i) la limite de mémoire du supercalculateur Summit (TOP#2) aurait été atteinte pour une simulation de Schrödinger (SA) utilisant environ 50 qubits (abaque gauche), ii) le temps nécessaire pour répliquer la simulation SFA sur le supercalculateur serait de 600 ans pour un algorithme sur 53 qubits et 16 portes (abaque droite).

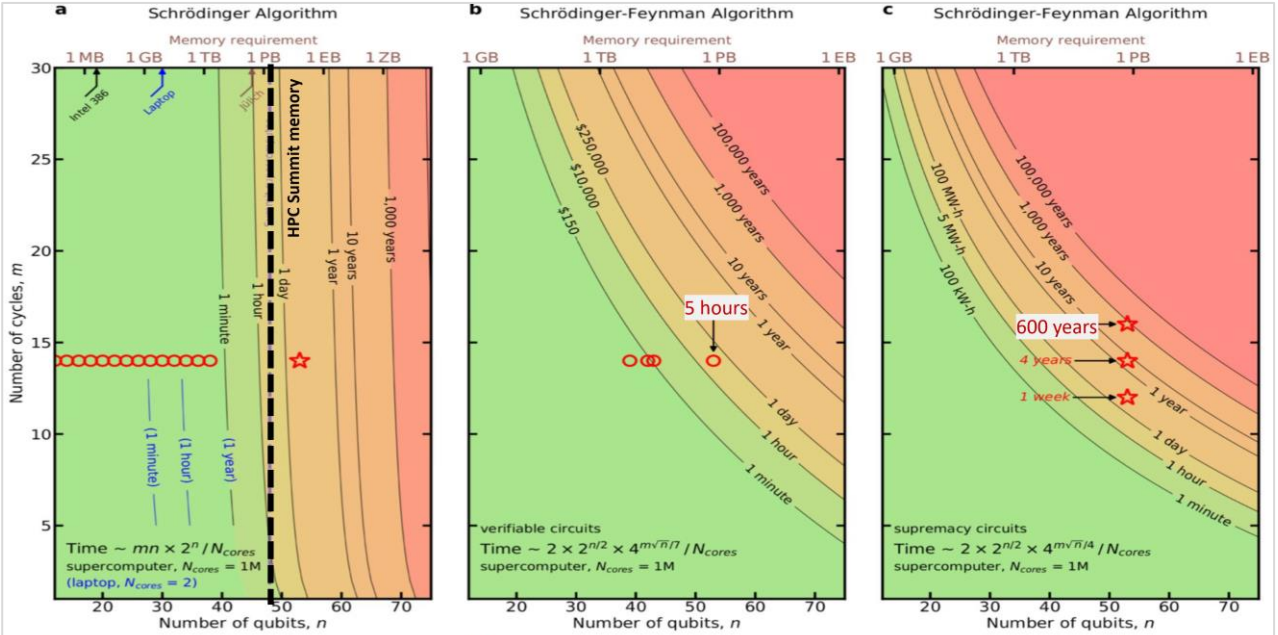


Figure S50: ***Scaling of the computational cost of XEB using SA and SFA. a,*** *For a Schrödinger algorithm, the limitation is RAM size, shown as vertical dashed line for the Summit supercomputer. Circles indicate full circuits with* $n = 12$ *to 43 qubits that are benchmarked in Fig. 4a of the main paper. 53 qubits would exceed the RAM of any current supercomputer, and is shown as a star.* ***b,*** *For the hybrid Schrödinger-Feynman algorithm, which is more memory efficient, the computation time scales exponentially in depth. XEB on full verifiable circuits was done at depth* $m = 14$ *(circle).* ***c,*** *XEB on full supremacy circuits is out of reach within reasonable time resources for* $m = 12$*, 14, 16 (stars), and beyond. XEB on patch and elided supremacy circuits was done at* $m = 14$*, 16, 18, and 20.*

Figure 108: Abaques du temps de calcul, et mémoire nécessaire pour réaliser deux simulations SA et SFA sur un supercalculateur de référence, comparé aux expériences réalisées par Google sur leur processeurs 54 bits (nombre de qubits utilisé en abscisse et nombre de portes activées en ordonnée)(cercle et étoile rouge). (Source: Google)

L'échéance de la vérifiabilité est d'autant plus proche que les simulateurs vont aussi bénéficier significativement des développements des ordinateurs quantiques plus généralistes. Pour ceux-ci, les défis futurs se situent tant au niveau hardware que software.

De nombreuses pistes d'implémentations de processeurs quantiques (à portes) sont actuellement explorées. Les systèmes actuels sont limités à quelques dizaines de qubits, sans correction d'erreurs, ce qui signifie qu'il n'y a pas de qubits logiques idéaux. Toutes les recherches partagent des objectifs communs : **l'amélioration i) des propriétés de cohérence des qubits** (objectif d'un temps de cohérence plus long dans l'absolu, mais surtout relativement aux temps d'activation des portes de la technologie considérée) et **ii) de la fidélité des portes logiques quantiques à un et deux qubits**, au moins au-delà du seuil de tolérance aux erreurs fixé à 10^{-2} (1 erreur sur 100). Sous ce niveau, **iii) des codes correcteurs d'erreurs** du type ***surface codes*** pourront, au moins en théorie, être utilisé **pour corriger les erreurs**. Dans la pratique, une fidélité beaucoup plus élevée serait souhaitable, car cela permettrait de limiter le nombre de qubits physiques par qubit logique.

On peut penser qu'au cours des cinq prochaines années, les premières démonstrations de qubits logiques et de portes tolérantes aux erreurs auront eu lieu (pour en arriver là, il aura alors fallu gagner 4 à 5 ordres de grandeur en nombre de qubits et diminuer de 2 ordres de grandeur les taux d'erreurs par rapport aux machines actuelles[98]).

L'étape suivante consistera à **iv) intégrer un plus grand nombre de qubits** dans l'ordinateur. Des choix techniques et de fabrication minutieux sont nécessaires, toutes les technologies ne sont pas éligibles à priori sur cette voie-là, ce qui ne signifie pas qu'elles ne sont pas intéressantes pour autant (Figure 16 p.21). Mais alors, pour faire fonctionner une machine quantique possédant des centaines de milliers ou millions de qubits physiques (LSQC) il faudra **v) s'assurer de la *scalabilité* des outils électroniques de contrôle**[195]**, des éléments de la pile logicielle** (Figure 109 *& Annexe 8*) et des technologies habilitantes, en particulier des cryostats. Du point de vue du contrôle thermique, les plateformes de qubits qui fonctionnent à des températures cryogéniques sont limitées par la puissance de refroidissement des cryostats et par le dégagement thermique qui s'y produit.

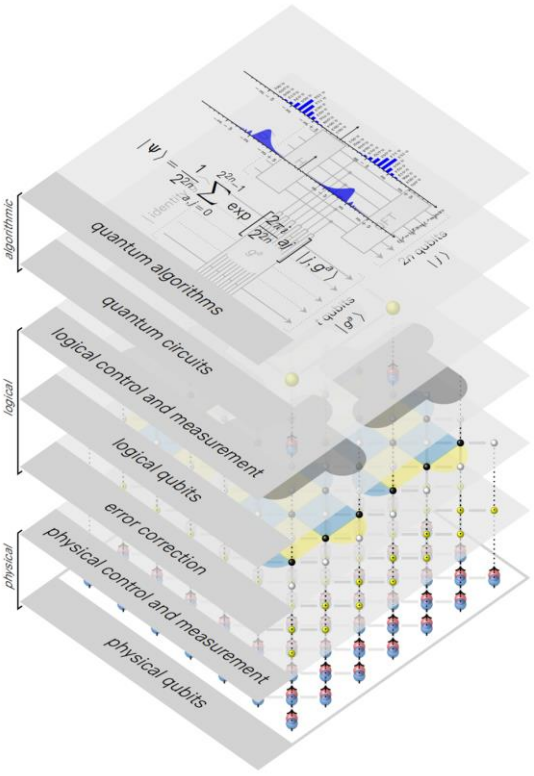


Figure 109: Pile logicielle d'un ordinateur quantique (Quantum Stack) (Source: https://www.chalmers.se/)

En parallèle de cette roadmap menant au LSQC à 10/15 ans[196], plusieurs pistes sont explorées pour pouvoir bénéficier des possibilités de calculs des ordinateurs NISQ actuels. Les travaux sur les architectures hybrides, les algorithmes variationnels ou tolérants aux fautes, ou la recherche de cas d'usage pertinents et utiles pourraient mener à la démonstration d'un véritable cas d'avantage ou de valeur quantique d'ici quelques mois. Néanmoins, les progrès actuels dans le domaine du calcul informatique traditionnel (en particulier du point de vue algorithmique, progrès parfois inspirés par des approches quantiques) font de l'avantage quantique une cible mouvante.

[195] La capacité de calibrer les qubits et la stabilité de ce calibrage dans le temps est un défi et une contrainte très concrète pour les ordinateurs quantiques pratiques (IBM calibre ses ordinateurs quotidiennement). Les fréquences (micro-ondes) utilisées pour manipuler les qubits (application des opérations de portes) doivent être réglées précisément sur le hotspot des qubits.
[196] L'**annexe 10**, est utile pour comprendre les délais dans lesquels un grand constructeur (IBM) pense que les applications à différents cas d'usages seront possibles.

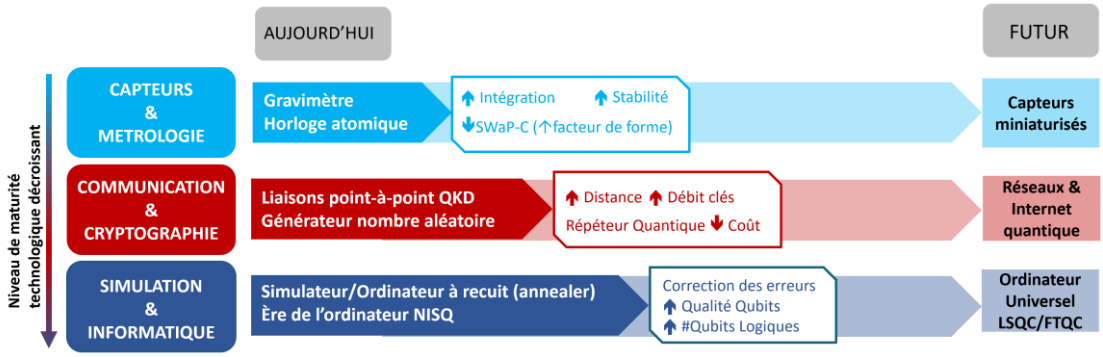
Conclusion

Vénérable centenaire, la physique quantique est aujourd'hui encore au cœur des technologies les plus modernes. Au 20ème siècle, ses premiers développements avaient conduit à des inventions majeures tels le laser, l'IRM, et le transistor, élément de base des circuits intégrés de nos ordinateurs et smartphones et, par conséquent, de notre civilisation de l'information et de la télécommunication.

La recherche aurait pu vivre sur ces acquis déjà fort honorables mais les progrès scientifiques et technologiques continus nous conduisent sans doute à l'aube d'**une seconde révolution, celle de l'information quantique.**

Le monde quantique est un univers particulier, celui des particules atomiques et subatomiques, où les probabilités et les étranges concepts de superposition, d'intrication, d'interférence règnent en maîtres.

La meilleure compréhension de ces phénomènes et le développement technologique nous fournissent des moyens d'action, de calcul et de diagnostic d'une précision et d'une puissance inégalées. Il est désormais possible de coder et de manipuler l'information au sein même de systèmes quantiques individuels, tels que les atomes, ou les photons, ce qui permet l'apparition d'une nouvelle génération d'appareils qui pourraient bouleverser des domaines aussi variés que la métrologie, les télécommunications et l'informatique, tant ils surpasseraient les performances des technologies existantes.



Les finalités de ces différentes applications sont variées : miniaturisation, cybersécurité, internet quantique, ordinateur quantique universel ; leurs horizons de mise en œuvre s'étendent sur 10 ou 15 ans. Si la plupart des technologies sous-jacentes sont émergentes, c'est certainement dans le domaine des capteurs qu'apparaitront assez rapidement les premières applications, suivies par les télécommunications, et en dernier lieu, les ordinateurs.

En **métrologie**, l'extrême sensibilité des systèmes quantiques aux influences externes les rend idéaux pour la réalisation de mesures de grandeurs physiques à haute précision et résolution (capteurs), mais aussi pour la définition du temps (horloge). Dès aujourd'hui, de tels instruments, utilisant par exemple des atomes refroidis par laser, sont opérationnels et commercialisés (gravimètre, horloge atomique). Les progrès à venir seront spécifiques à chacune des applications (LiDAR, imagerie...). Les bénéfices en termes de performance et de coût devront être démontrés par référence aux approches des capteurs actuels. Une **intégration plus poussée** de ces systèmes (e.g. sur puce) constituerait un progrès notable pour faciliter la mise au point de dispositifs de taille, de poids, de consommation et de coût réduits (***SWaP-C***[197]).

Les **télécommunications** cryptées sont dès aujourd'hui sous la menace d'un futur ordinateur quantique universel qui, par sa puissance de calcul exponentielle, pourrait compromettre les méthodes de cryptographie tel que le cryptage RSA largement utilisé sur internet. Le risque est d'autant plus imminent que de nombreuses communications d'ores et déjà enregistrées, pourront être déchiffrées quand la technologie le permettra, dans un avenir peut-être pas si lointain. Deux solutions, probablement

[197] Size,Weight, and Power – Cost.

complémentaires, émergent : l'une purement mathématique, l'autre fondée sur les principes d'intrication et de non clonage rendant inviolable la transmission d'informations quantiques[198] véhiculées par des photons.

Outre l'aspect sécuritaire, ces communications quantiques permettraient à terme de mettre en réseaux des capteurs et des ordinateurs quantiques, ce qui démultiplierait la puissance de calcul ainsi distribuée. A un horizon plus lointain, un internet quantique est enfin envisagé.

Moins avancée qu'en métrologie, la commercialisation de dispositifs quantiques garantissant une *certaine* sécurité des communications est néanmoins effective (génération aléatoire et distribution quantique de clés de chiffrement QKD). Leur utilisation reste toutefois modeste par rapport à la taille du marché potentiel, en raison des compromis entre d'une part la sécurité apportée et, d'autre part, le coût et les performances/limites techniques. Sur ce point, le développement d'un **répéteur quantique** garantira une sécurité inconditionnelle tandis que **l'augmentation du débit de génération** et **de la distance de transmission des clés quantiques** témoigneront des progrès réalisés dans le temps.

En exploitant les principes quantiques de superposition, d'intrication, et les interférences quantiques, les **simulateurs et ordinateurs quantiques** ont le potentiel de résoudre certains types de problèmes communs à de nombreux cas d'usage (simulation, optimisation combinatoire…) beaucoup plus rapidement que les ordinateurs classiques même si les résultats de calculs ne sont que probabilistes.

L'information quantique est codée sous forme de qubits, se matérialisant suivant les technologies, sur différents types de supports physiques (ions, atomes, électrons, photons). Ces plateformes se développent en parallèle, portées par des acteurs des mondes académiques, institutionnels et industriels (géants de l'IT et startups). Il est bien trop tôt pour savoir de quelle plateforme sortira le qubit idéal, même si, aujourd'hui les ions piégés et les supraconducteurs sont les plus avancés. Certains produits sont déjà commercialisés : les annealers (ordinateurs à recuit quantique) utilisables sur certaines problématiques d'optimisation, ou les premiers ordinateurs « bruités » de *l'ère NISQ*[199], plus généralistes utilisant des portes logiques quantiques permettant de construire des algorithmes.

Si la sensibilité des systèmes quantiques était un avantage en métrologie, elle est un inconvénient majeur pour le calcul et la simulation. La sensibilité des qubits aux bruits entraîne leur décohérence et des erreurs quantiques. Deux étapes se profilent alors sur la voie de l'**ordinateur universel dit « tolérant aux erreurs** ».

La première sera de **démontrer** grâce aux ordinateurs quantiques actuels (annealers ou ceux de *l'ère NISQ* qui débute) et à des algorithmes spécifiques (certainement hybrides[200]) **une réelle valeur quantique**[201] dans la résolution d'un problème pratique utile, quitte à devoir améliorer au préalable la qualité des qubits d'un ou deux ordres de grandeur.

La seconde étape sera la mise en œuvre des protocoles de **correction d'erreurs** et **l'augmentation** ultérieure **du nombre de qubits logiques**. Aujourd'hui, les codes correcteurs d'erreurs exigent un surcoût massif de qubits physiques si bien que les ressources nécessaires pour les mettre en place vont bien au-delà des capacités actuelles de la technologie.

Nous le voyons dans tous les domaines, il y a de nombreux jalons à franchir. Rien ne dit que ces objectifs soient inatteignables d'un point de vue théorique. Une course *au quantique* s'est engagée dans le monde entier car la maîtrise de ces technologies est perçue par de nombreux États comme un enjeu majeur pour leur souveraineté et leur économie[202].

[198] Servant à la génération de clés de chiffrement.
[199] Noisy Intermediate-Scale Quantum.
[200] Processus faisant appel à la fois à un ordinateur quantique et un ordinateur classique.
[201] Ne serait-ce que sur le point de vue de la consommation énergétique.
[202] Annexe 4

L’enjeu de souveraineté relève des deux sujets connexes : l’ordinateur quantique et les systèmes de communications quantiques sécurisées.

Les technologies quantiques sont aussi une opportunité de développement économique et sociétal. Elles ont le potentiel de créer des moyens fondamentalement nouveaux d’obtenir et traiter l’information, puis d’apporter des solutions jusqu’alors inatteignables à des problèmes inhérents à l’énergie, l’agriculture ou la santé.

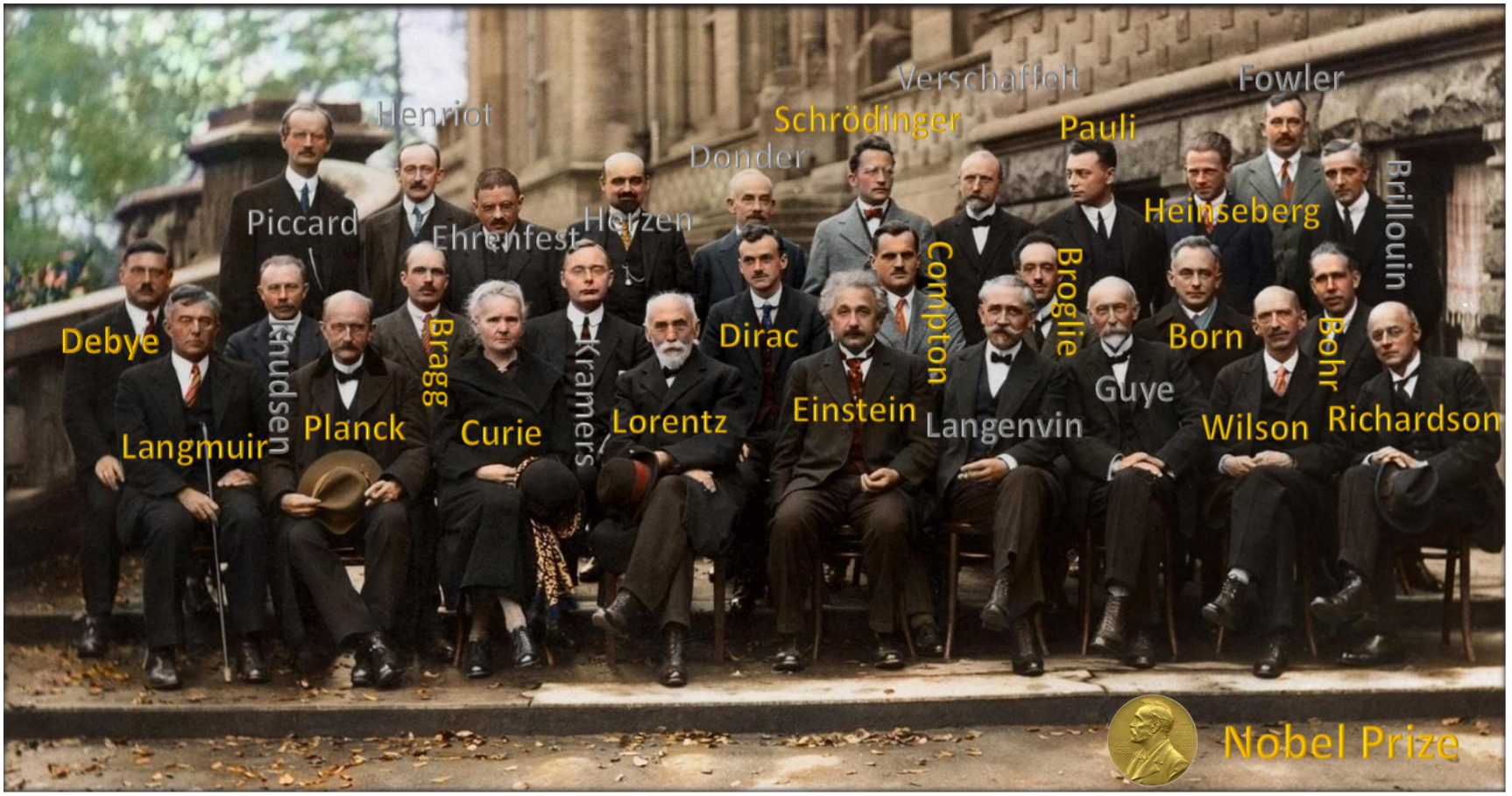
Cette course de fond pourrait également donner lieu à des applications auxquelles personne n’a encore songé. Qui sait ? Une chose semble certaine. Les ordinateurs quantiques ne remplaceront pas complètement les ordinateurs classiques, leurs spécificités ne les destinant pas à répondre à toutes les problématiques.

Quoiqu’il en soit, la révolution arrive… lentement… mais comme le disait un célèbre dramaturge français[203] :

> **Les vrais révolutions sont lentes et [elles] ne sont jamais sanglantes**

[203] Jean Anouilh, « Pauvre **BIT**OS » p.45.

- ANNEXE 1 - QUELQUES ELEMENTS HISTORIQUES (SOLVAY, CHRONOLOGIE, PRIX NOBEL)



Photographie originale de Benjamin Couprie (1927) – colorisée par Sanna Dullaway

Figure 1: Conférence Solvay, Bruxelles, 1927

Les conférences Solvay (en Belgique) sont probablement les plus célèbres conférences en physique et chimie. Elles ont joué un rôle clé dans l'histoire et le développement de la Science. **L'édition 1927**, immortalisée par cette photo colorisée, rassemblait les plus grands mathématiciens et physiciens de l'époque. Elle portait sur les électrons et photons, particules au cœur de la mécanique quantique et réunit presque tous les pères de cette discipline : Schrödinger, Pauli, Heisenberg, Dirac, de Broglie, Born, Bohr, Planck, et Einstein. **17 des 29 personnalités présentes ont obtenu un Prix Nobel**, et 6 en étaient déjà lauréat au moment de la réunion. Nous avons identifié les Nobel par la couleur or et un hyperlien redirige vers leur page Wikipedia.

Covid-19 oblige, la 28ème Conférence de physique, qui traitera de « la physique de l'information quantique », aura lieu en octobre 2021 au lieu d'octobre 2020 [196].

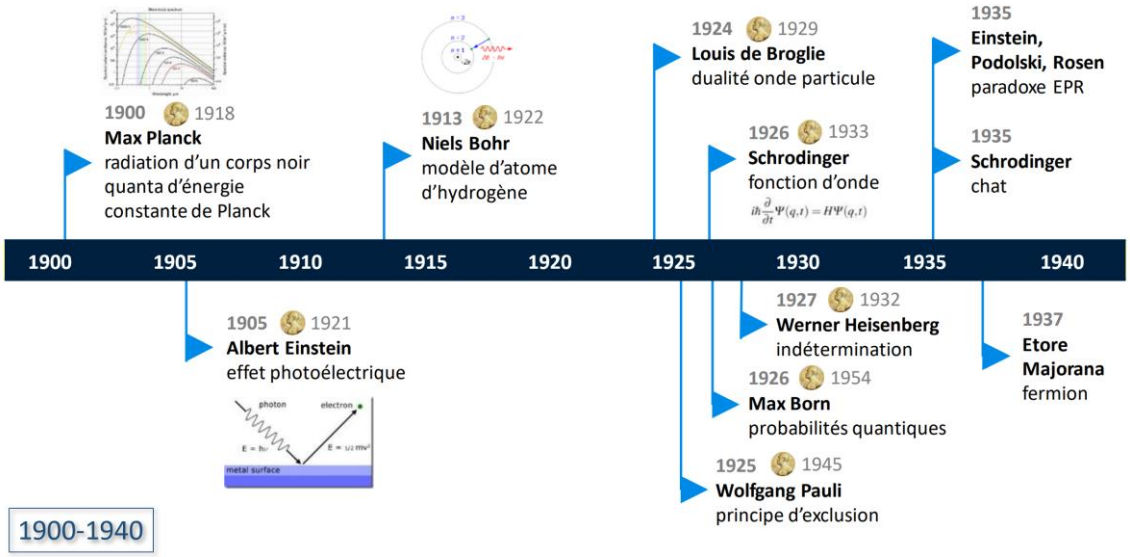


Figure 2: Physiciens et mathématiciens fondateurs de la physique quantique (d'après : O. Ezratty[144])

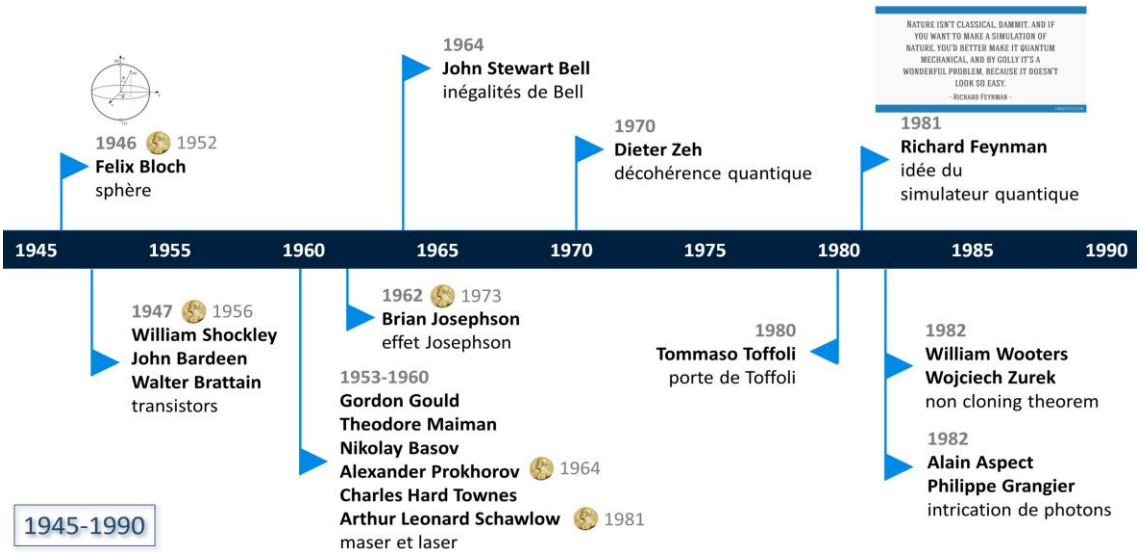


Figure 3: Mathématiciens, Physiciens, 1ère révolution quantique (d'après : O. Ezratty[144])

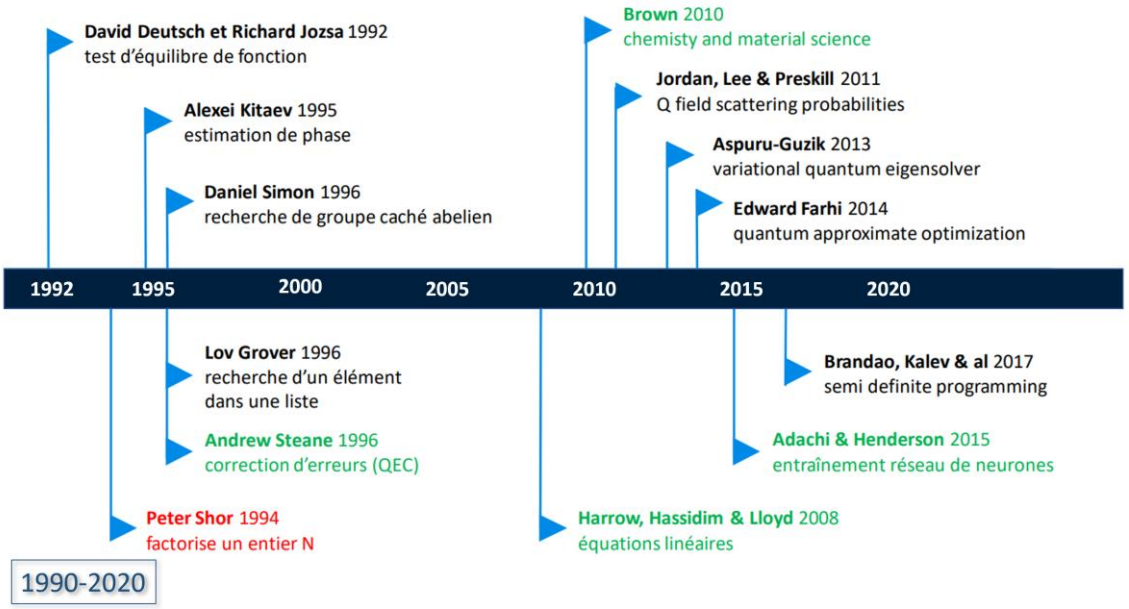


Figure 4: Mathématiciens, Physiciens, 2ème révolution quantique (d'après : O. Ezratty[144])

PRIX NOBEL

Nous recensons dans ce paragraphe la liste des prix Nobel de Physique dont les travaux récompensés ont eu un impact sur le développement de la physique quantique. Le prix Nobel de Physique a été créé en 1901. Il est destiné à récompenser les savants qui ont inventé ou fait des découvertes les plus révolutionnaires en physique. Les lauréats obtiennent une reconnaissance publique pour leur travail et sont censés jouer un rôle essentiel dans la définition des politiques futures en matière d'amélioration des développements technologiques.

Partant de la liste officielle[204], nous avons analysé les 113 prix décernés en Physique (à 293 lauréats) et la motivation de la récompense. Nous avons ainsi réduit la liste à 68 physiciens (Figure) dont les travaux sont en lien avec la physique quantique. Avec 24 prix (sans compter les multinationaux), les USA dominent le classement mais l'Europe est bien positionnée (Figure 5). Les prix reçus ces 8 dernières années par les deux français Gérard Mourou (laser) et Serge Haroche (manipulation et mesure des objets quantiques) sont des modèles d'excellence à la française notables.

Il ne s'agit bien sûr pas d'une liste exhaustive de tous les savants remarquables qui ont travaillé sur la quantique. De nombreux autres ont marqué l'histoire dans ce domaine comme Arnold Sommerfeld (Allemand 1868-1951) sans recevoir le prix Nobel. D'autre part, nous ne présentons ici que les lauréats en physique. Ainsi John A. Pople, chimiste, a reçu le prix Nobel de Chimie en 1998 pour le développement de méthodes informatiques en chimie quantique.

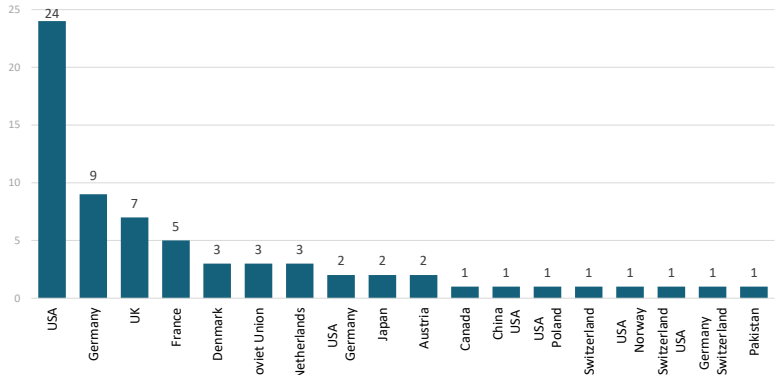


Figure 6: Nombre de prix Nobel de physique pour un travail en physique quantique par nationalité

Year	Laureate	Country	Rational
1902	Pieter Zeeman	Netherlands	"in recognition of the extraordinary service they rendered by their researches into the influence of magnetism upon radiation phenomena"
1906	Joseph John Thomson	United Kingdom	"for his theoretical and experimental investigations on the conduction of electricity by gases"
1918	Max Planck	Germany	"for the services he rendered to the advancement of physics by his discovery of energy quanta"
1921	Albert Einstein	Germany Switzerland	"for his services to theoretical physics, and especially for his discovery of the law of the photoelectric effect"
1922	Niels Bohr	Denmark	"for his services in the investigation of the structure of atoms and of the radiation emanating from them"
1927	Arthur Holly Compton	USA	"for his discovery of the effect named after him"
1929	Louis de Broglie	France	"for his discovery of the wave nature of electrons"
1932	Werner Heisenberg	Germany	"for the creation of quantum mechanics, the application of which has, inter alia, led to the discovery of the allotropic forms of hydrogen"
1933	Erwin Schrödinger	Austria	"for the discovery of new productive forms of atomic theory"
	Paul Dirac	United Kingdom	
1937	Clinton Joseph Davisson	USA	"for their experimental discovery of the diffraction of electrons by crystals"
	George Paget Thomson	United Kingdom	
1943	Otto Stern	USA Germany	"for his contribution to the development of the molecular ray method and his discovery of the magnetic moment of the proton"
1944	Isidor Isaac Rabi	USA Poland	"for his resonance method for recording the magnetic properties of atomic nuclei"
1945	Wolfgang Pauli	Austria	"for the discovery of the Exclusion Principle, also called the Pauli principle"

Figure 5: Liste des physiciens ayant reçus le prix Nobel pour leur contribution sur un sujet en lien avec la physique quantique (Souce : https://www.nobelprize.org/)

[204] https://www.nobelprize.org/

Year	Laureate	Country	Rational
1952	Felix Bloch	Switzerland USA	"for their development of new methods for nuclear magnetic precision measurements and discoveries in connection therewith"
	Edward Mills Purcell	USA	
1954	Max Born	Germany	"for his fundamental research in quantum mechanics, especially for his statistical interpretation of the wavefunction"
1956	John Bardeen	USA	"for their researches on semiconductors and their discovery of the transistor effect"
	Walter Houser Brattain	USA	
	William Bradford Shockley	USA	
1964	Nicolay Gennadiyevich Basov	Soviet Union	"for fundamental work in the field of quantum electronics, which has led to the construction of oscillators and amplifiers based on the maser–laser principle"
	Alexander Prokhorov	Soviet Union	
	Charles Hard Townes	USA	
1965	Richard Phillips Feynman	USA	"for their fundamental work in quantum electrodynamics (QED), with deep-ploughing consequences for the physics of elementary particles"
	Julian Schwinger	USA	
	Shin'ichirō Tomonaga	Japan	
1966	Alfred Kastler	France	"for the discovery and development of optical methods for studying Hertzian resonances in atoms"
1972	John Bardeen	USA	"for their jointly developed theory of superconductivity, usually called the BCS-theory"
	Leon Neil Cooper	USA	
	John Robert Schrieffer	USA	
1973	Leo Esaki	Japan	"for their experimental discoveries regarding tunneling phenomena in semiconductors and superconductors, respectively"
	Ivar Giaever	USA Norway	
	Brian David Josephson	United Kingdom	"for his theoretical predictions of the properties of a supercurrent through a tunnel barrier, in particular those phenomena which are generally known as the Josephson effect"
1975	Aage Bohr	Denmark	"for the discovery of the connection between collective motion and particle motion in atomic nuclei and the development of the theory of the structure of the atomic nucleus based on this connection"
	Ben Roy Mottelson	Denmark	
	Leo James Rainwater	USA	
1978	Pyotr Leonidovich Kapitsa	Soviet Union	"for his basic inventions and discoveries in the area of low-temperature physics"
1979	Sheldon Lee Glashow	USA	"for their contributions to the theory of the unified weak and electromagnetic interaction between elementary particles, including, inter alia, the prediction of the weak neutral current"
	Abdus Salam	Pakistan	
	Steven Weinberg	USA	
1985	Klaus von Klitzing	Germany	"for the discovery of the quantized Hall effect"
1987	Johannes Georg Bednorz	Germany	"for their important break-through in the discovery of superconductivity in ceramic materials"
	Karl Alexander Müller	Switzerland	
1989	Hans Georg Dehmelt	USA Germany	"for the development of the ion trap technique"
	Wolfgang Paul	Germany	
1997	Steven Chu	USA	"for development of methods to cool and trap atoms with laser light."
	Claude Cohen-Tannoudji	France	
	William Daniel Phillips	USA	
1998	Robert B. Laughlin	USA	"for their discovery of a new form of quantum fluid with fractionally charged excitations"
	Horst Ludwig Störmer	Germany	
	Daniel Chee Tsui	China USA	
1999	Gerard 't Hooft	Netherlands	"for elucidating the quantum structure of electroweak interactions in physics"
	Martinus J. G. Veltman	Netherlands	
2001	Eric Allin Cornell	USA	"for the achievement of Bose–Einstein condensation in dilute gases of alkali atoms, and for early fundamental studies of the properties of the condensates"
	Carl Edwin Wieman	USA	
	Wolfgang Ketterle	Germany	
2005	Roy J. Glauber	USA	"for his contribution to the quantum theory of optical coherence"
	John L. Hall	USA	"for their contributions to the development of laser-based precision spectroscopy, including the optical frequency comb technique"
	Theodor W. Hänsch	Germany	
2012	Serge Haroche	France	"for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems."
	David J. Wineland	USA	
2016	David J. Thouless	United Kingdom	"for theoretical discoveries of topological phase transitions and topological phases of matter"
	F. Duncan M. Haldane	United Kingdom	
	John M. Kosterlitz	United Kingdom	
2018	Arthur Ashkin	USA	"for groundbreaking inventions in the field of laser physics"
	Gérard Mourou	France	
	Donna Strickland	Canada	

- ANNEXE 2 -

ANALYSE DU PAYSAGE DES BREVETS PUBLIES SUR LES TECHNOLOGIES QUANTIQUES

Michel Kurek – Ecole Polytechnique – juin 2020

La première révolution quantique a permis des inventions telles que le laser et le transistor, l'élément de base des ordinateurs et des smartphones. Une seconde révolution est en marche. Nos capacités à contrôler, dans une plus large mesure qu'auparavant, les systèmes quantiques individuels, tels que les atomes, les ions, les molécules ou même les photons permet ainsi l'émergence d'une nouvelle génération d'appareils optiques et électroniques qui utilisent les effets quantiques pour améliorer considérablement les performances par rapport aux technologies "classiques" existantes.

Les technologies quantiques créent des opportunités importantes pour de nouvelles entreprises, mais pourraient également avoir des implications significatives pour la sécurité nationale ou la confidentialité des informations.

Compte tenu des opportunités et des menaces créées[205] par les technologies quantiques, des investissements importants se font depuis les 5 à 10 dernières années, dans les secteurs public et privé.

Plusieurs gouvernements ont lancé de vastes programmes pluriannuels avec des financement dépassant le milliard d'US$ - USA, Canada, Europe (UE), UK, Chine, Japon[197], [198]. Dans le privé, trente-deux opérations de financement de startups par du capital-risque ont été effectuées en 2018, pour un total annuel s'élevant à 173 m$ d'investissements [199]. En parallèle de nombreuses grandes entreprises multinationales travaillant déjà sur les marchés des télécommunications, de l'informatique ou des capteurs, reconnaissent le potentiel des technologies quantiques et investissent dans leur développement et commercialisation.

L'analyse du paysage des brevets est un moyen solide d'évaluer le potentiel économique des nouvelles technologies et de mesurer le niveau de transposition des résultats de ce qui a été jusqu'à présent essentiellement un domaine de recherche, en nouveaux produits, susceptibles de stimuler la croissance économique et contribuer au progrès sociétal.

En juin 2020, nous avons procédé à une large recherche et analyse des brevets en lien avec les technologies quantiques publiés depuis 2010 en exploitant la base de données proposée par Orbit[206].

Nous avons comptabilisé 9 905 brevets sur la période 2010-2020. Le délai de publications des brevets étant généralement de 18 mois, l'information pour les années 2019-2020 n'est pas complète et il manque certainement quelques brevets de 2018. Nous constatons une forte progression du nombre de brevets déposés depuis 2012, laquelle s'accélère encore depuis 2015, le taux de croissance annuel moyen s'élevant à 27.15%.

La très grande majorité de l'innovation sur les technologies quantiques émane de la Chine et des USA, dépassés récemment par les chinois. La production chinoise est plus du double de celle des USA et représente à elle seule 52% des brevets dans nos domaines d'étude. USA et Chine totalisent plus de 75% des brevets.

Parmi les 20 acteurs clés, représentant 20.2% des brevets, 11 sont chinois, dont le leader, Ruban Technology, qui œuvre dans le domaine des communications digitales. IBM et Intel complète le podium. Avec 6 multinationales américaines dans le TOP20, les places pour les autres nations sont limitées.

---

[205] Voir le document principal : les menaces sont celles liées essentiellement à la sécurité des communications chiffrées tandis que les opportunités de progrès sociétal sont nombreuses, par exemple dans le domaine des télécommunications, de la médecine et de la chimie, des transports, de la finance et celui de la recherche de ressources énergétiques.

[206] Logiciel d'analyse spécialisé de l'éditeur Questel, leader dans le secteur des bases de brevets : https://www.questel.com

L’innovation chinoise se concentre sur les technologies de sécurisation des communications par l’utilisation des propriétés quantiques de la lumière (particulièrement l’intrication de photons) tandis que les USA conservent un large avantage en informatique quantique. Nous illustrons les avancées chinoises dans le domaine des *communications quantiques* par l’exemple de SGCC, plus grand distributeur d’électricité au monde (voir §3.4).

La croissance des brevets dans le domaine spécifique de *l’informatique quantique* est encore plus vertigineuse que celle des autres technologies quantiques. Leur nombre a été multiplié par 11 en six ans. Si la Chine a fait des avancées ces dernières années, elle est, ici, encore très loin des USA qui ont déposé 51.4% des brevets sur ce sujet. Le paysage des acteurs clés mixe multinationales américaines et japonaises, startups spécialisées, universités et agences gouvernementales civiles ou militaires.

1. Objectifs

Une recherche bibliographique préalable à notre étude nous a permis d'identifier quelques documents existants analysant le paysage des brevets portant sur les technologies quantiques [200]–[204]. Certains se concentrent sur l'ordinateur quantique, d'autres ne sont pas récents ou mal cadrés par leur stratégie de recherche. Au final, nous avons souhaité avoir une vue personnelle, large et objective, en procédant à notre propre recherche de brevets et analyse. Les points que nous souhaitions aborder sont les suivants :

- Evolution au cours du temps du nombre de demandes de brevets déposés
- Répartition géographique des déposants et des domaines d'innovation couverts par les brevets
- Identification des 20 acteurs clés et de leurs principaux secteurs d'innovation
- Etude du cas d'un déposant chinois, SGCC
- Analyse des domaines technologiques les plus brevetés
- Répartition des citations de brevets entre les déposants
- Focus sur l'informatique et l'ordinateur quantique par une clé de recherche plus restreinte

2. Méthodologie

En juin 2020, nous avons recherché et analysé à partir des bases Orbit de Questel[207] et Patseer de Gridlogics[208], les familles de brevets en relation avec les technologies quantiques et retenu finalement la première qui paraissait plus complète. A travers notre stratégie de recherche, nous avons privilégié une exploration large s'étendant aux domaines clés de ce qui est souvent désigné comme la seconde révolution quantique, à savoir :

- Informatique quantique (ordinateur quantique)
- Communication quantique (télécommunication, réseau, sécurité, cryptographie)
- Capteur, métrologie, imagerie quantique
- Simulation quantique

Ces domaines sont ceux que l'on retrouve dans les documents détaillants les différentes initiatives gouvernementales (par exemple pour l'UE « Quantum Technologies Flagship Report » [205]).

Pour construire notre équation de recherche, nous avons combiné des critères portant sur la présence de mots-clés et sur la classification suivant les normes IPC (International Patent Classifications) ou CPC (Cooperative Patent Classification) :

```
(((TAC:((((quantum wd1 (comput* OR (data w proces*))) OR q?bit? OR (quantum memor*) OR (quantum AND (random access memory)) OR qram OR (quantum err* correct*)  OR (quantum inform*)) OR ((quantum* AND (entangl* OR superposit* OR *coherence? OR nonlocalit* OR teleport*)) OR (quantum metrolog*) OR (quantum sensor*) OR ( cold atom?) OR (atom* AND interferomet*) OR (ion? trap*)) OR (((simulat* OR model*) AND ((quantum OR photon* OR electron?) WD5 (entangl* OR superposit* OR spin?))) OR (quantum simulat*)) OR ((quantum w key?) OR qkd OR (quantum random number) OR qrng OR ((quantum OR entangl*) AND cryptol*) OR (quantum network?) OR (quantum repeat*) OR (quantum communica*))) AND SPRY:[2010 TO 2020])) OR AC:(H04L9/0852 OR H04L9/0855 OR  H04L9/0858 OR G06N10*))
```

Cette requête nous permet d'extraire les informations sur les brevets dont la date de priorité[209] est égale ou postérieure à 2010, contenant dans leur Titre, Abstract, ou Claims (revendications) les mots-clés génériques mentionnés dans l'encadré ci-dessus. Pour la requête effectuée sur la base de données Patseer nous avions rajouté explicitement les catégories IPC/CPC : H04L9/0852, H04L9/0855, H04L9/0858 et G06N10*. Les trois premières classent des brevets en cryptographie quantique, tandis que la dernière

[207] https://www.questel.com/
[208] https://patseer.com/
[209] La date de priorité est la date de dépôt de la toute première demande de brevet portant sur une invention donnée.

G06N10 a été créée, courant 2018, spécifiquement pour les brevets traitants d'ordinateurs quantiques. Les organismes IPC, CPC revoient leur classification au moins une fois par an. Il faut noter qu'auparavant, les brevets pour ces modèles d'ordinateurs étaient classés dans la catégorie G06N99/002 (*« Subject matter not provided for in other groups of this subclass »*, i.e. on y met ce que l'on n'a pas su classer ailleurs). La création d'un code spécifique est une reconnaissance normale vu la forte évolution du nombre de brevet sur le sujet.

3. Analyse

3.1. Evolution annuelle du nombre de brevets déposés

Avant de nous concentrer sur la période de notre étude 2010-2020, il est intéressant de visualiser l'évolution du nombre de brevets dans nos domaines de recherche sans limite de dates.

Sur toute la base disponible, nous avons ainsi relevé 15 245 brevets, dont 13 208 sont postérieurs à 2000. Les plus anciens remontent aux années 1950 et ce n'est qu'à partir de 1992 que le cap des 100 brevets par an a été franchi.

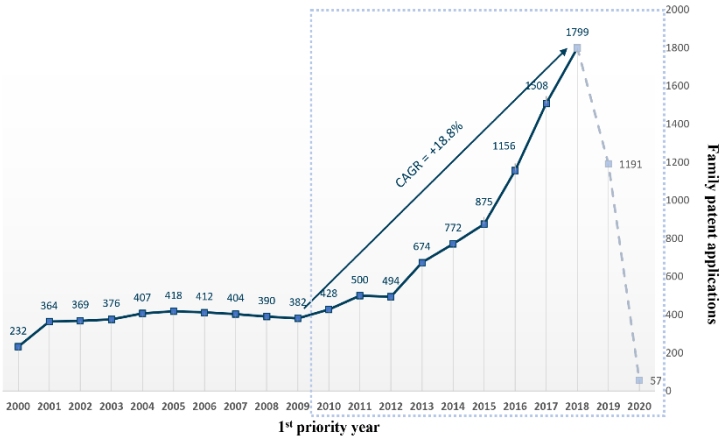


Figure 1: Evolution du nombre de familles de brevets depuis 2000

Sur la figure 1, nous présentons l'évolution annuelle depuis 2000. Après une période de stabilité entre 2001 et 2009, le nombre de brevets a commencé à augmenter, particulièrement à partir de 2012, pour passer de 382 (2009) à 1 799(2018) soit +371%, ce qui représente un taux de croissance annuel moyen (CAGR) de 18.8%. Sur les trois dernières années enregistrées (2015-2018) la croissance annuelle moyenne atteint même 27.15%.

Avant d'entamer l'analyse des dix dernières années, rappelons qu'il y a toujours un retard dans l'information publique disponible sur les brevets en raison du délai de 18 mois séparant le dépôt d'une demande et sa publication ou du secret demandé par le déposant. Ceci explique le comportement relevé sur la courbe précédente (Figure 1) depuis 2018. Sur les 10 dernières années, nous recensons à ce jour 9 905 brevets.

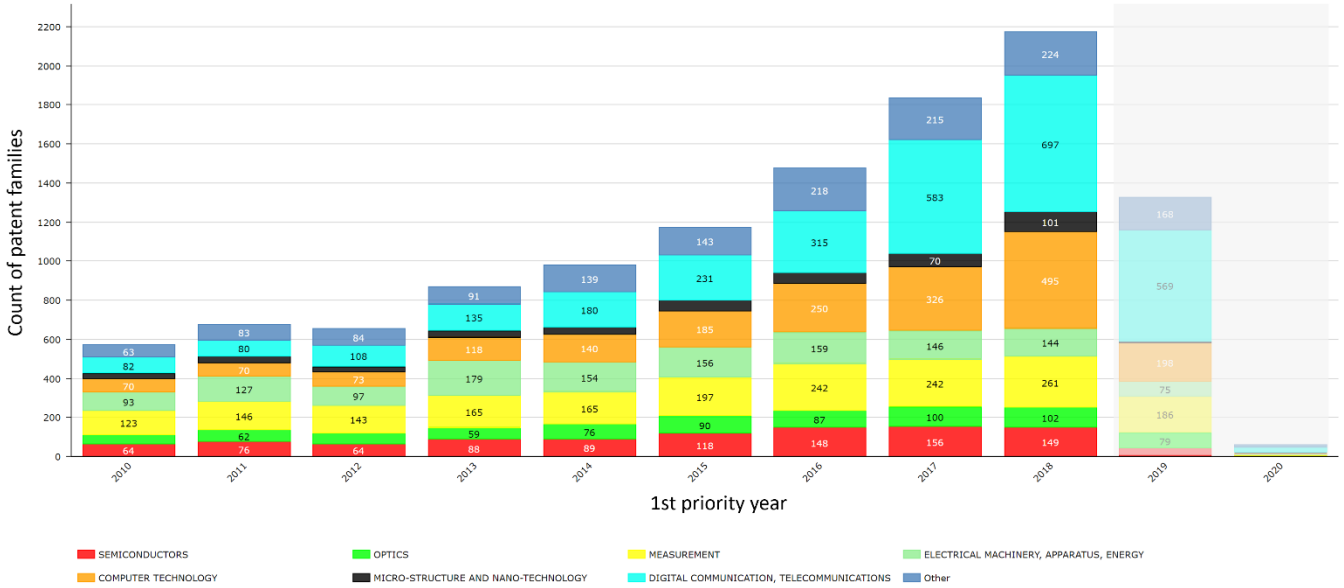


Figure 2: Evolution et répartition par domaine du nombre de brevets

La figure 2 précise l'évolution récente du nombre de brevets par domaine d'applications (tel que défini par les systèmes de classification IPC/CPC). On y relève les parts croissantes de ceux portant sur la technologie des ordinateurs (495 brevets en 2018 -orange) et les communications (697 -cyan). Dans ce secteur, beaucoup traitent de cryptographie, et en particulier de distribution quantique de clés de chiffrement (QKD) : 650 sur les 697. Les brevets peuvent être associés à plusieurs domaines ce qui explique que le total cumulé par année est supérieur à celui présenté sur la figure 1.

3.2. Répartition géographique

Comme c'est le cas dans d'autres secteurs[206], que l'on regarde la répartition géographique (Figure 3) sous l'angle du *pays de priorité*[210] ou de *la localisation de l'inventeur (R&D)*, la Chine est devenue le leader mondial en termes de brevets déposés sur la période (5 161 soit plus de la moitié des brevets 52.1%), devant les USA (2 401, environ 24%) et le Japon (768, 7.8%). C'est un fait remarquable puisqu'en 2013 la Chine était encore derrière le Royaume-Uni [202].

La Corée du Sud est elle aussi dans le TOP5. Le rang du Canada, et dans une moindre mesure celui de l'Allemagne et de quelques autres pays comme la France, dépend de la métrique utilisée – *pays de priorité* vs *localisation de l'inventeur*. Le Canada est réputé pour sa créativité et son écosystème dans le domaine des technologies quantiques. D-Wave est une entreprise canadienne très connue en informatique quantique dont la majorité des nombreux brevets[207] sont enregistrés comme *International Patent (WO)* avec comme pays de priorité les USA. En comptabilisant par localisation du centre de R&D, le Canada se place alors en 7eme position (235) devant la France (126).

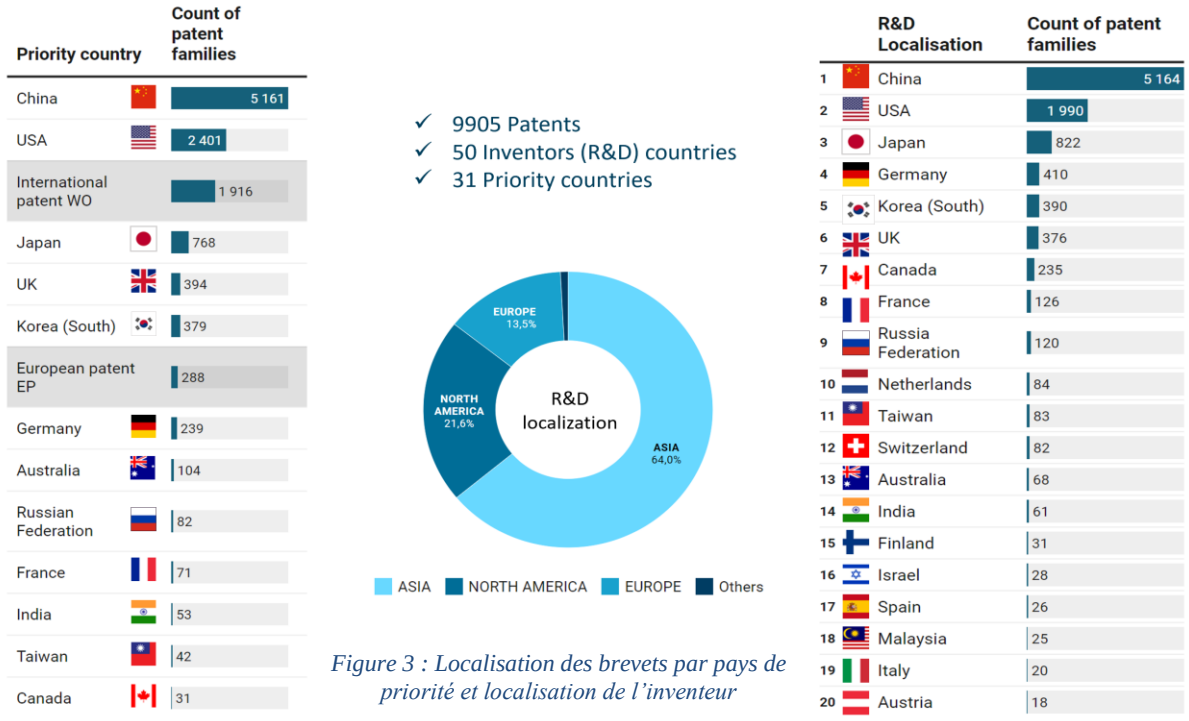


Figure 3 : Localisation des brevets par pays de priorité et localisation de l'inventeur

Avec Chine, Japon, Corée du Sud, Taïwan, Inde et Malaisie l'Asie totalise 64% des brevets (6 597). USA et Canada 21.6% (2 230) et l'Europe au sens large (incluant l'UE, le UK, la Suisse et la Russie) 13.5% (1 394). La contribution des autres continents est minime, l'Australie se distinguant tout de même comme une place d'innovation active.

L'évolution relative de la Chine se confirme sur la figure 4 par le nombre de brevets déposés par année par pays de priorité. Elle s'explique par les investissements et la production massive de la Chine dans les domaines des communications sécurisées grâce aux lois de la physique quantique (théorème de non-clonage) mais aussi par d'autres éléments politiques explicités dans le chapitre suivant.

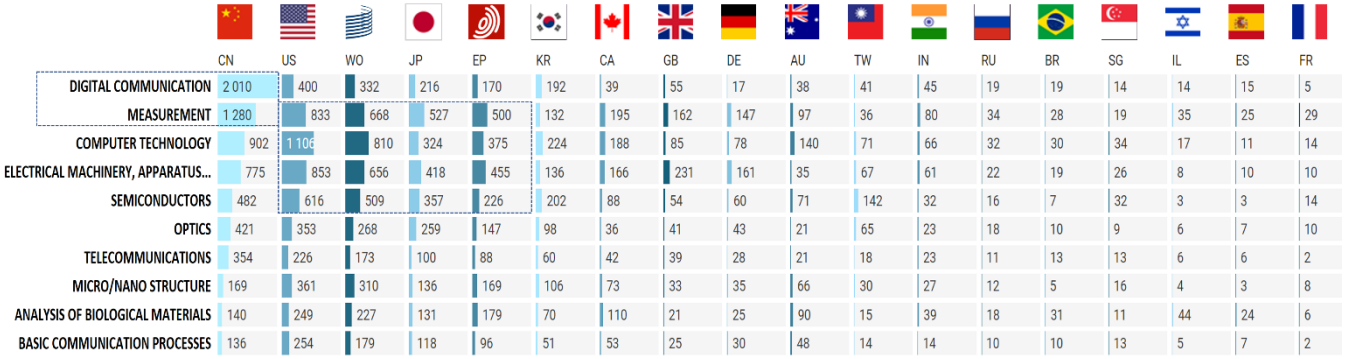
[210] Le pays prioritaire est le pays dans lequel le dépôt le plus ancien d'une demande de brevet est revendiqué.

	CN	US	JP	GB	KR	DE	RU	FR
2010	110	107	79	24	25	18	5	10
2011	128	145	87	33	26	26	6	6
2012	155	147	77	16	28	19	5	3
2013	231	185	93	46	26	20	10	4
2014	313	171	89	54	36	20	3	8
2015	385	214	82	31	38	36	7	9
2016	588	245	72	29	40	41	13	6
2017	885	280	67	29	82	19	8	10
2018	1 157	363	53	29	60	23	11	9

Figure 4: Nombre de brevets par an et par pays de priorité

La Chine est devenue le leader dans le domaine des communications quantiques (Figure 5). Depuis le lancement du satellite *Micius*, puis le test réussi en juin 2017, en première mondiale, de la liaison quantique de 1 200 km impliquant le satellite et une station au sol [208], ce pays n'a eu de cesse de développer les technologies de communication sécurisée et met actuellement en place les briques nécessaires à la construction d'un réseau de communication quantique (le record obtenu cette année pour la transmission d'information quantique via de la fibre optique sur une distance de 50 km [209] en atteste).

De leur côté, les USA gardent le leadership sur les technologies liées à la construction d'ordinateurs quantiques (*computer technology*, *electrical machinery*, *semiconductors*, *nanotechnology*).



	CN	US	WO	JP	EP	KR	CA	GB	DE	AU	TW	IN	RU	BR	SG	IL	ES	FR
DIGITAL COMMUNICATION	2 010	400	332	216	170	192	39	55	17	38	41	45	19	19	14	14	15	5
MEASUREMENT	1 280	833	668	527	500	132	195	162	147	97	36	80	34	28	19	35	25	29
COMPUTER TECHNOLOGY	902	1 106	810	324	375	224	188	85	78	140	71	66	32	30	34	17	11	14
ELECTRICAL MACHINERY, APPARATUS...	775	853	656	418	455	136	166	231	161	35	67	61	22	19	26	8	10	10
SEMICONDUCTORS	482	616	509	357	226	202	88	54	60	71	142	32	16	7	32	3	3	14
OPTICS	421	353	268	259	147	98	36	41	43	21	65	23	18	10	9	6	7	10
TELECOMMUNICATIONS	354	226	173	100	88	60	42	39	28	21	18	23	11	13	13	6	6	2
MICRO/NANO STRUCTURE	169	361	310	136	169	106	73	33	35	66	30	27	12	5	16	4	3	8
ANALYSIS OF BIOLOGICAL MATERIALS	140	249	227	131	179	70	110	21	25	90	15	39	18	31	11	44	24	6
BASIC COMMUNICATION PROCESSES	136	254	179	118	96	51	53	25	30	48	14	14	10	10	13	5	7	2

Figure 5: Répartition des brevets par pays de priorité et domaine technologique

D'une façon générale, pour toutes les nations, il faut nuancer le constat en notant que le fait de déposer ou non un brevet est appréhendé de façon très différente suivant les pays. Pour ne citer que l'exemple de la France, seul 15% des startups françaises détiennent au moins un brevet pendant leur phase d'amorçage contre 23% en Allemagne et 22% aux USA et en Chine [210].

Concernant la Chine, la situation est intéressante. Les brevets chinois sont généralement considérés comme « ayant peu de valeur »[211] car dans les centres de recherche chinois, l'un des indicateurs clés de performance (KPI) est strictement lié au nombre de brevets déposés, au niveau même de la politique de l'État. Par conséquent, ils déposent beaucoup de brevets dans le pays, mais s'ils essaient de breveter la même technologie à l'étranger, il leur arrive souvent d'être refusés en raison du manque de nouveauté.

Ceci dit, l'explosion du nombre de brevet chinois n'est pas spécifique à notre sujet d'intérêt spécifique. Il est général puisque la Chine est devenue en 2019 le principal déposant de brevets selon l'Organisation Mondiale de la Propriété Intellectuelle [206].

3.3. Répartition par déposant (*Assignee*)

Ce sont 2 802 déposants qui ont contribué aux 9 905 brevets recensés sur notre période d'étude. Il faut noter toutefois, qu'en particulier pour les brevets, les noms des déposants apparaissent souvent avec des variantes d'orthographe ce qui gonfle certainement un peu le décompte.

La liste des 20 organisations ayant déposé le plus de brevets est présentée Figure 6. Ces acteurs clés comptent à eux seuls pour 20.2% des brevets déposés.

Sans surprise, nous y retrouvons 11 organisations chinoises, surtout spécialisées dans les communications (Figure 7). La Chine est l'unique pays pour lequel nous avons des universités dans ce TOP20, ce qui s'explique par l'incitation aux dépôts de brevets venant de la politique locale, déjà mentionné.

Aux côtés des universités chinoises, un certain nombre d'entreprises, comme Anhui Asky Quantum Technology (Qasky), QuantumCTek et encore plus récemment Ruban Quantum Technology ont commencé à soumettre des demandes de manière très active et commercialisent leurs produits.
En nombre de dépôts de brevets, Ruban est devenu leader dans son domaine (télécommunication quantique) en l'espace de 2-3 ans seulement (Figure 8).

	Assignees	Count of patent families
1	RUBAN QUANTUM TECHNOLOGY	167
2	IBM	163
3	INTEL	150
4	MICROMASS	137
5	THERMO FISHER SCIENTIFIC	125
6	QUANTUMCTEK	117
7	UNIVERSITY OF SCIENCE & TECHNOLOGY OF CHINA	116
8	TSINGHUA UNIVERSITY	112
9	ANHUI ASKY QUANTUM TECHNOLOGY	107
10	BEIJING UNIVERSITY OF POSTS & TELECOMMUNICATIONS	104

	Assignees	Count of patent families
11	TOSHIBA	102
12	STATE GRID CORPORATION OF CHINA (SGCC)	98
13	SHIMADZU	83
14	GOOGLE	81
15	MICROSOFT TECHNOLOGY LICENSING	81
16	D WAVE SYSTEMS	79
17	ELECTRONIC SCIENCE RESEARCH INSTITUTE CHINA ELECTRONICS TECHNOLOGY	77
18	ZHEJIANG SHENZHOU LIANGZI NETWORK SCIENCE & TECHNOLOGY	71
19	SOUTH CHINA NORMAL UNIVERSITY	67
20	DALIAN INSTITUTE OF CHEMICAL PHYSICS	64

Figure 6: Déposants : les 20 acteurs clés (TOP20)

Dans le classement, cinq multinationales américaines sont présentes dont quatre : IBM, Intel, Google et Microsoft se distinguent par leur production dans les domaines software et hardware des ordinateurs quantiques. Supraconducteurs et semiconducteurs sont les solutions de plateformes physiques utilisées pour implémenter les qubits choisis par IBM, Google et bien d'autres sociétés d'ailleurs.

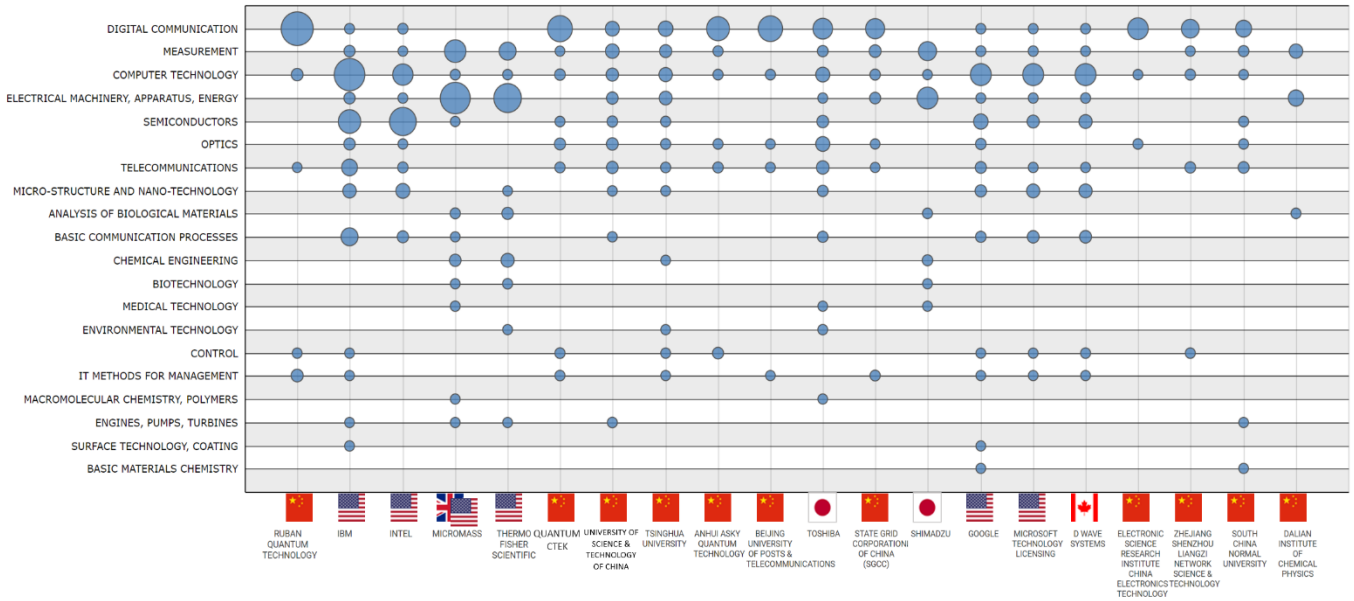


Figure 7: Les acteurs clés et leurs brevets par domaine de technologie

Thermo Fischer Scientific produit des instruments scientifiques, équipements de laboratoire pour la recherche ou l'industrie. Micromass, propriété de Waters, multinationale américaine, mais anciennement anglaise est d'une certaine façon la seule représente du Vieux Continent. Le Japon est

présent avec 2 groupes, Toshiba et Shimadzu, l'un des leaders dans l'instrumentation analytique. Le canadien D-Wave, qui commercialise déjà depuis plusieurs années des calculateurs quantiques construits autour de processeurs de recuit quantique (Annealer) se positionne tout près de Google et de Microsoft en nombre de brevets et de domaines couverts.

L'analyse par déposant, proposée en Figure 8, met en évidence la stratégie en matière de brevets (accroissement des investissements/brevets d'IBM) et identifie les nouveaux entrants comme Ruban Quantum et Electronic Science Research Institute ou ceux qui ne sont plus impliqués (Zhejiang Shenzou). Ces informations permettent également d'expliquer le pic des demandes de brevets sur les télécommunications ces dernières années puisque plusieurs acteurs chinois ont déposé un nombre important de demandes sur une courte période.

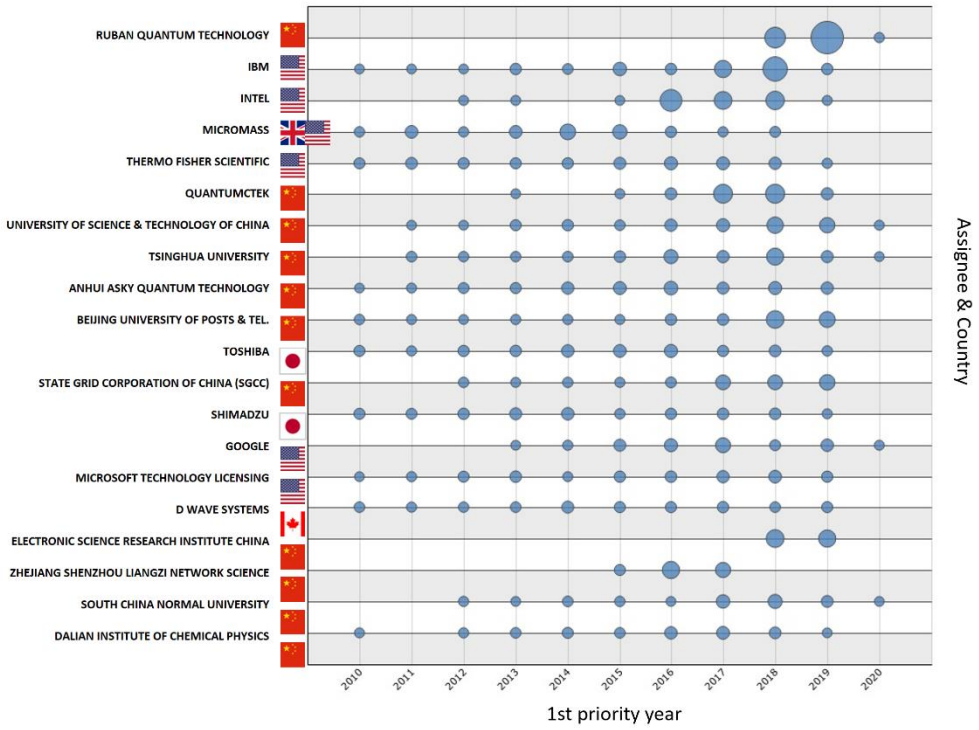


Figure 8: Evolution annuelle du nombre de dépôts des 20 acteurs-clés

3.4. Etude de cas: Grid & Quantum, la *Galaxie* State Grid Corporation of China (SGCC)

Dans le secteur de l'électricité, la sécurité des réseaux électriques et de communications est cruciale pour les entreprises gérantes de réseau énergétique, en particulier celle des communications aura une incidence directe sur le fonctionnement normal du premier.

La société chinoise d'état State Grid Corporation of China (SGCC ou 国家电网公司) est le plus grand gestionnaire de réseau, transporteur et distributeur d'électricité au monde. Elle est dans le TOP5 mondial en termes de revenu, emploie 927k personnes et a le monopole de 1.1 milliards de clients[211] !

Depuis 2012, la société s'intéresse aux technologies quantiques. Elle a organisé un certain nombre de projets de recherche dédiés aux technologies quantiques afin d'étudier la faisabilité de la sécurisation des communications du réseau électrique, et la mise en œuvre de protocoles de distribution quantique de clés de chiffrement multi-utilisateurs.

Comme on le voit sur les figure 6 à figure 8, SGCC a ainsi accru ses dépôts de brevets d'année en année et en revendique maintenant 98. Près des deux tiers (64 brevets soit 65.3%) touchent aux

[211] https://en.wikipedia.org/wiki/State_Grid_Corporation_of_China

télécommunications (protocole, distribution quantique de clés secrètes- QKD) et 16.3% aux systèmes de mesure (Figure 9). On relève également sur cette même illustration le lien étroit avec l'Université des Sciences et des Technologies de Chine (USTC) par l'intermédiaire de la filiale spécialisée dans l'électricité du groupe SGCC Electric Power.

En 2013, en collaboration avec SGCC, une équipe de chercheurs de l'USTC a expérimenté avec succès l'utilisation de protocoles de communication quantique (sécurisée) et la transmission de signaux quantiques dans l'environnement des câbles électriques aériens de plusieurs centrales de SGCC [212].

Lors du sommet du G20 à Hangzhou en 2016, une filiale de SGCC a déployé sa technologie de communication quantique pour assurer la sécurité des télécommunications voix/vidéo/données.

En 2017, une démonstration de réseau de communication quantique a été mis en place par SGCC entre Pékin, Shandong, Anhui, Jiangsu, Zhejiang et d'autres villes, ce fut l'occasion de vérifier le fonctionnement de l'ensemble suivant différents paramètres vitaux. Depuis, les développements se poursuivent.

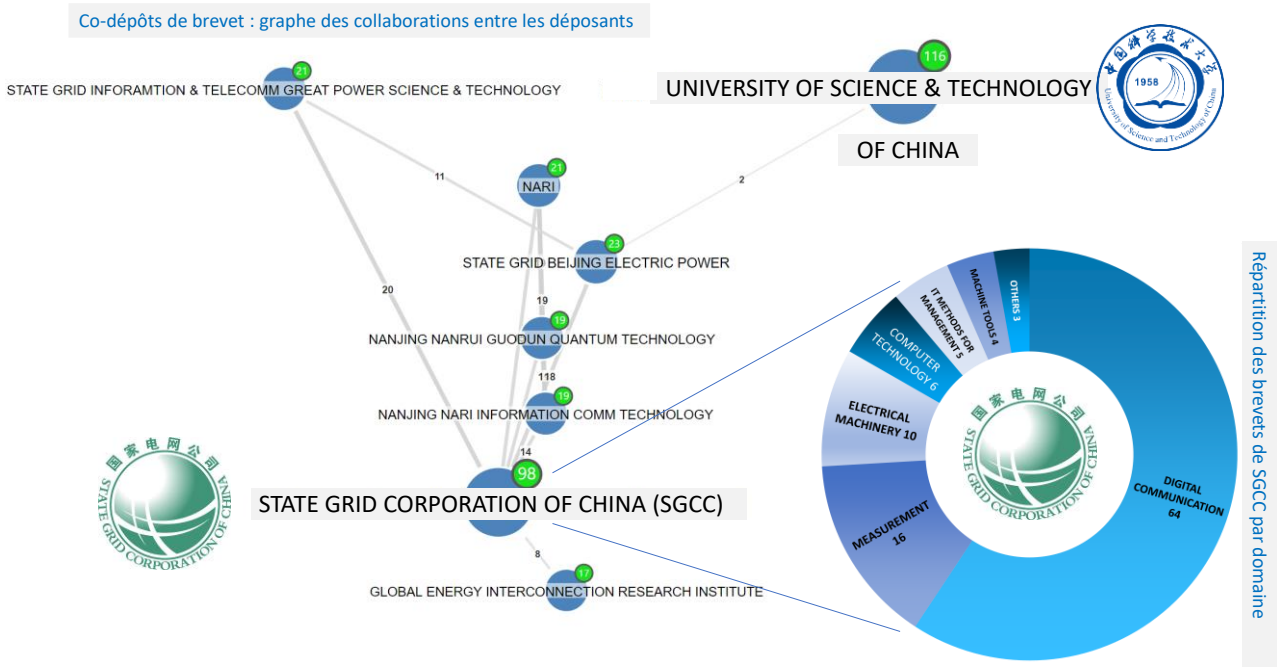


Figure 9: SGCC leader mondial du GRID au cœur d'un réseau de recherche sur les communications quantiques (Graphe adapté et source d'Orbit)

Si ce bref descriptif témoigne de l'effervescence actuelle en Chine autour des communications quantiques, il met aussi en exergue l'attrait qu'a cette région du monde pour ces technologies.

Ainsi, la Corée du Sud (5ème déposant) innove et investit aussi beaucoup dans le domaine. L'opérateur télécom sud-coréen SK vient de prendre le contrôle de la start-up suisse ID Quantique, entreprise spécialiste mondial en cryptographie quantique, et récupère ainsi le portefeuille de 18 brevets de l'entreprise genevoise [213].

Ceci dit les technologies de communications quantiques ne sont pas le seul domaine d'intérêt pour les chercheurs et les entreprises du reste du monde et nous proposons quelques éléments d'analyse supplémentaires dans la section suivante.

3.5. Informations supplémentaires sur les domaines d'applications des brevets

Nous revenons dans cette section sur les domaines d'applications des brevets recueillis dans notre étude en présentant quelques graphiques directement issus de la base Orbit.

La figure 10 permet d'identifier la diversité des brevets en utilisant une catégorisation par domaine technologique basée sur des regroupements de codes ICP (les brevets peuvent apparaître dans plusieurs catégories). Le code couleur témoigne néanmoins d'une concentration sur les domaines de l'ingénierie électrique (*computer technology*, *digital communication*), de l'instrumentation (*measurement*) et de la chimie (au sens large, matériaux, nanostructure).

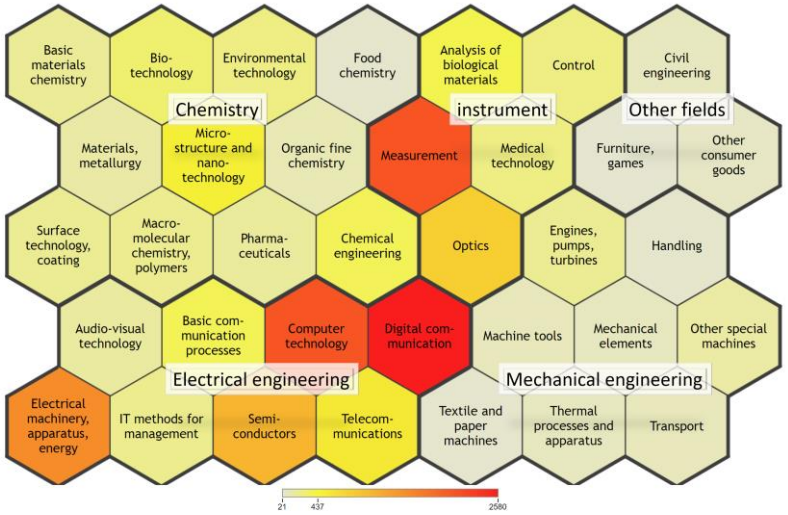


Figure 10: Aperçu des domaines technologiques (Source: calculé depuis Orbit sur 9 905 brevets)

La figure 11 est une illustration des concepts techniques les plus utilisés dans notre secteur étudié et appliqué à notre échantillon de brevets[212]. Plusieurs ilots se dessinent clairement mais pourraient être regroupés par exemple : *Qubit* et *Quantum Computer*.

Un mot concernant la simulation quantique, le nombre de brevets est très faible alors que la littérature académique ne l'est pas particulièrement. L'explication semble être lié au fait que la brevetabilité des méthodes de simulation (comme celle de modélisation ou d'IA) est complexe et souvent rejetée par les autorités des brevets [214].

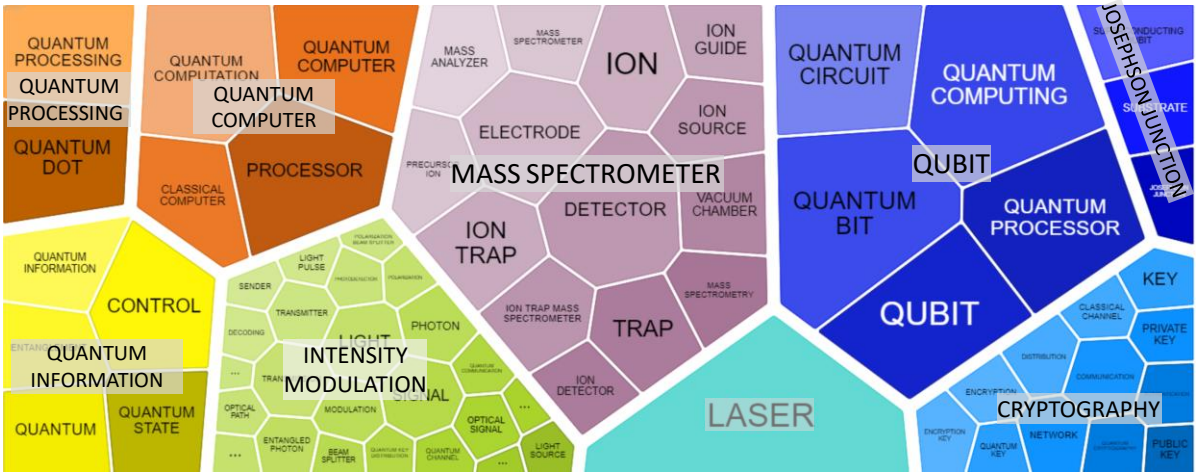


Figure 11: Clusters de concepts (Source: calculé depuis Orbit sur échantillon de 9 905 brevets)

[212] Les concepts sont définis par un algorithme proposé par Orbit.

Les technologies quantiques (informatique, communication, capteurs & métrologie, simulation) bénéficient d'un socle commun théorique et expérimentale : la science fondamentale sous-jacente, la Mécanique Quantique.

Une découverte faite dans un domaine particulier de cette science peut bénéficier à plusieurs technologies et ou domaines d'application simultanément. Le piégeage d'ions, les atomes froids, les boucles supraconductrices à jonction Josephson sont à la fois des technologies misent en œuvre dans les capteurs et en informatique quantique où ces trois techniques sont candidates pour être le support physique susceptible de coder l'unité d'information quantique, le qubit. De la même façon, une percée dans le contrôle des photons, peut être bénéfique à de nombreux domaines dont celui des communications quantiques, de la mesure, de la manipulation des qubits.

3.6. Citations entre déposants

L'analyse suivante va illustrer les citations entre brevets de différents titulaires. Cette information permet d'identifier les innovations qui ont de fortes interactions entre elles. A un niveau supérieur un déposant dont le portefeuille de brevets est fortement cité par la plupart des autres acteurs est susceptible d'être un portefeuille pionnier.

Pour des raisons de clarté de la présentation, nous avons limité notre analyse aux possesseurs de plus de 20 brevets en portefeuille et pour lesquels il y a plus de 6 citations.

Le graphe de relations (Figure 12) qui en ressort fait apparaitre trois clusters distincts dont les deux critères de formation semblent être le domaine technologique et la région du monde.

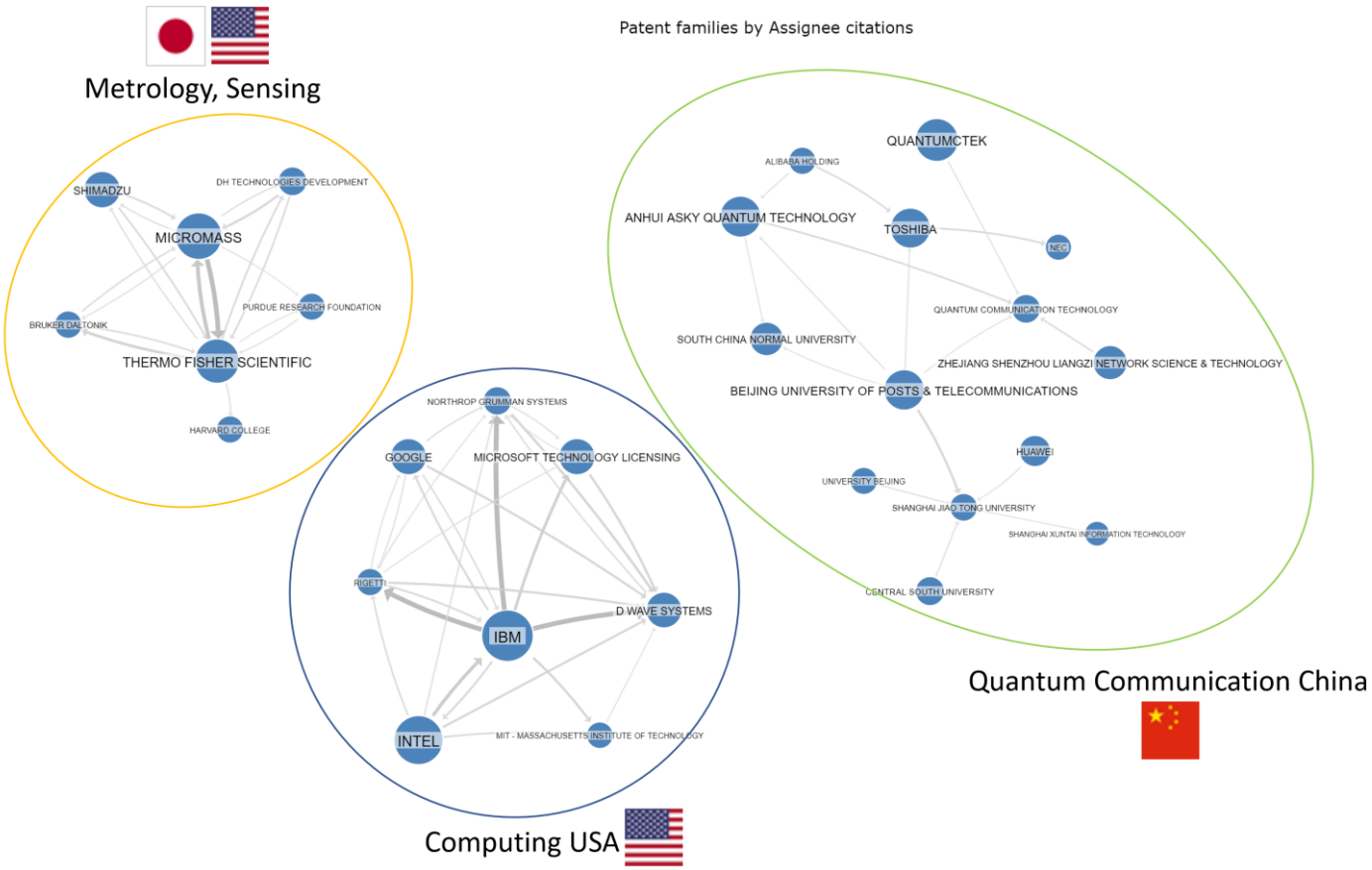


Figure 12: Relations entre les déposants de brevets par leurs citations mutuelles (Source: calculé depuis Orbit)

Le cluster lié aux technologies de communications quantiques (ellipse verte) est majoritairement constitué d'organisations chinoises (universités et entreprises), Toshiba et Nec étant les exceptions.

L'ordinateur quantique est le cœur d'un cluster nord-américain (ellipse bleue) dans lequel se retrouvent les multinationales américaines déjà rencontrées (IBM, Intel, Google, Microsoft), les deux startups spécialisées Rigetti et D-Wave (Canada) et Northrop Grumann, conglomérat américain du secteur de la défense. La seule université ou institut de recherche présent ici est le MIT. Il faut noter ici d'une part, la propension d'IBM à citer des brevets de ses confrères, et d'autre part le fait que D Wave peut vraiment être considéré comme un précurseur dans la mesure où leurs brevets sont souvent cités.

Le troisième cluster est celui de la métrologie, et des capteurs avec Micromass, Thermo Fisher, Shimadzu entre autres. Présent dans ce cluster mentionnons le Harvard College membre de l'université d'Harvard.

Une question se pose à présent : comment expliquer que le paysage des citations de brevets se cristallise de cette façon ? Alors que nous parlions d'une science fondamentale commune il semble qu'en pratique les déposants de brevets font plutôt référence à des brevets couvrant le même domaine de technologie.

A ceci s'ajoute le fait qu'il semble que les auteurs d'un pays soient plutôt à citer les brevets du même pays. Est-il étonnant que les retombées et flux technologiques se matérialisent essentiellement dans un voisinage proche ? Au final nous ne trancherons pas ici, le sujet est complexe et n'est certainement pas propre aux secteurs des technologies quantiques.

3.7. Le paysage des brevets dans le domaine de l'ordinateur quantique

Nous proposons dans la dernière section de cette analyse de brevets de faire un zoom sur l'informatique quantique. Notre équation de recherche est réduite à l'utilisation du nouveau code spécifique IPC/CPC G06N-10/00 identifiant « *Quantum Computers, i.e. Computer Systems Based On Quantum-Mechanical Phenomena* »[213] ainsi que l'ancien code CPC G06N-099/002.

((G06N-099/002)/CPC OR (G06N-010/00)/IPC/CPC) AND PRD >= 2010

Sans la contrainte de date, nous recensons 1 975 brevets dans la base, dont 1 550 déposés depuis 2010.

Les dépôts annuels (Figure 13) ont été limités à quelques dizaines entre 2000 et 2012 oscillant entre 27 et 58 brevets suivant les années[214]. Depuis 2012, leur nombre est en très forte augmentation puisque multiplié par 11, passant de 39 à 429 en 2018, ce qui représente un taux de croissance annuel moyen (CAGR) de 49.1%.

Trente-deux pays ont déposé au moins un brevet dont la date de priorité est postérieure à 2010. Les vingt pays les plus actifs cumulent 98.5% des brevets déposés (TOP20 - Figure 14). Le TOP5 et le TOP10 représentent respectivement 81.5% et 93.7% des dépôts.

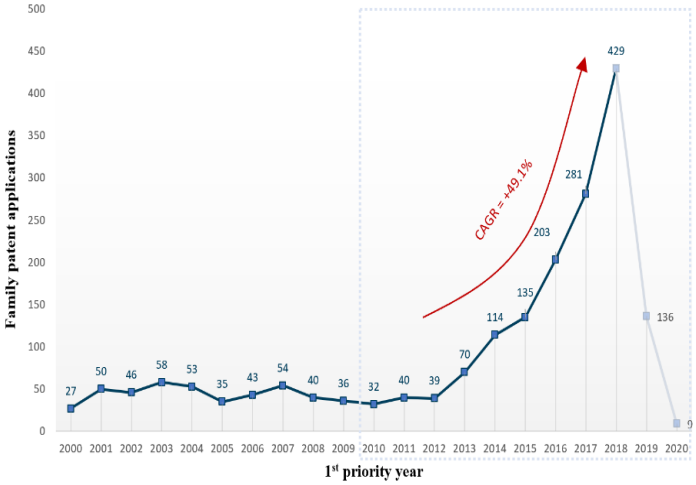


Figure 13: Evolution du nombre de familles de brevets en informatique quantique

[213] https://www.wipo.int/classifications/ipc/en/

[214] Les chiffres annuels qui ressortent dans cette analyse sont légèrement inférieurs à ceux présentés sur la Figure 2 car nous n'avons pas ajouté à notre seconde équation de recherche les mots-clés susceptibles d'identifier des brevets les plus anciens non classés dans les catégories IPC/CPC.

Les USA (874 soit 51.4% des brevets), sont très largement devant la Chine (185, 10.9%) et le Canada (160, 9.4%). Si l'on comptabilise l'ensemble des brevets européens, l'Europe (au sens large : UE(143), UK (65), Suisse (33), Russie (5)) serait en seconde position avec 246 brevets (14.5%) devant la Chine.

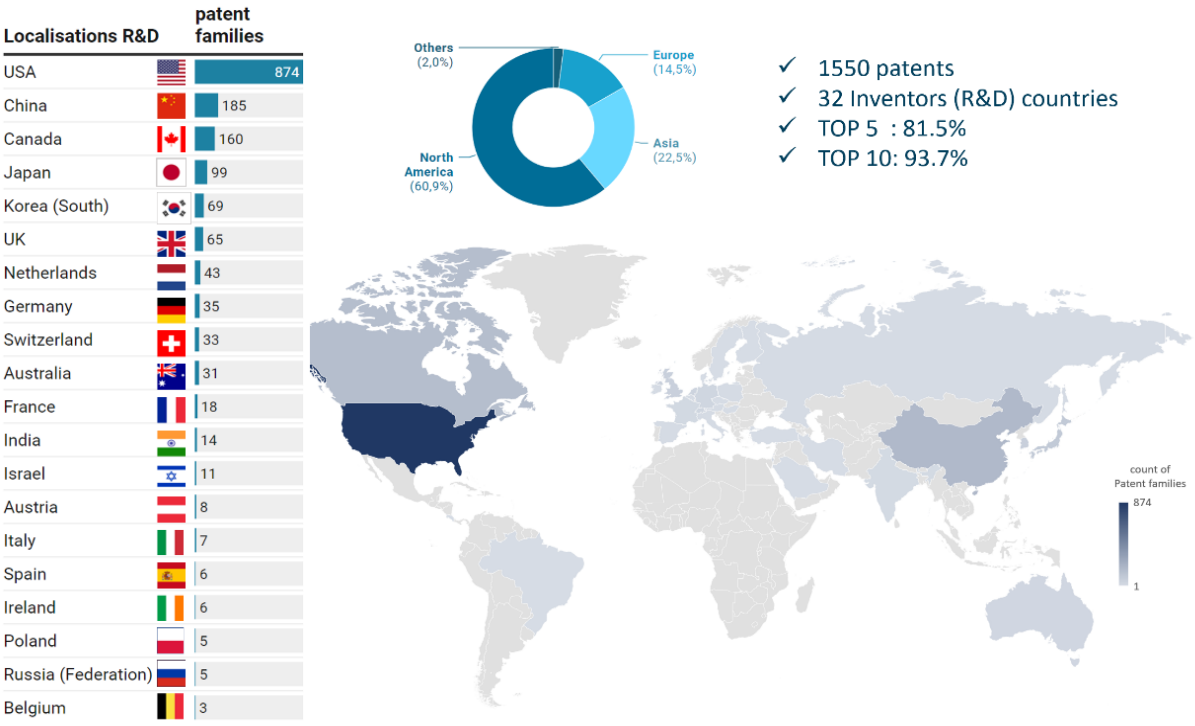


Figure 14: Répartition géographique par localisation R&D

La Figure 15 recense les 39 organisations qui ont déposé depuis 2010 plus de 5 brevets. 45% des brevets sont détenus par les déposants du TOP10, 33% par le TOP5. Sans surprise IBM est l'acteur clé du secteur mais les typologies des intervenants est assez diversifiée.

Nous avons dans cette liste différentes catégories d'acteurs :

- Des géants US des technologies de l'information (IBM, Intel, Microsoft, Google),
- Des conglomérats asiatiques, plutôt japonais historiquement positionnés sur les télécoms et le matériel électronique (illustré par un téléphone portable (📱) sur le graphique : Hitachi, Toshiba…),
- Des startups spécialisées (🦄) dans l'informatique quantique ayant construit un ordinateur quantique ou ayant cet objectif hardware (D Wave, Rigetti, Origin Quantum, IonQ, PsiQuantum). D'autres sont plutôt orientées sur le software (1QBit, Zapata) ou la sécurité des communications (ID Quantique). Une mention particulière pour Hefei Origin Quantum, startup chinoise, une première pour ce pays qui se positionne sur une offre full-stack (offre verticale de produits hardware et software),
- Des organisations du secteur de la défense et de la sécurité (Northrop Grumman coté entreprise, US Navy et US Army coté militaire) sont également présentes aux cotés de quelques agences civiles et établissements de recherche gouvernementaux (Sandia).
- Le secteur académique (🎓) est ici bien présent avec 12 établissements de différentes nationalités mais dont la moitié sont américains.

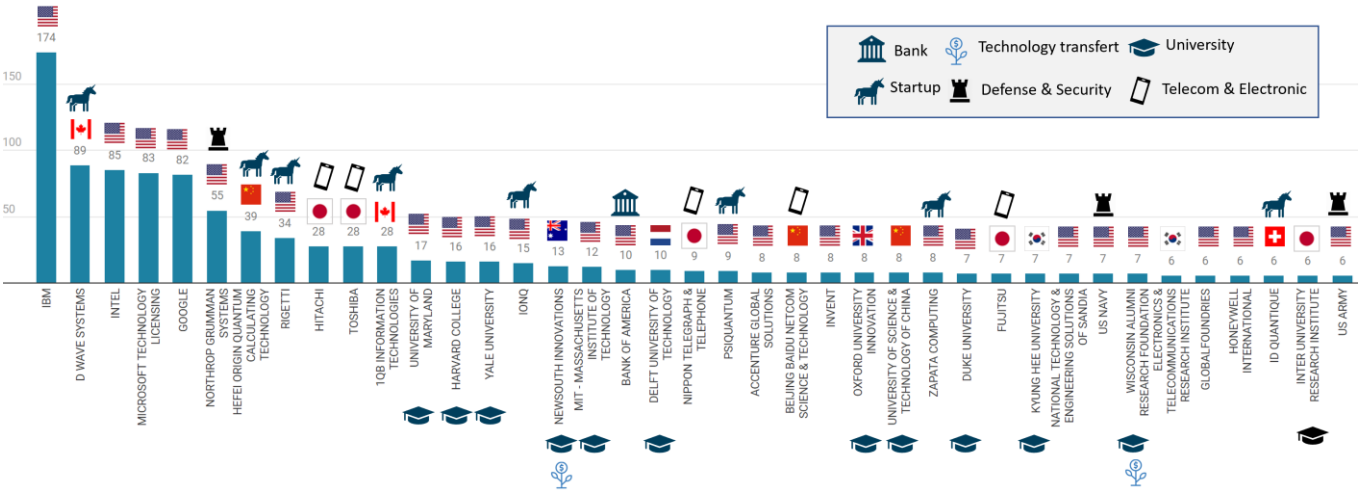


Figure 15: Organisations dépositaires de 6 brevets ou plus depuis 2010

Comme on peut le visualiser sur la figure 16, les problématiques techniques liées à la mise au point d'un ordinateur quantique sont très majoritairement abordés dans les brevets de notre échantillon que ce soit les aspects liés directement aux différentes possibilités d'implémentation physique des qubits (quantum dot, qubit supraconducteur, ion piégé…) ou à ceux de leur environnement (contrôle des qubits, vide, micro-onde, laser).

Si 1 438 brevets se réfèrent à ce type de sujet d'autres thèmes sont abordés (Figure 17) comme ceux liés à la sécurité des communications (QKD), à la génération quantique de nombre aléatoire (QRNG) et puis certaines applications sont détaillées (*IT methods for management*, *ingénierie chimique*, ou même *les transports*).

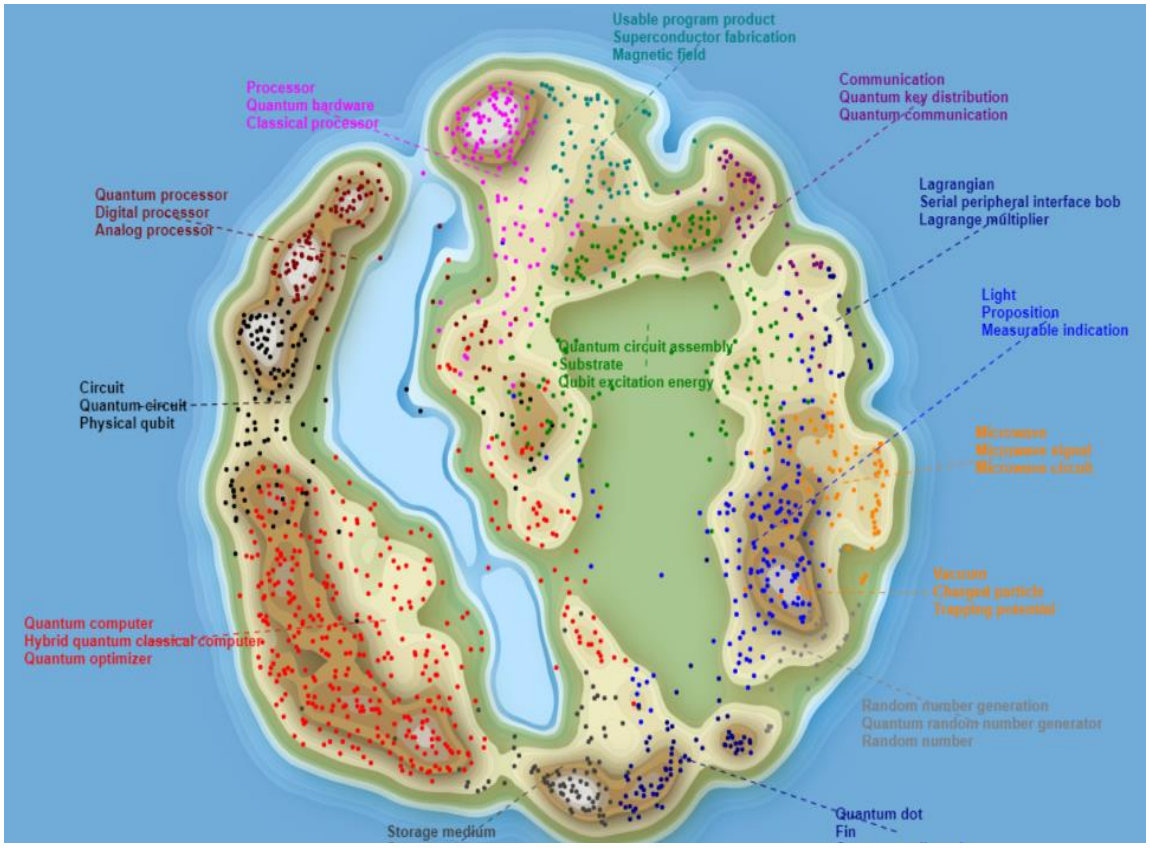


Figure 16: Carte des clusters technologiques (Source: Orbit sur échantillon de 1 550 brevets)

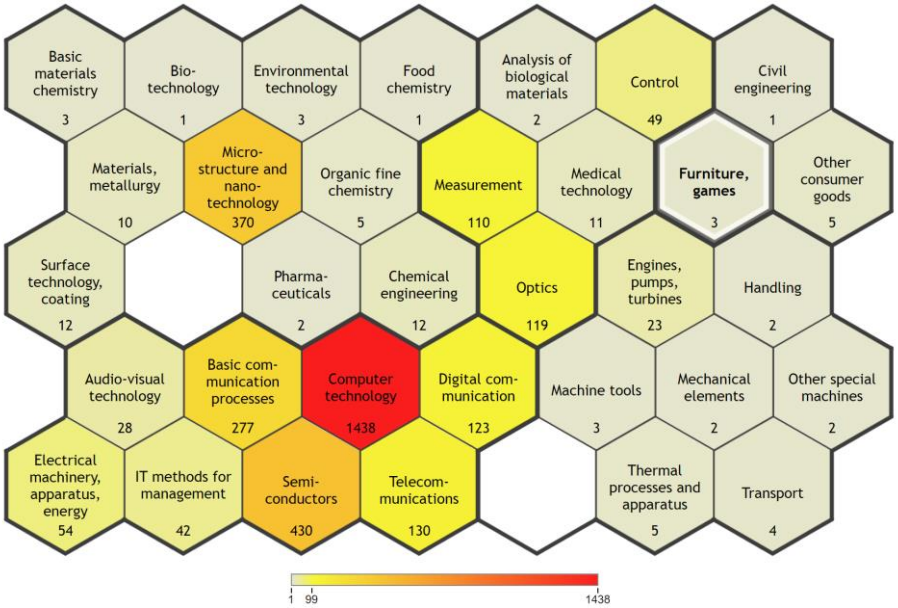


Figure 17: Domaines technologiques (Source: Orbit sur 1 550 brevets)

5. Conclusion

La présente étude visait à récolter, analyser et regrouper les informations relatives aux brevets sur les technologies quantiques dont la date de priorité était postérieure à 2009.

L'analyse et le regroupement des informations a confirmé l'importance du rôle tenu par la Chine dans le domaine des télécommunications quantiques ce qui, avec le reste de leur production de brevets, leur permet de revendiquer plus de la moitié des brevets déposés.

La forte progression globale des nombres de brevets se retrouve démultipliée sur le domaine spécifique de l'informatique quantique qui reste pour l'instant toujours sous la domination des USA avec plus de la moitié de l'innovation brevetée dans ce domaine.

La diversité des acteurs, multinationales des TIC, startups, universités, agences de transfert des technologies, agences gouvernementales militaires et civiles est à l'image de la diversité des technologies explorées et certainement un signe du potentiel disruptif de ces nouvelles technologies pour beaucoup de secteurs de l'activité humaine : télécommunication, finance, transport, médicine, chimie, nouveaux matériaux et molécules pour ne citer que ceux-là.

- ANNEXE 3 -

EVALUATION SCIENTOMETRIQUE DES PUBLICATIONS MONDIALES EN LIEN AVEC LA RECHERCHE EN INFORMATIQUE QUANTIQUE POUR LA PERIODE 2010-2020

Michel Kurek – Ecole Polytechnique – mai 2020

En nous basant sur les informations indexées dans la base de données Scopus[215] (www.scopus.com), nous proposons dans cette annexe une analyse quantitative de la recherche scientifique mondiale en informatique quantique sous l'angle des publications diffusées sur le sujet. Cette étude scientométrique analyse différents indicateurs sur les publications (papiers de recherche, conférences, chapitres de livres…) et les citations croisées mentionnant ces publications. Peu d'étude de ce type existe sur l'informatique quantique, soit les paramètres de recherches sont trop larges, ou trop restrictifs, soit les études datent (par exemple [215] qui analyse la période 2007-2016). Nous pensons donc que notre approche apportera quelques éléments d'éclairage nouveaux.

Le concept d'informatique quantique a émergé dans les années 1980 avec notamment les travaux de Richard Feynman [14] puis ceux de David Deutsch [216]. Aujourd'hui les preuves de principes sont nombreuses et certains produits sont même commercialisés depuis plusieurs années (par ex. le canadien D-Wave qui vend des ordinateurs quantiques de type *annealer*[216] et offre depuis peu un service Cloud [217], nous pouvons aussi citer IBM qui propose aussi des services dans le Cloud, Google, Rigetti…). La technologie n'est toutefois pas mature et les travaux de recherche fondamentale et de recherche appliquée seront encore longs [218].

Pour être en phase avec l'échelle de temps de la recherche et l'étude sur les brevets que nous avons présenté dans l'annexe précédente, nous avons choisi d'effectuer notre analyse sur une période de dix ans (2010-2019) à laquelle nous avons rajouté la production courante de 2020. Les informations ont été extraites puis téléchargées de Scopus le 21 mai 2020. L'année 2020 n'est donc pas complète. Elle est aussi particulière compte tenu de la crise sanitaire mondiale du SARS-CoV-2.

Pour résumer, nous avons recensé un total de 15 602 publications sur la décennie 2010-2019. Le taux de croissance annuel moyen a été de 10.4% et, au 21 mai 2020, chaque publication fut citée en moyenne 14.8 fois.

Pour 2020, 677 références sont actuellement dénombrées, ce qui, extrapolé sur une année complète, marquerait une baisse d'environ 20% de la production scientifique sur le sujet. L'échantillon total comprend au final 16 279 publications.

Les 10 premiers pays, les plus productifs en nombre de publications sur la période, totalisent 98.9 % des publications mondiales. Les USA représentent la part la plus élevée (26.4%) devant la Chine (22.8%).

L'Allemagne, l'Australie et les USA sont les trois pays dont les publications ont été, en relatif, les plus citées. La collaboration internationale a été un moteur important de la recherche dans ce domaine. Pour les 10 premiers pays, 8 articles sur 10 (83%) sont issus d'une publication collaborative internationale. L'Australie est le pays qui collabore le plus (130%) tandis que l'Inde est pour l'instant plus fermée (33%).

Physique et informatique sont les deux domaines de recherche les plus populaires rattachés à notre sujet. Notre étude identifie les 20 organisations et auteurs les plus productifs, les 20 revues les plus utilisées, ainsi que les 336 articles, très cités, avec plus de 100 citations par article.

---

[215] https://fr.wikipedia.org/wiki/Scopus_(Elsevier)

[216] Le recuit quantique ou « quantum annealing » est le principe mis en œuvre pour ces processeurs spécialisés pour des problèmes d'optimisation très spécifiques.

1. Objectifs

En traitant les informations recueillies de la base de données Scopus, nous cherchons dans cette étude à qualifier l'intérêt de la communauté scientifique sur le thème de l'informatique quantique par l'analyse de différentes métriques liées à ses publications sur le sujet. Nous développerons ici les points suivants:

- Evolution au cours du temps du nombre de publications
- Impact des publications par le nombre de citations recensées
- Répartition géographique, production des 10 pays les plus prolifiques
- Distribution de la recherche par sous domaine scientifique
- Profil des 20 organismes et auteurs les plus productifs
- Modes de communications privilégiés (articles, conférences, livres…)
- Profil bibliométrique des 336 articles les plus cités

2. Méthodologie

A la date du 21 mai 2020 nous avons interrogé Scopus à partir de l'équation de recherche :

TITLE-ABS-KEY ("quantum comput*") AND PUBYEAR > 2009

Cette requête nous permet d'extraire les informations sur les documents publiées depuis 2010 contenant dans leur titre, résumé (abstract), ou mots-clés (keywords) les combinaisons telles que *quantum computer*, ou *quantum computation*. Nous avons ensuite exploité les résultats de la recherche sous Excel.

3. Analyse

3.1. Evolution annuelle de la recherche mondiale en informatique quantique

Sur la période 2010-2020 le nombre de publications est de 16 279, passant de 895 en 2010 à 2 181 en 2019, soit un taux de croissance annuel moyen (CAGR) de 10.4%. Comme illustré par la figure 1, la forte hausse des années 2010-2012 a été suivi par une production quasi constante entre 2012 et 2015. Depuis 2015, l'intérêt sur notre sujet s'est accru avec une croissance moyenne de 9.6%/an[217].

L'année 2020 sera une année très particulière. En raison du confinement généralisé que nous avons connu suite à la pandémie du SARS-CoV-2 l'accès à la plupart des laboratoires a été bloqué, les travaux de recherche très ralentis, les conférences annulées. En extrapolant à partir des 677 publications publiées en 2020 à la date de rédaction de ce document une baisse de la production sur l'année complète est à prévoir à moins que la période ait été mise à profit pour des travaux de rédaction d'articles.

Année	Total publications (TP)	Total citations (TC)	Citations par publication (CPP)
2010	895	41 136	46,0
2011	1 047	25 387	24,2
2012	1 459	32 953	22,6
2013	1 468	32 549	22,2
2014	1 492	27 628	18,5
2015	1 511	23 615	15,6
2016	1 711	22 529	13,2
2017	1 759	16 990	9,7
2018	2 079	13 755	6,6
2019	2 181	4 787	2,2
2020	677	207	0,3
2010-2020	**16 279**	**241 536**	**14,8**

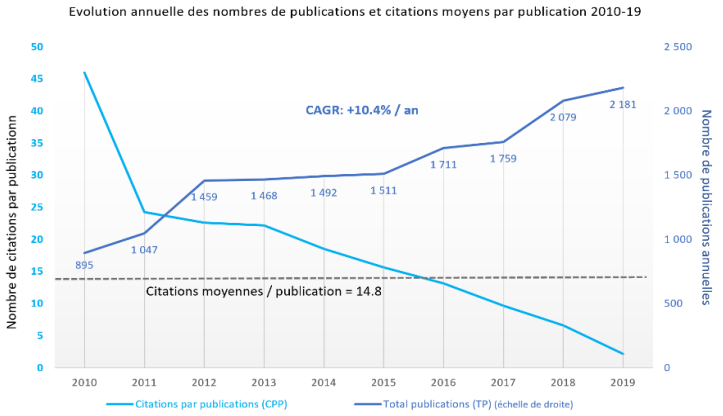


Figure 1 : Evolution du nombre de publications et citations globales dans la recherche en informatique quantique 2010-2020

[217] A titre de comparaison nous avons recensé sur Scopus le nombre de publications mentionnant « Artificial Intelligence » sur la période 2015-2019. Nous passons ici de 21 703 publications en 2015 à 27 657 en 2019, soit un CAGR de 6.25%.

Le nombre total de publications citant les 16 279 documents est actuellement de 241 536. Le taux moyen de citation sur la période 2010-2020 est de 14.8 citations par publication.

Les types de publication sont illustrés figure 2. Plus des deux tiers (67.7%) sont des articles scientifiques, près de 25% des actes de conférences ou de congrès. Les revues d'articles représentent 2.7% et les chapitres de livre 2.2%. Les revues de conférences et les livres complets représentent moins de 1% chacun.

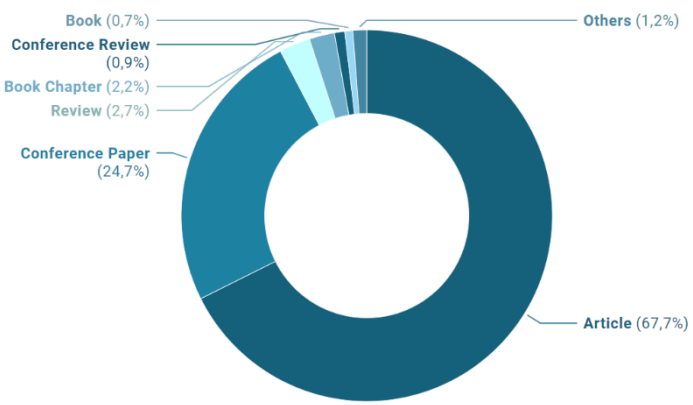


Figure 2: Types de publication

3.2. Répartition géographique de la recherche mondiale en informatique quantique

Les métadonnées « affiliation tag » et « country tag » disponibles dans Scopus permettent de définir les (le) pays d'origine des institutions auxquelles sont affiliés les (l') auteur(s) d'un document au moment de sa publication.

	Pays	TP	%TP	TC	%TC	CPP	RCI	%ICPEI
1	USA	4 295	26,4%	108 128	44,8%	25,2	1,7	70%
2	China	3 706	22,8%	38 611	16,0%	10,4	0,7	44%
3	UK	1 428	8,8%	32 435	13,4%	22,7	1,5	120%
4	Germany	1 400	8,6%	38 339	15,9%	27,4	1,9	123%
5	Japan	1 106	6,8%	20 996	8,7%	19,0	1,3	99%
6	Canada	1 056	6,5%	23 104	9,6%	21,9	1,5	124%
7	India	991	6,1%	5 847	2,4%	5,9	0,4	33%
8	Australia	777	4,8%	20 777	8,6%	26,7	1,8	130%
9	France	699	4,3%	14 016	5,8%	20,1	1,4	117%
10	Italy	635	3,9%	10 522	4,4%	16,6	1,1	116%
	Total 10 pays	16 093	98,9%	312 775	129,5%	19,4	1,3	83,1%
	Total monde	16 279		241 536		14,8		

*TP= Total Publication ; TC = Total Citation ; CPP = Citation par Publication = TC/TP ;
RCI = Relative Citation Index ; ICPEI = International Collaboration Publication Extended Index

Figure 3: Répartition des publications, citations et indice de collaboration pour les 10 pays les plus productifs dans la recherche en informatique quantique sur la période 2010-2020

Le tableau ci-dessus (Figure 3) résume les sept métriques que nous avons calculées puis analysées. Nous les retrouverons dans d'autres sections de cette étude mais pouvons les définir ici :

- TP : Total des Publications,
- %TP : Total des Publications en pourcentage du total mondial,
- TC : Total des Citations en nombre et pourcentage (%TC),
- CPP : Taux de Citation par Publication (CPP = TC/TP),
- Il faut noter que des chevauchements sont possibles dans les décomptes de quantités comme le nombre de publications (TP) ou de citations (TC). Ainsi une publication cosignée par plusieurs auteurs dont les affiliations sont de nationalités différentes est comptabilisée pour chacun des pays impliqués.

- RCI : « Relative Citation Index» [219] compare le taux de citation avec la moyenne mondiale (le taux global moyen de citation valant dans notre étude 14.8). Il est calculé en divisant le nombre moyen de citations par publication dans un sous-domaine donné, par le taux moyen mondial de citations pour toutes les publications. Un RCI supérieur à 1 indique un score plus élevé par rapport à la norme mondiale, un RCI inférieur à 1 une performance relativement plus faible.
- Enfin, l'Indice étendu de Collaboration Internationale des Publications (%ICPEI - International Collaborative Publications Extended Index) sera abordé dans la section suivante de ce document.

Sur la période 2010-2020, le sujet de l'informatique quantique a été largement abordé puisque le panel de pays représenté est très large, avec 111 pays.

La concentration est toutefois très forte. Le TOP 10 des pays les plus productifs (Figure 3) totalise 98.9% des publications. USA et Chine se détachent du classement. Les USA domine ainsi avec 26.4% suivi par la Chine avec 22.8% (Figure 4). Le UK est troisième avec 8.8%. La France se situe à la 9ème position avec 4.3% des publications.

Comme on peut le constater sur les figure 4 à figure 6, le Royaume-Uni et l'Allemagne, très proche l'un de l'autre, alterne à la 3ème position tant en termes de production annuelle que de citations.

L'Inde en 7ème position pour le nombre de publication n'est que 10ème pour les citations (Figure 4Figure 5). Son indice RCI de 0.4 est pratiquement 5 fois inférieur à celui de l'Allemagne et de l'Australie qui sont les pays dont les articles sont les plus cités (RCI = 1.9 et 1.8 respectivement).

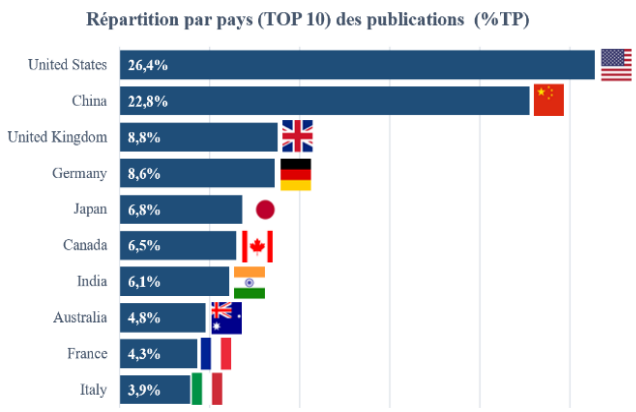


Figure 4: TOP 10 en nombre de publications

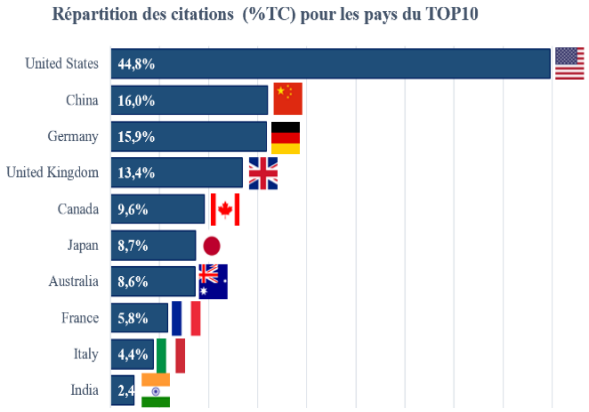


Figure 5: TOP 10 en nombre de citations

Outre les éléments déjà mentionnés, on peut remarquer sur la figure 6 le dynamisme récent en Inde et au Canada, le Chine marquant, quant à elle, un léger retrait en 2019.

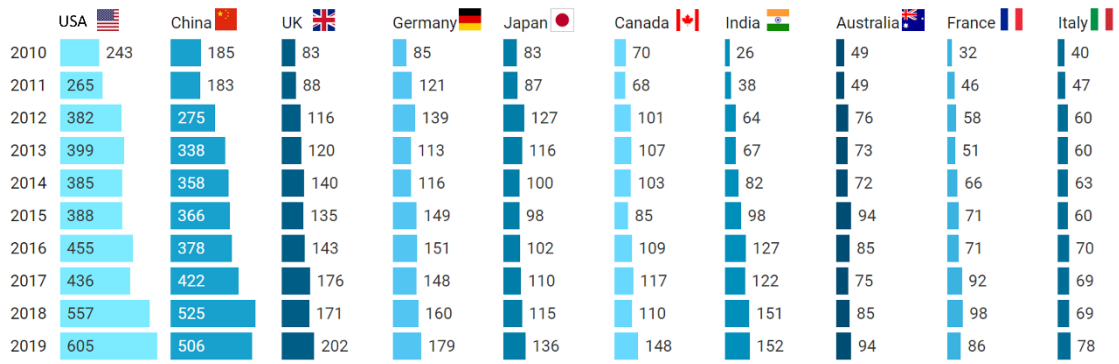


Figure 6: Evolution annuelle du nombre de publications pour les 10 pays les plus productifs (2010-2019)

3.3. Collaboration internationale

L'indice étendu de collaboration internationale des publications (%ICPEI) que l'on trouve dans le tableau de la figure 3 vise à mesurer la collaboration sur un domaine de recherche particulier d'un pays, d'un organisme d'affiliation (université, entreprise…), ou bien encore d'un auteur donné.

A notre connaissance c'est la première fois que cet indice est proposé dans la littérature sous cette forme. Il s'agit d'une extension de l'indice ICP (International Collaborative Papers) qui mesure le ratio entre le nombre de publications issues d'une collaboration internationale et le nombre total de publications. L'ICP crédite d'une même valeur une publication quel que soit le nombre de nationalités des cosignataires (ou des organismes d'affiliation).

Nous proposons et définissons dans cette étude un indice permettant d'être plus précis sur la mesure de la collaboration internationale d'une co-publication. A la différence de l'indice ICP, un papier co-signé par exemple par 3 pays différents aura une métrique ICPEI supérieure à un papier co-signé par 2 pays.

Notre indice est défini comme étant, pour un pays de référence (ou auteur ou organisme de référence), le ratio entre le nombre de liens internationaux pour les publications multinationales et le nombre de publications. La nationalité est définie par le pays de l'organisme d'affiliation des auteurs à la date de publication des documents.

$$\%ICPEI = \frac{\sum_{k=1}^{N} \begin{array}{c} Nombre\ de\ pays\ impliqués\ dans\ la\ rédaction \\ de\ la\ publication\ numéro\ k\ autre\ que\ le\ pays\ de\ référence \end{array}}{N},$$

$$où\ N = nombre\ de\ publication\ du\ pays\ de\ référence$$

A la différence de l'ICP, pour une publication donnée avec des auteurs multiples, nous comptabilisons le nombre total de pays impliqués. L'ICPEI d'une publication ayant un seul auteur vaut 0. L'indice d'une publication ayant plusieurs auteurs affiliés à des organismes identiques ou différents mais de même nationalité est également nul. Une publication issue de la collaboration de trois universités appartenant à trois pays différents (université_1 = université du pays A de référence, université_2 = pays B, université_3 = pays C) a un indice de 200%.

Comme on a pu le constater sur la figure 3, entre 2010 et 2020, la collaboration internationale des 10 pays les plus productifs dans la recherche en informatique quantique varie de 33% à 130% avec un taux moyen de 83.1%. Les pays les plus collaboratifs sont l'Australie, le Canada et l'Allemagne (130%, 124% et 120%). Les USA (70%), la Chine (44%) et l'Inde (33%) sont les pays qui ont le moins collaboré.

3.4. Distribution de la recherche par sous-domaine

Utilisant la classification de la base de données Scopus nous présentons en figure 8, les 10 domaines principaux ayant donné lieu à un travail de publication en lien avec l'informatique quantique.

Les catégories les plus représentées sont celles de la physique (32.6%), suivi de l'informatique (17.5%) et de l'ingénierie (14.8%). Les sujets mathématiques et de science des matériaux sont à peu près à part équivalente (11.7% et 11.4% respectivement).

Ces chiffres ont été normalisés pour tenir compte du fait que certaines publications abordent plusieurs sujets en même temps. D'autres statistiques sont présentées figure 7. Les publications multidisciplinaires et ayant trait à la chimie présentent le taux de citation (CPP) le plus élevé.

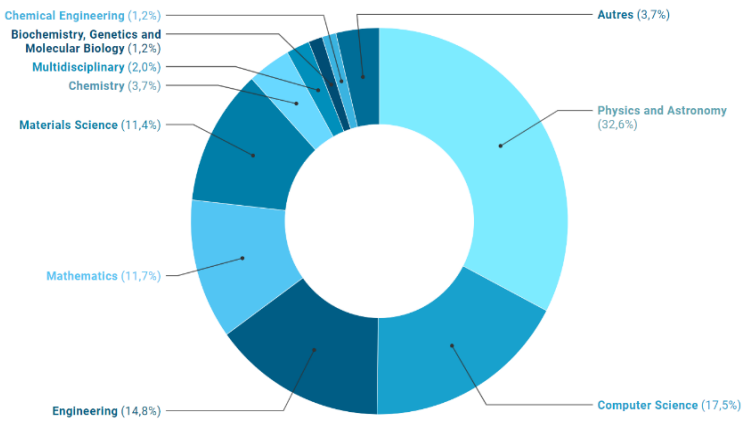


Figure 8: Répartition par sous-domaine scientifique

Domaine	TP	%TP	TC	CPP
Physics and Astronomy	10 004	32,6%	169 012	16,9
Computer Science	5 388	17,5%	33 011	6,1
Engineering	4 558	14,8%	32 803	7,2
Mathematics	3 583	11,7%	24 315	6,8
Materials Science	3 511	11,4%	40 940	11,7
Chemistry	1 140	3,7%	25 277	22,2
Multidisciplinary	627	2,0%	36 606	58,4
Biochemistry, Genetics and Molecular Biology	383	1,2%	10 125	26,4
Chemical Engineering	354	1,2%	9 177	25,9
Social Sciences	291	0,9%	2 024	7,0

Figure 7: Statistiques par sous-domaine des publications 2010-2020

3.5. Répartition des mots-clés les plus cités

Le nuage de mots de la figure 9 met en exergue les mots-clés les plus usités dans les différentes publications ressortant pour notre recherche.

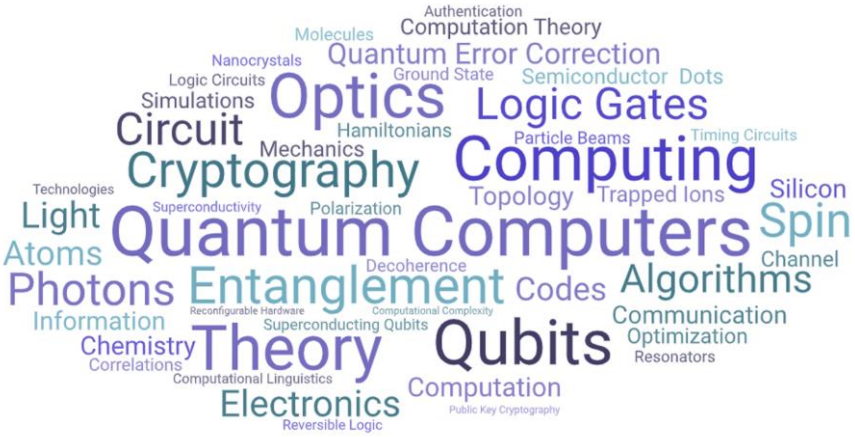


Figure 9: Nuage des 50 mots-clés les plus usités par les auteurs

Les cinq mots-clés les plus présents sont « Quantum Computers » employé 11 900 fois, puis « Quantum Optics » (4 558), « Quantum Theory » (4 068), « Quantum Computing » (3 325), « Quantum Entanglement » (2 962). On y retrouve également, sans surprise, les différentes technologies explorées ou utilisées aujourd'hui pour construire les ordinateurs quantiques : photon, ions piégés, atome, silicium supraconducteur, nanocristal, propriété topologique de la matière [220].

En dehors des éléments liés au matériel (*hardware*), les domaines d'applications comme la communication (cryptographie), la simulation (chimie) et l'optimisation sont mentionnés. Enfin les aspects algorithmiques ont une bonne place avec bien sûr les Qubits (bits quantiques), code correcteur d'erreurs, circuit et porte logique quantique [221].

3.6. TOP 20 des organismes mondiaux les plus productifs

Ce sont 2 506 organismes (université, entreprises…) qui ont publié sur le sujet de l'informatique quantique entre 2010 et 2020 mais la répartition est très inégale. Seules 154 institutions ont diffusé plus de 50 publications : 102 ont publié entre 50 et 99 fois, 29 ont fait entre 100 et 149 publications, 17 entre 150 et 299, et seulement 6 institutions ont publié plus de 300 fois.

Sur la période 2010-2020, le nombre de publications des 20 institutions les plus prolifiques (Figure 10) varie entre 160 et 524. Ensemble, le TOP 20 totalise 31.2% (5 078) des publications mondiales sur le sujet et 54.4% des citations (Figure 11).

Figure 10: TOP 20 des organisations (affiliations) les plus productives sur l'informatique quantique 2010-2020

	Institution	TP	TC	CPP	RCI	%ICPEI	HI
1	Chinese Academy of Sciences, China	524	7 262	13,9	0,93	75%	38
2	University of Science and Technology of China	362	7 093	19,6	1,32	56%	40
3	University of Waterloo, Canada	354	9 234	26,1	1,76	121%	39
4	National University of Singapore	340	5 887	17,3	1,17	143%	38
5	CNRS Centre National de la Recherche Scientifique, France	316	7 073	22,4	1,51	116%	39
6	Centre for Quantum Technologies Singapore	306	5 401	17,7	1,19	152%	35
7	University of Oxford, UK	298	8 676	29,1	1,96	115%	45
8	Massachusetts Institute of Technology, USA	271	8 334	30,8	2,07	85%	39
9	Tsinghua University, China	268	5 272	19,7	1,33	80%	32
10	University of Maryland, USA	243	9 625	39,6	2,67	47%	42
11	National Institute of Standards and Technology, USA	208	8 431	40,5	2,73	70%	38
12	University of Tokyo, Japan	202	4 342	21,5	1,45	78%	31
13	Delft University of Technology, Netherlands	185	5 827	31,5	2,12	149%	39
14	University of New South Wales UNSW Australia	184	5 439	29,6	1,99	108%	30
15	Ministry of Education China	183	2 089	11,4	0,77	19%	21
16	ETH Zürich, Switzerland	178	5 086	28,6	1,93	149%	39
17	Harvard University, USA	170	8 864	52,1	3,51	113%	47
18	University College London, UK	164	3 206	19,5	1,32	132%	28
19	University of California Santa Barbara, USA	162	9 701	59,9	4,04	68%	42
20	Perimeter Institute for Theoretical Physics, Canada	160	4 673	29,2	1,97	116%	29
	Total TOP 20 institutions	5 078	131 515	25,9	1,75	99%	37
	Total Monde	16 279	241 536				
	Part TOP 20 vs Monde	31,2%	54,4%				

Figure 11: Statistique sur le TOP 20 des organismes les plus productifs sur l'informatique quantique entre 2010-2020

Nous observons après une analyse plus détaillée de ce tableau :

- Neuf institutions du TOP 20 ont publié plus que la moyenne du groupe (254) : CAS et USTC en Chine, l'université de Waterloo au Canada, la National University et son centre Quantum Technologies à Singapour, le CNRS en France, l'université d'Oxford au UK, le MIT aux USA, et l'université chinoise de Tsinghua.
- Onze institutions ont un impact de citations supérieur à la moyenne du groupe (CPP=25.9) : UCSB USA (59.9), Harvard USA (52.1), le NIST USA (40.5), UMD USA (39.6), l'université de Delft Pays-Bas (31.5), MIT USA (30.8), UNSW Australie (29.6), le Perimeter Institute Canadien (29.2), Oxford UK (29.1), ETH Zurich Suisse (28.6), University of Waterloo Canada (26.1).
- Onze institutions ont eu une collaboration internationale supérieure à la moyenne du groupe (99%) : les cinq premières sont le Centre de technologie quantique de Singapour (152%), ETH Zurich Suisse (149%), Université de Delft Pays-Bas (149%), NUS Singapour (143%), UCL UK (132%).
- Les publications avec co-auteurs sont comptabilisées pour chacun des auteurs et affiliations. Retraité de ces doublons, nous arrivons à un total de 3 823 documents produits par le TOP 20, ce qui représente en fait 23.5% de la production mondiale (et non pas 31.2%). Avec la même logique, le nombre de citations pour ces documents est de 94 986, ce qui représente 39.3% du total mondial (vs 54.4%). Ce type de correction n'est pas systématiquement réalisé dans les études scientométrique (par ex. [215]) mais il nous paraissait intéressant de préciser les chiffres.
- Nous reportons sur le tableau l'indice Hirsch[218] (« h-index » noté ici HI) tel que calculé par Scopus sur l'ensemble des publications sélectionnées rattachées à chacune des institutions concernées. Selon ce critère deux institutions se situent au-dessus de 45 : Harvard USA (47) et Oxford UK (45).

3.7. TOP 20 des auteurs les plus prolifiques

Plusieurs milliers de chercheurs contribuent à la recherche en informatique quantique, mais comme l'atteste la plupart des roadmaps gouvernementales publiées jusqu'ici dans le monde, leur nombre serait trop faible par rapport aux besoins futures. L'éducation et la formation dans le domaine des technologies quantiques sont des objectifs majeurs (lire par exemple le roadmap stratégique du Flagship Européen publié en février 2020 [71]).

Dans le cadre de notre étude nous avons recensé 22 755 auteurs. La très grande majorité n'a publié qu'un à cinq articles sur les dix dernières années. Seuls 88 auteurs ont publié plus de 25 fois : 54 auteurs de 25 à 34 fois, 24 auteurs de 35 à 44 fois, et 10 auteurs comptent 45 à 84 publications.

Le nombre de publications des 20 auteurs les plus prolifiques varie entre 39 et 84 (Figure 12). Ensemble, le TOP 20 totalise 5.8% (945) des publications mondiales sur le sujet et 15% des citations (36 303).

[218] Proposé par J. Hirsch en 2005[222], le calcul de cet indice part de la distribution statistique des citations dont font l'objet les travaux d'un chercheur, d'un département, d'une université ou même d'un pays. D'après Hirsch : « Un scientifique a un indice *h* si h de [ses] N_p articles ont chacun au moins *h* citations, et les autres (N_p - *h*) articles ont au plus *h* citations chacun ». Cet indice est aujourd'hui assez controversé : https://fr.wikipedia.org/wiki/Indice_h.

	Auteur	Affiliation	TP	TC	CPP	RCI	%ICPEI	HI docs	HI auteur
1	Wille, R.	Johannes Kepler University Linz, Linz, Austria	84	887	10,6	0,7	160%	17	30
2	Nori, F.	University of Michigan, United States	61	2 520	41,3	2,8	261%	20	96
3	Munro, W.J.	Nippon Telegraph and Telephone Corporation, Tokyo, Japan	57	1 116	19,6	1,3	209%	16	50
4	Drechsler, R.	University of Bremen, Bremen, Germany	54	688	12,7	0,9	73%	15	36
5	Guo, G.C.	Chinese Academy of Sciences, Beijing, China	48	1 108	23,1	1,6	50%	17	17
6	Morimae, T.	Yukawa Institute for Theoretical Physics, Kyoto, Japan	48	677	14,1	1,0	86%	16	69
7	Pan, J.W.	University of Science and Technology of China, Hefei, China	46	3 214	69,9	4,7	102%	23	51
8	Gambetta, J.M.	IBM Thomas J. Watson Research Center, Yorktown Heights, United States	46	2 622	57,0	3,8	17%	26	77
9	Martinis, J.M.	Google LLC, Mountain View, United States	45	4 352	96,7	6,5	64%	27	48
10	Simmons, M.Y.	University of New South Wales (UNSW) Australia, Sydney, Australia	45	1 710	38,0	2,6	100%	17	86
11	Nemoto, K.	Research Organization of Information and Systems National Institute of Informatics, Tokyo, Japan	44	929	21,1	1,4	89%	13	37
12	Zhang, S.	Yanbian University, Yanji, China	43	520	12,1	0,8	33%	12	28
13	Schoelkopf, R.J.	Yale University, New Haven, United States	42	3 488	83,1	5,6	71%	26	69
14	Aspuru-Guzik, A.	Harvard University, Cambridge, United States	41	2 609	63,6	4,3	105%	22	15
15	Hollenberg, L.C.L.	University of Melbourne, Parkville, Australia	41	2 253	55,0	3,7	100%	17	51
16	Kwek, L.C.	National University of Singapore, Singapore	41	660	16,1	1,1	146%	13	59
17	Bhattacharyya, S.	RCC Institute of Information Technology, Kolkata, India	41	295	7,2	0,5	32%	10	38
18	Fowler, A.G.	Google LLC, Mountain View, United States	40	3 301	82,5	5,6	189%	23	33
19	Dzurak, A.S.	University of New South Wales (UNSW) Australia, Sydney, Australia	39	3 165	81,2	5,5	149%	19	36
20	Haghparast, M.	Islamic Azad University, Tehran, Iran	39	189	4,9	0,3	23%	8	12
		Total TOP 20 auteurs	945	36 303	38,4	2,6	109%	18	47
		Total Monde	16 279	241 536					
		Part TOP20 vs monde	5,8%	15,0%					

Figure 12: Statistiques des 20 auteurs les plus productifs en terme de publications en lien avec l'informatique quantique entre 2010-2020

Nous observons après une analyse plus détaillée du tableau :

- Les publications avec cosignataires de la liste sont comptabilisées pour chacun des signataires. Retraité de ces doublons, nous comptabilisons un total de 816 documents pour le TOP 20 ce qui représente en fait 5% de la production mondiale (et non pas 5.8%). Pour la même raison, le nombre de citations pour ces 816 documents est de 28 872, ce qui représente 12% du total mondial (contre 15%).
- Six auteurs ont publié plus de 47.25 fois, qui est la moyenne du groupe TOP 20 : Wille (84), Nori (64), Munro (57), Drechsler (54), Guo (48), Morimae (48).
- Neuf auteurs ont un taux de citation supérieur à la moyenne du TOP 20 (CPP= 38.4) : Martinis (96.7), Schoelkopf (83.1), Fowler (82.5), Dzurak (81.2), Pan (69.9), Aspuru-Guzik (63.6), Gambetta (57.0), Hollenberg (55.0), Nori (41.3).
- Six auteurs ont eu un taux de collaboration internationale supérieur à la moyenne (%ICPEI=109%) : Nori (261), Munro (209), Fowler (189), Wille (160), Dzurak (149), Kwek (146).
- Nous avons reporté sur le tableau l'indice Hirsch (HI) des publications sélectionnées pour chacun des auteurs (i.e. traitant de l'informatique quantique : HI docs) ainsi que le « score » global de chacun d'eux (i.e. pour toutes leurs publications : HI auteur).

3.8. TOP 20 des sources de communication utilisées

Les journaux scientifiques (
Figure 13) sont les médias majoritairement utilisés pour les publications (11 670 soit 71.7%). Les actes de conférences représentent 20.4%, le format livre 7.5% et les journaux commerciaux marginalement 0.4%.

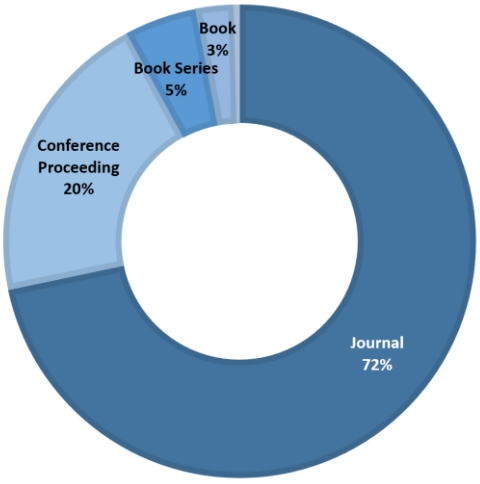


Figure 13: Type de source

Le nombre de publications des 20 journaux les plus représentés varie de 85 à 1 916. Ces 20 titres totalisent 6 028 articles, soit 51.7% de la production des articles publiés dans des journaux scientifiques pouvant traiter de sujets en rapport avec la recherche en informatique quantique sur la période 2010-2020.

Les revues de physique sont largement représentées (Figure 14), avec par exemple le mensuel *Physical Review A*, un des titres de l'American Physical Society (APS). Les recherches fondamentales et expérimentales pour déterminer le meilleur support physique de l'information quantique sont ainsi très actives [220] . C'est un des défis dans la course à l'ordinateur quantique universel (hardware) et les dispositifs candidats sont multiples (photons, ions, atomes).

	NOM DU JOURNAL	TP			
1	Physical Review A	1 916	11	Applied Physics Letters	133
2	Quantum Information Processing	738	12	Quantum Information And Computation	129
3	Physical Review Letters	730	13	Physical Review X	119
4	New Journal Of Physics	426	14	Wuli Xuebao Acta Physica Sinica	106
5	Physical Review B	331	15	Nature Physics	100
6	Scientific Reports	202	16	Optics Express	92
7	Chinese Physics B	174	17	IEEE Transactions On Information Theory	91
8	International Journal Of Theoretical Physics	167	18	Nano Letters	89
9	Nature	159	19	IEEE Access	86
10	Nature Communications	155	20	International Journal Of Quantum Information	85

Total TOP 20 Journal	6 028
Total Monde Journal	11 670
Part TOP20 vs monde	51,7%

Figure 14: TOP20 des journaux publiant le plus entre 2010-2020 et leurs éditeurs

Pour terminer cette section, nous présentons sur la figure 15 l'évolution du nombre de papiers en lien avec l'informatique quantique publié par le TOP 20 des journaux scientifiques entre 2010 et 2019.

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Physical Review A	87	99	216	218	166	237	253	236	236	131
Physical Review Letters	38	37	93	102	74	68	74	73	88	61
Quantum Information Processing	8	20	39	85	67	75	114	94	118	73
New Journal of Physics	20	27	40	43	49	46	59	41	60	36
Physical Review B	22	21	19	35	24	32	36	31	31	54
Scientific Reports		1	8	9	20	32	45	32	20	26
Chinese Physics B	5	12	22	19	24	23	10	19	28	11
International Journal of Theoretical Physics	7	6	3	10	21	12	20	21	25	29
Nature	16	17	12	10	8	7	14	17	22	26
Nature Communications	3	6	10	18	19	19	15	16	18	25
Applied Physics Letters	4	7	9	14	21	19	15	17	14	11
Quantum Information and Computation	17	11	8	9	19	16	12	8	12	12
Physical Review X		2	7	3	21	11	21	10	28	12
Wuli Xuebao/Acta Physica Sinica	3	2	6	7	5	17	13	9	26	17
Optics Express	1	3	3	8	10	16	10	10	15	13
Nature Physics	12	9	5	8	6	9	5	9	9	15
International Journal of Quantum Information	17	11	8	7	12	5	9	1	9	6
IEEE Transactions on Information Theory	5	6	6	9	16	9	3	9	9	12
Nano Letters	3	1	4	8	5	4	12	9	18	19
IEEE Access				1	3	3	4	12	11	32
TOTAL	268	298	518	623	590	660	744	674	797	621

Figure 15: Evolution du nombre de papiers publiés les journaux du TOP20 en lien avec l'informatique quantique sur 2010-2019

3.9. Publications les plus citées

Sur notre échantillon d'analyse, parmi les 16 279 publications recensées, seules 11 183 ont à ce jour au moins une citation. La publication la plus référencée est un article scientifique totalisant 9 739 citations. La moyenne est de 14.8 citations par publication.

Pour la suite de cette section, nous nous limiterons aux publications de type *article* (ou papier pour utiliser la terminologie anglaise) qui sont au nombre de 11 014 (soit près de 68% de notre base). Les articles cumulent 206 308 citations soit 85.4% du nombre total de citations 241 536.

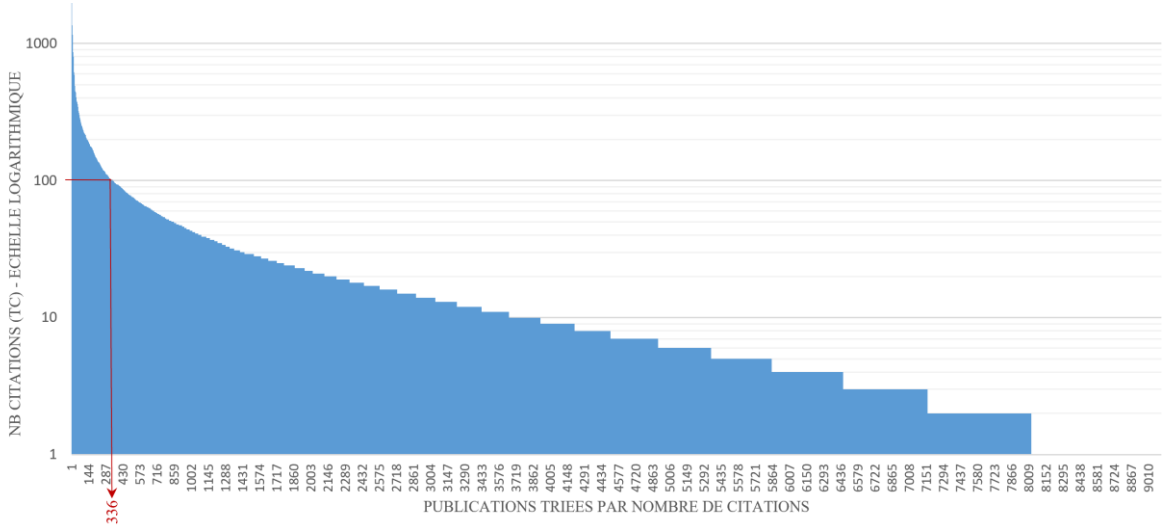


Figure 16: Répartition du nombre de citations par article (échelle logarithmique)

La distribution du nombre de citation est très étalée comme on peut le constater sur la figure 16 représentant les nombres de citations par papier classés dans l'ordre décroissant et en échelle logarithmique.

Nous nous concentrons à présent sur les articles ayant reçu plus de 100 citations pendant la période considérée. Cela exclut les articles de 2020, trop récents pour avoir atteint ce seuil. Cela ne doit préjuger en rien de leurs qualités.

A ce jour et sur la période de recherche considérée, 336 articles répondent à ce critère, soit 2.06% de la production mondiale de publications et 3.05% des articles. Comme on peut le constater sur l'histogramme de répartition du nombre de citations par papier (Figure 17), la distribution du nombre de citations est très inégale.

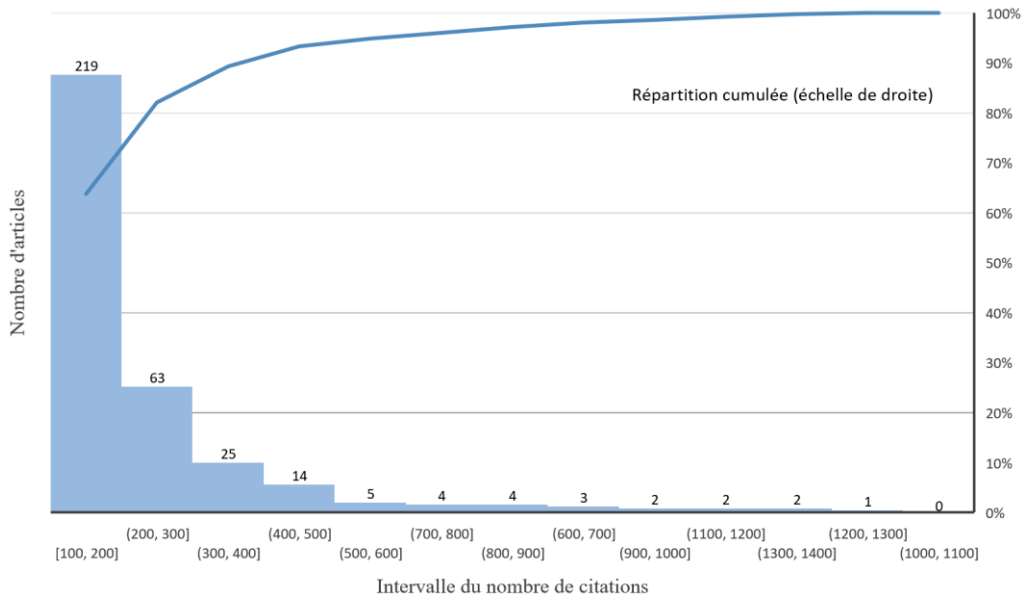


Figure 17: Histogramme du nombre de citations par article et cumul (%) – 1 article à 9 739 citations exclus

D'autres observations sont intéressantes :

- Sur les 336 articles les plus cités, 219 ont entre 100 et 200 citations, 63 ont entre 201 et 300 citations, 25 entre 301 et 400 citations, 14 entre 401 et 500 citations par papier. En fin de distribution un article non représenté sur l'histogramme possède 9 739 citations[219] à lui seul.
- Les 336 papiers cumulent 88 262 citations (provenant de 51 990 documents), soit une moyenne de 262.7 citations par papier.
- Une quarantaine de pays ont contribué à la rédaction de ces publications. Les USA domine largement avec 168 publications (50%), devant l'Allemagne (67), la Chine (53). La France est en 10ème position avec 20 articles.

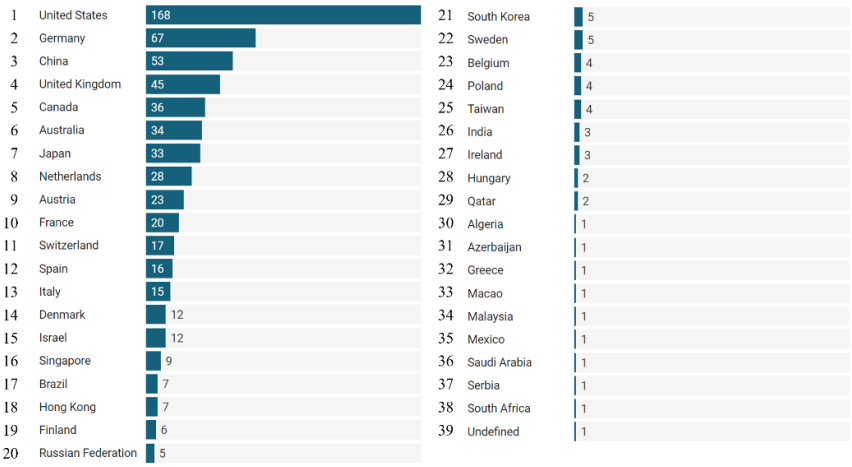


Figure 18: Origine des institutions ayant publié les 336 articles les plus cités (> 100 citations)

[219] Cet article de physique de la matière condensée écrit par Kane et Hazan[223] traite des isolants et supraconducteurs topologique, qui sont une des technologies possibles pour la construction d'un ordinateur quantique universel.

- Les mots-clefs les plus présents sont illustrés par le nuage de mots de la figure 19 :

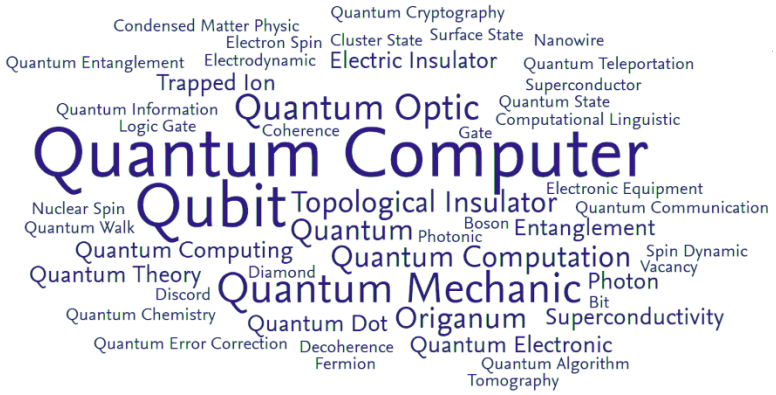


Figure 19: Mots clés les plus employés dans les 336 articles les plus cités

- Les 336 articles ont été écrit par 1 747 auteurs appartenant à 369 institutions. Les dix auteurs et institutions les plus actifs sont repris en figure 20. On peut constater que 6 des 10 premières institutions sont américaines.

	Auteur	Articles	TC	CPP	HI
1	Martinis, John M.	12	3 345	278,8	73
2	Pan, Jianwei	12	2 570	214,2	77
3	Sank, Daniel Thomas	10	2 605	260,5	41
4	Wenner, James	10	2 605	260,5	41
5	Cleland, Agnetta N.	9	2 846	316,2	55
6	Roushan, Pedram	9	2 404	267,1	31
7	Chen, Yu	9	2 354	261,6	32
8	Frunzio, Luigi	9	2 342	260,2	52
9	Schoelkopf, Robert J.	9	2 319	257,7	69
10	Lu, Chaoyang	9	2 167	240,8	40

	Institution	Auteurs	Articles	TC	CPP
1	University of California at Santa Barbara	62	25	7 271	290,8
2	Harvard University	46	24	5 330	222,1
3	Austrian Academy of Sciences	29	18	5 136	285,3
4	University of Science and Technology of China	85	17	3 457	203,4
5	Delft University of Technology	59	17	2 891	170,1
6	Massachusetts Institute of Technology	27	17	4 309	253,5
7	National Institute of Standards and Technology	58	17	4 015	236,2
8	University of Waterloo	24	15	3 021	201,4
9	University of Maryland, College Park	31	14	4 541	324,4
10	Yale University	46	14	3 743	267,4

Figure 20: TOP 10 des auteurs et institutions par nombre d'articles pour les 336 articles les plus cités

- D'après nos chiffres présentés en Figure 21, 195 papiers sur les 336 (58%) sont issus d'une collaboration d'au moins deux institutions de nationalités différentes. 63 (19%) ont été écrit au sein d'une même institution par au moins deux auteurs. 67 papiers (20%) sont issus de collaborations de plusieurs auteurs dans le même pays et enfin 11 articles (3%) ont été publié par un auteur unique.

Type de collaboration	(%)	Articles	TC	CPP
International collaboration	58,0%	195	45 689	234,3
Only national collaboration	20,0%	67	26 170	396,5
Only institutional collaboration	19,0%	63	12 771	202,7
Single authorship (no collaboration)	3,0%	11	3 354	304,9

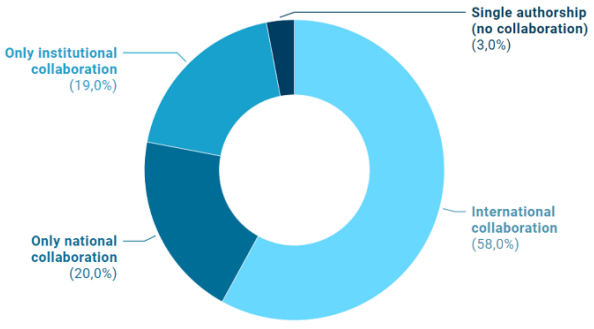


Figure 21: Type de collaboration pour les 336 articles les plus cités

4. Conclusion

Notre étude fournit une description quantitative et qualitative de la recherche en informatique quantique dans le monde au cours de la période 2010-2020. Nous nous sommes basés sur les données référencées dans la base de données transdisciplinaire Scopus de l'éditeur Elsevier.

A la date de rédaction de ce document, 16 279 publications en lien étroit avec le sujet de la recherche en informatique quantique ont été diffusé dans le monde avec une progression annuelle moyenne d'environ 10% par an depuis 10 ans. Il est fort probable par contre que la recherche et les publications soient impactés en 2020 par la crise sanitaire lié au SARS-CoV-2.

Les dix principaux pays dominants le monde de la recherche en informatique quantique sont : les USA, la Chine, le Royaume-Uni, l'Allemagne, le Japon, le Canada, l'Inde, l'Australie, la France et l'Italie, avec une part de 98.9 % des publications mondiales. Les publications ont un impact élevé de 14.8 citations par article en moyenne sur une fenêtre de citation de 10 ans.

Six des dix pays les plus productifs ont obtenu un indice de citation relatif (RCI) supérieur à la moyenne du groupe, soit 1.32. Les deux domaines scientifiques qui publient le plus sur les sujets liés à l'informatique quantique sont la physique (32.6%) et l'informatique (17%). Pour la physique, on peut évoquer les travaux théoriques et expérimentaux autour des différentes approches possible pour stocker et manipuler l'information quantique au niveau particulaire (conduisant au futur hardware de l'ordinateur quantique). L'informatique s'attèle quant à elle au sujet « software », programmation quantique, algorithme de correction d'erreurs, protocole de communication, cryptographie…

Les vingt institutions les plus productives sont situées exclusivement dans des pays développés, comme les USA (5), la Chine (4), Royaume-Uni (2), Singapour (2), Canada (2), Australie (1), le Japon (1), Suisse (1), Pays-Bas (1) et France (1). Les institutions de pays comme l'Australie, ou le Canada se démarquent par leur propension à collaborer, tandis que la Chine et l'Inde sont très en retrait.

Plus des deux-tiers des publications mondiales sur le sujet sont parues dans des revues spécialisées. Les 20 premières revues représentent plus de 50% de la production totale d'articles. Parmi les institutions ayant publié les articles les plus cités, 6 sur 10 sont américaines. La recherche en informatique quantique est mondiale mais elle est pour l'instant fortement concentrée.

- ANNEXE 4 - PAYSAGE MONDIAL DES INVESTISSEMENTS PUBLICS ET PRIVES

Michel Kurek – Ecole Polytechnique – Juillet 2020

La mécanique quantique est la théorie fondamentale des particules atomiques et subatomiques constituant les objets de l'univers et les forces animant ces objets. C'est selon les physiciens la meilleure théorie que nous ayons en physique mais pour laquelle il reste encore un certain nombre d'incertitudes[224].

Les technologies quantiques reposant sur cette science fondamentale ne sont pas matures pour la plupart. Au cours de ces dernières années, diverses initiatives ont été mis en place par plusieurs nations à travers le monde pour favoriser les développements de ces technologies potentiellement disruptives. Les maitriser est perçu par de nombreux États comme un enjeu majeur pour leur souveraineté et leur économie.

L'enjeu de souveraineté relève de deux sujets principaux liés : l'ordinateur quantique et les systèmes de communications quantiques sécurisées. Le risque existe de faire face, dans un futur proche, à des machines quantiques capables de casser les mécanismes de cryptage largement utilisés de nos jours dans la vie civile ou militaire.

Mais ces technologies qui progressent rapidement sont aussi une opportunité de développement sociétal. Elles sont susceptibles de créer des moyens fondamentalement nouveaux d'obtenir et de traiter l'information et de fournir des solutions jusqu'alors inatteignables à des problèmes liés, par exemple, à l'énergie, à la santé. Comme l'IA, les technologies quantiques représentent un atout pour le développement responsable de nos sociétés mais elles posent aussi des questions éthiques importantes.

Menaces et opportunités, une double analyse qui justifie des investissements significatifs tant publics que privés dont nous nous proposons d'analyser la teneur et l'évolution ces dix dernières années.

Cette étude comprend deux parties. Nous résumons dans la première section, les stratégies et investissements gouvernementaux en matière de technologies quantiques dans les principaux pays et régions du monde. Dans un second temps nous dressons un état des lieux des financements privés - plus particulièrement du capital risque (*venture capital*) - destinés à soutenir les startups se créant dans ces domaines.

1. Plans de développement et investissements publics

La figure 1 illustre l'ensemble des États ou union d'États ayant consacré ou budgété l'équivalent d'environ 1 milliard d'euros, ce qui est le cas de l'Union Européenne par exemple. Au sein de l'UE, des pays comme l'Allemagne ont également leur propre budget. Le plan français n'est pas encore confirmé mais nous avons fait le choix de le représenter avec un chiffre conservateur de 1G€ - le rapport Forteza (voir tableau ci-dessous) préconisant 1.4 G€.

La plupart des budgets ont été récemment augmentés (Allemagne, USA, UK, Inde, Israël). Le budget chinois traduit les efforts considérables fournis par cette nation pour développer son savoir-faire dans les domaines d'applications de la physique quantique (communications, ordinateurs, capteurs et métrologie) et soutenir les efforts de la défense nationale, ainsi que les innovateurs civils.

Figure 1: Investissement gouvernementaux notables (~1 milliards d'euros ou plus)

La table de la figure 2 détaille les éléments connus à ce jour au niveau mondial.

PAYS	STRATEGIE	INVESTISSEMENTS GOUVERNEMENTAUX
USA[1,2,3]	En 2018, signature de la loi sur l'initiative nationale quantique (NQI). Le NQI charge les organes du gouvernement fédéral (NIST, NSF et DOE) de catalyser la croissance du secteur des technologies quantiques par une collaboration avec les universités et l'industrie privée.	Le NQI a permis d'engager un financement de 1,2 B$ sur cinq ans. En février 2020, la présidence américaine a rajouté 860m$ de budget (dont 492m$ en 2021).
Canada[4,5]	En 2017, différents instituts publics (National Research Council of Canada, Natural Sciences and Engineering Research Council of Canada, Canadian Institute for Advanced Research) ont publié un rapport de symposium appelant à l'action pour: 1. Maintenir et développer l'excellence canadienne en matière de science quantique 2. Stimuler l'innovation pour saisir les opportunités du quantique.	Le Canada a investi plus d'un milliard de dollars canadien (660m€) dans la recherche quantique au cours de la dernière décennie.
UK[6,7]	Dès 2013, Le Royaume-Uni (UK) a été l'un des premiers pays européens à définir un plan d'actions et investir dans les technologies quantiques. En 2015, le rapport d'étape a précisé la stratégie nationale en identifiant cinq domaines d'actions prioritaires : 1. Permettre la mise en place d'une base solide de capacités sur ces technologies au UK 2. Stimuler les applications et les débouchés commerciaux au UK 3. Développer une main-d'œuvre qualifiée locale 4. Créer le contexte social et réglementaire adéquat 5. Maximiser les avantages pour le UK grâce à un engagement international.	Le programme britannique sur les technologies quantiques (National Quantum Technologies Programme) a permis d'investir plus d'un milliard de livres sterling depuis sa création en 2014 (public + privé) en deux vagues principales 270m£ en 2014 puis 350m£ en 2019.
UE[8,9]	Initié en 2016, et démarré dans les faits fin octobre 2018, la Commission européenne a lancé un programme dédié (Quantum Flagship Programme) dont les objectifs sont de : 1. Consolider et développer le leadership et l'excellence scientifiques européens dans la recherche quantique, y compris la formation des compétences pertinentes 2. Donner un coup de fouet à une industrie européenne compétitive dans le domaine des technologies quantiques afin de positionner l'Europe en tant que leader dans le futur paysage industriel mondial 3. Rendre l'Europe attrayante et dynamique pour la recherche innovante, les entreprises et les investissements dans les technologies quantiques, accélérant ainsi leurs développements et adoptions par le marché.	Le Quantum Flagship a reçu un financement de 1G€ sur 10 ans.
Germany[10,11,12]	En 2018, le gouvernement fédéral allemand a présenté un programme-cadre, partie intégrante de sa stratégie sur les High-Techs, visant à mettre les technologies quantiques sur le marché. Les ambitions su pays ont été confirmées dans le cadre du plan Post-Covid publié par la Chancellerie en juin 2020.	Aux 650m€ que le gouvernement voulait investir dans le développement d'ordinateurs quantiques (en particulier avec IBM), la Chancellerie allemande vient d'ajouter 1.35G€ (Juin 2020), ce qui représente donc une enveloppe de 2G€.
Suisse[13]	Les acteurs locaux du secteur des technologies quantiques ont publié le document *Quantum at the Crossroads* qui décrit le paysage quantique suisse et plaide pour un renforcement des investissements afin d'aider la Suisse à tirer parti de ses atouts en matière de quantique.	Le Centre National de Compétence en Recherche (NCCR "QSIT - Quantum Science and Technology"), science technologie a reçu un financement de 38m CHF entre 2010 et 2017.

France[14]	Fin 2019, le rapport de la mission parlementaire (Rapport Forteza) a été rendu. Celui-ci contient 6 recommandations : 1. Déployer sur le sol français une infrastructure de calcul quantique de pointe à destination de la recherche et l'industrie 2. Lancer un programme de développement technologique ambitieux 3. Mettre en place un programme de soutien au développement des usages 4. Créer un environnement d'innovation efficace 5. Déployer une stratégie de sécurité économique adaptée 6. Instaurer une gouvernance efficace Ce rapport devrait servir de support pour la préparation par le gouvernement d'un plan quantique français.	Le rapport Forteza préconise un investissement de 1.4 G€. Le plan français, en cours d'élaboration est attendu dans les mois qui viennent et devrait être de 1G€.
Pays-Bas[15,16]	En 2015, la coopération entre l'Université Technologique de Delft et TNO (The Netherland Organisation for Applied Scientific Research) a été formalisée par un solide engagement financier sur dix ans, fortement soutenu par différents néerlandais En 2019, les Pays-Bas ont publié un programme national sur les technologies quantiques en identifiant 4 domaines d'action pour renforcer son rôle dans les technologies quantiques : 1. Percées dans le domaine de la recherche et de l'innovation (avec 6 sujets : ordinateur, simulation, capteur, communication, algorithme, cryptologie post quantique) 2. Développement des écosystèmes, création de marchés et infrastructures 3. Capital humain : éducation, connaissances et compétences 4. Dialogue sociétal sur la technologie quantique.	135 m€ provenant de six entités seront investis dans QuTech, l'Institut de technologie quantique de l'Université de Delft et TNO (The Netherland Organisation for Applied Scientific Research) sur 10 ans.
Russie[17]	En 2012 s'est créé le Russian Quantum Center, un centre de recherche dédié aux trois principaux domaines des technologies quantiques (Ordinateurs, communications, capteurs et métrologie). Fin 2019 la Russie a annoncé son plan quinquennal sur les technologies quantiques en proposant d'injecter près de 1B$. Cette enveloppe fait partie d'un programme de 258 milliards de roubles (3.7 B$) pour la recherche et le développement dans les technologies numériques, que le Kremlin a jugé vital pour la modernisation et la diversification de l'économie russe. Au stade actuel, 3 entreprises sont responsables du développement du plan dans chacun des domaines.	La Russie désire investir 1B$ au cours des 5 prochaines années dans la recherche fondamentale et appliquée sur les quanta menée dans les principaux laboratoires russes, a déclaré le vice-premier ministre du pays. La moitié du financement serait public, le reste privé.
Israël[18,19]	En 2018 l'état israélien a décidé de la création d'un fonds destiné à soutenir la recherche universitaire israélienne dans les domaines des technologies quantiques. Fin 2019, le gouvernement a lancé un plan quantique beaucoup plus ambitieux. Le comité en charge du plan recommande en outre d'étendre le développement de systèmes et la recherche dans le domaine des communications quantiques, des capteurs quantiques dans l'industrie et la défense, des matériaux, de l'informatique en Cloud; de soutenir la construction d'une infrastructure de composants quantiques; de construire une infrastructure matérielle dans les établissements universitaires qui sera partagée par différentes disciplines et groupes de recherche; et d'investir dans la consolidation des efforts de coopération internationale. Le TELEM (Centre national pour la recherche et le développement) et le MAFAT (Ministère de la Défense) sont les principaux organismes impliqués.	Après avoir créé un fonds au capital limité en 2018 (27m$) le nouveau plan quantique 2019/2020 représenterait un investissement de 362m$ sur cinq ans.
Inde[20,21,22]	Pendant longtemps le potentiel des technologies quantiques ne fut pas très reconnu en Inde. L'inde est un acteur assez nouveau dans le secteur qui a commencé par investir en 2018 dans un plan de 27.9m$ sur 5 ans. En 2020, le gouvernement vient de décider d'investir beaucoup dans le secteur des ordinateurs, de la communication et la cryptographie quantique.	Les investissements font passer le plan quinquennal de 27.9m$ à 1.12B$.

Japon[23,24]	En 2018, le gouvernement japonais a lancé l'initiative Q-LEAP qui investit dans des projets de R&D en technologies quantiques dans les domaines suivants : - la simulation quantique et l'informatique quantique (objectif de construire un ordinateur à 100 qubit à 10 ans) - les capteurs et la métrologie quantique.	Le Japon prévoit plus de 30 milliards de yens (280 m$) pour des applications du quantique dans le cadre d'un plan décennal. Le programme Q-LEAP inclut un budget de 200m$ sur 10 ans. Le total des investissements réalisés par ces organismes de financement dans le domaine des sciences et technologies de l'information quantique au cours des 15 dernières années s'élève à 250 m$.
Chine[25,26,27]	En 2016, la Chine annonçait mettre l'accent sur les communications et l'informatique quantiques dans le cadre de son 13eme plan quinquennal (2016-2020). D'ici à 2030, la Chine entend étendre son l'infrastructure de communication quantique, développer un ordinateur quantique universel et construire un simulateur quantique efficace Un laboratoire national dédié (National Laboratory for Quantum Information Sciences - Hefei) est mis en place et a reçu 1 mds $ pour débuter tandis que des fonds additionnels sont disponibles grâce à d'autres initiatives nationales ou régionales	Le plan gouvernemental qui intègre la mise en place du centre d'Hefei est estimé à 10 milliards de dollars.
Australie[28]	En juin 2020, l'agence National CSIRO (Commonwealth Scientific and Industrial Research Organisation) a publié sa roadmap sur les technologies quantiques en préconisant : 1. Élaborer une stratégie nationale en matière de technologies quantique 2. Attirer, former et retenir les meilleurs talents dans ce domaine 3. Explorer des mécanismes de financement efficaces 4. Evaluer les capacités de l'industrie et les infrastructures.	~125mAUD$ (76m€) d'investissements entre 2017 et 2019.
Singapour[29]	Depuis 2007 la recherche sur le quantique est centralisée dans le Center for Quantum Technologies (CQT) de l'Université National de Singapour (NUS) avec un financement d'environ $15m$ annuels. Le centre travaille sur les calculateurs quantiques et la cryptographie quantique.	
Corée du Sud	En février 2019, le gouvernement coréen a annoncé un plan d'investissement sur 5 ans qui vise à développer les technologies clés pour l'informatique quantique. L'objectif est d'achever la démonstration d'un système informatique quantique exploitable de 5 qubits ayant une fiabilité de plus de 90 % d'ici 2023.	44.5 G Won (environ 33m€/40m$)
Taiwan[30]	Le programme taïwanais présente deux aspects intéressants : - le ministère fournira des subventions de 1.9m$ à chaque programme de recherche approuvé par les secteurs universitaires et industriels référents pour le développement de composants, d'algorithmes, d'ordinateurs ou des communications quantiques. Le ministère a déjà approuvé trois projets de cinq ans proposés par des équipes de recherche d'universités locales. En outre, le fabricant de semi-conducteurs TSMC a été désigné comme le premier participant industriel du programme - le ministère a signé un accord pour travailler avec la plate-forme d'informatique quantique cloud d'IBM.	Le gouvernement taïwanais financera de multiples efforts de recherche quantique avec un montant annuel de 60 millions de dollars taïwanais (environ 1,9 million de dollars US) par projet.

Figure 2: Plans gouvernementaux en faveur des technologies quantiques (stratégies et montants)

Listes des références : Stratégies, plans gouvernementaux et montants investis

[1] https://www.technologyreview.com/f/612679/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/
[2] https://techcrunch.com/2020/02/07/white-house-reportedly-aims-to-double-ai-research-budget-to-2b/
[3] https://www.whitehouse.gov/briefings-statements/president-trumps-fy-2021-budget-commits-double-investments-key-industries-future/
[4] https://nrc.canada.ca/sites/default/files/2019-03/2017_Symposium_Workshop_Report.pdf
[5] https://iopscience.iop.org/article/10.1088/2058-9565/ab029d
[6] https://www.gov.uk/government/publications/national-strategy-for-quantum-technologies
[7] https://www.gov.uk/government/news/1-billion-investment-makes-uk-a-frontrunner-in-quantum-technologies
[8] https://qt.eu/
[9] https://www.nature.com/news/europe-plans-giant-billion-euro-quantum-technologies-project-1.19796
[10] https://www.bmbf.de/upload_filestore/pub/Quantum_technologies.pdf
[11] https://www.businessinsider.com/germany-pumps-650-million-euros-into-ibm-quantum-computing-alliance-2019-9?IR=T
[12] https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Schlaglichter/Konjunkturpaket/2020-06-03-eckpunktepapier.pdf?__blob=publicationFile&v=9
[13] https://www.swiss-quantum.ch/SwissQuantum.pdf
[14] https://forteza.fr/wp-content/uploads/2020/01/A5_Rapport-quantique-public-BD.pdf
[15] https://qutech.nl/wp-content/uploads/2019/09/NAQT-2019-EN.pdf
[16] https://qutech.nl/investmentquantumtechnology/
[17] https://www.nature.com/articles/d41586-019-03855-z
[18] https://www.jpost.com/Israel-News/Israel-joins-the-race-to-become-a-quantum-superpower-574510
[19] https://en.globes.co.il/en/article-israel-joins-the-quantum-club-1001309384
[20] https://www.nature.com/articles/d41586-020-00288-x
[21] https://thenextweb.com/in/2020/02/01/india-finally-commits-to-quantum-computing-promises-1-12b-investment
[22] https://economictimes.indiatimes.com/tech/hardware/fms-rs-8000-crore-boost-will-help-india-bridge-gap-in-quantum-computing-with-us-china/articleshow/73835819.cms
[23] https://iopscience.iop.org/article/10.1088/2058-9565/ab0077
[24] https://asia.nikkei.com/Business/Technology/Japan-plots-20-year-race-to-quantum-computers-chasing-US-and-China
[25] https://www.cnas.org/publications/commentary/chinas-quantum-future
[26] https://www.scmp.com/news/china/society/article/2110563/china-building-worlds-biggest-quantum-research-facility
[27] https://www.leyton.com/blog/?p=3374-quantum-computing-review-investments-2018
[28] https://www.csiro.au/~/media/Do-Business/Files/Futures/Quantum/20-00095_SER-FUT_REPORT_QuantumTechnologyRoadmap_WEB_200518.pdf
[29] https://www.quantumlah.org/media/presentation/annualreport2017.pdf
[30] https://www.digitimes.com/news/a20181217PD203.html?mod=2-

2. Du public aux investissements privés

Devant le caractère potentiellement disruptif de produits qui émergeraient des recherches actuelles, nous avons vu dans la section précédente que des gouvernements ont décidé d'investir massivement dans ces domaines avec pour la plupart le triple enjeu :

- Enjeu de souveraineté, avec par exemple la capacité à protéger correctement les informations sensibles aujourd'hui cryptées mais potentiellement déchiffrables à terme par un ordinateur quantique suffisamment puissant et fiable.
- Enjeu technologique, avec la volonté de se positionner à la pointe de ces nouveaux domaines soit en capitalisant sur une tradition d'excellence scientifique (USA, UK, Allemagne, France), soit d'en développer une (Chine).
- Enjeu économique, avec la dynamisation des tissus industriels nationaux ou régionaux sur ces sujets.

La recherche est ainsi issue pour le moment principalement du secteur public dans les grands pays qui s'y investissent, mais compte tenu des bénéfices attendus[220] quelques très grands acteurs privés du numérique (Google, Intel, Microsoft, IBM, Honeywell, Amazon, Alibaba, Baidu…) se sont engagés dans des programmes de R&D, en informatique quantique, plus particulièrement.

Les montants des investissements sont généralement difficilement appréciables sauf lorsqu'ils sont rendus publiques par les services de communication des sociétés. Ce fut par exemple le cas en 2014 lorsqu'IBM annonça invertir plus de 3 milliards de dollars sur 5 ans dans deux vastes programmes de R&D dont l'objectif était de repousser les limites de la technologie des puces de silicium [226] en explorant éventuellement de nouvelles voies parallèles. Cela incluait, entres autres, la mise au point d'un processeur quantique. Fin juin 2020, soit six ans plus tard, IBM possède un parc de 18 ordinateurs quantiques. L'accès à cette flotte est disponible sur le Cloud, certaines machines étant libre d'accès (IBM Q Experience[221]) et d'autres réservées à IBM et aux membres du réseau IBM Network Q[222].

Au côté de ces grands noms, le paysages des entreprises privées commencent à se densifier de quelques centaines de startups à différents stades de maturité.

Les données concernant les investissements effectués dans les startups par des investisseurs privés (individu, fonds d'investissement, entreprise tierce) ou des fonds publics sont parfois présentes dans des bases de données telles que Pitchbook[223] ou Crunchbase[224] lorsqu'elles ne sont pas confidentielles. Nous avons pu ainsi extraire et recouper de telles informations pour une centaine de startups. Sur la période 2010-2020, nous recensons près de 300 transactions d'investissements de différents types (amorçage scaling, expansion …).

Comme l'illustre[225] la figure 3, c'est à partir de 2012 que les investisseurs ont commencé à s'intéresser aux startups du secteur. L'année 2017 a été particulièrement active avec plus de 300m$ investis, soit près du triple de l'année précédente, et ce fut essentiellement dans le *quantum computing (hardware)*.

---

[220] Par exemple, en 2019, le cabinet de conseil BCG estimait des économies de coûts et gains d'opportunités pour les utilisateurs de l'informatique quantique pouvant dépasser 450 milliards de dollars par an d'ici 20 ans et 850 mds après [225].
[221] IBM Q Experience est une plateforme en ligne qui permet aux utilisateurs d'accéder à un ensemble de processeurs quantiques d'IBM via le Cloud, https://www.ibm.com/quantum-computing/technology/experience
[222] IBM Q Network compte actuellement plus de 100 membres, partenaires industriels de différents secteurs (banques, automobiles, énergies…), startups, universités : https://www.ibm.com/quantum-computing/network/overview/
[223] https://pitchbook.com/
[224] https://www.crunchbase.com
[225] Nous avons adopté ici une classification identique à celle de l'article de la revue *Nature*[199] *« the quantum gold rush », oct2019*: *quantum computing*, *quantum software*, *quantum communication*.

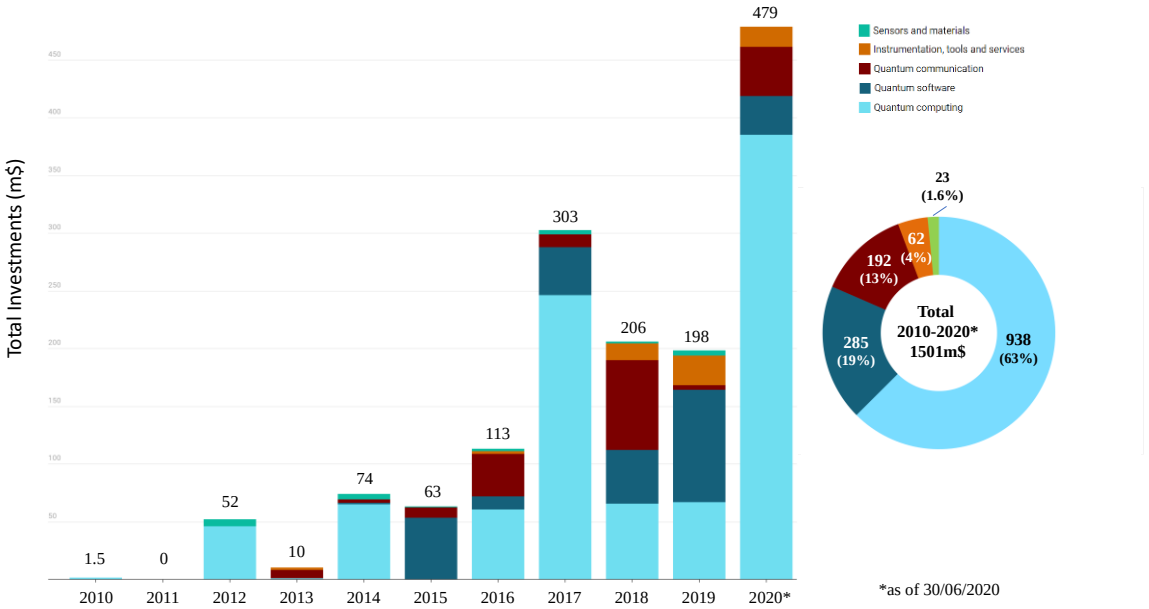


Figure 3: Investissements connus dans les startups des technologies quantiques 2010-2020

Avec en moyenne 200m$ par an, l'investissement s'est ensuite stabilisé pendant deux ans pour récemment augmenter très fortement sur le premier semestre 2020. Ainsi sur ce semestre, près de 480m$ ont servi à financer les développements des startups du quantique soit 58% de plus que l'année record 2017. Comme en 2017, c'est à nouveau le *quantum computing* qui concentre la majorité (80%) des accords de financement en montant du semestre.

Au total, depuis 2012, c'est 1.5G$ qui ont été investi dans les startups du secteur des technologies quantiques (80 recensées dans la base). Près des deux tiers des investissements (62.5%) déclarés ont été consacré aux 15 entreprises travaillant à la construction de processeur quantique (hardware). La partie Software, représentée par 37 firmes, a récolté quant à elle 285m$. Les 12 firmes travaillant sur les communications 192m$. Enfin 9 startups travaillant sur les techniques de mesures ou de détection basée sur la physique quantique et 8 construisant des composants de bases utilisés par les autres sociétés ont reçu respectivement 23m$ et 62m$.

La figure 4 complète cette analyse des montants investis par celle du nombre de transactions (*deals*) par année et secteur. Leur nombre a augmenté depuis 2015 avec une forte accélération en 2018 où de nombreux « petits » investissements ont été faits. Avec 24 deals sur le premier semestre 2020 il semble que le momentum des années passées n'ait pour l'instant pas été ralenti par la crise Covid-19. C'est ici le secteur du logiciel qui bénéficie le plus des investissements tandis capteurs et métrologie sont les parents pauvres du secteur.

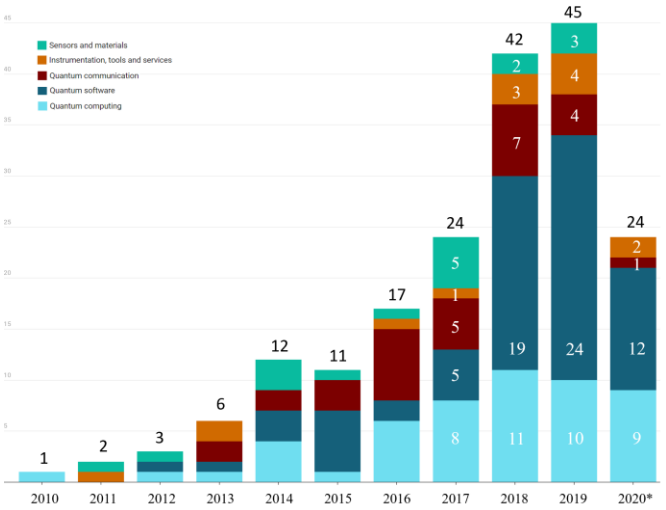


Figure 4: Evolution du nombre de deals de financement depuis 2010

Bien sûr, cette liste de startups, dont le financement est connu, n'est pas exhaustive. Beaucoup travaillent en mode furtif[226] ou encore à l'état embryonnaire. Un inventaire plus complet est proposé en fin d'annexe (figure 10).

[226] Une startup furtive (*stealth*) évite l'attention du public soit pour cacher des informations aux concurrents ou dans le cadre d'une stratégie marketing. Normalement, le mode furtif ne fonctionne que pendant les deux premières années.

Nous illustrons à présent en figure 5, l'emplacement ainsi que la liste des startups ayant reçu un investissement supérieur à 1m$ ainsi que les 25 plus importantes d'entre elles. Les plus importantes sont essentiellement en Amérique du Nord (PsiQuantum, D-Wave, IonQ, Rigetti).

Le cas de la firme suisse ID Quantique (IDQ), seule européenne dans le TOP5 est intéressant. Fondée en 2001 comme une startup spécialisée dans la sécurisation des communications au moyen de dispositifs de cryptographie quantique, elle commercialise son offre de service et produits depuis 2004 auprès d'entreprises, de différents secteurs comme celui de la finance, ou de gouvernements. En 2018, elle est passée sous le contrôle de l'opérateur de téléphonie mobile coréen SK Telecom[213].

En mai 2020, Samsung, SK et IDQ ont annoncé le lancement du premier mobile 5G équipé d'un chipset générateur quantique de nombres aléatoires (QRNG) [113], permettant aux usagers d'utiliser des services sélectionnés de manière sécurisée en générant de véritables nombres aléatoires qui ne peuvent pas être prédits (à la différence des pseudos nombres aléatoires générés au moyen d'algorithmes classiques).

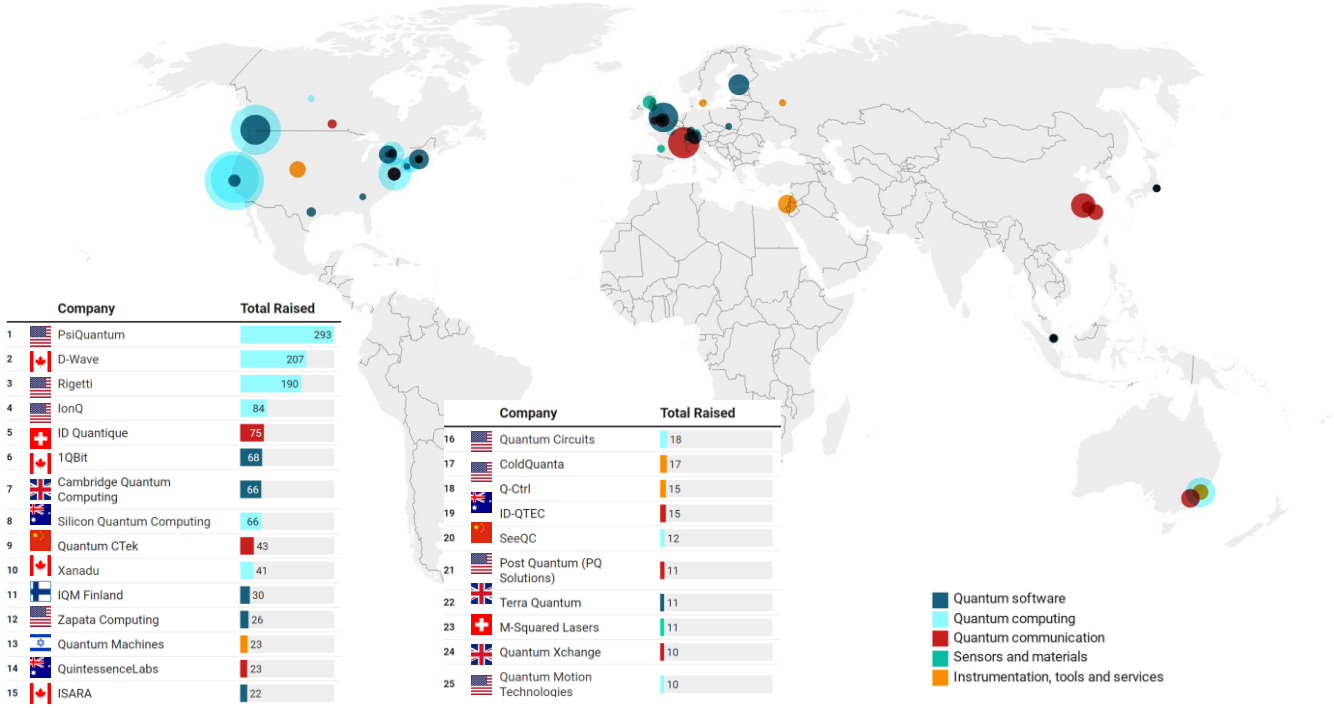


Figure 5: Localisation des startups ayant reçu des investissements≥ 1m$ entre 2010-2020 (m$)

A présent il est instructif de détailler la répartition des investissements effectués en *quantum computing* (hardware) par type de technologies employées par les différentes startups pour la construction des qubits, support de l'informations des ordinateurs quantiques (Figure 6).

La startup californienne PsiQuantum, fondée en 2016, projette de développer un processeur quantique photonique. Elle a reçu à elle seule 293m$. Ceci explique la part importante représentée par le financement d'architecture photonique (36%).

Les ordinateurs quantiques photoniques (ou à optique linéaire) encodent l'information dans des photons et non pas des ions, atomes ou électrons. Xanadu et ORCA Computing développent un projet similaire.

L'utilisation de la supraconductivité pour la construction des qubits mobilise un plus grand nombre d'acteurs. Au-delà des 225m$ investis dans des startups utilisant ces technologies, c'est sur ce type d'architecture que des acteurs majeurs comme IBM, Google, Rigetti, Alibaba ou même D-Wave investissent.

L'objet de cette section n'est pas de lister les avantages et inconvénient de chacune des technologies, mais retenons que tous les qubits ne sont pas équivalents. La famille des qubits supraconducteurs est elle-même particulièrement hétérogène.

Ainsi, les qubits supraconducteurs utilisés par D-Wave ont certaines particularités qui les cantonnent à la résolution de problèmes d'optimisations mathématiques spécifiques. Ils ne sont pas utilisés au sein de circuits de portes logiques quantiques comme cela peut être le cas pour les ordinateurs d'IBM, Google ou de la startup Rigetti.

Les ordinateurs de D-Wave, commercialisé depuis 2011, rentre dans la catégorie des ordinateurs à recuit simulé (annealing). La société a été récipiendaire de 207m$ soit 22% des fonds alloués depuis 2010.

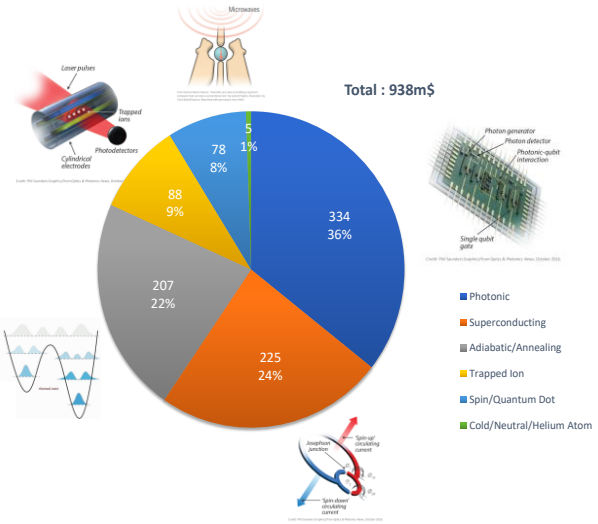


Figure 6: Répartition des investissements par technologie de qubit pour les startups travaillant sur le hardware

Les startups déployant des plateformes physiques à base d'ions piégés (*trapped ions*) ont recueilli 88m$ (9%), majoritairement alloués au leader IonQ. La firme autrichienne Alpine Quantum Technology (AQT), spin-off de l'université d'Innsbruck, reconnue pour ses travaux sur ces mêmes méthodes recourt aux subventions, financements non-dilutifs (la dernière étant de 11.2m$ en 2019). L'étude des ions piégés comme support de l'information quantique se poursuit aussi largement dans les laboratoires universitaires et l'arrivée récente sur ce créneau du géant Honeywell[227] traduit l'intérêt de toutes ces différentes catégories d'acteurs pour ce type de plateformes physiques.

La startup australienne Silicon Quantum Circuit (SQC), spin-off de l'université UNSW[227] a été créée en 2017. Elle travaille quant à elle, à la mise au point de qubits à base de semi-conducteurs et a reçu 66m$ d'investissements depuis sa création. Ces technologies, prometteuses, ont bénéficié de 8% des investissements. Elles sont également explorées par d'autres grands acteurs du secteur privé comme Intel mais aussi plusieurs organismes de recherche comme le laboratoire français du CEA-Leti, en pointe sur la recherche appliquée européenne.

Assez similaire dans son principe avec la technologie des ions piégés, l'utilisation d'atomes neutres est une approche plus récente étudiée par différentes startups comme la française Pasqal, ou la californienne Atom Computing. La startup ColdQuanta, qui collabore avec IonQ, travaille sur cette technologie dans un cadre plus élargi que la mise au point d'ordinateur quantique car elle est aussi utilisée dans le développement d'instruments de mesure et de capteurs ultra-sensibles.

Signalons enfin que les qubits topologiques, sur lesquels travaille Microsoft, et les qubits[228] à base de diamant (*NV Center*) n'apparaissent pas dans notre liste des financements de startups de l'informatique quantique.

Il est intéressant de comparer les résultats du sondage effectué en 2019 par le professeur et entrepreneur renommé Michele Mosca auprès de 22 professionnels du secteur des technologies quantiques[102]. La question était de classer les mises en œuvre physiques dans le but précis de réaliser un ordinateur quantique numérique avec 100 qubits logiques (i.e. programmables avec peu ou sans erreurs physiques) dans les 15 prochaines années.

[227] Université de Nouvelle-Galles du Sud, Australie
[228] Rentrant aussi dans la catégorie des qubits utilisant le degré de liberté, appelé spin, d'un électron.

Les réponses (Figure 7) indiquent un consensus assez général sur le fait que les plateformes favorites sont les systèmes supraconducteurs et les ions piégés. Ces résultats sont en phase avec les investissements réalisés à l'exception frappante des ordinateurs quantiques à optique linéaire. Ceci laisse à penser que si le potentiel technologique est élevé les investissements semblent très spéculatifs pour ce type de qubits.

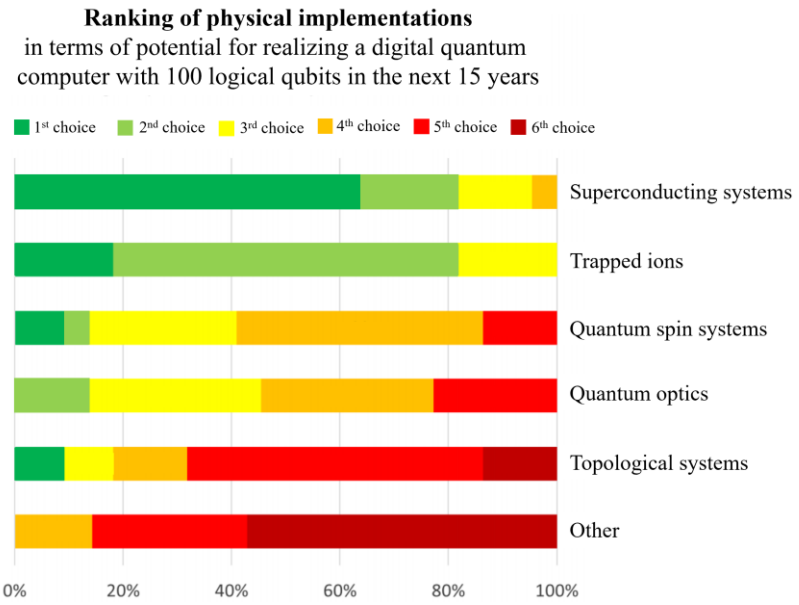


Figure 7: Classement d'opinions sur les différentes plateformes physiques dans le but précis de réaliser un ordinateur quantique (Source: Global Risk Institute and evolutionQ Inc.)

Pour terminer notre tour d'horizon, nous illustrons, sur la figure 8, les liens capitalistiques entre sociétés de capital-risque et startups. Nous y mettons en exergue les cas de Quantonation, fonds d'investissement français créée en 2018 spécialisé sur les startups de *Deep Physics* - en particulier dans le domaine des technologies quantiques - et D-Wave, fondée en 1999, qui s'est revendiquée comme la première entreprise d'informatique quantique au monde.

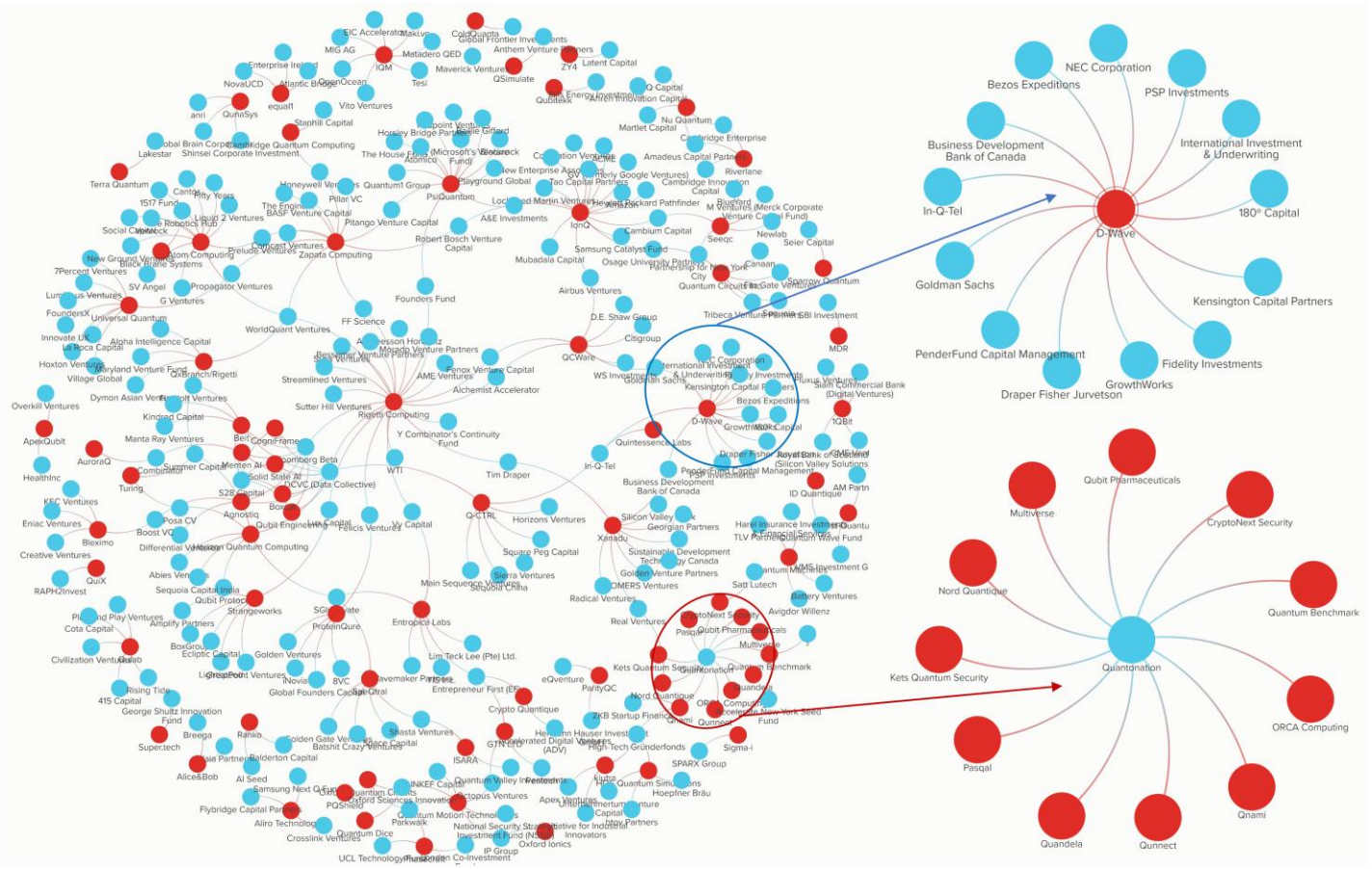


Figure 8: Cartographie des investissements de sociétés de capital-risque (VC) dans des startups du quantique (graphe réalisé à partir des données de www.quantumcomputingreport.com)

3. Conclusion

Les technologies quantiques devraient avoir des répercussions majeures sur la société et l'économie. La puissance unique des futurs ordinateurs quantiques et de l'internet quantique[229] pourrait apporter des solutions aux grands défis sociétaux tels que l'énergie, la santé et la sécurité. Nous ne sommes pas seulement dans le futur ou le conditionnel. Dès aujourd'hui, des instruments de mesures utilisant ces mêmes technologies offrent des précisions inégalées par les instruments classiques (voir par exemple les gravimètres ou les horloges vendus par la startup française Muquans).

Une course au quantique s'est engagée dans le monde entier. Les gouvernements occidentaux et asiatiques déploient des plans stratégiques associés à des enveloppes de financement conséquentes. Les institutions de recherche bénéficient généralement en premier lieu de ces investissements, tout comme ensuite les startups qui peuvent aussi compter sur un apport financier croissant de la part d'investisseurs privés (voir la répartition géographique et liste large présentées en figure 9 et figure 10).

A ce titre 2020 devrait être une année record pour l'investissement privé. La crise sanitaire mondiale ne semble pas avoir ralenti le rythme des investissements privés ou publics à l'instar de la décision allemande de tripler son budget dans le cadre de son plan post-COVID.

Certains acteurs majeurs des TIC complètent ensuite le paysage des investissements avec des stratégies de développement qui mixent R&D et commercialisation comme IBM ou Google. En parallèle ces acteurs collaborent avec des laboratoires publics parfois dans des régions différentes. Microsoft est proche de l'université de Delft aux Pays-Bas avec laquelle il travaille sur les qubits topologiques. Des équipes « quantiques » d'IBM sont proches géographiquement et probablement financièrement de l'Ecole Polytechnique de Zurich (ETH). En Chine, Alibaba travaille main dans la main avec l'Académie Chinoise des Sciences (CAS) tout en ayant d'autres laboratoires de recherche par ailleurs.

Les écosystèmes se construisent. Ils sont de plus en plus dynamiques. Les divisions public/privé, recherche/commercial deviennent floues, voire superposées... Beaucoup de startups sont issus de spin-off de laboratoire de physique et ce cas se rencontre même en Chine (Quantum CTek, Origin Quantum Computing).

Cette disparition des clivages traditionnels est une caractéristique frappante de l'écosystème quantique mondial. Ceci pourrait avoir un impact très positif sur la rapidité de la recherche et l'industrialisation du quantique. Mais cela pourrait aussi exacerber le risque de disparition (pour ne pas dire téléportation) des pépites individuelles (chercheurs) ou entrepreneuriales (startups) par appel de l'argent. Face à l'Amérique du Nord et la Chine, l'industrialisation des recherches issues de l'excellence scientifique de l'Europe (Allemagne, Royaume-Unis, France, Autriche, Pays-Bas…) voire les recherches locales elles-mêmes, pourraient pâtir de la complexité et de la lenteur des processus de transfert de technologie public/privé et du peu d'appétence aux risques long terme de certains financeurs privés locaux.

Nous avons relevé une autre caractéristique empirique qui pourrait être une tendance de fond des 5 à 10 prochaines années. Depuis quelques mois se développent des plateformes/réseaux qui centralisent l'offre diversifiée des ordinateurs quantiques existants : IBM Q Network, Microsoft Azur Quantum, Amazon AWS Braket.

Ainsi même si IBM propose un accès à ses ordinateurs quantiques développés sur la technologie des qubits supraconducteurs, un utilisateur/client du réseau Q Network peut également exécuter désormais son logiciel quantique sur les ions piégés du partenaire AQT en utilisant le même langage de programmation (IBM Qiskit). De la même façon, Pasqal, startup française qui développe un processeur quantique à base d'atome froid, collabore avec Google pour donner accès à sa technologie par l'intermédiaire de Cirq, le framework open-source de Google utilisé par ailleurs pour les ordinateurs quantiques (qubits supraconducteurs) de la firme de Mountain View.

[229] Ultime objectif du secteur des communications quantiques à (très) long terme.

Les gros acteurs sont donc conscients qu'il faut diversifier l'offre en attendant qu'une technologie de qubits physiques leader se dessine, ce qui effectivement pourrait prendre encore plusieurs années.

Dans le cas d'Amazon, dont l'ambition n'est pas de créer un ordinateur quantique, on pourrait même parler d'ubérisation d'un marché qui est pourtant à peine émergeant. Les petits acteurs mettent à disposition leur hardware chez AWS comme un chauffeur de VTC met à disposition son véhicule sur une plateforme. Les petits acteurs pourront-ils profiter de ce modus vivendi sur le moyen/ long terme ?

Il est fort à parier qu'au-delà des progrès technologiques à venir, le paysage du quantique va continuer à évoluer dans le futur proche mais qu'il dépendra fortement des actions entreprises aujourd'hui même par les différents acteurs privés et publics.

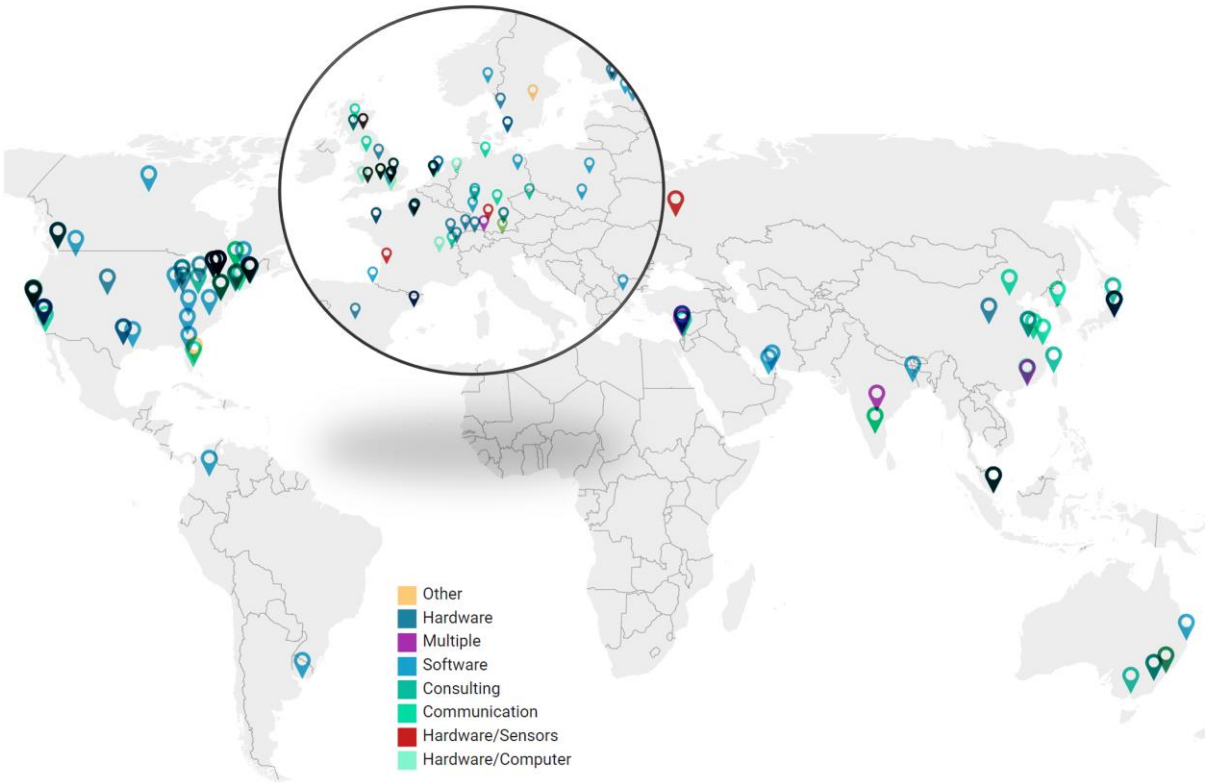


Figure 9: Répartition géographique 222 startups (Source: Pitchbook, Crunchbase, Quantum Computing Report, sites web sociétés)

Startup / Scaleup	Pays HQ	Secteur	Créé	Description (Sources : Sites web entreprises, et recherches diverses)
1QBit	Canada	Software	2012	1QBit est une société de logiciels et de conseils multi-sectorielle qui travaille sur des solutions aux problèmes difficiles. Ils ont développé des briques algorithmiques quantiques ou hybrides 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 domaines, via leur activité de conseil. Une grande partie de leur travail consiste en l'utilisation du matériel de recuit quantique (D-Wave) mais ils sont aussi partenaires du réseau IBM.
A*Quantum	Japan	Software	2018	A*Quantum est spécialisé dans le développement de solutions logicielles quantiques pour les ordinateurs à recuit quantique et ceux qui utilisent des portes quantiques universelles (circuit). Leur objectif est de créer des briques logicielles de haut niveau destinées à des utilisateurs.
AegiQ	UK	Hardware	2020	AegiQ est un spin-off de l'Université de Sheffield créée en 2019. La société se concentre sur les applications de photonique quantique à haute performance, sa technologie de base étant constituée de sources de photons uniques déterministes et indiscernables à base de semi-conducteurs.
Agnostiq	Canada	Software	2018	La mission d'Agnostiq est de développer des logiciels de sécurité robustes adaptés aux ordinateurs quantiques actuels (de type NISQ). Leurs solutions permettent aux utilisateurs de sécuriser leurs données et leurs algorithmes lorsqu'ils seront en traitement sur le Cloud quantique. Ainsi, même les utilisateurs les plus sensibles à la sécurisation de leurs données pourront profiter des avantages des ordinateurs quantiques sans compromettre la confidentialité (Blind Quantum Computing).

Aiqtech	Canada	Software	2018	AIQ utilise l'intelligence artificielle, l'analyse des données et la vision par ordinateur pour s'attaquer à certains des problèmes les plus complexes des entreprises.
Alice&Bob	France	Hardware/ Computer	2020	Spin-Off de l'ENS Lyon, Alice & Bob a pour objectif de construire un ordinateur quantique universel et sans erreur pour aider les industries et les chercheurs à résoudre les problèmes les plus difficiles. Jusqu'à présent, les erreurs étaient le principal obstacle à l'utilisation des ordinateurs quantiques. Leur bit quantique auto-corrigé permet un calcul quantique tolérant aux erreurs et peut exécuter n'importe quel algorithme quantique. Ils visent à augmenter considérablement leur puissance de calcul pour relever les défis les plus difficiles.
Aliro Quantum Technologies	US	Software	2019	Aliro Quantum Technologies 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.
Alpine Quantum Technologies, GmbH	Austria	Hardware/ Computer	2017	Alpine Quantum Technologies (AQT) est une spin-off récente formée par trois physiciens de l'Université d'Innsbruck et de l'Institute of Quantum Optics and Quantum Information de l'Académie autrichienne des sciences. L'objectif de l'entreprise est de construire un ordinateur quantique commercial en utilisant la technologie des ions piégés.
Ankh.1	US	Software	2018	Ankh lance Anubis-Cloud un service de machine virtuelle Quantique pour les data scientists avec l'intégration de bloc-notes Jupyter et Tensorflow + Keras.
Anyon Systems Inc.	Canada	Software	2014	Anyon Systems Inc. est une start-up technologique canadienne dont l'ambition est de fournir des toolkits « Quantum Electronic Design Automation" pour la conception et l'optimisation de l'électronique nano/quantique. Anyon fournit un simulateur de périphérique Quantum (QDS) pour concevoir et optimiser de nouveaux appareils électroniques quantiques.
ApexQubit	Netherlands	Software	2018	Apex Qubit est une société de logiciels quantiques développant une plateforme de 2e génération pour l'ingénierie de médicaments alimentée par l'informatique quantique qui permettra aux entreprises pharmaceutiques d'automatiser le processus de découverte de médicaments.
AppliedQubit	UK	Software	2019	Applied Qubit est un fournisseur de logiciels indépendant spécialisé dans l'application des sciences de l'information quantique pour les entreprises et l'industrie. Ils construisent, testent, déploient, supportent et markettent des logiciels dans le domaine des ordinateurs quantiques dans le but d'exploiter le potentiel du calcul quantique et produire des résultats à court terme pour les entreprises. Leurs deux axes de développement comprennent les algorithmes hybrides classiques/quantiques et l'apprentissage machine quantique (QML). Les secteurs de prédilections sont la Finance et la Chimie.
Aqintel	US	Software	2019	Peu d'informations. Le site redirige sur la page d'un développeur Microsoft
ArQit	UK	Communication	2016	ArQit est une startup qui se veut pionnière dans le domaine de la cybersécurité. La société souhaite construire le premier réseau mondial de distribution quantique de clés (QKD), qui fournira des services de cryptographie à sécurité quantique à partir d'une constellation de petits satellites en orbite basse à partir de 2022.
Artiste-qb.net	Canada	Software	2018	Artiste-qb.net a un modèle d'activité voisin de celui de 1Qbit. Ils développent des logiciels quantiques qui offrent aux clients des solutions aux défis posés en R&D ou aux problèmes business quantitatifs. Les dirigeants de cette société ont passé de nombreuses années à développer des algorithmes quantiques et ont déjà une grande bibliothèque de routines disponibles dont certaines méthodes sont d'ailleurs brevetées. Ils ont récemment lancé une plateforme appelée Bayesforge qui associe calcul quantique et IA. Cette librairie est fournie en open source pour les data scientists qui ont besoin d'outils analytiques avancés, ainsi que pour l'informatique quantique et les professionnels qui travaillent en informatique quantique. Artiste-qb.net vise le marché mondial avec un accent particulier sur la Chine où ils ont une société affiliée à Shenzhen.
Atom Computing	US	Hardware/ Computer	2018	Atom Computing se concentre sur la construction d'ordinateurs quantiques universels à l'échelle. En utilisant des techniques issues de la métrologie (mesures de précision), en l'occurrence celles des atomes neutres optiquement piégés, Atom Computing pense être capable de proposer une plateforme de calcul ayant un grand nombre de qubits. Ceci permettrait de mettre en œuvre les algorithmes de correction d'erreurs quantiques qui nécessitent un grand nombre de qubits physiques.
Aurea Technology	France	Hardware	2010	Fondée en 2010 Aurea développe, fabrique et commercialise une nouvelle génération d'instruments de mesures optiques de hautes performances, compactes, rapides et faciles d'utilisations basés sur des technologies de comptage de photons capable de détecter de très bas niveaux de lumière. Ces appareils sont notamment utilisés dans le domaine de la cryptographie quantique.
Aurora Quantum Technologies	Canada	Hardware	2017	AuroraQ (anciennement Qspice Labs) s'efforce de rendre les ordinateurs quantiques exploitables avec une technologie quantique hybride. Ils se spécialisent dans la création de systèmes de communication avec des qubits supraconducteurs.
Automatski	US	Software	2014	Automatski est une société holding de R&D ayant des bureaux à Bangalore et Los Angeles. Ils effectuent des recherches dans plusieurs domaines des logiciels quantiques ou inspirés du quantique pour simuler diverses configurations de calcul quantique. Cela inclut un simulateur quantique à base de circuits (qubits et porte logiques quantiques), un simulateur d'ordinateur quantique adiabatique, et un simulateur à recuit quantique. Ils espèrent que leur technologie leur permettra de simuler des configurations avec de très grands nombres de qubits.

Avanetix	Germany	Software	2019	Avanetix propose une approche logicielle verticalisée et hybride (ordinateur quantique et classique) dans le domaine du QML (Quantitative Machine Learning) avec l'objectif d'accroître la productivité et l'efficacité des chaînes d'approvisionnements par exemple dans l'industrie automobile.
BardeenQ Labs	US	Hardware	2019	BardeenQ Labs cherche à exploiter pleinement le potentiel des technologies quantiques. Leur premier produit, BardeenQ Waves, sera un système de vision utilisant le quantique et une puce IA quantique pour garantir la sécurité des voitures autonomes en utilisant une technologie basée sur des dispositifs quantiques fonctionnant à température ambiante.
Beit	Poland	Software	2016	L'objectif principal de Beit, spécialisée dans le QML et financée par l'Union Européenne est de concevoir et mettre en œuvre un algorithme pour résoudre des problèmes pertinents ayant une complexité de classe NP-complets en utilisant les ordinateurs quantiques. Cela comprend de nombreux problèmes du quotidien rencontrés dans la logistique, la fabrication et le stockage à l'échelle.
Bikash's Quantum	India	Software	2019	Quantum Bikash crée un logiciel quantique, développe des jeux quantiques, et publie des articles de recherche dans le domaine du calcul quantique.
Black Brane Systems	Canada	Software	2016	Black Brane est une startup spécialisée en apprentissage machine quantique et calcul quantique. Ils proposent une machine virtuelle de 128 qubits (VQM), utilisable dans le Cloud, appelée BLACKSTONE qui peut simuler des programmes quantiques écrits dans le langage Q# de Microsoft. Blackstone bénéficierait d'un avantage majeur dans le domaine des structures de données, ce qui permettrait de mettre en œuvre des calculs quantiques sans équivalent sur les ordinateurs classiques.
Bleximo	US	Hardware/ Computer	2017	Bleximo construit des accélérateurs supraconducteurs quantiques à base de qubits qu'ils appellent « qASIC » qui fonctionnent conjointement avec de puissants ordinateurs conventionnels pour résoudre des problèmes potentiellement inextricables sur des ordinateurs classiques. L'objectif initial de l'entreprise sera de fournir ces accélérateurs pour simuler structure, propriétés, réactions chimiques de molécules. En modélisant le comportement de certaines molécules, Bleximo souhaite aider à optimiser les processus de découverte et conception de médicaments dans le secteur pharmaceutique.
BlueFors	Finland	Hardware	2008	BlueFors est spécialisé dans les systèmes de réfrigération à dilution sans cryogène, avec un focus particulier sur l'informatique quantique. Leur objectif est de fournir les réfrigérateurs les plus fiables et les plus faciles à utiliser du marché. Ils offrent une large gamme de systèmes standards avec des options comprenant le câblage et les aimants supraconducteurs. En outre, leurs systèmes peuvent être personnalisés pour répondre aux besoins de chaque client.
Boxcat	Canada	Software	2017	Boxcat tire parti de la puissance de calcul quantique pour rendre le traitement des images et des vidéos plus rapides, moins cher et plus efficace que les méthodes actuelles. Ils ciblent les industries des médias et de l'imagerie médicale en tant que clients potentiels pour leur solution.
Bra-ket science	US	Hardware	2017	Bra-ket Science développe une nouvelle approche de stockage de qubits à température ambiante. Leurs premières publications et dépôts de brevets sont actuellement en cours.
BraneCell	US	Hardware/ Computer	2015	BraneCell construit un nouveau microprocesseur quantique qui peut fonctionner à température ambiante. Ses qubits utilisent un processus permettant de faire cohabiter un état condensé et non condensé de molécules, sans conduction électrique ni silicium, avec un procédé qui s'appuierait sur de la lumière infrarouge. De par leur nature, ces appareils sont faciles à utiliser pour l'intelligence artificielle et permettent l'informatique quantique portable grâce à leur température de fonctionnement modérée. L'approche de BraneCell est unique car ils visent à ce que leur technologie soit utilisée par des clients individuels en interne plutôt que d'y accéder par le cloud.
C12 Quantum Electronics	France	Hardware/ Computer	2019	Précédemment appelée CNT Nanotech, C12 est une société lancée en 2020 par des chercheurs de l'ENS Paris. Leur projet consiste à utiliser des nanotubes de carbone pour piéger les électrons utilisés dans des qubits CMOS. Cela permettrait de mieux les isoler de leur environnement ce qui améliorerait le temps de cohérence d'un facteur 100 (=>1 sec). Ils se contrôleraient par couplage spin-photon. Les défis et verrous technologiques sont nombreux mais la voie mérite d'être explorée.
Cailabs	France	Hardware	2013	Cailabs conçoit, fabrique et vend des solutions photoniques pour exploiter pleinement le potentiel industriel de la mise en forme de la lumière. Cela comprend une gamme de composants optiques uniques fondés sur son savoir-faire et ses innovations technologiques brevetées, en particulier la Conversion Multi-Plan de la Lumière (MPLC pour Multi-Plane Light Conversion). Les domaines d'application sont, entre autres, les télécommunications terrestres et spatiales, les lasers industriels.
Cambridge Quantum Computing Limited (CQC)	UK	Software	2015	CQC met l'accent sur le développement d'un système d'exploitation quantique, ainsi que sur des algorithmes et logiciels associés. CQC propose ainsi un OS propriétaire pour ordinateurs quantiques (t|Ket>) et une suite d'algorithmes quantiques pour des applications et des programmes à divers stades de développement. CQC travaille dans le domaine du calcul quantique pour la chimie et a récemment annoncé avoir mis en œuvre avec succès des algorithmes quantiques "état de l'art" sur un des ordinateurs quantiques d'IBM pour calculer les états excités de molécules.
Cambridge Space Technologies	UK	Communication	2019	L'objectif de Cambridge Space Technologies est de fournir une cryptographie quantique à l'échelle mondiale. Elle vise à fournir un accès simple et direct aux gouvernements ou entreprises commerciales à des clés quantiques distribuées (QKD) par des satellites en orbite basse. Leur premier projet consiste à placer un CubeSat en orbite terrestre basse (LEO) en utilisant les infrastructures et les systèmes de lancement actuellement disponibles pour faciliter une nouvelle norme de communication sécurisée.

Chainstarter	UK	Consulting	2017	Chainstarter offre des conseils technologiques et est spécialisée dans les Blockchains, l'informatique quantique, l'IA, les nanomatériaux, la fintech, les biotechnologies, les plateformes, les marchés et les modèles commerciaux de rupture, ce qui permet aux startups d'optimiser leurs business modèles et de préparer leurs projets d'investissement. La société propose également des services de conseil en matière de Family Office et de patrimoine privé.
Chicago Quantum	US	Consulting	2018	Chicago Quantum, est une division de l'entreprise américaine Advanced Computing, Inc. qui se concentre sur l'aide aux entreprises souhaitant explorer les possibilités des technologies quantiques en particulier dans le domaine de la sécurité des informations et communications.
Chromacity	UK	Hardware/ Sensors	2013	Fournisseur de lasers "tunables" destinés à offrir des systèmes qui transformeront les applications industrielles et de recherche fondamentale. L'offre de la société comprend des lasers à impulsions ultra-courtes qui peuvent être accordés à différentes applications par le biais d'une interface web comme les ordinateurs ou les appareils intelligents, permettant aux entreprises de proposer des technologies laser personnalisées pour des applications spécifiques aux utilisateurs finaux.
ClassiQ	Israel	Software	2020	Classiq désire combler le fossé qui existe entre la logique complexe de la physique quantique et son application dans le monde réel.
CogniFrame	Canada	Software	2016	CogniFrame est une société qui travaille sur l'apprentissage machine hybride (ie Quantique / Classique). Elle fournit aux institutions financières des solutions utilisant de l'apprentissage machine classique, de l'optimisation quantique et de l'échantillonnage pour les aider à améliorer les rendements de leurs actifs. Grâce à son moteur cognitif préconstruit, CogniFrame améliore les décisions de crédit pour une variété de produits de type prêt, lignes de crédit, hypothèques. Les algorithmes de CogniFrame s'appuient sur le levier apporté par la puissance du calcul quantique pour trouver les solutions optimales dans la problématique de la gestion de l'actif-passif.
ColdQuanta	US	Hardware	2007	ColdQuanta est un spin-off de l'Université du Colorado. Ils conçoivent et développent instruments, composants et systèmes pour les applications scientifiques et industrielles quantiques tels que l'expérimentation sur les atomes froids, la simulation quantique, le traitement quantique de l'information, les horloges atomiques et la détection d'inertie. Leur objectif est d'évoluer à terme vers la chaîne de production des ordinateurs quantiques et son marché, en plus de leur production de composants actuelle. Ils collaborent avec IonQ sur les qubits à base d'ions piégés.
CryoConcept	France	Hardware	2000	Depuis 2000, Cryo Concept se consacre à l'innovation dans le domaine des réfrigérateurs à ultra basse température. La société conçoit, fabrique, teste et installe des systèmes de réfrigération à dilution haute performance capables d'atteindre des températures inférieures à 10mK. En tirant parti des refroidisseurs à cycle fermé en dessous de 4K, Cryoconcept a développé une nouvelle conception de réfrigérateurs à dilution sans cryogénie.
Crypta Labs	UK	Communication	2014	Crypta Labs a développé des générateurs quantiques de nombres aléatoires (QRNG) pour produire des nombres vraiment aléatoires à utiliser dans le cryptage. Leur technologie, en instance de brevet, utilise les propriétés quantiques de la lumière provenant de la lentille d'un appareil mobile et des capteurs de lumière qui détectent les faisceaux de photons et comptent les photons pour générer un nombre aléatoire.
Crypto Quantique	UK	Communication	2016	Crypto Quantique a développé une puce qui génère des clés cryptographiques complètes aléatoires par effet tunnel quantique. Ils ont une offre clé en main qui intègre une API, leur protocole de cryptographiques et un système de gestion de clés sécurisé.
Crypto4A	Canada	Communication	2012	La plateforme Crypto4A simplifie les défis de la gestion de l'infrastructure de sécurité grâce à sa facilité de déploiement, d'utilisation et de gestion à distance. Au sein de la plateforme, leur HSM de nouvelle génération, QASM™, offre une adaptabilité cryptographique qui encapsule les informations sensibles dans un système cryptographique préparant à l'informatique quantique.
CryptoNext Security	France	Communication	2018	Spin-off de l'INRIA, et de l'Université de la Sorbonne, CryptoNext développe des algorithmes quantiques résistants pour la cryptographie post-quantique. Leur bibliothèque Quantum-Safe, est une bibliothèque cryptographique qui fournit des fonctionnalités clés pour le chiffrement publique la signature quantique de sécurité et l'échange de clés quantiques. Cette bibliothèque contient une sélection prometteuse d'algorithmes de sécurité quantique sélectionnés à l'IETF et lors de la deuxième étape du processus de normalisation post-quantique NIST.
D Slit Technologies	Japan	Software	2018	D Slit Technologies est une entreprise qui permet de résoudre des problèmes business en utilisant les principes de la mécanique quantique. Leurs services comprennent le développement d'algorithmes quantiques. Ils fournissent aussi une large gamme de conseils en informatique quantique, étudient les dernières recherches sur le quantique et livrent des PoC en guise de démonstration.
Delft Circuits	Netherlands	Hardware	2016	Delft Circuits fournit des composants matériels qui peuvent rentrer dans la composition d'ordinateurs quantiques à supraconducteurs. La société propose notamment des circuits de contrôle d'entrées/sorties, des circuits de contrôle de systèmes cryogéniques comme dans leur gamme de produits Cri/oFlex® et des guides supraconducteurs de micro-ondes.
Dividiti	UK	Software	2014	Dividiti développe des algorithmes quantiques notamment pour le machine learning ainsi que des méthodes hybrides. Leurs solutions sont open source. Grâce à des techniques de pointe d'analyse et d'optimisation des performances, ils optimisent simultanément le temps d'exécution, la consommation d'énergie, la taille, la fiabilité, la programmabilité et d'autres paramètres importants des systèmes informatiques.

Driven Quantum Technologies	US	Software	2019	Driven Quantum Technologies participe au développement de la propriété intellectuelle en vue de l'octroi éventuel de licences de technologie à des entreprises qui conçoivent des produits liés à l'informatique quantique pour la détection/métrologie quantique, la biologie quantique, l'armée/le renseignement, la médecine/assistance et d'autres applications. La société est toujours en mode furtif.
D-Wave Systems Inc.	Canada	Hardware/ Computer	1999	D-Wave a été l'une des premières sociétés à développer et commercialiser (dès 2011) un ordinateur quantique d'un type particulier utilisant le principe du recuit quantique adiabatique (annealing). Depuis différents modèles ont été proposé à la vente, la version actuelle a 2000 qubits et la prochaine devrait en avoir 5000. D-Wave propose cette machine à la vente aux clients qui souhaitent installer une machine sur place. D-Wave propose également des services de Cloud Computing pour les clients qui souhaitent accéder à cette capacité à distance. Enfin en plus du matériel, D-Wave commercialise également une suite complète d'outils de développement pour aider ses clients à accélérer le temps de développement des applications destinées à être utilisées sur leurs machines.
EeroQ	US	Hardware/ Computer	2017	EeroQ est une start-up de hardware quantique qui travaille sur le développement d'une puce quantique unique qui aurait des avantages potentiels par rapport aux autres technologies de qubits. Leur technologie repose sur une électronique utilisant des atomes d'hélium...mais ce n'est pas très clair...
Elyah	UAE	Software	2018	Elyah est une société de logiciels quantiques qui construit et améliore les algorithmes quantiques existants pour les rendre plus rapides et plus faciles à mettre en œuvre pour les futures applications de l'informatiques quantique.
Engine Room.io LABS	Australia	Other	2011	EngineRoom.io propose des services de recherche et d'ingénierie destinés à identifier et à créer des technologies innovantes. Les domaines de recherche de l'entreprise comprennent l'IA et le ML pour les sports, l'astrophysique, la marine et l'armée, ce qui permet aux clients d'acquérir des connaissances pour créer de nouvelles technologies.
Entanglement Partners	Spain	Consulting	2016	Entanglement Partners est un cabinet de conseil qui fournit des services de conseil dans les domaines des événements et des communications, Go-to-Market, Infrastructure, Applications quantiques, Conseil stratégique et Venture. Ils sont implantés en Espagne, Californie et Inde.
Entropica Labs	Singapore	Software	2018	Entropica Labs est une société de logiciels quantiques basée à Singapour. Elle se concentre sur l'emploi de l'informatique quantique dans le domaine des sciences du vivant et en particulier pour les applications en génomique, en pharmaceutique avec à la clé des développements plus rapides de thérapies, mais aussi en Agritech.
equal1.labs	US	Hardware/ Computer	2017	Equal1.labs développe depuis 2017, en collaboration avec l'University College de Dublin, une technologie d'ordinateur quantique basée sur le silicium (à spin d'électrons) fonctionnant à 4K.
Everettian Technologies	Canada	Software	2017	L'objectif d'Everettian Technologies est de repousser les frontières de l'apprentissage machine et de l'informatique quantique afin d'offrir une valeur commerciale significative à leurs clients.
evolutionQ	Canada	Communication	2015	EvolutionQ offre une gamme de produits et services exclusifs, qui comprend l'évaluation des risques quantiques, la conception de roadmaps et leurs mises en œuvre, du matériel et des logiciels « quantum-safe ». S'y ajoutent des services de formation pour permettre aux organisations d'éviter les menaces sur leur infrastructure informatique.
EYL	South Korea	Communication	2015	EYL fournit une minuscule puce quantique de 5 millimètres générant des nombres aléatoires basés sur une méthode à base d'isotopes radioactifs. La société développe également un crypteur à puce ultraléger pour tous les dispositifs de l'IdO ainsi qu'un générateur aléatoire quantique de type film mince pour les cartes d'identité et de crédit.
Future Quantum Intelligence Investment	Israel	Multiple	2008	Future Quantum Intelligence Investment est impliqué dans la recherche et la commercialisation des technologies quantiques. Il a mis au point un capteur intelligent qui peut être utilisé pour améliorer la capacité sensorielle des robots. Elle fournit également des produits et des services de sécurité des réseaux multiprotocoles basés sur les technologies quantiques
GTN LTD	UK	Software	2017	GTN technologie innove en utilisant de l'apprentissage machine quantique (QML) pour transformer le process de recherche de nouveaux médicaments. Leur technologie brevetée, appelée Generative Tensorial Networks utilise des techniques de QML pour simuler, filtrer et rechercher des molécules, voire en révéler des entièrement cachées tout en réduisant de moitié les coûts de développement.
HaQien	India	Communication	2019	HaQien se concentre sur les problèmes fondamentaux de la cybersécurité et conçoit des algorithmes cryptographiques pour prévenir les cyber-attaques actuelles mais aussi les éventuelles cyber-attaques futures provenant d'ordinateurs quantiques.
H-Bar Consultants	Australia	Consulting	2016	Créé par des experts en physique quantique et technologie, H-Bar est le premier cabinet de conseil spécialisé dans la technologie quantique. Ils agissent comme intermédiaires et/ou conseillers pour les organisations qui cherchent à faire des investissements ou simplement se renseigner sur des questions liées à la technologie quantique. Ils peuvent conseiller les clients au niveau mondial sur les questions commerciales et techniques.
Horizon Quantum Computing	Singapore	Software	2018	Horizon Quantum Computing est une start-up à un stade précoce basée à Singapour, axée sur la construction d'outils de développement de logiciels pour conduire la prochaine révolution informatique.

HQS Quantum Simulations	Germany	Software	2018	HQS Quantum Simulations (anciennement Heisenberg Quantum Simulations) développe des algorithmes quantiques dans le domaine de la simulation moléculaire organique et inorganique de molécules simples. Ils ont également mis au point un outil de portage open-source entre ProjectQ et Cirq (Google), appelé CirqProjectQ.
HyperLight	US	Hardware	2018	Concepteur et producteur de circuits optiques intégrés destinés à limiter les pertes de signal. L'offre de la société comprend des modulateurs intégrés à l'échelle de la puce, des puces photoniques pour les centres de données, datacoms et applications d'informatique quantique.
ID Quantique	Switzerland	Communication	2001	ID Quantique, basée en Suisse, fournit un cryptage de réseau quantique de sécurité, génération de clé quantique sécurisée et des solutions de distribution quantique de clés et de services à l'industrie financière, les entreprises et les organisations gouvernementales à l'échelle mondiale. Le coréen SK Telecom en a pris récemment le contrôle.
InfiniQuant	Germany	Communication	2018	InfiniQuant est hébergé à l'Institut Max Planck pour la science de la lumière. Ils sont dans une phase de démarrage précoce et se concentrent sur le développement de produits « Continuous Variable Quantum Key Distribution » (CV-QKD) utilisables pour la sécurisation des télécommunications sur des canaux quantiques fibre / satellite.
Innovatus Q	Singapore	Software	2020	Innovatus Q (Singapour) est un spin-off du Centre for Quantum Technologies de Singapour. Ils travaillent des algorithmes quantiques hybrides pour processeurs classiques et quantiques à base d'ions piégés et de supraconducteurs.
Intelline	Canada	Hardware	2018	Intelline construit des systèmes de cryogénie de masse sur mesure pour permettre une mise en œuvre généralisée des technologies de cryo-refroidissement.
IonQ	US	Hardware/ Computer	2017	IonQ est un spin-off de l'Université du Maryland spécialisée dans la conception d'ordinateurs quantiques universels à base d'ions piégés.
IQM Finland	Finland	Hardware	2018	IQM construit du hardware "scalable" pour ordinateur quantique universel basé sur des qubits supraconducteurs. C'est un spin-off du groupe de recherche informatique quantique et périphériques de l'Université Aalto et fait usage d'une technologie initialement brevetée dans ce groupe.
ISARA	Canada	Communication	2015	ISARA fournit des produits logiciels résistants à l'informatique quantique et aide également ses clients à planifier et préparer la prochaine ère de sécurité quantique. Un produit clé est la « ISARA Radiate Security Solution Suite » qui offre un chiffrement à clé publique et des algorithmes de signature numérique qui ne peut être brisés par un ordinateur quantique en utilisant l'algorithme de Shor ou par tout autre connu algorithme classique ou quantique.
Jij	Japan	Software	2018	Jij mène des activités de R & D et de développement de logiciels visant à l'application pratique des machines à recuit (annealer) par une équipe principalement composée d'experts qui mènent des recherches théoriques sur le recuit quantique et des recherches appliquées sur des problèmes du monde réel. Ils développent un logiciel Open Sources pour le modèle d'Ising (QUBO) appelé OpenJij.
JoS QUANTUM	Germany	Software	2018	JOS Quantum fournira des algos/logiciels pour les ordinateurs quantiques afin d'accélérer et améliorer l'industrie des services financiers. Ils prévoient de fournir des logiciels, des services d'intégration de système et une API permettant d'accéder à distance aux ordinateurs quantiques. L'accent est mis en particulier sur les problèmes d'optimisation et pour des cas d'usage tels que la gestion des risques, la détection des fraudes, le commerce, et plus encore. En plus de développer leurs propres produits, ils fourniront également de la Research-as-a-Service (RaaS) et des services de conseil pour le transfert de connaissances et l'intégration des logiciels.
Jumpedal	US	Other	2010	Jumpedal propose une technologie de compression de données pour le stockage et le transfert massif de données dans les fermes de serveurs afin d'améliorer les bandes passantes des réseaux. Pour cela Jumpedal propose un Chip dédié InfinityCoil et un process nommé BinaryAcceleration.
Ketita Labs	Estonia	Software	2018	Ketita Labs est un spin-off d'une université estonienne. Ils développent des logiciels en chimie analytique pour les ordinateurs quantiques de type NISQ.
KETS Quantum Security	UK	Communication	2016	KETS a développé une gamme de technologies pour les communications quantiques sécurisées. Cela comprend la distribution quantique de clé (QKD) et génération de nombres aléatoires quantique (QRNG). Leurs dispositifs sont basés sur les technologies photoniques intégrées conduisant à la miniaturisation, la fabrication rentable et fonctionnalités complexes. KETS fournit des services de conseil et de développements conjoints pour aider les PME et les sociétés mondiales dans le développement de solutions de sécurisation quantique sur mesure.
Kiutra	Germany	Hardware	2018	Kiutra développe des solutions entièrement automatiques qui génèrent des températures cryogéniques de l'ordre du Kelvin et sous-Kelvin pour des ordinateurs quantiques en utilisant une technique de réfrigération magnétique. Contrairement à d'autres technologies, leur approche ne nécessite pas l'utilisation de l'isotope hélium-3, qui est rare et cher. Leur solution serait facile d'utilisation, d'entretien et scalable. La société, fondée en juillet 2018, est un spin-off de l'Université technique de Munich (TUM).

Kuano	UK	Software	2020	Kuano fournit services et conseils allant d'une compréhension stratégique de l'impact des technologies quantiques à des projets de conception d'inhibiteurs biochimiques entièrement clés en main. L'approche unique de l'entreprise pour la conception de nouveaux inhibiteurs consiste à combiner des approches de simulation quantique et d'apprentissage machine pour créer des inhibiteurs très efficaces basés sur les mécanismes de l'enzyme cible.
Labber Quantum	US	Software	2016	Labber Quantum développe des solutions de contrôle pour le calcul quantique expérimental. Leur produit fournit une interface entre le dispositif quantique et l'électronique classique nécessaire pour le contrôle et la manipulation des Qubits. Leurs logiciels gèrent les instruments de contrôle, de génération de signaux, de calibration des qubits et de suppression d'erreurs dynamique. Cela garantit que les utilisateurs tirent le meilleur parti de leurs qubits et leur permet de mettre en œuvre avec précision les algorithmes quantiques désirés. Le logiciel, flexible, est conçu pour fonctionner avec tout type de qubit et tout fournisseur d'ordinateur. Labber Quantum a été acquise par Keysight Technologies en Mars 2020.
LakeDiamond	Switzerland	Hardware	2015	LakeDiamond est un leader mondial dans la production et la transformation de diamants ultra-purs cultivés en laboratoire pour des applications industrielles de haute technologie. La société vend des plaques de diamant et explore de nouvelles applications industrielles de haute technologie passionnantes au-delà du marché de la bijouterie haut de gamme, telles que les pièces micro-mécaniques en diamant, les rayons laser de puissance en diamant, les transistors de haute puissance en diamant et les magnétomètres de haute précision en diamant (centres NV).
LightOn	France	Hardware	2015	LightOn développe une technologie basée sur la lumière susceptible de diminuer le temps aujourd'hui nécessaire aux calculs d'intelligence artificielle à grande échelle. LightOn est un spin-off de certaines des meilleures universités de Paris. Leur premier produit est un coprocesseur matériel appelé Optical Processing Unit - ou OPU. Il est conçu pour stimuler certaines des tâches les plus exigeantes en matière de calcul dans le ML.
Low Noise Factory	Sweden	Hardware	2005	Low Noise Factory conçoit et vend des amplificateurs à faible bruit pour les environnements cryogénisés ou à température ambiante.
Magiq	US	Communication	1999	Magiq a par le passé mis au point des produits de distribution quantique de clé. Ceux-ci ne sont plus activement commercialisés comme des produits standards. Magiq souhaiterait proposer des solutions personnalisées pour les clients, lesquelles se baseraient sur la technologie qu'ils ont développée jusqu'à présent.
Max Kelsen	Australia	Software	2015	Max Kelsen est une société de conseil en apprentissage automatique et en IA. Ils sont experts dans la recherche, le développement et la mise en œuvre de l'apprentissage automatique à l'échelle, de la recherche médicale au déploiement de modèles de pointe et d'applications basées sur l'IA pour les entreprises du Fortune 500. Ils déploient des systèmes d'apprentissage automatique spécialisés pour automatiser les flux de travail manuels, extraire de la valeur des données internes du client, et créer des moyens personnalisés pour lui permettre de s'engager auprès de ses propres clients.
MDR	Japan	Hardware/ Computer	2008	MDR développe du matériel, middleware et applications pour l'informatique quantique, en collaboration avec des entreprises nationales japonaises, des organisations et des universités. MDR fournit un kit de développement (SDK) basé sur Python appelé Blueqat pour les ordinateurs quantiques universels et MDR Superfast, un simulateur basé sur NVIDIA CUDA. MDR a récemment annoncé un accord avec D-Wave pour utiliser leurs ordinateurs quantiques afin de développer des applications informatiques quantiques pour des problèmes d'apprentissage et d'optimisation machine.
Menten	Canada	Software	2018	Menten est une start-up de biotechnologie qui développe une plateforme logicielle pour la conception de protéines en utilisant les nouvelles technologies d'apprentissage machine et d'informatique quantique. L'équipe a fait des progrès significatifs vers leur objectif en développant le premier algorithme entièrement "scalable" pour la conception de peptides et de protéines sur un ordinateur quantique. Ils ont ainsi créé le premier peptide au monde conçu sur un ordinateur quantique.
M-Labs	Hong Kong	Multiple	2007	Le principal projet de M-Labs est aujourd'hui ARTIQ (Advanced Real-Time Infrastructure for Quantum physics), un système de contrôle de pointe pour des expériences d'information quantique. Cette solution matérielle et logicielle a été initialement développée en partenariat avec le groupe *Ion Storage* (ions piégés) au NIST, et est maintenant utilisé et soutenu par un nombre croissant d'institutions de recherche dans le monde entier.
Molecular Quantum Solutions	Denmark	Software	2019	La société développe un logiciel et un outil situé dans le Cloud qui fournit des prévisions sur les propriétés des (bio)produits chimiques en se basant sur des algorithmes basés sur de l'apprentissage machine (ML) et sur la chimie quantique. Les logiciels de l'entreprise utilisent du ML sur des super-ordinateurs ou des ordinateurs quantiques, ainsi que des modèles de chimie quantique permettant de calculer les propriétés des matériaux et des produits chimiques de manière rapide et efficace. Ceci permet aux scientifiques et aux développeurs de réduire le nombre d'expériences en R&D et de sélectionner de nouveaux matériaux pour les piles, les solvants verts, les nouveaux médicaments et les plastiques biodégradables.

M-Squared Lasers	UK	Hardware	2003	Développeur de solutions photoniques et de la technologie quantique utilisées spécifiquement pour la recherche quantique, la biophotonique et les applications de détection chimique. La société propose des systèmes lasers et des instruments optiques photoniques pour des applications dans les domaines de la télédétection, de la bio-photonique, de la défense, de la microscopie, de la spectroscopie et de la métrologie.
Multiverse Computing	Spain	Software	2017	Multiverse Computing fournit des logiciels pour les entreprises du secteur financier qui veulent tirer avantage de l'informatique quantique. Leurs domaines d'expertise incluent les problèmes d'optimisation de portefeuille, l'analyse de risques, et la simulation du marché.
MuQuans	France	Hardware/ Sensors	2011	Fabricant d'une nouvelle génération d'instruments de mesure de très haute précision utilisant la technologie des atomes froids. Le portefeuille de produits de l'entreprise comprend le gravimètre quantique absolu (AQG), capable de mesurer la gravité avec une sensibilité et une précision extrêmes ; MuClock, qui offre des mesures de temps avec une stabilité et une précision sans précédent, et une large gamme de systèmes laser et de composants laser de qualité. Muquans a sussi une recherche dédiée au refroidissement et à la manipulation des atomes ou des ions, aux sciences de l'information quantique et à la spectroscopie haute résolution, permettant aux scientifiques, aux chercheurs et aux entreprises d'informatique quantique d'observer et de réaliser des mesures de haute précision.
Nano-Meta Technologies	US	Hardware	2010	Nano-Meta Technologies, Inc. développe et commercialise la propriété intellectuelle. Elle se concentre sur la plasmonique, la nanophotonique et les métamatériaux
NetraMark	Canada	Software	2015	NetraMark utilise l'apprentissage machine classique et quantique pour aider les entreprises pharmaceutiques à anticiper défaut ou échec des essais cliniques et également pour prédire de nouvelles cibles thérapeutiques pouvant conduire à des économies massives en temps et en argent pour les entreprises de ce secteur. NetraMark a fait partie du programme Quantum Machine Learning Creative Destruction Lab de Toronto et ils travaillent actuellement avec plusieurs sociétés pharmaceutiques pour appliquer leur technologie.
NextGenQ	France	Hardware	2019	NextGenQ travaille à construire un ordinateur quantique en utilisant la technologie des ions piégés.
Nordic Quantum Computing Group	Norway	Software	2004	Nordic Quantum Computing Group (NQCG) 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.
Nu Quantum	UK	Communication	2018	Nu Quantum est un spin-out du laboratoire Cavendish de l'Université de Cambridge. La société développe des technologies de sécurité quantique.
Nvision	Germany	Hardware/ Sensors	2015	NVision a développé une technologie quantique destinée à améliorer l'imagerie médicale. Cette technologie tire parti des nouvelles avancées de la physique quantique pour bouleverser l'espace de l'imagerie médicale et du diagnostic en permettant aux spectromètres à résonance magnétique standard (par exemple, IRM, RMN) d'évaluer le métabolisme humain, ce qui permet aux professionnels de la santé d'effectuer un diagnostic avancé du cancer et de suivre en temps réel la réponse à la thérapie.
ODE, L3C	US	Software	2018	La mission d'ODE est de changer le monde en résolvant les problèmes de chimie dont la complexité de résolution est en temps polynomial non déterministe avec des algorithmes quantiques multiplateforme physique (matériels numériques, analogiques classiques, hybrides). Ils ont développé un algorithme appelé Quantum Learned Electrons and Nuclei (QLEAN) qui, selon eux, peut fournir de meilleures simulations que les progiciels de chimie computationnelle actuellement disponibles qui mettent en œuvre l'approximation de Born-Oppenheimer (BO).
Orange Quantum Systems	Netherlands	Consulting	2020	Orange Quantum Systems fournit un service d'ingénierie pour les laboratoires qui font de la recherche en physique quantique et en informatique quantique. Leur équipe a fait ses preuves en matière de conception, d'ingénierie, de fourniture et de livraison de dispositifs expérimentaux complexes. Ce savoir-faire est également utilisé pour développer leur propre ligne de produits d'ordinateurs quantiques, qu'ils développent en collaboration avec leurs partenaires d'innovation.
ORCA Computing	UK	Hardware/ Computer	2019	ORCA Computing développe une plateforme de processeur quantique "scalable" en utilisant la technologie photonique. Ils ont une technologie de mémoire quantique propriétaire qui permet un stockage et une plus grande synchronisation des opérations quantiques. Cela permet une opération « repeat-until-success », plutôt que d'exiger un grand nombre de composants distincts qui fonctionnent en parallèle.
Origin Quantum Computing	China	Software	2017	Origine Quantum Computing a été créée par l'équipe doctorale du laboratoire d'information quantique de l'Académie Chinoise des Sciences. C'est une des premières startups en Chine dont l'activité principale est le développement et l'application des ordinateurs quantiques. Ils ont sorti un kit de développement logiciel quantique appelé Qpanda 2.0 sur GitHub qui peut être utilisé pour créer des circuits quantiques et faire des tests sur différents ordinateurs quantiques. Origine Quantum Computing a développé une puce 2 qubits basée sur la technologie "Quantum Dot" et une puce de 6 qubits basée sur la technologie supraconductrice. Ils travaillent également sur un ordinateur quantique complet ainsi que sur des plates-formes de services de cloud quantique proposant à la fois simulateurs quantiques et véritable ordinateur quantique.

Oxford HighQ	UK	Hardware/ Sensors	2017	Oxford HighQ est un spin-off des départements des matériaux et de chimie de l'université d'Oxford qui développe la prochaine génération de capteurs chimiques et de nanoparticules. Leur technologie utilise des microcavités optiques qui fournissent un moyen d'amplifier les signaux optiques.
Oxford Ionics	UK	Hardware/ Computer	2019	Dans le monde de l'informatique quantique, Oxford Ionics est un nouveau spin-off du département de physique de l'Université d'Oxford. La société travaille à créer un ordinateur quantique commercialement viable construit sur une base d'ions piégés.
Oxford Quantum Circuits	UK	Hardware/ Computer	2017	Oxford Circuits Quantum ambitionne de construire un ordinateur quantique basé sur une approche de circuit de qubits supraconducteurs. L'intention est de tirer parti des dernières technologies dans ce domaine et relever le défi clé pour les chercheurs: l'adaptation du système à un grand nombre de qubits..
ParityQC	Austria	Other	2020	ParityQC est un spin-off de l'Université d'Innsbruck. C'est une société d'architecture quantique qui développe des plans pour des ordinateurs quantiques. Ils ont une suite de logiciels connexes appelés ParityOS qui optimise les algorithmes quantiques, ainsi que les paramètres matériels. Leur crédo est que le co-développement de la conception du matériel et des algorithmes quantiques permet d'augmenter les performances d'un ordinateur quantique lorsqu'il s'agit de résoudre des problèmes d'optimisation par exemple. L'architecture est compatible avec toutes les plateformes matérielles actuelles (portes quantiques et recuit (annealing)).
Pasqal	France	Hardware/ Computer	2019	Pasqal construit un ordinateur quantique utilisant des réseaux d'atomes froids neutres. La technologie est basée sur le travail effectué par le groupe Optique Quantique & Atomes au sein du Laboratoire Charles Fabry de l'Institut d'Optique.
Phase Space Computing	Sweden	Other	2017	Phase Space Computing est un 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	UK	Software	2018	PhaseCraft est une société de logiciels quantiques fondée par des professeurs de l'University College of London (UCL) et l'Université de Bristol. Ils travaillent sur un programme de recherche avec ces universités, et Google portant sur la modélisation et la simulation quantique.
Photon Spot	US	Hardware	2009	Photon Spot, Inc. fabrique des systèmes cryogéniques sub-Kelvin et des détecteurs de nanofils supraconducteurs à photon unique. Leurs systèmes sont utilisés par des groupes de recherche de premier plan, des laboratoires nationaux et des entreprises de premier plan menant des activités de R&D dans des domaines liés aux quanta dans le monde entier.
Photonic (USA)	Canada	Hardware	2016	Photonic est à la pointe de la conception et de la fabrication de technologies quantiques de haute qualité à base de silicium.
Photonic Nano-Meta Technology	Russia	Hardware/ Sensors	2012	Photonic Nano-Meta Technology fournit des services de recherche et développement liés aux sources de photons uniques de taille nanométrique. Les travaux de la société utilisent les propriétés optiques et quantiques des nanostructures et vise à offrir une intégration dans les puces des ordinateurs optiques et quantiques, permettant aux clients d'augmenter le taux d'émission de photons uniques dans les nano-diamants (NV).
Photonic System Inc.	Canada	Hardware	2019	Photonic est un spin-off du laboratoire « Silicon Development Lab » de l'Université Simon Fraser qui développe du matériel quantique utilisant de la photonique ainsi que des technologies de qubits de spin.
Polaris Quantum Biotech	US	Software	2020	Polaris QB souhaite développer une plateforme de découverte de médicaments. Leur outil serait une combinaison de technologie inspirée de l'informatique quantique, de l'apprentissage machine, de techniques hybrides (quantique/classique) et de simulations de mécanique moléculaire, permettant aux prestataires de soins de santé de faire des découvertes rentables qui seront utilisées pour le développement de nouveaux médicaments.
Post-Quantum (PQ Solutions)	UK	Communication	2009	Post-Quantum (PQ Solutions) offre une variété de produits et services de sécurité de l'information, ce qui inclut des algorithmes de chiffrement sécurisé quantiqus.
PQShield	UK	Communication	2018	PQShield est un spin-off de l'Institut de Mathématiques de l'Université d'Oxford, La société développe des algorithmes de cryptographie post-quantique à haute performance. Ils participent activement aux processus de normalisation de la cryptographie post quantique du NIST. Ils évaluent également plusieurs algorithmes d'autres candidats arrivés en phase 2 du processus de sélection.
Prevision.io	France	Software	2016	Prevision.io 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.
ProteinQure	Canada	Software	2017	ProteinQure est une entreprise de biotechnologie qui utilise des outils de calcul de R&D pour concevoir des médicaments in silico. Ils exploitent le potentiel de l'informatique quantique, des simulations moléculaires et de l'apprentissage par renforcement pour aider les ingénieurs à trouver de nouveaux agents thérapeutiques. ProteinQure a participé au programme Creative Destruction Lab à Toronto.
PsiQuantum	US	Hardware/ Computer	2016	PsiQuantum utilise une approche photonique pour la fabrication d'un ordinateur quantique universel dans une usine de fabrication de silicium CMOS. Ils sont toujours en mode furtif.

Q&I	UK	Consulting	2020	Q&I (Qandi) fournit du conseil sur toute la palette des technologies quantiques. Cela comprend la façon de résoudre les problèmes d'information quantique critiques et ceux liés aux technologies afin, par ailleurs, de mieux en exploiter les possibilités. Leurs activités couvrent la rédaction de rapports business et des études de conception détaillées spécifiques aux cas client. Leurs services comprennent aussi des évaluations de « readyness » (TRL) et de support avec due-diligence en technologies quantiques.
Qasky	China	Communication	2016	Qasky, appelé officiellement Anhui Qasky Science, commercialise la recherche en cryptographie quantique de l'Académie Chinoise des Sciences. Ils offrent ou projettent d'offrir toute une palette de produits et services : terminaux de communication avec cryptographie quantique, switchs réseau / équipements de routage, dispositifs opto-électroniques, instruments scientifiques et de contrôle de la sécurité du réseau, logiciels d'application, etc..
QbitLogic	US	Software	2014	QbitLogic est une société de logiciel informatique quantique avec une orientation générale sur des algorithmes IA pour les ordinateurs quantiques.
Qblox	Netherlands	Hardware	2019	Qblox est une start-up "early-stage", spin-off de QuTech, qui développe une technologie pour permettre un contrôle "scalable" des ordinateurs quantiques.
QC Ware	US	Software	2014	QC Ware Corp. développe des solutions logicielles agnostiques au type de qubit pour les ordinateurs quantiques. QC Ware offre ses services par l'intermédiaire d'une plateforme Cloud. La suite logicielle comprend des bibliothèques de fonctions plug-and-play en optimisation, en ML, et simulations quantiques.
Q-CTRL	Australia	Software	2017	Q-CTRL est une start-up australienne dirigée par le professeur Michael Biercuk de l'Université de Sydney. Ils élaborent un framework firmware pour les ordinateurs quantiques pour traiter la question du contrôle d'erreur. Q-CTRL a récemment lancé son premier produit logiciel appelé Black Opal, un logiciel de contrôle agnostique au type de plateforme de qubits qui vise à réduire la décohérence et les erreurs de la couche physique. La liste des utilisateurs qui ont déjà signé pour ce logiciel inclut IBM, Bleximo, et d'autres.
QDTI	US	Hardware/ Computer	2012	S'appuyant sur les recherches de pointe menées à l'université de Harvard, QDTI (Quantum Diamond Technologies) exploite des systèmes quantiques conçus dans des cristaux de diamant - appelés centres de vacance d'azote (NV). Ces centres NV sont le moteur de la nouvelle approche de détection des biomolécules.
QEYnet	Canada	Communication	2017	QEYnet travaille à construire le premier réseau mondial de distribution quantique de clé (QKD) en utilisant la technologie satellite pour surmonter les limitations de distance liées aux pertes de signal sur les câbles à fibres optiques.
Qilimanjaro Quantum Tech	Spain	Multiple	2018	L'objectif de Qilimanjaro est de construire une plateforme Cloud disponible pour tous ceux qui souhaiteraient explorer les possibilités de l'informatique quantique à faible coût. Ils prévoient la construction d'un ordinateur quantique adiabatique utilisant des qubits supraconducteurs à flux de courant persistant, puis d'en offrir un accès sur le Cloud. Ils auront également un ensemble de services qui aideront les particuliers et les entreprises à adapter leurs problèmes aux algorithmes quantiques. L'un des aspects les plus insolites de cette société est le plan de financement par une ICO libellée sur une crypto-monnaie qu'ils appellent le QBIT.
Qindom	Canada	Software	2018	Qindom Inc. est un fournisseur de services de recherche et de solution d'intelligence quantique (QI). Ils sont dédiés à l'utilisation du calcul quantique en IA pour la recherche et les applications (QML sur ordinateur D-Wave en particulier).
Q-Lion	Spain	Hardware	2019	Q-Lion est une entreprise de logiciels d'informatique quantique qui se concentre sur la création de codes de correction d'erreurs quantiques réalistes et tolérants aux défaillances (FTQECC) pour lutter contre la décohérence dans les ordinateurs quantiques à ions piégés.
QLM Technology	UK	Hardware/ Sensors	2017	QLM Technology développe des capteurs optiques quantiques ultra-compacts et de haute précision, conçus par exemple pour détecter des fuites de gaz naturel au niveau des têtes de puits et lors du transport par pipeline.
Qnami	Switzerland	Hardware	2017	Qnami est un spin-off du laboratoire de recherche en métrologie quantique de l'Université de Bâle. Elle conçoit et produit des solutions quantiques pour les applications de détection et d'imagerie de haute précision notamment à base de diamants artificiels (NV Centers). Ils offrent des solutions de microscopie B2C pour l'inspection de l'appareil et l'analyse des défaillances à l'échelle nano-métrique. De plus, ils soutiennent les entreprises avec une fonderie quantique pour la conception et la production de capteurs ultra sensibles dans plusieurs domaines, notamment celui des semi-conducteurs, de l'imagerie médicale et du diagnostic médical.
Qrithm	US	Software	2018	Qrithm développe de nouveaux algorithmes quantiques pour diverses applications : apprentissage machine, science des matériaux, cryptographie et trading à haute fréquence.
Qrypt	US	Communication	2018	Grâce à leurs expertises, les ingénieurs matériels et logiciels de Qrypt développent une solution cryptographique basée sur la génération de nombres aléatoires quantique à grand débit alimentée par des sources d'entropie multiples et ceci exclusivement sous licence de laboratoires nationaux tels que Oak Ridge National Lab. Ils combinent la génération aléatoire quantique de clés avec leurs propres algorithmes post-quantique et couches de protocoles de sécurisation des informations. Qrypt est un investisseur dans Quside basée à Barcelone, qui se concentre aussi sur le développement de générateurs de nombres aléatoires à haut débit.

QSimulate	US	Software	2018	QSimulate est un développeur d'outils destinés aux simulations moléculaires quantiques sur le Cloud. Ces simulations intéressent les industries chimiques et pharmaceutiques en permettant aux entreprises d'accélérer leur recherche et développement informatique. Elle collabore avec Amgen (Applied Molecular Genetics), Google AI Quantum Lab et Amazon Quantum Solutions Lab.
QTEC (Zhejiang Jiuzhou Quantum Technology)	China	Communication	2012	Fabricant de matériel de communication quantique.
Qu&Co	Netherlands	Software	2016	Quandco développe des solutions logicielles quantiques customisées pour de grandes entreprises, ainsi que des outils de benchmarking. La société vise en particulier des sujets liés à l'IA et à la simulation chimique. Ils sont partenaires de Microsoft et d'IBM Q Network.
Quacoon	US	Consulting	2020	Quacoon est un innovateur dans le domaine de l'informatique quantique et de l'intelligence artificielle, qui travaille sur des solutions logicielles adaptées à l'industrie. Sa mission est d'accélérer l'adoption et la mise en œuvre de l'informatique quantique et de l'intelligence artificielle dans le plus grand nombre de domaines possible.
Quandela	France	Hardware	2017	Quandela développe et commercialise des dispositifs compacts de haute performance pour des applications d'optique quantique. La technologie de base consiste en un générateur de photons uniques destiné au monde de la recherche à base de semi-conducteurs (quantum dot). Ses sources de photons peuvent servir dans la cryptographie quantique et, à terme, à créer des ordinateurs quantiques à base d'optique linéaire ou autres techniques.
Quantastica	Estonia	Software	2019	Quantastica développe des outils logiciels d'algorithmes quantiques hybrides dont leur "Quantum Programming Studio", un environnement de développement web graphique pour créer des algorithmes quantiques exécutables sur ordinateurs quantiques ou sur simulateurs, dont un simulateur classique qu'ils ont eux-mêmes développé.
Quanterro Labs	United Arab Emirates	Software	2019	Quanterro est une association de chercheurs et d'entrepreneurs travaillant dans le développement de l'information et de la sécurité quantiques. Ils répondent au besoin du marché mondial de se concentrer sur le développement de middleware et software pour le matériel quantique émergent de fournisseurs tels que D-Wave, Google, IBM et d'autres. La société fournit également des services d'hébergement, d'enseignement et de conseil dans de nombreux secteurs tels que la cybersécurité, la défense, la technologie du secteur public, l'automobile, la santé, l'industrie et l'éducation.
QuantFi	France	Software	2019	QuantFi est une startup-française qui se spécialise dans la création d'algorithmes informatiques quantique pour l'industrie des services financiers. Ils sont engagés dans la recherche universitaire en coordination avec divers organismes publics et ont pour stratégie à long terme d'utiliser l'informatique quantique pour faire de la gestion de portefeuille financier.
QuantiCor Security	Germany	Communication	2017	QuantiCor Security fournit des solutions de cryptographie post-quantique pour les objets connectés (IoT) et les applications blockchain. Ils ont reçu récemment un prix de l'innovation d'Accenture pour leurs solutions de sécurité. Le personnel clé est originaire de l'Université de Darmstadt.
Quantika	Japan	Consulting	2017	Quantika fournit des services de conseil pour naviguer dans le marché émergent des technologies quantiques. Quantika dispose d'un personnel basé au Royaume-Uni, France et Japon et travaille avec les investisseurs, startups, chercheurs ou innovateurs en entreprise pour réussir les transferts de technologie et créations de startups.
QuantLR	Israel	Communication	2017	QuantLR développe des solutions de cryptographie quantique destinées à protéger les données. Leurs solutions sont basées sur la technologie de distribution quantique de clés.
Quantopo	US	Software	2017	Quantopo propose des solutions d'apprentissage machine quantique (QML) pour améliorer les outils de modélisation statistique et d'analyse des données topologiques. Leurs algorithmes sont adaptés aux besoins analytiques des entreprises des secteurs pharmaceutique et biotechnologique, mais sont aussi applicables aux domaines de la défense, du marketing, des soins de santé, et d'autres industries.
Quantopticon	UK	Software	2017	Quantopticon est une startup au stade précoce qui produit des logiciels de modélisation uniques pour la conception et l'optimisation des composants quantiques - éléments constitutifs des technologies quantiques émergentes, tels que les ordinateurs quantiques et des canaux de communication quantique.
Quantropi	Canada	Communication	2018	Quantropi a mis au point un moteur d'encodage basé sur un logiciel utilisant les principes de la mécanique quantique pour protéger les communications de données. La solution est légère, à faible latence et sécurisé. Elle a été mise en œuvre dans un démonstrateur de distribution quantique de clés. L'objectif est de développer une solution alternative à la distribution quantique de clé photonique qui ne nécessiterait pas un nouveau matériel avec un focus particulier à court terme sur Internet des Objets (IoT).

Quantum Base	UK	Communication	2014	Quantum Base invente, conçoit et développe des solutions de sécurité quantique qui pourront être produites en masse et des dispositifs à l'échelle nanométrique. Ceux-ci sont basés sur la mécanique quantique plutôt que la complexité mathématique, assurant ainsi une sécurisation totale des informations numériques. Ils fournissent également un générateur quantique à l'échelle nanométrique de nombres aléatoires (Q-RAND) qui peut être intégrés dans les systèmes microélectroniques existants et nouveaux.
Quantum Benchmark Inc.	Canada	Software	2017	Quantum Benchmark Inc. est un spin-off de l'Institute for Quantum Computing et l'Université de Waterloo. Ils offrent une gamme de produits et services à destination à la fois des utilisateurs et des fournisseurs du secteur de l'informatique quantique en étant agnostique à l'architecture du matériel quantique. Leur produit phare est la suite logicielle True-Q, un outil standard de l'industrie pour l'optimisation à grande échelle de la performance du matériel quantique, qui étend et valide les capacités d'exécution pour différentes applications de l'utilisateur grâce à la technologie de diagnostic et d'atténuation d'erreurs. Ce savoir-faire en fait le leader dans son secteur.
Quantum Brilliance	Australia	Hardware	2019	Quantum Brilliance développe une plateforme de calcul quantique basée sur les défauts à l'échelle atomique du diamant (centres NV à vide d'azote) qui fonctionnera à température ambiante. Il s'agit d'un spin-out du programme de diamant quantique de l'Université nationale australienne.
Quantum Circuits, Inc. (QCI)	US	Hardware/ Computer	2015	Circuits Quantum (QCI) a été fondée par trois scientifiques du Département de physique appliquée de l'Université de Yale avec une expertise dans les dispositifs quantiques et les traitements quantiques de l'informations utilisant des dispositifs à semi-conducteurs. L'objectif à long terme de QCI est de développer, fabriquer et vendre les premiers ordinateurs quantiques génériques sur la base de qubits supraconducteurs Transmon. QCI commercialisera également des composants, des appareils et des logiciels qui permettront d'accélérer la recherche fondamentale et le passage à l'échelle de l'informatique quantique.
Quantum Computing & AI Research (QCAR)	Taiwan	Consulting	2017	Quantum Computing & AI Research (QCAR) est la première entreprise privée sur le calcul quantique à Taiwan. À l'heure actuelle, ils se concentrent sur la modélisation de nouveaux qubits topologiques et sont également consultants pour toutes les startups potentielles dans le domaine du quantique, non seulement à Taiwan, mais aussi dans le monde entier.
Quantum Computing (PINX: QUBT)	US	Software	2001	Quantum Computing Inc. commercialise des logiciels et des services d'applications d'informatique quantique.
Quantum Dice	UK	Communication	2019	Quantum Dice est un spin-off technologique de l'Université d'Oxford, qui commercialise un générateur quantique de nombres aléatoires (QRNG). Le dispositif sera intégré sur une puce. Les nombres aléatoires générés sont cryptographiquement sûrs, ce qui permettra de les utiliser dans toute une série d'applications commerciales.
Quantum Factory	Germany	Hardware/ Computer	2018	Quantum Factory ambitionne de construire un ordinateur quantique à base de d'ions piégés et de vendre la puissance de calcul en tant que service. Quantum Factory utilise une unité d'ions piégés propriétaire qui simplifie l'assemblage des modules de piégeage d'ions et l'établissement de jonctions entre ces modules.
Quantum Impenetrable	UK	Communication	2018	Quantum Impenetrable a mis au point un module de sécurité matériel cryptographique (HSM) inspiré par la génétique et la physique quantique et combiné avec un générateur quantique de nombres aléatoires.
Quantum Machines	Israel	Multiple	2018	Créée par trois physiciens de l'Institut Weizmann des sciences, Quantum Machines développe une couche de contrôle des qubits (orchestration) pour des ordinateurs quantiques supraconducteurs qui associe matériel et logiciel.
Quantum Microwave	US	Hardware	2016	Quantum Microwave développe et fabrique des composants micro-ondes cryogéniques pour les ordinateurs quantiques.
Quantum Motion Technologies	UK	Hardware/ Computer	2017	Quantum Motion Technologies a été fondée suite aux recherches menées par les professeurs Simon Benjamin (Département des matériaux, Oxford) et John Morton (Département des sciences de l'ingénieur, Oxford). L'objectif de l'entreprise est de développer des architectures informatiques quantiques basées sur la technologie de silicium CMOS pour atteindre un grand nombre de qubits et ainsi faire face aux problèmes de calcul quantiques pratiques (erreurs).
Quantum Opus	US	Hardware	2013	Quantum Opus fabrique des systèmes de nanofils supraconducteurs de pointe qui offrent une grande efficacité de détection, un faible bruit et des taux de comptage ultra élevés, dans un appareil compact. Ils offrent ces solutions de comptage de photons pour répondre aux besoins de l'optique quantique, de l'informatique quantique, de la communication optique ou quantique, de la biophotonique à faible flux et des mesures de fluorescence.
Quantum Phi	Czech Republic	Consulting	2018	Quantum Phi est une société de conseil, d'analyse et de recherche qui met l'accent sur les technologies quantiques, la connaissance de leurs principes, de leurs utilisations et de l'industrie des technologies quantiques elle-même. En plus des applications civiles, ils se spécialisent dans l'utilisation des technologies quantiques pour l'espace, la sécurité et l'industrie militaire.

Quantum Thought	US	Communication	2019	Quantum Though est un cabinet de conseil stratégique axé sur l'informatique quantique pour l'entreprise. Leur équipe, pluridisciplinaire, comprend des experts en informatique quantique, des spécialistes de l'IA et de la cybersécurité pour aider au mieux les entreprises à se préparer à un "futur quantique".
Quantum Xchange	US	Communication	2016	Quantum Xchange offre les premiers réseaux sécurisés quantiques commerciaux aux États-Unis qui utilisent la technologie QKD (Quantum Key Distribution) avec un service qu'ils appellent Phio. Ils sont partenaire du groupe Zayo, spécialiste des infrastructures de communication et propriétaire du réseau de fibre noire utilisé, d'ID Quantique pour le matériel de distribution quantique de clé (QKD) et de l'Institut de recherche Battelle pour le matériel des nœuds de confiance (relais). Quantum Xchange a récemment annoncé la première installation qui relie la zone de Wall Street à New York et les services de back-office de diverses sociétés financières dans le New Jersey.
Quantum CTek	China	Communication	2009	QuantumCTek est la première entreprise en Chine à fournir des produits et des services de sécurité réseau multi-protocoles basés sur la technologie quantique. La société produit des systèmes de communication quantique de pointe ainsi que des unités optoélectroniques avec des applications commerciales pour l'industrie financière, les organismes gouvernementaux et d'autres entreprises, ainsi que des applications dans la recherche pour les sociétés scientifiques. Les produits qu'ils offrent incluent le cryptage quantique, les passerelles quantiques et des switchs optiques. La société a été fondée par le premier groupe de recherche en physique quantique chinois du Laboratoire national Hefei pour la science physique à micro-échelle (HFNL) et de l'Université des Sciences et Technologies de Chine (USTC). Quantum CTek s'est distinguée comme la première IPO d'une entreprise du secteur quantique en Chine avec un cours de l'action en progression de plus de 900% lors de son premier jour de cotation.
Quantum Door	China	Communication	2018	QuantumDoor développe indépendamment des équipements terminaux de communication quantique à clé, des équipements de commutation/routage de réseau, des dispositifs optoélectroniques de base, des systèmes de contrôle et des logiciels d'application, etc. Elle fournit aux utilisateurs des solutions de systèmes de sécurité de l'information qui intègrent la technologie quantique.
Quantum-South	Uruguay	Software	2019	Quantum-South travaille sur des problèmes complexes d'optimisation des cargaisons en s'appuyant sur des logiciels d'informatique quantique. Leur objectif est d'obtenir de meilleurs résultats que les solutions conventionnelles actuelles et ainsi d'aider les entreprises à améliorer leurs revenus et à réduire leurs coûts. Ils travaillent également dans le domaine de la finance pour lequel un calcul quantique peut apporter de meilleures solutions à certains problèmes.
QuantumX	UK	Other	2017	QuantumX est un studio incubateur / venture ayant des bureaux à Cambridge et San Francisco. Son objectif est d'incuber le maximun de startups quantiques. QuantumX a un partenariat avec CQC (Cambridge Quantum Computing) qui leur fournit un accès à leur compilateur quantique.
Quantumz.io	Poland	Software	2019	Quantumz.io développe une plateforme de simulation quantique (QSP), selon eux très efficace, basée sur l'idée de la programmation parallèle sur GPU et qui sera offerte en tant que service. Le QSP sera équipé de fonctionnalités pour construire efficacement, exécuter et gérer les algorithmes quantiques du client. Ils développent également des solutions matérielles et logicielles de cryptographie post-quantique (PQC) nommée Banax.
QuBalt GmbH	Germany	Communication	2015	QuBalt a son siège administratif en Allemagne mais sa recherche à Riga, en Lettonie. Ils développent des algorithmes de cryptographie résistant aux ordinateurs quantiques et travaillent également sur des algorithmes de calcul quantique.
Qubit Engineering	US	Software	2018	Qubit Engineering est une société informatique du logiciel quantique qui a développé de nouvelles méthodes d'optimisation pour les éoliennes en micro-implantation. Le logiciel permettra d'améliorer considérablement l'efficacité des parcs éoliens et de réduire le coût global des projets.
Qubit Reset LLC	US	Communication	2018	Qubit Reset a pour principal domaine de recherche les répéteurs quantiques pour l'Internet quantique, mais ils travaillent aussi sur d'autres produits comme les interfaces réseaux classique/quantique et la distribution quantique de clé (QKD).
Qubitekk	US	Communication	2012	Qubitekk a récemment annoncé la disponibilité du premier générateur plug-and-play de photons intriqués au monde, le QES1. Comme les transistors au cœur des ordinateurs classiques, le QES1 permet la circulation de l'information au sein d'ordinateurs quantiques ou par l'intermédiaire de produit de cryptage quantique des communications - les deux produits seraient en cours de développement par la société.
Qubitera	US	Software	2018	Qubitera développe des solutions innovantes basées sur la recherche pour relever les défis de l'informatique quantique à court terme (NISQ) et des technologies assistées par l'IA.
Qubitor	Singapore	Other	2017	Qubitor est un incubateur de startups technologiques. Leur laboratoire de calcul quantique développe des applications quantiques en particulier dans l'apprentissage machine et IA.
QuDot	US	Software	2018	QuDot fournit des logiciels de simulation de circuit quantique en utilisant leur technologie en attente de brevet, QuDot Net, pour simuler les ordinateurs quantiques universels sur du matériel générique. QuDot Net utilise un type particulier de réseau bayésien qui permet la représentation efficace de certains systèmes de qubits.

QuEra Computing	US	Hardware/ Computer	2018	QuEra Computing utilise une plateforme technologique basée sur les atomes neutres pour construire un ordinateur quantique "scalable", ayant une capacité de calcul quantique importante et qui soit commercialement utile. L'équipe de recherche comprend de nombreux membres des groupes de recherche sur l'atome froid de l'Université d'Harvard.
Quintessence Labs	Australia	Communication	2008	Quintessence Labs fournit des générateurs quantiques de véritables nombres aléatoires et une plateforme de distribution quantique de clé. Ils ont actuellement en développement une seconde génération de produits qui pourra fonctionner sur les infrastructures existantes (fibres optiques) avec des taux très élevés de débit.
QuiX	Netherlands	Hardware/ Computer	2019	QUIX développe un processeur quantique photonique basée sur des guides d'ondes en nitrure de silicium. L'équipe fondatrice comprend des scientifiques de l'Université de Twente et l'AMOLF institut de recherche à Amsterdam. Quix a l'intention d'offrir les premiers éléments de leur ordinateur d'ici deux ans et leur technologie fonctionne à température ambiante ce qui élimine la nécessité d'employer des réfrigérateurs à dilution coûteux.
Qulab	US	Software	2017	Qulab est spécialisée dans la conception de molécules thérapeutiques en tirant parti de la puissance des ordinateurs classiques et quantiques.
Qulabs.ai	India	Multiple	2017	Qulabs.ai se concentre sur la construction de réseaux quantiques/Internet quantique et sur le développement d'une expertise dans l'apprentissage machine quantique (QML) pour la finance et la pharmaceutique. Ils ont créé une unité commerciale QuAcademy pour faciliter la formation des étudiants en combinant les compétences requises pour la conceptualisation, le développement et la traduction des nouvelles technologies quantiques. Ils travaillent actuellement avec les laboratoires de recherche de l'IIT Hyderabad, de l'IIT Roorkee et de l'IIT Bengaluru.
QunaSys	Japan	Software	2018	QunaSys a été fondée par des chercheurs des Université de Tokyo, d'Osaka, et Kyoto. Ils développent des applications utilisant l'informatique quantique en mettant l'accent sur la chimie quantique, l'apprentissage machine quantique et l'optimisation. Ils assurent aussi la maintenance évolutive du simulateur Qulacs initialement développé à l'université de Kyoto.
Qunnect	US	Communication	2017	Qunnect est un spin-off du groupe des Technologies de l'information quantique de l'Université Stony Brook (Long Island, NY, USA). Ils fournissent une boîte à outils commerciale de dispositifs quantiques spécialement conçus et optimisés pour améliorer la technologie de communication numérique en la rendant impiratable.
QuNu Labs	India	Communication	2016	Qunu Labs développe des produits de cybersécurité quantique à l'aide de distribution quantique de clés (QKD). Leur premier produit est un système QKD simple qui utilise un protocole de déphasage différentiel (Differential Phase-Shift Protocol) issu de 4 années de recherches initiales qui avaient été suivies d'une incubation à l'IIT Madras. La société indique que leurs systèmes sont optimisés pour les conditions d'exploitation en Inde et a un coût très compétitif.
Qureca	UK	Consulting	2019	Qureca (QUantum REsources & CAreers) fournit les services professionnels et les ressources nécessaires aux entreprises et aux institutions pour être prêtes, faire la différence et créer de la valeur grâce à la technologie quantique. Les services qu'elle propose comprennent le développement des entreprises, la veille économique, la formation et les ressources.
QuSecure	US	Communication	2019	Les produits et services de QuSecure comprennent entre autres une architecture blockchain résiliente quantique et des tests de pénétration quantique. L'équipe est composée de chercheur qui partagent des décennies d'expérience en matière de cybersécurité, Quantum Computing, Machine Learning et technologies Blockchain, combinés avec des chefs d'entreprise chevronnés de la Silicon Valley.
Quside	Spain	Hardware	2017	Quside est une un spin-off d'ICFO. Elle conçoit et commercialise un outil de génération ultrarapide de nombres aléatoires quantiques pour les environnements mobiles (IoT) et les datacenters.
QxBranch	US	Software	2014	QxBranch est une société de logiciel quantique créée en 2014 par les dirigeants de Lockheed Martin and Aerospace Concepts. Les compétences des équipes en ingénierie des systèmes, analyse des données, apprentissage automatique et informatique quantique sont mises à disposition des clients du monde entier dans divers des secteurs : bancaire & assurance, aérospatiale, sécurité. QxBranch a son siège à Washington, avec des bureaux à Hong Kong, Londres et Adelaide. QxBranch a été acquise par Rigetti Computing en Juillet 2019.
Rahko	UK	Software	2018	Rahko est une société de développement de logiciels d'apprentissage machine quantique (QML).
ReactiveQ	Canada	Software	2018	Fournisseur d'une plateforme d'informatique quantique destinée à créer des ordinateurs quantiques et à produire des supraconducteurs et des méta-matériaux. La plateforme de l'entreprise propose des simulations réalistes basées sur les technologies quantiques, permettant aux utilisateurs d'obtenir des technologies rentables et économes en énergie.
Rigetti	US	Hardware/ Computer	2013	Rigetti Computing est une entreprise informatique quantique "full stack" qui fournit un environnement informatique intégré (du logiciel au hardware : ordinateur quantique). Leur Quantum Cloud Services (SCQ) est une plateforme Cloud quantique qui donne aux utilisateurs un accès à l'ordinateur quantique de Rigetti (pas une simulation) dans un environnement de programmation virtuelle. Rigetti a acquis QxBranch en Juillet 2019 pour l'aider à optimiser son intégration verticale particulièrement importante dans l'ère du NISQ.

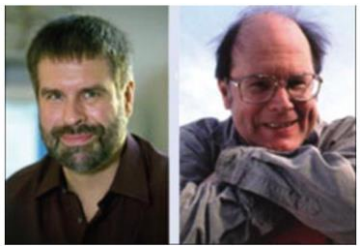
Riverlane	UK	Software	2016	Riverlane est une société de logiciels quantiques, spin-off de l'Université de Cambridge. Elle fournit des services de conseils aux clients industriels ou gouvernementaux, ainsi que du développement de nouveaux algorithmes quantiques permettant de résoudre des problèmes à forte valeur ajoutée dans le domaine de la chimie. En collaboration avec Dividiti Ltd, Riverlane développe "Quantum Collective Knowledge", un kit de développement logiciel qui permet de benchmarker, d'optimiser et de co-concevoir des logiciels et matériels quantiques, le tout en réduisant considérablement les délais de commercialisation et les coûts de R&D.
Seeqc	US	Hardware	2017	SeeQC est un spin-off du groupe américain Hypres, spécialisé dans la création d'électronique supraconductrice. Elle se focalise dans la création de circuits de contrôle de qubits supraconducteurs dotés de mémoires à base de technologique spintronique (spin d'électrons).
Semicyber	US	Software	2018	Semicyber est spécialisé dans la fourniture d'analyse de données, d'algorithmes quantiques et de services logiciels lors de missions critiques. Ils ont annoncé travailler dans le cadre du programme AFWERX de l'US Air Force sur la prochaine génération d'algorithmes quantiques.
S-Fifteen Instruments	Singapore	Hardware	2017	S-Fifteen est un spin-off du Centre des Technologies Quantiques (CQT) créé pour commercialiser des technologies quantiques propriétaires développées au cours de décennies de recherche. S-Fifteen offre une suite de solutions et d'applications sur le thème de la sécurité quantique pour servir les clients qui exigent une confiance et une transparence inégalées en matière de solutions pour leurs besoins cryptographiques. Ils développent aussi des systèmes de contrôle de qubits.
Shyn	Bulgaria	Software	2016	Shyn travaille sur la visualisation des données quantiques. Avec le financement initial de Google et le soutien d'Amazon, elle souhaite utiliser des algorithmes quantiques pour visualiser la variance des données : du cours des actions aux prévisions météorologiques. La société estime qu'une couche d'interface, alimentée par l'architecture quantique, peut aider les consommateurs de données à prendre de meilleures décisions.
Sigma-i	Japan	Consulting	2019	Sigma-i est une « société universitaire de technologie » mis en place en 2019 par trois chercheurs du groupe de R&D Quantum Annealing de l'Université de Tohoku, au Japon. Sa mission est d'industrialiser de nouvelles technologies après leur développement au sein des laboratoires de recherches académiques. Leur offre initiale sera de fournir des services de conseils quantiques et l'accès à la famille des systèmes D-Wave aux entreprises, universités et laboratoires de recherche à travers le Japon.
Silicon Quantum Computing	Australia	Hardware/ Computer	2017	Silicon Quantum Computing est un spin-off de l'Université de Nouvelle-Galles du Sud (UNSW) dont l'objectif est d'accélérer le développement et la commercialisation de la technologie du "Centre of Excellence for Quantum Computation and Communication Technology" (CQC2T). Cette société souhaite tirer parti de la technologie de qubits à base de silicium (CMOS) sur laquelle le CQC2T a travaillé. Leur objectif à court terme est de développer un prototype de circuit intégré quantique de 10 qubits en 2022 comme précurseur d'ordinateur quantique à base de silicium et d'élargir leur portefeuille de brevets.
Single Quantum	Netherlands	Hardware	2012	Simple Quantum est un spin-off de l'Institut Kavli des Nanosciences à la TU de Delft. La société développe et fabrique des systèmes simples de détection de photons basés sur la technologie de nanofils supraconducteurs. Les produits sont conçus pour des applications dans le domaine de l'informatique quantique, la communication quantique et la cryptographie quantique, la spectroscopie à résolution temporelle de l'infrarouge, la télémétrie laser et de détection à distance (LiDAR).
SoftwareQ	Canada	Software	2017	SoftwareQ offre une variété de logiciels quantiques et services incluant des simulateurs quantiques, des compilateurs quantiques, des optimiseurs, des logiciels éducatifs et des services de conseil. Les co-fondateurs sont le Dr Michele Mosca et le Dr Vlad Gheorghiu de l'Institut de l'informatique quantique (IQC).
Solid State AI	Canada	Software	2017	Solid State AI propose une plateforme SaaS en utilisant des algorithmes hybides d'apprentissage automatique classiques et quantiques qui permettent aux ingénieurs process et équipements d'augmenter les rendements de fabrication, d'optimiser les paramètres de processus et de réduire les coûts d'entretien de l'équipement et des temps d'arrêt. Ces algorithmes sont particulièrement efficaces pour prédire sur des ensembles de données rares - ceux qui ont des données limitées, ou avec un rapport signal/bruit faible. Solid State AI a fait partie du programme Quantum Machine Learning Creative Destruction Lab de Toronto.
Sparrow Quantum	Denmark	Hardware	2016	Sparrow Quantum est un spin-off du laboratoire photonique quantique de l'Institut Niels Bohr au Danemark. Ils vont développer et commercialiser des composants technologiques quantiques photoniques basés sur la recherche et les brevets de l'Institut. Leur premier produit est une puce générant un photon unique destiné aux chercheurs travaillant sur la photonique quantique.
SpeQtral	Singapore	Communication	2019	SpeQtral (anciennement connu sous le nom S15 Space Systems) est un spin-off du Centre for Quantum Technologies (CQT) de l'Université Nationale de Singapour (NUS). La société développe des systèmes de communication quantique pour l'espace en utilisant de petits satellites qui fourniront les clés de chiffrement au moyen de signaux quantiques. Cette technologie offrira une sécurité sans précédent face aux interceptions ou écoutes clandestines et permettra la mise en place de la prochaine génération de réseaux de communication sécurisés. La société dispose d'une technologie sous licence NUS nécessaire pour développer des sources de lumière quantique compactes et a également embauché d'anciens chercheurs du CQT.
Spin Quantum Tech	Columbia	Software	2018	Spin Quantum Tech est une société de logiciels quantiques. Leur approche est basée sur l'IA et l'informatique quantique pour permettre l'apprentissage et l'amélioration des modèles. Ils ont une équipe multidisciplinaire qui travaille sur la grippe aviaire depuis 15 ans et leurs marchés cibles comprennent des sociétés de cybersécurité, fournisseurs de solutions logicielles et de Cloud.

SpinQ	China	Hardware/ Computer	2018	SpinQ développe du matériel et des logiciels quantiques de petite taille. Elle fournit des solutions de recherche avancées et accessibles en informatique quantique aux scientifiques et aux développeurs.
Strangeworks	US	Software	2018	Strangeworks est une startup du logiciel informatique quantique. Son objectif est de rendre l'informatique quantique accessible via un logiciel conçu pour les développeurs, les gestionnaires du système, et les directeurs informatiques. Strangeworks maintient également sa plateforme Web "Strangeworks Community" qui fournit un front-end vers 5 frameworks quantiques différents : IBM, Microsoft, Rigetti, Google et D-Wave.
Stratum.ai	Canada	Software	2018	Stratum.ai propose des algorithmes à base d'IA et de quantique pour modéliser les réserves minières (en particulier d'or) avec 25 % de précisions supplémentaires par rapport aux autres logiciels de modélisation utilisés dans l'industrie de la prospection minière et basés sur des géostatistiques.
Super.tech	US	Software	2020	Super.tech est un spin-off d'une équipe de recherche de l'entité EPiQC dirigée par l'Université de Chicago. Ella a pour ambition de construire une offre full stack à architecture multicouches pour l'informatique quantique.
Terra Quantum AG	Switzerland	Multiple	2019	Terra Quantum AG est une société de technologie quantique qui développe des applications deep tech basées sur l'informatique quantique : matériel, logiciels et algorithmes.
Tokyo Quantum Computing	Japan	Software	2017	Tokyo Quantum Computing (TQC) est une start-up du logiciel quantique qui souhaite développer un logiciel de simulation d'ordinateur à recuit quantique.
Tundra Systems Global LTD	UK	Hardware/ Computer	2014	TundraSystems développe une gamme de systèmes basés sur un processeur quantique en optique linéaire. Une des premières cibles sera de créer un microprocesseur quantique qui sera utilisé dans le cadre d'une solution de système HPC quantique. Leur système sera basé sur la technologie photonique sur silicium qu'ils appellent Opticonductors et qui fonctionne à température ambiante.
Turing	US	Software	2016	Turing est une société de logiciel quantique toujours en mode furtif. Elle semble ambitionner 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. Elle développe aussi des systèmes de correction d'erreurs qu'ils commercialisent auprès d'autres spécialistes du secteur.
UniKlasers	UK	Hardware	2013	UniKlasers développe des lasers monofréquences destinés à des applications scientifiques et industrielles spécialisées. La société est spécialisée dans les lasers DPSS destinés à une large gamme d'applications, telles que l'inspection des puces électroniques, les technologies quantiques, l'avionique, la production d'énergie éolienne, la défense, les serveurs de données financières et la recherche biomédicale. Elle fournit ainsi à ses clients des lasers à faible bruit qui présentent un rendement de conversion élevé, une faible consommation d'énergie et un refroidissement thermoélectrique intégré.
Universal Quantum	UK	Hardware/ Computer	2019	Quantum Universal est un spin-off de la Ion Quantum Technology Group de l'Université du Sussex et est dirigée par le Professeur Winfried Hensinger. Leur objectif est de développer des ordinateurs quantiques en utilisant la technologie des ions piégés couplée à celles des micro-ondes et des champs magnétiques locaux en remplacement des grandes quantités de faisceaux laser individuels utilisés dans d'autres implémentations d'ions piégés.
VeriQloud	France	Communication	2017	Le développement de VeriQloud est centré sur les technologies de réseau quantique, couvrant tous les aspects de protocoles et d'applications mises en œuvre à l'aide de dispositifs optiques. Leur objectif est de construire une offre commerciale pour les clients qui ont des exigences élevées en matière de sécurité réseau, avec une architecture de réseau quantique et des protocoles spécialement conçus pour eux. VeriQloud estime qu'une utilisation appropriée des langages de programmation quantique peut pousser des réseaux quantiques beaucoup plus loin que la seule tâche d'établir des clés secrètes partagées par la distribution quantique de clé, même en n'utilisant que les technologies existantes aujourd'hui. A cet effet, ils mettent en œuvre des protocoles de réseau quantique pour diverses technologies de communication quantique, incluant l'application de protocoles connus aux problèmes industriels et le développement de nouveaux protocoles réseau qui profitent de la haute sécurité de communication quantique.
Wafer China	China	Hardware	2017	Cette société chinoise développe et produit des matériaux et équipements semi-conducteurs pour des diverses applications, entres autres, dans la communication optique, la détection 3D, le soudage industriel, les applications médicales, etc. La société fournit également des services de recherche et développement de matériaux semi-conducteurs et de matériaux optoélectroniques, ainsi que de développement de technologies de communication quantique.
Xanadu	Canada	Multiple	2016	Xanadu est une startup proposant une offre de type « full-stack ». Ils développent un processeur quantique photonique et une plateforme logicielle open source full-stack appelé "Strawberry Fields" pour le calcul quantique photonique. Strawberry Fields est mis en œuvre en Python et inclut un langage de programmation quantique appelé Blackbird. Xanadu a également commencé à publier des résultats en utilisant leur logiciel dans des domaines aussi divers que la chimie quantique, la théorie des graphes, l'apprentissage machine...Leur ordinateur à optique linéaire doit fonctionner théoriquement à température ambiante. Leurs qubits dénommés qumodes utilisent un encodage utilisant le principe de "Continuous Variable", qui stocke une information plus riche que les qubits.
Xlabs	US	Software	2014	Xlabs se présente comme un développeur de projets "moonshot". L'entreprise est engagée dans la conception et la commercialisation de projets utilisant l'intelligence artificielle, l'informatique quantique et la neurotechnologie.

Xofia	US	Software	2019	Xofia est une société d'informatique quantique qui fournit pour l'intelligence artificielle des algorithmes de classification visant à réduire les temps d'apprentissage. Xofia propose leur « Quantum Knowledge » pour améliorer les techniques d'IA courantes et augmenter la quantité et la qualité des données d'entrée pour de meilleurs résultats.
Zapata Computing	US	Software	2017	Zapata Computing est une société de logiciels de calcul quantique issue de l'Université de Harvard et lancée par un groupe de scientifiques de cette université. Ils développent des solutions pour un large éventail de secteurs, notamment la finance, la logistique, la chimie, le pétrole, les produits pharmaceutiques et les matériaux, l'aviation. La plateforme de Zapata, Orquestra ™, permet aux utilisateurs de créer des programmes quantiques ou hybrides et d'orchestrer leur exécution dans les technologies classiques et quantiques. Orquestra combine une plateforme logicielle puissante, des bibliothèques d'algorithmes quantiques et des exemples de workflow du type machine learning, simulation et optimisation.
Zurich Instrument	Switzerland	Hardware	2008	Zurich Instruments fabrique des instruments de pointe pour les scientifiques et les techniciens qui travaillent dans des laboratoires travaillant sur des phénomènes souvent difficiles à mesurer. Leur offre comprend des amplificateurs à verrouillage, des générateurs de formes d'onde arbitraires, des analyseurs d'impédance, des boucles à verrouillage de phase, des numériseurs, et des systèmes de contrôle de l'informatique quantique.
ZY4	Canada	Communication	2014	ZY4 revendique avoir mis au point une nouvelle classe de chiffrement symétrique quantique invulnérable. Elle serait un moyen rapide, et fiable de chiffrement de bout en bout avec authentification des communicants et qui fonctionnerait sur n'importe quel type de réseaux de données et quelle que soit la distance entre les intervenants

Figure 10: Liste Startups / ScaleUp
(Sources : Quantum Computing Report, Pitchbook, Crunchbase, sites internet de startup, autres sources)

- ANNEXE 5 - LE PROTOCOLE DE QKD - BB84



Le protocole BB84 est le premier mécanisme d'échange de clé quantique à avoir été formalisé. Il a été proposé en 1984 par Charles Bennett et Gilles Brassard [228]. Comme nous l'avons vu §4.2.4.2 l'idée est de permettre l'échange sécurisé d'une clé de chiffrement, clé qui pourra être ensuite utilisée pour chiffrer un message qui sera ensuite transmis sur un canal de communication classique.

Ce protocole repose sur l'envoi de l'information relative à la clé sur des photons ayant quatre types de polarisations rectilignes possibles réparties en deux bases distinctes: i) base rectilinéaire (R) 0°, 90° ; ii) base diagonale 45°,135°[229]

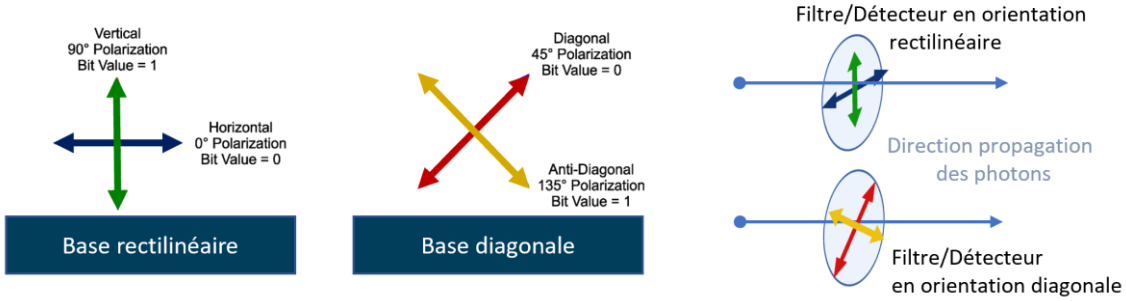


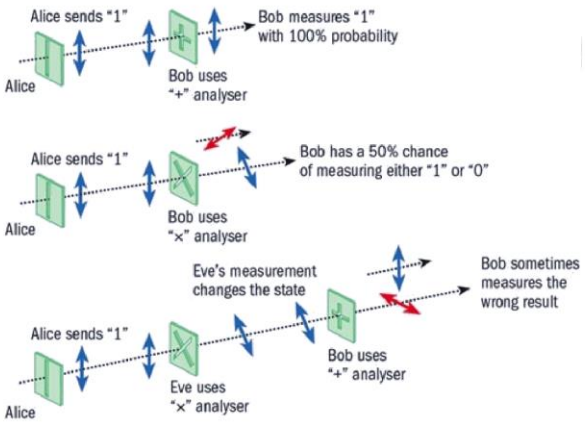
Figure 1: Bases de polarisation Rectilinéaire (0°, 90°) et Diagonale (45°, 135°) utilisées dans le protocole BB84 (Source: [229])

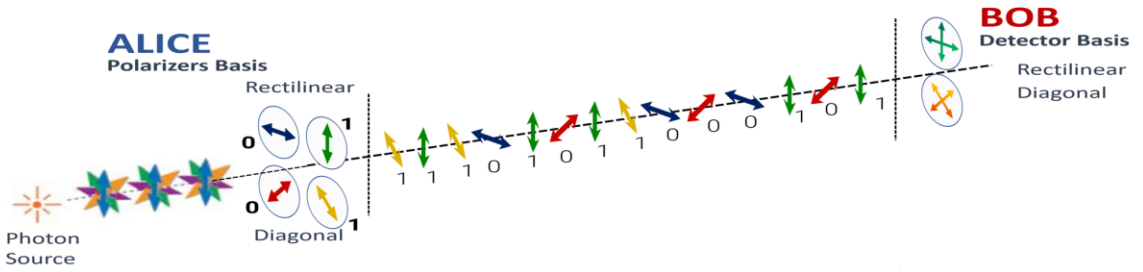
Conséquence du théorème de non-clonage, la lecture des photons par un intrus va modifier la clé, en projetant leur polarisation à 0° ou 90°, ou 45°/135° selon les cas. Toute intrusion en lecture sera détectée à l'arrivée. Si le protocole détecte un intrus, il peut en tenir compte et réinitialiser la communication.

Le protocole BB84 suit six étapes ([230], [231] et Figure 2)

1. Alice encode sa séquence de bits en sélectionnant de manière aléatoire la base rectilinéaire (verticale/horizontale) ou la base diagonale/anti-diagonale sans révéler ses choix à quiconque. Les photons, à présent porteurs d'une information quantique, sont ensuite transmis à Bob via le canal quantique (propagation libre ou fibre optique).

2. Bob reçoit les photons, les lit en choisissant de manière aléatoire une des deux bases d'analyse et enregistre les résultats. La séquence de bits correspondante est nommée « **raw key** ». Si pour un photon donné, Bob a choisi la « bonne » base, c'est-à-dire la même qu'Alice, il obtiendra à coup sûr le bon bit, 0 ou 1, envoyé par Alice. Si en revanche il a choisi l'autre base, il obtiendra 0 ou 1 avec 50% de probabilité. Et dans ce cas, il obtiendra le « mauvais » résultat une fois sur 2 en moyenne.





	QUANTUM EXCHANGE														
	Alice's random bit	1	1	1	0	1	0	1	1	0	0	0	1	0	1
1	Alice's random basis selection														
	Polarized photon sent by Alice														
2	Bob's random base selection														
	Bob's measured received bits	1	1	1	0	0	1	1	1	0	0	0	1	0	0
	Bob's and Alice's basis agreement ?	✓	×	✓	✓	×	×	×	✓	✓	×	✓	✓	✓	×
	PUBLIC CHANNEL														
3	Bob reports basis of received bits														
4	Alice says which basis were correct	✓		✓	✓				✓	✓		✓	✓	✓	
	Sifted key	1		1	0				1	0		0	1	0	
5	Bob reveals some key bits randomly			1	0					0					
	Alice confirms them			✓	✓					✓					
6	**OUTCOME**														
	Remaining shared secret bits	1	-	-	-	-	-	-	1	-	-	0	1	0	-

Figure 2: Les 6 étapes principales du protocole BB84

3 Bob communique à Alice via un canal publique (classique) ses choix de bases, mais pas la valeur mesurée associée à chaque photon.

4 Alice compare ses choix de bases avec ceux de Bob et identifie le sous ensemble de bits correspondants aux cas où ils ont tout les deux choisis la même base. Alice communique ensuite à Bob via le canal publique les positions correspondantes dans la séquence, les autres bits sont alors éliminés. La séquence alors obtenue se nomme «**sifted key** ».

5 Bob transmet ensuite à Alice via le canal publique un sous ensemble de ses résultats. Alice compare cette séquence de bits avec sa propre séquence et réalise alors une analyse d'erreurs.

6 Si le taux d'erreurs (QBER – Quantum Bit Error Rate) est plus faible que 11%, Alice déduit alors qu'il n'y a pas eu d'acte d'espionnage durant la procédure, et que par conséquent la communication à travers le canal quantique était sécurisée. Alice et Bob se servent alors des bits restant de leur *sifted key*, ceux qui n'ont pas été utilisé pour l'analyse d'erreurs, pour créer leur clé d'encryption. Si le QBER est supérieur à 11 %, on abandonne alors la procédure et on recommence le protocole à l'étape 1.[230]

[230] Voir [231]. il faut noter que le taux de transmission des fibres et la transparence des composants optiques ne sont pas parfaits si bien que des erreurs peuvent apparaître sans qu'il y ait eu de tentative d'interception par un adversaire.

En pratique, il y a de nombreux problèmes liés à ce protocole :

- le fait que le système de détection présente toujours un certain niveau de bruit (dark counts), par conséquent même en l'absence d'espion, les sifted keys d'Alice et Bob présenteront des différences.

- il est difficile de mettre au point des sources de photons uniques parfaites. Une possibilité d'attaque par un intrus repose sur la difficulté de produire des photons uniques : les équipements réels peuvent émettre plusieurs photons au lieu d'un seul, qu'un adversaire peut prélever du canal. Ce prélèvement est indétectable, et permet à l'adversaire de cloner des photons, violant ainsi l'hypothèse de sécurité. De nombreuses variantes de BB84 ont été imaginées pour contourner cette vulnérabilité, et il est possible en théorie d'établir une clé sûre en dépit de l'attaque.

L'ensemble de ces raisons expliquent pourquoi le seuil de sécurité lors de l'estimation du pourcentage d'erreur est fixé à 11% plutôt qu'à 0%. Pour compenser ces effets indésirables, deux étapes supplémentaires communes à tout les protocoles de cryptographie quantique doivent alors avoir lieu en fin de protocole, ces étapes qui correspondent à des algorithmes classiques sont connues sous les noms de « error correction» et « privacy amplification » que nous ne développerons pas ici.

- ANNEXE 6 - PORTES LOGIQUES CLASSIQUES ET PORTES QUANTIQUES

En informatique classique, l'algèbre de Boole (qui permet au final de faire tourner tous les programmes et les calculs) ne nécessite pour être exécuter qu'un ensemble restreint de portes différentes implantées en grand nombre dans les circuits intégrés des ordinateurs.

Nous présentons sur la figure 1 ci-contre ces portes logiques communes ainsi que leurs tables de vérité. Les valeurs booléennes FAUX/VRAI sont codés par des valeurs binaires 0/1 stockés dans des bits. L'état 0 représente le FAUX, et l'état 1 représente le VRAI.

Ces portes ont 1 à 2 entrées. La seule porte unaire[231] est la porte NOT. Celle-ci inverse le bit d'entrée : $0 \Rightarrow 1$ et $1 \Rightarrow 0$. Cette porte est réversible, car il est trivial de déterminer la valeur des bits d'entrée par rapport aux valeurs des bits de sortie. Les autres portes présentées comportent 2 entrées et 1 seule sortie, résultat de l'opération booléenne effectuée. Par exemple, la sortie de la porte AND vaut 1 si et seulement si ses deux entrées sont à 1 autrement la sortie est 0.

Cette porte, comme toutes les autres portes à deux entrées illustrées ici sont toutes des portes *irréversibles*, ce qui signifie que les valeurs des bits d'entrée ne peuvent pas être déduites du résultat de l'opération appliquée. Ainsi, si la sortie=1 d'une porte AND identifie uniquement l'entrée 11, une sortie=0 est ambigüe car associée à 00 ou 01 ou 10, sans que l'on puisse trancher.

L'irréversibilité implique que l'on ne peut pas revenir en arrière et que l'information d'entrée est perdue. Le cas des portes quantiques est différent, la majorité des opérations quantiques sont réversibles.

GATE		CIRCUIT SYMBOL	TRUTH TABLE
NOT	The output is 1 when the input is 0 and 0 when the input is 1.		Input: 0, 1 / Output: 1, 0
AND	The output is 1 only when both inputs are 1, otherwise the output is 0.		Input: 0 0, 0 1, 1 0, 1 1 / Output: 0, 0, 0, 1
OR	The output is 0 only when both inputs are 0, otherwise the output is 1.		Input: 0 0, 0 1, 1 0, 1 1 / Output: 0, 1, 1, 1
NAND	The output is 0 only when both inputs are 1, otherwise the output is 1.		Input: 0 0, 0 1, 1 0, 1 1 / Output: 1, 1, 1, 0
NOR	The output is 1 only when both inputs are 0, otherwise the output is 0.		Input: 0 0, 0 1, 1 0, 1 1 / Output: 1, 0, 0, 0
XOR	The output is 1 only when the two inputs have different value, otherwise the output is 0.		Input: 0 0, 0 1, 1 0, 1 1 / Output: 0, 1, 1, 0
XNOR	The output is 1 only when the two inputs have the same value, otherwise the output is 0.		Input: 0 0, 0 1, 1 0, 1 1 / Output: 1, 0, 0, 1

Figure 1: Portes logiques classiques

Il existe plusieurs variantes de portes à deux bits et celles-ci peuvent être combinées pour créer de nouvelles fonctions logiques. Le concept de jeu (ou ensemble) de **portes universelles** fait référence à des portes qui, à elles seules, peuvent reconstituer tous les résultats des autres portes. Généralement il suffit d'un petit nombre de portes pour constituer un tel ensemble universel et de plus il peut y avoir plusieurs combinaisons possibles. Par exemple, on peut montrer que la porte NOT et la porte AND forment ensemble un jeu de portes universelles. De même, la porte NAND elle-même est universelle, tout comme la porte NOR.

Les portes quantiques sont aux ordinateurs quantiques[232] ce que les portes logiques booléennes sont à l'informatique traditionnelle : les unités de calcul de base. Une porte quantique effectue des opérations élémentaires sur les qubits[233], comme une porte logique classique opère sur les bits ordinaires.

[231] Porte à une seule entrée.
[232] Ceux construits sur la base d'un circuit quantique, par opposition aux ordinateurs adiabatiques ou à recuit quantique.
[233] Système physique codant une variable quantique.

Les opérations appliquées aux qubits relèvent de l'algèbre linéaire et se formalisent par des multiplications de matrices. L'état d'un qubit est représenté par un vecteur de dimension 2, l'état de n qubits par un vecteur (registre) de dimension 2^n. Appliquer une porte quantique revient à multiplier la représentation vectoriel du qubit par la matrice caractéristique de cette porte. La taille de la matrice dépend du nombre de qubits en entrée de l'opération. Les portes communes fonctionnent avec 1 à 3 qubits en entrée. La représentation d'une porte à une entrée est une matrice 2x2 de nombres complexes comme représentées ci-dessus. Une porte à deux entrées est quant à elle caractérisée par une matrice 4x4, et d'une façon générale une porte opérant sur n qubits sera formalisée par une matrice de dimension $2^n x 2^n$.

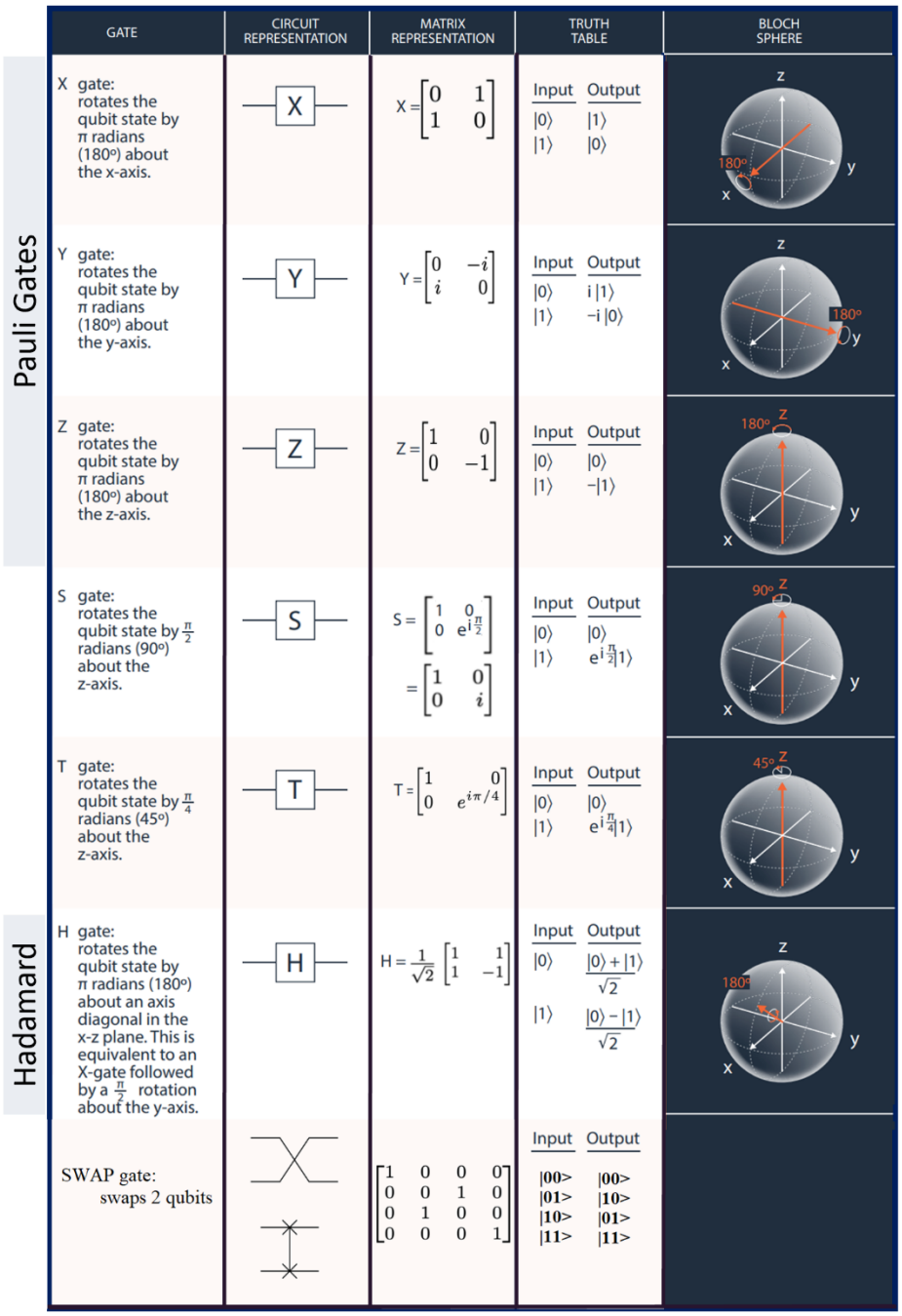


Figure 2: Quelques portes quantiques

Ces matrices ont la particularité d'être **unitaires**[234]: multipliées par leurs matrices adjointes, elles donnent la matrice identité. Les portes quantiques sont conçues pour modifier l'information des qubits

[234] A ne pas confondre avec unaire : à 1 entrée.

sans la lire et donc la détruire. Toutefois la mesure du résultat, intervenant en fin de calcul, détruira l'état quantique du qubit mesuré. Pour les portes unaires, les vecteurs bidimensionnels représentant l'état des qubits sont multipliés par des matrices unitaires de dimension 2x2. L'opération engendre une rotation du vecteur (visualisable dans la sphère de Bloch) représentant le qubit en état de superposition. Le module du vecteur reste égale à 1.

Quelques-unes des portes les plus communes sont présentée ci-dessous. La liste n'est pas exhaustive. Les portes unaires sont les trois portes de Pauli X, Y Z, les rotations S, T et la porte d'Hadamard H (Figure 2).

La porte H (Hadamard) est l'une des portes les plus utilisées, car c'est par son action qu'un algorithme peut générer des superpositions d'états dans un registre de qubits (Figure 3)

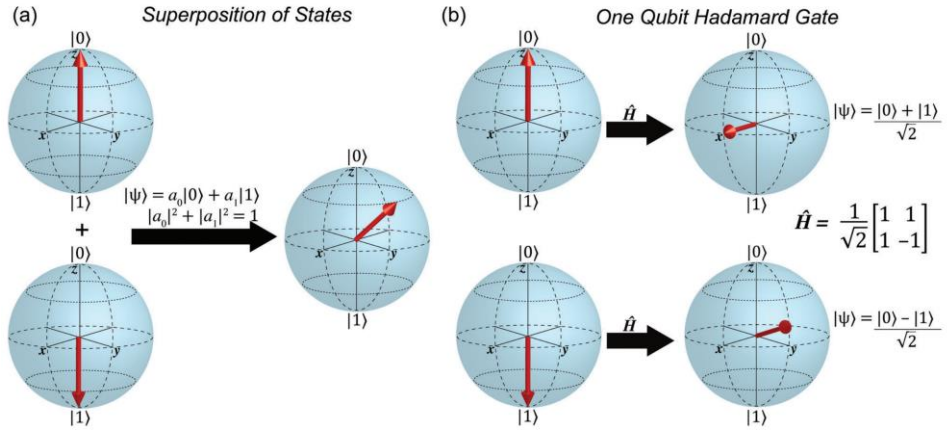


Figure 3: Illustration de l'action de la porte H qui transforme l'état discret d'un qubit (|0⟩ ou |1⟩) en état superposé (Source : https://doi.org/10.1039/C5CS00933B)

Géométriquement, la porte effectue une rotation de 180° autour de l'axe diagonal X+Z. On peut vérifier sur la figure 4 qu'elle est sa propre inverse (i.e. HH= H^2=I) : si on l'applique deux fois à un qubit il reviendra à son état initial.

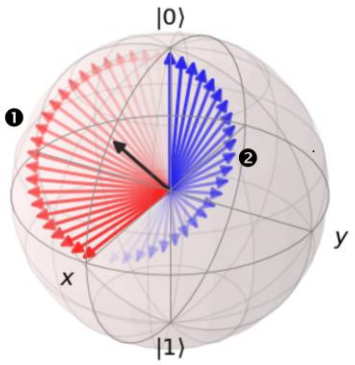


Figure 4: Application successive de 2 portes H (Source: https://physics.stackexchange.com

Les portes logiques quantique sont **réversibles**, elles ont autant d'entrées que de sorties. Les calculs peuvent être remontés en inversant simplement la séquence de portes appliquées. La réversibilité est lié à un principe thermodynamique et a pour conséquence qu'il n'y a pas d'augmentation de l'entropie du système au passage de la porte, autrement dit qu'il n'y a pas de dissipation ou consommation d'énergie. La consommation d'un circuit de portes quantiques, ou algorithme, est minime.

La figure 6 illustre deux portes binaires C-NOT et Z et une porte de Toffoli à 3 entrées. La porte C-NOT inverse la valeur d'un qubit d'entrée si le qubit de contrôle a pour valeur |1⟩ d'un autre qubit. C'est l'équivalent quantique de la porte logique XOR classique. La porte SWAP invertit les états quantiques de 2 qubits (non reprise ici). La figure 5 illustre que le résultat de deux manipulations (séries de portes) peut être identique même si les portes impliquées sont différentes (ici X = HZH).

Les portes sont classifiées selon deux groupes : Pauli et Clifford. Nous ne détaillerons pas ici la construction de ces groupes. Enfin comme en logique classique, on peut définir des ensembles de portes quantiques universelles dont la combinaison permet de répliquer l'action de n'importe quelle autres portes unitaires. Voici par exemple deux ensembles de portes universelles connus:

- Toffoli + Hadamard(H)
- CNOT + Hadamard+ T (45°)

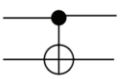
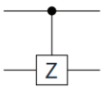
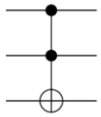
GATE	CIRCUIT REPRESENTATION	MATRIX REPRESENTATION	TRUTH TABLE
Controlled-NOT gate: apply an X-gate to the target qubit if the control qubit is in state $\|1\rangle$		CNOT = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	Input / Output $\|00\rangle$ / $\|00\rangle$ $\|01\rangle$ / $\|01\rangle$ $\|10\rangle$ / $\|11\rangle$ $\|11\rangle$ / $\|10\rangle$
Controlled-phase gate: apply a Z-gate to the target qubit if the control qubit is in state $\|1\rangle$		CPHASE = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	Input / Output $\|00\rangle$ / $\|00\rangle$ $\|01\rangle$ / $\|01\rangle$ $\|10\rangle$ / $\|10\rangle$ $\|11\rangle$ / $-\|11\rangle$
Toffoli Toffoli gate: (CCNOT, CCX, TOF) The Toffoli gate is a 3-bit input and 3-bit output logic gate. If the first two bits are equal to 1, the third bit is inverted.		TOF = $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	Input / Output |000> / |000> |001> / |001> |010> / |010> |011> / |011> |100> / |100> |101> / |101> |110> / |111> |111> / |110>

Figure 6: Quelques portes quantiques (suite)

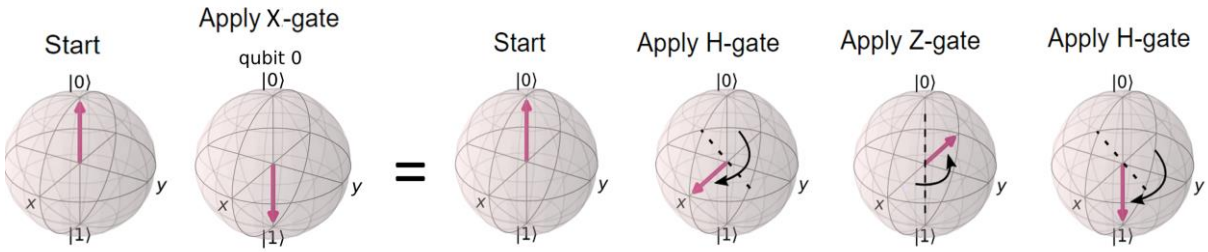
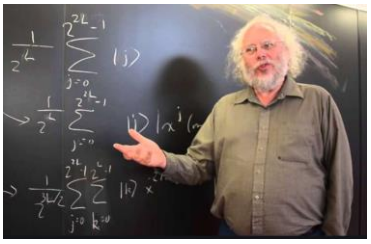


Figure 5: La séquence de portes H Z et H est équivalente à la porte X (i.e.X = HZH) (Source: IBM Qiskit)

- ANNEXE 7 - QUELQUES ELEMENTS SUR L'ALGORITHME DE SHOR (1994)



La factorisation de grands nombres entiers en nombres premiers est à la base de certaines des méthodes de chiffrement à clé publique (e.g. protocole RSA) largement utilisées pour la sécurisation des communications en particulier sur Internet pour protéger par exemple les transactions du commerce électronique. Ce problème d'arithmétique est particulièrement ardu à résoudre pour un ordinateur conventionnel lorsque le nombre à factoriser est grand. Cela garantit la robustesse du protocole face à une attaque malveillante.

Quels sont les facteurs premiers du nombre N = 507 906 452 803 ?
Réponse : N = 566 557 x 896 479 …
pas évident et encore N est petit ici…
une clé RSA-2048 a 617 chiffres décimaux (2048 bits)

Peter Shor proposa en 1994 un algorithme[97] qui, s'il existait un processeur quantique (universel à portes) capable de l'exploiter, permettrait de factoriser des grands nombres entiers N exponentiellement plus vite (Figure 1) qu'avec les algorithmes traditionnels existants, et donc constituerait une menace pour la méthode d'encryptage RSA et l'ensemble des communications l'utilisant.

L'algorithme de Shor utilise la transformée de Fourier (Figure 2) qui est fréquemment utilisée en mathématiques, physique et informatique. La transformée de Fourier classique permet d'identifier les fréquences (ou périodes) qui composent un signal tandis que la version quantique ne permet d'identifier que la fréquence (période) ayant l'amplitude la plus forte mais ce qui est suffisant pour le cas présent. La figure 3 en illustre le circuit quantique de la transformée de Fourier quantique (***QFT***).

Le principe mis en œuvre dans la résolution du **problème de factorisation** consiste à l'**assimiler** à un problème de **recherche de la période** d'une fonction particulière issue du théorème d'Euler (important théorème de la théorie des nombres).

La figure 4 illustre les étapes suivies par l'algorithme de Shor pour décomposer un nombre N en ses facteurs p et q. L'étape délicate est l'étape n°2, qui consiste à **rechercher la période**[235] **r** (nombre entier) de la fonction

$$f(x) = b^x \bmod N$$

issue du théorème d'Euler où x est entier, N est le nombre à factoriser, et b un nombre convenable-

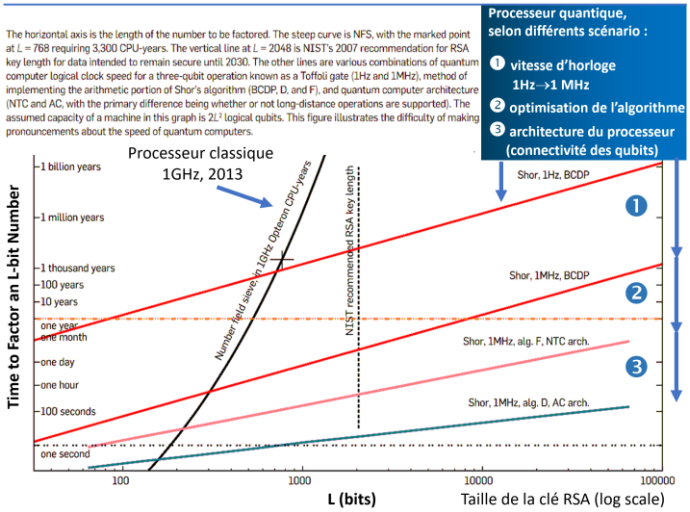


Figure 1:Comparaison du temps théorique nécessaire pour la résolution du problème de factorisation d'un nombre de L bits entre un ordinateur classique de référence et un ordinateur quantique suivant différents scénatios (amélioration de la vitesse d'horloge, logiciel, architecture) (Source: d'après Van Meter, 2013)

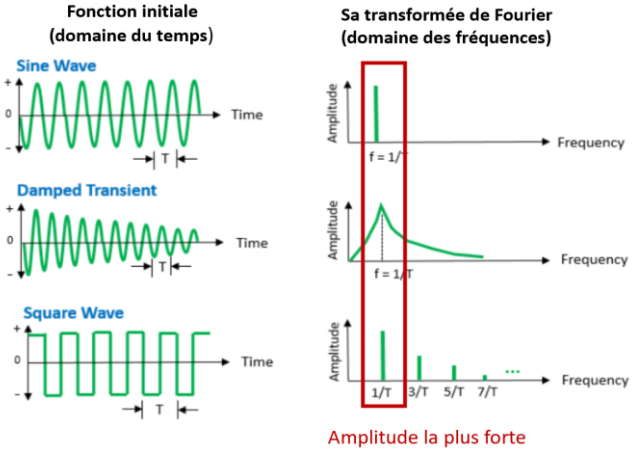


Figure 2: Exemples de transformée de Fourier

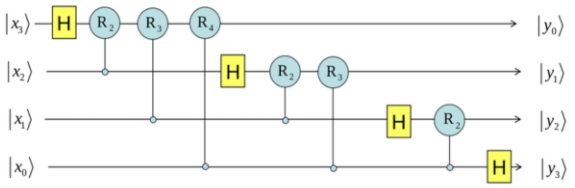


Figure 3: Circuit quantique de l'algorithme QFT (Fourier) sur 4 qubits (Source: Do Ngoc Diep)

[235] La période d'une fonction est la plus petite valeur r telle que la fonction se répète f(x+r)=f(x).

ment choisi et « mod » la relation de congruence[236] ou modulo. Une propriété arithmétique de la fonction $f(x)$ est qu'il suffit de résoudre l'équation en x, $b^x mod\ N = 1$ (qui s'écrit aussi $b^x \equiv 1\ mod\ N$) pour trouver la période (x=r).

Un algorithme classique calculerait la fonction pour chaque entier x successif afin de trouver celui qui vérifie f(x) = 1 (voir l'exemple pour N=15 - encadré step 2 - Figure 4), alors qu'en exploitant les propriétés du calcul quantique, l'algorithme de Shor est beaucoup plus efficace dans cette étape. Ses performances sont fortement reliées à :

- la capacité des qubits d'un ordinateur quantique d'être en état de superposition, ce qui permet ici de **calculer en parallèle toutes les valeurs d'une fonction** périodique $f(x) = b^x \bmod N$ pour toutes les valeurs de x puis trouver la période r grâce à la **transformée de Fourier quantique (QFT)**. C'est ce dont se charge le circuit quantique de la figure 4, le reste du workflow est classique.
- **sa nature probabiliste, comme beaucoup d'algorithmes quantiques,** et non pas déterministe. Il donne ses réponses avec des niveaux de probabilité associés. Toute l'astuce dans sa conception est de faire en sorte d'amplifier[237] l'amplitude de probabilité de la réponse (ici la période recherchée) la plus probable. L'algorithme de Shor cherche à déterminer la période d'une fonction et une fois qu'il l'a identifiée il fait en sorte qu'à la lecture final du résultat on obtienne la bonne réponse avec une grande probabilité.

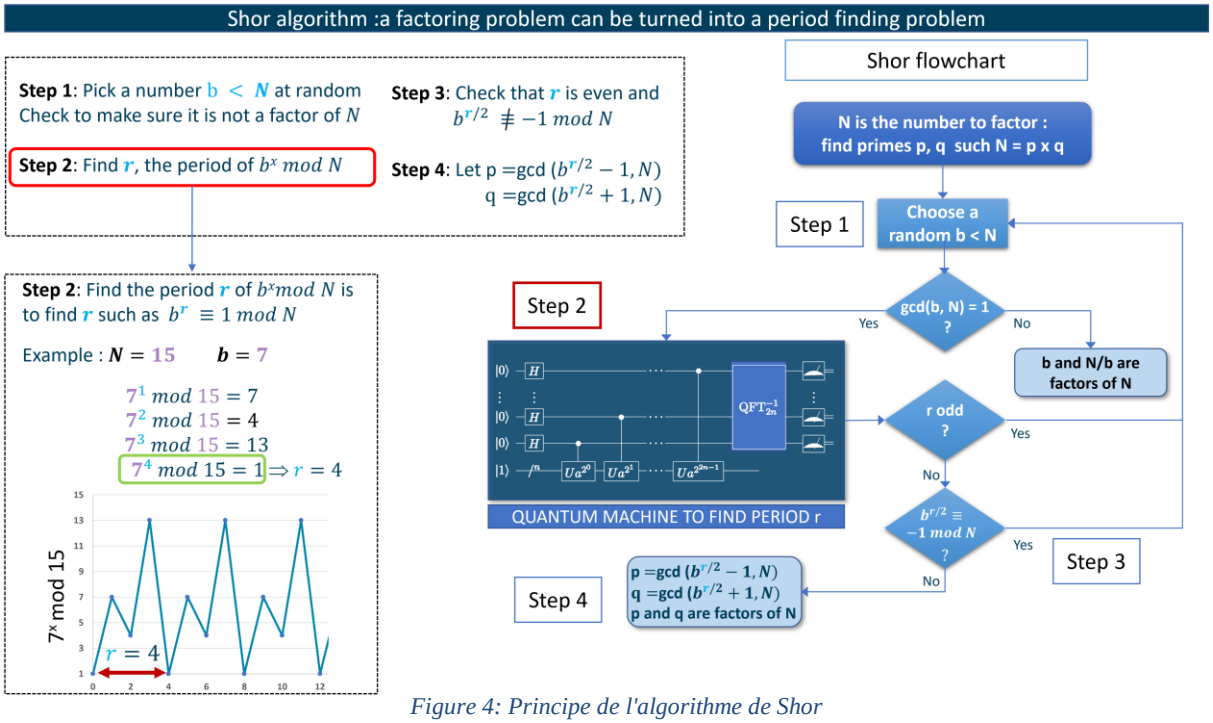


Figure 4: Principe de l'algorithme de Shor

Pour relativiser, il est important de se rendre compte que la taille de l'ordinateur quantique requise pour être utilisable dans le contexte de l'algorithme de Shor est beaucoup plus importante que celles des machines existantes.

Il faut à peu près deux fois plus de qubits logiques que de bits utilisés pour la clé RSA (voir [232], en fait : *2n+2,* avec n = taille en bits de la clé RSA). Ainsi pour factoriser une clé RSA de 2 048 bits, norme de sécurité actuelle, il faudra disposer d'au minimum 4 098 qubits logiques. **Compte tenu de la qualité des qubits actuels**, c'est en fait des milliers voire des dizaines de milliers de qubits physiques par qubits logiques qu'il faudrait et donc **casser une telle clé requerrait de l'ordre de 10^7 qubits** !

[236] L'opération modulo (abrégée en "mod") consiste simplement à trouver le reste en divisant un nombre par un autre. Par exemple, 17 mod 5 = 2 puisque 17÷5=3 et reste 2

[237] L'augmentation de l'amplitude de probabilité se construit grâce aux phénomènes d'interférences constructives (resp. destructives) pour augmenter (resp. diminuer) l'amplitude de probabilité d'une réponse correcte (resp. incorrecte).

Mais si cela était faisable, il ne suffirait que 8 heures selon les dernières estimations avec 20 millions de qubits [100].

Par ailleurs, notons qu'en théorie, l'algorithme de Shor peut être utilisé pour casser les cryptosystèmes à base de courbe elliptique (type ECDH) également très utilisés au prix d'un besoin en ressources encore plus élevé.

Coté records, le plus grand nombre qui ait été factorisé avec un ordinateur quantique à portes est 21 =3×7 en 2012[233]. En 2019, une équipe de chercheurs a échoué dans la factorisation du nombre 35 sur un ordinateur d'IBM comportant 16 qubits en raison du taux d'erreurs trop élevés des portes quantiques[234].

Signalons enfin qu'une autre technologie de calculateurs quantiques, celle des ordinateurs à recuit quantique (annealer), a été testé sur de la factorisation. Très spécifiques, ces ordinateurs sont potentiellement utiles pour résoudre certains problèmes d'optimisation. Or la factorisation peut être transcrite en un problème de minimisation, totalement différent de l'algorithme de Shor. C'est ce qui fut utilisé en 2020 par une équipe de chercheurs chinois et a mené à la factorisation du nombre 1 028 171[235].

- ANNEXE 8 - QUELQUES MOTS SUR LES OUTILS LOGICIELS

Un programme informatique est une liste d'instructions permettant à un ordinateur d'exécuter une tâche spécifique. Pour cela, le code source du programme aura souvent implémenté un algorithme conceptualisant la tâche à effectuer.

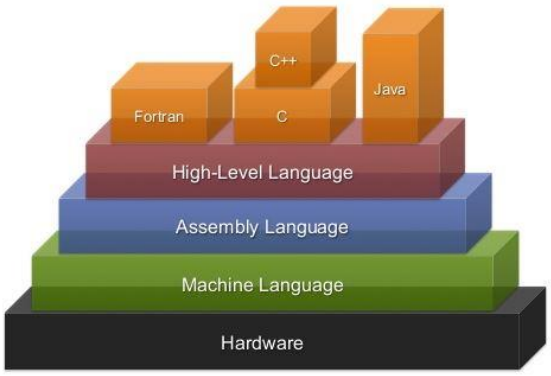


Figure 1: Les différentes couches (pile) de langages d'un ordinateur classique

Le développement et l'exécution d'un programme sur un ordinateur classique impliquent l'utilisation de différentes couches logicielles (ou langages), organisées en niveaux d'abstraction (Figure 1).

En bas de la pile, le langage machine, le seul compris par le processeur (CPU) de l'ordinateur. Juste au dessus le langage assembleur puis encore une ou plusieurs couches apportant chacune un niveau d'abstraction croissant. Les langages de haut niveau ont l'avantage de permettre l'écriture de programme sans avoir à se soucier de leur retranscrption en langage machine et ils peuvent donc fonctionner sur des machines ayant des processeurs différents. Enfin, c'est le rôle des compilateurs de transformer un code source écrit dans un langage de haut niveau, en un code objet généralement écrit en langage de plus bas niveau.

Comme nous l'avons vu §4.3, les ordinateurs quantiques sont aujourd'hui généralement contrôlés par des ordinateurs classiques. L'architecture d'un tel ensemble est complexe. La figure 2 en détaille les principaux blocs, divisés en couches réparties sur les machines quantiques (QPU) et classiques (CPU) (bleu et rose respectivement).

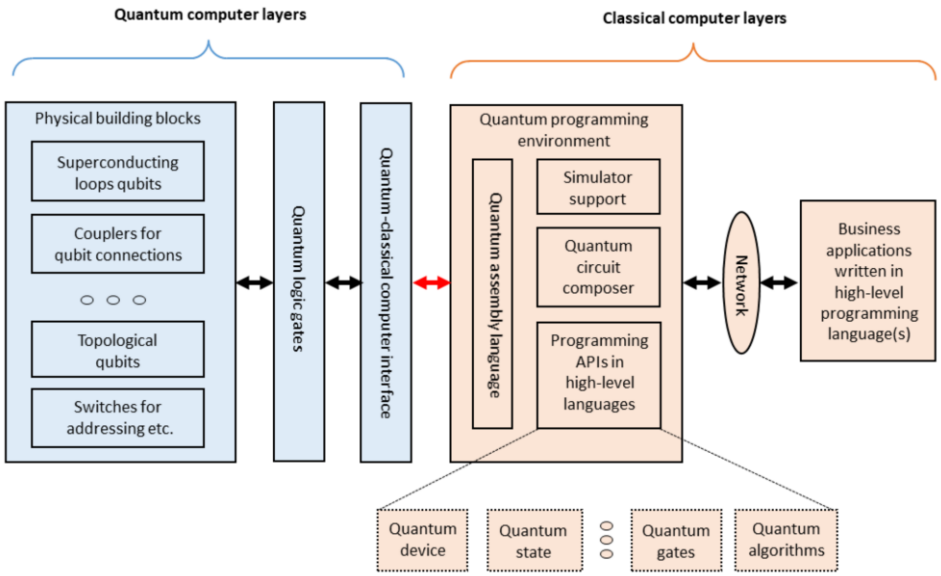


Figure 2: Architecture d'un système informatique quantique (Source: [233])

Sans entrer dans les détails qui pourront être retrouvés dans les références [236] ou [237], notons les points importants suivants :

- Pour fonctionner, un ordinateur quantique doit intégrer plusieurs couches d'une nouvelle pile technologique (*stack*), comprenant à la fois des composants matériels et logiciels.
- Les logiciels quantiques (couches) jouent, et vont jouer, un rôle essentiel dans l'exploitation du plein potentiel des ordinateurs quantiques (Annealers, Ordinateurs NISQ, puis universel FTQC…). Par exemple, lorsqu'un compilateur quantique retranscrit un programme quantique écrit dans un langage

de haut niveau, il doit s'assurer de l'optimisation des séquences de portes quantiques utilisées, en supprimant par exemple celles qui ne changent pas l'état d'un qubit, comme deux portes de Hadamard appliquées à la suite. Il peut aussi tenter de minimiser le nombre d'étapes de calcul en réarrangeant les portes. Signalons à ce niveau, que le rôle d'un compilateur quantique est en dernier lieu de retranscrire les portes en pulsations contrôlant les qubits (e.g. pulses micro-ondes pour des qubits supraconducteurs).

- Faire fonctionner un algorthime quantique sera d'autant plus complexe qu'à ce jour, c'est au moins sept types de supports physiques de qubits (§3.2) qui sont explorés pour la construction d'ordinateurs quantiques. Leurs niveaux de maturité technologique sont très différents, tout comme leurs caractéristiques techniques (temps de cohérence, connectivité entre qubits, possibilité d'appliquer ou pas telle ou telle porte logique quantique).

  Dans ce contexte, certains estiment qu'il est important de pouvoir offrir des plateformes logicielles agnostiques aux types de qubit. Dans ce cas, les compilateurs devront alors optimiser les opérations à mettre en œuvre lorsque certaines portes, nécessaires à l'implémentation d'un algorithme quantique, ne sont pas disponibles sur la plateforme cible (adaptation du jeu de portes universelles - Figure 3). A contrario, d'autres acteurs plaident pour le développement d'une architecture matérielle et logicielle très intégrée et spécifique à la technolgie de qubit employée, pour des raisons de performances.

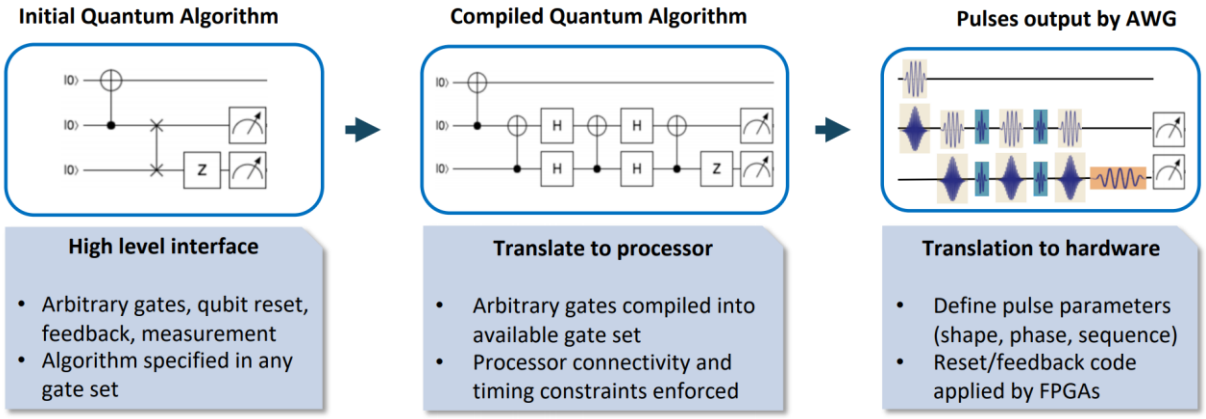


Figure 3: Pile de logiciels pour le développement (Source: How about quantum computing? , De Jong)

Tous ces élements, et bien d'autres encore, font du secteur du *software* quantique un secteur très dynamique. Celui-ci a été initialement poussé par l'emergence des langages de programmation quantiques (38 langages, open sources ou propriétaires, sont dénombrés dans [236] -Figure 5), mais il parait dorénavant primodial qu'une discipline complète de génie logiciel quantique soit développée dans un avenir proche. En effet, les problématiques liées au cycle de vie du logiciel s'appliqueront tout autant à l'informatique quantique (Figure 4) qu'elles ne s'appliquent à l'informatique classique (tests, maintenance…) [236].

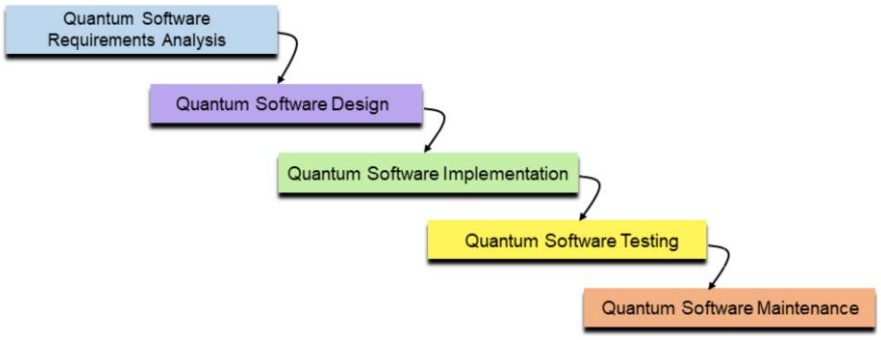


Figure 4: Cycle de vie du logiciel quantique (Source: [233])

Pour cela, l'industrie devrait pouvoir compter sur les multiples plans gouvernementaux lancés ces dernières années. L'axe de développement « formation et éducation » est généralement présent sur leur roadmap[71].

En attendant, le secteur est prêt à déployer largement ses premières solutions logicielles pour soutenir la concrétisation d'un premier avantage quantique. Il a de plus le support des investisseurs privés puisque, dans l'univers des startups de l'informatique quantique, ce sont les startups du *software* qui recueillent le nombre le plus important de transactions de capital-risque depuis trois ans (voir annexe 4).

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

Figure 5: Historique des langages de programmation quantique (Source: [236])

- ANNEXE 9 - PRINCIPAUX ALGORITHMES QUANTIQUES

Notre ambition n'est pas ici de détailler les 60 catégories d'algorithmes cataloguées sur le site https://quantumalgorithmzoo.org/ mais de donner quelques détails sur les algorithmes quantiques les plus marquants. A cette fin, il convient de considérer, d'une part, les algorithmes exploitables à l'ère des ordinateurs NISQ[238] qui seront les premiers systèmes quantiques à être disponibles dans un futur proche (0-5 ans) et, d'autres part, ceux destinés aux ordinateurs universels tolérants aux erreurs (FTQC/LSQC)[239] envisagés à plus long terme (10-15 ans).

Pour les ordinateurs **NISQ**[240], la principale qualité d'un algorithme sera sa **robustesse,** i.e. sa tolérance au bruit et aux erreurs quantiques. Une bonne analogie consiste à les considérer comme des algorithmes « chevaux de traits »(*workhorses* - Figure 1)[218].

Pour les **ordinateurs universels** tolérants aux erreurs (FTQC/LSQC), la qualité recherchée sera **l'accélération** apportée par rapport à un ordinateur classique lors de la résolution de problèmes plus ou moins courants. Ce sont les algorithmes « pur-sangs » (*purebreds*)[218].

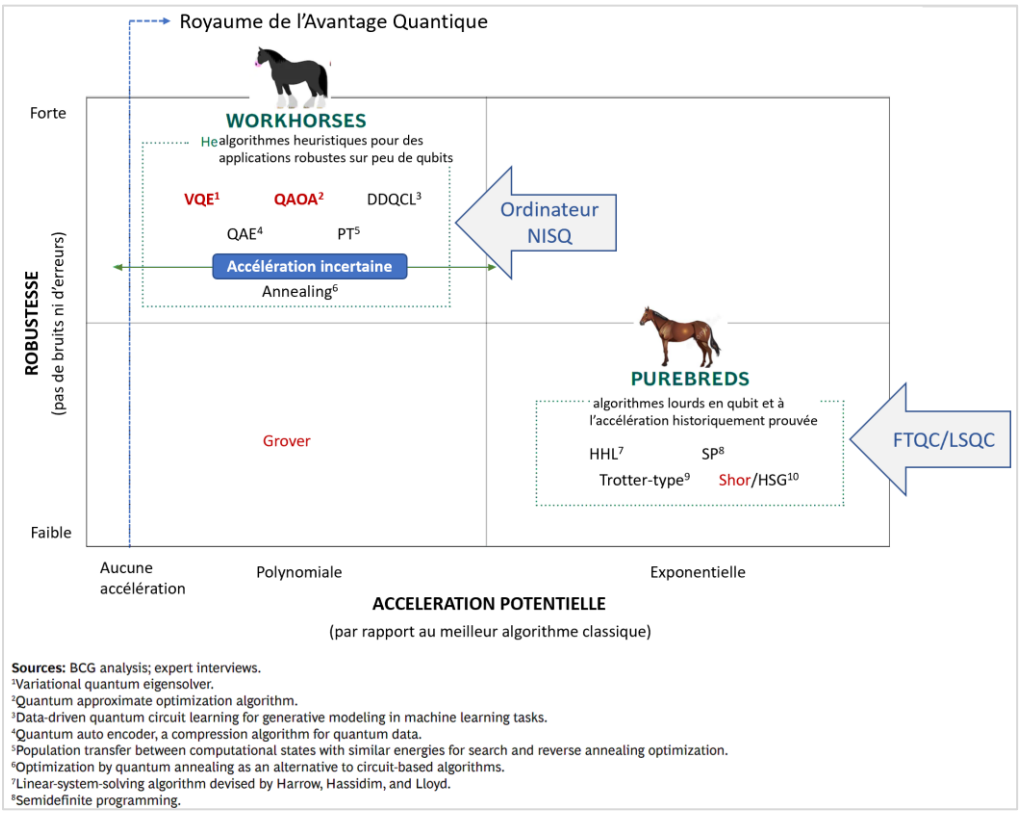


Figure 1: Les algorithmes « workhorses » domineront durant l'ère du NISQ (Source : d'après BCG)

1. Les algorithmes « workhorses » de l'ère du NISQ

Les annonces récentes de Google[241] ont ravivé l'intérêt pour les possibles réalisations accessibles aux ordinateurs quantiques actuellement disponibles. L'hypothèse la plus courante est que seuls des algorithmes résistants au bruit et aux erreurs seront mis en œuvre sur les ordinateurs quantiques à l'ère du NISQ, car la technologie des qubits n'est pas encore mature et la fidélité des portes quantiques limitée.

[238] Noisy Intermediate-Scale Quantum.
[239] Fault-Tolerant Quantum Computer / Large-Scale Quantum Computer.
[240] Disposant d'un taux d'erreurs suffisament bas grâce à des codes de corrections d'erreurs.
[241] Suprématie quantique de leur ordinateur quantique Sycamore, modélisation de molécules, etc…

Ces algorithmes pourront être équipés d'un système d'atténuation d'erreurs[242], mais leur principale caractéristique sera leur faible profondeur pour éviter que les erreurs ne s'accumulent trop et ne faussent les calculs(i.e. le nombre de portes -opérations- sera réduit). Ces algorithmes robustes (workhorses) devraient pouvoir fonctionner sur des machines ayant 50 à 100 qubits (les ordinateurs à recuit (annealer), bien que différents dans leur principe, entrent également dans cette catégorie). Le dilemme est que leurs performances de vitesse ne peuvent guère être prouvées avant qu'ils n'aient été soumis à des tests expérimentaux, si bien que les bénéfices par rapport auxmeilleurs algorithmes classiques restent incertains à ce jour[218].

La plupart des *workhorses*, existants aujourd'hui, s'intègrent dans une chaine de traitement hybride quantique/classique. C'est ainsi le cas des **algorithmes quantiques variationnels**, qui se positionnent d'emblée comme l'une des approches les plus prometteuses pour travailler avec les contraintes du NISQ sur des problématiques d'optimisation.

Le cœur de ces algorithmes est constitué d'un module effectuant des calculs sur un processeur quantique (Figure 2). Ce module est exécuté à plusieurs reprises en tant que sous-programme par un ordinateur classique qui est chargé de faire varier les paramètres d'entrée jusqu'à ce que le résultat souhaité soit atteint (objectif). Ces méthodes sont polyvalentes et plusieurs variantes sont à l'étude. Parmi beaucoup d'autres, on peut citer:

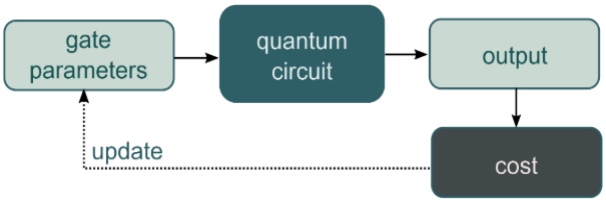


Figure 2: Principe des algorithmes variationnels (Source: xanadu.ai)

QAOA - *Quantum Approximate Optimisation Algorithm*[186] : cet algorithme peut être utilisé pour résoudre des **problèmes d'optimisation combinatoire**.

VQE - *Variational Quantum Eigensolver*[180] : cible les problèmes d'optimisation (assez généraux), ou de **simulation**, en particulier en chimie pour la recherche de niveaux d'énergie moléculaire[238].

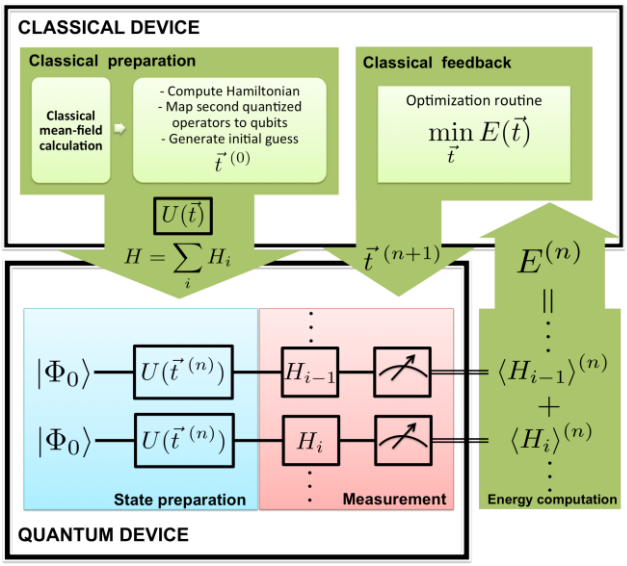


Figure 3: Principe de fonctionnement d'un algorithme VQE pour la recherche de niveaux d'énergie moléculaire (à partir de l'Hamiltonien[243] H du système) (Source: [238])

Toutes ces techniques ont déjà des applications commerciales potentielles, mais elles doivent encore faire leurs preuves face aux méthodes traditionnelles dans le cadre de problèmes d'une ampleur suffisante, voire, hors de portée des ordinateurs conventionnels.

[242] Les QECC (Quantum Error Code Correction) seront eux disponibles sur les ordinateurs universels.
[243] L'Hamiltonien formalise l'énergie totale du système quantique simulé et caractérise son évolution dans le temps.

Relayant les travaux sur les algorithmes variationnels, une activité de recherche croissante se cristallise sur le ***quantum machine learning*** (QML) - apprentissage par machine quantique.

L'objectif général de certaines des méthodes employées habituellement en ML est d'optimiser une fonction objective donnée. Il s'agit, par exemple, de trouver le minimum d'une fonction de coût mesurant l'adéquation d'un modèle de données aux données réelles. L'idée est ici encore d'utiliser conjointement un processeur quantique (QPU) et un processeur classique (CPU), avec un nombre minimal d'opérations effectuées sur le processeur quantique. Dans ce cadre hybride, la seule utilisation du processeur quantique est de préparer un état quantique donné, paramétré par un ensemble de paramètres variationnels et d'appliquer à la suite quelques opérations quantiques.

L'algorithme quantique variationnel nommé VQLS (Variational Quantum Linear Solver[239]), utilisant l'algorithme VQE, a été proposé récemment dans le but de résoudre des systèmes d'équations linéaires sur des machines NISQ plus efficacement que les algorithmes de calcul classiques. C'est une piste prometteuse puisque l'algorithme quantique le plus connu pour cette tâche est l'algorithme de HHL (abordé dans la section suivante), un *purebred*, qui n'est pas accessible aux ordinateurs NISQ.

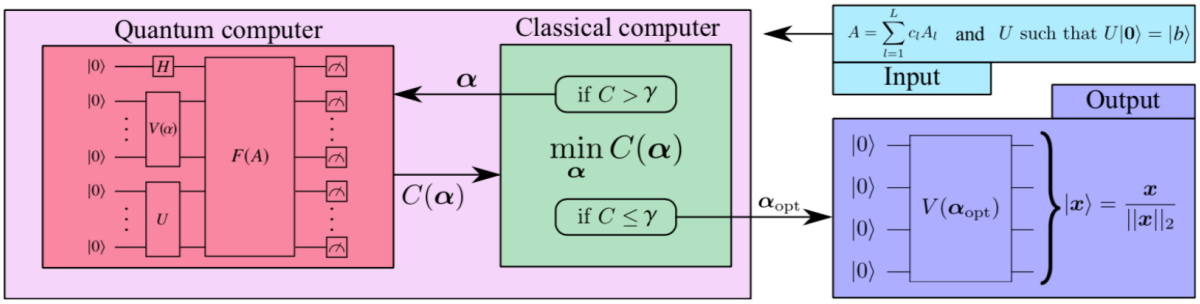


Figure 4: Principe de fonctionnement de l'algorithme VQLS (Source: [239])

La tableau de la figure 5 a été établi en 2017 dans [240]. Il synthétise les performances théoriques de certaines des autres méthodes explorées en machine learning en les associant à différentes techniques « habilitantes » (les accélérations en $log(N)$ sont plus importantes que celle en $\sqrt{N}$). Notons que certaines de ces propositions ne sont pas exploitables à l'heure actuelle. L'algorithme HHL ou la mémoire quantique (QRAM) ne sont aujourd'hui pas disponibles.

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

Figure 5: Accélération potentielle de quelques techniques de QML (Source: [240])

À ce jour, il n'existe aucune preuve concrète d'accélération par rapport aux meilleurs algorithmes classiques, d'autant plus que ceux-ci évoluent également dans le même temps. Parfois sont-ils même inspirés par des algorithmes quantiques comme c'est le cas de l'algorithme « classique » de recommandation[244] (ML) proposé par E. Tang[192], suite aux travaux publiés par I. Kerenidis et al. sur le même sujet mais destinés à un ordinateur quantique[187]. Ceci dit, la recherche progresse rapidement et plusieurs points d'amélioration ont été identifiés (voir §4.3.5.5). Souvenons-nous qu'il y a moins de 10 ans l'IA et le ML n'étaient pas où ils en sont actuellement. Les toutes prochaines années devraient être riches en enseignements.

[244] Les systèmes de recommandation a pour but de prédire la préférence qu'un utilisateur accorderait à un objet (film, livre…).

Pour terminer, la figure 6 resitue quelques-uns des algorithmes et problèmes mathématiques mentionnés. Comme nous l'avons vu au §4.3.5.6, les champs d'applications de la simulation, de l'optimisation, du machine learning s'étendent à de nombreux secteurs d'activité. Par conséquent, si un avantage, ou plutôt, une valeur quantique devait émerger, ce serait dans l'un d'entre eux: chimie, transport, énergie, finance...

Algorithm	Breakthrough	Advantage	Challenge	Chemical Simulation	Scenario Simulation	Optimization	AI
VQE Variational Quantum Eigensolver Uses energy states to calculate the function of the variables to optimize	Optimizes compute-intensive functions	Efficiently calculates complex portion of simulations	Qubit number increases significantly with problem size	●		▲	
QAOA Quantum Approximate Optimization Optimize combinatorial style problems to find solutions with complex constraints	Simplifies analysis clauses for constraints	Robust optimization in complex scenarios	Ability to expand to more optimization classes			▲	
QAE Quantum Amplitude Estimator Create simulation scenarios by estimating an unknown property, Monte Carlo style	Handles random distributions, instead of only sampling	Solve dynamic problems quadratically speeding up simulations	High quantum volume required for good efficiency		■	▲	◆
QSVM Quantum Support Vector Machines Supervised machine learning for high dimensional problem sets	Maps data to larger dimensions to enable separation	Better separate data points and achieve more accuracy	Runtime can be slowed by data structure			▲	◆
HHL Harrow, Hassidim, and Lloyd Estimate the resulting measurement of large linear systems	Solve high dimensional problems	Exponential speedup of matrix calculations	Hard to satisfy prerequisites				◆

Figure 6: Cas d'usage et algorithme (Source: Roadmap IBM)

2. Les algorithmes « purebreds » pour les ordinateurs tolérants aux fautes

La promesse à long terme des ordinateurs quantiques réside dans leur capacité à exécuter certains algorithmes quantiques offrant théoriquement des accélérations remarquables (exponentielles dans certains cas) par rapport aux algorithmes conventionnels[241]. Malheureusement, les ordinateurs quantiques universels (FTQC/LSQC) nécessaires pour effectuer ces calculs, ne requérant ni bruits, ni erreurs, ne seront pas disponibles avant au moins une décennie[245]. En effet, la mise en œuvre des techniques de corrections d'erreurs, utilisées pour réduire les taux d'erreurs, nécessite des centaines voire des millions de qubits (§4.3.4.2), ce qui dépasse de loin des capacités actuelles de la technologie. Par ailleurs, certains algorithmes impliquent aussi le développement d'une nouvelle mémoire quantique, la QRAM, qui n'existe pas.

La figure 1 positionne certains de ces algorithmes « purebreds » dont la puissance de calcul exponentielle est prouvée sur le papier. On y retrouve par exemple **l'algorithme de factorisation de P. Shor** susceptible d'être utilisé en cryptanalyse et qui menace la sécurité de certaines communications chiffrées (voir l'annexe 7 pour des détails sur son fonctionnement).

Mentionnons également les algorithmes *purebreds* conçus pour résoudre des problèmes d'optimisation semi-définie positive[246] (SP) [242], ou ceux utilisant la décomposition de Trotter permettant de simuler la dynamique d'un système à n-corps, particulièrement utile pour la simulation de la dynamique moléculaire[243].

Certains des algorithmes quantiques « purebreds » sont utilisés comme des sous-fonctions (primitives) d'autres algorithmes. Une liste des plus importants est présentée dans la section suivante.

[245] Les avis sur le sujet sont très variables. Voir par ex. https://globalriskinstitute.org/publications/quantum-threat-timeline/
[246] Qui généralisent les problèmes d'optimisation linéaire

- **Transformée de Fourier quantique (QFT)** : Cet algorithme est la base d'un certain nombre d'algorithmes dont le célèbre algorithme de Shor[247] pour la factorisation des nombres entiers (voir l'annexe 7). C'est l'implémentation quantique de la transformée de Fourier discrète classique. Il permet de passer d'une base de représentation naturelle des données (selon axe Z), à une base de représentation qui utilise la phase des qubits (angle de rotation autour de l'axe Z dans la sphère de Bloch, i.e. plan équatorial XY - Figure 7)

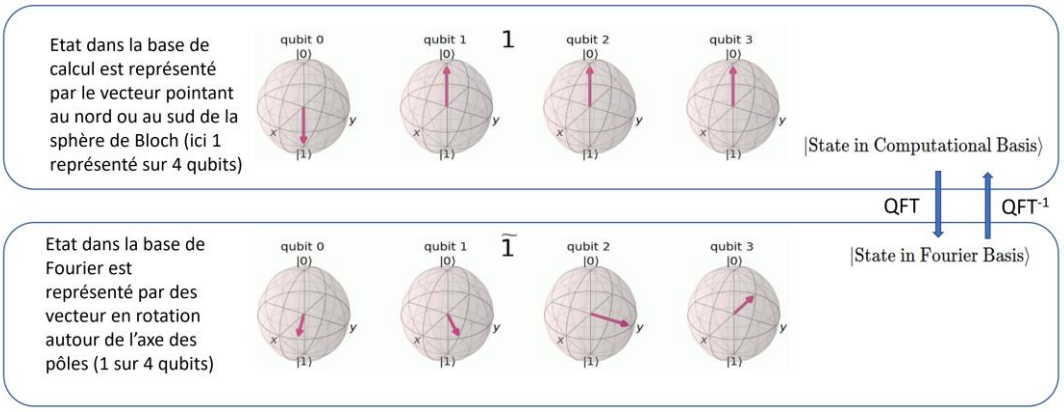


Figure 7: Transformée de Fourier quantique (Source: d'après IBM Qiskit - https://qiskit.org)

- **Estimation de phase quantique (QPE)**: cet algorithme[248] est une primitive utilisée dans beaucoup d'autres algorithmes, incluant la simulation quantique. Il fait lui-même appel à la transformée de Fourier quantique (Figure 8).

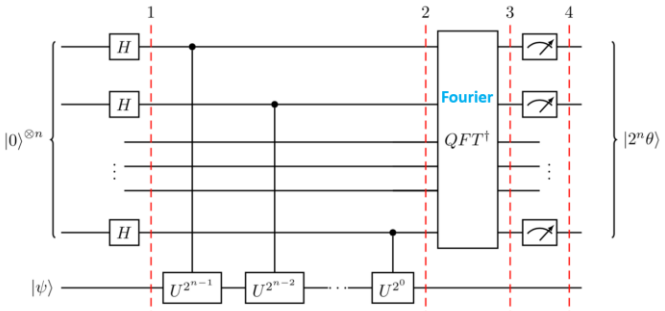


Figure 8: Algorithme QPE (Source: IBM Qiskit)

- **Harrow Hassidim Lloyd (HHL)** [244]: cet algorithme permet de résoudre, sous certaines conditions, assez restrictives, un système d'équations linéaires A.X =B en un temps proportionnel à log(N) où N est le nombre d'inconnues alors que les meilleurs algorithmes conventionnels ont une

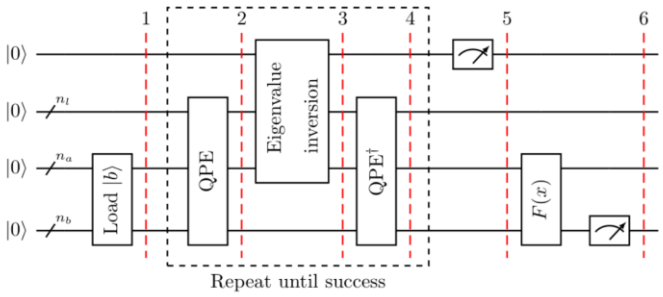


Figure 9: Algorithme de HHL (Source: IBM Qiskit)

[247] En fait c'est l'algorithme QPE qui utilise lui-même QFT que l'on retrouve dans l'algorithme de Shor (QFT → QPE→Shor).
[248] QPE permet d'estimer la valeur propre (ou sa phase, ce qui, dans ce cas précis, est équivalent) d'un opérateur unité associée à un vecteur propre donné. Mathématiquement, étant donné un opérateur unitaire U (matrice), l'algorithme estime **θ** tel que $U|\psi\rangle=e^{2\pi i\theta}|\psi\rangle$, où $|\psi\rangle$ est un vecteur propre et $e^{2\pi i\theta}$ est la valeur propre correspondante (Source : Wikipedia).

complexité entre N^2 et N^3dans les cas les plus généraux. Il fait appel à l'algorithme d'estimation de phase quantique (QPE - Figure 9) et, peut intervenir comme primitive dans différents algorithmes nécessitant la résolution de systèmes d'équations linéaires, ou l'inversion de matrice comme ceux mis en œuvre dans les réseaux de neurones (ML).

3. Les autres algorithmes pour les ordinateurs tolérants aux fautes (FTQC)

Tous les algorithmes quantiques ne fournissent pas une accélération exponentielle par rapport à un équivalent classique. C'est le cas de l'algorithme de Grover[166], proposé en 1996.

Celui-ci résout le problème d'inversion de fonction en un temps sous-linéaire (i.e. sous la droite O(n) - Figure 10). Ses applications sont multiples. Il permet de réaliser une recherche dans une base de données non structurée (i.e. non triée) en offrant un gain en temps quadratique par rapport à une heuristique traditionnelle. Ainsi, peut-il être utilisé en cryptographie pour craquer des codes de chiffrement, comme le fait l'algorithme de Shor (voir §4.2.1), mais avec un avantage bien moindre[249].

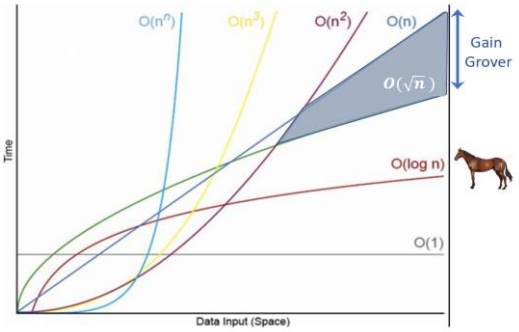


Figure 10: Complexité en temps fonction de la taille du problème

L'exemple qui illustre souvent cet algorithme est la recherche du nom associé à un numéro de téléphone donné dans un annuaire téléphonique ordinaire classé par ordre alphabétique. Les seules façons classiques de procéder sont de faire, soit une recherche exhaustive, soit, une recherche aléatoire. Dans tous les cas il faudra en moyenne N/2 tentatives pour trouver le bon nom dans un annuaire de N entrées. La recherche de Grover est capable de retrouver le nom avec seulement $\sqrt{N}$ essais.

Pour fonctionner, l'algorithme intègre deux éléments principaux(Figure 11)[250] :

1. Un « **oracle** », sorte de « boite noire quantique», dont le rôle est d'indiquer si un ensemble de qubits en entrée correspond au critère de recherche ou pas,
2. Un algorithme d'**amplification d'amplitude**, indépendant de l'oracle, qui permet d'exploiter l'information donnée par la boîte noire. C'est cette procédure qui nécessite $\sqrt{N}$ itérations.

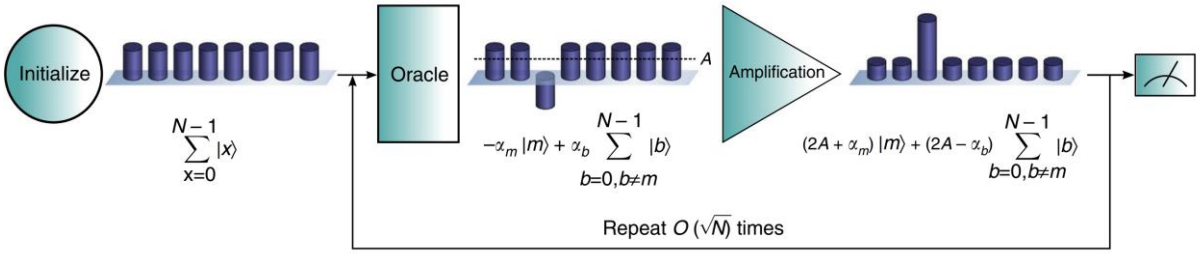


Figure 11: Algorithme de Grover (Source: C. Figgatt et al. Published in Nature Communications)

Mathématiquement, l'oracle se définit par une fonction $f_{critère}(x)$ qui indique si un état x vérifie le critère de recherche.

$$f_{critère}(x) = \begin{cases} 1, & \text{si } x \text{ vérifie le critère} \\ 0, & \text{sinon} \end{cases}$$

[249] L'algorithme quantique de recherche (par « force brute ») de Grover, utilisable pour décrypter des messages chiffrés par clé symétrique ne génère, par rapport à une méthode traditionnelle, qu'une accélération quadratique (temps de calcul augmente en $\sqrt{N}$, au lieu de N) et non pas exponentielle (log(N) au lieu de N) comme celui de Shor, applicable aux clés asymétriques.
[250] Source : Wikipedia https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Cet oracle est bien sûr capable d'accepter une superposition d'états en entrée, et donc de contrôler simultanément le critère pour tous les états de la superposition. Si l'on reprend l'exemple de l'annuaire, la fonction $f_{critère}(x)$ compare le numéro de téléphone recherché (critère) et celui qui lui est soumis (x) pour répondre « 1 » s'ils sont identiques et « 0 » sinon. L'oracle étant quantique, il peut évaluer cette fonction simultanément pour les 2^N états d'un registre[251] de N qubits. Il répondra donc « 1 » une fois et des « 0 » autrement.

A chaque réponse de l'oracle, l'objectif est de savoir si un « 1 » est sorti et, si oui, à quelle entrée il correspond. A cette fin, Grover utilise l'amplification d'amplitude qui va progressivement augmenter l'amplitude de probabilité associée à la combinaison de qubits codant le bon résultat[252] jusqu'à atteindre une valeur de 100% et faire converger les autres combinaisons de qubits vers 0 (Figure 12). A la fin du processus, la lecture de l'état quantique du système devrait alors donner la bonne réponse avec une probabilité proche de 100%.

Les différentes étapes de la procédure sont les suivantes[253]:

1. Préparation d'un état équisuperposé (toutes les entrées d'un annuaire y sont codées avec le même poids)
2. L'algorithme fait en sorte que l'oracle indique sa réponse en inversant la phase de l'état qui vérifie le critère
3. L'algorithme applique ensuite l'opération d'amplification d'amplitude, qui effectue un miroir des amplitudes autour de la moyenne des amplitudes. Cela a pour effet d'amplifier l'état cible, et de diminuer les autres états (Figure 12).
4. On itère les étapes 2 et 3, k fois avec $k = \frac{\pi}{4}\sqrt{2^N}$
5. Lecture du résultat

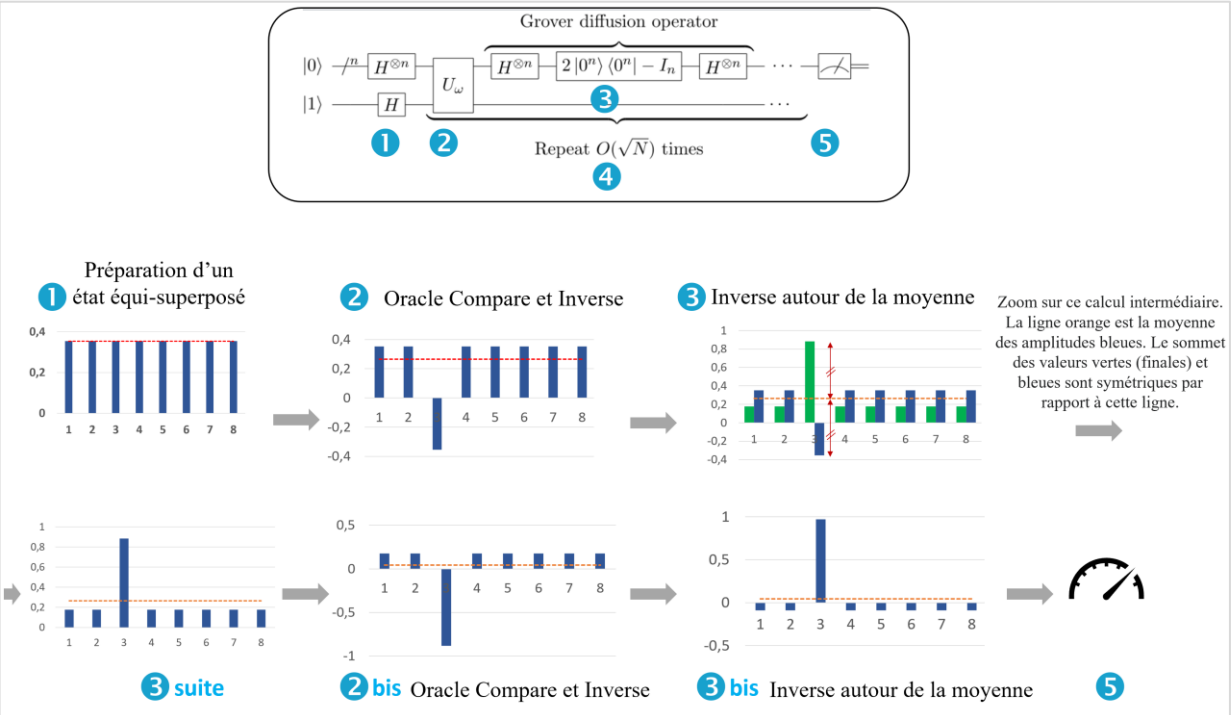


Figure 12: Exemple de fonctionnement de l'algorithme de Grover

[251] Pour reprendre l'exemple de l'annuaire, c'est dans les 2^N états du registre de qubits que sont codés toutes des entrées de l'annuaire. Si l'on a 3 qubits, on peut coder 8 index d'entrée dans l'annuaire |000⟩,|001⟩…|111⟩ (i.e états de |0⟩→|7⟩).
[252] Codant l'index du numéro de téléphone
[253] Source : Wikipedia https://fr.wikipedia.org/wiki/Algorithme_de_Grover

L’algorithme de Grover, comme certains autres algorithmes, peuvent être utilisés comme primitives d’autres algorithmes, en voici une liste non exhaustive.

Algorithmes quantiques « primitif » avec accélération quadratique

- **Amplification d’amplitude :** Cet algorithme est utilisé dans l'algorithme de recherche de Grover et permet d’avoir un gain de performance quadratique par rapport à des algorithmes classiques.
- **Marches quantiques** : Ce type d’algorithme est une généralisation des marches aléatoires. Il permet accélérer par exemple les méthodes de Monte-Carlo[254] de façon quadratique. Certaines versions offrirait un gain exponentiel.
- **Grover :** L'algorithme de Grover est très polyvalent: l'opérateur qui identifie les solutions du problème (l'Oracle) étant clairement dissocié du reste de l'algorithme, il peut être utilisé pour des problèmes très divers de recherche et/ou d’amplification.

Pour terminer, si bien d’autres algorithmes *purebreds* comme ceux de Deutsch-Jozsa, ou de Simon (algorithmes de recherche offrant une accélération exponentielle, basés sur un oracle,) auraient pu être mentionnés, il faut bien rappeler que tous relèvent d’une utilisation encore hypothétique.

Actuellement, les principaux travaux relatifs aux algorithmes se concentrent sur les workhorses, destinés aux ordinateurs quantiques de l’ère NISQ et susceptible d’apporter, qui sait, bientôt, une réelle valeur quantique. Sur ce point, l’annexe 10 apporte un éclairage sur la vision d’IBM, qui commercialise son offre d’ordinateurs quantiques sur le Cloud. Elle illustre les délais dans lesquels le fabricant pense que les applications à différents cas d’usages seront possibles.

[254] Les méthodes de Monte Carlo utilisent l'échantillonnage aléatoire pour estimer des quantités numériques qui sont difficiles à calculer de manière déterministe.

- ANNEXE 10 - ROADMAP IBM

IBM est le principal fournisseur de puissance de calcul quantique via le Cloud. Leur roadmap, présentée ci-dessous, illustre leur vision des délais qui seront nécessaires avant d'être capable d'adresser un ensemble de cas d'usage bien identifiés avec un ordinateur quantique. IBM a placé chacun de ces cas dans trois horizons temporels approximatifs.

- L'horizon 1 représente les applications qui devraient devenir possibles en utilisant un ordinateur de type NISQ au cours des prochaines années (0-5 ans peut-être 2)
- L'horizon 2 comprend celles qui nécessiteront des machines ayant un plus grand nombre de qubits de meilleure qualité mais qui ne seront pas encore corrigées des erreurs (QECC).
- Enfin, l'horizon 3 regroupe des cas qui ne devraient pas être possibles avant que des ordinateurs quantiques plus puissants et tolérants aux erreurs soient disponibles (10/15 ans ou plus).

  Comme toujours, ce type d'exercice est à prendre avec précautions puisque des avancées ou des verrous majeurs pourraient survenir au cours du processus de développement.

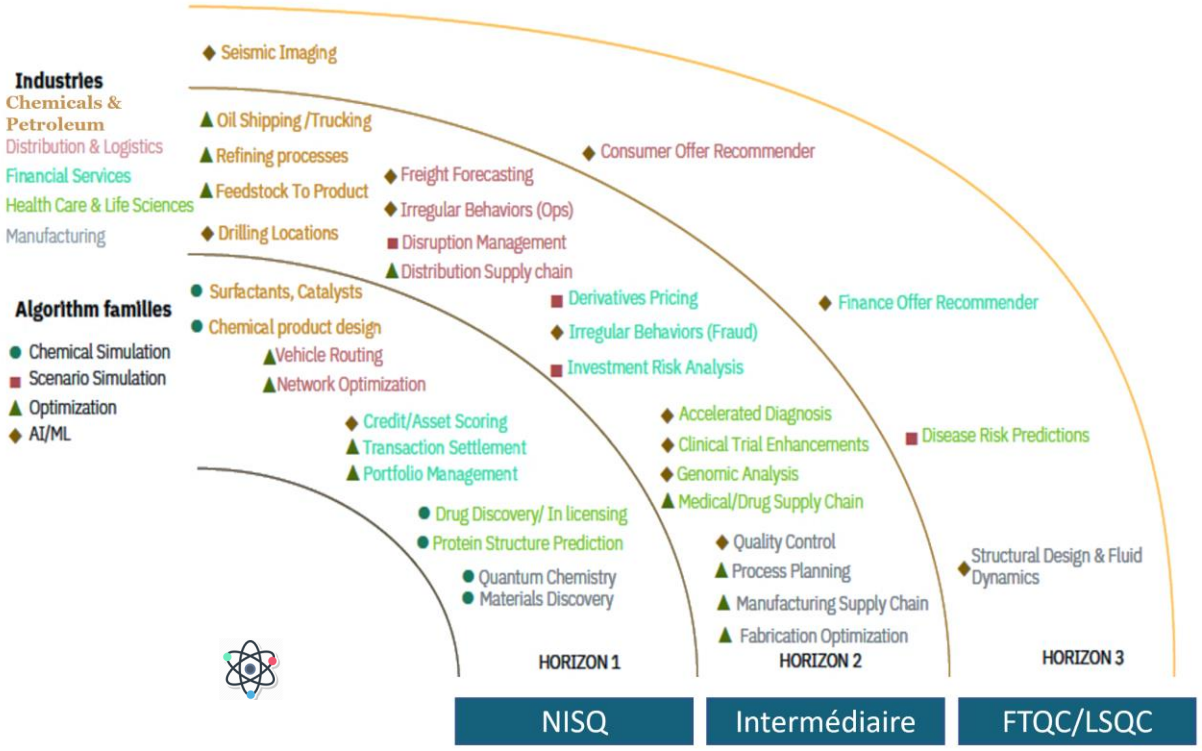


Figure 1: Roadmap IBM (Source : IBM)

- ANNEXE 11 - GLOSSAIRE[255]

Adiabatique : se dit d'un processus au cours duquel les conditions externes changent suffisamment lentement pour permettre l'adaptation du système auquel il est appliqué. En mécanique quantique, le théorème adiabatique est un concept à l'origine d'une méthode de calcul efficace d'optimaux. Par opposition, un processus diabatique dans lequel les conditions environnementales ou les inputs changent trop rapidement pour que le système puisse répondre ou s'adapter, en restant relativement inchangé.

Adjointe (matrice) : en algèbre linéaire, une matrice adjointe (aussi appelée transconjuguée) d'une matrice M à coefficients complexes est la matrice transposée de la matrice conjuguée de M. Dans le cas particulier où M est à coefficients réels, sa matrice adjointe est donc simplement sa matrice transposée.

Algèbre linéaire : branche des mathématiques qui s'intéresse aux espaces vectoriels et aux transformations linéaires, formalisation générale des théories des systèmes d'équations linéaires. Ses outils sont au centre de la modélisation de la mécanique quantique, et donc des ordinateurs quantiques, avec par exemple les espaces vectoriels et les combinaisons linéaires qui modélisent la superposition.

Algorithme de force brute : tout algorithme qui trouve une solution à un problème en énumérant exhaustivement toutes les possibilités, par opposition à une formule ou une heuristique qui va directement vers la solution.

Algorithme de Grover : algorithme quantique qui trouve l'entrée *x* d'une fonction particulière *f(x)* qui produit une valeur *y* de sortie spécifiée de manière nettement plus efficace qu'un algorithme comparable pour un ordinateur classique. Généralement considéré comme une solution pour la recherche dans une base de données (e.g. chercher un nom dans un annuaire à partir d'un numéro de téléphone).

Algorithme de Shor : algorithme quantique pour la factorisation en nombres premiers de très grands nombres entier, conçu pour exploiter la puissance d'un ordinateur quantique. Beaucoup de cryptosystèmes à clé publique, tels le RSA, deviendraient vulnérables si l'algorithme de Shor était un jour implémenté sur un calculateur quantique suffisamment puissant.

Algorithme NISQ : algorithme conçu et optimisé pour exploiter les ordinateurs quantiques bruyants à échelle intermédiaire (voir NISQ).

Algorithme quantique hybride : algorithme divisé en différentes parties : algorithmes classiques et algorithmes quantiques, de sorte que les classiques utilisent un ordinateur classique et les quantiques un ordinateur quantique.

Algorithme quantique : Un algorithme conçu pour être exécuté sur un ordinateur quantique. Un algorithme quantique est mis en œuvre par un circuit de logique quantique ou un programme quantique. Algorithmes célèbres: Grover, Shor.

Allotropique : se dit d'un corps qui garde ses propriétés chimiques malgré une modification de sa structure cristalline.

Amplitude de probabilité : en mécanique quantique, une amplitude de probabilité est un nombre complexe utilisé pour décrire le comportement d'un système. Le carré de son module donne la probabilité (densité de probabilité) que le système soit mesuré dans un état donné.

Antiparticule : particule qui possède les mêmes caractéristiques qu'une particule ordinaire, à l'exception d'une charge électrique opposée. Ces antiparticules forment de l'antimatière. La rencontre entre la matière et l'antimatière conduit à une annihilation des deux par transformation complète en photons.

Anyons : quasi-particules qui vivent en deux dimensions spatiales et qui ne sont ni des bosons ni des fermions, puisqu'ils obéissent à des statistiques quantiques fractionnaires. Les anyons existent : on sait qu'ils sont présents dans l'effet Hall quantique fractionnaire. Ces quasi-particules pourraient être utilisée pour construire qubit et ordinateur quantique topologique.

[255] Sources : Wikipedia, CEA ;…

Atome : brique de base de la matière ordinaire. Il est formé de nucléons (protons et neutrons) autour duquel gravitent des électrons chargés négativement. Les atomes peuvent s'agencer en molécules ou en réseau cristallin.

Atome artificiel : voir quantum dot.

Atomes froids : des qubits basés sur des ensembles stables d'atomes ultra-froids, se déplaçant lentement, offrent une plateforme évolutive potentielle pour l'informatique quantique. Voir refroidissement des atomes par laser.

Avantage computationnel (ou quantique) : pour un ordinateur quantique, la superposition et l'intrication des états quantiques fournissent un degré de parallélisme qui est intrinsèquement supérieur aux capacités d'un ordinateur classique. Cela recoupe aussi le cas d'ordinateurs quantiques possédant suffisamment de qubits pour ne plus pouvoir être simulés sur un ordinateur classique.

Bande interdite – directe ou indirecte : un semi-conducteur a une structure de bandes électroniques, plages d'énergie disponible pour les électrons dans la matière, liées à la nature périodique de l'arrangement atomique dans le cristal et à la nature ondulatoire des électrons. La bande interdite (gap) se situe entre une bande permise et pleine (ou quasi pleine à température non nulle), la bande valence, et une bande vide ou quasi vide, la bande de conduction. Les photons d'énergie supérieure à la bande interdite génèrent des porteurs de charge par transition des électrons entre les bandes permises. Le franchissement de la bande interdite peut se faire avec émission de phonons : il est alors question de bande interdite indirecte (cas du silicium) – ou sans émission (bande interdite directe).

Bandes d'énergie : plages d'énergie disponibles pour les électrons dans la matière.

BB84 : protocole de cryptage quantique développé par Charles Bennett et Gilles Brassard en 1984.

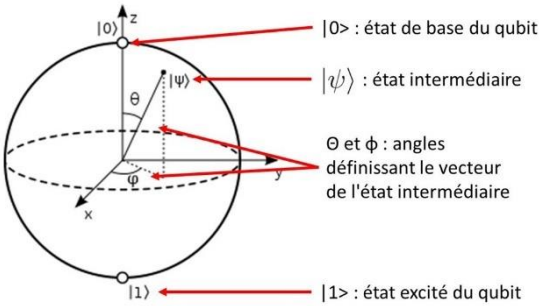
Bell (Etats de) : état quantique de deux qubits qui sont intriqués.

Bell (théorème de) : argument selon lequel la mécanique quantique ne peut pas être expliquée simplement en ajoutant des variables locales cachées à la mécanique classique.

Bit : unité élémentaire d'information en informatique classique qui est soit 0 soit 1, par opposition au qubit d'un ordinateur quantique qui peut être simultanément dans une superposition des états $|0\rangle$ et $|1\rangle$.

Bloch (Sphère de) : représentation géométrique à l'intérieur d'une sphère de rayon 1 de l'état quantique d'un qubit sous la forme d'un ou plusieurs vecteurs complexes, chacun ayant une amplitude ou une probabilité représentant la probabilité que le système quantique (qubit) soit

sphère de **Bloch**



dans l'état quantique particulier représenté par le vecteur complexe particulier. Utile pour visualiser la mécanique quantique sous-jacente d'un qubit.

Boite quantique : composant de dimension nanométrique dans lequel chaque électron n'a plus aucun degré de liberté, contraint par un semi-conducteur de plus grande bande interdite. Voir aussi quantum dot.

Bose-Einstein (Statistique de) : désigne, en mécanique quantique et en physique statistique, la distribution statistique de bosons indiscernables (tous similaires) sur les états d'énergie d'un système à l'équilibre thermodynamique. La distribution en question résulte d'une particularité des bosons : les particules de spin entier ne sont pas assujetties au principe d'exclusion de Pauli, à savoir que plusieurs bosons peuvent occuper simultanément un même état quantique.

Boson : particule de spin entier. Un boson obéit à la statistique de Bose-Einstein et échappe au principe d'exclusion de Pauli. Les photons par exemple sont des bosons.

Boucle supraconductrice : maintient un flux de courant sans résistance ni perte de chaleur. Utilisée pour construire un dispositif supraconducteur à interférence quantique ou SQUID. Utilisé dans la construction d'un qubit supraconducteur avec une jonction Josephson.

Bruit quantique : tout effet électromagnétique, thermique, acoustique ou de vibration provenant soit du milieu environnant soit de l'intérieur d'un système ou d'un appareil lui-même qui a pour effet de perturber l'état quantique d'un système quantique, comme les qubits d'un ordinateur quantique. Voir décohérence.

Câble coaxial : Câble électrique utilisé pour délivrer des impulsions micro-ondes à un processeur de qubit afin de contrôler l'état quantique du qubit. Un par qubit. Bien qu'il s'agisse en principe d'un câble électrique, avec deux conducteurs en cuivre, la fonction du câble coaxial est la transmission de radiations électromagnétiques, en particulier de signaux de radiofréquence (RF), qui comprennent des micro-ondes.

Calcul haute performante (HPC) : consiste à combiner la puissance de plusieurs milliers de processeurs pour effectuer des calculs complexes et des traitements de données massives en temps réel. Il existe plusieurs solutions de HPC mais la plus connue est bien-sûr la science des superordinateurs.

Calcul quantique adiabatique : algorithme pour trouver l'optimum d'une fonction en utilisant le théorème adiabatique quantique.

Calibration des qubits physiques : test et réglage des paramètres du matériel pour le contrôle d'un qubit physique. Cela doit être fait assez fréquemment et assez régulièrement (parfois quotidiennement).

Capteur quantique : dispositif (capteur) capable de détecter ou de mesurer des propriétés quantiques, telles que les propriétés d'un seul photon, d'un seul électron ou d'un seul atome et pouvant être utilisé par exemple pour des mesures très précises du temps ou de la gravité.

Cavité optique/micro-onde : voir résonateur optique/micro-onde.

Centre azote-lacune (ou **centre NV)** : Nitrogen-vacancy center - est l'un des nombreux types de défauts ponctuels présents dans la structure cristalline du diamant. Dans les technologies quantique, l'exploitation de ces défauts permet par exemple la construction de qubits ou de capteurs quantiques (sensibilité au magnétisme et au spin).

Circuit de Clifford : séquence d'une ou plusieurs portes de logique quantique fonctionnant sur un ou plusieurs qubits dont l'effet sur l'état quantique de ces qubits peut être exprimé comme une séquence de portes Clifford de base. Un circuit Clifford constitué uniquement de portes Clifford de base est un circuit Clifford unitaire.

Circuit intégré (**CI** ou **IC** en anglais) : circuit électronique dont les composants électroniques et les interconnexions ont été fabriqués sur un substrat isolant, par opposition à une carte de circuit imprimé contenant des composants électroniques discrets (montés sur la carte). Le CI est ensuite placé dans un boîtier (puce) qui pourra ensuite être inséré sur une carte de circuit imprimé.

Clé cryptographique : clé utilisée pour crypter et décrypter les messages chiffrés.

Clifford (Porte de base de) : désigne les portes logiques quantique de type H, T ou CZ.

Codage superdense : en théorie de l'information quantique, le codage superdense est un protocole de communication quantique qui permet d'envoyer deux bits d'information classiques dans un seul qubit grâce à l'intrication.

Cohérence : capacité d'un qubit à maintenir son état quantique sans subir d'erreurs quantiques ou perdre au moins une partie de son état au fil du temps. La cohérence d'un ordinateur quantique est pratiquement caractérisée par le nombre de portes quantiques qui peuvent être exécutées avant que les erreurs quantiques ne commencent à se produire, ou par le temps écoulé pour que ce nombre de portes soit exécuté. La correction des erreurs quantiques (QEC) peut être utilisée pour atténuer la décohérence quantique.

Communication quantique : utilisation des propriétés quantiques (intrication) des particules pour communiquer de l'information quantique de façon sécurisé sur une distance importante.

Complexité de calcul : approximation de la quantité de ressources de calcul qui sera nécessaire à un algorithme pour traiter des données d'entrée de tailles ou de valeurs diverses, en particulier le temps et la mémoire.

Complexité exponentielle : complexité de calcul d'un algorithme (calcul, problème) où le temps nécessaire pour terminer le traitement augmente de manière exponentielle avec la taille des données. Par opposition au temps polynomial. Par exemple, $O(2^n)$ vs. $O(n^2)$. Ce sont les problèmes pour lesquels les ordinateurs quantiques sont

considérés comme plus appropriés que les ordinateurs classiques.

Complexité polynomiale : complexité de calcul d'un algorithme (calcul, problème) où le temps nécessaire pour terminer le traitement augmente de manière polynomiale avec la taille des données, ce qui est une meilleure situation qu'avec une complexité exponentielle. L'un des principaux objectifs et avantages de l'informatique quantique est que les algorithmes adaptés ne prennent qu'un temps polynomial pour résoudre certaines classes de problèmes, alors que les meilleurs algorithmes sur un ordinateur classique prennent un temps exponentiel.

Conducteur : matériau qui facilite la transmission d'une charge électrique, par opposition à un isolant qui inhibe la transmission d'une charge électrique.

Connectivité « all-to-all » : architecture de processeurs quantiques où tout qubit peut être intriqué à tout autre qubit, plutôt que d'être restreint, comme par exemple uniquement aux voisins les plus proches.

Contrôle cohérent : Contrôle ou manipulation de l'état quantique d'un système quantique (même un seul qubit) en utilisant un champ externe tel qu'une impulsion laser ou une impulsion micro-onde.

Corps noir : désigne un objet idéal qui absorbe parfaitement toute l'énergie électromagnétique (toute la lumière quelle que soit sa longueur d'onde) qu'il reçoit. Cette absorption se traduit par une agitation thermique qui provoque l'émission d'un rayonnement thermique, dit rayonnement du corps noir.

(Code de) Correction des erreurs quantiques (QECC- QEC) : diverses techniques pour compenser les erreurs dans l'état quantique d'un qubit (décohérence, bruit extérieur, porte logique) telles que l'ajout de qubits de code. Voir qubit physique, logique.

Corrélation : lien existant entre deux variables statistiques. En physique quantique, on associe parfois l'idée de corrélation à son concept fondamental d'intrication puisque les mesures de propriétés physiques telles que le spin ou la polarisation effectuées sur des particules intriquées sont parfaitement corrélées.

Coupleur : dispositif électronique utilisé pour connecter ou coupler deux ou plusieurs qubits, par exemple pour permettre l'intrication quantique. Généralement une cavité ou un résonateur, ou une boucle supraconductrice.

Courant de fuite : courant parasite conduit par effet tunnel à travers l'isolant de grille.

Cristal : assemblage d'atomes, d'ions ou de molécules régulièrement répartis de façon périodique dans les trois directions de l'espace.

Crosstalk (Diaphonie): type d'erreurs se produisant dans la plupart des systèmes d'informatique quantique avec plus d'un qubit. Le crosstalk est l'effet d'une "action" (application d'une porte quantique) souhaitée sur un ou plusieurs qubits affectant involontairement un ou plusieurs autres qubits et qui peut être particulièrement préjudiciables aux méthodes de correction d'erreurs, qui repose généralement sur des erreurs locales et relativement prévisibles.

Cryogénie : s'intéresse à l'étude et la production de températures suffisamment froides pour que l'oxygène, l'azote, l'hydrogène et l'hélium se liquéfient. Comprend les techniques, les processus et les équipements nécessaires pour atteindre, maintenir et faire fonctionner ces températures ultra-froides, ainsi que le comportement des matériaux à ces températures comme la supraconductivité.

Cryostat : dispositif qui atteint et maintient la température cryogénique (ultra-froide) requise par certains processeurs quantiques. Voir cryogénie. Synonyme de réfrigérateur à dilution.

Cryptographie : Ensemble des procédés visant à crypter des informations pour en assurer la confidentialité entre l'émetteur et le destinataire.

Cryptographie post quantique : *post-quatum* ou *quantum-safe cryptography*, branche de la cryptographie visant à garantir la sécurité de l'information face à un attaquant disposant d'un ordinateur quantique en proposant l'utilisation de problèmes mathématiques, pour la génération et la distribution des clés de chiffrement, que même un calculateur quantique ne pourrait pas résoudre en un temps raisonnable (via l'algorithme de Shor par ex). Cette discipline est distincte de la cryptographie quantique, qui vise à construire des algorithmes cryptographiques utilisant des propriétés physiques quantiques (plutôt que mathématiques) pour garantir la sécurité.

Cryptographie quantique : consiste à utiliser les propriétés de la physique quantique pour établir

des protocoles de cryptographie qui permettent d'atteindre des niveaux de sécurité non atteignables en utilisant uniquement des méthodes classiques (c'est-à-dire non-quantiques) pour effectuer des tâches associées à la cryptographie. Cela intègre compris la distribution quantique de clés secrètes (QKD), le cryptage, le décryptage et la communication quantique.

Cybersécurité : englobe tous les moyens qui permettent d'assurer la protection et l'intégrité des données, sensibles ou non, au sein d'une infrastructure numérique (réseaux, autorisation d'accès, corruption ou perturbations des données). Les méthodes cryptographiques modernes sont utilisées pour limiter l'accès aux systèmes, aux réseaux et aux données. Malheureusement, les méthodes de cryptographie traditionnelles actuelles sont potentiellement vulnérables aux attaques par un ordinateur quantique, peut-être pas aujourd'hui, mais à terme.

Décohérence : tendance d'un ordinateur quantique à perdre sa cohérence quantique en raison d'erreurs quantiques, généralement dues à un mauvais isolement par rapport au milieu environnant. La cohérence d'un ordinateur quantique est pratiquement caractérisée par le nombre de portes quantiques qui peuvent être exécutées avant que les erreurs quantiques ne commencent à se produire, ou par le temps écoulé pour que ce nombre de portes puisse être exécuté. La correction des erreurs quantiques (QEC–Quantum Error Correction) peut être utilisée pour atténuer la décohérence quantique.

Détecteurs cohérents : équipements permettant de détecter les photons non pas à partir de leur interaction avec d'autres particules, mais à partir de l'amplitude et à la phase de leur signal électromagnétique.

Détection des erreurs : Capacité à détecter les erreurs. Nécessite généralement une sorte de redondance et de comparaison.

Diabatique : se dit d'un processus dans lequel les conditions externes évoluent trop rapidement pour que le système puisse réagir ou s'adapter, laissant le système relativement inchangé, par opposition à un processus adiabatique dans lequel les conditions changent assez lentement pour que le système soit capable de réagir et de s'adapter à l'évolution de l'environnement et des apports.

Diamant : une des trois formes allotropiques du carbone, à structure cristalline cubique et à indice de réfraction très élevé.

Diffraction : déviation que subit la direction de propagation des ondes (acoustiques, lumineuses…) lorsqu'elles rencontrent un obstacle ou une ouverture de dimensions du même ordre de grandeur que leur longueur d'onde.

Discret : discontinu

DiVincenzo (critères de) : cinq conditions nécessaires pour la construction d'un ordinateur quantique proposées par le physicien David DiVincenzo en 2000 : des qubits fiables, la capacité d'initialiser les qubits, un temps de cohérence long des qubits, un ensemble universel de portes (instructions) pour le fonctionnement des qubits, et un moyen de récupérer l'état final des qubits après l'exécution du programme (mesure).

Dopage N : dopage se traduisant par un excès d'électrons.

Dopage P : dopage se traduisant par un déficit d'électrons.

Dopant : atome étranger introduit dans un réseau cristallin afin d'en modifier les propriétés. Par exemple un semi-conducteur sera dopé pour voir ses propriétés électriques modifiées, par la présence d'un niveau énergétique discret permis dans la bande interdite près de la bande de valence ou de la bande de conduction. L'atome introduit cède ainsi un électron ou un trou mobile à l'une ou l'autre bande permise, ce qui augmente la conductivité électrique du matériau.

Dualité onde-particule : ou dualité onde corpuscule. Principe selon lequel un objet physique présente parfois des propriétés ondulatoires et parfois des propriétés corpusculaires.

Écart-type : mesure de la dispersion des valeurs d'un échantillon statistique. Cette grandeur sert entre autres à calculer des coefficients de corrélation.

Effet Doppler : décalage du spectre électro-magnétique (ie des longueurs d'onde) sous l'effet de la vitesse d'éloignement (ou du 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.

Effet Hall quantique : l'effet Hall classique décrit le phénomène d'une tension créée par un courant électrique traversant un matériau plongé dans un champ magnétique. Selon les conditions, cette tension croît par paliers, c'est l'effet Hall quantique.

Effet Josephson : en physique quantique, l'effet Josephson se manifeste par l'apparition d'un courant entre deux matériaux supraconducteurs séparés par une couche faite d'un matériau isolant ou métallique non supraconducteur. Le courant provient d'électrons (en fait paires d'électrons – dites paires de Cooper) qui traversent par effet tunnel l'isolant placé entre les deux supraconducteurs. Les jonctions Josephson sont des dispositifs électroniques exploitant cet effet.

Effet tunnel : possibilité pour un objet quantique (particule ou onde) de franchir une barrière de potentiel (ou un isolant) même si son énergie est inférieure à l'énergie minimale requise pour franchir cette barrière. L'effet tunnel est à l'œuvre dans l'effet Josephson et est exploité dans le principe des microscopes à effet tunnel.

Effondrement de l'état quantique (ou de la fonction d'onde) : l'observation(mesure) de l'état d'un système quantique ou d'un qubit entraîne l'effondrement de sa fonction d'onde à l'état mesuré, qui est équivalent à sa valeur classique mesurée. Il n'a plus de valeur quantique.

Electrodynamique quantique en cavité (cavity QED) : L'utilisation de la lumière piégée dans une cavité pour mettre en œuvre un qubit.

Électron : Un électron est un lepton. C'est un des constituants de l'atome, avec les nucléons. Il a une charge électrique négative de -1,6 10-19 C, qui est la charge électrique élémentaire (on dit donc que sa charge est -1). Sa masse est de 9,1 10-31 kg, soit 0,511 MeV.

Erreur Quantique : tout écart par rapport à l'état quantique approprié pour un qubit particulier ou l'ordinateur quantique dans son ensemble (tous les qubits). Cet écart peut être dû à la décohérence des qubits ou à des erreurs au moment de l'application des portes quantiques.

Espace de Hilbert : espace mathématique vectoriel qui, pour un système quantique, correspond à tous les états quantiques possibles du système quantique, comme pour un ordinateur quantique.

Etat de base : En mécanique quantique, un état quantique à la base d'un système quantique. Tous les autres états quantiques du système quantique peuvent être dérivés comme une combinaison linéaire des états de base. Les états de base et les états quantiques sont des vecteurs, les états de base sont des vecteurs de base, et un système quantique est en fait un espace vectoriel.

Etat excité : désigne les différents niveaux d'énergie quantique au-dessus de l'état fondamental d'un système quantique. Dans un qubit, il y a un état excité qui représente l'état de base $|1\rangle$, tandis que l'état fondamental représente l'état de base $|0\rangle$.

Etat fondamental (ground state) : état d'énergie le plus bas d'un système quantique, par opposition à un état excité.

État lié : Tendance d'une particule ou d'une onde à rester dans une région localisée de l'espace, par exemple en étant emprisonnée dans une cavité.

État quantique : notion qui se distingue de celle d'état d'un système physique classique, pour lequel les grandeurs physiques mesurées, comme la position et la vitesse, sont suffisamment déterminantes. L'état quantique fournit une loi de probabilité (représentée par la fonction d'onde) pour chacune des observables du système quantique auquel il se réfère.

Exciton : voir paire électron-trou

Faible bruit (ordinateur quantique) : traduction de *low-noise quantum computer* et par opposition à *noisy intermediate-scale quantum computer*. Architecture d'ordinateurs quantiques peu sujet aux erreurs quantiques.

Fermion : particule de spin demi-entier, il obéit à la statistique de Fermi-Dirac et au principe d'exclusion de Pauli. Les électrons, protons et neutrons sont des fermions.

Fluorescence : émission de lumière provoquée par l'absorption d'un flux incident (de lumière, de rayons X, ou d'électrons) puis la désexcitation rapide des électrons des couches atomiques externes du corps luminescent, cette partie d'énergie se traduisant par l'émission d'une nouvelle radiation électromagnétique. Si sa longueur d'onde se situe dans la partie visible du spectre, il y a luminescence.

Fonction d'onde (de Schrödinger) : concept fondamental de la mécanique quantique, c'est une fonction mathématique, souvent notée **Ψ(r,t)**, qui représente l'état quantique d'un système quantique. Elle correspond à une amplitude de probabilité, en général à valeur complexe. La probabilité de trouver une particule au voisinage de la position **r** à l'instant **t** est alors proportionnelle au carré du module de la fonction d'onde $|\Psi(r,t)|^2$, densité de probabilité (volumique) de présence, et à la mesure du volume du voisinage de r.

Fonction objective : fonction mathématique qu'un algorithme d'optimisation cherche à minimiser, ou maximiser. Voir recuit quantique.

FPGA : Field-Programmable Gate Array – processeurs flexibles dont le circuit intégré lui-même est reprogrammable.

Fractionalisation : phénomène par lequel les quasiparticules d'un système ne peuvent être construites comme les combinaisons de ses constituants élémentaires. Un exemple important et parmi les premiers trouvés est celui de l'effet Hall quantique fractionnaire. Dans ce cas, les particules constitutives sont des électrons, mais les quasiparticules ont une charge électrique qui est une fraction de celle d'un électron

Fréquence : en physique, la fréquence est le nombre de fois qu'un phénomène périodique se reproduit par unité de mesure du temps. C'est l'inverse mathématique de la période du phénomène. La fréquence est mesurée en cycles par seconde, appelé hertz. C'est une des caractéristiques d'un rayonnement électromagnétique.

Fullerène : troisième forme allotropique du carbone après le graphite et le diamant. Elle a la propriété de former des cages fermées dont la structure rappelle celle d'un ballon de football (C_{60}).

GPU : Graphics Processing Unit – processeurs dédiés au traitement d'images.

Graphite : une des trois formes allotropiques du carbone à structure cristalline en feuillets de graphène dans laquelle chaque atome est lié à trois de ses voisins.

Guide d'ondes : dispositif destiné à guider une onde électromagnétique entre deux points (peu éloignés) avec un minimum de perte d'énergie par rayonnent. Généralement utilisé pour les micro-ondes, mais la fibre optique est également un guide d'ondes.

Hamiltonien : opérateur en mécanique quantique qui correspond à l'énergie totale d'un système quantique que l'on trouve par exemple dans la célèbre équation de Schrödinger.

HPC : Acronyme de high-performance computer, en français calcul haute performance. Voir superordinateur.

Hybride (mode de fonctionnement) : processus dans lequel des parties d'opérations ou de calculs sont exécutées sur un ordinateur quantique et d'autres sur un ordinateur classique, ce qui permet d'avoir le meilleur des deux mondes, car les ordinateurs quantiques ne peuvent pas tout faire (ex gestion de fichier de donnée, instruction conditionnelle…).

In silico : utilisation d'un ordinateur pour simuler un processus biologique ou chimique. Par opposition à une expérience biologique ou chimique.

Indiscernable (particule): Les particules indiscernables ne peuvent être différenciées l'une de l'autre, même en principe. Ce concept prend tout son sens en mécanique quantique, où les particules n'ont pas de trajectoire bien définie qui permettrait de les distinguer l'une de l'autre.

Information quantique : informations ou données qui sont codées/conservées dans l'état quantique d'un système quantique - les qubits d'un ordinateur quantique.

Instruction : équivalent en informatique classique d'une opération quantique ou d'une porte logique quantique. L'équivalent quantique d'une séquence d'instructions d'un ordinateur classique serait un circuit quantique.

Interférence : La propriété d'interférence est inhérente à tout phénomène ondulatoire. C'est en particulier une manifestation typique du caractère ondulatoire de la lumière mais aussi le moyen de prouver la dualité onde-particule pour des objets microscopiques. L'interférence se produit lorsque l'on combine deux ondes. Elle peut être constructive (lorsque les deux ondes sont en phase) ou destructive (lorsque les deux ondes sont en opposition de phase). Voir phase.

Interprétation : interrogation centrale dans le monde de la physique quantique, pour comprendre en quoi elle consiste et quels sont les discours sur la relation entre le monde et sa représentation qu'elle autorise, ce qu'aucune science auparavant n'avait entraîné de manière si aiguë.

Intrication : phénomène (contre-intuitif) selon lequel deux ou plusieurs particules présentent des états quantiques dépendant l'un de l'autre indépendamment de la distance qui les sépare. Lorsqu'une action est effectuée sur l'une des particules intriquées, elle affecte leur état mutuel, même si elles sont séparées par de grandes distances.

Ion : atome (ou molécule) qui a perdu ou gagné un ou plusieurs électrons et se trouve ainsi électriquement chargé.

Isolant : matériau électriquement neutre qui inhibe la transmission des charges électriques, à l'exception d'une jonction Josephson qui permet de faire passer des électrons par un isolant, mais de manière contrôlée. Par opposition un conducteur facilite la transmission de la charge électrique.

Isolation : nécessité pour que l'état d'un système physique ne dépende pas du milieu environnant ni ne soit influencé par celui-ci. Une bonne isolation est obtenue et maintenue par un blindage contre les rayonnements électromagnétiques parasites, une séparation physique, une faible énergie et une basse température.

Jonction Josephson : jonction entre deux électrodes supraconductrices établie en les séparant par une couche d'isolant assez mince pour que les paires d'électrons (Cooper) puissent la traverser par effet tunnel. Communément utilisée pour construire des processeurs quantiques.

Jonction P/N : zone de création d'un champ électrique entre un semi-conducteur de type N et un de type P, qui deviennent respectivement chargés positivement et négativement.

Kelvin : Le kelvin (symbole K), est l'unité de base SI de température thermodynamique. À la différence du degré Celsius, le kelvin est une mesure absolue de la température qui a été introduite grâce au troisième principe de la thermodynamique. La température de 0 K est égale à −273,15 °C et correspond au zéro absolu.

Lacune : emplacement dans un réseau cristallin laissé vacant par un atome déplacé.

Localité : (principe de) notion exprimant que deux objets distants ne peuvent avoir une influence directe l'un sur l'autre.

Lois de Moore : conjonctures empiriques initialement émises par Gordon Moore qui ont trait à l'évolution de la puissance de calcul des ordinateurs et de la complexité du matériel informatique. Initialement exprimée en 1965, Moore réévalua en 1975 sa prédiction en posant que le nombre de transistors des microprocesseurs sur une puce de silicium double tous les deux ans.

Majorana (fermion ou particule de) : particule de type fermion qui est sa propre antiparticule et qui est l'objet de recherches en physique du solide. En théorie, ces particules pourraient servir à la réalisation d'ordinateurs quantiques (voir ordinateur topologique) moins sensibles au problème de décohérence.

Matrice identité : en algèbre linéaire, la matrice identité (ou matrice unité) est une matrice carrée avec des 1 sur la diagonale et des 0 ailleurs.

Matrice unitaire : matrice carrée dont la matrice ajointe (ou trans-conjuguée) est aussi son inverse.

Mécanique quantique : branche de la physique qui étudie et décrit les phénomènes fondamentaux à l'œuvre dans les systèmes physiques à l'échelle atomique et subatomique.

Mémoire quantique : procédé ou dispositif de stockage d'informations quantiques, notamment en liaison avec un canal de communication quantique.

Mesure : action de déterminer la valeur d'une grandeur, ce qui dans le monde quantique revêt une difficulté particulière. Par exemple pour un qubit, la mesure de son état quantique ne renvoie qu'une seule valeur en provoquant l'effondrement de l'état quantique de ce qubit, entraînant la perte du reste de l'état quantique (l'éventuelle superposition des états disparait).

Métrologie quantique : domaine d'application de la théorie quantique pour la réalisation de mesures à haute résolution ou très sensibles de paramètres physiques en exploitant notamment l'intrication. Ces développements permettent d'atteindre un niveau de précision bien supérieur à celui des méthodes classiques.

Micro-ondes : rayonnements électromagnétiques de longueur d'onde intermédiaire entre l'infra-rouge et les ondes radio normales. Dans le contexte de l'informatique quantique, elles peuvent être utilisées pour contrôler les qubits.

Millikelvin (mK) : un millième (1/1000) de degré kelvin (K). Température extrêmement froide proche du zéro absolu.

Moment cinétique (ou **angulaire**) : joue dans le cas d'une rotation, un rôle analogue à celui de la quantité de mouvement pour une translation. Voir spin.

Nanokelvin (nK) : un milliardième de degré kelvin (K). Température extrêmement proche du zéro absolu et ordre de grandeur du record de température obtenue en laboratoire.

Nanomètre : 1 nm = 10^{-9} m.

Nanoparticule/nanostructure : particule ou structure de taille nanométriques.

Nanotube de carbone : structure cristalline constituée d'un ou plusieurs feuillet(s) de graphène enroulés sur eux-mêmes, d'un diamètre nanométrique mais dont la longueur peut atteindre plusieurs centaines de micromètres. Il peut être soit métallique, soit semi-conducteur, selon l'orientation de l'enroulement. Les tubes de graphène peuvent servir de cage pour piéger des particules manipulées en vue de construire un système quantique.

NEMS (Nano Electro Mechanical System) : Système électromécanique nanoscopique.

Neutron : particule fondamentale électriquement neutre, de masse 1,675.10^{-27} kg. Les neutrons sont des nucléons qui constituent avec les protons, les noyaux des atomes.

Niobium : élément métallique qui devient supraconducteur à 9.2 K. Il est utilisé en alliage pour créer une boucle supraconductrice qui, associé à une jonction Josephson, sert à construire un qubit - transmon supra-conducteur.

NISQ : *Noisy Intermediate-Scale Quantum* – les technologies quantiques d'échelle intermédiaire bruitées désigne la classe des ordinateurs quantiques disponibles aujourd'hui et dans un avenir très proche. Il s'agit de machines proposant un petit nombre de qubits (de 10 à quelques centaines), supportant des profondeurs de circuit limitées à quelques dizaines de portes et relativement fiable mais sans correction d'erreurs. On trouve aussi la terminologie *near-term quantum computer*.

Niveau atomique : niveau d'énergie qu'un atome peut présenter suivant son état fondamental (ground state) ou excité (excited state).

Niveau de Fermi : niveau d'énergie représentant un lieu d'équilibre particulier (donné par la fonction de Fermi) entre le nombre d''électrons dans la bande de conduction et le nombre de trous dans la bande de valence. Dans un semi-conducteur intrinsèque, il se situe au milieu de la bande interdite. Dans un matériel dopé N, le niveau de Fermi se situe légèrement en dessous du minimum de la bande de conduction et dans un matériel dopé P, légèrement au-dessus du maximum de la bande de valence.

Nombre complexe : en mathématiques, l'ensemble des nombres complexes est 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. Les nombres complexes sont au cœur de la mécanique quantique, et donc au cœur du fonctionnement d'un ordinateur quantique et des états quantiques en particulier.

Non-clonage (Théorème) : en physique quantique, l'état quantique inconnu d'un système, ou d'une particule ne peut pas être copié à l'identique. Ainsi un algorithme quantique ne peut pas faire une copie exacte de l'état quantique complet d'un autre qubit, car cela serait comparable à la mesure du qubit laquelle entraine l'effondrement de sa fonction d'onde.

Non-localité quantique : capacité de deux systèmes quantiques physiquement séparés (deux électrons, deux photons…), à partager leur état quantique de manière à pouvoir interagir à distance - cas d'intrication quantique.

Notation bra-ket (ou de **Dirac**) : (du terme anglais bracket, crochet de parenthèse) formalisme facilitant l'écriture des équations de la mécanique quantique.

Nucléon : Un nucléon est un baryon. C'est un des composants de l'atome avec les électrons (il forme le noyau atomique). Il y a deux sortes de nucléons - les protons et les neutrons.

Observable : (n.f.) notion qui est au monde quantique ce qu'une grandeur physique (position, quantité de mouvement…) est au monde classique.

Opérateur quantique : dans le formalisme mathématique de la mécanique quantique, un opérateur quantique est caractérisé par une matrice que l'on multiplie par le vecteur représentant l'état quantique d'un système quantique et qui produit un nouvel état quantique. Mathématiquement, il s'agit donc simplement d'une multiplication matricielle. Voir portes logiques quantiques.

Optique linéaire (ordinateur quantique à) : approche qui vise à utiliser les photons comme objet de stockage et de manipulation de l'information quantique.

Optique quantique : désigne l'ensemble des expériences, à la frontière entre la mécanique quantique et l'optique, dans lesquelles la lumière ou bien l'interaction entre lumière et matière doivent être quantifiées. Dans le cadre de l'optique quantique, la lumière est considérée comme constituée de photons, objets quantiques qui se comportent comme des corpuscules dans leurs interactions avec la matière, et comme des ondes pour leur propagation. La description de la dynamique des photons relève de la mécanique quantique leur mouvement est donc décrit à l'aide de probabilités de présence en un point donné.

Ordinateur analogique : ordinateur dont la logique et les calculs sont basés sur les valeurs continues des signaux analogiques (comme la tension ou le niveau d'énergie) plutôt que sur les valeurs discrètes des bits numériques ou des bits quantiques comme dans un ordinateur numérique ou un ordinateur quantique.

Ordinateur quantique à grande échelle : traduction de *large-scale quantum computer*, généralement employé pour désigner un ordinateur quantique à usage général, en mettant l'accent sur sa capacité à traiter des problèmes de grande envergure ou de nature très différentes.

Ordinateur quantique analogique : désigne parfois un ordinateur utilisant un processeur à recuit quantique ou l'informatique quantique adiabatique.

Ordinateur quantique supraconducteur : ordinateur quantique construit avec la technologie des circuits électroniques supraconducteurs, tels que ceux utilisant sur les jonctions Josephson.

Ordinateur quantique : utilise les propriétés quantiques de la matière, telle que la superposition et l'intrication afin d'effectuer des opérations sur des données.

Paire de Cooper : électrons regroupés par deux pour former un système se comportant comme un boson, particule de spin entier, alors que les électrons isolés sont des fermions (particule de spin demi-entier). Cet appariement est en particulier à la base des phénomènes de supraconductivité et de superfluidité. Les deux électrons ont la même quantité de mouvement, mais de signe opposé. Utilisé comme base d'un qubit de charge, également appelé qubit de charge supraconductrice (voir effet et jonction Josephson), qubit de transmon supraconducteur ou simplement transmon.

Paire électron-trou (ou **exciton**) : paire de porteurs non liés à un atome et donc aptes à se déplacer dans l'ensemble du cristal où ils sont apparus et dont l'un est négatif (électron dans la bande de conduction) et l'autre positif (absence d'électron dans la bande de valence).

Paradoxe EPR : est une expérience de pensée élaborée en par les physiciens Einstein, Podolsky, Rosen, dont le but était de réfuter l'interprétation de l'école de Copenhague de la physique quantique. En 1964, John Stewart Bell produisit un théorème permettant de quantifier les implications du paradoxe EPR, ouvrant la voie à l'expérimentation : dès lors la résolution du paradoxe pouvait devenir une question expérimentale, plutôt qu'un choix épisté-mologique. La technologie de l'époque ne permettait pas de réaliser une expérience testant les inégalités de Bell, mais Alain Aspect a pu le réaliser en 1981.

Particule : dans le contexte de la physique quantique et de l'informatique quantique, *particule* désigne un électron, un photon, un ion, un atome voire une molécule.

Pauli (Principe d'exclusion de) : voir principe d'exclusion.

Permittivité diélectrique (ou **constante diélectrique**) : exprime le pouvoir électriquement isolant d'un matériau.

Phase d'un qubit : angle de rotation du vecteur représentant l'état d'un qubit autour de l'axe

vertical Z sur la sphère de Bloch, communément appelé phi (φ), mesuré en radians ou en degrés.

Phase : en physique des ondes la phase fait référence à la fois à la fréquence d'une onde et au moment du passage à zéro de l'onde, qui peut être exprimé soit en temps, soit en radians (angle) que l'onde traverserait pendant ce temps. La phase totale n'a pas de sens si elle est exprimée sans repère, par exemple sans l'instant et l'endroit où on la considère initiale. En pratique, seule la différence de phase (ou déphasage) entre deux ondes, est une grandeur mesurable et utile, qui permet de comparer deux ondes similaires. Le phénomène d'interférences résulte de la superposition de deux ondes de même fréquence et de déphasage constant entre elles (cohérentes). Si, les ondes sont en opposition de phase, les interférences sont destructives, si elles sont en phase, les interférences sont constructives.

Phonon : mode propre de vibration du réseau cristallin d'un solide.

Phosphorescence : émission lumineuse liée à la désexcitation *lente* d'atomes excités par un rayonnement lumineux (par ex. laser) dont l'énergie est absorbée par les électrons dans certains corps. Ce phénomène de photoluminescence se différencie de la fluorescence par la durée élevée séparant de l'absorption de la réémission.

Photon : quantum d'énergie d'un rayonnement électromagnétique. Particule élémentaire de masse nulle et sans charge électrique associée à ce rayonnement (lumière visible, infrarouge, ultraviolet, gamma ou X suivant son énergie). Un photon se comporte plus comme une onde que comme une particule, mais c'est bien les deux. L'énergie d'un photon est proportionnelle à sa fréquence. Un photon est un boson et le principe de Pauli ne s'applique pas.

Photovoltaïque : effet qui permet de convertir directement la lumière en électricité par le biais de la production et du transport de charges électriques dans un matériau semi-conducteur composé d'une partie présentant un excès d'électrons et d'une autre un déficit (trou).

Pièges à ion : dispositifs permettant de stocker des particules chargées (ions) pendant une longue durée, notamment dans le but de mesurer leurs propriétés avec précision. Ces dispositifs utilisent des champs électriques ou magnétiques et peuvent être utilisés pour construire les qubits d'un processeur quantique.

Planck (Constante de) : en physique, la constante de Planck, notée h, est utilisée pour décrire la taille des quanta. Cette valeur représente la plus petite quantité d'énergie existant dans le monde physique et c'est le coefficient de proportionnalité entre l'énergie d'un photon et sa fréquence : $E = h \nu$.

Point quantique : voir Quantum dot

Polarisation : propriété des ondes à vibrer selon une orientation privilégiée.

Pompage optique : procédé utilisé dans les lasers pour obtenir l'*inversion de population*, qui consiste à fournir l'énergie nécessaire pour obtenir plus d'atomes excités (à un niveau énergétique supérieur) que d'atomes non excités, en les éclairant avec un flash puissant.

Porte changement de phase (Rφ) : famille de portes qui agit sur un seul qubit sans en modifier son amplitude de probabilité mais en modifiant sa phase. Ceci équivaut à tracer un cercle horizontal à la latitude de φ radians sur la sphère de Bloch.

Porte CNOT : porte logique quantique à deux entrées qui fait basculer l'état quantique d'un qubit spécifié (le qubit cible) si et seulement si un autre qubit spécifié (le qubit de contrôle) est dans l'état $|1\rangle$ et agit alors ainsi comme un NOT classique. Cette porte est communément utilisée en conjonction avec la porte Hadamard (porte H) sur le qubit de contrôle pour enchevêtrer deux qubits.

Porte d'Hadamard (H): porte logique quantique qui fixe l'état quantique d'un qubit à une superposition des états de base $|0\rangle$ et $|1\rangle$, de sorte que lors de la mesure, les états de base auront une probabilité égale d'être lu (l'état $|0\rangle$ sera mesuré dans 50% des cas et l'état $|1\rangle$ dans 50%).

Porte logique quantique : dans le modèle de circuit quantique de l'informatique quantique, une porte logique quantique (ou porte quantique) est un circuit quantique élémentaire opérant sur un petit nombre de qubits. Les portes quantiques sont les briques de base des circuits quantiques, comme le sont les portes logiques classiques pour des circuits numériques classiques.

Porte logique classique : circuit intégré capable d'effectuer le traitement d'états logiques (bits) (existence d'une tension constante (bit 1) ou

existence d'une tension nulle (bit=0)).

Porte Pauli-X, -Y, -Z : chacune de ces 3 portes quantiques agit sur un seul qubit et correspond à une rotation de π radians du vecteur représentant le qubit selon l'axe X, Y ou Z de la sphère de Bloch (respectivement).

Porte SWAP : porte logique quantique qui échange les états quantiques de deux qubits.

Porteurs (de charge) : électrons de conduction - le courant électrique est un déplacement de porteurs de charge.

Postulats : principes non démontrés, utilisés pour construire une théorie.

Principe d'exclusion de Pauli : principe fondamental de la mécanique quantique où deux fermions (électrons, neutrons, protons) ne peuvent occuper le même état quantique (par exemple une même orbitale ne peut contenir que deux électrons de spins opposés). C'est ce principe qui permet tout simplement à la matière d'exister et de ne pas s'effondrer sur elle-même. Ce principe ne s'applique pas aux photons.

Principe d'incertitude (ou d'indétermination) de Heisenberg : désigne toute inégalité mathématique affirmant qu'il existe une limite fondamentale à la précision avec laquelle il est possible de connaître simultanément deux propriétés physiques d'une même particule ; de telles variables complémentaires peuvent être par exemple sa position et sa quantité de mouvement.

Processus de réduction du paquet d'ondes : concept fondamental de la mécanique quantique exprimant le fait qu'après une mesure un système quantique voit son état réduit à ce qui a été mesuré.

Profondeur de circuit (circuit depth) : nombre de portes logiques quantiques dans un circuit de logique quantique. Synonyme de profondeur de circuit à logique quantique, de nombre de portes ou de nombre de portes à logique quantique.

Profondeur de circuit réalisable : Le nombre de portes quantiques qui peuvent être exécutées dans un processeur circuit quantique avant que des erreurs ou une décohérence ne faussent le résultat. Synonyme de profondeur de circuit admissible.

Proton : particule élémentaire portant une charge électrique positive égale et opposée à celle de l'électron.

Puce quantique au silicium : processeur quantique bâti en utilisant la technologie standard des circuits intégrés semi-conducteurs en silicium. Voir point quantique (quantum dot) et atomes artificiels.

Puce quantique : circuit intégré contenant un ou plusieurs qubits ainsi que les circuits associés permettant de contrôler directement ce ou ces qubits.

Puits quantique : composant de dimension nanométrique dans lequel chaque électron ne peut se déplacer que dans deux dimensions de l'espace, contraint par un semi-conducteur de plus grande bande interdite.

QaaS : *Quantum as a Service* est une offre de services de calcul quantique - qui s'appuie sur un ordinateur quantique réel ou simulé - accessible sur un mode cloud.

QAOA : acronyme de *quantum approximate optimization algorithm* - algorithme d'optimisation hybride, quantique et classique, dans lequel un circuit quantique paramétrique et un optimiseur classique itère en boucle fermée pour résoudre les problèmes d'optimisation combinatoire.

QEC : acronyme de *quantum error correction*

QKD : acronyme de *Quantum Key Distribution* - méthode et protocole basés sur la mécanique quantique pour produire et échanger des clés cryptographiques entre deux parties afin qu'elles puissent communiquer en toute sécurité. Voir BB84.

QRAM : Acronyme de *quantum Random Access Memory* - Modélisation d'une mémoire vive (RAM d'un ordinateur classique) sur un ordinateur quantique.

Quantique : qui relève de la théorie développée à partir du principe des quanta de Planck (toute manifestation de l'énergie ne peut s'exprimer que par une valeur discrète appelé quantum) et du principe d'incertitude (ou d'indétermination) de Heisenberg selon lequel il n'est pas possible de mesurer en même temps avec précision la position et la vitesse d'une particule

Quantité de mouvement : produit de la masse par le vecteur vitesse d'un objet supposé ponctuel.

Quantum dots : Une boîte (ou point) quantique aussi connu sous son appellation anglophone de

quantum dot, est une nanostructure de semi-conducteurs. De par sa taille et ses caractéristiques, elle se comporte comme un puits de potentiel qui confine les électrons (et les trous) dans les trois dimensions de l'espace, dans une région d'une taille de l'ordre de la longueur d'onde des électrons, soit quelques dizaines de nanomètres dans un semi-conducteur. Ce confinement donne aux boîtes quantiques des propriétés proches de celles d'un atome, raison pour laquelle les boites quantiques sont parfois qualifiées d'*atomes artificiels*.

Quantum, quanta : plus petite mesure indivisible (d'énergie, de quantité de mouvement…).

Quantum, Quanta : En physique, quantum (pluriel : *quanta*) représente la plus petite mesure indivisible, que ce soit celle de l'énergie, de la quantité de mouvement ou de la masse.

Quasiparticules : entités conçues comme des particules et facilitant la description des systèmes de particules, particulièrement en physique de la matière condensée. Parmi les plus connues, on distingue les trous d'électrons qui peuvent être vus comme un "manque d'électron", et les phonons, qui décrivent des "paquets de vibration".

Qubit : est l'état quantique qui représente la plus petite unité de stockage d'information quantique. C'est l'analogue quantique du bit en informatique classique. Il désigne un système quantique (qui code l'information) dans lequel une observable considérée (par exemple le spin d'un électron, ou la polarisation d'un photon) est la superposition de deux états quantiques indépendants (dit de bases) par convention notés $|0\rangle$ et $|1\rangle$ (notation de Dirac ou bra-ket). Un état qubit est constitué d'une superposition quantique linéaire de ces deux états à la différence d'un bit classique qui ne peut prendre que la valeur 0 ou 1 à un instant donné. Si un qubit seul peut représenter deux valeurs simultanément alors qu'un bit classique ne peut représenter qu'une seule valeur à un moment donné, deux qubits peuvent représenter quatre valeurs simultanément, tandis qu'un bit classique seulement deux. En généralisant, n qubits peuvent représenter 2^n valeurs ou états quantiques simultanément, tandis que n bits classiques ne peuvent représenter que n valeurs (chacun un seul bit classique) à un seul moment. Les qubits peuvent également être intriqués. Le principal inconvénient d'un qubit est que sa valeur ne peut être lue (mesurée) sans que son état quantique superposé ne s'effondre en une seule valeur. Un autre inconvénient important est que la technologie quantique actuelle exige que les qubits soient refroidis à une valeur proche du zéro absolu afin de permettre la superposition et l'intrication et limiter le bruit, la décohérence et les erreurs.

Qubit à l'état solide (solid-state qubit) : qubit fabriqué à partir d'un état solide de la matière, c'est-à-dire avec plus d'un atome, par opposition à un qubit atomique constitué d'un seul atome, comme un piège à ions. Rentre donc dans cette catégorie les qubits supraconducteurs et des boites quantiques (silicium).

Qubit atomique : qubit constitué d'un seul atome, comme un piège à ions, par opposition à un qubit à l'état solide, comme un qubit de spin de silicium.

Qubit de charge : modalité de qubit - aussi connu sous le nom de transmon - basée sur la présence ou l'absence d'une charge électrique provenant d'une paire de Cooper additionnelle (doublet d'électrons) sur une ile supraconductrice isolée par une jonction Josephson. Les autres types de qubits supraconducteur sont les qubits de flux, les qubits de phase et les qubits de spin.

Qubit de flux : modalité de qubit basée sur le flux magnétique dont les états correspondent à des courants dans le sens des aiguilles d'une montre et dans le sens inverse circulant dans une boucle interrompue par des jonctions Josephson. Des impulsions micro-ondes sont utilisées pour manipuler l'état quantique du qubit. Les autres types de qubits supraconducteur comprennent les qubits de charge, les qubit de phase et les qubits de spin.

Qubit de phase : qubit supraconducteur basé sur la différence de phase entre deux supra-conducteurs. Les autres types de qubits supra-conducteur sont les qubits de flux, les qubits de charge et les qubits de spin.

Qubit de spin (dans le silicium) : Le spin de l'électron, qui comporte deux états, est une des réalisations possibles du qubit, grâce à un composant appelée boîte quantique (cf. quantum dot) dans lequel il est piégé. Les quantum dots sont réalisées sur des puces en silicium ce qui permet de bénéficier du savoir-faire de l'industrie des puces classiques et aussi envisager un passage à l' échelle pour des puces qui proposeraient plusieurs centaines de milliers de qubits.

Qubit logique : un qubit codé de manière redondante dans lequel les erreurs quantiques peuvent être identifiées et corrigées sans altérer le qubit codé. La construction d'un qubit logique performant nécessite l'utilisation d'un système de correction d'erreurs utilisant un grand nombre de qubit physiques (x1000).

Qubit physique : suivant le contexte, désigne soit un qubit sur un ordinateur quantique physique, par opposition à un ordinateur quantique simulé soit un qubit faisant parti d'un ensemble de qubits servant collectivement à représenter un qubit logique unique aux fins de la correction quantique des erreurs (QEC).

Qubit stationnaire : qubit immobile (la plupart des qubit en dehors des photons), par opposition à un qubit volant (photon) qui est mobile.

Qubit volant (flying qubit) : qubit mobile qui peut être transporté d'un endroit à l'autre, en conservant son état quantique, contrairement à un qubit stationnaire. Désigne généralement les photons, qui se déplace à la vitesse de la lumière.

Qubit auxiliaire : qubit supplémentaire nécessaire soit pour la correction d'erreurs, soit pour permettre l'utilisation d'une porte logique quantique réversible comme une porte logique non réversible et non quantique, par exemple pour pouvoir forcer un qubit à une valeur spécifique. Par définition, toutes les portes logiques quantiques sont des portes logiques quantiques réversibles.

Qubits voisins : signifie généralement que les qubits sont physiquement adjacents sur une puce quantique, mais ce n'est pas une exigence absolue. La condition essentielle est qu'il y ait une interconnexion entre les qubits, comme un résonateur qui permet les intriquer.

Qudit : principe similaire au qubit mais avec 10 états quantiques discrets ou plus, qui peuvent tous être superposés. Un qudit a une dimension de dix, ce qui signifie que ses états quantiques sont modélisés par un espace de Hilbert (espace vectoriel) à dix dimensions, et n qudits modélisés par un espace de Hilbert de dimension 10^n. Deux qudits représenteraient 100 (10 fois 10) états simultanés, plus que les 64 (2^6) états que 6 qubits peuvent représenter simultanément. Les 1 000 états simultanés de trois qudits seraient comparables aux 1 024 (2^{10}) états simultanés de 10 qubits Voir qubit et qutrit.

Qutrit : similaire au qubit, mais avec trois états quantiques, $|0\rangle$, $|1\rangle$ et $|2\rangle$, qui peuvent tous être superposés. Un qutrit a une dimension de trois, ce qui signifie que ses états quantiques sont modélisés par un espace de Hilbert (espace vectoriel) à trois dimensions, et n qutrits modélisés par un espace de Hilbert à dimension de 3^n.

Radiofréquence : souvent abrégé RF, fréquence d'onde électromagnétique située dans la gamme des fréquence radio (3kHz-300GHz) couvrant entre autres différents moyens de radio-communication comme la téléphonie mobile, le Wifi, la radiodiffusion, radars, fours micro-ondes.

RAM : La mémoire vive de l'ordinateur, aussi appelée RAM pour Random Acess Memory, sert à stocker des informations temporaires dans un ordinateur classique. Voir QRAM.

Rayonnement du corps noir : rayonnement thermique d'un objet idéal absorbant toute l'énergie électromagnétique qu'il reçoit.

Recuit : méthode de recherche d'extrema d'une fonction, inspirée d'un processus métallurgique alternant cycles de refroidissement lent et de réchauffage.

Recuit quantique (Ordinateur à) : ordinateur quantique spécialisé et algorithme permettant de trouver l'extremum global d'une fonction (objective).

Réduction du paquet d'onde : concept de la mécanique quantique selon lequel, après une mesure, un système physique voit son état entièrement réduit à celui qui a été mesuré.

Réfrigérateur à dilution : dispositif permettant de maintenir un froid intense en utilisant un mélange de deux isotopes d'hélium liquide pour le bon fonctionnement de certaines familles de processeurs quantiques. Voir cryostat.

Refroidissement d'atomes/ions par laser : Le refroidissement d'atomes par laser est une technique qui permet de refroidir un gaz atomique, jusqu'à des températures de l'ordre du mK (refroidissement Doppler), voire de l'ordre du microkelvin (refroidissement Sisyphe) ou encore du nanokelvin.

Registre quantique : séquence de qubits considérée comme une seule unité, qui peut représenter simultanément jusqu'à 2^n valeurs distinctes par superposition, où n est le nombre de

qubits du registre. Un registre classique, de même taille, constitué de n bits ne peut contenir qu'une seule valeur à un instant donné parmi les 2^n valeurs possibles.

Répéteur quantique : dans le cadre des communications quantiques utilisant des photons (qubits volants) voyageant dans du câble à fibres optiques, les signaux lumineux perdent de la puissance lorsqu'ils parcourent de longues distances. Ceci oblige les chercheurs à utiliser des répéteurs qui poussent et amplifient les signaux afin de transmettre l'information le long d'une ligne mais le défi est de faire cela sans perdre l'information quantique circulant (intrication…).

Réseau quantique : capacité de transmettre des informations quantiques entre des ordinateurs quantiques distants.

Résonateur de couplage : cavité (résonateur) utilisée pour intriquer l'état quantique de deux qubits.

Résonateur optique (ou micro-onde) : dispositif (aussi appelé cavité optique resp. micro-onde) dans lequel certains rayons lumineux (ou micro-ondes) sont susceptibles de rester confinés grâce à des miroirs (resp. parois) sur lesquels ils se réfléchissent. Ces cavités sont indispensables aux lasers pour que leur lumière passe plusieurs fois dans leur milieu amplificateur. Elles sont parfois présentes dans des interféromètres et des oscillateurs paramétriques optiques. Pour les micro-ondes, elles permettent un entrée en résonance et donc une amplification du signal.

Réversibilité (d'une porte logique/opérateur) : toute porte logique est dite réversible si aucune information n'est perdue à son passage, de sorte que les valeurs d'entrée peuvent être déduite de sans ambiguïtés des valeurs de sortie de la porte. Les portes logiques réversibles sont rares en logique classique, mais toutes les portes logiques quantiques (à l'exception des portes d'initialisation et de mesure) sont par définition des portes réversibles.

Révolution Quantique 2.0 : terme utilisé pour décrire la nouvelle vague de technologies quantiques qui utilisent la nature quantique fondamentale des particules, comme la superposition et l'intrication quantique.

RMN : résonance magnétique nucléaire.

RSA : le chiffrement RSA (dont les inventeurs sont Rivest-Shamir-Adleman) est un algorithme de cryptographie asymétrique (à clé publique), très utilisé dans le commerce électronique et plus généralement pour l'échange de données confidentielles sur Internet. L'algorithme de Shor serait susceptible de casser ce code pour peu qu'un ordinateur quantique suffisamment puissant dans un avenir proche.

Rydberg (atome) : En physique quantique, les scientifiques peuvent créer des atomes de Rydberg, l'état excité d'un atome, possédant un ou plusieurs électrons en orbite loin du noyau et dont le nombre quantique principal n (numéro de la couche) est très élevé. Actuellement, on utilise beaucoup des atomes de Rydberg constitués par des atomes de rubidium dans des expériences sur la décohérence quantique à l'aide de cavités optiques.

Semi-conducteur : matériau possédant une bande interdite ni purement isolant ni purement conducteur à température non nulle, et dont il est possible de faire varier les propriétés électroniques. Certains de ses électrons très faiblement liés à leurs atomes peuvent devenir des électrons de conduction. De type N (électrons porteurs de charge majoritaires) ou de type P (trous porteurs de charge majoritaires) selon les dopants utilisés. Les semi-conducteurs appartiennent à trois familles en fonction des groupes de la table périodique auxquels les éléments appartiennent : II-VI, III-V, et IV.

Seuil quantique (théorème du) : propriété selon laquelle la correction des erreurs quantiques peut réussir si le taux d'erreurs physique des portes en logique quantique est inférieur à un certain seuil.

Signal analogique : signal électronique, magnétique, mécanique ou optique qui est interprété comme une valeur continue de tension, de flux magnétique, de force mécanique ou de fréquence électromagnétique, par opposition à la valeur discrète d'un signal numérique (interprétée strictement comme les valeurs binaires classiques de 0 et 1).

Silicium : semi-conducteur le plus répandu utilisé dans la fabrication des circuits intégrés.

Simulateur d'ordinateur quantique : logiciel qui simule le fonctionnement d'un ordinateur quantique sur un ordinateur classique, en simulant l'exécution d'un programme quantique. Le

programme quantique s'exécute généralement beaucoup plus lentement que sur un véritable ordinateur quantique et est rapidement limité en termes de qubits ou d'opération quantiques.

Simulation en chimie : utilisation d'ordinateur quantique pour simuler des molécules et des réactions complexes (ou simples) en chimie.

Simulation hamiltonienne : utilisation d'un ordinateur quantique pour simuler l'énergie totale d'un système quantique, comme une particule ou multi-corps en physique, ou des atomes et des molécules en chimie.

Spin : propriété d'une particule comme peut l'être la charge électrique. Le spin d'une particule est son moment angulaire (ou moment de rotation interne intrinsèque). Le spin est une propriété quantique, il ne peut prendre que des valeurs entières ou demi-entières. Une particule de spin demi-entier est un fermion (par ex. électron), une particule de spin entier est un boson.

Spintronique : discipline qui se fonde sur le spin des électrons.

SQUID : Acronyme de *superconducting quantum interference device* – magnétomètre utilisé pour mesurer des champs magnétiques très faibles. Il est généralement constitué de une (rf-SQUID) ou deux jonctions Josephson (dc-SQUID) montée(s) dans une boucle supraconductrice fermée.

Structure hyperfine : consiste, dans un atome, en une séparation d'un niveau d'énergie en états d'énergie très proches. Ce phénomène est la conséquence de l'interaction entre le dipôle magnétique nucléaire résultant du spin nucléaire et le dipôle magnétique de l'électron (spin).

Substrat isolant : Surface sur laquelle sont fabriqués les composants électroniques et les interconnexions d'un circuit intégré. Isolant, cette surface électriquement neutre, assure que la charge électrique ne peut se déplacer entre les composants électroniques que par des interconnexions explicites.

Superordinateur : ordinateur classique, généralement un serveur, dont les performances et la capacité sont nettement supérieures à celles des serveurs moyens (voir Calcul Haute Performance - HPC).

Superposition (Principe de) : principe de la physique quantique selon lequel un même état quantique peut posséder plusieurs valeurs pour une de ses observables données. C'est l'un des facteurs clés qui permettent aux ordinateurs quantiques de fonctionner et qui permet à un qubit d'avoir une valeur de 0 et de 1 en même temps.

Supraconducteur : métal ou alliage dont la résistivité tombe brusquement à une valeur quasi nulle lorsqu'il est refroidi en dessous d'une température critique. Une autre caractéristique de la supraconductivité est le phénomène d'expulsion du champ magnétique à l'intérieur de certains matériaux supraconducteurs.

Système quantique : désigne dans notre document un objet étudié dans un contexte où ses propriétés quantiques sont intéressantes, par exemple un photon, un ensemble de particules.

Système quantique à plusieurs corps : contenant beaucoup de particules, un tel système peut être complètement caractérisé en mesurant toutes les corrélations entre les particules du système. Un Une molécule chimique ou organique est un bon exemple d'un tel système. Sa modélisation peut être extrêmement difficile à pratiquer et les ordinateurs quantiques pourraient être une solution pour le traitement des cas les plus complexes.

Taux d'erreurs quantique : probabilité qu'une erreur se produise lors de l'exécution d'une porte logique quantique. 1 sur 1 000 pour les opérations à un seul bit et 1 sur 100 pour les opérations à deux bits sont des ordres de grandeur à ce jour.

Téléportation quantique : Transmission de l'état quantique d'un système quantique (une particule ou un photon) sur une distance étendue, généralement pour la communication quantique. Il s'agit en quelque sorte d'une erreur d'appellation puisque la particule ou le photon n'est pas téléporté « physiquement ».

Température cryogénique : Température proche du zéro absolu (mesurée en degrés kelvin (K)). L'hélium gazeux se liquéfie à 4K, ce qui est considéré comme chaud selon les normes cryogéniques. Les ordinateurs quantiques actuels fonctionnent généralement à 15mK ou 20mK (1 mK = 1 millikelvin = 10^{-3}K).

Temps de cohérence (décohérence) : temps écoulé avant qu'un qubit ou un ordinateur quantique ne perde sa cohérence - l'état quantique des qubits commence à se détériorer.

Théorème de Bell : voir **Bell (théorème de)** :

Théorème de non-clonage (ou d'impossibilité du clonage quantique) : voir non-clonage.

Théorie des variables cachées locales : tentative d'explication de la mécanique quantique sans besoin de probabilité en supposant qu'il existe un état supplémentaire, les variables cachées locales, qui explique les probabilités apparentes des états quantiques.

Tolérance aux fautes : Capacité à détecter les erreurs ou les défaillances de composants et à les corriger ou les atténuer afin que le fonctionnement normal puisse se poursuivre comme si aucune erreur n'était survenue. Voir aussi : détection des erreurs, correction des erreurs.

Topologique (ordinateur quantique & qubit) : ordinateur quantique théorique utilisant des qubits construits à partir de tresses quantiques d'anyons (particule de Majorana) avec pour avantage leur longue durée de vie (temps de cohérence) et une plus grande facilité pour corriger les erreurs.

TPU : Tensor Processing Unit, processeurs dédiés au calcul dans les réseaux de neurones artificiels.

Transconjuguée : voir adjointe (matrice).

Transformée de Fourier : formule mathématique complexe qui consiste à évaluer le poids relatif de chaque fréquence présente dans un signal temporel afin d'en donner une représentation spectrale.

Transformée de Fourier quantique : transformée de Fourier discrète adaptée au calcul quantique. Est utilisé dans l'algorithme de Shor lors de sa recherche de décomposition d'un nombre entier en nombres premiers.

Transmon : en informatique quantique, type de qubit de charge dans un supraconducteur conçu pour réduire la sensibilité au bruit de charge.

Treillis (lattice) : arrangement régulier en 2D ou 3D d'objets de tout type, généralement des atomes, des ions et des molécules. Voir cristal. Désigne aussi par extrapolation, un arrangement d'objets plus grands, tels que des systèmes informatiques ou des processeurs au sein d'un système informatique à multiprocesseurs. Enfin suivant le contexte ce terme peut aussi faire référence à un objet mathématique associé à des problèmes d'optimisation (problème de réseau).

Vecteur de base : vecteur à la base d'un espace vectoriel en algèbre linéaire. Tous les autres vecteurs dans l'espace vectoriel peuvent être dérivés comme une combinaison linéaire des vecteurs de base.

Volume quantique : pour certains chercheurs notamment chez IBM, le nombre de qubits seul ne permet pas de capturer la complexité inhérente aux calculateurs quantiques et ils suggèrent que la puissance d'un calculateur quantique soit exprimée par un nombre appelé « volume quantique », qui regrouperait tous les facteurs pertinents, à savoir, le nombre et la connectivité des qubits, la profondeur de l'algorithme utilisé ainsi que d'autres mesures telles que la qualité des portes logiques, notamment le bruit du signal.

VQE : acronyme de *variational quantum eigensolver* - Méthode de calcul des états d'énergie pour des systèmes quantiques réels, par exemple pour la chimie computationnelle

Wafer : tranche fine de silicium sur laquelle sont gravés collectivement des circuits électroniques, puis qui est découpée, afin d'obtenir des circuits intégrés.

WDM : Wavelength Division Multiplexing, (multiplexage en longueur d'onde). Utilisée en communication optique, technique permettant d'augmenter le débit en faisant circuler dans un canal (une fibre, par exemple) des signaux de longueurs d'onde différentes.

Zéro absolu : La température théorique la plus basse, à laquelle tout mouvement et toute chaleur cessent. Zéro degré kelvin – 0.0 K. Sans l'attendre on peut s'en approcher à l'ordre du nano Kelvin. Des températures de l'ordre du mK sont nécessaires pour que l'informatique quantique basée sur les supraconducteurs fonctionne.

LISTE DES FIGURES

SOURCES

[1] É. Klein, *Petit voyage dans le monde des quanta*. Paris: Flammarion, 2009.

[2] F. G. Major, *The quantum beat: Principles and applications of atomic clocks: Second edition*. 2007, p. 479.

[3] « The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail », *Clayton Christensen*. //claytonchristensen.com/books/the-innovators-dilemma/ (consulté le août 05, 2020).

[4] F. Arute *et al.*, « Quantum supremacy using a programmable superconducting processor », *Nature*, vol. 574, nº 7779, p. 505-510, oct. 2019, doi: 10.1038/s41586-019-1666-5.

[5] J. Preskill, « Quantum computing and the entanglement frontier », *arXiv:1203.5813 [cond-mat, physics:quant-ph]*, nov. 2012, Consulté le: sept. 07, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1203.5813.

[6] « On "Quantum Supremacy" », *IBM Research Blog*, oct. 21, 2019. https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/ (consulté le août 30, 2020).

[7] « Chemistry is quantum computing's killer app », *Chemical & Engineering News*. https://cen.acs.org/articles/95/i43/Chemistry-quantum-computings-killer-app.html (consulté le août 31, 2020).

[8] « History of the Haber process », *Wikipedia*. juill. 17, 2020, Consulté le: août 30, 2020. [En ligne]. Disponible sur: https://en.wikipedia.org/w/index.php?title=History_of_the_Haber_process&oldid=968175572.

[9] J. W. Erisman, M. A. Sutton, J. Galloway, Z. Klimont, et W. Winiwarter, « How a century of ammonia synthesis changed the world », *Nature Geoscience*, vol. 1, nº 10, Art. nº 10, oct. 2008, doi: 10.1038/ngeo325.

[10] M. Capdevila-Cortada, « Electrifying the Haber–Bosch », *Nature Catalysis*, vol. 2, nº 12, Art. nº 12, déc. 2019, doi: 10.1038/s41929-019-0414-4.

[11] T. Brown, « Ammonia production causes 1% of total global GHG emissions », *AMMONIA INDUSTRY*, avr. 26, 2016. https://ammoniaindustry.com/ammonia-production-causes-1-percent-of-total-global-ghg-emissions/ (consulté le août 31, 2020).

[12] F. Arute *et al.*, « Hartree-Fock on a superconducting qubit quantum computer », *arXiv:2004.04174 [physics, physics:quant-ph]*, juill. 2020, Consulté le: août 31, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/2004.04174.

[13] « Google CEO Sundar Pichai on achieving quantum supremacy », *MIT Technology Review*. https://www.technologyreview.com/2019/10/23/102523/google-ceo-quantum-supremacy-interview-with-sundar-pichai/ (consulté le sept. 07, 2020).

[14] R. P. Feynman, « Simulating physics with computers », *International Journal of Theoretical Physics*, vol. 21, nº 6-7, p. 467-488, 1982, doi: 10.1007/BF02650179.

[15] S. Frabboni *et al.*, « The Young-Feynman two-slits experiment with single electrons: Build-up of the interference pattern and arrival-time distribution using a fast-readout pixel detector », *Ultramicroscopy*, vol. 116, p. 73-76, mai 2012, doi: 10.1016/j.ultramic.2012.03.017.

[16] B. Brezger, L. Hackermüller, S. Uttenthaler, J. Petschinka, M. Arndt, et A. Zeilinger, « Matter-wave interferometer for large molecules », *Physical Review Letters*, vol. 88, nº 10, p. 1004041-1004044, 2002.

[17] T. Juffmann *et al.*, « Real-time single-molecule imaging of quantum interference », *Nature Nanotechnology*, vol. 7, nº 5, p. 297-300, 2012, doi: 10.1038/nnano.2012.34.

[18] A. Shayeghi *et al.*, « Matter-wave interference of a native polypeptide », *Nature Communications*, vol. 11, nº 1, 2020, doi: 10.1038/s41467-020-15280-2.

[19] T. A. Isaev, « Direct laser cooling of molecules », *Physics-Uspekhi*, vol. 63, nº 3, p. 289-302, 2020, doi: 10.3367/UFNe.2018.12.038509.

[20] L. De Marco, G. Valtolina, K. Matsuda, W. G. Tobias, J. P. Covey, et J. Ye, « A degenerate Fermi

gas of polar molecules », *Science*, vol. 363, nº 6429, p. 853-856, 2019, doi: 10.1126/science.aau7230.

[21] W. Heisenberg, « Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik », *Z. Physik*, vol. 43, nº 3, p. 172-198, mars 1927, doi: 10.1007/BF01397280.

[22] Y. Y. Fein *et al.*, « Quantum superposition of molecules beyond 25 kDa », *Nature Physics*, vol. 15, nº 12, Art. nº 12, déc. 2019, doi: 10.1038/s41567-019-0663-9.

[23] W. K. Wootters et W. H. Zurek, « A single quantum cannot be cloned », *Nature*, vol. 299, nº 5886, Art. nº 5886, oct. 1982, doi: 10.1038/299802a0.

[24] B. Schumacher, « Quantum coding », *Phys. Rev. A*, vol. 51, nº 4, p. 2738-2747, avr. 1995, doi: 10.1103/PhysRevA.51.2738.

[25] G. E. Moore, « Cramming More Components Onto Integrated Circuits », *Proc. IEEE*, vol. 86, nº 1, p. 82-85, janv. 1998, doi: 10.1109/JPROC.1998.658762.

[26] « How Much Information is Stored in the Human Genome? », *Bitesize Bio*, mars 16, 2012. https://bitesizebio.com/8378/how-much-information-is-stored-in-the-human-genome/ (consulté le oct. 12, 2020).

[27] M. Laforest, *The mathematics of quantum mechanics*. University of Waterloo, 2015.

[28] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, et D. J. Wineland, « Demonstration of a Fundamental Quantum Logic Gate », *Phys. Rev. Lett.*, vol. 75, nº 25, p. 4714-4717, déc. 1995, doi: 10.1103/PhysRevLett.75.4714.

[29] C. D. Bruzewicz, J. Chiaverini, R. McConnell, et J. M. Sage, « Trapped-Ion Quantum Computing: Progress and Challenges », *Applied Physics Reviews*, vol. 6, nº 2, p. 021314, juin 2019, doi: 10.1063/1.5088164.

[30] C. Zhang *et al.*, « Submicrosecond entangling gate between trapped ions via Rydberg interaction », *Nature*, vol. 580, nº 7803, Art. nº 7803, avr. 2020, doi: 10.1038/s41586-020-2152-9.

[31] « Honeywell unveils plan for "most powerful" quantum computer ». https://phys.org/news/2020-03-honeywell-unveils-powerful-quantum.html (consulté le mars 04, 2020).

[32] J. M. Pino *et al.*, « Demonstration of the QCCD trapped-ion quantum computer architecture », p. 8.

[33] L. Henriet *et al.*, « Quantum computing with neutral atoms », *arXiv:2006.12326 [quant-ph]*, juin 2020, Consulté le: juill. 29, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/2006.12326.

[34] O. Firstenberg, C. S. Adams, et S. Hofferberth, « Nonlinear quantum optics mediated by Rydberg interactions », *J. Phys. B: At. Mol. Opt. Phys.*, vol. 49, nº 15, p. 152003, juin 2016, doi: 10.1088/0953-4075/49/15/152003.

[35] D. Tiarks, S. Schmidt-Eberle, T. Stolz, G. Rempe, et S. Dürr, « A photon–photon quantum gate based on Rydberg interactions », *Nature Physics*, vol. 15, nº 2, Art. nº 2, févr. 2019, doi: 10.1038/s41567-018-0313-7.

[36] J. A. Gordon, C. L. Holloway, et M. T. Simons, « Rydberg Atom Electric-Field Metrology », nov. 2017, Consulté le: juill. 30, 2020. [En ligne]. Disponible sur: https://www.nist.gov/publications/rydberg-atom-electric-field-metrology.

[37] A. Facon, « Chats de Schrödinger d'un atome de Rydberg pour la métrologie quantique », p. 371.

[38] M. Kjaergaard *et al.*, « Superconducting Qubits: Current State of Play », *Annual Review of Condensed Matter Physics*, vol. 11, nº 1, p. 369-395, 2020, doi: 10.1146/annurev-conmatphys-031119-050605.

[39] H.-L. Huang, D. Wu, D. Fan, et X. Zhu, « Superconducting Quantum Computing: A Review », *arXiv:2006.10433 [quant-ph]*, juin 2020, Consulté le: juill. 30, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/2006.10433.

[40] Y. Wang *et al.*, « Single-qubit quantum memory exceeding ten-minute coherence time », *Nature Photonics*, vol. 11, nº 10, Art. nº 10, oct. 2017, doi: 10.1038/s41566-017-0007-1.

[41] M. Saffman, « Quantum computing with atomic qubits and Rydberg interactions: progress and challenges », *J. Phys. B: At. Mol. Opt. Phys.*, vol. 49, nº 20, p. 202001, oct. 2016, doi:

10.1088/0953-4075/49/20/202001.

[42] C. Sheng *et al.*, « High-Fidelity Single-Qubit Gates on Neutral Atoms in a Two-Dimensional Magic-Intensity Optical Dipole Trap Array », *Phys. Rev. Lett.*, vol. 121, nº 24, p. 240501, déc. 2018, doi: 10.1103/PhysRevLett.121.240501.

[43] J. T. Muhonen *et al.*, « Storing quantum information for 30 seconds in a nanoelectronic device », *Nature Nanotechnology*, vol. 9, nº 12, Art. nº 12, déc. 2014, doi: 10.1038/nnano.2014.211.

[44] X. Rong *et al.*, « Experimental fault-tolerant universal quantum gates with solid-state spins under ambient conditions », *Nature Communications*, vol. 6, nº 1, Art. nº 1, nov. 2015, doi: 10.1038/ncomms9748.

[45] C. E. Bradley *et al.*, « A Ten-Qubit Solid-State Spin Register with Quantum Memory up to One Minute », *Phys. Rev. X*, vol. 9, nº 3, p. 031045, sept. 2019, doi: 10.1103/PhysRevX.9.031045.

[46] H. Wang *et al.*, « Boson Sampling with 20 Input Photons and a 60-Mode Interferometer in a 10^14-Dimensional Hilbert Space », *Phys. Rev. Lett.*, vol. 123, nº 25, p. 250503, déc. 2019, doi: 10.1103/PhysRevLett.123.250503.

[47] J. Koch *et al.*, « Charge-insensitive qubit design derived from the Cooper pair box », *Phys. Rev. A*, vol. 76, nº 4, p. 042319, oct. 2007, doi: 10.1103/PhysRevA.76.042319.

[48] P. Stipsić et M. Milivojević, « Control of a spin qubit in a lateral GaAs quantum dot based on symmetry of gating potential », *Phys. Rev. B*, vol. 101, nº 16, p. 165302, avr. 2020, doi: 10.1103/PhysRevB.101.165302.

[49] M. S. Carroll et T. D. Ladd, « Silicon Qubits », *Encyclopedia of Modern Optics*, vol. 1, Art. nº SAND-2017-5868J, févr. 2018, doi: 10.1016/b978-0-12-803581-8.09736-8.

[50] L. Petit *et al.*, « Universal quantum logic in hot silicon qubits », *Nature*, vol. 580, nº 7803, Art. nº 7803, avr. 2020, doi: 10.1038/s41586-020-2170-7.

[51] C. H. Yang *et al.*, « Operation of a silicon quantum processor unit cell above one kelvin », *Nature*, vol. 580, nº 7803, Art. nº 7803, avr. 2020, doi: 10.1038/s41586-020-2171-6.

[52] D. A. Hopper, H. J. Shulevitz, et L. C. Bassett, « Spin Readout Techniques of the Nitrogen-Vacancy Center in Diamond », *Micromachines*, vol. 9, nº 9, Art. nº 9, sept. 2018, doi: 10.3390/mi9090437.

[53] « Le diamant, plus précieux qu'on ne croit | Thales Group ». https://www.thalesgroup.com/fr/monde/magazine/le-diamant-plus-precieux-quon-ne-croit (consulté le juill. 30, 2020).

[54] D. Le Sage *et al.*, « Optical magnetic imaging of living cells », *Nature*, vol. 496, nº 7446, Art. nº 7446, avr. 2013, doi: 10.1038/nature12072.

[55] A. Tchebotareva *et al.*, « Entanglement between a diamond spin qubit and a photonic time-bin qubit at telecom wavelength », *Phys. Rev. Lett.*, vol. 123, nº 6, p. 063601, août 2019, doi: 10.1103/PhysRevLett.123.063601.

[56] J. N. Becker et E. Neu, « Chapter Seven - The silicon vacancy center in diamond », in *Semiconductors and Semimetals*, vol. 103, C. E. Nebel, I. Aharonovich, N. Mizuochi, et M. Hatano, Éd. Elsevier, 2020, p. 201-235.

[57] H. Bartolomei *et al.*, « Fractional statistics in anyon collisions », *Science*, vol. 368, nº 6487, p. 173-177, avr. 2020, doi: 10.1126/science.aaz5601.

[58] J. Nakamura, S. Liang, G. C. Gardner, et M. J. Manfra, « Direct observation of anyonic braiding statistics at the ν=1/3 fractional quantum Hall state », *arXiv:2006.14115 [cond-mat]*, juin 2020, Consulté le: sept. 02, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/2006.14115.

[59] M. Houzet, J. Meyer, et P. Simon, « Le spectre de Majorana: Des quasi-particules exotiques découvertes dans des nanostructures supraconductrices pourraient servir à construire un ordinateur quantique », *Reflets phys.*, nº 61, p. 4-10, mars 2019, doi: 10.1051/refdp/201961004.

[60] G. P. Collins, « Computing with Quantum Knots », *Sci Am*, vol. 294, nº 4, p. 56-63, avr. 2006, doi: 10.1038/scientificamerican0406-56.

[61] H.-H. Lu *et al.*, « Quantum Phase Estimation with Time-Frequency Qudits in a Single Photon »,

Advanced Quantum Technologies, vol. 3, nº 2, p. 1900074, 2020, doi: 10.1002/qute.201900074.

[62] P. Imany *et al.*, « High-dimensional optical quantum logic in large operational spaces », *npj Quantum Information*, vol. 5, nº 1, Art. nº 1, juill. 2019, doi: 10.1038/s41534-019-0173-8.

[63] E. Knill, R. Laflamme, et G. J. Milburn, « A scheme for efficient quantum computation with linear optics », *Nature*, vol. 409, nº 6816, Art. nº 6816, janv. 2001, doi: 10.1038/35051009.

[64] M. L. Bellac, *Le monde quantique*. EDP SCIENCES, 2010.

[65] M. Heuck, K. Jacobs, et D. R. Englund, « Controlled-Phase Gate Using Dynamically Coupled Cavities and Optical Nonlinearities », *Phys. Rev. Lett.*, vol. 124, nº 16, p. 160501, avr. 2020, doi: 10.1103/PhysRevLett.124.160501.

[66] « The potential and challenges of time-resolved single-photon detection based on current-carrying superconducting nanowires - IOPscience ». https://iopscience.iop.org/article/10.1088/1361-6463/ab4146 (consulté le juill. 31, 2020).

[67] T. Polakovic, W. Armstrong, G. Karapetrov, Z.-E. Meziani, et V. Novosad, « Unconventional Applications of Superconducting Nanowire Single Photon Detectors », *Nanomaterials*, vol. 10, nº 6, Art. nº 6, juin 2020, doi: 10.3390/nano10061198.

[68] S. Slussarenko et G. J. Pryde, « Photonic quantum information processing: a concise review », *Applied Physics Reviews*, vol. 6, nº 4, p. 041303, déc. 2019, doi: 10.1063/1.5115814.

[69] G. Koolstra, G. Yang, et D. I. Schuster, « Coupling a single electron on superfluid helium to a superconducting resonator », *Nature Communications*, vol. 10, nº 1, Art. nº 1, nov. 2019, doi: 10.1038/s41467-019-13335-7.

[70] D. I. Schuster, A. Fragner, M. I. Dykman, S. A. Lyon, et R. J. Schoelkopf, « Proposal for Manipulating and Detecting Spin and Orbital States of Trapped Electrons on Helium Using Cavity Quantum Electrodynamics », *Phys. Rev. Lett.*, vol. 105, nº 4, p. 040503, juill. 2010, doi: 10.1103/PhysRevLett.105.040503.

[71] Anonymous, « New Strategic Research Agenda on Quantum technologies », *Shaping Europe's digital future - European Commission*, mars 03, 2020. https://ec.europa.eu/digital-single-market/en/news/new-strategic-research-agenda-quantum-technologies (consulté le mars 24, 2020).

[72] OIDA, « OIDA Quantum Photonics Roadmap: Every Photon Counts », *OIDA Reports*, p. 3, mars 2020.

[73] S. M. Brewer *et al.*, « Al+ 27 Quantum-Logic Clock with a Systematic Uncertainty below 10-18 », *Physical Review Letters*, vol. 123, nº 3, 2019, doi: 10.1103/PhysRevLett.123.033201.

[74] A. D. Ludlow, M. M. Boyd, J. Ye, E. Peik, et P. O. Schmidt, « Optical atomic clocks », *Rev. Mod. Phys.*, vol. 87, nº 2, p. 637-701, juin 2015, doi: 10.1103/RevModPhys.87.637.

[75] Z. L. Newman *et al.*, « Architecture for the photonic integration of an optical atomic clock », *Optica, OPTICA*, vol. 6, nº 5, p. 680-685, mai 2019, doi: 10.1364/OPTICA.6.000680.

[76] CEA, « Révolutions quantiques - N°66 », *CEA/Médiathèque*, juin 14, 2018. http://www.cea.fr/multimedia/Pages/editions/clefs-cea/revolutions-quantiques.aspx (consulté le mars 09, 2020).

[77] V. Ménoret *et al.*, « Gravity measurements below 10 −9 g with a transportable absolute quantum gravimeter », *Scientific Reports*, vol. 8, nº 1, Art. nº 1, août 2018, doi: 10.1038/s41598-018-30608-1.

[78] L. Pezzè, A. Smerzi, M. K. Oberthaler, R. Schmied, et P. Treutlein, « Quantum metrology with nonclassical states of atomic ensembles », *Rev. Mod. Phys.*, vol. 90, nº 3, p. 035005, sept. 2018, doi: 10.1103/RevModPhys.90.035005.

[79] M. Keil, O. Amit, S. Zhou, D. Groswasser, Y. Japha, et R. Folman, « Fifteen years of cold matter on the atom chip: promise, realizations, and prospects », *J Mod Opt*, vol. 63, nº 18, p. 1840-1885, oct. 2016, doi: 10.1080/09500340.2016.1178820.

[80] A. Boretti, L. Rosa, J. Blackledge, et S. Castelletto, « Nitrogen-vacancy centers in diamond for nanoscale magnetic resonance imaging applications », *Beilstein J. Nanotechnol.*, vol. 10, nº 1, p.

2128-2151, nov. 2019, doi: 10.3762/bjnano.10.207.

[81] « Aircraft navigation - Magnetometers based on diamonds will make navigation easier | Science & technology | The Economist ». https://www.economist.com/science-and-technology/2020/07/18/magnetometers-based-on-diamonds-will-make-navigation-easier (consulté le juill. 18, 2020).

[82] A. Kuwahata *et al.*, « Magnetometer with nitrogen-vacancy center in a bulk diamond for detecting magnetic nanoparticles in biomedical applications », *Scientific Reports*, vol. 10, nº 1, Art. nº 1, févr. 2020, doi: 10.1038/s41598-020-59064-6.

[83] G. Kucsko *et al.*, « Nanometre-scale thermometry in a living cell », *Nature*, vol. 500, nº 7460, Art. nº 7460, août 2013, doi: 10.1038/nature12373.

[84] K. Okabe, R. Sakaguchi, B. Shi, et S. Kiyonaka, « Intracellular thermometry with fluorescent sensors for thermal biology », *Pflugers Arch - Eur J Physiol*, vol. 470, nº 5, p. 717-731, mai 2018, doi: 10.1007/s00424-018-2113-4.

[85] D. Halbertal *et al.*, « Nanoscale thermal imaging of dissipation in quantum systems », *Nature*, vol. 539, nº 7629, Art. nº 7629, nov. 2016, doi: 10.1038/nature19843.

[86] C. Zhang *et al.*, « Photonic thermometer with a sub-millikelvin resolution and broad temperature range by waveguide-microring Fano resonance », *Optics Express*, vol. 28, nº 9, p. 12599-12608, 2020, doi: 10.1364/OE.390966.

[87] pamela.corey@nist.gov, « Photonic Thermometry », *NIST*, mars 15, 2016. https://www.nist.gov/programs-projects/photonic-thermometry (consulté le sept. 03, 2020).

[88] L. Maccone et C. Ren, « Quantum Radar », *Phys. Rev. Lett.*, vol. 124, nº 20, p. 200503, mai 2020, doi: 10.1103/PhysRevLett.124.200503.

[89] S. Barzanjeh, S. Pirandola, D. Vitali, et J. M. Fink, « Microwave quantum illumination using a digital receiver », *Science Advances*, vol. 6, nº 19, p. eabb0451, mai 2020, doi: 10.1126/sciadv.abb0451.

[90] H. Vella, « Could quantum radars expose stealth planes? », avr. 18, 2019. https://eandt.theiet.org/content/articles/2019/04/could-quantum-radars-expose-stealth-planes/ (consulté le juill. 23, 2020).

[91] J. H. Shapiro, « The Quantum Illumination Story », *arXiv:1910.12277 [quant-ph]*, déc. 2019, Consulté le: sept. 03, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1910.12277.

[92] Z.-P. Li *et al.*, « Single-photon computational 3D imaging at 45 km », *Photon. Res.*, vol. 8, nº 9, p. 1532, sept. 2020, doi: 10.1364/PRJ.390091.

[93] M. Penasa, « Mesure au-delà de la limite quantique standard de l'amplitude d'un champ électromagnétique dans le domaine micro-onde », phdthesis, Université Pierre et Marie Curie - Paris VI, 2016.

[94] « Les enjeux de la 5G pour les objets connectés ». https://www.journaldunet.com/ebusiness/internet-mobile/1492531-tribune-libre-les-enjeux-de-la-5g-pour-les-objets-connectes/ (consulté le août 07, 2020).

[95] A. Weissberger, « Gartner: 5G IoT endpoints to triple between 2020 and 2021; Surveillance cameras to be largest market over next 3 years », *Technology Blog*, oct. 17, 2019. https://techblog.comsoc.org/2019/10/17/gartner-5g-iot-endpoints-to-triple-between-2020-and-2021-surveillance-cameras-to-be-largest-market-over-next-3-years/ (consulté le août 08, 2020).

[96] P. Guillot, *La cryptologie - L'art des codes secrets*, Librairie Eyrolles. .

[97] P. W. Shor, « Algorithms for quantum computation: discrete logarithms and factoring », in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, nov. 1994, p. 124-134, doi: 10.1109/SFCS.1994.365700.

[98] E. National Academies of Sciences, *Quantum Computing: Progress and Prospects*. 2018.

[99] « Quantum safe cryptography - the big picture », *Fact Based Insight*, mai 11, 2020. https://www.factbasedinsight.com/quantum-safe-cryptography-the-big-picture/ (consulté le mai 14, 2020).

[100] C. Gidney et M. Ekerå, « How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits », *arXiv:1905.09749 [quant-ph]*, déc. 2019, Consulté le: avr. 28, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1905.09749.

[101] F. Wilhelm, R. Steinwandt, B. Langenberg, P. Liebermann, A. Messinger, et P. Schuhmacher, « Entwicklungsstand Quantencomputer », 2019. https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer.html (consulté le juill. 31, 2020).

[102] « Quantum Threat Timeline », *Global Risk Institute*. https://globalriskinstitute.org/publications/quantum-threat-timeline/ (consulté le juin 30, 2020).

[103] « Le gouvernement du Kazakhstan a commencé à intercepter tout le trafic Internet HTTPS dans ses frontières, ce qui peut créer un dangereux précédent », *Developpez.com*. https://web.developpez.com/actu/270450/Le-gouvernement-du-Kazakhstan-a-commence-a-intercepter-tout-le-trafic-Internet-HTTPS-dans-ses-frontieres-ce-qui-peut-creer-un-dangereux-precedent/ (consulté le mars 11, 2020).

[104] « The Internet Society's Concerns on the Recent Government Action in Kazakhstan Regarding Encrypted Internet Traffic | Internet Society ». https://www.internetsociety.org/news/statements/2019/internet-society-concerns-kazakhstan-encryption (consulté le mars 11, 2020).

[105] M. Mosca, « Cybersecurity in a quantum world: will we be ready? », p. 44.

[106] M. Herrero-Collantes et J. C. Garcia-Escartin, « Quantum random number generators », *Rev. Mod. Phys.*, vol. 89, nº 1, p. 015004, févr. 2017, doi: 10.1103/RevModPhys.89.015004.

[107] P. X. Wang, G. L. Long, et Y. S. Li, « Scheme for a quantum random number generator », *Journal of Applied Physics*, vol. 100, nº 5, p. 056107, sept. 2006, doi: 10.1063/1.2338830.

[108] M. Naruse *et al.*, « Single-photon decision maker », *Scientific Reports*, vol. 5, nº 1, Art. nº 1, août 2015, doi: 10.1038/srep13253.

[109] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, et O. Benson, « An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements », *Appl. Phys. Lett.*, vol. 98, nº 17, p. 171105, avr. 2011, doi: 10.1063/1.3578456.

[110] « Quantum random-number generator based on a photon-number-resolving detector | Request PDF », *ResearchGate*. https://www.researchgate.net/publication/235512701_Quantum_random-number_generator_based_on_a_photon-number-resolving_detector (consulté le août 25, 2020).

[111] X. Ma, X. Yuan, Z. Cao, B. Qi, et Z. Zhang, « Quantum random number generation », *npj Quantum Inf*, vol. 2, nº 1, p. 16021, nov. 2016, doi: 10.1038/npjqi.2016.21.

[112] B. Sanguinetti, A. Martin, H. Zbinden, et N. Gisin, « Quantum random number generation on a mobile phone », *Phys. Rev. X*, vol. 4, nº 3, p. 031056, sept. 2014, doi: 10.1103/PhysRevX.4.031056.

[113] « ID Quantique & SK Telecom announce first QRNG 5G smartphone », *ID Quantique*, mai 13, 2020. https://www.idquantique.com/id-quantique-and-sk-telecom-announce-the-worlds-first-5g-smartphone-equipped-with-a-quantum-random-number-generator-qrng-chipset/ (consulté le juin 30, 2020).

[114] E. Diamanti, « Progrés et défis pour la cryptographie quantique », *Photoniques*, nº 91, p. 33-37, mai 2018, doi: 10.1051/photon/20189133.

[115] C. E. Shannon, « Communication theory of secrecy systems », *The Bell System Technical Journal*, vol. 28, nº 4, p. 656-715, oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[116] S. Pirandola *et al.*, « Advances in Quantum Cryptography », *arXiv:1906.01645 [math-ph, physics:physics, physics:quant-ph]*, juin 2019, Consulté le: févr. 11, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1906.01645.

[117] V. Zapatero et M. Curty, « Long-distance device-independent quantum key distribution », *Scientific Reports*, vol. 9, nº 1, Art. nº 1, nov. 2019, doi: 10.1038/s41598-019-53803-0.

[118] R. Valivarthi *et al.*, « Measurement-device-independent quantum key distribution coexisting with classical communication », *Quantum Sci. Technol.*, vol. 4, nº 4, p. 045002, juill. 2019, doi:

10.1088/2058-9565/ab2e62.

[119] E. Diamanti, H.-K. Lo, B. Qi, et Z. Yuan, « Practical challenges in quantum key distribution », *npj Quantum Inf*, vol. 2, nº 1, p. 16025, nov. 2016, doi: 10.1038/npjqi.2016.25.

[120] « Unhackable Chinese Communication Network Launches Soon », *EDGY_ Labs*, juill. 25, 2017. https://edgy.app/unhackable-chinese-communication-network-soon (consulté le août 31, 2020).

[121] A. Boaron *et al.*, « Secure Quantum Key Distribution over 421 km of Optical Fiber », *Phys. Rev. Lett.*, vol. 121, nº 19, p. 190502, nov. 2018, doi: 10.1103/PhysRevLett.121.190502.

[122] J.-P. Chen *et al.*, « Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km », *Phys. Rev. Lett.*, vol. 124, nº 7, p. 070501, févr. 2020, doi: 10.1103/PhysRevLett.124.070501.

[123] S.-K. Liao *et al.*, « Satellite-to-ground quantum key distribution », *Nature*, vol. 549, nº 7670, Art. nº 7670, sept. 2017, doi: 10.1038/nature23655.

[124] S. Wengerowsky *et al.*, « In-field entanglement distribution over a 96 km-long submarine optical fibre », *Proc Natl Acad Sci USA*, vol. 116, nº 14, p. 6684-6688, avr. 2019, doi: 10.1073/pnas.1818752116.

[125] « Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography - Aktas - 2016 - Laser & Photonics Reviews - Wiley Online Library ». https://onlinelibrary.wiley.com/doi/full/10.1002/lpor.201500258?casa_token=vLxbI3XKCzUAAAAA%3AIVhLuIWQS1tkh_mNlDKU3srVPqaFWqnKP_BOHmyIDUDQ0IOjEVWMINWYr1oT8-7gD37H12y1e6ty (consulté le août 31, 2020).

[126] J. Yin *et al.*, « Satellite-based entanglement distribution over 1200 kilometers », *Science*, vol. 356, nº 6343, p. 1140-1144, juin 2017, doi: 10.1126/science.aan3211.

[127] « La nouvelle révolution quantique... - Hors-série Pour la Science Avril 2020 - N°107 ». https://boutique.pourlascience.fr/tous-les-numeros/hors-serie-pour-la-science/dossiers-pour-la-science-107-mai-juin-2020.html (consulté le avr. 28, 2020).

[128] P. 26 O. 2016 | 15:00 GMT, « China's 2,000-km Quantum Link Is Almost Complete - IEEE Spectrum », *IEEE Spectrum: Technology, Engineering, and Science News*. https://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete (consulté le août 31, 2020).

[129] W. Munro, K. Azuma, K. Tamaki, et K. Nemoto, « Inside Quantum Repeaters », *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, p. 1-13, mai 2015, doi: 10.1109/JSTQE.2015.2392076.

[130] F. Rozpędek *et al.*, « Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission », *Phys. Rev. A*, vol. 99, nº 5, p. 052330, mai 2019, doi: 10.1103/PhysRevA.99.052330.

[131] Z.-D. Li *et al.*, « Experimental quantum repeater without quantum memory », *Nature Photonics*, vol. 13, nº 9, Art. nº 9, sept. 2019, doi: 10.1038/s41566-019-0468-5.

[132] N. Gisin, « Quantum-teleportation experiments turn 20 », *Nature*, vol. 552, nº 7683, Art. nº 7683, déc. 2017, doi: 10.1038/d41586-017-07689-5.

[133] D. Awschalom *et al.*, « Development of Quantum InterConnects for Next-Generation Information Technologies », *arXiv:1912.06642 [quant-ph]*, janv. 2020, Consulté le: août 31, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1912.06642.

[134] I. Khan, B. Heim, A. Neuzner, et C. Marquardt, « Satellite-Based QKD », *Optics & Photonics News, OPN*, vol. 29, nº 2, p. 26-33, févr. 2018, doi: 10.1364/OPN.29.2.000026.

[135] J. Yin *et al.*, « Entanglement-based secure quantum cryptography over 1,120 kilometres », *Nature*, vol. 582, nº 7813, p. 501-505, juin 2020, doi: 10.1038/s41586-020-2401-y.

[136] E. Diamanti, « A step closer to secure global communication », *Nature*, vol. 582, nº 7813, Art. nº 7813, juin 2020, doi: 10.1038/d41586-020-01779-7.

[137] H.-Y. Liu *et al.*, « Drone-based all-weather entanglement distribution », *National Science Review*, vol. 7, nº 5, p. 921-928, mai 2020, doi: 10.1093/nsr/nwz227.

[138] P. Sibson *et al.*, « Chip-based quantum key distribution », *Nature Communications*, vol. 8, nº 1, Art. nº 1, févr. 2017, doi: 10.1038/ncomms13984.

[139] T. Morimae, « Blind quantum computing can always be made verifiable », *arXiv:1803.06624 [quant-ph]*, mars 2018, Consulté le: sept. 04, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1803.06624.

[140] S. Wehner, D. Elkouss, et R. Hanson, « Quantum internet: A vision for the road ahead », *Science*, vol. 362, nº 6412, oct. 2018, doi: 10.1126/science.aam9288.

[141] V. Krutyanskiy, M. Meraner, J. Schupp, V. Krcmarsky, H. Hainzer, et B. P. Lanyon, « Light-matter entanglement over 50 km of optical fibre », *npj Quantum Information*, vol. 5, nº 1, Art. nº 1, août 2019, doi: 10.1038/s41534-019-0186-3.

[142] Collectif, J. Hennessy, et D.-A. Patterson, *Computer Architecture : A Quantitative Approach*. Cambridge, MA: Morgan Kaufmann Publishers In, 2017.

[143] C. E. Leiserson *et al.*, « There's plenty of room at the Top: What will drive computer performance after Moore's law? », *Science*, vol. 368, nº 6495, juin 2020, doi: 10.1126/science.aam9744.

[144] O. Ezratty, « L'ebook pour comprendre l'informatique quantique », *Opinions Libres - Le blog d'Olivier Ezratty*, https://www.oezratty.net/wordpress/2020/comprendre-informatique-quantique-edition-2020/.

[145] « Atos lance son nouvel émulateur quantique QLM-E. », *InformatiqueNews.fr*, juin 24, 2020. https://www.informatiquenews.fr/atos-lance-son-nouvel-emulateur-quantique-qlm-e-71370 (consulté le sept. 18, 2020).

[146] Z.-Y. Chen, Q. Zhou, C. Xue, X. Yang, G.-C. Guo, et G.-P. Guo, « 64-qubit quantum circuit simulation », *Science Bulletin*, vol. 63, nº 15, p. 964-971, août 2018, doi: 10.1016/j.scib.2018.06.007.

[147] « Why Did NASA, Lockheed Martin, and Others Spend Millions on This Quantum Computer? », *Gizmodo*. https://gizmodo.com/why-did-nasa-lockheed-martin-and-others-spend-million-1826241515 (consulté le sept. 17, 2020).

[148] J. Preskill, « Quantum Computing in the NISQ era and beyond », *Quantum*, vol. 2, p. 79, août 2018, doi: 10.22331/q-2018-08-06-79.

[149] D. P. DiVincenzo, « The Physical Implementation of Quantum Computation », *Fortschritte der Physik*, vol. 48, nº 9-11, p. 771-783, 2000, doi: 10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E.

[150] « Quantum computers vastly outperform supercomputers when it comes to energy efficiency », *Physics World*, mai 01, 2020. https://physicsworld.com/a/quantum-computers-vastly-outperform-supercomputers-when-it-comes-to-energy-efficiency/ (consulté le mai 08, 2020).

[151] K. Michielsen, M. Nocon, D. Willsch, F. Jin, T. Lippert, et H. De Raedt, « Benchmarking gate-based quantum computers », *Computer Physics Communications*, vol. 220, p. 44-55, nov. 2017, doi: 10.1016/j.cpc.2017.06.011.

[152] S. J. Devitt, K. Nemoto, et W. J. Munro, « Quantum Error Correction for Beginners », *Rep. Prog. Phys.*, vol. 76, nº 7, p. 076001, juill. 2013, doi: 10.1088/0034-4885/76/7/076001.

[153] J. Li, « Some Progress on Quantum Error Correction for Discrete and Continuous Error Models », *IEEE Access*, vol. 8, p. 46998-47012, 2020, doi: 10.1109/ACCESS.2020.2977344.

[154] J. Roffe, « Quantum Error Correction: An Introductory Guide », *Contemporary Physics*, vol. 60, nº 3, p. 226-245, juill. 2019, doi: 10.1080/00107514.2019.1667078.

[155] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, et W. K. Wootters, « Mixed-state entanglement and quantum error correction », *Phys. Rev. A*, vol. 54, nº 5, p. 3824-3851, nov. 1996, doi: 10.1103/PhysRevA.54.3824.

[156] R. Laflamme, C. Miquel, J. P. Paz, et W. H. Zurek, « Perfect Quantum Error Correction Code », *arXiv:quant-ph/9602019*, févr. 1996, Consulté le: sept. 22, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/quant-ph/9602019.

[157] A. M. Steane, « Error Correcting Codes in Quantum Theory », *Phys. Rev. Lett.*, vol. 77, nº 5, p.

793-797, juill. 1996, doi: 10.1103/PhysRevLett.77.793.

[158] P. W. Shor, « Scheme for reducing decoherence in quantum computer memory », *Phys. Rev. A*, vol. 52, nº 4, p. R2493-R2496, oct. 1995, doi: 10.1103/PhysRevA.52.R2493.

[159] R. Barends *et al.*, « Superconducting quantum circuits at the surface code threshold for fault tolerance », 2014, doi: 10.1038/nature13171.

[160] A. G. Fowler, M. Mariantoni, J. M. Martinis, et A. N. Cleland, « Surface codes: Towards practical large-scale quantum computation », 2012, doi: 10.1103/PhysRevA.86.032324.

[161] Z. Cai, M. A. Fogarty, S. Schaal, S. Patomaki, S. C. Benjamin, et J. J. L. Morton, « A Silicon Surface Code Architecture Resilient Against Leakage Errors », *Quantum*, vol. 3, p. 212, déc. 2019, doi: 10.22331/q-2019-12-09-212.

[162] D. Litinski, « Magic State Distillation: Not as Costly as You Think », *Quantum*, vol. 3, p. 205, déc. 2019, doi: 10.22331/q-2019-12-02-205.

[163] H. Bombin et M. A. Martin-Delgado, « Topological Computation without Braiding », *Phys. Rev. Lett.*, vol. 98, nº 16, p. 160502, avr. 2007, doi: 10.1103/PhysRevLett.98.160502.

[164] « Dynamic Concatenation of Quantum Error Correction in Integrated Quantum Computing Architecture | Scientific Reports ». https://www.nature.com/articles/s41598-019-39439-0 (consulté le oct. 02, 2020).

[165] J. M. Arrazola, A. Delgado, B. R. Bardhan, et S. Lloyd, « Quantum-inspired algorithms in practice », *Quantum*, vol. 4, p. 307, août 2020, doi: 10.22331/q-2020-08-13-307.

[166] L. K. Grover, « A fast quantum mechanical algorithm for database search », *arXiv:quant-ph/9605043*, nov. 1996, Consulté le: avr. 01, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/quant-ph/9605043.

[167] « Relever le défi de la résolution de l'équation de Schrödinger - L'Actualité Chimique ». https://www.lactualitechimique.org/Relever-le-defi-de-la-resolution-de-l-equation-de-Schrodinger (consulté le sept. 26, 2020).

[168] M. Reiher, N. Wiebe, K. M. Svore, D. Wecker, et M. Troyer, « Elucidating reaction mechanisms on quantum computers », *PNAS*, vol. 114, nº 29, p. 7555-7560, juill. 2017, doi: 10.1073/pnas.1619152114.

[169] S. McArdle, S. Endo, A. Aspuru-Guzik, S. Benjamin, et X. Yuan, « Quantum computational chemistry », *Rev. Mod. Phys.*, vol. 92, nº 1, p. 015003, mars 2020, doi: 10.1103/RevModPhys.92.015003.

[170] Y. Cao, J. Romero, et A. Aspuru-Guzik, « Potential of quantum computing for drug discovery », *IBM Journal of Research and Development*, vol. 62, nº 6, p. 6:1-6:20, nov. 2018, doi: 10.1147/JRD.2018.2888987.

[171] C. R. F.-04/09/2018 2 mins-Industrial, « Semi-Artificial Photosynthesis Method Produces Fuel More Efficiently Than Nature », *Labiotech.eu*, sept. 04, 2018. https://www.labiotech.eu/industrial/semi-artificial-photosynthesis-fuel/ (consulté le sept. 29, 2020).

[172] « Quantum techniques to enhance solar cell efficiency ». https://spie.org/news/6386-quantum-techniques-to-enhance-solar-cell-efficiency (consulté le sept. 26, 2020).

[173] « Cuprates ». http://www.supraconductivite.fr/fr/index.php?p=recherche-nouveaux-cuprates (consulté le sept. 26, 2020).

[174] « Volkswagen tests quantum computing in battery research », *Volkswagen Newsroom*. https://www.volkswagen-newsroom.com:443/en/press-releases/volkswagen-tests-quantum-computing-in-battery-research-351 (consulté le sept. 27, 2020).

[175] M. Streif, F. Neukart, et M. Leib, « Solving Quantum Chemistry Problems with a D-Wave Quantum Annealer », *arXiv:1811.05256 [quant-ph]*, mars 2019, Consulté le: sept. 27, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1811.05256.

[176] « Accenture et Biogen collaborent pour la découverte de médicaments ». https://www.accenture.com/fr-fr/company-news-release-accenture-biogen-collaborate-drug-

discovery (consulté le févr. 11, 2020).

[177] J. Cumbers, « Five Things Big Pharma—And Its Investors—Could Learn From Synthetic Biology », *Forbes*. https://www.forbes.com/sites/johncumbers/2020/05/11/five-things-big-pharma-and-its-investors-could-learn-from-synthetic-biology/ (consulté le sept. 28, 2020).

[178] D. J. Egger *et al.*, « Quantum computing for Finance: state of the art and future prospects », *arXiv:2006.14510 [quant-ph, q-fin]*, juin 2020, Consulté le: juill. 01, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/2006.14510.

[179] A. Kandala *et al.*, « Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets », *Nature*, vol. 549, nº 7671, Art. nº 7671, sept. 2017, doi: 10.1038/nature23879.

[180] A. Peruzzo *et al.*, « A variational eigenvalue solver on a photonic quantum processor », 2014, doi: 10.1038/ncomms5213.

[181] N. Moll *et al.*, « Quantum optimization using variational algorithms on near-term quantum devices », *Quantum Sci. Technol.*, vol. 3, nº 3, p. 030503, juill. 2018, doi: 10.1088/2058-9565/aab822.

[182] A. Ajagekar et F. You, « Quantum computing for energy systems optimization: Challenges and opportunities », *Energy*, vol. 179, p. 76-89, juill. 2019, doi: 10.1016/j.energy.2019.04.186.

[183] G. Carleo *et al.*, « Machine learning and the physical sciences », *Rev. Mod. Phys.*, vol. 91, nº 4, p. 045002, déc. 2019, doi: 10.1103/RevModPhys.91.045002.

[184] V. Havlíček *et al.*, « Supervised learning with quantum-enhanced feature spaces », *Nature*, vol. 567, nº 7747, Art. nº 7747, mars 2019, doi: 10.1038/s41586-019-0980-2.

[185] D. Willsch, M. Willsch, H. De Raedt, et K. Michielsen, « Support vector machines on the D-Wave quantum annealer », *Computer Physics Communications*, vol. 248, 2020, doi: 10.1016/j.cpc.2019.107006.

[186] E. Farhi, J. Goldstone, et S. Gutmann, « A Quantum Approximate Optimization Algorithm », *arXiv:1411.4028 [quant-ph]*, nov. 2014, Consulté le: sept. 30, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1411.4028.

[187] I. Kerenidis et A. Prakash, « Quantum Recommendation Systems », *arXiv:1603.08675 [quant-ph]*, sept. 2016, Consulté le: sept. 30, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1603.08675.

[188] I. Kerenidis, J. Landman, et A. Prakash, « Quantum Algorithms for Deep Convolutional Neural Networks », *arXiv:1911.01117 [quant-ph]*, nov. 2019, Consulté le: sept. 30, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1911.01117.

[189] C. Ciliberto *et al.*, « Quantum machine learning: a classical perspective », *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 474, nº 2209, p. 20170551, janv. 2018, doi: 10.1098/rspa.2017.0551.

[190] G. Cybenko, « Approximation by superpositions of a sigmoidal function », *Math. Control Signal Systems*, vol. 2, nº 4, p. 303-314, déc. 1989, doi: 10.1007/BF02551274.

[191] Y. Cao, G. G. Guerreschi, et A. Aspuru-Guzik, « Quantum Neuron: an elementary building block for machine learning on quantum computers », *arXiv:1711.11240 [quant-ph]*, nov. 2017, Consulté le: sept. 30, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1711.11240.

[192] E. Tang, « A quantum-inspired classical algorithm for recommendation systems », *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing - STOC 2019*, p. 217-228, 2019, doi: 10.1145/3313276.3316310.

[193] « Japan's Fugaku Tops Global Supercomputing Rankings », *HPCwire*, juin 23, 2020. https://www.hpcwire.com/2020/06/22/japans-fugaku-tops-supercomputing-list-415-petaflops/ (consulté le sept. 30, 2020).

[194] « How Much Power Will Quantum Computing Need? - IEEE Spectrum », *IEEE Spectrum: Technology, Engineering, and Science News*. https://spectrum.ieee.org/tech-talk/computing/hardware/how-much-power-will-quantum-computing-need (consulté le sept. 30, 2020).

[195] D-Wave Systems, « Computational Power Consumption and Speedup », *White-paper Series 2017*, 2017, Consulté le: sept. 30, 2020. [En ligne]. Disponible sur: https://www.dwavesys.com/sites/default/files/14-1005A_D_wp_Computational_Power_Consumption_and_Speedup.pdf.

[196] « Solvay Institutes ». http://www.solvayinstitutes.be/html/solvayconference.html (consulté le mai 29, 2020).

[197] « President Trump has signed a $1.2 billion law to boost US quantum tech », *MIT Technology Review*. https://www.technologyreview.com/2018/12/22/138149/president-trump-has-signed-a-12-billon-law-to-boost-us-quantum-tech/ (consulté le juin 10, 2020).

[198] D. Castelvecchi, « Europe shows first cards in €1-billion quantum bet », *Nature*, vol. 563, nº 7729, Art. nº 7729, oct. 2018, doi: 10.1038/d41586-018-07216-0.

[199] E. Gibney, « Quantum gold rush: the private funding pouring into quantum start-ups », *Nature*, vol. 574, nº 7776, Art. nº 7776, oct. 2019, doi: 10.1038/d41586-019-02935-4.

[200] UK IP Office Informatics Team, « Eight Great Technologies: Quantum Technologies - a patent overview », p. 52.

[201] R. Winiarczyk, P. Gawron, J. A. Miszczak, Ł. Pawela, et Z. Puchała, « Analysis of patent activity in the field of quantum information processing », *Int. J. Quantum Inform.*, vol. 11, nº 01, p. 1350007, févr. 2013, doi: 10.1142/S021974991350007X.

[202] UK IP Office Patent Informatics Team, « Quantum Technologies - A patent review for the Engineering and Physical Sciences Research Council », p. 28.

[203] M. Travagnin, European Commission, et Joint Research Centre, *Patent analysis of selected quantum technologies*. 2019.

[204] « U.S. Leads World in Quantum Computing Patent Filings with IBM Leading the Charge », *IPWatchdog.com | Patents & Patent Law*, déc. 04, 2017. https://www.ipwatchdog.com/2017/12/04/u-s-leads-world-quantum-computing-patent-ibm/id=90304/ (consulté le mars 07, 2020).

[205] marqube, « Quantum Technologies Flagship Report », *Shaping Europe's digital future - European Commission*, mai 12, 2016. https://ec.europa.eu/digital-single-market/en/quantum-technologies (consulté le févr. 21, 2020).

[206] « La Chine devient le principal déposant de demandes internationales de brevet en 2019, dans un contexte de forte croissance des services de propriété intellectuelle, des adhésions aux traités et des recettes de l'OMPI ». https://www.wipo.int/pressroom/fr/articles/2020/article_0005.html (consulté le juin 10, 2020).

[207] « Le canadien D-Wave et ses calculateurs quantiques pas comme les autres », *La Tribune*. https://www.latribune.fr/technos-medias/le-canadien-d-wave-et-ses-calculateurs-pas-comme-les-autres-832961.html (consulté le juin 11, 2020).

[208] « Real-world intercontinental quantum communications enabled by the Micius satellite ». https://phys.org/news/2018-01-real-world-intercontinental-quantum-enabled-micius.html (consulté le juin 09, 2020).

[209] Y. Yu *et al.*, « Entanglement of two quantum memories via fibres over dozens of kilometres », *Nature*, vol. 578, nº 7794, p. 240-245, févr. 2020, doi: 10.1038/s41586-020-1976-7.

[210] francitech, « Startuppeurs français, ayez la culture du brevet ! », *Invention - Europe*, avr. 11, 2018. https://invention-europe.com/2018/04/11/startuppeurs-francais-ayez-la-culture-du-brevet/ (consulté le juin 09, 2020).

[211] « Briefing: A large number of China's patents are actually worthless · TechNode », *TechNode*, sept. 27, 2018. https://technode.com/2018/09/27/china-patents/ (consulté le juin 10, 2020).

[212] J. Liu, G. Zhao, J. Wu, W. Jia, et Y. Zhang, « Unified Management Platform of Quantum and Classical Keys in Power Communication System », in *The 8th International Conference on Computer Engineering and Networks (CENet2018)*, Cham, 2020, p. 695-705, doi: 10.1007/978-3-030-14680-1_76.

[213] A. Seydtaghia, « Le genevois ID Quantique passe sous contrôle coréen pour 65 millions », *Le*

Temps, févr. 26, 2018. https://www.letemps.ch/economie/genevois-id-quantique-passe-controle-coreen-65-millions (consulté le juin 10, 2020).

[214] « Brevetabilité des méthodes d'IA et de simulation | Plasseraud IP ». https://www.plass.com/fr/articles/brevetabilite-des-methodes-dia (consulté le juin 10, 2020).

[215] S. M. Dhawan, B. M. Gupta, et S. Bhusan, « Global Publications Output in Quantum Computing Research: A Scientometric Assessment during 2007-16 », 2018, doi: 10.28991/esj-2018-01147.

[216] D. Deutsch et R. Penrose, « Quantum theory, the Church–Turing principle and the universal quantum computer », *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, nº 1818, p. 97-117, juill. 1985, doi: 10.1098/rspa.1985.0070.

[217] B. Théry, « D-Wave lance Leap 2, la nouvelle version de son service quantique Cloud », *Clubic.com*, févr. 27, 2020. https://www.clubic.com/technologies-d-avenir/actualite-887108-wave-leap-2-service-quantique-cloud.html (consulté le mars 06, 2020).

[218] P. Gerbert et F. Ruess, « The Next Decade in Quantum Computing—and How to Play », *https://www.bcg.com*. https://www.bcg.com/fr-fr/publications/2018/next-decade-quantum-computing-how-play.aspx (consulté le févr. 21, 2020).

[219] « Relative Citation Ratio », *Metrics Toolkit*, juill. 24, 2017. https://www.metrics-toolkit.org/relative-citation-ratio/ (consulté le mai 25, 2020).

[220] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, et J. L. O'Brien, « Quantum computers », *Nature*, vol. 464, nº 7285, Art. nº 7285, mars 2010, doi: 10.1038/nature08812.

[221] M. A. Nielsen et I. L. Chuang, *Quantum computation and quantum information*, 10th anniversary ed. Cambridge ; New York: Cambridge University Press, 2010.

[222] J. E. Hirsch, « An index to quantify an individual's scientific research output », *PNAS*, vol. 102, nº 46, p. 16569-16572, nov. 2005, doi: 10.1073/pnas.0507655102.

[223] M. Z. Hasan et C. L. Kane, « Colloquium: Topological insulators », *Rev. Mod. Phys.*, vol. 82, nº 4, p. 3045-3067, nov. 2010, doi: 10.1103/RevModPhys.82.3045.

[224] V. S. MBE, « Quantum Theory & Our Understanding of Everything », *Thought Economics*, mai 26, 2020. https://thoughteconomics.com/ (consulté le juin 29, 2020).

[225] BCG - Boston Consulting Group, « Where Will Quantum Computers Create Value—and When? », *https://www.bcg.com*, mai 13, 2019. https://www.bcg.com/fr-fr/publications/2019/quantum-computers-create-value-when.aspx (consulté le juin 29, 2020).

[226] « IBM Announces $3 Billion Research Initiative To Tackle Chip Grand Challenges For Cloud And Big Data Systems », *IBM News Room*, juin 29, 2020. https://newsroom.ibm.com/2014-07-09-IBM-Announces-3-Billion-Research-Initiative-To-Tackle-Chip-Grand-Challenges-For-Cloud-And-Big-Data-Systems (consulté le juin 30, 2020).

[227] « Honeywell Achieves Breakthrough That Will Enable The World's Most Powerful Quantum Computer ». https://www.honeywell.com/content/honeywell/us/en/newsroom/pressreleases/2020/03/honeywell-achieves-breakthrough-that-will-enable-the-worlds-most-powerful-quantum-computer.html (consulté le mars 06, 2020).

[228] C. H. Bennett et G. Brassard, « Quantum cryptography: Public key distribution and coin tossing », *Theoretical Computer Science*, vol. 560, p. 7-11, déc. 2014, doi: 10.1016/j.tcs.2014.05.025.

[229] A. I. Nurhadi et N. R. Syambas, « Quantum Key Distribution (QKD) Protocols: A Survey », in *2018 4th International Conference on Wireless and Telematics (ICWT)*, juill. 2018, p. 1-5, doi: 10.1109/ICWT.2018.8527822.

[230] « Alice to Bob ». http://physique.unice.fr/sem6/2014-2015/PagesWeb/PT/Tomographie/?page=bb84 (consulté le sept. 24, 2020).

[231] P. W. Shor et J. Preskill, « Simple Proof of Security of the BB84 Quantum Key Distribution Protocol », *Phys. Rev. Lett.*, vol. 85, nº 2, p. 441-444, juill. 2000, doi: 10.1103/PhysRevLett.85.441.

[232] T. Häner, M. Roetteler, et K. M. Svore, « Factoring using 2n+2 qubits with Toffoli based modular

multiplication », *arXiv:1611.07995 [quant-ph]*, juin 2017, Consulté le: sept. 23, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1611.07995.

[233] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, et J. L. O'brien, « Experimental realization of Shor's quantum factoring algorithm using qubit recycling », 2012, doi: 10.1038/nphoton.2012.259.

[234] M. Amico, Z. H. Saleem, et M. Kumph, « Experimental study of Shor's factoring algorithm using the IBM Q Experience », *Phys. Rev. A*, vol. 100, nº 1, p. 012305, juill. 2019, doi: 10.1103/PhysRevA.100.012305.

[235] B. Wang, F. Hu, H. Yao, et C. Wang, « Prime factorization algorithm based on parameter optimization of Ising model », *Scientific Reports*, vol. 10, nº 1, Art. nº 1, avr. 2020, doi: 10.1038/s41598-020-62802-5.

[236] J. Zhao, « Quantum Software Engineering: Landscapes and Horizons », *arXiv:2007.07047 [quant-ph]*, juill. 2020, Consulté le: oct. 06, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/2007.07047.

[237] K. Bertels *et al.*, « Quantum Computer Architecture: Towards Full-Stack Quantum Accelerators », *arXiv:1903.09575 [quant-ph]*, sept. 2019, Consulté le: oct. 06, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1903.09575.

[238] J. Romero, R. Babbush, J. R. McClean, C. Hempel, P. Love, et A. Aspuru-Guzik, « Strategies for quantum computing molecular energies using the unitary coupled cluster ansatz », janv. 2017, Consulté le: oct. 07, 2020. [En ligne]. Disponible sur: https://www.arxiv-vanity.com/papers/1701.02691/.

[239] C. Bravo-Prieto, R. LaRose, M. Cerezo, Y. Subasi, L. Cincio, et P. J. Coles, « Variational Quantum Linear Solver », *arXiv:1909.05820 [quant-ph]*, juin 2020, Consulté le: oct. 07, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1909.05820.

[240] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, et S. Lloyd, « Quantum machine learning », *Nature*, vol. 549, nº 7671, p. 195-202, sept. 2017, doi: 10.1038/nature23474.

[241] A. Montanaro, « Quantum algorithms: an overview », *npj Quantum Inf*, vol. 2, nº 1, p. 15023, nov. 2016, doi: 10.1038/npjqi.2015.23.

[242] F. G. S. L. Brandao et K. Svore, « Quantum Speed-ups for Semidefinite Programming », *arXiv:1609.05537 [quant-ph]*, sept. 2017, Consulté le: oct. 07, 2020. [En ligne]. Disponible sur: http://arxiv.org/abs/1609.05537.

[243] G. C. Knee et W. J. Munro, « Optimal Trotterization in universal quantum simulators under faulty control », *Phys. Rev. A*, vol. 91, nº 5, p. 052327, mai 2015, doi: 10.1103/PhysRevA.91.052327.

[244] A. W. Harrow, A. Hassidim, et S. Lloyd, « Quantum algorithm for solving linear systems of equations », *Phys. Rev. Lett.*, vol. 103, nº 15, p. 150502, oct. 2009, doi: 10.1103/PhysRevLett.103.150502.