Opinions Libres
le blog d'Olivier Ezratty

Comprendre l'informatique quantique – autres technologies

Après les ordinateurs quantiques supraconducteurs, **adiabatiques** et **universels**, qui constituent l'essentiel de l'offre commerciale d'aujourd'hui, faisons maintenant le tour des autres technologies d'ordinateurs quantiques qui, si elles ne sont pas encore commercialement disponibles, pourraient être cependant prometteuses. Tout du moins, selon les cas.

Seront ici couvertes les technologies CMOS à spins d'électrons, les cavités de diamants, les ions piégés, l'optique linéaire et le topologique. Je ne couvre pas dans le détail les autres technologies existantes qui n'ont pas l'air de sortir des laboratoires, comme celles qui utilisent des atomes froids pour réaliser des qubits.

CMOS – spin d'électrons / quantum dots

Les qubits à base de semi-conducteurs CMOS sont une voie en devenir permettant d'utiliser des processus de fabrication existants de composants CMOS au silicium. Pour mémoire, le CMOS qui veut dire "Complementary Metal Oxyde Semiconductor", est la technologie utilisée de manière dominante pour produire des processeurs dans le monde, pour les processeurs d'ordinateurs (Intel, AMD), que des GPU (Nvidia, AMD), des chipsets pour smartphones (Qualcomm, Mediatek, HiSilicon, etc) et dans tout un tas de secteurs spécialisés (micro-contrôleurs, composants radio, …).

Dans les processeurs quantiques, c'est la voie choisie par un bon nombre de laboratoires de recherche dans le monde et par quelques entreprises privées telles que Nokia / Bell Labs, les NTT Basic Research Laboratories au Japon, et surtout, par Intel. En France, c'est l'une des deux voies d'exploration sérieusement étudiées au CEA.

Le principe général utilisé pour créer des qubits de ce type est le suivant :

- L'**état quantique** du qubit est le spin d'un électron individuel d'un atome piégé dans une structure semi-conductrice. Le spin est assimilable à l'orientation magnétique de l'électron.
- Les **portes quantiques unitaires** utilisent le principe de l'ESR, ou "electron spin resonance". Comme pour les qubits supraconducteurs, ces portes s'appuient sur l'émission de micro-ondes envoyées par conduction vers les qubits.
- Les **portes quantiques à deux qubits** utilisent généralement une technique différente comme des interactions entre dipôles dans les circuits.
- La **mesure de l'état d'un qubit** utilise la conversion du spin d'électron, son orientation magnétique, en charge électrique.

L'intérêt de cette technique est de permettre l'intégration d'un grand nombre de qubits dans un circuit, avec

potentiellement jusqu'à des milliards de qubits sur un seul chipset. C'est même d'ailleurs semble-t-il la seule technologie qui permettrait d'atteindre ce niveau d'intégration.

Le tout se ferait avec un temps de cohérence très long des qubits et un taux d'erreur au moins aussi bon qu'avec les qubits supraconducteurs universels. L'une des difficultés est de relier les qubits entre eux par couplage pour permettre l'exécution de portes quantiques à deux qubits.

Ces qubits CMOS présentent aussi l'intérêt de pouvoir généralement fonctionner en théorie à une température moins basse que les qubits supraconducteurs, de l'ordre de 1 K au lieu de 15 mK. Ces qubits manipulant des électrons individuels, ils seraient moins sujets aux perturbations extérieures que les qubits supraconducteurs qui s'appuient sur des courants portés par des millions d'électrons. Au passage, la cryogénie à cette température permet d'éviter l'usage de l'hélium 3 dont nous **avions vu** qu'il était plutôt rare et cher.

C'est l'une des raisons qui permettrait à cette technologie de mieux "scaler" en nombre de qubits. En effet, cette température plus élevée permet de placer une électronique de commande plus dense autour des qubits sans que cela n'échauffe trop le circuit. En effet, cette électronique dégage de la chaleur et cette chaleur acceptable est conditionnée par la température de fonctionnement des qubits. Plus cette température est basse, plus la chaleur acceptable dégagée par l'électronique de contrôle des qubits est basse.

Les données de références sont les suivantes : on ne peut consommer qu'un milliwatt d'énergie à 20 mK. Cela limite l'électronique de contrôle à environ 10 000 transistors (en CMOS). C'est expliqué dans **28nm Fully-Depleted SOI Technology Cryogenic Control Electronics for Quantum Computing**, 2018 (2 pages), issu du CEA-LETI et de STMicroelectronics.

Ces chipsets CMOS nécessitent l'emploi de codes de correction d'erreurs en masse, comme les "surface codes" qui sont évoqués dans une **partie précédente**.

Voici les principaux laboratoires de recherche qui creusent la piste du CMOS, très souvent dans de la recherche partenariale multi-laboratoires et multi-pays :

UNWS / Qutech : le laboratoire hollandais Qutech issu de l'Université TU Delft collabore avec l'Université de New South Wales en Australie et avec une architecture CMOS et SOI (*ci-dessus).* Le SOI pour "silicon on insulator" ou "silicium sur isolant" est une technologie issue des français CEA-LETI et SOITEC. Elle ajoute une couche d'isolant en oxyde de silicium (SiO2 ou "BOX", buried oxyde) au-dessus des wafers de silicium et sur laquelle sont ensuite gravés les transistors et autres conducteurs des circuits à créer. Cf **Silicon CMOS architecture for a spin-based quantum computer**, 2016 (13 pages). L'UNWS collabore parallèlement avec le CEA-LETI dans cette voie.

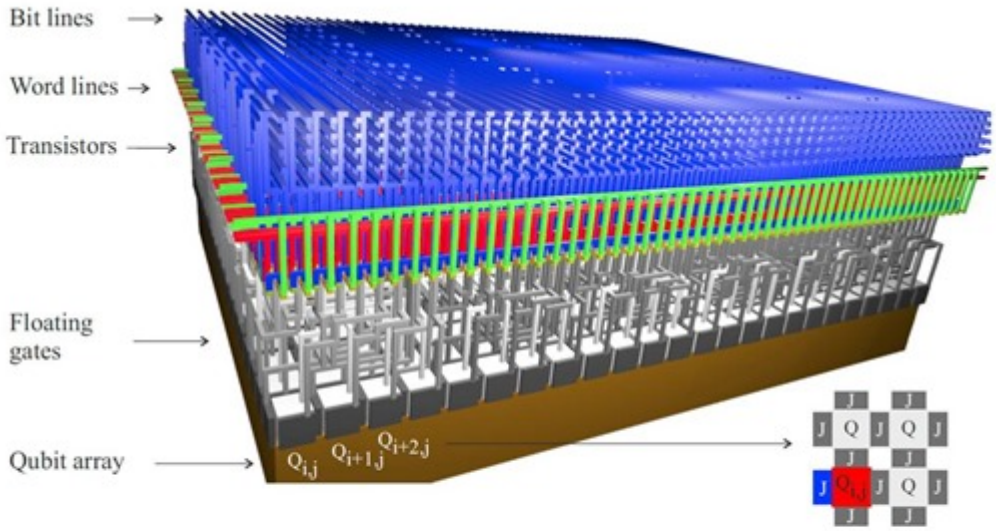
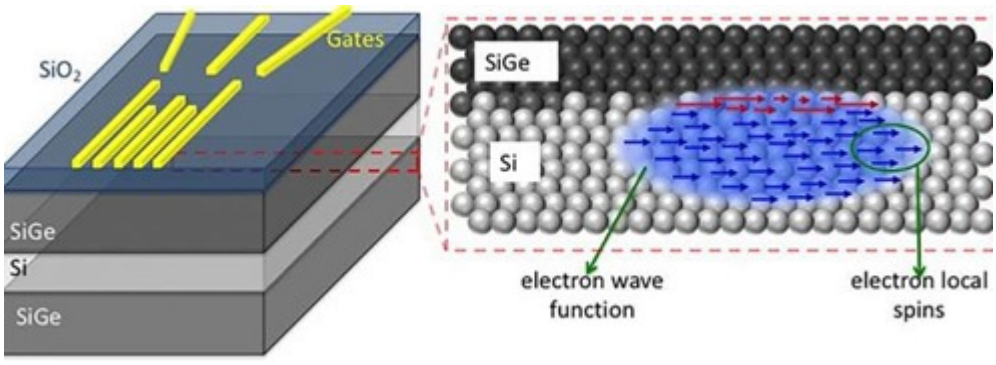


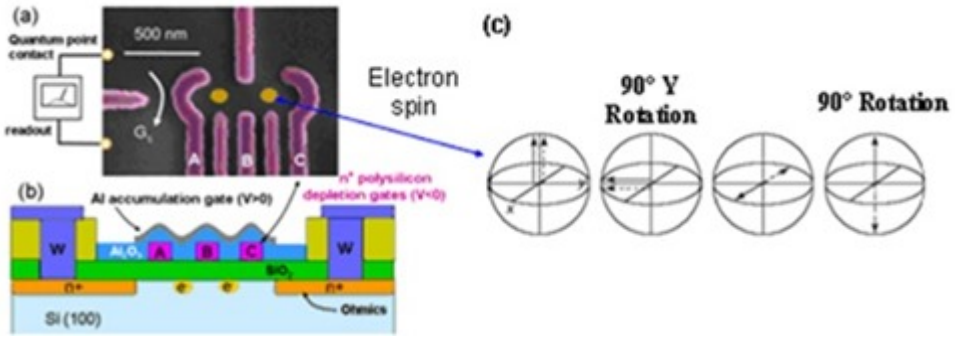
FIG. 1. **Physical quantum processor. a** A silicon-on-insulator (SOI) wafer is processed, such that the bottom layer of isotopically enriched silicon-28 contains the 2D qubit array and the top layer of silicon forms the transistors to operate the qubits. These are interconnected through the oxide regions using polysilicon vias. **b** Electrical circuit for the control of one Q-gate and one J-gate allowing the required individual, row-by-row, or global operations, as explained in the main text. **c** Physical architecture to operate one unit module containing 480 qubits. The inset on the bottom right shows a plan view cross-section through the qubit plane. Each J gate and qubit is connected via the circuit shown in **(b)**.

UNSW / Purdue : l'University of New South Wales en Australie et de la Purdue University aux USA (qui est financée par Microsoft) ont aussi expérimenté un système des atomes de phosphore intégrés dans un substrat de silicium, les états des qubits étant le spin d'électrons des atomes de phosphore. La recherche porte surtout sur le couplage entre qubits, à base de liaisons entre dipôles électriques. Ils prévoient d'atteindre 10 qubits d'ici 2022 ce qui est modeste. C'est documenté dans **Silicon quantum processor with robust long-distance qubit couplings**, 2017 (17 pages). L'UNSW a bénéficié d'un financement de A$83 originaire de l'opérateur télécom Telstra, de la Commonwealth Bank et des gouvernements australiens et de la région Nouvelles-Galles du Sud.

Purdue / TU Delft / Wisconsin : des travaux conjoints de l'Université de Purdue dans l'Indiana, de TU Delft aux Pays-Bas et de l'Université du Wisconsin-Madison évoquent la possibilité d'intégrer des millions de qubits dans des circuits en silicium et germanium exploitant le spins d'électrons, dans **Silicon provides means to control quantum bits for faster algorithms**, juin 2018. L'avantage du germanium dans les qubits est de permettre de créer des portes quantiques très rapides allant de 0,5 à 5 ns. Voir aussi **Quantum control and process tomography of a semiconductor quantum dot hybrid qubit**, 2014 (12 pages).



Sandia Labs, USA est une filiale du groupe Honeywell qui travaille surtout pour le Département de l'Energie US (DoE) avec des laboratoires dans le Nouveau Mexique et en Californie. C'est une sorte de CEA US. Ils travaillent ainsi sur l'armement nucléaire des USA ! Ils travaillent notamment sur la physique des qubits CMOS et leurs codes de correction d'erreurs. Ils visent une température d'opération intermédiaire de 100 mK. Ci-dessous, leur architecture de qubit à base de double quantum dot de silicium (**source**).



Princeton, USA, travaille notamment sur réalisation de porte CNOT à deux qubits en CMOS à très haut niveau de fiabilité et faible temps d'opération, respectivement de 200 ns et 99%. Vu dans **Quantum CNOT Gate for Spins in Silicon**, 2017 (27 pages). Ce sont aussi des qubist à double quantum dots utilisant du silicium et du germanium.

Les laboratoires de **HRL Malibu**, filiale de recherche commune de Boeing et General Motors, située en Californie et **Nokia** travaillent sur des qubits en arséniure de gallium qui nécessitent un refroidissement à moins de 1K. Ce seraient des qubits avec de longs temps de cohérence permettant de faire des calculs avec un grand nombre de portes quantiques et codes de corrections d'erreurs.

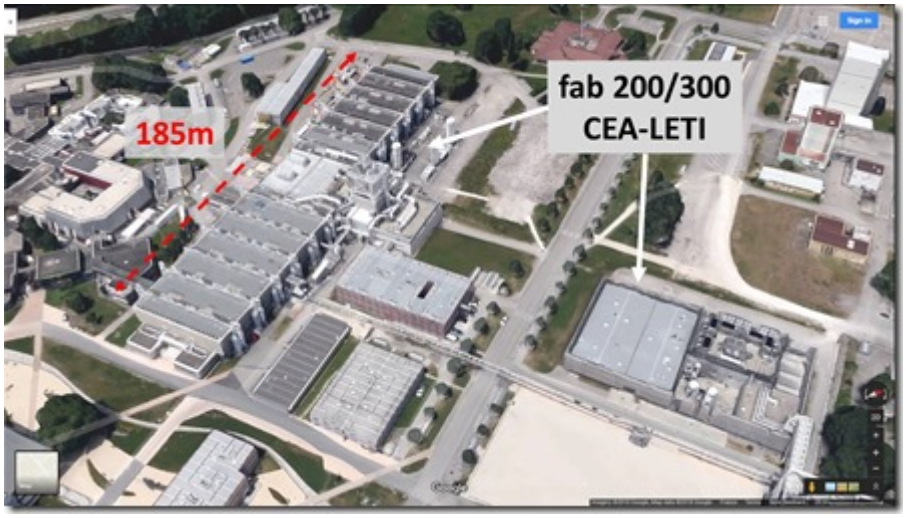
Le CEA-LETI de Grenoble est le laboratoire européen en pointe sur la recherche appliquée dans les qubits CMOS à spins d'électrons.

L'équipe en charge du quantique y est dirigée par **Maud Vinet**. Le laboratoire est au cœur d'un écosystème de recherche quantique labellisé **Grenoble Quantum Silicon** qui comprend le CNRS, l'institut Néel, l'INAC et l'Université Grenoble Alpes. L'approche est pluridisciplinaire, ce qui est assez rare dans la recherche, avec un beau **panel de chercheurs**.

L'équipe de l'INAC (Institute for Nanoscience and Cryogenics) qui associe le CEA et l'Université de Grenoble et celles de l'Institut Néel qui associe le CNRS et l'Université Joseph Fourier de Grenoble qui fait partie du CNRS apportent leur expertise dans la création d'électronique de contrôle fonctionnant à température cryogénique, dans le contrôle d'électrons individuels dans des structures semiconductrices. D'autres chercheurs de l'INAC aident à modéliser les composants semi-conducteurs des qubits. Les ingénieurs en microélectronique du LETI complètent l'ensemble avec une connaissance des processus de conception, d'intégration, de fabrication et de tests des circuits semiconducteurs.

L'objectif de cette équipée est de créer des qubits CMOS à forte intégration et surtout une capacité à monter en puissance en termes de nombre de qubits. Les premier qubits en CMOS ont été créés en 2016. Il s'agit maintenant de créer des chipsets comprenant des millions de qubits, puis des dizaines et centaines de millions de qubits.

Au-delà de la physique, ces chipsets exploitent la capacité d'intégration et de fabrication des composants CMOS à grande échelle et leur fonctionnement possible à 1K au lieu de 15-20 mK qui permet d'y adjoindre une électronique de contrôle consommant un peu plus d'énergie que celle des qubits supraconducteurs. Les expériences en laboratoire montrent pour l'instant que les qubits CMOS génèrent un taux d'erreur raisonnable, voisin de celui des qubits supraconducteurs.



Le LETI est l'un des rares laboratoires publics au monde disposant d'une plateforme de production de test de composants CMOS. Basée à Grenoble, elle comprend tout l'outillage de production de composants CMOS sur wafers de 200 et 300 mm. Elle permet de produire des composants CMOS en tout genre et en matériaux III-V (photonique, arséniure de gallium, etc). L'équipement comprend des machines de lithogravure, notamment originaires du leader mondial ASML, avec une résolution pouvant descendre à 7 nm, des machines pour le dépôt de matériaux semiconducteurs et conducteurs utilisant toutes les techniques imaginables (plasma, …) ainsi que pour l'ajout de dispositifs MEMS (micro-électro-mechanical systems). Le tout occupe plusieurs bâtiments, dont le principal qui fait 184 m de long (vue Google Maps *ci-dessus*).

La production validée peut ensuite être transférée vers de la production en volume dans des fabs commerciales comme celles de STMicroelectronics, Global Foundries ou Samsung qui supportent les processus FD-SOI sur lesquels le CEA s'appuie en général. Mais à ses débuts, la taille du marché des ordinateurs quantiques sera modeste. Et rien que dans un batch classique de 25 wafers, on pourra produire d'un seul coup quelques milliers de puces quantiques, de quoi alimenter une belle base de supercalculateurs quantiques.

A Grenoble, le LETI dispose aussi d'une plateforme de nanocaractérisation (PFNC ou NanoCarac) qui comprend sur 2500 m2 des dizaines d'outils de métrologie permettant de vérifier la qualité des composants CMOS fabriqués. Avec Fanny Bouton, j'ai pu visiter tout cela en juillet 2018 et c'était impressionnant ! La double salle blanche du LETI cumule environ un milliard d'euros d'équipements avec des machines dont le coût s'étale de quelques millions à 80 millions d'Euros ! Ce sont des moyens bien plus lourds que pour produire des qubits supraconducteurs à cause du niveau d'intégration qui est plus élevé.

Les qubits supraconducteurs sont en effet bien moins intégrés, faisant plusieurs dizaines de microns de largeur. Rigetti produit ses chipsets supraconducteurs en interne avec $10M d'équipement. Les qubits CMOS pourront descendre à une taille de 100 nm x 100 nm. Les fabs classiques ne sont pas optimisées dans leurs processus de fabrication pour créer des qubits CMOS. Cela nécessiterait un gros travail de tuning et un besoin de flexibilité pas évident à obtenir. Avec une densité de 100 nm, on pourrait théoriquement caser un milliard de qubits dans une puce CMOS de 1 cm2. L'objectif est de démarrer à 1 million de qubits avec un taux d'erreur qui serait de deux ordres de grandeur plus faible (1/100) qu'avec les qubits supraconducteurs. Le LETI s'est donné une roadmap avec trois grandes étapes : d'ici 5 ans, d'ici 10 ans et au-delà, pour développer ces chipsets à plusieurs millions de qubits.

Le CEA travaille aussi sur la technologie **CoolCube** permettant de disposer les composants en 3D (**détails**), ce qui permettrait de résoudre divers problèmes de mise à l'échelle. Elle serait applicable aux qubits CMOS et plus largement, à d'autres applications du CMOS.

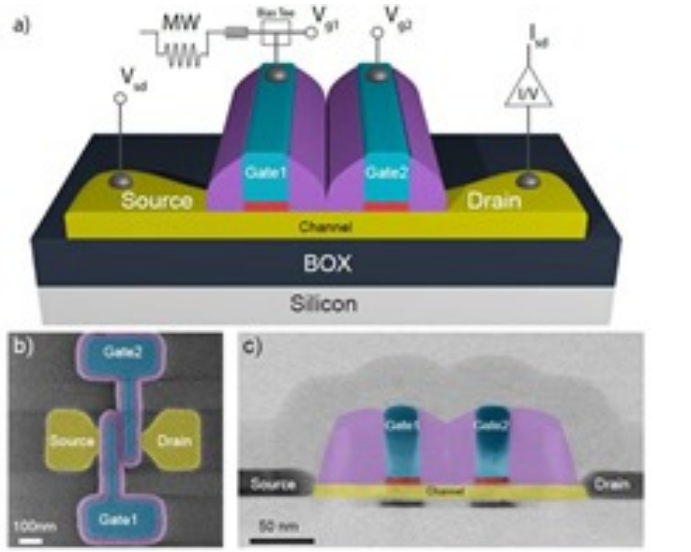


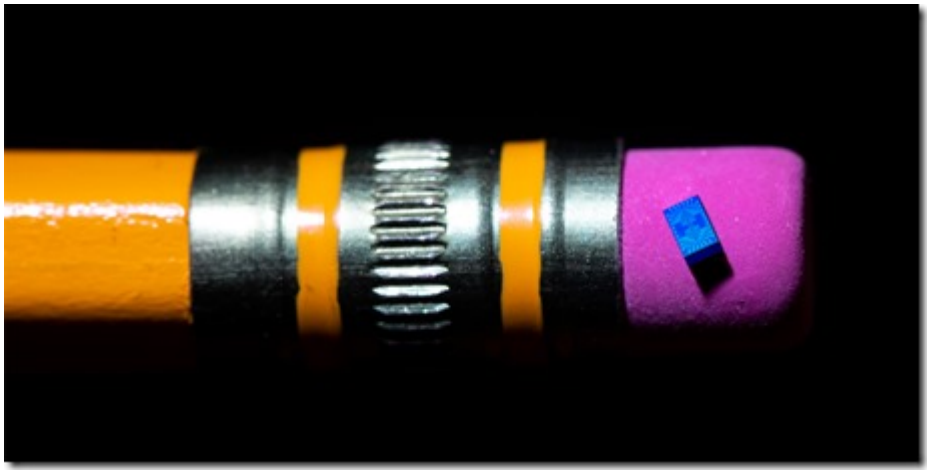
FIG. 1. **CMOS qubit device.** a, Simplified 3-dimensional schematic of a SOI nanowire field-effect transistor with two gates Gate1 and Gate2. Using a bias-T, Gate 1 is connected to a low-pass-filtered line, used to apply a static gate voltage V_{g1}, and to a 20-GHz bandwidth line, used to apply the high-frequency modulation necessary for qubit initialization, manipulation and readout. b, Colorized device top view obtained by scanning electron microscopy just after the fabrication of gates and spacers. c, Colorized transmission-electron-microscopy image of the device along a longitudinal cross-sectional plane.

Les publications de référence de ces équipes sur les qubits CMOS sont nombreuses. On compte notamment **A CMOS silicon spin qubit,** 2016 (12 pages) qui définit les bases du qubit CMOS à double quantum dots (*schéma ci-dessus*), **SOI technology for quantum information processing**, 2016 qui complète cette description ainsi que **Conditional Dispersive Readout of a CMOS Single-Electron Memory Cell** 2018 (9 pages) qui décrit dans le cadre d'un partenariat avec l'Université de Londres, le travail sur la lecture de l'état d'un qubit quantum dot CMOS.

Intel travaille aussi sur la piste des composants CMOS utilisant des spins d'électrons avec un premier wafer produit avec des chipsets de 26 qubits en 2017. Le choix des qubits à base de silicium et de spins d'électron résulte d'une forme de biais cognitif : Intel maitrise la fabrication de composants CMOS et recherche donc une technologie quantique qui puisse s'appuyer sur ce savoir-faire. Mais comme nous l'avons vu au-dessus, il y a une grande logique à poursuivre cette voie qui semble l'une des rares capable de scaler en nombre de qubits.

Ses qubits sont fabriqués dans un niveau d'intégration "ancien", de 300 nm, mais s'appuyant sur des wafers de silicium plus purs d'un point de vue isotopique avec une très faible variation isotopique des atomes de silicium utilisés. Les wafers utilisés dans les qubits CMOS sont en effet en Silicium 28, l'isotope du silicium à spin de noyau nul, qui est le plus abondant sur Terre mais doit être produit par rafinage. Il comprend 14 neutrons et autant de protons.

En juin 2018, Intel faisait une annonce de plus avec une puce très intégrée utilisant cette technologie CMOS, censée pouvoir compter jusqu'à 1500 qubits (*ci-dessous*). Elle est fabriquée dans la fab D1D située dans l'Oregon. Et cette fois-ci, avec une densité de gravure de l'ordre de 50 nm, six fois plus grande que la génération du début de 2018. Mais bien entendu, sans aucune information sur le bruit généré, qui est indispensable pour le bon fonctionnement du système ni d'ailleurs, le nombre exact de qubits de la puce en question.

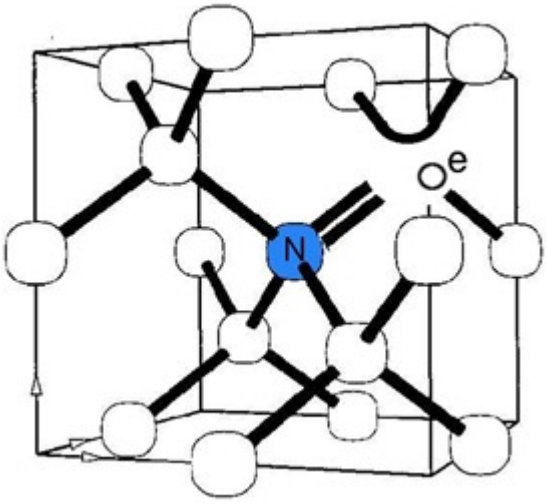


Que ce soit pour Tangle Lake en supraconducteurs ou pour les différentes versions à spins d'électrons, on est donc dans un brouillard quantique sur la qualité de l'ensemble.

Le hollandais QuTech et Intel travaillent bien ensembles. QuTech a bénéficié de $50M d'investissements de la part d'Intel depuis 2015 pour explorer la voie du qubit en CMOS. L'investissement global d'Intel reste modeste sur le quantique. Il peut l'être tant que l'on n'en est pas au niveau de la fabrication en série.

Cavités de diamants / NV Centers

Cette technique consiste à créer un défaut artificiel dans une structure cristalline de carbone avec un atome de carbone remplacé par un atome d'azote et un autre atome de carbone remplacé par un vide sans atome. Le résultat est une structure de spin 1 qui peut être contrôlé optiquement et par micro-ondes. L'ensemble fonctionnerait à température ambiante. A vrai dire, la littérature évoque parfois la température de 4K, qui est loin d'être ambiante mais dans le grand froid, tout est relatif ! La technique est notamment documentée dans **NV-centers in Nanodiamonds How good they are** 2017 (18 pages).



Il existe des variantes de cette technique avec des défauts introduits dans du carbure de silicium dopé au

phosphore qui présenteraient l'avantage de créer des qubits dont la mesure est plus précise car reposant sur l'émission d'une fluorescence de fréquence étroite. Cf **Study Takes Step Toward Mass-Producible Quantum Computers**, 2017.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est le spin des électrons situés dans la cavité.
- Les **portes quantiques unitaires** sont activées par laser.
- Les **portes quantiques à deux qubits** utilisent aussi des lasers.
- Le **mesure de l'état d'un qubit** utilise la captation de la fluorescence de la cavité avec un capteur CCD.

La technologie n'est pas facile à industrialiser à grande échelle, qu'il s'agisse du chipset lui-même où des lasers de contrôle.

QDTI est la seule startup connue s'étant lancée dans la mise au point d'un ordinateur quantique à base de NV Centers. Créée par une équipe issue de l'Université d'Harvard, elle est basée logiquement dans le Massachusetts. La startup a plusieurs cordes à son arc en plus de la création de processeurs quantiques. Elle planche notamment sur des systèmes d'imagerie médicale utilisant aussi ces NV centers, avec la création de magnétomètres de précision associés à de l'IRM. La société n'a pas l'air particulièrement active depuis 2016.

Ions piégés

Cette technique a été imaginée dans les années 1950 par **Wolfgang Paul**, prix Nobel de physique en 1989. Les premiers à les tester furent Juan Cirac et Peter Zoller en 1995. Les ions piégés sont des ions qui sont piégés magnétiquement dans un espace confiné, et placés les uns à côté des autres. Les atomes utilisés ont un électron manquant, dans la seconde colonne du tableau de Mendeleïev. Le calcium est le plus courant.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est le niveau d'énergie de l'ion piégé.
- Les **portes quantiques unitaires** sont activées par micro-ondes, par lasers ou par des dipôles magnétiques.
- Les **portes quantiques à deux qubits** utilisent des lasers avec des photons intriqués.
- La **mesure de l'état d'un qubit** utilise la captation de la fluorescence de la cavité avec un capteur CCD après excitation par un laser.

L'Autrichien Rainer Blatt de l'**Université d'Innsbruck** est un des pionniers de cette filière. Il créé un registre intriqué de 14 qubits adressables en 2011. Il passe à 20 qubits adressables et individuellement contrôlables en 2018. Ce sont des qubits à base d'ions calcium organisés en ligne servant de qubits et intriqués via un système

de lasers.

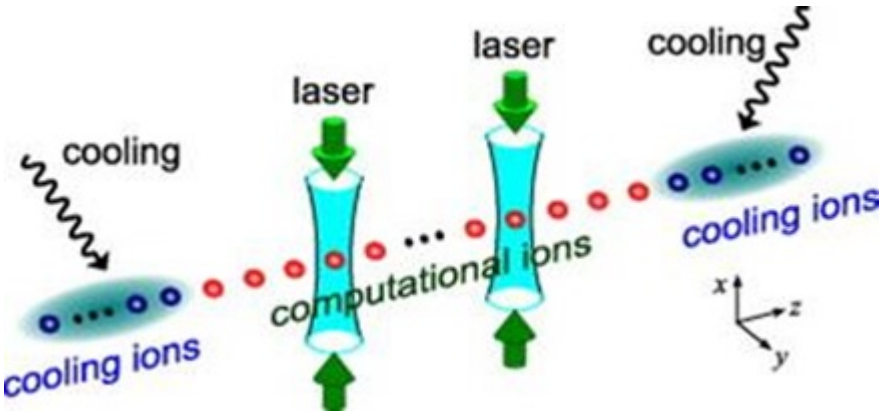
Les ions piégés ont un temps de décohérence long, de plusieurs dizaines de secondes, mais c'est compensé par des gate time tout aussi longs en proportion. Ils présentent l'avantage de générer un taux d'erreur assez faible et de pouvoir être tous intriqués les uns avec les autres dans leur confinement alors que dans les technologies supraconductrices, seuls les qubits voisins d'un qubit donné peuvent être intriqués, ce qui créé des contraintes dans la conception et/ou la compilation d'algorithmes quantiques.

L'inconvénient principal est que la solution ne sera probablement pas facile à faire grandir en nombre de qubits confinés. Ne serait-ce que par le nombre de lasers à aligner pour leur contrôle et par l'espacement entre les ions alignés en rangs d'on-ions (facile…) qui est d'environ 2mm. Enfin, la technique est difficile à miniaturiser à cause des systèmes de contrôles divers et à l'inexistence de lignes de production adaptées.

Les ions piégés sont explorés par quelques acteurs et surtout par les laboratoires de recherche. Le plus connu est celui de l'**Université de Maryland,** où officie un grand spécialiste du sujet, Christopher Monroe, et dont la spin-off **IonQ** est le seul acteur commercial de cette typologie de qubits.

Côté laboratoire, il Il faut aussi compter avec **IQOQI** (Autriche, cf Rainer Blatt) et l'**IQST** (Allemagne), qui sont coauteurs de **Observation of Entangled States of a Fully Controlled 20-Qubit System**, portant sur un prototype de 20 qubits réalisé avec des ions calciums. Il y a aussi l'**University of West Sussex** au Royaume Uni qui travaille sur un prototype de 10 qubits et recherche du financement pour créer un ordinateur quantique à 1000 qubits.

IonQ est donc une spin-off de l'Université de Maryland spécialisée dans la conception d'ordinateurs quantiques universels à base d'ions piégés, avec une trentaine de collaborateurs. Créé par Christopher Monroe, la startup n'a levé que $20M, dont une partie chez Google Ventures et Amazon.



Le laboratoire planche dessus depuis longtemps. Le record actuel serait de 53 qubits cohérents et intriqués sachant que l'Université de Maryland teste un dispositif à 121 qubits. L'ion est à base d'un atome d'ytterbium, une terre rare aussi utilisée dans la production de certains lasers.

Le cofondateur d'IonQ et Chief Scientist est Christopher Monroe, un professeur de cette université. Cf **A**

Reconfigurable Quantum Computer par David Moehring, 2017 (20 slides). La topologie du système permet de créer des portes arbitraires de deux à trois qubits reliant n'importe lequel des qubits alignés. C'est dû aux couplages entre les ions qui exploitent des forces de Coulomb de longue portée.

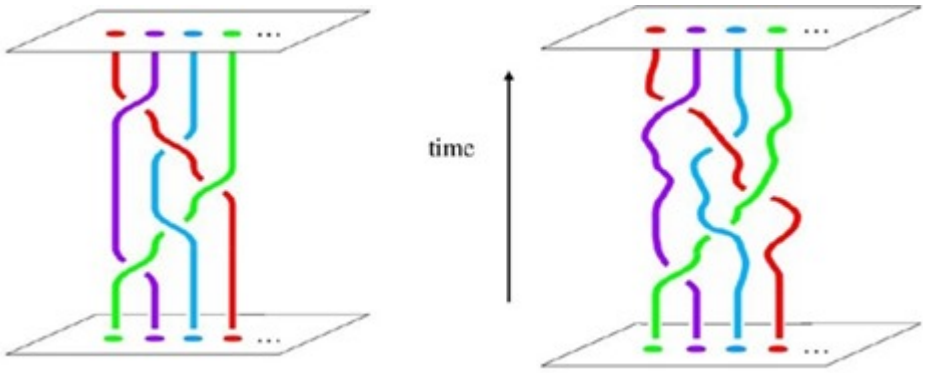
Ils proposent une offre logiciel de programmation en cloud. L'approche est aussi "full stack". Mais l'approche logicielle a l'air d'être très propriétaire.

Topologique

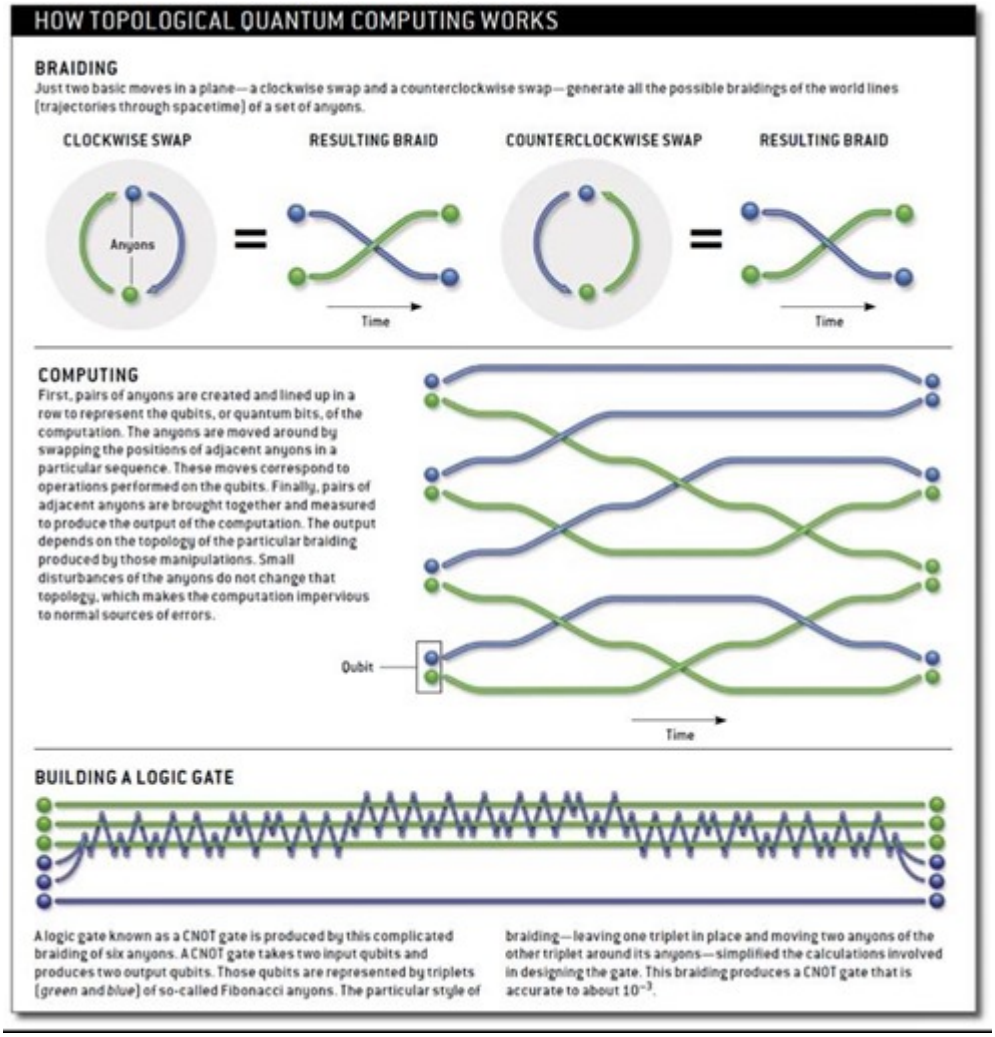
Il faut distinguer dans cette catégorie d'ordinateurs quantique la notion de "topologique" qui définit un type de qubits à base d'anyons et les "fermions de Majorana" qui ne sont qu'une variante d'anyons pour créer des qubits topologiques. De tous les types de qubits, ce sont les plus mystérieux et complexes à appréhender, et donc à vulgariser en langage naturel. On nage en pleine méta-complexité !

Le principe du quantique topologique repose sur la notion d'anyons qui sont des "quasi-particules" intégrées dans des systèmes à deux dimensions. Sachant qu'il y a des anyons abéliens et non abéliens ! Pour faire simple, les anyons sont des structures physiques asymétriques et à deux dimensions dont la symétrie peut être modifiée. Cela permet d'appliquer des principes de topologie avec des ensembles de permutations successives appliquées aux couples d'anyons qui se trouvent à proximité dans des circuits. Les algorithmes associés s'appuient sur les concepts d'organisations topologiques de tresses ou de nœuds ("braids").

La représentation *ci-dessous* explique cela, avec une évolution temporelle des permutations d'anyons temporelle allant du bas vers le haut sachant que dans d'autres représentations, elle va de haut en bas.



Le schéma suivant issu de **Computing with Quantum Knots** de **Graham Collins** publié en 2006 dans Scientific American (8 pages) précise un peu les choses. On y apprend notamment que les portes quantiques topologiques nécessitent un long enchaînement de permutations anyoniques comme avec la porte CNOT présentée en bas du schéma. Le tout, en conservant bien les notions de superposition et d'intrication ! C'est **Alexei Kitaev**, à l'époque chercheur chez Microsoft, qui eu cette idée en 1997 d'utiliser des anyons pour des calculs quantiques.

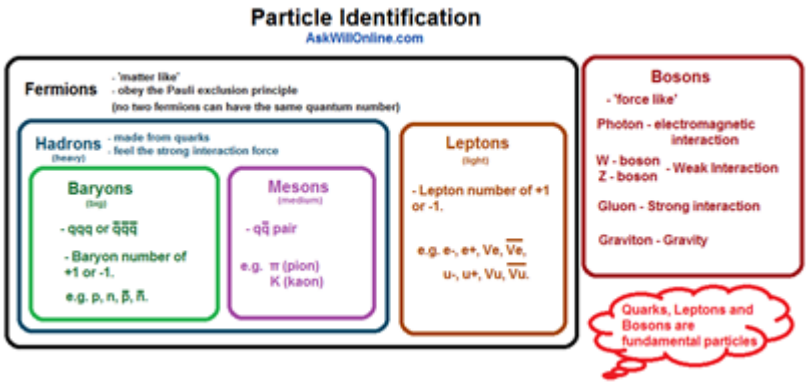


D’un point de vue physique, les anyons sont des “quasi-particules”, à savoir des modèles de représentation de particules qui décrivent l’état de nuages d’électrons autour d’atomes (pour faire simple).

Les fermions de Majorana sont un type spécifique de quasi-particules. Ils ont des comportements collectifs d’électrons dans des réseaux cristallins à très basse température. L’explication, en français, la plus proche de la notion de compréhension humaine est un article de **La Recherche** de novembre 2017, **Les promesses des fermions de Majorana** de Manuel Houzet, Julia Meyer et Pascal Simon.

La complexité du sujet pourrait déclencher une véritable onde de choc dans l’enseignement de l’informatique car ces concepts associent mathématiques, physique et informatique à un niveau doctorat. On est loin de 42 ! C’est la thèse de Hugo de Garis dans **Topological Quantum Computin The TQC Shock Wave and its Impact on University Computer Science Teaching**, 2011 (29 pages).

Pour comprendre le topologique et les fermions de Majorana, il faut se plonger dans le bestiaire de la physique des particules. Les fermions sont les particules de la matière et comprennent les leptons (électrons, neutrinos) et les baryons (protons, neutrons, à base de quarks) et qui composent les noyaux des atomes.



Les fermions de Majorana en sont un cas particulier qui correspondent à une sorte d'état de nuages d'électrons autour du noyau d'atomes et qui se manifestent aux deux bouts de fils supraconducteurs.

Un débat court chez les physiciens sur l'existence même de ces fermions. Leo Kouwenhoven des Delft Lab (puis MSR) annonçait la détection de quasi-particules en 2012 à TU Delft. Cette découverte était ensuite confirmée en 2016 au MIT. Plus récemment, un groupe de trois université américaines UC Irvine, UCLA et Stanford aurait découvert de vrais fermions de Majorana. La source française de cette annonce **Une particule théorique pour créer un ordinateur quantique impossible à hacker** (2018) illustre au passage la difficulté de vulgariser le domaine. Les inexactitudes et approximations y sont énormes. En effet, la hacking d'ordinateur quantique n'est pas plus facile avec des fermions de Majorana qu'avec la totalité des autres technologies de qubits. Le hack, s'il a lieu, sera d'ailleurs toujours possible au niveau de l'indispensable ordinateur traditionnel qui pilote le processeur quantique.

Avec cela en tête, voyons où en sont les deux acteurs principaux de ce domaine, Microsoft et Nokia. Leur investissement parallèle n'ayant rien à voir avec la mésaventure dans les smartphones qui a relié les deux marques il y a quelques années.

Microsoft

Microsoft Research planche sur le quantique topologique et les fermions de Majorana depuis pas mal n'années mais n'a pas encore de prototype à ce stade. Microsoft fait un pari de s'appuyer sur une particule virtuelle dont on n'a pas encore véritablement vérifié l'existence. C'est un pari très risqué, avec plein d'avantages stratégiques si cela fonctionne ! En effet, les qubits Majorana seraient bien plus fiables et générant moins d'erreurs, de l'ordre de 10 puissance moins 30, avec comme implication, le fait que l'on peut se passer des codes de correction d'erreurs utilisés avec les qubits supraconducteurs.

Médaille Fields en 1986 pour ses travaux sur la conjecture de Poincaré, **Michael Freedman** de l'Université de Santa Barbara rejoint Microsoft en 1997. Dans **Topological Quantum Computation** publié en 2002 et mis à jour en 2008 (12 pages), il démontre avec Alexei Kitaev la possibilité de faire du quantique avec une particule hypothétique, le fermion de Majorana, conceptualisé en 1937 par l'Italien Ettore Majorana à partir de la résolution d'équations mathématiques de Dirac.

Ce fermion est une particule étrange, dont la charge et l'énergie sont nulles et qui et sa propre antiparticule. Freedman et Kitaev seront recrutés par Microsoft Research. Piloté par Michael Freedman, Microsoft Quantum Santa Barbara (Station Q) est installé sur le campus de l'Université de Santa Barbara en Californie d'où il vient. Microsoft valorise ainsi des résultats de la recherche européenne : Pays-Bas (Delft), Danemark (Niels Bohr

Institute) et Italie (Majorana, OK, il est mort il a plus de 80 ans). Mais pas que, puisqu'il s'appuie aussi sur des recherches provenant des USA.

Ettore Majorana 1906-1938	Michael Freedman et Alexei Kitaev MSR	Leo Kouwenhoven Delft Lab puis MSR	Charles M. Marcus Niels Bohr Institute et MSR
fermions théorisés en 1937, particule virtuelle sans énergie ni charge qui est sa propre antiparticule	**publient « Topological Quantum Computation » en 2002, jettant les bases de l'informatique quantique topologique**	**détection de quasi-particules en 2012 à TU Delft puis en 2016 au MIT**	**mise au point des qubits à base de fermions de Majorana**

D'un point de vue pratique et matériel, les fermions de Majorana sont en fait des comportements étranges d'électrons et de leur spin que l'on trouve aux deux bouts de fils supraconducteurs. Les fermions de Majorana opèrent donc aussi à très basses températures, comme pour les qubits supraconducteurs. Vus de près, ces qubits sont des variantes sophistiquées de qubits supraconducteurs. Ils doivent eux aussi être refroidis à environ 15-20 mK.

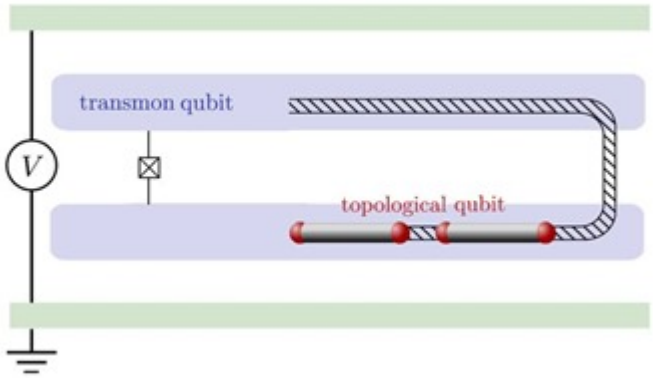
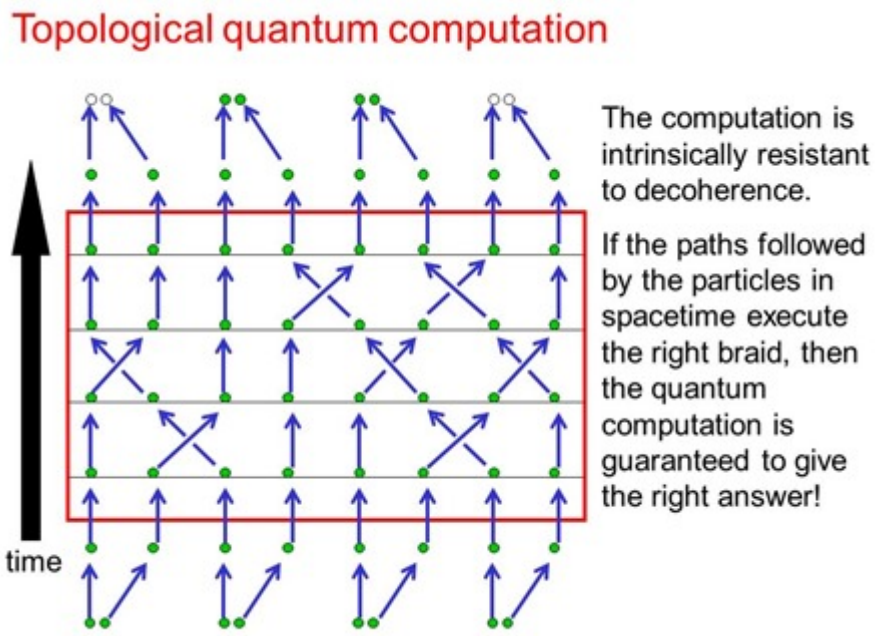


Fig. 6: *Read out of a parity qubit in a Cooper pair box. Two superconducting islands (blue), connected by a split Josephson junction (crosses) form the Cooper pair box. The topological Majorana qubit is formed by four Majorana fermions (red spheres), at the end points of two undepleted segments of a semiconductor nanowire (striped ribbon indicates the depleted region). A magnetic flux Φ enclosed by the Josephson junction controls the charge sensitivity of the Cooper pair box. To read out the topological qubit, two of the four Majorana fermions that encode the logical qubit are moved from one island to the other. Depending on the quasiparticle parity, the resonance frequency in a superconducting transmission line enclosing the Cooper pair box (green) is shifted upwards or downwards by the amount which is exponentially small in* E_J/E_C.

Ces associations "topologiques" en mailles apportent une protection contre la décohérence des qubits car la forme des tresses importe peu tant que leur topologie est stable.



Microsoft annonçaient à la conférence Build de mai 2018 qu'ils sortiraient leur premier ordinateur quantique à base de fermions de Majorana en 2023, ce qui est un peu loin, surtout dans la mesure où ils ne précisent pas le nombre de qubits associés. En 2023, les prévisions de marché des ordinateurs quantiques sont autour de $1,9B, ce qui n'est pas grand-chose et est déjà pas mal compte-tenu de sa maturité actuelle.

Realizations	Lifetimes	Gate Speed	ECC cost
Topological (Majorana)	1 minute	Nanoseconds	10^1
Flux Qubit	$/ 10^{10}$	same	$10^3 - 10^4$
Charge Qubit	$/ 10^{10}$	same	$10^3 - 10^4$
Transmon	$/ 10^7$	same	$10^3 - 10^4$
Ion Trap	$/ 10^2$	10^3 slower	$10^3 - 10^4$

- ECC is extremely painful (no "quantum refresh" like DRAM)
- Many can be fabricated with variations on standard semiconductor techniques

qubits plus stables
faible bruit de décohérence
peu d'erreurs
temps de cohérence long
rapidité des portes

} prototype en cours de réalisation
algorithmes différents

Microsoft a évidemment investi côté logiciels, d'abord avec sa plateforme Liquid, puis avec F# pour le scripting et avec le langage Q# servant à la programmation quantique, lancé fin 2017. Contrairement à d'autres approches, ce n'est pas un langage quantique "cross-platform" adapté aux autres types de qubits. L'une des contributrices de ces efforts est la chercheuse Krysta Svore qui vient de l'Université de Columbia.

Voici quelques pistes pour en savoir plus : **A Software Design Architecture and Domain-Specific Language for Quantum Computing** 2014 (14 pages), **Quantum Computing at Microsoft** (56 slides) et **Quantum Computing Research at Microsoft** (59 slides) de Dave Wecker et **A short introduction to topological quantum computation** de Ville Lahtinen et Jiannis Pachos, 2017, (43 pages). Et quelques vidéos : **keynote de novembre 2017** avec notamment Leo Kouwenhoven (43 mn), **conférence Build de mai 2018** sur Q# (1h15mn) et **Majorana qubits** de Xiao Hu, en mai 2017 (22 mn).

Les Bell Labs de Nokia aux USA, situés à Murray Hill dans le New Jersey, travaillent aussi sur le topologique mais sont relativement discrets sur le sujet. Cf **Quantum computing using novel topological qubits at Nokia Bell Labs** publié en 2017 qui décrit leur approche dans le topologique sachant qu'aucune roadmap n'est communiquée.

Nokia soutient aussi l'initiative **Quopal** de l'Université d'Oxford sur l'usage du quantique dans le machine learning.

Au passage, Nokia aime à rappeler que les algorithmes de Grover et Shor ont été découverts par leurs créateurs dans les Bell Labs. Et logiquement, Nokia planche aussi sur la cryptographie quantique, au moins au niveau de son transport sur fibres optiques comme en témoigne ce **partenariat** avec le Coréen SK Telecom de 2017.

Optique linéaire

L'optique linéaire est utilisée pour créer des qubits exploitant la polarisation de photons. Aujourd'hui, c'est un outil de laboratoire qui n'est pour l'instant pas sérieusement pris en main par des acteurs commerciaux comme le sont les qubits à base de supraconducteurs, d'ions piégés ou de quantum dots CMOS.

L'avantage de la photonique est de permettre de gérer des qubits assez stables avec un taux d'erreurs très faible, surtout au regard de celui des qubits à supraconducteurs. Ils fonctionnent aussi à température ambiante.

Leur inconvénient réside dans la difficulté à assembler plus que quelques qubits et à gérer leur superposition et leur intrication. Seuls les Chinois communiquent sur le sujet comme nous le verrons dans une partie à venir mais sans force détails.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est un photon unique.
- Les **portes quantiques unitaires** sont activées par des circuits optiques.
- Les **portes quantiques à deux qubits** utilisent aussi des circuits optiques.
- La **mesure de l'état d'un qubit** utilise des détecteurs de photons uniques.

Laboratoires qui bossent dessus ? Ils sont surtout issus du Royaume Uni et des USA, notamment dans les Universités d'Oxford, de Bristol, de Cambridge et de Southhampton, selon **Quantum Age technological opportunities** du gouvernement UK Office of Science en 2016 (64 pages).

Pour en savoir plus, voir aussi **Why I am optimistic about the silicon-photonic route to quantum computing**, de Terry Rudolph, publié en 2016 (14 pages) ainsi que l'application de l'**échantillonnage de bosons**.

HP fait de la recherche en informatique quantique dans son laboratoire de Bristol au Royaume-Uni. Cela couvre à la fois le calcul quantique, la cryptographie et les communications quantiques. Ils ont investi dans leur projet “The Machine” qui est conceptuellement un peu éloigné d’un ordinateur quantique universel et utilise un bus optique pour relier les différents composants de ce supercalculateur. Bref, tout cela n’est pas bien clair ni bien avancé.

En partenariat avec HP, des scientifiques américains et japonais proposaient en 2008 la création d’un HPQC, High Performance Quantum Computer, avec des matrices 3D de qubits réalisés en optique linéaire contenant 7,5 milliards de qubits physiques permettant d’accumuler 2,5 millions de qubits logiques dans **High performance quantum computing** (7 pages). Un projet qui n’a pas été suivi d’effets ! Les yeux plus gros que le ventre ?

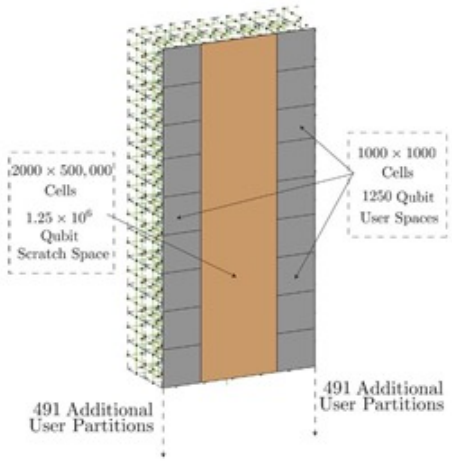


Fig. 3 Illustrated is an example partitioning of the global 3D lattice for a HPQC mainframe. This global lattice measures 4000 × 500, 000 unit cells and requires approximately 7.5×10^9 photonic chips to prepare. If utilized as a single cluster computer, 2.5 million logical qubits are available with sufficient topological protection for approximately 10^{16} time steps (where a time step is defined as the measurement of a single layer of unit cells, corresponding approximately to 10^{11} logical, non-Clifford group operations [5]).

TundraSystems Global est une minuscule startup de Cardiff au Royaume Uni créée en 2015 qui ambitionne de créer une solution d’ordinateur quantique optique full-stack. Leur Advisory Board comprend deux scientifiques chinois, Xinliang Zhang et Pochi Yeh qui sont spécialisés en optronique (**site**).

Xanadu est une startup de Toronto créée en septembre 2016 par Christian Weedbrook, un **chercheur prolifique**, et financée à hauteur de $7M. La société prévoit de proposer ses ressources de calcul quantiques en cloud. Elle a développé une plateforme logicielle **Strawberry Fields** qui est adaptée au développement de solutions quantiques adaptées aux calculateurs quantiques optiques.

Ils ont créé les qubits “qumodes” qui permettent de manipuler de l’information continue permettant d’avoir plus de stockage quantique dans le calculateur. C’est documenté dans **The power of one qumode for quantum**

computation, 2016 (10 pages).

Atomes neutres piégés

L'Université du Wisconsin est l'un des laboratoires de recherche qui creuse la piste des qubits à base d'atomes neutres.

Le principe général de ces qubits est le suivant :

- L'**état quantique** du qubit est l'état "hyperfin" – un niveau d'énergie – d'un atome neutre unique. Les qubits sont arrangés en matrice sur une plaque. Ils sont refroidis par laser. Un qubit peut utiliser un seul atome ou un groupe d'atomes selon les méthodes employées.
- Les **portes quantiques unitaires** sont activées par micro-ondes ou lasers.
- Les **portes quantiques à deux qubits** utilisent également des micro-ondes et lasers.
- La **mesure de l'état d'un qubit** utilise une caméra CCD qui détecte la fluorescence des atomes.

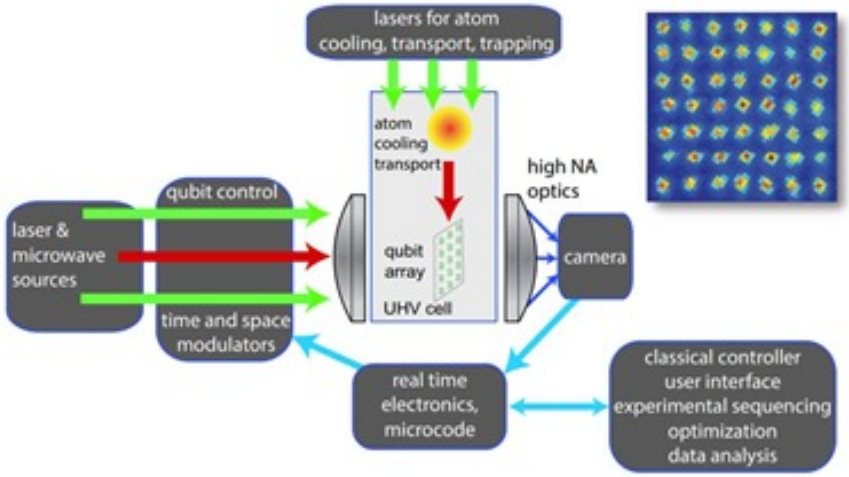


Figure 1. Architecture for a neutral atom quantum computer. The inset shows a fluorescence image of a 49 site qubit array[13].

Ils ont de longs temps de cohérence mais des taux d'erreurs encore trop élevés, de l'ordre de 1%. On assemble jusqu'à 51 qubits en laboratoires. Tout cela mériterait plus de détails mais cela commence à faire long !

Pour en savoir plus, direction **Quantum computing with atomic qubits and Rydberg interactions: Progress and challenges**, 2016 (28 pages, d'où est extrait le schéma *ci-dessus*), **Randomized benchmarking of single qubit gates in a 2D array of neutral atom qubits**, 2015 (7 pages) ainsi que **Scientists demonstrate one of largest quantum simulators yet, with 51 atoms**, 2017.

Interconnexions quantiques

Une technologie d'ordinateurs quantiques va jouer un rôle complémentaire à celles des processeurs de qubits : celles qui permettent l'interconnexion entre processeurs quantiques, sans perdre l'état quantique des qubits. C'est une technologie qui deviendra vite indispensable pour permettre la répartition de calculs quantiques sur plusieurs processeurs quantiques, un peu comme on le fait avec les chipsets multi-coeurs ou avec les architectures de répartition de traitement sur plusieurs CPU et plusieurs serveurs. Cela sera notamment utile pour les architectures de qubits qui seront limitées en nombre de qubits par systèmes de cryogénie, notamment

dans les supraconducteurs, qui ne pourront en consolider que quelques centaines grand maximum. Il faudra donc pouvoir relier des qubits de processeurs distants pour permettre leur intrication selon les algorithmes utilisés.

Différentes techniques d'interconnexion quantiques sont possibles. La plus générique est optique et elle est faiblement contrainte par la distance. A courte distance, des liaisons par micro-ondes sont envisageables, notamment pour coupler des qubits supraconducteurs.

L'Université de **Princeton** associée à celle de **Konztanz** en Allemagne travaille de son côté sur l'interconnexion optique entre processeurs quantiques CMOS. C'est documenté dans **Quantum Computing Advances With Demo of Spin–Photon Interface in Silicon**, 2018. La magie consiste à transférer l'état quantique d'un spin d'électron à un photon au niveau de sa phase.

Nous en avons terminé avec le tour des grands acteurs des ordinateurs quantiques. Dans la **partie suivante**, nous ferons un inventaire de l'écosystème mondial des startups de l'informatique quantique en passant par les quelques fonds d'investissement spécialisés dans l'informatique quantique. Puis nous aborderons le vaste sujet de la **cryptographie quantique et post-quantique**.

Cet article a été publié le 21 août 2018 et édité en PDF le 15 mars 2024.