Les défis des technologies quantiques

Par Ilarion PAVEL
Conseil général de l'économie

Le développement des technologies quantiques est aujourd'hui l'objet d'importants efforts de recherche, mais les résultats seront-ils à la hauteur des attentes ? L'ordinateur quantique peut résoudre certains problèmes difficiles, qui demandent à l'ordinateur classique un temps de calcul trop important, et peut également attaquer les schémas actuels de cryptage. Cependant, la réalisation d'un ordinateur quantique suffisamment puissant pour résoudre des problèmes pratiques demeure un véritable défi technologique. Il existe plusieurs technologies d'implémentation *hardware*, chacune avec ses avantages et ses inconvénients. Comme ils sont plus faciles à réaliser, la recherche se dirige également vers la mise au point d'ordinateurs quantiques analogiques et de simulateurs quantiques. Parallèlement, ces travaux ont pour conséquence la conception de capteurs extrêmement sensibles, qui ont de nombreuses applications dans l'industrie de la prospection géologique, dans l'imagerie médicale, dans les technologies militaires et la mise au point de nouvelles méthodes de cryptage immunes contre l'attaque par un algorithme quantique.

Introduction

Les programmes de R&D dans le domaine des technologies quantiques sont actuellement en plein essor.

En effet, l'investissement mondial de R&D dans le domaine du calcul quantique depuis 2001 est estimé à 30 milliards d'euros, il est de 2,5 milliards d'euros en 2022. Parmi les acteurs on compte quelque 350 *start-up*.

L'Union européenne a alloué 1 milliard d'euros de financement sur 10 ans pour lancer le projet European Quantum Flagship[1] en 2018, qui implique plus de 3 500 académiques et industriels, dont le but est de consolider et étendre le *leadership* et l'excellence scientifiques européens dans ce domaine de recherche afin de relancer une industrie européenne de la technologie quantique.

En 2018, l'Allemagne a alloué 650 millions d'euros à son programme de technologies quantiques et à un programme-cadre visant à commercialiser les technologies quantiques[2]. En 2020, le gouvernement fédéral allemand a annoncé un effort quantique supplémentaire de 2 milliards d'euros sur 5 ans s'ajoutant au milliard d'euros investis par l'Union européenne.

La France investissait chaque année 60 millions d'euros dans les technologies quantiques avant 2021, date à laquelle le gouvernement a annoncé un plan d'investissement sur cinq ans de 1,8 milliard d'euros dans les technologies quantiques, financé par l'État en partenariat avec des industriels, dont une part publique annuelle d'environ 200 millions d'euros[3].

Le Royaume-Uni a investi 385 millions de livres entre 2015 et 2019 dans une première phase de développement des technologies quantiques (capteurs gravitationnels ultra-sensibles, simulateurs quantiques et ordinateurs quantiques, horloges atomiques miniatures), qui a connu un grand succès. En conséquence, on a annoncé une deuxième phase de cinq ans, avec un investissement de 153 millions de livres de la part de l'État britannique et de 205 millions de livres de la part des industriels. En 2018 a été créé au Royaume-Uni un centre national d'informatique quantique pour développer un ordinateur quantique[4].

Depuis 25 ans, les États-Unis financent des programmes de recherche quantique liés à la défense. En 2018, ils ont lancé le programme NQI (National Quantum Initiative[5]) avec un budget de plus de 1,2 milliard de dollars pendant 5 ans, destiné principalement au NIST, NSF, DoE mais aussi à divers partenaires industriels et académiques.

On estime que la Chine aurait investi environ 10 milliards de dollars dans les technologies quantiques. D'ici 2030, le pays vise à étendre son infrastructure nationale de communications quantiques, à développer un prototype d'ordinateur quantique et à construire un simulateur quantique.

[1] https://qt.eu

[2] www.science-allemagne.fr/wp-content/uploads/2021/02/Dossier_Quantique_Communication.pdf

[3] www.futura-sciences.com/tech/actualites/ordinateur-quantique-france-investit-18-milliard-euros-technologies-quantiques-85283/

[4] https://uknqt.ukri.org/

[5] www.quantum.gov

Encadré 1 : Le chat de Schrödinger

Un exemple bien connu de système quantique est le chat de Schrödinger : imaginons un chat enfermé dans une boîte opaque, qui contient un atome dont la probabilité de se désintégrer dans l'heure qui suit est de 50 %. Si la désintégration a lieu, elle déclenche un mécanisme qui brise une fiole de cyanure et tue le chat. Quel est l'état du chat après une heure ? Réponse : moitié vivant et moitié mort divisé par √2 ! Conformément aux lois quantiques, le système est décrit comme une superposition de deux états : vivant et mort. Initialement, le chat se trouve à l'état vivant, puis il évolue dans le temps, suivant l'équation de Schrödinger, pour se trouver une heure plus tard dans une superposition moitié vivant et moitié mort. Il n'est donc ni vivant ni mort, mais dans un état superposé.

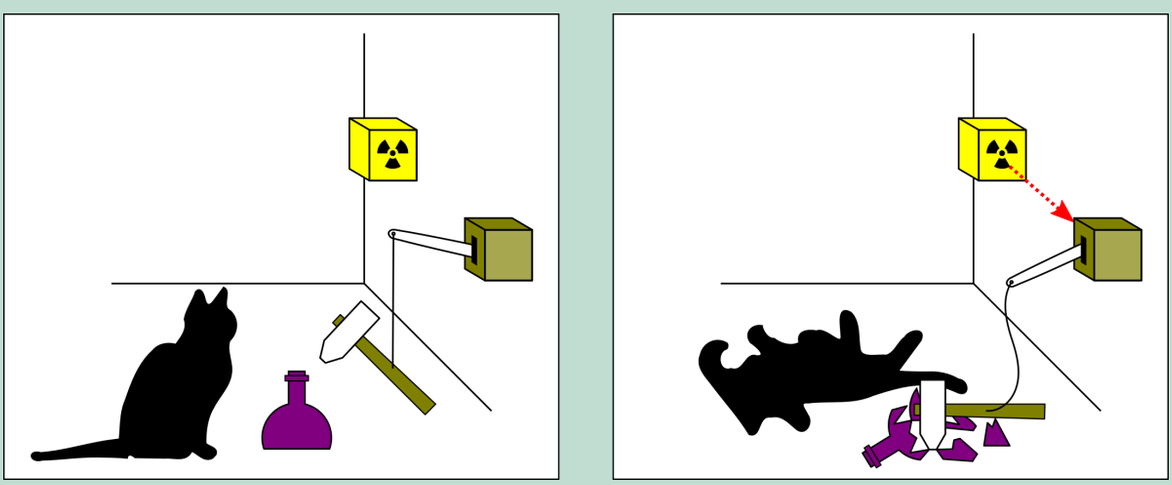

Figure a : Le chat est enfermé dans une boîte, munie d'un dispositif qui casse une fiole de cyanure. Ce dispositif est activé par la désintégration d'un atome, dont la probabilité de désintégration dans l'heure suivante est de 50 %.

Et si on ouvre la boîte ? Cela équivaut à effectuer une mesure, on projette alors l'état du chat sur un des états propres (vivant ou mort), avec les probabilités, dans notre cas, de 50 % et 50 %. En d'autres termes, si on effectue un grand nombre d'expériences identiques avec un grand nombre de chats, statistiquement, lorsqu'on ouvre les boîtes, la moitié des chats sont vivants, l'autre moitié sont morts.

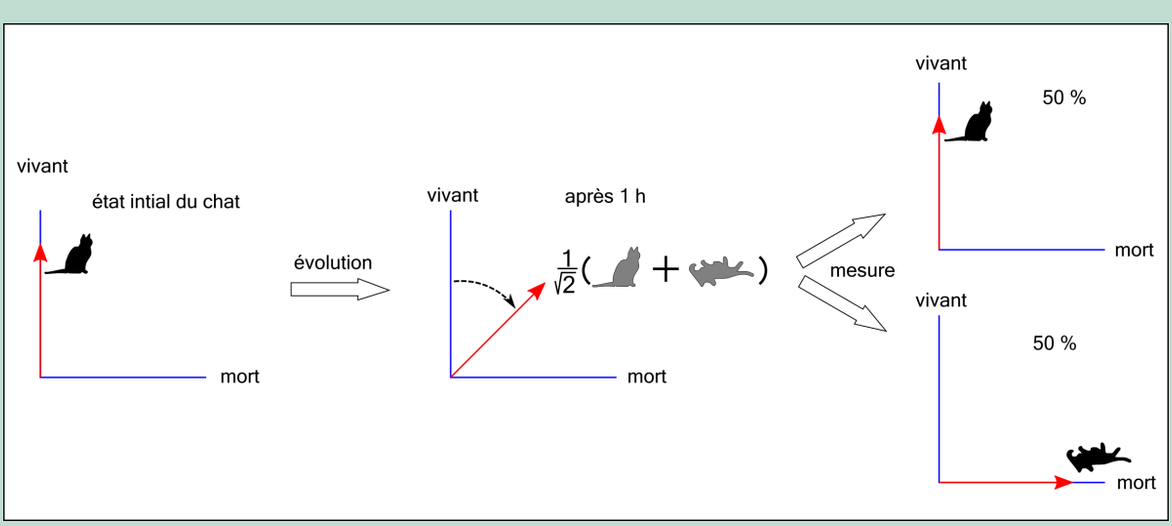

Figure b : Initialement le chat se trouve dans l'état vivant, mais après une heure, suivant l'équation d'évolution de Schrödinger, il se trouve dans un état superposé vivant + mort. En ouvrant la boîte, on effectue le processus de mesure : dans 50 % des cas le chat est vivant, dans 50 % il est mort.

Au Japon, l'investissement dans les technologies quantiques s'élève à 700 millions de dollars depuis 2001. En 2018, le gouvernement japonais a lancé l'initiative Quantum Leap dans diverses technologies quantiques (simulation et calcul quantique, détection quantique, laser à impulsions ultracourtes). Un des projets du programme Moonshot investira 150 millions de dollars pour créer un ordinateur quantique universel tolérant aux pannes en 2050.

Les résultats seront-ils à la hauteur des énormes moyens investis ?

Principes généraux

Les concepts quantiques ont été développés au début du XX^{e} siècle pour permettre la compréhension des phénomènes que la physique classique ne pouvait pas expliquer : le rayonnement du corps noir, l'effet photoélectrique, le spectre atomique discret, la stabilité de l'atome. Les formalismes mathématiques furent développés : la mécanique matricielle en 1925 par Heisenberg, et la mécanique ondulatoire en 1926 par Schrödinger, qui sont de fait des formulations équivalentes. La mécanique quantique reste un des plus grands succès de la physique et n'a jusqu'à présent jamais été prise en défaut.

Alors qu'en mécanique classique, l'état d'un système est donné par la position et la vitesse de ses composants, en mécanique quantique, il est décrit par un vecteur d'état dans un espace de Hilbert. En mécanique quantique une observable physique est représentée par un opérateur hermitien (valeurs propres réelles et vecteurs propres orthogonaux), l'état de tout système peut être écrit comme une superposition d'états propres de l'opérateur et son évolution dans le temps est décrite par l'équation de Schrödinger. Lorsqu'on effectue une opération de mesure, on projette l'état du système sur un des vecteurs propres de l'observable mesurée, avec une probabilité proportionnelle avec le module carré de la projection du vecteur d'état sur le vecteur propre.

Ce formalisme reste abstrait et en quelque sorte contre-intuitif mais il est absolument nécessaire pour décrire les comportements des objets de taille atomique. Cependant, plus la taille des objets augmente, plus les effets quantiques s'estompent, on retrouve alors le formalisme de la physique classique : c'est le principe de correspondance de Bohr.

En ce qui nous concerne, nous sommes des êtres macroscopiques, munis d'organes sensoriels qui, ne nous permettent pas de mesurer directement les atomes et les photons individuels, mais plutôt la moyenne de leur effets collectifs. Nous n'avons donc pas un accès direct au monde quantique, c'est pourquoi la mécanique quantique nous paraît contre-intuitive.

Ordinateur quantique

L'ordinateur quantique fonctionne suivant le formalisme mathématique de la mécanique quantique et fait intervenir les concepts de superposition, intrication et interférence. La force du calcul quantique réside dans une parallélisation[6] massive, qui résulte de la superposition et de l'intrication des états. Dans un ordinateur classique, un bit peut prendre deux valeurs, 0 et 1, alors que dans un ordinateur quantique, le bit quantique (qubit) peut prendre toute superposition des deux états, notés |0> et |1>. Dans un ordinateur classique, N bits peuvent décrire 2N états, dans un ordinateur quantique, les N qubits peuvent être intriqués, ce qui permet alors de décrire 2^N états. Ainsi, 300 qubits forment environ 10^{90} états, nombre énorme, qui dépasse largement le nombre des particules de l'Univers.

Les capacités de calcul d'un ordinateur quantique semblent pratiquement illimitées, cependant, lorsqu'on effectue le processus de mesure, on ne peut mesurer qu'un seul des 2^N états (ou une seule combinaison de ces états), ce qui détruit tout l'avantage de la parallélisation. La situation est partiellement sauvée par la possibilité de faire interagir les qubits entre eux en utilisant le phénomène quantique d'interférence. Cela conduit à construire des portes logiques et à les combiner astucieusement pour réaliser des circuits quantiques

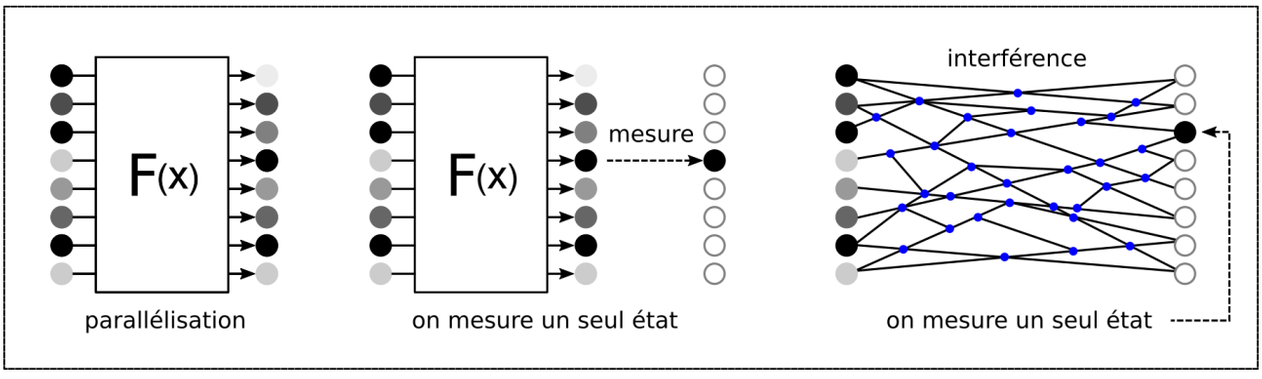

Figure 1 : Le quantique permet une parallélisation massive. Malheureusement, lors du processus de mesure, on ne peut mesurer qu'un seul état. Cependant, en tirant partie du phénomène d'interférence, on peut faire interagir les qubits *via* des portes logiques qu'on assemble pour former des circuits quantiques, capables d'exécuter des algorithmes.

[6] Il s'agit d'effectuer un grand nombre de calculs simultanément, ce qui permet de diviser un problème donné en problèmes plus petits, qui peuvent ensuite être traités en même temps, ce qui permet un gain de temps substantiel.

capables d'effectuer des algorithmes quantiques. Un tel algorithme doit produire un état final dont la probabilité de mesure est égale soit à 1, soit à 0. C'est en mesurant cet état qu'on peut alors caractériser les 2^N états initiaux, ce qui équivaut, dans quelques cas, à la résolution d'un problème précis, comme on le verra par la suite.

Par rapport à l'ordinateur classique, l'ordinateur quantique peut résoudre très rapidement certains problèmes, mais il ne dispose pas d'une grande flexibilité : il reste relativement difficile de mettre au point des algorithmes quantiques utiles dans la résolution de problèmes pratiques importants, leur nombre est malheureusement bien plus faible que celui des algorithmes classiques. D'ailleurs, l'ordinateur quantique ne remplacera pas son homologue classique, mais il sera plutôt utilisé pour accélérer l'exécution de certains sous-programmes dont le temps d'exécution par l'ordinateur classique est trop long.

On peut alors construire une large gamme de portes quantiques, dont les plus importantes sont la rotation de phase, le control NOT (CNOT) et la porte Hadamard.

Combinées de façon appropriée, ces portes quantiques permettent de réaliser des circuits quantiques implémentant des algorithmes quantiques. Par exemple, en associant une porte Hadamard avec une porte CNOT, on obtient un circuit qui crée des états intriqués, c'est-à-dire qui ne peuvent pas s'écrire comme produit de deux états indépendants. On ne peut pas mesurer les qubits de manière indépendante : la mesure de l'un détermine automatiquement l'autre. Les états intriqués trouvent des applications importantes dans la cryptographique quantique, comme le protocole BB84 de distribution des clés cryptographiques (voir l'encadré 3).

Parmi les algorithmes quantiques les plus connus figurent l'algorithme de Grover et l'algorithme de Shor[7].

L'algorithme de Grover accélère la recherche dans les listes non structurées, par exemple pour chercher le nom d'une personne dans une liste de noms présentés dans un ordre aléatoire. Avec l'algorithme classique, le nombre d'opérations effectuées pour trouver le nom recherché augmente de manière proportionnelle au nombre *N* d'éléments de la liste, alors que dans l'algorithme de Grover, il n'augmente qu'avec $\sqrt{N}$. Cependant, l'algorithme de Grover ne sera pas utilisé pour effectuer des recherches dans les bases de données. En général, celles-ci sont structurées, et dans une liste structurée, pour un algorithme classique, le nombre d'opérations n'augmente qu'avec *log(N),* donc l'algorithme de recherche classique appliqué à une liste structurée est plus efficace que l'algorithme quantique de Grover dans une liste non structurée. Ensuite, dans l'algorithme quantique, le nombre de portes quantiques nécessaires pour implémenter cet algorithme est environ *log(N)*, ce nombre est du même ordre de grandeur que le nombre de cellules mémoire nécessaires pour implémenter l'algorithme classique. L'algorithme de Grover sera plutôt utilisé pour chercher des solutions à des problèmes difficiles, comme par exemple trouver un cycle Hamiltonien dans un graphe[8] ou résoudre le problème du voyageur de commerce[9].

L'algorithme de Shor permet de factoriser un nombre entier en facteurs premiers beaucoup plus vite que tout autre algorithme classique, ce qui permettrait à un ordinateur quantique d'attaquer les protocoles actuels de cryptage comme le protocole RSA ou ceux fondées sur les courbes elliptiques.

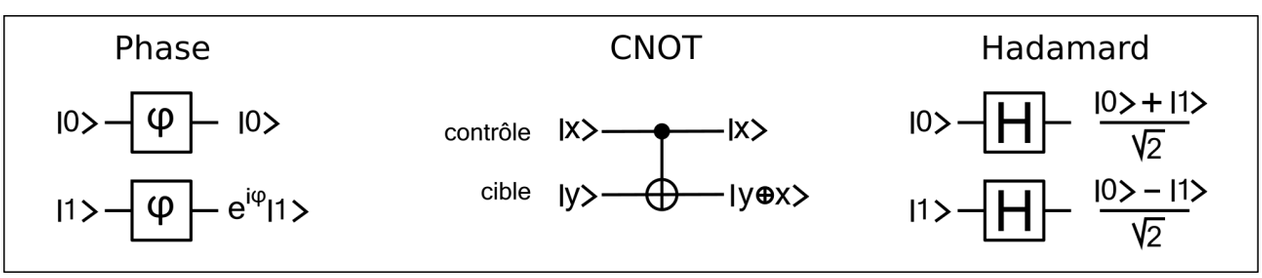

Figure 2 : La porte de phase rajoute une phase à l'état |1>, elle laisse l'état |0> inchangé. Dans la porte CNOT, si le qubit de contrôle est 1, la porte CNOT change le qubit cible de |0> en |1>, ou de |1> en |0>. Si le qubit de contrôle est 0, le qubit cible reste inchangé. La porte Hadamard transforme les états |0> ou |1> en superposition d'états orthogonaux.

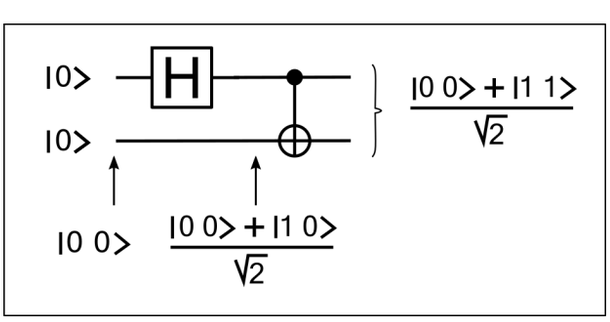

Figure 3 : Un simple circuit quantique qui permet de réaliser des états intriqués. Si on mesure un qubit, l'autre est alors automatiquement déterminé. Par exemple, si la mesure rend la valeur 0 pour le premier qubit, le deuxième qubit aura la valeur 0, si la mesure rend la valeur 1 pour le premier qubit, le deuxième aura la valeur 1.

[7] Voir par exemple N. David Mermin - *Quantum computer science: an introduction* (Cambridge University Press, 2007).

[8] Cycle qui passe par tous les sommets d'un graphe forcément une fois et pas plus d'une fois.

[9] Étant donné un ensemble de villes à visiter, il faut établir le circuit le plus court qui passe par chaque ville une seule fois.

Encadré 2 : Complexité des algorithmes

La complexité d'un algorithme nécessaire pour résoudre un problème énoncé nous montre comment le nombre de pas, et en conséquence le temps de calcul, augmente avec le nombre de données à l'entrée.

Ainsi, la classe de problème *P* (deterministic Polynomial) est formée par les problèmes qui peuvent être résolus par un ordinateur classique dans un nombre de pas qui augmente de manière polynomiale avec les nombres de données à l'entrée. Ce sont des algorithmes faciles, par exemple rechercher un nom dans une liste non ordonnée de *N* noms, ce qui demande au plus *N* pas, ou résoudre un système de *N* équations avec *N* inconnues par la méthode du pivot de Gauss, ce qui nécessite au plus de l'ordre de N^3 pas.

La classe *NP* (Non deterministic Polynomial) représente des problèmes dont la solution peut être vérifiée dans un nombre de pas qui augmente de manière polynomiale avec le nombre de données à l'entrée. Ce sont donc des problèmes faciles à vérifier, en revanche trouver la solution n'est pas nécessairement facile. Bien entendu $P \subset NP$, en revanche on pense que $P \neq NP$ bien que cela ne soit pas toujours pas démontré (c'est un des sept problèmes du millénaire proposé par l'Institut Clay de mathématiques, dont la résolution sera récompensée par un million de dollars).

Les problèmes *NP* les plus difficiles forment la classe *NP – complet* par exemple le problème du voyageur de commerce, trouver les cliques (sous-graphe dont les sommets deux-à-deux adjacents) dans un graphe, le problème de coloration du graphe[1], trouver un cycle hamiltonien, le problème du sac à dos[2], trouver l'ensemble dominant maximal[3].

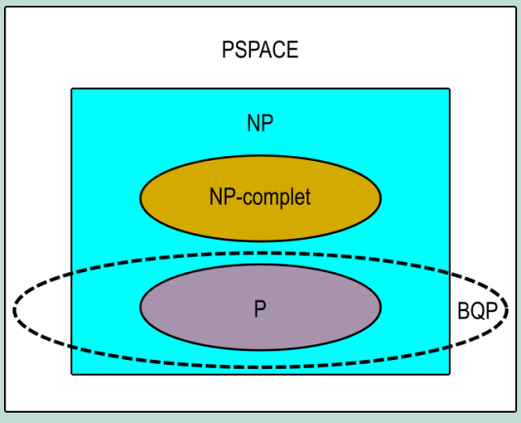

Figure a : Diagramme simplifié des classes de complexité d'un problème algorithmique tel qu'on le pense aujourd'hui, il n'y a pas encore de preuve mathématique.

La classe de problèmes *BQP* (Bounded Error Quantum Polynomial) consiste en problèmes qui peuvent être résolus par un ordinateur quantique dans un nombre de pas qui augmente de manière polynomiale avec le nombre de données à l'entrée. On pense aujourd'hui que l'ordinateur quantique est en mesure de résoudre des problèmes plus difficiles que la classe *P* en revanche il ne pourrait pas résoudre les problèmes *NP – complet* mais nous n'avons pas la preuve mathématique de cette affirmation. Parmi les algorithmes en mesure de résoudre des problèmes *BPQ* figurent l'algorithme de Shor, le calcul du logarithme discret (analogue de l'algorithme de Shor pour les courbes elliptiques), l'algorithme Harrow Hassidim Lloyd (résolution de systèmes d'équations linéaires), approximation de polynômes de Jones.

La classe *PSPACE* est constituée par les problèmes qui nécessitent une quantité polynomiale de mémoire, elle inclut les classes *NP* et *BQP*.

---

[1] Consiste à colorer chaque sommet du graphe de sorte que deux sommets reliés par une arête aient des couleurs différentes. On cherche alors à déterminer le nombre minimal de couleurs.

[2] On dispose de plusieurs objets ayant divers poids, qu'on veut mettre dans un sac, sans dépasser une valeur maximale fixée préalablement. Lesquels d'entre eux faut-il choisir afin de maximiser le poids du sac ?

[3] L'ensemble dominant est un sous-ensemble des sommets d'un graphe, tel que tout sommet du graphe qui n'appartient pas à cet ensemble possède au moins une arête liée à un des sommets de l'ensemble dominant. Le problème de l'ensemble dominant est de déterminer, étant donné le graphe et un nombre entier n, si le graphe admet un ensemble dominant d'au plus n sommets.

Encadré 3 : Protocole BB84 de distribution de clés cryptographiques.

Proposé par Charles Bennett et Gilles Brassard en 1984, c'est le premier protocole de ce type. Deux personnes, Alice et Bob, veulent établir une clé cryptographique commune. Alice utilise des paires de photons dont les polarisations sont intriquées. On ne connaît pas *a priori* la direction précise de l'orientation de ces polarisations, mais juste le fait qu'ils sont orientés dans la même direction. Les paires étant intriquées, si en mesurant la polarisation d'un photon on obtient une orientation donnée, la polarisation de l'autre photon aura la même orientation. Alice effectuera alors des mesures sur un des photons de la paire, en plaçant les polariseurs de manière aléatoire suivant deux classes de directions : horizontal/vertical et 45/- 45 degrés. Elle décide qu'un photon polarisé horizontalement représente un bit 0, polarisé verticalement un bit 1, polarisé à - 45 un bit 0, polarisé à 45 un bit 1.

L'autre photon de la paire intriquée est envoyé à Bob, qui effectuera les mêmes types des mesures qu'Alice, en utilisant également de manière aléatoire les deux classes de polariseurs, horizontal/vertical et 45/- 45 degrés. Pour chaque mesure, il notera la classe utilisée, ainsi que le résultat de sa mesure, un 0 ou un 1. Ensuite, Alice et Bob vont établir une communication classique, par exemple par téléphone, pour vérifier *a posteriori* les deux classes de polariseurs utilisées. Lorsque les deux ont utilisé la même classe de polariseurs, le résultat de la mesure est validé : les photons étant intriqués, les résultats d'Alice et de Bob sont identiques. Lorsqu'ils ont utilisé des classes différentes, le résultat de la mesure n'est pas pris en considération. Ainsi, Alice et Bob arrivent finalement à obtenir une suite identique de 0 et 1, qu'ils peuvent utiliser comme clé cryptographique.

Une personne malintentionnée, Eve, qui voudrait intercepter la clé ne connaîtra pas à l'avance la classe de polariseurs utilisée par Alice. De plus, si Eve mesure le photon envoyé par Alice (avant sa réception par Bob) en utilisant la mauvaise classe de polariseur, elle peut changer l'état du photon, qui à son arrivée chez Bob, peut donner un résultat de mesure différent de celui mesuré par Alice : la clé sera alors erronée et Alice et Bob vont alors se rendre compte que leur communication a été interceptée. Une question naturelle se pose alors : pourquoi Eve ne fait pas purement et simplement une copie du photon envoyé par Alice ? Elle ne le peut pas : il est impossible de copier à l'identique un état quantique inconnu (théorème du non-clonage quantique), résultat qui se démontre facilement à partir des principes de base de la mécanique quantique.

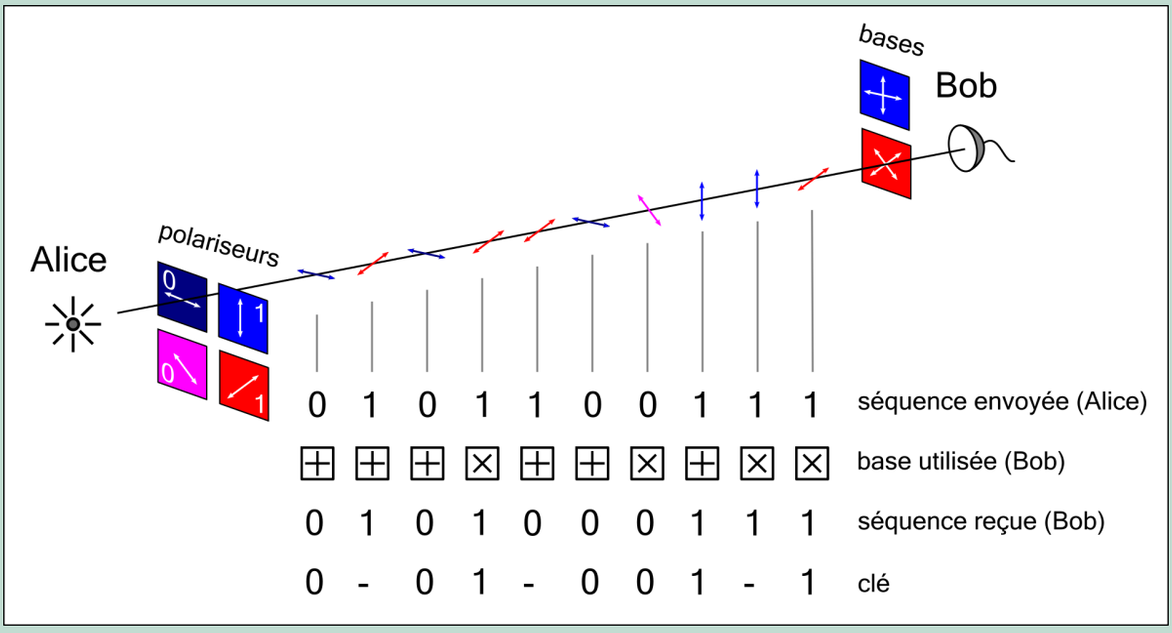

Figure a : Illustration de l'implémentation du protocole BB84 entre Alice et Bob.

En pratique, l'implémentation du protocole BB84 soulève plusieurs défis. D'abord, il nécessite l'utilisation de sources à un seul photon et de détecteurs très sensibles. Malheureusement, ces dispositifs ne sont pas parfaits, ce qui peut créer des failles de sécurité. Par exemple, Alice est contrainte d'utiliser

des sources à plusieurs photons, ce qui peut permettre à Eve de mesurer quelques photons et de laisser passer le reste à Bob. Une solution consiste à améliorer les protocoles afin qu'ils soient sécurisés malgré les imperfections des dispositifs.

Un autre défi important est la perte éventuelle de photons dans le canal de transmission (habituellement la fibre optique) par des phénomènes de diffraction, absorption ou perte de cohérence, ce qui limite la distance à laquelle la clé cryptographique peut être envoyée. De nouveau, on pourrait améliorer les protocoles, mais au prix d'une diminution importante du débit de transmission. Une autre solution consiste à mettre au point des répéteurs quantiques capables de téléporter l'état quantique[1], leur développement est en cours. Enfin, puisque dans l'espace les pertes sont beaucoup moins importantes et la décohérence négligeable, la communication quantique par satellite est considérée comme une solution plus prometteuse et a récemment réalisé d'importants progrès.

Plusieurs expériences ont déjà été réalisées. Ainsi, en 1995, Nicolas Gisin a transmis des clés cryptographiques à une distance de 23 km sur des fibres optiques commerciales passant au-dessous du lac Léman. En 2007, Anton Zeilinger l'a fait sur une distance de 144 km, par propagation atmosphérique, entre La Palma et Tenerife, deux des îles Canaries. Plus récemment, en 2016, une équipe chinoise l'a réalisé sur une distance de 1 120 km, dans l'espace, *via* le satellite Micius.

Plusieurs entreprises sont en train de développer des solutions de distribution de clé cryptographique : des PME comme ID Quantique (Suisse), QuintessenceLabs (Australie), Qubitekk (US), MagiQ Technologies (US), QuantumCTek (Chine), Quantum Xchange (US), Post-Quantum (US), Qasky (Chine), Quantinuum (US), Aurea Technologies (France), et des grands groupes comme Toshiba, NEC, NTT, Mitsubishi, Huawei, Fujitsu et ATT.

Notons qu'il existe de nombreux autres protocoles de distribution de clé cryptographique, par exemple E91, KMB09, Decoy state, qui sont des améliorations du BB84. Ainsi, E91, mis au point par Artur Ekert en 1991, peut détecter plus facilement les éventuelles interceptions effectuées par une personne malintentionnée. Le protocole KMB09 (Khan, Murphy et Beige) est plus robuste par rapport au bruit présent dans les canaux de communication, ce qui permet d'augmenter la distance de distribution des clés. Decoy state permet d'utiliser des sources à plusieurs photons et de détecter une éventuelle interception.

[1] Il est impossible de copier à l'identique un état quantique quelconque tout en gardant l'original (théorème du non-clonage quantique). La seule possibilité est de créer à distance un nouvel état quantique identique, mais en détruisant l'original, opération appelée téléportation quantique.

Même si la construction d'un ordinateur quantique capable de casser ces protocoles n'est pas envisagée à court et moyen terme, en 2016, la NIST a lancé un appel à projet pour mettre au point de nouvelles méthodes de cryptage (cryptographie *post* quantique) aussi bien pour l'échange de clé cryptographique que pour la signature électronique, qui ne pourront pas être attaquées par les algorithmes quantiques. Plusieurs technologies sont possibles : cryptographie sur réseau, polynômes multivariés, isogénie de courbes elliptiques, code correcteur d'erreurs, fonctions de hachage. Après quatre étapes de sélection, sur 69 candidats, la NIST a retenu en 2023 trois technologies pour la signature électronique et une technologie pour l'échange de clé cryptographique[10]. Quatre candidats supplémentaires ont été proposés pour l'échange de clé cryptographique. Le standard final est attendu vers 2024 et on estime qu'il faudra 10 ans pour remplacer les protocoles actuels.

[10] https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4

Implémentation *hardware*

Un ordinateur quantique doit satisfaire aux critères de DiVincenzo : initialiser, faire évoluer, puis mesurer des qubits, disposer d'un temps de décohérence suffisamment long pour lui permettre de faire les calculs, être composé de portes quantiques universelles permettant un passage à l'échelle. La difficulté de le construire tient au fait qu'il faut à la fois isoler les qubits de l'environnement pour garder la cohérence quantique et les coupler avec l'extérieur pour les mesurer et réaliser la correction d'erreurs. Ces corrections d'erreurs impliquent qu'un qubit logique (qui est pris en compte dans les algorithmes quantiques) ne puisse être réalisé que par un nombre important de qubits physiques, entre 5 et 10 000, en fonction de l'implémentation *hardware* choisie.

Pour construire des ordinateurs quantiques, il existe alors plusieurs technologies : ions piégés, qubits supraconducteurs, spin quantum dots, centres lacune azote, atomes froids, photonique, qubits topologiques. Chaque technologie présente des avantages et des inconvénients.

Ions piégés

Ils peuvent être piégés et confinés dans l'espace à l'aide de champs électromagnétiques variables (pièges de Paul[11]). Les qubits sont alors représentés par les états électroniques de chaque ion, les informations quantiques sont transférées *via* leur mouvement quantifié collectif dans ce piège partagé, où les ions interagissent également entre eux *via* la force électromagnétique. Pour réaliser ces transferts, on utilise des lasers.

L'avantage des ions piégés est leur grande stabilité, leur long temps de cohérence et la fiabilité des portes logiques. En revanche, il est difficile d'avoir un grand nombre de qubits dans un piège partagé, il faudrait donc réaliser plusieurs pièges et les coupler par d'autres moyens, par exemple *via* des réseaux photoniques connectés, ce qui complique l'architecture du système. Un autre inconvénient est la lenteur des opérations et la nécessité d'utiliser un grand nombre de lasers.

Plusieurs *start-up* utilisant cette technologie ont été récemment créées : Alpine Quantum Technologies (Autriche), EleQtron (Allemagne), IonQ (USA), Quantinuum (USA, UK), Quantum Factory (Allemagne), Oxford Ionics (UK).

Qubits supraconducteurs

Ils sont réalisés par des états quantiques de charge, phase ou flux magnétique de certains circuits formés à l'aide des jonctions Josephson, qui consistent en deux conducteurs séparés par une très fine couche isolatrice. Refroidis à basse température, les électrons se groupent deux par deux pour former des paires de Cooper et collapsent sur l'état de plus basse énergie pour former des condensats de Bose-Einstein. Ces paires de Cooper se trouvent sur les deux conducteurs mais peuvent également passer d'un conducteur à l'autre, à travers l'isolant, par effet tunnel. L'effet tunnel induit un comportement non-linéaire qui implique des espacements non uniformes entre les niveaux d'énergie quantifiés du circuit, ce qui permet d'implémenter les qubits. Les couplages entre qubits sont effectués par des guides micro-ondes en fonction de la géométrie du circuit.

La fabrication de qubits supraconducteurs suit les techniques de fabrication bien maîtrisées de la microélectronique : photolithographie, gravure, oxydation contrôlée, dépôt métallique. La manipulation et le contrôle de qubits sont réalisés par des impulsions micro-ondes, produites et mesurées par des appareils conventionnels (générateur de fréquence, analyseur de spectre), ce qui constitue un bon atout. En revanche, les circuits doivent être refroidis dans des cryostats en cascade pour atteindre des températures inférieures à 15 mK, ce qui implique une connectique complexe. Les qubits supraconducteurs sont également très sensibles au bruit de l'environnement et leur temps de décohérence est faible, ce qui peut limiter le nombre des pas des algorithmes qui peuvent être implémentés.

Cette technologie est utilisée par plusieurs grands groupes comme Google, IBM, Microsoft, mais aussi par des PMI et *start-up* comme Anyon Sytems (Canada), Atlantic Quantum (US), Bleximo (US), IQM (Finlande), Oxford Quantum Circuits (UK) et Rigetti Computing (US).

Spin quantum dots

Ce sont des îlots semi-conducteurs de taille nanométrique, capable de piéger des électrons. Des tensions électriques bien choisies sont utilisées pour peupler ou dépeupler ces îlots avec des électrons. En présence d'un champ magnétique, selon l'orientation du spin de l'électron, haut ou bas, il se forme deux niveaux d'énergie, ce qui permet l'implémentation des qubits. Les opérations sont induites par des champs magnétiques de radiofréquence oscillants, véhiculés par des lignes de transmission microruban.

De même que pour les qubits supraconducteurs, la technologie spin quantum dots tire avantage de techniques de fabrication de la microélectronique. La taille de ses composants est bien inférieure à celle de la technologie de qubits supraconducteurs, ce qui lui confère un excellent potentiel pour la miniaturisation. Pour leur fonctionnement, les composants spin quantum dots ne nécessitent que des températures de l'ordre d'un kelvin, plus facile à réaliser et maintenir. Les qubits sont également plus stables. En revanche, intriquer plusieurs qubits reste une tâche extrêmement difficile, ce qui limite les progrès de cette technologie. Récemment, Intel a annoncé la fabrication d'une puce avec 12 qubits. Il faudra probablement se contenter de fabriques de modules avec un faible nombre de qubits et de les interconnecter par d'autres moyens, notamment photoniques.

L'acteur principal de cette technologie est Intel, mais il existe aussi quelques *start-up* : Equal1 Laboratories (Irlande), Photonic Inc (Canada), Quantum Motion (UK), Silicon Quantum Computing (Australie).

Centres lacune azote (centre NV)

C'est un cristal de diamant qui présente un défaut ponctuel : une paire d'atomes de carbone voisins sont remplacés par un atome d'azote et une lacune du réseau, c'est-à-dire l'absence d'atome. En appliquant un champ magnétique, certains niveaux d'énergie des électrons localisés au voisinage du centre NV, peuvent être utilisés comme qubit. Le spin de ces électrons peut être contrôlé avec des champs électriques et magnétiques statiques ou avec du rayonnement électromagnétique. Ces qubits peuvent fonctionner à température ambiante et présentent un temps de cohérence long et une très bonne stabilité, en revanche ils sont très difficiles à intriquer. C'est pourquoi cette technologie semble difficilement applicable dans la construction d'un ordinateur quantique, la sensibilité des centres NV par rapport au champ magnétique peut cependant conduire à des applications importantes en métrologie et dans le domaine des capteurs ultrasensibles.

[11] Une particule chargée ne peut pas être piégée dans les trois directions de l'espace par un champ électrique ou magnétique statiques. En revanche, en ajoutant des champs électriques qui oscillent rapidement dans le temps, on peut créer une force de confinement moyenne, capable de piéger la particule : c'est le piège de Paul.

Plusieurs *start-up* travaillent sur cette technologie, certaines visant plutôt les applications dans le domaine des capteurs : Diatope (Allemagne), Quantum Brilliance (Autriche), Quantum Diamond Tech (US), NVision (Allemagne).

Atomes froids

Il s'agit d'atomes de césium ou de rubidium, piégés dans le vide par des champs magnétiques et des faisceaux lasers qui confinent leur mouvement, ce qui revient à les refroidir à des températures extrêmes. Ces pièges ont une bonne versatilité, ce qui permet de configurer les atomes dans des réseaux géométriques spécifiques. D'autres lasers peuvent mettre ces atomes dans des états hautement excités, appelés états de Rydberg (l'électron de la dernière couche se trouvant loin du noyau), qui sont utilisés pour implémenter les qubits. Les portes quantiques sont réalisées par couplage entre les qubits *via* des sources micro-ondes ou laser.

Cette technologie permet d'obtenir des qubits avec des temps de cohérence assez longs, une connectivité robuste et des configurations flexibles, la réalisation de portes logiques plus complexes, un passage à l'échelle aisée en 2D, voire des géométries 3D. En revanche, elle nécessite de nombreux lasers et la vitesse des portes logiques reste à améliorer.

Plusieurs *start-up* utilisent la technologie d'atomes froids : Atom Computing (US), ColdQuanta (US), QuEra Computing (US), et Pasqal (France).

Photonique

Pour implémenter les qubits, on utilise soit les états de polarisation du photon, soit certains états dits « comprimés ». Les photons sont envoyés par des guides optiques à travers divers circuits optiques (lames séparatrices, déphaseurs optiques) qui constituent les portes logiques. Ils sont ensuite détectés par des photodétecteurs qui effectuent l'opération de mesure.

Cette technologie implique des composants optiques intégrés, dont la fabrication est bien maîtrisée et qui fonctionnent à température ambiante. En revanche, construire un nombre important de portes quantiques qu'il faut interconnecter reste un grand défi, ce qui rend assez délicat le passage à l'échelle.

Plusieurs *start-up* ont été créées : ORCA Computing (UK), PsiQuantum (US), Quandela (France), QuiX Quantum (Pays-Bas), TundraSystems (UK), Xanadu Quantum Technologies (Canada).

Qubits topologiques

Utilise des quasi-particules spécifiques aux systèmes bidimensionnels, appelées anyons, dont les lignes d'évolution s'entourent et forment des chemins dans un espace-temps tridimensionnel (deux dimensions spatiales et une dimension temporelle). Ces chemins constituent les portes logiques.

Dans les autres technologies énumérées auparavant, de petites perturbations se cumulent et peuvent conduire à une décohérence des états quantiques et, en conséquence, introduire des erreurs dans le calcul. Cependant, les qubits topologiques sont robustes par rapport à ces perturbations. L'implémentation des qubits topologiques a d'abord été proposée sur des bases purement théoriques, puis réalisée pratiquement sur des systèmes bidimensionnels à base de semi-conducteurs en arséniure de gallium, à très basse température, soumis à de forts champs magnétiques. C'est la technologie la plus futuriste, des travaux de recherche sont encore nécessaires pour décider de la validité d'une telle approche. Microsoft, Google et certains laboratoires académiques sont les principaux acteurs de cette technologie.

Chaque technologie présente donc ses avantages et ses inconvénients. Des travaux sont en cours pour les développer davantage et pour savoir laquelle semble plus adaptée à l'algorithme spécifique qu'on souhaite réaliser. Actuellement, les technologies les plus avancées sont les boucles supraconductrices et les ions piégés, mais d'importants progrès ont récemment été obtenus dans la technologie des atomes froids.

Ordinateur quantique analogique

Aujourd'hui, les ordinateurs quantiques à portes logiques ont un taux important d'erreurs, des temps de cohérence faible et ils nécessitent des codes correcteurs d'erreurs. C'est pourquoi certains acteurs du domaine, comme la société D-Wave, se sont orientés vers la mise au point d'ordinateurs quantiques analogiques (recuit quantique), dont les qubits sont plus résistants au bruit, permettent un passage à l'échelle plus facile, mais sont moins flexibles et ne permettent l'implémentation que d'une catégorie restreinte d'algorithmes. D'autres acteurs construisent des simulateurs quantiques, systèmes analogiques qui permettent de simuler des systèmes physiques (transition de phase, magnétisme, phénomènes de transport, modélisation des molécules) dont la simulation dépasse largement les capacités des ordinateurs classiques. Il existe également des travaux de *machine learning* quantique, promus particulièrement par des entreprises comme Athos.

Même si la réalisation d'un ordinateur quantique semble un objectif à long terme, ces travaux vont conduire à des améliorations substantielles de la technologie de capteurs de champ magnétiques avec des applications dans la microscopie et l'imagerie médicale, dans la mise au point de gravimètres capables de mesurer de faibles variations du champ gravitationnel, avec des applications dans la prospection géologique ou dans la prédiction d'éruptions volcaniques. Ces capteurs pourront avoir également des applications militaires, notamment la mise au point de centrales inertielles extrêmement précises qui permettront une navigation sans GPS (dont le signal reste très vulnérable aux brouillages), et peut-être la construction de systèmes de radar quantique (plus résistants aux brouillages).

Le calcul quantique pourrait avoir une large palette d'applications dans la prospection géologique, la mise au point de nouveaux matériaux, molécules, l'optimisation des processus de production ou dans la logistique et la finance.

Encadré 4 : Quelques projets faisant intervenir des algorithmes quantiques

Dans le domaine de l'automobile, Volkswagen et Google Automobile ont travaillé sur l'optimisation des grandes flottes de véhicules autonomes. Dans le domaine de l'énergie, Dubai Electricity a mis au point des algorithmes capables de prédire la consommation d'énergie électrique et le département de l'énergie américain a développé des algorithmes pour l'optimisation du réseau électrique.

Pour des clients comme Apple, Amazon, Google and Facebook, IBM a réalisé des algorithmes en mesure de faire des prédictions météorologiques.

En finance, Caixa Bank a travaillé sur le trading automatisé, la prévision des marchés financiers et l'analyse de risque, KPMG sur l'optimisation du portefeuille à court terme, PayPal et IBM sur la détection des fraudes, Anthem et IBM sur les primes d'assurance santé.

Dans le domaine de la logistique, D-Wave a réalisé des algorithmes pour l'optimisation des itinéraires et du trafic, Coca-Cola pour l'optimisation de la chaîne d'approvisionnement et des stocks.

En fabrication, Daimler et IBM ont travaillé dans l'optimisation de la conception des batteries et des puces pour les véhicules.

En matière de santé, la société 1QBit a réalisé des algorithmes afin de prédire les interactions médicamenteuses (1QBit), Roche, Crownbio et Cambridge Quantum ont travaillé sur des sujets de médecine personnalisée et génomique.

En technologie logiciel, IBM travaille sur l'accélération de l'apprentissage automatique *via* le calcul quantique.

Plateformes de calcul quantique

Comme on vient de le voir, le domaine quantique attire un nombre important d'acteurs industriels, aussi bien de grandes entreprises que des *start-up*. Il existe également des plateformes qui permettent la réalisation d'algorithmes quantiques comme Microsoft Azure, IBM Q Experience, Amazon Braket et Google Quantum Playground.

Toute personne peut y avoir accès et développer ses propres algorithmes quantiques qui peuvent être implémentés sur diverses plateformes *hardware*.

Conclusion

Le montant de l'investissement mondial de R&D dans les technologies quantiques montre l'intérêt pour ce domaine dont le potentiel est considérable. Il est très médiatisé alors que le passage à l'échelle de ces technologies est loin d'être facile. Les aspects *software* sont bien plus avancés que l'implémentation *hardware*. L'ordinateur quantique analogique se trouve plus avancé que l'ordinateur à portes quantiques. Les simulateurs quantiques restent très utiles pour simuler des systèmes physiques complexes qui sont pratiquement impossibles à simuler avec des supercalculateurs classiques.

Enfin, on attend des retombées importantes dans le domaine des capteurs magnétiques et gravitationnels, avec de multiples applications scientifiques, industrielles et militaires. Il est très probable que les protocoles de cryptographie *post* quantique seront mis en place bien avant la réalisation d'un ordinateur quantique en mesure d'attaquer les protocoles actuels.

Cependant, il n'y a pas encore de preuve mathématique qu'un algorithme *post* quantique ne peut pas être attaqué par un ordinateur quantique.