

N°05

Le 3,14

 Polytechnique insights

« Rendre le quantique accessible à tous »

Alain Aspect
prix Nobel de Physique 2022

LE QUANTIQUE

Une deuxième révolution en ébullition

Les secteurs bouleversés par le quantique

Pourquoi courons-nous après le quantique ?

BONUS

La téléportation pour un internet quantique ?



Clément Boulle

Directeur exécutif
de Polytechnique Insights

On ne va pas se mentir. Quand nous avons évoqué en réunion de rédaction ce projet de magazine sur le quantique, j'ai rapidement admis que je n'y comprenais pas grand-chose. Pour moi un cantique n'était alors qu'un chant d'action de grâces destiné à remercier Dieu. En travaillant sur le sujet, j'ai découvert que le quantique était aussi un champ d'action et de recherche destiné à comprendre les lois de l'univers, mais aussi à développer des technologies qui révolutionnent des secteurs aussi variés que la santé, le spatial ou encore l'électronique.

Je ne connais pas de théorie aussi difficile à comprendre qui ait débouché sur des applications aussi essentielles. Détruire de petites cellules cancéreuses, découper une cornée, réaliser une IRM, remplacer de vieilles ampoules par des LED moins énergivores, communiquer grâce à la fibre optique : toutes ces actions sont permises grâce à la recherche en physique quantique et aux développements qui y sont associés.

Aujourd'hui, nous sommes à l'aube de ce que le prix Nobel de physique 2022, Alain Aspect, nomme la « *deuxième révolution quantique* » et qui pourrait à nouveau déboucher sur des technologies de rupture comme l'ordinateur quantique. L'interview qu'il nous a accordé vous permettra, je l'espère, de mieux comprendre cette révolution explorée dans ce nouveau 3,14, qui est, dans le fond, un cantique des quantiques.

clement.boulle@polytechnique-insights.com



Polytechnique insights

LA REVUE DE L'INSTITUT POLYTECHNIQUE DE PARIS

[La newsletter](#) | [Articles](#) | [Vidéos](#) | [Les 3,14](#) |



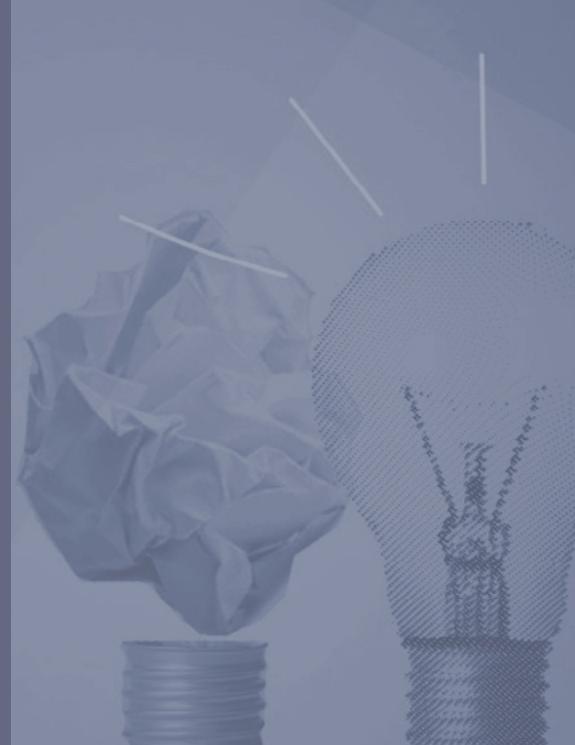
Comprendre les
grands enjeux, à
travers la science

Les bases

La physique quantique a déjà changé la face du monde **5**
Pierre Henriet, docteur en physique nucléaire et chroniqueur chez Polytechnique Insights

La physique quantique accessible à tous **8**
Alain Aspect, directeur de recherche CNRS émérite à l'Institut d'Optique Graduate School (Université Paris-Saclay - CNRS), professeur à l'École polytechnique (IP Paris) et co-lauréat du prix Nobel de Physique 2022

5 percées récentes faites grâce au quantique **11**
Isabelle Dumé, journaliste scientifique pour Polytechnique Insights



Les secteurs

Le quantique, allié indispensable de la médecine moderne **16**
Pierre Henriet, docteur en physique nucléaire et chroniqueur chez Polytechnique Insights

Santé, tech, espace : le quantique bénéficie déjà à l'industrie **20**
Pierre Henriet, docteur en physique nucléaire et chroniqueur chez Polytechnique Insights



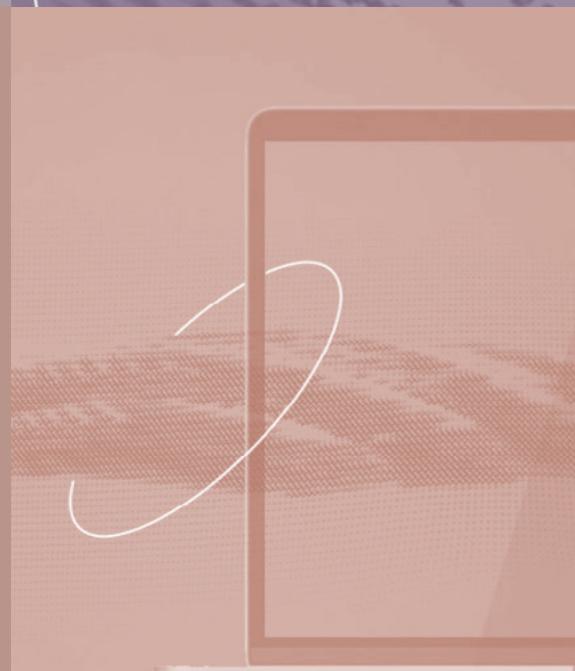
Les ordinateurs

Ordinateurs quantiques : comment ça marche ? **25**
Landry Bretheau, professeur et chercheur en physique quantique à l'École polytechnique (IP Paris)

Pourquoi États et entreprises courrent-ils après le quantique ? **29**
Landry Bretheau, professeur et chercheur en physique quantique à l'École polytechnique (IP Paris)

BONUS

Une téléportation multinœuds robuste et « incassable » pour un internet quantique ? **33**
Sophie Hermans, chercheuse en postdoctorat à l'IQIM (Caltech)



PREMIÈRE PARTIE

Les bases

Qu'est-ce la physique quantique ? Pourquoi parle-t-on d'une deuxième révolution ? Voici des bases pour mieux comprendre la science de l'infiniment petit.



La physique quantique a déjà changé la face du monde

20 septembre 2023  5 min. de lecture

par Pierre Henriquet



Pierre Henriquet

Docteur en physique nucléaire et chroniqueur chez Polytechnique Insights

La physique quantique permet d'expliquer le comportement et les interactions entre particules, ainsi que les champs de forces qui les animent. Née il y a plus d'un siècle, c'est probablement aussi la théorie la moins intuitive de toutes celles à disposition des scientifiques pour décrire et comprendre le monde.

Dans l'univers de l'infiniment petit, les concepts les plus évidents de notre expérience du quotidien sont battus en brèche. Une particule possède, par exemple, des propriétés à la fois corpusculaires et ondulatoires.

Son emplacement n'est pas déterminé par une position précise, mais par un « nuage de probabilités » qui la fait exister un peu partout à la fois, avec des chances plus ou moins grandes de la trouver si on cherche finalement à l'observer. De plus, le concept même de mesure prend un sens totalement différent.

Dans le monde quantique, on ne peut pas mesurer une propriété d'une particule avec une précision infinie. Pire encore, selon le principe des vases communicants, plus on aura de précisions sur certaines propriétés (sa position, par exemple), moins on en aura sur d'autres (son énergie, par exemple).

Et ces limitations ne viennent pas de nos instruments de mesure : au contraire, elles sont fondamentalement inscrites dans les règles qui régissent le monde de l'infiniment petit. Enfin, et c'est ce qui lui donne son nom, la mécanique quantique décrit aussi les échanges d'énergie que les particules ont entre elles. Et contrairement à notre monde macroscopique classique, où l'énergie d'une balle de tennis ou d'une voiture peut prendre n'importe quelle valeur, un électron dans un atome ne peut émettre ou absorber que des quantités d'énergie précisément déterminées. ▶

« Un électron ne peut émettre que des quantités d'énergies précisément déterminées. »

Chaque « paquet » d'énergie que l'électron absorbe ou émet est appelé « quantum » d'énergie (d'où le nom de physique « quantique »). Ces échanges se font par bonds successifs, et non de manière continue comme nous en avons l'habitude à notre échelle.

Toutes ces étranges règles aboutissent à des situations qui peuvent sembler paradoxales, comme le fait qu'un objet quantique peut exister dans plusieurs états simultanément, ou que deux particules dites « intriquées » sont si fondamentalement liées que si l'on effectue un changement sur l'une, l'autre en subira instantanément les conséquences, indépendamment de la distance qui les sépare.

La physique quantique au quotidien

Ces situations bizarres sont observées quotidiennement dans tous les laboratoires de recherche du monde. Et, bien au-delà des portes des instituts de recherche, ces phénomènes sont utilisés pour faire fonctionner quantité d'appareils que l'on utilise chaque jour. Une découverte bien étonnante de la physique quantique est la fameuse « dualité onde-particule ». Au XIX^e siècle, quantité d'expériences avaient montré le caractère ondulatoire de la lumière, mais c'est en 1905 qu'Albert Einstein démontre un effet appelé « photoélectrique » qui prouve que la lumière peut frapper des électrons et les éjecter comme des boules de pétanque.

Il faudra attendre 20 ans pour que le physicien français Louis de Broglie comprenne que, loin d'être un problème, la lumière (et toute particule matérielle) se comporte à la fois comme une onde et comme une particule. Cette découverte est à l'origine de plusieurs applications quotidiennes comme les panneaux photovoltaïques ou les capteurs CCD de nos appareils photo.

De même, la quantification des échanges d'énergie entre les électrons de la matière a apporté plusieurs innovations fondamentales sans lesquelles notre technologie moderne n'existerait pas.

Commençons par le laser que l'on utilise dans les lecteurs CD, en industrie pour la découpe de matériaux, en astronomie pour mesurer la distance Terre-Lune, en médecine pour découper ou cautériser les tissus, dans les supermarchés pour lire les codes-barres, dans les imprimantes laser ou dans les fibres optiques pour communiquer d'un continent à l'autre.

Cette lumière très spéciale, composée de photons (c'est le nom qu'on a donné aux particules de lumière) tous identiques, est produite en forçant les atomes à émettre tous ensemble les mêmes quanta d'énergie. On obtient alors cette lumière particulière dont il serait difficile de se passer aujourd'hui.

Une autre application de la théorie des quanta n'est ni plus ni moins que... toute l'électronique moderne ! ▶



« La physique quantique a révolutionné la manière dont les humains façonnent le monde. »

Cette technologie présente dans nos téléphones portables, nos montres, nos véhicules, nos ordinateurs, nos dispositifs médicaux (pacemaker, pèse-personne, tensiomètre, défibrillateur cardiaque) et une infinité d'autres applications courantes, fonctionne grâce à la compréhension du comportement des électrons dans une catégorie de matériaux appelés « semi-conducteurs » – c'est-à-dire naturellement isolants, mais qui peuvent facilement devenir conducteurs si une petite tension électrique leur est appliquée. Cette propriété, qui permet de contrôler à volonté le passage (ou non) d'un courant électrique, sert à construire les diodes et les transistors qui sont les éléments de base de toute l'électronique.

Et lorsque vous mélangez émission contrôlée de lumière et semi-conducteurs, vous construisez des LED (diodes électroluminescentes), dans le but de remplacer une grosse partie des anciennes ampoules électriques, beaucoup plus énergivores.

Physique quantique et phénomènes naturels

La mécanique quantique est partout autour de nous : dans les différentes applications technologiques que nous avons développées, mais aussi dans tous les phénomènes naturels qui nous entourent et qu'on ne peut comprendre sans utiliser le formalisme quantique.

Si le Soleil brille, c'est à cause des processus de fusion nucléaire en son cœur, eux-mêmes permis grâce à une autre bizarrerie quantique : l'effet tunnel, qui permet à des particules de « sauter » des barrières de potentiel autrement infranchissables dans le monde classique. Quant au bleu du ciel, il est dû à la manière dont la lumière du Soleil interagit avec les molécules de l'atmosphère terrestre.

Même la photosynthèse (ce processus par lequel les plantes transforment l'énergie reçue du Soleil en matière organique, elle-même absorbée par les herbivores, consommés à leur tour par les carnivores) est soupçonnée, dans les recherches les plus récentes, de devoir son existence à des phénomènes quantiques dont la biologie doit encore lever le mystère.

La physique quantique a révolutionné la manière dont les humains comprennent et façonnent le monde. Mais depuis la fin du XXe siècle, une « deuxième révolution quantique » est en cours, dans laquelle les processus les plus fondamentaux de la mécanique quantique sont exploités pour faire évoluer nos technologies à un niveau encore jamais atteint. ■

Pierre Henrquet

La physique quantique accessible à tous

13 octobre 2023  5 min. de lecture

avec Alain Aspect

La physique quantique est l'ensemble des lois physiques qui régissent le comportement du monde au niveau des électrons, des atomes, des molécules et des cristaux. Les lois de la mécanique newtonienne que nous connaissons à notre échelle ne sont plus valables à l'échelle du nanomètre (un milliardième de mètre), qui correspond à la taille d'un atome. La physique quantique a commencé à se développer dans le premier quart du 20e siècle avec Planck et Einstein, et à partir de 1925 les grands physiciens Heisenberg, Schrödinger et Dirac ont mis au point un formalisme mathématique qui est utilisé depuis lors.

Cette discipline est indispensable, par exemple, pour expliquer pourquoi la matière est stable. Depuis la fin du 19e siècle, on sait que la matière est constituée de charges positives et négatives et que ces charges positives et négatives s'attirent. La matière devrait donc s'effondrer sur elle-même. Il n'en est rien grâce au comportement quantique de l'électron, qui n'est pas seulement une particule, mais aussi une onde. Lorsque vous essayez de confiner un électron, vous êtes obligé de considérer une longueur d'onde de plus en plus petite et donc une énergie de plus en plus grande. Cette énergie n'étant pas disponible, l'électron ne peut être confiné dans une dimension inférieure à la taille de l'atome. La physique quantique permet également de comprendre la liaison chimique entre atomes.

Son formalisme permet aussi de décrire le courant électrique dans les matériaux au niveau microscopique, ce qui a permis aux physiciens d'inventer et fabriquer des transistors et des circuits intégrés, à la base des ordinateurs. Il permet aussi de comprendre comment les photons (particules de lumière) sont absorbés ou émis par la matière, ce qui a été essentiel pour inventer le laser.

Quid des ordinateurs quantiques ?

Le concept d'ordinateur quantique est apparu au cours des deux dernières décennies environ et a été déclenché par plusieurs percées expérimentales réalisées à partir des années 1970 : la première est que nous avons appris à observer et à contrôler des objets microscopiques individuels. Auparavant, nous ne pouvions manipuler que de grands ensembles de particules. Aujourd'hui, nous pouvons piéger un électron, un atome et l'observer et le contrôler. Nous pouvons aussi émettre un photon unique et l'utiliser.

La deuxième série d'avancées est liée à l'intrication quantique, décrite pour la première fois dans l'article d'Einstein, Podolsky et Rosen de 1935 et qui n'est concevable que dans le cadre de la physique quantique. ▶



Alain Aspect

Directeur de recherche CNRS émérite
à l'Institut d'Optique Graduate School (Université Paris-Saclay - CNRS) et professeur à l'École polytechnique (IP Paris) et à l'Institut d'Optique, co-lauréat du prix Nobel de Physique 2022

« L'ordinateur quantique idéal existera, mais je serai étonné que cela arrive dans un avenir proche. »

L'intrication se produit lorsque deux particules ayant interagi dans le passé puis séparées dans l'espace, forment un tout quantique inséparable qui contient plus d'informations que celle contenue dans la somme des informations de chaque particule. C'est cette propriété qui ouvre la porte à l'informatique quantique : en effet, si au lieu d'avoir seulement deux bits quantiques intriqués dans lesquels encoder l'information quantique, vous en avez trois, quatre, cinq, dix ou cent, la quantité supplémentaire d'information, par rapport à une mémoire classique, contenue dans ces particules est gigantesque, car elle croît de manière exponentielle.

La décohérence est un obstacle majeur

Aujourd'hui cependant, nous sommes encore loin d'un ordinateur quantique parfait, car les bits quantiques (qubits) dont nous disposons ne sont pas stables et subissent ce que l'on appelle la « décohérence » lorsqu'ils interagissent avec leur environnement. Cela signifie qu'au bout d'un certain temps ils se comportent comme des objets classiques et perdent l'information quantique qu'ils contiennent. La décohérence est un obstacle à la réalisation d'un ordinateur quantique, qui va demander un gros effort technologique. Mais rien n'interdit que l'on puisse surmonter la difficulté plus vite que prévu. Par exemple, nous pourrions trouver un sous-espace des états quantiques protégé de la décohérence. Si tel était le cas, nous pourrions voir un ordinateur quantique de mon vivant.

Je suis convaincu que tôt ou tard, un ordinateur quantique idéal fonctionnant parfaitement existera, car d'après mon expérience, lorsque quelque chose qui semble faisable n'est pas interdit par les lois fondamentales de la physique, les ingénieurs parviennent à trouver un moyen de le réaliser. Cependant, il faut être réaliste, je serais étonné que cela arrive dans un avenir proche.

Un futur réseau quantique et la téléportation

Un internet quantique, ou si l'on veut être plus précis, un réseau quantique, utiliserait deux ou plusieurs ordinateurs quantiques communiquant entre eux en envoyant des informations quantiques directement à partir de l'état quantique, sans passer par un état classique intermédiaire. Cela permettra de transmettre une très grande quantité d'informations. On peut le mettre en œuvre par un processus connu sous le nom de téléportation quantique, qui a déjà été démontré pour des particules individuelles et de petits ensembles de particules, mais sur des distances n'excédant pas quelques dizaines de kilomètres. ▶

Si le problème de la décohérence n'est pas résolu à court terme, une catégorie d'ordinateurs quantiques « dégradés » apparaîtra probablement en premier. Ces machines de taille intermédiaire seront beaucoup plus efficaces qu'un ordinateur classique pour certaines tâches, comme les problèmes d'optimisation (le fameux problème du voyageur de commerce, par exemple, ou l'optimisation des réseaux électriques).

La deuxième révolution quantique

On parle souvent aujourd'hui de « quantum 2.0 », mais je préfère parler de « la deuxième révolution quantique », car c'est une révolution radicale. La première révolution quantique était d'abord conceptuelle et scientifique, la mise en œuvre d'un nouveau formalisme mathématique pour décrire la dualité onde-particule. Elle a conduit à une bien meilleure compréhension du monde physique, et à des applications qui ont bouleversé la société. La seconde révolution est basée sur deux concepts nouveaux : notre capacité à isoler et à contrôler des objets quantiques individuels ; et la possibilité d'intriquer ces objets et d'exploiter cette intrication dans des applications réelles.

Ces technologies quantiques nouvelles bouleverront-elles notre société comme l'ont fait le transistor et le laser ? Il est trop tôt pour le dire, mais je pense qu'il est important que les entreprises investissent dans ces technologies, car si elles apportent réellement les avancées révolutionnaires que nous attendons, ceux qui n'auront pas investi seront hors-jeu. Il sera important de disposer en interne d'experts en physique quantique capables d'exploiter rapidement ces avancées. Aujourd'hui, nous manquons de personnes ayant des compétences en physique quantique, et je pense que les entrepreneurs doivent s'associer aux universités pour mieux faire face à ce problème.

À Paris-Saclay, par exemple, nous avons un programme appelé ARTeQ, auquel l'École polytechnique s'est associée. Un certain nombre d'industriels le soutiennent financièrement. ARTeQ permet à des étudiants en sciences, mais pas forcément en sciences quantiques, d'acquérir une bonne base en culture quantique afin de pouvoir appliquer les connaissances acquises dans leur futur métier.

Nous avons besoin de chercheurs, d'ingénieurs et de techniciens quantiques. Mon message est donc : investissez dans la recherche, la technologie et la formation. ■

Propos recueillis par Isabelle Dumé



5 percées récentes faites grâce au quantique

09 octobre 2023  11 min. de lecture

par Isabelle Dumé



Isabelle Dumé
Journaliste scientifique pour
Polytechnique Insights

1 Vers des ordinateurs quantiques à grande échelle grâce à des améliorations dans la correction quantique des erreurs¹

Les ordinateurs quantiques utilisent des bits quantiques (qubits). Ces bits sont différents des bits informatiques standards, qui peuvent être soit 0 soit 1, car ils peuvent être à la fois 0 et 1. Ces machines pourraient être beaucoup plus rapides que les ordinateurs les plus rapides qui existent aujourd'hui, car elles seraient capables de calculer avec de nombreux qubits, ce qui entraînerait une augmentation exponentielle de la puissance de calcul. Les qubits peuvent être fabriqués à partir de différentes plateformes matérielles, telles que les supraconducteurs ou les ions piégés. Parmi les autres méthodes à venir figurent les processeurs photoniques qui utilisent la lumière.

Un véritable ordinateur quantique nécessitera l'intégration de nombreux qubits dans un seul dispositif, ce qui ne sera pas tâche facile, car ils sont très délicats et l'information quantique qu'ils contiennent peut facilement être détruite, ce qui entraîne des erreurs dans les calculs quantiques.

Pour corriger ces erreurs, un système de correction des erreurs quantiques (QEC) sera indispensable. Il s'agit généralement d'encoder un bit d'information quantique sur un ensemble de qubits qui agissent ensemble comme un seul « qubit logique ». L'une de ces techniques est le code de surface, dans lequel un bit d'information quantique est codé sur un réseau de qubits. Cette approche pose toutefois un problème, car l'ajout de qubits supplémentaires au système ajoute à son tour des sources d'erreur supplémentaires.

Une vraie informatique quantique à grande échelle requerra un taux d'erreur d'environ un sur un million selon les physiciens, mais les meilleures technologies de correction d'erreur actuelles ne peuvent atteindre que des taux d'environ un sur mille. Il reste donc un long chemin à parcourir. ▶

Des chercheurs de Google Quantum AI ont récemment créé un schéma de code de surface qui devrait s'adapter au taux d'erreurs requis dans un processeur quantique composé de qubits supraconducteurs constituants, soit des qubits de données pour l'exploitation, soit des qubits de mesure, adjacents aux qubits de données pouvant mesurer un retournement de bits ou un retournement de phases. Ce sont deux types d'erreurs qui affectent les qubits.

Les chercheurs ont constaté qu'un « réseau de qubits de distance-5 » comprenant un total de 49 qubits physiques avait un taux d'erreur de 2,914 %, contre 3,028 % pour un « réseau de distance-3 » comprenant 17 qubits. Cette réduction montre que l'augmentation du nombre de qubits est une voie viable vers l'informatique quantique tolérante aux pannes et qu'un taux d'erreur supérieur à un sur un million pourrait être possible dans un « réseau de qubits de distance-17 » comprenant 577 qubits.

2 Un convertisseur pour les dispositifs quantiques divers²

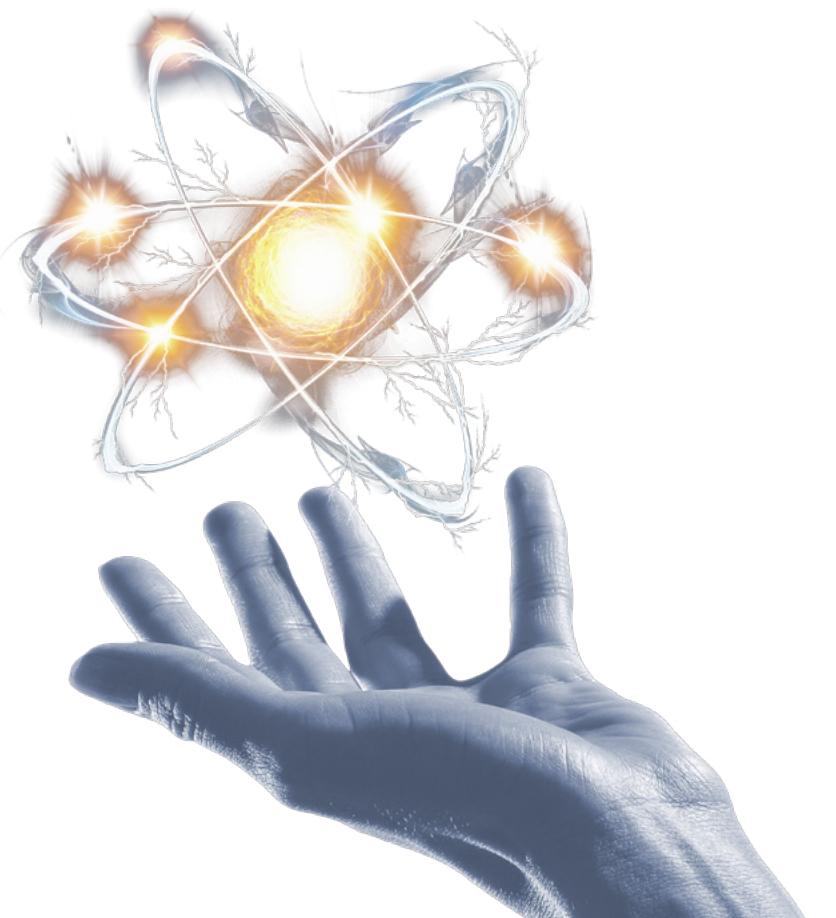
Les plateformes développées pour les ordinateurs quantiques sont actuellement basées sur différents systèmes quantiques tels que les photons, les atomes neutres, les ions, les supraconducteurs et les semi-conducteurs. Dans les futurs réseaux quantiques, ces systèmes devront communiquer entre eux, mais comme ils reposent sur plusieurs types de codage, cela pourrait s'avérer difficile.

Des chercheurs du Laboratoire Kastler Brossel (LKB), en France, viennent de créer un convertisseur qui permet à des dispositifs quantiques basés sur différentes plateformes de communiquer. « Nous avons conçu une sorte de boîte noire qui permet de passer d'un encodage d'information quantique à un autre grâce au phénomène d'intrication », explique le physicien Julian Laurat, l'un des membres de l'équipe du LKB. L'intrication, qui a fait l'objet du prix Nobel de physique 2022, est un phénomène purement quantique, par lequel deux ou plusieurs particules peuvent avoir une relation plus étroite que celle permise par la physique classique. Cela signifie que si nous déterminons l'état de l'une des particules, nous pouvons instantanément déterminer l'état quantique de l'autre, quelle que soit la distance qui les sépare. Autrefois considérée comme une bizarrerie du monde quantique, cette « action étrange à distance », comme l'appelait Albert Einstein, est aujourd'hui exploitée dans les systèmes de cryptographie et de communication quantiques, ainsi que dans les capteurs utilisés pour détecter les ondes gravitationnelles.

Grâce à l'intrication, les chercheurs du LKB ont pu préserver le signal d'information des codes quantiques, qui est fragile, tout en changeant la base sur laquelle il est écrit.

« Le succès de ce procédé est une étape importante pour les infrastructures de la technologie quantique, souligne Beate Asenbeck, doctorante au LKB. Une fois que nous pourrons interconnecter des dispositifs quantiques, des réseaux plus complexes et plus efficaces pourront être construits. »

Les chercheurs ont déposé un brevet pour protéger leur technologie qui est désormais exploitée par Welingq, une start-up fondée par Julien Laurat et son collègue Tom Darras. ▶



3 La correction quantique des erreurs pourrait améliorer l'imagerie astronomique³

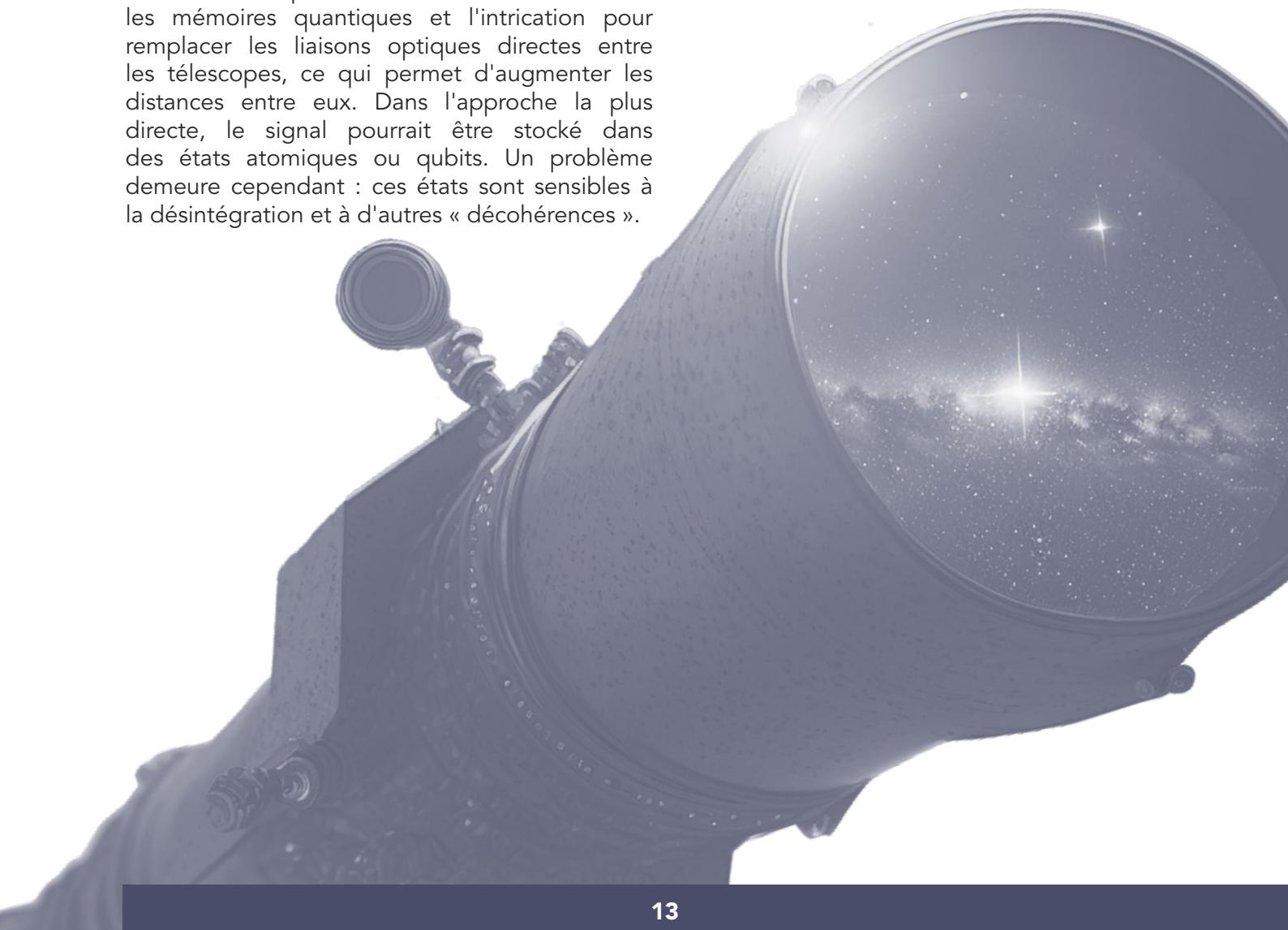
Les interféromètres optiques à haute résolution et à longue base révolutionneraient l'imagerie astronomique : la lumière provenant de deux ou plusieurs télescopes, placés à une certaine distance les uns des autres, est combinée pour créer une image d'un objet céleste, tel qu'une étoile. Les images ainsi obtenues sont beaucoup plus fines que celles obtenues avec chaque télescope individuel. De cette manière, les télescopes multiples agissent comme un gigantesque télescope « virtuel » dont le diamètre est beaucoup plus grand que celui de n'importe quel télescope réel.

En théorie, plus les télescopes sont éloignés les uns des autres, plus la résolution de l'image est élevée. Dans la pratique, cependant, le bruit et les pertes de transmission de la lumière dégradent la qualité des signaux lumineux, ce qui limite la distance possible entre les instruments.

Les technologies quantiques peuvent aider à contourner ces pertes de transmission en utilisant les mémoires quantiques et l'intrication pour remplacer les liaisons optiques directes entre les télescopes, ce qui permet d'augmenter les distances entre eux. Dans l'approche la plus directe, le signal pourrait être stocké dans des états atomiques ou qubits. Un problème demeure cependant : ces états sont sensibles à la désintégration et à d'autres « décohérences ».

Des chercheurs de l'Université Macquarie en Australie et de l'université nationale de Singapour (NUS) ont maintenant trouvé un moyen de contourner cet obstacle en montrant que les codes QEC peuvent être utilisés pour protéger l'information quantique contenue dans la lumière stellaire capturée.

Dans leur nouvelle technique, les chercheurs couplent l'état de la lumière de l'étoile provenant des deux télescopes de manière à ce qu'elle soit sous une forme partagée, protégée des bruits de l'environnement. En effectuant ensuite des mesures spécifiques, toute erreur dans les qubits peut être détectée et corrigée avant de récupérer l'information contenue dans la lumière de l'étoile. Cette information est ensuite utilisée pour construire l'image de l'étoile. ▶



4 Les fluctuations du vide quantique pour fabriquer un générateur de nombres aléatoires⁴

La cryptographie moderne repose sur la production de nombres aléatoires qui sont ensuite utilisés comme clés pour crypter les énormes quantités de données produites par les gouvernements et les grandes entreprises, par exemple. Bien que des algorithmes soient couramment utilisés pour générer des nombres apparemment aléatoires, un pirate informatique pourrait en principe découvrir les étapes pré-déterminées d'un algorithme et ainsi prédire son résultat.

Un meilleur système serait plutôt basé sur un processus véritablement aléatoire, comme la nature probabiliste des phénomènes qui se produisent au niveau quantique.

Le vide de l'espace n'est pas vraiment un vide, mais regorge de fluctuations quantiques aléatoires dues à des paires de particules et d'antiparticules qui sont spontanément créées puis annihilées lorsqu'elles entrent en collision les unes avec les autres.

Ces processus se produisent à des échelles de temps extrêmement courtes et ont déjà été utilisés pour produire des nombres aléatoires. Le problème est que ces systèmes sont soumis à des bruits parasites provenant de leurs propres composants, ce qui ralentit le processus.

Pour résoudre ce problème, des chercheurs de l'université de Gand, en Belgique, ont fabriqué une puce informatique (mesurant à peine 5 mm de long) et ont ensuite cartographié toutes les imperfections dans cette puce ainsi que les sources de bruit qui s'y trouvent.

Cela leur a permis d'identifier l'origine des interférences et de mesurer les fluctuations quantiques avec beaucoup plus de sensibilité. Le résultat : une puce capable de générer des nombres aléatoires 200 fois plus vite que les dispositifs commerciaux existants.

5 L'avantage quantique sans correction d'erreur⁵

Des chercheurs d'IBM ont montré qu'il était possible d'obtenir un avantage (ou « suprématie ») quantique sans avoir recours à la correction d'erreurs. Pour ce faire, ils ont utilisé un processeur quantique de 127 qubits pour calculer l'aimantation d'un matériau avec un modèle Ising 2D. Ce modèle représente les propriétés magnétiques d'un matériau 2D en utilisant un réseau de spins quantiques qui interagissent avec leurs voisins les plus proches. Bien qu'apparemment simple, ce modèle est connu pour être extrêmement difficile à résoudre.

Les chercheurs ont utilisé une technique appelée « calcul quantique d'échelle intermédiaire bruite » (NISQ computation en anglais), dans laquelle le calcul est effectué rapidement pour éviter l'accumulation d'erreurs. Ce type de calcul permettra d'élaborer des algorithmes quantiques plus généraux à court terme, avant que des ordinateurs quantiques véritablement tolérants aux pannes ne soient disponibles.

Le calcul a été effectué avec une puce quantique supraconductrice qui comprend 127 qubits, et qui exécute des circuits quantiques d'une profondeur de 60 couches avec un total d'environ 2 800 portes à deux qubits. Ces portes sont des analogues quantiques des portes logiques conventionnelles.

Le circuit quantique génère des états quantiques hautement intriqués que les chercheurs ont ensuite utilisés pour programmer le modèle Ising 2D en effectuant une séquence d'opérations sur les qubits et les paires de qubits. Bien que cette méthode permette d'éliminer une grande partie du bruit, des erreurs subsistaient.

Les chercheurs ont donc appliqué un processus d'atténuation des erreurs quantiques à l'aide d'un logiciel informatique conventionnel. La technique fonctionne grâce à la capacité du processeur de 127 qubits à encoder un grand nombre de configurations du modèle d'Ising. Les ordinateurs conventionnels ne disposeraient pas d'une mémoire suffisante pour réaliser un tel exploit. ■

[1] Suppressing quantum errors by scaling a surface code logical qubit. *Nature* 614, 676–681

[2] A quantum-bit encoding converter. *Nature Photonics* 17, 165–170

[3] Imaging Stars with Quantum Error Correction. *Phys. Rev. Lett.* 129, 210502

[4] 100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations. *PRX Quantum* 4, 010330

[5] Evidence for the utility of quantum computing before fault tolerance. *Nature* 618 500–505

Isabelle Dumé

DEUXIÈME PARTIE

Les secteurs

La physique quantique est déjà exploitée en dehors des laboratoires de recherche. Voici quelques industries qui bénéficient de ses avancées.



Le quantique, allié indispensable de la médecine moderne

03 octobre 2023  5 min. de lecture

par Pierre Henriquet



Pierre Henriquet
Docteur en physique nucléaire et
chroniqueur chez Polytechnique
Insights

La physique quantique, qui décrit le comportement d'atomes ou d'autres particules plus petites encore, est la structure de base qui permet de déduire le comportement physique de la matière, non seulement à l'échelle microscopique, mais aussi, en théorie, jusqu'à notre échelle. Après tout, ne sommes-nous pas un gros assemblage (extrêmement complexe, certes) d'atomes et de molécules qui obéissent toutes aux lois du monde de l'infiniment petit ?

Dans la réalité, il en va autrement. De la même manière qu'il n'est pas nécessaire de connaître les subtilités de la mécanique des fluides pour se verser un verre d'eau, il n'est pas nécessaire de comprendre finement l'interaction des 1028 atomes de notre corps pour commencer à se soigner. Car la physique quantique est très présente dans la médecine moderne : voyons comment l'infiniment petit nous aide à nous maintenir en bonne santé au quotidien.

Un scalpel fait de lumière

Cela peut sembler surprenant, mais l'un des outils les plus précis à disposition de la médecine moderne est... la lumière. Ou plus exactement un faisceau de lumière parfaitement calibré pour que tous les photons aient la même énergie et que toutes les ondes lumineuses soient parfaitement cohérentes entre elles : le laser (de l'anglais Light Amplification by Stimulated Emission of Radiation).

Ce contrôle extrêmement fin de l'émission de lumière vient du fait que, d'après la mécanique quantique, les atomes ont des niveaux d'énergie discrets (quantifiés) et qu'en faisant sauter les électrons d'une orbite précise à une autre, on n'émet plus que des photons parfaitement identiques.

Prédit par Albert Einstein en 1917 et mis au point en 1960, le laser a tout de suite trouvé des applications médicales en ophtalmologie (Campbell, 1961) ou en dermatologie (Goldman, 1963). ▶

« Dès sa mise au point, le laser a tout de suite trouvé des applications médicales. »

Aujourd’hui, on l’utilise aussi bien pour traiter les décollements de rétine que pour coaguler des plaies, détruire des petites tumeurs cancéreuses, découper/abréger une cornée de manière extrêmement précise ou, en chirurgie dentaire, pour traiter des pathologies liées aux gencives.

Mais outre ses applications en chirurgie, cette technologie permet aussi des traitements plus légers : effacement d’un tatouage, traitement antirides ou encore épilation laser.

Voir le corps grâce à la physique nucléaire

L’une des techniques d’imagerie les plus répandues est l’IRM (Imagerie par Résonance Magnétique nucléaire).

Cette imagerie consiste à observer le comportement de noyaux des atomes d’hydrogène plongés dans un champ magnétique intense. Pourquoi l’hydrogène ? Parce qu’il est le composant principal de l’eau (H_2O) qui occupe environ 60 % de la masse totale d’un être humain, et que rares sont les autres molécules biologiques qui ne contiennent pas du tout d’hydrogène.

Le principe de l’IRM est le suivant : le noyau d’hydrogène est composé d’un unique proton qui, pour cette application, peut être considéré comme un minuscule aimant. En situation « naturelle », un corps humain ne possède pas d’aimantation particulière, et chaque noyau d’hydrogène pointe dans une direction aléatoire.

La première étape est de plonger le patient dans un champ magnétique extrêmement intense (environ 30 000 fois l’aimantation naturelle de la Terre) pour « ranger » tous les protons dans le même sens, tous parallèles les uns aux autres. On modifie alors cet équilibre en émettant une onde radiofréquence (RF) et on écoute l’onde RF émise en retour par ces protons lorsqu’ils reviennent à leur état initial. ▶



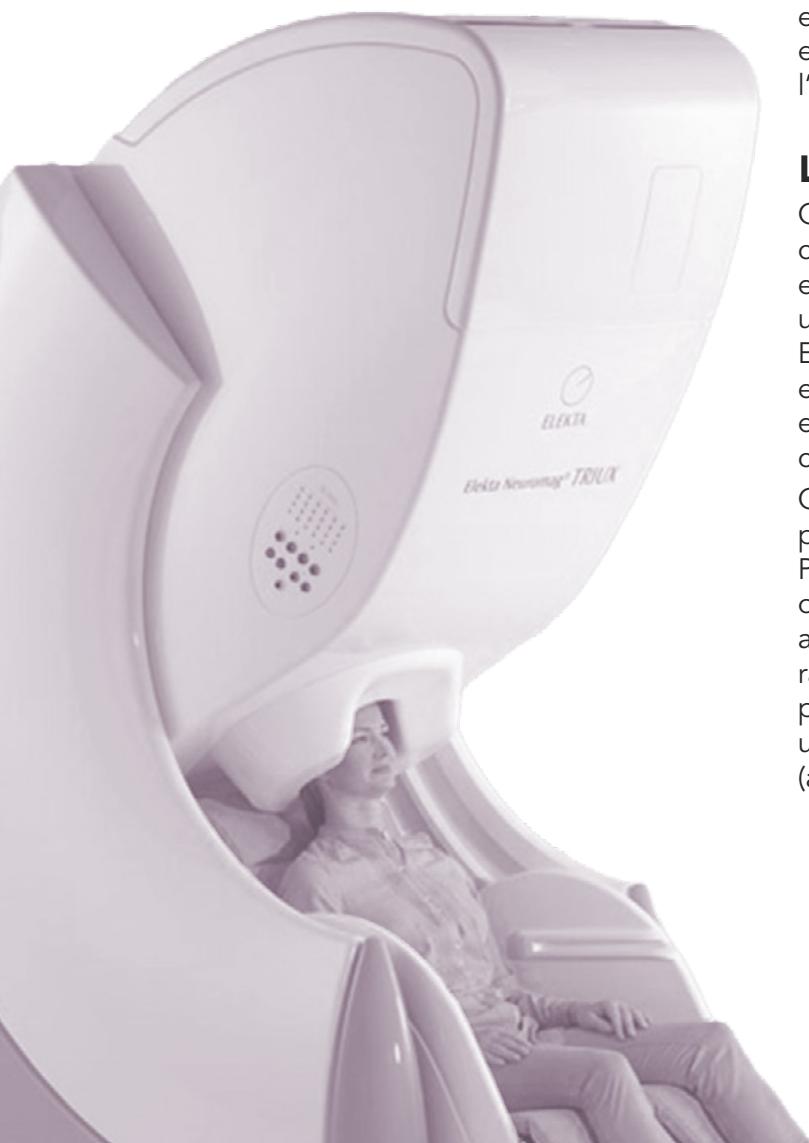
Selon la nature du milieu, ces protons ne retourneront pas à leur état initial à la même vitesse. On peut ainsi reconstruire une image 3D du corps en différenciant chaque tissu.

Sans la physique quantique et la compréhension fine du comportement des noyaux d'atomes dans un champ électromagnétique, cette technique d'imagerie de pointe non invasive ne pourrait pas être utilisée.

La matière dans tous ses états

Même les états les plus exotiques de la matière, sur lesquels des recherches fondamentales sont encore menées aujourd'hui dans tous les laboratoires de recherche du monde, sont essentiels en imagerie médicale.

On l'a dit plus haut, l'IRM nécessite, pour fonctionner, de plonger le patient dans un champ magnétique extrêmement intense. Plus ce champ est élevé, plus le signal émis lors du retour à l'équilibre de l'aimantation est fort, et meilleure sera la qualité de l'image.



Le problème : ces champs magnétiques sont si intenses que si l'on utilisait un simple électro-aimant classique pour les générer, la quantité de chaleur provoquée par l'intense courant électrique nécessaire les ferait fondre en quelques instants.

Pour pallier ce problème, on utilise des aimants dits « supraconducteurs », qui ont la propriété d'avoir une résistance électrique rigoureusement nulle. Avec de tels aimants, pas d'échauffement électrique. On peut potentiellement y faire parcourir des courants électriques aussi intenses qu'on le souhaite et aussi longtemps qu'on le veut (sans dissipation du courant, même lorsque l'alimentation est coupée).

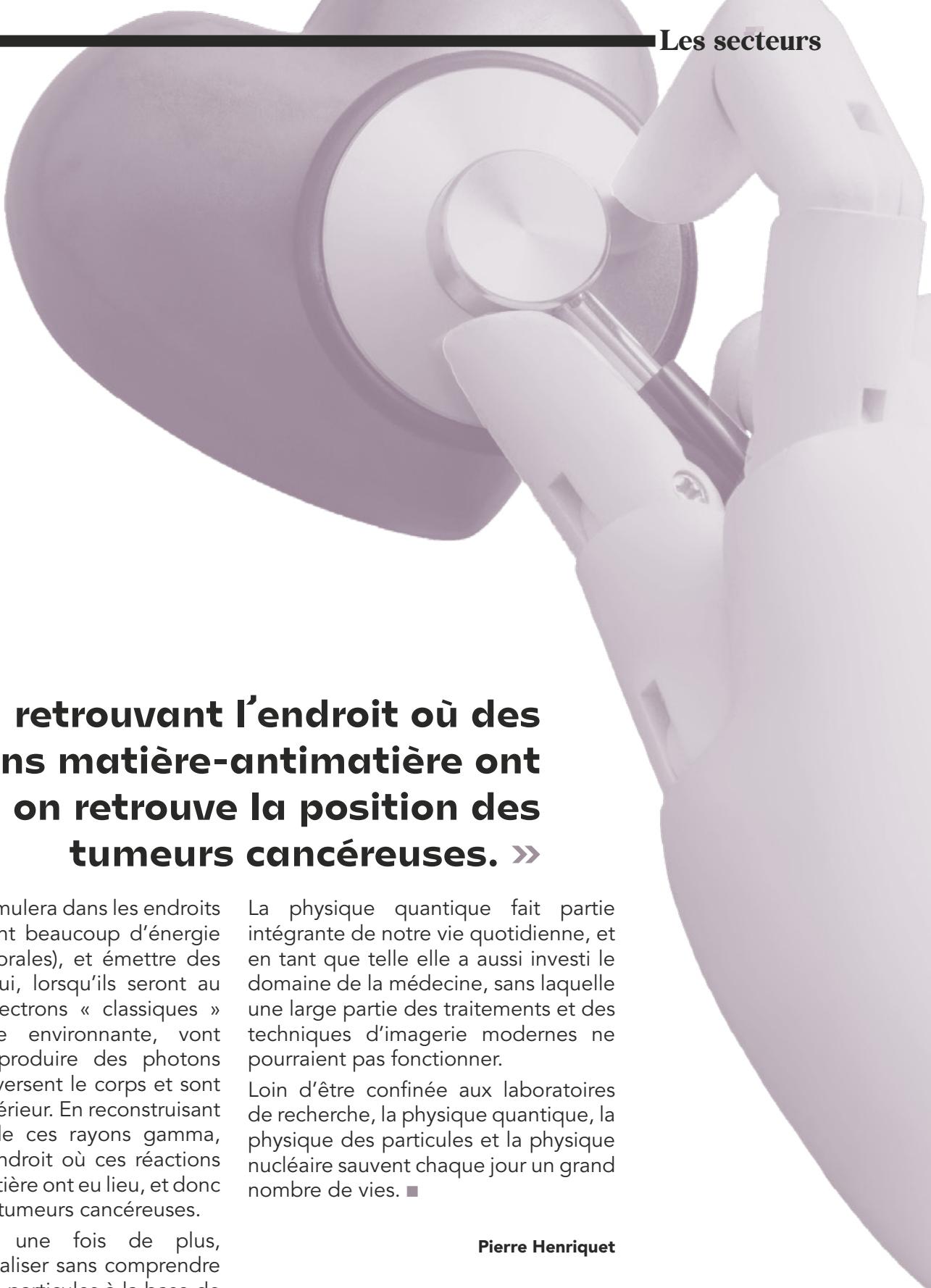
Cette supraconductivité est l'une des rares manifestations à notre échelle d'un comportement purement quantique de la matière. Les électrons s'y comportent comme un seul et même superfluide et s'écoulent sans aucune résistance.

On utilise aussi ces éléments supraconducteurs en magnétoencéphalographie pour enregistrer, en temps réel et de manière non invasive, l'activité électrique du cerveau.

L'antimatière à la rescousse

Comment savoir où se situent les zones cancéreuses dans le corps humain et comment elles évoluent avec le temps ? Pour cela, on utilise l'hyperactivité des cellules cancéreuses. En effet, une cellule cancéreuse se divise en permanence, de manière anarchique, et dépense donc beaucoup d'énergie. Son carburant : le sucre.

C'est pour cette raison que lors d'un examen par TEP (Tomographie par Émission de Positons), on fait avaler au sujet du sucre dont on a légèrement changé la composition. On a attaché à chaque molécule de sucre un atome radioactif (du Fluor 18 par exemple) qui a la propriété, lorsqu'il se désintègre, d'émettre une particule d'antimatière : un antiélectron (aussi appelé positon). ▶



« En retrouvant l'endroit où des réactions matière-antimatière ont eu lieu, on retrouve la position des tumeurs cancéreuses. »

Le sucre s'accumulera dans les endroits qui consomment beaucoup d'énergie (les zones tumorales), et émettre des antiélectrons qui, lorsqu'ils seront au contact des électrons « classiques » de la matière environnante, vont s'annihiler et produire des photons gamma qui traversent le corps et sont détectés à l'extérieur. En reconstruisant la trajectoire de ces rayons gamma, on retrouve l'endroit où ces réactions matière-antimatière ont eu lieu, et donc la position des tumeurs cancéreuses.

Ingénieux et, une fois de plus, impossible à réaliser sans comprendre la physique des particules à la base de cette technique d'imagerie médicale.

La physique quantique fait partie intégrante de notre vie quotidienne, et en tant que telle elle a aussi investi le domaine de la médecine, sans laquelle une large partie des traitements et des techniques d'imagerie modernes ne pourraient pas fonctionner.

Loin d'être confinée aux laboratoires de recherche, la physique quantique, la physique des particules et la physique nucléaire sauvent chaque jour un grand nombre de vies. ■

Pierre Henriquet

Santé, tech, espace : le quantique bénéficie déjà à l'industrie

26 septembre 2023  5 min. de lecture

par Pierre Henriet

La physique quantique est maintenant largement entrée dans notre vie quotidienne. La « première révolution quantique » a débouché sur quantité de dispositifs et de techniques que l'on utilise presque tous les jours. Lasers, électronique, éclairage à LED, panneaux photovoltaïques, médecine nucléaire, aucune de ces technologies du quotidien ne pourrait être utilisée sans une connaissance fine des processus qui se déroulent à l'échelle de l'atome, grâce à la compréhension du comportement des particules élémentaires et des interactions entre la matière et la lumière.

Mais la mécanique quantique n'a pas fini de changer notre monde. Les toutes dernières découvertes issues des laboratoires de recherche préfigurent une deuxième révolution quantique, dans laquelle la maîtrise des processus à l'œuvre dans l'infiniment petit risque à nouveau de changer profondément notre manière de vivre, de communiquer et de comprendre le monde. Partons pour un petit tour des prochaines applications de la physique quantique dans le monde industriel.

La spintronique : l'électronique du futur

Le contrôle toujours plus fin de flux d'électrons dans des dispositifs de plus en plus petits a permis à l'électronique d'atteindre un certain niveau de miniaturisation inégalé. En 2021, IBM annonçait la mise au point d'une puce faite de transistors de 2 nanomètres, dont la densité atteignait 333 millions de transistors par mm².

Malgré sa charge électrique, l'électron possède une autre propriété appelée le « spin ». Cette grandeur quantique est sans équivalent classique mais peut être comparée à un « moment magnétique », comme si l'électron était un minuscule aimant en rotation sur lui-même. Le principe de la spintronique est donc de manipuler le spin des électrons plutôt que leur charge électrique afin de créer de nouvelles applications, mais aussi de baisser énormément la consommation électrique des composants.

Aujourd'hui, la spintronique est déjà utilisée dans plusieurs composants électroniques comme les mémoires d'ordinateurs (qui a valu à ses découvreurs le prix Nobel de Physique en 2007) ou certains capteurs magnétiques pour l'automobile ou la robotique. ▶



La spintronique est déjà utilisée dans les mémoires d'ordinateurs. »

Mais, comme précisé plus haut, la miniaturisation des dispositifs électroniques est si évoluée que leurs éléments de base ne feront bientôt plus que la taille de quelques atomes seulement. Une taille qui rendra leur comportement presque exclusivement quantique. Pour lire et écrire sur des mémoires aussi petites, une équipe de l'Institut Rayonnement-Matière de Saclay (IRaMiS) a étudié le comportement d'une molécule (appelée FeTTP) qui joue normalement un rôle dans le transport de l'oxygène par l'hémoglobine¹.

Cette molécule déposée sur du graphène (une couche d'atome de carbone d'un atome d'épaisseur) peut changer de spin facilement et à volonté. Cela constitue un nouveau mécanisme de lecture/écriture d'un spin moléculaire unique, encore plus petit et économique en énergie que les dispositifs existants aujourd'hui.

Le Centre de Nanosciences et de Nanotechnologies de l'Université Paris-Saclay essaye, quant à lui, de donner plus de flexibilité aux systèmes d'intelligence artificielle². Dans les systèmes informatiques classiques, l'information de base est codée sous la forme de 0 ou de 1. De nouveaux systèmes spintroniques permettent d'introduire des nuances dans le code binaire comme des états 0+ ou 1-, et d'intégrer cette logique « floue » dans des réseaux de neurones artificiels, dont le fonctionnement se rapprocherait plus de celui des neurones biologiques organiques de notre cerveau.

Capteurs quantiques : mesurer l'immesurable

Un grand nombre de capteurs sont construits autour de différents phénomènes quantiques qui leur donnent la capacité de mesurer des signaux infimes avec une excellente résolution, ouvrant la voie à de nouveaux champs d'application.

Dans un microscope, la limite de résolution est donnée par les propriétés de la lumière utilisée. Globalement, il n'est pas possible de « voir » un objet plus petit qu'une longueur d'onde de cette lumière. Dans le domaine visible, cette longueur d'onde avoisine les 500 nanomètres. ▶

« Avec le quantique, on a une capacité de mesure 1 million de fois supérieure. »

Il existe en physique quantique un principe appelé « dualité onde-particule » selon lequel des objets quantiques (particules, atomes...) ont un comportement à la fois corpusculaire et ondulatoire. On peut donc leur associer une longueur d'onde, comme la lumière, et imaginer un « microscope à ondes de matière ». Son avantage : la longueur d'onde associée à des atomes est 1 million de fois plus courte que celle de la lumière. On dispose donc d'une capacité de mesure 1 million de fois meilleure que ce que la physique permet avec la lumière. De tels dispositifs existent. On les appelle par exemple « capteurs inertIELS par interférométrie atomique ». Les champs d'application sont très larges, allant des géosciences (détection de nappes de pétrole par mesure de variation du champ de gravité local) aux sciences du vivant (mesure du champ électrique ou magnétique émis par une seule cellule) en passant par la navigation inertielle (sur Terre ou dans l'espace). En 2022, un article de Nature proposait un tel capteur de gravité utilisant le comportement quantique d'atomes en chute libre pour mesurer plus précisément que jamais les microscopiques variations de gravité terrestre afin de sonder les structures du sous-sol terrestre³.

La mécanique quantique au service de la santé

L'industrie pharmaceutique a, elle aussi, passé le cap quantique depuis longtemps.

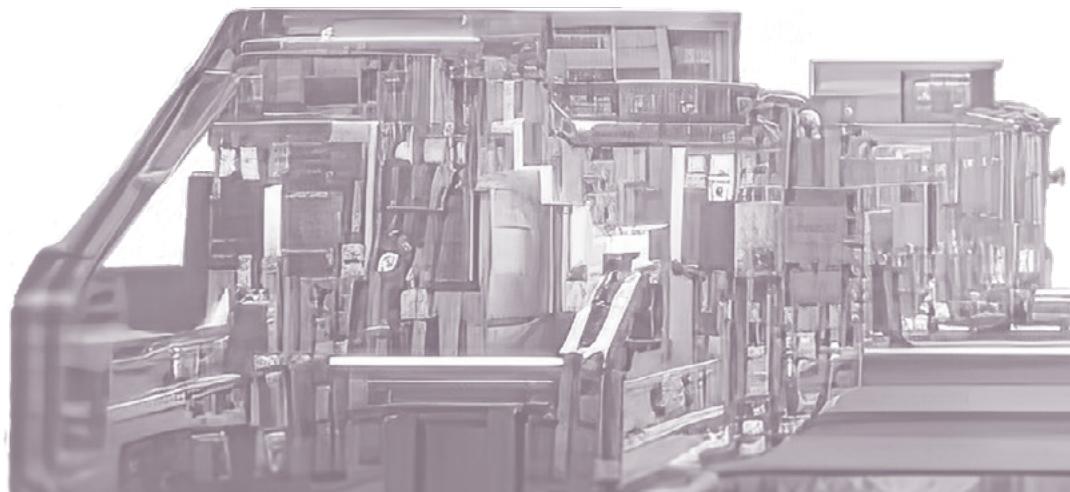
Un médicament, c'est une molécule qui va se lier à d'autres structures du vivant pour apporter un bénéfice à la santé du patient. La manière dont ces molécules interagissent entre elles est étudiée par un domaine scientifique spécifique appelé « chimie quantique ».

Avant qu'une molécule thérapeutique ne soit autorisée sur le marché, elle doit subir une batterie de tests et d'essais cliniques qui prennent souvent difficilement moins qu'une décennie. Pour cibler très vite les molécules d'intérêt, il existe une étape appelée « criblage virtuel haut débit », où des algorithmes extrêmement complexes testent en parallèle la capacité de milliers de molécules à démontrer l'effet biochimique souhaité sur la cible.

Cette compréhension de la manière dont une molécule individuelle se lie chimiquement à d'autres structures nanométriques passe par la mise au point d'outils de simulation numérique intégrant tous les principes de la mécanique quantique et de la chimie, tout en ayant pour objectif de délivrer leur résultat le plus rapidement possible, malgré la colossale complexité des calculs mis en jeu.

En France, une startup appelée Qbit pharmaceuticals développe de nouvelles méthodes de calcul combinant réseaux de neurones, supercalculateurs et ordinateurs quantiques afin de cibler toujours plus vite et efficacement les médicaments de demain⁴. ■

Pierre HenrIquet

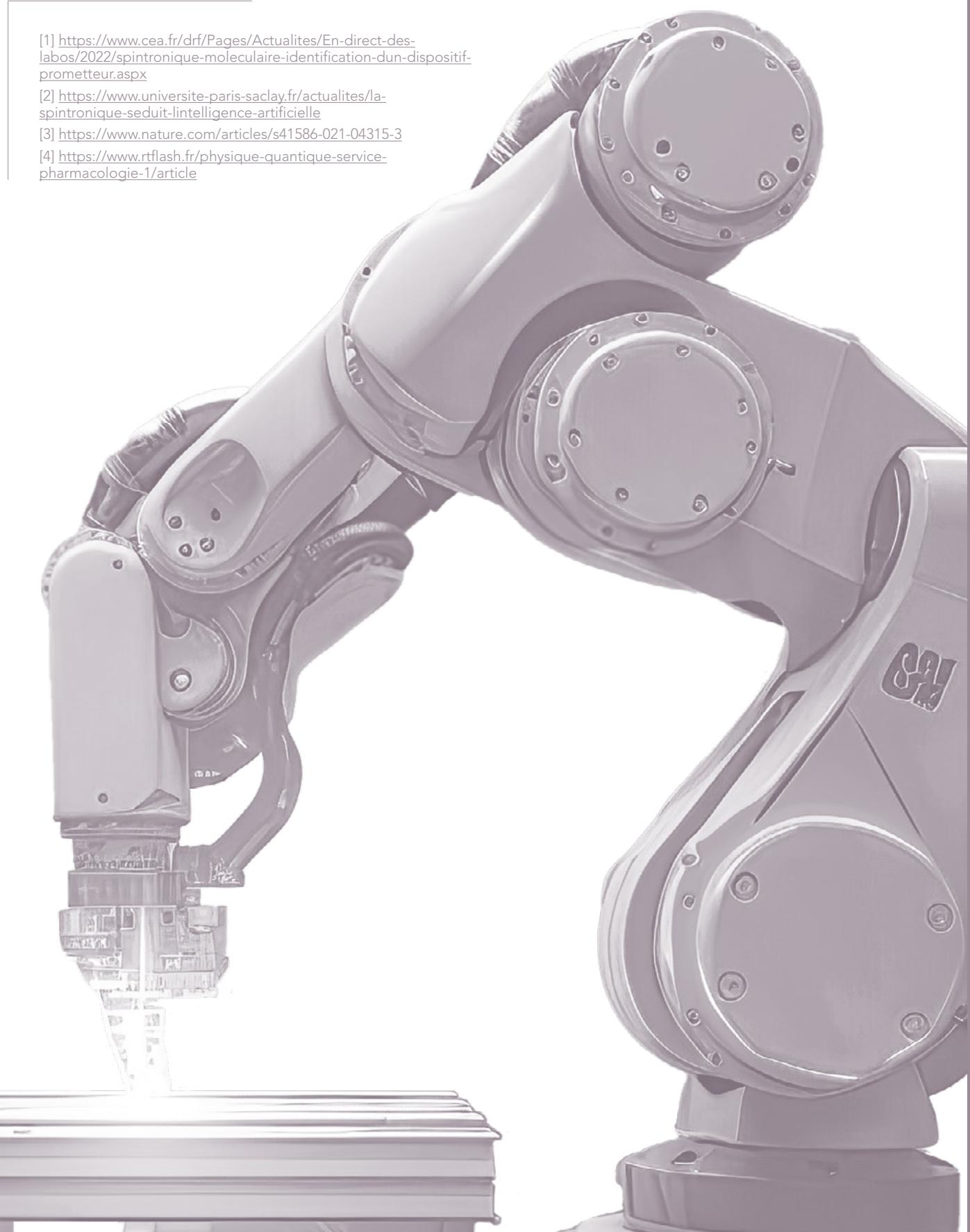


[1] <https://www.cea.fr/dr/Actualites/En-direct-des-labos/2022/spintronique-moleculaire-identification-dun-dispositif-prometteur.aspx>

[2] <https://www.universite-paris-saclay.fr/actualites/la-spintronique-seduit-lintelligence-artificielle>

[3] <https://www.nature.com/articles/s41586-021-04315-3>

[4] <https://www.rfflash.fr/physique-quantique-service-pharmacologie-1/article>



TROISIÈME PARTIE

Les ordinateurs

Le quantique aurait un potentiel révolutionnaire dans l'informatique. Voici les promesses qui poussent les grandes entreprises et les États les plus puissants à s'y investir autant.



Ordinateurs quantiques : comment ça marche ?

02 juillet 2021  5 min. de lecture

avec Landry Bretheau

Les universités et laboratoires du monde entier ainsi que les grandes entreprises les plus puissantes, comme Google, IBM, Intel et Microsoft, sont en train d'étudier et de développer les ordinateurs quantiques à un rythme effréné. Les enjeux sont importants. Mais en quoi consiste exactement cette technologie ?

Un ordinateur quantique n'est pas vraiment un « ordinateur » en tant que tel, mais plutôt un supercalculateur, capable d'exécuter certains algorithmes puissants beaucoup plus rapidement qu'un processeur ordinaire. Et ce en utilisant les principes de la mécanique quantique, qui dictent le comportement des particules élémentaires comme les photons, les électrons et les atomes, mais aussi celui de systèmes plus gros comme les circuits supraconducteurs.

De tels systèmes permettent d'implémenter des bits quantiques (« qubits »), des systèmes quantiques à deux états, qui représentent la brique computationnelle de base en information quantique.

Contrairement aux ordinateurs classiques, qui codent les informations de façon binaire, les qubits ne sont pas limités à « 0 » et « 1 » mais peuvent être dans n'importe quelle combinaison (ou « superposition ») des deux. Cette démultiplication, associée au fait que N qubits peuvent également être combinés ou 'intriqués' pour représenter 2^N états simultanément, permet ainsi de réaliser des calculs en parallèle, ainsi ouvrant un immense champ de possibilités. Un ordinateur quantique pourrait donc, en principe, surpasser un ordinateur classique pour certaines tâches importantes, comme le tri de grandes listes non triées ou la décomposition de grands nombres en facteurs premiers. Cette dernière constitue la base de la plupart des algorithmes de cryptage en usage à l'heure actuelle – notamment pour les opérations bancaires.

Les ordinateurs quantiques ne ressemblent pas non plus à leurs homologues classiques. Les modèles actuels ressemblent plutôt à de grosses boîtes de conserve suspendues au plafond, refroidies proche du zéro absolu (-273.14 °C), auxquelles pendent des centaines de câbles.

Un fléau pour un ordinateur quantique : la décohérence

Quiconque souhaitant construire un ordinateur quantique aujourd'hui doit d'abord surmonter un gros problème : le fait que les qubits sont extrêmement fragiles et difficiles à stabiliser. ▶



Toute interaction avec le « bruit » externe de leur environnement peut les faire s'effondrer comme un soufflé et les faire perdre leur nature quantique dans un processus destructeur connu sous le nom de décohérence. Si cela se produit avant la fin de l'exécution d'un algorithme, le résultat est un désordre confus (et non pas un résultat d'un calcul), car toute information stockée dans le qubit est perdue (imaginez un ordinateur qui doit redémarrer toutes les secondes). Et la difficulté à maintenir leur cohérence augmente à mesure que le nombre de qubits croît. Si bien que même les processeurs quantiques les plus avancés de nos jours peinent à dépasser les 60 qubits physiques. Or un dispositif réel nécessiterait plusieurs milliers de qubits...

En raison de ce problème, un ordinateur quantique doit être bien isolé du monde extérieur, ce qui nécessite des conditions très précises : des systèmes simples et très froids, à l'écart de toute nuisance. Ce confinement crée cependant une situation paradoxale, car plus l'ordinateur est isolé, plus il est difficile pour nous de communiquer avec lui (pour que l'on accède aux résultats de ses calculs) et de contrôler ce qu'il fait.

« Un dispositif réel nécessiterait plusieurs milliers de qubits. »

Éviter la décohérence ?

Isoler, isoler, isoler

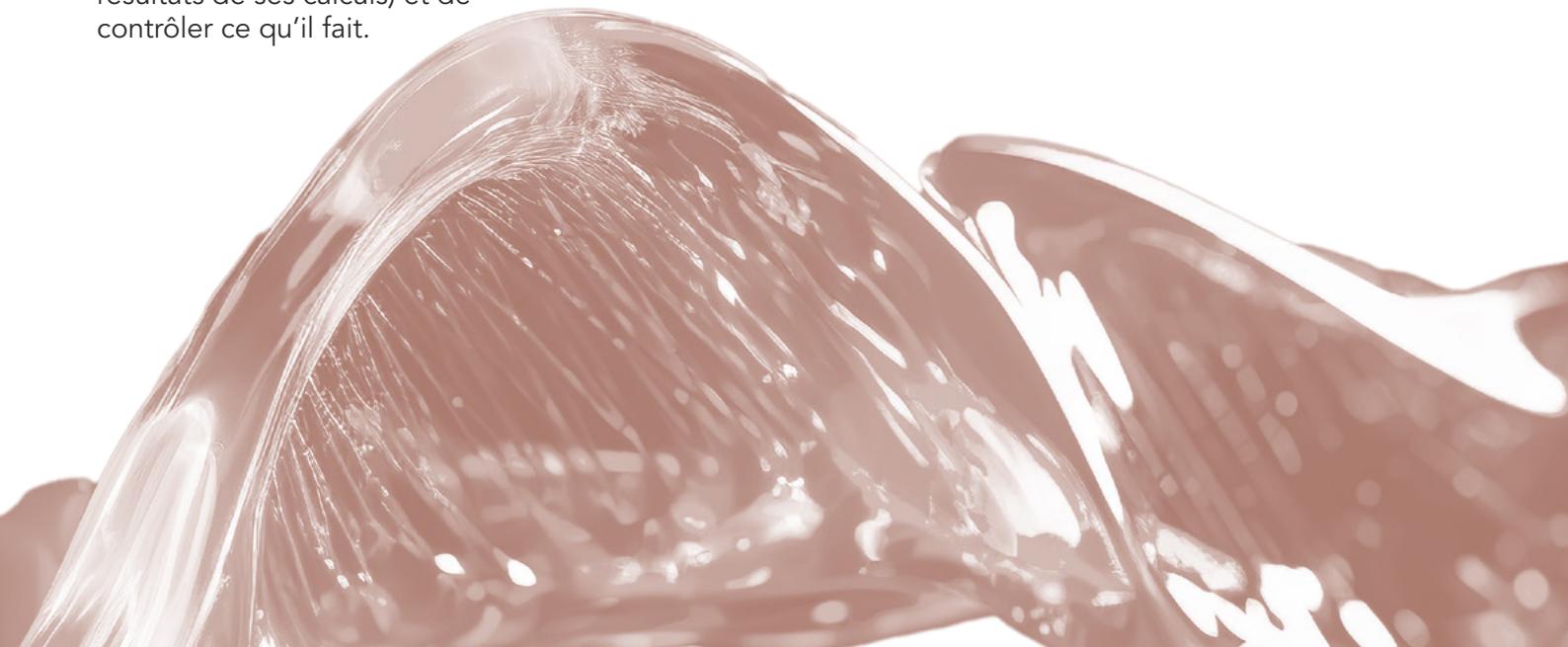
Ces dernières années, des qubits ont été fabriqués à partir d'un certain nombre de systèmes isolés qui restent cohérents le temps d'exécuter des algorithmes. Il s'agit notamment d'ions (des atomes auxquels on ôte ou ajoute un électron) piégés, d'atomes de « Rydberg » ultra-froids, et de photons (particules de lumière).

Un ordinateur reposant sur les pièges à ions stocke les informations dans les niveaux d'énergie d'ions individuels. C'est ainsi que sont formés les qubits dans ce système. Les informations sont partagées entre ces qubits, puis des impulsions laser manipulent leurs états et créent une intrication entre eux. Cette technologie est assez avancée et les chercheurs ont récemment réussi à créer un état totalement intriqué de « 24-qubits-GHZ » (GHZ pour « Greenberger-Horne-Zeilinger ») en utilisant des ions de calcium¹.



Landry Bretheau

Professeur et chercheur en physique quantique à l'École polytechnique (IP Paris)



« Ces dernières années, nous sommes passés à l'intrication de 3 qubits à plus de 50 qubits. »

D'autres systèmes sont basés sur des matériaux solides que l'on pourrait intégrer aux dispositifs électroniques traditionnels. Ces structures, qui ont la taille d'un micron, sont petites à l'échelle du quotidien, mais grandes par rapport aux atomes et peuvent se comporter comme des particules quantiques, tels des électrons ou des atomes. Dans cette famille « d'objets quantiques artificiels » on peut citer les « points quantiques » (minuscules morceaux de semi-conducteurs), les circuits supraconducteurs, et les diamants contenant un type particulier de défauts appelés « lacunes d'azote ». Un ordinateur quantique basé sur des qubits supraconducteurs, par exemple, est refroidi à des températures de l'ordre du millikelvin (ce qui est plus froid que l'espace interstellaire) et est contrôlé à l'aide de micro-ondes². Les chercheurs tentent également de déterminer lesquels de ces systèmes feraienr les meilleurs qubits.

Un paramètre important est, bien sûr, la résistance d'un qubit à la décohérence, qui peut être évaluée en matière de « fidélité » d'une opération quantique. Même si la fidélité n'est pas parfaite (à 100 %), toute valeur inférieure entraînera des erreurs après de multiples opérations ; la plupart des ordinateurs quantiques actuels sont très sensibles aux erreurs.

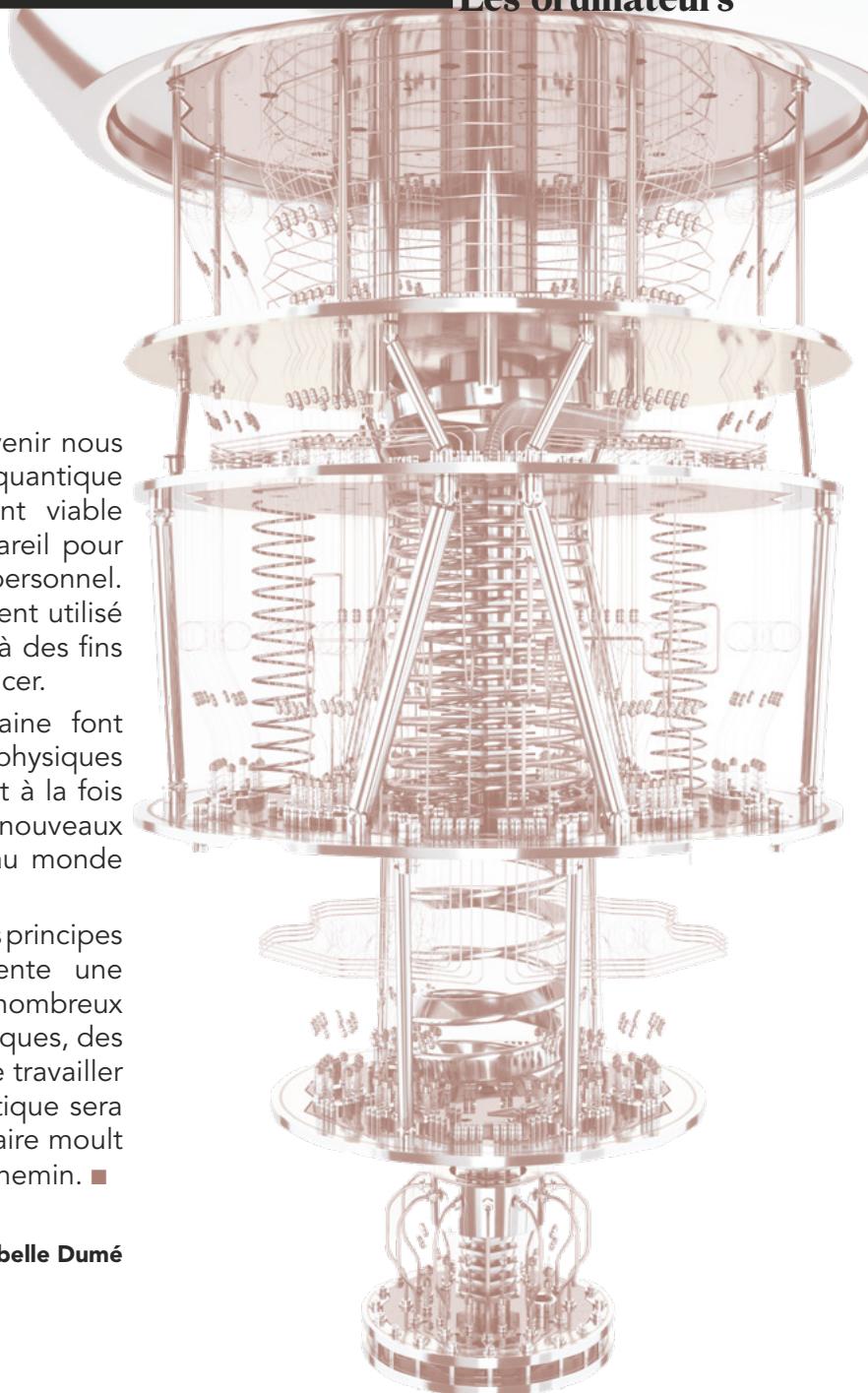
Si les protocoles de « correction d'erreur quantique » peuvent atténuer la décohérence, ils sont coûteux d'un point de vue hardware et un système fonctionnel doit être doté d'une fidélité suffisamment élevée au départ.

Les chercheurs progressent toutefois dans ce domaine et des travaux récents ont montré qu'une porte à deux qubits en entrée peut être fabriquée à partir de deux points quantiques en silicium³. Cette porte peut atteindre une fidélité de 98 % pour l'opération CROT, un composant essentiel d'un ordinateur quantique.

Que peuvent réaliser les ordinateurs quantiques aujourd'hui et que nous réserve l'avenir ?

L'idée d'un ordinateur quantique a été avancée pour la première fois par le regretté physicien et lauréat du prix Nobel Richard Feynman dans les années 1980 pour simuler les équations complexes de la mécanique quantique, trop longues à résoudre sur un ordinateur classique. Aujourd'hui, les domaines d'application sont beaucoup plus variés : cryptographie, simulation des propriétés des matériaux (en vue de les améliorer), résolution ultrarapide d'équations différentielles et optimisation de l'apprentissage automatique. Le progrès est impressionnant et les chercheurs sont passés à l'intrication de seulement trois qubits à plus de 50 qubits ces dernières années, avec un taux d'erreur de 1 sur 1000⁴.





Bien qu'il soit difficile de prévoir ce que l'avenir nous réserve, il est peu probable qu'un ordinateur quantique pleinement fonctionnel et commercialement viable voie le jour dans un avenir proche. C'est pareil pour un quelconque type d'ordinateur quantique personnel. Un dispositif quantique sera plus probablement utilisé pour la recherche fondamentale, la R&D ou à des fins gouvernementales et militaires pour commencer.

Aujourd'hui, les chercheurs dans ce domaine font progresser non seulement les machines physiques elles-mêmes (le hardware), mais développent à la fois des logiciels innovants (le software) avec de nouveaux types d'algorithmes spécialement adaptés au monde quantique.

Si l'informatique quantique repose bien sur des principes de la physique fondamentale, elle présente une formidable occasion pour les scientifiques de nombreux domaines – de l'informatique, des mathématiques, des sciences des matériaux et de l'ingénierie – de travailler ensemble. La route vers un ordinateur quantique sera certes longue, mais elle nous permettra de faire moult découvertes passionnantes tout au long du chemin. ■

Propos recueillis par Isabelle Dumé

[1] <http://dx.doi.org/10.1103/PRXQuantum.2.020343>

[2] <https://www.nature.com/articles/s41586-021-03268-x>

[3] <https://www.nature.com/articles/s41586-019-1197-0>

[4] <https://www.nature.com/articles/s41586-019-1666-5>

Découvrez d'autres articles de Landry Bretheau :

- [Pourquoi États et entreprises courrent-ils après le quantique ?](#)
- [L'ordinateur quantique : tout comprendre en 15 minutes](#)

Pourquoi États et entreprises courrent-ils après le quantique ?

03 mars 2021  5 min. de lecture

avec Landry Bretheau

En tant que chercheur dans le domaine de la physique quantique, pouvez-vous nous expliquer pourquoi le gouvernement français accorde autant d'attention à ce domaine en ce moment ?

Parce que c'est en ce moment que ça se passe ! Nombreux sont ceux qui pensent que nous entrons dans la seconde révolution quantique. Il faut d'ailleurs garder à l'esprit que la première s'est produite dans les années 1920-30, grâce aux travaux de scientifiques aussi connus qu'Einstein ou Planck. À l'époque, il s'agissait d'abord d'une révolution conceptuelle, qui s'est produite lorsque l'on a réussi à comprendre des notions telles que la « dualité onde-particule », le « rayonnement du corps noir » ou l'« interaction lumière-matière ».

Avant l'arrivée de la physique quantique, les scientifiques ne pouvaient pas expliquer ces phénomènes. Leurs découvertes ont donné naissance à des technologies révolutionnaires qui ont fait entrer l'ingénierie dans l'ère numérique, comme les lasers ou les transistors. Ces derniers permettent de contrôler les signaux électroniques, et sont à la base des processeurs informatiques.

Il y avait cependant un aspect qui prêtait à confusion pour les chercheurs : le concept d'« intrication quantique ». Sans trop entrer dans les détails, on a longtemps ignoré si l'intrication qu'ils prédisaient était un phénomène naturel, ou si elle était due à une mauvaise compréhension de la physique quantique. Nous savons aujourd'hui qu'elle est naturelle, et ce grâce aux expériences qui ont été réalisées sur des objets quantiques individuels, comme celles du professeur Alain Aspect, considéré comme un pionnier du domaine. Il a d'ailleurs joué un rôle très important dans la promotion de la seconde révolution quantique et dans la constitution du plan quantique avec le gouvernement. ▶

Quelle est l'importance d'une telle proposition ?

En bref, le Plan Quantique est central parce qu'il y a une promesse de nouvelles technologies. Maintenant que le phénomène de l'intrication est bien établi, il est possible d'envisager de futures applications utilisant des technologies quantiques pour le calcul, les communications, la détection et la simulation, avec des retombées potentielles dans les domaines de l'énergie, de la santé et de la sécurité. Mais le principal argument de vente, c'est l'ordinateur quantique.

Beaucoup de gens auront entendu parler des ordinateurs quantiques sans savoir ce qu'ils sont, et il faut dire que le mot « ordinateur » est légèrement trompeur. Il est peu probable que nous voyions à l'avenir un ordinateur quantique universel qui remplacera le PC ou le smartphone, par exemple. Les ordinateurs quantiques sont en fait des super-calculateurs, capables d'exécuter des algorithmes quantiques spécifiques et puissants beaucoup plus rapidement qu'un processeur ordinaire.

L'idée est d'exploiter des phénomènes quantiques tels que la superposition et l'intrication pour effectuer des calculs plus rapidement. Un ordinateur quantique manipule l'information en utilisant un grand nombre de bits quantiques, qui peuvent être préparés dans des états massivement intriqués.

« Il faut dire que le mot *ordinateur* est un peu trompeur. »

Cela permet d'encoder plusieurs résultats de calcul en une seule étape, grâce à un phénomène connu sous le nom de « parallélisme quantique ».

Ce qui peut conduire à une accélération quantique pour des algorithmes spécifiques, tels que la factorisation en nombres premiers, étant à la base du cryptage RSA. Cette méthode de chiffrement est très largement utilisée pour échanger des données confidentielles sur Internet, en particulier dans les transactions bancaires. Il est extrêmement difficile pour un ordinateur standard de casser le chiffrement RSA, mais un ordinateur quantique pourrait le faire bien plus rapidement, et ainsi décoder des communications cryptées.

Cette technologie présente donc un intérêt tout particulier pour le secteur de la défense militaire. Le fait que certains États acquièrent cette capacité pourrait poser d'importants problèmes de sécurité militaire, et c'est pour cette raison que le ministère américain de la Défense finance massivement un programme de recherche sur l'informatique quantique. ▶

Les États (Chine, États-Unis) et les entreprises (Google et Facebook) les plus puissants investissent déjà dans l'informatique quantique. Y a t-il vraiment une chance pour que la France arrive à suivre le rythme ?

Depuis 2018, les États-Unis ont annoncé un investissement de 2 milliards de dollars dans la recherche et la Chine aurait dépensé au moins 10 milliards pour son Laboratoire national des sciences de l'information quantique. Des financements ont également été prévus en Europe. L'Allemagne a lancé son programme il y a trois ans et l'UE finance le projet Quantum Flagship depuis 2018, en offrant 1 milliard d'euros pour les dix prochaines années. Donc, oui, le Plan Quantique, qui s'appuie sur la recherche d'excellence déjà présente en France, nous permettra de suivre le rythme : nous ne sommes pas les premiers, mais nous restons extrêmement bien placés.

Par ailleurs, le secteur privé français sera également impliqué. Des entreprises nationales et européennes comme Total ou Airbus ont promis d'investir. Et des start-ups apparaissent dans tout le pays ; Quandela, Pasqal et Alice & Bob pour n'en citer que trois, sont des spin-offs de laboratoires de recherche français. Jusqu'à présent, personne ne dispose d'un ordinateur quantique pleinement opérationnel, avec une puissance de traitement significative. Google est parmi les plus avancés, avec un processeur limité à 53 bits quantiques. Il s'agit d'un véritable tour de force expérimental, mais il est encore trop petit pour être véritablement utile. ▶



Laurent Sanchez-Palencia
Directeur de recherche CNRS en physique quantique et professeur à l'École polytechnique (IP Paris)

L'intrication pour la cryptographie

L'intrication est un phénomène purement quantique qui intéresse l'équipe de Laurent Sanchez-Palencia, dans lequel deux particules ou plus peuvent avoir des corrélations beaucoup plus profondes que ne le permet la physique classique.

Par exemple, les propriétés observables d'une particule quantique sont généralement indéterminées, de sorte que les résultats de mesure sont aléatoires. Néanmoins, lorsque les particules sont intriquées, la détermination de l'état d'une particule fixe instantanément l'état de l'autre, ou des autres, et ce quelle que soit la distance qui les sépare.

Cette puissante « action fantôme à distance », comme l'appelait Einstein, semble transcender l'espace et le temps, de sorte que nous pouvons déterminer l'état d'une particule simplement en mesurant celui de sa partenaire intriquée. Par exemple, si vous mesurez le spin d'une particule, disons un électron, vous pouvez déterminer le spin de l'autre sans jamais l'observer.

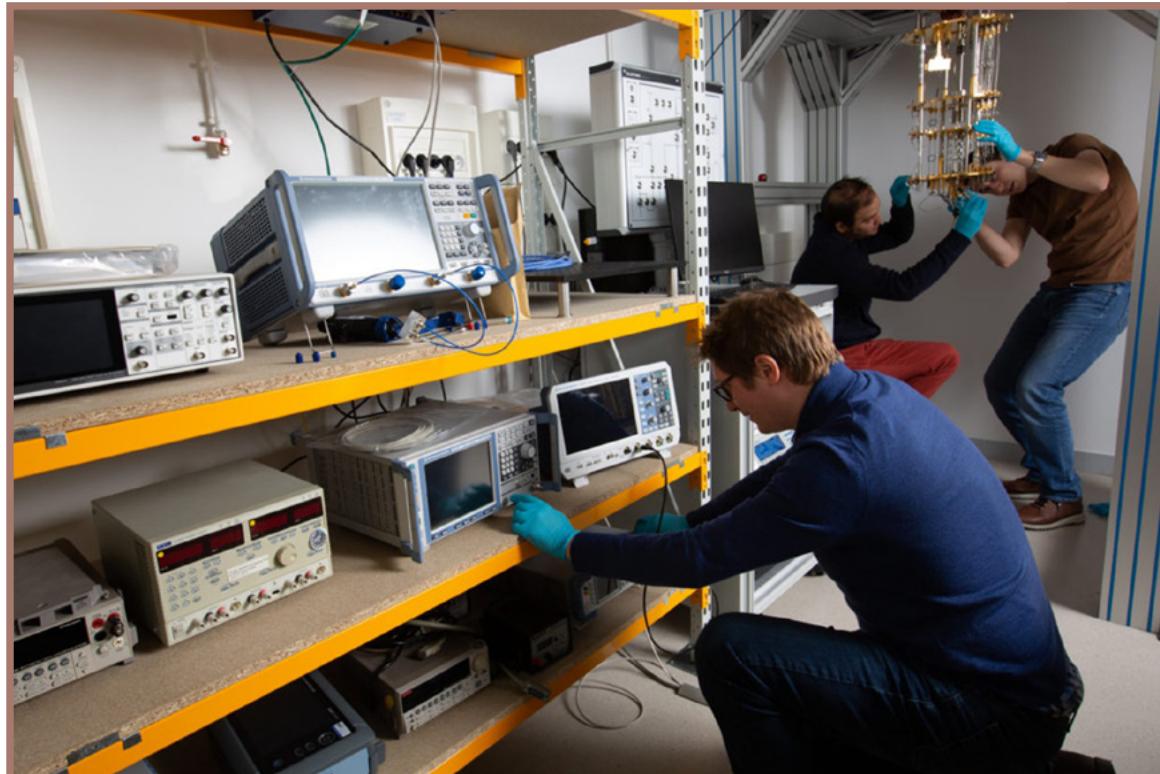
On commence à peine à exploiter les applications de ce spectaculaire effet de corrélation à distance, même s'il est déjà utilisé dans la cryptographie de certaines télécommunications : en termes simples, supposons que l'émetteur et le récepteur partagent une paire intriquée, de sorte que les résultats de leurs mesures sont aléatoires mais identiques. Pour intercepter la communication, un espion doit effectuer une mesure, dont le résultat est aléatoire mais surtout qui modifie l'état de la paire, qui n'est plus intriquée.

Les mesures de l'émetteur et du récepteur ne sont alors plus corrélées et ils pourront le constater en comparant les résultats de leurs mesures. La force d'une telle méthode de cryptage est qu'elle ne repose pas sur la difficulté d'espionner sans être repéré mais sur une impossibilité basée sur les lois fondamentales du monde quantique.

Une autre application du caractère aléatoire de la mesure est la possibilité de fabriquer des générateurs de nombres aléatoires parfaits et des clés cryptographiques totalement aléatoires. ■

Isabelle Dumé

Vous pourriez dire : « Oh, eh bien, ajoutons juste plus de qubits pour rendre le processeur plus puissant », mais il y a un problème. Les états quantiques sont très fragiles – plus vous en avez, moins ils sont stables. C'est pourquoi les ordinateurs quantiques doivent être fortement confinés. Mais cela crée en soi un paradoxe, car plus ils sont confinés, plus il nous est difficile de communiquer avec eux pour contrôler ce qu'ils font.



De gauche à droite :
Jean-Damien Pillet,
Landry Bretheau
et Ambroise Peugeot
Crédit : Jérémie Barande

Qu'est-ce que cela signifie pour la recherche française en physique quantique ?

Ce n'est pas demain que nous aurons un ordinateur quantique. Mais un financement comme celui-ci est une chance. Nous n'aurons peut-être pas un ordinateur quantique pleinement opérationnel dans dix ans, mais il est certain que nous découvrirons d'autres choses passionnantes en cours de route. Et même lorsque nous en créerons un, il est peu probable qu'il s'agisse d'un objet du quotidien. Les ordinateurs quantiques seront plus probablement des outils stratégiques, servant des besoins très spécifiques, comme la recherche fondamentale, la R&D, ou la défense.

D'ailleurs, les innovations ne se feront pas qu'au niveau du hardware, c'est-à-dire des machines physiques : il y a aussi un besoin de nouvelles idées sur le plan software. La recherche théorique, à l'interface entre la physique, l'informatique et les mathématiques, doit ainsi découvrir de nouveaux algorithmes permettant une accélération quantique. Un tel financement est donc très encourageant pour les jeunes qui entrent sur le marché du travail ! Il peut leur permettre d'orienter leur parcours professionnel, et de se diriger vers une carrière de chercheurs ou d'ingénieurs quantiques. Et pour les plus impatients, nous pouvons quand même rappeler qu'il existe déjà des ordinateurs quantique IBM accessibles sur le cloud. Même si leurs performances restent assez limitées, ils permettent aux étudiants de se familiariser avec l'informatique quantique, et de réaliser leurs premiers travaux ! ■

Propos recueillis par James Bowers

Une téléportation multinœuds robuste et « incassable » pour un internet quantique

09 octobre 2023  5 min. de lecture

avec Sophie Hermans

**Sophie Hermans**Chercheuse en postdoctorat à l'IQIM
(Caltech)

Les chercheurs du Ronald Hanson Lab de QuTech (une collaboration entre l'université technologique de Delft aux Pays-Bas et TNO) travaillent sur la transmission d'informations quantiques en utilisant des bits quantiques (qubits) dans le diamant. Ils ont récemment démontré qu'ils pouvaient transférer ces informations entre deux nœuds non directement connectés par téléportation quantique - une première. À terme, ce type de téléportation pourrait être utilisé pour créer un internet quantique, car il est robuste et « incassable ».

La téléportation quantique nous fait souvent penser à Star Trek. Si la téléportation n'est pas possible pour des objets tels que des êtres humains, elle l'est pour des états quantiques encodés sur des particules se comportant selon la mécanique quantique. Le processus n'implique aucun transfert physique de matière, mais le transfert instantané d'un état quantique entre des particules séparées par une distance immense ; il est effacé sur le site de l'expéditeur et apparaît immédiatement sur le site du destinataire.

De tels systèmes permettent d'implémenter des bits quantiques ('qubits'), des systèmes quantiques à deux états, qui représentent la brique computationnelle de base en information quantique.

« Action fantôme à distance »

L'idée de base de la téléportation est que deux nœuds de réseau, traditionnellement appelés Alice et Bob, partagent une paire de particules intriquées (en cryptographie quantique, Alice est l'expéditrice d'un message et Bob est le destinataire). Les particules intriquées sont celles qui restent liées d'une manière impossible en physique classique, quelle que soit la distance qui les sépare. Albert Einstein a appelé cet effet « action fantôme à distance ». Alice interagit ensuite avec une troisième particule - dans un état inconnu - avec sa moitié de la paire intriquée, mesure le résultat de l'interaction et en informe Bob par un canal classique. Muni de cette information et d'une mesure sur sa moitié de la paire intriquée, Bob peut reconstruire l'état inconnu d'origine, qui est celui qui a été téléporté. ▶

« Théorisée en 1993, la téléportation a été démontrée expérimentalement en 1997. »

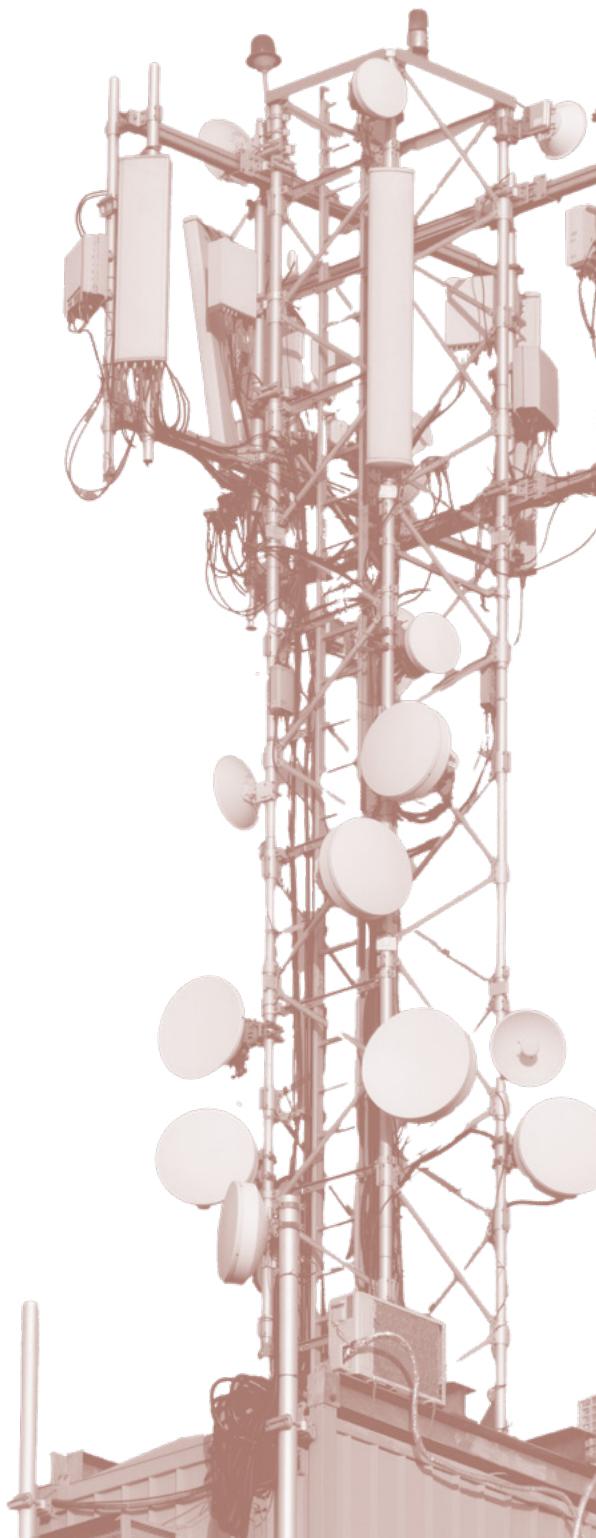
La téléportation a été proposée théoriquement pour la première fois en 1993 et a été démontrée expérimentalement pour la première fois en 1997 avec la téléportation de la polarisation d'un photon. Depuis, plusieurs équipes de chercheurs ont téléporté les états des spins atomiques, des spins nucléaires et des ions piégés, pour ne citer que trois exemples. Les chercheurs ont également réussi à téléporter « deux degrés de liberté » - le spin et le moment angulaire orbital - entre des photons individuels.

Un réseau quantique à trois nœuds

Ronald Hanson et ses collègues ont récemment réalisé le tout premier réseau quantique à trois nœuds en utilisant des « centres de vacance d'azote » (notés « NV ») dans le diamant comme qubits. Les centres de vacance d'azote sont des défauts dans le réseau d'atomes de carbone du matériau où un atome d'azote s'est substitué à un atome de carbone. Chaque nœud contient un qubit de communication et un nœud contient également un qubit de mémoire qui peut stocker l'information quantique dans le nœud.

Pour téléporter des informations quantiques d'un émetteur à un récepteur, leurs qubits respectifs doivent être intriqués. Lorsqu'une « mesure de l'état de Bell » est effectuée sur le qubit de l'expéditeur, son état quantique est téléporté, c'est-à-dire qu'il disparaît du nœud de l'expéditeur et apparaît dans celui du destinataire. Cet état quantique, qui arrive sous une forme cryptée, peut ensuite être décrypté en utilisant le résultat de la mesure de l'état de Bell, c'est-à-dire en l'envoyant au récepteur par un canal classique, tel qu'une fibre optique.

Jusqu'à présent, ce processus n'avait été démontré que pour deux points de réseau adjacents, Alice et Bob. L'ajout d'un troisième point (appelé Charlie) n'est pas facile, car l'intrication entre Alice et Charlie doit être créée par l'intermédiaire de Bob. L'intrication doit également être d'une grande fidélité pour que la téléportation réussisse.



Une pléthore d'améliorations

Ronald Hanson et ses collègues y sont parvenus en installant des détecteurs supplémentaires qui identifient mieux les « faux » signaux provenant des photons indésirables émis dans leur système. Ils ont également amélioré la mémoire utilisée pour stocker les informations en protégeant le qubit de mémoire des interactions avec le qubit de communication et l'environnement cristallin. ▶

Ces interactions provoquent un phénomène connu sous le nom de décohérence qui fait perdre au qubit l'information quantique qu'il contient. Enfin, ils ont amélioré la lecture de la mémoire du qubit en filtrant les « mauvaises » lectures en temps réel, ce qui augmente in fine la fidélité.

Toutes ces mesures leur permettent de téléporter des informations quantiques entre les nœuds Alice et Charlie non adjacents. Pour ce faire, ils ont d'abord intriqué les qubits d'Alice et de Charlie via le qubit de Bob. Charlie stocke ensuite une partie des états intriqués sur son qubit de mémoire et prépare l'état quantique à téléporter sur son qubit de communication. L'application de la mesure d'état de Bell à Charlie téléporte l'état vers Alice.

Les chercheurs travaillent actuellement à l'augmentation du nombre de qubits de mémoire, ce qui permettra d'exécuter des protocoles plus complexes.

Ils envisagent également d'intégrer des fibres optiques conventionnelles dans leur expérience. Cela permettrait de sortir la technologie du laboratoire et de l'intégrer dans des réseaux déjà utilisés dans le monde réel. Enfin, le développement d'une « pile de contrôle » du réseau quantique, similaire à celle utilisée dans l'internet actuel, sera également nécessaire pour un futur internet quantique fonctionnel. ■

Propos recueillis par Isabelle Dumé

The Ronald Hanson Lab : <https://qutech.nl/lab/hanson-lab/>
TNO : <https://www.tno.nl/en>
Publication dans Nature : <https://www.nature.com/articles/s41586-022-04697-y>

Crédits :

Directeur exécutif : Clément Boule
Cheffe de projet : Viviane de Castro Rodriguez
Rédacteur en chef : James Bowers
Chef d'édition : Pablo Andres
Assistante d'édition : Loraine Odot
Maquettiste : Pablo Andres
Graphiste : Anne-Laure Amigues
Photothèque : Adobe Stock



