LA FORCE QUANTIQ

LES TECHNOLOGIES QUANTIQUES, EXPLOITANT LES PROPRIÉTÉS DÉROUTANTES DES PARTICULES ET DES ATOMES, BÉNÉFICIENT D'INVESTISSEMENTS QUI SE COMPTENT EN MILLIARDS D'EUROS. LES PHYSICIENNES ET PHYSICIENS SUISSES SONT À LA POINTE MONDIALE DANS CE DOMAINE ALLIANT CRYPTOGRAPHIE, ORDINATEURS, SENSEURS ET MATÉRIAUX QUANTIQUES.

La physique quantique est une théorie déroutante. Visibles en principe uniquement à toute petite échelle, ses propriétés sont profondément contre-intuitives. Les spécialistes du domaine parlent en effet sans sourciller (ni sourire) de téléportation, d'intrication, de non-localité et d'autres superpositions et interférences quantiques. Autant de phénomènes qui n'ont aucun équivalent dans le monde classique si ce n'est dans les livres de science-fiction ou, peut-être, de magie. Ces concepts, bien réels, sont pourtant à la base de ce que d'aucuns appellent déjà une révolution technologique susceptible de bouleverser des pans importants de notre société, à commencer par ceux de la communication et de l'informatique.

Signe qui ne trompe pas, les grandes puissances – États-Unis et Chine en tête – suivies de près par les compagnies géantes telles que Google, IBM, Microsoft ou encore Amazon, injectent des milliards de dollars dans ce secteur afin d'être parmi les premiers à développer un ordinateur quantique, à la puissance de calcul décuplée, ou un système de cryptographie quantique réputé absolument inviolable. L'Union européenne (UE) n'est pas en reste avec notamment le Flagship quantique, un mégaprojet d'un milliard d'euros sur dix ans, censé affirmer le leadership du continent dans ce secteur. Certains pays membres jouent également la partie en mode individuel et font monter les enchères encore plus haut. La France a ainsi promis en janvier 2021 un budget de 1,8 milliard d'euros sur cinq ans pour les technologies quantiques. L'Allemagne a annoncé en mai le déblocage de 2 milliards d'euros pour construire un ordinateur quantique d'ici à 2025. Quant au Royaume-Uni, il affirme avoir dépassé le milliard de livres d'investissements cumulés dans les technologies quantiques.

LA COMMISSION EUROPÉENNE A DÉCIDÉ CE PRINTEMPS QUE LA RECHERCHE DANS LES TECHNOLOGIES QUANTIQUES ÉTAIT DÉSORMAIS STRATÉGIQUE

Tout porte cependant à croire que dans cette course, la Suisse devra jouer en solo. La Commission européenne a en effet décidé ce printemps que la recherche dans les technologies quantiques était désormais stratégique, à l'image du domaine spatial. En d'autres termes, les projets et les financements dans ces disciplines doivent être réservés aux seules équipes issues des pays membres de l'UE.

Pour ne rien arranger, le Conseil fédéral a, au mois de mai, abandonné l'accord-cadre avec l'UE. Ce geste a eu pour effet de reléguer le statut de la Suisse à celui de pays tiers non associé à Horizon Europe, le 9e programme-cadre de recherche et d'innovation de l'UE (dont le budget est estimé à 95 milliards d'euros pour la période 2021-2027). Même si elle est contournable via des financements directs assurés par la Confédération, cette évolution ne fait qu'isoler davantage les « quantiques » suisses.

Les conséquences ne se sont pas fait attendre : les physiciens et les physiciennes suisses ont d'abord vu se fermer cette année les portes de l'European Quantum Communication Infrastructure (EuroQCI), un programme d'envergure visant à développer une structure de communication quantique à l'échelle du continent. Ils et elles ont ensuite été exclu-es officiellement du Flagship quantique, auquel des chercheurs genevois participent pourtant depuis trois ans. La Suisse, et Genève en particulier, a pourtant de sérieux atouts à faire valoir en la matière. Un livre blanc, *Les technologies quantiques en Suisse, réflexions et recommandations du Conseil suisse de la science (CSS)*, réalisé de manière un peu prémonitoire en 2020 à l'adresse du Conseil fédéral, en fait l'inventaire (*lire aussi l'encadré ci-contre*). L'Université de Genève, par exemple, est à la pointe en cryptographie quantique, en matériaux quantiques et en simulations quantiques. L'École polytechnique fédérale de Zurich (ETHZ), l'Institut Paul Scherrer et l'Université de Bâle sont actifs dans le domaine des ordinateurs quantiques et des senseurs quantiques, tandis que l'École polytechnique fédérale de Lausanne (EPFL) se distingue dans celui des senseurs et « logiciels quantiques ». Tour d'horizon avec Nicolas Brunner, professeur au Département de physique appliquée (Faculté des sciences).

Campus : Tout le monde parle de révolution quantique. De quoi s'agit-il exactement ?

Nicolas Brunner : Il s'agit en fait d'une deuxième révolution quantique. La première a eu lieu au milieu du XXe siècle, avec des découvertes comme le laser et, surtout, le transistor. Celles-ci sont en effet basées sur la théorie de la mécanique quantique qui décrit de manière extraordinairement précise le monde microscopique, soit ce qui se passe à l'échelle des particules, des atomes et des molécules. Développée à l'origine par des scientifiques tels que Max Planck, Albert Einstein, Niels Bohr ou encore Erwin Schrödinger, cette première révolution quantique a en particulier permis de comprendre les propriétés semi-conductrices de certains matériaux. Des propriétés que les physiciens américains John Bardeen, Walter Brattain et William Shockley ont exploitées pour développer en 1947

Nicolas Brunner
Professeur au Département de physique appliquée, Faculté des sciences

Formation : Après un doctorat de physique de l'Université de Genève, il passe cinq ans à l'Université de Bristol, au Royaume-Uni. Il décroche ensuite un poste de professeur boursier, ce qui lui permet de revenir à l'Université de Genève.

Parcours : Nommé professeur associé en 2016, Il mène de nombreux projets, dont un prestigieux ERC Starting Grant. Il est un spécialiste mondialement reconnu en information quantique et en non-localité.

«UNE ACTION FANTOMATIQUE À DISTANCE»

LA PHYSIQUE QUANTIQUE PRÉDIT TOUTES SORTES DE PHÉNOMÈNES CONTRE-INTUITIFS, RADICALEMENT DIFFÉRENTS DU MONDE MACROSCOPIQUE QUI NOUS ENTOURE. VISITE GUIDÉE.

DANS TOUS LES ÉTATS À LA FOIS

Une particule peut, selon les lois de la nature qui régissent l'infiniment petit, se trouver dans un état de superposition quantique, c'est-à-dire qu'elle peut se trouver, par exemple, à plusieurs endroits en même temps (ou être polarisée dans toutes les directions à la fois). On parle alors d'un état totalement indéterminé. Ce qui est encore plus surprenant, c'est que lorsqu'un observateur mesure cette particule, celle-ci est «projetée» à un endroit précis, c'est-à-dire qu'elle se retrouve, finalement, dans un état bien déterminé. Une mesure quantique entraîne donc une modification de l'état quantique d'une particule et ce processus est à la fois aléatoire (le résultat relève du parfait hasard) et irréversible (la mesure détruit ou perturbe irrémédiablement le système, en l'occurrence la particule). Bien que la théorie quantique prédise cet effet, elle ne fournit aucune explication. Ce paradoxe est illustré par la fameuse expérience de pensée du «chat de Schrödinger». Le pauvre animal est enfermé dans une boîte munie d'un dispositif de mise à mort déclenché par la désintégration d'un atome radioactif. Imaginons que l'atome est préparé de telle manière qu'il se trouve dans un état quantique indéterminé, c'est-à-dire qu'il est à la fois intact et désintégré. Du coup, s'il était dans un monde quantique, le chat serait à la fois mort et vivant. Mais lorsqu'on ouvre la boîte (et que l'on mesure le système), on découvre que le chat est mort ou vivant, selon que l'atome se soit désintégré ou pas.

L'INTRICATION

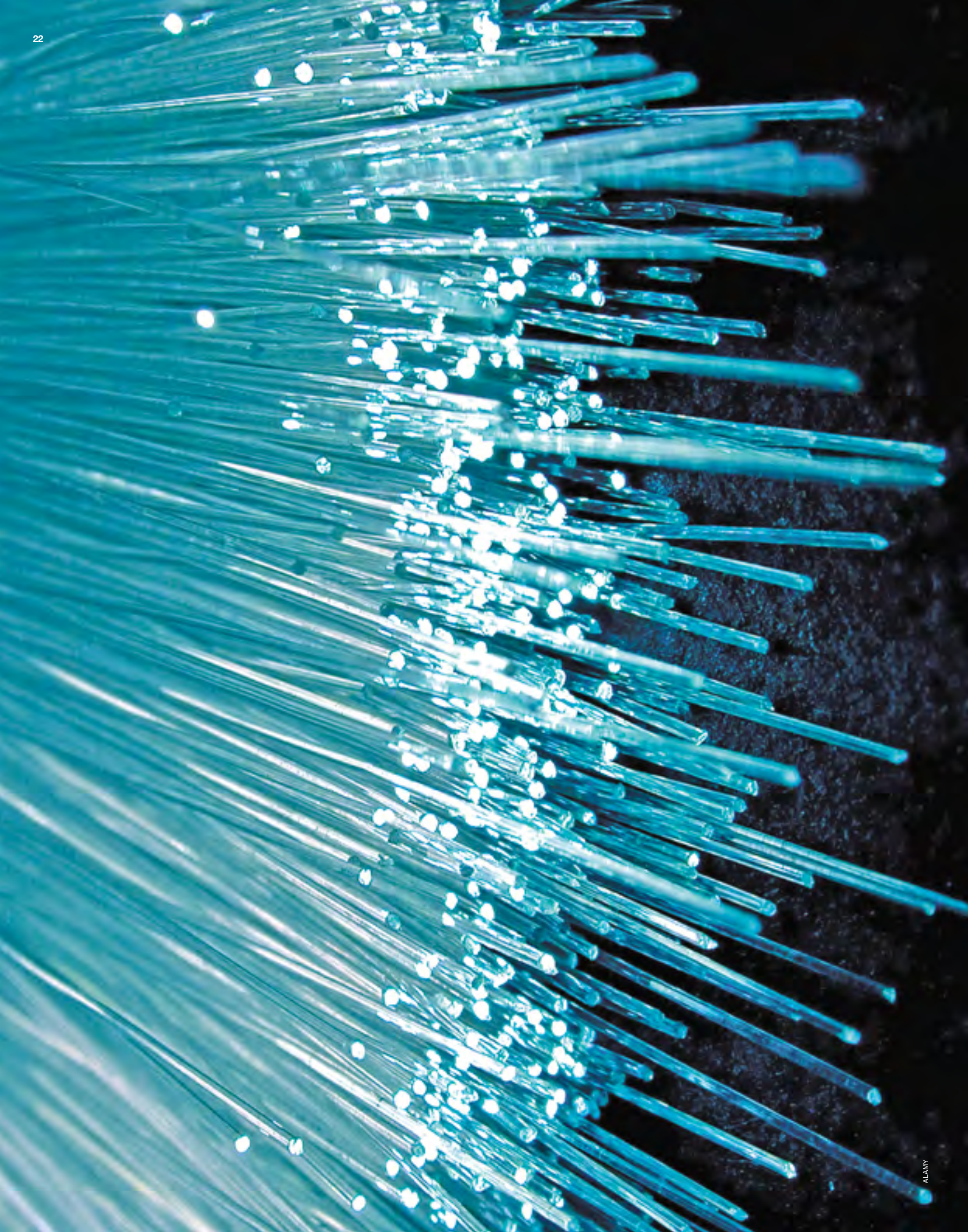
Dans le monde quantique, il est possible de préparer un système de deux particules (ou plus) dans un état quantique dit «intriqué». Dans ce cas, les deux particules sont intimement liées et se comportent de manière fortement corrélée. En fait, la physique quantique affirme que ces deux particules ne forment qu'un seul et unique système physique. Et cela reste valable même lorsque les deux particules sont séparées par une grande distance. Par conséquent, si on agit sur une des particules, en la mesurant par exemple, l'état quantique de l'autre s'en trouve instantanément modifié. Albert Einstein, qui a contribué à découvrir cette propriété, l'a qualifiée d'«action fantomatique à distance». L'intrication quantique est cependant bien réelle. Elle est observée quotidiennement en laboratoire depuis la première expérience qui l'a mise en évidence et qui est due au physicien français Alain Aspect au début des années 1980. Elle représente d'ailleurs la ressource clé pour de nombreuses technologies quantiques.

LA NON-LOCALITÉ

Puisque deux particules intriquées forment un seul et même système physique, la mesure de l'une influence immédiatement l'état de l'autre. En pratique, des expériences (menées notamment à Genève) ont pu démontrer que ce phénomène est véritablement instantané. Cette propriété purement quantique ne possède aucun équivalent en physique classique où toute information ou influence se propage de proche en proche et ne peut dépasser la vitesse de la lumière. Dans le cas des deux particules intriquées, les experts préfèrent toutefois renoncer à l'idée d'une influence (ou d'une communication) entre elles. À la place, on parle de non-localité quantique. Les deux particules forment le même objet, même si elles sont à des endroits très différents. Cela peut se vérifier en pratique par une expérience proposée par le physicien américain John Bell dans les années 1960 et réalisée aujourd'hui de manière routinière dans les laboratoires.

LA TÉLÉPORTATION

La téléportation quantique est une manifestation de la non-localité quantique. Le principe consiste à téléporter un état quantique d'une particule à une autre en utilisant l'intrication. Le résultat de l'opération est que l'état de la première disparaît et réapparaît sur la seconde. Un peu comme le ferait le personnage de Spock dans la série *Star Trek* à la différence que le procédé de téléportation quantique permet de téléporter un état quantique mais pas de l'énergie ou de la matière. Les lois de la relativité générale, dont celle qui stipule que rien ne peut dépasser la vitesse de la lumière, sont donc respectées.



ALAMY

Fibres optiques.

le premier transistor, qui est le composant de base de tout appareil électronique. En d'autres termes, sans la physique quantique, nous n'aurions aujourd'hui ni ordinateur, ni téléphone portable, ni télévision, et j'en passe.

Et qu'en est-il de la deuxième révolution ?
Il se trouve qu'en plus de décrire avec une très grande précision la physique des particules et des atomes, la théorie quantique prédit également l'existence de phénomènes contre-intuitifs, tels que l'intrication, la non-localité ou encore la téléportation quantique qui se manifestent à toute petite échelle (*lire aussi encadré en page 21*). Aujourd'hui, on peut non seulement observer ces phénomènes en laboratoire mais aussi les contrôler avec suffisamment de précision afin de les exploiter et de développer des technologies nouvelles qui forment justement le cœur de ce qu'on appelle la deuxième révolution quantique.

Quelles sont ces technologies ?
On peut les regrouper en trois grandes catégories. La première est celle des communications quantiques, avec notamment la cryptographie quantique et la téléportation quantique, des domaines dans lesquels l'Université de Genève est pionnière, notamment grâce aux travaux menés depuis les années 1990 par Nicolas Gisin, professeur honoraire à la Faculté des sciences, et qui ont abouti, entre autres, à la création il y a vingt ans d'ID Quantique, une start-up unique en son genre (*lire aussi en page 34*). On mentionnera ensuite les senseurs quantiques et, bien sûr, l'ordinateur quantique.

Qu'est-ce que la cryptographie quantique ?
La cryptographie est l'art d'envoyer des messages secrets. En exploitant les propriétés quantiques des photons (les particules de lumière), la cryptographie quantique permet la transmission d'informations de manière parfaitement sécurisée et donc, en principe, inviolable. L'idée est d'établir une clé de codage secrète entre deux protagonistes distants, communément appelés Alice et Bob. Alice crée des paires de photons intriqués (ils sont corrélés au point de représenter un seul et même objet), dont elle envoie un des membres à Bob qui les mesure au fur et à mesure qu'ils arrivent. En vérifiant l'intégrité des propriétés quantiques de cette transmission, les deux interlocuteurs peuvent garantir la confidentialité de la clé. En d'autres termes, pour obtenir de l'information sur cette clé, un potentiel espion perturberait forcément le phénomène d'intrication et se révélerait. Aujourd'hui, la cryptographie quantique permet déjà de sécuriser des communications sur quelques centaines de kilomètres. Pour aller au-delà, il faudrait pouvoir s'appuyer sur des relais quantiques. C'est un domaine sur lequel nous travaillons depuis plusieurs années. Des expériences de faisabilité ont été réalisées mais le système n'est pas encore suffisamment performant pour être utilisé en pratique.

« LA SUISSE A LES MOYENS DE CRÉER UN RÉSEAU DE COMMUNICATION QUANTIQUE À L'ÉCHELLE NATIONALE »

Qui peut être intéressé par un réseau de communication pareillement sécurisé ?
En Suisse, on peut citer toutes les infrastructures pour lesquelles la sécurité des données et des canaux de communication est un impératif : les réseaux de télécommunications ou de transport, comme les chemins de fer, les installations d'approvisionnement en énergie et certains services, publics ou privés, tels que les systèmes de vote électronique (l'expérience a d'ailleurs été menée à Genève en octobre 2007) ou les services financiers. En Chine, qui est en avance sur cette question et qui a lancé le développement d'un immense réseau au niveau national, la motivation est clairement d'échapper à l'espionnage des communications par d'autres grandes puissances. Les États-Unis, en particulier, conservent en effet pour l'instant le contrôle des systèmes de cryptage actuels, basé sur des algorithmes déterministes et non sur le caractère parfaitement aléatoire de la physique quantique. Et ils en profitent, comme l'a révélé entre autres l'affaire Edward Snowden, du nom de l'ancien agent américain de la CIA.

La Suisse pourrait-elle aussi se doter d'une telle infrastructure ?
La Suisse a les moyens de créer un réseau de communication quantique à l'échelle nationale. En utilisant les fibres optiques de Swisscom par exemple, il est déjà possible de mettre en place des systèmes de cryptographie

Photo du processeur de l'ordinateur quantique de Google, le Sycamore, contenant 54 qubits (dont un défectueux).

quantique. Les photons ont la particularité d'interagir de manière extrêmement faible avec les atomes dans les fibres optiques. Cela permet de transmettre des photons uniques sur des distances allant jusqu'à 200 km en pratique, et jusqu'à 400 km en conditions de laboratoire, ce qui a été réalisé notamment par une équipe genevoise.

Quels sont les autres domaines du savoir concernés par les technologies quantiques ?
Un autre domaine moins connu mais tout aussi fascinant et prometteur est celui des senseurs quantiques. Il s'agit de systèmes capables de mesurer des grandeurs physiques (température très basse, champ magnétique, force de gravitation…) avec une extrême précision (*lire en page 41*). Le principe consiste une fois de plus à exploiter les propriétés purement quantiques de la matière et de la lumière. Cela permet de développer des instruments de mesure d'une sensibilité inédite et de très petite taille. On peut ainsi obtenir des thermomètres nanoscopiques pouvant être placés sur une cellule ou encore des instruments de navigation indépendants du GPS. La Suisse compte déjà des start-up actives dans ce domaine, notamment Qnami à Bâle. Il y a aussi tout le champ de recherche ouvert par la découverte du graphène, cette feuille de carbone dont l'épaisseur n'est que d'un atome et dont les propriétés surprenantes peuvent bouleverser de nombreuses technologies (*lire en page 43*).

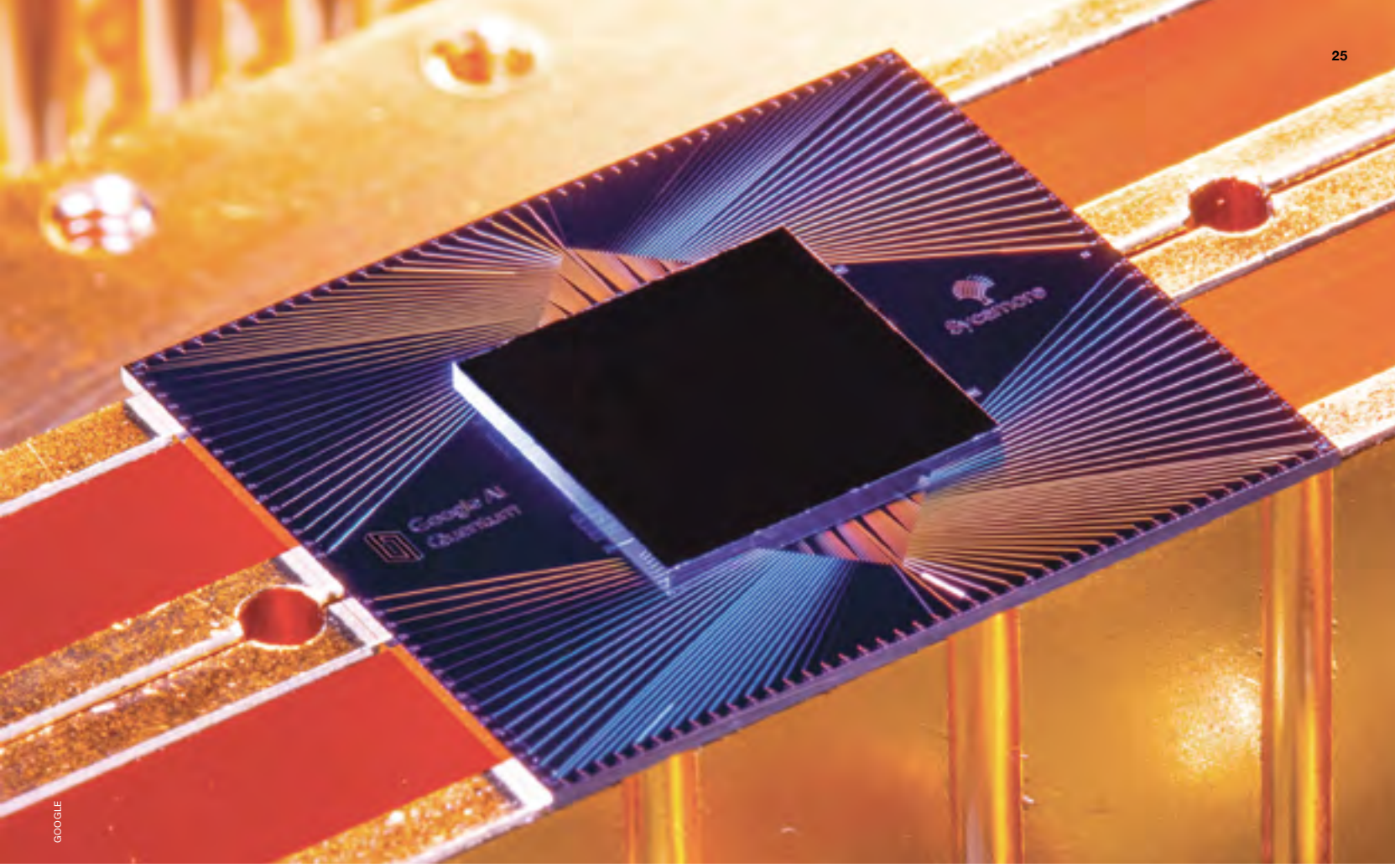
« LES ORDINATEURS QUANTIQUES PERMETTRONT DE RÉSOUDRE CERTAINS TYPES DE PROBLÈMES ABSOLUMENT HORS DE PORTÉE DES ORDINATEURS CLASSIQUES »

Et qu'en est-il des ordinateurs quantiques ?
Il s'agit d'ordinateurs d'un genre nouveau. Leur fonctionnement est basé sur une logique radicalement différente de celle utilisée par les ordinateurs actuels. Dans un ordinateur quantique, l'information est stockée et manipulée sous forme de bits logiques quantiques, appelés « qubits ». Tout comme un bit d'information classique, un qubit peut porter l'information 0 ou 1. Ce qui est nouveau, c'est que le qubit peut également porter les deux valeurs de 0 et de 1 en même temps. C'est ce qu'on appelle une superposition quantique. Un ordinateur quantique devra être composé d'un très grand nombre de qubits, qui interagiront au sein d'un « circuit quantique ».

Quel est leur avantage ?
Ces machines ne remplaceront pas nos bons vieux ordinateurs dans la vie de tous les jours. Elles permettront en revanche de résoudre certains types de problèmes absolument hors de portée des ordinateurs classiques, aussi puissants soient-ils, tels que celui consistant à trouver un seul élément donné dans une gigantesque base de données. Pour y arriver, les machines classiques doivent passer en revue toutes les possibilités, c'est-à-dire explorer de fond en comble la base de données. Un ordinateur quantique, lui, sera capable de tester toutes les possibilités en même temps, autrement dit d'inspecter toute la base de données d'un seul coup. Ce « parallélisme quantique » ouvre de nombreuses perspectives, par exemple pour déterminer la structure d'une molécule ou factoriser de grands nombres très rapidement.

Existe-t-il déjà des ordinateurs quantiques ?
Certains groupes de recherche ont réalisé et testé des prototypes d'ordinateurs quantiques, c'est-à-dire des machines pouvant manipuler une centaine de qubits environ. Le défi est très grand car pour préserver les propriétés quantiques des qubits, il faut travailler à une température très proche du zéro absolu. Les grandes entreprises d'informatique se sont elles aussi lancées dans la course à l'ordinateur quantique. IBM et Google ont notamment annoncé ces dernières années avoir franchi des étapes importantes dans ce domaine (*lire aussi en page 37*). En Suisse, à l'École polytechnique fédérale de Zurich (ETHZ), des équipes sont elles aussi à la pointe. Elles travaillent depuis de nombreuses années sur des plateformes expérimentales visant à développer un ordinateur quantique et explorent différentes technologies (ions piégés, supraconductivité, systèmes hybrides…).

Faut-il des logiciels spéciaux pour faire tourner ces machines ?
Oui, et cela représente un champ de recherche important, exploré notamment par des chercheurs des écoles polytechniques fédérales de Lausanne et Zurich. La programmation sur un ordinateur quantique est complètement différente de celle d'un ordinateur classique. Un des premiers résultats – théoriques – en la matière a d'ailleurs consisté à montrer qu'un ordinateur quantique pourrait factoriser de grands nombres très rapidement et ainsi casser les systèmes de cryptage actuels. C'est assez ironique car, d'un côté, la sécurité des communications est mise en péril par l'arrivée de l'ordinateur quantique tandis que de l'autre, la théorie quantique nous fournit une élégante parade sous la forme de la cryptographie quantique, qui est à l'épreuve même d'un ordinateur quantique.



GOOGLE

LE LIVRE BLANC DE LA QUANTIQUE SUISSE

Le Conseil suisse de la science (CSS) a publié en 2020 à l'adresse du Conseil fédéral un livre blanc, *Les technologies quantiques en Suisse, réflexions et recommandations.* Son contenu a pris une tournure particulièrement urgente depuis que les scientifiques suisses se sont retrouvés marginalisés par l'Union européenne, en particulier dans le domaine des technologies quantiques *(lire article principal).* Selon Jean-Marc Triscone, vice-recteur de l'Université de Genève et coauteur du livre blanc, faire cavalier seul dans cette course technologique qui demande de relever d'immenses défis scientifiques et techniques n'est pas idéal. La Suisse risque ainsi de perdre la position enviable qu'elle occupe dans de nombreux domaines. De plus, quand des entreprises privées, qui ont des moyens presque illimités, mettent des milliards de dollars sur la table, il y a le danger bien réel de voir certains chercheurs et chercheuses des institutions helvétiques être débauchés.

Cela dit, précise Jean-Marc Triscone, il ne faut pas baisser les bras, mais trouver des moyens pour faire face à la situation et tout tenter pour rejoindre rapidement les programmes européens. La Suisse a des arguments à faire valoir. Une étude bibliométrique de 2019 a en effet confirmé la grande compétitivité de la recherche fondamentale helvétique dans le domaine quantique. Bien qu'elle ne puisse pas rivaliser avec la Chine, les États-Unis ou l'Allemagne en termes de nombre absolu de publications, la Suisse (avec l'Autriche) est largement en tête en termes de proportion d'articles les plus cités.

Les Programmes de recherche nationaux (PRN) «*QSIT Science et technologie quantiques*», encore en cours, et ceux qui ont précédé ont joué un rôle important dans la position internationale des institutions suisses de recherche. L'instauration du PRN «Spin Qubits in Silicon» en 2020 (piloté par l'Université de Bâle) ainsi que les efforts menés aux écoles polytechniques fédérales de Lausanne (EPFL) et Zurich, à l'Institut Paul Scherer et à l'Université de Genève devraient contribuer à la maintenir.

Une des recommandations «prémonitoires» des auteurs du livre blanc est d'«*aménager d'autres possibilités de financement au-delà des structures existantes que sont le Fonds national national, Innosuisse, le domaine des EPF ou les programmes européens*». Cette solution commence peut-être à se concrétiser à l'échelle locale puisque l'Université de Genève est en train de mettre en place le Geneva Quantum Center et discute avec l'EPFL de l'idée d'ouvrir ses cours et de permettre de développer des masters dans ce domaine. Des discussions et des projets au niveau suisse sont également en développement.

Selon le livre blanc, la Suisse dispose en outre des capacités et ressources nécessaires pour favoriser et développer une industrie quantique viable. Pour le CSS, promouvoir l'essor des technologies quantiques en Suisse exige néanmoins un soutien constant à la recherche fondamentale et à la formation de jeunes talents ainsi qu'un encouragement des transferts de technologie. Cela passe aussi par une intensification de la communication et de la coordination entre les milieux académiques, les start-up, les investisseurs et les secteurs industriels potentiellement concernés. Cette dernière recommandation revêt une actualité brûlante, étant donné l'exclusion des chercheurs quantiques des programmes européens.

Référence: «Les technologies quantiques en Suisse, réflexions et recommandations du Conseil suisse de la science (CSS)», mars 2020, https://bit.ly/3lGtUuk

Réplique du « cryptex », petit coffre-fort protégé par un code secret, apparaissant dans le film « Da Vinci Code » (2006).

CRYPTOGRAPHIE

LE CODE PARFAIT EST UN RÊVE DEVENU RÉALITÉ

L'UNIVERSITÉ DE GENÈVE JOUE UN RÔLE DE **LEADER MONDIAL** DANS LA RECHERCHE EN MATIÈRE DE CRYPTOGRAPHIE QUANTIQUE. PETIT RETOUR SUR LES ÉTAPES CLÉS D'UNE HISTOIRE QUI DURE DEPUIS BIENTÔT TRENTE ANS.

Nicolas Gisin
Professeur honoraire à la Faculté des sciences

Formation : Il obtient son doctorat en physique à l'Université de Genève en 1981 pour sa thèse en physique quantique et statistique. Après un postdoc à l'Université de Rochester, il intègre le monde de l'industrie. En 1988, il revient à l'Université de Genève où il est nommé professeur au Département de physique appliquée.

Parcours : Auteur de nombreuses premières dans le domaine de l'information quantique, il est récompensé entre autres par le prix Descartes en 2004, le tout premier prix John Stewart Bell en 2009 et le prix Marcel-Benoist en 2014.

La cryptographie, autrement dit l'art de coder des messages, a une longue et fascinante histoire qui remonte à l'Antiquité. Du code de César au chiffrement asymétrique d'aujourd'hui, en passant par la machine Enigma et le code Navajo durant la Deuxième Guerre mondiale, les développements aussi bien dans le chiffrement que dans le déchiffrement ont été constants et les anecdotes innombrables. Cette histoire se poursuit aujourd'hui. Elle est même entrée de plain-pied dans l'ère des technologies quantiques. Les propriétés déroutantes et contre-intuitives de la physique quantique permettent en effet de mettre au point un processus assurant une confidentialité, une authenticité et une intégrité parfaites aux messages transmis entre deux personnes (communément appelées Alice et Bob). Si le dispositif est bien conçu, les lois de la nature rendraient alors impossible toute tentative de décodage, quelle que soit la puissance de calcul à disposition de l'éventuel espion (représenté par Ève).

« JE ME SUIS DIT QUE J'AVAIS LES CONNAISSANCES NÉCESSAIRES ET TOUT CE QU'IL FALLAIT DANS MON LABORATOIRE POUR RÉALISER UNE EXPÉRIENCE DE CRYPTOGRAPHIE QUANTIQUE »

Aujourd'hui, ce genre de dispositifs existe déjà dans la réalité et hors des laboratoires de recherche. La Chine et la Corée du Sud, par exemple, mettent en effet en place des réseaux de cryptographie quantique sur leur territoire par tronçons de fibres optiques d'une ou deux centaines de kilomètres. La Suisse pas encore. Pourtant, la proximité des centres urbains, comme Genève et Lausanne ou Berne et Zurich, en fait un lieu idéal pour ce genre d'infrastructures.

« La technologie, notamment celle de la start-up genevoise ID Quantique, permet aujourd'hui de créer une nouvelle clé quantique par seconde et sur une distance de 100 kilomètres, explique Nicolas Gisin, professeur honoraire à la Faculté des sciences. *On peut donc en changer sans cesse. Habituellement sur Internet, les échanges utilisent une nouvelle clé classique par session. Elle est changée une fois par jour ou une fois par semaine, selon les cas de figure. Mais pour les applications très demandeuses de confidentialité, en particulier dans le domaine financier qui est une des spécialités de la Suisse, il est intéressant de disposer d'un système qui soit remis à jour continuellement. Et c'est là que la cryptographie quantique revêt tout son sens. Si Ève parvient, par miracle, à casser une clé quantique, elle ne pourra intercepter au maximum qu'une seconde de données, ce qui est négligeable. »*

Un autre argument en faveur d'un réseau de cryptographie quantique en Suisse, c'est qu'une de ses institutions, l'Université de Genève, joue un rôle de pionnière dans cette discipline depuis bientôt trente ans, c'est-à-dire depuis presque le début. Rétrospective.

Les débuts C'est le physicien britannique Artur Ekert qui, le premier, décrit concrètement, dans la revue *Physical Review Letters* du 5 août 1991, ce à quoi pourrait ressembler une expérience de cryptographie quantique. L'idée reste d'abord confinée à une petite communauté de spécialistes mais elle parvient assez rapidement aux oreilles de Nicolas Gisin. Sa réaction ne se fait pas attendre.

ADOBE STOCK

«En lisant les quelques articles traitant de ce sujet, je me suis dit que j'avais les connaissances nécessaires et tout ce qu'il fallait dans mon laboratoire pour réaliser une expérience de cryptographie quantique», se rappelle-t-il. Il en fait rapidement un axe de sa recherche.

Le profil du chercheur genevois est unique à cette époque. Il possède en effet une formation en physique quantique ainsi qu'une expérience de cinq ans dans l'industrie des télécommunications, qui lui a permis de se familiariser avec le maniement des fibres optiques et les effets de polarisation de la lumière qui les traverse. Il dispose également dans son laboratoire de détecteurs de photons capables de mesurer ces grains de lumière individuellement. C'est grâce à eux qu'il bricole l'une des premières démonstrations expérimentales de cryptographie quantique.

Clé de cryptage L'équipe qu'il dirige parvient en effet à transmettre un embryon de clé de cryptage – celle qui sert à coder des messages – à travers un kilomètre de fibre optique, comme elle l'expose dans un article paru dans la revue *Europhysics Letters* du 20 août 1993. Protégée par les lois de la physique quantique et basée sur la polarisation de photons (particules de lumière) qui sont transmis l'un après l'autre, cette clé est parfaitement aléatoire et confidentielle. En d'autres termes, si Ève tente de lire le contenu d'une telle clé, elle ne peut le faire qu'en mesurant les photons, ce qui les détruirait et alerterait du même coup Alice et Bob. Ces résultats font connaître l'équipe genevoise dans le monde de la physique internationale.

Nicolas Gisin et ses collègues cherchent ensuite à perfectionner le système. Ils changent alors de fibres optiques, choisissent celles qui sont exploitées par Swisscom (alors Télécoms PTT) et développent des détecteurs de photons uniques adaptés à ces nouvelles longueurs d'onde. Cette évolution leur permet de sortir la cryptographie quantique du laboratoire. Une première expérience de transmission de clé quantique dans des fibres industrielles, rapportée par la revue *Nature* du 30 novembre 1995, est réalisée sur 23 km, entre Genève et Nyon, en passant sous le lac. La communication quantique entre dans le monde réel.

De l'intrication à la téléportation L'équipe genevoise réalise également des expériences d'intrication quantique, une propriété de la physique quantique potentiellement très intéressante pour la cryptographie quantique. L'intrication désigne ce lien qui peut exister entre deux particules et qui fait qu'une mesure sur la première influence immédiatement l'état de la seconde, comme si elles formaient un seul et même objet alors qu'elles peuvent être éloignées de plusieurs kilomètres l'une de l'autre.

La première preuve expérimentale de l'existence de l'intrication est apportée par le physicien français Alain Aspect en 1982. Mais, comme le rapporte la revue *Science* du 25 juillet 1997, c'est une fois de plus le groupe

de Nicolas Gisin qui se distingue en réalisant la première expérience d'intrication dans des fibres optiques télécoms sur une distance de 10 kilomètres, entre les villages de Bernex et de Bellevue.
La maîtrise du phénomène de l'intrication ouvre la porte à la « téléportation quantique », c'est-à-dire au transfert de l'état physique d'une particule (la valeur de sa polarisation, par exemple) à une autre, par l'entremise d'une paire de particules intriquées (il n'est pas question ici de téléporter de l'énergie ou de la matière mais bien un état quantique).

La quête du répéteur Le principal intérêt de la téléportation quantique est qu'elle est potentiellement capable de résoudre un des problèmes techniques sur lequel bute la cryptographie quantique : la distance. En effet, s'il est désormais possible de créer des clés de chiffrement parfaitement aléatoires et de les transmettre de manière totalement confidentielle entre deux interlocuteurs, les propriétés quantiques se perdent dans les fibres optiques et au bout de quelques centaines de kilomètres. La nécessité d'une amplification du signal se fait donc sentir.
« *Le souci, c'est que les effets quantiques ne peuvent être amplifiés*, précise Nicolas Gisin. *La téléportation quantique permet en revanche de concevoir des « répéteurs ». Grâce à eux, la communication quantique pourrait s'allonger et traverser des distances beaucoup plus importantes qu'aujourd'hui.* »
Jamais à la traîne, l'équipe genevoise parvient, en 2003, à réaliser la première téléportation quantique à longue distance dans des fibres optiques télécoms (2 kilomètres), dont les résultats paraissent dans la revue *Nature* du 30 janvier de la même année. Quelques années après, Nicolas Gisin et ses collègues réussissent à « stocker » durant une microseconde le premier membre d'une paire de photons intriqués dans un cristal composé de centaines de millions d'atomes refroidis à l'extrême et à le récupérer ensuite, sans que son intrication avec le deuxième ait été rompue. Un dispositif, présenté dans la revue *Nature* du 27 janvier 2011, qui commence à ressembler furieusement au premier prototype d'un « répéteur quantique ». Un tel prototype n'existe pas encore mais des progrès considérables ont été accomplis, en particulier dans les laboratoires de physique genevois. Le problème principal des dispositifs expérimentaux actuels, fonctionnant à une température proche du zéro absolu, c'est qu'ils manquent d'efficacité. Et augmenter cette dernière s'avère techniquement très difficile.

Même si la cryptographie quantique a fait des progrès fulgurants ces dernières décennies, son équivalent classique n'a évidemment pas encore dit son dernier mot. Certaines équipes essayent ainsi de développer une cryptographie classique dite « post-quantique ». Elle serait à l'épreuve des ordinateurs quantiques (qui seraient théoriquement capables de casser en un temps raisonnable n'importe quelle clé de chiffrement classique actuelle). « *Le problème, c'est que l'on ne peut pas prouver que ces nouvelles techniques seront résistantes*, précise Nicolas Gisin. *On peut juste demander aux meilleurs hackers de la planète de tenter de casser ces clés. Même si parmi ces derniers, il y en a très peu qui maîtrisent les ordinateurs quantiques qui, d'ailleurs, n'existent pas encore. Cela n'empêche pas les Américains de pousser, malgré tout, la solution post-quantique dans l'espoir de l'imposer à tout le monde. Les Chinois, qui ont pris une certaine avance dans l'implémentation de la cryptographie quantique justement pour échapper à l'espionnage des États-Unis, ne se plieront cependant jamais à une telle injonction. Ces bisbilles géopolitiques sont l'aspect le plus désagréable de la cryptographie quantique. Mais elles sont inévitables.* »

MÊME SI LA CRYPTOGRAPHIE QUANTIQUE A FAIT DES PROGRÈS FULGURANTS, SON ÉQUIVALENT CLASSIQUE N'A PAS ENCORE DIT SON DERNIER MOT

RECORD DU MONDE

TOUJOURS PLUS LOIN, TOUJOURS PLUS PETIT

LES SCIENTIFIQUES DU DÉPARTEMENT DE PHYSIQUE APPLIQUÉE TRAVAILLENT AU PERFECTIONNEMENT DE LA CRYPTOGRAPHIE QUANTIQUE. **ILS DÉTIENNENT LE RECORD DE DISTANCE** (421 KILOMÈTRES) SUR LAQUELLE CETTE TECHNIQUE A PU ÊTRE MISE EN ŒUVRE. ILS ONT AUSSI RÉUSSI À MINIATURISER UNE PARTIE DU DISPOSITIF DANS UNE PUCE DE MOINS D'1 MILLIMÈTRE.

Hugo Zbinden
Professeur associé au Département de physique appliquée, Faculté des sciences

Formation: Il obtient son doctorat à l'Université de Berne en 1991. Il rejoint le Département de physique appliquée en 1993. En tant que maître d'enseignement et de recherche, il y dirige les activités expérimentales du groupe.

Parcours: Nommé professeur associé en 2012, il reçoit, entre autres, en 2016 le prix Heinrich Greinacher de l'Institut de physique de l'Université de Berne et la Médaille de l'innovation de l'Université de Genève en 2017 en tant que cofondateur de la start-up ID Quantique.

Dans les systèmes de communication quantique, l'élément essentiel est ce qu'on appelle la distribution d'une clé quantique (QKD, pour *Quantum key distribution*) entre deux interlocuteurs fictifs (appelés par convention Alice et Bob). Et le record du monde de la plus grande distance sur laquelle une telle distribution a pu avoir lieu dans une seule fibre optique est détenu par l'équipe d'Hugo Zbinden, professeur associé au Département de physique appliquée (Faculté des sciences). Dans un article paru le 5 novembre 2018 dans la revue *Physical Review Letters*, lui et ses collègues, dont Alberto Boaron, premier auteur de l'article, présentent en effet une expérience de QKD à travers 421 kilomètres de fibre optique, battant ainsi le record précédent de 404 km obtenu par des chercheurs chinois en 2016. L'équipe genevoise a pu repousser les limites de l'exercice en optimisant toutes les parties du système. Elle a recouru à des fibres optiques de nouvelle génération transmettant plus efficacement la lumière à de nouveaux détecteurs de photons uniques dans leur conception et à une nouvelle méthode d'encodage des signaux quantiques permettant de simplifier le dispositif expérimental tout en préservant son efficience. Elle a aussi augmenté le taux de génération des états quantiques pour atteindre 2,5 GHz, ce qui signifie que 2,5 milliards de signaux sont envoyés par seconde.

LE RECORD DES PHYSICIENS GENEVOIS REPRÉSENTE UNE ÉTAPE IMPORTANTE EN VUE D'UN RÉSEAU DE COMMUNICATION QUANTIQUE ENTRE LES VILLES EUROPÉENNES

Les clés de cryptage quantiques sont inviolables. Cette infaillibilité est basée sur les lois de la physique quantique qui stipulent qu'il est impossible de copier un objet (état) quantique sans le perturber. Les deux utilisateurs s'échangent des états quantiques via des photons dans lesquels sont encodées des informations. Si un tiers tente d'intercepter cette communication, il introduit nécessairement des erreurs et dévoile immédiatement sa présence. La distance de transmission obtenue par les physiciens genevois représente une étape importante en vue de l'établissement d'un réseau de communication quantique entre les villes, par exemple à l'échelle européenne.

Par satellite « *Pour être honnête, depuis notre record, d'autres groupes dans le monde ont couvert des distances plus grandes*, précise Hugo Zbinden. *Mais ils l'ont fait à l'aide d'un dispositif très différent, avec une source de photons située entre deux portions de fibres optiques distinctes, ce qui permet tout de suite de diminuer les pertes et de doubler la distance. Ce système est vraiment plus complexe que le nôtre et difficile à mettre en œuvre. Il n'est pas sûr qu'il représente un réel avantage.* » Une équipe chinoise a ainsi pu atteindre une distance de 600 km (ou plutôt deux fois 300 km), selon l'article paru le 7 juin 2021 dans *Nature Photonics*.

Il convient de citer également le fait qu'une autre équipe chinoise a réussi à transférer une clé quantique entre deux stations terrestres (une en Autriche et l'autre en Chine) en passant par un satellite, baptisé Micius, spécialement conçu pour cela. Dans ce cas de figure, il est nécessaire de faire « confiance » au satellite, qui connaît la clé de cryptage. Pour résoudre ce problème, les chercheurs chinois ont répété l'expérience entre deux stations séparées de 1203 kilomètres à l'aide d'une source de paires de photons intriqués embarquée sur le satellite. Dans l'idée d'une généralisation de la cryptographie quantique à toutes les

Vue d'Alice, le nom donné à la partie de l'expérience de cryptographie quantique qui envoie la clé de codage à son interlocuteur, Bob. Ce qui encombrait il y a quelques années encore une table optique entière (atténuateurs, modulateurs, miroirs, lentilles, coupleurs, interféromètres…) est désormais confiné dans le « chip » doré, visible ci-contre.

communications et donc à celles qui passent par les réseaux de satellites, cela représente une étape importante (d'autres agences spatiales développent d'ailleurs leurs propres projets). Mais pour l'instant, de tels satellites sont très chers, le taux de génération de clés quantiques est très faible et l'instrument, placé en orbite basse, se déplace très vite (il fait le tour de la Terre en une heure environ), laissant peu de temps pour la transmission.

Miniaturisation En attendant, sur Terre, Hugo Zbinden et ses collègues poursuivent leurs efforts de perfectionnement du dispositif de QKD. Leur attention se porte actuellement sur la miniaturisation des composants optiques. Ce qui pouvait encombrer il y a quelques années encore une table optique entière (atténuateurs, modulateurs, miroirs, lentilles, coupleurs, interféromètres…) a ainsi pu être rangé dans un circuit intégré tellement petit qu'il est à peine visible. Tout n'a pas encore pu être miniaturisé de la sorte mais le gain de volume est déjà spectaculaire. Le laser est encore externe par exemple, mais il est de toute façon déjà très petit. Le tout tient dans une petite boîte et c'est désormais la connectique et les appareils informatiques de pilotage qui prennent le plus de place.

UN AUTRE AXE DE RECHERCHE DU LABORATOIRE VISE À L'AUGMENTATION DE LA QUALITÉ DU HASARD PRODUIT PAR UN DISPOSITIF QUANTIQUE

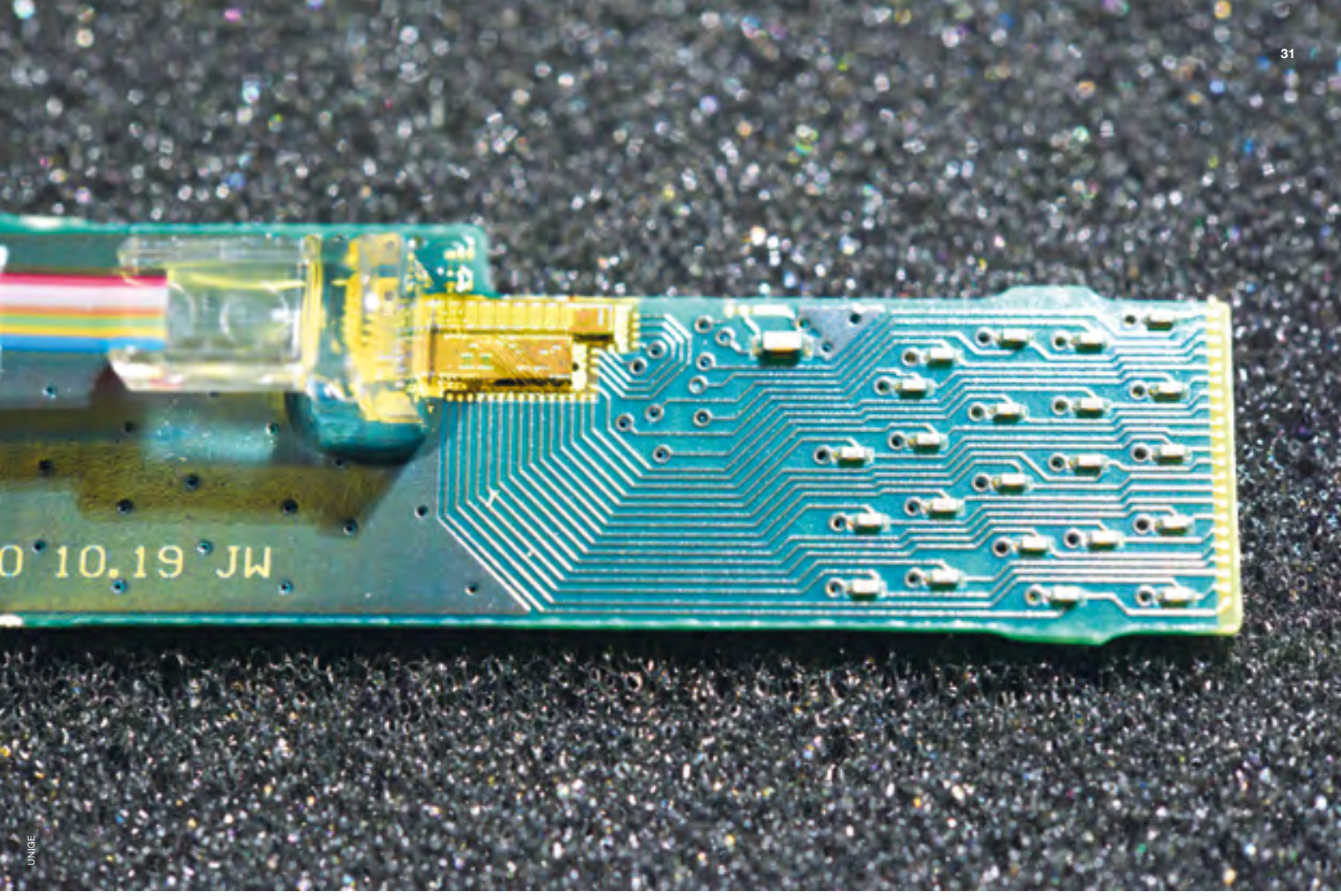
La puce est conçue par une entreprise de design de circuits intégrés et fabriquée par une fonderie en Europe. C'est un changement majeur car jusqu'à présent, le groupe a toujours développé et contrôlé toutes les parties de ses dispositifs de communication quantique. *« Maintenant, si le « chip » a un défaut, ce qui arrive, il nous est évidemment impossible d'aller voir à l'intérieur et de le réparer*, précise Rebecka Sax, qui prépare sa thèse sous la direction d'Hugo Zbinden. *Il nous faut en commander un autre. Un processus qui prend à chaque fois six mois.* »

Du plus beau hasard Un autre axe de recherche du laboratoire vise à l'augmentation de la qualité du hasard produit par un dispositif quantique. C'est en effet un générateur de nombres aléatoires (fabriqué par ID Quantique, la spin-off de l'UNIGE, *lire aussi en page 34*), basé sur les propriétés quantiques des particules élémentaires, en l'occurrence des photons, qui permet de créer des clés de cryptage de manière parfaitement aléatoire.

Cette perfection a été démontrée par les tests statistiques les plus sophistiqués. Ces tests ont néanmoins leurs limites. En réalité, les chercheurs font confiance à la théorie quantique pour prétendre à cette perfection. Le processus physique utilisé dans les générateurs de nombres aléatoires produit, par définition, du hasard parfait. Mais cela n'est valable dans le monde réel que si l'appareil qui l'exploite est suffisamment bien conçu. Pour dire les choses autrement : le doute subsiste.

Pour le dissiper, les physiciens et physiciennes de l'UNIGE ont inventé un système qui améliore un générateur de nombres aléatoires de manière à ce qu'il puisse mesurer ven direct la qualité du hasard qu'il produit lui-même. Le système permet ensuite d'opérer une sélection dans les données que le générateur fournit pour garantir un hasard parfait à 100 %.

Ce travail, réalisé dans le cadre du projet QRange du Flagship Quantique de l'Union européenne, dirigé par Hugo Zbinden, est arrivé à sa fin. Désormais exclus de ce programme *(lire l'article d'ouverture du dossier)*, les « quantiques » suisses devront à l'avenir jouer leur partition en solo.



UNIGE

QUELQUES NOTIONS DE CRYPTOGRAPHIE QUANTIQUE GENEVOISE

La cryptographie quantique se base sur des lois de la physique quantique qui ont été maintes fois vérifiées en laboratoire. L'une d'entre elles affirme qu'il est impossible d'effectuer une mesure d'un système quantique (une simple particule, par exemple) sans le perturber, voire le détruire. Dans l'idée de transmettre un message secret, cela est bien utile, puisque si un espion (dénommé Ève) désire l'intercepter, il alerterait immédiatement les deux interlocuteurs (Alice et Bob).

Dans le dispositif original de cryptographie quantique mis au point au Département de physique appliquée (Faculté des sciences), le système de cryptage se base sur des paires d'impulsions laser ultracourtes, séparées l'une de l'autre de 200 picosecondes (millièmes de milliardième de seconde, de sorte qu'on peut juste distinguer leur temps d'arrivée.

L'intensité de la paire d'impulsions laser est tellement atténuée qu'il n'y a, en général, pas plus d'un seul photon. Celui-ci est présent soit dans la première, soit dans la seconde impulsion. Ce sont les deux états possibles du petit système quantique qui est transmis d'Alice à Bob. L'un correspond à un 1 et l'autre à un 0.

À cela s'ajoute un troisième état, un peu spécial, indéterminé, dans lequel le photon se trouve dans les deux états à la fois. Un peu comme si les deux impulsions étaient « à moitié » remplies, comme le permet la physique quantique. Cet état n'a été imaginé que pour induire Ève en erreur et dévoiler sa présence si l'idée lui venait d'intercepter la transmission de la clé.

Le processus se déroule ensuite en plusieurs étapes.

Au moment de créer une clé de cryptage, Alice prépare l'état de chaque photon avant de l'envoyer à Bob. Il peut s'agir de l'état 1, 0 ou indéterminé. C'est un générateur de nombres aléatoires, basé sur la nature totalement indéterminée d'une valeur physique du photon, qui permet de définir la séquence. Cette dernière n'est le résultat d'aucun logiciel mais bien le fruit du parfait hasard. Il est impossible de casser une telle clé, surtout si celle-ci est au moins aussi longue que le message à coder.

ENVOI D'ALICE	MESURE DE BOB DANS LA base **X**	base **Z**
▮ _	1	Rien
_ ▮	0	Rien
▮ ▮	1 ou 0	OK

▮ photon dans une impulsion
▮ ▮ photon dans les deux impulsions à la fois

Bob, de son côté, mesure les paires d'impulsions et note leur ordre d'arrivée. Il peut effectuer la mesure soit dans la base (**X**) qui permet de détecter les états 1 et 0 (l'état indéterminé fournit dans ce cas lui aussi un 1 ou un 0, mais de manière totalement aléatoire), soit dans la base (**Z**) qui permet de déterminer si la paire d'impulsions se trouve ou non dans le troisième état.

Dans la première base, il mesure simplement le temps d'arrivée de l'impulsion, à partir duquel il détermine s'il s'agit de la première ou de la seconde impulsion à l'intérieur de la paire. Dans la seconde, il utilise un autre type de mesure, basée sur l'interférométrie. Il ne peut pas mesurer dans les deux bases à la fois. Il les choisit au hasard.

Il conserve tous les 1 et les 0 obtenus avec la première base et néglige tous les autres résultats (dont les erreurs). Il envoie à Alice les temps d'arrivée des 1 et 0 retenus ainsi que la séquence des bases qu'il a utilisées pour effectuer ces mesures. Ces informations peuvent transiter publiquement, sans aucune précaution, puisqu'elles ne fournissent aucune indication sur l'ordre des 1 et des 0 retenus par Bob.

Alice envoie en retour les détections que Bob peut garder et celles qu'il doit enlever (dont celles correspondant aux états indéterminés et dont elle ne peut pas connaître le résultat obtenu par Bob).

À partir de là, Alice et Bob peuvent reconstituer la même clé. Cette opération, qui a l'air fastidieuse, est réalisée 2,5 milliards de fois par seconde. Dès que la clé a la longueur désirée, Alice encode son message et l'envoie à Bob qui peut le décoder. Aucun ordinateur au monde ni aucun espion ne pourra en décrypter le contenu.

Si Ève tente malgré tout d'intervenir au moment où la clé est élaborée, lors de l'échange de photons, elle perturbe inévitablement la communication. Bob et Alice n'ont alors qu'à choisir une séquence prise au hasard de la clé qu'ils ont fabriquée et la comparer pour voir si des incohérences apparaissent. Ève ne peut pas non plus réinjecter dans le canal quantique établi entre Alice et Bob un photon identique à celui qu'elle a espionné et donc détruit. Car si elle mesure le photon alors qu'il se trouve dans son état indéterminé, elle ne peut pas le reconnaître en tant que tel puisque sa mesure fournira forcément un 1 ou un 0, lois de la quantique obligent.

Alors bien sûr, si quelqu'un espionne directement ce qu'Alice tape sur son clavier, par exemple à l'aide de méthodes aussi sophistiquées que l'analyse fine des vibrations de la fenêtre générées par le bruit des touches, toute cette technologie perd de son intérêt. Mais quel genre de cachottière serait Alice si elle prenait le risque de se confier depuis une pièce aussi exposée ?

RELAIS QUANTIQUE

RÉPÉTITION GÉNÉRALE

LA CRYPTOGRAPHIE QUANTIQUE PAR FIBRE OPTIQUE EST AUJOURD'HUI LIMITÉE À QUELQUES CENTAINES DE KILOMÈTRES. **LA SOLUTION POUR ALLER PLUS LOIN PASSE PAR DES RÉPÉTEURS QUANTIQUES** MAIS LEUR CONCEPTION REPRÉSENTE UN DÉFI TECHNOLOGIQUE CONSIDÉRABLE

OLIVIER ZIMMERMANN

Expérience d'activation d'une mémoire quantique. Le laser jaune sert à manipuler les atomes pendant le processus de stockage. Le cristal qui sert à stocker les photons se trouve à l'intérieur du boîtier (haut de l'image).

Aujourd'hui, il est possible d'utiliser la cryptographie quantique en conditions réelles (hors laboratoire) dans une fibre optique d'une longueur de quelques centaines de kilomètres. Au-delà, les photons se perdent et le signal s'amenuise. Comme on ne peut pas copier ou amplifier ce même signal quantique, sous peine de le détruire (c'est le propre d'un état quantique et c'est aussi ce qui assure la confidentialité de la transmission), il est nécessaire de développer des sortes de relais. Exploitant eux aussi les caractéristiques quantiques de la matière, ceux-ci doivent être capables de répéter le signal de loin en loin afin de pouvoir le diffuser sur de plus longues distances. Ce qui est exactement le domaine de recherche de Mikael Afzelius, maître d'enseignement et de recherche au Département de physique appliquée (Faculté des sciences).

« *En 2008, nous avons imaginé une méthode qui nous permettrait de fabriquer une mémoire quantique et de l'utiliser comme répéteur dans un réseau de communication quantique*, explique-t-il. *Depuis, nous travaillons sans relâche à la réaliser.* »

LE PROBLÈME, C'EST QU'IL FAUT QUE LE STOCKAGE DURE ASSEZ LONGTEMPS POUR PERMETTRE LA CRÉATION D'UNE INTRICATION ENTRE TOUT UN RÉSEAU DE MÉMOIRES

Le système imaginé par le chercheur exploite l'intrication, un phénomène purement quantique et largement contre-intuitif. Il désigne le fait que deux photons, par exemple, peuvent être corrélés : une action sur l'un engendre un effet immédiat sur l'autre, qu'ils soient éloignés d'un millimètre ou de plusieurs kilomètres et alors qu'aucun lien tangible ne les unit. Deux photons intriqués peuvent être considérés comme deux manifestations, à deux endroits différents, d'un seul objet. Un concept de « non-localité » qui n'existe pas dans le monde classique et qui permet notamment de réaliser de la cryptographie quantique.

Mémoires intriquées L'objectif consiste donc à créer une paire de photons intriqués et à les acheminer chacun vers une mémoire quantique. Une fois à l'intérieur de ce solide, le photon transfère son état quantique, y compris son intrication, à un grand nombre d'atomes du cristal avant de disparaître. Au final, il ne reste que deux mémoires quantiques intriquées entre elles. Le problème, c'est qu'il faut que le stockage dure assez longtemps pour permettre la création d'une intrication entre tout un réseau de mémoires.

Les physiciens genevois ont réalisé des progrès importants dans ce domaine. Il y a dix ans, ils réussissent, pour la première fois, à stocker un photon intriqué durant 100 nanosecondes (milliardièmes de seconde). En 2017, la marque atteint une microseconde, soit 10 000 fois mieux. Et l'équipe genevoise est sur le point de publier le temps record d'un dixième de seconde.

« *Pour un état quantique, c'est une éternité*, commente Mikael Afzelius. *Mais notre objectif pour les années à venir, dans l'optique de réaliser un jour un réseau de communication quantique, c'est d'atteindre un stockage qui tienne le coup une dizaine de secondes et de le réaliser à bonne distance, typiquement après une dizaine de kilomètres de fibre optique.* »

Des milliers de photons à la fois Le temps de stockage et la distance ne sont pas les seuls défis technologiques à relever. Le dispositif doit aussi atteindre une bonne efficacité et, surtout, pouvoir stocker des milliers de photons en même temps. Et cela, c'est encore de la musique d'avenir.

L'équipe de Mikael Afzelius travaille actuellement avec des mémoires quantiques constituées de cristaux dopés avec de petites quantités de terres rares comme l'ytterbium et l'europium. L'expérience est maintenue à une température très basse, à 3 ou 4 degrés au-dessus du zéro absolu (-273,15 °C), afin de pouvoir conserver l'intégrité des états quantiques. En effet, dès que la température monte à 10° au-dessus du zéro absolu, l'agitation thermique dans le cristal devient suffisante pour détruire l'intrication des atomes.

« *Les répéteurs quantiques serviront à porter la cryptographie quantique sur des distances plus grandes que quelques centaines de kilomètres*, explique Mikael Afzelius. *Mais ils pourront aussi contribuer à ce qu'on appelle l'Internet quantique. Il s'agit d'un réseau qui connecterait les futurs ordinateurs quantiques entre eux et permettrait de les faire fonctionner en parallèle. Et donc de multiplier d'autant plus leur puissance de calcul.* »

Mikael Afzelius
Maître d'enseignement et de recherche au Département de physique appliquée, Faculté des sciences

Formation : En 2004, il obtient sa thèse à l'Université de Lund, en Suède. Il rejoint alors l'Université de Genève.

Parcours : Il obtient un poste de maître d'enseignement et de recherche au Département de physique appliquée en 2007.

ENTREPRISE

ID QUANTIQUE, À LA CONQUÊTE DE L'ESPACE ET DES SMARTPHONES

LA START-UP SPÉCIALISÉE DANS LA COMMUNICATION QUANTIQUE, NÉE IL Y A EXACTEMENT VINGT ANS À L'UNIVERSITÉ DE GENÈVE, EST **UNE VÉRITABLE «SUCCESS-STORY»**. RÉCIT

Grégoire Ribordy
Directeur d'ID Quantique

Formation: Titulaire d'une thèse sur la cryptographie quantique expérimentale en 2000 et d'un certificat de gestion d'entreprise à l'Université de Lausanne.

Parcours: Avec Nicolas Gisin et Hugo Zbinden, il fonde ID Quantique qu'il dirige encore aujourd'hui. L'entreprise emploie une centaine de personnes dans le monde. Elle a remporté plusieurs prix, dont la Médaille de l'innovation de l'Université de Genève en 2017 et le Prix de l'innovation de la Chambre de commerce et d'industrie de Genève en 2019.

Vingt ans d'âge, 85 employés à Carouge (une centaine dans le monde), des revenus cumulés atteignant plus de 100 millions de francs: ID Quantique, la start-up issue de l'Université de Genève, développe et commercialise des générateurs de nombres aléatoires, des systèmes de cryptographie quantique, des détecteurs de photons uniques: tout ce qu'il faut, en somme, pour mettre en place un système de communication quantique à l'épreuve de toute tentative d'espionnage et, surtout, à la pointe de la technologie. Bref, l'entreprise roule sur la voie du succès. Une voie relativement dégagée jusqu'à présent mais qui s'annonce nettement plus cahoteuse dans les mois, voire les années à venir. La faute à l'éviction de la Suisse des grands programmes de recherche européens (*lire article d'ouverture de dossier*).

«*Nous sommes passés subitement de partenaire à part entière à celui de sous-traitant, voire de fournisseur en équipement*, confirme Grégoire Ribordy, cofondateur et directeur d'ID Quantique. *Comme, en plus, le domaine du quantique est devenu stratégique, au même titre que le spatial, il ne fait aucun doute que l'Europe va chercher à développer des entreprises concurrentes à la nôtre à l'intérieur de ses frontières. Afin de conserver notre position de leader dans notre domaine, nous cherchons donc à nous implanter en Europe, où le marché est plus important qu'en Suisse. Nous ne supprimerons pas de postes en Suisse mais nous en créerons de nouveaux à l'étranger.*»

La situation est d'autant plus paradoxale qu'ID Quantique doit une grande partie de son succès à ces mêmes programmes-cadres européens dont elle est une créature, en quelque sorte, puisqu'elle y a participé en tant partenaire industriel incontournable dans les projets de technologie quantique depuis sa fondation en 2001.

Formation en cachette L'idée de créer une entreprise naît dans la tête de Grégoire Ribordy à la fin des années 1990, alors qu'il n'a pas encore terminé son travail de thèse sur la cryptographie quantique expérimentale à la Section de physique. Au cours de son doctorat, il décide ainsi de suivre en parallèle un certificat de gestion d'entreprise à l'Université de Lausanne. Il le fait en catimini, car il craint que son directeur de thèse Nicolas Gisin, alors professeur au Département de physique appliquée (Faculté des sciences), lui reproche de ne pas consacrer tout son temps à son travail. Crainte infondée car il termine les deux formations avec succès.

«*À la fin de ma thèse, une compagnie américaine déjà active dans les technologies quantiques et intéressée par les travaux du laboratoire est venue nous voir*, se souvient Grégoire Ribordy. *Elle voulait collaborer avec nous et nous acheter une licence afin de pouvoir commercialiser des appareils basés sur nos résultats. Nous avons refusé, car nous aurions perdu le contrôle de nos découvertes. Nous avons préféré tenter l'aventure par nous-mêmes.*»

LE PREMIER NOM IMAGINÉ POUR L'ENTREPRISE EST Q-SEC MAIS IL EST RAPIDEMENT ÉCARTÉ POUR CAUSE DE JEU DE MOTS DOUTEUX

Et c'est ainsi qu'en octobre 2001, Grégoire Ribordy, Nicolas Gisin, aujourd'hui professeur honoraire à la Faculté des sciences, et deux autres chercheurs du département, Hugo Zbinden, actuellement professeur à la Section de physique, et Olivier Guinnard fondent une start-up active dans la technologie quantique. Le premier nom imaginé pour l'entreprise est Q-sec mais il est rapidement écarté pour des raisons de jeux de mots douteux. «*À l'époque, sur la tour de la Télévision suisse romande, qui se trouve juste derrière nos locaux, était affiché en grand le slogan «idée suisse»*, s'amuse Grégoire Ribordy. *Nous l'avons repris pour en faire idée quantique.*»

Le but de la start-up est, bien sûr, de commercialiser des appareils de cryptographie quantique. Mais un tel marché n'existe pas encore. Nicolas Gisin et Grégoire Ribordy décident donc de commencer par les instruments les plus simples à développer dans ce domaine et qui pourraient être utiles pour d'autres applications, à savoir des détecteurs de photons uniques et des générateurs de nombres aléatoires.

Le premier acheteur ne se fait pas attendre. Un laboratoire de l'Université de Boston aux États-Unis passe en effet commande pour un détecteur de photons uniques avant même que la start-up ne soit formellement créée.

Le Cerberis XG (ci-dessus), dernier modèle de distribution de clés quantiques (QKD) d'ID Quantique.

L'instrument, lui, n'existe que sur le papier. Grégoire Ribordy fait néanmoins une offre, accompagnée d'un schéma de l'appareil tel qu'il l'imagine et envoie le tout par fax. Affaire conclue. Les Genevois ont six mois pour produire le détecteur.
« *C'est à ce moment que la montre a commencé à tourner*, raconte Grégoire Ribordy. *Elle ne s'est plus arrêtée depuis.* »

Départ modeste Le premier appareil est livré en 2002 en temps et en heure. Les fonds propres de départ, l'argent encaissé lors de cette première vente et un prix décerné par la Fondation W. A. de Vigier lancent la start-up, même si les sommes engagées sont encore modestes. Les premiers générateurs de nombres aléatoires, assez volumineux au départ, intéressent rapidement les sociétés proposant des jeux de hasard en ligne. Les détecteurs de photons uniques, quant à eux, attirent surtout les laboratoires de recherche.
Durant les premiers mois, ID Quantique bénéficie d'un espace au sein de l'Université de Genève pour mener ses activités de recherche, de développement et de production. En décembre 2003, une première levée de fonds permet de rassembler 1,5 million de francs et ID Quantique déménage à Carouge afin d'intégrer ses propres locaux, après avoir engagé son premier employé en janvier 2003.
Petit à petit, les affaires se développent et, en 2007, ID Quantique est à même de commercialiser un système de distribution de clés quantiques (QKD pour *Quantum Key Distribution*) qui permet de mettre en œuvre, dans la vie réelle, la cryptographie quantique. Entre 2007 et 2015, le système est notamment déployé à Genève dans le cadre des élections fédérales et cantonales pour sécuriser la ligne reliant l'espace de dépouillement d'Uni Mail à son centre de données des Acacias.
« *C'était une expérience fantastique*, se souvient Grégoire Ribordy. *Nous avions mis du temps pour nouer des contacts mais dès que la décision de mettre en place ce système de cryptographie quantique a été prise, nous l'avons fait en un mois. Les autorités nous ont beaucoup aidés. L'idée était d'assurer non seulement la confidentialité des informations mais aussi, et surtout, leur intégrité. L'expérience s'est soldée par un succès mais s'est malheureusement arrêtée d'elle-même au bout de quelques années. Cela dit, elle pourrait tout à fait être réactivée.* »

Dans l'espace Conservant toujours des liens étroits avec les équipes du Département de physique appliquée, ID Quantique participe à différents records du monde de distance pour la distribution de clés quantiques : 307 kilomètres en 2014, puis 421 km en 2018.
En 2017, ArianeGroup sélectionne l'instrumentation de la start-up genevoise – y compris un ensemble de détecteurs de photons uniques supraconducteurs à haute sensibilité et ultrarapides – pour être intégrés aux équipements de test au sol dédiés au lanceur Ariane 6, dont le premier tir est prévu pour 2022.
Tout aussi spectaculaire est l'intégration, dans un modèle de téléphone mobile sud-coréen Samsung, d'un générateur de nombres aléatoires miniaturisé en une puce de 2 millimètres de côté. Le dispositif peut être utilisé par les applications téléchargées sur le smartphone (pour l'instant exclusivement sur Android) et permet de produire des clés de cryptage parfaites en vue de sécuriser la transmission de certaines informations sensibles entre le téléphone et des serveurs distants.
La production de ces petits générateurs est réalisée avec des partenaires en Corée du Sud qui disposent du savoir-faire nécessaire dans le secteur des semi-conducteurs. Elle pourrait passer rapidement de quelques centaines de milliers d'unités à plusieurs millions. D'autant plus qu'un deuxième « modèle quantique », le Samsung Galaxy Quantum 2, est sorti en avril 2021.
Toujours en Corée du Sud, ID Quantique collabore avec le principal opérateur de télécommunications, SK Telecom, (qui a récemment investi 65 millions de dollars dans l'entreprise genevoise) pour déployer un réseau de communication quantique à l'échelle nationale et relier ainsi une quarantaine de sites officiels du gouvernement. En dehors de ce qui se fait en Chine, il s'agit du plus important réseau de communication quantique au monde.
« *La taille de ce pays est idéale pour ce genre d'infrastructure*, précise Grégoire Ribordy. *Les différents sites gouvernementaux sont éloignés les uns des autres de 100 kilomètres maximum, ce qui est la distance typique sur laquelle on peut propager la cryptographie quantique. Ils peuvent donc jouer le rôle de relais de confiance entre deux tronçons parfaitement sécurisés, en attendant le développement des premiers répéteurs quantiques encore à l'étude* (lire article en page 32). »
Plus petite et plus densément peuplée que la Corée du Sud, la Suisse pourrait d'ailleurs s'en inspirer pour lancer un projet similaire.

ADOBE STOCK

Cryostat servant à refroidir l'ordinateur quantique expérimental d'IBM à une quinzaine de degrés au-dessus du zéro absolu (-273,15 °C).

MAÎTRISE DES QUBITS

L'ORDINATEUR QUANTIQUE EST À LA CROISÉE DES CHEMINS

IL EXISTE DÉJÀ DES ORDINATEURS QUANTIQUES MAIS ILS SONT ENCORE TROP PETITS POUR ÊTRE CAPABLES DE SURPASSER LEURS HOMOLOGUES CLASSIQUES. **LE POTENTIEL DE TELLES MACHINES EST TOUTEFOIS ÉNORME**. LES DÉFIS SCIENTIFIQUES ET TECHNOLOGIQUES POUR LES DÉVELOPPER LE SONT TOUT AUTANT.

Depuis des décennies, la puissance des ordinateurs classiques suit une progression vertigineuse. Cela ne suffira cependant probablement jamais pour résoudre certains problèmes identifiés par les scientifiques et les ingénieurs. Qu'il s'agisse de factoriser un (très, très) grand nombre en nombres premiers, de prévoir la structure électronique et les propriétés dynamiques des molécules et matériaux complexes, de simuler un système quantique comprenant plus qu'une cinquantaine de particules libres ou encore d'optimiser le trajet du commis voyageur visitant un certain nombre de villes (problème emblématique de la théorie de la complexité), les machines classiques pourraient, en effet, ne jamais faire l'affaire. Il manque souvent la méthode, analytique ou numérique, pour venir à bout de ces systèmes complexes en des temps inférieurs à celui de l'âge de l'Univers.

Les ordinateurs quantiques, eux, pourraient y arriver. À condition bien sûr qu'ils atteignent un stade de développement technologique suffisant. Ce qui n'est pas encore le cas. « *Nous nous trouvons à la croisée des chemins*, estime Thierry Giamarchi, professeur au Département de physique de la matière quantique (Faculté des sciences). *Il existe déjà des ordinateurs quantiques mais de taille encore très modeste. Le potentiel de ces machines est phénoménal. Les défis scientifiques et, surtout, technologiques à relever le sont cependant tout autant.* »

Le principe de fonctionnement des ordinateurs quantiques diffère grandement des machines ordinaires. Tandis que la plus petite unité de stockage d'information classique est un « bit » valant 1 ou 0, son équivalent quantique est un « qubit ». Ce dernier, possédant des propriétés quantiques, n'a pas une valeur déterminée mais correspond à une combinaison, ou plus précisément une superposition, d'un 1 et d'un 0, chacune de ces deux valeurs étant, en plus, associée à un « poids », ou à une sorte de probabilité de survenir en cas de mesure. Le qubit vaut donc toutes les valeurs comprises entre 1 et 0 à la fois.

Un qubit tout seul ne sert à rien, pas plus qu'un bit d'ailleurs. Mais on peut en préparer plusieurs et les intriquer, ce qui, en langage quantique, signifie qu'ils sont fortement corrélés les uns avec les autres.

Dans le monde classique, une série de trois bits ne peut prendre qu'une seule valeur sur les huit possibles, telle « 101 ». Dans le monde quantique, en revanche, trois qubits intriqués sont décrits par une seule « fonction d'onde » qui contient toutes les valeurs possibles à la fois (000, 001, 010, 011, 100, 101, 110 et 111), chacune étant associée à une certaine probabilité. Cela signifie que le système quantique peut traiter toutes les possibilités simultanément. En augmentant le nombre de qubits, on augmente le nombre de combinaisons de manière exponentielle. Ainsi, un système quantique de 50 qubits compte plus d'un million de milliards de configurations possibles.

Massivement parallèle « *L'idée de génie est d'avoir imaginé agir sur un ensemble de qubits de telle manière à pouvoir effectuer un grand nombre d'opérations logiques en même temps*, explique Thierry Giamarchi. *C'est comme si l'on avait un ordinateur massivement parallèle. Dès que toutes les opérations, programmées par un algorithme spécial, sont achevées, le système, toujours intriqué, est décrit par une fonction d'onde sur laquelle on pourrait effectuer une mesure qui fournirait le résultat recherché. Cela représente une accélération gigantesque de la capacité de calcul.* »

En théorie, même si le principe de fonctionnement est contre-intuitif, ça marche très bien. D'ailleurs, des chercheurs ont commencé à développer des logiciels quantiques avant même que le premier ordinateur de ce type ne voie le jour. L'un des premiers d'entre eux est celui du mathématicien américain Peter Shor qui a montré, en 1994, qu'un ordinateur quantique pourrait casser la clé de cryptage la plus sophistiquée de l'époque en un temps raisonnable (une réussite précoce qui a d'ailleurs immédiatement dopé l'intérêt pour la cryptographie quantique qui, elle, est à l'épreuve de n'importe quel ordinateur quantique).

En pratique, c'est un peu plus compliqué. Le premier défi, et pas des moindres, consiste à fabriquer des qubits. Plusieurs voies sont explorées : des systèmes avec des ions piégés, avec des semi-conducteurs, avec des supraconducteurs, etc.

Thierry Giamarchi

Professeur au Département de physique de la matière quantique, Faculté des sciences

Formation : Diplômé de l'École normale supérieure de Paris, il obtient son doctorat à l'Université Paris XI en 1987. Membre permanent du CNRS depuis 1986, il effectue un post-doctorat aux Laboratoires Bell, aux États-Unis.

Parcours : Lauréat du prix Anatole et Suzanne Abragam de l'Académie des sciences française en 2000, il est nommé en 2002 professeur au Département de la matière condensée. Il est notamment l'auteur d'une monographie « Quantum physics in one dimension ».

L'essentiel consiste à avoir des « objets » assez petits et assez froids pour pouvoir révéler leur nature quantique et l'exploiter. Ces qubits, qu'il s'agisse d'atomes froids ou de jonction supraconductrice, doivent aussi être intriqués de manière à former un objet unique ou cohérent.

« *Or, le plus grand ennemi d'un ordinateur quantique est la décohérence*, souligne Thierry Giamarchi. *Aucun système, aucune opération, n'est parfait. Il y a des sources de bruits extérieures (des ondes essentiellement) que l'on ne maîtrise pas. Et le problème, c'est qu'une fonction d'onde qui comprend beaucoup de qubits intriqués entre eux est incroyablement fragile. La moindre perturbation ou la moindre erreur dans le dispositif lui-même risque de provoquer sa décohérence et de rendre toute l'opération de calcul caduque.* »

Le paradoxe, c'est qu'il faut à la fois protéger les qubits de l'influence extérieure afin de conserver leur intégrité et pouvoir les manipuler individuellement, avec un laser, un champ magnétique ou un courant électrique infime, afin d'effectuer des opérations logiques.

UN SYSTÈME QUANTIQUE DE 50 QUBITS COMPTE PLUS D'UN MILLION DE MILLIARDS DE CONFIGURATIONS POSSIBLES

Avantage quantique Il existe déjà des prototypes d'ordinateur quantique. Leur puissance de calcul, par contre, n'a pas encore convaincu la communauté scientifique. Le Sycamore de Google est probablement l'une des machines les plus abouties à ce jour. Il est formé d'un processeur de 54 qubits supraconducteurs (dont un défectueux). Selon l'article qui le présente, paru dans la revue *Nature* du 23 octobre 2019, le Sycamore aurait réalisé en 200 secondes une tâche qui aurait pris 10 000 ans au meilleur supercalculateur classique de la planète. IBM, le grand rival de Google dans la course à l'ordinateur quantique, a immédiatement répondu que cette tâche – sans intérêt scientifique mais spécialement adaptée au fonctionnement d'un ordinateur quantique – pouvait en fait être réalisée en quelques jours seulement avec un microprocesseur classique à condition d'utiliser le bon logiciel.

« *Ce qui a vraiment écorné l'annonce de Google, c'est le travail d'une équipe de l'Université de Grenoble*, précise Thierry Giamarchi. *Ces chercheurs ont en effet montré que si le résultat du calcul effectué par le Sycamore avait été très précis, Google aurait eu raison de revendiquer ce qu'on appelle de manière peu élégante la « suprématie quantique », un terme auquel je préfère « avantage quantique ». Mais, en réalité, le résultat publié est entaché d'une certaine marge d'erreur. Du coup, si on accepte une telle imprécision, alors on peut effectuer la même tâche plus rapidement avec un ordinateur portable et un logiciel très bien conçu.* »

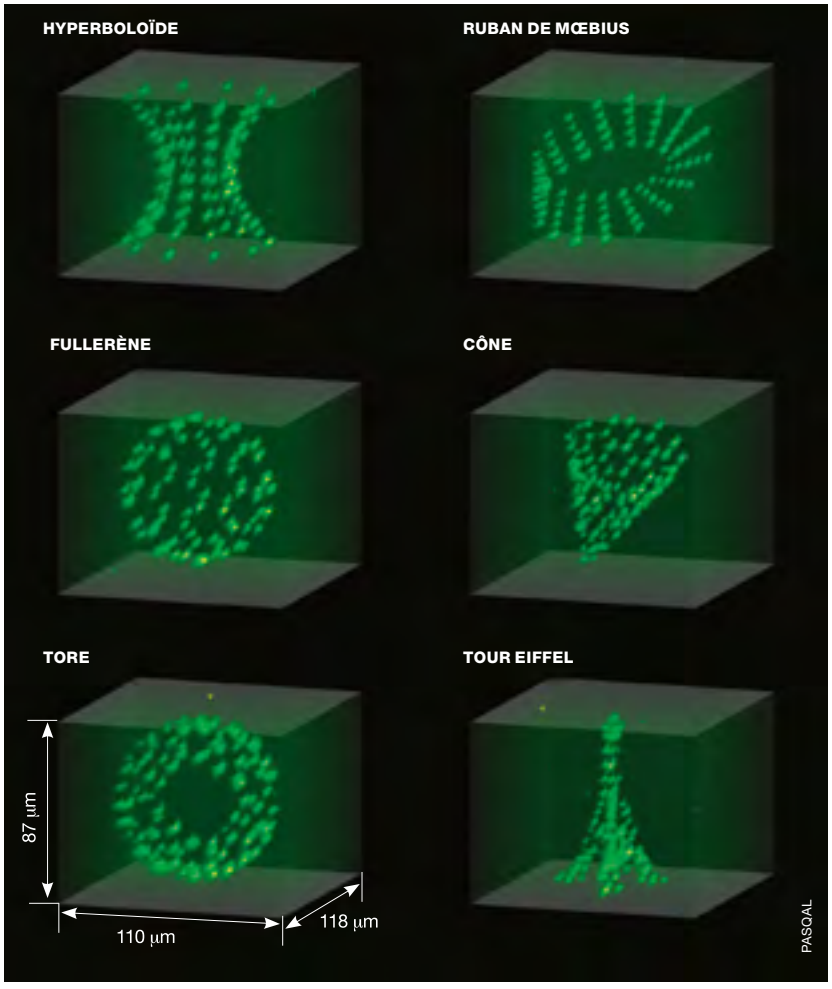
Car un autre problème inhérent aux ordinateurs quantiques est celui de la correction d'erreurs, lesquelles peuvent survenir à tout moment dans le processus de calcul. À cause des propriétés de la mécanique quantique, il est impossible de copier une fonction d'onde afin de la mettre en mémoire. Les ingénieurs ont donc dû se résoudre à consacrer, pour chaque qubit fonctionnel, un certain nombre de qubits supplémentaires destinés à la seule correction de ces erreurs.

Le Sycamore n'est pas le seul prototype d'ordinateur quantique. De son côté, IBM développe une machine concurrente (Quantum System One) qui comptait 27 qubits en 2019. Une équipe chinoise a également présenté un ordinateur quantique « photonique », le Jiuzhang, de 76 qubits dans la revue *Science* du 18 décembre 2020. L'une des limites de cette dernière machine, cependant, est qu'elle est conçue pour n'effectuer qu'un seul type de tâche tandis que l'ordinateur quantique de Google pourrait être programmé pour exécuter une variété d'algorithmes.

Plusieurs laboratoires disposent par ailleurs de leurs propres machines ou plateformes quantiques. L'École polytechnique fédérale de Zurich, par exemple, utilise actuellement des calculateurs quantiques comptant jusqu'à 17 qubits. Elle et l'Institut Paul Scherrer ont créé cette année un *Quantum computing hub* dont l'objectif est le développement d'un ordinateur quantique de 100 qubits.

« *La recherche dans ce domaine, scientifique autant que technologique, avance vraiment rapidement*, note Thierry Giamarchi. *Si on arrive à doubler (au grand minimum) le nombre de qubits par rapport à ce qui se fait de mieux aujourd'hui, à les rendre le plus robustes possible, à bien corriger les erreurs, alors les ordinateurs quantiques devraient pouvoir faire la preuve de leur utilité, à savoir résoudre des problèmes intéressants. J'ignore si l'effort international consenti dans ce domaine accouchera un jour d'un véritable ordinateur quantique qui tienne toutes ses promesses. En revanche, je suis sûr qu'il en sortira de toute façon quelque chose de très intéressant, peut-être pour d'autres applications dont nous n'avons encore aucune idée.* »

LE SUCCÈS MONUMENTAL DES « SIMULATIONS QUANTIQUES »



Les points verts représentent des atomes de rubidium refroidis à quelques microdegrés au-dessus du zéro absolu (-273,15 °C) dans un piège magnéto-optique. Les atomes peuvent être manipulés un par un avec des lasers pour les organiser selon différentes formes géométriques en 3D.

Les promesses de l'ordinateur quantique occultent souvent une technologie alternative, appelée les « simulations quantiques », qui, contrairement au premier, a déjà engrangé quelques résultats notables.

« *Le principe est assez simple*, estime Thierry Giamarchi, professeur au Département de physique de la matière quantique (Faculté des sciences). *Il s'agit de faire une expérience qui représente la réalisation la plus proche possible du modèle théorique que l'on aimerait tester ou résoudre. Ce sont en général des modèles concernant la physique de la matière condensée, c'est-à-dire des solides. L'expérience ressemblant presque parfaitement au modèle, il n'y a donc plus qu'à lire la mesure pour répondre à la question posée.* »

Une des techniques mises au point est basée sur des atomes froids piégés. L'idée consiste à créer un champ électromagnétique stationnaire formant un véritable réseau, avec des creux et des bosses, dans lequel on peut placer des atomes, un peu comme des œufs dans leur boîte.

Pour que cela fonctionne, il faut que les atomes froids soient vraiment très froids. En l'occurrence, les expériences se déroulent à des températures de quelques dizaines de nanoKelvins (milliardième de degré Kelvin), soit quasiment au zéro absolu. L'agitation thermique, si elle devient trop importante, annulerait les effets quantiques recherchés et, surtout, permettrait aux atomes de s'échapper de leur piège délicat.

Aujourd'hui, de nombreux laboratoires dans le monde sont capables de contrôler tous les paramètres définissant la géométrie de ces « boîtes à œufs »: distance de la maille, profondeur des creux, disposition en trois dimensions, etc. Comme elle le montre dans un article paru dans la revue *Nature* en 2018, une équipe de l'Institut d'optique de l'Université de Paris-Saclay a même réussi à reproduire un ruban de Mœbius, un hyperboloïde ou encore une tour Eiffel à l'aide d'atomes piégés dans des boucles magnétiques judicieusement placées (*voir l'image ci-contre*).

Une fois le réseau d'atomes froids disposé convenablement, les scientifiques peuvent effectuer les mesures qu'ils souhaitent. Ils ont devant eux une « simulation quantique » d'un solide, un matériau artificiel en quelque sorte, sur lequel il est possible de tester directement leurs modèles théoriques. À l'aide de lasers ultra-rapides, notamment, ils peuvent mesurer des corrélations et des propriétés très fines, réaliser des expériences hors équilibre, observer le passage d'un matériau de l'état suprafluide à celui d'isolant. Autant de « simulations quantiques » qui seraient impossibles à réaliser à l'aide d'un ordinateur classique.

L'entreprise française Muquans (rachetée par iXblue) a installé son Gravimètre quantique absolu sur l'Etna, en Italie, en 2020. L'appareil fonctionne sur la base d'une mesure de la chute libre d'atomes refroidis dans une chambre à vide et bombardé par un laser (lire l'encadré ci-contre). Il surveille actuellement de manière autonome et continue les activités volcaniques à 2820 mètres d'altitude.

SENSEURS

UNE SENSIBILITÉ À FLEUR DE PARTICULES

EXPLOITANT LES PROPRIÉTÉS DE LA THÉORIE QUI RÉGIT LE MONDE DU TOUT PETIT, LES CAPTEURS QUANTIQUES OFFRENT **UNE SENSIBILITÉ ET UNE PRÉCISION INÉDITES**, À L'EXEMPLE D'UN DISPOSITIF – THÉORIQUE – CAPABLE DE TRANSFORMER LA PLUS MINUSCULE AUGMENTATION DE CHALEUR EN UN COURANT ÉLECTRIQUE UTILE.

Géraldine Haack

Professeure assistante au Département de physique appliquée, Faculté des sciences

Formation: Elle obtient sa thèse à l'Université de Genève en 2012, avant d'effectuer un post-doctorat à l'Université libre de Berlin et au Commissariat à l'énergie atomique et aux énergies alternatives en France.

Parcours: Elle revient à l'UNIGE en 2015 au bénéfice d'un subside Marie Heim-Vögtlin du Fonds national suisse. Elle est nommée professeure assistante en juin 2021.

La maîtrise des propriétés quantiques de la matière ouvre la porte au développement de capteurs d'une toute nouvelle catégorie. Il existe déjà sur le marché des appareils qui mesurent des champs magnétiques, des particules de lumière, des différences de température minimes ou encore des variations de la force de gravitation avec une très grande précision. Mais cela n'est encore rien par rapport à ce que les senseurs quantiques seront – ou sont parfois déjà – capables d'accomplir.

On évoque ainsi des systèmes de navigation sans GPS, des détecteurs sensibles à la moindre cavité ou masse enfouie dans le sous-sol (ou sous l'eau), des moyens de prévision des éruptions volcaniques, des mesures de l'activité neuronale ou encore des dispositifs permettant de gérer la dissipation d'énergie des composés nanoélectroniques, présents notamment dans les téléphones mobiles.

Certains de ces appareils existent déjà, même s'ils sont en général très volumineux et maintenus à des températures frisant le zéro absolu et donc le plus souvent encore confinés dans les laboratoires. La plupart n'existent cependant que sur le papier, où se développent les théories, ou dans les ordinateurs, qui font tourner les simulations. Un travail théorique auquel contribue Géraldine Haack, professeure assistante au Département de physique appliquée (Faculté des sciences) et bénéficiaire d'une bourse Prima du Fonds national suisse.

L'OBJECTIF CONSISTE À EXPLOITER LES PROPRIÉTÉS DE LA PHYSIQUE QUANTIQUE POUR TRANSFORMER LA MOINDRE DIFFÉRENCE DE TEMPÉRATURE EN UN COURANT ÉLECTRIQUE MESURABLE

Réchauffement minime Elle mène notamment un projet de dispositif thermoélectrique quantique d'une très grande sensibilité. L'effet thermoélectrique classique est connu depuis la fin du XIXe siècle. Il caractérise certains matériaux dans lesquels une différence de température génère un courant électrique (et inversement, une tension électrique crée un courant de chaleur). L'objectif de la chercheuse genevoise consiste à exploiter les propriétés de la physique quantique pour augmenter cet effet thermoélectrique et transformer la moindre différence de température en un courant électrique plus facilement mesurable en laboratoire.

« *Mon domaine initial, c'est l'étude du transport d'électrons dans des circuits électriques simples mais fonctionnant à l'échelle quantique*, explique Géraldine Haack. *Dans le cadre de notre projet, mon collègue italien Francesco Giazotto, directeur de recherche à l'Institut des nanosciences de Pise, et moi-même avons donc imaginé un dispositif qui comprend ce qu'on appelle une boucle Aharonov-Bohm. Il s'agit d'un circuit électrique de très petite taille – de l'ordre de quelques micromètres – qui relie une source dite chaude à une source dite froide (la différence de température peut être infime). Les électrons circulent de la source chaude à la source froide en vertu de la deuxième loi de la thermodynamique. Ils le font via une connexion qui, à un moment donné, se divise en deux branches qui se rejoignent juste après, laissant la possibilité aux particules chargées de passer par deux chemins différents.* »

DR

DANS LES MOINDRES DÉTAILS

Deux catégories de senseurs quantiques sont actuellement en plein développement et parfois proches de la commercialisation. La première correspond aux centres NV (pour « *nitrogen vacancy* »). Il s'agit d'une pointe en diamant comptant des milliards d'atomes parfaitement alignés et un seul défaut, à savoir un atome d'azote et une lacune à la place de deux atomes de carbone. Ces deux impuretés se comportent en fait comme des atomes uniques dont on peut, grâce à une lumière laser notamment, mesurer le « spin », un terme qui désigne un moment magnétique quantique propre à certaines particules élémentaires, sans équivalent dans le monde classique et que l'on peut se représenter comme une petite aiguille sensible à un champ magnétique. Ce dispositif est extraordinairement sensible à de minimes changements de lumière et de champ magnétique. La start-up bâloise Qnami, cofondée par Patrick Maletinsky, professeur à l'Université de Bâle et auteur d'avancées importantes dans le domaine des centres NV, en développe et en commercialise. En plus de servir de microscope magnétique ultrasensible utile en laboratoire et dans un grand nombre d'applications technologiques, ce genre de dispositif pourrait aussi entrer dans le développement d'instruments de navigation, ajusté sur le champ magnétique terrestre et permettant de se diriger très précisément dans des lieux que le GPS ne peut pas atteindre, par exemple sous l'eau.
L'autre catégorie de senseurs quantiques très en vogue comprend les interféromètres à atomes. Ces dispositifs reposent sur un nuage de quelques millions d'atomes refroidi par laser à une température de seulement un millionième de degré au-dessus du zéro absolu. Dans ces conditions où l'agitation thermique est réduite au minimum, les atomes se déplacent si lentement qu'il devient possible de mesurer avec une très grande précision les forces auxquelles ils sont soumis, comme la gravitation. Pour ce faire, on laisse les atomes chuter sous l'effet de la gravité. Ils sont alors bombardés par un laser qui place chaque atome dans une superposition d'état quantique – il se trouve dans celui de n'avoir pas absorbé de photon laser et en même temps dans celui où il a reçu une vitesse supplémentaire. On peut alors faire interférer les deux états – selon le même principe qui permet de faire fonctionner la boucle Aharonov-Bohm pour l'effet thermoélectrique *(lire article principal)* – et en déduire avec une très grande efficacité la valeur de l'accélération terrestre. Certaines études font état d'une précision d'un milliardième, soit la variation de pesanteur ressentie lorsqu'on s'élève de trois millimètres de la surface de la Terre.
Avec des gravimètres atomiques d'une telle précision, il devient imaginable de détecter des volumes de plus en plus petits dont les densités diffèrent de leur environnement et contribuent ainsi à une légère augmentation ou diminution locale de la pesanteur : des nappes phréatiques, certains types de roches, des arrivées de magma, etc.
Une entreprise française, Muquans, (rachetée depuis par iXblue, française également), commercialise d'ores et déjà de tels gravimètres atomiques.

Comprendre plus précisément l'effet Aharonov-Bohm demande cependant de faire un gros plongeon dans un bain de physique quantique, puisque ce phénomène découle du fait qu'une particule comme l'électron possède, à toute petite échelle, des propriétés à la fois corpusculaires et ondulatoires.

Par les deux chemins à la fois Du point de vue du formalisme quantique, le petit paquet d'ondes qui forme la particule peut donc passer par les deux chemins en même temps : par le bras supérieur *et* par le bras inférieur – comme le ferait une onde à la surface de l'eau empruntant deux parcours différents. Parce que les deux chemins ne sont pas de la même longueur et que le tout est baigné dans un champ magnétique, les paquets d'ondes acquièrent une phase différente entre les chemins supérieur et inférieur et forment, à l'arrivée, ce qu'on appelle une figure d'interférences, avec des maximums et des minimums, là où les ondes s'additionnent ou se détruisent, comme lorsque les ronds dans l'eau générés par deux cailloux se rencontrent. Parce qu'elles sont issues d'un unique électron pouvant être décrit comme un paquet d'ondes, ces interférences quantiques produisent au final un courant électrique qui oscille en fonction du flux magnétique et que l'on peut mesurer.
Géraldine Haack et Francesco Giazotto ont montré, dans un article paru le 23 décembre 2019 dans la revue *Physical Review B*, que leur dispositif, en théorie du moins, développe un formidable effet thermoélectrique.
« *Il est tellement sensible qu'il pourrait détecter une augmentation de chaleur aussi petite que celle provoquée par l'absorption d'un unique photon (ou grain de lumière)*, explique Géraldine Haack. *On peut imaginer jouer avec les paramètres de notre dispositif de telle façon qu'il soit optimisé pour des photons d'une certaine longueur d'onde. Certains groupes de recherche ont actuellement une telle maîtrise dans la fabrication de ces structures mésoscopiques (c'est-à-dire de taille relativement « grande » mais conservant des propriétés quantiques), qu'il ne devrait pas être trop compliqué de réaliser l'expérience en laboratoire.* »

Photons uniques En tant que capteur thermoélectrique, le détecteur basé sur la boucle Aharonov-Bohm pourrait permettre de mesurer de toutes petites différences de chaleur à une température très proche du zéro absolu (-273,15 °C), ce qui tient en général de la gageure dans les laboratoires de recherche. Plus concrètement, avec ce dispositif quantique on pourrait atteindre une efficacité jusqu'à quatre fois plus importante que les matériaux thermoélectriques classiques les plus performants.

« *Le fait qu'une petite augmentation de chaleur puisse générer un courant de charge peut aussi intéresser tous les secteurs qui doivent faire face au phénomène de dissipation de chaleur*, poursuit Géraldine Haack. *Ce problème de dissipation touche l'ensemble des appareils électroniques, des téléphones portables aux fermes géantes de serveurs, et peut nuire gravement à leurs performances. On peut bien sûr construire ces immenses data centers dans des environnements froids – ce qui se fait déjà – mais ce n'est pas un choix très durable. On peut aussi essayer de comprendre les mécanismes intimes, voire quantiques, de cette dissipation de chaleur pour tenter de l'atténuer. Un dispositif comme le nôtre pourrait servir à cela.* »

LE PETIT PAQUET D'ONDES QUI FORME LA PARTICULE PEUT DONC PASSER PAR LES DEUX CHEMINS EN MÊME TEMPS

Une autre piste serait d'exploiter cette chaleur résiduelle (qui est de toute façon impossible à éviter) pour la transformer en électricité, laquelle pourrait être réinjectée dans le circuit de l'appareil en question ou, pourquoi pas, faire tourner un mini-moteur. « *Un des points de ma recherche, c'est justement de concevoir des moteurs ou des machines thermiques à l'échelle quantique* », note au passage Géraldine Haack.

NOUVEAUX MATÉRIAUX

LE GRAPHÈNE, UN MONDE EN DEUX DIMENSIONS

LE GRAPHÈNE, **UNE COUCHE MONOATOMIQUE DE CARBONE**, AINSI QUE SES DÉRIVÉS (COMPOSÉS D'AUTRES ÉLÉMENTS) POURRAIENT REPRÉSENTER, GRÂCE À LEURS PROPRIÉTÉS SURPRENANTES, LES BRIQUES DE BASE POUR FABRIQUER LES MATÉRIAUX DE DEMAIN.

Alberto Morpurgo
Professeur au Département de physique de la matière quantique, Faculté des sciences

Formation : Après une maîtrise en physique à l'Université de Gênes (Italie), il est passé par la Scuola Normale de Pise et l'Université de Groningue (Pays-Bas), où il a obtenu un doctorat en 1998.

Parcours : Après un post-doctorat à l'Université Stanford et plusieurs années à l'Université de Delft, il obtient un poste de professeur à l'Université de Genève en 2008. En 2016, il est élu au Conseil de la recherche du Fonds national suisse.

Le graphène est aussi mince que possible, plus résistant que l'acier, flexible, transparent. C'est un excellent conducteur, il est léger comme l'air, sélectivement perméable et, surtout, en deux dimensions. Ce matériau quantique aux mille promesses est en effet composé d'une seule couche d'atomes de carbone dont l'empilement forme le graphite, le même que celui des crayons gris. La prouesse de son découvreur, Andre Geim, de l'Université de Manchester, est « simplement » d'avoir réussi à isoler une seule de ces feuilles en 2004.

Depuis, des progrès considérables ont été accomplis dans ce vaste champ de recherche qui s'est subitement ouvert aux scientifiques. On a découvert au graphène une propriété remarquable après l'autre. On lui promet un avenir radieux comme composant ultraléger pour la voiture ou l'aéronautique, comme superpile pour le stockage de l'énergie, comme détecteur chimique hypersensible, comme transistor extra-rapide ou encore dans la fabrication d'écrans tactiles flexibles.

ON LUI PROMET UN AVENIR RADIEUX COMME COMPOSANT ULTRALÉGER, SUPERPILE, DÉTECTEUR CHIMIQUE HYPERSENSIBLE, TRANSISTOR EXTRA-RAPIDE OU ENCORE DANS LA FABRICATION D'ÉCRANS TACTILES FLEXIBLES

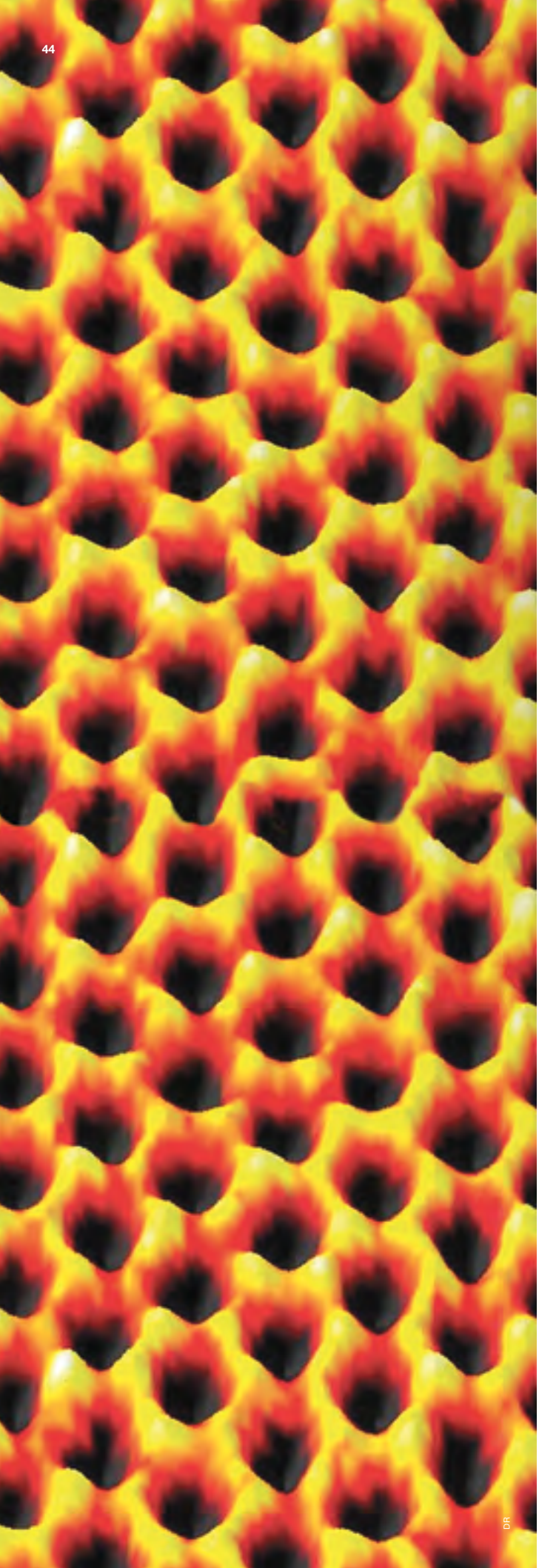
Matériau quantique « *Le graphène est un matériau de nature quantique dans le sens qu'on n'arrive à maîtriser ses composants au niveau atomique et à obtenir des propriétés nouvelles qui ne peuvent s'expliquer que par la physique quantique* », commente Alberto Morpurgo, professeur au Département de physique de la matière quantique (Faculté des sciences) et responsable adjoint de l'une des six divisions (Enabling science and materials) du Graphene Flagship, un projet phare de l'Union européenne lancé en 2013 *(lire encadré)*.

Depuis plusieurs années, les atomes de carbone disposés en hexagones sont remplacés par d'autres éléments capables eux aussi de se tenir dans la même configuration *bidimensionnelle et d'exhiber de nouvelles caractéristiques. On a même commencé à déposer une monocouche sur l'autre, afin de combiner les propriétés et d'en obtenir de nouvelles.*

Cette technique est d'ailleurs un des sujets de recherche d'Alberto Morpurgo. Lui et ses collègues travaillent en effet sur des structures bidimensionnelles capables d'émettre de la lumière ou, plus récemment, sur d'autres possédant des propriétés magnétiques inédites.

Dans un article publié le 3 février 2020 par la revue *Nature Materials*, il a notamment montré que la superposition de deux monocouches permettait d'obtenir des dispositifs capables d'émettre de la lumière, potentiellement « à la carte », c'est-à-dire de la couleur souhaitée, en choisissant les bons composants pour chacune des deux monocouches. Leur travail a aussi, et surtout, présenté une solution au problème de la superposition de deux feuilles de quelques angströms (dixièmes de milliardième de mètre) d'épaisseur dont les mailles cristallines ne correspondent pas parfaitement ou qui sont légèrement décalées l'une par rapport à l'autre, ce qui aurait normalement pour résultat d'annihiler l'effet photoluminescent recherché.

« *Disposer de cette souplesse dans la conception de nouveaux matériaux représente un atout majeur dans une perspective*



DR

Le graphène, vu ici au microscope à champ proche, est composé d'une monocouche d'atomes de carbone, disposés selon une maille hexagonale.

LES PROMESSES DU GRAPHÈNE

Découvert en 2004, le graphène a provoqué un engouement tel qu'en 2013, l'Union européenne a lancé le Graphene Flagship, doté d'un budget d'un milliard d'euros sur dix ans. Ce projet, le premier de ce type, a été conçu, entre autres, pour éviter de se faire distancer sur le plan industriel, notamment par la Chine et la Corée du Sud, où la plupart des brevets dans ce domaine ont à ce jour été déposés. Le succès semble être au rendez-vous. En février de cette année, le consortium européen a annoncé la mise en place d'une ligne de production capable de fabriquer des films de graphène sans défauts de 30 centimètres de diamètre, prêts à être intégrés sur des plaques de silicone cristallin destinées aux circuits intégrés. Selon son rapport d'activité 2020, soit trois ans avant la conclusion du programme, le Graphene Flagship affirme également avoir donné naissance à environ 90 produits intégrant le graphène d'une manière ou d'une autre, avec des applications aussi disparates que des capteurs à effet Hall (permettant de mesurer les champs magnétiques et l'intensité des courants électriques) dix fois plus sensibles que leurs homologues en silicium ou des écouteurs aux aigus et basses améliorés. Parmi les autres produits de niche, on trouve aussi un pneu de vélo ayant une excellente adhérence, une raquette de tennis à flexibilité et durabilité supérieures, un casque de moto capable de disperser les impacts avec grande efficacité ou encore un climatiseur à haute performance. Le Flagship a également lancé les projets «Spearhead» (fer de lance), dont le but est de mettre au point des prototypes utilisant le graphène pour des applications commerciales. Conformes aux Objectifs de développement durable des Nations unies, ces projets comprennent l'utilisation de produits à base de graphène pour contribuer à la santé et au bien-être, à la production d'eau potable et d'une énergie propre et abordable, à des villes et des communautés durables, ainsi qu'à l'amélioration de l'innovation industrielle et des infrastructures en Europe.

https://graphene-flagship.eu

industrielle, explique le professeur genevois. *En termes de coûts et d'efficacité, il est en effet préférable d'avoir une certaine tolérance dans le processus de fabrication afin de ne pas risquer de perdre à la moindre imprécision les propriétés désirées, si fragiles par essence car dépendantes de paramètres réglés à l'échelle atomique.* »

Les sauts des électrons Il existe déjà dans le commerce des matériaux capables d'émettre de la lumière. Il s'agit de semi-conducteurs, utilisés dans des secteurs aussi divers que les télécommunications, les LED présents dans de nombreux appareils quotidiens (ampoules économiques, éclairage public, écrans plats…) ou le diagnostic dans le secteur médical. Ces dispositifs électroluminescents exploitent le fait que dans ces matériaux, les électrons peuvent sauter d'un niveau d'énergie élevé à un autre plus bas et émettre en même temps un grain de lumière dont la longueur d'onde (couleur) correspond exactement à la différence d'énergie des deux niveaux.

TOUTES LES LONGUEURS D'ONDE NE SONT PAS DISPONIBLES.LES MATÉRIAUX TELS QUE LE GRAPHÈNE REPRÉSENTENT UNE SOLUTION ÉLÉGANTE À CETTE LIMITATION

Mais seuls certains matériaux peuvent faire l'affaire. Et toutes les longueurs d'onde ne sont pas disponibles.

Les matériaux bidimensionnels tels que le graphène et ses dérivés représentent donc une solution élégante à cette limitation. Ces cristaux parfaits, une fois empilés, se comportent en effet comme des semi-conducteurs « artificiels » dont les niveaux d'énergie peuvent être contrôlés en sélectionnant la composition chimique et l'épaisseur des matériaux formant la structure.

Les premiers semi-conducteurs artificiels ont été réalisés il y a quatre ou cinq ans. Au début, pour que le dispositif émette de la lumière, il fallait que les deux cristaux 2D aient la même structure cristalline et que les atomes soient tous parfaitement alignés. Des conditions très strictes et rarement remplies.

Pour dépasser cette limitation, l'équipe d'Alberto Morpurgo a exploité deux propriétés issues de la physique quantique. La première consiste à se passer des liaisons chimiques covalentes (obtenues par échange d'électrons), qui maintiennent fermement deux couches monoatomiques ensemble, et d'utiliser à la place la force de Van der Waals. La faible intensité de cette interaction électrique qui agit directement entre deux atomes dès qu'ils sont assez proches permet aux deux couches de coulisser et de tourner plus facilement l'une par rapport à l'autre.

La seconde propriété est plus technique et vise à trouver une classe de matériaux pour laquelle la « quantité de mouvements » des électrons avant et après le passage d'un niveau d'énergie à l'autre est nulle. Ce cas de figure idéal satisfait toujours les conditions nécessaires pour l'émission de lumière, indépendamment des détails des réseaux cristallins et de leur orientation relative.

Et il se trouve qu'il existe un grand nombre de matériaux répondant à ces deux exigences. « *Dans notre recherche, nous avons utilisé du séléniure d'indium (InSe) sur lequel nous avons déposé différentes dichalcogénures de métaux de transition (des matériaux à base de molybdène ou de tungstène)*, explique Alberto Morpurgo. *Par la suite, nous avons identifié de nombreux autres composés qui pourraient être utiles pour élargir la gamme de couleurs de la lumière émise par ces nouveaux semi-conducteurs artificiels. Nous proposons ainsi de nouvelles stratégies pour manipuler cette lumière comme bon nous semble, avec l'énergie et la couleur que l'on souhaite obtenir.* »