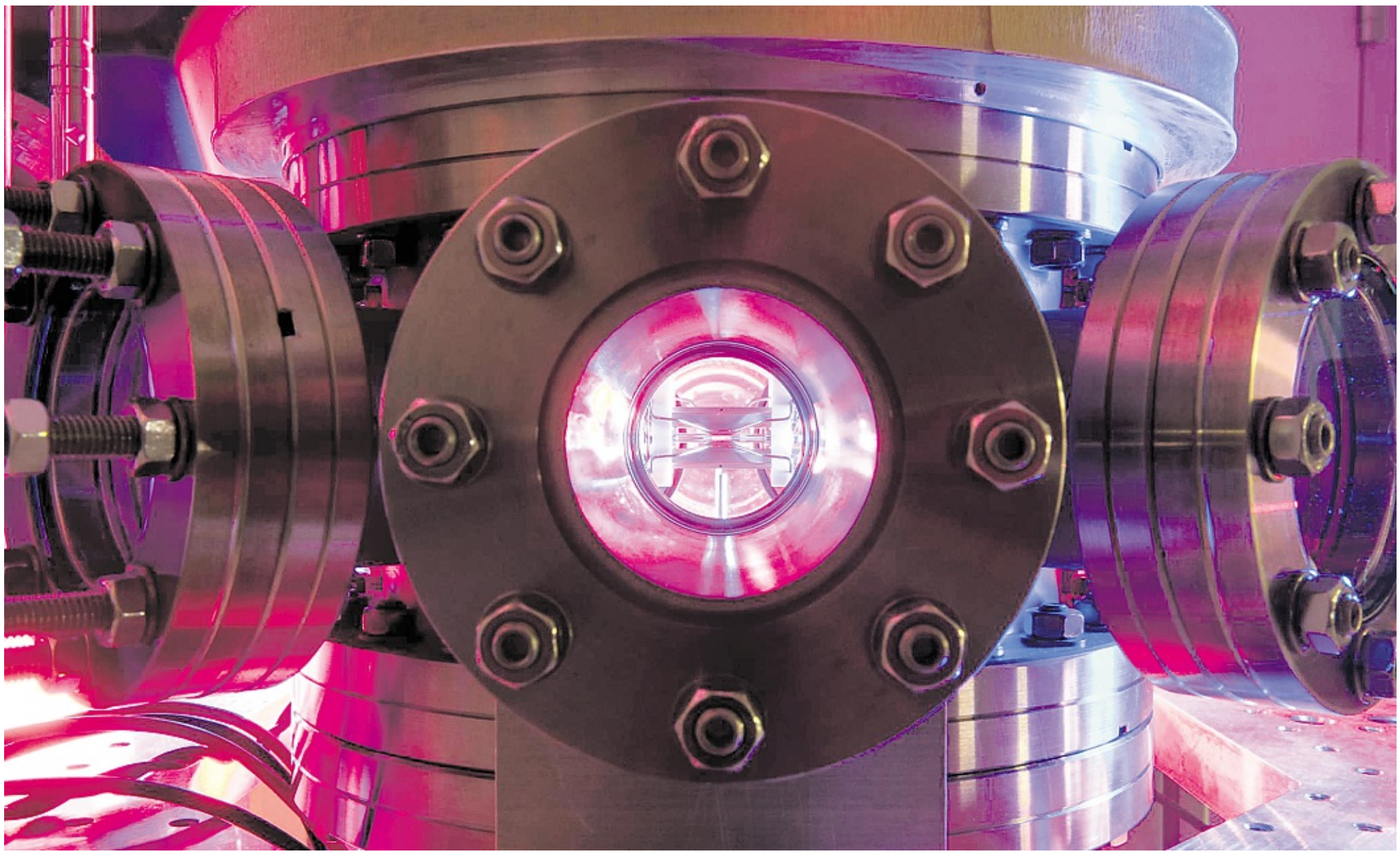
science & médecine
Le Monde



A l'université d'Innsbruck (Autriche), une enceinte à vide enfermant des atomes chargés, qui pourraient servir de nœud de réseau d'un futur Internet quantique. ROBBIE SHONE

Aux portes de la communication **quantique**

L'ordinateur n'est pas la seule révolution promise par la physique de l'infiniment petit. Un Internet dont la sécurité des échanges s'appuierait sur des propriétés de photons commence également à sortir des labos. Le point sur une technologie « disruptive »

DAVID LAROUSSERIE

Comme un clin d'œil de l'histoire. Dans les sous-sols d'un hôtel particulier parisien, dont la construction a enjambé la Révolution française, une petite communauté s'agite pour bâtir une autre révolution. Celle-ci sera technologique et reposera sur la physique quantique.

Quantique ? Le mot encore mal connu a commencé à percer dans le grand public. Surtout depuis qu'une entreprise du numérique archicélèbre, Google, a prétendu fin octobre avoir battu un ordinateur classique avec une machine d'un nouveau genre s'appuyant sur les principes de la physique quantique, cette théorie qui décrit le monde des particules.

Cependant, le 5 novembre, la quarantaine de personnes, dont une dizaine de femmes, massées pour deux jours dans les caves de l'hôtel Bourrienne, dans le 10e arrondissement, en teeshirt jaune, ne veulent pas révolutionner le calcul mais les communications. Ou, plus directement, contribuer à l'émergence d'un Internet quantique. *« Vous êtes là pour imaginer les premières applications qui utiliseront la physique quantique pour sécuriser les communications »,* rappelle Pierre-Emmanuel Emeriau, doctorant au laboratoire d'informatique LIP6 à Sorbonne Université. Il est aussi l'un des jeunes coorganisateurs de ce premier événement paneuropéen sous forme de hackathon, un exercice de travail collectif inspiré de l'informatique conventionnelle. Cinq autres villes y participent, Sarajevo, Padoue (Italie), Genève (Suisse), Dublin et Delft (Pays-Bas).

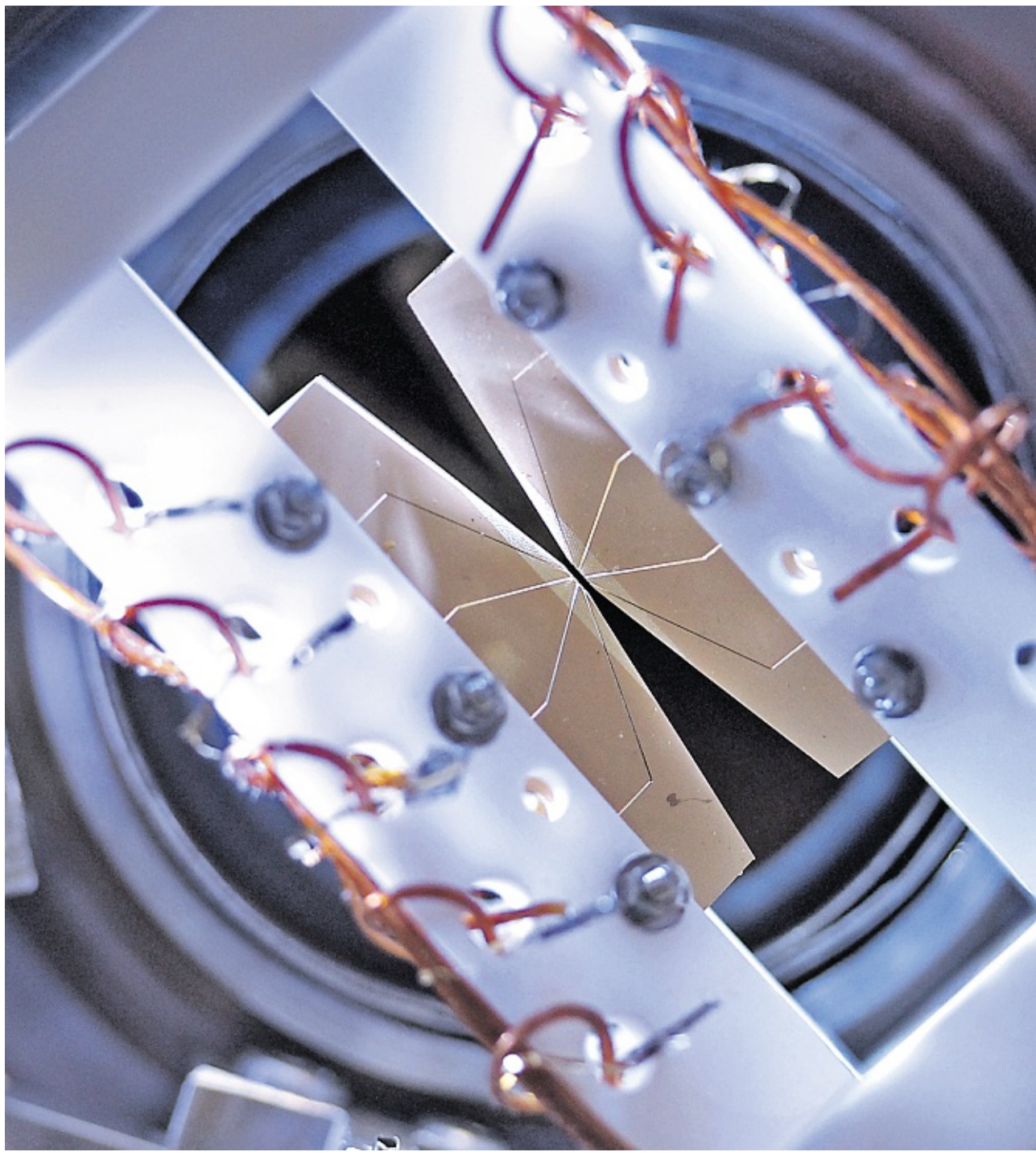
La mission de la centaine de volontaires est, plus concrètement, de programmer et de simuler des protocoles pour communiquer grâce aux diverses particularités quantiques, comme – en caricaturant – pouvoir être dans deux états à la fois, se téléporter ou changer instantanément d'état. Ces étranges propriétés permettent d'échanger des clés de chiffrement entre deux points, d'anonymiser des transmissions, de certifier des identités, voire de payer en ligne avec des chèques ou des cartes bancaires quantiques… *« La sécurité ne veut pas dire seulement des systèmes incassables. On peut penser à des techniques plus efficaces, plus rapides, moins chères, plus adaptées »,* prévient Elham Kashefi, directrice de recherche CNRS au LIP6 et professeure à l'université d'Edimbourg. Elle-même a imaginé, dès 2009, une manière d'effectuer des calculs « aveugles » sur un ordinateur quantique distant, de telle sorte que le propriétaire de cette machine ne puisse pas extraire d'informations sur ce que le demandeur du calcul est en train de faire.

Son protocole est l'un des soixante déjà proposés par la recherche académique et détaillés sur un site Web, baptisé « zoo des protocoles », créé il y a deux ans par le LIP6, dont les membres sont en force dans l'organisation ou parmi les participants du hackathon parisien.

Dans une des pièces, un étrange ballet commence. Face à face, en deux rangs, les participants ont trente secondes pour se présenter, avant de se décaler et de recommencer afin de faire connaissance et de former les cinq équipes. La moitié d'entre eux seulement sont « quantiques », maîtrisant soit la physique, soit les algorithmes.

➔ LIRE LA SUITE PAGES 4-5

Les premiers pas d'un Internet **quantique**



A l'université du Maryland (Etats-Unis), ces lames métalliques créent des pièges électromagnétiques pour confiner des atomes chargés que l'on peut intriquer ensemble pour des opérations de calcul ou de communication quantique. ROBBIE SHONE

▶ SUITE DE LA PREMIÈRE PAGE

Les autres se divisent entre spécialistes des technologies de réseau classique, employés d'industrie et consultants. *« On a déjà la victoire en nombre de participants ! »*, constate Harold Ollivier, autre membre du LIP6.

A l'étage aussi, on s'agite. L'hôte de l'événement, le fonds d'investissement Quantonation, peaufine son investissement dans une cinquième start-up issue de la physique fondamentale, la suisse Qnami, qui développe un microscope quantique très sensible pour détecter les champs électriques ou magnétiques. En décembre 2018, elle a soutenu Kets, une société britannique de matériel de communication quantique. *« La période est favorable, notamment avec l'annonce de Google. La dynamique est positive, mais en deçà de ce qui se passe en intelligence artificielle »*, constate Christophe Jurczak, l'un des fondateurs de Quantonation, en 2018, avec Olivier Tonneau et Charles Beigbeder, propriétaire des lieux. Leur but est de lever 50 millions d'euros en 2020.

Pas de chance, le hackathon démarre mal. Moins d'une heure après le début de l'épreuve, le Wi-Fi sature. Une équipe est rapidement évacuée à l'étage pour qu'elle se connecte à une autre borne. Tout va mieux. La révolution peut commencer.

Tandis que, au sous-sol de l'hôtel particulier, de jeunes ingénieurs et chercheurs jouent à blanc aux « communicants » quantiques, d'autres, en surface, essaient de donner vie à un futur réseau. *« On pourrait penser que le public comprend plus facilement le sujet du calcul quantique que celui des communications. Mais, comme il s'agit de questions concrètes de sécurité, de banque, de protection de la vie privée ou d'accès aux données de santé, le message est très bien compris aussi »*, rappelle Tommaso Calarco, président du Quantum Community Network, réseau communautaire européen quantique, chargé d'animer la communauté concernée, de définir des plans de route et de mobiliser la Commission européenne pour des financements. En septembre 2018, plus de 135 millions ont déjà été alloués pour trois ans, en attendant 1 milliard potentiel pour les prochaines années. Le volet communications compte pour un quart, réparti sur cinq projets. *« L'effort de recherche sur les communications a en fait toujours été très fort. Le domaine est même plus vivant que celui du calcul »*, précise Tommaso Calarco.

Les grandes manœuvres sont lancées

Des applications commerciales sont déjà là, contrairement à celles impliquant des calculs. Depuis 2001, la société suisse ID Quantique vend ainsi des systèmes d'envoi de clés de chiffrement, dont la sécurité repose sur la physique. *« Envoyer une clé entre deux points est comme envoyer des balles avec des 0 et des 1 écrits dessus,* aime à dire Grégoire Ribordy, son PDG. *Le défaut est que cela peut être intercepté. La physique quantique permet de faire cet échange avec des balles "fragiles" comme des bulles de savon, si bien que, si on les intercepte, leur message est perdu. »* Si l'entreprise ne communique pas sur ses ventes, elle a annoncé travailler au câblage de la Corée du Sud pour le squelette du réseau 5G de l'opérateur local SK Telecom, par ailleurs son actionnaire majoritaire. En 2008, un réseau de démonstration à Vienne (Autriche) avait connecté cinq lieux, reliés par les « bulles » de la société. Depuis, Toshiba est aussi entré dans la compétition.

DES APPLICATIONS COMMERCIALES DANS LE DOMAINE DES COMMUNICATIONS SONT DÉJÀ LÀ

Alors, pourquoi continuer la recherche puisque cela marche déjà ? *« Ces techniques sont limitées en distance à cause des pertes dans les fibres optiques et de la disparition des propriétés quantiques,* rappelle Eleni Diamanti, chercheuse CNRS au LIP6. *On ne peut pas dépasser les 100 kilomètres. »* Les bulles de savon éclatent après un trop long voyage.

Une des solutions est de passer par un satellite, car l'air atténue moins le signal qu'une fibre optique. Les Chinois l'ont fait grâce à Micius, lancé en 2016, qui a même fait voyager des clés entre la Chine et l'Autriche pour chiffrer un flux de visioconférence. Autre parade, ajouter tous les 100 kilomètres environ des nœuds de répétition, qui lisent les précieuses clés de chiffrement, les stockent, puis les réémettent. C'est la solution choisie pour la Corée. Et pour la Chine, entre Pékin et Shanghaï, sur 2 000 kilomètres et 32 nœuds. Problème, la clé est visible dans ces nœuds, ouvrant une faille potentielle.

La mécanique quantique y remédierait. Pour faire passer une information d'un point A à un point B très distant, un troisième nœud C intermédiaire est introduit qui ne copie pas l'information, mais rend solidaires A et B, par la magie quantique. Et ainsi de suite. Personne, pour l'instant n'a cependant réussi à fabriquer un tel répéteur quantique.

Ce qui n'empêche pas les grandes manœuvres de commencer. En France, les équipes participant aux projets QIA (Quantum Internet Alliance) et Open QKD, financés par l'Union européenne, ont l'intention de déployer des liens expérimentaux sur des fibres commerciales, entre Paris centre et Saclay (Essonne) ou, à Nice, entre Sophia Antipolis et le campus de l'université. A Paris, les chercheurs testeront notamment un protocole d'échange de clés différent de celui d'ID Qantique.

FORMER DES INGÉNIEURS ET DES INFORMATICIENS

Pour accompagner le développement des technologies quantiques, il faut aussi une révolution dans l'enseignement », estime Alexia Auffèves, chercheuse CNRS à l'institut Néel. Il est vrai que les bizarreries quantiques ne sont enseignées pour l'instant que dans les cours de physique pour ceux qui s'orientent plutôt vers l'enseignement ou la recherche. Or, il s'agit maintenant de convaincre les ingénieurs et les informaticiens qu'ils peuvent aussi s'intéresser à ces questions.

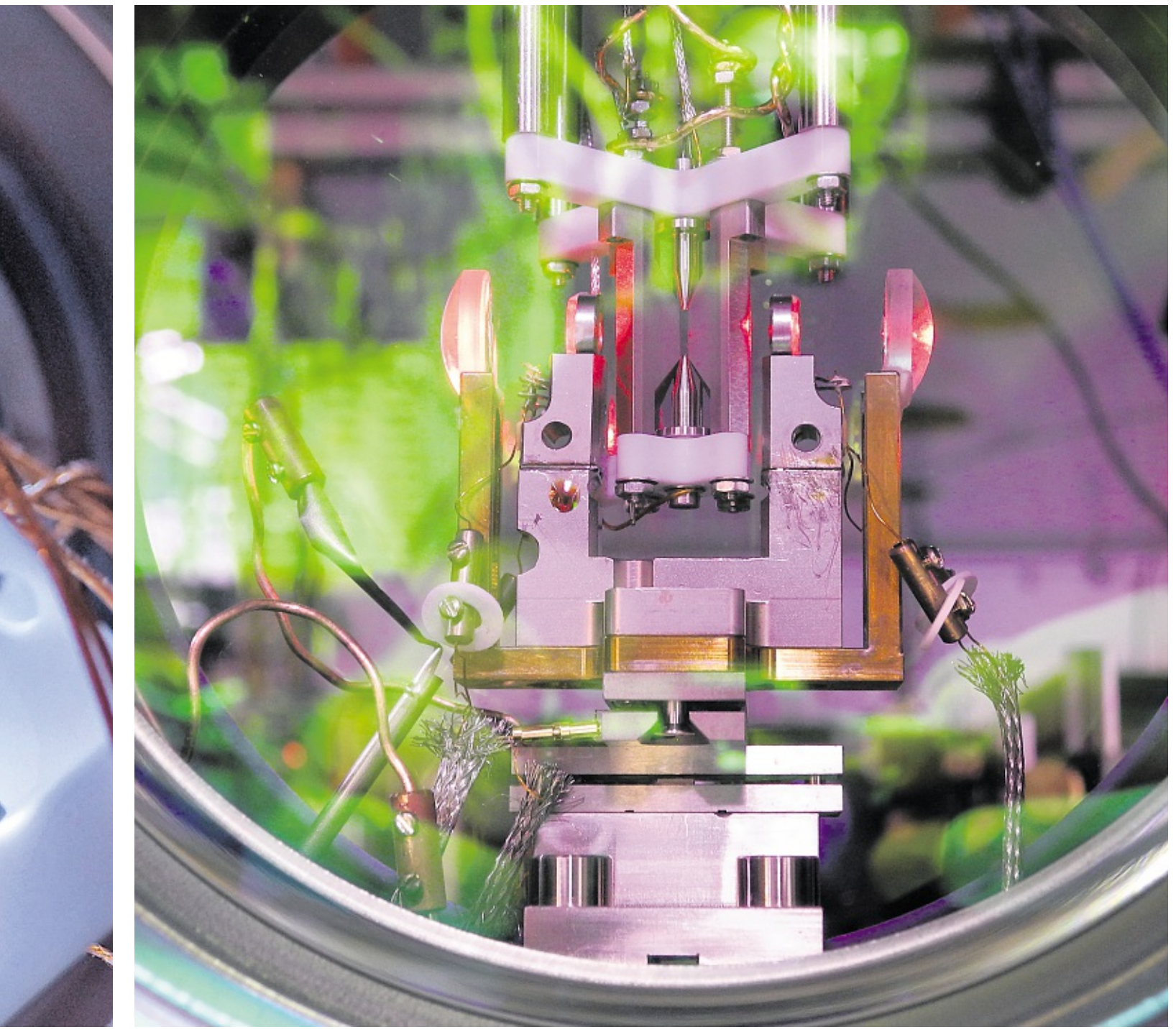
« Je pense même que l'information quantique est une excellente porte d'entrée pour l'apprentissage de la mécanique quantique elle-même. Ses concepts sont peut-être même techniquement et mathématiquement plus simples à manier que ceux venus de la physique enseignés actuellement », estime la spécialiste, qui rappelle que chaque époque a abordé cette discipline avec les technologies du moment. D'abord le nucléaire, puis la physique atomique. C'est donc au tour de l'informatique, de ses portes logiques, ses algorithmes, ses protocoles de communication... de changer le regard sur la discipline.

Autre point à améliorer, *« il y a encore trop de cloisonnement entre la physique et l'ingénierie,* regrette Pascale Senellart, chercheuse CNRS et chargée d'une mission pour l'université Paris-Saclay, consistant notamment à définir de nouveaux cursus de formation. *Les physiciens ne font pas forcément de bons ingénieurs. Et la physique elle-même est très thématique et forme des experts en matériaux, nanosciences, physique atomique... alors que ces sujets, du point de vue des technologies quantiques, sont en fait très liés. A l'inverse, les informaticiens n'ont pas assez de contacts avec le "matériel". »* La spécialiste essaie donc de multiplier les ponts entre tous ces domaines, profitant de sa récente expérience d'entrepreneuse, depuis la création de Quandela, entreprise qui fabrique des sources de photons. Visiblement, les technologies semblent assez mûres pour que les ingénieurs puissent développer leur savoir-faire dans l'optimisation, le développement, le contrôle, le design, la certification... *« Il faut augmenter la masse critique d'ingénieurs quantiques »*, tranche Pascale Senellart.

Petit à petit, la magie quantique descend donc des écoles doctorales vers les masters et les écoles d'ingénieurs. En Europe, aux Pays-Bas, l'établissement le plus important du domaine, QuTech à Delft, a une « académie », qui propose des cours en ligne ou avec des enseignants. En France, Télécom Paris a son propre cursus depuis quatre ans avec stages, tutorats et liens avec d'autres établissements. L'Ecole centrale, les universités Paris-Saclay et Grenoble-Alpes suivront. *« Une thèse dans le domaine est même un vrai plus pour les recruteurs »*, note Romain Alléaume, enseignant-chercheur et responsable de la formation quantique à Télécom Paris. *« Il y a quelques freins, bien sûr, car les enseignants doivent changer leurs cours,* souligne Alexia Auffèves. *Mais les barrières commencent à tomber. »*

Comme Pascale Senellart, elle constate aussi l'intérêt pour de la formation continue de la part d'entreprises dont le cœur de métier est parfois éloigné de ces hautes technologies futuristes. EDF, Total, Airbus, BMW, DowDuPont, BASF ou SAP rejoignent des groupes plus attendus comme Google, IBM, Atos. Signe des temps, des consultants essaient déjà de convaincre les entreprises de s'y mettre. Le hackathon paneuropéen, organisé par le fonds d'investissement Quantonation, les 5 et 6 novembre, s'inscrit aussi dans cette veine. *« Notre activité a besoin de développer l'écosystème des technologies quantiques en intéressant au-delà des acteurs traditionnels. On participe à l'évangélisation »*, rappelle Christophe Jurczak, cofondateur de ce fonds. ■

D. L.



Détail d'un piège à atome chargé, porteur d'une information que les chercheurs de l'université d'Innsbruck (Autriche) essaient de transférer sur un photon pour l'envoyer dans des fibres optiques.
ROBBIE SHONE

« 3 + 3 = 4 », ET AUTRES RECETTES DE SÉCURITÉ

Superposition, téléportation, intrication... sont trois des propriétés incontournables des futurs réseaux de communication, impliquant une, deux ou trois particules.

Commençons par les solutions à une particule, par exemple un grain de lumière, ou photon. Admettons qu'il existe des photons noirs et des photons blancs. En fait, la mécanique quantique autorise que les photons ne soient ni noirs ni blancs, mais « gris », c'est-à-dire à la fois noir et blanc. Ce n'est que lorsqu'un détecteur de « couleur » entrera en action que le photon gris sera vu comme noir ou blanc, avec une chance sur deux d'être vu dans l'un de ses états. C'est le concept de superposition. Rien qu'avec cela, les chercheurs Charles Bennett et Gilles Brassard ont proposé, en 1984, un protocole de communication sûr entre deux points pour échanger des bits d'information, qui constituent notamment une clé pour chiffrer et déchiffrer des documents. L'une de leurs idées est que si un espion intercepte un photon entre les deux points, alors celui-ci perd son caractère mélangé, ce que sauront alors les interlocuteurs, qui choisiront de ne pas prendre en compte ce bit d'information. L'entreprise ID Quantique commercialise un tel système pour échanger des clés.

Téléporter la « couleur »

Passons à deux photons et à l'intrication. Il est possible de fabriquer une paire magique de photons, liés par une « colle » invisible, qu'on pourrait envoyer en deux points très distants. S'ils n'étaient pas liés ou intriqués, mesurer la couleur de l'un n'aurait aucune influence sur la mesure de l'autre, qui resterait aléatoire, noir ou blanc à 50-50 de chance. Mais comme on les a intriqués, leur corrélation est très forte, si bien que trouver que l'un est noir impose que l'autre le soit aussi (on peut aussi décider que quand l'un est noir, l'autre est blanc). Grâce à ce principe, il est possible de téléporter, comme en science-fiction, la « couleur » d'un photon sur un autre. Si Alice possède un photon d'une couleur, qu'elle veut téléporter à Bob, elle crée en plus une paire intriquée dont elle envoie un membre vers Bob et fait interagir l'autre avec le sien. Aussitôt le photon intriqué reçu par Bob se transforme, reproduisant l'état de la particule initiale d'Alice (qui est « perdu »).

Dans cet esprit, on peut aussi arriver non pas à téléporter un état d'un point à un autre, mais faire en sorte d'intriquer deux photons à distance entre Alice et Bob, réalisant un répéteur quantique, un Graal, qui augmenterait la distance de transmission d'informations sensibles.

Enfin, avec trois photons, les chercheurs peuvent aussi s'amuser en créant non pas seulement une paire, mais un trio intriqué. On peut alors faire une drôle d'opération : 3 + 3 = 4... En effet, si l'on prend deux paires de photons intriqués et qu'un membre d'une des paires interagit avec un membre de l'autre, on peut arriver à intriquer les deux membres restants. Mais, parti d'une paire intriquée, on arrive à une paire intriquée. On n'a rien gagné. En revanche, deux trios qui interagissent en détruisant deux photons laissent, eux, un quatuor intriqué, soit un membre de plus. Et ainsi de suite. De quoi, en théorie, étendre une intrication à l'échelle de tout un réseau et faire profiter le plus grand nombre de la magie quantique. ■

D. L.

« On assiste à un boom de ce sujet », salue Sébastien Tanzilli, chercheur CNRS à l'université de Nice et responsable du réseau qui structure la communauté française. Du 13 au 15 novembre à Paris, un colloque a salué les dix ans de cette initiative fédératrice. Les conférenciers européens invités ont exposé leur savoir-faire : fabrique de photons un par un, échange de clés de chiffrement à travers les airs sur un campus, simulation, par la lumière, de dizaines de nœuds de futurs réseaux quantiques, certification de protocoles, correction d'erreurs inhérentes à ces objets fragiles... *« C'est vraiment intéressant de discuter avec des gens d'horizons différents comme des informaticiens, des spécialistes de protocoles et bien sûr des physiciens »*, apprécie Tracy Northup, qui, à l'université d'Innsbruck (Autriche), a déjà réussi à transférer de l'information d'un atome à un photon prêt à partir sur le réseau. Dans quelques mois, elle envisage de se servir de celui-ci pour coupler des atomes à d'autres atomes situés 400 mètres plus loin sur le campus. Ce qui serait l'ébauche du fameux répéteur que tout le monde cherche. En Espagne, au Royaume-Uni ou aux Pays-Bas, d'autres le tenteront aussi. *« Dans deux ans, on aura comme un Arpanet européen »,* espère Elham Kashefi, en évoquant l'embryon historique américain d'Internet dans les années 1970-1980.

Préparer, téléporter, mesurer

Pendant ce temps, le hackathon progresse. Tout le monde a installé un logiciel de simulation d'un réseau quantique, le SimulaQron, développé à l'université de Delft. Le programme remplace par quelques lignes de code toutes les opérations que doivent réaliser les physiciens : préparer des objets quantiques, les téléporter, les mesurer... Sur fond noir, les instructions se succèdent. L'équipe Quantum Winter essaie de programmer un chèque sécurisé. Les Qnoobs veulent transmettre anonymement des informations. *« On a hacké le hackathon ! »,* plaisante Frédéric Grosshans, également du LIP6, dont l'équipe ne respecte pas les règles. Elle s'attaque en effet à un protocole qui n'est pas encore dans le « zoo », car tout juste publié... par le chef de cette équipe. *« Nous aussi, on a hacké ! »,* rétorque un concurrent, qui résout deux problèmes en même temps : finir une animation ludique et pédagogique présentant les bizarreries quantiques (bientôt en ligne sous forme d'un carré magique) et faire du calcul aveugle. La fibre ludique a aussi inspiré l'équipe de Sarajevo qui veut créer un jeu s'inspirant de *Guitar Heroe*, où il s'agit non pas de mettre les doigts au bon endroit sur les cordes d'une guitare, mais de répliquer les mesures quantiques qui arrivent à la queue leu leu... Y arriveront-ils ?

A plus grande échelle, la tension est aussi palpable. La France attend que la mission chargée par le premier ministre d'élaborer une « feuille de route pour les technologies quantiques » rende ses conclusions... depuis septembre. *« Les chercheurs en attendent des moyens, bien sûr, mais nous espérons aussi un plan structurant qui envoie un signal rapidement »,* indique Christophe Jurczak.

SI UN ORDINATEUR QUANTIQUE DÉBARQUE, IL CASSERA LES CLÉS, ET ON POURRA DIRE ADIEU AUX CONNEXIONS SÉCURISÉES EN LIGNE, AUX PAIEMENTS PAR CARTE BANCAIRE...

L'Europe aussi est dans l'attente. En juin, sept pays, mais pas la France, ont signé une « déclaration de coopération » souhaitant la construction d'une infrastructure de communication quantique tant terrestre que spatiale, baptisée QCI. En septembre, un appel d'offres a été émis par l'Union européenne pour financer deux études de faisabilité d'un tel déploiement. Mais, si l'Union veut faire vite, elle devra se tourner vers deux entreprises ayant des systèmes opérationnels, ID Quantique et Toshiba, mais toutes deux extérieures à l'Europe des Vingt-Sept. Cette option serait alors défavorable à l'essor d'une industrie européenne. A l'inverse, elle peut décider de miser à plus long terme sur des technologies plus complexes à développer, ce qui limiterait les retombées pour l'industrie. *« Il est clair que la communauté doit encore démontrer les avantages des technologies quantiques en matière de communication. A long terme, c'est clair, mais beaucoup moins à court ou moyen terme. D'où les hésitations actuelles »,* résume Eleni Diamanti.

Ce dilemme explique pourquoi la France n'a pas rejoint le projet QCI. La sécurité quantique se justifie en partie à cause de la faiblesse actuelle des protocoles de chiffrement. Si un ordinateur quantique débarque, il cassera « facilement » les clés, et on pourra dire adieu aux connexions sécurisées en ligne, aux paiements par carte bancaire... Pire, un espion peut enregistrer aujourd'hui les flux de communication pour les déchiffrer plus tard, lorsqu'une machine quantique sera disponible. Un cauchemar. Les partisans du quantique font valoir que leur canal étant par définition inviolable, ils ont la solution. *« C'est oublier que les protocoles quantiques d'échange de clés fonctionnent point à point entre des nœuds de confiance et pas sur des réseaux multipoints et ouverts comme Internet. Donc, ils ne sont pas adaptés à toutes les applications »*, tempère Romain Alléaume, enseignant-chercheur à Télécom Paris.

Par ailleurs, l'école « classique » n'a pas dit son dernier mot, puisqu'une compétition a été lancée en 2015 pour trouver des algorithmes résistant aux attaques d'un hypothétique ordinateur quantique. Des propositions sont déjà sur la table. *« Les pays qui ont une communauté cryptographique forte, comme la France ou les Etats-Unis, privilégient la crypto classique de nature mathématique et ne sont donc pas trop favorables aux systèmes quantiques d'échange de clés »,* résume Romain Alléaume, qui a répondu, avec un consortium, à l'appel d'offres QCI. En France, c'est en effet la position de l'Agence nationale de la sécurité des systèmes d'information, qui explique au *Monde* que, *« là où les échanges quantiques de clés seraient possibles, il existe en fait aussi des solutions de cryptographie classique »* rendant non nécessaires de fait les technologies quantiques. *« Un des écueils de cette situation est qu'elle ne favorise pas la collaboration avec le monde de la cybersécurité, étape pourtant essentielle à l'essor de solutions industrielles en cryptographie quantique »,* regrette Romain Alléaume.

« Des idées comme des blagues »

Pour sortir de l'impasse, ce dernier propose, comme d'autres, une sécurisation des infrastructures de communication reposant sur une combinaison mêlant classique et quantique. Par exemple, un des défauts des systèmes classiques actuels est qu'ils peuvent être « écoutés » par l'analyse de leur rayonnement, leur consommation électrique... *« On peut imaginer d'intégrer des composants quantiques qui, par définition, ne pourraient pas être écoutés et serviraient de points d'ancrage permettant de renforcer la confiance numérique »,* estime Romain Alléaume. Il songe aussi à des systèmes de stockage où les informations à protéger seraient cassées en morceaux et non stockées en un seul point. Les morceaux seraient ensuite rapatriés via des liens « quantiques ».

Loin de ce tumulte, le soleil se couche dans les jardins de l'hôtel Bourrienne, marquant la fin du hackathon. *« Il y a vingt ans, quand nous écrivions au tableau nos idées comme des blagues, je n'aurais jamais imaginé qu'il y aurait des gens en train de les programmer aujourd'hui »,* estime Elham Kashefi, par ailleurs fondatrice de VeriQloud, une jeune entreprise de développement de logiciels de communication quantique. *« Vous l'avez fait en deux jours ! Soit vous êtes géniaux, soit c'est que ce n'est pas si compliqué »,* a-t-elle ajouté, ironique, en conclusion. Tous n'ont cependant pas été au bout. Les *guitar heroes* de Sarajavo, eux, ont réussi leur pari. Tout comme les Quantum Winter. Sur leur écran défilent les différentes étapes d'un paiement par chèque : fabrication, signature, authentification, paiement...

Ne manque plus qu'à fabriquer les bons vrais photons, à les contrôler, les téléporter... ■

DAVID LAROUSSERIE