OPTIQUE APPLIQUÉE

POUR QUELQUES KILOMÈTRES QUANTIQUES DE PLUS

DES PHYSICIENS GENEVOIS ONT RÉUSSI À **TRANSMETTRE UNE CLÉ QUANTIQUE SECRÈTE À TRAVERS UNE FIBRE OPTIQUE** D'UNE LONGUEUR RECORD DE 421 KM. UNE AVANCÉE SUPPLÉMENTAIRE POUR CETTE TECHNIQUE QUI POURRAIT OFFRIR UNE CONFIDENTIALITÉ ABSOLUE AUX TRANSMISSIONS SUR INTERNET.

Archive ouverte N° 112310

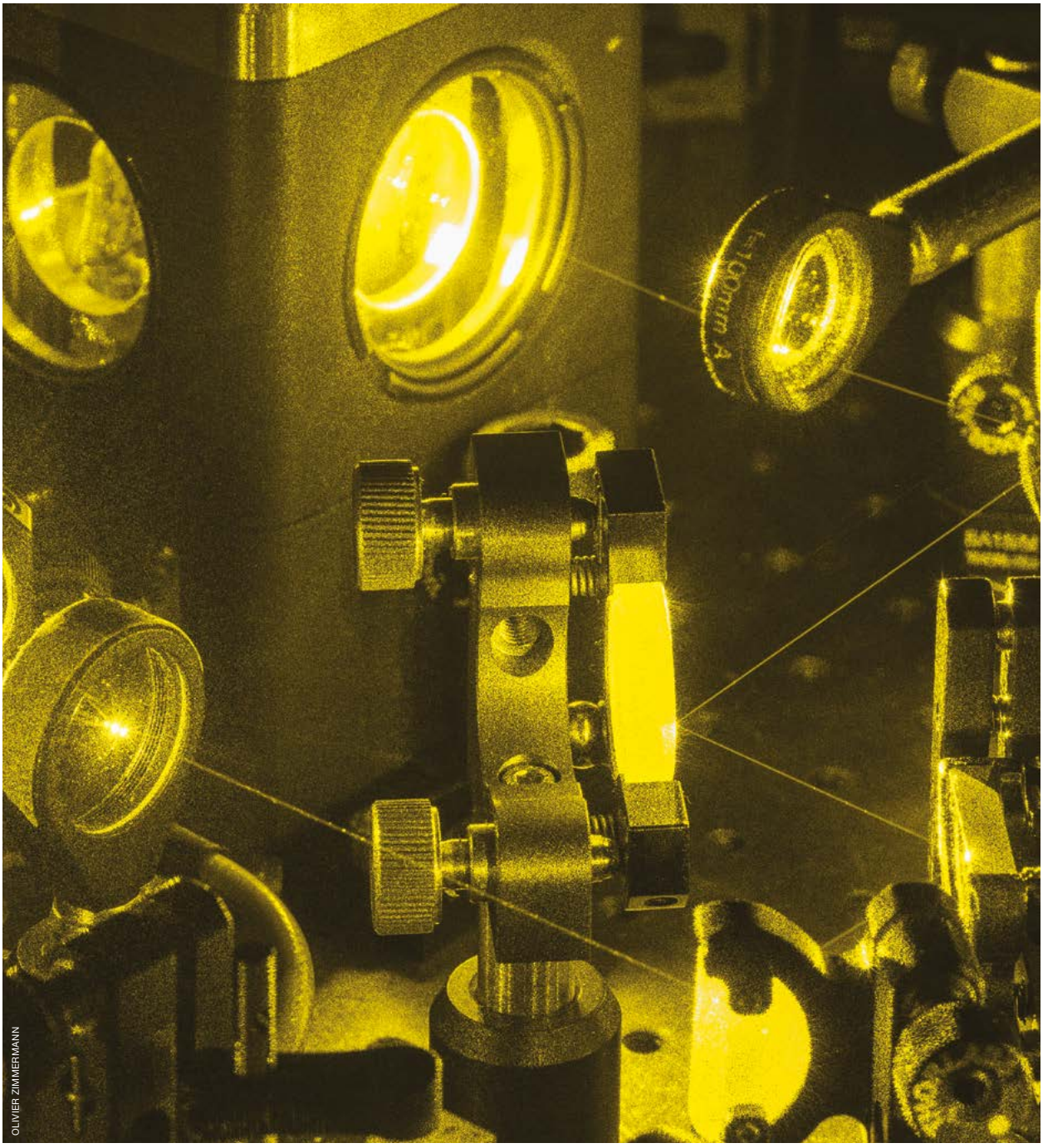
En optimisant toutes les composantes de son montage expérimental, Alberto Boaron a réussi à transmettre une clé de chiffrement quantique à travers 421 kilomètres de fibre optique. Comme le précise un article paru le 3 novembre dans la revue *Physical Review Letters*, le doctorant au Département de physique appliquée (Faculté des sciences) bat ainsi le record de 404 km détenu depuis deux ans par des physiciens chinois tout en améliorant significativement la vitesse de transmission.
Ce n'est d'ailleurs pas tant la perspective de surpasser des concurrents nantis de budgets colossaux qui a motivé Alberto Boaron que celle de pousser au maximum les capacités actuelles de la cryptographie quantique, une technique qui promet la transmission de messages codés impossibles à déchiffrer – même par les futurs mais d'ores et déjà réputés redoutables ordinateurs quantiques.

Donner la clé En cryptographie, une clé de chiffrement permet à l'émetteur (que le jargon appelle Alice) de coder un message et au récepteur (Bob) de le déchiffrer. Crypter un document de manière inviolable est possible (*lire encadré*). Mais transmettre la clé à son interlocuteur – indispensable pour lire le contenu – sans qu'une tierce personne (baptisée Ève) puisse l'intercepter, la deviner ou la casser est nettement plus hasardeux.
On peut transporter physiquement des clés dans des fourgons sécurisés ou des valises diplomatiques mais une telle opération est lourde et comporte des risques évidents. Échanger des clés par Internet n'est pas très prudent non plus tant le réseau global est massivement espionné par différentes agences gouvernementales.
Pour contourner ces faiblesses, les techniques de chiffrement actuelles dans les télécommunications utilisent des algorithmes et des constructions complexes (avec notamment des systèmes asymétriques comprenant des clés publiques et privées). Cependant, toutes demeurent cassables à condition de disposer d'une puissance de calcul adaptée.

LES ORDINATEURS QUANTIQUES POURRAIENT RÉSOUDRE DES PROBLÈMES JUSQUE-LÀ INSOLUBLES ET, SURTOUT, CASSER LES CLÉS DE CHIFFREMENT CLASSIQUES LES PLUS COMPLEXES.

La grande menace vient des ordinateurs quantiques. Ces machines, qui sont basées sur les propriétés contre-intuitives de la physique quantique, la théorie qui décrit le monde à toute petite échelle, n'existent pas encore. Mais un nombre croissant d'équipes dans le monde travaillent à leur conception. Ces appareils ne seraient pas forcément plus rapides que les ordinateurs conventionnels mais auraient un fonctionnement différent. Ils pourraient résoudre des problèmes jusque-là insolubles et, surtout, casser – avec une grande facilité, prétendent certains – les clés de chiffrement classiques les plus complexes.

Confidentialité Face à la puissance de ces machines du futur, la communication quantique, et en particulier la distribution sécurisée d'une clé quantique (QKD, pour *Quantum Key Distribution*), se profile comme la seule solution capable d'assurer un cryptage d'une confidentialité absolue.
L'idée de la QKD consiste à transmettre un à un des photons d'Alice à Bob. Chacune de ces



OLIVIER ZIMMERMANN

Montage optique avec un laser et différentes lentilles, qui a servi à l'expérience de cryptographie quantique.

Une course internationale. Bien qu'il soit impossible de connaître les montants avec précision, la Chine a investi ces dernières années des sommes très importantes dans la conception et le développement d'ordinateurs quantiques, de réseaux quantiques et même d'un satellite quantique. Cela lui a permis de devenir leader dans de nombreux domaines, notamment dans la communication quantique, tandis que les géants américains Google et Microsoft sont en avance dans la recherche sur l'ordinateur quantique.

L'Europe cherche, quant à elle, à rester dans la course grâce au lancement du Quantum Flagship. Ce programme est doté d'un milliard d'euros sur dix ans. L'Université de Genève participe à trois projets (dont un dirigé par Hugo Zbinden, professeur au Département de physique appliquée) sur la vingtaine retenue.

DE 32 CENTIMÈTRES À 1200 KILOMÈTRES

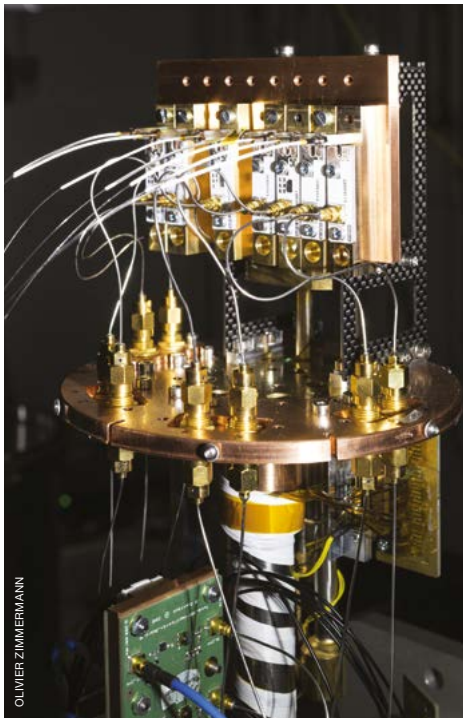
La première distribution d'une clé quantique (QKD) a été réalisée en 1992 par des chercheurs américains et canadiens. Les photons ont traversé l'air sur une distance de 32 centimètres. Grâce aux progrès technologiques, il existe désormais des dispositifs basés sur les fibres optiques permettant de distribuer une clé quantique sur quelques centaines de kilomètres de distance.

Le record précédent de 404 kilomètres (battu depuis par les physiciens genevois, lire article principal), établi en 2016, a été obtenu par une équipe de l'Université de sciences et de technologie de Hefei en Chine. En 2017, une autre expérience de QKD a eu lieu entre le satellite chinois Micius – placé en orbite basse autour de la Terre – et des récepteurs terrestres, comme le rapporte un article paru dans la revue *Nature* du 9 août 2017. Profitant du vide de l'espace, des photons porteurs de l'information quantique ont ainsi pu parcourir pas moins de 1200 kilomètres. Les particules leur sont parvenues à un rythme de 1 kHz, c'est-à-dire 1000 fois par seconde.
Le problème du satellite, c'est qu'il ne fonctionne qu'en l'absence de nuages. Il nécessite également beaucoup de temps pour transmettre une clé assez grande pour être utile alors qu'il bouge rapidement dans le ciel. À cela s'ajoutent d'importants problèmes de synchronisation entre l'émetteur, le récepteur et le satellite. Malgré ces obstacles, la Chine prévoit de lancer d'autres satellites dans les quatre ou cinq ans à venir, dont un placé bien plus haut, sur une orbite géostationnaire.

APRÈS 421 KILOMÈTRES, SEUL 1 PHOTON SUR 10 MILLIONS RÉUSSIT À TRAVERSER LA FIBRE SANS ÊTRE DIFFUSÉ OU ABSORBÉ PAR LA MATIÈRE.

Le masque jetable, également appelé chiffre de Vernam, est un chiffrement théoriquement impossible à casser. Le principe est simple. La clé de chiffrement doit être une suite de caractères au moins aussi longue que le message à chiffrer, les caractères composant la clé doivent être choisis de façon totalement aléatoire et chaque clé ne doit être utilisée qu'une seule fois.

Pour l'espion qui ne connaît que le texte chiffré, toutes les clés imaginables sont équiprobables, ce qui signifie que tous les textes clairs de cette longueur sont possibles et avec la même probabilité.



OLIVIER ZIMMERMANN

particules de lumière est placée dans un « état quantique » qui est parfaitement aléatoire mais qui ne peut prendre que deux valeurs. La mesure de la succession de ces états se traduit par une série de *0* et de *1*, ce qui permet de construire progressivement une clé de chiffrement de la longueur désirée en fonction du temps à disposition.

L'avantage d'une telle transmission est son inviolabilité. Si Ève choisit de pirater la transmission de la clé entre Alice et Bob, elle est obligée de mesurer l'état quantique des photons qui passent. Une telle action détruirait la particule ou la perturberait suffisamment pour alerter Alice et Bob de la présence de l'espionne. Et même si l'indésirable parvenait à « lire » certains des photons sans interrompre la communication, il existe des protocoles subtils permettant de réduire à zéro la quantité d'information, qu'elle pourrait en retirer.

« *La physique quantique offre la possibilité de générer des clés de chiffrement parfaitement aléatoires et de n'importe quelle longueur et de les transmettre d'Alice à Bob de manière totalement confidentielle*, résume Hugo Zbinden, professeur au Département de physique appliquée et directeur de la thèse d'Alberto Boaron. *En pratique, toutefois, elle est limitée par de nombreux facteurs tels que l'atténuation du signal dans la fibre, le « bruit » du détecteur, etc.* »

Partir fort Le travail d'Alberto Boaron a donc consisté à optimiser chaque étape du dispositif de QKD. La première est le générateur d'états quantiques que le physicien genevois a réussi à améliorer de manière à ce qu'il produise 2,5 milliards d'impulsions par seconde, soit le taux le plus haut jamais atteint à ce jour. « *C'est important de partir fort, car les pertes sont nombreuses en chemin* », précise Alberto Boaron. Elles commencent d'ailleurs avec la fibre optique elle-même. Même si l'expérience utilise le meilleur produit disponible sur le marché, après 421 kilomètres, seul 1 photon sur 10 millions réussit à traverser la fibre sans être diffusé ou absorbé par la matière.

Le système de détection, basé sur la technologie des supraconducteurs et fonctionnant à une température de 0,8 K, est développé depuis cinq ans dans le laboratoire genevois. Il est capable de détecter un photon à la fois avec un niveau de bruit particulièrement bas mais aussi avec une efficacité située entre 40 et 60%.

Mille fois plus efficace Enfin, les physiciens ont modifié le protocole d'acquisition de la clé de chiffrement quantique. Ils l'ont simplifié sans réduire les performances de sécurité. En additionnant toutes les composantes, Alberto Boaron a réussi à faire en sorte que, sur une distance de plus de 400 km, Bob reçoive d'Alice toutes les 2 secondes un bit (un *0* ou un *1*) utilisable pour fabriquer sa clé secrète. En faisant tourner le système 12,7 heures (sans tenir compte des interruptions), il a ainsi extrait une clé de 22 124 bits. Cela peut paraître lent, mais c'est un taux plus de 1000 fois plus élevé que celui de l'expérience chinoise (qui a obtenu une clé de seulement 2584 bits en trois mois).

Cela dit, les améliorations apportées par les chercheurs genevois sont surtout utiles pour les distances plus courtes, de l'ordre de 100 km, suffisantes pour relier deux villes voisines, par exemple. Pour une telle longueur de fibre et avec le dispositif mis au point par Alberto Boaron, la vitesse d'acquisition avoisine actuellement le million de bits par seconde. Une expérience en cours vise à atteindre une valeur 100 fois plus élevée. Cependant, si l'on veut construire un réseau de cryptographie quantique plus étendu, à l'échelle d'un pays ou d'un continent, l'utilisation de relais s'avère indispensable. La Chine a déjà commencé à fabriquer un tel système sur plus de 2000 km entre Pékin et Shanghai. Le problème, c'est qu'il n'existe pas encore de relais quantiques dignes de ce nom – dotés d'une mémoire et d'un répéteur eux aussi quantiques – capables de reproduire le signal de manière confidentielle. Pour l'instant, il est en effet nécessaire de faire confiance aux gestionnaires de ces relais où transite de manière classique l'information concernant les clés quantiques. En Chine, c'est le gouvernement qui en a le contrôle. Il est peu probable qu'une telle configuration soit acceptable dans les démocraties occidentales.

Anton Vos