Comment LA PHYSIQUE protégera notre vie

QUANTIQUE privée

Artur Ekert et Renato Renner

Les méthodes de chiffrement actuelles ne sont pas aussi fiables qu'on le pense. Comment alors protéger nos données et nos communications ? Des recherches récentes montrent que la cryptographie quantique offre des solutions robustes.

L'écrivain américain et cryptographe amateur Edgar Allan Poe constatait dans sa nouvelle *Le Scarabée d'or* (1843) : « On peut affirmer sans ambages que l'ingéniosité humaine ne saurait concocter un code secret que l'ingéniosité humaine ne puisse résoudre. » Dès lors, sommes-nous condamnés à devoir renoncer à la confidentialité de nos communications, quels que soient nos efforts pour protéger notre vie privée ? Si l'histoire des communications secrètes peut servir de guide en la matière, la réponse est un « oui » retentissant. Les exemples ne manquent pas pour illustrer comment les efforts des meilleurs codeurs ont toujours été rattrapés par l'ingéniosité des décrypteurs. Il pourrait en aller autrement avec la cryptographie quantique, imaginée il y a près de trente ans. Les progrès les plus récents dans ce domaine confirment qu'il

Kenn Brown/Mondolithic Studio

est possible de concevoir des systèmes de chiffrement capables de protéger la vie privée de façon fiable.

Dans le domaine du chiffrement, être paranoïaque est un atout. S'interroger de façon systématique sur les qualités et les défauts d'un système qui chiffre des données permet de se prémunir des mauvaises surprises. Ainsi, il est naturel de se poser les questions suivantes : nos secrets sont-ils à l'abri d'adversaires qui détiennent une capacité technologique supérieure ? Peut-on faire confiance à ceux qui nous fournissent les systèmes de chiffrement ou même peut-on avoir confiance en nous-même, en notre libre arbitre ? Les systèmes de chiffrement modernes n'y répondent pas toujours à la hauteur de nos espérances. Cependant, la physique quantique va nous offrir des solutions efficaces.

La menace de l'ordinateur quantique

L'alliée de demain en matière de chiffrement est ainsi la physique quantique. De façon étonnante, elle est aussi le domaine de recherche dont les progrès mettent en péril les systèmes de chiffrement utilisés quotidiennement dans notre monde hyperconnecté. En effet, nos courriels ou nos données bancaires, bien que chiffrés, ne sont pas à l'abri d'avancées techniques dont profiteraient les indiscrets. L'une des plus grandes menaces aujourd'hui est la possibilité de construire un ordinateur quantique. Un tel dispositif, dont les capacités de calcul reposent sur les principes de la physique quantique, décrypterait rapidement les messages chiffrés par les meilleurs systèmes utilisés aujourd'hui.

Par exemple, une méthode de chiffrement très répandue est le système RSA, proposé en 1977. Son principe repose sur deux clés, l'une publique et l'autre privée *(voir l'encadré page ci-contre)*. Une personne désirant vous envoyer un message chiffré utilisera votre clé publique, connue de tous. Mais seule la clé privée, que vous êtes le seul à connaître, permet d'inverser la procédure pour récupérer le message en clair. Les deux clés ne sont pas arbitraires : la clé publique est un très grand nombre, égal au produit de deux nombres premiers qui constituent la clé privée. Ainsi, une façon d'attaquer le système pour décrypter le message consiste à déterminer les nombres premiers dont est composée la clé publique. Or la factorisation d'un grand nombre est un problème dit difficile, car il requiert beaucoup de calculs qui dépassent les capacités des ordinateurs actuels. Avec le système RSA, vos données sont *a priori* bien protégées.

Cependant, en 1994, le mathématicien Peter Shor, alors aux laboratoires d'AT&T-Bell, a montré qu'un ordinateur quantique pourrait factoriser de grands nombres assez rapidement. L'algorithme de Shor rendrait ainsi le système RSA obsolète – à condition que l'on parvienne à fabriquer un ordinateur quantique ! Ce ne sera probablement pas le cas avant plusieurs décennies, mais qui peut prouver, ou donner des garanties fiables, que cet horizon est si lointain ? Ainsi, c'est sur la confiance en la lenteur du progrès technologique que repose la sécurité des meilleures méthodes actuelles de chiffrement.

Il est donc raisonnable de chercher d'autres façons de chiffrer nos données. Pour y parvenir, il est important de bien comprendre les exigences d'une communication parfaitement sécurisée. En substance, tout ce dont nous avons besoin pour construire un chiffrement parfait est de partager une séquence de bits aléatoires, la « clé de chiffrement ». Deux utilisateurs (traditionnellement nommés Alice et Bob) partagent la clé, qu'ils utilisent pour communiquer secrètement grâce à une procédure de chiffrement. Une méthode simple et supposée inviolable est le masque jetable, ou chiffre de Vernam. La clé est une suite de caractères au moins aussi longue que le message à chiffrer. Chaque lettre du message est combinée à un caractère de la clé, dont on additionne les valeurs (A = 1, B = 2, etc.) pour donner une nouvelle lettre.

On suppose robuste la méthode tant que le masque est une suite aléatoire de caractères et que chaque masque n'est utilisé qu'une fois. Même si elle connaît la méthode générale de chiffrement, une tierce personne – Ève – qui intercepte le message chiffré ne sera pas en mesure d'en tirer des informations utiles sans la clé. Mais cette méthode pose un problème insoluble, celui de la distribution de la clé : comment Alice et Bob peuvent-ils se transmettre cette dernière en toute sécurité ? Les méthodes de cryptographie asymétrique à deux clés, telles que RSA, contournent la difficulté. Cependant, comme nous l'avons vu, elles pourraient un jour devenir vulnérables.

La cryptographie quantique offre une solution alternative au problème de la distribution des clés. En s'appuyant sur

L'ESSENTIEL

- La réalisation d'un ordinateur quantique rendrait caduques les méthodes de cryptage actuelles.
- Des méthodes de chiffrement fondées sur des propriétés quantiques, dont l'idée a été émise il y a plus de vingt ans, pourraient contrer cette menace.
- Des chercheurs ont montré que, moyennant certaines conditions, la cryptographie quantique peut assurer une confidentialité parfaite.
- Plusieurs dispositifs de cryptage quantique sont déjà en service dans le monde.

des propriétés des systèmes quantiques, Alice et Bob pourraient échanger certaines informations leur permettant de construire une clé commune. Ils seraient aussi en mesure de savoir si ces informations ont été interceptées et, le cas échéant, de décider de définir une nouvelle clé.

Une solution idéale contre l'espionnage

La distribution quantique des clés a d'abord été proposée en 1984 par Charles Bennett, chercheur chez IBM, et Gilles Brassard, alors à l'université Cornell. La sécurité de la transmission de la clé y est garantie par le principe d'incertitude de Heisenberg, selon lequel certaines paires de propriétés physiques, telles la position et la quantité de mouvement d'une particule, sont complémentaires et ne peuvent être connues avec précision simultanément. Cette idée a été appliquée à la polarisation de photons *(voir l'encadré pages 30 et 31)*. Puis, en 1991, l'un de nous (Artur Ekert) a proposé un dispositif de distribution quantique des clés reposant sur la « monogamie de l'intrication quantique », propriété de certaines corrélations quantiques qui ne peuvent être partagées avec plus d'une personne. Nous y reviendrons.

L'idée d'utiliser des phénomènes quantiques pour améliorer le secret des communications n'était au début qu'une simple curiosité académique, mais, avec les progrès des technologies, elle a été reprise par les physiciens expérimentateurs et finalement développée en une proposition commerciale viable *(voir l'encadré page 33)*.

En théorie, la cryptographie quantique offre le système de chiffrement le plus sécurisé. En pratique, cependant, tout système peut présenter des failles de conception, qui exposent les données chiffrées à des attaques. De telles failles peuvent être involontaires, résultant de l'ignorance ou de la négligence d'individus honnêtes qui conçoivent les systèmes de chiffrement quantique ; mais elles peuvent aussi être malveillantes, implantées subrepticement par des adversaires puissants.

Étant donné que certains des défauts peuvent nous être inconnus, comment avoir la certitude que personne n'intercepte nos communications ? Ce maillon faible semblait incontournable et nous avons longtemps

LES AUTEURS


Artur EKERT est professeur de physique quantique à l'université d'Oxford, en Grande-Bretagne, et directeur du Centre des technologies quantiques de l'université de Singapour.

Renato RENNER est directeur de recherche à l'Institut de physique théorique de l'École polytechnique de Zurich, en Suisse.

Article publié avec l'aimable autorisation de *Nature*.

CHIFFRER DES DONNÉES AUJOURD'HUI

À chaque fois que vous faites un achat sur Internet, votre navigateur et le site du vendeur doivent échanger une clé pour chiffrer les informations qui seront transmises. Avec le chiffrement symétrique, les interlocuteurs utilisent la même clé. Dans le cas du chiffrement asymétrique, tel RSA, une clé publique sert à chiffrer les messages, une autre est gardée secrète pour les déchiffrer.

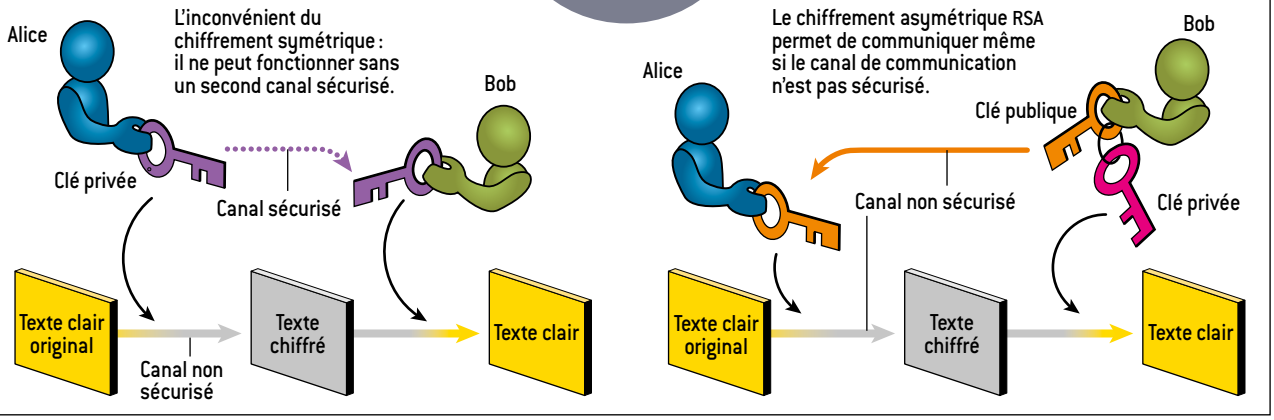
CHIFFREMENT SYMÉTRIQUE

Alice chiffre son message avec une clé et le transmet à Bob. Si quelqu'un intercepte le message, celui-ci sera illisible. Pour retrouver le message en clair, Bob utilise la même clé, envoyée par Alice sur un canal caché et sécurisé.

Le chiffrement asymétrique RSA est fiable dans la mesure où les ordinateurs classiques ne peuvent factoriser de grands nombres.

CHIFFREMENT ASYMÉTRIQUE RSA

Bob, le destinataire du message, définit deux clés : une clé publique – un très grand nombre –, qu'Alice utilise pour chiffrer son message, et une clé privée – deux nombres premiers dont le produit est égal à la clé publique – que Bob utilise pour déchiffrer.



Jen Christiansen

cru que les limites de la confidentialité étaient là : aussi efficace que soit le système de chiffrement utilisé, tout espion technologiquement plus avancé aura le dessus – que ce soit la NSA ou le FBI, par exemple. Or il s'est avéré que la cryptographie quantique n'est pas exposée aux failles possibles du système. Elle peut en effet garantir la confidentialité avec un minimum d'ingrédients : d'une part, des corrélations monogames, à savoir des liens entre grandeurs physiques que seuls Alice et Bob peuvent mesurer ; d'autre part, une petite dose de « libre arbitre », défini ici comme la capacité de faire des choix indépendants de tout ce qui est préexistant, donc des choix imprévisibles.

Ces conditions suffisent pour créer et distribuer des clés sûres. Plus étonnant, elles assurent que, même si nous utilisons des dispositifs de provenance inconnue ou douteuse, voire fabriqués par nos ennemis, la sécurité des données est assurée.

Évidemment, quelques précautions sont de mise : les dispositifs de chiffrement doivent être placés dans des lieux bien isolés pour empêcher toute fuite des données enregistrées servant à construire la clé de chiffrement, et seules des personnes de confiance doivent y avoir accès. Dans ces conditions, on montre qu'un test statistique suffit pour valider la sécurité du système, même sans aucune connaissance de son fonctionnement interne. On parle de cryptographie « indépendante du dispositif ». Ces dernières années, des progrès rapides ont permis de confirmer la fiabilité de ce type de cryptographie, qui constitue l'un des domaines de recherche les plus actifs en sciences de l'information quantique.

Communiquer avec des pièces magiques

Nous avons présenté les concepts essentiels de la cryptographie quantique. Cependant, il reste à clarifier les notions de corrélation monogame et de libre arbitre et à voir comment les mettre en œuvre. Comme nous l'avons souligné, le problème crucial est celui de la distribution de la clé de chiffrement : pour que leur communication reste confidentielle, Alice et Bob doivent trouver un moyen de générer et se partager les bits de la clé. Comment faire ? Dans un premier temps, imaginons un système fictif qui illustre les notions cruciales de corrélations monogames et de libre arbitre.

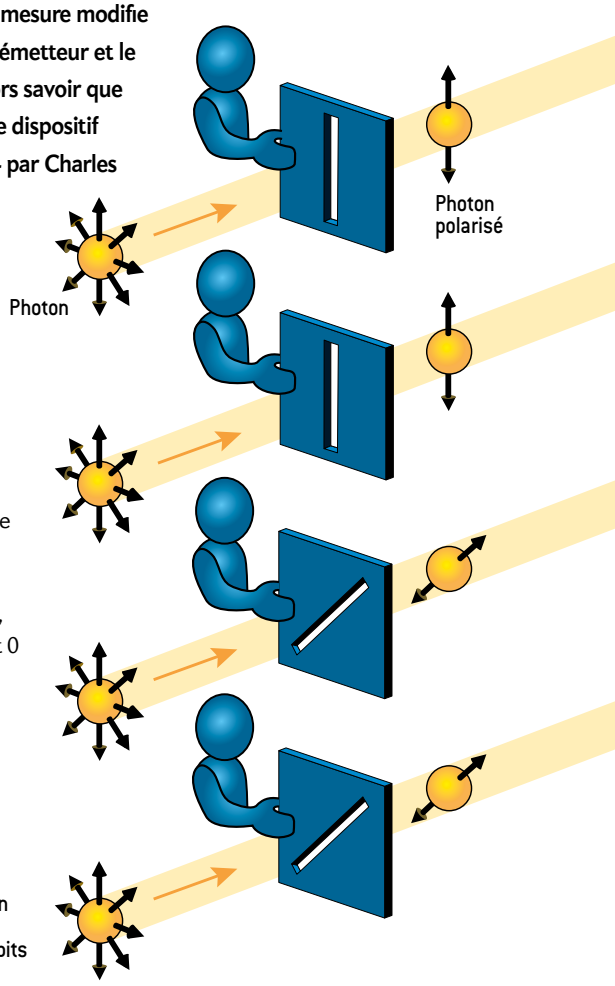
Supposons que l'on dispose de deux pièces de monnaie liées de façon magique, de telle sorte qu'elles présentent toujours le même côté lorsqu'on les tire à pile ou face (et en supposant que le côté pile a la même probabilité d'apparaître que le côté face). Alice et Bob, chacun muni d'une pièce, peuvent alors lancer ces pièces en notant « 0 » pour face et « 1 » pour pile. Après plusieurs lancers, la chaîne binaire obtenue, la clé, est aléatoire et connue simultanément d'Alice et de Bob.

Cette clé est-elle secrète ? Pas nécessairement. Ève, munie de capacités technologiques supérieures, pourrait fabriquer une pièce supplémentaire, magiquement liée à celles détenues par Alice et Bob. Les trois pièces concordant toujours, Ève connaîtrait aussi les bits obtenus par Alice et Bob.

À l'évidence, pour que le secret soit garanti, Alice et Bob doivent pouvoir faire quelque chose qui échappe au contrôle d'Ève. Par exemple, Alice et Bob peuvent avoir le choix entre deux pièces différentes (A_1 ou A_2 pour Alice, B_1 ou B_2 pour Bob). Pour chaque lancer, chacun n'utilise qu'une pièce et il est interdit de lancer ses deux pièces en même temps. On suppose les liens magiques tels que les pièces d'Alice et de Bob donnent toujours un résultat identique, sauf quand ils lancent A_1 et B_2, qui donnent toujours

CHIFFRER SES DONNÉES GRÂCE À LA PHYSIQUE QUANTIQUE

En cryptographie quantique, la distribution d'une clé se fait grâce à un flux de photons polarisés (présentant une direction de spin particulière). Si une tierce personne tente de mesurer la polarisation de ces photons en chemin, le seul acte de la mesure modifie la polarisation de certains photons. L'émetteur et le destinataire du message pourront alors savoir que quelqu'un a tenté de lire l'échange. Le dispositif présenté ici est celui imaginé en 1984 par Charles Bennett et Gilles Brassard.



Jen Christiansen

un résultat opposé. Cette magie peut être résumée par les quatre conditions suivantes :

$A_1 = B_1$ $\quad B_1 = A_2$

$A_2 = B_2$ $\quad B_2 \neq A_1$

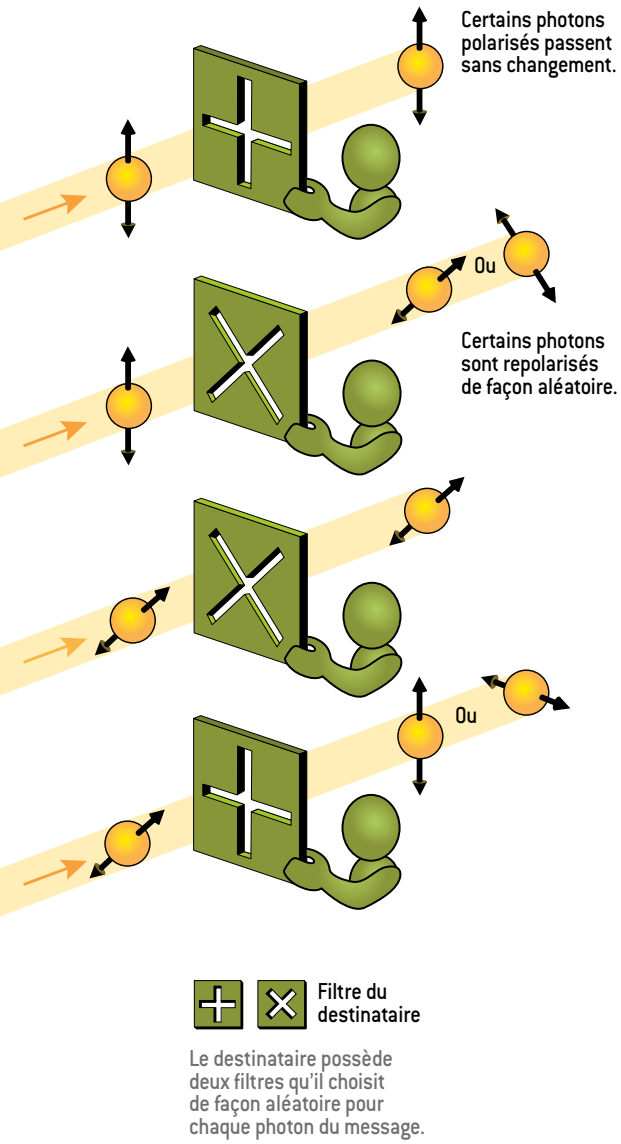
Ces conditions sont clairement contradictoires : il est impossible d'assigner à A_1, A_2, B_1 et B_2 des valeurs telles que les quatre conditions soient simultanément satisfaites. Mais il faut se rappeler qu'Alice et Bob ne peuvent lancer qu'une pièce chacun, et qu'ils ne peuvent donc tester qu'une seule des quatre conditions à la fois ; cela ne conduit à aucune contradiction.

Mais si, par exemple, Alice enfreint la règle et lance ses deux pièces A_1 et A_2 en même temps, que se passe-t-il ? Supposons qu'Alice obtienne deux faces ou deux piles ($A_1 = A_2$) ; alors Bob n'a pas d'autre choix que de lancer B_1, parce que c'est le seul lancer compatible avec les conditions des pièces magiques. De la même façon, si Alice obtient une pièce face et une pièce pile ($A_1 \neq A_2$), le seul choix qui reste à Bob est de lancer B_2.

Ainsi, lorsque Alice lance ses deux pièces, elle prive Bob de sa liberté de choisir la pièce qu'il veut tirer. Cette situation bizarre implique qu'Alice ne peut pas lancer ses deux pièces en même temps, sous peine de contradictions. Cela implique aussi que les pièces magiques ne peuvent pas être clonées. Si Ève avait une pièce Z constituant un clone de A_1, lorsque Alice lance A_2, on retrouverait des contradictions comme précédemment.

En conclusion, si les choix d'Alice et de Bob sont libres, les corrélations doivent être monogames, c'est-à-dire qu'aucune pièce tierce ne peut être corrélée à A_1, A_2, B_1 ou B_2. Cela redonne à Alice et Bob l'avantage sur Ève : ni elle, ni personne d'autre ne peut fabriquer une pièce qui correspondra toujours avec l'une quelconque des pièces détenues par Alice et Bob.

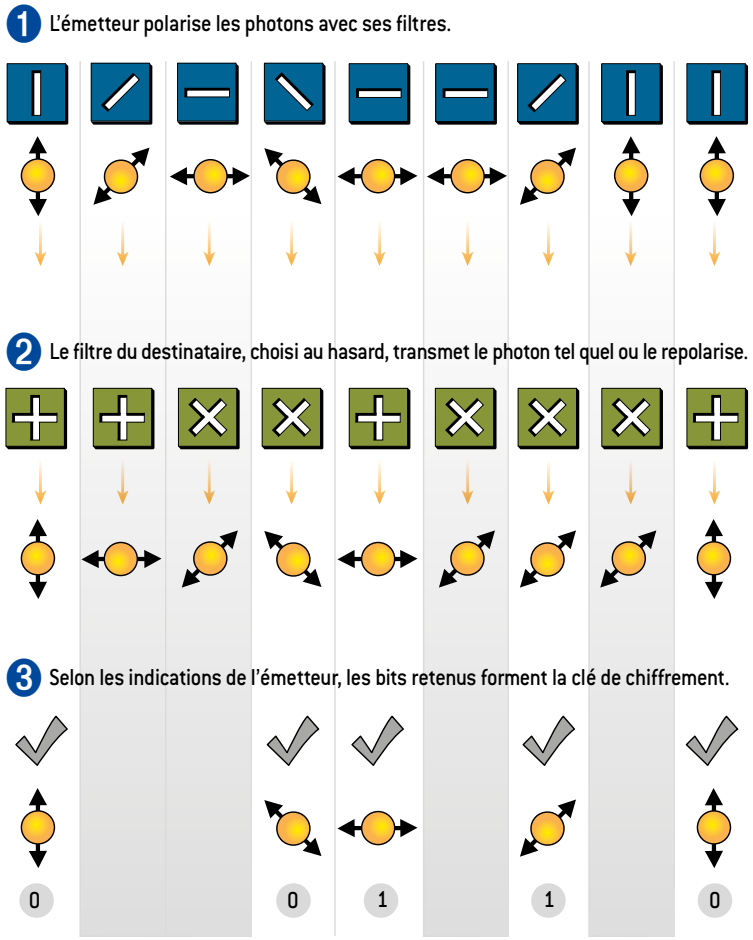
Tous les ingrédients de la distribution sécurisée des clés sont désormais en place. Concrètement, pour créer une clé de chiffrement, Alice et Bob lancent leurs pièces magiques. À chaque lancer, Alice et Bob

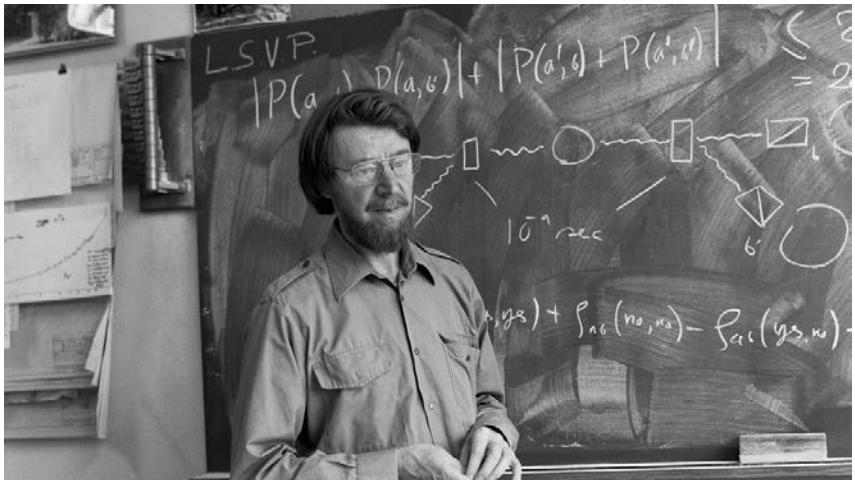


Le destinataire possède deux filtres qu'il choisit de façon aléatoire pour chaque photon du message.

DÉFINIR UNE CLÉ DE CHIFFREMENT

Le destinataire enregistre la polarisation de chaque photon reçu, puis précise publiquement quelle séquence de filtres il a utilisée. L'émetteur lui indique alors, en fonction de sa propre séquence de filtres, ceux qui n'ont *a priori* pas modifié le photon transmis. Les bits correspondants forment la clé.





© CERN

LE PHYSICIEN JOHN BELL pose devant un tableau sur lequel figure *(en haut)* une certaine formulation des inégalités qui portent son nom, en 1982. Le schéma décrit le principe d'une expérience qui permet de vérifier expérimentalement si les inégalités de Bell sont violées, conformément aux prévisions de la théorie quantique. Une telle expérience a été menée en France par l'équipe d'Alain Aspect la même année.

choisissent au hasard et indépendamment l'un de l'autre la pièce concernée. Après le lancer, ils annoncent publiquement la pièce que chacun a choisie, mais pas le résultat obtenu. Comme les pièces vérifient les conditions énoncées précédemment, Alice et Bob savent ce que l'autre a obtenu : un résultat identique, sauf quand A_1 et B_2 ont été lancés, auquel cas les deux résultats sont opposés. Ève n'a aucun moyen de connaître le résultat puisqu'elle ne peut pas cloner les pièces. Pour établir une clé plus longue, Alice et Bob répètent simplement la procédure autant de fois que nécessaire.

Remarquons qu'Alice et Bob n'ont pas besoin de faire des hypothèses sur la provenance des pièces. Tant que les pièces vérifient les quatre conditions des pièces magiques, la sécurité du chiffrement est garantie. Pour s'assurer que les pièces vérifient effectivement ces conditions et n'ont pas été truquées ou clonées par un ennemi, Alice et Bob se communiquent les résultats d'un certain nombre de tirages choisis au hasard et vérifient s'ils sont en accord avec les conditions des pièces magiques. Ces résultats dévoilés publiquement sont ensuite éliminés, et la clé est composée des résultats des lancers restants, qui n'ont jamais été révélés publiquement. Si Alice et Bob remarquent un désaccord dans les tirages comparés, cela signifie que quelqu'un a essayé d'intercepter la clé. Alice et Bob jettent l'ensemble des bits de la clé et font un nouvel essai avec un autre jeu de pièces.

Bien sûr, Alice et Bob doivent s'assurer que le résultat des lancers non révélés, qui sert à construire la clé, est sous bonne garde. Il faut aussi supposer qu'Alice et Bob communiquent publiquement sans que personne ne modifie leurs messages ou n'usurpe leur identité. Dès lors, le secret de la clé est uniquement fondé sur la monogamie des corrélations magiques et sur une hypothèse anodine mais essentielle : Alice comme Bob peuvent choisir librement la pièce à lancer.

Des photons polarisés et intriqués

Il semble que nous ayons atteint notre objectif : Alice et Bob sont capables de générer et communiquer une clé de façon sécurisée. Il n'y a qu'un petit ennui avec notre solution au problème de distribution des clés : les corrélations magiques n'existent pas. En d'autres termes, nous ne connaissons aucun processus physique qui puisse les reproduire. Mais tout n'est pas perdu, car il existe des corrélations physiques suffisamment « magiques » pour nos besoins : bienvenue dans le monde quantique !

La théorie quantique gouverne tous les objets, grands et petits, mais ses conséquences sont plus marquées dans les systèmes microscopiques tels que les atomes individuels et les photons. Pour concevoir des systèmes quantiques de chiffrement, nous faisons appel à des photons polarisés, c'est-à-dire de polarisation bien définie. La polarisation d'un photon correspond à la direction de son spin (son moment cinétique intrinsèque).

Quand on mesure la polarisation selon une direction, seuls deux résultats sont possibles, indiquant si la polarisation du photon juste après la mesure est parallèle ou orthogonale à la direction de mesure. Nous noterons 1 et 0 ces résultats.

Pour le système de chiffrement d'Alice et Bob, les photons polarisés doivent être, en plus, « intriqués ». Deux objets quantiques (ici deux photons) sont intriqués lorsque les états qui les décrivent sont indissolublement liés. La mesure de la polarisation d'un des deux photons intriqués fixe son état de polarisation et, simultanément et instantanément, fixe celui de l'autre photon, même si ce dernier est très éloigné. Cette intrication a ainsi un caractère non local : les états des deux photons sont corrélés même si aucun signal n'a eu le temps d'être échangé entre les deux particules.

Albert Einstein, très attaché au principe de localité, était un farouche critique de l'intrication quantique. En 1935, avec Boris Podolsky et Nathan Rosen, il a formulé ses objections sous la forme d'un paradoxe (connu sous le nom de paradoxe EPR). Pour ces trois physiciens, l'intrication quantique impliquait soit que les deux particules ont échangé des informations qui se propagent plus vite que la lumière (ce qui violerait la théorie de la relativité restreinte), soit que la physique quantique est incomplète et que des « variables cachées », inconnues des physiciens, donnent l'illusion de l'intrication quantique.

Le physicien danois Niels Bohr, en revanche, a souligné qu'il n'y a pas de contradiction si l'intrication quantique est un phénomène non local, indépendant de la position des particules. En 1964, le physicien nord-irlandais John Bell a formalisé la question du paradoxe EPR sous la forme d'inégalités qui portent son nom, et qui sont violées si l'intrication est non locale.

Les inégalités de Bell jouent un rôle crucial dans le système de chiffrement quantique. Voyons comment. On remplace les pièces magiques d'Alice et de Bob par des paires de photons intriqués (les physiciens disposent de diverses techniques pour produire des paires de photons intriqués en polarisation). Une source émet ces paires, dont un photon est envoyé à Alice et l'autre à Bob. Au lieu de lancer des pièces magiques, Alice et Bob mesurent la polarisation des photons selon des directions particulières, définies par des angles notés α_1 et α_2 pour Alice et β_1 et β_2 pour Bob. Pour chaque

paire de photons intriqués, Alice et Bob choisissent chacun une direction de mesure de la polarisation. Les photons étant intriqués, ils répondent de façon coordonnée aux mesures effectuées séparément.

L'intrication quantique joue le rôle de la connexion magique entre les pièces, mais la situation physique des photons n'est pas aussi simple que celle des pièces magiques. Par exemple, si Alice utilise la pièce A_1 et Bob la pièce B_1, ils obtiendront à coup sûr le même résultat. Avec les photons, la probabilité qu'Alice et Bob trouvent le même résultat est égale à $\cos^2(\alpha - \beta)$. On définit une grandeur, notée ε, qui quantifie la déviation par rapport aux corrélations des pièces magiques ($\varepsilon = 0$ correspond au cas des pièces magiques). On montre alors que pour tout choix d'angles, il est impossible d'annuler ε. La valeur physique la plus petite admissible pour ε est 0,146. On l'obtient avec les angles $\alpha_1 = 0$, $\alpha_2 = 2\pi/8$, $\beta_1 = \pi/8$ et $\beta_2 = 3\pi/8$.

Il est ainsi impossible de fabriquer des pièces magiques à partir des photons polarisés et intriqués. Or la connexion magique des pièces garantissait qu'Ève ne puisse pas espionner la discussion entre Alice et Bob. La question qui se pose est donc de savoir si une valeur non nulle de ε permet d'avoir un système de chiffrement fiable. La réponse est oui : il est possible de montrer que l'on obtient un système opérationnel avec des valeurs basses de ε.

Les inégalités de Bell à l'épreuve

Lorsque $\varepsilon \geqslant 1/4$, les corrélations sont dites classiques ; dans cette situation, on peut supposer, sans que l'on se heurte à des contradictions, que les polarisations selon les angles α_1, α_2, β_1 et β_2 ont une valeur bien définie avant la mesure. Ce n'est plus le cas quand $\varepsilon < 1/4$; dans cette situation, supposer que les polarisations ont des valeurs préalables à la mesure conduit à la violation de l'une au moins des quatre conditions des pièces magiques.

Le fait de ne pas pouvoir affecter une valeur numérique à une grandeur physique avant de la mesurer est une bizarrerie inhérente à la physique quantique. Après tout, nous expérimentons au quotidien une réalité *a priori* objective dans laquelle les objets ont des propriétés physiques qui peuvent être quantifiées et dont les valeurs existent indépendamment du fait que nous les mesurions ou non. Et pourtant, même si c'est perturbant, notre monde n'est pas ainsi fait. Des inégalités statistiques, telles que $\varepsilon \geqslant 1/4$, dérivées de l'hypothèse selon laquelle les valeurs des quantités physiques non mesurées existent effectivement et que l'on appelle communément les inégalités de Bell, ont été violées dans un certain nombre d'expériences minutieuses, comme celle qu'Alain Aspect, de l'Institut d'optique à Orsay, et ses collègues ont menée en 1982.

L'une des conséquences de la violation des inégalités de Bell est que la probabilité qu'Ève devine correctement un résultat particulier ne peut dépasser $(1+4\varepsilon)/2$. Si ε est suffisamment petit, Alice et Bob sont en mesure de construire une clé presque parfaite à partir des résultats, en utilisant

Les systèmes de chiffrement quantique sont déjà là

Le principe de chiffrement quantique proposé par Charles Bennett et Gilles Brassard en 1984 est plus simple à mettre en pratique que celui conçu par Artur Ekert en 1991. Les premiers dispositifs sont déjà testés et fonctionnent depuis une dizaine d'années.

La cryptographie quantique a vraiment commencé à sortir des laboratoires au début des années 2000, lorsque les physiciens ont trouvé une solution au refroidissement des dispositifs afin de limiter la perte de photons. Ils ont remplacé l'azote liquide, peu pratique pour un usage à grande échelle, par des systèmes électriques.

Les dispositifs de chiffrement ne prennent pas forcément un grand volume, et peuvent être contenus dans l'équivalent d'une mallette. Une petite diode laser envoie de la lumière sur un filtre si opaque qu'il ne laisse passer, en moyenne, qu'un photon à la fois. Ce photon est polarisé selon une certaine direction pour porter la valeur 0 ou 1 d'un bit. Le photon est ensuite envoyé dans une fibre optique reliée au dispositif du destinataire, qui mesure à son tour la polarisation du photon.

Dans la procédure de Bennett et Brassard, l'expéditeur et le destinataire se concertent pour déterminer les bits qui formeront la clé de chiffrement de leur message. Un espion ne peut deviner la valeur de ces bits, et s'il interceptait les photons lors de leur transmission dans la fibre, cela perturberait leur polarisation. En comparant les mesures sur un échantillon de photons, l'expéditeur et le destinataire détectent aisément si un tiers a tenté d'« écouter » leur échange.

De tels dispositifs sont déjà mis en place. La société Battelle Memorial Institute, aux États-Unis, a par exemple installé un réseau entre deux de ses sites pour échanger des rapports financiers ou d'autres informations confidentielles. La distance parcourue par la fibre optique est limitée à quelques dizaines de kilomètres. Au-dessus d'une centaine de kilomètres, le signal est fortement détérioré du fait de l'absorption des photons par la fibre.

Les chercheurs de Battelle travaillent avec la firme suisse ID Quantique pour mettre au point des réseaux plus étendus à l'aide de boîtes relais. Celles-ci, refroidies à –40 °C, capteraient les photons polarisés et les réémettraient à l'identique. Ces boîtes relais devraient cependant être parfaitement scellées et sécurisées pour empêcher toute intrusion malveillante. Par sécurité, la détection d'une tentative d'intrusion conduirait alors le système à s'éteindre aussitôt.

En attendant que cette idée aboutisse, des projets pour relier la réserve fédérale américaine à ses banques régionales sont à l'étude. Et le gouvernement chinois voudrait installer un dispositif similaire pour son usage et celui des institutions financières entre Shanghai et Beijing, distantes de 2 000 kilomètres.

La mise en place à grande échelle de ces systèmes de cryptographie avec fibres optiques est confrontée à un autre obstacle. Les connexions s'accommodent mal d'un réseau ramifié. On retrouve là les difficultés des débuts du téléphone au XIX^e siècle et ses énormes quantités de câbles pour établir des contacts point à point.

Mais déjà de nouveaux systèmes sont imaginés, toujours plus petits et portatifs. Le secteur pourrait croître très vite dans les années à venir.

– Sean Bailly
Pour la Science

une technique dite d'amplification de la confidentialité. L'idée est assez simple : imaginez que vous ayez deux bits et que votre adversaire en connaisse au plus un (sans que vous sachiez lequel). Additionnez les deux bits modulo 2 : le bit résultant sera inconnu de votre adversaire. Avec davantage de bits, il existe des moyens bien plus élaborés pour amplifier la confidentialité.

Pour résumer, à chaque fois que l'on donne à Alice et Bob des dispositifs qui produisent des résultats corrélés, ils peuvent faire tourner le protocole de distribution des clés, complété par un « test d'honnêteté » statistique afin d'estimer ε. Si cette valeur est suffisamment petite, disons $\varepsilon = 0{,}15$, le résultat final, après amplification de la confidentialité, est une clé de chiffrement parfaite. Nous obtenons ainsi une confidentialité fiable à partir de dispositifs non fiables.

Les corrélations monogames assorties à une quantité même faible de libre arbitre suffisent pour protéger notre vie privée

Certains points sont à vérifier avant que l'on soit sûr que notre système n'a pas de faille. En particulier, Alice et Bob peuvent-ils se faire confiance ? Il est difficile d'être plus paranoïaque que cela. Sont-ils libres de leurs choix, ou bien sont-ils contrôlés par une force qui leur échappe ?

Nous avons déjà souligné l'importance du libre arbitre dans le processus. Le choix de la pièce à lancer ou de la direction de polarisation à mesurer doit être fait librement (aléatoirement) et indépendamment. En général, dans les réalisations pratiques, des générateurs de nombres (pseudo)aléatoires se chargent de tels choix. Mais le hasard qu'ils simulent est-il de qualité satisfaisante ?

Il est évident que si tout est prédéterminé, si tous nos choix sont prévisibles ou préprogrammés par nos adversaires, il n'y a pas de confidentialité qui tienne.

Doper le libre arbitre

En réalité, il suffit que la prédétermination ne soit pas complète et qu'il reste un petit peu de liberté. Si une fraction des choix faits par nos générateurs de nombres aléatoires ne peut être déterminée par l'adversaire, alors la confidentialité est encore possible, parce que le caractère aléatoire local peut être amplifié. L'amplification du hasard est obtenue avec des protocoles indépendants du dispositif, et fonctionne même si la fraction de hasard initial est arbitrairement petite.

Tout cela semble bizarre et trop beau pour être vrai. Nous avons montré qu'il est, en théorie, possible d'amplifier le libre arbitre et la confidentialité pour obtenir une méthode de chiffrement totalement fiable. C'est cependant assez difficile à mettre en pratique.

Comme nous l'avons vu, l'un de nous (Artur Ekert) a proposé en 1991 un système de distribution quantique des clés fondé sur la violation des inégalités de Bell. L'année suivante, une démonstration de principe a été réalisée à la Defence Evaluation and Research Agency (aujourd'hui QinetiQ) à Malvern, au Royaume-Uni. Cependant, le caractère « indépendant du dispositif » (c'est-à-dire sans connaître parfaitement l'origine du dispositif) de ce protocole n'a été démontré qu'en 2007. Prouver la sécurité d'un tel système en conditions réelles n'a pas été facile. Il a fallu plus d'une décennie pour s'accorder sur une définition utile du secret, ne serait-ce que pour des dispositifs fiables, et pour réaliser une longue série de tests prenant en compte toutes les ressources quantiques qu'Ève peut mettre à son service. Un défi majeur consiste à rendre ces arguments de sécurité quantitatifs et robustes vis-à-vis du bruit et des imperfections du système.

Pour finir, il convient de souligner que les protocoles indépendants des dispositifs et leurs preuves de sécurité n'ont pas encore atteint le degré de sophistication qui est maintenant la norme pour le scénario dépendant des dispositifs. En particulier, des efforts sont nécessaires pour améliorer l'efficacité des protocoles de distribution des clés, et pour identifier les conditions dans lesquelles des dispositifs non éprouvés peuvent être réutilisés sur de multiples cycles de ces protocoles.

Les fondements quantiques du principe de chiffrement décrit ici sont aussi sujets à des interrogations. Nous avons implicitement supposé qu'il n'y a rien au-delà de la théorie quantique. Cependant, si Alice et Bob sont assez paranoïaques pour supposer qu'Ève a des capacités « postquantiques » (des technologies plus puissantes que les technologies quantiques, reposant sur des phénomènes physiques non encore découverts et non décrits par la physique quantique), ils peuvent encore avoir recours à des protocoles moins efficaces, mais ne reposant pas sur la théorie quantique *(voir l'article de Phong Nguyen page 36)*.

BIBLIOGRAPHIE

G. Brassard, **Cryptography in a quantum world**, *Lecture Notes in Computer Science* (Springer), vol. 9587, pp 3-16, 2016.

B. Hensen *et al.*, **Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometers**, *Nature*, vol. 526, pp. 682-686, 2015.

A. Ekert et R. Renner, **The ultimate physical limits of privacy**, *Nature*, vol. 507, pp. 443-447, 2014.

C. Bennett *et al.*, **La cryptographie quantique**, *Dossier Pour la Science*, n° 36, juillet-octobre 2002.

A. Ekert, **Quantum cryptography based on Bell's theorem**, *Phys. Rev. Lett.*, vol. 67, n° 6, pp. 661-663, 1991.

Par ailleurs, le système de chiffrement quantique décrit ici repose surtout sur la violation des inégalités de Bell et le caractère non local de l'intrication quantique. Celui-ci est un fait expérimental confirmé par de nombreuses équipes. Pour convaincantes qu'elles soient, ces expériences laissent ouvertes certaines brèches. Par exemple, il est en principe possible que les photons détectés dans les expériences ne constituent pas un échantillon représentatif de tous les photons émis par la source (« échappatoire de détection ») ou que les différentes parties ou composantes de l'expérience aient été causalement reliées (« échappatoire de localité »).

L'expérience d'Alain Aspect, en 1982, par exemple, utilisait deux instruments suffisamment éloignés l'un de l'autre pour éviter qu'une communication à la vitesse de la lumière fausse les résultats des mesures. Mais cette expérience souffre de l'échappatoire de détection. En effet, tous les photons intriqués n'arrivent pas aux détecteurs, car certains sont absorbés en chemin. Comment garantir que le sous-groupe des photons qui arrivent aux détecteurs est représentatif de tous les photons émis ? Il est très difficile de combler la faille de détection, parce que presque tout composant optique ajoute des pertes et des imperfections au dispositif.

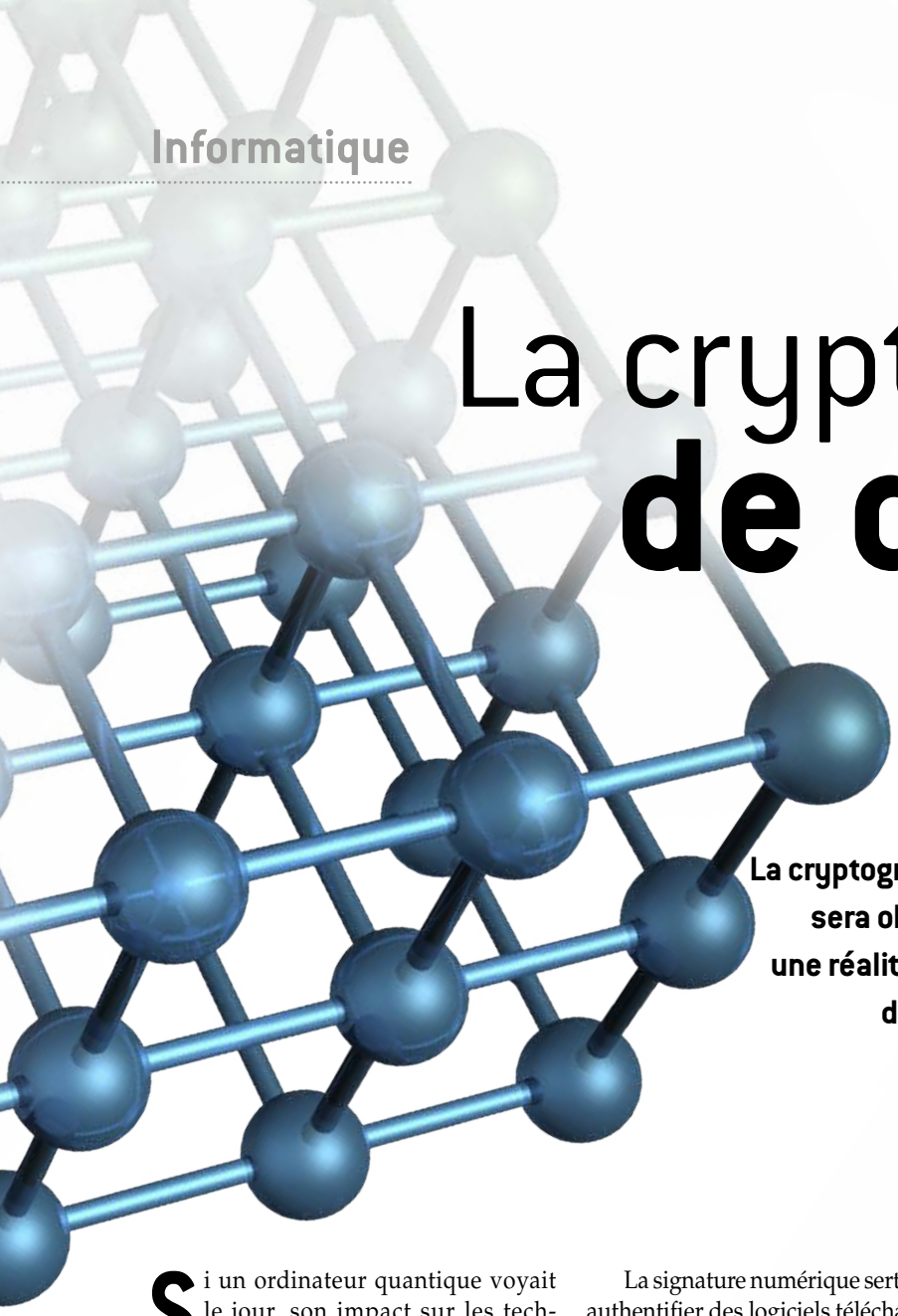
Il y avait peu de chance que la nature soit assez malveillante pour nous tromper de manière sélective – par l'échappatoire de localité dans certaines expériences, et par l'échappatoire de détection dans d'autres. En revanche, rien n'empêche un espion d'être trop curieux. Et il pourrait exploiter ces échappatoires à son profit.

Des expériences sans échappatoire

En 2013, l'équipe d'Anton Zeilinger, de l'université de Vienne, et celle de Paul Kwiat, de l'université de l'Illinois, ont montré qu'il était possible de contrôler l'échappatoire de détection. Mais sans garantir l'échappatoire de localité... Une autre expérience, mise au point en 2015 par l'équipe de Ronald Hanson, de l'université de Delft, aux Pays-Bas, contrôle les deux échappatoires. Ainsi, nous pouvons être rassurés sur la violation des inégalités de Bell et la fiabilité de la cryptographie quantique indépendante des dispositifs.

Cette dernière est tout sauf facile à mettre en pratique, mais les progrès technologiques réalisés jusqu'à présent portent à l'optimisme *(voir l'encadré page 33)*.

Depuis une quinzaine d'années, la cryptographie quantique a beaucoup évolué et de nombreux travaux ont renforcé la fiabilité du système. Elle est aussi une source d'inspiration très fertile pour la recherche fondamentale. La quête des limites ultimes de la confidentialité est encore en chantier, mais nous savons que l'on peut garantir la confidentialité sous des hypothèses étonnamment faibles. Les corrélations monogames, de quelque origine qu'elles soient, assorties à une quantité arbitrairement faible de libre arbitre, suffisent à dissimuler tout ce que nous voulons. Le libre arbitre est notre atout le plus précieux. Et à bien y réfléchir, s'il n'y a pas de libre arbitre, à quoi bon cacher quoi que ce soit de toute façon ? ■



La cryptographie de demain

Phong Nguyen

La cryptographie à clé publique utilisée aujourd'hui sera obsolète si l'ordinateur quantique devient une réalité. Toutefois, des méthodes alternatives, dites postquantiques, sont déjà à l'étude.

Si un ordinateur quantique voyait le jour, son impact sur les techniques cryptographiques déployées aujourd'hui serait considérable. Les deux fonctionnalités les plus menacées par ses capacités de calcul sont le chiffrement à clé publique et la signature numérique.

Le chiffrement à clé publique est très utilisé sur Internet, notamment pour sécuriser le commerce électronique en protégeant les numéros de carte bancaire. Lorsque vous envoyez un tel numéro à un destinataire, vous le chiffrez en utilisant la clé publique que votre interlocuteur vous transmet. Cette clé sert à chiffrer, mais pas à déchiffrer le numéro : seul le destinataire peut retrouver le numéro initial en utilisant une clé privée, qui a servi à définir la clé publique. Il est théoriquement possible de retrouver la clé privée à partir de la clé publique, mais difficile en pratique… sauf avec les algorithmes qu'un ordinateur quantique pourra utiliser.

La signature numérique sert surtout à authentifier des logiciels téléchargés (sur téléphone mobile ou sur ordinateur), les clés de chiffrement et les sites internet.

Comment anticiper le jour où le chiffrement à clé publique et la signature numérique ne seront plus sûrs ? Un texte chiffré pourrait être stocké aujourd'hui pour être décrypté demain par un ordinateur quantique. La cryptographie quantique *(voir l'article d'Artur Ekert et Renato Renner, pages 26 à 35)* ne répond que très partiellement à cette question, car elle ne fournit ni signature, ni chiffrement à clé publique, mais offre seulement un certain type d'échange de clés, ce qui est insuffisant pour beaucoup d'applications courantes. Pour résister à l'attaque d'un ordinateur quantique, il existe actuellement quatre approches, qualifiées de postquantiques : la cryptographie à base de hachage, la cryptographie multivariable, celle à base de codes correcteurs et celle à base de réseaux.

Les fonctions de hachage sont répandues en cryptographie ; elles servent par exemple à protéger les mots de passe. Ces fonctions associent à tout message une petite chaîne de caractères : l'empreinte. En cryptographie, les fonctions de hachage utilisées doivent être à sens unique, c'est-à-dire qu'il doit être impossible de retrouver un message à partir de son empreinte.

Les fonctions de hachage ne permettent pas à elles seules de fournir un chiffrement à clé publique. En revanche, il a été montré qu'elles sont suffisantes pour construire des signatures numériques sûres (même si ces dernières ont l'inconvénient d'être volumineuses). En 1979, l'informaticien américain Leslie Lamport a en effet proposé une méthode pour signer un message grâce au hachage. On choisit d'abord des nombres aléatoires qui forment la clé privée du signataire : les empreintes de chacun des nombres de la clé privée par la fonction de hachage constituent la clé publique. La

signature est un sous-ensemble de la clé privée dépendant du message. Pour vérifier la signature, on hache chacun de ses éléments et on vérifie qu'on obtient le bon sous-ensemble de la clé publique.

La signature de Lamport est simple à mettre en œuvre, mais elle ne peut être utilisée qu'une fois, pour des raisons de sécurité, car elle révèle une partie de la clé privée. Pour signer plusieurs messages, l'Américain Ralph Merkle a inventé ce qu'on nomme aujourd'hui des arbres de hachage, dans lesquels on passe d'un niveau à un autre en appliquant la fonction de hachage. Les arbres de hachage sont couramment utilisés : on les trouve dans la monnaie virtuelle bitcoin et dans les réseaux pair à pair, pour vérifier l'intégrité d'une partie d'un fichier par exemple.

Une autre approche est la cryptographie multivariable, développée dès 1988 sous l'impulsion de deux chercheurs japonais, Tsutomu Matsumoto et Hideki Imai. Elle repose sur la difficulté à résoudre des systèmes d'équations polynomiales à plusieurs inconnues. Au lycée, on apprend à résoudre une équation du second degré à une seule variable. Ce problème devient très difficile lorsque le nombre de variables et le nombre d'équations sont élevés.

Dans le cas d'une signature multivariable, la clé publique est un système d'équations polynomiales ; le message définit le second membre de ce système d'équations, et la signature d'un message n'est autre qu'une solution du système avec second membre. Ainsi, on vérifie la validité d'une signature en vérifiant qu'elle est bien solution du système. La cryptographie multivariable s'applique au chiffrement à clé publique et aux signatures numériques de façon assez efficace.

Cependant, l'inconvénient de cette méthode est que les systèmes d'équations utilisés ont des structures cachées qui, découvertes, constituent des brèches : de nombreux systèmes multivariables ont ainsi été cassés, à commencer par le système de Matsumoto-Imai, contre lequel Jacques Patarin, de l'université Versailles-Saint-Quentin-en-Yvelines, développa une attaque astucieuse en 1995. Un autre cas d'école est la signature numérique Sflash, conçue en 2001 par des chercheurs de la société Schlumberger, et recommandée par le projet européen NESSIE en 2003. Elle a été cassée en 2007 par les cryptographes Vivien Dubois, Pierre-Alain Fouque, Adi Shamir et Jacques Stern.

Enfin, la cryptographie à base de codes correcteurs et celle à base de réseaux reposent sur des problèmes assez voisins : filtrer du bruit. On cache un élément dans un code correcteur d'erreurs (des objets mathématiques très structurés) ou bien dans un réseau euclidien (un arrangement régulier de points dans l'espace à n dimensions) en lui ajoutant du bruit. Il est alors difficile de retrouver l'élément, c'est-à-dire d'enlever le bruit. Dans l'exemple des réseaux, l'élément est un point du réseau, et on le bruite en le déplaçant légèrement : quand la dimension augmente et que le réseau n'est pas trop particulier, il est très difficile de retrouver la perturbation. Cela permet de construire assez naturellement un chiffrement à clé publique : c'est ce qu'a fait Robert McEliece dès la fin des années 1970 pour les codes correcteurs. Fondé sur la même idée, le chiffrement à base de réseaux NTRU est peut-être le chiffrement à clé publique le plus rapide du monde.

L'Institut américain des normes et de la technologie a lancé un appel international pour normaliser ces algorithmes postquantiques

Malgré leurs similitudes, les codes correcteurs et les réseaux euclidiens ont des différences significatives. Par exemple, on connaît des signatures à base de réseaux très efficaces, contrairement au cas des codes correcteurs. Et les réseaux euclidiens offrent des fonctionnalités que n'a pas la cryptographie traditionnelle : on peut citer le cas du chiffrement complètement homomorphe, qui permet d'effectuer des opérations arbitraires sur des données chiffrées sans que l'on connaisse la clé secrète. Pour toutes ces raisons, la cryptographie à base de réseaux est la méthode postquantique la plus étudiée à l'heure actuelle.

Ces quatre approches postquantiques ont des avantages et des défauts. En février 2016, le NIST (l'Institut américain des normes et de la technologie) a lancé un appel international pour normaliser ces méthodes postquantiques. Cette initiative permettra peut-être de déterminer l'approche la plus adaptée pour remplacer les systèmes de cryptographie à clé publique utilisés aujourd'hui, tel RSA. ■

L'AUTEUR

Phong NGUYEN est directeur de recherche à l'Inria et dirige le laboratoire franco-japonais d'informatique du CNRS.

BIBLIOGRAPHIE

National Institute of Standards and Technology, **Report on Post-Quantum Cryptography**, Internal Report 8105, 2016.

P. Q. Nguyen et B. Vallée (éd.), **The LLL Algorithm, Survey and Applications**, Springer, 2010.

D. J. Bernstein *et al.* (éd.), **Post-Quantum Cryptography**, Springer, 2009.

P. Nguyen, **La géométrie des nombres : de Gauss aux codes secrets**, *Dossier Pour la Science*, n° 36, juillet-octobre 2002.