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.

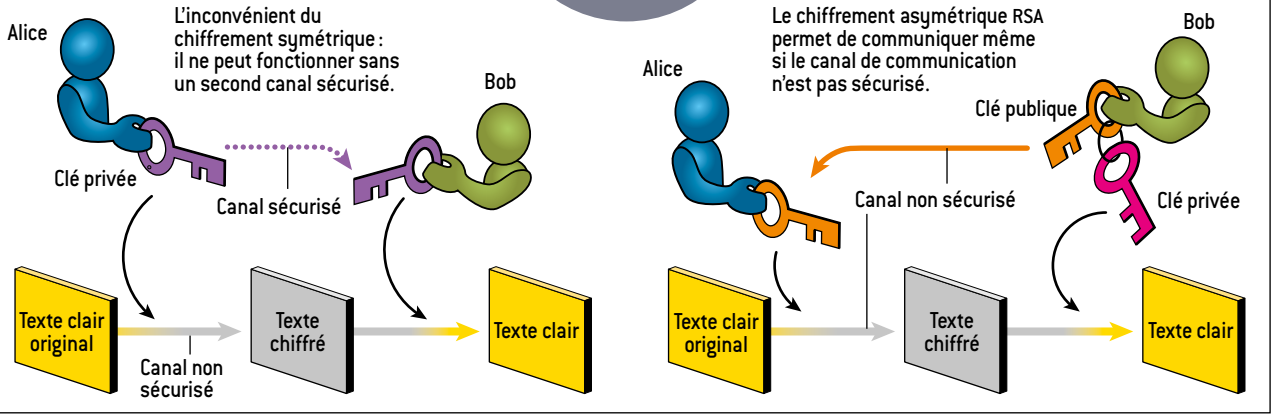
CHIFFREMENT SYMÉTRIQUE

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