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.

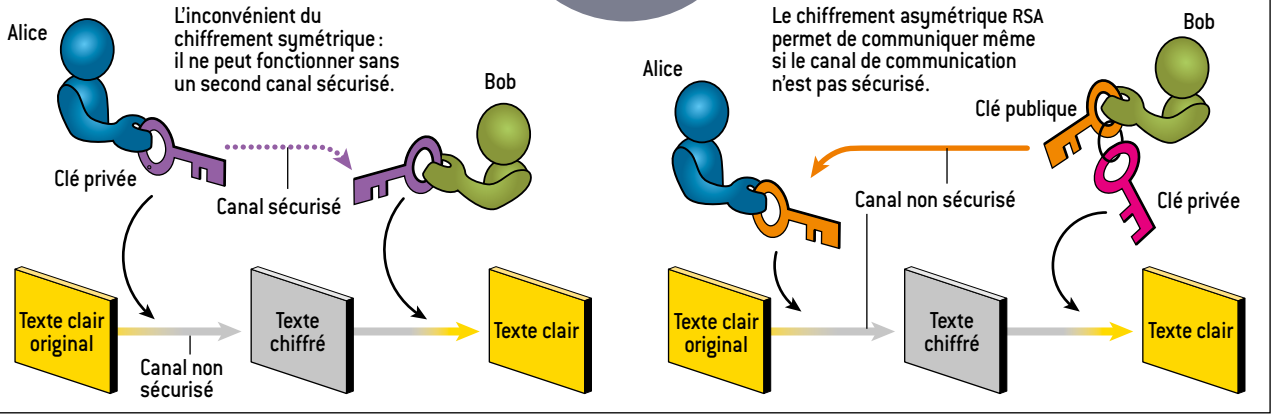
CHIFFREMENT SYMÉTRIQUE

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