

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

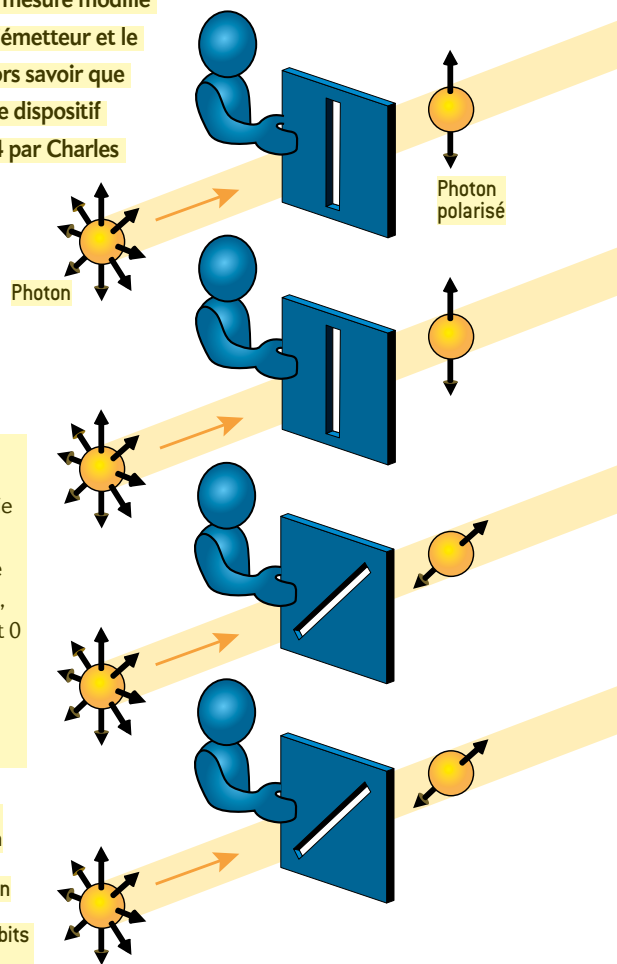
En cryptographie quantique, la distribution d'une clé se fait grâce à un flux de photons polarisés (présentant une direction de spin particulière). Si une tierce personne tente de mesurer la polarisation de ces photons en chemin, le seul acte de la mesure modifie la polarisation de certains photons. 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.

L'émetteur possède quatre filtres polarisants parmi lesquels il choisit selon la valeur du bit qu'il veut transmettre.

ENVOI ET RÉCEPTION DE PHOTONS POLARISÉS

L'émetteur (en bleu) transmet une série de photons qui passent par l'un des quatre filtres polarisants. Chaque filtre polarise le photon selon une direction, à laquelle on assigne une valeur de bit 0 ou 1 (voir ci-dessous). Le destinataire (en vert) mesure la polarisation après le passage du photon par l'un de ses deux filtres.

Filtres d'émission				
Polarisation				
Valeur des bits attribuée	0	1	0	1



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

$$\begin{array}{ll} A_1 = B_1 & B_1 = A_2 \\ A_2 = B_2 & B_2 \neq A_1 \end{array}$$

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

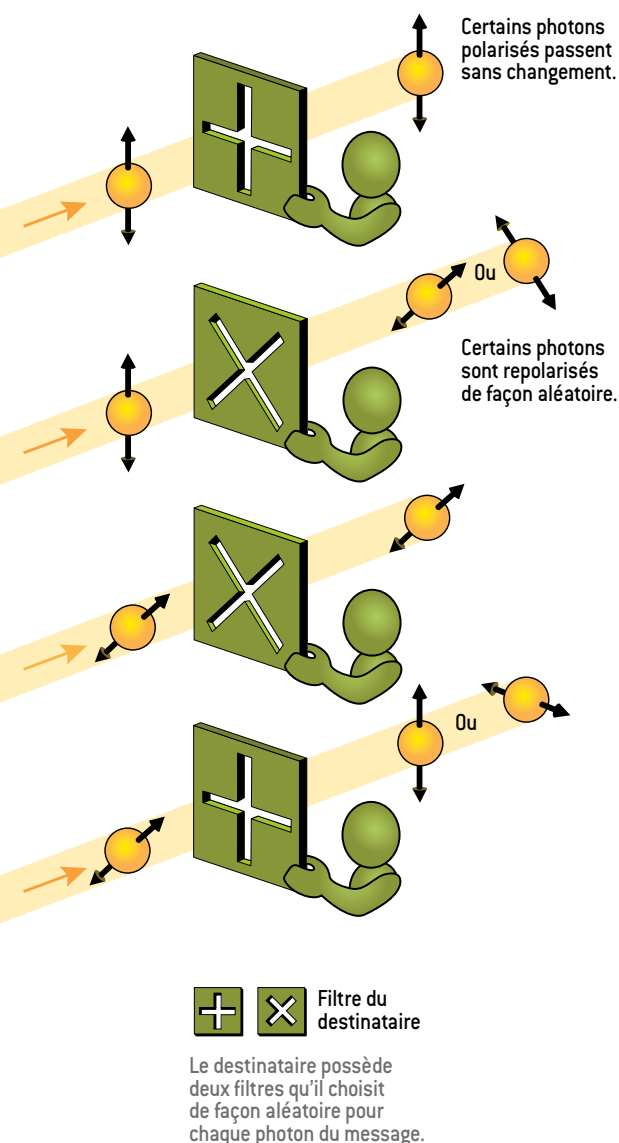
qu'Alice obtienne deux faces ou deux piles ($A_1 = A_2$) ; alors Bob n'a pas d'autre choix que de lancer B_1 , parce que c'est le seul lancer compatible avec les conditions des pièces magiques. De la même façon, si Alice obtient une pièce face et une pièce pile ($A_1 \neq A_2$), le seul choix qui reste 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 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.

