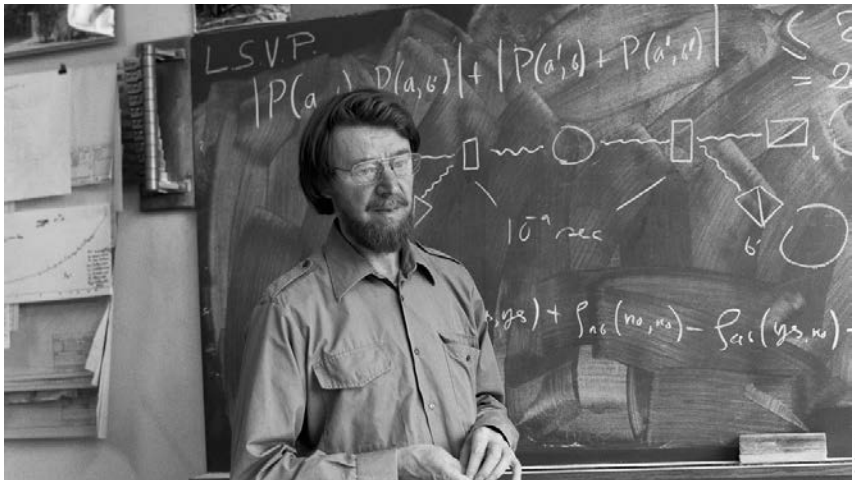

© CERN

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