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

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

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

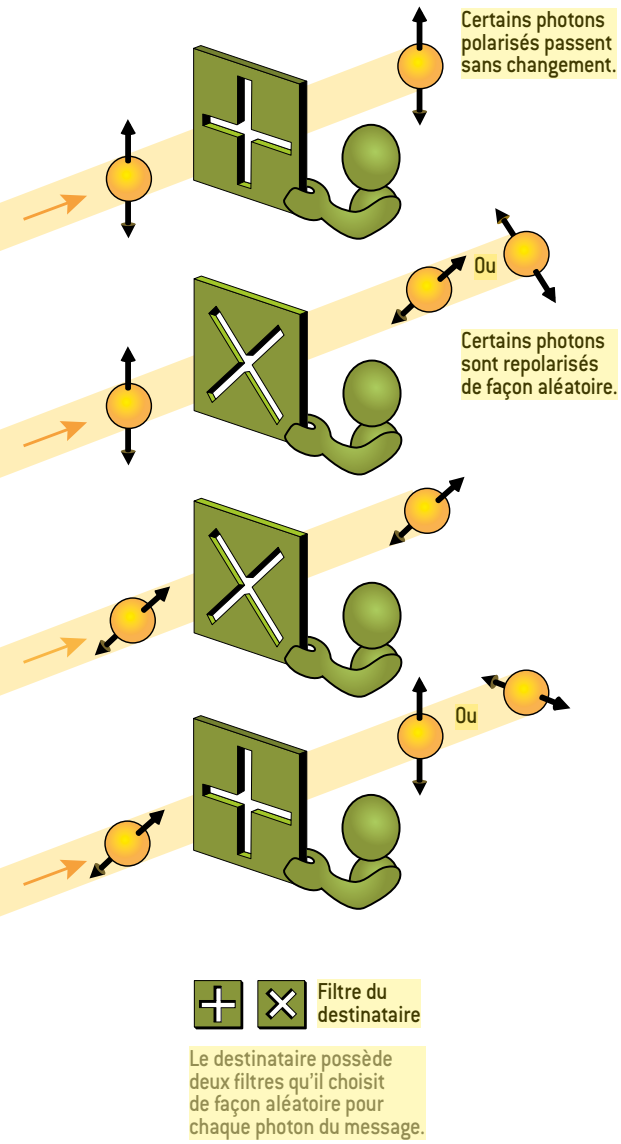
Ces conditions sont clairement contradictoires : il est impossible d'assigner à A_1, A_2, B_1 et B_2 des valeurs telles que les quatre conditions soient simultanément satisfaites. Mais il faut se rappeler qu'Alice et Bob ne peuvent lancer qu'une pièce chacun, et qu'ils ne peuvent donc tester qu'une seule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

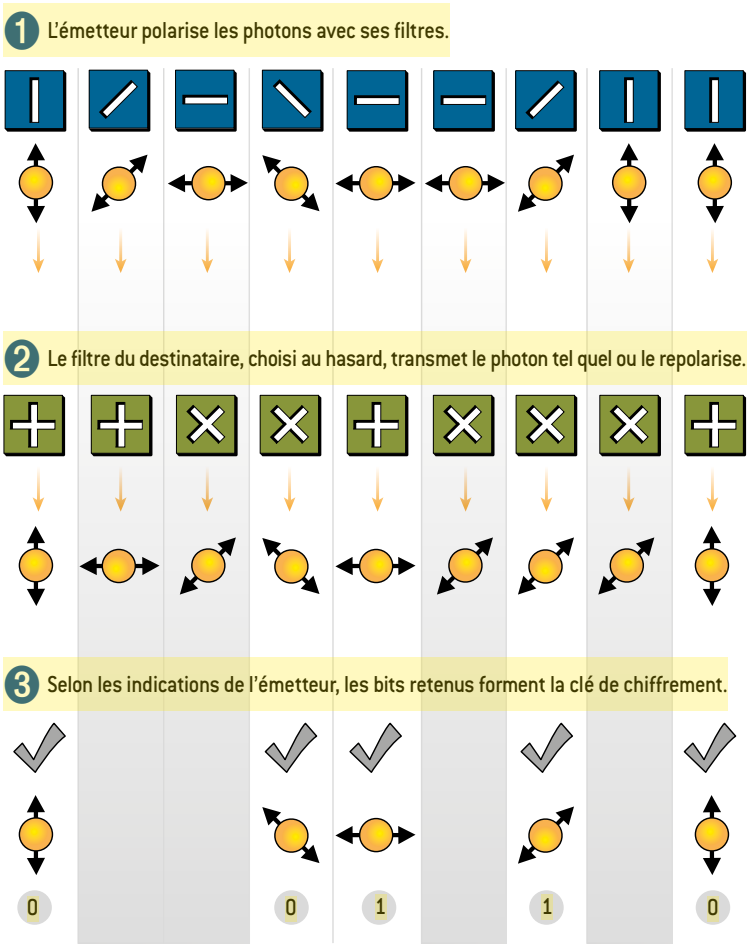
Tous les ingrédients de la distribution sécurisée des clés sont désormais en place. Concrètement, pour créer une clé de chiffrement, Alice et Bob lancent leurs pièces magiques. À chaque lancer, Alice et Bob

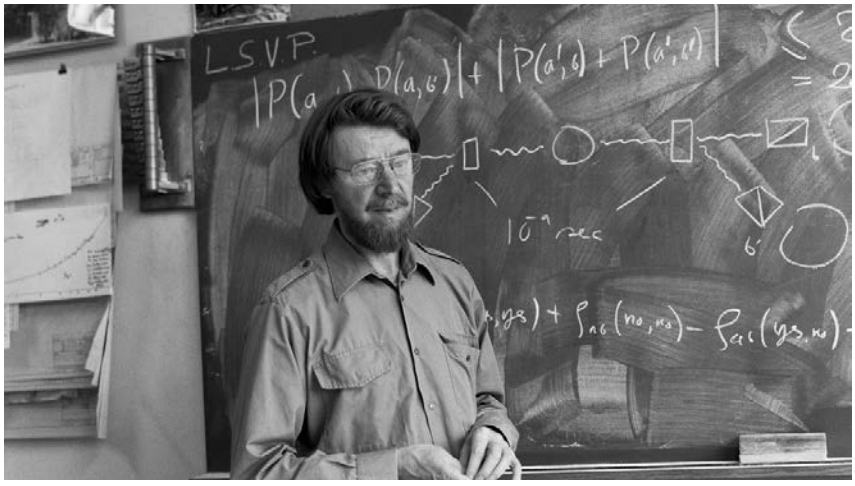


Le destinataire possède deux filtres qu'il choisit de façon aléatoire pour chaque photon du message.

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