

quisition de l'information sur certains systèmes quantiques les perturbe irrémédiablement. C'est une conséquence du principe d'incertitude d'Heisenberg : mesurer une grandeur associée à un objet interdit d'en connaître d'autres ; plus grave, elle en fait un autre objet. L'information quantique a une réalité physique différente de l'abstraction de l'information classique.

Cette propriété quantique selon laquelle la mesure modifie l'objet mesuré trouble depuis longtemps ceux qui tentent de comprendre la mécanique quantique. Un exemple de cette difficulté, la détermination de la direction de polarisation d'un photon, est détaillée sur la figure 1.

Informations aléatoires et indéterminisme

Cet exemple du photon montre aussi que l'information quantique est parfois authentiquement aléatoire : si, après avoir polarisé un photon selon une direction a , on le fait passer dans un filtre polarisant dont l'axe fait un angle de 45° avec a , on le détectera exactement une fois sur deux. En envoyant dans le dispositif une série de photons identiques, on obtient une

suite de détections symbolisée par une suite de 1 et de 0 (1 pour une détection ; 0 pour une absence de détection) qui possède toutes les propriétés attendues d'une suite de 0 et de 1 parfaitement aléatoire. De telles suites sont intéressantes pour des méthodes de calcul comme la méthode de Monte-Carlo ou le cryptage des informations. Aussi cette propriété a-t-elle conduit à proposer des générateurs de bits aléatoires fondés sur des mécanismes quantiques (voir la rubrique Logique et calcul du mois de mars 1998, qui traite des suites aléatoires en informatique).

Copier l'information

Les moines du Moyen Âge, nos photocopieuses et les lecteurs de disquette de nos ordinateurs copient des informations sans rencontrer d'obstacles fondamentaux. Dupliquer l'information classique et en faire de multiples versions est facile et ne coûte presque rien. Comme cette information n'est pas de nature physique, elle n'est pas liée à son support, et elle est donc copiable. Dans le monde quantique, la copie n'est pas toujours possible. Le principe de non-duplication («no-

cloning principle») énoncé par W. Wootters, W. Zurek et D. Dieks en 1982 exprime cette impossibilité : un état quantique inconnu ne peut pas être dupliqué.

Reprenons l'exemple du photon : vous ne réussirez jamais à dupliquer un photon dont vous ne savez rien, car vous ne pourrez jamais connaître complètement son état quantique. Si vous essayez, dès que vous commencez à mesurer certaines quantités observables (la polarisation selon une direction par exemple), vous détruisez l'état quantique du photon et vous ne pouvez mesurer d'autres observables. Cette impossibilité interdit la duplication. Notons quand même que le principe de non-duplication n'empêche pas la création de plusieurs objets identiques (par exemple, plusieurs photons de même polarisation) lorsque l'information liée aux objets est connue, car elle résulte du moyen de fabrication.

Cacher l'information, et distribuer des clefs secrètes

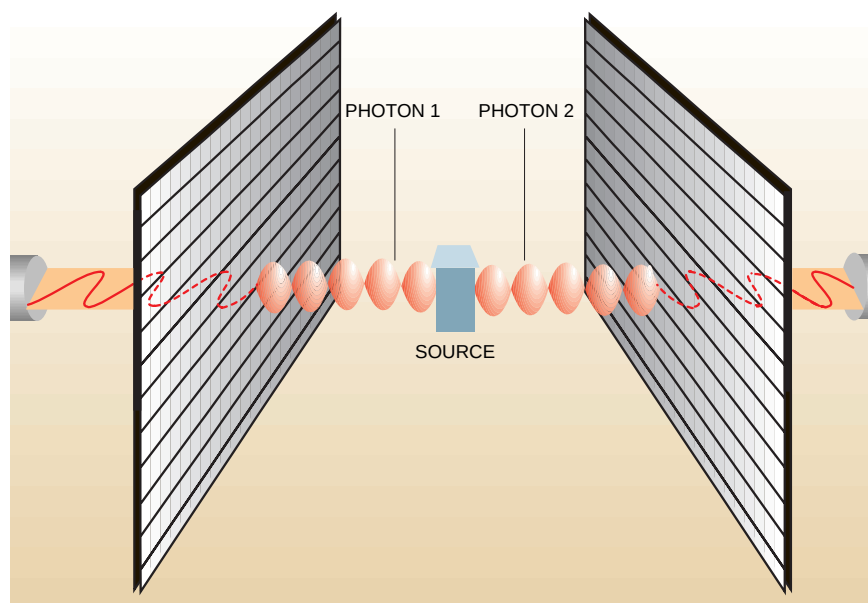
Cacher de l'information classique – ce qui est le but de la cryptographie – est théoriquement difficile : la plus grande partie des méthodes de cryptographie mathématique utilisées aujourd'hui se fonde sur des conjectures non démontrées et sont donc incertaines. Cet état de fait arrange les agences de renseignements, qui laissent croire que les codes légalement autorisés sont inviolables, alors qu'elles savent déchiffrer certains d'entre eux.

En revanche, la cryptographie quantique, qui utilise le principe de non-duplication des photons quantiques, propose des méthodes de distribution de clefs secrètes sûres et sans équivalent classique. Ces méthodes garantissent absolument le secret des échanges.

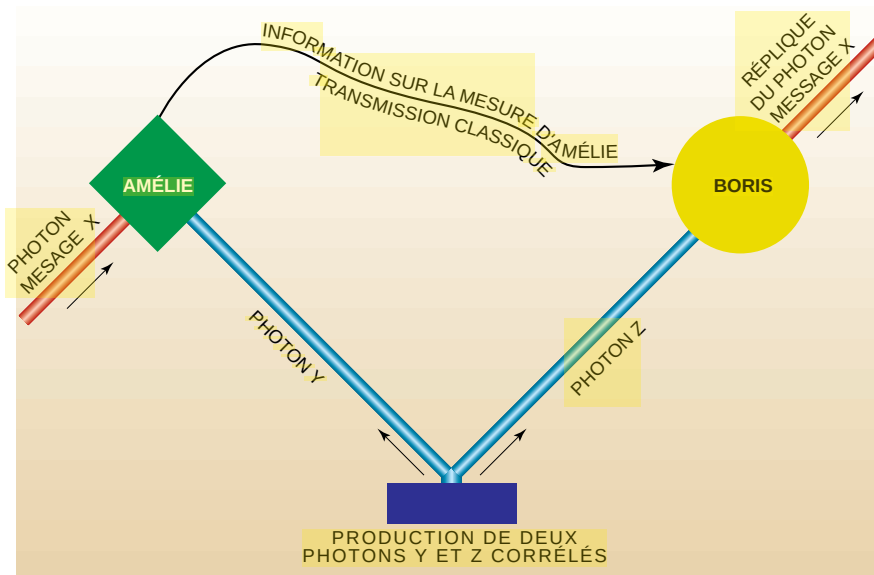
La cryptographie quantique est aujourd'hui suffisamment développée pour qu'avec des fibres optiques on sache distribuer des clefs secrètes entre des points distants de plusieurs dizaines de kilomètres. L'utilisation commerciale ou militaire de ces méthodes est sur le point de se faire (et a peut-être déjà eu lieu... de manière secrète).

Isoler l'information : la non-localité

Une autre propriété singulière de l'information quantique, étrange et difficile à comprendre, est la non-localité :



2. PHOTONS CORRÉLÉS ET INFORMATION ÉTALÉE. On sait produire des paires de photons corrélés, c'est-à-dire dont les directions de polarisation sont inconnues, mais identiques. Une telle paire contient une information non locale, possibilité exclue dans le monde classique. Cette non-localité de l'information se manifeste de la manière suivante : si l'on dispose sur le trajet des photons des filtres polarisants de même orientation, les deux photons corrélés émis par une source seront tous les deux interceptés ou tous les deux transmis, quelle que soit la distance qui sépare les photons au moment de la mesure (on a mené des expériences où les photons sont séparés l'un de l'autre de 10 kilomètres). Tout se passe comme si le premier photon savait comment l'autre se comporte : aussi faut-il admettre que deux photons corrélés forment un objet physique unique qui contient une information étalée dans tout l'espace.



3. LA TÉLÉPORTATION QUANTIQUE est un moyen de faire voyager de l'information inconnue (un état quantique) à la vitesse de la lumière. Amélie veut transmettre l'état quantique d'un photon X à Boris. Elle ne peut prendre totalement connaissance de cet état quantique et doit quand même le communiquer par radio à Boris. Pour réaliser la téléportation de l'état quantique de X, Amélie et Boris créent une paire de photons corrélés Y et Z ; Amélie garde Y et Boris garde Z. (Les photons Y et Z pourront, peut être, un jour être créés et stockés avant qu'Amélie et Boris ne s'éloignent l'un de l'autre ; aujourd'hui, les photons corrélés sont créés entre Amélie et Boris et leur sont envoyés.) Amélie fait interagir X avec Y, ce qui lui fournit une information classique, qu'elle envoie par radio à Boris. Grâce à celle-ci, Boris peut opérer une transformation de Z qui place Z dans l'état quantique de X, lequel a donc été recréé. Dans une telle opération, en théorie applicable à des systèmes quantiques plus complexes, l'information quantique a été séparée en deux composantes, l'une classique qui voyage à la vitesse de la lumière par le signal radio, l'autre quantique qui voyage en quelque sorte instantanément par utilisation de la corrélation entre Y et Z. Le principe d'inconnaissabilité n'est pas violé, car ni Amélie ni Boris n'ont eu connaissance de l'état quantique téléporté X. Le principe de non-duplication est respecté lui aussi, car X, lors de la combinaison de X avec Y, a été détruit par Amélie.

une information quantique peut ne pas être localisée en un endroit précis, mais être diffuse dans l'espace entier comme si on l'avait parfaitement étalée. John Bell a en effet établi en 1964 que les prévisions de la mécanique quantique ne peuvent être reproduites par aucune théorie où chaque information est située en un point précis de l'espace.

Les conclusions de Bell ont été vérifiées par Alain Aspect, Jean Dalibard, Philippe Grangier et Gérard Roger en 1982 (voir la figure 2) : l'information n'est ni dans l'un des composants du système ni dans un autre, mais dans l'ensemble. J. Bell a ainsi montré que l'on pouvait coder l'information dans les corrélations entre diverses parties éloignées d'un système physique (possibilité qui est, par définition, exclue du modèle général des ordinateurs classiques où, à chaque instant, chaque information est localisée) et que l'on peut manipuler cette information non locale. Cette propriété confère une puissance supérieure au calcul quantique,

et les expériences de calcul quantique de ces derniers mois ont confirmé les prévisions des modèles théoriques.

La transmission d'une information dans le monde classique (relativiste) peut se faire à la vitesse de la lumière : il suffit d'envoyer un signal lumineux ou radio qui contient l'information que l'on veut faire voyager.

On ne peut, en principe, pas transmettre l'information d'un état quantique par codage d'un signal lumineux, car cette information est inconnue ; on pourrait alors envisager de transmettre le système quantique lui-même, mais, s'il possède une masse, il est impossible de le faire à la vitesse de la lumière. L'information quantique voyagerait-elle moins bien que l'information classique ?

La téléportation

Il n'en est rien : la technique de téléportation, proposée en 1993 par C. Bennett, G. Brassard, C. Crépeau,

R. Jozsa, A. Perez et W. Wootters fait voyager à la vitesse de la lumière un état quantique inconnu (voir la figure 3). Grâce à cette méthode étonnante (dont on se demande pourquoi elle n'a pas été découverte plus tôt), l'information quantique voyage aussi vite que l'information classique. En revanche, la non-localité de l'information quantique n'autorise pas la transmission de l'information à une vitesse supérieure à celle de la lumière : dans l'expérience avec les deux photons corrélés, je peux, en mesurant la polarisation de mon photon, certes connaître instantanément celle de mon partenaire éloigné, mais ce n'est pas un échange : celui-ci ne peut me transmettre instantanément une information choisie par lui.

Soulignons une particularité : la méthode de téléportation quantique, qui utilise des paires de photons corrélés (de l'information non locale), oblige que l'on détruise à son point de départ l'état quantique qu'on veut déplacer (si cela n'était pas le cas on pourrait le dupliquer, ce qui est interdit). De surcroît, ni l'émetteur ni le récepteur ne peuvent connaître complètement l'information qu'on fait ainsi voyager, car lire l'information, c'est la détruire.

Ainsi, dans le monde quantique, la situation est nette : on peut transférer à la vitesse de la lumière l'information décrivant un système quantique, mais à la condition incontournable que le système complexe soit détruit en son point de départ et qu'on n'en prenne pas connaissance. Les auteurs de science-fiction semblent avoir deviné cette règle : dans *Star Trek*, par exemple, la téléportation qu'utilise l'équipage du vaisseau *Enterprise* pour de petites distances s'accompagne – sauf accident – de l'annihilation au point de départ du voyageur.

Les méthodes quantiques de téléportation ne sont pas seulement de la science-fiction, et si l'on est très loin de téléporter un être humain une équipe autrichienne a réussi, il y a quelques mois, à appliquer la méthode à l'état quantique d'un photon (voir *La téléportation quantique*, in *Pour La Science*, février 1998, page 30).

La téléportation quantique pourrait devenir utile, car elle est en mesure de régler le problème qui fait que la cryptographie quantique ne peut fonctionner que sur des distances limitées