

# Des photons intriqués aux bits quantiques

Alain ASPECT et Philippe GRANGIER

En 1935, Einstein lance un défi à la théorie quantique, qu'il juge incomplète. Un défi que les étrangetés quantiques ont relevé avec brio, tout en traçant la voie vers des applications révolutionnaires.

**L**a théorie quantique, née dans les années 1920, a modifié de fond en comble notre conception de la réalité. Elle nous oblige ainsi à accepter qu'une particule puisse se trouver à la fois ici et là, ou qu'une porte quantique puisse être à la fois ouverte et fermée. Elle a tout autant bouleversé notre vie à travers les lasers, les transistors ou les circuits intégrés qui équipent d'innombrables appareils. Albert Einstein a contribué à son émergence puisqu'en 1905, il expliquait l'effet photoélectrique en supposant la lumière formée de grains indivisibles d'énergie, des quanta que l'on devait nommer plus tard photons.

Néanmoins, dès la fin des années 1920, Einstein s'est opposé au physicien danois Niels Bohr sur l'interprétation des lois quantiques. Le débat a duré jusqu'à la fin de la vie de ces grands physiciens. À partir de 1935, il s'est focalisé sur une sérieuse objection à la théorie quantique faite par Einstein et deux collègues, Boris Podolsky et Nathan Rosen. Le débat a laissé à la plupart des physiciens l'impression que Bohr et son école, dite de Copenhague, avaient clarifié le sujet et bien répondu aux objections d'Einstein. Pourtant, dans les années 1960, celles-ci ont entraîné une nouvelle vague de progrès importants. D'une part, les travaux théo-

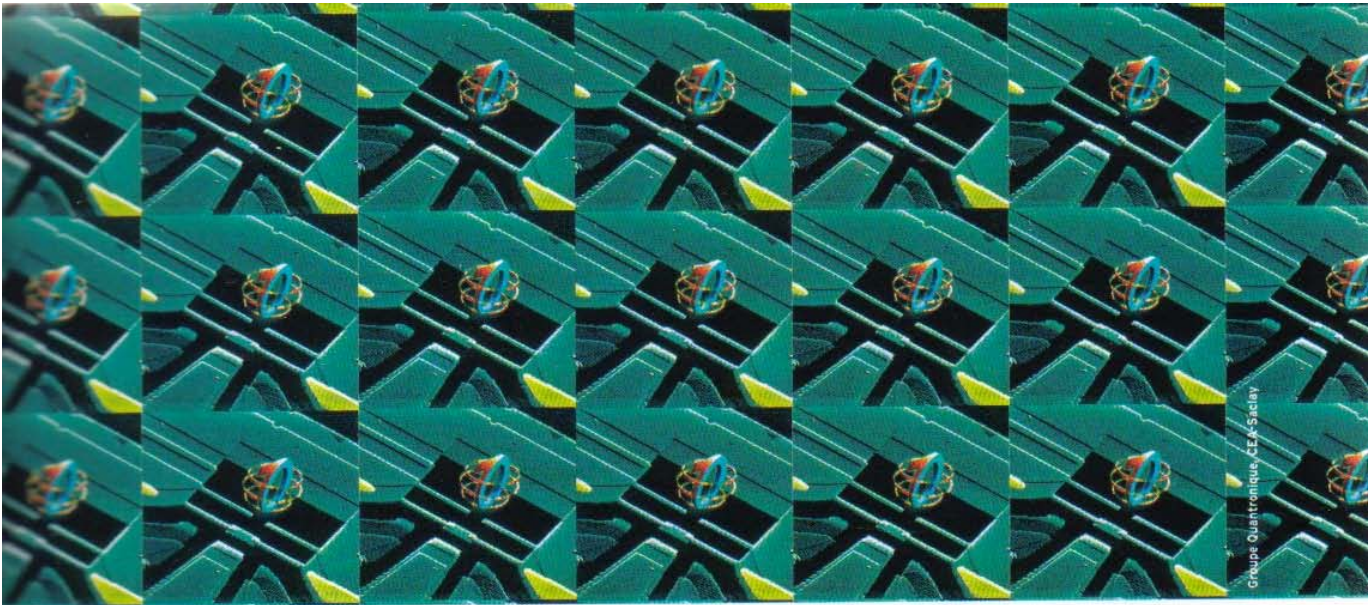
riques du physicien irlandais John Bell, suivis d'expériences de plus en plus fines, ont prouvé la propriété extraordinaire qu'est l'inséparabilité quantique – une paire d'objets préparés dans un état quantique dit intriqué se comportent comme un système unique, même si les deux objets sont très éloignés l'un de l'autre. D'autre part, les physiciens ont appris à manipuler un par un des électrons, des ions, des atomes ou des photons. Il fallut alors clarifier la façon d'appliquer le formalisme quantique – de nature probabiliste – à des objets individuels, et pas seulement à des assemblées statistiques d'objets, ce qui était une autre facette du questionnement d'Einstein.

Ces deux avancées ont marqué le début d'une nouvelle révolution : on ne compte plus les travaux théoriques et expérimentaux visant à les exploiter dans des applications qui pourraient, à leur tour, bouleverser la société. C'est la révolution de l'information quantique, avec la cryptographie quantique, dont les premiers démonstrateurs existent déjà, et l'ordinateur quantique, plus futuriste. N'est-il pas remarquable que les deux ingrédients de cette nouvelle révolution quantique soient précisément les points qu'Einstein ne cessa de mettre en avant – certes pour les contester, mais dont il avait saisi, plus que tout autre, le caractère stupéfiant ?

## La théorie quantique soumise à rude épreuve

Revenons aux débuts de cette histoire. La mécanique quantique s'est construite au prix de révisions radicales et douloureuses des concepts de la physique classique – par exemple celui de trajectoire, les « relations d'incertitude de Heisenberg » ayant montré que l'on ne peut mesurer avec exactitude et au même instant à la fois la position et la vitesse d'une particule. Ce renoncement était si radical que plusieurs physiciens, au premier rang desquels Einstein et Louis de Broglie, refusaient son caractère inéluctable, à la différence de Bohr et de son école. Aux congrès Solvay de 1927 et 1930, Einstein lança contre l'interprétation de Copenhague une série d'attaques mémorables, fondées sur des expériences de pensée, c'est-à-dire sur l'examen de situations compatibles avec les lois de la physique, mais difficiles à envisager avec les moyens expérimentaux de l'époque. Bohr put toutefois répondre de façon convaincante à ces attaques et il semble qu'à partir de 1930, Einstein ait admis la validité et la cohérence interne du formalisme quantique.

S'il ne remet plus en cause les lois mathématiques de la théorie quantique, ni ses prévisions, Einstein reste néanmoins insatisfait. À ses yeux, les renoncements contenus dans l'interprétation



Groupe Quantronique, CEA-Saclay

**1. LE CŒUR D'UN ORDINATEUR QUANTIQUE**, vu en gros plan, ressemblera-t-il à cela ? Nul ne peut le dire : le calcul quantique n'est pour l'heure qu'une lointaine perspective. L'idée de principe réside dans la faculté des systèmes quantiques, tels qu'atomes, ions, photons, etc., de se trouver dans plusieurs états à la fois. Dans le montage

ci-dessus, la photographie dupliquée est celle d'un microcircuit supraconducteur réalisé en 2001 par des physiciens du CEA à Saclay ; ce microcircuit peut être dans une superposition de deux états électriques, et constitue donc un bit quantique, symbolisé au centre des clichés par un 1 (en rouge) accolé à un 0 (en bleu).

de l'école de Copenhague ne traduisent que l'inachèvement de la théorie quantique. En 1935, la publication de l'article d'Einstein, Podolsky et Rosen (EPR), intitulé *La description quantique de la réalité physique peut-elle être considérée comme complète ?*, relance le débat. Einstein et ses coauteurs étudient des états quantiques particuliers de deux particules – des états dits intriqués ou « états EPR » –, pour lesquels le formalisme quantique prédit de très fortes corrélations entre les deux particules, quelle que soit la distance les séparant. Ils en concluent que la théorie quantique est incomplète.

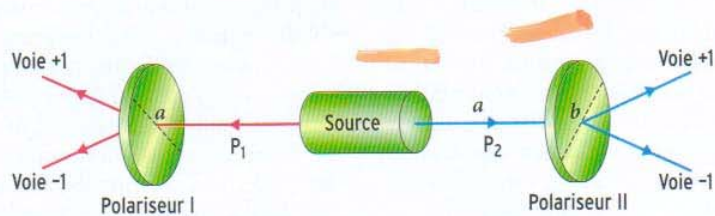
En quoi consiste l'argument ? Considérons ici des paires de photons dont les polarisations sont corrélées – systèmes qui ont ultérieurement permis de démontrer en laboratoire les propriétés de l'intrication. La lumière est dite polarisée quand son champ électromagnétique vibre (dans le plan perpendiculaire à la direction de propagation) suivant une direction fixe. Imaginons un dispositif polariseur qui, placé sur le trajet d'un faisceau lumineux, laisse passer les photons selon l'une de deux voies : une voie que l'on notera +1, et une voie notée -1. Le photon qui passe selon la voie +1 est polarisé dans la direction  $a$  du polariseur ; le photon sortant selon la voie -1 est polarisé dans la direction perpendiculaire à  $a$ . Il n'y a pas d'autres résultats possibles : un photon incident émerge soit selon la voie +1, soit selon la voie -1. La traver-

sée du dispositif détermine l'état de polarisation du photon.

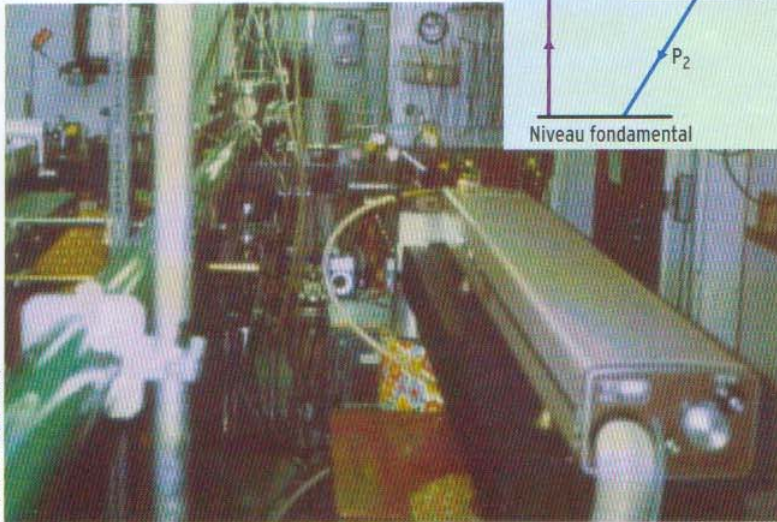
Examinons maintenant une paire de photons  $P_1$  et  $P_2$  émis simultanément vers la gauche et vers la droite, et effectuons sur ces photons, à l'aide de polariseurs I et II orientés respectivement suivant les directions  $a$  et  $b$ , des mesures conjointes de polarisation (voir la figure 2). Pour un certain état intriqué de la paire de photons, du type introduit par Einstein, Podolsky et Rosen – et que l'on sait aujourd'hui obtenir en pratique –, la mécanique quantique prédit que si les polariseurs ont le même axe ( $a = b$ ), les résultats seront totalement corrélés. Plus précisément, si l'on obtient le résultat +1 pour  $P_1$  (pour l'état intriqué considéré, cela arrive aléatoirement, dans 50 pour cent des cas), alors on obtient avec certitude +1 pour  $P_2$ , et si l'on obtient -1

pour  $P_1$  alors on obtient avec certitude -1 pour  $P_2$ .

Cela paraît anodin, mais, si les deux photons sont très éloignés au moment de la mesure, le résultat de la mesure sur l'un ne saurait déterminer le résultat de la mesure sur l'autre : sinon, cette influence devrait se propager plus vite que la lumière, ce qui contredirait le principe de causalité de la relativité. Pour comprendre, selon une conception classique de la réalité, la corrélation parfaite entre les résultats, on devrait admettre que chaque photon jouit, avant la mesure, d'une propriété qui fixe son résultat, par exemple une polarisation bien définie et déterminée dès le moment de l'émission. Si les photons d'une même paire ont initialement la même polarisation, il est clair que les mesures de polarisation conjointes donneront des résultats corrélés. Or pour une paire intriquée,



**2. ON SAIT PRODUIRE DES PAIRES DE PHOTONS  $P_1$  ET  $P_2$**  dont les états de polarisation sont intriqués, c'est-à-dire tels que le résultat d'une mesure de polarisation sur  $P_1$  et le résultat de la mesure sur  $P_2$  sont fortement corrélés, quelle que soit la distance séparant les deux photons. On mesure ces corrélations dans des expériences du type schématisé ici, où une mesure par le polariseur I (respectivement II) produit pour résultat +1 si le photon  $P_1$  (respectivement  $P_2$ ) émerge avec sa polarisation dirigée selon l'axe  $a$  (respectivement  $b$ ) du polariseur, et -1 s'il émerge avec une polarisation perpendiculaire, ces deux possibilités étant les seules.



A. Aspect, Institut d'optique CD-Roy

**3. DANS LES EXPÉRIENCES RÉALISÉES EN 1982** par l'équipe d'Alain Aspect, deux faisceaux laser excitaient un certain niveau atomique, l'atome absorbant deux photons, puis se désexcitant par l'émission en cascade de deux photons intriqués  $P_1$  et  $P_2$ . Les photons étaient émis en faisceaux opposés, vers des polariseurs se trouvant à six mètres de la source. Grâce à des commutateurs optiques, l'orientation de chaque polariseur pouvait être modifiée très rapidement, en un temps plus court que celui mis par une éventuelle influence se propageant d'un polariseur à l'autre à la vitesse de la lumière. Les corrélations des mesures ne résultent donc pas d'une telle influence.

la mécanique quantique n'attribue aucune propriété de ce type à chaque photon pris séparément (selon la théorie quantique, la polarisation de chacun des photons intriqués n'est objectivement pas déterminée avant la mesure). C'est donc, nous disent Einstein et ses coauteurs, que le formalisme de la mécanique quantique est incomplet, qu'il ne rend pas compte de la totalité de la réalité physique. Il faut alors tenter de le compléter, de mettre au jour les paramètres cachés qui pré-déterminent l'état individuel de chaque particule.

Bohr fut bouleversé par l'argument, qui s'appuie sur la théorie quantique elle-même pour en démontrer le caractère incomplet et provisoire. Il lui semblait que si le raisonnement était correct, compléter le formalisme quantique ne suffirait pas, c'est toute la théorie qui s'effondrerait. Bohr contesta l'argument en affirmant que, dans un état intriqué, parler des propriétés individuelles de chaque particule est dépourvu de sens, et ce même si les particules sont très éloignées l'une de l'autre. Sa réponse ne convainquit pas Einstein, et le débat se poursuivit.

En fait, cette controverse n'eut pas un grand écho chez les physiciens : en 1935, la mécanique quantique allait de succès en succès et la plupart des

physiciens ignorèrent ce débat qui leur paraissait académique. L'adhésion à l'une ou l'autre des positions leur semblait une affaire de goût personnel ou de conception épistémologique, dépourvue de conséquences sur les calculs ou les expériences.

### Hypothèse de localité : quelque chose cloche...

Trente ans plus tard, en 1964, cette attitude relativement consensuelle se voit bousculée par John Bell, théoricien irlandais travaillant au CERN à Genève. En quelques lignes, Bell démontre que pour deux particules intriquées, les prédictions quantiques sont incompatibles avec tout modèle intégrant de façon explicite des paramètres supplémentaires – on dit aussi des « variables cachées » – qui, dans notre cas, détermineraient la polarisation initiale de chacun des deux photons dès leur émission. En d'autres termes, aucune théorie à paramètres supplémentaires ne peut, pour l'ensemble des orientations possibles des deux polariseurs, reproduire les valeurs des corrélations prédites par la mécanique quantique.

Plus précisément, le théorème démontré par Bell établit que, dans toute théorie à variables cachées, les

corrélations pour les paires intriquées vérifient certaines inégalités. Or les corrélations prévues par la mécanique quantique violent ces inégalités, d'où la conclusion qu'on ne peut rendre compte des corrélations de type EPR par un modèle où des paramètres supplémentaires détermineraient l'état individuel des particules.

Ce résultat a une grande portée conceptuelle. La violation des inégalités de Bell par les prédictions quantiques démontre que les corrélations quantiques ne peuvent se comprendre à l'aide de concepts classiques. L'autre conséquence importante est la possibilité de trancher par l'expérience le débat entre Einstein et Bohr : il suffit en principe de mesurer les corrélations dans une situation où la mécanique quantique prédit une violation des inégalités de Bell pour savoir s'il faut renoncer à une interprétation à la Einstein, ou si, au contraire, on a identifié une situation où la mécanique quantique est prise en défaut.

Bell insista dès le début sur le fait que la démonstration des inégalités, donc la contradiction avec les prédictions quantiques, repose sur une hypothèse de localité. En particulier, on suppose que le résultat de la mesure par le polariseur I ne peut dépendre de l'orientation du polariseur II, et *vice versa*. La condition de localité paraît naturelle, mais elle ne découle d'aucune loi fondamentale : rien n'interdit qu'une interaction inconnue permette à l'orientation du polariseur II d'influer sur le polariseur I. Cependant, Bell souligna qu'en modifiant assez rapidement les orientations des polariseurs au cours de la propagation des photons entre la source et les polariseurs, une action d'un polariseur sur l'autre serait impossible puisqu'aucune interaction physique ne peut, selon la théorie de la relativité, se propager plus vite que la lumière.

Dans cette situation, l'expérience des photons intriqués mettrait à l'épreuve les idées d'Einstein, à savoir la possibilité de compléter le formalisme quantique et l'impossibilité d'une interaction à une vitesse supérieure à celle de la lumière. C'est donc bien le conflit entre la vision du monde défendue par Einstein et la mécanique quantique qu'allaient sonder les tests expérimentaux des inégalités de Bell.

Après une première génération d'expériences dans les années 1970, notre équipe à l'Institut d'optique d'Orsay, dirigée par A. Aspect, parvint en 1982 à tester cette hypothèse de localité pour la première fois. Dans l'expérience, les polariseurs étaient éloignés de 12 mètres l'un de l'autre (voir la figure 3), ce qui correspond à un temps de propagation de 40 nanosecondes pour la lumière. Il fallait modifier aléatoirement l'orientation de chaque polariseur à une cadence assez élevée pour interdire toute dépendance directe entre le choix de l'orientation d'un polariseur et la mesure par l'autre. Or il est impossible de modifier l'orientation de polariseurs massifs en quelques nanosecondes (aucun matériau n'y résisterait).

Nous avons contourné la difficulté en développant des commutateurs optiques rapides qui, soit laissent passer la lumière vers un premier polariseur, soit l'aiguillent vers un deuxième polariseur orienté différemment. L'ensemble constitué d'un commutateur et de deux polariseurs équivaut à un seul polariseur basculant entre deux orientations, à une cadence limitée seulement par le commutateur. Les 40 nanosecondes de propagation de la lumière étant une durée nettement plus longue que l'intervalle de temps entre deux basculements successifs d'un commutateur (environ dix nanosecondes), la condition de localité était vérifiée. Or l'expérience a mis en évidence une nette violation des inégalités de Bell : les prédictions quantiques étaient réalisées, au détriment des conceptions d'Einstein.

Ces premiers résultats ont été confirmés par la suite avec de nouvelles sources de paires de photons intriqués, exploitant des effets d'optique non linéaire dans des cristaux anisotropes. Grâce à ces sources, on maîtrise la direction d'émission des photons, ce qui permet d'injecter les deux photons d'une paire dans des fibres optiques de directions opposées. On a ainsi réalisé des expériences avec des distances source-détecteur de plusieurs centaines de mètres, voire des dizaines de kilomètres, comme dans les expériences réalisées dès 1998 par une équipe de l'Université de Genève et qui utilisent le réseau de fibres optiques de la Compagnie suisse de télécommunica-

tions (voir la figure 4). Avec de telles distances, il devient possible de choisir de façon totalement aléatoire l'orientation de chaque polariseur pendant la durée de propagation des photons depuis la source. C'est ce qu'ont fait en 1999 Anton Zeilinger et ses collègues, à l'Université d'Innsbruck, expérience qui a confirmé sans ambiguïté la violation des inégalités de Bell. D'autres expériences ont été effectuées en 2001 par David Wineland et ses collègues, à Boulder aux États-Unis, en intriquant non pas les polarisations de deux photons, mais les états électroniques de deux ions.

Ainsi, de nos jours, un grand nombre de données expérimentales indiquent clairement que les inégalités de Bell sont violées. De plus, l'accord quantitatif avec les prédictions de la théorie quantique est tel, qu'il est désormais difficile d'imaginer une théorie non quantique capable de reproduire les prédictions quantiques à ce niveau de précision. Nous devons accepter l'idée que l'on ne peut pas toujours concevoir le monde comme formé de sous-systèmes séparés, aux propriétés physiques définies localement et qui ne s'influenceraient pas lorsque les sous-systèmes sont séparés au sens relativiste. Il nous faut renoncer à la vision dite « réaliste locale » du monde que défendait Einstein.

## Intriquer pour crypter en sécurité

Les sept décennies qui vont de l'article EPR aux inégalités de Bell et aux expériences qu'elles ont suscitées pourraient donner le sentiment frustrant d'une conclusion négative : l'intrication quantique est avérée et nous oblige à renoncer à notre vision traditionnelle de la réalité physique. Or ce renoncement est porteur de progrès : on commence à appliquer l'intrication quantique au traitement et à la transmission de l'information.

L'idée directrice de l'information quantique, champ de recherche nouveau et actif, est que l'on peut, en mettant à profit les particularités quantiques, concevoir de nouvelles façons de calculer et de communiquer. Il s'agit, d'une part, de méthodes de cryptage dont la sécurité serait garantie ; d'autre part, de procédés de calcul incomparablement plus efficaces que ceux des ordinateurs actuels. Aussi, ces recherches ne concernent pas seulement les physiciens, mais également les mathématiciens et les informaticiens.

En cryptographie, l'objectif est la transmission d'un message secret entre un émetteur (Alice) et un récepteur (Bernard), en minimisant les risques qu'un espion (Ève) intercepte et déchiffre le message. Le plus souvent,



**4. Dès 1998**, une équipe de l'Université de Genève a réalisé des expériences où l'on produisait des paires intriquées de photons qui se propageaient dans les fibres optiques du réseau commercial suisse de télécommunications. La source, située à Cornavin (a), était à plus de dix kilomètres des détecteurs, situés à Bellevue (b) et à Bernex (c). Ces expériences ont confirmé que l'intrication persiste sans affaiblissement même lorsque les deux membres de la paire s'éloignent à des distances considérables.

## UN PROTOCOLE DE CRYPTAGE QUANTIQUE

L'une des méthodes possibles de cryptage quantique repose sur l'échange de photons et la mesure de leurs états de polarisation. On suppose qu'Alice et Bernard veulent communiquer en toute sécurité et, pour ce faire, utilisent des paires de photons intriqués, Alice recevant l'un des membres de chaque paire, et Bernard l'autre. Les deux correspondants conviennent de mesurer les polarisations suivant deux bases différentes, au choix : soit la base constituée par les directions horizontale (**h**) et verticale (**v**), soit la base constituée par un axe incliné à 45 degrés à droite (**d**) ou un axe incliné à 45 degrés à gauche (**g**). Dans la base **hv** (en bleu sur le schéma), la mesure de la polarisation d'un photon a pour résultat soit **h**, soit **v** ; de même, dans la base **dg** (en rouge sur le schéma), le résultat est soit **d**, soit **g**. On démontre que ces deux bases sont incompatibles : si par exemple on a mesuré la polarisation d'un photon dans la base **hv** avec pour résultat **h**, une mesure ultérieure selon la base **dg** donnera un résultat aléatoire, c'est-à-dire **d** ou **g** avec des probabilités égales. En d'autres termes, le changement de base brouille complètement l'état de polarisation qui a été déterminé par la première mesure.

Ces propriétés peuvent être exploitées de la façon suivante. Alice choisit au hasard pour chaque photon sa base de mesure, sans divulguer son choix. Bernard fait de même, de son côté. Puis Bernard communique (sans précautions particulières) à Alice tous ses choix de base, en indiquant le résultat de la mesure pour une partie des photons reçus. En analysant les cas où les choix de base de Bernard sont identiques aux siens, Alice peut déterminer s'il y a eu ou non interception par un espion (Ève). En effet, dans le cas où la base choisie par Alice et Bernard est la même (seuls cas illustrés sur le schéma ci-dessous), les résultats de leurs mesures doivent être identiques : si Bernard obtient un résultat différent (cas illustrés par les deuxième et cinquième colonnes du schéma), c'est qu'Ève a brouillé la polarisation du photon en effectuant une mesure selon la mauvaise base. En d'autres termes, quand Ève intercepte un photon, elle le brouille une fois sur deux en moyenne, et ces perturbations sont décelables par Alice au moyen d'une analyse statistique portant sur les cas où les choix de base d'Alice et de Bernard ont été identiques. Si l'analyse montre qu'il n'y a pas eu d'interception, Alice pourra se servir d'une partie des résultats non divulgués par Bernard pour constituer sa clef de codage, en indiquant à Bernard les numéros des photons correspondants.

Alice							Bases d'Alice
							Polarisations détectées par Alice
Ève							Bases d'Ève
							Polarisations détectées par Ève
Bernard							Bases de Bernard
							Polarisations détectées par Bernard

la cryptographie classique utilise des algorithmes de codage qui ne peuvent être cassés en un temps raisonnable avec les moyens de calcul disponibles. La sécurité ainsi obtenue est acceptable, mais elle n'est pas absolue : elle dépend des moyens dont dispose l'adversaire. De plus, on ne peut généralement pas la prouver mathématiquement.

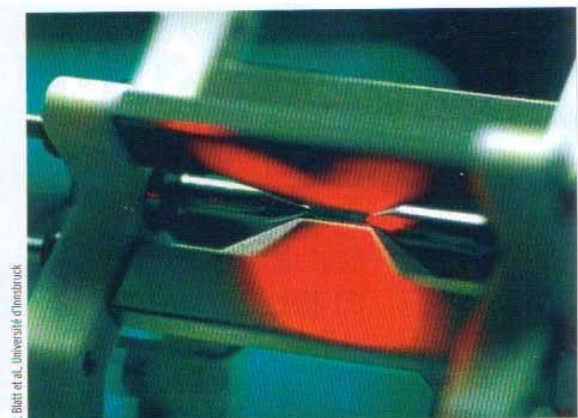
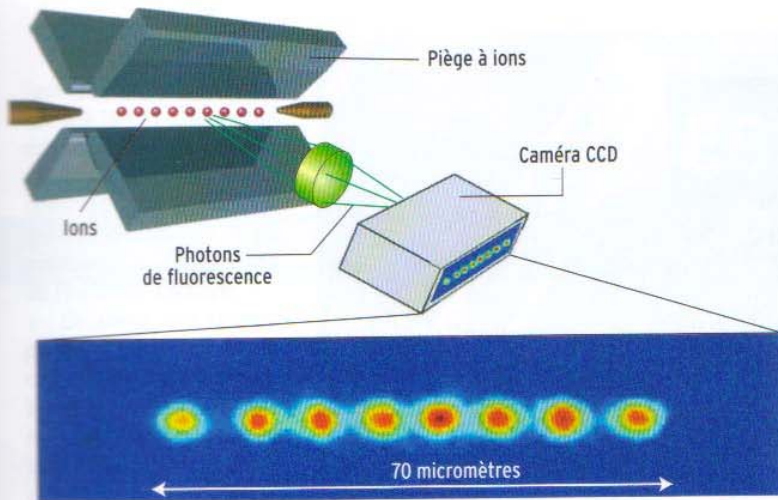
Il existe cependant une méthode de cryptographie simple et dont la sécurité est totale du point de vue mathématique. Elle suppose qu'Alice et Bernard ont échangé par avance une clef secrète, c'est-à-dire une longue suite de caractères ou de nombres connue d'eux seuls. Cette clef secrète servira à coder le message qui sera échangé sur un canal non sécurisé. Le mathématicien américain Claude Shannon a démontré en 1948 que si la clef secrète est aussi longue que le message, et si elle n'est utilisée qu'une seule fois, alors le cryptage est d'une sécurité totale. La sécurité de la communication est ici reportée sur la sécurité du partage de la clef de cryptage. C'est à ce stade que la cryptographie quantique peut intervenir : elle permet à Alice et Bernard de disposer de deux copies identiques d'une même clef secrète, avec une sécurité garantie par les principes mêmes de la physique quantique.

### Quand l'indiscrétion se révèle

De nombreux protocoles de cryptographie quantique ont été proposés, soit avec des photons uniques (par exemple, le protocole BB84, publié en 1984 par Charles Benett, d'IBM, et Gilles Brassard, de l'Université de Montréal), soit avec des photons intriqués (voir l'encadré ci-contre). La sécurité d'un tel protocole repose sur le fait que si un espion, Ève, intercepte une partie des photons échangés entre Alice et Bernard, cette interception perturbe inévitablement les états quantiques des photons, perturbation qu'Alice et Bernard sont en mesure de détecter. On ne peut même pas envisager que l'espion fasse juste une copie à l'identique des photons échangés, sans les modifier : en 1982, William Wothers et Wojciech Zurek, du Laboratoire de Los Alamos, ont prouvé qu'il est impossible de cloner (c'est-à-dire faire une copie exacte) un état quantique sur lequel on n'a aucune information préalable.

Actuellement, les distances de transmission obtenues dans les dispositifs expérimentaux de cryptage quantique atteignent quelques dizaines de kilomètres, grâce notamment aux fibres optiques. Ces systèmes sont en concurrence avec les systèmes cryptographiques conventionnels. Qui plus est, l'intérêt du cryptage quantique est devenu manifeste en 1994, lorsque Peter Shor, qui travaillait aux Laboratoires Bell, aux États-Unis, a ébranlé la confiance dans les systèmes cryptographiques classiques.

L'idée en filigrane des travaux de P. Shor est celle du calcul quantique. De quoi s'agit-il ? Un ordinateur classique manipule des bits classiques, c'est-à-dire des états électroniques binaires que l'on symbolise par des 0 ou des 1. Ces bits prennent soit la valeur 0, soit la valeur 1. On peut envisager des bits quantiques, c'est-à-dire des



**S. PLUSIEURS ÉQUIPES DANS LE MONDE** tentent de créer et de contrôler des ensembles de quelques bits quantiques, notamment pour réaliser un jour un ordinateur quantique. Un exemple tout récent est constitué par les expériences de Rainer Blatt et ses collègues à l'Université d'Innsbruck, où ces physiciens ont créé, contrôlé et mesuré

des états intriqués de huit particules. Il s'agit ici d'ions de calcium 40 retenus à l'intérieur d'un piège électromagnétique (à droite). Les ions (à gauche) sont manipulés à l'aide d'un faisceau laser, qui les porte de leur état d'énergie fondamental à un certain état excité. Ils sont détectés à l'aide d'un autre laser, qui provoque leur fluorescence.

systèmes quantiques (atomes, photons, etc.) décrits par deux états quantiques de base, notons-les  $|0\rangle$  et  $|1\rangle$ . La particularité quantique, inconcevable en physique classique, est que l'état du système est généralement une superposition des états de base ; autrement dit, l'état décrivant le système est de la forme  $a|0\rangle + b|1\rangle$ , où  $a$  et  $b$  sont des coefficients numériques, qui déterminent les probabilités d'obtenir, lors d'une mesure de l'état du système, la valeur 0 ou la valeur 1. Pour les physiciens, un tel système se trouve à la fois dans l'état  $|0\rangle$  et dans l'état  $|1\rangle$ , et son comportement se distingue de celui d'un système classique qui serait soit dans l'état 0, soit dans l'état 1 avec certaines probabilités.

### Calcul quantique : un parallélisme massif

Si l'on imagine à présent un registre formé par un ensemble de  $N$  bits quantiques dont l'état de chacun est une combinaison des deux états de base, on comprend que cet ensemble peut représenter  $2^N$  nombres *simultanément*, alors qu'un registre classique de  $N$  bits n'en représente qu'un seul (choisi parmi  $2^N$ ). La manipulation de bits quantiques apporterait ainsi un parallélisme intrinsèque et massif, qui accroîtrait de façon exponentielle les capacités des ordinateurs.

Or P. Shor a conçu un algorithme de calcul, fondé sur des bits quantiques, montrant qu'un ordinateur quantique pourrait décomposer n'importe quel

grand nombre en ses facteurs premiers beaucoup plus rapidement qu'un ordinateur classique. D'où l'impact sur la cryptographie, car l'une des méthodes de cryptage les plus sûres utilisées actuellement – la méthode RSA – est précisément fondée sur la difficulté de factoriser de grands nombres. Si l'ordinateur quantique rend une telle tâche facile, la sécurité du chiffage est caduque !

L'ordinateur quantique serait en tout cas un instrument révolutionnaire, que ce soit pour la cryptographie ou pour d'autres domaines scientifiques et techniques. Reste que la concrétisation d'un tel dispositif sera, sinon une utopie, du moins d'une difficulté extrême. Si le calcul quantique devient réalité, ce sera dans un avenir assez lointain, dans quelques dizaines d'années au moins. À l'heure actuelle, il est possible d'effectuer des opérations élémentaires mettant en jeu quelques bits quantiques, que l'on peut aussi placer dans des états intriqués. Parmi les progrès récents, citons la téléportation quantique, qui consiste à transférer un état quantique d'un qubit à un autre, sans jamais connaître cet état – une prouesse qui exploite de façon subtile les propriétés de l'intrication.

Toutefois, les scientifiques sont encore très loin d'obtenir et de contrôler des ensembles formés d'un grand nombre de bits quantiques, comme l'exigerait un ordinateur quantique. Les idées les plus prometteuses pour réaliser l'ingénierie nécessaire semblent liées à la manipulation d'objets quan-

tiques individuels (photons, atomes, ions, spins, circuits de taille nanométrique, etc.), qu'il faudrait à terme assembler à une grande échelle. Ce changement d'échelle n'ayant pas encore de réalité, il est impossible de prédire si l'ordinateur quantique calculera un jour et, dans l'affirmative, s'il ressemblera à ce que l'on peut imaginer aujourd'hui ou s'il fera appel à des techniques auxquelles personne n'a encore songé. Quoiqu'il en soit, on peut déjà affirmer que l'intrication quantique, concept extraordinaire dont Einstein fut l'un des principaux découvreurs, a fécondé la science et ouvert de nouveaux horizons à ses applications.

**Alain ASPECT et Philippe GRANGIER** sont directeurs de recherche au CNRS et travaillent au Laboratoire Charles Fabry de l'Institut d'optique.

J. S. BELL, *Speakable and unspeakable in quantum mechanics*, Cambridge University Press (2<sup>e</sup> édition), 2004.

Ph. GRANGIER et I. ABRAM, *Single photons on demand*, in *Physics World*, p. 31, février 2003.

A. ASPECT, *Bell's theorem: the naive view of an experimentalist*, in *Quantum [un]speakables, from Bell to quantum information*, R.A. Bertlmann et A. Zeilinger (éds.), Springer, 2002 (en ligne : <http://hal.ccsd.cnrs.fr/ccsd-00001079>).

N. Gisin et al., *Quantum cryptography*, in *Rev. Mod. Phys.*, vol. 74, p. 145, 2002 (en ligne : <http://arxiv.org/abs/quant-ph/0101098>).

M. A. NIELSEN et I. L. CHUANG, *Quantum computation and quantum information*, Cambridge University Press, 2000.

Cours de J. Preskill : <http://www.theory.caltech.edu/people/preskill>