et, depuis, les expériences n'ont cessé de se rapprocher du dispositif idéal proposé par Bell. Les expériences ont trouvé des corrélations qui violent l'inégalité de Bell, ce qui éliminait les théories locales à variables cachées. Mais jusqu'en 2015, toutes ces expériences reposaient sur une ou plusieurs hypothèses *ad hoc* à cause d'imperfections des dispositifs. Ces hypothèses comportaient des failles que les théories locales à variables cachées pouvaient en principe exploiter pour réussir le test.

Grâce à l'intrication quantique, il est possible de créer des générateurs de nombres vraiment aléatoires

Dans presque toutes les expériences de ce type au XX^{e} siècle, les scientifiques ont produit des photons intriqués à partir d'une source, et les ont envoyés dans des stations de mesure (représentant Alice et Bernard). Ces dernières enregistraient la polarisation d'un photon de la paire, c'est-à-dire la direction dans laquelle oscille le champ électrique du photon. Les chercheurs calculaient alors les corrélations moyennes entre les résultats des deux stations et examinaient si les inégalités de Bell étaient respectées ou violées.

Dans les premières expériences, les mesures étaient effectuées selon des directions fixes. Dans ce cas, une interaction avait le temps de s'établir entre les dispositifs et créer d'éventuelles corrélations. Autrement dit, des signaux cachés indiqueraient à Bernard, sans voyager plus vite que la lumière, quelle direction Alice a utilisée pour mesurer son photon. Cette « échappatoire (ou faille) de localité » signifie qu'une théorie locale à variables cachées obtiendrait les mêmes corrélations que la théorie quantique. En 1982, Alain Aspect, de l'Institut d'optique, à Orsay, et ses collègues ont effectué un test amélioré dans lequel les photons étaient envoyés à deux extrémités d'une pièce. Pendant que ces photons intriqués étaient en vol, l'angle de polarisation du dispositif de mesure changeait périodiquement. À la fin des années 1990, Anton Zeilinger, aujourd'hui à l'université de Vienne, et son équipe ont perfectionné cette stratégie en utilisant des directions de mesure de polarisation vraiment aléatoires (et non simplement périodiques) et déterminées juste avant que les mesures n'aient lieu. Si les signaux cachés existent, ils devraient se propager plus vite que la lumière pour influer sur ces mesures. La faille de localité était hermétiquement comblée.

Mais ces expériences présentaient un inconvénient de taille : il est difficile de travailler avec des photons, particules qui peuvent se perdre en vol ou tout simplement ne pas être vues par les détecteurs. La plupart du temps, une mesure ne donnait pas de résultat, car les photons se perdaient en chemin. Les expérimentateurs étaient obligés d'éliminer les mesures ratées et de supposer que les mesures réussies étaient représentatives de l'ensemble des paires intriquées (l'« hypothèse d'échantillonnage sans biais »). Sans cette supposition, il est impossible de garantir que l'ajout des photons perdus ne donne pas un résultat compatible avec les théories à variables cachées.

Les scientifiques ont éliminé cette échappatoire de détection au début de ce siècle, en abandonnant les photons au profit d'autres systèmes intriqués et mesurés avec une bonne efficacité : des ions piégés, des atomes et des circuits supraconducteurs. Le problème est que, dans ces cas, les contraintes techniques imposaient que les particules soient assez proches, ce qui laissait ouverte la faille de localité. Un test de Bell pour lequel toutes les échappatoires seraient supprimées est devenu l'un des grands défis de la science quantique.

Grâce aux progrès réalisés dans le contrôle et la mesure des systèmes quantiques, il est devenu possible en 2015 d'effectuer un test de Bell avec un dispositif idéal, ce qu'on appelle un test de Bell sans échappatoire (ou sans faille). En fait, en peu de temps, quatre groupes différents de physiciens ont trouvé des résultats violant les inégalités de Bell tout en éliminant les deux échappatoires. Ces expériences ont ainsi fourni des preuves indiscutables qui réfutent les théories locales à variables cachées.

ÉLIMINER LES FAILLES

L'un d'entre nous (Ronald Hanson) a effectué avec ses collègues la première expérience éliminant toutes les échappatoires à l'université de technologie de Delft, aux Pays-Bas (*voir la photo page 55 et l'encadré pages 56 et 57*). Nous avons intriqué les spins de deux électrons présents chacun dans un défaut cristallin d'un diamant, c'est-à-dire dans un site où il manque un atome de carbone. Les deux électrons intriqués étaient dans des laboratoires situés de part et d'autre du campus, et pour être sûrs qu'aucune communication n'était possible entre les deux, nous avons utilisé un générateur de nombres >

> aléatoires rapide pour sélectionner la direction de mesure. Cette mesure était finalisée et enregistrée localement sur un disque dur avant que la moindre information concernant la mesure de l'autre côté n'ait eu le temps d'arriver, même à la vitesse de la lumière. Un signal caché indiquant à l'un des dispositifs de mesure la direction utilisée par l'autre n'aurait pas eu le temps de faire le trajet entre les deux laboratoires : on contrôlait ainsi entièrement la faille de localité.

TÉLÉPORTATION D'INTRICATION

Ce chronométrage strict nous a imposé de séparer les deux électrons de plus de un kilomètre, une distance supérieure de deux ordres de grandeur aux précédents records mondiaux pour des particules de matière intriquées. Comment intriquer des électrons sur une telle distance ? Nous avons utilisé une technique nommée « téléportation d'intrication », où l'on commence par intriquer chaque électron avec un photon. Nous envoyons alors les photons à la rencontre l'un de l'autre, à mi-chemin des deux laboratoires. Ils se retrouvent sur un miroir semi-réfléchissant où nous avons placé des détecteurs de chaque côté. Si nous détectons les photons sur des côtés opposés du miroir, alors les spins des électrons intriqués avec chaque photon deviennent eux-mêmes intriqués. En d'autres termes, l'intrication entre les électrons et les photons est transférée aux deux électrons.

Ce processus de transfert échoue souvent, car les photons se perdent entre les diamants et le miroir, comme dans les expériences précédentes. Mais nous ne lançons un test de Bell que si les deux photons sont détectés ; ainsi, nous traitons la perte de photons en amont. De cette façon, nous éliminons la faille de détection, parce que nous n'excluons aucun résultat des tests de Bell sur des électrons intriqués. La perte de photons liée à la grande distance de séparation ne limite donc pas la qualité de l'intrication, mais, en revanche, elle réduit de façon drastique le nombre d'événements à notre disposition pour le test de Bell – quelques-uns par heure.

Après plusieurs semaines de mesures en juin 2015, nous avons trouvé que l'inégalité de Bell était violée à hauteur de 20 %, en accord avec les prédictions de la théorie quantique. La probabilité d'obtenir par hasard un tel résultat dans le cadre d'un modèle à variables cachées locales (et en admettant que les dispositifs aient conspiré en utilisant toutes les données disponibles) était de 3,9 %. Lors d'une deuxième série de mesures en décembre 2015, nous avons trouvé un taux similaire de violation des inégalités de Bell.

La même année, trois autres groupes ont effectué des tests de Bell sans échappatoire. En septembre, l'équipe du NIST (l'Institut américain des normes et de la technologie), dirigée par l'un d'entre nous (Krister Shalm), et celle d'Anton Zeilinger ont utilisé des photons intriqués. Peu après, Harald Weinfurter, de l'université Ludwig-Maximilian, à Munich, et ses collègues ont utilisé des atomes de rubidium distants de 400 mètres dans un protocole similaire à celui du groupe de Ronald Hanson.

Les équipes du NIST et de Vienne ont intriqué les états de polarisation de deux photons au moyen de lasers intenses dirigés sur un matériau cristallin particulier. Très rarement (environ une fois pour un milliard de photons pénétrant dans le cristal), un photon émis par un laser interagissait d'une façon particulière en donnant naissance à une paire de photons dont les états de polarisation étaient intriqués. Avec des lasers assez puissants, les chercheurs ont produit des dizaines de milliers de paires de photons intriqués par seconde. On envoyait alors ces photons

L'INTRICATION QUANTIQUE SUFFIT-ELLE POUR FAIRE DES SYSTÈMES SÉCURISÉS ?

L'intrication quantique est exploitée dans de nombreuses applications, en particulier pour sécuriser des communications. Il est par exemple possible d'utiliser des photons intriqués pour établir, à distance, une clé de chiffrement qui sera utilisée pour sécuriser un message. Alice et Bernard mesurent la polarisation d'une série de photons intriqués (la polarisation « horizontale » codant pour le bit « 0 » et « verticale » pour le bit « 1 »). En plus de fournir la clé, ce système indique aussi si la transmission de la clé a été interceptée par un ennemi. En effet, une mesure sur un photon influe sur son état. Dès lors, si quelqu'un « écoute » la transmission de la clé, Alice et Bernard peuvent le savoir et il leur suffit de renvoyer une nouvelle clé jusqu'à être certain que celle-ci n'a pas été compromise. Si la théorie est robuste, c'est souvent la réalisation expérimentale qui introduit des failles. Par exemple, la transmission des photons dans une fibre optique de plus de 10 kilomètres de longueur conduit à une perte de signal : un attaquant pourrait alors exploiter la faille de détection. En 2016, Sébastien Tanzilli, du CNRS et de l'université Côte-d'Azur, Nicolas Gisin, de l'université de Genève, et leurs collègues ont étudié le cas où l'attaquant a un contrôle relatif (mais non total) sur l'efficacité de détection du système. En interceptant une partie des photons, il peut acquérir une partie de la clé. Malgré cela, les chercheurs ont montré que des inégalités de Bell plus générales restent violées. Tant que son contrôle reste limité, l'adversaire peut ainsi être démasqué. Les systèmes de cryptographie quantique offrent une grande robustesse contre des attaques et sont efficaces pour sécuriser un réseau de communication, mais ils ne sont pas pour autant invulnérables. Mal conçus, ces systèmes s'exposent à des failles fatales que les attaquants cherchent inlassablement…

vers des stations séparées (de 184 mètres dans l'expérience du NIST, de 60 mètres dans l'expérience de Vienne) où l'on mesurait les états de polarisation. La direction de mesure était décidée pendant le temps de vol des photons, ce qui éliminait la faille de localité.

Pour la faille de détection, il fallait récupérer plus des deux tiers des photons intriqués pour que l'on soit sûr d'avoir un échantillon représentatif. Au NIST, nous avons développé des détecteurs de photons uniques ultraperformants et constitués de matériaux supraconducteurs froids. Ces capteurs sont capables d'observer plus de 90% des photons qui les atteignent. La faille de détection était ainsi supprimée.

En répétant plus de 100 000 fois par seconde ces mesures, nous avons très vite accumulé des résultats statistiques significatifs sur les corrélations entre les états de polarisation des photons; les corrélations observées dans les deux expériences étaient beaucoup plus fortes que celles prédites par les théories à variables cachées. De fait, la probabilité que les résultats du NIST soient le fruit du hasard est de l'ordre de un milliardième, et les chances sont encore plus faibles avec l'expérience viennoise. Aujourd'hui, le groupe du NIST utilise une version améliorée du dispositif pour violer les inégalités de Bell à un degré similaire en moins de une minute, et des perfectionnements attendus accéléreront encore le processus de deux ordres de grandeur.

DES GÉNÉRATEURS D'ALÉA

Ces expériences nous obligent à conclure que tous les modèles à variables cachées, tels ceux que soutenait Einstein, sont incompatibles avec la nature. Les corrélations que nous avons observées entre particules défient notre intuition, et nous démontrent que la fantomatique action à distance a bien lieu.

Nos résultats mettent aussi en avant la remarquable puissance de l'intrication pour d'éventuelles applications. À court terme, une situation où des tests de Bell sans faille seraient utiles est la génération de nombres aléatoires. De nombreuses techniques de cryptographie reposent sur la capacité à produire des nombres aléatoires. Or, en pratique, ces derniers sont difficiles à produire. Les générateurs de nombres aléatoires sont loin d'être infaillibles et s'il est possible d'anticiper les nombres qu'ils produisent, de nombreux systèmes financiers et de communication seraient en danger. Une bonne source de nombres aléatoires est donc d'une importance cruciale.

Pour générer des nombres aléatoires, on recourt le plus souvent à des algorithmes ou à des processus physiques. Avec les algorithmes, si l'on connaît les paramètres utilisés comme valeurs initiales, il est souvent possible de prédire le résultat. Avec les processus physiques, une compréhension détaillée de la physique sous-jacente du système est nécessaire. Il suffit qu'un détail vous échappe, et un pirate exploitera cette faille. L'histoire de la cryptographie regorge d'exemples de générateurs de nombres aléatoires des deux types qui ont été cassés.

La physique quantique est une aubaine pour ces applications. Il est possible d'« extraire » le hasard inhérent aux processus quantiques afin de produire des nombres véritablement aléatoires. On peut convertir les corrélations mesurées dans un test de Bell sans échappatoire en une chaîne de nombres aléatoires. En 2018, l'équipe du NIST a utilisé son dispositif pour produire 1024 bits véritablement aléatoires à partir de 10 minutes de données expérimentales. La violation des inégalités de Bell garantit que la chaîne de bits est aléatoire.

Il est possible de quantifier la robustesse du système: il y a une chance sur un billion que la chaîne de bits du NIST ne soit pas parfaitement aléatoire. En comparaison, il faudrait plusieurs centaines de milliers d'années à un générateur classique de nombres aléatoires pour acquérir assez de données assurant une telle qualité d'aléa. Les chercheurs travaillent maintenant à développer un outil public: le générateur servirait de source de référence de nombres aléatoires datés et transmis sur internet à intervalles fixes pour être utilisés dans des applications de sécurité.

Plus généralement, les techniques développées dans les expériences de Bell sans faille rendraient possibles le déploiement de nouveaux types de réseaux de communication. De tels réseaux, qui constituent ce que l'on appelle souvent l'« internet quantique », effectueraient des tâches dépassant les capacités des réseaux classiques. Un internet quantique garantirait des communications sécurisées, la synchronisation des horloges, et bien d'autres tâches sensibles.

De tels projets reposent sur l'intrication quantique et la qualité des dispositifs, comme dans nos expériences. En 2017, l'équipe de Delft a fait la démonstration d'une méthode pour améliorer la qualité des spins intriqués, et en 2018, elle a amélioré ses taux d'intrication de trois ordres de grandeur. En s'appuyant sur ces progrès, les chercheurs travaillent au développement d'une première version rudimentaire d'un internet quantique qui devrait être déployé en 2020 dans quelques villes des Pays-Bas.

Il y a quatre-vingts ans, quand la théorie quantique faisait ses débuts, les sceptiques se chagrinaient de sa contradiction apparente avec des siècles d'intuition physique. Désormais, quatre expériences ont asséné le coup final à cette intuition; mais, en même temps, ces résultats ont ouvert une porte pour exploiter la nature d'une façon que ni Einstein ni Bell n'avaient anticipée. La révolution silencieuse que John Bell a mise en branle bat maintenant son plein. ■

BIBLIOGRAPHIE

J. Maldacena, **L'intrication quantique est-elle un trou de ver ?**, *Pour la Science*, n° 475, mai 2017.

B. Hensen *et al.*, **Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometers**, *Nature*, vol. 526, pp. 682-686, 2015.

M. Giustina *et al.*, **Significant-loophole-free test of Bell's theorem with entangled photons**, *Phys. Rev. Lett.*, vol. 115, art. 250401, 2015.

L. K. Shalm *et al.*, **Strong loophole-free test of local realism**, *Phys. Rev. Lett.*, vol. 115, art. 250402, 2015.