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.