Par ailleurs, le système de chiffrement quantique décrit ici repose surtout sur la violation des inégalités de Bell et le caractère non local de l'intrication quantique. Celui-ci est un fait expérimental confirmé par de nombreuses équipes. Pour convaincantes qu'elles soient, ces expériences laissent ouvertes certaines brèches. Par exemple, il est en principe possible que les photons détectés dans les expériences ne constituent pas un échantillon représentatif de tous les photons émis par la source (« échappatoire de détection ») ou que les différentes parties ou composantes de l'expérience aient été causalement reliées (« échappatoire de localité »).

L'expérience d'Alain Aspect, en 1982, par exemple, utilisait deux instruments suffisamment éloignés l'un de l'autre pour éviter qu'une communication à la vitesse de la lumière fausse les résultats des mesures. Mais cette expérience souffre de l'échappatoire de détection. En effet, tous les photons intriqués n'arrivent pas aux détecteurs, car certains sont absorbés en chemin. Comment garantir que le sous-groupe des photons qui arrivent aux détecteurs est représentatif de tous les photons émis ? Il est très difficile de combler la faille de détection, parce que presque tout composant optique ajoute des pertes et des imperfections au dispositif.

Il y avait peu de chance que la nature soit assez malveillante pour nous tromper de manière sélective – par l'échappatoire de localité dans certaines expériences, et par l'échappatoire de détection dans d'autres. En revanche, rien n'empêche un espion d'être trop curieux. Et il pourrait exploiter ces échappatoires à son profit.

Des expériences sans échappatoire

En 2013, l'équipe d'Anton Zeilinger, de l'université de Vienne, et celle de Paul Kwiat, de l'université de l'Illinois, ont montré qu'il était possible de contrôler l'échappatoire de détection. Mais sans garantir l'échappatoire de localité... Une autre expérience, mise au point en 2015 par l'équipe de Ronald Hanson, de l'université de Delft, aux Pays-Bas, contrôle les deux échappatoires. Ainsi, nous pouvons être rassurés sur la violation des inégalités de Bell et la fiabilité de la cryptographie quantique indépendante des dispositifs.

Cette dernière est tout sauf facile à mettre en pratique, mais les progrès technologiques réalisés jusqu'à présent portent à l'optimisme *(voir l'encadré page 33)*.

Depuis une quinzaine d'années, la cryptographie quantique a beaucoup évolué et de nombreux travaux ont renforcé la fiabilité du système. Elle est aussi une source d'inspiration très fertile pour la recherche fondamentale. La quête des limites ultimes de la confidentialité est encore en chantier, mais nous savons que l'on peut garantir la confidentialité sous des hypothèses étonnamment faibles. Les corrélations monogames, de quelque origine qu'elles soient, assorties à une quantité arbitrairement faible de libre arbitre, suffisent à dissimuler tout ce que nous voulons. Le libre arbitre est notre atout le plus précieux. Et à bien y réfléchir, s'il n'y a pas de libre arbitre, à quoi bon cacher quoi que ce soit de toute façon ? ■