une technique dite d'amplification de la confidentialité. L'idée est assez simple : imaginez que vous ayez deux bits et que votre adversaire en connaisse au plus un (sans que vous sachiez lequel). Additionnez les deux bits modulo 2 : le bit résultant sera inconnu de votre adversaire. Avec davantage de bits, il existe des moyens bien plus élaborés pour amplifier la confidentialité.

Pour résumer, à chaque fois que l'on donne à Alice et Bob des dispositifs qui produisent des résultats corrélés, ils peuvent faire tourner le protocole de distribution des clés, complété par un « test d'honnêteté » statistique afin d'estimer ε. Si cette valeur est suffisamment petite, disons $\varepsilon = 0{,}15$, le résultat final, après amplification de la confidentialité, est une clé de chiffrement parfaite. Nous obtenons ainsi une confidentialité fiable à partir de dispositifs non fiables.

Les corrélations monogames assorties à une quantité même faible de libre arbitre suffisent pour protéger notre vie privée

Certains points sont à vérifier avant que l'on soit sûr que notre système n'a pas de faille. En particulier, Alice et Bob peuvent-ils se faire confiance ? Il est difficile d'être plus paranoïaque que cela. Sont-ils libres de leurs choix, ou bien sont-ils contrôlés par une force qui leur échappe ?

Nous avons déjà souligné l'importance du libre arbitre dans le processus. Le choix de la pièce à lancer ou de la direction de polarisation à mesurer doit être fait librement (aléatoirement) et indépendamment. En général, dans les réalisations pratiques, des générateurs de nombres (pseudo)aléatoires se chargent de tels choix. Mais le hasard qu'ils simulent est-il de qualité satisfaisante ?

Il est évident que si tout est prédéterminé, si tous nos choix sont prévisibles ou préprogrammés par nos adversaires, il n'y a pas de confidentialité qui tienne.

Doper le libre arbitre

En réalité, il suffit que la prédétermination ne soit pas complète et qu'il reste un petit peu de liberté. Si une fraction des choix faits par nos générateurs de nombres aléatoires ne peut être déterminée par l'adversaire, alors la confidentialité est encore possible, parce que le caractère aléatoire local peut être amplifié. L'amplification du hasard est obtenue avec des protocoles indépendants du dispositif, et fonctionne même si la fraction de hasard initial est arbitrairement petite.

Tout cela semble bizarre et trop beau pour être vrai. Nous avons montré qu'il est, en théorie, possible d'amplifier le libre arbitre et la confidentialité pour obtenir une méthode de chiffrement totalement fiable. C'est cependant assez difficile à mettre en pratique.

Comme nous l'avons vu, l'un de nous (Artur Ekert) a proposé en 1991 un système de distribution quantique des clés fondé sur la violation des inégalités de Bell. L'année suivante, une démonstration de principe a été réalisée à la Defence Evaluation and Research Agency (aujourd'hui QinetiQ) à Malvern, au Royaume-Uni. Cependant, le caractère « indépendant du dispositif » (c'est-à-dire sans connaître parfaitement l'origine du dispositif) de ce protocole n'a été démontré qu'en 2007. Prouver la sécurité d'un tel système en conditions réelles n'a pas été facile. Il a fallu plus d'une décennie pour s'accorder sur une définition utile du secret, ne serait-ce que pour des dispositifs fiables, et pour réaliser une longue série de tests prenant en compte toutes les ressources quantiques qu'Ève peut mettre à son service. Un défi majeur consiste à rendre ces arguments de sécurité quantitatifs et robustes vis-à-vis du bruit et des imperfections du système.

Pour finir, il convient de souligner que les protocoles indépendants des dispositifs et leurs preuves de sécurité n'ont pas encore atteint le degré de sophistication qui est maintenant la norme pour le scénario dépendant des dispositifs. En particulier, des efforts sont nécessaires pour améliorer l'efficacité des protocoles de distribution des clés, et pour identifier les conditions dans lesquelles des dispositifs non éprouvés peuvent être réutilisés sur de multiples cycles de ces protocoles.

Les fondements quantiques du principe de chiffrement décrit ici sont aussi sujets à des interrogations. Nous avons implicitement supposé qu'il n'y a rien au-delà de la théorie quantique. Cependant, si Alice et Bob sont assez paranoïaques pour supposer qu'Ève a des capacités « postquantiques » (des technologies plus puissantes que les technologies quantiques, reposant sur des phénomènes physiques non encore découverts et non décrits par la physique quantique), ils peuvent encore avoir recours à des protocoles moins efficaces, mais ne reposant pas sur la théorie quantique *(voir l'article de Phong Nguyen page 36)*.

BIBLIOGRAPHIE

G. Brassard, **Cryptography in a quantum world**, *Lecture Notes in Computer Science* (Springer), vol. 9587, pp 3-16, 2016.

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

A. Ekert et R. Renner, **The ultimate physical limits of privacy**, *Nature*, vol. 507, pp. 443-447, 2014.

C. Bennett *et al.*, **La cryptographie quantique**, *Dossier Pour la Science*, n° 36, juillet-octobre 2002.

A. Ekert, **Quantum cryptography based on Bell's theorem**, *Phys. Rev. Lett.*, vol. 67, n° 6, pp. 661-663, 1991.