DES NOMBRES BIEN ALÉATOIRES

Produire des nombres aléatoires est d'importance capitale pour les techniques cryptographiques, car ces dernières sont fondées sur des clés de chiffrement, de longues chaînes de 0 et de 1. Si ces clés ne sont pas générées de façon parfaitement aléatoire, un pirate informatique serait éventuellement capable de percer leur logique; il pourrait alors les reconstituer et accéder aux données.

Depuis plusieurs années, les cryptologues s'intéressent à un domaine où l'aléatoire et l'imprévisible font loi: la physique quantique. Dans ce cadre, une équipe du NIST (l'institut américain des étalons et de la technologie) vient de présenter une méthode permettant de produire des nombres bien aléatoires.

Peter Bierhorst et ses collègues ont conçu un dispositif où l'on mesure la polarisation (la direction du champ électrique) de photons. Une source y émet des paires de photons dont les polarisations sont intriquées, c'est-à-dire étroitement corrélées par un phénomène quantique. La direction de la polarisation mesurée pour un photon est ensuite traduite en un bit 0 ou un bit 1. Et la valeur mesurée du bit est garantie aléatoire si la paire de photons est quantiquement intriquée. Or les chercheurs ont calculé, à partir des corrélations d'un ensemble de paires, que seule une petite part des bits générés a un caractère vraiment aléatoire. Les autres seraient éventuellement le résultat d'un processus non quantique, où l'aléatoire n'est pas garanti.

Les propriétés de la physique quantique sont exploitées pour générer des suites aléatoires de 0 et de 1.

Les chercheurs ont alors associé à leur dispositif un extracteur d'aléa, un outil courant en cryptographie qui prend un grand nombre de bits pour en donner un plus petit, mais dont le caractère aléatoire est fortement augmenté. L'équipe de Peter Bierhorst a ainsi pu générer des chaînes de 1024 bits presque parfaitement aléatoires. ■

DONOVAN THIEBAUD

P. Bierhorst *et al.*, *Nature*, vol. 556, pp. 223-226, 2018