Bientôt un système de chiffrement quantique pour sécuriser les paiements bancaires ?

GETTY IMAGES

UN WEB QUANTIQUE UN MILLION DE FOIS PLUS SÛR

Paiements bancaires, dossier médical global, messageries instantanées, objets connectés… : vous êtes-vous jamais demandé comment le transfert de vos données en ligne était protégé ? La méthode de cryptage la plus couramment utilisée est le « chiffrement RSA ». Mais il risque d'être bientôt dépassé. L'éventualité de voir apparaître bientôt le premier ordinateur quantique croît en effet de jour en jour. Et cette machine aura des capacités de calcul si démentielles que le décryptage des données chiffrées RSA sera pour elle un jeu d'enfant. Les hackers en salivent d'avance.

D'où l'empressement des spécialistes de trouver la parade en développant des systèmes de chiffrement… quantiques, eux aussi. Les Chinois seront-ils les premiers ? Fin 2017, ils ont en tout cas réussi la première communication intercontinentale par vidéoconférence entre Pékin et Vienne, protégée par un système cryptographique quantique apparemment inviolable. Le flux vidéo était protégé contre le piratage grâce à une technique au moins « un million de fois plus sûre que les méthodes conventionnelles de cryptage », selon l'Académie des sciences autrichienne.

Cette prouesse s'inscrit dans un projet de recherche financé par la Chine depuis 2013 et dénommé Quess pour « Expérimentation quantique à l'échelle spatiale ». C'est pour le réaliser que, le 16 août 2016, une fusée chinoise Longue Marche a placé en orbite basse Micius, le premier satellite quantique au monde. En cryptographie quantique, une clé de déchiffrement commune est bâtie entre l'expéditeur et le destinataire. Elle est une suite de bits informatiques représentés par les photons intriqués (c'est-à-dire connectés par un lien invisible qui existe quelle que soit la distance qui les sépare). Chaque photon est polarisé selon une certaine direction afin de porter la valeur 0 ou 1 d'un bit. Si un espion intercepte ces photons, il bloque leur polarisation, rendant illisible le message chiffré et la communication inviolable.

Micius a émis des photons intriqués et ceux-ci ont été réceptionnés dans deux télescopes séparés de 7 400 kilomètres, la distance entre Vienne et Pékin. Jamais cryptographie quantique n'avait été réalisée sur une si grande distance. Certaines entreprises et villes, comme Kazan en Russie, ont déjà installé une protection quantique mais sur de très courtes distances, en empruntant une voie exclusivement terrestre : un laser lance des photons intriqués dans de la fibre optique tendue entre l'expéditeur et le destinataire. Mais l'information s'atténuant lors de son passage, elle ne peut être transmise au-delà de 200 kilomètres. Pour des communications à plus grande distance, il faut un satellite quantique.

« Les expériences chinoises ouvrent une nouvelle ère. Relier quantiquement des systèmes éloignés devient réalité », s'enthousiasme Ronald Hanson, directeur de Qutech, un grand labo quantique européen, interrogé par *Le Monde*. L'essai devrait être répété entre Pékin et Singapour, puis avec l'Italie, l'Allemagne et la Russie, toujours via le satellite chinois Micius. Objectif ultime : créer un réseau Internet quantique mondial. Pour rendre l'utilisation du Web théoriquement inviolable. **LAETITIA THEUNIS**