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.

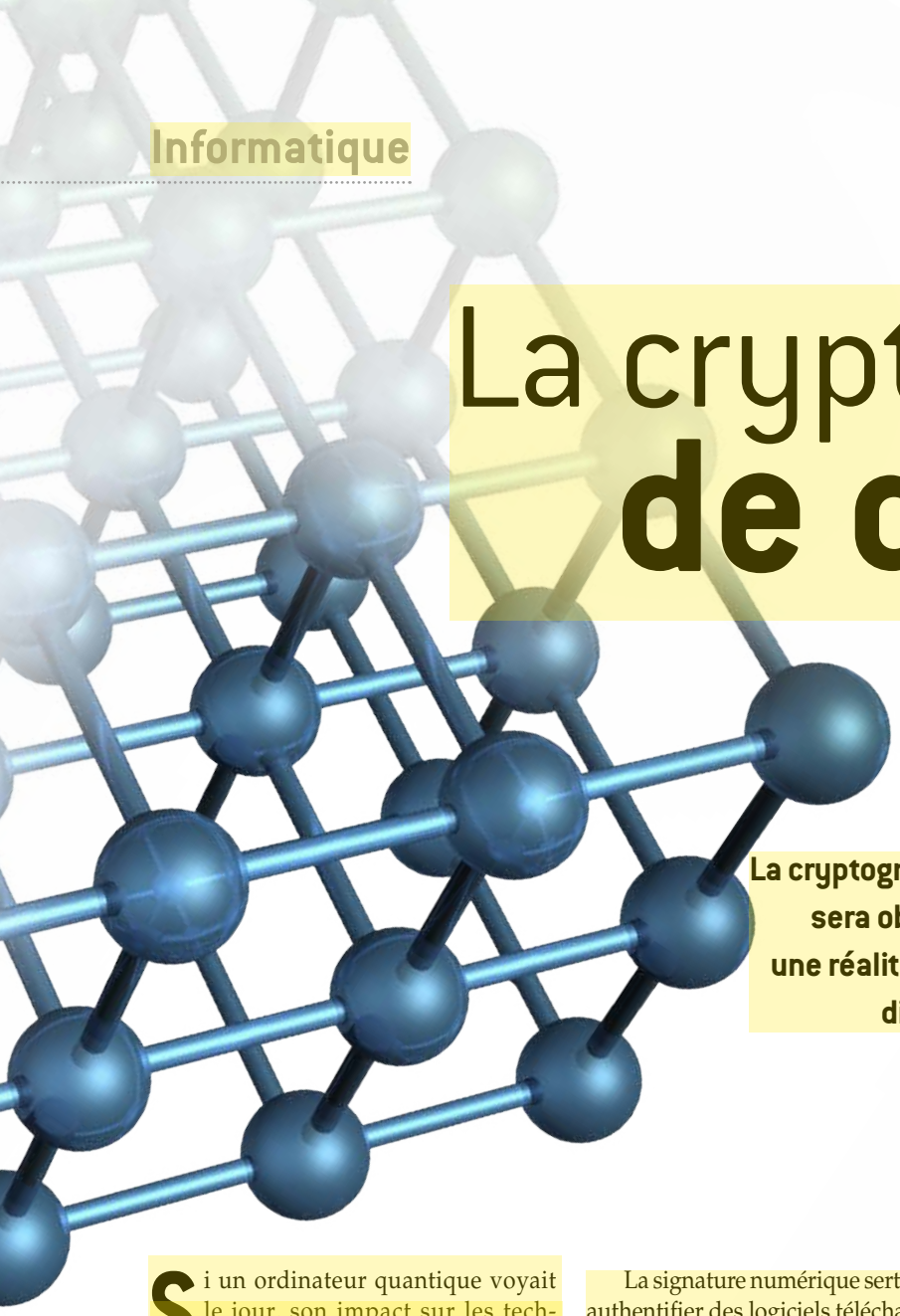
Il y avait peu de chance que la nature soit assez malveillante pour nous tromper de manière sélective – par l'échappatoire de localité dans certaines expériences, et par l'échappatoire de détection dans d'autres. En revanche, rien n'empêche un espion d'être trop curieux. Et il pourrait exploiter ces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



La cryptographie de demain

Phong Nguyen

La cryptographie à clé publique utilisée aujourd'hui sera obsolète si l'ordinateur quantique devient une réalité. Toutefois, des méthodes alternatives, dites postquantiques, sont déjà à l'étude.

Si un ordinateur quantique voyait le jour, son impact sur les techniques cryptographiques déployées aujourd'hui serait considérable. Les deux fonctionnalités les plus menacées par ses capacités de calcul sont le chiffrement à clé publique et la signature numérique.

Le chiffrement à clé publique est très utilisé sur Internet, notamment pour sécuriser le commerce électronique en protégeant les numéros de carte bancaire. Lorsque vous envoyez un tel numéro à un destinataire, vous le chiffrez en utilisant la clé publique que votre interlocuteur vous transmet. Cette clé sert à chiffrer, mais pas à déchiffrer le numéro : seul le destinataire peut retrouver le numéro initial en utilisant une clé privée, qui a servi à définir la clé publique. Il est théoriquement possible de retrouver la clé privée à partir de la clé publique, mais difficile en pratique... sauf avec les algorithmes qu'un ordinateur quantique pourra utiliser.

La signature numérique sert surtout à authentifier des logiciels téléchargés (sur téléphone mobile ou sur ordinateur), les clés de chiffrement et les sites internet.

Comment anticiper le jour où le chiffrement à clé publique et la signature numérique ne seront plus sûrs ? Un texte chiffré pourrait être stocké aujourd'hui pour être décrypté demain par un ordinateur quantique. La cryptographie quantique *(voir l'article d'Artur Ekert et Renato Renner, pages 26 à 35)* ne répond que très partiellement à cette question, car elle ne fournit ni signature, ni chiffrement à clé publique, mais offre seulement un certain type d'échange de clés, ce qui est insuffisant pour beaucoup d'applications courantes. Pour résister à l'attaque d'un ordinateur quantique, il existe actuellement quatre approches, qualifiées de postquantiques : la cryptographie à base de hachage, la cryptographie multivariable, celle à base de codes correcteurs et celle à base de réseaux.

Les fonctions de hachage sont répandues en cryptographie ; elles servent par exemple à protéger les mots de passe. Ces fonctions associent à tout message une petite chaîne de caractères : l'empreinte. En cryptographie, les fonctions de hachage utilisées doivent être à sens unique, c'est-à-dire qu'il doit être impossible de retrouver un message à partir de son empreinte.

Les fonctions de hachage ne permettent pas à elles seules de fournir un chiffrement à clé publique. En revanche, il a été montré qu'elles sont suffisantes pour construire des signatures numériques sûres (même si ces dernières ont l'inconvénient d'être volumineuses). En 1979, l'informaticien américain Leslie Lamport a en effet proposé une méthode pour signer un message grâce au hachage. On choisit d'abord des nombres aléatoires qui forment la clé privée du signataire : les empreintes de chacun des nombres de la clé privée par la fonction de hachage constituent la clé publique. La

signature est un sous-ensemble de la clé privée dépendant du message. Pour vérifier la signature, on hache chacun de ses éléments et on vérifie qu'on obtient le bon sous-ensemble de la clé publique.

La signature de Lamport est simple à mettre en œuvre, mais elle ne peut être utilisée qu'une fois, pour des raisons de sécurité, car elle révèle une partie de la clé privée. Pour signer plusieurs messages, l'Américain Ralph Merkle a inventé ce qu'on nomme aujourd'hui des arbres de hachage, dans lesquels on passe d'un niveau à un autre en appliquant la fonction de hachage. Les arbres de hachage sont couramment utilisés : on les trouve dans la monnaie virtuelle bitcoin et dans les réseaux pair à pair, pour vérifier l'intégrité d'une partie d'un fichier par exemple.

Une autre approche est la cryptographie multivariable, développée dès 1988 sous l'impulsion de deux chercheurs japonais, Tsutomu Matsumoto et Hideki Imai. Elle repose sur la difficulté à résoudre des systèmes d'équations polynomiales à plusieurs inconnues. Au lycée, on apprend à résoudre une équation du second degré à une seule variable. Ce problème devient très difficile lorsque le nombre de variables et le nombre d'équations sont élevés.

Dans le cas d'une signature multivariable, la clé publique est un système d'équations polynomiales ; le message définit le second membre de ce système d'équations, et la signature d'un message n'est autre qu'une solution du système avec second membre. Ainsi, on vérifie la validité d'une signature en vérifiant qu'elle est bien solution du système. La cryptographie multivariable s'applique au chiffrement à clé publique et aux signatures numériques de façon assez efficace.

Cependant, l'inconvénient de cette méthode est que les systèmes d'équations utilisés ont des structures cachées qui, découvertes, constituent des brèches : de nombreux systèmes multivariables ont ainsi été cassés, à commencer par le système de Matsumoto-Imai, contre lequel Jacques Patarin, de l'université Versailles-Saint-Quentin-en-Yvelines, développa une attaque astucieuse en 1995. Un autre cas d'école est la signature numérique Sflash, conçue en 2001 par des chercheurs de la société Schlumberger, et recommandée par le projet européen NESSIE en 2003. Elle a été cassée en 2007 par les cryptographes Vivien Dubois, Pierre-Alain Fouque, Adi Shamir et Jacques Stern.

Enfin, la cryptographie à base de codes correcteurs et celle à base de réseaux reposent sur des problèmes assez voisins : filtrer du bruit. On cache un élément dans un code correcteur d'erreurs (des objets mathématiques très structurés) ou bien dans un réseau euclidien (un arrangement régulier de points dans l'espace à n dimensions) en lui ajoutant du bruit. Il est alors difficile de retrouver l'élément, c'est-à-dire d'enlever le bruit. Dans l'exemple des réseaux, l'élément est un point du réseau, et on le bruite en le déplaçant légèrement : quand la dimension augmente et que le réseau n'est pas trop particulier, il est très difficile de retrouver la perturbation. Cela permet de construire assez naturellement un chiffrement à clé publique : c'est ce qu'a fait Robert McEliece dès la fin des années 1970 pour les codes correcteurs. Fondé sur la même idée, le chiffrement à base de réseaux NTRU est peut-être le chiffrement à clé publique le plus rapide du monde.

L'Institut américain des normes et de la technologie a lancé un appel international pour normaliser ces algorithmes postquantiques

Malgré leurs similitudes, les codes correcteurs et les réseaux euclidiens ont des différences significatives. Par exemple, on connaît des signatures à base de réseaux très efficaces, contrairement au cas des codes correcteurs. Et les réseaux euclidiens offrent des fonctionnalités que n'a pas la cryptographie traditionnelle : on peut citer le cas du chiffrement complètement homomorphe, qui permet d'effectuer des opérations arbitraires sur des données chiffrées sans que l'on connaisse la clé secrète. Pour toutes ces raisons, la cryptographie à base de réseaux est la méthode postquantique la plus étudiée à l'heure actuelle.

Ces quatre approches postquantiques ont des avantages et des défauts. En février 2016, le NIST (l'Institut américain des normes et de la technologie) a lancé un appel international pour normaliser ces méthodes postquantiques. Cette initiative permettra peut-être de déterminer l'approche la plus adaptée pour remplacer les systèmes de cryptographie à clé publique utilisés aujourd'hui, tel RSA. ■

L'AUTEUR

Phong NGUYEN est directeur de recherche à l'Inria et dirige le laboratoire franco-japonais d'informatique du CNRS.

BIBLIOGRAPHIE

National Institute of Standards and Technology, **Report on Post-Quantum Cryptography**, Internal Report 8105, 2016.

P. Q. Nguyen et B. Vallée (éd.), **The LLL Algorithm, Survey and Applications**, Springer, 2010.

D. J. Bernstein *et al.* (éd.), **Post-Quantum Cryptography**, Springer, 2009.

P. Nguyen, **La géométrie des nombres : de Gauss aux codes secrets**, *Dossier Pour la Science*, n° 36, juillet-octobre 2002.