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.