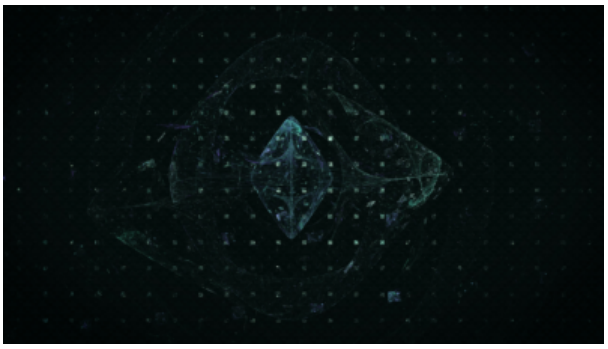
Un professeur de mathématiques de l'Université Brown récompensé pour ses travaux en cryptographie post-quantique



Le *National Institute of Standards and Technologies* (NIST) a publié sa première sélection de quatre algorithmes de cryptographie qui serviront de normes pour les nouveaux systèmes de cryptage plus robustes et plus résistants aux cyberattaques d'un ordinateur quantique. Ces systèmes de cryptage dits à clé publique sont largement utilisés pour assurer la sécurité des communications des systèmes numériques comme les services bancaires en ligne, l'accès aux données privées et les logiciels de messagerie.

Les idées développées dans les travaux menés par une équipe de mathématiciens de l'Université de Brown du Rhode-Island, les professeurs Jeffrey Hoffstein, Joseph Silverman et Jill Pipher, autour des réseaux euclidiens, dès avant les années 2000 ont joué un rôle central dans la mise au point de 3 des 4 algorithmes retenus. Le cadre original de NTRU (abréviation signifiant « Number Theorists R Us ») était motivé par l'idée de trouver une méthode de cryptographie à clé publique qui soit plusieurs fois plus rapide que la méthode RSA (3) et qui puisse fonctionner sur des appareils de faible puissance. Le Professeur Jeffrey Hoffstein est très heureux de voir ses travaux ainsi reconnus : « il est très important pour l'IOT (internet des objets) d'avoir un schéma de signature numérique sécurisé pour l'ère quantique, très rapide et nécessitant une petite puissance de traitement pouvant fonctionner, par exemple, sur un téléphone portable ou sur une carte à puces » (4).

Les algorithmes développés jusqu'à présent reposent sur des problèmes mathématiques si complexes que même les ordinateurs classiques les plus rapides ne peuvent les résoudre. Or les avancées liées au calcul quantique vont vite remettre en question les systèmes de cryptage actuels et en rendre certains obsolètes. Avec ce qui sera un jour un ordinateur quantique, le temps nécessaire pour résoudre le problème et trouver les clefs de chiffrement va se réduire drastiquement. C'est la raison pour laquelle le NIST a demandé en 2016 aux cryptographes du monde entier de concevoir puis de passer au crible des méthodes de cryptage capables de résister à une attaque d'un futur ordinateur quantique plus puissant que les machines disponibles aujourd'hui.

La sélection de cette année 2022 constitue une étape importante dans le projet de normalisation de la cryptographie post-quantique du NIST (1). A ce stade, les algorithmes à clés symétriques sont considérés comme résistant au quantique. Aussi le NIST s'est concentré sur deux tâches principales : la signature numérique, utilisée pour l'authentification des identités, et l'échange de clefs (dit aussi cryptage général) utilisé pour protéger les informations échangées sur un réseau public.

Pour l'« échange de clés » , le NIST a finalement préféré l'algorithme CRYSTALS-Kyber, lui aussi basé sur des manipulations de réseaux euclidiens, mais qui repose sur des travaux ultérieurs menés au CNRS et à l'Université de Limoges, à l'algorithme original NRTU. Parmi ses avantages figurent des clés de chiffrement relativement petites que deux parties peuvent échanger facilement, ainsi que sa rapidité d'exécution. Les autres algorithmes encore à l'étude pour le cryptage général reposent sur des techniques radicalement différentes.

Mais l'équipe de mathématiciens de l'Université de Brown a participé à la sélection du NIST aussi sur le volet « signature numérique » en proposant l'algorithme FALCON (Fast Fourier lattice-based compact signatures over NTRU), que M. Jeffrey Hoffstein a conçu en collaboration avec neuf autres cryptographes issus d'un consortium (2) comprenant notamment l'université Brown, l'Université de Rennes, Qualcomm, IBM, Thalès, OnBoard Security et NCC group (entreprise de cyber sécurité).

Les trois algorithmes CRYSTALS-Dilithium, FALCON et SPHINCS+ sélectionnés par

les examinateurs du NIST pour le volet « signature numérique » sont d'une grande efficacité notamment pour les deux premiers basés sur des problèmes mathématiques faisant appel à des réseaux euclidiens. SPHINCS+ utilise lui des fonctions de hachage dans son approche mathématique.

La société française CryptoNext Security a participé à la sélection du NIST et figure aussi en bonne place dans cette compétition notamment suite au dépôt de l'algorithme GeMSS pour les signatures numériques courtes qui reste à l'étude. L'entreprise a proposé un système cryptographique multi variable qui consiste à utiliser un système d'équations faisant intervenir le produit de plusieurs variables. La société se positionne par ailleurs sur le marché de la cryptographie post-quantique en proposant une plateforme de cryptage post-quantique capable d'implémenter chacun des algorithmes retenus comme finalistes par le NIST – y compris par exemple Frodo recommandé de son côté par l'ANSSI. L'équipe de CryptoNext a par ailleurs mis en place une expérimentation en collaboration avec le MEAE pour la transmission cryptée de messages diplomatiques (voir article sur le quantique).

A terme le NIST disposera d'une solide base d'outils de référence pour contrer les menaces qui se présenteront avec la puissance d'un ordinateur quantique.

Rédacteurs :

Jean-Philippe Nicolaï, Attaché pour la science et la technologie au Consulat Général de France à Boston

Xavier Bressaud, Attaché pour la science et la technologie, Ambassade de France a Washington, DC

Références:

1. NIST Announces First Four Quantum-Resistant Cryptographic Algorithms
2. Falcon et Falcon, NIST Post-Quantum Cryptography Project
3. La méthode RSA est un système cryptographique pour le chiffrement à clé publique souvent utilisé pour la sécurisation des données confidentielles. RSA, décrit pour la première fois en 1977, désigne les initiales des trois inventeurs: Ron **R**ivest, Adi **S**hamir et Leonard **A**dleman du MIT

(Massachusetts Institute of Technology). Le chiffrement à clé publique, également appelé chiffrement asymétrique, utilise deux clés différentes, mais mathématiquement liées, une publique et l'autre privée. La clé publique peut être partagée avec quiconque, tandis que la clé privée doit rester secrète

4. Entretien avec Professeur Jeffrey Hoffstein du 17 novembre 2022