Par e-mail : https://www.lemonde.fr/sciences/article/2022/07/07/securite-informatique-la-cryptographie-post-quantique-prete-a-entrer-en-lice_6133795_1650684.html

# Sécurité informatique : la cryptographie post-quantique prête à entrer en lice

L'agence américaine chargée de la standardisation a sélectionné les meilleurs algorithmes capables de résister aux attaques d'ordinateurs quantiques. Des équipes françaises figurent parmi les lauréats.

Par David Larousserie

Publié le 07 07 2022

Ça y est, nos communications et transactions électroniques futures sont sécurisées. Le 5 juillet, l'agence gouvernementale américaine chargée de la standardisation, le NIST, après six ans d'évaluation, a sélectionné les meilleurs dispositifs de chiffrement et de signature capables de résister à un péril qui plane sur tous nos échanges (e-mails, cartes bancaires, Web, mobiles…). Bref, tout ce qui garantit la confiance dans le monde numérique.

Ce danger, c'est l'ordinateur quantique, une machine qui n'existe pas encore dans sa forme la plus aboutie, mais qui serait capable de casser en peu de temps les techniques actuelles de sécurisation des échanges. Celle-ci repose sur l'idée qu'il est facile de fermer un cadenas mais pas de l'ouvrir, ce qui en l'espèce traduit le fait que certaines opérations mathématiques sont faciles à réaliser dans un sens mais pas dans l'autre. On peut ainsi aisément multiplier deux grands nombres premiers entre eux, mais à l'inverse, si l'on dispose de leur produit, il est très difficile de les retrouver. Sauf pour un ordinateur quantique, qui calcule différemment et dont il a été prouvé qu'il pourrait, en théorie, faire tourner des algorithmes inversant ces opérations facilement et donc révéler les précieux secrets.

## Les chercheurs français en vedette

D'où l'appel à l'aide lancé par le NIST en février 2016 auprès des meilleurs chercheurs mondiaux : trouver des opérations mathématiques qui résistent à l'ordinateur quantique et les utiliser pour en faire des protocoles de chiffrement (pour brouiller un message) et de signature (pour authentifier une personne ou un document).

En décembre 2017, 69 propositions sont retenues. Puis 26, en janvier 2019, et 7, en juillet 2020 (avec 8 autres solutions de secours), après que les équipes se furent « attaquées » entre elles pour débusquer des failles. Deux ans plus tard, et avec six mois de retard sur le calendrier prévu, il n'en reste donc plus que quatre : une pour le chiffrement, Crystals-Kyber, et trois pour la signature, Crystals-Dilithium, Falcon et Sphincs +. Trois sur quatre comptent des chercheurs français parmi la dizaine de membres qui les ont conçues. Quatre autres propositions, pour le chiffrement, ont droit à un tour de repêchage.

*« Nous sommes contents et soulagés, car cela a été long et stressant. Cela nous apporte une grande visibilité internationale »*, fait savoir Léo Ducas, chercheur au centre de recherche CWI à Amsterdam et professeur à l'université de Leiden, présent dans les équipes de deux de ces solutions, Crystals-Kyber et Crystals-Dilithium. « *C'est une reconnaissance forte de notre travail*, estime

Damien Stehlé, professeur à l'ENS de Lyon, membre lui aussi de ces deux équipes. *Le fait que plusieurs coauteurs des algorithmes retenus soient passés par des labos en France montre que nous avons des forces académiques. Mais aussi que nous n'arrivons pas toujours à les garder, plusieurs ayant quitté les laboratoires nationaux. »*

Outre l'ENS de Lyon, l'université de Rennes compte des lauréats parmi l'équipe Falcon. Mais d'autres Français ou chercheurs ayant travaillé en France se trouvent désormais aux Pays-Bas, au Canada, en Angleterre, aux Etats-Unis ou en Suisse… *« Cette annonce est gratifiante. Elle montre que la cryptographie n'est pas que de la théorie et que notre travail va servir à des milliards de personnes »*, apprécie Pierre-Alain Fouque. Professeur à l'université de Rennes, membre de Falcon, il est à la tête d'un projet national, PQTLS, doté de huit millions d'euros sur la cryptographie post-quantique. « *Cette compétition a stimulé la recherche et c'est comme cela que la sécurité progresse »*, assure-t-il.

> « Comme on dit dans le milieu, un cryptographe ne dort jamais sur ses deux oreilles » – Léo Ducas, chercheur présent dans les équipes de deux des solutions retenues

Excepté Sphincs +, ces *« cadenas »* du futur reposent sur le même objet mathématique. Pour le comprendre, il faut imaginer un réseau périodique de points à deux dimensions, obtenu par la répétition d'une grande maille (faite de deux grands vecteurs). Une opération difficile est de trouver le plus petit lien reliant deux points de ce réseau. En réalité, c'est simple à deux dimensions, mais extrêmement difficile lorsqu'il y a plus d'une centaine de dimensions, comme, en pratique, pour les algorithmes choisis…

Hasard du calendrier, le même jour que l'annonce du NIST, une des médailles Fields remises par l'Union internationale des mathématiciens récompensait l'Ukrainienne Maryna Viazovska pour des travaux concernant ces énormes réseaux de points, dont elle étudie la compacité.

*« Comme on dit dans le milieu, un cryptographe ne dort jamais sur ses deux oreilles. Donc la découverte soudaine d'une nouvelle approche révolutionnaire et dévastatrice contre tel ou tel protocole ne peut pas malheureusement être formellement exclue »*, rappelle Léo Ducas. *« Pour démontrer la solidité de ces algorithmes,* explique Damien Stehlé, *nous avons apporté des preuves qu'ils sont effectivement difficiles à résoudre, y compris par des attaques quantiques. Pour le cas des réseaux, il arrive parfois que des chercheurs prétendent dans des prépublications qu'ils ont trouvé des algorithmes quantiques efficaces. Mais, jusqu'à présent, ils contiennent tous de grosses erreurs et les affirmations ne tiennent pas. »*

Mais, ces derniers mois, ce n'est pas l'ordinateur quantique qui a fait peur à ces informaticiens. Ce sont plutôt de complexes histoires de brevets. Durant le dernier tour de sélection, le CNRS et l'université de Limoges ont fait valoir que des brevets pourraient concerner certains algorithmes finalistes. Or, le NIST considérait à juste titre que cela pouvait être de nature à ralentir le déploiement de ces solutions, comme cela avait été constaté par le passé. Il pouvait donc être tenté d'opter pour une solution, NTRU, non concernée par ces brevets, car elle a déjà été mise dans le domaine public par ses auteurs.

Finalement, en même temps que les résultats, le NIST a annoncé avoir signé un accord de licence, confidentiel, avec l'université de Limoges et le CNRS, ainsi qu'avec deux autres acteurs, l'entreprise Isara et le chercheur américain Jintai Ding. Le département d'Etat américain a même salué l'événement d'un tweet, tout comme le CNRS par un communiqué, qui, en revanche, ne

relève pas que les auteurs du brevet sont retenus pour un quatrième tour et que deux solutions lauréates sont issues de laboratoires associés à l'organisme.

L'accord permettra aux utilisateurs, essentiellement les fabricants de puces ou les grands acteurs de l'informatique, de ne pas payer de licences ou de coûteuses procédures judiciaires en contestation de brevets. *« Je reste persuadé que, scientifiquement, ces brevets ne s'appliquent pas à notre algorithme de chiffrement »*, note Damien Stehlé. Néanmoins, cette histoire de brevets n'est pas complètement réglée, car, dans son rapport justifiant ses choix, le NIST prévient que si l'accord de licence n'est pas finalisé, il est prêt à choisir NTRU plutôt que Crystals-Kyber.

Deux ans seront encore nécessaires au NIST pour travailler à la standardisation, la procédure permettant d'utiliser ces algorithmes avec des règles garantissant la sécurité. Puis le déploiement à grande échelle pourra avoir lieu, y compris en cohabitation avec les systèmes préquantiques actuels, les nouvelles techniques présentant des caractéristiques d'usage comparables. Ordinateur quantique ou pas, l'ère post-quantique vient de démarrer.

David Larousserie