Cybersécurité : comment la crypto se prépare au post-quantique

E n 2040, il n'y aura sans doute pas un ordinateur quantique dans chaque bureau ou entreprise, mais il y a fort à parier que les services de renseignements et peut-être même certaines organisations criminelles utilisent une telle machine pour casser les codes de chiffrement.

La menace est identifiée depuis 1995. C'est un article publié par le mathématicien américain Peter Shor qui expliquait le danger que font courir les ordinateurs quantiques à l'ensemble de la sécurité de l'économie. Portés par un calculateur quantique, les algorithmes de Shor et de Grover peuvent, en effet, casser de nombreux algorithmes à clé publique très couramment utilisés aujourd'hui.

À la trappe, RSA, courbes elliptiques… même l'algorithme de chiffrement symétrique AES ne pourra résister qu'au prix d'un allongement significatif de la taille de ses clés.

« Les algorithmes à clé symétrique et de hachage ne seront impactés qu'à la marge, mais les algorithmes de chiffrement à clé publique sont sous la menace, à long terme, des ordinateurs quantiques, » explique David Renty, cybersecurity manager chez Wavestone. « Ces algorithmes sont très utilisés dans notre quotidien, puisque ce sont eux qui chiffrent nos communications Internet, l'accès aux sites de banques en ligne, aux sites d'e-commerce, la signature des actes notariés ou, encore, la blockchain. Si jamais cette cryptographie devient caduque, cela va poser de très gros problèmes. »

Une communauté de chercheur PQC s'est constituée

Depuis 25 ans, on sait que la sécurité numérique sera remise en cause par le calcul quantique.
Face à cette menace qui semble inéluctable, de nombreux chercheurs se sont lancés dans le développement d'algorithmes capables de résister à cette nouvelle approche de l'informatique.

Ce sont des algorithmes post-quantiques ou « Quantum Safe ». Car, à part inventer des algorithmes de chiffrement que l'on considère comme mathématiquement sûrs contre une tentative de déchiffrement par un calculateur quantique, l'industrie doit harmoniser les algorithmes finalement choisis pour sécuriser une transaction bancaire, un paiement sur Internet ou l'envoi d'un fichier sensible.

Dès la fin des années 2000, le comité de standardisation IEEE lançait des travaux sur la question, imité en cela par l'ANSI ou, encore, le National Institute of Standards and Technology (NIST) américain. Ce dernier était déjà à l'origine de la standardisation de l'incontournable AES et de SHA-3, fonction de hachage cryptographique conçue par Guido Bertoni, Joan Daemen, Michaël Peeters et Gilles Van Assche.

Mathématiquement, déjouer les capacités d'un calculateur quantique n'est pas hors de portée des chercheurs, mais encore faut-il choisir un algorithme qui ne présente pas de faiblesses mathématiques, qui n'est pas trop gourmand en puissance machine et n'alourdisse pas excessivement les échanges de données.

La compétition lancée par le NIST a mobilisé 87 équipes internationales de chercheurs.
La première phase d'évaluation a vu 69 algorithmes acceptés, un nombre abaissé en 2019, après une deuxième phase de test et enfin la liste des candidats pour la phase 3 a été arrêtée en juillet 2020. Quatre algorithmes sont encore en lice pour le chiffrement à clé publique, trois pour la signature électronique…

L'objectif du NIST est d'aboutir à des algorithmes standardisés en 2022 pour que les industriels puissent les implémenter et que ces algorithmes soient mis en production d'ici à 2024.

David Renty précise : « On estime que les ordinateurs quantiques pourraient arriver à l'horizon 2035-2040, mais c'est une problématique à laquelle il faut penser dès aujourd'hui. On peut imaginer que des gouvernements stockent des données chiffrées impossibles à casser, mais qui le seront dans 20 ans. C'est un point très important à intégrer par les États et les industriels de l'armement, notamment. C'est la raison pour laquelle, si beaucoup reste à faire en cybersécurité pour traiter des problématiques de patching ou d'hygiène informatique des utilisateurs, les entreprises doivent désormais intégrer cette dimension quantique au niveau de leurs cellules de veille. »

Un partage de clés par intrication quantique

Outre ces recherches pour mettre en œuvre des algorithmes post-quantiques sur des infrastructures IT classiques, une autre option est en train de se dessiner à beaucoup plus long terme : l'utilisation des technologies quantiques pour sécuriser les échanges de données.
L'idée est d'utiliser un réseau quantique, un « quantum information network (QIN) » pour transmettre les clés de chiffrement au moyen du phénomène d'intrication quantique de deux particules.

De nombreux centres de recherche ont expérimenté cette technique révolutionnaire via des réseaux de fibres optiques, échangeant des clés de chiffrement au moyen de photons intriqués. Mais l'exemple le plus spectaculaire de cette approche fut la visioconférence encryptée de façon quantique établie, en 2017, entre Bai Chunli, président de l'Académie des sciences chinoise, et son homologue autrichien Anton Zeilinger.

Exploitant le phénomène d'intrication quantique, le satellite a distribué les photons intriqués entre les deux centres – l'un en Chine, l'autre en Autriche – à 7 600 km de distance pour partager une clé de chiffrement sans que celle-ci ne puisse être interceptée par un tiers.

Une approche révolutionnaire qui pourrait bien bousculer à nouveau le monde de la cryptographie au-delà de 2040 !

par **Alain Clapaud**