Le chiffrement testé pour survivre à l'informatique quantique

L'ordinateur quantique permettra de résoudre en quelques secondes des calculs complexes qui prendraient des milliers d'années, voire des millions, pour des systèmes classiques. Mais la médaille a son revers, puisque les ordinateurs quantiques pourront aussi **briser la protection par chiffrement asymétrique** qui sécurise les échanges sur Internet… Des scientifiques cherchent la parade.

Mettre à niveau le chiffrement

Des chercheurs de l'éditeur Microsoft, du fabricant de semi-conducteurs NXP et de l'université de technologie du Queensland (Australie) planchent sur une mise à niveau du protocole de sécurisation des échanges **TLS (Transport Layer Security)**. Ils testent une version du protocole capable de résister aux attaques d'un ordinateur quantique, rapporte la MIT Technology Review.

« Les ordinateurs quantiques sont en cours de développement, il est donc essentiel de se préparer. Cela peut prendre une décennie ou plus pour qu'un nouvel algorithme cryptographique – ou 'primitive' – soit correctement testé et largement déployé », a expliqué à la revue Krysta Svore, chercheuse à la tête du Quantum Architectures & Computation Group (QuArC) de Microsoft Research.

Aujourd'hui, lorsque qu'une banque, ou une messagerie, utilise le protocole TLS, elle s'appuie sur l'algorithme de cryptographie asymétrique RSA (en référence aux initiales de ses trois inventeurs). L'algorithme RSA utilise une paire de clés de chiffrement, l'une publique pour chiffrer, l'autre privée pour déchiffrer. Si l'on découvre quels nombres premiers ont été utilisés pour rendre la clé publique, on peut aussi recréer la clé privée et ainsi déchiffrer les données… Les ordinateurs conventionnels ne peuvent pas le faire rapidement, mais les ordinateurs quantiques pourraient le faire demain.

Sur les terres du qubit

La version du protocole TLS testée par les chercheurs génère des clés de chiffrement en utilisant une autre approche mathématique. Elle serait hors de portée des ordinateurs conventionnels et quantiques. Le système a été testé pour crypter les données circulant entre deux ordinateurs, l'un jouant le rôle d'un navigateur et l'autre d'un serveur Web. Avec cette version expérimentale de TLS, les données auraient été transférées sans heurts d'un ordinateur à l'autre. En revanche, elles ont été transférées moins rapidement (**21% moins vite**) qu'avec la version du protocole utilisant la cryptographie à base de courbes elliptiques, et utilisée par des sites web aujourd'hui.

Des progrès restent à faire, mais le jeu en vaut la chandelle, selon les chercheurs. Ils veulent sensibiliser davantage de scientifiques et de développeurs sur la puissance de l'informatique quantique. Pour Krysta Svore, *« il y a un besoin urgent de trouver d'autres primitives cryptographiques. »*

A lire aussi :

Comprendre l’ordinateur quantique (infographie)
Inria : « Un ordinateur quantique dans dix ans ? Impossible de l’affirmer »

crédit photo © Pavel Ignatov / Shutterstock