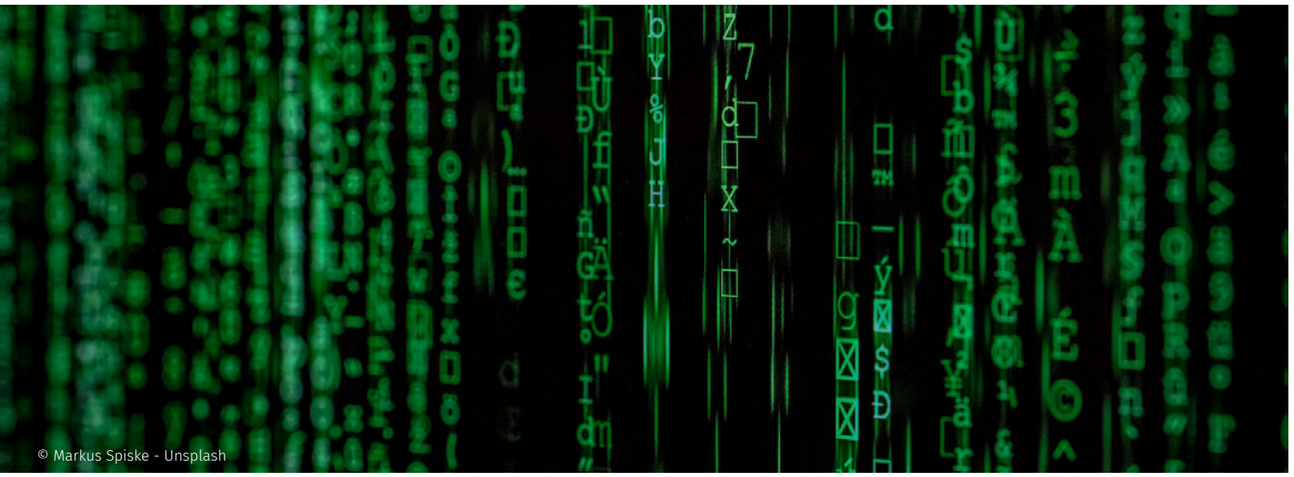
Cacher l'information à l'ère des ordinateurs quantiques



© Markus Spiske - Unsplash

Les futurs ordinateurs quantiques, plus rapides que les ordinateurs classiques, sauront déjouer les systèmes de brouillage de données actuels. Les mathématiciens élaborent déjà des systèmes post-quantiques aptes à leur résister. Pour s'assurer de leur fiabilité, ils essaient de concevoir toutes les attaques imaginables.

Cet été, un protocole de cryptographie de nouvelle génération, dénommé SIKE, a été « cassé ». Damien Robert, chercheur au sein du centre Inria de l'université de Bordeaux (Institut national de recherche en sciences et technologies du numérique) a ainsi démontré que les messages rendus secrets par ce système peuvent être déchiffrés rapidement.

Au quotidien, des informations sensibles sont transmises entre plusieurs appareils : paiements bancaires, connexions à des sites internet… La cryptographie permet de les rendre illisibles à celles et ceux qui les intercepteraient, sauf pour le destinataire.

Pour recevoir un message, il met à disposition de tous une clé publique qui est une suite de nombres. Ensuite, l'expéditeur chiffre le message grâce à un algorithme utilisant cette clé. Pour retrouver le message initial, le destinataire utilise alors sa clé privée, inconnue de tous et qui a servi à calculer la clé publique. Le lien mathématique entre les deux clés permet au destinataire, et à lui seul, de déchiffrer très rapidement le message.

Des systèmes théoriquement cassables

Problème : la clé privée peut être théoriquement obtenue à partir de la clé publique. Mais Damien Robert rassure : « Il faudrait que tous les ordinateurs du monde calculent pendant toute la durée de l'univers pour y parvenir », même en utilisant l'algorithme le plus efficace connu. Néanmoins, « il est peut-être possible de construire des algorithmes encore plus performants », nuance-t-il.

Si cette question reste sans réponse pour les ordinateurs classiques, il existe bien un meilleur algorithme utilisant les ordinateurs quantiques pour casser les protocoles de chiffrement actuels. Ces machines réduiraient drastiquement le temps nécessaire pour résoudre certains problèmes, mais elles sont encore théoriques et il n'existe pas de prototype réel complet. Cependant des algorithmes qu'elles pourraient exécuter ont déjà été imaginés. « Ça reste donc une menace pour celles et ceux qui ont besoin de garder des informations secrètes à très long terme », prévient le chercheur.

Contrer la menace quantique

De nouveaux systèmes de chiffrement doivent donc être trouvés, où la meilleure attaque connue, même en quantique, doit rester démesurément lente. C'est la cryptographie post-quantique. Les scientifiques cherchent à exploiter de nouveaux principes mathématiques. Par exemple, les « réseaux et les graphes » sont au cœur de trois systèmes de chiffrement retenus par les États-Unis pour renforcer les systèmes de communication. « Il y a un prix à payer pour avoir cette résistance quantique », prévient Damien Robert. « Les protocoles chiffrent plus lentement ou utilisent des clés qui prennent plus de place en mémoire. »

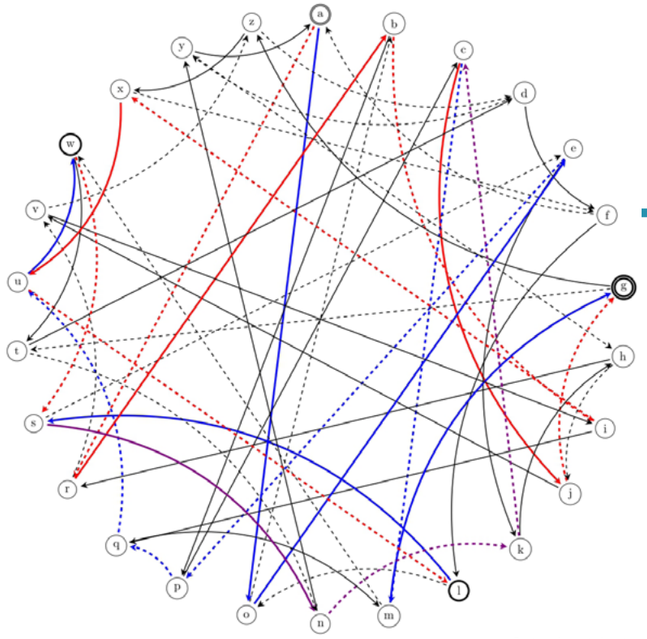
Après la conception, vient le test de résistance. Comme personne ne sait prouver qu'un système est totalement inviolable, les scientifiques s'efforcent de construire les attaques les plus sophistiquées possibles pour les tester. « Pour les systèmes de réseaux et de graphes, en dix ans, personne n'a réussi à les casser. »

Des failles découvertes plus tard par hasard

Parfois, certains systèmes cryptographiques sont bel et bien « cassés ». Lorsqu'une vulnérabilité de conception est repérée, les scientifiques l'utilisent pour inventer une méthode de déchiffrement des messages. Pour SIKE, cela a pris dix ans. Damien Robert raconte : « Castryck et Decru ont trouvé la faille un peu au hasard. […] Mais c'est leur expertise qui leur a permis de l'exploiter. » L'attaque qu'ils ont alors inventée ne s'appliquait qu'à des cas particuliers. Damien Robert l'a ensuite étendue au cas général : « J'ai utilisé des théorèmes dont j'ai eu besoin pour d'autres problèmes que j'ai pu adapter pour mon attaque. » Si la découverte de failles dépend souvent du hasard, leur exploitation exige une expertise que les scientifiques se forgent grâce à des années de recherche.

Si les attaques des scientifiques ne donnent rien après des années, les systèmes de cryptographie sont considérés comme fiables et peuvent être implémentés en machine. Une étape tout aussi cruciale.

Maxime Traineau



© Damien Robert

Graphe simplifié utilisé par les protocoles d'échange de clés comme SIKE