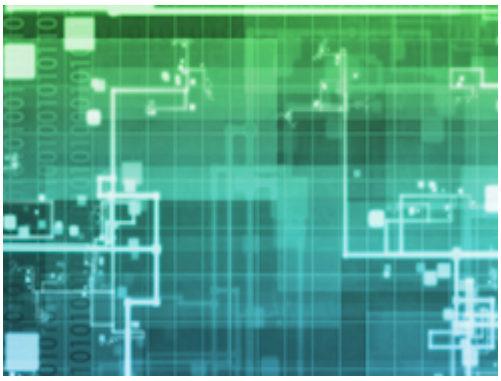
Sécuriser les données de chiffrement pour contrer la menace des futurs ordinateurs quantiques

Lorsque les ordinateurs quantiques seront disponibles, un algorithme existant pourra s'attaquer à des techniques de chiffrement actuellement considérées comme sûres. Les travaux réalisés par un projet financé par l'UE pose les bases d'une solution.



© kentoh, Shutterstock

Dans un article récemment paru dans la revue 'Nature', des chercheurs décrivent plusieurs approches pour développer de nouvelles techniques de chiffrement capables de résister aux attaques quantiques. Une approche évidente consiste à développer de nouvelles méthodes ne faisant pas appel aux techniques actuelles, car ces dernières risquent d'être affaiblies à l'avenir.

Le problème des techniques de chiffrement actuelles

Actuellement, notre sécurité en ligne dépend en grande partie du système RSA (Rivest-Shamir-Adleman) qui est largement utilisé pour les opérations de chiffrement. Il repose sur l'utilisation de clés publiques résultant du produit de deux nombres premiers. Actuellement, les ordinateurs les plus puissants mettraient un temps considérable pour identifier ces deux nombres premiers, par un procédé appelé factorisation: les superordinateurs les plus performants mettraient des siècles à résoudre ce casse-tête.

À l'autre extrémité du système de chiffrement se trouve le destinataire du message, qui détient une clé privée se présentant sous la forme d'un nombre qui n'est connu que de lui-même et de l'expéditeur. Une opération mathématique permet d'obtenir à

partir de la clé privé les deux nombres premiers nécessaires au décodage du message. Cette méthode de chiffrement est sûre, aussi longtemps que la clé privée n'est pas interceptée.

Mais avec l'arrivée prochaine d'ordinateurs quantiques plus puissants, on disposera de la puissance de calcul nécessaire pour casser ce chiffrement, ce qui affaiblira considérablement un procédé jusqu'à présent hautement sécurisé. Cette faiblesse est connue depuis 1994, lorsque fut publié un algorithme destiné aux ordinateurs quantiques et capable de diviser, en quelques secondes ou en quelques minutes, une clé publique de grande taille en deux nombres premiers.

Des chercheurs identifient les premières étapes d'une solution

L'équipe de PQCRYPTO (Post-Quantum CRYPTOgraphyfor long-term security) a décrit une approche à deux volets: outre l'idée qu'une solution viable devrait être basée sur le développement de nouvelles techniques de chiffrement, une autre suggestion est de privilégier les techniques utilisant des opérations mathématiques que les ordinateurs ne traitent pas de façon efficace.

Les chercheurs mettent en avant plusieurs contraintes pour les techniques qui devront être mises au point. Celles-ci doivent inspirer la confiance et leur utilisation ne doit pas être trop coûteuse et trop exigeante pour les systèmes informatiques. Il faudrait également éviter l'usage de clés d'une longueur excessive. Les auteurs insistent sur un aspect important du développement des futurs systèmes de chiffrement post-quantiques: une prise en compte précoce de la normalisation car toutes les parties devront utiliser les mêmes systèmes de cryptographie.

Pour plus d'informations, veuillez consulter:
site web du projet PQCRYPTO

Pays

Pays-Bas

Projets connexes

PROJET

PQCRYPTO

Post-quantum cryptography for long-term security

7 Septembre 2023

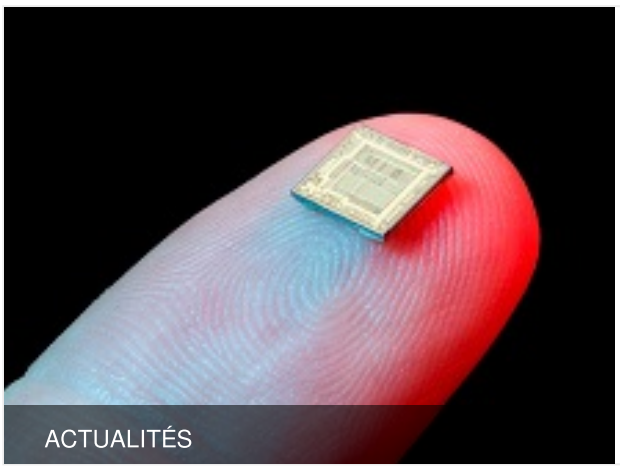
Articles connexes

ACTUALITÉS

PROGRÈS SCIENTIFIQUES

Peut-on prévenir les cyberattaques quantiques? Une initiative de l'UE répond par l'affirmative et nous montre comment

26 Mars 2020



ACTUALITÉS

PROGRÈS SCIENTIFIQUES

Un saut quantique pour les puces de silicium: Le couplage des spins de photons devient désormais une réalité

27 Février 2018

PROGRÈS SCIENTIFIQUES

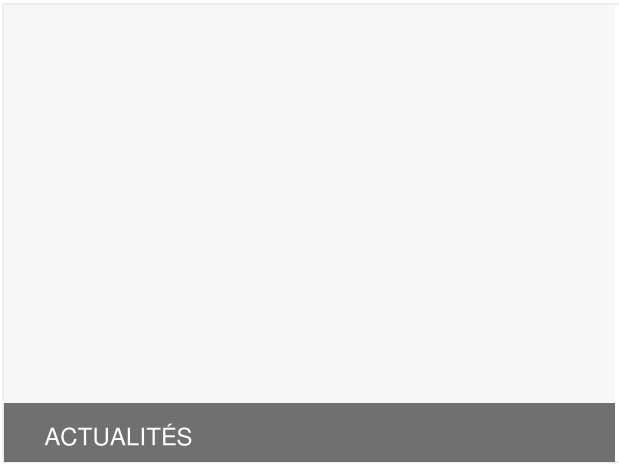
Les avantages des effets quantiques pour les réseaux biologique, social et technologique

9 Février 2018

PROGRÈS SCIENTIFIQUES

Un bond en avant quantique pour des mesures ultra-précises et le codage de l'information?

24 Novembre 2017



Dernière mise à jour: 11 Octobre 2017

Permalink: https://cordis.europa.eu/article/id/122627-securing-encryption-data-against-the-threat-of-future-quantum-computers/fr