Les ordinateurs quantiques, épée de Damoclès au-dessus de l'économie numérique

Nous sommes de plus en plus amenés à évoluer dans le monde Cyber, soit en tant qu'agent économique, soit en tant que citoyen mais maintenant également en tant que patient ou touriste. Si nous avons été rapidement conquis par les avantages que nous procure ce monde Cyber, nous avons tardé à percevoir les dangers que nous pouvons y rencontrer. Les événements récents nous y ont contraints brusquement. Les ransomwares tels Wannacry ou encore les fake news ont envahi l'actualité et nous ont ouvert les yeux.

Heureusement face aux risques de ces nouveaux usages, nous avons deux atouts importants. Nous avons à notre disposition deux grandes familles d'algorithmes cryptographiques qui nous apportent d'une part la garantie de l'identité et d'autre part la confidentialité des échanges. Les algorithmes de la première famille reposent sur des clés asymétriques. Dans un échange, chaque intervenant possède une clé privée et une clé publique qu'il fournit à ses interlocuteurs. La clé privée lui permet de signer ses messages et les destinataires peuvent s'assurer de son intégrité en vérifiant sa signature grâce à la clé publique. Le lien entre la clé publique et la clé privée permet également au destinataire de vérifier l'identité de l'émetteur. Ils peuvent également envoyer une réponse chiffrée avec la clé publique et seule la personne en possession de la clé privée correspondante peut la déchiffrer. Très souvent, ces clés sont des clés RSA, initiales du nom de leurs inventeurs (Ronald Rivest, Adi Shamir et Leonard Adleman).

Leur principe est connu depuis 1977. Il repose sur la difficulté de retrouver à partir du produit de deux grands nombres premiers chacun des nombres premiers qui le composent. Si le nombre de bits nécessaires pour représenter ce produit est inférieur à 256bits, la clé peut être cassée en quelques minutes sur un PC quelconque. La longueur recommandée aujourd'hui est de 2048 bits, ce qui met la factorisation hors de portée des ordinateurs actuels pour de très nombreuses années. C'est grâce à ces clés que la grande majorité des transactions numériques sont sécurisées, des cartes de crédit aux cartes de santé, fondement de la transformation digitale de notre société.

Or l'apparition des ordinateurs quantiques bouscule tout cela ; en effet, le mathématicien David Shor a montré en 1994 qu'ils pouvaient en théorie être utilisés pour factoriser rapidement de grands nombres, rendant inopérant non seulement les clés RSA, mais aussi celles utilisant les mécanismes de courbes elliptiques. L'année dernière, un article est paru dans la revue Nature (https://www.nature.com/articles/s41598-018-36058-z) a annoncé la factorisation des nombres 15, 143, 59989, et 376289 en utilisant 4, 12, 59, et 94 qubits logiques. Le qubit est l'unité élémentaire que manipulent ces ordinateurs ; contrairement aux bits des ordinateurs classiques, ils ne correspondent pas à un seul état possible mais à un ensemble d'états. Le nombre de qubits permet de mesurer la puissance des ordinateurs quantiques. Ces résultats ont été atteint grâce à un ordinateur D-WAWE 2000Q. Comme son nom l'indique, cet ordinateur est constitué de 2000 qubits, mais ces qubits sont d'un type particulier qui ne pouvait pas être utilisé pour le problème de factorisation. Les ordinateurs quantiques utilisables pour y exécuter l'algorithme de Shor sont à ce jour beaucoup moins puissants, avec moins de 80 qubits, car ils sont plus complexes à construire. Il s'agit donc d'une étape significative. S'il reste encore beaucoup de chemin pour la factorisation de nombres de 2048 bits, puisque le plus grand des nombres premiers factorisés correspond à 18 bits, il existe maintenant une épée de Damoclès au-dessus de la sécurité des clés RSA.

Il est donc important de commencer dès maintenant à se préoccuper de trouver de nouveaux algorithmes qui vont permettent de résister à l'avènement de l'informatique quantique. C'est pour cela que l'organisme de normalisation américain a lancé dès la fin de l'année 2016, un concours pour désigner le successeur de l'algorithme RSA. Nous en sommes maintenant au 2éme tour et les candidats en lice sont connus (https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions). Beaucoup d'équipes françaises ont répondu à l'appel. La validation des propositions, et le choix d'une d'entre elles, va être un processus long dont l'aboutissement n'est pas prévu aujourd'hui avant 2024.

L'autre algorithme, que nous n'avons pas encore abordé, assure, lui, la confidentialité des échanges. Il s'agit de l'Advanced Encryption Standard (AES) issu également d'un concours du NIST débuté en 1997. Lui aussi est vulnérable, mais dans une moindre mesure, aux avancées du calcul quantique. L'algorithme de Grover permettrait de diviser par deux la sécurité liée à la longueur des clés. Aujourd'hui la longueur minimale d'une clé considérée sûre est de 128-bits, ce qui ne sera plus le cas en utilisant l'algorithme de Grover. Cependant la longueur standard utilisée de nos jours est de 256-bits et serait donc suffisante.

Afin de garantir une transition dans les meilleures conditions, il est important de se préparer à ces changements dès que possible. Il est très difficile de prévoir quand les premiers ordinateurs quantiques assez puissants seront construits ou même s'ils existeront un jour, mais lorsqu'éventuellement ils seront là, il sera trop tard pour agir.