Un ordinateur quantique casseur de clé de chiffrement

Les jours des systèmes de chiffrement basés sur la factorisation des grands nombres, type RSA, sont-ils comptés ? Si la question ne se pose pas aujourd'hui avec les ordinateurs à architecture binaire classique, elle devient pertinente avec les évolutions de l'informatique quantique. Des équipes du MIT (Massachussetts Institute of Technology) et de l'Université autrichienne d'Innsbruck ont annoncé avoir mis au point un ordinateur quantique à 5 qubits (quantum bit) capable de s'attaquer aux systèmes de chiffrement traditionnels tels que ceux utilisés pour protéger les cartes bancaires, les documents secrets et autres données confidentielles.

[[Retrouver l'infographie : Comprendre l'ordinateur quantique]]

Rappelons que l'informatique quantique utilise les trois états du qubits, à savoir 0, 1 et « 0 et 1 en même temps » là l'informatique traditionnelle s'en contente de deux (0 ou 1). Une particularité qui décuple les capacités de calculs en parallèle et peut être utilisée pour dénombrer les facteurs premiers des grands nombres, ceux justement utilisés dans les opérations de chiffrement. Jusqu'à présent, le nombre 15 pouvait être, en informatique quantique, décomposé à partir de 12 qubits. Dans un article publié le 4 mars dans la revue *Science*, les scientifiques annoncent avoir mis au point un ordinateur quantique permettant de réduire ce nombre à 5 avec *« un niveau de confiance supérieur à 99% »*.

Un problème d'ingénieur plus que de physique fondamentale

Pour y parvenir, les chercheurs ont utilisé un laser capable de maintenir des atomes de calcium de manière stable afin d'appliquer l'algorithme quantique mis au point en 1994 par Peter Shor, professeurs de mathématiques appliquées au MIT, qui calcule les facteurs primaires des grands nombres. Si le système se limite à calculer les facteurs de 15, le plus petit nombre démontrant véritablement l'algorithme de Shor, l'innovation des scientifiques vise à montrer qu'il suffit désormais d'associer les lasers et atomes pour élargir les capacités de leur ordinateur quantique pour appliquer les calculs aux grands nombres utilisés dans les opérations de chiffrement.

« Nous montrons que l'algorithme de Shor, l'algorithme quantique le plus complexe connu à ce jour, est réalisable d'une manière où tout ce que vous avez à faire est d'aller dans le laboratoire, travailler plus sur la technologie, et vous devriez être en mesure de rendre un ordinateur quantique plus performant », assure Isaac Chuang, professeur au MIT et contributeur du projet, à *MIT News*. Avant d'ajouter que la fabrication d'un tel ordinateur n'est pas à la portée du premier venu, et coûte encore beaucoup d'argent. Mais l'idée est de constater que la limite de l'ordinateur quantique n'est plus une question de physique. *« Maintenant, cela nécessite plus un effort d'ingénierie, qu'une question de physique fondamentale »*, assure le scientifique. Si l'ordinateur quantique décodeur d'algorithme de chiffrement n'est pas tout à fait pour demain, les gouvernements et autres entreprises qui veulent garder leurs secrets ont intérêts à commencer à chercher d'autres solutions pour protéger leurs

données chiffrées.

Lire également
L’informatique quantique… sur du bon vieux silicium ?
Le chiffrement testé pour survivre à l’informatique quantique
Ordinateur quantique : IBM fait une percée sur les terres du qubit

crédit photo © Pavel Ignatov / Shutterstock