Physique quantique et informatique

L'informatique quantique met-elle en danger notre sécurité numérique ?

Robin Wilton • Juin 2020

Les ordinateurs que nous utilisons aujourd'hui reposent sur un système de valeurs binaires (**« bits »**) représentant une valeur de 0 ou 1. Les ordinateurs quantiques utilisent quant à eux un bit quantique (**« qubit »**), faisant appel à une propriété des particules subatomiques pour maintenir (ou **« superposer »**) différents états simultanément. Cela signifie qu'un qubit peut être à la fois un 0 et un 1 en même temps. Un ordinateur quantique peut donc calculer plusieurs valeurs au même moment, contrairement à un ordinateur classique. Cette capacité est susceptible de mettre à mal la manière dont nous utilisons le chiffrement pour sécuriser une grande partie de notre vie numérique, qu'il s'agisse de la protection de données confidentielles telles que les informations bancaires ou, plus simplement, de la confidentialité de nos communications en ligne.

Par exemple, lorsque vous essayez de résoudre des problèmes et que plusieurs réponses sont possibles, choisir la bonne nécessite, statistiquement parlant, de nombreux essais de la part d'un ordinateur classique. Un ordinateur quantique ayant, quant à lui, la capacité d'essayer toutes les solutions possibles à la fois, le temps nécessaire pour trouver la bonne réponse s'en verra considérablement diminué. Ce principe peut être mis en application pour cerner les deux formes dominantes de chiffrement utilisées de nos jours : **symétrique** et **asymétrique**.

Ordinateurs quantiques et chiffrement

Le chiffrement symétrique utilise une clé pour « verrouiller » les données, et une clé identique pour les « déverrouiller », de la même manière dont on se servirait d'une simple caisse. Une méthode pour briser le chiffrement symétrique, appelée « attaque exhaustive » ou « attaque par force brute », consiste à essayer toutes les clés de déchiffrement possibles jusqu'à trouver la bonne.

Les bons algorithmes de chiffrement symétrique sont conçus pour garantir, dans un premier temps, que sans la clé, la méthode la plus efficace de déchiffrer les données reste l'attaque exhaustive. Ils sont également conçus de telle sorte que le nombre de clés possibles est tellement immense qu'une attaque exhaustive n'entre pas dans les capacités d'un ordinateur classique. La quantité d'effort requis (le **« facteur travail »**) pour monter une attaque exhaustive peut être quantifiée, en fonction de la longueur de la clé et des ressources nécessaires, comme la puissance de calcul, la mémoire, l'énergie et l'argent. Des clés suffisamment longues entraînent un nombre de mauvaises réponses possibles tellement colossal que le facteur travail dépasse les limites pratiques de l'espace et du temps. Il serait tout à fait possible que l'énergie nécessaire pour alimenter les ordinateurs chargés d'effectuer ce travail ne parvienne jamais à être suffisante, ou même qu'il n'y ait pas assez de silicium pour fabriquer suffisamment de puces informatiques indispensables à la fabrication de ces ordinateurs.

Mais avec l'informatique quantique, de nombreuses clés possibles peuvent être essayées simultanément et, grâce à

CC BY-NC-SA 4.0

de nouvelles façons de trier les résultats[1], le temps nécessaire pour trouver la bonne clé s'avère considérablement réduit. Cette réduction est si importante que cela reviendrait à diminuer de moitié la longueur de la clé utilisée, ramenant ainsi la difficulté du problème à sa racine carrée. Un exemple simple : si, pour une longueur de clé déterminée, il existait 10 000 clés possibles à essayer, réduire de moitié la longueur de cette clé réduirait le facteur travail à devoir essayer seulement 100 clés possibles.

Le chiffrement asymétrique utilise une clé pour « verrouiller » les données et une clé différente pour les « déverrouiller », comme pour le verrouillage d'un cadenas. Tout le monde peut fermer un cadenas ouvert, mais seule la personne possédant la clé ou la combinaison peut le rouvrir. De nombreux protocoles de communication reposent sur un chiffrement asymétrique, notamment pour sécuriser un échange initial de clés symétriques entre partenaires communicants.

L'informatique quantique ne met pas le chiffrement en péril, ou du moins... pas encore.

Défis pratiques

Le nombre de qubits utilisés par un ordinateur quantique opérationnel a augmenté au fur et à mesure des avancées technologiques, passant d'une dizaine en 2010 à environ 80 en 2019. Le nombre de qubits nécessaires pour attaquer une clé symétrique de 128 bits reste encore malgré tout insuffisant, sans parler d'une clé asymétrique de 4 096 bits.

Le tableau suivant illustre le nombre de qubits nécessaires pour ce que l'on considère en général aujourd'hui comme une clé « raisonnablement forte »[3] pour chaque type d'algorithme cryptographique.

Type d'algorithme	Longueur d'une clé « raisonnablement forte »	Nombre de qubits requis par bit de clé	Nombre total de qubits requis
Symétrique (p. ex. AES)	128 bits	1	128
Elliptic Curve (basé sur les courbes elliptiques)	256	~9	2304
RSA	3072	2 (et 2 en plus)	6146

Figure 1: nombre de qubits utilisables nécessaires pour différents types d'algorithmes

Le chiffrement asymétrique est basé sur des opérations mathématiques qui sont faciles à effectuer dans un sens, mais dont le chemin inverse s'avère plus compliqué. Pour mieux se représenter ce concept, vous remarquerez qu'il est beaucoup plus facile de calculer 1303 x 1307 que de déterminer quels sont les deux nombres à multiplier pour obtenir 1 703 021.[2] Les attaques contre ce type de chiffrement sont basées sur la tentative de résoudre ces problèmes mathématiques plutôt que sur la recherche exhaustive d'une clé. Pourtant, comme dans le cas du chiffrement symétrique, une combinaison de calcul quantique et de techniques de tri pourrait réduire considérablement le temps et les efforts nécessaires pour mener une telle attaque.

Un autre défi réside dans le fait que les qubits ont tendance à « se désintégrer », en particulier à température ambiante. Ils ont besoin d'un refroidissement très important et sont facilement perturbés par des effets électriques ou environnementaux, voire même les uns par rapport aux autres. La stabilité d'utilisation pose plusieurs problèmes dont la résolution coûte de l'argent.

Si les mécanismes cryptographiques existants pour chiffrer et signer les données sont vulnérables aux attaques, il en va de même pour les données chiffrées et signées à l'aide de ces techniques. Nous dépendons également du chiffrement pour sécuriser les authentifications. Saisir son mot de passe pour se connecter à un site Web, saisir son code PIN pour autoriser une transaction par carte, ou même déverrouiller sa voiture à distance : toutes ces actions du quotidien sont sécurisées grâce à des mécanismes de chiffrement. Cependant, le remplacement de composants obsolètes ou de mécanismes non sécurisés dans une entreprise et une infrastructure réseau est un processus traditionnellement lent. La migration d'un ensemble d'algorithmes de chiffrement à un autre implique généralement des modifications techniques, opérationnelles et procédurales au niveau de l'organisation tout entière, et entre en concurrence avec les activités commerciales habituelles au niveau des priorités, des ressources et du budget.

1 Pour plus d'informations sur cet aspect, recherchez « algorithme de Grover » pour les clés symétriques et « algorithme de Shor » pour le chiffrement asymétrique basé sur la factorisation.

2 Remarque : Oui, il est effectivement possible de multiplier 1 par 1 703 021, mais ça ne compte pas dans le cas présent, car 1 n'est pas une clé très utile.

3 Outil de comparaison de longueur de clé « BlueKrypt » : https://www.keylength.com/fr/4/

CC BY-NC-SA 4.0

Si vous avez stocké des archives de données chiffrées au fil des ans, imaginez la quantité de travail qui sera nécessaire pour chiffrer à nouveau toutes ces archives à court terme, juste parce que la cryptanalyse quantique a tout à coup rendu leur déchiffrement possible. Qu'en serait-il si vous deviez remplacer du jour au lendemain les signatures numériques d'une archive de documents à long terme comme des titres de propriété, ou encore réémettre les clés physiques pour toutes les voitures d'un modèle particulier ?

En réponse à cet affaiblissement potentiel des algorithmes asymétriques populaires tels que RSA et Elliptic Curve dû à l'informatique quantique, la recherche identifie un certain nombre d'alternatives résistantes à la quantique ayant recours à d'autres types de problèmes mathématiques[4].

Que devraient faire les parties prenantes ?

En tant qu'utilisateurs, nous ne sommes peut-être pas en mesure de fournir des solutions techniques, mais il nous incombe de comprendre les enjeux et d'exprimer un point de vue éclairé, si l'occasion se présente, aux décideurs et aux prestataires de services.

Étant donné que l'informatique quantique viable aurait pour effet de réduire de moitié la longueur de clé effective pour les algorithmes symétriques, la contre-mesure évidente pour les développeurs de produits de chiffrement est d'au moins doubler la longueur des clés utilisées.

Les décideurs doivent veiller à ce que la technologie de chiffrement soit traitée comme un élément critique de l'infrastructure informatique et consentir les investissements adéquats au niveau de la gouvernance, l'évaluation des risques et la planification. Leur stratégie devrait :

- S'attacher à surveiller les développements de l'informatique quantique et du chiffrement résistant à la quantique.
- Inclure la technologie de chiffrement dans les cycles réguliers d'évaluation des risques organisationnels.
- Explorer les orientations nationales et régionales pertinentes, telles que celles publiées par le National Institute for Standards and Technology (« Institut national des normes et de la technologie ») aux États-Unis : Quantum encryption algorithm selection and validation (« sélection et validation des algorithmes de chiffrement quantique »)[5] ; les directives sur les mécanismes cryptographiques[6] ; l'ébauche des directives Getting Ready for Post-Quantum Cryptography (« Préparation au chiffrement post-quantique »)[7].
- Planifier le rechiffrement des données au repos et la resignature des artéfacts signés numériquement.[8]
- Optimiser l'agilité des algorithmes au cas où un changement d'algorithme ou de technologie serait nécessaire, en particulier à court terme.[9]
- Cultiver, au sein de l'organisation, la capacité d'actualisation et de déploiement de technologies de sécurité correspondant aux meilleures pratiques.[10]
- Veiller à ce qu'une technologie de sécurité obsolète ne puisse pas être maintenue dans l'infrastructure au-delà de la période où son utilisation a été jugée sûre.

CC BY-NC-SA 4.0