Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS

16 mai 2024

Considérations technologiques

Ordinateur quantique et cryptographie post-quantique

1 Introduction

Pas plus tard qu'en 2019, dans la revue scientifique *Nature*, Google a annoncé avoir atteint la suprématie quantique[1]. Les médias parlent également beaucoup d'informatique quantique, des dangers et des menaces qui en découlent pour les procédés actuels et de la nécessité de pouvoir utiliser la cryptographie en toute sécurité, y compris face aux ordinateurs quantiques. Parfois, cet écho médiatique fait aussi naître de grandes incertitudes et craintes concernant les limites de la cryptographie. Le présent guide s'attache donc à décrire brièvement les caractéristiques d'un ordinateur quantique, les problèmes qu'il pose pour la sécurité de certaines techniques, le concept de cryptographie post-quantique (CPQ) et les domaines où il faut intervenir.

2 Ordinateur quantique

L'ordinateur traditionnel fonctionne selon les lois de la physique classique, tandis que l'ordinateur quantique se base sur les lois de la mécanique quantique. Ce dernier permet en effet d'exploiter les propriétés quantiques telles que la superposition ou l'intrication. L'ordinateur quantique ne s'appuie pas sur le bit, mais sur le bit quantique ou qubit (parfois écrit « qbit »). Un qubit représente le plus simple système non trivial possible et peut théoriquement se retrouver dans une infinité d'états superposés différents (parallélisme quantique). De nouvelles approches et possibilités peuvent ainsi être explorées pour la calculabilité.

Du fait de sa conception élaborée et de ses caractéristiques, l'ordinateur quantique est surtout adapté pour résoudre des tâches qui sont hors de portée d'un ordinateur classique ou qui lui demandent beaucoup de temps. Il peut s'agir de simulations (sciences naturelles et ingénierie), d'optimisations (logistique et finance), d'apprentissage automatique

[1] https://www.nature.com/articles/s41586-019-1666-5

(intelligence artificielle) ou de la résolution de problèmes mathématiques dont la complexité garantit la sécurité de certains procédés cryptographiques. Même si l'utilisation d'ordinateurs quantiques à grande échelle reste à l'heure actuelle une construction essentiellement théorique, de nombreux acteurs y travaillent d'arrache-pied. En effet, des travaux de recherche et de développement sont menés non seulement par de grandes entreprises technologiques telles qu'IBM, Google, Microsoft ou Intel, mais aussi par des universités, des entreprises dérivées (*spin-offs*) et des start-ups. Actuellement, les ordinateurs les plus avancés sont dotés de quelques centaines de qubits (p. ex. 433 pour le processeur quantique Osprey, présenté par IBM en 2022). Toutefois, l'entreprise IBM prévoit de développer un système à 100 000 qubits d'ici 2033[2]. Si elle concrétise cette ambition, elle pourrait aboutir à ce qu'on appelle un « ordinateur quantique cryptographiquement pertinent » (CRQC). La question de savoir quelle taille doit avoir un ordinateur quantique pour être considéré comme un CRQC n'est aujourd'hui pas tranchée. L'une des raisons, c'est que bon nombre d'algorithmes quantiques utilisent des qubits tolérants aux erreurs appelés *qubits logiques*. Les qubits physiques utilisés actuellement sont en effet sujets aux erreurs. Pour les corriger, il faut créer un qubit logique en assemblant plusieurs qubits physiques. C'est ce qu'on appelle la *correction d'erreur quantique*. Récemment, de nombreux progrès ont été réalisés dans ce domaine. Une autre approche consiste à créer directement des qubits logiques avec des méthodes relevant de l'optique quantique.

Quoi qu'il en soit, la construction d'un CRQC serait un saut technologique plus important que la suprématie quantique évoquée en introduction. En fin de compte, le terme *suprématie quantique* signifie simplement qu'un ordinateur quantique peut résoudre plus rapidement un problème mathématique qu'un superordinateur classique. Cette définition dépend bien sûr fortement du problème de base et ne peut pas donc pas être généralisée. Il faut aussi prendre avec des pincettes les déclarations de l'entreprise D-Wave Systems[3] : les ordinateurs qu'elle commercialise disposent certes de milliers de qubits, mais ils ne peuvent pas être utilisés à large échelle. En effet, ils ne servent que pour certaines tâches d'optimisation et ne semblent même pas plus performants que les ordinateurs traditionnels dans ce domaine[4].

3 Problèmes

Comme le suggère sa dénomination, un *Cryptographically Relevant Quantum Computer* permettrait de résoudre des problèmes mathématiques qui sont la clé de voûte sécuritaire de certains procédés cryptographiques. Il s'agit surtout de la cryptographie asymétrique, qui est basée sur le problème de factorisation des grands nombres, à l'instar du chiffrement RSA, ou sur le problème du logarithme discret, à l'instar de l'échange de clés Diffie-Hellman, de l'algorithme de signature numérique (DSA) et des techniques cryptographiques fondées sur les courbes elliptiques. En 1994, Peter W. Shor a déjà montré comment un ordinateur quantique suffisamment puissant ou un CRQC peut résoudre ces problèmes mathématiques et donc casser les systèmes cryptographiques qui les intègrent [1]. Contrairement à un ordinateur classique, l'algorithme de Shor a un temps d'exécution polynomial et il est efficace au sens de la théorie de la complexité.

Comme les systèmes de cryptographie asymétrique menacés par l'algorithme de Shor sont actuellement très répandus, le développement d'un CRQC aurait des répercussions

[2] https://www.ibm.com/quantum/blog/100k-qubit-supercomputer

[3] https://www.dwavesys.com

[4] https://dl.acm.org/doi/10.1145/3459606

majeures sur leur sécurité. Parfois, on parle aussi de *Q-Day*, c'est-à-dire le jour où un CRQC sera capable de casser les protocoles cryptographiques actuels.

Pour résoudre des problèmes cryptographiques complexes, les algorithmes quantiques ont besoin dans tous les cas de qubits logiques qui augmentent de façon linéaire en fonction de la longueur de clé. Il en faut par exemple plusieurs milliers pour casser le chiffrement RSA. Avec les techniques de correction d'erreur actuelles, on multiplie le nombre de qubits physiques nécessaire. Toutefois, si l'entreprise IBM arrive à tenir son objectif, à savoir développer un ordinateur quantique à 100 000 qubits d'ici 2033, elle fera peser une menace sérieuse sur de nombreux systèmes de cryptographie asymétrique.

Même si, théoriquement, un ordinateur quantique peut aussi servir à casser les systèmes de cryptographie symétrique, les répercussions sur la sécurité des techniques y relatives sont moins importantes. En 1996, l'informaticien Lov K. Grover a proposé un algorithme permettant de réduire de 2^n à $2^{n/2}$ le temps nécessaire à la recherche complète d'une clé de longueur *n* bits [2]. En théorie, cette méthode fragilise les générateurs de nombres pseudoaléatoires, les codes d'authentification de message et les chiffrements symétriques, mais il est possible de compenser cette faiblesse assez facilement en doublant la longueur de clé. Un CRQC n'affecterait que marginalement la sécurité des systèmes de cryptographie symétrique. En outre, l'algorithme de Grover a atteint son potentiel maximum.

Bien qu'il soit impossible à l'heure actuelle de développer un CRQC puissant, il subsiste le problème de la récolte de données à grande échelle pour les déchiffrer plus tard avec un CRQC. Cette stratégie, résumée par la formule *Harvest Now, Decrypt Later*, ou attaque de type HNDL est aujourd'hui la principale raison qui justifie la recherche rapide de solutions pratiques.

4 Solutions

Comme les travaux de recherche et de développement menés par les entreprises technologiques susmentionnées vont bon train, que le développement d'un ordinateur quantique universel est en bonne voie et que des attaques de type HNDL peuvent survenir, il convient de se pencher sur la façon de construire des systèmes cryptographiques capables de résister aux ordinateurs quantiques. Cette branche de la cryptographie s'appelle la *cryptographie post-quantique (*CPQ) et suscite actuellement un vif intérêt. La CPQ repose sur la cryptographie asymétrique. Dans le domaine de la cryptographie symétrique, il n'y a presque pas besoin d'intervenir, car – comme évoqué plus haut – on peut continuer à utiliser les systèmes cryptographiques actuels en doublant la longueur de clé[5]. Ce faisant, on contrecarre les effets de l'algorithme de Grover. En d'autres termes, le niveau de sécurité reste plus ou moins le même. Concrètement, il s'agit d'utiliser le chiffrement AES-256 au lieu du AES-128. En pratique, les inconvénients sont mineurs, voire inexistants (la longueur de clé n'est pas un facteur décisif pour la vitesse de chiffrement et de déchiffrement).

La CPQ vise à élaborer des procédés et des systèmes de cryptographie asymétrique que l'on peut déployer efficacement, mais qui reposent sur des problèmes mathématiques réputés complexes et pratiquement insolubles, même pour un ordinateur quantique. Le National Institute of Standards and Technology (NIST) organise d'ailleurs depuis 2017 un concours international très prisé[6]. Il a publié en 2022 une liste des quatre premiers

[5] Cette opération a du sens jusqu'à un certain point : à partir de 256 bits, elle n'est absolument plus nécessaire.

[6] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

algorithmes sélectionnés pour le chiffrement asymétrique ou transport de clé (KEM[7]) et les signatures numériques. Le NIST est en train d'établir des normes de cryptographie post-quantique en s'appuyant sur ces algorithmes. Celles-ci sont en phase finale. Les FIPS 203 s'appliquent aux ML-KEM et les FIPS 204 aux ML-DSA. Ces standards ont été définis sur la base des algorithmes CRYSTALS-Kyber et CRYSTALS-Dilithium, fondés sur les réseaux euclidiens. L'algorithme SPHINCS+, qui utilise des fonctions de hachage, sert de base aux FIPS 205 SLH-DSA. L'algorithme de signature FALCON, également fondé sur les réseaux euclidiens, sera standardisé ultérieurement. Pour le KEM, le concours se poursuit : plusieurs algorithmes basés sur des codes passent un tour supplémentaire. Quant aux signatures numériques, le NIST a finalement lancé un deuxième concours en 2023. Pour l'instant, on ne sait donc pas encore si et quand d'autres algorithmes pourraient s'ajouter à la liste des futurs standards. Outre le NIST, d'autres organisations telles que l'Internet Engineering Task Force (IETF), l'European Telecommunications Standards Institute (ETSI) et l'International Organization for Standardization (ISO) planchent sur la standardisation d'algorithmes CPQ.

Ce serait une erreur de remplacer maintenant tous les procédés actuels de cryptographie asymétrique par des procédés CPQ. En effet, seul l'avenir nous dira si ces derniers sont vraiment sûrs (bon nombre de procédés et d'algorithmes CPQ reposent sur des idées qui sont relativement récentes et qui comportent encore des zones d'ombre). Il est plutôt indiqué de combiner ces procédés. On parle alors de *cryptographie hybride*. Les applications de messagerie chiffrées de bout en bout Signal et iMessage combinent par exemple le protocole d'échange de clés de Diffie-Hellman, basé sur les courbes elliptiques, et le mécanisme d'encapsulation de clé Kyber. Pour les signatures numériques et les certificats y relatifs, il faudra aussi compter sur des approches hybrides.

La cryptographie quantique (ou l'accord de clé post-quantique comme principal et même unique moyen d'utiliser la cryptographie quantique) et le générateur quantique de nombres aléatoires ne constituent pas explicitement des solutions aux problèmes exposés dans le présent guide. Ces deux processus sont étroitement liés et peuvent être aussi utilisés à des fins commerciales. Toutefois, la cryptographie quantique pose tellement de problèmes pratiques que ni la National Security Agency[8] (NSA) ni quatre agences européennes réunies[9] ne généralisent son utilisation. Le générateur quantique de nombres aléatoires ne représente qu'une des techniques possibles pour générer des nombres au hasard. Les avantages qu'il procure ne sont pas suffisamment importants pour imposer son utilisation.

---

[7] L'abréviation KEM signifie *Key Encapsulation Mechanism*. Il s'agit d'un protocole permettant de transmettre en toute sécurité une clé cryptographique à un interlocuteur. La clé à transmettre est générée aléatoirement et chiffrée (« encapsulée ») à l'aide de la clé publique de l'interlocuteur de manière à ce qu'il puisse déchiffrer la clé uniquement avec la clé privée correspondante. Ce qu'il faudrait en réalité, c'est un protocole d'échange de clés qui fonctionne comme l'algorithme Diffie-Hellman (pas non plus interactif). Il n'en existe pas jusqu'à présent. Le KEM est donc un pis-aller.

[8] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[9] https://cyber.gouv.fr/en/actualites/uses-and-limits-quantum-key-distribution

5 Recommandations et marche à suivre

Réussir à développer un CRQC suffisamment puissant est un énorme défi technique. Ce n'est donc pas pour demain. Néanmoins, comme des attaques de type HNDL sont possibles à grande échelle, il est déjà indiqué de faire appel à la CPQ. Il convient d'agir avec prudence et de manière réfléchie[10]. En effet, le recours à des solutions rapides, voire hâtives serait plutôt négatif pour la sécurité, même si elles permettaient à première vue de résister aux attaques lancées depuis des ordinateurs quantiques. Passer à la cryptographie post-quantique est un long processus. Il s'agit donc de le planifier en tenant compte de la standardisation actuelle des algorithmes CPQ[11].

Différents acteurs s'efforcent d'ailleurs de les standardiser et de les intégrer dans des protocoles de sécurité et des produits. Les applications Signal et iMessage disposent ainsi déjà de nouveaux protocoles de chiffrement post-quantiques. Déjà au milieu des années 2010, Google a tenté d'intégrer l'algorithme Frodo (qui a précédé l'algorithme Kyber) au protocole TLS et travaille depuis lors sur différentes extensions pour ses produits[12]. Il en va de même pour Microsoft, Cloudflare et d'autres entreprises technologiques. En principe, plus un système est ouvert, plus il est difficile et chronophage d'y inclure la CPQ. En ce sens, l'utilisation de la CPQ dans des protocoles de sécurité internet standardisés (p. ex. IPsec, TLS, …) représente une difficulté majeure pour l'IETF et ses groupes de travail.

Tous les efforts fournis pour migrer vers la CPQ garantissent en fin de compte la cryptoagilité et doivent être pris en considération à cet égard. Les systèmes et applications doivent être conçus et implantés de manière à pouvoir utiliser et soutenir différents procédés et algorithmes cryptographiques. Cette forme d'agilité est déjà essentielle aujourd'hui et prendra sans doute de plus en plus d'importance à l'avenir. Elle nécessite une architecture logicielle adaptée. Pour les implémentations matérielles qui servent habituellement à augmenter les exigences de performance et/ou de sécurité, les possibilités qu'offre la cryptoagilité sont en général limitées. Dans tous les cas, il convient de consigner dans une liste (SBOM / CBOM) les composants, les procédés et les algorithmes cryptographiques utilisés. Indépendamment de la question de la CPQ, cette inventorisation est primordiale pour faire face à la recrudescence des attaques de la chaîne d'approvisionnement.

---

[10] En 2023, lors d'un forum organisé dans le cadre de la *RSA Conference* et portant sur le thème *Migrating to Post-Quantum Schemes* (« Migrer vers des procédés post-quantiques »), Adi Shamir a donné un conseil qui résume bien la situation : « *If you want to switch to post-quantum algorithms, walk, don't run* » (« Si vous voulez passer aux algorithmes post-quantiques, allez-y pas à pas, ne vous précipitez pas »). (https://www.rsaconference.com/library/presentation/usa/2023/Panel%20Migrating%20to%20Post-Quantum%20Schemes).

[11] https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

[12] https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography

Abréviations

AES	*Advanced Encryption Standard*
CBOM	*Cryptography Bill of Materials*
CPQ	Cryptographie post-quantique
CRQC	*Cryptographically Relevant Quantum Computer*
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DSA	*Digital Signature Algorithm*
ETSI	European Telecommunications Standards Institute
FIDO2	*Fast IDentity Online*
FIPS	*Federal Information Processing Standards* (US)
HNDL	*Harvest Now, Decrypt Later*
IETF	Internet Engineering Task Force
IPsec	*Internet Protocol Security*
ISO	International Organization for Standardization
KEM	*Key Encapsulation Mechanism*
ML	*Module Lattice*
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OFCS	Office fédéral de la cybersécurité
RSA	Rivest, Shamir, Adleman
SBOM	*Software Bill of Materials*
SLH	*Stateless Hash*
TLS	*Transport layer security*

Références

[1] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, novembre 1994, Santa Fe, NM, pp. 124–134.

[2] Lov K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, In: Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, mai 1996, pp. 212–219.