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

8 décembre 2025

Considérations technologiques

Ordinateur quantique et cryptographie post-quantique

1 Introduction

Depuis plusieurs années, les médias évoquent abondamment l'informatique quantique, les menaces qu'elle fait peser sur les procédés cryptographiques actuels et la nécessité de disposer de solutions cryptographiques sécurisées face aux ordinateurs quantiques. Cet écho médiatique suscite parfois des incertitudes et des craintes quant à la sécurité des méthodes en vigueur. Le présent document vise donc à décrire brièvement les caractéristiques d'un ordinateur quantique, les problèmes qu'il pose pour la sécurité de certains procédés, le concept de cryptographie post-quantique (CPQ), les avancées réalisées dans ce domaine et les axes de progression.

2 Ordinateur quantique

L'ordinateur traditionnel fonctionne selon les lois de la physique classique. L'ordinateur quantique, quant à lui, se base sur les lois de la mécanique quantique et en exploite les propriétés, par exemple la superposition ou l'intrication. Il ne s'appuie pas sur le bit (dont l'état est soit de 0 soit de 1), mais sur le bit quantique ou qubit. Cette unité représente le système quantique non trivial le plus simple et peut se trouver simultanément dans les états 0 et 1 (état dit *superposé*). Ce principe permet à un registre de plusieurs qubits de représenter simultanément une multitude d'états et de les traiter en parallèle (parallélisme quantique), ouvrant ainsi de nouvelles approches et possibilités en matière de calcul.

Grâce à sa conception élaborée et à ses caractéristiques, l'ordinateur quantique est particulièrement adapté à la résolution de tâches exploitant le parallélisme quantique. Ces dernières sont hors de portée d'un ordinateur classique ou lui demandent beaucoup de temps. Il peut s'agir de simulations (sciences naturelles et ingénierie), d'optimisations (logistique et finance), d'apprentissage automatique (intelligence artificielle) ou de problèmes mathématiques dont la complexité sous-tend la sécurité de certains procédés cryptographiques, le sujet du présent document.

Bien que le développement d'ordinateurs quantiques à grande échelle reste largement théorique à ce jour, de nombreux acteurs y travaillent activement. En effet, des travaux de recherche et de développement sont menés non seulement par des géants de la technologie tels qu'IBM, Google, Microsoft, Amazon ou Intel, mais aussi par des universités, des entreprises dérivées (*spin-offs*) et des start-ups. Actuellement, les systèmes les plus avancés comptent quelques centaines de qubits (p. ex. 433 pour le processeur Osprey, présenté par IBM en 2022) ou, au mieux, de plusieurs milliers (p. ex. 6100 pour le réseau construit par Caltech)[1]. IBM prévoit de développer un système à 100 000 qubits d'ici 2033[2]. Si cet objectif ambitieux se concrétise, on se rapprochera d'un « ordinateur quantique cryptographiquement pertinent » ou CRQC (*Cryptographically Relevant Quantum Computer*). La question de la taille nécessaire pour qualifier un système de CRQC n'est toutefois pas tranchée. L'une des raisons est que de nombreux 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*. Des progrès significatifs ont été réalisés récemment dans ce domaine. Une autre approche consiste à générer directement des qubits logiques avec des méthodes relevant de l'optique quantique. Compte tenu de ces multiples évolutions, il est difficile de prédire avec précision quand un CRQC sera réellement disponible. Quoi qu'il en soit, l'avènement d'un CRQC représenterait un saut technologique bien plus important que la suprématie quantique souvent mise en avant dans les médias. Cette dernière signifie simplement qu'un ordinateur quantique peut résoudre un problème mathématique particulier plus efficacement qu'un superordinateur classique. Cette définition dépend toujours fortement du problème considéré et ne peut être généralisée. Il convient également de prendre avec des pincettes les déclarations de l'entreprise D-Wave Systems[3] : ses ordinateurs, bien qu'ils comptent des milliers de qubits, ne sont pas des ordinateurs à portes logiques pouvant être utilisés à large échelle. En effet, ils sont limités à certaines tâches d'optimisation et ne semblent pas surpasser systématiquement les ordinateurs classiques dans ce domaine[4].

3 Problèmes

Comme le laisse penser son nom, un CRQC permettrait de résoudre efficacement des problèmes mathématiques qui constituent le fondement de la sécurité de certains procédés cryptographiques. Il s'agit surtout de la cryptographie asymétrique, fondée soit sur la factorisation de grands nombres (comme dans l'algorithme de signature RSA), soit sur le logarithme discret (échange de clés Diffie-Hellman, DSA, cryptographie sur courbes elliptiques). En 1994, Peter W. Shor a démontré qu'un ordinateur quantique suffisamment puissant (un CRQC) pouvait résoudre ces problèmes mathématiques et donc compromettre les systèmes cryptographiques qui les intègrent [1]. Contrairement aux algorithmes classiques, l'algorithme de Shor s'exécute en temps polynomial et il est donc efficace au sens de la théorie de la complexité.

Étant donné l'utilisation répandue de systèmes de cryptographie asymétrique vulnérables à Shor, le développement d'un CRQC aurait des répercussions majeures sur leur sécurité.

---

[1] À noter que, pour la stabilité des qubits et la correction des erreurs, les différentes technologies ont leurs propres particularités, si bien qu'on ne peut pas toujours comparer directement le nombre de qubits. C'est particulièrement le cas pour le réseau de 6100 qubits : il n'est pas possible de le comparer avec un ordinateur quantique.

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

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

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

Pour désigner le jour où un CRQC pourra effectivement briser ces systèmes, on utilise parfois le terme de *Quantum Day* ou *Q-Day*.

Pour que les algorithmes quantiques puissent résoudre des problèmes cryptographiques complexes, il faut qu'un certain nombre de qubits logiques augmentent de façon linéaire en fonction de la longueur de clé (plusieurs milliers pour le chiffrement RSA, par exemple). Avec les techniques de correction d'erreur actuelles, on multiplie fortement le nombre de qubits physiques nécessaire. Si IBM parvenait à tenir son objectif d'ici 2033, son système à 100 000 qubits pourrait déjouer les systèmes de cryptographie asymétrique.

En principe, un ordinateur quantique peut aussi servir à briser la cryptographie symétrique, mais les répercussions sur les protocoles de sécurité sont bien moindres. En 1996, l'informaticien Lov K. Grover a proposé un algorithme qui réduit le temps de recherche d'une clé de n bits de 2^n à $2^{n/2}$ [2], fragilisant en théorie les générateurs de nombres pseudoaléatoires, les codes d'authentification de message et les chiffrements symétriques. Toutefois, il suffit de doubler la longueur de clé pour compenser cette faiblesse. L'algorithme de Glover menace même les fonctions de hachage cryptographiques sans clé, et plus précisément la propriété appelée *résistance aux collisions*. Là encore, la faille peut être comblée : il suffit de doubler la valeur de hachage. En fin de compte, un CRQC n'affecterait que marginalement la sécurité des systèmes de cryptographie symétrique et des fonctions de hachage cryptographiques. Jusqu'à présent, il s'avère que l'algorithme de Glover reste purement théorique et ce qui se fait de mieux : aucun algorithme quantique plus performant n'a été trouvé pour rechercher un élément dans un ensemble désordonné[5]. Cette accélération théorique du temps de recherche avec un ordinateur quantique semble même difficilement applicable, ce qui relativise quelque peu la recommandation de doubler la longueur de clé ou la valeur de hachage.

Même s'il est impossible à l'heure actuelle de développer un CRQC, il subsiste le risque qu'un cybercriminel récolte des données à grande échelle pour les déchiffrer plus tard (*Harvest Now, Decrypt later* ou HNDL) avec un CRQC. Les attaques HNDL sont aujourd'hui la principale raison qui justifie la recherche rapide de solutions pratiques. Autre problème : les identités et les signatures numériques auxquelles on se fie maintenant pourraient être falsifiées avec un CRQC (*Trust Now, Forge Later* ou TNFL). Les procédures d'authentification étant la plupart du temps éphémères et les signatures pouvant être renouvelées en tout temps avec de nouvelles clés, les attaques TNFL sont considérées comme moins préoccupantes. C'est pourquoi les efforts actuels se concentrent principalement sur la défense contre des attaques HNDL.

4 Solutions

L'avancée des travaux menés par les entreprises technologiques susmentionnées pour développer un ordinateur quantique à large échelle et les possibles attaques HNDL (et en partie TNFL) imposent de concevoir des systèmes cryptographiques résistants aux ordinateurs quantiques. Cette branche s'appelle la *cryptographie post-quantique* (CPQ) et suscite actuellement un vif intérêt. La CPQ repose sur la cryptographie asymétrique.

[5] https://arxiv.org/abs/quant-ph/9701001

Pour la cryptographie symétrique, presque aucune intervention n'est nécessaire : doubler la longueur de clé suffit à contrer Grover[6] et à conserver un niveau de sécurité équivalent (ex. : 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), une agence américaine, organise d'ailleurs depuis 2017 un concours international très suivi[7]. Pour le chiffrement asymétrique ou transport de clé (KEM[8]) et les signatures numériques, il a publié en 2022 une liste des quatre premiers algorithmes sélectionnés. Les algorithmes ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium) et SLH-DSA (SPHINCS+) ont été normalisés, car ils figurent respectivement dans les standards publics FIPS 203[9], FIPS 204[10] et FIPS 205[11]. Ce n'est pas encore le cas pour l'algorithme FALCON (nom d'origine ; il en va de même pour les autres noms mis entre parenthèses à la phrase précédente). Le concours se poursuit : en 2025, le NIST a par exemple choisi HQC comme alternative à ML-KEM. Pour les signatures numériques, il a lancé un deuxième concours en 2023. Pour l'instant, on ne sait 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.

Remplacer immédiatement tous les procédés actuels de cryptographie asymétrique par des procédés CPQ serait une erreur. 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). Les procédés CPQ sont en outre plus difficiles à implémenter, ce qui fait qu'ils restent vulnérables (par exemple face à des attaques par canal auxiliaire). Plutôt que de remplacer les procédés usuels, il convient de les combiner avec les procédés CPQ. 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 ML-KEM. Pour les signatures numériques et les certificats y relatifs, les approches hybrides sont aussi à l'étude (même si les défis techniques dans ce domaine sont plus importants).

---

[6] Cette opération a du sens jusqu'à un certain point. Par exemple à partir de 256 bits, il n'est plus nécessaire de doubler la longueur de clé. En effet, même en la réduisant de moitié, la longueur effective reste supérieure à 128 bits.

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

[8] 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 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.

[9] https://csrc.nist.gov/pubs/fips/203/final

[10] https://csrc.nist.gov/pubs/fips/204/final

[11] https://csrc.nist.gov/pubs/fips/205/final

La distribution quantique de clé (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 document. Ces deux méthodes sont étroitement liées et peuvent être aussi utilisées à des fins commerciales. Toutefois, la cryptographie quantique et en particulier la distribution quantique de clé posent tellement de problèmes pratiques que ni la National Security Agency[12] (NSA) ni quatre agences européennes réunies[13] ne généralisent son utilisation. Il y a en revanche des domaines dans lesquels les générateurs quantiques de nombres aléatoires procurent certains avantages par rapport aux générateurs utilisés habituellement.

5 Recommandations et marche à suivre

Réussir à développer un CRQC est un énorme défi technique. Ce n'est donc pas pour demain[14]. Néanmoins, comme des attaques HNDL (et en partie TNFL) sont possibles à grande échelle, il est déjà opportun de migrer vers la CPQ. Avant de se lancer, il convient toutefois d'agir avec prudence et de manière réfléchie[15]. En effet, le recours à des solutions rapides, voire hâtives serait plutôt négatif pour la sécurité globale, 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 bien le planifier en tenant compte de la standardisation actuelle des algorithmes CPQ[16].

Différents acteurs s'efforcent d'ailleurs de standardiser et d'intégrer des algorithmes CPQ dans des protocoles de sécurité et des produits. Les applications déjà évoquées Signal et iMessage disposent ainsi 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 CPQ pour ses produits[17]. Il en va de même pour Microsoft, Cloudflare et d'autres entreprises technologiques. Ainsi, une part non négligeable du trafic de données internet sécurisé par le protocole TLS est actuellement aussi protégé par des algorithmes CPQ. Même les développeurs de logiciels open source s'affairent à intégrer ces algorithmes ; c'est par exemple le cas avec OpenSSH[18]. En principe, plus un système est ouvert, plus il est difficile et chronophage de les inclure. 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. Malgré tout, les avancées dans ce domaine sont bien réelles et des extensions CPQ sont déjà proposées pour de nombreux protocoles de sécurité internet.

---

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

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

[14] Dans de nombreuses publications scientifiques, les progrès du CRQC sont exagérés, car les arguments sont fondés sur des chiffres hypothétiques et donc fictifs (voir à ce sujet l'article disponible à l'adresse https://eprint.iacr.org/2025/1237.pdf).

[15] 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 »). Source : https://www.rsaconference.com/library/presentation/usa/2023/Panel%20Migrating%20to%20Post-Quantum%20Schemes.

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

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

[18] https://www.openssh.org/pq.html

Tous les efforts convergeant vers la CPQ garantissent aussi 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 vraisemblablement de plus en plus d'importance à l'avenir. Elle nécessite une architecture logicielle adaptée : par rapport aux implémentations logicielles, les implémentations matérielles, usuelles lorsque les exigences de performance et/ou de sécurité sont élevées, offrent en général moins de possibilités concernant la cryptoagilité. 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. Tant qu'on ne saura pas dans quel domaine et dans quelle mesure l'on dépendra des procédés et des algorithmes cryptographiques, on ne pourra pas être en mesure de développer et de mettre en place un dispositif de sécurité idoine. Il est donc judicieux d'établir une SBOM ou une CBOM pour appréhender le sujet. La marche à suivre est fonction de la CBOM, des particularités de l'organisation ou de l'entreprise et de ses objectifs.

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
HQC	Hamming Quasi-Cyclic
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
SSH	Secure Shell
TLS	Transport layer security
TNFL	Trust Now, Forge Later

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.