Cybersécurité: préparez-vous pour le saut quantique

La migration vers la cryptographie post-quantique signe le début d'une nouvelle ère

PAIEMENT CONNECTIVITÉ CYBERSÉCURITÉ

POSTÉ LE 05.05.25

Ceux qui voient le verre à moitié vide considèrent la migration vers la cryptographie post-quantique uniquement comme une défense qui s'impose face à la menace que fait planer l'ordinateur quantique sur les cyberdéfenses actuelles. Ceux qui voient le verre à moitié plein y voient en revanche une formidable opportunité d'accroître la cybersécurité contre des risques bien réels auxquels nous sommes déjà confrontés aujourd'hui. Et vous, voyez-vous le verre à moitié plein, ou à moitié vide ? Etes-vous prêts à envisager la migration post-quantique et le futur de la cybersécurité sous un nouveau jour ?

La plus grande évolution de cybersécurité depuis le déploiement de la cryptographie asymétrique

La migration vers la cryptographie post-quantique s'annonce comme l'un des chantiers majeurs du 21e siècle. **Ce chantier d'envergure mondiale concerne tous les secteurs d'activité**, pour peu qu'ils s'appuient sur des services en ligne ou utilisent des appareils connectés. Autrement dit, absolument tous les secteurs d'activité. Le monde de la cybersécurité n'a pas connu une transformation d'une telle envergure depuis l'adoption de la cryptographie asymétrique il y a une cinquantaine d'années.

A l'été 2024, la Maison Blanche a réuni les dirigeants du gouvernement et de l'industrie des États-Unis pour dévoiler les nouveaux standards de cryptographie post-quantique du NIST (*National Institute of Standards and Technology*). Avec cette annonce, **le NIST a officiellement donné le coup d'envoi de la migration post-quantique**, en appelant tous les acteurs de la sécurité numérique à implémenter ces standards sans tarder.

A travers le monde, d'autres organismes de standardisation et agences gouvernementales ont également franchi le pas en sélectionnant leurs propres algorithmes résistants à l'ordinateur quantique : en Europe, en Corée du Sud ou en Chine, par exemple. **Les prochaines étapes de standardisation s'organisent désormais au niveau des grandes organisations industrielles** comme l'IETF (*Internet Engineering Task Force*), le W3C (*World Wide Web Consortium*), l'ISO (*International Organization for Standardization*), l'ETSI (*European Telecommunications Standards Institute*), GlobalPlatform et la GSMA. Il leur revient à présent de mettre à jour leurs spécifications et leurs feuilles de route afin d'y intégrer la cryptographie post-quantique.

Les ordinateurs quantiques qui font les gros titres actuellement, développés par des sociétés comme Google, Microsoft, IBM ou des équipes de recherche en Chine, **se concentrent sur des applications qui n'ont rien à voir avec le fait de factoriser des grands nombres** pour casser les crypto-systèmes actuels. En fait, les cas d'usage principaux de ces premiers ordinateurs quantiques se concentrent sur le *machine learning*, la recherche médicale ou l'optimisation logistique. **Néanmoins, le sentiment d'urgence est bien présent au sein de la communauté des experts en**

cybersécurité, car les avancées technologiques qui rendent ces ordinateurs quantiques de plus en plus performants pourraient finalement les rendre plus facilement adaptables à la factorisation des grands nombres. En parallèle, l'algorithme de Shor, précisément conçu pour factoriser des grands nombres avec un ordinateur quantique, continu d'être optimisé de façon à utiliser moins de qubits, ce qui abaisse de facto le seuil matériel à franchir pour pouvoir casser les systèmes cryptographiques actuels.

Sous l'impulsion de ces avancées des mathématiques et technologies quantiques, et avec l'impératif d'assurer la sécurité de certaines données pour des dizaines d'années, **le calendrier de migration vers la cryptographie post-quantique est particulièrement resserré**. A titre d'exemple, la feuille de route du NIST[1] précise déjà que certaines tailles de clés utilisées par de nombreux crypto-systèmes à clés publiques seront obsolètes à partir de 2030 (c'est à dire encore utilisables, mais en connaissance des risques). **En 2035, de nombreux algorithmes seront interdits**, dans le sens où les produits et systèmes qui les utilisent ne répondront plus aux normes FIPS. Cela concernera non seulement **les crypto-systèmes RSA**, largement utilisés depuis les années 1980 pour chiffrer et signer des documents et des emails ou pour authentifier des transactions en ligne, **mais aussi des crypto-systèmes utilisant les courbes elliptiques**. Le sentiment d'urgence est similaire au niveau de l'Union Européenne où 18 Etats Membres ont signé une déclaration commune[2] préconisant de mettre en place, d'ici 2030, les sécurités nécessaires pour protéger les cas d'usage les plus critiques.

Les délais sont très courts et la tâche est colossale, c'est indéniable. Cependant **les bénéfices d'une migration post-quantique réussie seront incommensurables**, au point même où le développement d'un ordinateur quantique dont le but serait de casser les clés cryptographiques pourrait finalement s'avérer en grande partie caduc. Avec la migration des systèmes, la motivation à exploiter l'informatique quantique pour des attaques contre la cryptographie va probablement diminuer, même si le développement de telles machines à des fins de démonstration restera de l'ordre des possibles, à mesure que la technologie deviendra plus accessible.

Migration post-quantique: la sécurité élevée à l'état de l'art dans tous les secteurs

Le premier bénéfice significatif de la migration est l'étape indispensable qui consiste à **faire l'inventaire de tous les actifs cryptographiques**. Cet inventaire servira de point de départ pour une mise à niveau généralisée vers les normes de sécurité les plus récentes.

Au moment de la migration, **les systèmes et protocoles les plus anciens seront abandonnés** au profit des algorithmes et protocoles les plus récents. C'est ainsi le fruit de plusieurs d'années de travail dans la mise au point de ces nouveaux protocoles plus performants et plus sécurisés qui se concrétisera enfin à large échelle. La migration vers la cryptographie post-quantique accélèrera aussi très probablement le déploiement des dernières spécifications au niveau de chaque secteur.

Cette migration post-quantique aura un impact de cybersécurité sans précédent car elle nécessitera une approche de bout-en-bout. Chaque élément de la chaine devra bénéficier d'une mise à jour de sécurité : les HSMs, les éléments sécurisés, les appareils connectés, les OS, les protocoles, les librairies cryptographiques, etc. L'étendue des mises à jour nécessaires a été mise en lumière lors du Mobile World Congress 2025, lors duquel IDEMIA Secure Transactions a fait la démonstration de **la migration d'un appareil IoT doté d'une eSIM**, ce qui a nécessité la mise à jour de la puce, du protocole TLS de l'appareil ainsi que du serveur gérant les mises à jour du profil eSIM. Les algorithmes de cryptographie post-quantique exigent généralement des ressources de calcul plus importantes, ce qui peut avoir une incidence sur les applications sensibles à la latence, telles que les paiements ou l'authentification sécurisée. Pour que la cryptographie post-quantique s'intègre de manière optimale au sein des infrastructures physiques et digitales existantes, **il est essentiel d'adopter une approche complète, en tenant compte du cas d'usage**.

La préparation de la migration vers une sécurité résistante à l'ordinateur quantique devrait être considérée comme l'opportunité de faire un pas de géant dans le **renforcement des défenses de cybersécurité de toutes les industries**. Elle sera l'occasion de poser des fondations solides pour un avenir plus sûr.

Crypto-agilité : des mises à jour de sécurité en continu et plus efficaces

La migration vers la cryptographie post-quantique permettra également de **mieux gérer les actifs cryptographiques à l'avenir** en introduisant des mécanismes de mise à jour plus agiles, plus fréquents et plus systématiques.

A l'heure actuelle la maintenance de sécurité de nombreux appareils s'avère compliqué à long terme. Le risque est limité une fois que les appareils sont déployés car ils sont protégés par une cryptographie robuste qui les protège contre l'installation de malware ou de ransomware. Mais ce rempart cryptographique pourrait tomber si un ordinateur quantique venait à en déchiffrer les clés, d'autant que **les cyberattaques sont de plus en plus sophistiquées et prennent une ampleur nouvelle avec l'utilisation de l'IA**.

La crypto-agilité, qui est l'un des principes fondamentaux de la migration post-quantique, permettra de maintenir à l'état de l'art les défenses cryptographiques de ces appareils, de façon continue. Ce nouveau mécanisme mis en place pour permettre la maturation et l'évolution de la cryptographie post-quantique contribuera à **améliorer la cybersécurité dans la durée**, en introduisant des mises à jour de sécurité plus automatisées, ne nécessitant pas l'intervention d'un utilisateur ou d'un technicien.

La migration vers la cryptographie post-quantique devrait également **permettre d'étendre la sécurité plus largement dans le domaine de l'IoT** grâce à l'utilisation d'eSIMs crypto-agiles comme crypto-processeurs.[3] Cette nouvelle approche permettra d'harmoniser la façon dont la cryptographie est implémentée dans les appareils connectés, apportant une amélioration par rapport aux implémentations cryptographiques multiples généralement faites dans les systèmes Linux embarqués de ces appareils. L'autre avantage significatif à utiliser l'eSIM comme crypto-processeur résistant à l'ordinateur quantique et à gérer les mises à jour de sécurité via cet élément crypto-agile, est de ne pas impacter la certification de sécurité de l'appareil ou du système concerné. Celle-ci restera donc valide. **Du point de vue de la certification, cela représente un progrès incontestable** par rapport aux mises à jour effectuées actuellement au niveau du système Linux qui nécessitent, en principe, une nouvelle certification de l'appareil ou du système, laquelle est souvent négligée.

Des implémentations cryptographiques plus uniformisées, faciles à déployer et à maintenir à l'état de l'art sans impact sur la certification des appareils ; **des mises à jour de sécurité plus fréquentes et plus efficaces : la crypto-agilité va véritablement changer la donne** face aux enjeux toujours croissants de cybersécurité.

Cryptographie post-quantique : un nouveau chapitre de la cybersécurité

Si l'ampleur et la complexité de la tâche à accomplir sont évidentes, **les avantages à long terme** de la migration vers la cryptographie post-quantique constituent une forte motivation pour aller de l'avant. Tous les acteurs qui vont participer à la migration post-quantique dans les dix années qui viennent vont **écrire l'histoire de la cybersécurité**. Chez IDEMIA Secure Transactions nous sommes fiers d'y contribuer et de **rendre possible un avenir plus sûr** au côté de nos clients et partenaires.

[1] https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
[2] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5
[3] https://www.youtube.com/watch?v=gnVl8fO1xUo