RAPPORT DE VEILLE – JANVIER-FÉVRIER 2025

28/02/2025

Introduction

La communication quantique est un domaine de la physique appliquée et des technologies de l'information qui exploite les lois de la mécanique quantique pour transmettre de l'information de manière extrêmement sécurisée. Contrairement à la communication classique, la communication quantique utilise les propriétés des particules subatomiques, comme l'intrication ou la superposition, pour assurer une transmission inviolable. L'une de ses applications les plus concrètes est la distribution quantique de clés (QKD), qui permet de générer et échanger des clés de chiffrement impossibles à intercepter sans être détecté. En plus de cela, elle se base sur la génération de clés de chiffrement de manière réellement aléatoire et non en suivant un protocole. Accentuant ainsi de manière très significative la sécurité de la transmission d'information.

Durant les mois de janvier et février 2025, plusieurs événements et annonces importantes ont marqué l'avancée de cette technologie. Ce rapport analyse trois temps forts : la mise en place d'un système de communication quantique inviolable à Ulm en Allemagne, l'initiative de l'entreprise SEALSQ dans l'infrastructure de clé racine post-quantique, et l'annonce par la Chine de ses propres standards cryptographiques résistants au quantique. Ces initiatives témoignent d'une accélération internationale vers un monde sécurisé post-quantique.

Développements récents

Lancement d'une communication quantique inviolable à Ulm

Le 27 janvier 2025, le Centre aérospatial allemand (DLR) et l'Université d'Ulm ont inauguré un système de communication quantique entre le campus universitaire et le DLR, reposant sur la distribution de clés quantiques (QKD). Ce système repose sur l'envoi de photons à travers une fibre optique et permet de détecter toute tentative d'interception. Ce projet constitue un jalon important pour l'Allemagne dans le développement d'un réseau national sécurisé par des moyens quantiques, tout en montrant la faisabilité de solutions concrètes à l'échelle urbaine.

Source : https://www.dlr.de/en/latest/news/2025/launch-of-eavesdrop-proof-quantum-communication-in-ulm

Lancement du Quantum Root Key par SEALSQ

Le 31 janvier 2025, la société SEALSQ a dévoilé sa nouvelle infrastructure de clé racine, appelée Quantum RootCA. Cette technologie repose sur les algorithmes de cryptographie post-quantique CRYSTALS-Dilithium et FALCON, sélectionnés par le NIST. L'objectif est de préparer les systèmes de cybersécurité à résister à des attaques qui pourraient être menées

par de futurs ordinateurs quantiques. SEALSQ ambitionne d'étendre cette technologie à grande échelle, notamment dans le secteur bancaire, gouvernemental et les objets connectés industriels.

Source : https://www.globenewswire.com/news-release/2025/01/31/3018841/0/en/SEALSQ-To-Launch-Post-Quantum-Cryptography-Root-Key

La Chine lance ses propres normes de cryptographie post-quantique

En février 2025, la Chine a annoncé le développement de ses propres standards de cryptographie résistante aux attaques quantiques, cherchant à se détacher des normes élaborées aux États-Unis par le NIST. Cette décision s'inscrit dans une logique d'indépendance stratégique sur les questions de sécurité numérique. En parallèle, elle vise à proposer des solutions plus adaptées à l'environnement technologique et réglementaire chinois. Ce mouvement accentue la fragmentation potentielle des standards internationaux, mais il souligne aussi l'importance globale du passage à une cybersécurité post-quantique.

Source : https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard

Analyse

Ces trois événements révèlent plusieurs dynamiques complémentaires. D'une part, les démonstrations de faisabilité technique (comme celle d'Ulm) montrent que la communication quantique n'est plus une idée de laboratoire, mais une technologie concrète prête à être déployée. D'autre part, les initiatives industrielles (comme celles de SEALSQ) révèlent une prise en main du secteur privé, soucieux de sécuriser ses systèmes face aux évolutions de l'informatique quantique. Enfin, la Chine, par sa volonté d'autonomisation cryptographique, illustre un enjeu géopolitique majeur autour de la souveraineté technologique et de la standardisation future des communications sécurisées à l'échelle mondiale.

Conclusion

La période de janvier à février 2025 confirme que la transition vers une ère de communication et de cryptographie post-quantique est bien engagée. Les gouvernements, les chercheurs et les entreprises accélèrent leurs efforts pour intégrer ces technologies dans les infrastructures critiques. À l'avenir, il sera essentiel de suivre l'harmonisation (ou non) des standards, ainsi que les premières grandes implémentations commerciales de ces solutions.

Sources

https://www.dlr.de/en/latest/news/2025/launch-of-eavesdrop-proof-quantum-communication-in-ulm

https://www.globenewswire.com/news-release/2025/01/31/3018841/0/en/SEALSQ-To-Launch-Post-Quantum-Cryptography-Root-Key

https://thequantuminsider.com/2025/02/18/china-launches-its-own-quantum-resistant-encryption-standard