Cryptographie post-quantique : comment décider sans savoir ?

Stéphane Bortzmeyer

27 mai 2026

Petit rappel de cryptologie

- La cryptographie est indispensable à la sécurité de l'Internet,
- Repose sur des problèmes mathématiques considérés comme très durs, voire impossibles,
- Algorithmes typiques : RSA, ECDSA, Ed25519…
- La cryptanalyse cherche à « casser » ces algorithmes.

Les calculateurs quantiques

- « Si vous croyez comprendre la quantique, c'est que vous ne comprenez pas la quantique. » (Richard Feynman)
- Il existe des algorithmes de cryptanalyse qui, **si** on a un calculateur quantique, permettent de casser les algorithmes de cryptographie typiques **très vite**.
- Puis-je commander un calculateur quantique sur AliExpress ? Non.
- Quand pourrais-je ? **On ne sait pas**. C'est un problème de physique fondamentale, pas d'ingéniérie.

La cryptographie post-quantique

- La solution est simple : remplacer les algorithmes de cryptographie typiques par des algorithmes **post-quantiques**. Merci, les mathématicien·nes.
- Plusieurs sont déjà normalisés (ML-DSA, ML-KEM, SLH-DSA…).
- Normalement, ils résistent aux calculateurs quantiques (et à la cryptanalyse classique).

Faut-il y passer du temps ?

- Inventer, normaliser, programmer, déployer… Tout cela coûte du temps et de l'argent.
- Est-ce que ça vaut la peine ? La menace le justifie t-elle ?
- On ne peut pas forcément se permettre d'attendre : certains secrets chiffrés devront rester secrets des dizaines d'années.
- Or, le déploiement prendra du temps donc c'est aujourd'hui qu'il faut réléchir.

L’incertitude

- Personne de sérieux ne peut prévoir la date de disponibilité des CRQC (*Cryptographically Relevant Quantum Computers*).
- Mais il faut bien décider si on sort le carnet de chèques !
- Et il est difficile de décider au milieu de tout le baratin commercial (Google : « j’ai atteint la suprématie quantique », Microsoft : « j’utilise un nouvel état de la matière, avec les paires de Majorana »).