Les Echos

Comment le secteur financier se prépare à la menace quantique

D'ici à quelques années, les ordinateurs quantiques auront le potentiel de « casser » les mécanismes de chiffrement qui protègent actuellement nos transactions et autres données sensibles.

L'informatique quantique pourrait permettre de contourner les systèmes d'authentification et d'usurper des identités numériques, ouvrant potentiellement la voie à des fraudes massives. (iStock)

Par Rachel Cotte
Publié le 3 févr. 2025 à 07:00Mis à jour le 3 févr. 2025 à 09:03

De la sécurisation de nos conversations électroniques à celle de nos achats en ligne, la cryptographie joue un rôle essentiel pour préserver la confidentialité de nos données au quotidien. Aujourd'hui, nos systèmes de chiffrement reposent sur des problèmes mathématiques extrêmement difficiles à résoudre pour un ordinateur classique. Mais à l'heure du développement de l'informatique quantique, cette sécurité pourrait être compromise dans un futur relativement proche.

Les ordinateurs quantiques - notamment mis au point par des géants de la tech comme Google ou IBM - pourraient avoir un jour une puissance de calcul susceptible de « casser » les systèmes de cryptage classiques en quelques minutes, voire en quelques secondes. Les institutions financières, en raison de leur dépendance accrue au chiffrement pour protéger les transactions et données sensibles, y seraient particulièrement vulnérables. Selon l'Agence nationale de la sécurité des systèmes

d'information (Anssi), un tel risque pourrait se matérialiser d'ici à 2030 - une échéance surnommée le « Q-Day ».

Usurpation d'identité

Concrètement, la technologie pourrait permettre à des acteurs malveillants de contourner les systèmes d'authentification, d'usurper des identités numériques et d'accéder aisément à des bases de données sensibles, ouvrant potentiellement la voie à des fraudes massives.

Les institutions financières sont globalement conscientes de la nécessité d'opérer leur transition vers des systèmes de chiffrement résistants au quantique - on parle de « cryptographie post-quantique ». Le National Institute of Standards and Technology (NIST) a sélectionné, en juillet 2022, quatre algorithmes en mesure de remplacer les protocoles actuels.

« Nous estimons qu'il est important pour la communauté des acteurs du paiement d'amorcer ce virage technologique sans délai : recenser les algorithmes de chiffrement et établir un plan de transition post-quantique », résume Valérie Fasquelle, directrice des systèmes d'information de la Banque de France.

Dans son dernier rapport sur la sécurité des moyens de paiements, l'institution recommande, entre autres, aux acteurs concernés d'inventorier les différents dispositifs de sécurité de leurs systèmes d'information, de hiérarchiser les données selon leur degré de sensibilité, mais aussi d'expérimenter l'implémentation de nouveaux types d'algorithmes.

Manque de maturité

Certains acteurs peuvent hésiter à se lancer, notamment face au manque de maturité ou de standardisation des solutions post-quantiques existantes. Cette immaturité n'est toutefois « que transitoire et ne devrait pas servir de prétexte à l'inaction », alertait l'Anssi dans un rapport publié en octobre 2024. Certaines actions devront être mises en oeuvre sans délai et d'autres pourront « être déployées progressivement, dans les années à venir », précisait alors l'agence.

« Certains n'ont pas commencé la migration, mais ils vont devoir s'y mettre assez rapidement car les temps de migration sont longs, et les régulations commencent à apparaître », confirme Pierre Jaeger, directeur technique chez IBM chargé d'établir des partenariats stratégiques liés aux technologies quantiques. Le géant de la tech, qui a participé au codéveloppement de ces nouveaux algorithmes de chiffrement, accompagne plusieurs acteurs financiers dans ce processus - principalement des banques de détail, des assureurs et des gestionnaires d'actifs.

Travail titanesque

Le travail d'évaluation préalable à la migration est à lui seul déjà titanesque, en particulier pour un grand établissement bancaire, « à l'échelle duquel la cryptographie est partout », commente Thomas Hutin, responsable cybersécurité chez FTI Consulting. « L'essentiel est d'avoir déjà un plan interne. Ça va être une vague, il faut partir au bon moment pour ne pas la prendre sur la tête. »

Si se prémunir des risques associés au quantique est un enjeu crucial, cette rupture technologique est aussi « porteuse de promesses » pour le secteur, rappelle Valérie Fasquelle. Par leur capacité à traiter de gigantesques masses de données en un clin d'oeil, les ordinateurs quantiques pourraient aider à réaliser des analyses prédictives ultra-rapides pour anticiper les tendances de marché, optimiser les portefeuilles d'investissement ou encore la gestion des risques, notamment en association avec l'intelligence artificielle.

La Banque de France teste la cryptographie post-quantique

La Banque de France a mené diverses initiatives destinées à évaluer l'efficacité des algorithmes résistants au quantique. En novembre, l'institution a annoncé le succès d'une expérience menée avec l'Autorité monétaire de Singapour reposant sur l'utilisation de cryptographie post-quantique pour la signature et le chiffrement d'e-mails. Le superviseur travaille par ailleurs avec le groupe Allianz à la mise en oeuvre d'un canal sécurisé pour le transfert de documents statistiques ou prudentiels. La Banque de France entend élargir ce type d'initiative à d'autres entreprises du secteur en 2025.

Rachel Cotte