

Cryptographie post-quantique

*Les organisations ne peuvent plus
attendre pour migrer*

L'informatique quantique constitue désormais une **menace identifiée** pour la sécurité des systèmes d'information, à laquelle le secteur financier est particulièrement exposé. Entre 2024 et 2026, trois évolutions ont transformé un sujet de veille technologique en obligation de gouvernance : la finalisation par le NIST américain des premiers standards de cryptographie post-quantique, l'annonce d'un calendrier contraignant par l'ANSSI, et l'entrée en application de deux règlements européens, NIS 2 et DORA, qui engagent désormais la responsabilité personnelle des dirigeants sur ce sujet.

Un risque déjà engagé, avant même l'existence de l'ordinateur quantique

Afin de rendre le risque quantique tangible et de l'ancrer dans une hypothèse réaliste, le cas de CYBank, une banque fictive représentative des pratiques actuelles du secteur, servira de référence. Son architecture fera office de fil rouge pour comprendre où se trouvent les dépendances cryptographiques et comment organiser leur transition.

CYBank chiffre les échanges avec ses clients, authentifie ses services et signe ses mises à jour au moyen de mécanismes éprouvés : TLS 1.3 avec ECDHE, certificats RSA et signatures numériques. À ce jour, ces protections ne présentent aucune faiblesse apparente : elles sont robustes face aux attaques classiques et correspondent à un standard de sécurité solide.

Cette absence de signal explique en grande partie pourquoi la menace reste difficile à percevoir. Un acteur malveillant peut aujourd'hui intercepter et conserver des flux chiffrés de CYBank sans chercher à les déchiffrer immédiatement. Cette stratégie, connue sous le nom de **Store Now, Decrypt Later** (ou Harvest Now, Decrypt Later), consiste à collecter des données chiffrées dans l'attente qu'un ordinateur quantique suffisamment puissant permette, dans plusieurs années, de les déchiffrer rétroactivement.

L'évaluation de ce risque repose sur un cadre d'analyse simple, connu sous le nom de **théorème de Mosca**, qui met en regard trois durées :

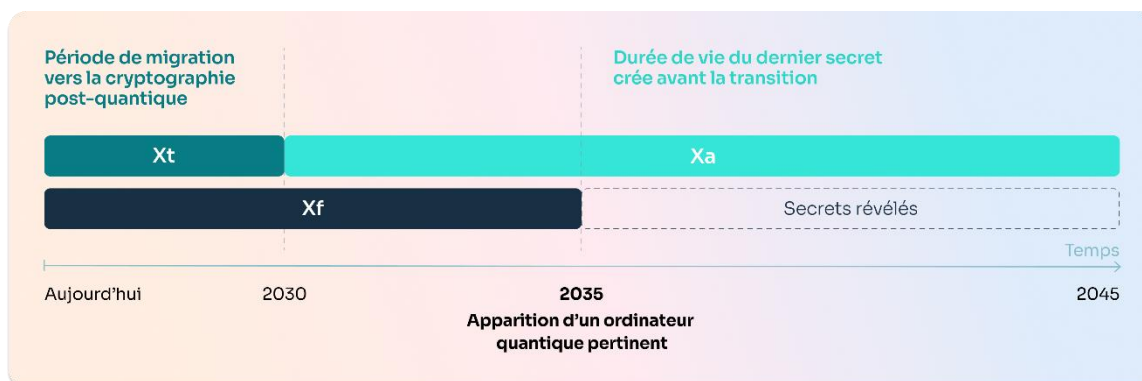
Xa, la durée pendant laquelle les données doivent rester confidentielles. Pour une institution financière, cette durée concerne notamment les dossiers de

crédit, les informations patrimoniales ou les données contractuelles, dont la protection s'étend généralement sur quinze à vingt ans ;

Xt, le temps nécessaire à la migration complète d'une infrastructure cryptographique vers des mécanismes post-quantiques, estimé entre trois et cinq ans pour un système d'information de la taille d'une banque de réseau ;

Xf, l'horizon estimé d'apparition d'un ordinateur quantique cryptographiquement pertinent, c'est-à-dire capable de compromettre la cryptographie asymétrique actuelle. Les estimations de l'industrie situent aujourd'hui cet horizon autour de 2035.

Le théorème établit une règle de décision claire : dès lors que **Xa + Xt dépasse Xf**, l'organisation est déjà exposée, indépendamment de l'existence effective de l'ordinateur quantique. Appliqué à CYBank, ce calcul est défavorable : quinze à vingt ans de confidentialité requise, additionnés à trois à cinq ans de migration, excèdent largement la dizaine d'années qui sépare aujourd'hui de l'horizon 2035. Les données que CYBank chiffre actuellement pourraient donc devenir lisibles avant même la fin de leur durée de vie contractuelle si elles sont interceptées dès aujourd'hui. L'exposition au risque quantique ne débute pas à la mise en service de l'ordinateur quantique, mais dès l'instant où cette équation cesse d'être favorable.



Des fondations cryptographiques structurellement remises en cause

La sécurité de la cryptographie asymétrique utilisée par CYBank, comme par la quasi-totalité des institutions financières, repose sur des problèmes mathématiques dont la résolution exige, avec des moyens de calcul classiques, des durées considérables : **la factorisation de grands nombres**, sur laquelle repose **RSA**, et le **logarithme discret sur courbes elliptiques**, sur lequel reposent **ECDHE** et **ECDSA**. Ces problèmes ne sont pas insolubles en théorie ; ils requièrent simplement, avec les moyens de calcul classiques, un temps de résolution qui excède largement l'échelle utile d'une attaque.

Un ordinateur quantique manipule des qubits, des unités de calcul qui, à la différence des bits classiques limités à 0 ou 1, peuvent représenter une combinaison de ces deux états. Cette propriété permet à certains algorithmes quantiques de traiter des structures mathématiques d'une manière inaccessible aux ordinateurs conventionnels. L'algorithme de Shor exploite ces propriétés pour identifier rapidement les régularités mathématiques cachées dans la factorisation et le logarithme discret, et de résoudre ces problèmes **en un temps radicalement réduit**.

Pour une architecture telle que celle de CYBank, cette évolution emporte deux conséquences distinctes.

- 1- La première concerne la **confidentialité** des échanges : dans un échange ECDHE, le client et le serveur publient des informations permettant de construire une clé secrète commune, sans jamais transmettre cette clé sur le réseau. Un attaquant classique observant cet échange ne peut pas en reconstituer le secret ; un attaquant disposant d'un ordinateur quantique suffisamment puissant pourrait, en revanche, exploiter ces mêmes informations publiques pour reconstruire ce secret, y compris plusieurs années après l'interception.
- 2- La seconde conséquence concerne l'**authenticité** : RSA et ECDSA servent à signer les certificats, les mises à jour logicielles et à authentifier les systèmes ; leur compromission future ouvrirait la voie à la falsification de signatures et à l'usurpation d'identité numérique.

Cette perspective n'est plus seulement théorique : IBM a déjà présenté Condor, un processeur de 1 121 qubits physiques, et poursuit une feuille de route visant un ordinateur quantique pratique, doté d'environ 200 qubits logiques, en 2029. Toutefois, les machines actuelles restent très éloignées

d'un ordinateur quantique tolérant aux pannes capables de compromettre, en pratique, RSA-2048 ou les cryptographies à courbes elliptiques. La correction d'erreurs impose un surcoût majeur : les approches conventionnelles peuvent nécessiter plus de 1 000 qubits physiques par qubit logique, et certaines estimations pour RSA-2048 atteignent 20 millions de qubits physiques. Les échéances restent donc très incertaines ; une enquête d'experts rapportée en 2024 plaçait à 50 % la probabilité qu'une telle capacité soit atteinte d'ici 2040.

Si les feuilles de route industrielles ne doivent pas être interprétées comme une prévision certaine, elles confirment néanmoins que le risque ne peut plus être traité comme un scénario lointain ou purement spéculatif. Dès lors que l'exposition de CYBank a déjà commencé au sens du théorème de Mosca, une vigilance active et l'engagement progressif de la transition post-quantique se justifient davantage qu'une posture d'attente.

La cryptographie symétrique n'est pas affectée de la même manière. L'algorithme quantique de Grover permet en théorie d'accélérer la recherche exhaustive d'une clé, mais son effet se traduit essentiellement par une réduction de la marge de sécurité, l'équivalent d'une clé de 256 bits se comportant alors comme une clé de 128 bits, ce qui demeure largement suffisant au regard des capacités de calcul envisageables. Pour CYBank, cette distinction est déterminante : la migration ne consiste pas à remplacer indistinctement l'ensemble des mécanismes cryptographiques, mais à cibler **ceux qui reposent sur la factorisation et le logarithme discret**, à savoir l'établissement de clés, les signatures numériques et l'infrastructure de gestion des certificats (PKI).

Un cadre réglementaire qui transforme un choix technique en obligation de gouvernance

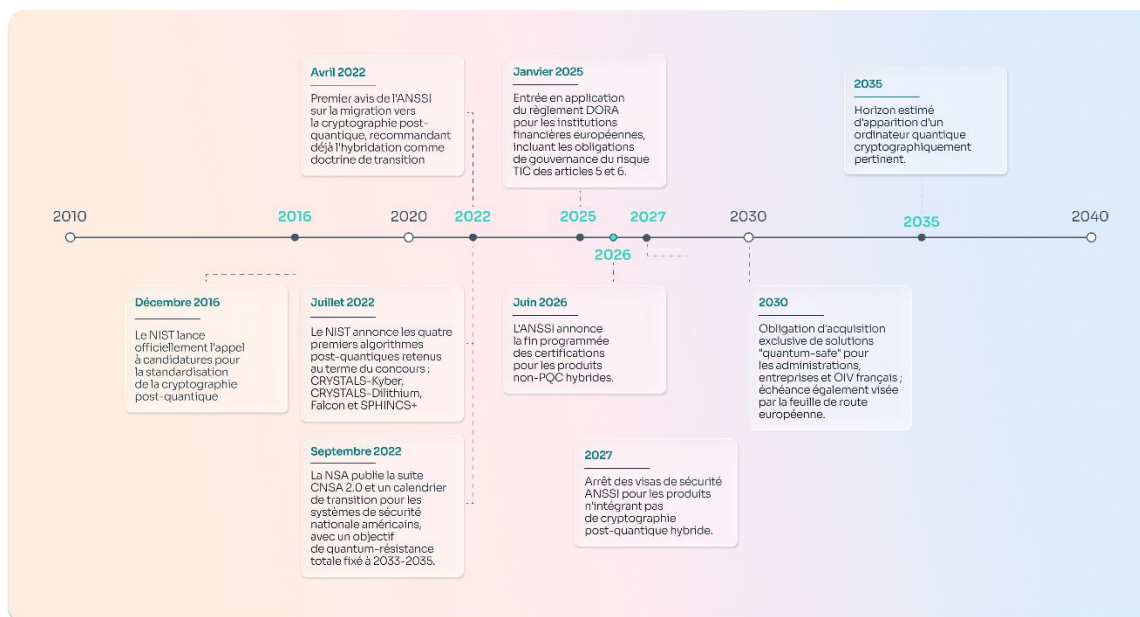
Jusqu'à récemment, la migration post-quantique demeurait une question de planification technique, à traiter selon un calendrier propre à chaque organisation. Trois évolutions récentes ont modifié cette donne.

La première provient du **NIST**. En août 2024, l'institut américain a publié les trois premiers standards finaux de cryptographie post-quantique : FIPS 203 (**ML-KEM**, pour l'établissement de clés), FIPS 204 (**ML-DSA**, pour les signatures numériques) et FIPS 205 (**SLH-DSA**, une famille de signatures fondée sur des fonctions de hachage) ([NIST, communiqué du 13 août 2024](#)). Cette publication emporte une conséquence directe pour les régulateurs européens : les

réglementations NIS 2 et DORA exigent des entités concernées la mise en œuvre de mesures de sécurité reflétant l'« état de l'art ». Dès lors que des standards finaux existent, la cryptographie post-quantique fait juridiquement partie de cet état de l'art.

La deuxième évolution est française. Le 16 juin 2026, à l'occasion de la conférence France Quantum, l'ANSSI a annoncé la fin, à compter de 2027, de la délivrance et du renouvellement de ses certifications et visas de sécurité pour les produits de cybersécurité n'intégrant pas de cryptographie post-quantique hybride ; à compter de 2030, seules des solutions qualifiées « quantum-safe » pourront être acquises par les administrations, les entreprises et les opérateurs d'importance vitale ([ITSocial, 2026](#)). Un éditeur de pare-feu, de VPN ou de module matériel de sécurité (HSM) qui n'aura pas engagé cette adaptation d'ici 2027 perdra de facto l'accès aux marchés publics et aux appels d'offres critiques.

La troisième évolution concerne directement la gouvernance des institutions financières. Sous **NIS 2**, l'article 20 impose aux organes de direction des entités essentielles et importantes d'approuver eux-mêmes les mesures de gestion des risques cyber, d'en superviser la mise en œuvre, et prévoit qu'ils peuvent être tenus personnellement responsables en cas de manquement. Sous **DORA**, applicable spécifiquement aux institutions financières, l'article 5 dispose que l'organe de direction porte la responsabilité ultime de la gestion du risque lié aux technologies de l'information et de la communication, ce qui inclut la définition d'une stratégie de résilience numérique et le maintien de politiques garantissant la confidentialité et l'intégrité des données ; l'article 6 complète ce dispositif en exigeant la mise en place d'un cadre formel de gestion du risque TIC. Pour un conseil d'administration, l'absence d'évaluation du risque quantique ne constitue donc plus une option neutre, mais un manquement potentiel à une obligation réglementaire directe.

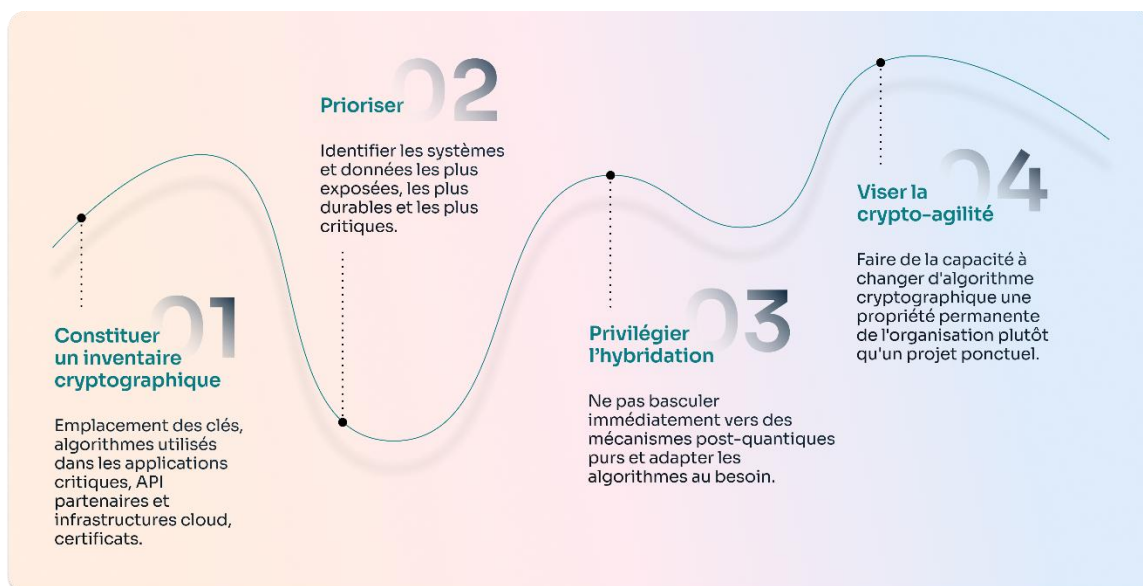


Cette exigence dépasse le seul périmètre interne des institutions financières. DORA impose également une vigilance renforcée sur les prestataires de services TIC critiques : un éditeur de VPN, un fournisseur de HSM ou un hébergeur cloud dont la feuille de route post-quantique ne serait pas documentée constituerait un point de fragilité dans la chaîne de conformité de la banque elle-même. L'audit de la maturité post-quantique des fournisseurs stratégiques constitue ainsi une extension directe de l'obligation de gouvernance portée par les articles 5 et 6 de DORA.

Ce virage réglementaire s'inscrit dans les enjeux plus larges de résilience opérationnelle et de conformité que Sia accompagne auprès des institutions financières, au titre de ses activités [Compliance & Regulations](#) et [Cybersecurity & AI Trust](#).

Une feuille de route de migration : de l'inventaire à la crypto-agilité

La migration post-quantique ne consiste pas à substituer un algorithme à un autre. Elle s'organise généralement en quatre étapes, sur une période de dix-huit à trente-six mois pour une infrastructure de la taille d'une banque de réseau.



Première étape : Constituer un inventaire cryptographique (CBOM). Cet inventaire recense l'emplacement des clés, les algorithmes utilisés dans les applications critiques, les API partenaires et les infrastructures cloud, ainsi que les certificats protégeant les liaisons réseau. Il constitue le préalable indispensable à toute décision de priorisation.

Deuxième étape : Prioriser les systèmes selon leur exposition au risque. L'ensemble des systèmes ne présente pas le même niveau d'urgence face à la menace *Store Now, Decrypt Later*. Les connexions externes durables et les données à forte valeur de confidentialité, telles que les liens interbancaires, les informations patrimoniales ou les dossiers de crédit, doivent être traitées en priorité, avant les processus d'authentification à durée de vie moyenne, puis les sessions à courte durée de vie, dont l'exposition est structurellement plus faible.

Troisième étape : Privilégier l'hybridation plutôt qu'un remplacement direct. L'ANSSI, comme l'ENISA et le BSI allemand, recommande de **ne pas basculer immédiatement** vers des mécanismes post-quantiques purs. Cette prudence se justifie par le caractère récent de ces algorithmes, qui n'ont pas encore été soumis à l'épreuve du temps à laquelle RSA ou AES ont résisté pendant plusieurs décennies. L'histoire récente de la cryptographie illustre la pertinence de cette approche : en 2022, le schéma de signature post-quantique candidat Rainbow, alors finaliste du processus de standardisation du NIST, a fait l'objet d'une attaque de récupération de clé privée réalisable en un week-end sur un ordinateur portable pour son jeu de paramètres de sécurité le plus faible.

L'hybridation consiste à combiner un mécanisme classique éprouvé, tel qu'ECDHE, avec un mécanisme post-quantique tel que **ML-KEM**, de sorte que la sécurité de la session demeure garantie tant que l'un au moins des deux mécanismes reste non compromis. Le même principe peut s'appliquer aux signatures, en associant temporairement une signature classique et une signature post-quantique telle que ML-DSA.

Au-delà de ML-KEM et ML-DSA, qui constituent les choix les plus généralistes, d'autres familles répondent à des besoins spécifiques. **FrodoKEM** privilégie une approche mathématiquement plus conservatrice, au prix de clés plus volumineuses. **HQC**, fondé sur les codes correcteurs d'erreurs plutôt que sur les réseaux euclidiens, permet de diversifier les hypothèses mathématiques sur lesquelles repose la sécurité globale. Du côté des signatures, **Falcon** offre une compacité intéressante pour les environnements contraints en bande passante, tandis que **SLH-DSA**, fondé sur des fonctions de hachage, constitue une option pour les usages exigeant une forte diversification, tels que la signature de composants racines. Ce choix relève d'un **arbitrage multicritère entre taille des clés, performance de calcul et niveau de maturité de chaque famille mathématique**, à traiter conjointement par les équipes cryptographie, architecture et gestion des risques.

Quatrième étape : viser la crypto-agilité comme objectif d'architecture durable. Les standards post-quantiques continueront d'évoluer, et une organisation incapable de modifier rapidement ses algorithmes restera vulnérable à chaque nouvelle avancée cryptanalytique. La conception d'architectures modulaires, permettant un changement de mécanisme cryptographique par simple mise à jour plutôt que par refonte complète, constitue l'investissement le plus pérenne pour CYBank comme pour toute institution financière.

Cette transition ne se limite pas à un choix d'algorithmes : elle emporte des conséquences opérationnelles concrètes à anticiper dans la planification. Les mécanismes post-quantiques reposent sur des structures mathématiques nettement plus volumineuses que leurs équivalents classiques ; une clé publique ML-KEM ou une signature ML-DSA occupe ainsi plusieurs fois l'espace d'une clé RSA ou d'une signature ECDSA. Cette différence de volume a **des implications techniques directes** : elle augmente la taille des paquets échangés lors de l'établissement d'une connexion TLS, ce qui peut saturer les mémoires tampons de certains équipements réseau anciens, et elle pèse particulièrement sur les terminaux aux ressources limitées, tels que les distributeurs automatiques, les terminaux de paiement ou les objets

connectés déployés à grande échelle par les banques. Falcon, en raison de la compacité de ses signatures, est parfois envisagé pour ces cas d'usage contraints ; son implémentation repose toutefois sur des calculs d'échantillonnage complexes, plus difficiles à sécuriser contre les attaques par canaux auxiliaires, ce qui en fait un candidat à réserver à des équipes disposant d'une expertise cryptographique avancée plutôt qu'un remplacement systématique.

Pour un RSSI, cette exigence doit dès aujourd'hui figurer dans tout cahier des charges ou revue d'architecture : la capacité de crypto-agilité d'un système ou d'un fournisseur devient un critère de sécurité à part entière, au même titre que les critères existants.

Enseignements et décisions à prendre sur la transition post-quantique

La trajectoire de CYBank dépasse le cas d'une seule institution et met en évidence **trois enseignements transposables à toute entreprise** :

Le risque quantique se mesure en durée de confidentialité des données, non en date d'apparition d'un ordinateur quantique. Dès lors qu'une donnée doit rester protégée plus longtemps qu'il ne reste de temps avant l'horizon de menace estimé, l'exposition est déjà réelle.

La migration ne se réduit pas au remplacement d'un algorithme. L'établissement de clés, les signatures numériques, l'infrastructure de gestion des certificats et le chiffrement symétrique répondent à des logiques différentes, et appellent des traitements différenciés plutôt qu'un remplacement uniforme.

L'hybridation et la crypto-agilité constituent un nouveau standard de prudence, non des mesures transitoires. Elles permettent de bénéficier progressivement des propriétés post-quantiques sans abandonner immédiatement des mécanismes classiques éprouvés, tout en conservant la capacité de s'adapter aux prochaines évolutions cryptographiques sans nouvelle refonte complète.

Sur cette base, **quatre décisions** s'imposent aux directions de la cybersécurité et aux comités de direction des institutions financières :

- 1- Lancer un inventaire cryptographique de l'écosystème, y compris auprès des prestataires tiers ;
- 2- Formaliser une politique de transition budgétée, soumise à l'approbation du conseil d'administration ;
- 3- Auditer la maturité post-quantique des fournisseurs stratégiques d'ici 2027 ;
- 4- Intégrer la crypto-agilité comme principe de conception dans tout nouveau projet d'architecture.

La transition post-quantique est un projet d'ampleur, mais aussi une occasion rare de moderniser en profondeur son architecture de sécurité. Les institutions qui l'abordent avec méthode en sortiront non seulement protégées, mais mieux outillées pour les prochaines ruptures technologiques.

Optimists for change

Sia est un groupe international de conseil en management de nouvelle génération, fondé en 1999. Nés à l'ère du digital, nous sommes augmentés par la data, enrichis par la créativité et guidés par la responsabilité. Nous collaborons avec nos clients pour relever les défis et saisir les opportunités. Dans un monde en pleine mutation, nous croyons que l'optimisme est un puissant levier de transformation. Avec une expertise couvrant un large éventail de secteurs et de services, nos 3 000 consultants accompagnent des clients dans le monde entier, depuis 48 bureaux répartis dans 19 pays. Notre expertise produit des résultats concrets. Notre optimisme change la donne.