NOTE STRATEGIQUE 2025

CRYPTO POST QUANTIQUE : LA TRANSITION S'ACCÉLÈRE.

THEGREENBOW

LA TRANSITION S'ACCÉLÈRE : LE TEMPS EST À L'ACTION

« On ne parle pas du tout assez de l'ordinateur quantique, ou de la menace quantique. [...] On ne sait ni quand, ni si ça va se produire, mais le jour où ça se produira, ça sera la première vraie révolution technologique dans le champ de la cybersécurité. » soulignait **Vincent Strubel, Directeur général de l'ANSSI** fin 2024.

« Dans le domaine défensif de la cryptographie résistante au quantique, pour le moment, c'est une nouvelle fois l'Amérique qui ouvre la voie en déterminant les premiers standards d'algorithmes résistants au quantique. Bien que les chercheurs et industriels européens soient très impliqués dans la recherche et la mise au point de ces nouveaux algorithmes, c'est bien l'organisme de normalisation américain (le NIST) qui les sélectionne et définit les standards. De son côté, la Chine vient d'annoncer qu'elle lançait également une initiative ambitieuse pour développer ses propres standards. Cette décision découle d'un manque de confiance mais également d'une volonté affirmée d'assurer son indépendance technologique dans un domaine qu'elle considère comme capital pour sa sécurité nationale et sa souveraineté.

Face à cette dynamique mondiale, l'Europe doit s'appuyer sur ses forces et prendre son indépendance numérique. Ne plus subir, ne plus être tributaire, mais imposer nos propres standards, encourager nos champions technologiques et faire de la cybersécurité un pilier de notre souveraineté. L'heure n'est plus aux constats : nous devons agir dès maintenant, à tous les niveaux – politique, industriel et technologique – pour garantir un avenir numérique sécurisé et autonome pour l'Europe. »

Mathieu Isaïa
Directeur général TheGreenBow

CHAPITRE I

OÙ EN EST LA RÉVOLUTION QUANTIQUE ?

La révolution quantique en cours repose sur des progrès majeurs en physique, en ingénierie et en informatique. Ces avancées sont principalement liées à la supraconductivité, aux pièges à ions et aux circuits photoniques, qui permettent aujourd'hui la construction de processeurs quantiques de plus en plus puissants.
En 2019, Google a revendiqué la suprématie quantique en exécutant en 200 secondes un calcul qui aurait pris des milliers d'années à un superordinateur classique. D'autres acteurs, tels qu'IBM, ont contesté cette affirmation, mais l'événement a marqué un tournant. Depuis, des progrès considérables ont été réalisés. IBM travaille actuellement sur son Q System Two avec un processeur Heron à 133 qubits qui sera porté à 156 avec l'idée d'en coupler plusieurs pour augmenter le nombre de qubits.[1] Ces avancées confirment que l'augmentation du nombre de qubits et la réduction des taux d'erreur sont au cœur de la course technologique. **D'ici 2026, le nombre de bits quantiques (qubits) devrait être multiplié par dix par rapport aux quelques 400 qubits atteints fin 2022, ce qui augmentera considérablement la capacité de traitement des ordinateurs quantiques et leur permettra de résoudre des problèmes de plus en plus complexes.** [2]

Parallèlement, les circuits photoniques quantiques suscitent un intérêt croissant pour leur capacité à surmonter certaines limitations des qubits supraconducteurs, notamment en matière de stabilité et de connectivité à grande échelle. Des entreprises comme Xanadu (Canada) et PsiQuantum (USA) misent sur cette approche pour dépasser la barre du million de qubits fonctionnels d'ici la fin de la décennie.

Un autre domaine clé est le quantum annealing ou recuit quantique, notamment exploré par D-Wave (USA), PartyQC (Autriche), qui vise des applications spécifiques en optimisation. Bien que ce type de machine quantique ne soit pas universel, il apporte déjà des solutions pour des problèmes concrets en finance, logistique et intelligence artificielle.

Au cours des deux dernières années, les fonds de capital-risque ont investi 3,5 milliards de dollars dans le développement du quantique à travers le monde.

Plusieurs programmes européens sont à l'œuvre :

- EuroQCI (European Quantum Communication Infrastructure) : Développement d'un réseau de communication quantique sécurisé intégrant PQC et distribution quantique de clés (QKD).
- Horizon Europe & Quantum Flagship : Financement de projets de recherche et développement sur la cybersécurité post-quantique.
- Collaboration entre institutions et entreprises européennes (Thales, Eviden, Cryptonext, Pasqal, Genci) pour favoriser l'industrialisation des solutions PQC.

La France pour rappel s'est dotée en 2021 d'une stratégie nationale quantique reposant sur un engagement global public-privé de 1,8 Md€, sur quatre ans, dont 1Md€ financé par l'État.
Elle s'appuie sur 5 objectifs :

- Développer les technologies et usages du calcul quantique
- Maîtriser les technologies de capteurs quantiques
- Développer et diffuser la cryptographie post-quantique
- Développer les technologies de communications quantiques
- Maîtriser les technologies habilitantes du quantique

D'après les estimations du gouvernement français, les start-up quantiques ont levé plus de 350 millions d'euros, ce qui fait de la France le premier pays européen en termes de levées de fonds et le troisième au niveau mondial derrière les Etats-Unis et le Canada.[3] La France compte aussi des pôles de recherche régionaux : NaQuiDis, hub d'innovation quantique de la région Nouvelle Aquitaine, qui associe des centres de recherche et des pôles de compétitivé, l'Institut Quantique Occitan à Toulouse, aQCess («Atomic quantum computing as a service – aQCess»), une plateforme publique en physique quantique à Strasbourg, ou encore la Fédération QuantAlps à Grenoble. La Plateforme nationale de calcul quantique hybride HQI (HPC Quantum Initiative) » ou encore l'International Research Network (IRN) franco-canadien en sciences et technologies quantiques impulsé par le CNRS lancé en janvier 2023.
Le Gouvernement a lancé en 2024 le programme PROQCIMA.
L'objectif : disposer en 2032 d'au moins deux prototypes d'ordinateurs quantiques universels avec 128 qubits logiques étendus à 2048 qubits logiques en 2035.

1. Understanding Quantum Technologies 2024
2. https://www.thalesgroup.com/fr/monde/identite-et-securite-numeriques/press_release/consortium-europeen-lance-le-projet-pqc4emrtd
3. https://www.info.gouv.fr/upload/media/content/0001/09/d6afa78052f-892351fa83b14dd66344d26f03e7a.pdf

LA CRYPTOGRAPHIE POST-QUANTIQUE : ANTICIPER LA MENACE QUANTIQUE

L'une des conséquences les plus critiques de la révolution quantique concerne la sécurité de l'information. L'informatique quantique menace les algorithmes de cryptographie asymétrique actuels (RSA, ECC, Diffie-Hellman), qui reposent sur des problèmes mathématiques complexes facilement résolus par un ordinateur quantique suffisamment puissant. Le jour où un ordinateur quantique disposera des capacités de calcul nécessaire pour casser les systèmes de cryptographie actuels, autrement dit quand il sera capable de jouer avec succès l'algorithme de Shor, est surnommé le « Q-Day ». Ce jour représente une menace existentielle pour la sécurité nationale, ainsi que pour le système financier mondial ; le Hudson Institute estimant que les dommages pourraient s'élever à 2 000 milliards de dollars.

Alors que 73 % des entreprises reconnaissent que l'informatique quantique représente une menace pour la cryptographie traditionnelle, 61 % n'ont pas encore défini de stratégie dans un monde post-quantique.[4]

L'algorithme de Shor, démontré théoriquement en 1994, est capable de factoriser des grands nombres de manière exponentiellement plus rapide qu'un ordinateur classique, mettant en péril la majorité des infrastructures de cybersécurité actuelles. **Même si les ordinateurs quantiques n'ont pas encore atteint cette capacité, il est impératif d'anticiper cette menace avec la cryptographie post-quantique (PQC).**

Dès 2023, l'European Policy Center a rédigé un document appelant l'Union européenne à adopter un plan d'action coordonnée pour se préparer aux cyberattaques basées sur le quantique. Face à ce risque, le NIST (National Institute of Standards and Technology) a lancé en 2016 un concours visant à standardiser de nouveaux algorithmes résistants aux attaques quantiques. En 2022, quatre finalistes ont été sélectionnés, CRYSTAL-Kyber, conçu pour le chiffrement, ainsi que CRYSTAL-Dilithium, Falcon et SPHINCS+, destinés à vérifier les signatures numériques. Aujourd'hui, trois des quatre algorithmes sont officiellement finalisés dans le cadre des normes PQC du NIST. En 2023, la US National Cybersecurity Strategy a fait de la protection contre les cyberattaques quantiques un objectif stratégique.

Cette priorité englobe l'utilisation du chiffrement post-quantique et la nécessité de remplacer le matériel, les logiciels et les applications vulnérables qui pourraient être compromis.
Mais ce n'est pas terminé. Le concours se poursuit pour ce qui est de l'échange de clés. Pour les signatures électroniques un autre concours a été ouvert pour amener de la diversité. Là est tout l'enjeu pour ces algorithmes. « *Les algorithmes auxquels s'intéressent la France et le BSI notamment ne sont pas forcément ceux retenus par le NIST. La Chine vient de lancer son propre concours. Ils préfèrent développer leurs propres standards parce qu'ils redoutent les backdoors et doutent de la fiabilité.* » soutient Arnaud Dufournet, TheGreenBow.

> *« L'informatique quantique peut constituer une menace pour la cryptographie classique, mais elle nous donne également la possibilité de créer des formes fondamentalement nouvelles de communication sécurisée »*[5]
>
> **Frédéric Jacquet, AI & Ethics, Digital Experience, Advanced technologies & Quantum Computing**

4. https://www.thalesgroup.com/fr/monde/securite/press_release/thales-et-quantinuum-lancent-kit-entreprises-se-preparer-aux#:~:text=Alors%20que%2073%20%25%20des%20entreprises,à%20répondre%20à%20cette%20menace.
5. https://www.linkedin.com/pulse/securing-future-role-post-quantum-cryptography-frederic-jacquet-ienyf/

CHAPITRE II

SÉCURITÉ DE L'INFORMATION ET QUANTIQUE : COMMENT S'ADAPTER ?

La révolution quantique impacte la sécurité de l'information sous plusieurs angles :

1. Menace sur la cryptographie actuelle : toute donnée chiffrée aujourd'hui avec RSA ou ECC (Elliptic Curve Cryptography) et Diffie-Hellman pourra être déchiffrée dans le futur lorsqu'un ordinateur quantique sera opérationnel. Le phénomène du « Harvest Now, Decrypt Later » (« stocker maintenant et décrypter plus tard ») notamment pousse les organisations à protéger dès maintenant leurs données sensibles avec des solutions résistantes aux attaques quantiques.

2. Développement de la cryptographie post-quantique : la cryptographie post-quantique (PQC, Post-Quantum Cryptography) se développe afin de proposer des alternatives robustes aux attaques quantiques. Ces méthodes, basées sur des problèmes mathématiques réputés résistants aux capacités des ordinateurs quantiques, sont au cœur de divers efforts de normalisation à l'échelle mondiale.

3. Développement de la cryptographie quantique : contrairement à la PQC qui reste basée sur des principes mathématiques, la cryptographie quantique utilise directement les propriétés de la physique quantique pour sécuriser les communications. Le quantum key distribution (QKD), illustré par le protocole BB84, permet d'échanger des clés cryptographiques avec une sécurité théoriquement inviolable grâce au principe d'intrication théorisé par Einstein et Schrödinger et d'indétermination de Heisenberg. Des entreprises et des programmes gouvernementaux développent déjà des réseaux QKD fonctionnels.

4. Normes et régulations : Le NIST et l'ISO travaillent sur l'intégration des algorithmes post-quantiques dans les infrastructures critiques. Des avancées majeures ont eu lieu en 2024. L'Union européenne et les États-Unis accélèrent également leurs efforts en matière de cybersécurité quantique pour garantir une transition sécurisée.

I. Le processus de standardisation du NIST

En août 2023, le NIST a publié un projet de norme pour Kyber, Dilithium, Falcon et SPHINCS+, et une quatrième phase a été ouverte pour évaluer d'autres candidats, notamment pour des alternatives en chiffrement à base de codes et de multivariés. Parallèlement au NIST, plusieurs organisations travaillent sur l'intégration de la PQC dans leurs propres standards : l'ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) travaille à intégrer la cryptographie post-quantique dans ses normes de sécurité, notamment ISO/IEC 18033 (chiffrement) et ISO/IEC 14888 (signature numérique). L'IETF (Internet Engineering Task Force) mène plusieurs initiatives pour adapter les protocoles de communication à la PQC, notamment avec le projet PQ-TLS pour les communications sécurisées (TLS 1.3 post-quantique) et l'adoption de schémas hybrides combinant PQC et algorithmes classiques. La NSA (National Security Agency, États-Unis) a publié des recommandations dans le cadre du programme CNSA 2.0 (Commercial National Security Algorithm Suite), incitant à l'adoption de la cryptographie post-quantique pour la protection des données classifiées. Le NCCoE (National Cybersecurity Center of Excellence, États-Unis) développe un projet pour aider les entreprises à migrer vers la cryptographie post-quantique, en proposant des guides pratiques et des implémentations de référence. L'ANSSI (Agence nationale de la sécurité des systèmes d'information, France) suit de près les recommandations du NIST et de l'ISO tout en menant des recherches indépendantes sur la résilience des algorithmes post-quantiques.
D'ici fin 2025, le NIST devrait finaliser les versions officielles des standards PQC.

Cette période sera marquée par :

- L'intégration des algorithmes sélectionnés dans les principales normes internationales (ISO/IEC, IETF, ETSI, ANSSI, etc.).
- L'adoption progressive par les entreprises et les gouvernements, notamment via des solutions hybrides combinant PQC et cryptographie classique.
- Le développement de matériels optimisés pour exécuter efficacement les nouveaux algorithmes, notamment dans les cartes à puce, les modules HSM (Hardware Security Modules) et les infrastructures de clés publiques (PKI).
- Les premières mises en production dans des infrastructures critiques, notamment les services bancaires, les communications gouvernementales et les réseaux d'énergie.

II. De l'importance de la diversité des algorithmes

L'objectif de la diversité dans les algorithmes de PQC est d'assurer une sécurité robuste et pérenne face aux différentes menaces, qu'elles soient classiques ou quantiques. Cette diversité permet d'atténuer le risque d'une vulnérabilité unique, d'assurer une flexibilité et une adaptation aux cas d'usage. En diversifiant les bases mathématiques des algorithmes post-quantiques, on réduit le risque qu'une vulnérabilité unique entraîne un effondrement généralisé de la sécurité. La diversité permet donc de sélectionner les algorithmes les plus adaptés à chaque besoin, plutôt que d'imposer une solution unique qui ne conviendrait pas à tous les environnements.

Il s'agit aussi d'éviter une centralisation excessive de la sécurité. Si un seul standard cryptographique était adopté mondialement, une attaque réussie contre cet algorithme pourrait avoir des conséquences catastrophiques. En favorisant une diversité d'algorithmes, on encourage une approche redondante et résiliente, où plusieurs solutions coexistent et peuvent servir d'alternative en cas de vulnérabilité détectée. Cela permet de faciliter la transition hybride. La transition vers la cryptographie post-quantique ne sera pas immédiate pour tout le monde. Dans l'intervalle, de nombreuses solutions adoptent des approches hybrides, combinant des algorithmes classiques et post-quantiques pour assurer une double protection.

III. L'hybridation pour une transition en douceur

L'approche hybride consiste à combiner des algorithmes cryptographiques classiques avec des algorithmes post-quantiques afin d'assurer une sécurité robuste pendant la transition. Cette méthode garantit la protection des systèmes critiques tout en permettant une adoption progressive des nouvelles normes.

En France, l'approche prudente de l'ANSSI. En attendant la finalisation des normes, l'agence recommande une approche progressive et encourage le développement de solutions hybrides associant un algorithme classique éprouvé (comme RSA ou ECC) et un algorithme post-quantique standardisé (Kyber, Dilithium, etc.) ou en cours de standardisation (FrodoKEM) entre 2025 et 2030, puis une mise en œuvre complète de la PQC d'ici 2030.

En Europe, l'ENISA (European Union Agency for Cybersecurity) recommande l'adoption de protocoles hybrides dans les infrastructures critiques européennes, des tests approfondis pour évaluer la performance et la sécurité des algorithmes PQC en combinaison avec les algorithmes actuels et une migration progressive des infrastructures de clés publiques (PKI) vers des solutions hybrides. L'UE finance également des projets de recherche sur l'implémentation de chiffrement hybride dans les communications gouvernementales et bancaires. La Commission européenne travaille à l'élaboration d'un plan stratégique européen ambitieux pour les puces quantiques, un "EU Quantum Chips Plan", qui doit être présenté avant l'été, ainsi qu'à un règlement quantique – un "Quantum Act" –, qui sera proposé avant la fin de l'année.[6]

Aux États-Unis, la NSA, le CISA (Cybersecurity and Infrastructure Security Agency) et le NIST ont adopté une stratégie plus offensive en 2023. Intitulée Quantum-Readiness: Migration to Post-Quantum Cryptography, elle annonce que les systèmes gouvernementaux et les services publics fédéraux migreront en premier, et devront être compatibles avec des algorithmes post-quantiques d'ici 2035. Elle recommande une transition hybride via son programme CNSA 2.0 (Commercial National Security Algorithm Suite). Le NIST, en parallèle de sa sélection d'algorithmes PQC, travaille avec l'IETF pour intégrer la PQC hybride dans les protocoles tels que TLS, IPsec et SSH.

> *« Le document appelle ses destinataires à commencer dès maintenant à faire un inventaire de leurs vulnérabilités PQC. Une attention particulière est portée au protocoles réseaux, serveurs, programmes et librairies associées. »*[7]
>
> **Antoine Glory, Chargé de mission pour la Science et la Technologie, Ambassade de France à Washington D.C.**

Le coût estimé de la migration des systèmes d'information prioritaires d'ici 2035 est de plus de 7 milliards de dollars.[8] Les coupes budgétaires drastiques appliquées par l'administration Trump II au CISA laisse désormais planer un doute sur la poursuite de ces travaux et de leurs avancées.

La Chine investit massivement dans la cryptographie quantique et post-quantique. Une étude menée par des chercheurs de l'université de Shanghai en 2024 affirme avoir mis au point ce qu'ils considèrent comme « la première attaque efficace contre une méthode de chiffrement très répandue », en utilisant un ordinateur quantique. *« En utilisant D-Wave, ils ont réussi à attaquer les algorithmes Present, Gift-64 et Rectangle, tous représentatifs de la structure SPN (Substitution-Permutation Network), qui fait partie des fondements de la norme de chiffrement avancée (AES) largement utilisée dans l'armée et la finance. »*[9] Si ces déclarations, dont aucune ressource scientifique ne permet de valider la véracité, s'avèrent exactes et que les algorithmes de chiffrement venaient effectivement à être cassés, toutes les industries du secteur bancaire aux échanges confidentiels sur internet, en passant par les communications militaires seraient concernées. Le gouvernement chinois a déjà imposé des tests de solutions hybrides de chiffrement dans les infrastructures critiques et travaille sur une migration accélérée pour ses services de communication sécurisée.

6.https://www.lemonde.fr/economie/article/2025/03/02/puces-quantiques-l-europe-prepare-son-quantum-act-pour-reglementer-le-secteur_6572889_3234.html
7. https://france-science.com/recommendations-autoritaires-dagences-federales-pour-le-passage-a-la-cryptographie-post-quantique
8. https://www.soprasteria.fr/perspectives/details/quest-ce-que-la-cryptographie-post-quantique
9. https://www.scmp.com/news/china/science/article/3282051/chinese-scientists-hack-military-grade-encryption-quantum-computer-paper

A. Implications et impacts de l'approche hybride : pourquoi faut-il agir maintenant ?

Si cela peut paraître prématuré, compte tenu des échéances floues et lointaines de la prégnance de l'ordinateur quantique, le temps presse pourtant déjà. D'abord, parce que la migration vers la PQC prendra plusieurs années. La cryptographie est omniprésente et la mise en œuvre de la PQC est assez complexe. La première étape, le seul inventaire des systèmes de cryptage existants pourrait prendre des mois, voire des années. La PQC doit pouvoir faire face au phénomène du « Harvest Now, Decrypt Later » (« stocker maintenant et décrypter plus tard »). Il s'agit pour les attaquants qui peuvent voler et copier des données chiffrées de les conserver et les déchiffrer plus tard, quand les ordinateurs quantiques seront suffisamment puissants.

L'adoption d'une cryptographie hybride a plusieurs conséquences sur les mesures de sécurité, les performances et l'infrastructure existante. Si l'ajout d'une couche cryptographique post-quantique augmente la résilience des systèmes, elle complexifie leur gestion. Certains algorithmes post-quantiques, comme CRYSTALS-Kyber (chiffrement basé sur les réseaux euclidiens), sont relativement efficaces mais ils nécessitent des clés de plusieurs kilobits, contre 2048 bits pour RSA. Cette augmentation a un impact sur l'efficacité du stockage, de la transmission et du calcul. Par conséquent, les organisations doivent prendre en compte les compromis entre le renforcement de la sécurité et la dégradation potentielle des performances, en particulier dans les environnements disposant de ressources informatiques limitées, tels que les appareils IoT. D'autres, comme SPHINCS+ (signature basée sur des arbres de hachage), ont un coût computationnel plus élevé.

Autre sujet, celui des problèmes de vulnérabilité et de stabilité.

> *« De nombreux algorithmes de PQC n'ont pas encore été testés de manière aussi approfondie que les algorithmes conventionnels, qui ont fait leurs preuves depuis des décennies. Ce manque d'évaluation signifie que des vulnérabilités potentielles peuvent encore exister. Un exemple notable est l'algorithme SIKE, qui était initialement considéré comme sûr contre les attaques quantiques, mais qui a ensuite été compromis à la suite de percées dans le domaine de la cryptanalyse. »*
> **Frédéric Jacquet, AI & Ethics, Digital Experience, Advanced technologies & Quantum Computing.**

L'hybridation PQ doit prendre en compte ces impacts sur la performance, notamment l'augmentation de la taille des clés et des signatures, la nécessité d'optimiser les cycles CPU (unité centrale de traitement) et l'usage de la mémoire ou encore l'adaptation des protocoles de communication pour supporter ces nouvelles charges. Les systèmes PKI, les VPN, les systèmes bancaires et les applications cloud doivent in fine être compatibles avec les solutions hybrides. Cela implique des mises à jour logicielles et matérielles, ainsi qu'une interopérabilité entre les différentes générations de cryptographie.

Face aux progrès techniques récents, il est probable que les autorités bancaires des États-Unis et d'Europe imposent des calendriers de migration vers la PQC d'ici à 2026. En France, les infrastructures gouvernementales les plus sensibles devraient aussi adopter ce calendrier. Les secteurs critiques comme l'énergie, la santé, la finance et les télécommunications adopteront progressivement ces nouvelles solutions de chiffrement entre 2027 et 2030. Wells Fargo a par exemple déposé de multiples brevets et prévoit de déployer la PQC avant 2030.[10] En attendant, elles recommandent aux banques de dresser un inventaire de leurs systèmes cryptographiques actuels et de définir une stratégie de migration vers la PQC.

10. https://www.soprasteria.fr/perspectives/details/quest-ce-que-la-cryptographie-post-quantique

B. De l'importance de la cryptoagilité

L'agilité cryptographique est une fonctionnalité d'un dispositif/système permettant de mettre à jour ce dernier pour l'exécution de mécanismes cryptographiques plus robustes, sans avoir besoin de remplacer les composants physiques du système et en assurant ainsi la continuité des activités. Cela signifie qu'il faudra mettre en place de nouveaux systèmes permettant des changements rapides et fréquents des algorithmes cryptographiques. Jusqu'à présent, il n'était nécessaire de modifier les algorithmes cryptographiques qu'à intervalles peu fréquents. Cette agilité cryptographique est désormais nécessaire, car nous ne savons pas avec certitude si les algorithmes PQC identifiés aujourd'hui résisteront au temps. Il se peut qu'il faille les changer, et lorsque ce besoin se présentera, il faudra pouvoir le faire rapidement.
Le nouveau règlement européen Cyber-Resilience Act (CRA) exige que les dispositifs de calcul personnel prennent en charge des fonctionnalités de mise à jour.

« Il faut démarrer le plus tôt possible la transition vers le post-quantique. L'intégration se veut longue et complexe. Pour le logiciel, il s'agit de repenser l'infrastructure. Pour le hardware, cela va être plus complexe. La cryptoagilité repose sur une approche de résilience qui invite à ajouter la cryptographie post quantique en complément de l'existant. Les algorithmes post quantiques sont encore récents, il peut donc y avoir des problèmes lors de l'implémentation. Nous devons gagner en maturité en ce qui concerne celle-ci. Cette transition doit donc être agile et permettre de garder un filet de sécurité. D'autant que si des changements futurs sont à opérer, il faudra pouvoir le faire rapidement. L'Union européenne conseille d'ailleurs aux États membres de tendre vers de l'hybride. La résilience en utilisant des communications quantiques doit aussi être réfléchie. Bien que cela puisse arriver dans un temps 2, là encore, il va falloir intégrer ces sujets dès à présent. »

Ludovic Perret, Professeur à l'EPITA.

Cas Concrets

Le secteur bancaire, très moteur

Dans le secteur bancaire, les régulateurs et les banques centrales travaillent depuis plusieurs années déjà sur la PQC. Les banques centrales française et allemande ont mené un projet pilote, Project Leap, qui a permis la mise en place d'un canal de communication résistant au quantique pour protéger les données financières. En 2022, la Banque de France a réalisé avec succès la mise en œuvre expérimentale d'une solution de sécurisation de communications par des algorithmes post-quantiques. Elle a consisté à mettre en œuvre, dans une chaîne opérationnelle complète, une bibliothèque d'algorithmes « quantum résistants », issus de l'appel à contributions du NIST, et à la combiner à des algorithmes actuels pour des échanges sécurisés de données.
La Banque de France a ainsi pu vérifier la capacité de ces algorithmes post-quantiques à s'intégrer dans son système d'information dans une logique hybride permettant une évolution souple vers les futurs standards de sécurisation des données.

Fin 2024, c'est avec l'Autorité Monétaire de Singapour (MAS) que la Banque de France a annoncé le succès d'une expérimentation conjointe en matière de PQC menée sur plusieurs continents, en utilisant les technologies Internet conventionnelles marquant une étape cruciale dans l'évolution de la protection des communications électroniques internationales face aux menaces en matière de cybersécurité posées par l'informatique quantique. Des algorithmes cryptographiques résistant aux technologies quantiques, à savoir CRYSTALS-Dilithium et CRYSTALS-Kyber, ont été utilisés pour la signature et le chiffrement d'e-mails. L'objectif est de maintenir le niveau de sécurité actuel des communications électroniques dans le futur, tout en conservant la compatibilité avec les normes, technologies et canaux de communication digitaux existants. Le projet a suivi une approche hybride, alliant la robustesse des algorithmes actuels à celle des algorithmes post-quantiques. Plusieurs enseignements sont partagés : la standardisation des algorithmes et bibliothèques cryptographiques PQC pour les signatures numériques et le chiffrement n'est pas suffisante. Les protocoles d'application et les normes actuelles, comme l'infrastructure à clé publique, les certificats numériques, les échanges de clés ou les e-mails sécurisés, doivent être standardisés pour intégrer les algorithmes PQC. Cela facilitera l'adoption et l'interopérabilité de la PQC. Il existe également un potentiel d'intégration de cette technologie dans les réseaux de paiement qui permettrait aux institutions financières de préparer leurs mesures de sécurité face à la menace imminente de l'informatique quantique, garantissant l'intégrité et la confidentialité à long terme des données financières sensibles.[11]

11. https://www.banque-france.fr/fr/communiques-de-presse/la-banque-de-france-et-lautorite-monetaire-de-singapour-realisent-une-experimentation-en-matiere-de

Le secteur de la Défense

Outre les technologies de l'IA et du cyber, le quantique sera au cœur des engagements des armées en 2025. Au programme du ministère : la création d'un observatoire du quantique, le développement de cette technologie au sein des trois armées et de multiples partenariats internationaux. Les technologies quantiques vont bouleverser la physionomie du champ de bataille et *« la manière de faire la guerre ». Les centrales inertielles quantiques seront dans nos sous-marins et nos Rafales et des horloges atomiques quantiques seront embarquées dans nos satellites. L'enjeu global est de « rendre l'invisible perceptible et l'imprévisible prédictible »*. Le ministère des Armées s'intéresse aux capteurs, à la cryptographie post-quantique, au calcul et aux télécommunications. L'observatoire du quantique ministériel sera doté d'une capacité de recherche et de développement orientée vers les applications de Défense. Il réunira de nombreux experts, issus aussi bien des laboratoires académiques que de la Direction générale de l'armement, des start-up ou des grandes entreprises. Le supercalculateur permettra de mettre en œuvre d'immenses opérations mathématiques, pour préserver et traiter des données confidentielles. Il assurera *« notre souveraineté sur le temps long »*.[12]

Le programme civilo-militaire Proqcima lancé en 2024 dans le cadre de France 2030 a pour objectif de construire deux ordinateurs quantiques d'ici 2032. 5 start-up sont aujourd'hui intégrées au programme. *« Il y aura différentes phases : 2024/2028, 2028/2032 et 2032/au-delà. Nous sommes actuellement dans la phase preuve de concept sur la partie hardware. En 2032, il y aura la première livraison d'un prototype par les deux start-up finalistes. Débutera ensuite une phase d'industrialisation. »* explique le ministère des Armées. Sur la question de la migration, le ministère travaille sur l'intégration dans ses programmes de la cryptographie post-quantique.

Indépendamment du concours du NIST et de ses résultats, il continue les recherches *« de son côté. Nous souhaitons avoir nos propres algorithmes et être indépendants. »* soutient l'institution.

> *« Les centrales inertielles quantiques seront dans nos sous-marins et nos Rafales et des horloges atomiques quantiques seront embarquées dans nos satellites. L'enjeu global est de « rendre l'invisible perceptible et l'imprévisible prédictible ».*
> **Sébastien Lecornu, ministre des Armées**

12. https://www.defense.gouv.fr/actualites/annee-2025-revolution-quantique-armees

IV. Passer directement à une cryptographie 100 % post-quantique : faisabilité, avantages et défis

Dans certains cas, l'hybridation n'est pas forcément recommandée et mieux vaut sauter cette étape pour aller directement sur une crypto 100 % PQC. Une migration directe permettrait d'éviter la double transition, réduisant ainsi les coûts et la complexité du processus à long terme. Certaines organisations (banques, administrations, entreprises technologiques) stockent des données qui doivent rester confidentielles pendant plusieurs décennies. Passer immédiatement à une cryptographie 100 % PQC assure une protection à long terme, notamment pour les données gouvernementales et militaires, les communications bancaires et financières, les dossiers médicaux et informations personnelles sensibles.

Bien que les algorithmes du NIST soient considérés comme robustes, ils pourraient être révisés ou améliorés dans les années à venir et enrichis par d'autres algorithmes retenus par le NIST. Adopter une cryptographie 100 % PQC dès maintenant comporte donc un risque d'obsolescence si de meilleures solutions émergent. Ces facteurs peuvent poser des problèmes d'adaptation pour les systèmes embarqués (cartes à puce, IoT), les protocoles de communication et les infrastructures existantes. Une transition complète à la PQC nécessite des mises à jour profondes des logiciels, du matériel et des infrastructures. Si une organisation passe directement à une cryptographie 100 % PQC, elle risque de perdre l'interopérabilité avec des services tiers qui n'ont pas encore migré.

Des passeports sécurisés

L'initiative PQC4eMRTD (Post-Quantum Cryptography for electronic Machine-Readable Travel Documents) financée par l'Union européenne vise à relever les défis de sécurité posés par l'essor de l'informatique quantique, en se concentrant sur la normalisation et la promotion de protocoles cryptographiques résistants aux futures menaces quantiques, pour les documents de voyage électroniques lisibles par machine (eMRTD). Ce projet est coordonné par l'Allemagne, avec plusieurs partenaires clés en France, en Espagne et en Slovénie. Il se concentrera sur la transmission des résultats de recherche sur la cryptographie post-quantique existants aux groupes de travail de normalisation internationaux afin de faciliter l'adoption des protocoles post-quantiques.

Google a déjà intégré CRYSTALS-Kyber dans Chrome, Signal a déployé un nouveau protocole (PQCXDH) qui combine l'algorithme ECC et CRYSTALS-Kyber, sur Apple le protocole PQ3 est disponible pour sa messagerie iMessage sur iOS 17.4 et macOS 14.4 (CRYSTALS-Kyber pour KEM et ECC) quand Zoom a introduit la cryptographie post quantique dans ses réunions vidéo. Toshiba Digital Solutions et KT Corporation ont démontré des communications sécurisées hybrides quantiques avec la Shinhan Bank en Corée du Sud, intégrant QKD et PQC pour renforcer la cybersécurité des réseaux financiers. NXP Semiconductors travaille sur des solutions pour protéger les appareils IoT, les véhicules et d'autres dispositifs contre les menaces posées par les ordinateurs quantiques. Ils ont contribué au développement de l'algorithme CRYSTALS-Kyber, sélectionné pour standardisation par le NIST.

The steps to quantum-safe security

1. Agility
Future-proof your cryptographic primitives - implement Quantum Resistant Algorithms (QRA)

2. Security
Guarantee forward secrecy and data integrity - Quantum Key Generation and Distribution (QKD)

3. Entropy
Get random with a genuine source of entropy - Quantum Random Number Generator (QRNG)

CHAPITRE III

QUELLE MATURITÉ DES SOLUTIONS TECHNOLOGIQUES ?

La transition vers la PQC nécessite des solutions techniques robustes pour l'intégration dans les infrastructures existantes et l'interopérabilité avec les systèmes classiques. Les entreprises et institutions impliquées dans la PQC développent des solutions pour l'implémentation logicielle et matérielle des algorithmes post-quantiques, l'intégration dans les protocoles de sécurité (TLS, IPsec, SSH, PKI, signatures numériques) et l'optimisation des performances et la réduction des coûts.

RESQUE : Une initiative européenne pour la résilience quantique

Le projet RESQUE (RESilience QUantiquE), vise d'ici à 3 ans à développer une solution de chiffrement post-quantique pour protéger les communications, les infrastructures et les réseaux des collectivités locales et des entreprises contre les futures attaques permises par les capacités d'un ordinateur quantique. Financé par le gouvernement dans le cadre de France 2030 et par l'Union européenne - Next Generation EU dans le cadre du plan France Relance, ce projet est également soutenu par Bpifrance, à hauteur de 6 millions d'euros.
Porté par Thales, TheGreenBow, CryptoExperts, CryptoNext Security, l'ANSSI et l'Institut national de recherche en sciences et technologies du numérique (Inria), le projet étudie deux cas d'usage clés :

- Un VPN (virtual private network) post-quantique hybride permettant un accès simple, sécurisé et résistant aux différents systèmes d'information des utilisateurs ;
- Un HSM (hardware security module) post-quantique haute performance apportant la sécurisation de l'ensemble et pouvant être embarqué sur d'autres produits.

Au sein du consortium, **TheGreenBow** apporte sa connaissance des technologies VPN et du développement de logiciels en cybersécurité, **CryptoExperts et CryptoNext Security** leur expertise en chiffrement et en algorithmie cryptographique standards et avancés, **Thales** son leadership en matière d'intégration des algorithmes et sa vision applicative, l'**ANSSI** fournit le cadre de la recherche et évalue les critères de validité des cas d'usage et l'Inria fait bénéficier l'ensemble des acteurs de sa recherche fondamentale en chiffrement post-quantique.

Thales : Une approche intégrée de la sécurité post-quantique

Thales dispose déjà de composants post-quantiques prêts à l'emploi ou en prototype pour les systèmes de paiement, tant au niveau front-end (cartes PQ et éléments sécurisés) qu'au niveau back-end (serveurs OTA et Cloud, HSM, serveurs de gestion des clés…). Le Major français a récemment lancé son kit Entreprises PQC (Post-Quantum Cryptography) en collaboration avec Quantinuum. Première du genre, cette offre aide les entreprises à se préparer à la cryptographie post-quantique. Le kit fournit aux entreprises un environnement de confiance pour tester des clés de chiffrement à disposition pour la PQC, renforcées pour le quantique, et comprendre les implications à venir de l'informatique quantique sur la sécurité de leur infrastructure. En utilisant les algorithmes proposés actuellement par le NIST et intégrés dans le système, les clients peuvent tester divers cas d'utilisation relatifs à la sécurité – dont des infrastructures à clé publique, la signature de code, les certificats TLS et l'IdO – puis observer l'impact de la mise en œuvre de la technologie PQC dans ces scénarios simulés en laboratoire de test, le tout sans impacter les processus opérationnels dans les environnements de production réels. Les entreprises pourront également identifier les éventuelles faiblesses dans leur déploiement du chiffrement et appliquer des modifications dans leur infrastructure informatique pour se protéger. La première option de kit Entreprises PQC disponible intègre des HSM Luna et la technologie de génération de nombres aléatoires quantiques (QRNG) de Quantinuum, permettant aux clients de s'assurer que leurs clés sont générées et stockées en toute sécurité, tout en testant les algorithmes PQC. Le kit propose un éventail de HSM Luna et Quantum Origin de Quantinuum, la seule source au monde d'entropie quantique vérifiée. Un kit Entreprises PQC pour le chiffrement réseau utilisant des dispositifs de chiffrement réseau HSE (High Speed Encryption) de Thales sera disponible ultérieurement.

Le laboratoire de cryptographie de Thales, basé à Gennevilliers, a développé l'algorithme de signature Falcon, sélectionné par le NIST américain comme l'une des normes de la cryptographie post-quantique.[13] Thales a intégré la cryptographie post-quantique dans son application mobile sécurisée « Cryptosmart by ERCOM », utilisant une SIM 5G comme coffre-fort pour la PQC. Cette approche hybride combine des mécanismes de défense pré et post-quantiques pour sécuriser les communications mobiles.[14]

Eviden (Atos) : Sécurité quantique pour l'industrie et les services critiques

Eviden, filiale d'Atos, a annoncé en avril 2023 la mise à jour de ses produits de gestion de l'identité numérique, notamment IDnomic PKI et Cryptovision Greenshield, pour les adapter à l'ère post-quantique. Ces versions sont conçues sur une architecture crypto-agile, permettant une utilisation optimale des algorithmes traditionnels et des futurs algorithmes résistants au quantique. Eviden a intégré des algorithmes de cryptographie post-quantique dans son module de sécurité matériel (HSM) Trustway Proteccio™. Cette intégration facilite une transition progressive vers des solutions de chiffrement hybrides, combinant algorithmes classiques et post-quantiques, renforçant ainsi la sécurité des infrastructures contre les menaces futures.[15] En octobre 2024, Eviden a lancé une offre de HSM en tant que service (HSMaaS) souveraine au niveau européen, basée sur son HSM Trustway Proteccio™. Cette solution supporte les algorithmes de cryptographie post-quantique, offrant un chiffrement résilient face aux avancées de l'informatique quantique, tout en répondant aux exigences de la directive NIS2.

TheGreenBow : la cryptographie post-quantique pour sécuriser les communications

TheGreenBow fournit des solutions VPN de confiance et dont l'expertise repose sur la sécurisation des communications. Premier opérateur à avoir été certifié CC EAL3+, qualifié standard et agréé DR OTAN et UE en 2013, pour son logiciel Client VPN Windows, TheGreenBow, l'acteur de référence des Clients VPN, distribue ses logiciels dans plus de 70 pays. Depuis fin 2019, TheGreenBow détient le label « Utilisé par les armées françaises » pour le produit Client VPN Windows Certifié. Ce label atteste de la mise en œuvre du logiciel par les services du ministère des Armées françaises. Face à l'évolution des menaces posées par l'informatique quantique, l'entre-

13. https://www.thalesgroup.com/fr/group/innovation/news/cyber-thales-co-developpe-le-bouclier-post-quantique?utm
14. https://www.thalesgroup.com/fr/monde/identite-et-securite-numeriques/press_release/des-appels-telephoniques-securises?utm
15. https://atos.net/fr/2023/communiques-de-presse_2023_04_05/eviden-supporte-des-algorithmes-post-quantiques-au-sein-de-son-hsm-trustway-proteccio?utm

prise a adapté ses solutions pour intégrer la cryptographie post-quantique (PQC) et garantir une transition sécurisée. Après avoir initié des tests d'intégration de la PQC dans ses solutions, notamment pour l'authentification et l'échange de clés, TheGreenBow a ajouté à son catalogue de produits un tout nouveau Client VPN résistant au quantique et destiné aux organisations qui veulent répondre à l'urgence de protection de leurs données sensibles.
L'adoption de ces nouveaux algorithmes est une étape clé pour garantir la sécurité des tunnels chiffrés dans un environnement post-quantique. Dès 2022, TheGreenBow a publié un livre blanc intitulé « Quand la cryptographie s'impose au cœur de la révolution quantique ». Ce document explore les défis posés par l'émergence des ordinateurs quantiques et souligne déjà la nécessité d'adopter des solutions de cryptographie résistantes aux attaques quantiques. TheGreenBow est membre du consortium RESQUE, coordonné par Thales. L'entreprise s'engage activement dans la sensibilisation aux enjeux de la cryptographie post-quantique.

Keyfactor : Sécurisation des infrastructures PKI et gestion des certificats

Keyfactor a introduit en 2024 le PQC Lab, une version SaaS gratuite de sa plateforme PKI, EJBCA Enterprise, préconfigurée pour émettre des certificats résistants au quantum. Cet outil permet aux organisations d'expérimenter et de se préparer à la transition vers la PQC.[16] Cette année, Keyfactor propose une solution prête à l'emploi pour déployer facilement une infrastructure PKI sans avoir à assembler, intégrer ou sécuriser les composants individuellement : EJBCA Hardware Appliance. Offrant une architecture résiliente et évolutive, cette appliance matérielle autonome permet de gérer facilement une autorité de certification (CA), une autorité d'enregistrement (RA) et une autorité de validation (VA) sans dépendre d'une solution cloud. Elle a une capacité de traitement allant de quelques milliers à plusieurs millions de certificats et répond aux problématiques d'entreprises, de toutes tailles, confrontées à des contraintes de bande passante, de connectivité ou de conformité réglementaire. Keyfactor s'engage aussi dans une démarche éducative et de sensibilisation importante. L'entreprise fournit des ressources complètes, notamment des webinaires, des livres électroniques et des guides, pour aider les organisations à comprendre et à se préparer aux défis de la PQC. Ils ont même créé une bande dessinée !

16. https://www.keyfactor.com/fr/blog/keyfactor-introduces-pqc-lab-a-post-quantum-pki-ready-in-minutes/?utm

Keyfactor collabore avec des entités comme le National Cybersecurity Center of Excellence (NCCoE) et participe à des initiatives telles que le consortium « Migration to Post-Quantum Cryptography Building Block », visant à faciliter la transition vers des infrastructures sécurisées post-quantiques.

Cryptonext Security : Un acteur de la transition vers la PQC

Cryptonext, éditeur de logiciels spécialisé dans la cryptographie résistante aux ordinateurs quantiques propose sa suite logicielle leader C-QSR « Quantum Safe Remediation Suite » comprenant sa bibliothèque de référence « Quantum Safe Library » (C-QSL) avec les dernières mises à jour des normes du NIST américain et des algorithmes de cryptographie post quantique recommandés par l'UE, ainsi qu'un ensemble complet d'outils d'intégration crypto-agile et hybrides et de connecteurs et plugins applicatifs pour les entreprises utilisatrices finales et les intégrateurs, afin de les aider dans leur migration et leurs opérations à l'ère de la sécurité post-quantique.

Politique.
Benjamin Haddad, Ministre délégué auprès du ministre de l'Europe et des Affaires étrangères, chargé de l'Europe veut « *l'allègement des procédures d'aides d'Etat pour que les entreprises du quantique puissent débloquer rapidement des fonds en phase initiale.* » Il souhaite rationaliser le règlement d'exemption par catégories (RGEC) au niveau européen, aligner les conditions d'éligibilité pour simplifier l'utilisation croisée mais aussi les modalités d'utilisation des options de coûts simplifiées (OCS) dans le cadre des fonds européens. Il appuie de fait la proposition de la Commission européenne de créer un 28e régime pour les jeunes entreprises innovantes. « *Cette mesure pourrait être la clé de voûte de la nouvelle « EU start-up and scale-up strategy » et permettrait d'accompagner les jeunes entreprises en phase de croissance.* » Il insiste sur la nécessité de rendre l'investissement européen plus attractif, rappelant que 300 milliards d'euros d'épargne privée sont actuellement investis hors d'Europe, principalement aux États-Unis. La création d'un produit d'épargne européen est une piste explorée.[17]

17. https://www.actuia.com/actualite/structurer-lecosysteme-quantique-europeen-la-vision-de-benjamin-haddad/

CHAPITRE IV

NEXT STEP : VERS UNE SÉCURITÉ ADAPTATIVE ET UN ÉCOSYSTÈME EUROPÉEN STRUCTURÉ

I. Les prochaines étapes de la PQC s'articulent autour de 4 axes stratégiques

1. Fixer un cap avec des directives et des échéances claires.

Une feuille de route nationale est essentielle.

> *« Compte tenu de l'évolution rapide que peut représenter la menace quantique, les enjeux de migrations et le temps nécessaire, il est urgent de fixer un calendrier avec des guidelines précises. Cela pourrait être conduit sous l'égide de l'ANSSI qui dispose de l'expertise, de la visibilité et de la légitimité. La dynamique à l'œuvre n'est pas suffisamment rapide. Le temps est à l'accélération. Cela permettra aussi de stimuler le marché et la maturité des solutions technologiques. »*
>
> **Ludovic Perret, Professeur à l'EPITA.**

2. Le renforcement de la crypto-agilité, indispensable pour répondre aux évolutions rapides des menaces et des standards cryptographiques.

La crypto-agilité est un des sujets clés au cœur du projet RESQUE pour permettre de trouver des solutions de mise en œuvre car la préparation post-quantique commence par la crypto-agilité.

La crypto-agilité permet de pérenniser son organisation en :[18]

- ayant la capacité de changer rapidement les protocoles, les clés et les algorithmes
- utilisant une technologie flexible et évolutive
- réagissant rapidement aux menaces cryptographiques, telles que l'informatique quantique
- complétant sa pile technologique avec un minimum de perturbations, voire aucune.

3. La sensibilisation et la préparation accrues des entreprises et institutions, afin de garantir une adoption maîtrisée et sécurisée.

Cela passera par des expérimentations de plus en plus nombreuses à l'image du « Quantum Readiness Program » aux États-Unis ou du « PQC Transition Testing » en Europe.
Les organisations, privées comme publiques doivent impérativement rester en veille active. L'état de la menace (développement de l'ordinateur quantique), l'évolution des standards et des nouveaux algorithmes résistants au quantique, l'évolution des réglementations (la PQC deviendra l'état de l'art en matière de cryptographie et sera exigée), l'évolution des certifications et visas de sécurité (ils vont progressivement intégrer la PQC dans l'évaluation des produits) sont autant de points de vigilance des prochains mois et années.

18. Thales

4. Investir dans l'éducation et la formation

Il est essentiel de développer des programmes éducatifs et des ressources de formation. Ces initiatives devraient se concentrer sur la sensibilisation aux risques quantiques et doter les professionnels de la cybersécurité des compétences nécessaires pour gérer et déployer efficacement des systèmes cryptographiques résistants à l'informatique quantique. TheGreenBow a en ce sens signé un partenariat avec l'école Guardia pour sensibiliser les étudiants en cybersécurité à la menace quantique. Dans ce cadre, les étudiants ont eu l'opportunité de réfléchir à la conduite d'un projet de migration vers la PQC.
Le NIST souligne de fait l'importance de l'éducation et de la formation dans ses efforts pour se préparer à l'informatique quantique. Il a lancé diverses initiatives, notamment des webinaires, des ateliers et des programmes de recherche en collaboration avec des établissements universitaires et des partenaires industriels. *« Nous allons devoir former les ingénieurs et les chercheurs mais aussi développer des formations tant pour les étudiants que pour les professionnels déjà en poste. Cela commence à se mettre en place. Aujourd'hui, nous montons en compétence. Les formations sont en croissance, à l'EPITA nous sommes autour d'une trentaine d'étudiants. »* explique Ludovic Perret.

5. La structuration de l'écosystème quantique européen, visant à renforcer l'indépendance et la souveraineté technologique du continent face aux avancées américaines et chinoises.

> *« Nous allons devoir former les ingénieurs et les chercheurs mais aussi développer des formations tant pour les étudiants que pour les professionnels déjà en poste. Cela commence à se mettre en place. Aujourd'hui, nous montons en compétence. Les formations sont en croissance, à l'EPITA nous sommes autour d'une trentaine d'étudiants. »*
> **Ludovic Perret, Professeur à l'EPITA.**

II. Tendances à horizon 2027-2030

● **Augmentation de la puissance des ordinateurs quantiques :** les grandes entreprises internationales et de nombreuses start-up spécialisées ambitionnent de dépasser la barrière du million de qubits physiques tout en améliorant la correction d'erreurs. Un ordinateur quantique tolérant aux fautes pourrait émerger d'ici à 5 ans, ouvrant la voie à des calculs réellement exploitables pour des applications industrielles.

● **Le remplacement des infrastructures cryptographiques existantes** impliquant une migration progressive vers des algorithmes PQC dans les protocoles comme TLS, IPsec, SSH et PGP et le déploiement d'algorithmes résistants aux attaques quantiques dans les infrastructures cloud et IoT.

● **L'adoption accrue des algorithmes post-quantiques :** Les entreprises et les institutions commenceront à intégrer massivement les algorithmes de PQC dans leurs infrastructures de sécurité. La NSA exige que ses fournisseurs de logiciels, de micrologiciels et d'équipements réseau adoptent exclusivement la cryptographie post-quantique dès 2030, avec des échéances spécifiques pour d'autres produits en 2033 et 2035.

● **L'émergence de nouveaux algorithmes complémentaires.** De nouveaux protocoles pourraient voir le jour, exploitant des avancées en cryptographie basée sur des codes, les isogénies supersingulières et les fonctions multivariées. La maîtrise au niveau européen des standards PQC est un enjeu majeur. Les Etats-Unis montrent la voie et fixent les règles du jeu quand la Chine a lancé le développement de ses propres standards. Alors que l'Etats-Unis prennent leur distance et qu'un nouvel ordre mondial est en marche, l'indépendance de l'Europe sur ces sujets est cruciale.

● **Le renforcement des réglementations et des obligations légales.** Les gouvernements pourraient imposer des délais de migration vers des solutions post-quantiques. Cela nécessitera l'adoption de nouvelles normes pour les certifications de sécurité, intégrant la résistance aux attaques quantiques comme critère essentiel, en particulier la prise en compte de la PQC dans les cibles de sécurité des certifications de l'ANSSI.

● **Progrès en télécommunications quantiques :** la Chine, avec son satellite Micius, a déjà démontré la transmission sécurisée par QKD à l'échelle intercontinentale. Les prochaines années pourraient voir émerger un Internet quantique, avec des nœuds de communication intriqués offrant une sécurité inégalée.

● **Développement de nouvelles architectures matérielles :** l'émergence de nouveaux types de qubits (qubits topologiques, qubits en silicium) pourrait réduire les contraintes actuelles et faciliter la miniaturisation des ordinateurs quantiques.

● **Prise en compte des considérations environnementales et éthiques**
Les algorithmes PQC nécessitent plus de puissance de calcul et de ressources que les méthodes cryptographiques conventionnelles, ce qui entraîne une augmentation de la consommation d'énergie. Des études démontrent déjà des expérimentations avec des améliorations significatives en termes de gains d'efficacité énergétique et de réduction de l'empreinte des ressources nécessaires. Pour garantir un accès équitable aux technologies résistantes au quantique et protéger les libertés civiles au cours de cette transition, il sera nécessaire de mettre en place des processus et des politiques de développement transparents.

En encourageant la coopération, en investissant dans l'éducation et en élaborant des stratégies globales, les organisations peuvent surmonter les complexités de la mise en œuvre de la PQC. La prise en compte des préoccupations environnementales et éthiques permettra d'assurer la durabilité et l'équité de cette transition, en préservant l'intégrité et la confidentialité des communications numériques à l'ère quantique.

Le moment d’agir est maintenant, avant que l’ordinateur quantique à grande échelle ne devienne une réalité.

Auteure : Mélanie BENARD-CROZAT
Conception graphique : ESPRIT COM’

Imprimé en France

A propos de TheGreenBow

Créé en 1998, TheGreenBow est un éditeur français de logiciels de Cybersécurité qui fournit des solutions VPN de confiance et dont l'expertise repose sur la sécurisation des communications. En 2013, TheGreenBow devient le premier opérateur à obtenir une certification CC EAL3+ de l'ANSSI pour son client VPN Windows. Acteur de référence des Clients VPN, nos logiciels sont distribués dans plus de 70 pays. Depuis fin 2019, TheGreenBow détient le label *« Utilisé par les armées françaises »* pour le produit TheGreenBow VPN Client Windows Certifié CC EAL3+. Ce label atteste de la mise en œuvre du logiciel par les services du Ministère des Armées.

THEGREENBOW