LE LAB Banque de France

RAPPORT D'EXPÉRIMENTATION

Novembre 2022

SOLUTION DE SÉCURISATION POST-QUANTIQUE DES ÉCHANGES DE DONNÉES

1 INTRODUCTION

Si la perspective de disposer d'ici une dizaine d'années de processeurs quantiques utilisables pour des applications opérationnelles reste encore incertaine, elle devient chaque jour plus crédible alors que les annonces successives des grands acteurs technologiques permettent d'envisager une accélération du calendrier de développement de cette technologie.

L'informatique quantique promet des améliorations significatives dans des domaines qui intéressent particulièrement la Banque de France (modélisation macroéconomique et financière, optimisations de traitements, intelligence artificielle). Elle permettrait le traitement de problèmes inaccessibles à ce jour ainsi qu'une réduction importante du temps d'exécution et de la consommation d'énergie par rapport aux applications informatiques existantes. La Banque de France s'y intéresse donc de près et s'est engagée dans une veille active sur cette technologie.

Mais il est admis qu'une des premières utilisations pratiques de cette technologie portera sur la factorisation des grands nombres et les fonctions de recherche, permettant de casser les algorithmes généralement utilisés pour chiffrer et authentifier les échanges de données, lesquels sont la clé de la sécurité des communications sur Internet et des infrastructures informatiques. Ces algorithmes sont en effet utilisés pour sécuriser les communications sur Internet et les infrastructures informatiques (sites web sécurisés, VPN, solutions de paiement, infrastructures de gestion des identités, signature digitale, blockchain…).

Cette révolution quantique représente donc une menace systémique sur l'intégrité et la sécurité de nos données. Les autorités responsables de la sécurité de l'information, en France (ANSSI), comme dans la plupart des pays industrialisés partagent déjà cette préoccupation.

La Banque de France, elle-même utilisatrice de solutions cryptographiques pour ses activités, ne peut négliger pour elle-même cette « menace quantique ». Plus largement, au titre de sa mission relative à la stabilité financière, elle ne peut ignorer l'impact que la technologie quantique pourrait avoir à l'avenir sur la sécurité des échanges financiers et la confiance du public dans l'économie numérique.

C'est pourquoi la Banque de France, a souhaité expérimenter la mise en œuvre de solutions de sécurisation des communications dites « post-quantiques », pour vérifier leur capacité à s'intégrer dans les systèmes d'information actuels. Elle a retenu une logique « hybride », conforme aux préconisations de l'ANSSI, de rétrocompatibilité avec les standards actuels et privilégie également une démarche « crypto-agile », par la mise en œuvre de plusieurs algorithmes choisis parmi ceux en cours de sélection par le National Institute of Standards and Technology (NIST) aux États-Unis ou recommandés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France et le Bundesamt für Sicherheit in der Informationstechnik (BSI - Federal Office for Information Security) en Allemagne.

La Banque de France a donc lancé en janvier 2022 une expérimentation, conclue en juillet, de déploiement d'une bibliothèque d'algorithmes « quantum-robustes » répondant parfaitement à ces exigences[1]. Dans une première étape, cette solution est testée pour des échanges de données protégés par un VPN IPSec avec une chaîne de confiance complète en mode hybride résistant au quantique (authentification, échange de clé pour chiffrement et HSM).

La Banque de France a collaboré sur ce projet avec la startup Cryptonext Security, fondée en 2019, spin-off d'INRIA, de Sorbonne Université et du CNRS. CryptoNext Security a apporté au projet, au travers des produits logiciels qu'elle a développés, sa maîtrise des algorithmes innovants résistants au quantique et de l'hybridation des protocoles de sécurité ainsi qu'une assistance technique précieuse dans les travaux de déploiement de sa solution au sein des infrastructures de la Banque de France.

Le succès de cette expérimentation permet à la Banque de France d'acquérir la compréhension des technologies de cryptographie post-quantique et s'inscrit à ce titre dans sa démarche stratégique d'évolution permanente de ses systèmes de communication et de sécurité de l'information, permettant en particulier de répondre, le moment venu et si elle se concrétise, à la menace quantique.

1 La Banque de France réalise avec Cryptonext Security une expérimentation de sécurité post-quantique | Banque de France (banque-france.fr).

2 POURQUOI CETTE EXPÉRIMENTATION

2.1 LA « MENACE QUANTIQUE » : DE QUOI PARLE-T-ON ?

Toutes les données échangées sur Internet sont sécurisées par des algorithmes de cryptographie réputés sûrs. Les deux plus utilisés sont RSA (et son alternative plus récente les courbes elliptiques), de nature asymétrique (une clé dite publique et une clé privée, mathématiquement et intimement liées) et AES, de nature symétrique (une seule clé, donc nécessairement « privée » mais partagée entre l'émetteur et le récepteur), qui peuvent être utilisés alternativement ou complémentairement.

Exemple :

lorsqu'on utilise un navigateur Web pour visiter un site Web sécurisé, le site fournit au navigateur un certificat numérique (généralement basé sur l'algorithme de chiffrement asymétrique RSA) qui porte les informations nécessaires à l'authentification du site par le navigateur (en particulier le mode de chiffrement asymétrique appliqué et la clé « publique » du site), grâce à la vérification, à l'aide de la clé publique, de la signature appliquée aux données par le site avec la clé privée associée au certificat.

Après cette étape d'authentification, un algorithme d'échange de clé (comme Diffie-Hellman), basé sur des clés asymétriques, permet au navigateur et au site d'échanger une clé symétrique commune, qui permettra de chiffrer les échanges à l'aide de l'algorithme de chiffrement choisi (par ex. AES).

Les systèmes de chiffrement à clé publique les plus couramment utilisés aujourd'hui (RSA, courbes elliptiques), qui reposent sur des problèmes mathématiques insolubles, en tout cas dans un temps raisonnable, même pour les ordinateurs conventionnels les plus rapides, garantissent la sécurité des échanges.

Cependant, un ordinateur quantique d'une puissance suffisante (exprimée en nombre de « qubits »), dont la technologie, différente de celle des ordinateurs aujourd'hui à notre disposition, lui permettrait d'exécuter simultanément un nombre extrêmement grand d'opérations, pourrait résoudre ces problèmes mathématiques beaucoup plus rapidement.

Des algorithmes sont déjà identifiés pour attaquer les principaux systèmes de sécurité aujourd'hui utilisés. L'algorithme de Shor permettrait ainsi de briser le chiffrement asymétrique (algorithmes de type RSA et courbes elliptiques), alors que l'algorithme de Grover pourrait être utilisé pour casser le chiffrement symétrique (tel que AES).

L'algorithme de Shor est à l'origine de l'engouement de la communauté scientifique pour le quantique depuis 1994. En effet, les algorithmes utilisés en informatique classique pour factoriser des nombres et donc attaquer le chiffrement RSA deviennent rapidement impraticables quand la complexité du problème augmente[2], alors que l'algorithme de Shor pourrait, sur un ordinateur quantique, casser le RSA en temps polynomial.

En effet, l'algorithme de Shor, grâce à la capacité de calcul parallèle de l'ordinateur quantique sur toutes les valeurs possibles entre 0 et 2^n, permet une attaque performante par « force brute » sur une clé de chiffrement asymétrique avec une probabilité finie d'obtenir le bon résultat, sachant qu'il est trivial (et donc très rapide) de tester la solution obtenue jusqu'à obtenir par essais successifs, le résultat recherché.

Une publication récente du CEA-List confirme la pertinence de cet algorithme alors qu'elle n'avait jusqu'à présent pu être vérifiée, faute d'outils adaptés[3].

2 La complexité du problème évolue de façon exponentielle avec le nombre de bits de la clé publique.

3 https://www.cea-tech.fr/cea-tech/Pages/2022/logiciels-quantiques-une-implementation-de-l-algorithme-de-shor-verifiee-pour-la-premiere-fois-.aspx

En l'état de la recherche algorithmique, on estime cependant qu'il faudrait un ordinateur quantique avec 22 millions de qubits « bruités »[4] pour percer une clé RSA de 2 048 bits[5]. Par contre, dans une publication de septembre 2021, des chercheurs du CEA estiment qu'en ajoutant une mémoire quantique à l'ordinateur, le nombre de qbits requis descendrait à 20 000, voire 13 000 après optimisations[6].

En sachant qu'en 2023, selon les informations disponibles dans les feuilles de route des acteurs technologiques engagés sur ce sujet, le meilleur ordinateur quantique comportera au mieux 1 000 qubits (IBM Quantum Computing | Roadmap), et peut-être 10 000 en 2026, le temps nécessaire pour parvenir à construire un ordinateur capable de casser le chiffrement RSA dans un temps acceptable se compte probablement en années (sans qu'il soit possible aujourd'hui d'estimer la date à laquelle cela interviendrait).

S'agissant des algorithmes de sécurisation par clés symétriques, l'algorithme de Grover peut réduire le nombre d'itérations à la racine carrée de la clef. Ainsi, pour AES-128, le nombre est réduit à 2^64 (ce qu'on peut considérer comme fragile face à la puissance d'un ordinateur quantique), tandis que pour des clés de type AES-256 il est encore de 2^128, ce que l'on peut considérer comme robuste face à la capacité cryptanalytique d'un ordinateur quantique.

2.2 LES RÉPONSES POSSIBLES

La première réaction possible consisterait à augmenter la taille des clés utilisées dans les algorithmes actuels pour accroître la difficulté de résolution du problème mathématique de « cassage » des clés, ou bien d'augmenter la fréquence de mise à jour des clés. Cependant, si cela peut dans un premier temps parer à la menace des ordinateurs quantiques, ce répit ne serait que de court terme, et il est nécessaire d'envisager d'ores et déjà d'autres réponses, durables, au problème de la sécurité « post-quantique » des communications.

À cette fin, deux voies sont envisageables :

- Recourir à la physique quantique elle-même pour échanger de manière sécurisée des clés de chiffrement : c'est la distribution quantique de clés (Quantum keys distribution – QKD) qui requiert en l'état de la technologie une très haute maîtrise des conditions physiques de l'échange de clés, laquelle constitue un défi pour une mise en œuvre opérationnelle ;

- Utiliser de nouveaux mécanismes de chiffrement des clés et/ou des données, dont la difficulté de cryptanalyse dépasserait même les capacités d'un ordinateur quantique : c'est la Cryptographie « post-quantique » (Post-quantum cryptography – PQC) qui présente l'avantage de pouvoir être mise en œuvre avec des ordinateurs « classiques »[7]. C'est la voie la plus fréquemment choisie car la plus aisément réalisable. C'est aussi celle qu'a choisie la Banque de France pour son expérimentation.

2.2.1 Quels algorithmes pour la cryptographie post-quantique ?

Le NIST a publié en juillet 2022[8] un premier groupe d'outils de chiffrement (3 pour sécuriser l'échange de clés et un pour la signature) conçus pour résister au potentiel des ordinateurs quantiques. Les quatre algorithmes de chiffrement sélectionnés feront partie de la norme cryptographique post-quantique du NIST, qui devrait être finalisée d'ici deux ans.

Chacun de ces algorithmes propose un compromis spécifique entre les différentes contraintes que sont la taille de la clé et des signatures, la complexité et donc la charge de calcul pour l'échange de clés et le niveau d'assurance de la sécurité.

Pour l'échange de clés, utilisé notamment pour l'accès aux sites Web sécurisés, le NIST a sélectionné l'algorithme CRYSTALS-Kyber. Parmi ses avantages figurent des clés de chiffrement relativement petites que deux parties peuvent échanger facilement, ainsi que sa vitesse de fonctionnement.

Pour les signatures numériques, souvent utilisées pour vérifier des identités lors d'une transaction numérique ou signer un document à distance, le NIST a sélectionné les trois algorithmes CRYSTALS-Dilithium, FALCON et SPHINCS+.

4 Correspondant à 14 238 qbits logiques, chacun d'eux occupant 1 568 qbits physiques.

5 banegasPresentation.pdf (inria.fr) et publication de l'Université Cornell : [1905.09749] How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits (arxiv.org).

6 Espace Presse - Avec une mémoire quantique, l'ordinateur quantique est 1 000 fois plus petit ! (cea.fr).

7 Les termes « Cryptographie post-quantique » sont parfois critiqués car porteurs d'ambiguïté. Il faudrait plutôt parler de cryptographie résistante au quantique (« quantum robust »).

8 Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates | CSRC (nist.gov).

Les examinateurs ont noté la grande efficacité des deux premiers, et le NIST recommande CRYSTALS-Dilithium comme algorithme principal, avec FALCON pour les applications qui nécessitent des signatures plus petites que celles que Dilithium peut fournir. Le troisième, SPHINCS+, est un peu plus lourd et plus lent que les deux autres, mais il est précieux comme possible solution alternative car basé sur une approche mathématique différente de celle des trois autres sélections du NIST (fonctions de hachage au lieu de problèmes mathématiques du type « réseaux structurés »).

En parallèle, quatre autres algorithmes d'échange de clés sont à l'étude pour être inclus à terme dans la norme et apporter une variété d'algorithmes pour chaque cas d'utilisation, permettant de faire face au cas où l'un d'eux s'avérerait vulnérable.

Il est à noter que l'algorithme SIKE (Supersingular Isogeny Key Encapsulation), qui avait franchi les 4 premières étapes du concours du NIST, a été récemment mis en échec par des chercheurs du groupe Computer Security and Industrial Cryptography (CSIS) de l'université Belge de KU Leuven ce qui démontre, si besoin était, que la solidité de ces algorithmes reste à démontrer dans la durée.

Même si cette attaque n'a pas impact sur les quatre premiers algorithmes sélectionnés par le NIST comme normes en août, qui reposent tous sur des mathématiques complètement différentes de SIKE, elle montre la nécessité que les chercheurs continuent à mettre à l'épreuve ces algorithmes pour essayer de trouver d'éventuelles vulnérabilités et en parallèle recherchent d'autres approches mathématiques complémentaires de celles déjà identifiées.

Cette marge d'incertitude sur la solidité des algorithmes impose aux acteurs de se tenir prêts, en cas de faiblesse identifiée dans un algorithme, à basculer très rapidement sur un autre, ce que l'on nomme la « crypto-agilité ».

2.2.2 Les recommandations des autorités de sécurité

La cryptographie post-quantique est encore au stade de la recherche et développement et elle est de ce fait encore relativement immature. Cependant, cette immaturité ne peut être une justification pour les acteurs concernés de différer la réflexion sur leur stratégie d'adaptation à la menace quantique, dans le respect des préconisations des autorités nationales et internationales de sécurité[9].

Le « Department of Homeland Security » américain a récemment publié une feuille de route pour sa transition, appelant notamment à cataloguer les données les plus sensibles dans le secteur public et le secteur privé.

L'ANSSI[10] encourage à entamer sans attendre une transition graduelle afin d'accroître progressivement la confiance dans les algorithmes post-quantiques et leurs implémentations tout en garantissant l'absence de régression en ce qui concerne la sécurité classique (pré-quantique) dans le cadre d'une démarche hybride.

Un mécanisme hybride d'établissement de clé ou de signature combine l'application d'un algorithme à clé publique pré-quantique et d'un algorithme post-quantique. Cette hybridation permet de bénéficier à la fois de la robustesse démontrée du premier contre les attaques classiques et de la résistance du second contre les attaquants quantiques.

La plupart des algorithmes post-quantiques impliquant des tailles de messages échangés beaucoup plus grandes que les schémas pré-quantiques actuels, le surcoût de performance d'un schéma hybride reste faible par rapport au coût du seul schéma post-quantique. L'ANSSI estime qu'il s'agit d'un prix raisonnable à payer pour garantir une sécurité pré-quantique au moins équivalente à celle apportée par les algorithmes normalisés pré-quantiques actuels.

Pour les primitives symétriques, l'ANSSI encourage la recherche d'un niveau de sécurité post-quantique cohérent avec l'algorithme post-quantique sélectionné, soit en pratique au moins le même niveau de sécurité que l'AES-256 pour les chiffrements par blocs et au moins le même niveau de sécurité que SHA2-384 pour les fonctions de hachage.

Comme indiqué précédemment, l'incertitude sur la robustesse des algorithmes post-quantiques qui subsistera tant qu'ils n'auront pas été exposés de manière prolongée à des attaques réelles justifie par ailleurs aux yeux de l'ANSSI une démarche de crypto-agilité. En parallèle de la menace quantique, il ne faut d'ailleurs pas non plus négliger que les attaques classiques peuvent également évoluer et rendre certains mécanismes cryptographiques ou tailles de clé obsolètes. En pratique, la crypto-agilité signifie donc également que les solutions cryptographiques devraient avoir la capacité de prendre en compte les mises à jour d'algorithmes cryptographiques afin de réagir aux recommandations à venir et aux mises à jour des normes.

FrodoKEM, aux niveaux 3 et 5, est l'un des deux algorithmes post-quantiques recommandés par l'Office fédéral allemand de la sécurité de l'information (BSI) comme cryptographiquement adaptés à la confidentialité à long terme. Un développeur devrait pouvoir obtenir un visa de sécurité pour un produit implémentant FrodoKEM en mode hybride, quelle que soit la décision du NIST d'en faire une des premières normes PQC.

9 ANSSI en France, BSI en Allemagne, ENISA en Europe…

10 Avis de l'ANSSI sur la migration vers la cryptographie post-quantique | Agence nationale de la sécurité des systèmes d'information.

2.3 LA MENACE QUANTIQUE VUE PAR LA BANQUE DE FRANCE

La généralisation de la dématérialisation des échanges, financiers comme non financiers, dans un contexte d'internationalisation de ces échanges rend nos économies dépendantes de la robustesse des techniques de sécurisation des communications et des données, qu'elles garantissent l'authenticité et l'intégrité des données comme des identités (algorithmes d'authentification et de signature).

2.3.1 Pour la Banque de France elle-même

Comme toute entité utilisatrice des technologies de l'information et spécialement des échanges de données sur les réseaux publics avec des contreparties tierces, la Banque de France serait exposée à la rupture de la confidentialité de ses communications, mais aussi des données stockées, temporairement ou durablement, de façon chiffrée, dans des systèmes externes mais encore au décryptage de données transmises aujourd'hui sur des réseaux avec un chiffrement robuste, mais qui pourraient être captées par des acteurs (publics ou privés) dans l'objectif de les déchiffrer plus tard, lorsque les technologies disponibles le permettront (logique du « *store now, decypher later* »).

Dans le cadre d'une stratégie d'évolution de nos systèmes de sécurisation des données et des communications, et sans attendre la disponibilité de technologies post-quantiques, l'utilisation plus systématique d'AES256 pour le chiffrement des données froides et l'augmentation régulière de la taille des clés RSA pour notre PKI permet de gagner quelque répit.

La Banque de France, comme tous les acteurs publics et privés, devra intégrer ces contraintes dans sa feuille de route stratégique sur l'évolution de ses dispositifs de sécurité des données et des communications, permettant d'effectuer une transition efficace, fondée sur :

- un inventaire exhaustif de l'utilisation de la cryptographie dans les applications et infrastructures ;
- l'acquisition d'infrastructures de communication intégrant ces nouvelles technologies post-quantiques ;
- l'adaptation de l'ensemble de son SI, en commençant par les éléments les plus sensibles, pour une intégration de bout en bout de ces technologies.

Néanmoins certains protocoles hybrides sont en cours de normalisation notamment pour TLS 1.3 ou pour IKEv2. La nécessité de protéger les données échangées le plus rapidement possible ET la maturité de ces protocoles a conduit la Banque de France à expérimenter dès cette année une solution technique susceptible de protéger à terme les communications entre différents sites de l'institution puis avec ses partenaires.

2.3.2 Pour l'industrie financière

Plus peut-être que tout autre secteur économique, le secteur financier échange massivement des données dont la confidentialité et l'intégrité sont des exigences cruciales pour la confiance des acteurs et in fine la stabilité financière.

Les banques, les compagnies d'assurance et les autres établissements du secteur financier sont donc dépendants de canaux de communication parfaitement sécurisés, que ce soit pour leurs échanges bilatéraux de données ou pour accéder aux services des infrastructures de marchés (réseaux de communication interbancaires, systèmes de négociation de transactions sur devises et instruments financiers, systèmes de paiement et de règlement-livraison de titres…), d'importance vitale pour le bon fonctionnement des services financiers.

Les clés asymétriques sont largement utilisées pour sécuriser ces communications. Des attaques réussies contre ces algorithmes compromettraient les services bancaires mobiles, le commerce électronique, les transactions de paiement, les retraits d'espèces aux GAB et les communications via un réseau privé virtuel (RPV), pour n'en citer que quelques-unes.

Généralement investies d'une responsabilité sur la stabilité financière, les banques centrales se doivent notamment de veiller à la robustesse opérationnelle du secteur et de ses acteurs. À ce titre, la capacité de l'ensemble des acteurs à se protéger d'attaques contre la sécurité de leurs données et de leurs communications constituent pour elles un sujet d'attention.

Elles ne peuvent par ailleurs pas ignorer qu'au-delà de la sphère financière traditionnelle et réglementée, les applications basées sur les DLT qui supportent les actifs numériques aujourd'hui prisés comme Bitcoin et Ethereum, reposent également sur la cryptographie par clé publique pour garantir la sécurité des transactions.

Anticiper la menace quantique à l'échelle de tout le secteur financier suppose, après un inventaire des techniques de cryptographie utilisée par les acteurs eux-mêmes, mais aussi de celle employée par leurs fournisseurs, un chantier structuré de déploiement progressif de technologies « quantum-robustes », assurant la coexistence, le temps de la migration, avec les technologies existantes.

Ce plan, à définir à l'échelle du secteur et qui devra être défini à une échelle internationale compte tenu de l'interconnexion des places financières, devrait se fonder sur les préconisations des autorités de sécurité et en premier lieu l'hybridation et la crypto-agilité.

« Il est important de prendre les devants car la transition risque d'être très longue, puisque l'on parle de l'intégralité des logiciels qui chiffrent ou qui signent. Il va falloir des années avant que tout le monde ait franchi le pas. Par ailleurs, la menace la plus importante actuellement consiste à retenir les informations qui transitent aujourd'hui pour les déchiffrer rapidement quand on aura un ordinateur quantique », ajoute Damien Stehlé, professeur à l'ENS de Lyon, membre du Laboratoire d'informatique du parallélisme (Lip).

2.3.3 Les objectifs de l'expérimentation de la Banque de France

Dans ce contexte, la Banque de France a poursuivi trois objectifs au travers de son expérimentation :

- Comprendre les technologies post-quantiques,
- Mesurer leur degré de maturité et donc la faisabilité d'une application dans une solution opérationnelle,
- À cette fin, tester la capacité de la Banque à intégrer ces technologies dans son système d'information et évaluer leur potentiel et leurs limites, en particulier du point de vue des performances.

3 COMMENT ?

La Banque de France a retenu plusieurs principes pour cadrer l'expérimentation et donc opté pour la recherche d'une solution :

- La plus proche possible des contraintes opérationnelles,
- Impliquant la totalité des composants de la chaine de sécurité : y compris la conservation sécurisée des clés,
- Mettant en application les meilleures pratiques dans l'esprit des préconisations des autorités de sécurité : robustesse des algorithmes, hybridation et crypto-agilité,
- Réalisable dans un cadre expérimental, sans mobiliser des ressources (notamment d'expertise) dépassant les capacités de l'institution.

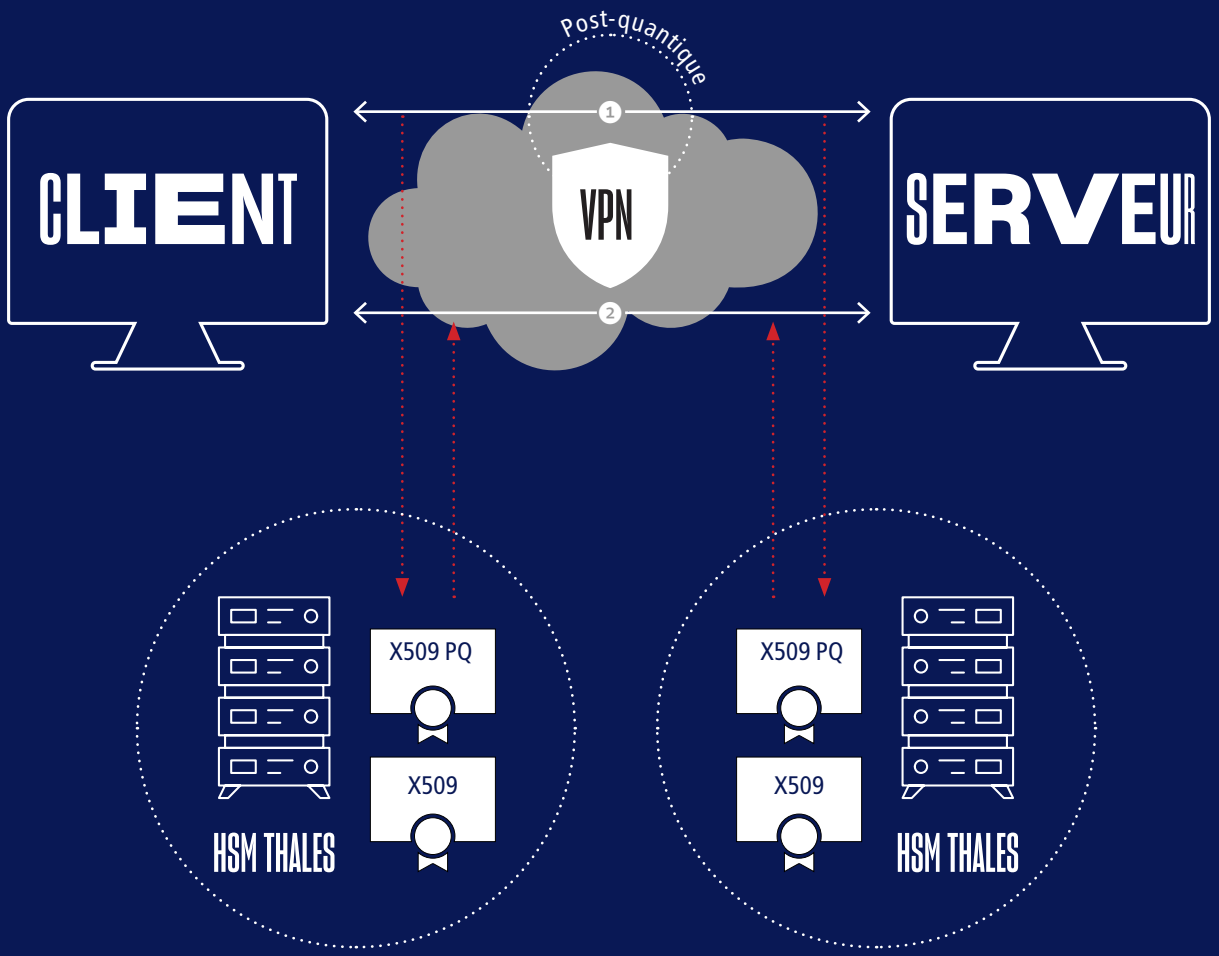
3.1 ARCHITECTURE FONCTIONNELLE

En application des principes précités, la Banque de France a retenu :

- Un projet d'infrastructure portant sur la seule sécurisation des échanges entre équipements réseaux sans impliquer d'applications, ce qui aurait compliqué le projet, mobilisé des ressources supplémentaires et créé un risque d'échec ;
- Centré sur la sécurisation post-quantique de l'échange de clés symétriques, représentatif de la mise en œuvre des algorithmes du NIST. L'échange de données lui-même est sécurisé par des clés symétriques (algorithme AES) à la fois éprouvé, performant, et estimé robuste aux attaques quantiques (en tous cas dans un premier temps) ;
- En conséquence, le choix a été fait de tester une solution post-quantique sur un échange au niveau réseau via VPN IPSEC qui :
    - permet de sécuriser au niveau du tunnel n'importe quel type d'échange de données existant,
    - et, via le protocole IKE, d'implémenter une solution hybride, reposant sur des algorithmes classiques (Diffie-Hellman) et post-quantiques ;
- Parmi les algorithmes post-quantiques préconisés par le NIST, ont été retenus :
    - Pour l'authentification avant échange des clés : **Dilithium,**
    - Pour l'échange de clés : **FRODO KEM** (retenu en ligne avec les recommandations ANSSI), **KYBER.**

Le choix de deux algorithmes d'échange de clés a permis de vérifier la capacité crypto-agile de la solution au travers d'un test de bascule de la sécurisation de FRODO à KYBER.

LE SCHÉMA GLOBAL DE LA SOLUTION



1. AUTHENTIFICATION IPSECPQ (+RSA)
   + Échange de clés PQ (+ Diffie-Hellman)

2. TRANSMISSION DE DONNÉES CHIFFRÉES (AES)

3.2 ARCHITECTURE TECHNIQUE

3.2.1 Matérielle

L'architecture matérielle mise en jeu est totalement classique avec des machines virtuelles en configurations suivantes :

- Pour le serveur VPN :
    - 2 CPU (Intel(R) Xeon(R) CPU E7540 @ 2.00GHz), 4Go RAM
    - Système d'exploitation : Debian Bullseye 5.10.120-1 (2022-06-09)
- Pour le client VPN :
    - 2 CPU (Intel(R) Xeon(R) CPU E7540 @ 2.00GHz), 4Go RAM
    - Système d'exploitation : Debian Bullseye 5.10.120-1 (2022-06-09)

La conservation et la gestion des clés ont été effectuées dans les équipements standards de la Banque de France (Thales Luna 7 NetHSM) connectés au serveur et au client.

3.2.2 Logicielle

Le choix s'est porté sur une solution basée sur des librairies post-quantiques fournies par Cryptonext Security SA, pour permettre à la Banque de France de profiter de l'expérience de cette entreprise dans ces technologies et dans leur déploiement opérationnel.

À l'inverse, l'option du développement d'une solution sur la base d'une librairie Open Source (Open Quantum Safe) n'a pas été retenue au regard de la charge prévisible et des risques de dérive, voire d'échec d'un projet sensiblement plus complexe.

Deux configurations ont été implémentées :

Configuration 1 :

Serveur VPN IPSEC Opensource Strongswan et client VPN IPSEC Strongswan, les deux parties étant connectées à un NetHSM Thales Luna 7, doté d'un Fonctionnality Module chargé avec les librairies Post-Quantiques fournies par Cryptonext Security.

Algorithmes utilisés :
- Signature : DILITHIUM
- Échange de clé : FRODO level 5

Configuration 2 :

Serveur VPN IPSEC Opensource Strongswan et client VPN IPSEC propriétaire The Green Bow, les deux parties utilisant les librairies Post-Quantiques en mode logiciel.

Algorithmes utilisés :
- Signature : DILITHIUM
- Échange de clé : FRODO level 5, et Kyber

Une série de scripts shell ont été développés pour automatiser le déploiement des différentes configurations au niveau client et au niveau serveur, lancer les tests de transfert de données dans le tunnel, récupérer les différents logs obtenus au niveau client, au niveau serveur, au niveau réseau, puis les analyser.

4 ENSEIGNEMENTS

Le projet a été concrétisé avec succès, puisqu'il a permis de déployer et de tester la solution VPN IPSEC Post-Quantique définie ci-dessus pour les configurations suivantes :

Configuration 1 :

- Serveur VPN IPSEC Strongswan connecté à NetHSM Luna 7
- Client VPN IPSEC Strongswan connecté à NetHSM Luna 7

Configuration 2 :

- Serveur VPN IPSEC Strongwan
- Client VPN IPSEC The Green Bow

Les tests effectués ont permis de s'assurer que la solution pouvait fonctionner avec des clients VPN IPSEC différents (Strongswan et The Green Bow). La crypto-agilité a été testée en substituant l'algorithmes d'échange de clé Kyber à Frodo.

L'expérimentation a, cela étant, permis d'identifier les points d'attention suivants :

- L'implémentation stricte de ces solutions requiert pour obtenir un niveau maximal de sécurité que l'ensemble des composants utilisés soient compatibles avec les algorithmes post-quantiques utilisés (en particulier les NetHSM avec Fonctionnality Module et librairies cryptographiques) ;

- La mise en œuvre de la solution requiert la mise en œuvre de certificats x509 post-quantiques (avec clés DILITHIUM), en parallèle de certificats x509 classiques (avec clés RSA). Il faut donc pouvoir se procurer des certificats post-quantiques auprès d'une ou plusieurs autorités de certification de confiance (dans le cadre du projet, ils ont été adaptés ad hoc par l'équipe projet) ;

- L'établissement du tunnel VPN IPSEC connecté au NetHSM avec un algorithme FRODO en level 5 nécessite de 4 à 5 secondes. Cela n'apparaît pas problématique pour le cas d'usage testé, car le temps est pris uniquement au moment de la connexion initiale entre le client et le serveur. Mais ce temps long d'établissement serait à réexaminer pour d'autres cas d'usages (en particulier pour une connexion TLS).

5 CONCLUSION

Le succès de ce projet d'expérimentation, pour l'instant conduit sur un périmètre interne à la Banque de France appelle, pour en approfondir les enseignements, une prolongation des tests en impliquant des acteurs tiers, permettant de tester l'échange de clés dans une configuration encore plus proche de la réalité, impliquant le déploiement de la solution dans des contextes techniques différents de celui de la Banque de France, voire un échange entre des solutions différentes, permettant de tester leur interopérabilité.

À cette fin, la Banque de France a établi des contacts avec plusieurs établissements bancaires français pour envisager soit des échanges d'information, soit des tests bilatéraux.

Par ailleurs, la Banque de France va prochainement participer, conjointement avec la Deutsche Bundesbank, à un projet conduit par le centre Eurosystème du Hub d'Innovation de la Banque des règlements internationaux[11] pour tester ce type de solution dans un cadre transfrontière.

L'ensemble des résultats obtenus, qui seront largement partagés, viendront alimenter la réflexion stratégique de la Banque de France sur un double plan :

- La stratégie d'évolution de ses systèmes de sécurité, et donc la feuille de route d'investissement dans le renouvellement des équipements de communication et de sécurité ;

- La préparation du secteur financier français (et européen dans le cadre des missions de l'Eurosystème sur la stabilité financière) à faire face à une possible concrétisation de la menace quantique.

11 Le Hub d'Innovation de la BRI (BIS IH) est un réseau de centre d'innovations auquel l'Eurosystème participe au travers d'un Centre disposant de deux implantations hébergées par la Banque de France et la Deutsche Bundesbank.

LE LAB Banque de France

822393 BdF Dircom Studio Création – 11/2022