Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique

14/04/2022

Dans cet avis scientifique et technique, l'ANSSI résume les différents aspects et enjeux de la menace quantique sur les systèmes cryptographiques actuels. Après un bref aperçu du contexte de cette menace, ce document introduit un planning prévisionnel de migration vers une cryptographie post-quantique, i.e. résistante aux attaques que l'émergence d'ordinateurs quantiques de grande taille rendrait possibles. L'objectif est de se prémunir par anticipation contre cette menace tout en évitant toute régression de la résistance aux attaques réalisables au moyen des ordinateurs classiques actuels. Cet avis vise à fournir une orientation aux industriels développant des produits de sécurité et à décrire les impacts de cette migration sur l'obtention des visas de sécurité délivrés par l'ANSSI [4].

Qu'est-ce qu'un ordinateur quantique ?
Les ordinateurs quantiques sont des calculateurs reposant sur des principes physiques fondamentalement différents des ordinateurs classiques actuels. Si de tels ordinateurs de grande taille sont un jour construits, ils pourraient effectuer certaines tâches beaucoup plus rapidement que ces derniers.

Même si certains prototypes d'ordinateurs quantique existent aujourd'hui, souvent désignés par l'acronyme NISQ, de l'anglais `Noisy Intermediate Scale Quantum computers`, la conception d'ordinateurs quantiques re-programmables capables de manipuler des grands nombres est aujourd'hui un problème de recherche ouvert encore très amont. Plusieurs pistes de recherche en physique quantique sont aujourd'hui à l'étude dans le monde académique, mais aucune n'est certaine d'aboutir. L'ampleur des retombées scientifiques d'une telle réalisation n'est pas encore totalement délimitée et peut être colossale. En conséquence, l'industrie, les gouvernements et les universités du monde entier consacrent d'importantes ressources à la recherche en informatique quantique. A titre d'exemple, en 2021, le gouvernement français a annoncé un "plan quantique" d'investissement de plus d'un milliard d'euros dans les technologies quantiques, dont l'informatique quantique [7]. Une enquête complète sur l'état du développement de l'ordinateur quantique a été détaillée par le BSI, homologue allemand de l'ANSSI [6].

Menace quantique : quel serait l'impact sur les infrastructures numériques actuelles ?
La sécurité de la majorité des systèmes d'informations repose aujourd'hui sur la cryptographie à clé publique, ou PKC pour `Public Key Cryptography` en anglais. Cette technologie permet de sécuriser les communications entre des entités, typiquement des utilisateurs ou des serveurs, qui ne partagent aucun secret préalable. Plus précisément, la PKC permet deux fonctionnalités principales : l'établissement de canaux sécurisés (établissement de clés) et l'authentification d'informations numériques (ainsi que l'authentification des protagonistes d'une communication au moyen de signatures numériques).

Aujourd'hui, ces techniques reposent essentiellement sur deux problèmes mathématiques : la factorisation de grands nombres et le calcul de logarithme discret. Ceux-ci sont dimensionnés pour être impossibles à résoudre en un temps raisonnable compte tenu des ressources informatiques et des connaissances mathématiques actuelles. Par exemple, l'algorithme à clé publique RSA, largement reconnu et déployé, repose sur la factorisation de grands nombres.

Ces deux problèmes fondamentaux pourraient être atteignables par un ordinateur quantique de grande taille. Ainsi, l'existence d'un tel ordinateur impliquerait un effondrement de la sécurité de la cryptographie à clé publique actuellement déployée. En effet, en 1994, le chercheur P. Shor a introduit un algorithme [14] capable de résoudre ces problèmes efficacement. Cet algorithme est quantique, c'est-à-dire qu'il ne peut pas être exécuté sur des ordinateurs classiques, mais il pourrait être exécuté sur des ordinateurs quantiques de grande taille. Pour éviter la confusion avec les prototypes d'ordinateurs quantiques existants, le NCSC, homologue britannique de l'ANSSI, introduit la dénomination d'ordinateurs quantiques pertinents pour la cryptographie, abrégés en CRQC pour `Cryptographically Relevant Quantum Computers` (voir le livre blanc sur la cryptographie post-quantique [11]). En d'autres termes, un CRQC est un ordinateur quantique capable d'implémenter des instances pertinentes de l'algorithme de Shor et ainsi de menacer la cryptographie à clé publique déployée aujourd'hui.

Les prototypes d'ordinateurs quantiques existants sont encore loin de la capacité et stabilité requises des CRQC et ne constituent donc pas aujourd'hui une menace pour la cryptographie à clé publique.

De nombreux défis de recherche en physique, en ingénierie et en informatique doivent être surmontés avant de pouvoir passer à l'échelle et résoudre les problèmes de factorisation et de logarithme discret sur lesquels repose la cryptographie à clé publique actuelle.

Néanmoins, la menace d'attaques rétroactives ne doit pas être écartée. Une famille d'attaque, désignée en anglais par **`store now, decrypt later attacks`**, consiste en effet à enregistrer dès aujourd'hui des communications chiffrées dans le but de les déchiffrer plus tard. Plus précisément, un attaquant pourrait stocker les données transmises pendant l'établissement d'un canal sécurisé (utilisant de la PKC) ainsi que les messages échangés sur ce canal afin de pouvoir potentiellement les déchiffrer plus tard avec un CRQC disponible. La menace d'attaques rétroactives est d'autant plus pertinente que les informations échangées aujourd'hui sont sensibles et doivent demeurer longtemps confidentielles. Elle n'est donc pas à écarter dans certains contextes.

En outre, la menace quantique peut aussi peser sur les signatures électroniques d'une manière différente. En effet, un CRQC pourrait aussi forger des signatures et permettre l'usurpation de l'identité de serveurs ou d'autres entités impliquées dans des échanges électroniques. Contrairement à la menace d'attaques rétroactives de type `store now, decrypt later`, cette menace ne serait effective que pour des signatures susceptibles d'avoir été générées à un moment où un CRQC existe. Ainsi, les signatures vérifiées à la volée, comme dans l'établissement de canaux authentifiés, ne pourront pas être directement impactées avant l'arrivée d'un CRQC. Néanmoins, dans un contexte de signature de documents, la validité à long terme est parfois nécessaire et peut être compromise par l'arrivée d'un CRQC. La problématique de la migration des signatures pre-quantiques devra ainsi être traitée avant l'avènement de CRQC pour éviter une usurpation d'identité a posteriori.

Menace quantique : le cas de la cryptographie symétrique

La cryptographie symétrique, une branche de la cryptographie différente et complémentaire de la PKC, pourrait également être ciblée par d'éventuels CRQC. Un algorithme quantique générique introduit par L. Grover en 1998 [10] accélère de manière quadratique la recherche exhaustive de la clé secrète des algorithmes symétriques paramétrés par une telle clé. L'algorithme de Grover a également permis l'accélération d'attaques dites par recherche de collisions contre les fonctions de hachage. Toutes ces attaques nécessitent aussi l'usage de CRQCs et pour d'assez nombreux algorithmes l'on peut raisonnablement présumer qu'elles peuvent être évitées en ajustant la taille des clés et les tailles de sortie de fonctions de hachage. Par exemple, l'adaptation peut consister à utiliser des clés de 256 bits au lieu de 128 bits pour le mécanisme de chiffrement symétrique AES et des tailles de haché d'au moins 384 bits pour les fonctions de hachage SHA-2 et SHA-3. Ainsi, l'impact générique de l'algorithme de Grover sur la cryptographie symétrique est beaucoup plus limité que celui de l'algorithme P. Shor pour la cryptographie à clé publique.

Pourquoi la menace quantique doit-elle être prise en compte dès aujourd'hui ?

A cause de l'attaque rétroactive `store now, decrypt later` décrite plus haut, la menace quantique doit être prise en compte avant de savoir si le développement d'un CRQC deviendra un jour réalisable. Ainsi, un changement profond de la cryptographie à clé publique doit être globalement initié pour anticiper un éventuel effondrement de la sécurité des infrastructures cryptographiques actuelles. La protection des systèmes contre cette menace lointaine a un coût évident, mais la recherche de solutions cryptographiques alternatives peut aussi avoir des répercussions largement bénéfiques. En effet, au-delà de la menace quantique, la cryptographie n'est jamais infaillible et des failles de sécurité, même exploitables sur ordinateurs classiques, sont régulièrement trouvées. Ainsi, on ne peut pas totalement exclure la découverte d'une faille de sécurité matérielle et/ou algorithmique nécessitant le remplacement immédiat d'algorithmes cryptographiques. Actuellement, la cryptographie à clé publique actuellement déployée est très proche d'une monoculture algorithmique et bénéficierait fortement de l'introduction de nouveaux algorithmes alternatifs.

La distribution quantique de clés pourrait-elle être une solution ?

La distribution quantique de clés (QKD pour `Quantum Key Distribution` en anglais), parfois appelée cryptographie quantique, permet un échange sécurisé de clés résistant aux attaques classiques et quantiques. Néanmoins, cette technique ne fournit pas un équivalent fonctionnel complet de la cryptographie à clé publique et offre des applications limitées en raison notamment de ce qu'elle nécessite une infrastructure de communication dédiée et sans réelles capacités de routage. La position détaillée de l'ANSSI sur le sujet est accessible en [2]. En un mot, à l'exception d'applications de niche où, utilisée en complément et

non en remplacement de la cryptographie algorithmique, la QKD pourrait définir une forme de défense en profondeur, cette technique n'est aujourd'hui pas considérée par l'ANSSI comme une contre-mesure appropriée pour atténuer la menace quantique.

En quoi consiste la cryptographie post-quantique ?
La cryptographie post-quantique, ou `Post-Quantum Cryptography` (PQC) en anglais, est un ensemble d'algorithmes cryptographiques classiques comprenant les établissements de clés et les signatures numériques et assurant une sécurité conjecturée [1] contre la menace quantique en plus de leur sécurité classique. Les algorithmes post-quantiques peuvent être exécutés sur des appareils et ordinateurs classiques. Ainsi, ils peuvent être déployés sur les infrastructures et canaux de communications existants sans modification matérielle majeure, contrairement à la distribution quantique de clés. De plus, ces algorithmes ne sont pas seulement destinés à être utilisés après la construction d'un CRQC, ils peuvent être facilement déployés par anticipation.

Pour l'ANSSI, la PQC représente la voie la plus prometteuse pour se prémunir contre la menace quantique.

L'effort international de la communauté de recherche en cryptographie post-quantique a été initié de longue date mais s'est accéléré en 2015 à la suite d'une publication de la NSA conseillant de prendre en compte la menace quantique dans un avenir proche [8]. En 2017, le NIST (`National Institute of Standards and Technologies`), organisme de normalisation américain, a lancé une campagne d'appel à propositions en vue de normaliser des algorithmes post-quantiques (d'établissement de clés et de signatures). Ce processus est aujourd'hui toujours en cours [12]. A ce jour, il en est à son troisième et avant dernier tour. Contrairement aux autres campagnes organisées par le NIST où un seul algorithme finaliste était sélectionné, la campagne post-quantique se terminera avec plusieurs algorithmes finalistes pour différents cas d'usage. Ces algorithmes feront l'objet de normes, publiées d'ici un à quatre ans par le NIST

Ce processus de normalisation a joué un rôle de catalyseur, permettant une forte implication de la communauté internationale de recherche en cryptographie et concentrant les efforts d'analyse sur un nombre restreint d'algorithmes candidats tout en préservant la diversité des problèmes sous-jacents. Ce processus a aussi permis d'ouvrir l'analyse à divers cas d'utilisation concrets comme les composants embarqués.

Quels sont les différents algorithmes post-quantiques ?
Les différentes familles d'algorithmes post-quantiques candidats sont avant tout définies par la structure du problème mathématique sur lequel elles reposent. Les algorithmes post-quantiques sont principalement fondés sur :

- les réseaux euclidiens structurés ou non structurés ;
- les codes correcteurs d'erreur ;
- les isogénies entre courbes elliptiques ;
- les systèmes polynomiaux multivariés ;
- les fonctions de hachage.

Même si ces problèmes mathématiques ont été introduits durant le siècle dernier, les algorithmes post-quantiques sont relativement récents. Ils offrent divers compromis entre la taille de la clé, des signatures ou des échanges d'établissement de clé, la complexité de calcul et l'assurance de la sécurité. Une étude technique des algorithmes et des problèmes mathématiques sous-jacents a été publiée par l'ENISA [9].

Quelle est l'implication de la France face à la menace quantique ?
Un fort intérêt académique pour cette thématique est historiquement présent en France. C'est pourquoi la communauté française participe activement à la conception et à l'analyse de la sécurité des primitives, mais aussi à l'analyse de leurs implémentations. Un groupe national composé d'universitaires, d'industriels et de chercheurs de l'ANSSI s'est constitué sous le nom de "Regroupement de l'Industrie française pour la Sécurité Post-Quantique" (RISQ). Un livre blanc est en passe d'être publié [13].

En tant qu'autorité nationale de cybersécurité en France, l'ANSSI a suivi et a participé à l'effort de recherche dans le domaine de la cryptographie post-quantique. Elle continuera son investissement dans les années à venir.

1. pour laquelle aucune attaque quantique efficace n'existe aujourd'hui.

D'une manière plus générale, l'ANSSI publie régulièrement des recommandations générales sur le choix des algorithmes cryptographiques dans les produits de sécurité et délivre des visas de sécurité pour les produits répondant aux exigences générales de sécurité. Cependant, il est à noter que l'ANSSI n'est pas une agence de normalisation, son rôle n'est pas d'élaborer des normes cryptographiques. Plus précisément, l'ANSSI a un double rôle en ce qui concerne la cryptographie : consultatif et réglementaire. D'une part, l'ANSSI promeut l'utilisation d'algorithmes cryptographiques à l'état de l'art en publiant un guide de sélection d'algorithmes cryptographiques [1] ainsi qu'un référentiel technique utilisable dans le cadre de l'évaluation de produits de sécurité et relatif au choix et au dimensionnement des algorithmes cryptographiques [**?**]. L'ANSSI participe aussi à la publication de recommandations européennes sur la sélection des algorithmes cryptographiques [15]. D'autre part, l'ANSSI supervise l'évaluation et la délivrance des visas de sécurité, comme par exemple les certificats Critères Communs (CC). Dans le schéma de certification français, chaque évaluation inclut entre autres une évaluation cryptographique dédiée. Il est important de souligner qu'il n'existe pas de liste fermée d'algorithmes cryptographiques éligibles pour qu'un produit obtienne un visa de sécurité. De manière générale, l'utilisation d'algorithmes cryptographiques normalisés par un organisme international de normalisation (par exemple ISO, ITU, ETSI, etc.) est fortement recommandée. Cependant, un algorithme cryptographique validé par de solides publications scientifiques peut être potentiellement jugé suffisant pour fournir un niveau d'assurance de sécurité adéquat. À l'inverse, il n'y a pas de reconnaissance automatique et universelle de tous les algorithmes normalisés par de tels organismes.

Les futures normes du NIST seront-elles assez matures pour être implémentées dans les futurs produits de sécurité ?
L'objectif initial du NIST étant de définir des normes, les trois derniers tours de la campagne de normalisation du NIST fournissent une large variété d'algorithmes avec des analyses précises de sécurité. Bien que cette nouvelle boîte à outils post-quantique puisse sembler commode pour les développeurs, le niveau de maturité des algorithmes post-quantiques présents dans la campagne du NIST ne doit pas être surestimé. Pour différents aspects de leur sécurité, l'on manque encore de recul cryptanalytique ou l'on en est même au stade de la recherche, qu'il s'agisse de l'analyse de la difficulté du problème sous-jacent dans des modèles de sécurité classiques et quantiques, du dimensionnement, de l'intégration des algorithmes dans des protocoles de communication ou (plus encore) de la conception d'implémentations sécurisées. Cette situation perdurera pour un temps après la publication des normes NIST.

> Il est important de reconnaître et de tenir compte de l'immaturité de la PQC : l'ANSSI n'approuvera aucun remplacement direct à court ou moyen terme.
> Cependant, cette immaturité ne doit pas servir d'argument pour reporter les premiers déploiements. L'ANSSI encourage tout de même à entamer l'initiation dans les mois qui viennent d'une transition graduelle, "en biseau", 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).

Comment graduellement passer d'algorithmes pré-quantiques à des algorithmes post-quantiques ?
Un mécanisme *hybride* d'établissement de clé ou de signature combine les calculs d'un algorithme à clé publique pré-quantique reconnu et d'un algorithme post-quantique supplémentaire. Cela permet de bénéficier à la fois de la forte assurance sur la résistance du premier contre les attaquants classiques et de la résistance conjecturée du second contre les attaquants quantiques. Certains protocoles hybrides sont en cours de normalisation notamment pour TLS 1.3 [16] ou pour IKEv2 [17]. Plus généralement, pour l'établissement de clé, on peut effectuer à la fois un établissement de clé pré-quantique et post-quantique, puis combiner les deux résultats, par exemple à l'aide d'une fonction de dérivation de clé (KDF pour `Key Derivation Function`). Alternativement, pour certaines applications spécifiques, il est possible d'appliquer une KDF pour combiner une clé pré-partagée et une clé obtenue à partir d'un schéma pré-quantique. En ce qui concerne l'authentification d'entités ou de messages, des signatures hybrides peuvent être obtenues en concaténant des signatures émises au moyen d'un schéma pré-quantique et d'un schéma post-quantique. Une telle signature doit être considérée comme valide que si les deux signatures sous-jacentes le sont.

Même si l'hybridation est une construction relativement simple, l'ANSSI souligne que le rôle de l'hybridation dans la sécurité cryptographique est crucial pour les phases 1 et 2 présentées ci-dessous. En outre, la sécurité de l'implémentation de la technique d'hybridation doit également être prise en considération.

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 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.

En quoi consiste la cryptoagilité ?

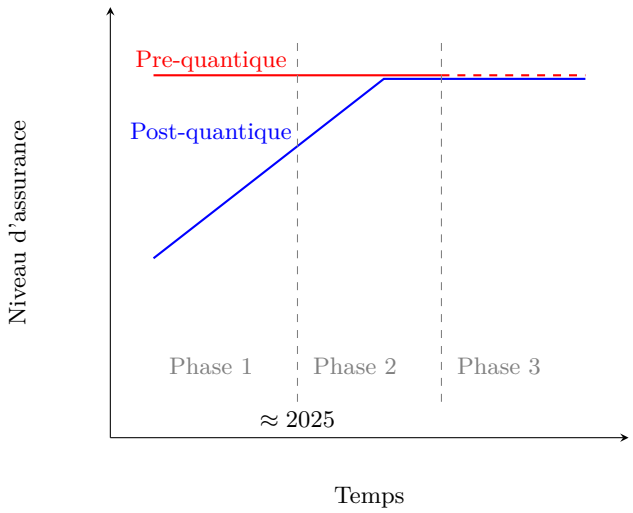
Comme cela sera détaillé dans la suite, le déploiement de PQC hybride n'est pas obligatoire à ce jour. Cependant, l'ANSSI encourage autant que possible l'introduction de capacités de *cryptoagilité* dans les futurs produits. Plus précisément, un produit de sécurité est dit cryptoagile s'il est possible de mettre à jour les algorithmes cryptographiques qu'il met en œuvre sans avoir à le rappeler ni à le substituer par un nouveau produit. La menace quantique rend la cryptoagilité particulièrement pertinente, et au-delà de cette menace, les attaques classiques peuvent également évoluer et rendre certains mécanismes cryptographiques ou tailles de clé obsolètes.

En pratique, la cryptoagilité signifie également qu'en plus de la possibilité de faire des correctifs, les produits pourraient avoir la capacité de permettre des mises à jour d'algorithmes cryptographiques afin de réagir aux recommandations à venir et aux mises à jour de normes. Même si les mises à jour des algorithmes cryptographiques devraient être beaucoup moins fréquentes que les correctifs, la cryptoagilité n'est pas une propriété triviale à mettre en œuvre en raison des besoins de rétrocompatibilité fréquemment rencontrés, des besoins de protection cryptographique des procédures de mises à jour et, si le produit est certifié, de l'exigence potentielle de visas de sécurité supplémentaires lorsque des mises à jour sont effectuées. Cependant, la motivation pour la cryptoagilité étant aujourd'hui très pertinente, l'ANSSI estime qu'elle doit au moins être prise en compte lors de l'analyse de risque de futurs produits de sécurité.

En quoi consiste la transition post-quantique "en biseau" ?

Pour pouvoir graduellement gagner en confiance tout en limitant le risque de régression de sécurité, l'ANSSI prévoit une transition "en biseau" en 3 phases (voir ci-dessous pour les descriptions détaillées).

- Phase 1 (aujourd'hui) : hybridation pour fournir une *défense en profondeur* post-quantique supplémentaire à l'assurance de sécurité pré-quantique.
- Phase 2 (probablement après 2025) : hybridation pour fournir une *assurance de sécurité post-quantique* tout en évitant toute régression de sécurité pré-quantique.
- Phase 3 (probablement après 2030) : hybridation optionnelle.



Qu'est-ce qui est recommandé pour chaque phase ?

Phase 1 : sécurité pré-quantique obligatoire, PQC en option, aucune reconnaissance d'une assurance de résistance à la menace quantique.

Cette phase correspond à la situation actuelle. La sécurité post-quantique n'est pas une exigence, mais est considérée comme une défense en profondeur optionnelle. La campagne de normalisation du NIST étant toujours en cours, l'idée de cette phase est de permettre les premiers déploiements post-quantiques avec flexibilité, tout en préservant la sécurité pré-quantique grâce à des mécanismes hybrides.

> L'ANSSI recommande d'appliquer une défense en profondeur post-quantique dès que possible pour les produits de sécurité visant à offrir une protection longue durée des informations (jusqu'après 2030) ou qui seront potentiellement utilisés après 2030 sans possibilité de mise à jour.

Les deux conditions ci-dessous doivent être remplies.

1. Il est impératif que la méthode d'hybridation choisie garantisse l'absence de régression de sécurité, c'est-à-dire que la sécurité totale doit être au moins équivalente à la sécurité du schéma pré-quantique éprouvé sous-jacent.
2. Bien que l'ANSSI ne publie pas de recommandations fermées pour le choix d'un algorithme post-quantique (mécanismes d'établissement de clé ou de signature), l'algorithme choisi doit avoir des spécifications stables et bien étudiées, par exemple être un finaliste du NIST ou un finaliste alternatif [2] de confiance. De plus, le niveau de sécurité post-quantique conjecturé doit être aussi élevé que possible, de préférence au niveau V du NIST (AES-256). Par exemple, les candidats NIST FrodoKEM, Crystals-Kyber, Crystals-Dilithium ou Falcon pourraient être de bonnes options pour de premiers déploiements. Le choix des algorithmes sélectionnés par le NIST pour la normalisation n'est pas un prérequis absolu [3].

Pour les primitives *symétriques*, l'ANSSI encourage à utiliser un niveau de sécurité post-quantique cohérent avec l'algorithme post-quantique sélectionné – 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.

Notons que les signatures fondées sur les problèmes de fonctions de hachage constituent une exception à la nécessité d'hybridation : en raison de la confiance liée au problème mathématique sous-jacent, l'ANSSI estime que ces algorithmes pourraient être utilisés aujourd'hui sans hybridation [4]. Cependant, leur spectre d'applications potentielles est limité (faible nombre de requêtes de signatures ou grandes tailles de signatures).

Cette phase se prolongera après l'annonce des premières normes du NIST et devrait durer jusqu'après 2025.

Phase 2. Sécurité pré-quantique obligatoire, PQC en option avec le cas échéant reconnaissance d'une assurance de résistance à la menace quantique.

Dans cette deuxième phase, les algorithmes post-quantiques continueront d'être systématiquement inclus dans des mécanismes hybrides (à l'exception des signatures fondées sur le hachage pour lesquelles l'hybridation est facultative comme présenté dans la phase 1).

2. catégorie définie par le NIST lors du troisième tour de la campagne.

3. Bien que peu d'exceptions soient attendues dans la pratique, du moins pour la majorité des usages, un algorithme qui n'est pas une norme NIST, mais qui peut être raisonnablement conjecturé au moins aussi solide qu'une norme NIST, pourrait constituer une telle exception. Par exemple, 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.

4. Il s'agit néanmoins d'un choix d'algorithme non standard par rapport à l'utilisation des normes PKC actuelles. Ainsi, lorsqu'un produit soumis à une évaluation de sécurité utilise un algorithme de signature fondé sur le hachage, l'ANSSI peut être amenée à réaliser une analyse cryptographique de cet algorithme dans le cadre de cette évaluation, ce qui peut conduire à un allongement de sa durée.

Pour cette phase, la partie post-quantique ne sera plus considérée comme une *défense en profondeur* : la résistance quantique pourra être revendiquée comme une propriété de sécurité. Dans ce cas, l'évaluation devra permettre de vérifier que des *assurances de sécurité post-quantique* suffisantes sont offerte à la fois pour *la PKC mais aussi pour les mécanismes symétriques* en tant que partie intégrante de l'analyse de sécurité. D'ici là, l'ANSSI aura identifié des critères pour les algorithmes post-quantiques en fonction de leur assurance de sécurité post-quantique associée. Il se peut que les algorithmes ou familles d'algorithmes considérés comme acceptables ne correspondent pas exactement aux normes NIST. Pour cette phase, l'ANSSI recommandera vivement la transition post-quantique pour les produits revendiquant une sécurité à long terme.

Cette phase devrait durer au moins jusqu'aux environs de 2030.

Phase 3 : PQC avec hybridation optionnelle.

L'ANSSI s'attend à ce qu'après plusieurs années d'analyse, le niveau d'assurance de sécurité fourni par les algorithmes post-quantiques soit aussi élevé que le niveau d'assurance pré-quantique actuel. Ainsi, l'utilisation de certains schémas post-quantiques sera potentiellement possible sans hybridation.

Notons que les recommandations présentées ci-dessus évolueront potentiellement en fonction des avancées de la recherche sur la cryptographie post-quantique et de l'avancement de la campagne de normalisation du NIST. Le calendrier prévisionnel sera adapté en conséquence.

Quel est l'impact sur la délivrance des visas de sécurité ?

L'utilisation de la PQC aura également un impact sur la délivrance des visas de sécurité. L'ANSSI accompagnera cette transition et adaptera ses modalités d'évaluation selon le calendrier prévisionnel décrit ci-dessus. La procédure générale [3] sera mise à jour suivant les trois phases comme suit.

> **Phase 1 :** les visas de sécurité *assurent uniquement une sécurité pré-quantique*. La sécurité post-quantique facultative est considérée comme une défense en profondeur.

La méthode d'évaluation des produits de sécurité qui n'utilisent pas de PQC reste inchangée. Pour les produits utilisant la *défense en profondeur* post-quantique, la méthode d'évaluation pour un visa de sécurité sera définie comme suit.

- Tous les mécanismes de sécurité pré-quantiques sont évalués suivant la procédure actuelle [3].
- Le mécanisme d'hybridation sera évalué pour s'assurer qu'il n'induit pas de diminution de la sécurité pré-quantique.
- Même si l'ANSSI examinera les spécifications des algorithmes post-quantiques utilisés, ce derniers ne seront pas évalués par les Centres d'Évaluation de Sécurité (CESTIs). Donc l'assurance post-quantique *ne fera partie d'aucun visa de sécurité*.

En résumé, les visas de sécurité attesteront une évaluation de la sécurité pré-quantique et une vérification que l'utilisation de mécanismes post-quantiques est une *défense en profondeur* qui n'a aucun impact négatif. Aucun jugement formel ne sera porté sur la sécurité quantique offerte par la PQC.

> **Phase 2 :** l'ANSSI pourra délivrer des visas de sécurité assurant une sécurité à long terme pré-quantique et éventuellement post-quantique (toujours avec hybridation obligatoire).

Comme dans la phase 1, la procédure d'évaluation des produits qui n'appliquent pas de protection post-quantique reste inchangée. Pour les produits de sécurité qui suivent les recommandations de l'ANSSI et utilisent l'hybridation avec la PQC, la méthode d'évaluation comprendra une analyse de la sécurité pré-quantique, de l'hybridation et de la résistance quantique. Pour cette dernière, l'analyse devra inclure à la fois des mécanismes symétriques et asymétriques et devra se conformer aux directives officielles sur la résistance quantique qui seront mises à jour d'ici là.

> **Phase 3 :** l'ANSSI pourra délivrer des visas de sécurité assurant une sécurité à long terme pré-quantique et post-quantique avec hybridation facultative. Suivant le contexte, l'ANSSI pourrait continuer ou non de délivrer des visas de sécurité pour les produits ne revendiquant qu'une assurance de sécurité pré-quantique.

Cette dernière phase de transition dépend fortement des avancées de la recherche en cryptographie post-quantique et en informatique quantique. Les spécificités de cette phase seront adaptées au cours de la prochaine décennie.

Quelle est la position des autres autorités nationales de cybersécurité ?
Plusieurs autorités nationales de cybersécurité ont publié des avis similaires recommandant de préparer une migration post-quantique de la cryptographie. Le point de vue de l'ANSSI rejoint la position du BSI allemand[5] sur de nombreuses questions comme la nécessité de la migration, l'hybridation ou la cryptoagilité.

Références

1. ANSSI. Guide des mécanismes cryptographiques. https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf.
2. ANSSI. L'avenir des communications sécurisées passe-t-il par la distribution quantique de clés ? https://www.ssi.gouv.fr/agence/publication/lavenir-des-communications-securisees-passe-t-il-par-la-distribution-quantique-de-cles/.
3. ANSSI. Modalités pour la réalisation des analyses cryptographiques. https://www.ssi.gouv.fr/uploads/2014/11/anssi-cc-cry-p-01-modalites-pour-la-realisation-des-analyses-cryptographiques_v4.1.pdf.
4. ANSSI. Security visas. https://www.ssi.gouv.fr/entreprise/visa-de-securite/.
5. BSI. Migration zu Post-Quanten-Kryptografie. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf;jsessionid=4E25811453CDCA572EE4B949296E89EB.internet472?__blob=publicationFile&v=1.
6. BSI. Status of quantum computer development. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_2.pdf?__blob=publicationFile&v=1.
7. CNRS. La recherche française au cœur du Plan Quantique. https://www.iledefrance-gif.cnrs.fr/fr/cnrsinfo/la-recherche-francaise-au-coeur-du-plan-quantique.
8. CNSS. CNSS advisory memorandum. https://cryptome.org/2015/08/CNSS_Advisory_Memo_02-15.pdf, 2015.
9. ENISA. Post-Quantum Cryptography : Current state and quantum mitigation. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.
10. L. K. Grover. A framework for fast quantum mechanical algorithms. In *30th ACM STOC*, pages 53–62. ACM Press, May 1998.
11. NCSC. Preparing for Quantum-Safe Cryptography. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.
12. NIST. Post-Quantum Cryptography (official standardization webpage). https://csrc.nist.gov/projects/post-quantum-cryptography.
13. RISQ. à paraître. https://risq.fr/.
14. P. Shor. Algorithms for quantum computation : Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, Nov. 1994.
15. SOG-IS. Agreed Cryptographic Mechanisms. https://www.sogis.eu/uk/supporting_doc_en.html.
16. D. Stebila, S. Fluhrer, and S. Gueron. Hybrid key exchange in tls 1.3 (draft IETF). https://tools.ietf.org/id/draft-stebila-tls-hybrid-design-03.html.
17. C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van-Geest, O. Garcia-Morchon, and V. Smyslov. Multiple key exchanges in IKEv2 (draft IETF). https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-multiple-ke/.