Avis de l'ANSSI sur la migration vers la cryptographie post-quantique (suivi 2023)

21 décembre 2023

Ce document est une mise à jour de la position de l'ANSSI sur la transition vers la cryptographie post-quantique au regard des avancées récentes sur le sujet. Il doit être lu comme un addendum à la publication de 2022 [1]. Nous détaillerons nos recommandations en termes d'algorithmes post-quantiques et de techniques d'hybridation.

L'ANSSI a également décidé d'accélérer l'agenda initial. Les premiers visas de sécurité français pour les produits mettant en œuvre de la cryptographie post-quantique hybride devraient être délivrés vers 2024-2025.

L'impact à grande échelle d'un potentiel ordinateur quantique sur nos infrastructures numériques actuelles a été discuté dans le document de synthèse publié par l'ANSSI en 2022 [1]. Bien que la menace quantique n'ait pas connu d'avancée décisive depuis la publication de [1], la cryptographie post-quantique[1], en anglais abrégé PQC, devient de plus en plus une réalité. En effet, les efforts de recherche et de développement sur la conception et l'analyse des algorithmes post-quantiques ont fortement augmenté ces dernières années, tant du point de vue de la sécurité théorique que des implémentations sécurisées. En témoigne le nombre croissant de projets de collaboration et de publications scientifiques sur le sujet en Europe et dans le monde.

Par exemple, comme cela a été récemment publié dans le rapport national sur la stratégie quantique [10, Page 23], le gouvernement français a annoncé avoir investi 350 millions d'euros dans des projets de recherche sur les technologies quantiques et post-quantiques au cours des deux dernières années. Cet investissement comprend cinq projets de recherche en cryptographie post-quantique (PQTLS, RESQUE, HYPERFORM, μPQRS, X7PQC). En outre, quatre schémas ont obtenu le statut de futures normes PQC du NIST [2] : CRYSTALS-Kyber [23], CRYSTALS-Dilithium [14], Falcon [22] et SPHINCS+ [11]. La campagne du NIST pour sélectionner des nouveaux algorithmes post-quantiques se poursuit et d'autres algorithmes candidats rejoindront les quatre futures normes dans les années à venir. Parallèlement, un effort de normalisation croissant sur les protocoles hybrides post-quantiques est perceptible [24, 25, 13]. Plusieurs entreprises déclarent avoir expérimenté des protocoles hybrides pour une grande variété de produits matériels et logiciels.

L'ANSSI considère que ces efforts de recherche et ces développements pratiques sont très positifs et continue d'encourager les concepteurs de produits de sécurité à expérimenter et à prototyper des solutions hybrides post-quantiques et pré-quantiques (c'est à dire classiques), en particulier pour les produits visant une protection de la confidentialité au-delà de 2030 ou les produits qui sont susceptibles d'être encore utilisés après 2030.

1 Recommandations techniques initiales

L'ANSSI encourage toutes les industries à inclure la menace quantique dans leur analyse de risque et à envisager d'inclure des mesures de protection quantique dans les produits cryptographiques concernés.

1. C'est à dire conjecturés résistants à la menace quantique, plus de détails dans la position 2022 [1].

1.1 Hybridation

L'hybridation consiste à combiner des algorithmes asymétriques post-quantiques avec une cryptographie asymétrique pré-quantique bien connue et bien étudiée, fondée sur la factorisation ou le logarithme discret (voir la section 3 pour plus d'informations techniques).

Comme indiqué dans le précédent document de synthèse [1], l'ANSSI insiste toujours fortement sur la nécessité de l'hybridation[2] partout où une protection post-quantique est nécessaire, à la fois à court et à moyen terme.

En effet, même si les algorithmes post-quantiques ont fait l'objet d'une grande attention, ils ne sont pas encore suffisamment matures pour garantir à eux seuls la sécurité. Par exemple, plusieurs algorithmes post-quantiques ont subi des attaques classiques au cours des dernières années : [3, 6]. Cette position est alignée sur celle d'autres agences européennes de cybersécurité comme le BSI en Allemagne [4]. Le BSI a ainsi réaffirmé la nécessité de l'hybridation dans sa récente mise à jour des lignes directrices techniques sur les mécanismes cryptographiques [5, Section 4].

1.2 Stratégie de transition

L'ANSSI encourage toutes les industries à définir une stratégie de transition progressive vers une cryptographie résistante aux attaques quantiques pour les produits cryptographiques concernés. L'utilisation d'une protection hybride post-quantique est recommandée en particulier pour les produits de sécurité destinés à offrir une protection durable des informations (jusqu'à après 2030) ou qui seront potentiellement utilisés après 2030 sans mise à jour.

1.3 Cryptographie symétrique

Bien qu'il n'y ait aucune preuve concrète que les mécanismes cryptographiques symétriques soient menacés de manière significative par les ordinateurs quantiques, on peut s'attendre à une accélération de la recherche exhaustive avec l'algorithme de Grover et d'autres algorithmes avancés basés sur Grover. Ainsi, par mesure de prudence, l'ANSSI encourage également à dimensionner les paramètres des primitives symétriques de manière à assurer une sécurité post-quantique conjecturée ; en pratique, au moins le même niveau de sécurité que l'AES-256 pour les algorithmes de chiffrement par bloc et au moins le même niveau de sécurité que SHA2-384 pour les fonctions de hachage. Cet encouragement est légèrement plus conservateur que les recommandations actuelles du NIST [20] et du BSI [5, Section 4].

2 Algorithmes post-quantiques

L'ANSSI ne fournit traditionnellement pas de liste fermée d'algorithmes recommandés afin de ne pas proscrire des algorithmes innovants qui pourraient être bien adaptés à certains cas d'utilisation particuliers. Ceci est encore plus pertinent pour la cryptographie post-quantique qui est en constante évolution. Nous présentons ci-dessous une liste non exhaustive de mécanismes d'encapsulation de clés asymétriques post-quantiques (ou KEM en anglais abrégé) et d'algorithmes de signatures numériques qui seraient des choix appropriés au moins pour les produits cryptographiques courants. Cette liste est plus particulièrement destinée aux non-experts qui cherchent des orientations dans ce domaine émergent. Il convient de noter que bien que certaines rédactions de normes du NIST aient été récemment publiés [17, 18, 19], il n'est pas possible à ce stade de citer des specifications correctes et fixes pour mettre en œuvre ces algorithmes car les normes ne sont pas encore finalisés.

2. Veuillez noter que l'hybridation est considérée comme étant nécessaire uniquement dans le cas où une protection post-quantique est pertinente.

Mécanismes d'encapsulation de clé.

— **CRYSTALS-Kyber, aussi appelé ML-KEM** [23, 18] : la sécurité de ce schéma est fondée sur le problème mathématique « Module Learning With Errors ». Ce problème est lui-même lié à la difficulté de trouver des vecteurs courts dans un réseau euclidien structuré (nous nous référons à une étude [21] pour plus d'informations sur ce problème et sur les réseaux euclidiens en général). Ces problèmes fondés sur des réseaux euclidiens ont été particulièrement étudiés au cours de la dernière décennie. En outre, l'efficacité de CRYSTALS-Kyber le rend comparable aux solutions pré-quantiques : le temps de calcul est similaire, avec une expansion modérée de la taille des messages et des clés échangés. Son efficacité et sa simplicité font partie des raisons pour lesquelles CRYSTALS-Kyber a été choisi comme une future norme post-quantique du NIST. CRYSTALS-Kyber devrait donc être le principal KEM post-quantique dans les produits de sécurité et les protocoles internet.
Bien que plusieurs résultats théoriques permettent d'avoir confiance en la sécurité de cet algorithme, la sécurité post-quantique est encore conjecturée, en particulier pour le régime de paramètres concrets choisis.

Si cet algorithme est retenu pour être inclus dans des produits cryptographiques, l'ANSSI formule les recommandations suivantes :

1. Il est important d'éviter de modifier les paramètres de l'instance normalisée.
2. Les paramètres sont définis pour plusieurs niveaux de sécurité. Nous recommandons d'utiliser le niveau de sécurité NIST le plus élevé possible, de préférence le niveau 5 (équivalent à l'AES-256) ou le niveau 3 (équivalent à l'AES-192).
3. Nous recommandons d'utiliser autant que possible des clés éphémères. L'utilisation systématique de clés privées éphémères permet de prévenir de nombreuses attaques telles que les attaques utilisant des oracles d'échecs de déchiffrement.
4. Nous recommandons également d'utiliser la version sécurisée contre les attaques actives (IND-CCA) qui sera normalisée par le NIST. Dans certains cas, comme dans les protocoles authentifiés disposant de preuves de sécurité, la version sécurisée contre les attaquants passifs (IND-CPA) en mode statique ou éphémère peut être considérée comme sûre. Mais il faut alors veiller à ce qu'aucun oracle d'échec de déchiffrement ne soit disponible en toutes circonstances, même en cas d'attaque par canaux auxiliaires.

— **FrodoKEM** [16] : ce schéma est considéré comme une variante plus conservatrice de CRYSTALS-Kyber. Sa sécurité est fondée sur le problème mathématique « Learning With Errors » (et non « Module Learning With Errors »). La propriété non structurée du réseau euclidien sous-jacent le rend plus sûr en théorie, car les attaques pourraient potentiellement tirer parti de la structure du réseau euclidien de CRYSTALS-Kyber et pourraient être déjouées par l'absence de structure dans le réseau utilisé par FrodoKEM. Le prix à payer pour cette sécurité plus conservatrice réside dans les performances. FrodoKEM est plus lourd en ce qui concerne les taille de clés et plus lent que CRYSTALS-Kyber, ce qui en fait une option moins pertinente pour de nombreux cas d'utilisation. Cependant, l'ANSSI encourage l'inclusion de FrodoKEM comme une option valable et conservatrice dans les applications de haute sécurité où la pénalité de performance résultante (en particulier en ce qui concerne la bande passante) n'est pas prohibitive.

Si un développeur choisit d'inclure cet algorithme post-quantique conservateur dans un produit cryptographique, les recommandations concernant CRYSTALS-Kyber s'appliquent également à FrodoKEM.

Signatures numériques.

— **CRYSTALS-Dilithium, aussi appelé ML-DSA** [14, 17] : cette signature appartient à la même suite que CRYSTALS-Kyber et a été choisie par le NIST comme future norme post-quantique. La

sécurité de cette signature est également basée sur des problèmes de réseaux euclidiens structurés. La conception est proche des signatures de Schnorr, bien connues dans le domaine des signatures numériques.Cet algorithme est relativement facile à mettre en œuvre, mais les signatures ne sont pas aussi compactes que les solutions pré-quantiques. Comme pour les autres signatures fondées sur des réseaux euclidiens structurés, la découverte de faiblesses relatives au problème de réseau euclidien (structuré) sous-jacent dans les années à venir n'est pas totalement exclue.

Pour les produits cryptographiques susceptibles d'inclure cet algorithme, l'ANSSI formule les recommandations suivantes :

1. Il est important d'éviter de modifier les paramètres de l'instance normalisée.
2. Les paramètres sont définis pour plusieurs niveaux de sécurité. Nous recommandons d'utiliser le niveau le plus élevé possible, de préférence le niveau 5 (équivalent à l'AES-256) ou le niveau 3 (équivalent à l'AES-192).

— **Falcon, aussi appelé FN-DSA** [22] : cette signature a aussi été choisie par le NIST comme future norme post-quantique. Il s'agit d'une alternative à CRYSTALS-Dilithium compacte et plus efficace. Comme elle est fondée sur des problèmes de réseaux euclidiens structurés, le même avertissement concernant la sécurité s'applique. La conception est ici fondée sur une structure plus récente [8] avec un paradigme de hachage suivi d'une signature (« hash and sign » en anglais). Elle est plus difficile à mettre en œuvre et nécessite que certaines variables intermédiaires soient représentées par des nombres flottants.

Pour les produits cryptographiques susceptibles d'inclure cet algorithme, l'ANSSI formule les recommandations suivantes :

1. Il est important d'éviter de modifier les paramètres de l'instance normalisée. La mise en œuvre de Falcon n'étant pas simple, nous recommandons de veiller à respecter la conception afin d'éviter les attaques qui exploiteraient des erreurs d'implementation. Il convient également de noter que les distributions gaussiennes de Falcon jouent un rôle important dans la sécurité et qu'elles ne doivent pas être remplacées.
2. Les paramètres sont définis pour plusieurs niveaux de sécurité. Nous recommandons d'utiliser le niveau le plus élevé possible, de préférence le niveau 5 (équivalent à AES-256).
3. Veuillez noter que les contre-mesures contre les attaques par canaux auxiliaires sont particulièrement difficiles à appliquer pour Falcon. De plus, des publications scientifiques montrent régulièrement que les attaques par canaux auxiliaires peuvent mettre en échec les implémentations non protégées de Falcon.

— **XMSS** [12] / **LMS** [15] : ces algorithmes de signature étaient initialement candidats à la campagne de normalisation post-quantique du NIST, mais en 2018, ils ont été placés dans un processus de normalisation distinct. La version IETF de leur spécification est citée ci-dessus. Ces algorithmes sont considérés comme des options conservatrices car l'hypothèse de sécurité sous-jacente est très minimaliste. Leurs preuves de sécurité sont fondées sur la sécurité des fonctions de hachage. La particularité de ces signatures réside dans leur caractère évolutif et dans le nombre potentiellement limité de signatures possibles par bi-clés. *Pour les contextes dans lesquels le nombre maximal de signatures par bi-clés est restreint et où un état peut être soigneusement stocké, typiquement pour les mises à jour de logiciels par exemple, l'ANSSI convient que XMSS ou LMS peuvent être une option pertinente, avec les recommandations suivantes :*

1. Il est important d'éviter de modifier les paramètres de l'instance normalisée, y compris la fonction de hachage sous-jacente.
2. Les paramètres doivent offrir le niveau de sécurité le plus élevé possible.
3. La recommandation sur l'hybridation (voir la section 3 pour plus d'informations) est facultative pour cette signature.

4. L'état interne de l'algorithme de signature est une donnée très critique et doit être protégé en intégrité. Il doit également être protégé contre les attaques par rejeu.

— **SPHINCS+, aussi appelé SLH-DSA** [11, 19] : ce schéma de signature a été choisi par le NIST comme future norme post-quantique. Il s'agit d'une variante sans état interne à conserver de XMSS. Ce schéma est également considéré conservateur, car sa preuve repose également sur la sécurité des fonctions de hachage. Il est moins compétitif en termes de performances et de compacité, ce qui le rend difficile à appliquer dans certains cas d'utilisation.

Dans les contextes où SPHINCS+ peut être supporté, l'ANSSI considère que cette signature est une option pertinente et conservatrice. L'hybridation pour SPHINCS+ peut également être optionnelle (voir section 3 pour plus d'informations). Les trois premières recommandations pour XMSS/LMS s'appliquent également ici.

Nous rappelons que d'autres systèmes post-quantiques peuvent également constituer de bonnes options, par exemple les candidats encore en lice pour la campagne de normalisation du NIST. Nous recommandons toujours d'utiliser des algorithmes qui sont bien étudiés et analysés dans un grand nombre de publications de recherche.

3 Modes d'hybridation

L'hybridation consiste à combiner deux schémas cryptographiques (ou plus) permettant d'obtenir la même fonctionnalité de manière robuste. En d'autres termes, la combinaison doit être sûre dans le modèle de preuve classique/quantique tant qu'au moins un schéma sous-jacent est sûr dans ce modèle. Nous nous référons à [1] pour plus de détails sur la définition.

3.1 Modes d'hybridation pour les mécanismes d'encapsulation de clés

Considérons un système d'encapsulation de clés pré-quantique fondé sur RSA ou Diffie-Hellman, par exemple ECDH. Pour prévenir la menace quantique, l'objectif est de combiner la clé dérivée avec une (ou plusieurs) clé(s) supplémentaire(s) des types suivants.

— Une clé pré-partagée peut être stockée par les deux parties. Cette technique garantit une certaine résistance post-quantique car elle repose sur le paradigme de la cryptographie symétrique. En fonction du contexte, cette technique peut être considérée comme une bonne (bien qu'imparfaite) solution dans des contextes spécifiques (par exemple, les VPN), mais l'ANSSI émet les avertissements suivants :

1. La confidentialité et l'intégrité de la clé pré-partagée sont des conditions préalables essentielles.
2. Chaque clé pré-partagée ne doit être partagée que par deux parties et non par un groupe de trois parties ou plus.
3. Il convient de noter qu'une telle technique ne permet pas de garantir une confidentialité parfaite dans le temps (abrégé en anglais par PFS) contre les adversaires quantiques.

— Une autre solution privilégiée qui ne souffre pas des limitations d'une hybridation avec une clé pré-partagée consiste à calculer des clés supplémentaires à l'aide de KEMs post-quantiques tels que ceux décrits à la section 2.

Une fois que toutes ces clés sont dérivées, le problème se résume à la manière dont les deux clés sont combinées ensemble et à la manière dont l'échange est authentifié.

Comment combiner les clés en toute sécurité ? Il existe de nombreuses façons de concevoir des techniques de combinaison. Remarquons que la concaténation des clés ne garantit pas la sécurité contre les attaquants passifs (IND-CPA), car si une clé sous-jacente est compromise, la clé concaténée n'est pas uniformément aléatoire. En outre, le fait d'additionner les clés ensemble (à l'aide d'un ou exclusif ou XOR)

offre une sécurité contre les attaquants passifs [9, Lemme 1]] mais pas contre les attaquants actifs en raison des attaques « mix and match » [9, Lemma 2]. L'utilisation d'une fonction de dérivation de clé (Key Derivation Function - KDF) est un élément essentiel pour combiner des clés en toute sécurité. Ces fonctions permettent de produire une (ou plusieurs) clé(s) à partir d'une source commune. Les modes d'hybridation présentés dans [7] contiennent (1) un combineur parallèle qui consiste en l'application d'une concaténation et l'application d'une KDF et (2) un mode cascade qui peut être considéré comme un combineur en série. Ces deux solutions sont étayées par des preuves de sécurité et semblent être de bonnes solutions pour combiner des clés entre elles.

De manière générale, comme pour toute fonction cryptographique, l'ANSSI recommande d'utiliser des normes ou des modes bien étudiés avec des preuves de sécurité validées.

La sécurité des implémentations de l'hybridation est également très importante pour éviter les attaques physiques qui contourneraient certaines encapsulations de clés.

L'hybridation est-elle disponible dans les protocoles existants ? Certains travaux visent à inclure la cryptographie post-quantique en tant qu'option dans TLS avec un mode d'hybridation utilisant une concaténation et une KDF [24]. Le protocole IKE évolue également pour inclure la cryptographie post-quantique hybride. Dans la RFC publiée en mai 2023 [25], les mécanismes utilisent des modes d'hybridation inspirés des deux combineurs présentés dans [7].

3.2 Modes d'hybridation pour les signatures

Les solutions pour les signatures hybrides sont moins diversifiées que les solutions KEM hybrides. Considérons un ensemble de schémas de signature pré-quantique et post-quantique. Un moyen robuste et naturel de combiner ces signatures consiste à les concaténer et à accepter cette concaténation de signatures comme une signature valide si, et seulement si, toutes les signatures sont valides. Ce combineur s'avère sûr dans le modèle de sécurité le plus courant pour les signatures (EUF-CMA).

À un niveau supérieur, l'hybridation des signatures peut être réalisée au niveau du certificat. Cependant, les conceptions et les preuves de sécurité de ces protocoles de certificats hybrides sont encore en évolution, l'ANSSI n'a pas encore identifié de schéma bien défini qui pourrait être cité ici.

4 Mise à jour de la procédure de délivrance des visas de sécurité français

Comme décrit dans [1], l'ANSSI entend suivre une feuille de route en trois phases pour la délivrance des visas de sécurité. La date de démarrage de la deuxième phase était initialement prévue aux alentours de 2025. Nous rappelons que dans la deuxième phase, les tâches d'évaluation cryptographique des visas de sécurité comprennent une analyse de tous les algorithmes cryptographiques, y compris les algorithmes post-quantiques avec une hybridation obligatoire. En plus de la reconnaissance classique de l'assurance de l'état de l'art, le certificat délivré par l'ANSSI pourra désormais mentionner la présence d'une protection post-quantique à l'état de l'art.

L'ANSSI est en train d'accélérer l'agenda initial. Les premiers visas de sécurité de la phase 2 pour les produits mettant en œuvre la cryptographie post-quantique hybride devraient être délivrés vers 2024-2025.

Les développeurs intéressés par l'évaluation de leurs produits mettant en œuvre la PQC hybride sont invités à contacter les centres d'évaluations (CESTIs) pour plus de détails. Dans ce qui suit, nous apportons une clarification concernant l'évaluation des produits mettant en œuvre la PQC hybride qui n'a pas été incluse dans la publication originale [1].

Distinguons deux types de produits de sécurité : les produits finaux et les produits intermédiaires ou produits-plateformes.

Le premier type concerne les produits finaux. Dans ce cas, tout produit qui inclut une protection post-quantique doit mettre en œuvre l'hybridation, sauf dans les rares cas où la protection post-quantique repose uniquement sur des signatures basées sur le hachage comme XMSS, LMS ou SPHINCS+, pour lesquelles l'hybridation est facultative [3].

Le deuxième type consiste en des produits-plateformes qui fournissent des fonctionnalités cryptographiques à une couche supérieure (applicative). Dans le contexte de l'évaluation de la sécurité de ces produits, la mise en œuvre d'une simple cryptographie post-quantique sans hybridation peut parfois être pertinente, car l'hybridation fera partie des couches supérieures orientées vers l'utilisateur. Les équipes d'évaluation de l'ANSSI exigeront dans ce cas (1) la mise en œuvre d'une application avec un mode d'hybridation à des fins de test et (2) l'inclusion dans les guides pour les utilisateurs d'une recommandation d'utiliser exclusivement l'algorithme post-quantique fourni en combinaison avec un algorithme classique reconnu dans le cadre d'un mode d'hybridation.

Bibliographie

[1] ANSSI. Avis de l'ANSSI sur la migration vers la cryptographie post-quantique. https://cyber.gouv.fr/publications/avis-de-lanssi-sur-la-migration-vers-la-cryptographie-post-quantique.

[2] ANSSI. Sélection par le nist de futurs standards en cryptographie post-quantique. https://cyber.gouv.fr/actualites/selection-par-le-nist-de-futurs-standards-en-cryptographie-post-quantique.

[3] W. Beullens. Breaking rainbow takes a weekend on a laptop. In Y. Dodis and T. Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 464–479, Cham, 2022. Springer Nature Switzerland.

[4] BSI. Migration to post quantum cryptography. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html.

[5] BSI. Technical guideline on cryptographic mechanisms : Recommendations and key lengths, 2023. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile.

[6] W. Castryck and T. Decru. An efficient key recovery attack on sidh (preliminary version). Cryptology ePrint Archive, Paper 2022/975, 2022. https://eprint.iacr.org/2022/975.

[7] ETSI. Quantum-safe hybrid key exchanges.

[8] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. pages 197–206, 2008.

[9] F. Giacon, F. Heuer, and B. Poettering. Kem combiners. In M. Abdalla and R. Dahab, editors, *Public-Key Cryptography – PKC 2018*, pages 190–218, Cham, 2018. Springer International Publishing.

[10] F. Government. France national quantum strategy. https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2023/04/france2030_quantique_rapport_activite_2022_vdef2.pdf.

[11] A. Hulsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, J.-P. Aumasson, B. Westerbaan, and W. Beullens. SPHINCS+. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[12] A. Hulsing, D. Butin, S. Gazdag, J. Rijneveld, and A. Mohaisen. XMSS : eXtended Merkle Signature Scheme. https://datatracker.ietf.org/doc/rfc8391/.

[13] IETF. Post-quantum use in protocols (pquip). = https ://datatracker.ietf.org/wg/pquip/about.

[14] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehlé, and S. Bai. CRYSTALS-DILITHIUM. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

3. Il s'agit néanmoins d'un choix d'algorithme non standard par rapport à l'utilisation des normes 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.

[15] D. McGrew, M. Curcio, and S. Fluhrer. Leighton-micali hash-based signatures. https://datatracker.ietf.org/doc/rfc8554/.

[16] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia, P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. FrodoKEM. Technical report, National Institute of Standards and Technology, 2020. available at https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions.

[17] NIST. Module-lattice-based digital signature standard. https://csrc.nist.gov/pubs/fips/204/ipd.

[18] NIST. Module-lattice-based key-encapsulation mechanism standard. https://csrc.nist.gov/pubs/fips/203/ipd.

[19] NIST. Stateless hash-based digital signature standard. https://csrc.nist.gov/pubs/fips/205/ipd.

[20] NIST. FAQ on post-quantum cryptography, 2018. https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs.

[21] C. Peikert. A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939, 2015. https://eprint.iacr.org/2015/939.

[22] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. FALCON. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[23] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, G. Seiler, D. Stehlé, and J. Ding. CRYSTALS-KYBER. Technical report, National Institute of Standards and Technology, 2022. available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.

[24] D. Stebila, S. Fluhrer, and S. Gueron. Hybrid key exchange in TLS 1.3 (draft IETF). https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/.

[25] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van-Geest, O. Garcia-Morchon, and V. Smyslov. Multiple Key Exchanges in IKEv2 (IETF). https://datatracker.ietf.org/doc/html/rfc9370.