ANSSI views on the Post-Quantum Cryptography transition (2023 follow up)

December 21, 2023

This document is an update of ANSSI's position on the post-quantum cryptography transition in view of the recent advances in the topic. It should be read as an addendum to 2022's publication [1]. We will detail our recommendations in terms of post-quantum algorithms and hybridation techniques.

ANSSI also decided to speed-up the original agenda. First French security visas for products implementing hybrid post-quantum cryptography are expected to be delivered around 2024-2025.

The impact of a potential large scale quantum computer on our current digital infrastructures has been discussed in ANSSI 2022's position paper [1]. While the quantum threat did not undergo any game-changing advance since the publication of [1], post-quantum cryptography, PQC for short, is becoming more and more a reality. Indeed, the research and development efforts on the design and analysis of post-quantum algorithms has highly increased in the last few years, concerning both theoretical hardness and secure implementations perspectives. This is attested by the increasing number of collaborative projects and scientific publications on the subject in Europe and abroad.

For instance, as recently published in a report [10, Page 23], the French government has announced investing 350M euros in research projects on quantum technologies in the past two years. This investment includes five post-quantum cryptography research projects (PQTLS, RESQUE, HYPERFORM, μPQRS, X7PQC). Furthermore, four schemes have gained the status of NIST first future PQC standards [2]: CRYSTALS-Kyber [23], CRYSTALS-Dilithium [14], Falcon [22] and SPHINCS+ [11]. The NIST campaign for post-quantum algorithms is still ongoing and other candidate algorithms will join the four future standards in the next years. In parallel, an increasing standardization effort on hybrid post-quantum protocols is noticeable [24, 25, 13]. Several companies report having now experimented hybrid protocols for a large variety of hardware and software products.

ANSSI considers that such research efforts and practical developments are very positive and continues to encourage designers of security products to start experimenting and prototyping hybrid post-quantum and pre-quantum solutions, especially for products aiming at a confidentiality protection that will last beyond 2030 or products that are likely to still be used after 2030.

1 Initial technical recommendations

ANSSI encourages all industries to include the quantum threat in their risk analysis and to consider including quantum mitigation in the relevant cryptographic products.

1.1 Hybridation

Hybridation consists of combining asymmetric post-quantum algorithms with well known and well studied pre-quantum asymmetric cryptography based on factorization or discrete logarithm (see Section 3 for more technical information).

As outlined in the previous position paper [1], ANSSI still strongly emphasizes the necessity of hybridation[1] wherever post-quantum mitigation is needed both in the short and medium term.

Indeed, even if the post-quantum algorithms have gained a lot of attention, they are still not mature enough to solely ensure the security. For example, several post-quantum schemes have suffered from classical attacks in the past years, e.g. [3, 6]. This position is aligned with the one of other European cybersecurity agencies like BSI in Germany [4]. BSI has even re-stated the need for hybridation in their recent updated technical guideline on cryptographic mechanisms [5, Section 4].

1.2 Transition strategy

ANSSI encourages all industries to define a progressive transition strategy towards quantum-resistant cryptography for relevant cryptographic products. The use of hybrid post-quantum mitigation is recommended especially for security products aimed at offering a long-lasting protection of information (until after 2030) or that will potentially be used after 2030 without updates.

1.3 Symmetric cryptography

While there is no concrete evidence that symmetric cryptographic mechanisms would be significantly threatened by quantum computers, a speedup can be expected in certain cases with Grover algorithm and other advanced Grover-based algorithms. Thus, as a conservative measure, ANSSI also encourages to dimension the parameters of symmetric primitives as to ensure a conjectured post-quantum security – in practice at least the same security level as AES-256 for block ciphers and at least the same security level as SHA2-384 for hash functions. This encouragement is slightly more conservative than NIST's [20] and BSI's current recommendation [5, Section 4].

2 Post-quantum algorithms

ANSSI traditionally does not provide any closed list of recommended algorithms in order to avoid proscribing innovative state-of-the-art algorithms that could be well-suited for some particular use cases. This is even more relevant for the ever-moving post-quantum cryptography. We present below a non exhaustive list of post-quantum asymmetric key encapsulation mechanisms (KEMs) and digital signature algorithms that would be appropriate choices at least for mainstream cryptographic products. This list is particularly aimed at non-experts looking for directions on this emerging domain. Note that while some draft NIST standards were recently published [18, 17, 19], pointing at fixed correct manners to implement these algorithms is not possible at this stage as the standards are not finalized yet.

Key Encapsulation Mechanisms.

- **CRYSTALS-Kyber also called ML-KEM** [23, 18]: the security of this scheme is based on the module-learning with errors lattice problem (we refer to a survey [21] for more information on lattices). This problem is itself related to the difficulty of finding short vectors in structured lattices. These lattice-based problems have been particularly studied during the last decade. Besides, the efficiency of CRYSTALS-Kyber makes it comparable to the pre-quantum solutions: the computation time is similar, with a moderate expansion on the size of exchanged messages and keys. Its competitive efficiency and simplicity are part of the reasons why CRYSTALS-Kyber was selected as a first NIST post-quantum

[1] Please note that hybridation is necessary only if a post-quantum protection is relevant.

standard. Hence, CRYSTALS-Kyber is expected to be the primary post-quantum KEM in security products and internet protocols.

While several theoretical results provide a good confidence in the security of this scheme, the post-quantum security is only conjectured, especially in the chosen range of concrete parameters.

If this scheme is chosen for being included in cryptographic products, ANSSI makes the following recommendations:

1. It is important to avoid modifying the parameters of the standardized instance.
2. The parameters are defined for several minimum security levels. We recommend to use the highest NIST security level as possible, preferably level-5 (i.e. equivalent to AES-256) or level-3 (i.e. equivalent to AES-192).
3. We recommend to use ephemeral keys as much as possible. The systematic use of ephemeral private keys allows to prevent many attacks like decryption failures ones.
4. We also recommend to use the actively secure version (IND-CCA) that will be standardized by NIST. There are some cases, like in provable authenticated protocols, where the passively secure (IND-CPA) version in static or ephemeral mode may still be secure. But an extra care must then be paid to make sure that no decryption oracle is available under any circumstance even in the case of side-channel attacks.

- **FrodoKEM** [16]: this scheme is considered as a more conservative variant of CRYSTALS-Kyber. Its security is based on plain (and not module) learning with errors. The unstructured property of the underlying lattice makes it more secure in theory as attacks might potentially leverage the lattice structure of CRYSTALS-Kyber and might be defeated by the absence of structure in the lattice used by FrodoKEM. The price to pay for this more conservative security lies in the performance. FrodoKEM is heavier in terms of key sizes and slower than CRYSTALS-Kyber which makes it a less relevant option for many use cases. However, ANSSI would encourage including FrodoKEM as a valid and conservative option in high security applications where the resulting performance penalty (in particular in terms of bandwidth) is not prohibitive.

  If a designer chooses to include this conservative post-quantum algorithm in a cryptographic product, the recommendations for CRYSTALS-Kyber also apply for FrodoKEM.

Digital signatures.

- **CRYSTALS-Dilithium also called ML-DSA** [14, 17]: this signature belongs to the same suite as CRYSTALS-Kyber and has been chosen by NIST as a future post-quantum standard. The security of this signature is also similarly based on structured lattice problems. The design is close to Schnorr signatures, it is issued from a well-known identification protocol. This scheme is relatively easy to implement but the signatures are not as compact as pre-quantum solutions. Similarly to other structured lattice-based schemes, note that one could not entirely preclude the discovery of weaknesses relative to the (structured) lattice underlying problem in the coming years.

  For cryptographic products that may include this scheme, ANSSI makes the following recommendations:

  1. It is important to avoid modifying the parameters of the standardized instance.
  2. The parameters are defined for several minimum security levels. We recommend to use the highest level as possible, preferably level-5 (i.e. equivalent to AES-256) or level-3 (i.e. equivalent to AES-192).

- **Falcon also called FN-DSA** [22]: this signature has been chosen by NIST as a future post-quantum standard. It is a compact and more efficient alternative to CRYSTALS-Dilithium. Since it is based on structured lattice problems, the same warning about the security applies. The design is here based on a more recent framework [8] with a hash-and-sign paradigm on lattices. It is more difficult to implement and needs intermediate variables to be defined as floats.

  For cryptographic products that may include this scheme, ANSSI makes the following recommendations:

  1. It is important to avoid modifying the parameters of the standardized instance. As implementing Falcon is not straightforward, we recommend to pay attention to stick to the design in order to avoid misuse attacks. We should also note that the Gaussian distributions in Falcon play an important role in the security and they should not be replaced.
  2. The parameters are defined for several minimum security levels. We recommend to use the highest level as possible, preferably level-5 (i.e. equivalent to AES-256).
  3. Please note that side-channel countermeasures are particularly difficult to apply and research has proved that side-channel attacks may defeat unprotected implementations of Falcon.

- **XMSS** [12] / **LMS** [15]: these signature schemes were initially candidates in the NIST post-quantum standardization campaign but in 2018, they have been moved into a separate standardization process. The IETF version of their specification is cited above. These schemes are considered as conservative options because the underlying security hypothesis is very minimalist. Their security proofs are based on the security of hash functions. The particularity of these signatures is their statefulness and the potentially limited number of possible signatures per key pair.

  For contexts where the maximum number of signatures per key pair is restricted and where a state can be carefully stored, typically for software updates for example, ANSSI agrees that XMSS or LMS can be a relevant option, with the following recommendations:

  1. It is important to avoid modifying the parameters of the standardized instance including the underlying hash function.
  2. The parameters should provide the highest security level as possible.
  3. Hybridation (see Section 3 for more information) is optional for this signature.
  4. The state is a very critical data and should be protected in integrity. It should also be protected against replay attacks.

- **SPHINCS+ also called SLH-DSA** [11, 19]: this signature scheme has been chosen by NIST as a future post-quantum standard. It is a stateless variant of XMSS. This scheme is also considered as conservative as its proof relies on the security of hash functions as well. It is less competitive in terms of performance and compactness which makes it difficult to apply in certain use cases.

  For contexts where one can afford SPHINCS+, ANSSI considers that this signature is a relevant and conservative option. Hybridation for SPHINCS+ may also be optional (see Section 3 for more information). The first three recommendations for XMSS / LMS also apply here.

We recall that some other post-quantum schemes may be good options too, for example candidates that are still in the run for the NIST standardization campaign. We always recommend to use algorithms that are well studied and analyzed in a large number of research publications.

3 Hybridation modes

The hybridation consists in combining two (or more) cryptographic schemes achieving the same functionality in a robust way. In other words, the combination should be secure in the classical/quantum computation

model as long as one underlying scheme is secure in that model. We refer to [1] for more details about the definition.

3.1 Hybridation modes for key encapsulation mechanisms

Consider a pre-quantum key encapsulation scheme based on RSA or Diffie-Hellman, for instance ECDH. To prevent the quantum threat, the goal is to combine the derived key with one (or more) extra keys of the following types.

- A pre-shared key can be stored by both parties. This technique ensures a certain post-quantum resistance as it relies on a symmetric cryptographic basis. Depending on the context, this technique might be seen as a good (though non perfect) solution in specific contexts (e.g. VPNs) but ANSSI raises the following warnings:
  1. The confidentiality and integrity of the pre-shared key is a crucial pre-requisite.
  2. Each pre-shared key must only be shared by two parties and not by a group of three or more parties.
  3. Note that such a technique fails to ensure perfect forward secrecy (PFS) against quantum adversaries.

- Another preferred solution that does not suffer from the limitations of an hybridation with a pre-shared key is to compute extra keys with post-quantum KEMs algorithms like the ones outlined in Section 2.

Once all these keys are derived, the issue boils down to the way both keys are combined together and the way the exchange is authenticated.

How to securely combine the keys together? There are actually many ways to design combining techniques. Let us remark that concatenating the keys would not ensure security against passive attackers (IND-CPA) as if an underlying key is compromised, the concatenated key is not uniform. In addition, xoring the keys together provides security against passive attackers [9, Lemma 1] but not against active attackers because of mix and match attacks [9, Lemma 2]. One essential building block for securely combining keys together is the use of a Key Derivation Function (KDF). Such functions allow to output one or more keys from a common input key material. The hybridation modes presented in [7] contain (1) a parallel combiner that consists of a concatenation and KDF application and (2) a cascade mode that can be viewed as a serial combiner. Both are backed-up by security proofs and seem good solutions for combining keys together.

In general, as for any cryptographic function, ANSSI recommends to use standards or well studied modes with validated security proofs.

The implementation security of the hybridation is also very important to avoid attacks that would bypass certain key encapsulations.

Is hybridation available in existing protocols? There is some work to include post-quantum cryptography as an option in TLS with an hybridation mode using concatenation and KDF [24]. The protocol IKE is also evolving to include hybrid post-quantum cryptography. In the RFC published in May 2023 [25], the design uses hybridation modes inspired from both combiners presented in [7].

3.2 Hybridation modes for signatures

The solutions for hybrid signatures are less diverse than hybrid KEM solutions. Let us consider a set of pre-quantum and post-quantum signature schemes. A robust and natural way of combining these signatures together consists of concatenating the signatures and accepting such a concatenation of signatures as a valid

signature if and only if all of them are valid. This combiner is proved secure in the more common security model for signatures (EUF-CMA).

On a higher level, the hybridation of signatures can be performed at a certificate level. However, the designs and security proofs of such hybrid certificate protocols are still currently moving, ANSSI did not yet identify any well-defined design that could be cited here.

4 Update on the French security visas delivery process

As described in [1], ANSSI intends to follow a 3-phase roadmap for delivering security visas. The start date of the second phase was initially planned around 2025. We recall that in the second phase, the cryptographic evaluation tasks of security visa evaluation comprise an analysis of all cryptographic algorithms including the post-quantum algorithms with mandatory hybridation. In addition to the classical state-of-the-art assurance recognition, the security visa report can now mention the presence of state-of-the-art post-quantum protection.

ANSSI is currently speeding-up the original agenda. First phase-2 security visas for products implementing hybrid post-quantum cryptography are expected to be delivered around 2024-2025.

Developers interested in evaluating their products implementing hybrid PQC are invited to contact ITSEFs for details. In the following, we provide a clarification regarding evaluation of products implementing hybrid PQC that was not included in the original publication [1].

Let us distinguish two types of security products: end products and intermediate products. The first type means final products. In that case, any product that includes post-quantum mitigation shall implement hybridation except if the quantum mitigation only relies on hash-based signatures like XMSS, LMS or SPHINCS+ for which hybridation is optional[2].

The second type consists of platform products that provide raw cryptographic functionalitites to an upper (applicative) layer. In the context of the security evaluation of such products, implementing mere post-quantum cryptography without hybridation can sometimes be relevant as hybridation will be part of upper user-oriented layers. ANSSI evaluation teams will require in that case (1) an implementation of an hybridation mode for test purposes and (2) the inclusion in the user guidance documentation of a recommendation to exclusively use the provided post-quantum algorithm in combination with a recognized classical algorithm as part of an hybridation mode.

References

[1] ANSSI. ANSSI views on the post-quantum cryptography transition. https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition.

[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.

[2] This is nevertheless a non-standard algorithm choice compared to the use of current standards. Thus, some analysis of the algorithm may have to be performed by ANSSI as part of an evaluation, and this may lead to an increase of the certification process duration.

[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.

[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.