ANSSI views on the Post-Quantum Cryptography transition

March 30, 2022

In this position paper, the current ANSSI views on the so-called post-quantum cryptography transition are outlined. In particular, ANSSI recalls the context of the quantum threat and introduces a *provisional transition agenda* to prevent this quantum threat with a progressive increase of assurance on the new post-quantum algorithms without introducing any vulnerability accessible via today's classical computers. The objective of this paper is twofold: providing directions to industrials developing security products and outlining the transition agenda in terms of French security visas [4].

What are quantum computers?
Quantum computers are based on physical principles that are fundamentally different from those underlying today's classical computing. At a large scale, they would be capable of performing certain tasks much faster than today's computers.

While prototypes of small quantum computers, often designated by NISQ (Noisy Intermediate Scale Quantum computers) already exist, building large scale re-programmable ones is still at a very upstream research stage. There are many lines of research in quantum physics for the creation of such quantum computers but none of them is certain to succeed. Though their potential benefits are not fully known, they could obviously be high. Thus, the industry, governments and academia around the world are devoting significant resources to research in quantum computing. For example, in 2021, the French government announced an investment of more than 1 billion € in quantum technologies, including quantum computing [8]. A complete survey on the status of quantum computer development has been detailed by the BSI, the German counterpart of ANSSI [7].

Quantum threat: what is the impact on our current digital infrastructures?
The security of the majority of digital infrastructures relies on public key cryptography (PKC), a technology that enables secure communications between entities, typically users or servers, that do not share any pre-established secret. More precisely, PKC serves two main functionalities: protected channel establishment (key establishment) and authentication of digital information (including authentication of parties inside a communication protocol by the use of digital signatures).

Today, these techniques are essentially based on two mathematical problems: the factorization of large numbers and the discrete logarithm computation. Both are dimensioned to be virtually impossible to solve with our current computing resources and mathematical knowledge. For example, the well-known RSA public key algorithm relies on the factorization of large numbers.

These two fundamental problems will no longer be unsolvable if a large scale quantum computer is built and thus the security of currently deployed public key cryptography could potentially collapse. Indeed, in 1994, P. Shor introduced a quantum algorithm [15] able to solve these problems quite efficiently. This algorithm cannot be performed on classical computers but it could be performed on large scale ones. To avoid any confusion with the existing prototypes of small scale quantum computers, the NCSC, British counterpart of ANSSI, introduced the name of Cryptographically Relevant Quantum Computers, CRQCs (see the NCSC's whitepaper on quantum-safe cryptography [12]). In other words, a CRQC is a quantum computer that is able to execute relevant instances of Shor's algorithm and thus threatening today's public-key cryptography.

The prototypes of quantum computers that exist are presently far from the required scale and stability of CRQCs and therefore they are currently not a threat to public key cryptography. Many research challenges in physics, engineering and computer science must be overcome before scaling up to large quantum computers able to solve the factorization and discrete logarithm problems on which the current PKC is based.

However, the threat of retroactive attacks cannot be ruled out. A family of attacks, called **"store now, decrypt later attacks"**, constist in storing today the data exchange corresponding to a secure channel establishment and the encrypted messages over such a channel, with the purpose of eventually decrypting these messages once a CRQC becomes available. This threat could be relevant in certain scenarios involving very sensitive information, e.g. classified information.

Furthermore, the quantum threat could also impact digital signatures. Indeed, a CRQC could be used to forge signatures and allow impersonation attacks. Unlike the threat of retroactive "store now, decrypt later attacks", this threat would only be effective if the signatures are generated at a time when a CRQC exists. Thus, the signatures that are verified on the fly, like in authenticated channels, cannot be directly impacted before the existence of a CRQC. However, in a context of document signing, the long-term validity is sometimes required in certain specific use cases, and these signatures can be compromised by the existence of a CRQC. The transition from pre-quantum signatures to post-quantum ones should be tackled before the existence of any CRQC to avoid any a posteriori impersonation attack.

Quantum threat: what about symmetric cryptography?
Symmetric cryptography, a different and complementary branch of cryptographic algorithms, could also be targeted by potential large scale quantum computers. A generic quantum algorithm introduced by Grover in 1998 [11] quadratically speeds up the exhaustive search of secret keys in symmetric algorithms. Grover's algorithm can also speed up certain attacks on hash functions called collision finding attacks. These attacks also require the use of CRQCs but for numerous algorithms one can reasonnably assume that they could be mitigated by adjusting the sizes of the hash outputs and keys (using 256 bits keys instead of 128 for the AES symmetric encryption mechanism and using 384 bits hash outputs for SHA-2 and SHA-3 for instance). Thus, the generic impact of Grover's algorithm on symmetric cryptography is far more limited than the impact of Shor's algorithm on PKC.

Why the quantum threat should be taken into account today?
Because of a "store now, decrypt later" attack outlined above, the quantum threat should be taken into account before the question of whether the development of a CRQC will ever become achievable in the future is cleared up. Thus, a profound change of today's public key cryptography towards quantum-resistant algorithms should be globally initiated to anticipate a possible collapse of our current cryptographic infrastructure. Even though protecting our current public key cryptography against this distant threat has a cost, researching alternative cryptographic solutions can be beneficial from another perspective. Indeed, beyond the quantum threat, cryptography is never infallible; weaknesses are found from time to time, even on cryptographic mechanisms implemented in classical computers. Thus, it is not possible to totally rule out a discovery of a potential weakness impacting the security of hardware and/or software and requiring replacement of algorithms. Nowadays, the public key cryptography used worldwide is close to a mono culture and would strongly benefit from the introduction of new alternative algorithms.

Is quantum key distribution a solution?
Quantum Key Distribution (QKD), sometimes called quantum cryptography, is a way of enabling secure communications without being vulnerable to classical and quantum computers by using so-called quantum channels. Nevertheless, this technique does not provide a complete functional equivalent to public key cryptography and offers limited applications due to the need of a dedicated communication infrastructure and without real routing capabilities. More information on the ANSSI position can be found under reference [5]. As such, except for niche applications where QKD is used for providing some extra physical security on top of algorithmic cryptography (and not as a replacement), it is not considered by ANSSI as a suitable countermeasure to mitigate the quantum threat.

What is post-quantum cryptography?
Post-Quantum Cryptography (PQC) is a family of cryptographic algorithms including key establishment and digital signatures that ensures a conjectured[1] security even against an attacker equipped with quantum computers. Post-quantum algorithms can be executed on classical computers with classical communication channels and thus can be deployed in existing infrastructures, unlike QKD. Besides, these algorithms are not only for use after a CRQC is built, they can be deployed in anticipation.

For ANSSI, PQC represents the most promising avenue to thwart the quantum threat.

The international research effort on post-quantum cryptography accelerated in 2015 after NSA's release advising to "shift to quantum resistant cryptography in the near future" [9]. In 2017, the National Institute of Standards and Technologies (NIST) started a standardization campaign to define standard post-quantum public key algorithms (key establishments and signatures). At the time of writing, this process is still ongoing [13] and currently at its third round. Standards are expected to be published

[1] for which no efficient quantum attack exists today.

within the next one to four years. Contrary to other standardization campaigns where there was only one finalist, the post-quantum campaign will end up with several standards for different applications.

This standardization process has acted as a catalyst allowing a strong involvement of the international cryptography research community and focusing the analysis efforts on a restricted number of candidate algorithms while preserving the diversity of the underlying problems. This process has also broadened the analysis to various implementation use cases like embedded components.

What are the different post-quantum algorithms?
The different families of post-quantum public key candidate algorithms are defined by the mathematical structure on which they are built. Nowadays, post-quantum public key algorithms are mostly based upon:

- Structured or un-structured Euclidean lattices ;
- Error-correcting codes ;
- Isogenies between elliptic curves ;
- Multivariate systems ;
- Hash trees.

While the mathematical problems were introduced in the last century, the PQC algorithms are relatively recent. They offer various compromises between key size, signatures or ciphertext size, computational complexity and security assurance. A technical survey of the algorithms and the underlying mathematical problems can be found in [10].

What is being done in France to address the Quantum threat?
There is a high academic interest in France for this thematic. This is why the French community is actively participating to the design and security analysis of the primitives but also to their cryptanalysis. A national group comprising academics, industrials and ANSSI has been formed, called RISQ[2], and will publish a whitepaper in 2022 [14].

As the national cybersecurity authority in France, ANSSI has followed closely and participated to the progress in post-quantum cryptography. ANSSI has planned to continue its effort in the future.

More generally, ANSSI publishes recommendations on the selection of cryptographic algorithms in security products and delivers security labels for products meeting general security requirements. But, ANSSI is not a standardization agency, its role is not to develop cryptographic standards. More precisely, ANSSI has a twofold role when it comes to the use of cryptographic algorithms: advisory and regulatory. On the one hand, it promotes the use of well-studied, state-of-the-art cryptographic algorithms by publishing national guidelines on cryptography [2,1] and by participating to the publication of European guidelines on the selection of cryptographic algorithms [16]. On the other hand, ANSSI supervises the evaluation and delivery of security labels, e.g. Common Criteria (CC) certificates. In the French certification scheme, each evaluation comprises specific cryptographic evaluation tasks according to the evaluation level. It is important to highlight that there is no closed list of cryptographic algorithms eligible in order for a product to obtain a security label. Generally, the use of cryptographic algorithms that are fitted with a formal standard status delivered by an international standardization body (e.g. ISO, ITU, IETF, ETSI etc.) is strongly recommended. However, a cryptographic algorithm supported by a strong record of scientific publications can be potentially judged sufficient to provide an adequate security assurance level. Conversely, there is no automatic and universal recognition of all algorithms that obtained a formal standard state from such organizations.

Are the future NIST standards mature enough to be implemented in security products?
Beyond the NIST objective to derive standards, the past three rounds of the NIST standardization campaign provide a variety of algorithms along with security analysis. Although this new post-quantum toolbox may seem handy for developers, the maturity level of the post-quantum algorithms presented to the NIST process should not be overestimated. Many aspects lack cryptanalytical hindsight or are still research topics, e.g. analysis of the difficulty of the underlying problem in the classical and quantum computation models, dimensioning, integration of schemes in protocols and more importantly the design of secure implementations. This situation will probably last some time after the publication of NIST standards.

[2] "Regroupement de l'industrie française pour la sécurité post-quantique".

Acknowledging the immaturity of PQC is important: ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term. However, this immaturity should not serve as an argument for postponing the first deployments. ANSSI encourages all industries to initiate in the next months a gradual overlap transition in order to progressively increase trust on the post-quantum algorithms and their implementations while ensuring no security regression as far as classical (pre-quantum) security is concerned.

How to transition smoothly from pre-quantum to post-quantum algorithms?
A *hybrid* mechanism (key establishment or signature) combines the computations of a recognized pre-quantum public key algorithm and an additional algorithm conjectured post-quantum secure. This makes the mechanism benefit both from the strong assurance on the resistance of the first algorithm against classical attackers and from the conjectured resistance of the second algorithm against quantum attackers. Certain hybrid protocols are in standardization processes like [17] for TLS 1.3 or [18] for IKEv2. More generally, for key establishment, one can perform both a pre-quantum and a post-quantum key establishment and then combine both results, e.g. using a Key Derivation Function (KDF). Alternatively, one may use for some specific applications a KDF on a pre-shared key and a shared key obtained from a pre-quantum scheme. For signature schemes, hybrid signatures can be achieved with the concatenation of signatures issued by a pre-quantum and a post-quantum scheme and the requirement that *both* signatures be valid in order for the hybrid signature to be valid.

Even though hybridation is a relatively simple construction, ANSSI emphasizes that the role of hybridation in the cryptographic security is crucial and will be mandatory for phases 1 and 2 presented in the sequel. In addition, the implementation security of the hybridation technique should be also taken in consideration.

Given that most post-quantum algorithms involve message sizes much larger than the current pre-quantum schemes, the extra performance cost of an hybrid scheme remains low in comparison with the cost of the underlying post-quantum scheme. ANSSI believes that this is a reasonable price to pay for guaranteeing an additional pre-quantum security at least equivalent to the one provided by current pre-quantum standardized algorithms.

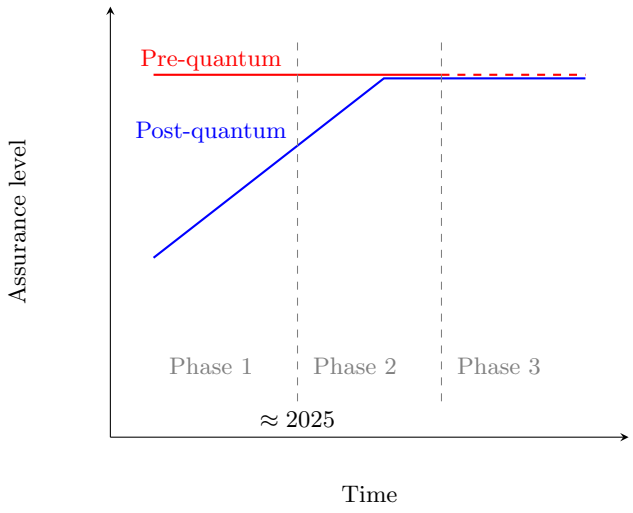
What is cryptoagility?
As detailed in the sequel, the deployment of hybrid PQC is not a mandatory feature as of today. However, ANSSI will encourage the initiation of progress towards *cryptoagility* as much as possible for future products. More precisely, a product is said cryptoagile if it includes the possibility to update its cryptographic algorithms without recalling it or substituing it with a new one. The quantum threat makes cryptoagility particularly relevant, and beyond this threat, classical attacks may also evolve and make cryptographic mechanisms or key lengths obsolete.

In practice, cryptoagility also means that in addition to the possibility of patching, products could include an extra surface for allowing potential updates in order to react to upcoming cryptographic recommendations and standard updates. Even though updates of the cryptographic algorithms should be much less frequent than patches, the cryptoagility feature is non-trivial to implement due to the need for retro-compatibility and the potential requirement for additional security visas if the product is certified. However, as the motivation for cryptoagility is very relevant nowadays, ANSSI believes that cryptoagility features should be taken into account during the benefit/risk analysis of future products.

What is the recommended post-quantum transition roadmap?
To support a gradual transition, ANSSI encourages the following 3-phase roadmap (see below for a detailed description):

- Phase 1 (today): hybridation to provide some additional post-quantum *defense-in-depth* to the pre-quantum security assurance.
- Phase 2 (not earlier than 2025): hybridation to provide *post-quantum security assurance* while avoiding any pre-quantum security regression.
- Phase 3 (probably not earlier than 2030): optional standalone post-quantum cryptography.

What is recommended for each phase?
Phase 1: mandatory pre-quantum security, optional PQC, no claimed quantum resistance. This phase



corresponds to the current situation. The post-quantum security should not be a mandatory requirement but is considered as an optional "defense-in-depth". As the standardization campaign is still ongoing, the idea of this phase is to enable the first post-quantum deployments with flexibility while preserving the pre-quantum security with hybrid mechanisms.

> ANSSI recommends introducing post-quantum defense-in-depth as soon as possible 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.

The two following conditions below should be met.

1. The chosen hybridation technique must ensure no security regression i.e. the security of the mechanism must be at least equivalent to the security of the included recognized pre-quantum scheme.
2. While there is no strict guidance for the choice of a post-quantum public key algorithm (key establishment or signature mechanisms), the chosen algorithm should have stable and well-studied specifications, e.g. be a NIST finalist or a trusted alternate finalist[3]. Moreover the conjectured post-quantum level should be as high as possible, preferably NIST level V (AES-256). For example, at the time of the writing, the NIST candidates FrodoKEM, Kyber, Dilithium or Falcon could be good options for first deployments. Choosing algorithms selected by NIST for standardization is not an absolute prerequisite[4].

ANSSI encourages to use a conjectured post-quantum security level on *symmetric* primitives consistent with the selected post-quantum PKC algorithm – 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.

Please note that hash-based signatures are an exception for hybridation: due to their well-studied underlying mathematical problem, ANSSI estimates that these algorithms could be used today without hybridation[5]. However, their potential application range is limited (low number of signatures queries or large signature sizes).

[3] as defined by NIST in round 3 of the campaign.

[4] While few exceptions are expected in practice, at least for mainstream cryptography, an algorithm that is not a NIST standard, but that is demonstrably stronger that a NIST standard, could constitute such an exception. For example, a developer should be able to obtain a security visa for a product implementing an hybrid FrodoKEM whether NIST decides that FrodoKEM will be one of the first PQC standards or not.

[5] This is nevertheless a non-standard algorithm choice compared to the use of current PKC 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.

This phase should last until after NIST's first standards are announced and it is planed to last until after 2025.

Phase 2. Mandatory pre-quantum security, optional PQC with claimed quantum resistance. In this second phase, all post-quantum PKC algorithms shall continue to be systematically included inside hybrid mechanisms (except for hash-based signatures whose hybridation is optional as presented in phase 1). For this phase, the post-quantum part will be more than an *defense-in-depth*: the quantum resistance could be claimed as a feature. In that case, a *post-quantum security assurance* should be mandatory for *both public key and symmetric mechanisms* as integral part of the security analysis. By then, ANSSI will have identified criteria for acceptable post-quantum PKC algorithms depending on their associated post-quantum security assurance. Such selected algorithms may not exactly match NIST standards. For this phase, ANSSI will highly recommend the post-quantum transition for products claiming long-term security. In that sense, for certain types of security products claiming long-term security, post-quantum security could become a mandatory feature.
This phase should last until at least 2030.

Phase 3: Optional standalone PQC with claimed quantum resistance. ANSSI expects that after years of analysis, the security assurance level provided by post-quantum algorithms will be as high as today's pre-quantum assurance level. Thus, the usage of some post-quantum schemes should be possible without hybridation.

Please note that the presented recommendations will potentially evolve depending on the global advances on post-quantum cryptography and on the progress of NIST standardization campaign. The estimated timeline of the roadmap could be advanced or slowed down accordingly.

What is the impact on security visas delivery?
The use of PQC will also impact the delivery of security visas. ANSSI will accompany this transition and adapt its evaluation procedures according to the roadmap described above. The general procedure [3] will be updated following the three phases as follows.

> **Phase 1:** The security visas *only claim a pre-quantum security assurance*. The optional post-quantum security feature is only considered as an additional defense-in-depth add-on.

Therefore, the evaluation method for security products that do not use PQC stays unchanged. For products that use post-quantum *defense-in-depth*, the evaluation method for a security visa will be defined as follows :

- All pre-quantum security mechanisms are evaluated as currently defined [3].
- The hybridation mechanism will be evaluated to ensure that it does not degrade security.
- While ANSSI may go through the PQC algorithms specification, it will not be evaluated by IT Security Evaluation Facilities (ITSEF) and thus it will *not be part of any security visa*. If necessary, it is possible to contact ANSSI for advice on the choice of PQC algorithms.

In a nutshell, security visas will attest that pre-quantum security is evaluated and that the use of post-quantum *defense-in-depth* mechanisms do not have any negative impact. No formal judgement will be made on the quantum security offered by PQC.

> **Phase 2:** ANSSI will deliver security visas claiming a pre-quantum and, optionally, post-quantum long-term security assurance (still with mandatory hybridation).

As in phase 1, evaluation procedure for products that do not use post-quantum long-term security remains unchanged. For long-term security products that follow ANSSI recommendations and use hybridation with PQC, the evaluation method will include pre-quantum security analysis, hybridation and quantum resistance analysis. For the latter, the analysis should include both symmetric and asymmetric mechanisms and should comply with the official guidelines on quantum resistance that will be updated by then.

Phase 3: ANSSI will deliver security visas claiming a pre-quantum and post-quantum long-term security assurance with optional hybridation. Depending on the context, ANSSI could continue to deliver security visas claiming only pre-quantum security assurance.

This final transition phase strongly depends on the advances of research in post-quantum cryptography and quantum computing. The specific details of this phase will be adapted in the next decades.

What is the position of other governments?
Several governments have published similar position papers recommending to prepare the post-quantum transition. ANSSI's views are similar to the BSI's position [6] on many issues (e.g. necessary migration, hybridation, cryptoagility).

References

1. ANSSI. Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B2.pdf.
2. ANSSI. Guide des mécanismes cryptographiques. https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf.
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. ANSSI. Should Quantum Key Distribution be Used for Secure Communications? https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/.
6. 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.
7. 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.
8. 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.
9. CNSS. CNSS Advisory Memorandum. https://cryptome.org/2015/08/CNSS_Advisory_Memo_02-15.pdf, 2015.
10. ENISA. Post-Quantum Cryptography: Current state and quantum mitigation. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.
11. L. K. Grover. A framework for fast quantum mechanical algorithms. In *30th ACM STOC*, pages 53–62. ACM Press, May 1998.
12. NCSC. Preparing for Quantum-Safe Cryptography. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.
13. NIST. Post-quantum Cryptography (official standardization webpage). https://csrc.nist.gov/projects/post-quantum-cryptography.
14. RISQ. To appear on RISQ official webpage. https://risq.fr/.
15. P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, Nov. 1994.
16. SOG-IS. Agreed Cryptographic Mechanisms. https://www.sogis.eu/uk/supporting_doc_en.html.
17. D. Stebila, S. Fluhrer, and S. Gueron. Hybrid key exchange in TLS 1.3 (draft IETF). https://www.ietf.org/id/draft-ietf-tls-hybrid-design-03.html.
18. 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/.