NÚKIB

QUANTUM THREAT AND QUANTUM-RESISTANT CRYPTOGRAPHY

Annex to the document:
Minimum Requirements for Cryptographic Algorithms

Non-binding EN translation of CZ version 2.0, valid as of February 1, 2025

Contents

Introduction

The main motivation for this Annex to the document "Minimum Requirements for Cryptographic Algorithms" is to support the preparations for the transition to quantum-resistant cryptography in cybersecurity. Given the anticipated complexity of this process, the primary objective of this Annex is to explain the cryptographic principles and context and to further substantiate the presented cryptographic recommendations.

For questions of a legal nature, please contact the secretariat of the National Cyber and Information Security Agency:

National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky

Phone: +420 541 110 777
E-mail: nckb@nukib.gov.cz

Questions, comments, and suggestions of a cryptological nature can be sent to the e-mail address: kryptoalgoritmy@nukib.gov.cz

1 Quantum Threat

(1) Nature of the quantum threat

In 1994, Peter Shor published a quantum algorithm that is almost exponentially more efficient than the best known classical algorithms for factoring large numbers or for finding the discrete logarithm[1],[2]. This implies that, in principle, using Shor's algorithm, one can efficiently break all asymmetric cryptographic algorithms whose security is based on the difficulty of any of the following problems:

- factorization of large numbers,
- finding the discrete logarithm over a finite field,
- finding the discrete logarithm over an elliptic curve[3].

The security of most asymmetric cryptographic algorithms in use today is based on the assumption of practical intractability of these problems. All classical asymmetric cryptographic algorithms approved in the document "Minimum Requirements for Cryptographic Algorithms" can be broken using Shor's algorithm.

In 1996, Lov Grover discovered a quantum algorithm that can be used to find keys of arbitrary cryptographic systems by brute force[4]. However, it is significantly less efficient than Shor's algorithm. Consequently, only block and stream ciphers with key lengths of 256 bits or more are considered safe against Grover's algorithm[1].

In 1997, Brassard, Høyer, and Tapp published a quantum algorithm (BHT algorithm) based on Grover's algorithm that reduces the difficulty of finding hash function collisions compared to classical collision search methods based on the birthday paradox[5]. Today, only hash functions with an output length of at least 384 bits are considered safe against attacks using the BHT algorithm[2].

[1] The risks associated with brute force quantum attacks based on Grover's algorithm on the approved block ciphers with a key length of 128 bits will likely be very low even after the construction of cryptanalytically relevant quantum computers, and similar risks for a key length of 192 bits will likely be almost negligible.

[2] The risks associated with brute force quantum attacks based on the BHT algorithm and its enhancements on the approved hash functions with an output length of 256 bits will likely be almost negligible even after the construction of cryptanalytically relevant quantum computers.

(2) Cryptanalytically relevant quantum computer, a necessary condition for realizing the quantum threat

For the practical use of the above-mentioned quantum algorithms in cryptanalysis, they need to run on a so-called "cryptanalytically relevant quantum computer". Such a computer should be universal, scalable and reliable[3].

Quantum computing based on ion traps and quantum computing with superconducting qubits have long been considered the most promising areas of research and development towards this goal. Significant progress is also being made in the field of photonic quantum computing. None of the quantum computers realized so far have even come close to the properties of cryptanalytically relevant quantum computers[4]. In this context, alternative methods of factorization are also being proposed, using a quantum computer which in general may be neither universal nor fully fault-tolerant[5] [25].

At present, it remains uncertain when cryptanalytically relevant quantum computers will be realized. Various studies are being published with different estimates, and the result of an opinion poll among experts on the subject is often presented as one of the best estimates[6], sl. 11 a 13. Also very well known are the estimates given by M. Mosca[6], sl. 12, according to which it will occur in 2026 with a probability of ⅐ and it will occur by 2031[6] with a probability of ½.

The German BSI[7], pp. 28 and 35 estimates that the first cryptanalytically relevant quantum computers will be realized in the early 2030s. In accordance with the BSI, we consider this estimate to be highly uncertain.

---

[3] The term universal quantum computer is the quantum analogue of the term classical universal computer. Very roughly speaking, a universal quantum computer can run any quantum algorithm. The scalability of a quantum computer means that a small increase in the scope of its computations (e.g., lengthening the inputs) will not be extremely demanding, and that the lengths of the inputs to a scalable quantum computer will gradually be extended more and more. A reliable (fault-tolerant) quantum computer should remove errors of an arbitrarily long quantum computation with sufficient accuracy.

[4] Current universal quantum computers are referred to as NISQ – Noisy Intermediate Scale Quantum (Computer). Probably the biggest problem on the road to constructing cryptanalytically relevant quantum computers is the difficulty of providing sufficiently reliable noise removal. According to some estimates, thousands of physical qubits are needed to realize a single reliable logical qubit[23], [24]. A logical qubit is the quantum analogue of a bit. Quantum algorithms work with logical qubits. A physical qubit is a quantum system with controllable general superpositions of two basis states. Logical qubits are systems of physical qubits that are able to represent qubits in quantum algorithms in reliable quantum computations.

[5] For example, in [25], an alternative method of factorizing large numbers based on digitized adiabatic quantum computation is proposed, which does not require much computational depth and therefore need not be completely resistant to errors. And since it is based on the Ising model typical of optimization (quantum) computations[65], it need not be universal either.

[6] There is a very small group of reputable experts who argue that the realization of universal, scalable and reliable quantum computers is unlikely to happen in ten or even twenty years, but in a much longer time, perhaps never [8], [9], [10], [11].

At the same time, in accordance with the BSI[7], we consider it to be a guideline for preparing the transition to quantum-resistant cryptography in the protection of sensitive information of a critical level of confidentiality or integrity[8].

(3) Quantum-vulnerable algorithms requiring faster replacement

From the above, it is clear that we should transition to quantum-resistant cryptography for the protection of highly sensitive information roughly by the early 2030s.

The problem is that there are types and uses of cryptographic algorithms that, even if the aforementioned BSI´s estimate is correct, require much faster replacement with their quantum-resistant alternatives. These are, first, cryptographic algorithms designed to protect the confidentiality of data, and second, digital signature algorithms designed to protect the integrity of firmware during updates.

In the former case, it is necessary to address the possibility that an attacker will record and store the encrypted communication and they will decrypt it once there is a cryptanalytically relevant quantum computer available (a.k.a. "harvest now, decrypt later" scenario).

In the latter case, we must consider the possibility that some device memories containing public keys may not be rewritable in the future.

In these two cases, the urgency to transition to quantum-resistant cryptography is much higher than in other cases.

[7] In the case of "high security applications", the BSI works on the hypothesis that cryptanalytically relevant quantum computers will be available in the early 2030s[7, p. 35].

[8] The critical level of confidentiality/integrity/availability is the highest level of confidentiality/integrity/availability according to Annex 1 to Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, cyber security reporting requirements and data disposal (the Cyber Security Decree).

2 Quantum-Resistant Cryptography

(1) Main possible responses to the quantum threat

The possibility for broader and novel applications of symmetric cryptography

Since symmetric cryptography with a key length of 256 bits is not quantum-vulnerable, one possible response would be to revert to using only symmetric cryptography. However, this would lead to the loss of the benefits of asymmetric cryptography.

In some specific cases of cryptographic protocols, it is possible to use pre-distributed symmetric keys as part of the input to the session key derivation function. However, this is going to increase the requirements for the protection of these pre-distributed keys.

The possibility of moving to post-quantum cryptography

Another option is to use different asymmetric cryptographic algorithms that are resistant to attacks based on quantum computing. These algorithms are often called quantum-secure cryptography or quantum-resistant cryptography, but they are most commonly referred to as post-quantum cryptography (PQC). The transition to its use is supported by relevant security authorities who consider it the most appropriate way to respond to the quantum threat[7], [36], [37], [55], [56].

The possibility of using quantum key distribution

In the long term, the use of quantum key distribution (QKD) may be promising. It has substantial security advantages, but for the time being also substantial security and practical disadvantages, and therefore the transition to its widespread use in the near future is not (unlike its research) currently supported by major security authorities[7], [52], [53], [54], [69].

We recommend transitioning to quantum-resistant cryptography by adopting post-quantum cryptography.

(2) Post-quantum cryptography

The term post-quantum cryptography was introduced by the American cryptologist Dan Bernstein[59], sl. 21, to refer to those asymmetric cryptographic algorithms that remain secure even in the era of cryptanalytically relevant quantum computers. This requires that their security be based on the difficulty of solving mathematical problems other than those that are breakable by Shor's algorithm. However, to ensure their security, it is also necessary that these cryptographic systems are not breakable by any other quantum algorithm and, of course, by classical algorithms either.

a) Main types of current post-quantum cryptography

1) **Code-based cryptography:** Its security is based on the difficulty of efficient decoding of a generic linear error-correcting code. Selected algorithms from this category, such as Classic McEliece, are considered to have one of the highest security guarantees. Their major practical drawback are their extremely long public keys.

2) **Lattice-based cryptography**: Its security is based on the difficulty of solving some problems on lattices, such as shortest vector problem, nearest vector problem, learning with errors. Currently, thanks to its security combined with its practical properties, it is considered one of the most promising areas of post-quantum cryptography. The practical properties of these post-quantum algorithms can be improved by defining them on structured lattices. It should be noted that too high "structuredness" of the lattice can lead to successful cryptanalysis.

3) **Hash-based cryptography**: Its security is based on the security features of the underlying hash functions. Since the quantum resistance of hash functions is well founded, these signature algorithms are considered as post-quantum cryptography with high security guarantees. However, this is redeemed by certain practical problems. In some cases, the maximum number of signatures per key is substantially limited, in others the public key is extremely long, and thus they are only suitable for specific use cases.

4) **Isogeny-based cryptography**: Its security is based on the difficulty of finding an isogeny between two supersingular elliptic curves (if such isogeny exists). This approach was considered highly promising for quite a while; however, in 2022 an effective attack has been found on one of the isogeny-based cryptosystems, which seriously compromises their security[13].

5) **Multivariate cryptography**: Its security is based on the difficulty of solving polynomial equation systems with many variables over algebraic number fields. This area of cryptography has been the target of many successful attacks, so guarantees of its security are not currently considered very credible[14], [15].

3 Standardization of Post-Quantum Cryptography Led by NIST

Since 2016[17], [18] the process of standardization of post-quantum cryptography is organized by NIST in the form of a public competition. At the end of its third round, the first quartet of post-quantum algorithms were selected for standardization (see Section 3, par. (4)) and another quartet of cryptographic algorithms advanced to the fourth round, in which a decision on the possible standardization of some of them should be made (see Section 3, par. (5)).

In 2020, NIST standardized (out of competition but in consensus with the expert community) a pair of post-quantum digital signatures, LMS and XMSS, based on hash functions[16].

(1) Competition categories in terms of algorithm functionalities

Post-quantum cryptography is intended to replace the currently used asymmetric cryptography in two areas:

- cryptography for key establishment and for asymmetric encryption,
- digital signatures.

The two main categories of the NIST competition are very much in line with this:

A) *KEM/Encryption*[9] – methods for establishing symmetric keys based on asymmetric encryption[10]
B) *Signatures* – digital signatures

(2) NIST requirements for the safety of post-quantum candidates

In quantum-resistant cryptography, it is essential to consider not only its security against classical attacks, but also its resistance to possible future attacks using quantum computers[17], [18].

[9] In this context, KEM and Encryption are two close methods, the essence of which is asymmetric encryption of symmetric keys:

- *Encryption* here means standard asymmetric encryption of symmetric keys.
- *KEM* means the key encapsulation mechanism[33]. It differs from asymmetric encryption in that the encapsulation process first generates a random secret, encrypts it using a public key to ciphertext, and derives a symmetric key by hashing from the random secret.

[10] Implications of the choice of KEM/Encryption functionalities:

The algorithms selected in the KEM/Encryption category are supposed to complement or replace either classical asymmetric key encryption or Diffie-Hellman exchange (classical or over an elliptic curve). In the case of classical asymmetric encryption, it will be a replacement by an algorithm of the same type, but in the case of Diffie-Hellman exchange, it will be a replacement by KEM or asymmetric encryption, i.e., a different type of cryptographic algorithm. This may be one of the many sources of problems in the transition to quantum-resistant cryptography in this area.

The security requirements for the post-quantum candidates submitted to the competition are specified by assuming limitations on the computational capabilities of the attacker, by making standard assumptions about the attacker's access capabilities to the attacked device, and also by using attack success criteria. In this case, the attacker's computational capabilities also include the possibility of using a large-scale quantum computation.

a) Security levels

NIST has defined five different assumptions about the limitations of an attacker's computational capabilities, and has assigned a security level to each of these five options[18] pp. 15-18. The security levels of post-quantum algorithms defined by NIST are determined by the number of steps, either classical or quantum cryptanalytic, needed to break a given scheme[11].

NIST Security Levels:

- Level 1, corresponds to the difficulty of a brute force attack on AES-128[12]
- Level 2, corresponds to the difficulty of generic SHA-256 collision search
- Level 3, corresponds to the difficulty of a brute force attack on AES-192
- Level 4, corresponds to the difficulty of generic SHA-384 collision search
- Level 5, corresponds to the difficulty of a brute force attack on AES-256

A deeper study of the limitations of the attacker's capabilities defining security level 5 shows that the requirements for this level are significantly oversized in terms of estimates of his realistic capabilities in the medium-term future. This is why NIST, when announcing the

[11] NIST defined three of these security levels (1, 3, and 5) using the computational complexity of brute force AES block cipher key search. The levels are distinguished by key lengths (128, 192, and 256 bits). In the classical case, the considered levels correspond to the computational complexities of 2^{127}, 2^{191} and 2^{255} AES encryptions. In the quantum case without parallelization, they would correspond to 2^{64}, 2^{96} and 2^{128} steps of Grover's algorithm. If we consider the possibility of parallelization and the error-free computation depth constraint, the concrete content of the definition becomes much more complex[19], [20].

The two remaining security levels (2 and 4) are defined using the computational complexity of the brute force SHA-2 hash function collision search. The levels are distinguished by the lengths of the SHA-2 output, namely 256 and 384 bits. In the classical case, the considered levels correspond to computational complexities of 2^{128} and 2^{192} computations of the SHA-2 compression function. In the quantum case, they should correspond to 2^{85} and 2^{128} steps of the BHT algorithm[5]. However, the latter requires an unrealistically large quantum memory. This is probably why NIST did not specify quantum complexity in the definitions of levels 2 and 4. In 2017 and 2019, more efficient alternatives[21], [22] to the BHT algorithm have been proposed with significantly lower (though still very high) quantum memory size requirements, so the paper [20] also addresses the quantum demands of levels 2 and 4.

[12] From here we get a different view of the quantum vulnerability/resistance of symmetric cryptography with key lengths of 128 bits and 192 bits. It corresponds to security levels 1 and 3 of post-quantum cryptography. Similarly, the quantum vulnerability/resistance of SHA-2 with a key length of 256 bits corresponds to security level 2 of post-quantum cryptography.

competition, encouraged developers to focus mainly on security levels 1 to 3, as these can be expected to provide sufficient security in the foreseeable future[13].

b) NIST security requirements in terms of considered attack scenarios

In terms of the considered attack scenarios, NIST has standard requirements[18] pp. 14-15:

A) In the case of KEM/Encryption schemes, semantic security is required for adaptive chosen-ciphertext attacks, i.e., IND-CCA2 security is required[14].

B) In the case of digital signature algorithms, it is required that the attacker, in a so-called chosen-message attack, is unable to construct any valid fraudulent message-signature pair. Thus, EUF-CMA security is required.

c) Additional security requirements for candidates[18] p. 19

Perfect forward secrecy[15]: Some properties of post-quantum candidates could make it difficult to ensure forward secrecy. For example, the generation of new public/private key pairs could be too slow, which could make it difficult to change them frequently enough, or the the public keys could be too long, which could complicate their transmission. NIST prefers candidates that do not have these problems.

Resistance to physical side-channel attacks: NIST has announced that it will prefer post-quantum cryptography schemes that are less challenging to make resistant to side-channel attacks.

Resistance to multi-key attacks: Ideally, an attacker should not gain a relevant advantage by simultaneously attacking multiple keys used by a given scheme.

Resistance to incorrect implementations and incorrect use of the scheme: Another desirable property of post-quantum schemes can be formulated roughly as follows: The security of the scheme should not be dramatically devastated under situations such as a limited (minor) error in the scheme code, or a failure of the random generator, or the reuse of the private/public key pair in a KEM/Encryption scheme with ephemeral keys, etc.

---

[13] However, in case of possible future breakthroughs in cryptanalysis or technology, it also asked for the specification of parameters corresponding to a significantly higher security level than 3[18] p. 18.

[14] NIST also considered KEM/Encryption with ephemeral public keys, i.e., one-time use keys. The important point here is that when the first error occurs in the symmetric key establishment protocol, a new public/private key pair is generated, and the old pair is deleted when it is no longer needed. In this case, of course, only the semantic security of a chosen-plaintext attack, i.e., IND-CPA, will suffice.

[15] In the case of KEM/Encryption, forward secrecy protects the confidentiality of previously encrypted data in the event that an attacker had eavesdropped on and stored encrypted communications in the past and then captured one of the private keys currently in use. In order for previously encrypted data to be protected even in these circumstances, it is necessary that the relevant private keys be deleted after use and replaced with newly generated private keys.

(3) Other criteria for evaluating candidates

a) Performance, length of transmitted cryptographic variables and others[18] p. 20

Public key, ciphertext, and signature size: In cases where the usage patterns of the scheme do not require frequent transmission of public keys, their length does not have serious practical implications. The opposite situation arises, for example, whenever perfect forward security is required.

Computational efficiency of public and private key operations: These properties of the scheme are almost always important, but there are uses of post-quantum cryptography for which they may be critical.

Computational efficiency of key generation: This property of the scheme is particularly important when perfect forward security is required.

Decryption failures: For schemes with the possibility of decryption failure[16], NIST requires assurances that it will occur with negligible (virtually zero) probability.

b) Other required characteristics collectively referred to as flexibility[18] p. 21

By flexibility of the scheme, NIST understands properties such as:

- The possibility of modifying the scheme in a not-too-difficult way to obtain additional desired properties.
- The possibility of modifying the parameters of a scheme easily enough to achieve other security or operational properties.
- The possibility of parallelizing the implementation.
- The possibility of integrating the scheme into existing protocols and applications requiring only minimal changes to the scheme[17].

[16] In certain post-quantum cryptography schemes, it is theoretically possible for a decryption failure (here, a ciphertext rejection) to occur even in circumstances where the scheme was correctly implemented and the ciphertext was correctly generated and not altered on the way to the decryption device.

[17] Excessive lengths of public keys or ciphertexts, or slowness of cryptographic operations, can complicate the integration of post-quantum schemes into existing protocols and applications.

(4) Post-quantum algorithms selected by NIST for standardization

In July 2022[26], [27], NIST selected the first four quantum-resistant algorithms in the competition to be standardized. In August 2024, standards have been published for three of them (CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+), the fourth one (Falcon) is still in progress.

a) CRYSTALS algorithms, the real winners of the competition

Although NIST has so far selected four algorithms for standardization, CRYSTALS algorithms have a special position among them. In the KEM/Encryption category, only one algorithm has been selected for standardization so far, namely CRYSTALS-Kyber. While three algorithms have been selected in the Signatures category, CRYSTALS-Dilithium, which is one of them, is recommended by NIST as the primary digital signature algorithm to be used[26], sl. 13.

NIST assesses both algorithms as having a good scientific basis for their design[18], being relatively simple, easy to implement, and achieving good performance in cryptographic operations. Part of the implementation of both algorithms may be shared.

In August 2024, NIST published the standards for both algorithms, namely:

- FIPS 203[66], standardizing CRYSTALS-Kyber as ML-KEM (Module Lattice Based Key Encapsulation Mechanism)[19]
- FIPS 204[67], standardizing CRYSTALS-Dilithium as ML-DSA (Module Lattice Based Digital Signature Algorithm)

b) KEM/Encryption category

In this category, NIST has so far selected a single algorithm for standardization:

CRYSTALS-Kyber (standardized as **ML-KEM**)
It is an IND-CCA2 secure post-quantum scheme based on structured lattices[20].
It was chosen for standardization because of its security and performance. Its performance on various platforms is rated excellent by NIST.

[18] The security of the two mentioned CRYSTALS algorithms is based on the difficulty of solving the Module-LWE (i.e., Module Learning with Errors) problem, which corresponds to the problem of finding a small vector on a structured (modular) lattice.

[19] The standardized ML-KEM algorithm slightly differs from the original Kyber algorithm submitted to the third round of the NIST competition. However, basic mathematical and cryptographic principles of both variants are the same and for the purposes of this document they can be treated as equal in many places. The same holds for ML-DSA and Dilithium algorithms.

[20] Its security is based on the difficulty of solving the Module-LWE problem.

The FIPS 203[66] standard defines three variants of ML-KEM, which correspond to the variants of CRYSTALS-Kyber:

- ML-KEM-512 – Kyber-512 (Level 1)
- ML-KEM-768 – Kyber-768 (Level 3)
- ML-KEM-1024 – Kyber-1024 (Level 5)

For security levels 1, 3 and 5, its public keys are 800, 1184 and 1568 bytes in length, respectively, and its ciphertexts are 768, 1088 and 1568 bytes in length, respectively.

The CRYSTALS developers recommend[60] using Kyber in a hybrid mode with classical asymmetric cryptography. They recommend Level 3 as the preferred variant in this combination, arguing that "according to a very conservative analysis, [it] achieves more than 128 bits of security against all known classical and quantum attacks".

c) Signatures category

In this category, NIST has so far selected three algorithms for standardization:

CRYSTALS-Dilithium (standardized as **ML-DSA**)
It is an EUF-CMA secure post-quantum signature scheme based on structured lattices[21]. It was chosen for standardization because of its security, high performance, and relatively simple design scheme. It is evaluated by NIST as a highly efficient scheme with easy implementation and strong security guarantees.

The FIPS 204[67] standard defines three variants of ML-DSA, which correspond to the variants of CRYSTALS-Dilithium:

- ML-DSA-44 – Dilithium 2 (Level 2)
- ML-DSA-65 – Dilithium 3 (Level 3)
- ML-DSA-87 – Dilithium 5 (Level 5)

For security levels 2, 3 and 5, its public keys are 1312, 1952 and 2592 bytes in length, respectively, and its signatures are 2420, 3293 and 4595 bytes in length, respectively.

The CRYSTALS developers recommend[61] using Dilithium in a hybrid mode with a classical signature algorithm. They recommend Level 3 as the preferred variant in this combination, arguing that "according to a very conservative analysis, [it] achieves more than 128 bits of security against all known classical and quantum attacks".

Falcon (to be standardized as **FN-DSA**)
It is an EUF-CMA secure post-quantum signature scheme based on structured lattices[22]. It has the advantage of small key and digital signature lengths. Its disadvantage is its very complex design, which makes it difficult to understand the details of the scheme well and to implement

[21] The security of the CRYSTALS-Dilithium algorithm is based on the difficulty of solving the Module-LWE and Module-SIS problems.

[22] The security of the Falcon algorithm is based on the difficulty of solving the SIS problem on the NTRU lattice.

it correctly. The short length of keys and signatures together with good security guarantees was the reason for its selection for standardization.

NIST expects to standardize the variants[26], sl. 14:

- Falcon-512 (Level 1, to be standardized as FN-DSA-512)
- Falcon-1024 (Level 5, to be standardized as FN-DSA-1024)

For security levels 1 and 5, its public keys are 897 and 1793 bytes in length, respectively, and its signatures are 666 and 1280 bytes in length, respectively.

Its standard has not been published yet[23].

SPHINCS+ (standardized as **SLH-DSA**)

It is an EUF-CMA secure post-quantum signature scheme based on hash functions. Its security is based on the security of the hash function used, in this case either SHAKE256, or SHA-256, or Haraka.

Unlike the XMSS and LMS schemes, SPHINCS+ does not require the signing device to maintain information about the signatures created by a given key and therefore has no limitation on the number of signatures by the same key. However, this is largely balanced by the extremely long digital signatures. This signature algorithm was chosen for standardization because it has very strong security guarantees and because it is constructed on a different basis than lattices.

SPHINCS+ variants based on SHA2 a SHA3 (SHAKE) hash functions were standardized:

A) Based on SHA2

- SLH-DSA-SHA2-128s (Level 1), SLH-DSA-SHA2-128f (Level 1)
- SLH-DSA-SHA2-192s (Level 3), SLH-DSA-SHA2-192f (Level 3)
- SLH-DSA-SHA2-256s (Level 5), SLH-DSA-SHA2-256f (Level 5)

B) Based on SHAKE

- SLH-DSA-SHAKE-128s (Level 1), SLH-DSA-SHAKE-128f (Level 1)
- SLH-DSA-SHAKE-192s (Level 3), SLH-DSA-SHAKE-192f (Level 3)
- SLH-DSA-SHAKE-256s (Level 5), SLH-DSA-SHAKE-256f (Level 5)

(5) Other competition candidates relevant to the recommended quantum-resistant cryptography

Four finalists and five alternate candidates in the KEM/Encryption category and three finalists and three alternate candidates in the Signatures category entered the third round of the NIST PQC Standardization competition.

[23] At the time of publication of this version of the Annex.

a) Other third-round candidates with high security guarantees[28]

For practical recommendations for quantum-resistant cryptography in the near future, we also find other candidates in the KEM/Encryption category essential, namely Classic McEliece (3rd and 4th round candidate) and FrodoKEM (alternate 3rd round candidate). The reason why this is so is closely related to their security. They have in principle higher theoretical security guarantees than the winner in this category, CRYSTALS-Kyber. And the reasons why they have not (yet) been selected for standardization are related to some of their practical properties[7], p. 34.

Classic McEliece is an IND-CCA2 secure post-quantum code-based algorithm. In the forty years since its publication, no major attacks have been found on this algorithm[30], sl. 3, although it is, from a security point of view, one of the most thoroughly researched candidates in the competition[24]. Therefore, the expert community has extreme confidence in its long-term security[42], sl. 88. The BSI[20] p. 39 recommends it for immediate hybrid use as a post-quantum KEM algorithm with the highest security guarantees. It performs very well in terms of the speed of cryptographic operations. Its main drawback is the extremely long public keys (from 250 kB for level 1 to 1.3 MB for level 5). This means that it is mainly suitable for applications in which the public key is static and does not need to be transmitted. It has not yet been selected for standardization by NIST, but as a candidate it has advanced to the fourth round of competition.

FrodoKEM The use of an unstructured lattice significantly improves its theoretical security, even compared to the CRYSTALS-Kyber, winner in the KEM/Encryption category. This is the reason why the BSI[7], p. 34, [29], p. 35 and ANSSI[57], sl. 20 recommend it for immediate hybrid use as a post-quantum KEM. However, it did not advance to the fourth round of the NIST competition as an alternate candidate. This is due to its relatively low performance, long private and public keys, and NIST's effort to also standardize other candidates than lattice-based ones.

FrodoKEM security levels:

- FrodoKEM-640, Level 1,
- FrodoKEM-976, Level 3,
- FrodoKEM-1344, Level 5.

b) Other fourth-round candidates of the NIST competition

Other fourth-round candidates of the NIST standardization competition, and possible future standards, are the BIKE and HQC algorithms. Their shared advantage over the Classic McEliece algorithm (from the same family of post-quantum algorithms – code-based) is a significantly shorter length of public and private keys. On the other hand, compared to the Classic McEliece

[24] Throughout all this time, the security parameters of the Classic McEliece algorithm only changed in relation to the growth of a potential attacker's computational capabilities and to the possibility of realizing quantum computers.

algorithm they are relatively new, which can be considered a disadvantage, since they have been exposed to expert analysis for a shorter period of time.

HQC is an IND-CCA2 secure post-quantum algorithm based on quasi-cyclic codes. The fourth-round submission uses a composition of Reed-Muller and Reed-Solomon error-correcting codes. For security levels 1, 3 and 5, its public keys are from 2249 to 7245 bytes in length, and its ciphertexts are from 4497 to 14485 bytes in length. The private key length for all security levels is only 40 bytes.

BIKE is a post-quantum algorithm based on QC-MDPC (quasi-cyclic moderate density parity-check codes). Compared to other alternate candidates, its advantage is very short public keys and ciphertexts, on the other hand, there is no proof published yet for its IND-CCA2 security. For security levels 1, 3 and 5, its public keys are roughly from 1541 to 5122 bytes in length, its ciphertexts roughly from 1573 to 5154 bytes in length, and its private keys roughly from 281 to 580 bytes in length.

c) Warning surprises in the NIST final

Rainbow was a finalist in the Signatures category of the NIST competition. It was also the only finalist based on polynomials with many variables (multivariate cryptography). Shortly thereafter, its variant of security level 1 was broken by an attack on a laptop over a weekend[15].

SIKE was an alternate candidate in the third round of the NIST competition in the KEM/Encryption category and was the only alternate candidate based on isogenies of supersingular elliptic curves. However, unlike the Rainbow algorithm, it made it through to the fourth round of the competition. And shortly thereafter, it was broken by a devastating attack on a classical computer for all its security levels[13].

The SIKE case is particularly alarming. Cryptography based on isogenies of supersingular elliptic curves has long been considered highly promising, and there were no serious doubts about its sound security basis. Yet it was recently broken by a practical attack on a classical computer.

d) NIST call for proposals for additional post-quantum digital signatures[27]

In September 2022, NIST called for proposals from the expert community for additional post-quantum signatures. It is particularly interested in algorithms[27], p. 2 based on principles other than structured lattices. For certain applications, in particular certificate authentication, NIST will likely be interested in digital signature algorithms with short output and fast signature validation.

(6) Trusted post-quantum cryptographic algorithms of the NIST competition

a) Intended use

The main objective of this subsection is to choose post-quantum algorithms of the NIST competition, the use of which can be recommended to protect sensitive information of

a critical level of confidentiality or integrity against the quantum threat[25]. Based on the consensus of the expert community and European security authorities, we anticipate that initially they will be used in hybrid combinations with appropriate approved classical asymmetric algorithms.

b) Digital signature for general use

In the case of post-quantum digital signature algorithms with expected general use, we consider trustworthy the current winners of the competition, which have already been standardized:

- ML-DSA Levels 3 and 5
- SLH-DSA Levels 3 and 5

FN-DSA Level 5 is likely to be added after its standardization.

c) KEM/Encryption

This category has only one winner so far, CRYSTALS-Kyber, standardized as ML-KEM.

The expert community, and the BSI in particular, have drawn attention to candidates who, although they did not win the competition, have high security guarantees compared to the winner. These include the Classic McEliece algorithm, which has not been successfully attacked in its 40 years of existence, and the FrodoKEM algorithm, which is defined on unstructured lattices and therefore has higher theoretical security than the winner of the competition[7], p. 34.

We consider the algorithms which correspond to levels 3 and 5 to be trustworthy.

Table 1: Trusted post-quantum KEM/Encryption algorithms[26]

ML-KEM-1024	FrodoKEM-1344	mceliece8192128	mceliece8192128f
ML-KEM-768	FrodoKEM-976	mceliece6688128	mceliece6688128f
		mceliece460896	mceliece460896f

[25] Therefore, we will not mention in this subsection the already standardized digital signatures LMS and XMSS, which, although they did not take part in the NIST competition, have such high security guarantees that they are recommended by all relevant authorities for independent deployment, especially to protect the integrity of software and firmware.

[26] As far as security levels are concerned, in the case of ML-KEM (CRYSTALS-Kyber) we rely on the final recommendation of its developers and in the case of the other two algorithms mainly on the recommendations of the BSI[29] pp. 35-36.

4 Hybrid or Standalone Use of Post-Quantum Cryptography?

(1) Reasons for hybrid use of post-quantum cryptography in the near future

There is a long-standing consensus in the scientific community that for some time post-quantum cryptography should only be used to protect information in hybrid combination with classical asymmetric cryptography[27]. This approach is still insisted upon by most European security authorities such as the German BSI[29], p. 25 and the French ANSSI[56].

Indeed, some newer post-quantum algorithms have been broken by attacks relying solely on classical computers[28]. In these cases, the use of standalone post-quantum algorithms instead of the approved asymmetric cryptography would lead to security degradation. However, a hybrid combination of post-quantum cryptography with classical secure asymmetric cryptography will at least be secure against classical attacks[29].

One reason for the breakability of some post-quantum algorithms is that certain types of post-quantum cryptography are relatively new. This means that we do not yet have sufficient guarantees that the corresponding mathematical problems, on whose practical intractability the security of the respective post-quantum algorithms is based, are indeed practically intractable, even on current computers[30].

But even the fact that the security of a relatively new cryptographic algorithm is based on a truly practically intractable mathematical problem does not necessarily mean that the algorithm is secure.[31]

---

[27] The BSI[7], p. 38 (and not only the BSI) proposes a more general approach, namely that a hybrid combination of any two of the following three mechanisms could be used to establish symmetric keys: classical asymmetric cryptography, post-quantum cryptography, and protection based on (possibly) pre-distributed keys.

[28] Or, they were broken by attacks requiring only classical computers and using physical side channels as well.

[29] If attacks on new post-quantum algorithms were based only on quantum algorithms, there would be no reason to use hybrid combinations of post-quantum and classical asymmetric cryptography.

[30] An example is the post-quantum KEM algorithm SIKE, long considered highly promising, on which a devastating attack requiring only a laptop has been found[13].

[31] An example is the classic attack on the Rainbow algorithm[15], which even made it to the finals of the third round of the competition[28]. Another example is the erroneous cloning of a random oracle in the constructions of some newer post-quantum KEM algorithms, which led in some cases to their breaking[35].

(2) CNSA 2.0 quantum-resistant algorithm suite approved by the U.S. NSA

In September 2022, the U.S. NSA published CNSA 2.0, the Commercial National Security Algorithm suite. The algorithms contained therein are approved by the NSA for use in National Security Systems (NSS). The CNSA 2.0 suite replaces the previous CNSA 1.0 suite with quantum-resistant cryptographic algorithms.

a) CNSA 2.0 algorithms[36]

The CNSA 2.0 suite contains algorithms divided into three application areas:

- Algorithms for software- and firmware-signing
- Symmetric-key algorithms
- General-use quantum-resistant asymmetric algorithms

Algorithms for software- and firmware-signing

The NSA recommends moving as quickly as possible in this area to the use of digital signature algorithms based on hash functions that have already been standardized by NIST. These are specified by NIST SP 800-208[64]. These algorithms are:

- LMS (*Leighton Micali Signature*) with recommended hash functions SHA-256/192
- XMSS (e*Xtended Merkle Signature Scheme*)

All their parameters are approved for all classified levels.
For the LMS and XMSS algorithms, NSA recommends their standalone use.

Symmetric-key algorithms

In this area, the following algorithms are approved for the NSS:

- AES-256 according to FIPS PUB 197
- SHA-384 or SHA-512 according to FIPS PUB 180-4

They are approved for all classified levels.

General-use quantum-resistant asymmetric algorithms

In this area, the following algorithms are approved for the NSS:

- ML-KEM – asymmetric key establishment algorithm
- ML-DSA – asymmetric digital signature algorithm

They are (only) approved in their Level 5 variants for all classified levels.
For the ML-KEM and ML-DSA algorithms, the NSA approves their standalone use.

b) NSA's rationale[37] for approving the standalone use of the CRYSTALS algorithms (ML-KEM a ML-DSA)

The NSA's decision to allow the CRYSTALS family of algorithms to be used on their own in U.S. national security systems was surprising to most experts because it contradicts the widely held consensual view that post-quantum cryptography should only be used in hybrid combinations in the near future. We therefore present below the NSA's rationale.

To the question: "How strong does NSA believe CNSA 2.0 algorithms are?", the NSA responds that it has conducted its own analysis of these algorithms and considers them suitable for long-term use in protecting various U.S. NSS[37], p. 3.

To the question: "What is NSA's position on the use of hybrid solutions?", NSA responds that it has confidence in the CNSA 2.0 algorithms and will not require NSS developers to use hybrid certified products for security reasons[37], p. 13.

To the question: "Should one use a hybrid or other non-standardized QR solution while waiting for a final NIST post-quantum standard?", NSA recommends against using hybrid or other non-standardized solutions in NSS missions. It encourages limited purchase for research and planning, but only for the purpose of transitioning to CNSA 2.0. Because NSA believes that CNSA 2.0 will adequately protect the NSS, it does not require hybrid solutions for security purposes[37], p. 14.

To the question: "What complications can using a hybrid solution introduce?", the NSA presents the following arguments, among others[37], pp. 13-14:

- The hybrid solution increases the complexity of the protocols involved, especially by the need for additional negotiation and error handling.
- The hybrid solution introduces interoperability problems since both algorithms of the hybrid solution must be common to all parties.
- After some time, the switch will be made to using only quantum-resilient algorithms. In the case of a hybrid solution, another transition will be required.
- More security products will fail due to implementation or configuration errors than due to the cryptographic algorithms used. If we have limited resources to increase cryptographic complexity, we can potentially weaken security.

Canadian Centre for Cyber Security's position on the suitability of hybrid solutions

In a presentation made in March 2023, the Canadian Centre for Cyber Security makes a number of specific arguments, mostly against the use of hybrid solutions, which show that it has a reserved position on the advisability of its use[39], sl. 10. It notes that the Government of Canada "has not yet made a decision on where hybrid PQC should be used", and that "system owners will need to make a policy decision on when to use hybrid"[39], sl. 10.

c) Limiting the approval of ML-KEM and ML-DSA to security level 5

Experience with the history of attacks on lattice cryptography suggests that their main consequence is the need to gradually increase the security parameters of lattice cryptography[42], sl. 88. And the choice of security level 5 represents a huge practical security margin[32].

[32] Recall that the CRYSTALS developers are confident that security level 3 is sufficient for their use.

(3) NÚKIB's position on the standalone use of ML-KEM and ML-DSA Level 5

The consensus of the expert community and European security authorities on the need to use a hybrid combination of post-quantum cryptography with an additional protection mechanism holds.

On the other hand, the U.S. NSA is one of the most sophisticated security authorities in the world with a high sense of its national security responsibilities. The likelihood of the NSA recommending, on the basis of its own analysis, cryptography for use in US national security systems (NSS) that would prove to be weak in the medium term is negligible.

Therefore, NÚKIB currently accepts both approaches for deploying quantum-resistant cryptography to protect sensitive information of critical confidentiality or integrity in the near term. Thus, both hybrid combinations and standalone uses of ML-KEM and ML-DSA of security level 5, implemented according to their respective NIST standards[66],[67], will be accepted.

(4) Special status of quantum-resistant digital signatures LMS and XMSS

Quantum-resistant digital signatures LMS and XMSS have been standardized by NIST already in 2020, so there is no obstacle to their implementation. When used correctly, they have high security guarantees and do not require a hybrid combination with a classical digital signature algorithm. They are suitable for protecting firmware integrity during updates and can be treated as approved algorithms with long-term security.

The NSA recommends their immediate deployment to protect software and firmware integrity[36], pp. 2-3. The BSI also recommends their use for this purpose[7], p. 62.

NÚKIB's position on the standalone deployment of LMS and/or XMSS to protect software and firmware integrity

NÚKIB recommends that the transition to the use of standalone quantum-resistant LMS and XMSS algorithms for protecting software and firmware updates should be made as soon as possible.

5 Quantum-Vulnerable Algorithms Approved in the "Minimum Requirements for Cryptographic Algorithms"

(1) Meaning of the term "quantum-vulnerable algorithm" as used below

a) Basic types of quantum-based attacks on cryptography

Current literature distinguishes two basic types of quantum-based attacks on cryptographic algorithms.

1) Attacks on cryptography protecting classical information represented by bit strings. In these scenarios, the attacker is assumed to have information in bits (e.g., ciphertexts or digital signatures) and to use, among other things, quantum algorithms implemented on quantum computers in the future to crack or forge them.

2) Attacks on cryptography protecting quantum information represented by strings of entangled qubits. These scenarios are based on the assumption that in the future a quantum internet will be implemented and used to enable communication using quantum information. This will qualitatively expand the attacker's capabilities, as their input will no longer be classical information, but quantum information.

The above shows that many currently known cryptographic algorithms, which are quantum-resistant in protecting classical information, would fail to protect quantum information transmitted over the future quantum internet.

b) Specification of the term "quantum-vulnerable algorithm" as used in this Annex

Based on available estimates, we do not expect the quantum internet to be realised until 15 to 20 years from now.

Therefore, both within the main document "Minimum Requirements for Cryptographic Algorithms" and within this Annex, we will strictly understand a quantum-vulnerable (cryptographic) algorithm to be only an algorithm that is vulnerable to attacks using a cryptanalytically relevant quantum computer when protecting classical information.

Thus, in both documents, we consider exclusively the above-mentioned scenario 1) and ignore the existence of scenario 2).

(2) Quantum resistance/vulnerability of symmetric cryptography

Quantum resistance of approved modes of symmetric cryptography
We consider the approved modes of symmetric cryptography to be quantum-resistant if they are used with a quantum-resistant approved block cipher or a quantum-resistant approved hash function.

Quantum resistance/vulnerability of approved block and stream ciphers
All approved block and stream ciphers with a key length of 256 bits are quantum-resistant. All approved block and stream ciphers with key lengths of 128 bits and 192 bits are quantum-vulnerable.

Urgency of the transition to quantum-resistant approved block and stream ciphers
The transition to quantum-resistant approved block ciphers is neither too urgent nor too difficult. A slightly higher degree of urgency is required when a 128-bit key cipher is used to protect data confidentiality[33]. It is recommended to move as much as possible to using approved symmetric ciphers with only a 256-bit key by the mid-2030s[34].

(3) Quantum resistance/vulnerability of hash functions

Quantum resistance/vulnerability of approved hash functions
All approved hash functions with an output length of 384 bits or more are quantum-resistant. All approved hash functions with an output length of 256 bits are quantum-vulnerable.

Urgency of the transition to quantum-resistant approved hash functions
The transition to quantum-resistant approved hash functions is neither urgent nor too demanding[35]. Nevertheless, we recommend moving to use, to the maximum extent possible, approved hash functions with output lengths of 384 bits or more by the mid-2030s[36].

(4) Quantum vulnerability of approved classical digital signature algorithms

a) General use of classical digital signature algorithms

Quantum vulnerability of approved classical digital signature algorithms
None of the approved classical digital signature algorithms are quantum resistant.

---

[33] The quantum resistance/vulnerability of symmetric cryptography with 128-bit and 192-bit key lengths corresponds by definition to security levels 1 and 3, respectively, of post-quantum cryptography. The BSI states[29], p.37 that "the use of Grover's algorithm could theoretically accelerate the search of the key space of symmetric mechanisms quadratically. Whether an acceleration compared to a classic exhaustive search of the key space can also be achieved in practice is the subject of current research and has not been definitively answered yet." On the other hand, the transition to quantum-resistant symmetric cryptography is relatively easy. It suffices to replace ciphers with too short keys by approved ciphers with a key length of 256 bits.

[34] Recall that the NSA's CNSA 2.0 suite only allows AES-256.

[35] The quantum vulnerability of hash functions with an output length of 256 bits is closely related[20] to the security level 2 of post-quantum cryptography. According to Figure 1 in [20], it is even close to level 3 for more realistic memory requirements. On the other hand, the transition to fully quantum-resistant hash functions is relatively easy. It is sufficient to replace hash functions with an output length of 256 bits with hash functions with an output length of 384 bits.

[36] Recall that the NSA's CNSA 2.0 suite only allows SHA-384 and SHA-512.

Urgency of the transition to quantum-resistant digital signatures in most cases
Unlike approved symmetric cryptography and approved hash functions, approved asymmetric cryptography will be breakable once cryptanalytically relevant quantum computers are deployed. Therefore, its replacement with quantum-resistant cryptography must occur before such computers are constructed. By most estimates, this will be around the early 2030s. In most use cases of digital signatures, it will be sufficient to re-sign quantum-forgeable signatures using quantum-resistant algorithms shortly before that.

b) Digital signatures used for integrity protection during firmware updates

Approved digital signatures used for integrity protection during firmware updates have a higher urgency for their replacement with quantum-resistant algorithms. This is due to the fact that some memories that store public keys for integrity protection during firmware updates may not be rewritable later.

There exist standards for quantum-resistant digital signatures, LMS and XMSS, whose security is generally accepted by both the expert community and security authorities. We therefore recommend that the transition to using LMS and XMSS algorithms to protect the integrity of firmware during updates be initiated as soon as possible[37].

(5) Urgency of transition to quantum-resistant cryptography in the area of classical algorithms for key establishment

Quantum vulnerability of approved classical key establishment algorithms
None of the approved classical algorithms for key establishment are quantum-resistant.

Urgency of the transition to quantum-resistant key establishment algorithms
Once cryptanalytically relevant quantum computers are made real, it will be possible to use them to crack all currently approved asymmetric cryptography. If the attacker stores the intercepted cryptographically protected communication, then by the time he has a suitable quantum computer, he will be able to decrypt it. Therefore, the transition to quantum-resistant cryptography in the area of key establishment is of high urgency, especially when protecting long-term sensitive information[38] of a critical level of confidentiality[8], and it should be performed in the next few years.

---

[37] The timely transition to the use of LMS or XMSS to protect the integrity of firmware and software is primarily in the economic interest of the cryptographic system operator. Once the practical implementation of cryptanalytically relevant quantum computers is imminent, this transition will need to be made very quickly.

[38] Sensitive data can be divided according to the length of time their sensitivity is maintained. Short-term sensitivity of data means that it is certain that the sensitivity period will not exceed a few months. Such situations, where we know in advance that a given application or device will only handle short-term sensitive information, are rare and also difficult to detect. Given that in practice it is often very difficult to distinguish in bulk between short-term sensitive and medium- to long-term sensitive information, we recommend that all critically sensitive information should be treated as requiring at least medium-term protection.

6 Choice of Quantum-Resistant Cryptography

(1) Quantum-resistant cryptography for symmetric key establishment

As for approved classical cryptography for key establishment, the urgency of its replacement by quantum-resistant cryptography is high. For the case of cryptographic protection of sensitive information of critical level of confidentiality, we estimate the appropriate deadline for completing the transition to quantum-resistant key establishment to be the end of 2030[39].

a) Types of transition to quantum-resistant symmetric key establishment

Replacing classical asymmetric cryptography with symmetric cryptography

We consider symmetric cryptography with a key length of 256 bits to be quantum-resistant. However, asymmetric cryptography has significant advantages over symmetric cryptography in terms of security and practicality. There is no need to distribute private keys, and when distributing public keys, protecting their integrity is sufficient. Therefore, we do not recommend the transition to quantum-resistant cryptography based on symmetric cryptography, with justified exceptions.

Moving to standalone use of ML-KEM Level 5

Here, the ML-KEM Level 5 algorithm needs to be implemented according to the NIST FIPS 203 standard[66]. We recommend this algorithm as one of the main methods of transitioning to quantum-resistant key establishment.

Transition to hybrid combinations

In a hybrid combination, at least two of the following options[40] must be used to derive the symmetric keys[7], p. 38:

- classical asymmetric key establishment (key agreement or asymmetric encryption),
- post-quantum KEM/Encryption scheme,
- pre-distributed keys[41].

In specific cases, quantum key distribution can be included in addition.

[39] This timeframe is set in accordance with the joint statement of the majority of EU member states regarding the PQC transition[12].

[40] The main purpose of hybrid solutions is to provide (at least partial) security even in situations where one of the components is broken. Thus, the key derivation mechanism requires that the security of at least one of the established secrets from which it is derived is sufficient to ensure the security of the derived key.

[41] A typical representative of pre-distributed keys are the so-called PSKs (Pre-Shared Keys).

(2) Quantum-resistant hybrid combinations for symmetric key establishment

a) Use of pre-distributed keys

Typically, this will be a situation where the default cryptographic system already uses approved classical asymmetric cryptography and pre-distributed keys[42] to establish keys. The symmetric key of the hybrid solution is derived using KDF[43] from both the secret established by classical asymmetric cryptography and the corresponding pre-shared key. The use of classical asymmetric cryptography protects against classical attacks when a pre-shared key is compromised. But not against quantum-based attacks. Thus, for this use of pre-shared keys to be meaningful at all, it is necessary that their compromise never occurs during their life cycle[44]. Therefore, these hybrid solutions are not recommended except in exceptional well-founded cases, and if used, will only be approved for the short term.

In hybrid combinations involving the use of post-quantum cryptography and pre-shared-key protection (and possibly also classical asymmetric cryptography), we will consider the protection provided by pre-shared keys as complementary only. The main guarantee of quantum resistance in these cases will be provided by the use of post-quantum cryptography.

b) Hybrid combination of classical asymmetric and post-quantum cryptography for key establishment

Classical asymmetric cryptography for hybrid key establishment
For hybrid combination with post-quantum cryptography, any approved classical algorithms for key establishment can be used.

Post-quantum cryptography for hybrid key establishment
Any of the algorithms listed in Table 1: "Trusted KEM/Encryption post-quantum algorithms" in Section 3, par. (6), point c) may be used for hybrid combination with an approved algorithm for key establishment.

We recommend these hybrid combinations as one of the main methods of transitioning to quantum-resistant key establishment.

[42] A typical representation of pre-distributed keys are PSKs (Pre-Shared Keys) to ensure the authenticity of the Diffie-Hellman exchange.

[43] Key derivation function.

[44] Protection against quantum threat in this case translates to physically protecting the confidentiality of pre-distributed keys during their distribution and protecting their confidentiality until they are deleted. Adequate confidentiality protection can be quite costly.

c) Use of quantum key distribution

The main advantage of quantum key distribution is its absolute theoretical security arising from the laws of quantum mechanics. But even in this case, theoretical security does not imply practical security. Quantum key distribution, like other types of cryptography, is breakable by attacks on security flaws in its implementation.

The main problems of quantum key distribution include its cost and, in particular, the practical limitations of its applicability. In certain cases, where its practical limitations are not a concern, it can be used, but only as an additional protection mechanism, typically in conjunction with post-quantum cryptography, i.e., only within specific hybrid solutions.

(3) Practical and security aspects of the main recommended types of quantum-resistant key establishment

Main recommended types of quantum-resistant key establishment

- Standalone use of ML-KEM Level 5 implemented according to the NIST standard.
- Hybrid combination of approved classical asymmetric cryptography and post-quantum cryptography as per 6 (2) b).

Standalone use of ML-KEM Level 5 implemented according to the NIST FIPS 203 standard[66]

The security guarantees of this solution are based on the fact that the U.S. NSA has approved it for the NSS on the grounds that it has high confidence in its long-term security. It means that this solution is highly likely to be of a longer-term nature and will not need to be changed in the near future. We anticipate that ML-KEM Level 5 implementations compliant with the FIPS 203 standard will stay among the approved quantum-resistant algorithms for the long term.

Advantages and disadvantages of the proposed hybrid solutions compared to the use of the standalone ML-KEM algorithm

Hybrid solutions are likely to be considered transitional in the sense that sooner or later they will be replaced by standalone post-quantum cryptography. On the other hand, they generally provide stronger security guarantees, given the lower maturity of post-quantum cryptosystems and hence the potential for currently unknown attacks on them.

Hybrid solutions with McEliece or FrodoKEM may have higher theoretical security than using standalone ML-KEM of the same security level. This is true only on the condition that these algorithms are implemented according to accepted standards, which is contrary to the ambition to implement them as soon as possible.

Classic McEliece has a relatively short ciphertext, very slow key generation, and extremely long public keys[41], sl. 14. Thus, it will typically be used for a large number of encryptions with the same public key. In that case, its forward security will be problematic.

FrodoKEM has relatively fast cryptographic operations, relatively large public keys, and roughly equally large ciphertexts[41], sl. 14. It will be possible to use it in compliance with the

forward security requirement, but in that case, it will be necessary to handle the frequent transmission of long public keys.

The hybrid combination of ML-KEM Level 3 and ECDH may have better practical properties than using ML-KEM Level 5 alone. However, it will have lower security guarantees with respect to quantum attacks.

(4) Quantum-resistant cryptography for digital signatures to protect authenticity during firmware updates

LMS and XMSS, standardized digital signature algorithms based on hash functions

We recommend that the LMS and XMSS algorithms for integrity protection during software and firmware updates be implemented following the NIST standards as soon as possible.

(5) Quantum-resistant cryptography for general-purpose digital signatures

a) General-purpose quantum-resistant digital signature mechanisms

Standalone post-quantum algorithm

- ML-DSA Level 5 in accordance with the NIST standard[67]
- SLH-DSA Levels 3 and 5 in accordance with the NIST standard[68]

Hybrid combination – dual digital signature

- Hybrid combination of a classical digital signature and a post-quantum digital signature using the dual signature method[45].

b) Recommended components of a hybrid (dual) digital signature

Classical asymmetric cryptography

Any approved classical digital signature algorithm can be used for a hybrid combination with post-quantum cryptography.

Post-quantum cryptography

For a hybrid combination with an approved classical digital signature algorithm, one of the following post-quantum algorithms can be used:

- ML-DSA Levels 3 and 5
- SLH-DSA Levels 3 and 5

FN-DSA Level 5 is likely to be added after its standardization.

[45] The dual digital signature of a message is performed by first signing the message using one method and then signing the concatenation of the message and its first digital signature using the other method[43], p. 19.

c) Comments on practical and security aspects

Main recommended types of quantum-resistant general-purpose digital signatures

- Standalone use of ML-DSA Level 5 implemented according to the FIPS 204 standard.
- Hybrid combination of approved classical asymmetric cryptography and post-quantum cryptography.

Standalone use of ML-DSA Level 5 implemented according to the FIPS 204 standard

The advantages of this solution are similar to those of using the standalone ML-KEM. It is highly likely to be of a long-term nature, so it will not need to be changed in the near future. It can be expected to be one of the long-term approved quantum-resistant algorithms.

Hybrid combination of EC-DSA and Falcon-1024 (future FN-DSA 1024)

This solution may be relevant when the use case for quantum-resistant cryptography requires the shortest possible signature.

Hybrid combination containing SLH-DSA Level 5

In cases where even higher security guarantees are required than those provided by ML-DSA Level 5, SLH-DSA Level 5 can be used as the post-quantum component instead.

7 Incorporating Post-Quantum Cryptography into Cryptographic Protocols

(1) The need to develop new variants of cryptographic protocols in the context of post-quantum cryptography implementations

The transition to the use of quantum-resistant cryptography will require not only the implementation of post-quantum algorithms, but also the adaptation of cryptographic protocols to the properties of these algorithms[46].

Post-quantum public key lengths

In some cryptographic protocols, public key lengths are limited, and switching to using post-quantum cryptography with typically longer public keys can lead to problems. It will be necessary to implement mechanisms to handle this problem.

Replacing the Diffie-Hellman key exchange with KEM/Encryption

The Diffie-Hellman exchange is a process where it does not matter which of the participants is the initiator and which is the responder. KEM or asymmetric encryption is a process where the initiator generates its public key and sends it to the responder. The latter generates a symmetric key, encrypts it with the initiator's public key and sends it to the respondent. This means that their roles are not symmetric, and this must be taken into account when moving from Diffie-Hellman key exchange to KEM.

Hybrid combination of post-quantum cryptography with a classical mechanism

By classical mechanism here we mean either classical asymmetric cryptography or the specific use of pre-shared keys to protect against the quantum threat. The intended hybrid combination must not have lower security than either the use of post-quantum cryptography alone or the use of the corresponding classical mechanism alone.

Use of KEM in some key establishment protocols instead of digital signatures

The lengths of post-quantum digital signatures are quite large, which can cause problems in some key establishment protocols. Therefore, work is underway to provide implicit authenticity of key establishment using static KEM. A typical example is the development of the KEMTLS protocol[45].

[46] Modification, development and testing of new variants of cryptographic protocols is the responsibility of cryptologists and standardization bodies in cooperation with commercial companies active in the field.

(2) Approaches to mechanisms for combining the hybrid solution components

a) KDF-based approach recommended by NIST[26], sl. 16 and BSI[7] for key establishment

This approach assumes that the original key establishment protocol implements a cryptographically sound KDF (key derivation function) with a variable input length, whose input was a secret established by classical asymmetric cryptography, and whose output was the derived established symmetric key.

In this case, transitioning to the hybrid extension by post-quantum cryptography means that the concatenation of both established secrets enters the KDF, i.e., both the secret established by classical cryptography and the secret established by post-quantum cryptography[47].

BSI recommends the following generalizations of the previous procedure: first, the possibility of a more general use of the KDF[7], p. 37 per NIST SP 800-56C[63], and second, the possibility that inputs to the KDF include at least two of the following three secrets:

a) secrets established by classical asymmetric cryptography,
b) secrets established by post-quantum cryptography,
c) the corresponding pre-shared key.

To this pair of secrets, the BSI also adds as an option a secret established on the basis of quantum key distribution. However, its use does not reduce the requirement for using two of the three secrets mentioned above[7], p. 38.

Note that NIST[26], sl. 16 also specifies the method of establishing the two secrets, in the form of a serial combination of classical and post-quantum secret establishment.

b) The principle of dual KEM and dual signature recommended by ENISA

This approach in the case of dual KEM[43], pp. 17-18 assumes that two subkeys have been established: one based on classical KEM and the other based on post-quantum KEM. The resulting combined (hybrid) key is obtained by applying a hash function to the concatenation of the two public keys used and the two established subkeys.

In the case of the dual signature[43], p. 19, either we first sign the given input using the classical signature algorithm and then sign the concatenation of the input and the result using the post-quantum algorithm, or vice versa. Both methods have advantages and disadvantages.

[47] BSI also considers the possibility of a more general use of KDF, but in the case of specific protocols, it is primarily concerned with the possibility of concatenating secrets of different origins entering the KDF.

(3) Cryptographic agility

During the transition to quantum-resistant cryptography, there may be a need for repeated replacements of cryptographic algorithms. In the case of using hybrid combinations, this is obvious, but the need to replace some cryptography based on unexpected new findings cannot be ruled out.

Therefore, when deploying new cryptographic systems, care should be taken to ensure that they are cryptographically agile, i.e., that they allow potential exchanges of cryptographic algorithms to take place as easily and smoothly as possible. This requires both backward compatibility, i.e., the ability to support multiple sets of cryptographic algorithms at the same time, and also the flexibility to exchange them easily.

8 Recommendations in Summary

(1) Urgency levels for transition to quantum-resistant cryptography in different areas

a) High-priority areas

Key establishment algorithms to protect sensitive information of critical level of confidentiality

The transition to quantum-resistant hybrid combinations or standalone post-quantum KEM/Encryption in this area of information protection is highly urgent. We estimate the end of 2030 as the appropriate completion date.

Digital signatures to protect firmware and software integrity during updates

The transition to post-quantum LMS or XMSS algorithms in this area should start as soon as possible. LMS and XMSS algorithms are already among the approved algorithms.

b) Priority areas

The transition to quantum-resistant cryptography in these areas of information protection will need to be completed before the implementation of cryptanalytically relevant quantum computers. Current estimates are that this will occur in the early 2030s.

Other[48] digital signatures for the protection of sensitive information of critical level of integrity[8]

Transition to standalone post-quantum signatures or quantum-resistant hybrid digital signatures is necessary. All digital signatures legally relevant at the time of implementation of the anticipated quantum computers will need to be signed with a quantum-resistant digital signature.

Key establishment algorithms to protect the confidentiality of other sensitive information

Transition to standalone post-quantum cryptography or hybrid quantum-resistant cryptography is necessary.

Symmetric encryption with a key length of 128 or 192 bits to protect sensitive information of a critical level of confidentiality[49]

Symmetric encryption with a key length of 128 or 192 bits, either standalone or as part of authenticated encryption, will need to be replaced by encryption with a key length of 256 bits.

[48] By "other digital signatures" we mean digital signatures that are not intended to protect firmware and software integrity during updates (see Section 8, par. (1), point a)).

[49] Extending the key lengths of approved symmetric cryptography to 256 bits will be relatively easy compared to the other steps required. It is therefore advisable to proceed with it as soon as possible.

c) Other areas of the transition to quantum-resistant cryptography

We will estimate the appropriate date for completing the transition to quantum-resistant cryptography in these areas at some later date.

General purpose digital signature for the protection of other sensitive information
We presume the transition to standalone quantum-resistant cryptography.

Symmetric ciphers with key lengths of 128 or 192 bits for the protection of other sensitive information
Symmetric ciphers with a key length of 128 or 192 bits will need to be replaced by ciphers with a key length of 256 bits. This applies to all their use in symmetric cryptography[50].

Hashing with an output length of 256 bits
Transition to hashing with an output length of 384 bits or more[51].

(2) Recommended quantum-resistant cryptography

a) Recommended standalone post-quantum cryptography

- LMS and XMSS for digital signatures for software and firmware integrity protection
- ML-KEM-1024 for key establishment
- ML-DSA-87 for general-purpose digital signatures

b) Recommended hybrid quantum-resistant cryptography

Key establishment
The recommended hybrid quantum-resistant cryptography for key establishment is described in Section 6, par. (2), point b) "Hybrid combination of classical asymmetric and post-quantum cryptography for key establishment". The essence of the recommended hybrid combination methods is described in Section 7, par. (2) "Approaches to mechanisms for combining the hybrid solution components". These solutions can be treated as approved cryptographic algorithms with a presumably reduced validity period[52].

---

[50] Using quantum computers to crack the symmetric ciphers under consideration will be extremely computationally expensive, according to current knowledge. Therefore, we expect that in the case of protecting "other sensitive information" there will be a number of justified exceptions.

[51] Justified exceptions may also apply to the hashing of sensitive information. This is due to the high memory and computational requirements of the BHT algorithm improvements known so far.

[52] The assumption of a reduced validity period is related to the subsequent transition to standalone post-quantum cryptography.

Digital signatures

The recommended hybrid cryptography for general-purpose digital signatures is described in Section 6, par. (5) "Quantum-resistant cryptography for general-purpose digital signatures".

(3) Incorporation of quantum-resistant cryptography into systems

a) Cryptographic agility

When deploying new cryptographic systems, care should be taken to ensure that they are cryptographically agile, i.e., that they allow potential exchanges of cryptographic algorithms to take place as easily and smoothly as possible[53].

b) Incorporation into cryptographic protocols

Due to some of the properties of quantum-resistant cryptography, its incorporation into information and communication systems will require a number of modifications and adaptations to cryptographic protocols[54].

[53] For more information see Section 7, par. (3) of this document.

[54] For more information see Section 7, par. (1) of this document.

9 References

[1] P. W. Shor: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, IEEE, 1994, Algorithms for quantum computation: discrete logarithms and factoring – Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on

[2] P. W. Shor: Polynomial Time Algorithms for Prime Factorizations and Discrete Logarithms on a Quantum Computer, arXiv:quant-ph/9508027v2 25 Jan 1996

[3] J. Proos, Chr. Zalka: Shor's discrete logarithm quantum algorithm for elliptic curves, arXiv preprint quant-ph/0301141 (2003). [quant-ph/0301141] Shor's discrete logarithm quantum algorithm for elliptic curves (arxiv.org)

[4] L. K. Grover: A Fast Quantum mechanical Algorithm for Database Search, [quant-ph/9605043] A fast quantum mechanical algorithm for database search (arxiv.org)

[5] Brassard, Høyer, Tapp: Quantum Algorithm for the Collision Problem, [quant-ph/9705002] Quantum Algorithm for the Collision Problem (arxiv.org)

[6] M. Mosca: The Latest View on Quantum Computing and its Impact on Critical Digital Infrastructures, PowerPoint Presentation (securetechalliance.org)

[7] BSI: Quantum-safe cryptography – fundamentals, current developments and recommendations, Quantum-safe cryptography – fundamentals, current developments and recommendations (bund.de)

[8] N. Koblitz: QUANTUM COMPUTING: REALITY OR HYPE? TiaSangQC.pdf (washington.edu)

[9] G. Kalai: The Argument against Quantum Computers, the Quantum Laws of Nature, and Google's Supremacy Claims, Laws, Rigidity and Dynamics, Proceedings of the ICA workshops 2018 & 2019 Singapore and Birmingham, [2008.05188] The Argument against Quantum Computers, the Quantum Laws of Nature, and Google's Supremacy Claims (arxiv.org)

[10] M.I. Dyakonov: When will we have a quantum computer? 1903.10760.pdf (arxiv.org)

[11] M.I. Dyakonov: Will we ever have a quantum computer? Will We Ever Have a Quantum Computer? | SpringerLink

[12] Securing Tomorrow, Today: Transitioning to Post-Quantum Cryprography, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=3

[13] W. Castryck, T. Decru: An efficient key recovery attack on SIDH, An efficient key recovery attack on SIDH (iacr.org)

[14] Multivariate Public Key Cryptography and its Cryptanalysis, Quantum Cryptanalysis, Simons Institute, 02.2020, mpkc-hhl-1.pdf (berkeley.edu)

[15] W. Beullens: Breaking Rainbow Takes a Weekend on a Laptop: 214.pdf (iacr.org)

[16] D. A. Cooper, D. C. Apon Q. H. Dang, M. S. Davidson, M. J. Dworkin, C. A. Miller: NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes, Recommendation for Stateful Hash-Based Signature Schemes (nist.gov)

[17] L. Chen: NIST Post-Quantum Cryptography Standardization, AWACS 2016, Microsoft PowerPoint – AWACS-PQC-2016-05082016 (cryptoexperts.com)

[18] Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process, call-for-proposals-final-dec-2016.pdf (nist.gov)

[19] S. Jaques, M. Naehrig, M. Roetteler, F. Virdia: Implementing Grover Oracles for Quantum Key Search on AES and LowMC, 1910.01700.pdf (arxiv.org)

[20] P. Kim, D. Han, K. Chul Jeong: Time–space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2, [1805.05534] Time-Space Complexity of Quantum Search Algorithms in Symmetric Cryptanalysis (arxiv.org)

[21] A. Chailloux, M. Naya-Plasencia, A., Schrottenloher: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: ASIACRYPT 2017. pp. 211–240 (2017], and in: 847.pdf (iacr.org)

[22] M. N.Plasencia, A. Schrottenloher, A. Chailloux, L. Grassi: New Algorithms for Quantum (Symmetric) Cryptanalysis, New Algorithms for Quantum (Symmetric) Cryptanalysis (malb.io)

[23] Physical and Logical Qubits, WikipediA, The Free Encyclopedia, Physical and logical qubits - Wikipedia

[24] A. G. Fowler, M. Mariantoni, J. M. Martinis, A. N. Cleland: "Surface codes: Towards practical large-scale quantum computation". Physical Review A. 86 (3) 032324, [1208.0928] Surface codes: Towards practical large-scale quantum computation (arxiv.org)

[25] N. N. Hegade, P. Koushik , F. Albarrán-Arriagada, Xi Chen, E. Solano: Digitized Adiabatic Quantum Factorization, 2105.09480.pdf (arxiv.org)

[26] D. Moody: NIST PQC: LOOKING IN THE FUTURE, Selected presentations of the Fourth PQC Standardization Conference, NIST PQC: LOOKING INTO THE FUTURE

[27] NIST: Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process, Call for Additional Digital Signature Schemes for the PQC Standardization Process (nist.gov)

[28] Overview of NIST Round 3 Post-Quantum cryptography Candidates, Round-3.pdf (pqsecurity.com)

[29] BSI TR-02102-1, BSI-Technical Guideline, Designation: Cryptographic Mechanisms and Key Length, Version: 2024-01, Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2024-01 (bund.de)

[30] M. R. Albrecht, D. J. Bernstein, T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, Ed. Persichetti, Chr. Peters, P. Schwabe, N. Sendrier, J. Szefer, M. Tomlinson, W. Wang: Classic McEliece: conservative code-based cryptography: Classic McEliece Round 3 Update (nist.gov)

[31] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, Chr. Peikert, An. Raghunathan, D. Stebila: FrodoKEM, A simple and conservative KEM from generic lattices, FrodoKEM Practical post-quantum key exchange from the Learning with Errors Problem (nist.gov)

[32] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, Chr. Peikert, An. Raghunathan, D. Stebila: FrodoKEM practical quantum-secure key encapsulation from generic lattices. =1=FrodoKEM practical quantum-secure key encapsulation from generic lattices (nist.gov)

[33] T. Lange: KEM-DEM Framework 2WF80, Introduction to Cryptology, KEM-DEM framework (hyperelliptic.org)

[34] P. Campbell, M. Groves, D. Shepherd: SOLILOQUY: A Cautionary Tale, S07_Groves_Annex.pdf (etsi.org)

[35] M. Bellare, H. Davis, F. Güther: Separate Separate Your Domains: NIST PQC KEMs, Oracle Cloning and Read-Only Indifferentiability, Separate Your Domains: NIST PQC KEMs, Oracle Cloning and Read-Only Indifferentiability (iacr.org)

[36] National Security Agency | Cybersecurity Information Sheet, Announcing the Commercial National Security Algorithm Suite 2.0, CSA_CNSA_2.0_ALGORITHMS_.PDF (defense.gov)

[37] National Security Agency | Cybersecurity Information Sheet, The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ, CSI_CNSA_2.0_FAQ_.PDF (defense.gov)

[38] National Security Agency | Frequently Asked Questions, Quantum Computing and Post-Quantum Cryptography, Quantum_FAQs_20210804.PDF (defense.gov)

[39] CANADIAN CENTRE FOR CYBERSECURITY: How the Canadian goverment is Preparing for PQC, PKI Comsortium, Post-Quantum Cryptography Conference, March 2023, PowerPoint Presentation (pkic.org)

[40] GSMA: Post Quantum Telco Network Impact Assessment Whitepaper, Version 1.0, 17 February 2023, PQTN_1_Doc_006 PQTN White Paper CLEAN (gsma.com)

[41] D. Bong: A bouquet of crypto flowers, The Impacts of Post Quantum Cryptography (post-quantum.nl)

[42] D. Bernstein, T. Lange: Post-Quantum Cryptography: Detours, delays, and disasters, slides-dan+tanja-20220820-pqcrypto-16x9.pdf

[43] ENISA: POST-QUANTUM CRYPTOGRAPHY, Integration study. Post-Quantum Cryptography - Integration study — ENISA (europa.eu)

[44] T. Lange: Post-quantum cryptography, 2022, Post-quantum cryptography (hyperelliptic.org)

[45] D. Stebila: Recent Results in KEMTLS, 20220512-TII.pdf

[47] D. Moody: Let's Get Ready to Rumble-The NIST PQC "Competition": Let's Get Ready to Rumble- The NIST PQC "Competition"

[48] D. Moody: What was NIST thinking? Round 2 of the NIST PQC "Competition", Round 2 of the NIST PQC "Competition" - What was NIST Thinking?

[49] L. Chen: An Overview of NIST PQC Standardization, Microsoft PowerPoint - CHEN_NIST.pptx (etsi.org)

[50] NIST IR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8413, PQC Project Third Round Report | CSRC

[51] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, Gr. Seiler, D. Stehle: CRYSTALS (Cryptographic Suite for Algebraic Lattices) CCA KEM: Kyber Digital Signature: Dilithium, CRYSTALS-Dilithium (nist.gov)

[52] National Security Agency | Central Security Service, Quantum Key Distributions and Quantum Cryptography, Quantum Key Distribution (QKD) and Quantum Cryptography QC (nsa.gov)

[53] ANSII: SHOULD QUANTUM KEY DISTRIBUTION BE USED FOR SECURE COMMUNICATIONS? Should Quantum Key Distribution be Used for Secure Communications? | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

[54] National Cyber Security Centre: Whitepaper, Quantum security technologies, Quantum security technologies - NCSC.GOV.UK

[55] National Cyber Security Centre: Whitepaper, Quantum-safe cryptography, Quantum-safe cryptography - NCSC.GOV.UK

[56] ANSSI views on the Post-Quantum Cryptography transition March 25, 2022, anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

[57] B. A. Macchia: The Long Road Ahead to Transiton to Post-Quantum Cryptography, MS Ressearch of Security & cryptography, 19-October 2022, IEEE SecDev 2022, PowerPoint Presentation (ieee.org)

[58] D. J. Bernstein, Ch. Dobraunig, M. Eichlseder, S. Fluhrer, S. L. Gazdag, A. Hülsing, P. Kampanakis, S. Kölbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, Ch. Rechberger, J. Rijneveld, P. Schwabe: SPHINCS+, SPHINCS+ (nist.gov)

[59] T. Lange: Introduction to post-quantum cryptography, 22 June 2017, Executive School on Post-Quantum Cryptography, Introduction to post-quantum cryptography (pqcrypto.org)

[60] Kyber Home, CRYSTALS, Cryptographic Suite for Algebraic Lattices, Kyber (pq-crystals.org)

[61] Dilithium Home, CRYSTALS, Cryptographic Suite for Algebraic Lattices, Dilithium (pq-crystals.org)

[62] GSM Association Non-Confidential Official Document PQ.01, Post Quantum Telco Network Impact Assessment Whitepaper, Post Quantum Telco Network Impact Assessment Whitepaper, Version 1.0, 17 February 2023, PQTN_1_Doc_006 PQTN White Paper CLEAN (uk5g.org)

[63] E. Barker, L. Chen, R. Davis: NIST Special Publication 800-56C, Revision 2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, August 2020, Recommendation for Key-Derivation Methods in Key-Establishment Schemes (nist.gov)

[64] D. A. Cooper, D. C. Apon, Q. H. Dang, M. S. Davidson, M. J. Dworkin, C. A. Mille: NIST Special Publication 800-208, Recommendation for Stateful Hash-Based Signature Schemes, October 2020, Recommendation for Stateful Hash-Based Signature Schemes (nist.gov)

[65] E. R. Anschuetz, J. P. Olson, A. Aspuru-Guzik, Y. Cao: Variational Quantum Factoring, [1808.08927] Variational Quantum Factoring (arxiv.org)

[66] National Institute of Standards and Technology (2024) Module-Lattice-based Key Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[67] National Institute of Standards and Technology (2024) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[68] National Institute of Standards and Technology (2024) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf https://doi.org/10.6028/NIST.FIPS.205.ipd

[69] French Cybersecurity Agency (ANSSI), Federal Office for Information Security (BSI), Netherlands National Communications Security Agency (NLNCSA), Swedish National Communications Security Authority, Swedish Armed Forces; Position Paper on Quantum Key Distribution
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.html

Document version

Date (original)	Date (translation)	Version	Changed (name)	Change
July 1, 2023	-	1.0	OBIT, NÚKIB	Document creation
Feb. 1, 2025	May 20, 2025	2.0	OBIT, NÚKIB	Document revision, NIST post-quantum standards, BIKE and HQC algorithms, timeline adjustments based on the EU states' joint statement[12]