CN-pytec
centro criptológico nacional

CCN-TEC 009

Recommendations for a safe post-quantum transition

CCN
centro criptológico nacional

December 2022

COURTESY TRANSLATION

Edition:

CCN-PYTEC

Edition Date: December 2022

INDEX

1. INTRODUCTION

1. A major development of quantum computing has taken place in the last few years and it has become a subject that is attracting considerable attention in the scientific community. This attention is related to the enormous advantages of the emergence of a quantum computer with high calculation capability to address problems that are difficult to solve today, such as those related to logistics, aeronautics, biotechnology, pharmacology, etc.

2. No one has dared to state a date when relevant quantum computing will become reality. For a few years, it has been said that this computation will be available in 20-25 years, but years has passed and this period does not change. The most optimistic ones consider that we could have quantum computing with high computing capability by the end of the 30's, but there is no clear evidence of it.

3. Other aspects of our lives that will be significantly affected by the advances in quantum computing, will be those related to security, protection and custody of information. It will have such a great calculation power that it will be able to solve most of the mathematical problems on which the security of current cryptography is based, rendering it without defence, that is, allowing access to confidential information. In other words, cryptography as we know it today will no longer achieve its objectives of confidentiality, integrity, authentication, and non-repudiation.

4. In any case, as the protection of information is a complex task that falls within the competence of all states and all sectors of society (companies, institutions, users, etc.) it is necessary to start taking steps so that, no matter when quantum computing becomes a reality (short/medium/long term), society as a whole will be prepared to guarantee the protection of information.

5. It is well known that the security of the most commonly used asymmetric (or public-key) cryptosystems today depends on two mathematical problems that are considered difficult to solve with the computers currently available and that can be considered as pre-quantum problems.

6. These problems are: the integer factorization problem (IFP) (see Annex A.1), which consists in determining the prime factors dividing a given compound integer, and the discrete logarithm problem (DLP) (see Annex A.2), which requires determining the power (in the case of a multiplicative group) to which the given generator in the group concerned should be raised, or the multiple of the generator in the case of the additive group.

7. The first of these two problems is the basis of RSA cryptosystem security 5.[28]; while the latter is, in its multiplicative version, the ElGamal cryptosystem 5.[8], and in its additive version, the elliptic curve-based cryptosystems 5.[15], 5.[19].

8. As already mentioned, both the integer factorization and the discrete logarithm problems have been traditionally considered two computationally safe problems, because the computational capacity of today's computers requires a sub-exponential runtime to be able to break any of them.

9. However, Peter Shor in 1997, published two quantum algorithms capable of effectively breaking both problems, that is, at a polynomial runtime, if a quantum computer with sufficient computing power was available 5.[31]. These algorithms cannot be implemented in conventional computers and require quantum computers to be executed.

10. Thus, it can be said that Shor algorithms have shown that today's asymmetric cryptography is vulnerable to quantum computing, making it imperative to search for and establish new asymmetric systems that are invulnerable to this type of computing. In fact, if a conventional computer needs $O\ (2^{\sqrt[3]{\log n}})$ bit operations to break one of these two problems, a quantum computer, using the corresponding Shor algorithm, would reduce that number of bit operations to 0 (log $^3 n$) with a memory storage of 0 (log n) bits.

11. We should bear in mind that the same problems used to ensure the security of asymmetric encryption systems are those used to guarantee the reliability of the processes of production and verification of electronic signatures. Thus, in general, the security of the former is the same as that the latter.

12. However, in the case of signatures, especially when used for authentication processes, they only need to ensure their security until they are verified, which often requires a much shorter period of time than that needed to maintain information confidentiality. Indeed, if a signature scheme was compromised by a quantum computer, it is very likely that the digital certificate with which it was made would have expired and the security of the signature would not be compromised. A different situation would be if the signature would be valid for several years (as firmware, for instance).

13. Symmetric (or secret-key) cryptosystems do not seem to be vulnerable to quantum computing to date. The best quantum algorithms that attack this type of cryptography are Grover 5.[10], 5.[11] and Simon 5.[32] algorithms, that would reduce the calculation time required to break them to the square root of the current time. That is, if a quantum computer were to be developed with sufficient computing capacity, the security of the current symmetric systems would be equivalent to that of the same systems but with half-length keys. That is, if a current computer needs $O(n)$ bit operations to break one of these symmetric systems, with the Grover algorithm this time would be reduced to a $O(\sqrt{n}\ )$ bit operations and would require memory storage of $O(\log n)$ bits.

14. So far, there are no news about the existence of a quantum computer with enough computing capacity to break the cryptographic protocols currently in use, and everything suggests that it will not be available soon; however, in order to anticipate future developments that will jeopardize current systems, the Centro Criptológico Nacional (CCN) publishes this document in order to raise awareness among cryptography users (organizations and companies) of the need to migrate to more robust cryptographic systems and resistant to quantum computing (quantum resistant).

15. We should also take into account that for applications that handle information that needs to remain confidential for long periods of time or with high security requirements, this migration to new systems is a necessity. Such a need, comes from the paradigm known as “store now, decrypt later”, which could be a reality when a relevant quantum computer is available.

2. POST QUANTUM CRIPTOGRAPHY

16. Due to the development of quantum computing and its application to disrupt pre-quantum cryptographic systems (currently used), for a few years now, the cryptographic community has begun researches to propose new cryptographic systems that are resistant to such computing. This new cryptography, based on different mathematical problems from those currently used (such as IFP and DLP), has been called "post-quantum cryptography" (PQC) or "quantum computing-resistant cryptography" (QR).

17. Due to the above mentioned threat posed by quantum computing, the NIST (National Institute of Standards and Technology), entity responsible for American standardization processes, made an international call in November 2016 to select new quantum computing-resistant algorithms in order to include them as new standards 5.[22]. In this process, the NIST only included asymmetric encryption, Key Encapsulation Mechanism (KEM) and digital signature.

18. The security of the algorithms submitted to this process has been based on mathematical problems that are part of the following five areas:

    a) Error-correcting codes (code-based cryptography).

    b) Lattices (lattice-based cryptography).

    c) Hash functions (hash-based cryptography).

    d) Multivariate quadratic polynomials (multivariate quadratic cryptography).

    e) Isogenies on elliptic curves (isogeny-based cryptography).

19. Having published the candidates who passed the different rounds that are part of the final selection process, the NIST published 5.[25]5.[26] the list of selected algorithms in July 2022 (while waiting for a fourth round).

20. These candidates are listed in **Table 1** and **Table 2**. Both tables indicate the areas to which the candidates belong and, in parentheses, the corresponding mathematical problems: MLWE (Module Learning with Errors, see Annex A.3) and SIS (Short Integer Solution, see Annex A.4).

Asimmetric Cryptosystem and KEM	Area and mathematical problem
CRYSTALS-Kyber	Structured lattice (MLWE)

Table 1. KEM candidate selected by the NIST after the third round and associated mathematical primitive

Digital signature	Area and mathematical problem
CRYSTALS-Dilithium	Structured lattice (MLWE)
Falcon	Structured lattice (SIS)
SPHINCS$^+$	Hash functions

Table 2. Signature candidates selected by the NIST after the third round and associated mathematical primitives

21. The only algorithm selected to date for KEM is CRYSTALS-Kyber [30]; whereas CRYSTALS-*Dilithium* [17], Falcon (*FAst-Fourier Lattice-based COmpact signatures over NTRU*) [27] and SPHINCS+ [12] have been selected for signatures.

22. As shown in Table 1 and Table 2, with the exception of the digital signature SPHINCS+, all proposals that passed the third round are lattice-based security. However, the NIST's standardization process is not complete, so new proposals are likely to be added to the previous ones in the not too distant future.

23. In fact, the NIST has not completely ruled out other proposals. Another four algorithms will therefore be analysed in the fourth round, that is: BIKE (Bit Flipping Key Encapsulation) [2], HQC (Hamming Quasi-Cyclic) [1], Classic McEliece [3] and SIKE (Supersingular Isogeny Key Encapsulation) [14]. All of them are listed in Table 3. **KEM candidates to be analysed by the NIST in the fourth round and associated mathematical primitives**

24. .

Asymmetric Cryptosystem and KEM	Mathematical Primitive
BIKE	Quasi-cyclic moderate density code
HQC	Hamming quasi-cyclic codes
Classic McEliece	Goppa codes
SIKE†	Isogenies on elliptic curves
† recent researches have shown that the SIKE algorithm is vulnerable, see paragraph 27	

Table 3. KEM candidates to be analysed by the NIST in the fourth round and associated mathematical primitives

25. Both BIKE and HQC are based on structured codes and either of them could be considered suitable as KEM for not lattice-based general purposes. It is believed that the NIST will select one of these two candidates for standardization at the end of the fourth round.

26. Although Classic McEliece was proposed as a final candidate in the third round, the NIST seems not to consider it as a possible standard at present, as —though safe— it will not be likely used due to the large size of its public key.

27. In addition, despite the fact that at the time of the release of the third-round candidates, SIKE was an attractive candidate for the NIST due to its smaller sizes of key and encrypted text, it is not expected to be considered in the future. Researchers from the Catholic University of Louvain have submitted a paper in which they claim to have found an

efficient key-recovery attack for SIKEp434 (security level 1), by using a single core processor, in approximately one hour [5].

28. On the other hand, the CCN is really interested in the study of key agreement algorithms. Therefore, in addition to the CRYSTALS-Kyber selected by the NIST and listed in Table 1, it also considers the unstructured lattice-based algorithm FrodoKEM [21]. Regarding its security, this algorithm can be considered as a conservative option. More details on this recommendation will be provided in section 3.2.

29. Finally, it is important to note that the NIST will make a new call for digital signature algorithms with short signatures and quick verification that are resistant to quantum computing. The NIST is expected to seek new signature schemes that are not based on structured lattices.

3. CCN RECOMMENDATIONS

30. The CCN closely follows the publications made by the NIST regarding the establishment of new standards that resist quantum computing. In this regard, the CCN, in collaboration with other international, and especially European, organizations, carries out its own research on the proposed post-quantum algorithms.

31. There is no doubt about the threat posed to current cryptography by the development of quantum computers, which is why it is of the utmost importance for the CCN that the Spanish cryptographic community, as well as the industry, organizations and companies, begin to prepare, as soon as possible, to prevent or at least counter such a threat. This requires adapting to new developments and taking into account the proposals that go beyond the various security filters. For this reason, the CCN recommends taking the necessary actions to initiate the migration processes necessary to implement the recommended postquantum algorithms to alleviate the adverse aspects of quantum computing. These recommendations are outlined below.

3.1 MIGRATION PLAN

32. Taking into account the above-mentioned principle of "store now and decrypt later", it is necessary to develop a **migration plan** which should include the following points:

- Determine what information must remain secured and for how long.
- Do an inventory of products and cipher machines that are being use to protect my information and assets.
- Rigorously analyse whether or not such products and cipher machines resist quantum computing.
- Establish a migration plan to hybrid solutions (see Section 3.6).
- Decide what new products do I need, and how much time I need to purchase and deploy them.
- Determine how much time I have available (see Mosca's Theorem in ANNEX B).

3.2 KEY ENCAPSULATION MECHANISMS

33. As mentioned above, the CCN currently has a greater interest in key encapsulation algorithms (KEM) than in signature algorithms. In particular, the CCN, like other European security agencies, has not abandoned the FrodoKEM algorithm, based on the LWE problem defined on lattices, which is included in Tabla 4.

Asymmetric Cryptosystem and KEM	Mathematical primitive
CRYSTALS-Kyber	Structured lattice (MLWE)
FrodoKEM	Unstructured lattice (LWE)

Tabla 4. KEM algorithms recommended by the CCN and associated mathematical primitives

34. We should remember that FrodoKEM was included by the NIST in the third round as an alternative algorithm and not as a final one, having been discarded on the third round [23].

35. The reasons cited by the NIST for its decision on FrodoKEM are primarily based on its lower performance than other lattice-based algorithms.

36. It is accepted that this lower performance is due to the fact that FrodoKEM does not use any additional mathematical structure (plain LWE) as opposed to other lattice-based algorithms, such as defining a ring (RLWE) or a modulus (MLWE) underlying structure. This lack of structure makes FrodoKEM the most conservative security option, hence the CCN maintains it as an algorithm for KEM.

37. The additional structures mentioned (ring or module) offer the advantage that the algorithms based on them are more efficient in performing their computations and require smaller keys. However, the existence of such an underlying structure could be the cause of attacks against the algorithms that use them. In fact, this view, shared by some European security agencies, seems to be somewhat endorsed by the NIST itself, which considers FrodoKEM to be a kind of conservative back-up algorithm in the case of attacks against structured lattice-based algorithms.

38. Obviously, the CCN also considers the NIST selected KEM, i.e. the CRYSTAL-Kyber presented in Table 1, as authorized, while taking into account the result of the fourth round in which the KEMs shown in Table 3. **KEM candidates to be analysed by the NIST in the fourth round and associated mathematical primitives**

39. are considered, i.e. BIKE, HQC and Classic McEliece.

40. In addition to other recommended mechanisms, the above mentioned algorithm, with its corresponding parameters, is included in the Guide of Cryptographic Mechanisms Authorized by the CCN [6].

3.3 DIGITAL SIGNATURES

41. The CCN also recommends the signatures selected by the NIST after the third round, i.e. CRYSTALS-Dilithium, Falcon and SPHINCS+. These signatures are listed in Table 5.

Digital signature	Mathematical primitive
CRYSTALS-Dilithium	Structured Lattice (MLWE)
Falcon	Structured Lattice (SIS)
SPHINCS+	Hash functions

Table 5 CCN-recommended signature schemes and associated mathematical primitives

3.4 HASH-BASED SIGNATURES FOR FIRMWARE UPDATES

42. One type of algorithm that has not been considered in the call made by the NIST is stateful hash-based digital signature methods. This is probably justified because the security offered by these algorithms has been studied at length and they are considered safe in quantum computing. However, it is known that although there are some disadvantages, such as that only a limited number of signatures can be made, they are particularly suitable for signing firmware updates, because they last longer than the usual signatures and the number of signatures to be generated, given a key, is limited.

43. Such algorithms are known as the *Leighton-Micali Signature* or LMS (Leighton-Micali Signature) [18] and the extended Merkle Signature Scheme or XMSS [4] [13] and have been standardized by the IETF (Internet Engineering Task Force). The NIST also released the Special Publication SP800-208 adopting these standards [24].

44. The CCN recommends the **immediate use of the XMSS scheme for firmware upgrade,** as shown in Table 6.

Signature for firmware	Mathematical primitive
XMSS	Stateful hash functions

Table 6. Firmware signing scheme recommended by the CCN and associated mathematical primitive

3.5 KEY LENGTHS FOR SYMMETRIC ALGORITHMS AND HASH FUNCTIONS

45. As mentioned above in Section 1. , symmetric encryption algorithms are considered less vulnerable to quantum computing than asymmetric ones, since the threat posed so far is that, if there is a quantum computer with sufficient computing capacity, the security they provide would be equivalent to that of the same algorithm whose key was half the original length.

46. For this reason, the recommendation is to use algorithms with keys of at least 256 bits, since such security, in the presence of a quantum computer, would be equivalent to that of the same algorithm with a 128-bit key, which is currently considered acceptable.

47. Therefore, the use of symmetric algorithms, type AES, with 256-bit keys, and especially in cases where data protection is important, is recommended.

48. Similarly, the use of hash functions of less than 256 bits is not recommended. Therefore, the recommended hash functions are those of the SHA2 and SHA3 families that are larger than 256 bits.

49. Table 7 lists the symmetric algorithms and hash functions recommended by the CCN

Algorithms	Key/hash length
AES	256
SHA2	256 384 512
SHA3	256 384 512

Table 7. Symmetric algorithms recommended by the CCN and corresponding key lengths and hashes.

3.6 HYBRID SOLUTIONS

50. Given that post-quantum cryptographic algorithms in the process of standardization are relatively new, it is clear that they will require a long-term analysis to ensure they are secure. In addition, attacks against them have been published in recent years, which mainly exploit errors in their implementations and side-channel or fault-inducing attacks. For these reasons, the recommendation to use hybrid solutions should be considered, i.e. combining simultaneously post-quantum algorithms with pre-quantum ones.

51. In other words, a "hybrid solution" consists in building a solution that combines pre-quantum (current) and post-quantum primitives, in order to obtain both traditional cryptographic guarantees and those offered by solutions resistant to quantum computing [16].

52. Another additional advantage of hybrid solutions is that they facilitate the development of crypto-agile solutions (see Section 3.7). Indeed, if one of the solution's algorithms were to be vulnerable, it would be easily replaced by another of its family.

53. On the other hand, it is clear that hybridization is not a permanent solution. In fact, it is an intermediate step in the migration from current to post-quantum cryptography since as time goes by, PQC will become an increasingly reliable solution.

54. As an example, in key encapsulation mechanisms, the outputs of both algorithms are sent to a Key Derivation Function (KDF) to produce the key for symmetric encryption (See Figure 1).

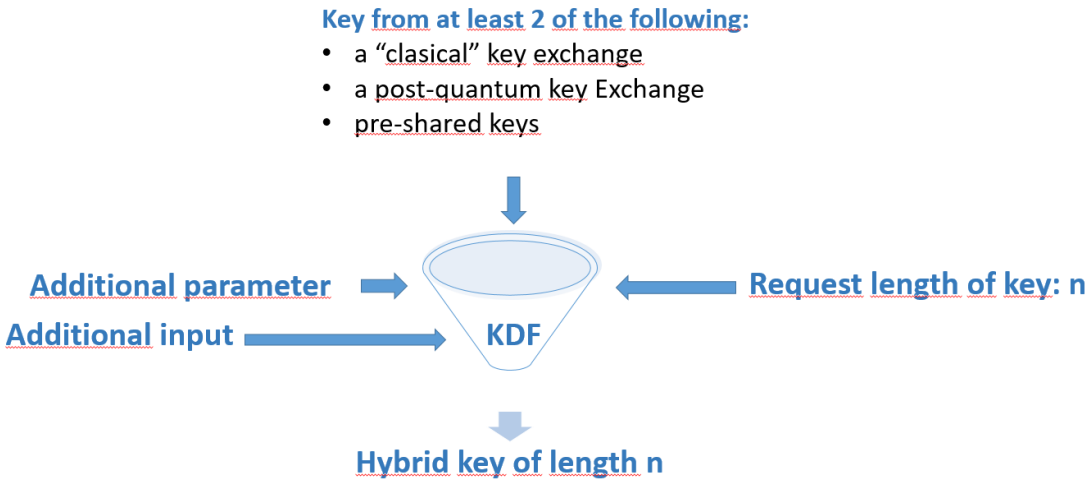


Figure 1. Hybrid solution for key exchange as a transitional measure

55. In addition, the use of hybrid solutions sometimes requires tuning the cryptographic protocols currently in use. In fact, there are already recommendations in this regard for the Transport Layer Security (TLS) [33] and IKEv2 (Internet Key Exchange) [9][34] protocols.

56. The CCN recommends **the use of hybrid solutions as soon as possible**.

3.7 CRIPTO-AGILITY

57. The concept of «crypto-agility» or cryptographic agility is the ability of a security system to rapidly switch to new encryption mechanisms in the event of vulnerabilities or threats to the algorithms commonly used by that system.

58. The idea behind this concept is a rapid adaptation to new cryptographic standards so that it does not entail major changes in the infrastructure used. It should be noted that this change might lead to important decisions. If such situation arises, an organization must be able to quickly switch to a different encryption method to minimize damages. This process includes changing cryptographic algorithms, security keys, certificates and other cryptographic technologies.

59. Therefore, crypto-agility not only encourages the development and evolution of the system, but also acts as a security measure or incident response mechanism.

60. It is possible that new attacks against the cryptographic systems currently used will be published, and that a quantum computer with sufficient computing capacity will be available to break the current cryptosystems. This is why crypto-agility becomes more important and special attention must be paid to the cryptographic mechanisms used, so that they are flexible enough to allow them to react quickly and mitigate the threats of new developments and to ensure the necessary level of security.

61. In sum, crypto-agility should become a design criterion for new products, regardless of the state of development of quantum computers.

3.8 RECOMMENDED TRANSITION ROADMAP

62. In the light of the previous comments, it seems appropriate to establish a transition roadmap for carrying out the recommended actions so that the shift from pre-quantum to post-quantum cryptography takes place following a gradual transition.

63. The recommended transition should follow the following steps:

PHASE 1	• Immediate use of hash-based signatures for firmware updates.
PHASE 2	• Use of hybrid solutions to provide greater defence to pre-quantum cryptography.
PHASE 3	• Use of hybrid solutions with the security guarantees provided by post-quantum cryptography.
PHASE 4	• Adoption of post-quantum cryptographic algorithms considered resistant to quantum computing.

64. More precisely, the actions in each of the phases are as follows:

- **Phase 1**: As discussed in Section 3.4, the CCN recommends the immediate use of XMSS scheme for firmware update (see Table 6).
- **Phase 2**: Section 3.6 highlights the importance of using hybrid solutions to combine pre-quantum primitives with post-quantum ones in order to obtain the proven security guarantees provided by the former, in addition to those provided by the latter. These guarantees would be aligned with the advantages of crypto-agility discussed in section 3.7. This second phase should be initiated as soon as possible, using the algorithms recommended by the CCN and mentioned in this document, either KEM (see Tabla 4), digital signature (see Table 5), hash-based signatures for firmware updates (see Table 6) or symmetric (see Table 7). This phase is expected to last until 2025.
- **Phase 3**: The hybridization process will be enhanced so that the post-quantum algorithms recommended by the CCN are added to the secure algorithms of pre-quantum cryptography. In this sense, it is likely that the algorithms already commented in phase 2 will be strengthened, while some of the algorithms that are being analysed in the fourth phase called by NIST can be considered (see Table 3. **KEM candidates to be analysed by the NIST in the fourth round and associated mathematical primitives**
-). This phase will not probably start until 2030.
- **Phase 4**: At this stage, the algorithms recommended by the CCN should be widely adopted and implemented, abandoning hybrid solutions as far as possible. This phase will not probably start until 2030.

65. Figure 2 shows the recommended timetable for implementing the above-mentioned phases.

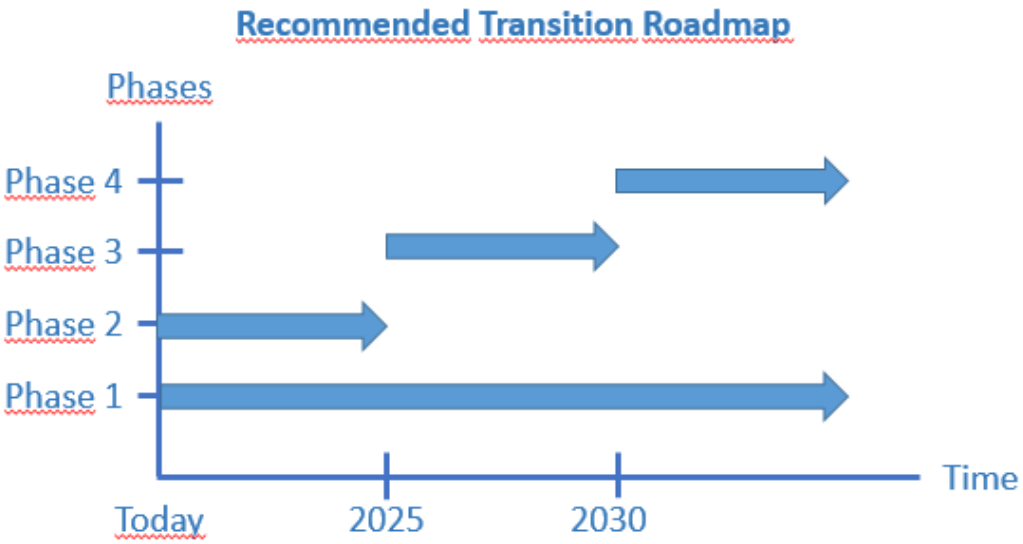


Figure 2. Recommended transition roadmap for the transition of pre-quantum to post-quantum cryptography

4. REFERENCES

[1] C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O.Blazy, J.C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, and J. Bos. HQC (Hamming Quasi-Cyclic). NIST, Round 2, 2020. http://pqc-hqc.org/index.html.

[2] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. Aguilar Melchor, R. Misoczki,E. Persichetti, N. Sendrier, J.P. Tillich, G.Zemor, and V. Vasseur. *BIKE (Bit Flipping Key Encapsulation)*. NIST, Round 2, 2020. https://bikesuite.org/files/v4.0/BIKE_Spec.2020.05.03.1.pdf.

[3] D.J. Bernstein, T. Chou, T. Lange, I. von Maurich R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer,and W. Wang. *Classic McEliece*. NIST, Round 2, 2020. https://classic. mceliece.org/.

[4] J. Buchmann, E. Dahmen, and A. Hülsing. XMSS - a practical forward secure signature scheme based on minimal security assumptions. In *Proc. Post-Quantum Cryptography (PQCrypto 2011), Lecture Notes Comput. Sci.*, volume 7071, pages 117–129, 2011. https://doi.org/10.1007/ 978-3-642-25405-5_8.

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

[6] CCN-STIC 221. *Guía de Mecanismos Criptográficos Autorizados*. Centro Criptológico Nacional, 2022.

[7] R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué. *El criptosistema RSA*. RA-MA, Madrid, España, 2005. https://www.ra-ma.es/libro/ el-criptosistema-rsa_141831/.

[8] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31:469–472, 1985. https://doi.org/10.1109/TIT.1985.1057074.

[9] S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov. *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*. Internet Engineering Task Force, RFC 8784, 2020. https://tools.ietf.org/html/rfc8784.

[10] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th annual ACM symposium on Theory of Computing (STOC'96)*, pages 212–219, 1996. https://doi.org/10.1145/800070.802214.

[11] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, 1997. https://doi.org/10.1103/PhysRevLett.79.325.

[12] A. Hulsing, D.J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L.Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M.M. Lauridsen, F. Mendel,R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, and J.-P. Aumasson.SPHINCS+. Online

publication, 2020. https://sphincs.org/.

[13] A. Hülsing, D. Butin, S.L. Gazdag, J. Rijneveld, and A. Mohaisen. *XMSS: extended Merkle signature scheme*. Internet Engineering Task Force, RFC 8391, 2018. https://tools.ietf.org/html/rfc8391.

[14] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik. SIKE: Supersingular Isogeny Key Encapsulation,2016. http://sike.org.

[15] N. Koblitz. Elliptic curve cryptosytems. *Math. Comp.*, 48(177):203–209, 1987. https://doi.org/10.1090/S0025-5718-1987-0866109-5.

[16] B.A. LaMacchia. *Getting Ready for the Post-Quantum Transition*. Microsoft Utimaco Webinar, 2020. https://ecstech.com/wp-content/uploads/2020/08/2020_ISO_BLaMacchia_Final.pdf.

[17] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, andD. Stehle. CRYSTALS-DILITHIUM. Online publication, 2020. https:// pq-crystals.org/.

[18] D. McGrew, M. Curcio, and S. Fluhrer. *Leighton-Micali hash-based signatures*. Internet Engineering Task Force, RFC 8554, 2019. https://tools.ietf.org/html/rfc8554.

[19] V.S. Miller. Use of elliptic curves in cryptography. *Lecture Notes Comput. Sci.*, 218:417–426, 1986. https://doi.org/10.1007/3-540-39799-X_31.

[20] M. Mosca. *Cybersecurity in a Quantum World: will we be ready?* Universtiyof Waterloo, 2015. https://csrc.nist.gov/csrc/media/events/ workshop-on-cybersecurity-in-a-post-quantum-world/documents/ presentations/session8-mosca-michele.pdf.

[21] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia,P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. FrodoKEM. Online publication, 2020. https://frodokem.org/.

[22] NIST. Post-quantum cryptography. On-line publication, 2017. https:// csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[23] NIST. PQC standardization process: Third round candidate announcement. Online publication, 2020. https://csrc.nist.gov/News/2020/ pqc-third-round-candidate-announcement.

[24] NIST. *Recommendation for Stateful Hash-Based Signature Schemes*. National Institute of Standard and Technology, Special Publication, SP800-208, 2020. https://doi.org/10.6028/NIST.SP.800-208.

[25] NIST. Post-quantum cryptography. selected algorithms 2022. On-line publication, 2022. https://csrc.nist.gov/Projects/ post-quantum-cryptography/selected-algorithms-2022.

[26] NIST. PQC standardization process: Announcing four candidates to be standardized, plus fourth round candidates. Online publication, 2022. https://csrc.nist.gov/News/2022/ pqc-candidates-to-be-standardized-and-round-4.

[27] T. Prest, P.A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. Falcon. Online publication, 2020. https://falcon-sign.info/.

[28] R. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. https://doi.org/10.1145/359340.359342.

[29] A. Fúster Sabater, L. Hernández Encinas, A. Martín Muñoz, F. Montoya Vitini, and J. Muñoz Mas qué. *Criptografía, protección de datos y aplicaciones. Guía para estudiantes y profesionales*. RA-MA, Madrid, España, 2012. https://www.ra-ma.es/libro/ criptografia-proteccion-de-datos-y-aplicaciones-una-guia-para\-estudiantes-y-profesionales_48492/.

[30] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, G.Seiler, and D. Stehle. CRYSTALS-KYBER. Online publication, 2020. https://pq-crystals.org/.

[31] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. https://doi.org/10.1137/S0097539795293172.

[32] D.R. Simon. On the power of quantum computation. *SIAM Journalon Computing*, 26(5):1474–1483, 1997. https://doi.org/10.1137/S0097539796298637.

[33] D. Stebila, S. Fluhrer, and S. Gueron. *Hybrid key Exchange in TLS 1.3 (draft-ietf-tls-hybrid-design-04).* Internet Engineering Task Force, RFC 7296. https://tools.ietf.org/html/ draft-stebila-tls-hybrid-design-03, year = 2020.

[34] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, and V. Smyslov. *Multiple Key Exchanges in IKEv2 (draft-ietf-ipsecme-ikev2-multiple-ke-08)*. Internet Engineering Task Force, RFC 7296, 2023. https://datatracker.ietf.org/doc/pdf/ draft-ietf-ipsecme-ikev2-multiple-ke-08.

ANNEX A. MATHEMATICAL PROBLEMS

66. This annex contains definitions of the mathematical problems underlying the security of certain cryptosystems mentioned in this document, as well as other mathematical aspects considered appropriate for the readers' convenience.

A.1. INTEGER FACTORISATION PROBLEM (IFP)

67. The mathematical problem underlying the security of one of the most widely used public key cryptosystems in use today (RSA) is the integer factorisation problem [7], [29].

68. The **Fundamental Theorem of Arithmetic** is well known, which states that every composite number n ≥ 2 admits a single factorisation as a product of powers of primes:

$$n = \prod_{i=1}^{k} p_i^{e_i} = p_1^{e_1} \bullet p_2^{e_2} \bullet \dots \bullet p_k^{e_k}$$

69. Being the p_i different primes and each e_i a positive integer. The following problem arises from this theorem:

Definition 1
The «**factorisation problem**» of a composite integer consists in determining its factorisation as product of its prime factors.

70. Factorisation methods are classified in two groups depending, mainly, on the execution time: "General purpose" and "special purpose". The computation time of general-purpose ones depend only on the size of the composite number to be factored; whereas the latter provide better results, i.e. their computation time improves if the number to be factored has special properties.

71. The group of general-purpose methods include the quadratic sieve and the general screening of the numerical field sieve; whereas the group of the special-purpose methods include the successive division method, Pollard's $\rho(ro)\ y\ p-1$ methods, the elliptic curves method and the general number field sieve screening method.

72. As a rule, special-purpose methods should be used first when dealing with the problem of factoring a composite number, since they are usually more efficient. For this reason, one should initially search for the small prime factors of the given composite number using, whenever possible, some of the properties of the number. If these methods do not provide the desired solution, general-purpose methods can be used.

A.2. DISCRETE LOGARITHM PROBLEM (DLP)

73. The "discrete logarithm problem" is a particular case of the general problem of calculating logarithms. The logarithm of *a* in the base *b* is known to be the number $x \in \mathbb{R}$, written, $log_b a = x$, precisely if *x* is the power to which the base has to be raised to obtain the given number: $b^x = a$

74. However, when the set of real numbers is replaced by the multiplicative group $\mathbb{Z}^*_p$, then we speak of the discrete logarithm [7], [29]. More precisely,

Definition 2 Given a prime number *p*, a generator *g* of the multiplicative cyclical group $\mathbb{Z}_p^*$ and an element $a \in \mathbb{Z}_p^*$, the ***problem of the discrete logarithm*** is to determine efficiently the integer $x\ with\ 0 \leq x \leq p-2$ so that $g^x \equiv a\ \ (mod\ p)$, that is, $x = log_g a (mod\ p)$.

75. If the cyclical group is additive, every element of the group *G* will be a multiple of the generator g, $g + g + \cdots + g = k \cdot g$. Therefore, in this case you have the following

Definition 3 Given a cyclical additive group *G*, an element *a* ∈ *G* and a generator *g*, the ***problem of the elliptical logarithm*** (sometimes called additive discrete logarithm) is to efficiently determine the integer *x with* $0 \leq x \leq p-2$ so that $x \cdot g = a$.

76. The discrete logarithm problem is the one on which the security of certain cryptographic protocols, such as the Diffie-Hellman (DH) key change protocol and the ElGamal encryption scheme, is based. The elliptical logarithm problem is the basis of the security of the Diffie-Hellman analogue key-changing protocol over elliptic curves (ECDH) and elliptic curve-based encryption schemes (ECC).

A.3. LEARNING WITH ERRORS PROBLEM (LWE)

77. The learning with errors problem (LWE) is parametrised by an integer n, a prime number $q \geq 2$ and a probability distribution $\chi\ over\ \mathbb{Z}_q$.

78. Typically χ is a normal distribution of mean v and standard deviation δ:

$$\chi = G(x) = \frac{1}{\delta\sqrt{2\pi}} exp^{\frac{1}{2}\left(\frac{x-v}{\delta}\right)^2}$$

79. A distribution $A_{s,\chi}$ of a LWE problem on $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled by choosing uniformly and randomly $a \xleftarrow{\chi} \mathbb{Z}_q^n$, $e \xleftarrow{\chi} \mathbb{Z}_q$ and considering as output the pair r $(\boldsymbol{a}, b), where\ b = \langle s, \boldsymbol{a} \rangle + e\ (mod\ q)$

80. There are two versions of a LWE problem: search and decision.

81. In **the search version of the LWE problem** are given m independent samples $(\boldsymbol{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\ de A_{s,\chi}\ with\ b_i = \langle s, \boldsymbol{a}_i \rangle + e_i\ (mod\ q) \in \mathbb{Z}_q$ and it is about finding the secret vector $s \in \mathbb{Z}_q^n\ where\ m > n$.

82. The idea is to determine the value *s* from *m* given samples:

$$a_1 \xleftarrow{\chi} \mathbb{Z}_q^n, \quad b_1 = \langle s, a_1 \rangle + e_1\ (mod\ q)$$

$$a_2 \xleftarrow{\chi} \mathbb{Z}_q^n, \quad b_2 = \langle s, a_2 \rangle + e_2\ (mod\ q)$$

$$\vdots$$

$$a_m \xleftarrow{\chi} \mathbb{Z}_q^n, \quad b_m = \langle s, a_m \rangle + e_m\ (mod\ q)$$

83. In **the decision version of the LWE problem**, the goal is to distinguish between two vector pairs

$$(a_i, b_i) \; y \; (\bar{a_\iota}, \bar{b_\iota}) \; where \; a_i, \bar{a_\iota} \underset{\chi}{\leftarrow} \mathbb{Z}_q^n, \; b_i = \langle s, \boldsymbol{a}_i \rangle + e_i \; (mod \; q) \epsilon \; \mathbb{Z}_q \; y \; \bar{b_\iota} \; \epsilon \; \mathbb{Z}_q$$

That is, it is a question of deciding, for a given pair of vectors, whether the second vector is the scalar product of the first vector by some secret vector, *s* added with some error, or whether the second vector is uniformly random.

84. In the case where underlying ring structure is considered in the lattice, one speaks of the Ring Learning with Errors (RLWE), and if such a structure is the module structure, one speaks of the de LWE problem on modules or *Module Learning With Errors* (MLWE).

A.4. SHORT INTEGER SOLUTION PROBLEM (SIS)

85. In the problem of the Short Integer Solution (SIS) are considered m uniformly random vectors $a_i \in \mathbb{Z}_q^n$ that define a matrix $A \in \mathbb{Z}_q^{n \times m}$, and the aim is to find a non-zero vector $z \in \mathbb{Z}^m of \; norm \; \| z \| \leq \varepsilon$ such that:

$$A \cdot z = \sum_{i=1}^{m} a_i z_i = 0 \; \in \mathbb{Z}_q^n$$

ANNEX B. MICHELE MOSCA'S THEOREM

86. Mosca's theorem can be stated in the following terms [20]:

87. **Theorem.** Being x the length of time (in years) one needs to keep their confidential data secure, y the time (in years) one needs to re-equip existing infrastructure with a quantum computing (QR) resilient solution and z the time (in years) that it will take to build a large-scale quantum computer (or any other relevant advance). Then, if $x + y > z$, we have a serious problem.

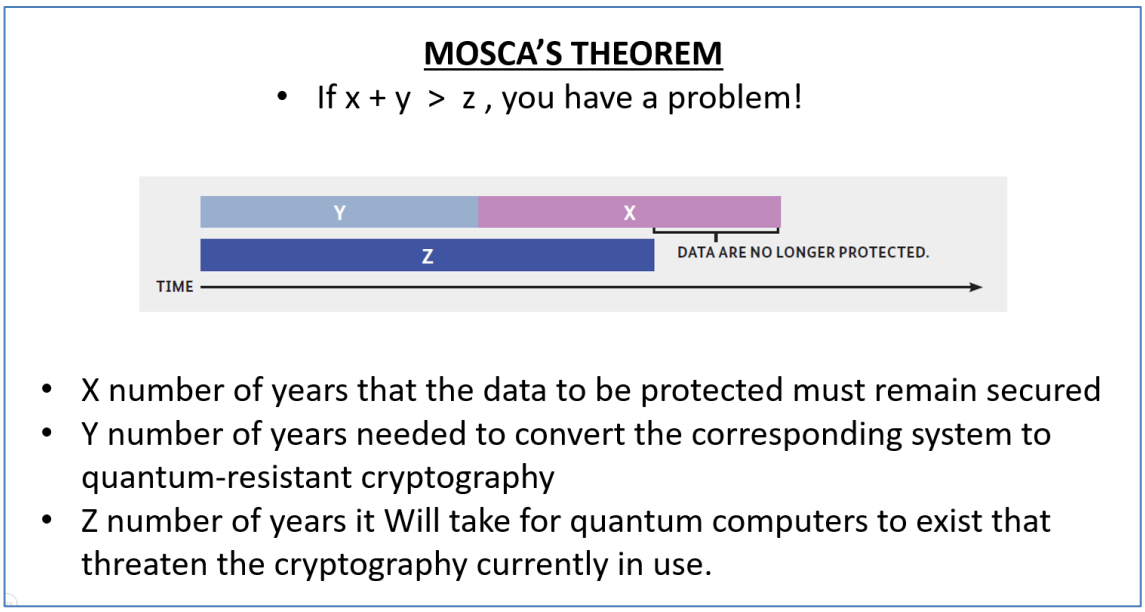


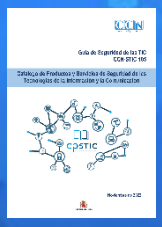
Figure 3. Graphic scheme of the Mosca's theorem

CCN-PyTec
centro criptológico nacional

The ICT Security Products and Technologies Department of the Centro Criptológico Nacional (CCN-PyTec) promotes the development, evaluation, certification and use of products to ensure the security of information and communication technology systems.

CPSTIC
CATÁLOGO DE PRODUCTOS Y SERVICIOS STIC

CATALOGUE OF ICT SECURITY PRODUCTS AND SERVICES



PDF

ONLINE

ccn-pytec@cni.es

@CCNPYTEC

CCN-PYTEC

www.ccn.cni.es **https://oc.ccn.cni.es** **www.ccn-cert.cni.es**