Volume XXVIII 2025
MBNA Publishing House Constanta 2025

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

A Quantum Resistant Authentication Survey

To cite this article: Rogobete Marius G., Oprina Carmen-Silvia, Cornaciu Veronica, Rogobete Mara, Scientific Bulletin of Naval Academy, Vol. XXVIII 2025, pg. 245-250.

Submitted: 29.04.2025
Revised: 25.07.2025
Accepted: 25.11.2025

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-25-I1-023

A Quantum Resistant Authentication Survey

Marius G. Rogobete[1,2], Carmen-Silvia Oprina[3], Veronica Cornaciu[2], Mara Rogobete[4]

[1]Harman International Romania
[2]Titu Maiorescu University
[3]Military Technical Academy of Romania
[4]Babes-Bolyai University
marius.rogobete@yahoo.com

Abstract. With the development of quantum computing, it will be relatively easy to brute force attack common symmetric (e.g. AES) and asymmetric algorithms (as RSA) to find the essential cryptographic information (cryptographic keys). In this context, there are two currently viable protection approaches, both of which aim to increase the processing complexity for this type of attack: (1) the use of classical algorithms, but with an increase in the size of the attached keys, and (2) approach using quantum-resistant cryptographic algorithms. In this paper, we will focus on analyse of the second case that is applicable on asymmetric authentication schemas. We analyse different methods in order to decide if different schematic purposes could increases the degree of cybersecurity in the context of quantum computing. Finally, a critical conclusion is presented regarding the analysed authentication methods.

1. Introduction

Quantum computing represents a tremendous improvement in computing power, which leads to special implications for cybersecurity and cryptography.

Compared to classical computers, which process information using Boolean algebra, quantum computers use quantum bits or qubits. The fact that these qubits can exist simultaneously in multiple states allows quantum computers to solve some complex problems much faster than classical computers.

This dramatic increase in computing power is certainly one of the great current challenges regarding the security of cryptographic algorithms used in encrypting/decrypting messages, including the security of digital communications.

A good example of quantum cryptography is quantum key distribution (QKD). QKD shares data between two entities in a secure, indestructible, and eavesdropping-proof manner.

QKD has a unique quality, namely that it allows communicating parties to detect any eavesdropping attempts. Due to properties of quantum mechanics - such as the no-cloning theorem - external observers cannot directly observe data transmitted over a QKD network. Any attempt introduces errors into the qubits, which immediately alert the communicating parties that the connection is not secure.

Furthermore, quantum cryptography is theoretically resistant to any increase in quantum computing power. In other words, computing power cannot violate the laws of physics, so quantum cryptography is protected by the very laws of its nature.

However, the most important nations apply a strategy known as “harvest now, decrypt later,” in which they collect and store, when they have access to it, vast amounts of encrypted data, anticipating future advances in quantum computing that will allow them to decrypt the information.

2. State-of-the-art

2.1. Symmetric algorithms

As the most used symmetric algorithm, we have just to remember that AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys.

NSA (National Security Agency) describes the design and strength of all key lengths (i.e., 128, 192 and 256) of the AES algorithm are protect classified information up to the SECRET level. For TOP SECRET information level is required to use of either the 192 or 256 key lengths.

In [1] NIST (National Institute of Standards and Technology) highlighted that Grover's quantum algorithm (designed to search for keys by brute force using a quadratic number of steps fewer than would be required in a classical implementation) offers no significant advantage in attacking AES, and, moreover, the difficulty of parallelizing Grover's quantum algorithm shows that AES 256 will continue to be secure for a very long time.

Although there are symmetric PQC systems in development, post-quantum cryptography (PQC) systems are primarily asymmetric (public key). The tendency for asymmetric systems to be PQC is due to the fact that symmetric cryptography is apparently resistant to quantum computers, at least for the foreseeable future.

2.2. Asymmetric algorithms

ML-KEM

Based on the 2024 NIST standardization, the ML-KEM (formerly CRYSTALS-Kyber) [2] key encapsulation mechanism and the ML-DSA (formerly CRYSTALS-Dilithium) [3] signature algorithm are approved as quantum-resistant algorithms. They should be used instead of the common public-key algorithms RSA and ECC, even if RSA-4096 is considered quantum-resistant at least until 2050.

ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) is a KEM in because it creates a pair (decapsulation key, encapsulation key), such that any entity can use the encapsulation key to share a secret key with the holder of the decapsulation key.

Conform NIST [5], KEM is a key-encapsulation mechanism based on several algorithms that can be used by two parties during a handshake process to establish a shared secret key over a public channel. This secret key can be used by symmetric-key cryptographic algorithms, for encryption and authentication. ML-KEM is a standard that specifies a key-encapsulation mechanism. The security of ML-KEM is related “to the computational difficulty of the Module Learning with Errors problem. At present, ML-KEM is believed to be secure, even against adversaries who possess a quantum computer. This standard specifies three parameter sets for ML-KEM. In order of increasing security strength and decreasing performance, these are ML-KEM-512, ML-KEM-768, and ML-KEM-1024.”

There are three algorithms [5] of KEM schematic: key generation probabilistic, algorithm (KeyGen), ”encapsulation” probabilistic algorithm (Encaps) and ”decapsulation” probabilistic algorithm (Decaps).

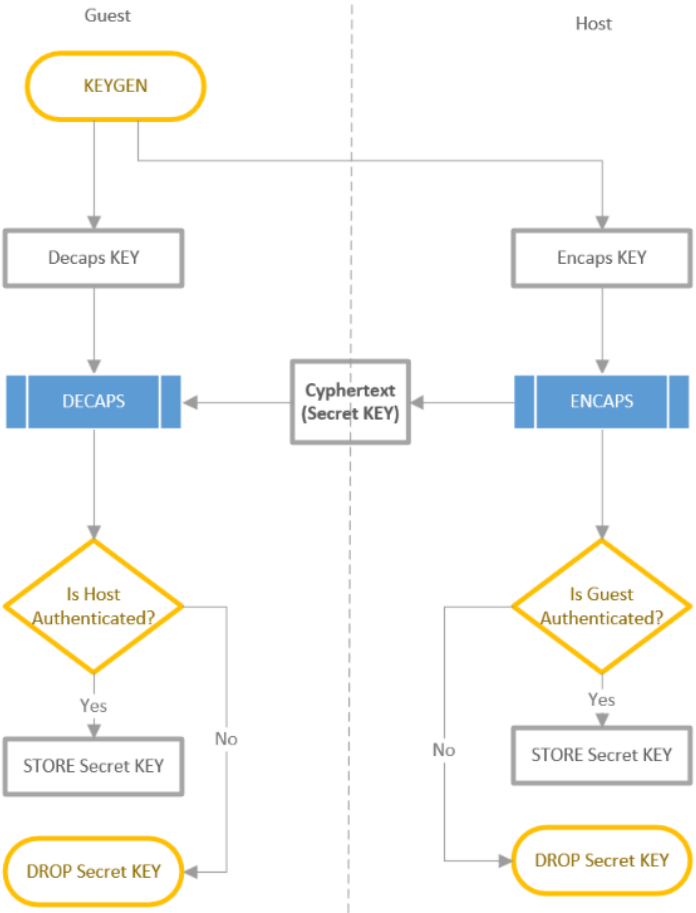

Figure 1 – Key establishment using KEM

ML-DSA

Module-Lattice-Based Digital Signature Standard (ML-DSA) is designed to protect digital signatures used when signing messages/data and is based on CRYSTALS-Dilithium. Other important signature algorithm is SLH-DSA (and in future FN-DSA), standardised in FIPS-204.

As security properties, ML-DSA is designed as a SUF-CMA (strongly existentially unforgeable under chosen message attack) algorithm. ML-DSA has relatively fast key operations, medium-sized keys (1312- 2592 bytes verification key, 2528-4864 bytes signing key) and medium-sized signatures (2420-4595 bytes).

The ML-DSA (Module-Lattice-Based Digital Signature Standard) Dilithium signature scheme is consisting of next main algorithms: Key Generation (KeyGen) that produces a pair of keys (a public key and a private key) and Signature Generation (Sign) that uses the private key to generate a signature for a given message.

ML-DSA is a Schnorr signature algorithm but with some optimizations. Module-Lattice-Based Digital Signature Standard and similar lattice signature schemes are based on the construction of a signature scheme from an analogous interactive protocol in which a verifier who knows the matrix $\mathbf{A} \in \mathbb{Z}_q^{K\times L}$, $\mathbf{S_1} \in \mathbb{Z}_q^{L\times n}$ and $\mathbf{S_2} \in \mathbb{Z}_q^{L\times n}$ $m2 \in \mathbb{Z}K\times n$ q with small coefficients (for $\mathbf{S_1}$ and $\mathbf{S_2}$) demonstrates knowledge of these matrices to a verifier who knows $\mathbf{A}$ and $\mathbf{T} \in \mathbb{Z}_q^{K\times L} = \mathbf{AS_1} + \mathbf{S_2}$ [6].

Table 1. Schnorr vs. ML-DSA

Schnorr	Module-Lattice-Based Digital Signature Standard
Schnorr signature scheme is applying the Fiat-Shamir heuristic to an interactive protocol between a verifier who knows g - the generator of a group in which discrete "logs" are believed to be difficult - and the value $y=g^x$ and a prover who knows g and x [6]. These interactive protocol, where the prover demonstrates knowledge of x to the verifier, consists of three steps: Commitment, Challenge and Response [6]	This protocol is transformed into a non-interactive one by a signature scheme that replaces the random choice of c by the verifier in step 2 with a deterministic process that derives pseudo-random c from a digest of the commitment g^r concatenated with the message to be signed. In this scheme, x is the private key and y is the public key with which the signature is verified [6].
1. *Commitment*: The prover generates a random positive integer r that is less than the order of g and commits to its value by sending g^r to the verifier [6]	1. *Commitment*: The prover generates $\mathbf{y} \in \mathbb{Z}_q^L$ with small coefficients and commits to its value by sending $\mathbf{w}_{\text{Approx}} = \mathbf{Ay} + \mathbf{y}_2$ to the verifier, where $\mathbf{y_2} \in \mathbb{Z}_q^n$ is a vector with small coefficients.[6]
2. *Challenge*: The verifier sends a random positive integer c that is less than the order of g to the prover [6]	2. *Challenge*: The verifier sends a vector $\mathbf{c} \in \mathbb{Z}_q^n$ with small coefficients to the prover [6].
3. *Response*: The prover returns $s = r - cx$ reduced modulo the order of g, and the verifier checks whether $g^s \cdot y^c = g^r$ [6].	3. *Response*: The prover returns $\mathbf{z} = \mathbf{y} + \mathbf{S}_1\mathbf{c}$, and the verifier checks that $\mathbf{z}$ has small coefficients and that $\mathbf{Az} - \mathbf{Tc} \approx \mathbf{w}_{\text{Approx}}$ [6].

3. Public Key Certificate Algorithms

3.1. PKC algorithms for digital signatures

Dilithium is a digital signature scheme that is strongly secure under chosen message attacks based on the hardness of lattice problems over module lattices [3].

As Dilithium is an important candidate algorithm for NIST post-quantum cryptography project [3], it's versions are benchmarked against some Public Key Certificate algorithms for digital signatures and signature verification [4].

PKC Algorithm to sign	Certificate	Public key	Private key	Digital sign
RSA 1024	~522	128	128	128
RSA 2048	~785	256	256	256
RSA 4096	~1298	512	512	512
SECP384r1	~455	96	48	103
SECP521r1	~529	132	65	139
PQC - Dilithium1	~2575	896	2096	1387
PQC - Dilithium3	~4465	1472	3504	2701

The RSA standard algorithm and Diffie-Hellman keys are 2048-bit that is roughly estimated that one million qubits would be needed to break this. However, as the industry is generally migrating to 4096-bit keys, the estimation is of ~1.3 billion qubits.

3.2. PKC algorithms for key-exchange/key-encapsulation

Some main characteristics of Public Key Certificate algorithms for key exchange (server key and client key) exchange [2] are presented in next table.

PKC Algorithm for key exchange	**Public key**	**Private key**	**Ciphertext/Key ID**
ECDHE – x25519	32	32	–
ECDHE – SECP256r1	64	32	–
ECDHE – SECP384r1	96	48	–
ECDHE – SECP521r1	132	65	–
PQC - Kyber512	800	1632	736
PQC - Kyber768	1184	2400	1088
QKD	–	–	36

Where:

- ECDHE = Elliptic-curve Diffie–Hellman
- SECP256r1 = "Standards for Efficient Cryptography," "P" represents the prime field, "256" signifies the bit length of the prime field, and "r1" indicates that it is the first curve of its kind recommended by SECG
- PQC - Kyber = Post-Quantum Cryptography - CRYSTALS-Kyber
- QKD = Quantum Key Distribution

4. Conclusion

Analysing quantum and postquantum cryptographic methods, it can be distinguished three different but complementary approaches: QKD experimentation, PQC signature method, and PQC for key exchange (PKC for key exchange) in secure communications.

Experimentally the Quantum Key Distribution was successfully demonstrated, including the integration of QKD into 5G architecture.

Regarding the PKC for digital signatures, which has made significant progress by optimizing the Crystals-Dilithium implementation, it has significantly reduced memory usage, while maintaining compliance with the FIPS 204 standard, which is constantly evolving. Future developments will need to produce a highly secure and reliable solution that is certified according to Common Criteria. The NIST PQC standardization process represents a challenge to be taken into account for any implementation and integration of the solution in critical applications such as secure identity management or corporate security infrastructures.

Finally, PKC for key exchange lays the foundation for a robust cryptographic solution, already tested and optimized in various commercial environments, e.g. 5G.

The three approaches - QKD, PKC for digital signatures and PKC for key exchange - represent an irreducible framework to protect communication systems against current and especially future threats, which also include quantum computing. This system paves the way for a secure communication infrastructure, especially resistant to quantum threats that will emerge in the next years.

References

1. Alagic G, Bros M, Ciadoux P, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu YK, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Silberg H, Smith-Tone D, Waller N (2025) Status Report on the Fourth Round of the NIST Post-Quantum Cryptography

Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8545. https://doi.org/10.6028/NIST.IR.8545
2. Cheng, Song, Chen, Jiansheng, Li, Jianyang, Yao, Kan, Gao, Shunxian, Rui, Kangkang, Cui, Yijun, Optimized Design and Implementation of CRYSTALS-KYBER Based on MLWE, Security and Communication Networks, 2025, 7884158, 15 pages, 2025. https://doi.org/10.1155/sec/7884158
3. Alagic G, Bros M, Ciadoux P, Cooper D, Dang Q, Dang T, Kelsey J, Lichtinger J, Liu YK, Miller C, Moody D, Peralta R, Perlner R, Robinson A, Silberg H, Smith-Tone D, Waller N (2025) Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST IR 8545. https://doi.org/10.6028/NIST.IR.8545
4. Bai S., Ducas L., Kiltz E., Lepoint T., Lyubashevsky V., Schwabe P., Seiler G., Stehlé D., Crystals-Dilithium (2023), https://pq-crystals.org/dilithium/index.shtml
5. National Institute of Standards and Technology (2024) Module-Lattice-Based KeyEncapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://doi.org/10.6028/NIST.FIPS.203
6. 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://doi.org/10.6028/NIST.FIPS.204