Post-Quantum Cryptography Performance – Overview Comparison of Lattice-Based Algorithms and Potential Concerns

Marijana Jeremić[1], Tijana Dimitrijević[2], Vladimir Vuković[3], Milan Čabarkapa[1]

***Abstract* — The rise of quantum computers threatens classical cryptosystems through Shor's and Grover's algorithms. Post-quantum cryptography (PQC) addresses this challenge, with lattice-based schemes emerging as leading candidates. This paper presents an overview in this emerging field with main focus on Kyber method for key exchange and Dilithium method for digital signatures. It has been shown why these methods are good candidates for the future implementation in real-world protocols. However, the paper also presents concerns regarding different types of applications of such a methodology, especially because of the attacks in constrained environments.**

***Keywords* — Cryptosystems, Post-quantum cryptography, Key exchange, Digital signature**

I. Introduction

The development of quantum computers represents one of the most significant technological breakthroughs in modern informatics and computing. Unlike classical computers, which use bits to represent information, quantum computers use quantum bits (qubits) that can exist in a superposition of states, allowing them to perform a vast number of operations in parallel. This property makes quantum computers extremely powerful for solving certain classes of mathematical problems that are practically unsolvable for classical computers within a reasonable time frame. However, this very power of quantum computing poses a serious threat to existing cryptographic systems. Algorithms such as RSA (based on the factorization of large numbers) and ECC (based on the discrete logarithm problem of elliptic curves) form the foundation of today's digital security, from SSL/TLS protocols and email communication to banking transactions and digital signatures [1]. Quantum algorithms, such as Shor's algorithm, can efficiently factor large integers and compute discrete logarithms, effectively breaking RSA and ECC encryption schemes, while Grover's algorithm significantly reduces the complexity of key search in symmetric schemes, thereby fundamentally undermining trust in the current security infrastructure. This scenario has led to the emergence of a new field known as post-quantum cryptography (PQC). The goal of PQC is not to replace cryptographic protocols but to evolve them, to design algorithms that will remain secure even in the presence of quantum computers. Cryptosystems based on lattice problems play a particularly important role in this process, as their security relies on mathematical tasks for which no efficient quantum algorithms are currently known. Among them, Kyber, an algorithm designed for secure key exchange (Key Encapsulation Mechanism – KEM), and Dilithium, an algorithm for digital signatures, stand out. Both schemes have been recommended by the National Institute of Standards and Technology (NIST) and are included in the standardization process as future global standards (FIPS 203 and FIPS 204). Their importance lies not only in their mathematical resilience but also in their practical applicability; they can be integrated into existing network protocols, such as TLS 1.3, with minimal infrastructure changes. Despite the advantages they offer, the implementation of these algorithms also brings certain challenges. Larger key and signature sizes, increased resource consumption, and the complexity of certification processes represent real obstacles to widespread adoption. Resource-constrained environments, such as IoT systems, where memory, processing power, and bandwidth are significantly limited, are particularly challenging. For this reason, the development of hybrid systems that combine classical and post-quantum algorithms is becoming a crucial step during the transition period.

This paper aims to provide an overview of post-quantum cryptography, with a particular focus on the lattice-based algorithms Kyber and Dilithium, analyzing their performance, integration into modern network protocols, and highlight potential challenges and limitations in real-world applications.

II. Fundamentals of Post-Quantum Cryptography

A. The Need for Post-Quantum Cryptography

Modern cryptographic systems such as RSA, Diffie–Hellman, and ECC base their security on mathematical problems that are extremely difficult for classical computers to solve (e.g., integer factorization, discrete logarithms, etc.). However, the development of quantum computers changes this security paradigm. Quantum algorithms like Shor's algorithm can solve these problems exponentially faster, directly

[1]Marijana Jeremić and Milan Čabarkapa are with the Faculty of Engineering, University of Kragujevac (corresponding email: mcabarkapa@uni.kg.ac.rs)

[2]Tijana Ž. Dimitrijević is with University of Niš, Faculty of Electronic Engineering, Aleksandra Medvedeva 4, 18000 Niš, Serbia, and University of Kragujevac, Faculty of Engineering, Sestre Janjić 6, 34000 Kragujevac, Serbia (e-mail: tijana.dimitrijevic@elfak.ni.ac.rs).

[3]Vladimir Vuković is with the Faculty of Diplomacy and Security, Belgrade, Travnička 2, 11000 Belgrade, Serbia (e-mail: vladimir.vukovic@fdb.edu.rs).

threatening the security of most current cryptosystems [2]. Additionally, Grover's algorithm accelerates key search in symmetric algorithms, effectively halving their security level. For this reason, it is necessary to develop new cryptographic methods that will remain secure even in the presence of quantum computers. Post-quantum cryptography (PQC) represents this new generation of algorithms, whose security is based on mathematical problems for which no efficient quantum algorithms are currently known. PQC algorithms are designed to be implementable on classical hardware and easily integrated into existing network protocols without the need for specialized quantum devices.

B. Main Mathematical Foundations of PQC Algorithms

Post-quantum algorithms based on lattice cryptography derive their security from mathematical problems that are extremely difficult for both classical and quantum computers to solve. The most important among them are LWE (Learning With Errors), which is based on solving systems of linear equations with random errors, and SIS (Short Integer Solution), which requires finding a short vector that satisfies certain modular conditions. Their optimized variants, such as Ring-LWE, leverage algebraic structures to reduce key sizes and improve implementation efficiency. The complexity of these problems is mathematically related to well-known lattice challenges such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), for which no efficient quantum algorithms currently exist. As a result, they provide a reliable foundation for building post-quantum cryptosystems and guarantee a high level of security even in a quantum environment.

C. NIST Standards and Current State of PQC Algorithms

Given the growing need for quantum-resistant solutions, the National Institute of Standards and Technology (NIST) launched a multi-phase process for the standardization of PQC algorithms in 2016. After five years of evaluation and more than 80 submitted candidates, NIST announced the first generation of official post-quantum cryptography standards in 2024. These include three main algorithms: FIPS 203(ML-KEM-Kyber) - a key exchange algorithm based on the Module-LWE problem [3]. It combines high security, efficiency, and relatively low overhead, making it suitable for a wide range of applications, including TLS, VPN, and secure communication protocols. FIPS 204 (ML-DSA/Dilithium) - a digital signature algorithm based on the Module-LWE and SIS problems. Its simple and deterministic structure enables easy implementation and high verification speed. Although its signatures are larger than those of ECDSA, its security and resistance to quantum attacks significantly surpass classical solutions. FIPS 205 (SLH-DSA/SPHINCS+) - a hash-based signature algorithm, intended as an alternative solution in scenarios requiring additional security or diversity. Although slower than Dilithium, it offers a different security foundation and provides an additional layer of protection. These standards represent a milestone in the history of cryptography, enabling a gradual and planned transition from classical algorithms to quantum-resistant schemes. Their widespread adoption is already being planned in security protocols such as TLS 1.3, IPsec, SSH, as well as in systems for digital signatures, electronic voting, and critical infrastructure protection [4].

III. LATTICE-BASED ALGORITHMS

Lattice-based cryptosystems represent the most promising group of algorithms in the field of post-quantum cryptography, with their security relying on mathematical problems that remain unsolvable even with quantum computers. Among these algorithms, Kyber and Dilithium stand out as they have been recommended by NIST as part of the first generation of post-quantum standards.

A. Kyber (ML-KEM)

Kyber is a lattice-based Key Encapsulation Mechanism (KEM) whose security is based on the Module-LWE problem. The main idea is that two parties can securely exchange a secret key over an insecure channel, while an attacker cannot reconstruct the key even with access to all public information. Advantages of Kyber: High security: Resistant to all known quantum attacks due to the mathematical complexity of the LWE problem. Efficiency: Significantly faster encapsulation and decapsulation compared to RSA and ECDH, making it suitable for real-time applications. Practical integration: Kyber can be easily integrated into network protocols such as TLS 1.3, SSH, and VPN without requiring major infrastructure changes. Limitations of Kyber: Key size: Public and private keys are larger than those of classical algorithms, increasing memory and bandwidth requirements. Impact on network performance: In resource-constrained environments (e.g., IoT), larger keys can significantly affect performance [5].

B. Dilithium (ML-DSA)

Dilithium is a digital signature algorithm based on the Module-LWE and SIS problems. Its primary function is to verify the authenticity and integrity of messages, and the signing process itself is deterministic and straightforward to implement. Advantages of Dilithium: Simple implementation: Designed for easy deployment and optimized for modern processors. High security: Resistant to known quantum attacks with provable security based on hard mathematical problems. Fast verification: Signature verification is faster than many alternative PQC algorithms, making it ideal for large-scale systems. Limitations of Dilithium: Signature size: Signatures are larger compared to ECDSA, increasing certificate sizes and requiring higher network bandwidth. Regulatory and legal challenges: Signatures are not yet fully recognized under current legal frameworks (e.g., eIDAS), limiting their use in official systems [6].

C. Comparison of Kyber and Dilithium Algorithms

Although both Kyber and Dilithium are based on similar mathematical principles, primarily the Module-LWE problem, with Dilithium also leveraging SIS, their purpose, structure, and performance differ in several key aspects. Kyber is designed for key exchange (KEM) and is primarily used during the establishment of secure communication between two parties. Its main operations are encapsulation and decapsulation of the secret key, with public and private keys ranging from approximately 800 bytes to 1.5 KB, which is

significantly larger than classical methods like ECDH. Kyber's main advantage lies in its exceptional speed and resistance to quantum attacks, making it widely used in network protocols such as TLS, SSH, IPsec, and VPN solutions. However, the larger key sizes and increased memory requirements can pose challenges in resource-limited environments such as IoT devices. On the other hand, Dilithium is designed for digital signing and message verification (DSA). Its main operations are signing and verification, with key sizes ranging from about 1.5 to 2.5 KB, while the signatures themselves are significantly larger than those produced by classical algorithms, typically around 2.5 to 3 KB. This increase impacts overall certificate size and can be problematic in systems with limited bandwidth. Nevertheless, Dilithium features deterministic signatures and high verification speeds, making it suitable for applications with a high transaction volume, such as blockchain systems, digital certificates, e-government, and electronic voting systems. From a performance standpoint, Kyber excels in key exchange speed and real-time efficiency, while Dilithium offers highly reliable and fast signature verification, which is critical for large-scale and distributed systems. While Kyber provides the foundation for secure communication, Dilithium ensures trust and data integrity. Ultimately, their combined use offers a complementary solution: Kyber secures the establishment of communication and shared secret keys, while Dilithium enables authentication and protection against data manipulation. This synergy makes them fundamental components of modern and future post-quantum security architectures [7].

IV. Integration of PQC Into Network Protocols -The TLS Case

Modern digital society relies heavily on network protocols that ensure the confidentiality, integrity, and authenticity of communications. Among them, Transport Layer Security (TLS) plays a central role, as it forms the foundation of secure data exchange over the internet, from HTTPS traffic to email protection and VPN connections. However, the advent of quantum computers changes the security paradigm: encryption schemes that were unbreakable for decades can now be compromised in real time. For this reason, integrating post-quantum algorithms into the TLS 1.3 protocol is a crucial step toward ensuring the future resilience of information systems.

A. PQC in TLS Architecture

TLS 1.3 operates through a series of phases, the most critical of which is the initial handshake, where algorithms are negotiated, keys are exchanged, and a secure channel is established. It is precisely in this phase that post-quantum algorithms come into play. Kyber, as a Key Encapsulation Mechanism (KEM), is used for the secure distribution of a symmetric key between the client and the server. Its role is to ensure that even if an attacker eavesdrops on the communication, they cannot reconstruct the key due to the complexity of the Module-LWE problem. Dilithium, on the other hand, is used for digital signatures and authentication of both the server and the client. It guarantees that the communication partner is who they claim to be and that the message content has not been tampered with during transmission. Such integration of PQC algorithms into the handshake phase does not require radical changes to existing TLS implementations. Most current libraries can be extended with new algorithms with minimal modifications, which simplifies the transition from classical to post-quantum schemes [8].

B. Hybrid Schemes as a Transitional Solution

Although PQC algorithms promise strong resistance against quantum attacks, industrial practice shows that the best approach is often a hybrid strategy that combines classical and post-quantum algorithms. In such systems, security does not rely solely on one technology. For example, if a future vulnerability were discovered in the Kyber algorithm, the classical ECDH mechanism would still provide a baseline level of protection. Similarly, combining Dilithium signatures with ECDSA provides redundancy in authentication. This strategy reduces risk and enables organizations to gradually deploy PQC into their systems without service interruptions or significant migration costs.

C. Experiments and Performance Analysis

Major technology companies like Google and Cloudflare have already conducted experimental implementations of TLS protocols using PQC algorithms. The results show that introducing Kyber and Dilithium does not significantly increase latency, the time required to establish a secure connection remains almost unchanged compared to classical algorithms. The only noticeable effect occurs with very large certificates (over 40 KB), where a slight increase in latency is observed due to the transmission of additional data. However, even in these cases, the overall latency remains within acceptable limits for most network applications.

D. Optimization Techniques

To further improve performance and reduce overhead, innovative techniques such as KEMTLS and Merkle Tree Certificates (MTC) have been developed: KEMTLS eliminates the need for digital signatures in certain stages of the connection setup, thereby reducing the number of exchanged messages and the total handshake time. Merkle Tree Certificates, on the other hand, compress the certificate structure using Merkle trees, significantly reducing the amount of data transmitted and speeding up connection establishment [9]. NTRU Prime represents a secure, simple, and independent family of lattice-based cryptosystems that strengthens the theoretical foundations of post-quantum cryptography, offers an efficient and auditable implementation for practical use, and provides crucial algorithmic diversity to safeguard the future of Internet cryptography beyond Kyber [10]. In Table 1, we present comparisons of three main optimization techniques from different aspects. According to OQS and pqm4 benchmarking, Kyber-512 (1184 / 1088), NTRU Prime 761 (1047 / 1039), and FrodoKEM-640 (9616 / 9720) show respective key and ciphertext sizes, with computation speeds of 3-5 ms on x86 (200–300 ms on Cortex-M4), 6-8 ms for NTRU Prime, and 40–60 ms for FrodoKEM; Kyber-512 requires about 20 kB RAM during encapsulation [11],[12].

E. Compatibility and Transition

One of the key challenges in deploying PQC algorithms is compatibility with existing network systems and protocols. The solution comes in the form of hybrid TLS packages, which allow both classical and post-quantum algorithms to be used within the same protocol. This ensures that older clients and servers that do not support PQC can still communicate, while newer systems can benefit from quantum-resistant protection. This approach is particularly important in critical sectors such as finance, cloud platforms, healthcare information systems, and other environments where continuous service availability is essential. However, the integration of PQC algorithms introduces practical constraints, particularly in resource-limited environments such as IoT and embedded systems. For instance, the maximum IEEE 802.15.4 frame size is only 127 bytes, including both header and payload, while the public and private keys in algorithms such as Kyber and Dilithium range from several hundred bytes to over 3 kilobytes.

V. Conclusion

Post-quantum cryptography is no longer a theoretical concept, it is now a practical necessity. As the era of quantum computing approaches, traditional cryptosystems like RSA and ECC are losing their long-term reliability. Algorithms such as Kyber and Dilithium offer solutions that combine strong security, proven resistance, and practical applicability, making them the cornerstone of the future digital infrastructure. However, the path to full PQC implementation is not without challenges. These include performance optimization, reducing key and signature sizes, legal and regulatory alignment, and the development of new standards. Future research must focus on developing efficient hybrid schemes, improving implementation security, and ensuring timely certification of algorithms. Despite these challenges, it is clear that post-quantum cryptography will become a pillar of digital security in the 21st century, and its deployment must begin now to ensure that data remains secure in a future where quantum computers become a reality.

ACKNOWLEDGMENT

This research was supported by the Ministry of Education, Science and Technological Development of Republic of Serbia (Grant number 451-03-137/2025-03/ 200102).

References

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annu. Symp. Foundations of Computer Science (FOCS), IEEE, 1994, pp. 124–134.
[2] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM J. Comput., vol. 26, no. 5, pp. 1484–1509, 1997.
[3] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Project," 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
[4] D. J. Bernstein *et al.*, "SPHINCS+ Signature Scheme, Version 3.1," 2024. [Online]. Available: https://sphincs.org/data/sphincs+-r3.1-specification.pdf
[5] Cloudflare, "The Post-Quantum Internet: 2024 Update," Cloudflare Blog, 2024. [Online]. Available: https://blog.cloudflare.com/pq-2024/
[6] D. J. Bernstein, T. Lange, and M. Niederhagen, "Kyber: Algorithm Specifications and Supporting Documentation," IACR Cryptology ePrint Arch., Rep. 2023/1891, 2023.
[7] J. Bos et al., "CRYSTALS – Kyber: A CCA-Secure Module-Lattice-Based KEM," IACR Cryptology ePrint Arch., Rep. 2016/1017, 2016.
[8] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF RFC 8446, Aug. 2018.
[9] M. Alkim, J. Bos, L. Ducas, T. Lepoint, P. Schanck, D. Schwabe, G. Seiler, and D. Stebila, "FrodoKEM: Learning With Errors Key Encapsulation," IACR Cryptology ePrint Arch., Rep. 2020/534, 2020.
[10] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, "NTRU Prime: Reducing Attack Surface at Low Cost," IACR Cryptology ePrint Arch., Rep. 2017/634, 2017.
[11] Open Quantum Safe Project, "OQS Benchmarking Results." [Online]. Available: https://openquantumsafe.org/benchmarking/
[12] ETH Zürich, "pqm4: Post-Quantum Cryptography on the ARM Cortex-M4," GitHub Repository. [Online]. Available: https://github.com/mupq/pqm4

TABLE I
COMPARISONS OF MAIN OPTIMIZATION TECHNIQUES

Aspect	CRYSTALS-Kyber	NTRU Prime	FrodoKEM
Mathematical Basis	Module-LWE (Learning With Errors)	NTRU-like lattice, prime modulus	Plain LWE (no structure)
Design Goal	High efficiency with strong theoretical security	Simplicity, resistance to algebraic/subring attacks	Conservative design with minimal structure
Ring / Structure	Structured lattice (polynomial ring)	Irreducible polynomial ring, minimal symmetry	Unstructured matrix lattice
Key Size (approx., bytes)	800–1500	900–1200	9,600–12,000
Ciphertext Size (approx., bytes)	700–1500	900–1200	9,000–12,000
Computation Speed	Very fast (optimized NTT transforms)	Moderate (uses convolution, no NTT)	Slow (large matrices, no structure)
Memory Requirements	Low	Moderate	High
Side-Channel Resistance	Actively researched; masked implementations available	Designed to be simple and constant-time	Easier to harden due to no structure
Algorithmic Diversity	Similar structure to Saber and Dilithium	Distinct design, independent security basis	Independent (different LWE family)
Implementation Complexity	Moderate (requires NTT & modular reduction)	Simple and auditable (no complex transforms)	High (large matrix operations)
Best Use Cases	TLS, VPNs, general Internet encryption	IoT, embedded systems, hybrid PQ TLS	High-security applications, hardware with ample resources
Representative Implementations	Open Quantum Safe (OQS), Cloudflare PQ-TLS, OpenSSL 3.x	Cloudflare PQ testbed, OQS, pqm4 (ARM Cortex-M4)	IBM, Microsoft Research, OQS
Key Advantage	Balance of efficiency and security	Clean structure, resistance to subring attacks	Strong conservative design, simplest assumptions
Main Trade-off	Uses structured lattice — possible future risk	Slightly slower, larger key than Kyber	Very large size, slower performance