Comparative Analysis of the Performance of RSA, ECDSA, and CRYSTALS-Dilithium Digital Signature Algorithms in the Post-Quantum Era

Tovma Oleh Mykolayovych[1]
[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, oleksandr.tovma@nure.ua

Balagura Dmytro Serhiiovych[2]
[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, dmytro.balahura@nure.ua

Abstract. *The development of quantum computing poses unprecedented challenges to modern cryptographic infrastructures, as Shor's algorithm can efficiently solve integer factorization and discrete logarithm problems underlying RSA and ECDSA. This paper presents a comparative performance analysis of three key digital signature algorithms - RSA, ECDSA, and CRYSTALS-Dilithium - in the context of transitioning to post-quantum cryptography. The study evaluates the time required for key generation, signature creation, and signature verification. Results demonstrate that the Dilithium algorithm, standardized by NIST in 2022, provides high computational efficiency and strong resistance to quantum attacks, making it suitable for practical implementation in future secure systems.*

Keywords: *Digital signature; RSA; ECDSA; Dilithium; post-quantum cryptography; performance; NIST PQC*

I. Introduction and Problem statement

Modern digital infrastructure critically depends on digital signature algorithms that ensure authentication, data integrity, and non-repudiation. However, the advent of quantum computing poses a serious threat to classical schemes such as RSA and ECDSA due to their vulnerability to Shor's algorithm [1]. In response, the U.S. National Institute of Standards and Technology (NIST) initiated the Post-Quantum Cryptography Standardization Process in 2016 [2], which culminated in 2022 with the selection of CRYSTALS-Dilithium as the primary post-quantum digital signature standard. The aim of this work is to evaluate the performance of RSA, ECDSA, and Dilithium to determine their suitability for practical application [3].

The transition to post-quantum digital signature algorithms is critically important due to the rapid advancement of quantum processors capable of executing operations on hundreds or even thousands of qubits. Such progress introduces a significant threat to the long-term confidentiality and integrity of data protected by classical cryptographic primitives. Given these developments, one of the key research objectives is not only to assess the cryptographic robustness of emerging post-quantum schemes but also to evaluate their computational efficiency and implementation overhead when integrated into existing security protocols such as TLS, VPN, and PKI.

The study presented in this paper provides a comprehensive comparative analysis of the performance of classical and lattice-based digital signature algorithms, enabling the identification of optimal parameter sets for practical deployment within post-quantum information systems. Particular emphasis is placed on balancing security assurance and operational efficiency, which is crucial for the scalability of next-generation secure communication infrastructures.

Modern information systems including financial, governmental, and defense networks already face an urgent need to adopt algorithms that are resistant to quantum attacks. Therefore, the comparative evaluation of classical and post-quantum digital signature schemes holds both theoretical and applied significance. Furthermore, performance benchmarking facilitates the estimation of computational and communication overheads associated with the migration toward quantum-resistant public key infrastructures.

II. Problem solution and Results

This study examines several digital signature algorithms. RSA (FIPS 186-4) is based on the computational hardness of large integer factorization [1]. Although secure, its performance degrades with increasing key size. ECDSA (NIST SP 800-186) relies on the elliptic curve discrete logarithm problem, offering smaller key sizes and higher efficiency but lacking quantum resistance [1]. CRYSTALS-Dilithium is based on lattice cryptography and the Module Learning With Errors (M-LWE) problem, providing security against both classical and quantum attacks [2, 4].

The experimental implementation was carried out in Java using the Bouncy Castle cryptographic library. During the study, the time required for key generation, signing, and verification was measured for each algorithm [3]. Testing was performed on a MacBook Air M2 (2022) with 16 GB of RAM. Performance was evaluated under the following parameters:

– RSA: key sizes of 2048, 3072, and 4096 bits;

– ECDSA: curves secp256r1, secp384r1, and secp521r1;

– Dilithium: levels 2, 3, and 5 (corresponding to key sizes of 256, 384, and 512 bits) [3, 5].

To ensure the reproducibility of the results, each experiment was repeated at least ten times, and the average execution time for each operation was calculated. In addition, the sizes of the generated keys and signatures were evaluated, as these parameters are critically important for implementations in embedded systems and network protocols with limited bandwidth. The experimental results indicated that the RSA algorithm requires significantly more time for key generation compared to ECDSA and Dilithium, whereas the latter demonstrates the most favorable trade-off between computational performance and security level.

The obtained results (Table 1) reflect the time required for key generation, signature creation, and verification across all algorithms. Testing under various key sizes and security levels enables objective assessment of RSA, ECDSA, and CRYSTALS-Dilithium efficiency under different conditions [3, 4].

Table 1. Comparison of Signature Algorithms

Algorithm	Key size (bits)	Key generation (ms)	Signing (ms)	Verification (ms)
RSA-2048	2048	142.98	3.25	0.12
RSA-3072	3072	343.99	7.54	0.17
RSA-4096	4096	909.03	7.77	0.19
ECDSA-secp256r1	256	26.76	1.56	3.67
ECDSA-secp384r1	384	5.16	3.71	2.43
ECDSA-secp521r1	521	6.53	6.29	4.51
Dilithium-2	256	12.81	9.53	1.90
Dilithium-3	384	2.70	7.53	1.21
Dilithium-5	512	1.79	6.97	1.88

Analyzing the data presented in the table, it can be concluded that ECDSA demonstrates the lowest signing time for smaller key sizes; however, its signature verification is slower compared to RSA. The Dilithium algorithm exhibits more balanced performance, providing both fast signature generation and verification while maintaining a significantly higher level of cryptographic security. These characteristics make Dilithium a promising candidate for deployment in cloud environments, mobile devices, and IoT systems.

III. CONCLUSIONS

The results of the study indicate that RSA and ECDSA remain efficient in classical computing environments; however, their cryptographic strength does not meet post-quantum security requirements due to their vulnerability to quantum attacks, particularly to Shor's algorithm [1]. In contrast, CRYSTALS-Dilithium, based on lattice cryptography, demonstrated an optimal balance between performance and quantum resistance [2],[4],[5]. The experimental results confirm its suitability for practical implementation in modern and next-generation information security systems. Therefore, the transition to post-quantum digital signature algorithms, primarily based on CRYSTALS-Dilithium, is technically justified and does not require significant trade-offs in computational efficiency [3],[5]. A gradual migration of cryptographic protocols should be implemented, considering industry-specific requirements, available computational resources, and organizational security priorities.

In future research, it is relevant to extend the analysis by including other algorithms recommended by NIST within the Post-Quantum Cryptography (PQC) standardization process, such as Falcon and SPHINCS+, in order to obtain a more comprehensive understanding of the performance characteristics across different classes of post-quantum digital signatures. Another promising direction is the evaluation of Dilithium integration into real-world network protocols (e.g., TLS 1.3, VPN, and SSH) and the investigation of its energy efficiency on embedded devices.

REFERENCES

[1] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee.

[2] Alagic, G., Bros, M., Ciadoux, P., Cooper, D., Dang, K., Dang, T., ... and Waller, N. (2025). *Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process.* U.S. Department of Commerce, National Institute of Standards and Technology.

[3] Dong, B., & Wang, Q. (2024). Evaluating Post-Quantum Cryptography on Embedded Systems: A Performance Analysis. arXiv preprint arXiv:2409.05298.

[4] Gupta, N., Jati, A., & Chattopadhyay, A. (жовтень 2023 р.). CRYSTALS-Dilithium на процесорі RISC-V: легке безпечне завантаження з використанням постквантового цифрового підпису. У 2023 IEEE/ACM International Conference on Computer Aided Design (ICCAD) (стор. 1-7). IEEE.

[5] Dziechciarz, D., & Niemiec, M. (2024). Efficiency analysis of NIST-standardized post-quantum cryptographic algorithms for digital signatures in various environments. Electronics, 14(1), 70.