Impact Factor: 9.9
ISSN-L: 2544-980X

PROSPECTS AND PRACTICAL SOLUTIONS OF POST-QUANTUM CRYPTOGRAPHY

Khusanova Mokhirakhon Kurbanaliyevna
Assistant Professor, Department of Software Engineering and Cybersecurity, Fergana State Technical University,
e-mail: mokhira.khusanova@gmail.com

Rakhmonov Ozodbek Shavkatjon ugli
Assistant Professor, Department of Software Engineering and Cybersecurity, Fergana State Technical University,
e-mail: antonanonovich326@gmail.com

Abstract: With the rapid advancement of information technologies, cybersecurity threats are increasing at an alarming rate. In particular, the emergence of quantum computers poses a serious risk to traditional cryptographic algorithms such as RSA, ECC, and DSA, which rely on mathematical problems that are difficult to solve using classical computing. However, these same problems can be efficiently solved on a quantum computer using Shor's algorithm, thus endangering the security of nearly all current public-key cryptosystems. In response, the concept of Post-Quantum Cryptography (PQC) is gaining global attention as a future-proof solution.

Keywords: Cryptography, Quantum Computers, Post-Quantum Cryptography, Information Security, Encryption, Algorithms

Introduction

The era of quantum computing is approaching rapidly, and it threatens to undermine the foundations of modern cryptography. Traditional encryption techniques that rely on hard mathematical problems, such as integer factorization and discrete logarithms, are vulnerable to quantum algorithms. Shor's algorithm, introduced in the mid-1990s, has shown that a sufficiently powerful quantum computer could efficiently break these cryptographic systems. Consequently, this creates an urgent need to develop and adopt cryptographic methods that are secure in a post-quantum world.

Post-Quantum Cryptography (PQC) refers to a class of cryptographic algorithms that are designed to be secure against both classical and quantum attacks. These algorithms are built upon mathematical problems that are believed to be hard even for quantum computers. Given the increasing investment in quantum computing by governments and private companies alike, transitioning to PQC is becoming a priority for nations and organizations seeking to secure sensitive information for the long term.

Methods

This study employs a qualitative research methodology centered on an extensive review of academic literature, institutional reports, and industrial implementation practices related to Post-Quantum Cryptography (PQC). The analysis integrates findings from a broad spectrum of sources, including peer-reviewed journal articles, cryptographic conference proceedings, white papers, and technical documentation published by global standards organizations. A key focus has been placed on evaluating the ongoing standardization process led by the U.S. National Institute of Standards and Technology (NIST), which has been at the forefront of defining PQC algorithms that are resistant to quantum-based attacks.

Impact Factor: 9.9 ISSN-L: 2544-980X

The research process involves comparative analysis of multiple PQC algorithm families, such as lattice-based, code-based, hash-based, and multivariate polynomial-based schemes. Special attention is given to understanding their theoretical underpinnings, cryptographic assumptions, and levels of resistance against both classical and quantum adversaries. In doing so, the study assesses the computational complexity, key and signature sizes, memory requirements, and overall performance characteristics of each algorithm in diverse deployment environments—including high-performance computing systems, cloud platforms, and constrained devices like IoT nodes.

In addition to academic perspectives, the study incorporates insights from industry-led pilot projects and technology deployments. For instance, implementation trials conducted by Google, Cloudflare, and Amazon Web Services (AWS) are analyzed to understand practical issues involved in migrating from classical to post-quantum cryptographic infrastructures. Documentation from these corporations sheds light on real-world challenges such as backward compatibility, integration into legacy protocols (e.g., TLS, VPN), latency considerations, and resource overhead.

Furthermore, the study surveys the role of international standard-setting bodies and collaborative efforts in driving global adoption of PQC. This includes reviewing the activities of the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), and the European Union's PQCrypto project. The analysis considers how these organizations contribute to protocol design, algorithm benchmarking, and interoperability testing in post-quantum contexts. Their contributions provide a foundation for understanding how PQC is expected to evolve from academic proposals to mature, globally standardized technologies.

To ensure a comprehensive perspective, the research also draws upon open-source software repositories and simulation tools, such as Open Quantum Safe (OQS), PQClean, and liboqs, which offer practical frameworks for benchmarking and evaluating PQC implementations. These resources are instrumental in examining the practical feasibility of integrating PQC algorithms into modern cryptographic stacks.

By synthesizing findings across scholarly, governmental, and commercial domains, the methodology adopted in this study provides a multi-dimensional view of the current landscape and future trajectory of PQC development. This approach ensures that both the theoretical soundness and practical viability of post-quantum algorithms are thoroughly evaluated, offering a balanced assessment of their readiness for real-world deployment and policy adoption.

Results

The NIST PQC standardization project, launched in 2016, is one of the most significant global efforts to identify secure and efficient quantum-resistant algorithms. The competition has gone through multiple rounds, and as of 2022, three primary algorithms have been recommended for standardization:

- CRYSTALS-Kyber for public-key encryption and key establishment
- CRYSTALS-Dilithium and Falcon for digital signatures

These algorithms are all lattice-based, leveraging hard mathematical problems like the Learning With Errors (LWE) problem. They have been selected for their strong security guarantees, performance efficiency, and ease of integration into existing systems.

In addition to lattice-based algorithms, other approaches include code-based (e.g., McEliece), hash-based (e.g., SPHINCS+), multivariate polynomial, and isogeny-based cryptography. Each comes with its trade-offs in terms of key sizes, computational efficiency, and implementation complexity.

Real-world testing and early adoption are already underway. Google and Cloudflare have experimented with Kyber in their TLS implementations. AWS has launched a PQC testbed for enterprise users. These developments signal a readiness to transition from experimental phases to real-world deployment.

Impact Factor: 9.9 ISSN-L: 2544-980X

Discussion

The adoption of Post-Quantum Cryptography (PQC) introduces a wide range of both technical and strategic complexities that demand meticulous attention from policymakers, technologists, and cryptographic practitioners. One of the most prominent technical obstacles lies in the substantial increase in key sizes and ciphertext overhead for certain PQC algorithms. For example, code-based schemes such as McEliece require public keys that exceed several hundred kilobytes, making them impractical for constrained environments like Internet of Things (IoT) devices, embedded systems, and edge computing nodes where bandwidth, storage, and computational capacity are limited. Similarly, some hash-based and multivariate algorithms generate large digital signatures or exhibit performance bottlenecks under real-time operational conditions.

Another challenge concerns the integration of PQC into existing cryptographic ecosystems. Most contemporary infrastructure, including Transport Layer Security (TLS), Virtual Private Networks (VPN), secure email, and blockchain protocols, have been architected around classical public-key schemes like RSA and ECC. Replacing these with quantum-resistant alternatives necessitates not only algorithmic substitution but also extensive revisions to communication protocols, firmware, and hardware implementations. To mitigate transition risks, many experts advocate hybrid encryption models that combine traditional algorithms with PQC counterparts to ensure backward compatibility and maintain transitional security assurances. However, these approaches require additional computational resources and protocol redesign, complicating standardization and deployment timelines.

Despite these challenges, global efforts toward PQC adoption are accelerating. Several leading economies—such as the European Union, Japan, South Korea, Canada, and China—have initiated large-scale national programs focused on the development, evaluation, and implementation of PQC technologies. These initiatives encompass academic research grants, industrial testbeds, pilot deployments, and collaborations with international standardization bodies. Their primary objective is to ensure cryptographic sovereignty while aligning with international security benchmarks, particularly those defined by NIST and the Internet Engineering Task Force (IETF).

For emerging digital economies like Uzbekistan, the implications of adopting PQC are both strategic and urgent. As the country moves forward with digitalization initiatives in key sectors—such as electronic governance platforms, digital payment systems, educational information systems, and nationwide health databases—the integrity and confidentiality of transmitted and stored data become paramount. The long-term viability of these services depends on proactive defense mechanisms capable of withstanding future quantum threats.

To that end, investing in the domestic capacity to develop, test, and adapt PQC solutions is a critical priority. This includes establishing academic research programs in post-quantum cryptography, incentivizing collaboration between universities and tech industry stakeholders, and integrating open-source PQC toolkits such as PQClean and Open Quantum Safe into national IT infrastructure. The creation of dedicated cryptographic test environments will enable engineers and policymakers to evaluate algorithmic performance, interoperability, and resilience in real-world conditions, thereby accelerating the transition toward quantum-resilient systems.

Moreover, active participation in international PQC discourse—through conferences, working groups, and bilateral knowledge exchange—will empower Uzbekistan to contribute to and benefit from the evolving global cryptographic standards. By adopting a forward-looking approach, the nation can not only secure its critical information assets but also position itself as a regional leader in cybersecurity innovation and policy formulation in the post-quantum era.

Conclusion

Post-Quantum Cryptography is no longer a theoretical concept; it is a practical necessity. The transition to PQC must begin now to ensure that today's data remains secure in the quantum future.

Impact Factor: 9.9 ISSN-L: 2544-980X

Standardized algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium offer promising solutions that balance security and efficiency.

For Uzbekistan, embracing PQC means not only safeguarding its digital infrastructure but also participating in global cybersecurity innovation. By fostering research, international collaboration, and technical implementation, the nation can establish a robust and future-proof cybersecurity posture.

References

1. Turdimatov M., Mukhtarov F., Ibrokhimov N., Umarov SH., Mirzayev J., & Rakhmatov R. (2024, November). Mathematical approximator based on basic spline approximation. In *E3S Web of Conferences* (Vol. 508, p. 04010). EDP Sciences.
2. Akbarov D., Umarov S., Turdimatov M., Sotvoldiyev K., Ibrokhimov N., & Sadirova K. (2024, November). Algorithm of the electronic sign-code signature on the basis of the composition of existing complexities. In *E3S Web of Conferences* (Vol. 508, p. 03009). EDP Sciences.
3. Azizjonovich U. S., & Abdulhay A. (2024). AXBOROT XAVFSIZLIGI TIZIMLARINI INTELLEKTUALLASHTIRISH MASALALARI. *Al-Farg'oniy avlodlari*, *1*(1), 4-10.
4. Turdimatov, M., Xusanova, M., Sadirova, X., Abdurakhmonov, S., & Bilolov, I. (2024, November). On the method of approximation and quantization of information transmission through communication channels. In E3S Web of Conferences (Vol. 508, p. 03007). EDP Sciences.
5. Raxmonov O. SH., Musojonov X. M., & Abdullayev A. R. (2023). SECURITY PROTOCOLS, SAFEGUARDING THE DIGITAL FRONTIER. *SCHOLAR*, *1*(30), 70–74.
6. Qurbonaliyevna, X. M. (2025). KORXONA VA TASHKILOTLARNING AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA VPN TARMOQ QURISHNING ZAMONAVIY YECHIMLARI. Al-Farg'oniy avlodlari, 1(2), 122-125.
7. Bernstein D. J., et al. (2017). Post-Quantum Cryptography. Springer.
8. Qurbonaliyevna,X.M.(2024). Tarmoq qurilmalarida demilitarizatsiyalangan zona (DMZ) ni sozlash orqali xavfsizlikni ta'minlash. Al-Farg'oniy avlodlari, (4), 236-239.
9. Рахимов, З. (2025). Использование методов машинного обучения для распознавания цифровых следов в мобильных устройствах: от теории к практике. Engineering problems and innovations, 3(2), 49-53.
10. Khusanova, M. K. (2022). Network security and monitoring. Research Focus, 1(4), 177-183.
11. Shukhratjon, U., & Ozodbek, R. (2024). ASSESSMENT OF THE LEVEL OF SECURITY AVAILABLE IN 4G AND 5G MOBILE COMMUNICATION NETWORKS. Al-Farg'oniy avlodlari, (4), 294-297.