Analysis of Problems and Prospects of Implementation of Post-Quantum Cryptographic Algorithms

Andriy Horpenyuk[1], Ivan Opirskyy[1], and Pavlo Vorobets[1]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79000, Ukraine*

Abstract

The paper provides an overview and analysis of the current state, problems, and prospects of post-quantum cryptography. Considered the status of the Post-Quantum Cryptography Standardization Process. Organizations like the National Institute of Standards and Technology (NIST) are actively working on standardizing post-quantum cryptography. Evaluation rounds have been conducted, thoroughly analyzing numerous candidate post-quantum algorithms to select the most efficient and secure ones. Identified main categories of post-quantum cryptographic algorithms. Described key size of post-quantum cryptographic algorithms. Open-source libraries like Open Quantum Safe (OQS) have been developed, offering implementations of various post-quantum algorithms. These libraries enable researchers, developers, and engineers to utilize and test post-quantum algorithms in various applications. There is growing awareness of the need to prepare for the post-quantum computing era. Many companies, organizations, and governments are exploring the implications of quantum computing for their infrastructure and data security and considering the adoption of post-quantum cryptographic solutions.

Keywords

Post-quantum cryptography, quantum computers, standardization process, NIST.

1. Introduction

The concept of a quantum computer is no longer just a theory. The battle for supremacy in quantum technology is on among nations since it is the most significant technology in the world [1, 2]. Technology will shorten the amount of time it takes to compute from years to hours or even minutes. The scientific community will greatly benefit from the power of quantum computing. It does, however, highlight significant cybersecurity risks. Theoretically, an attack might be launched against any cryptographic algorithm. When practical quantum computers with millions of qubits capacity become available, they will be able to decrypt almost all current public-key cryptography systems.

Modern cryptography algorithms are built on complex mathematical functions and principles to provide strong security and protect sensitive information from unauthorized access and attacks. But quantum computers have the potential to break many of the classical cryptographic algorithms that are currently in widespread use. Traditional cryptographic systems, such as RSA and ECC, rely on mathematical problems that are computationally hard to solve using classical computers. However, quantum computers can leverage their unique quantum properties, such as superposition and entanglement, to perform certain calculations exponentially faster than classical computers. The vulnerability of classical cryptography to quantum attacks arises from the fundamental differences in the computational capabilities of quantum and classical computers. Quantum computers can perform certain mathematical operations in parallel, thanks to the superposition of qubits, which allows them to solve problems that would take classical computers an impractical amount of time. As a result, the development and standardization of post-quantum cryptographic

CQPC-2023: Classic, Quantum, and Post-Quantum Cryptography, August 1, 2023, Kyiv, Ukraine
EMAIL: gorpenuk_ay@polynet.lviv.ua (A. Horpenyuk); ivan.r.opirskyi@lpnu.ua (I. Opirskyy); pavlo.vorobets94@gmail.com (P. Vorobets)
ORCID: 0000-0001-5821-2186 (A. Horpenyuk); 0000-0002-8461-8996 (I. Opirskyy); 0009-0007-3870-829X (P. Vorobets)

algorithms have become imperative. Post-quantum cryptography aims to create cryptographic systems that remain secure even in the presence of powerful quantum computers (Table 1). These algorithms rely on mathematical problems that are believed to be hard for both classical and quantum computers to solve.

Table 1
Current status of security of classical cryptosystems to quantum computers

Cryptosystem	Status
RSA	Broken
DSA	Broken
Diffie-Hellman key-exchange	Broken
ECDSA, ECDH (Elliptic curve cryptography)	Broken
DES, 3DES	Broken
AES	Larger key sizes needed
SHA-1	Broken
SHA-2, SHA-3	Larger key sizes needed
Chacha/Salsa20	Larger key sizes needed
Blowfish, Twofish	Larger key sizes needed

Post-quantum cryptography evolves and becomes more relevant in the face of advances in quantum computing, several challenges and problems have emerged in the standardization of post-quantum cryptographic algorithms. Some of these issues include a lack of mature algorithms, performance considerations, key size and bandwidth, interoperability and integration, transition period, NIST standardization process, quantum attack timeline uncertainty, and algorithm agility.

Despite these challenges, the research and standardization efforts in post-quantum cryptography continue to progress, and as more secure and efficient algorithms are developed and tested, the deployment and adoption of post-quantum cryptographic standards are expected to become more feasible.

2. Literature Review and Problem Statement

Cryptography is an essential aspect of modern life, providing the necessary security and trust in our digital interactions, financial transactions, communication, and data privacy. Its widespread use ensures the confidentiality, integrity, and authenticity of information in various aspects of our daily lives.

When you visit a website with HTTPS (Hypertext Transfer Protocol Secure) in the URL, cryptography is at work. It encrypts the data exchanged between your web browser and the website's server, ensuring that sensitive information like passwords, credit card details, and personal data are protected from unauthorized access. Also, websites and applications use cryptographic hash functions to store user passwords securely. The actual password is not stored, only a hash (irreversible output) of the password. This way, even if the database is compromised, passwords remain protected.

Cryptography is used to secure online banking transactions. When you log in or transfer funds through Internet banking, encryption ensures that your financial information remains confidential and cannot be intercepted by malicious actors.

Messaging platforms like WhatsApp, Signal, and Telegram use end-to-end encryption. This means that only the sender and recipient can read the messages, ensuring privacy and preventing eavesdropping. Email communication can be secured using encryption methods like Pretty Good Privacy (PGP) or Secure/Multipurpose Internet Mail Extensions (S/MIME). These techniques protect email content and attachments from unauthorized access during transmission.

We are currently on the brink of a revolution in the field of cryptography due to the emergence of quantum computers, which have the potential to disrupt long-standing principles of system security. Traditional cryptographic algorithms, such as RSA and ECC, rely on mathematical problems that are hard to solve using classical computers. However, quantum computers can efficiently solve some of these problems, such as integer factorization and discrete logarithms, using algorithms like Shor’s algorithm and Grover's algorithm [3]. These quantum algorithms could potentially break many of the cryptographic algorithms currently in use, posing a threat to the security of numerous systems and infrastructures that rely on these algorithms. However, the cost and complexity of building quantum computers on a scale that would allow them to break modern cryptographic algorithms remain uncertain [4].

Post-quantum cryptography, also known as quantum-resistant or quantum-safe cryptography, is an emerging field that addresses the potential threat posed by quantum computers to current cryptographic systems. Quantum computers have the potential to solve certain mathematical

problems much more efficiently than classical computers, which could render many widely used cryptographic algorithms, such as RSA and ECC, vulnerable to attacks [5, 6].

The central goal of post-quantum cryptography is to develop cryptographic methods that remain secure against both classical and quantum attacks. These methods are based on mathematical problems that are believed to be hard even for powerful quantum computers. Unlike traditional cryptographic algorithms, which rely on the hardness of factoring large integers or solving the elliptic curve discrete logarithm problems, post-quantum algorithms use alternative mathematical structures such as lattices, error-correcting codes, multivariate polynomials, and isogenies.

One of the significant challenges in post-quantum cryptography is the transition from current cryptographic standards to quantum-resistant ones. This process requires careful evaluation, standardization, and integration into existing systems and protocols. Cryptographers, researchers, and industry experts are collaborating to develop and test these algorithms to ensure their security and efficiency in real-world applications.

Post-quantum cryptography is an interdisciplinary field that involves mathematics, computer science, and quantum physics. It represents a critical area of research and development to ensure the long-term security and resilience of our digital communication and data in the face of evolving computing technologies. By embracing post-quantum cryptographic standards, we can fortify our cryptographic systems and stay ahead of potential threats in the era of quantum computing.

3. Problems of Post-Quantum Cryptography

In recent years, the rapid development of quantum computing has sparked growing concerns about the security of traditional cryptographic systems. Quantum computers have the potential to solve certain mathematical problems much more efficiently than classical computers, which could render many of today's widely used cryptographic algorithms, such as RSA, DSA, and ECDSA. This scenario poses a significant threat to the confidentiality, integrity, and authenticity of sensitive information in various sectors of our lives.

Post-quantum cryptography, also known as quantum-resistant or quantum-safe cryptography, aims to address these security challenges by designing cryptographic algorithms that remain secure against attacks from both classical and quantum computers. The main objective is to develop cryptographic methods based on mathematical problems that are believed to be hard even for powerful quantum computers [7].

The need for post-quantum cryptographic standards is becoming increasingly urgent. While quantum computers capable of breaking current cryptographic systems are still in the realm of theoretical research and large-scale quantum computing is not yet a reality, the potential threat is real. It is crucial to prepare in advance for the inevitable emergence of more powerful quantum computers.

3.1. Lack of Mature Algorithms

Many of the proposed post-quantum cryptographic algorithms are relatively new and have not undergone extensive real-world testing. The lack of a long track record for these algorithms raises concerns about their security and efficiency. Established cryptographic algorithms have undergone years of cryptanalysis and peer review, which provides a high level of confidence in their security. In contrast, the newness of post-quantum algorithms means that their security might not be as thoroughly understood. It is essential to subject these algorithms to rigorous analysis to ensure their resistance to both classical and quantum attacks.

The lack of a long history of real-world deployment leaves open the possibility of unforeseen attacks. Unlike well-studied classical algorithms, there may be unexplored vulnerabilities that could be exploited by adversaries. Due to their relative novelty and the ongoing standardization process, post-quantum cryptographic algorithms may not be readily available in commercial products and applications. This hinders their practical deployment in the current cryptographic landscape.

3.2. Quantum Attack Timeline Uncertainty

The timeline for the emergence of powerful quantum computers capable of breaking traditional cryptographic algorithms remains uncertain. This uncertainty complicates the

decision-making process for adopting post-quantum cryptographic solutions.

Quantum computers use qubits instead of bits. Unlike classical bits, which can represent either a 0 or a 1, qubits can exist in a superposition of states, meaning they can simultaneously represent both 0 and 1 at the same time. In classical computing, bits are the fundamental building blocks used to represent and process information. They can be in one of two states: 0 or 1. These binary states are used to perform logical operations and store data in classical computers. The first quantum computer with one qubit was created and demonstrated in 1998. Since then, we have seen the number of qubits represented in a quantum computer grow over time (see Table 2). Here is a basic qubit advance timeline by year as of this writing, based on various vendor claims.

Table 2
Qubit growth over time

Year	Qubit Number
2000	5 and 7
2006	12
2008	28
2012	84
2015	1000
2017	2000
2022	5000
2023	Announced 100000

It is important to recognize that number of qubits is not the sole determinant of a quantum computer's performance or computational power. Having more qubits is a good have, but not all qubits are equal, and a quantum computer's ability to solve something is determined by more variables than just the sheer number of qubits [8].

The quality of qubits is critical. Quantum computers are highly sensitive to noise and errors, and maintaining qubit coherence is challenging. High-fidelity qubits with long coherence times are essential for reliable quantum computations. The arrangement and connectivity of qubits in a quantum processor are vital. The ability to efficiently perform multi-qubit operations and implement quantum error correction codes depends on qubit connectivity. Quantum computers must employ error correction techniques to mitigate the impact of quantum errors that naturally occur during computation. Quantum error correction introduces additional qubits and computational overhead. Developing efficient quantum algorithms and software tailored to the hardware is vital for maximizing quantum computing performance.

Quantum computing is an interdisciplinary field that involves physics, computer science, materials science, and more, and it requires significant advancements in hardware, software, and algorithms to achieve practical quantum advantage in solving complex problems. Significant progress has already been made, but it remains in the field of research and experimentation [9].

3.3. Transition Period and Standardization Process

As post-quantum cryptographic standards are being developed, there is a transitional period where both traditional and post-quantum algorithms need to coexist. Managing this transition effectively without compromising security is a significant concern. The National Institute of Standards and Technology is leading the effort to standardize post-quantum cryptography. However, the process is time-consuming, and there are various candidate algorithms to consider, making the selection and standardization process challenging.

The NIST Post-Quantum Cryptography (PQC) Standardization Process began in December 2016 [10], when NIST issued a public call for submissions of post-quantum public-key cryptographic algorithms. They identified five main categories of post-quantum cryptographic algorithms:

- Lattice-based cryptography uses lattices and their associated mathematical properties to provide security. A lattice is a set of points in a multi-dimensional space that form a regular grid-like structure. Lattice-based cryptography leverages the hardness of certain lattice problems to provide security against quantum attacks. Lattice-based cryptographic algorithms seem to be the most promising and quantum-resistant [11].

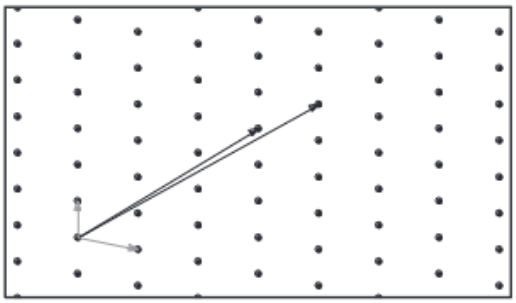

Figure 1: Lattice-based graph

● Code-based cryptography relies on error-correcting codes to provide security. The security of these schemes is based on the hardness of decoding certain structured codes, making them resistant to quantum attacks. Code-based cryptography is a strong contender for post-quantum cryptography because it is thought that this problem is computationally taxing the complexity of the decoding solution is still hard, although the precise complexity is a topic of ongoing research.

● Hash-based cryptography built upon cryptographic hash functions. These schemes are based on the hardness of finding collisions in the hash function, offering a potential post-quantum solution. Hash-based cryptography's fundamental benefit is that it is a commonly used, well-researched technique that ensures great resistance to quantum assaults, making it a candidate for long-term security in the post-quantum period (as a long enough key is utilized). However, hashing-based cryptography can also have problems. First, if attackers find a collision, the security of the hash function can be compromised. Second, since conventional algorithms have exponential complexity but are only efficient for short keys, Grover's algorithm can crack hash functions in time $\sqrt{N}$ (where N is the length of the key), which can lead to increased processing time and more memory. Hash-based signature is a set of one-time signature schemes that use a tree data structure to efficiently combine multiple signatures. To sign a message, a Hash-based signature selects one of the one-time signatures from its collection and uses it. You should never use the same signature twice, as this will break security.

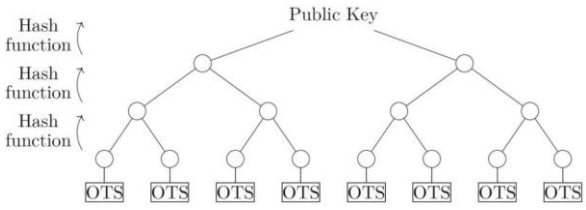

Figure 2: Hash-based graph

● Multivariate polynormal cryptography relies on algebraic equations with multivariate polynomials. Security is based on the difficulty of solving systems of multivariate polynomial equations. These polynomials can be defined both over the basic and over the expansion field in certain situations. Research has shown that solving systems of multidimensional polynomial equations is a task that requires a minimum amount of work. However, algebraic, differential, and Gröbner basis attacks also affect Multivariate polynormal cryptography. As a result, Multivariate polynormal cryptography is essentially not used [12].

● Isogeny-based cryptography is based on the mathematics of elliptic curves and isogenies. These schemes rely on constructing mappings between elliptic curves. Security is based on supersingular isogeny problems, or finding an isogeny mapping between two supersingular elliptic curves with the same number of points. This is one of the few difficult mathematical problems that currently resist quantum computer attacks. Isogeny-based protocols require a very small key compared to any other post-quantum cryptography variant but are still much larger than conventional elliptic curve algorithms. However, compared to lattice-based cryptography, they are less efficient and suitable for more complex cryptographic primitives. This cryptosystem is relatively new and untested, therefore there may be unforeseen flaws or weak places that attackers can take advantage of. Furthermore, even though isogeny-based cryptography only needs small key sizes, the computational cost of key creation is still quite high, which could be a drawback for systems with limited resources.

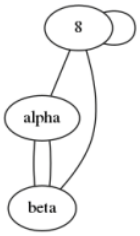

Figure 3: Supersingular l-isogeny graph

These categories are considered potential candidates for quantum-resistant cryptographic standards. A total of 82 candidates were submitted by the November 2017 deadline [13]. In Dec. 2017, NIST announced that 69 of these candidates met both the submission requirements and the minimum acceptability criteria and were accepted into the first round of the standardization process.

After careful consideration during the third round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. NIST will recommend two primary algorithms to be implemented for most use cases: CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures). In addition, the signature

schemes FALCON and SPHINCS+ will also be standardized. The four algorithms selected for this fourth round are BIKE, Classic McEliece, HQC, and SIKE.

It is important to stay updated with the progress of standardization efforts, as cryptographic standards play a critical role in ensuring the security and resilience of digital communications in the post-quantum era.

3.4. Performance Considerations

Some post-quantum cryptographic algorithms are computationally intensive, which can lead to slower encryption and decryption speeds compared to traditional cryptographic algorithms. This performance overhead may limit their practical adoption, especially in resource-constrained environments [14].

The labor required to generate and validate keys is frequently substantially more than with classical cryptography, even if a quantum-resistant cryptographic standard has smaller key sizes. Because of this, the NIST competition necessitates extensive performance testing, and participants make every effort to speed up their algorithms. Although switching to a post-quantum algorithm is expected to reduce overall performance even on the greatest and fastest computers and devices, NIST will most likely choose a post-quantum standard that has a good performance/security trade-off. After careful thought, a production environment or product must switch entirely to a quantum-resistant algorithm [15].

The performance analysis of the algorithms is done using the Open Quantum Safe (OQS) project. It is a project, developing and prototyping quantum-resistant cryptography algorithms. OQS project provides an open-source library that implements several post-quantum cryptographic algorithms. The OQS library aims to facilitate the research, development, and integration of quantum-resistant algorithms into various applications and systems. The performance of post-quantum algorithms can vary significantly depending on the specific algorithm, its implementation, and the hardware on which it is executed. The OQS also offers benchmarking information for different quantum-resistant algorithms, which is used in this paper to compare the runtime behavior and memory usage of the algorithms [16]. The algorithms' runtime behavior and memory usage data are gathered based on the algorithms' execution on Amazon Web Service (AWS) with a CPU model of an Intel Xeon Platinum 8259CL CPU running at 2.5 GHz.

Performance analysis of numerous quantum-safe algorithms reveals that these algorithms typically demand a large number of CPU cycles for their fundamental activities, such as key creation, encrypt/decryption, key exchange, signing, and verifying, among others (see Table 3). Additionally, the algorithms demand very large public key and private key sizes. Compared to traditional cryptographic techniques, these approaches consume a lot of memory at runtime. The higher CPU cycle and memory usage is constrained to the Information Communication Technology systems and devices. The resource constraints can be resolved for the systems like a laptop, desktop, or high-end server up to some extent [17, 18]. However, it is a challenging issue for small devices like smartphones, sensor networks [19], smart-grid, IoT [20], smart devices [21], smart homes [22], etc.

It is important to remember that post-quantum algorithms are still being actively researched and optimized. The performance characteristics of these algorithms might change over time as researchers discover more efficient implementations and further refine their designs.

When evaluating the performance of post-quantum algorithms, it is essential to consider factors such as key size, encryption and decryption speeds, memory requirements, and the targeted hardware platform. Performance trade-offs are often made to achieve a balance between security and efficiency, depending on the specific application's requirements and constraints.

3.5. Key Size and Bandwidth

Post-quantum cryptographic algorithms require larger key sizes compared to classical algorithms. This can lead to increased bandwidth requirements for secure communication and can be problematic for devices with limited storage and processing capabilities.

When comparing the key sizes of various post-quantum cryptographic algorithms, it is essential to understand that different algorithms have different security levels and performance trade-offs. Key size is one of the factors that can affect the security and efficiency of the cryptographic system. Generally, larger key sizes offer higher

security, but they may also result in increased memory and bandwidth requirements.

Table 3

Performance Assessment

Algorithm	Type	Performance
CRYSTALS-KYBER	Lattice-based	Overall performance of CRYSTALS-KYBER in software, hardware, and hybrid settings is excellent.
CRYSTALS-Dilithium	Lattice-based	It uses pseudorandomness and truncated storage techniques to improve performance. The scheme does not use floating-point arithmetic, which is an advantage. Highly efficient and relatively simple in implementation.
Falcon	Lattice-based	The verification process is fast and requires low bandwidth. It is the best choice for some constrained protocol scenarios.
SPHINCS+	Hash-based	Key generation and verification are much faster than signing
BIKE	Code-based	The performance of BIKE would be suitable for most of the applications as confirmed by several hardware benchmarks
HQC	Code-based	The bandwidth of the HQC exceeds that of BIKE, HQC's key generation but decapsulation only requires a fraction of the kilocycles required by BIKE. HQC is one of the top two alternate KEMs. The overall performance of the HQC is not optimal but still, it is acceptable.
Classic McEliece	Code-based	It has the smallest ciphertext among any of the NIST PQC candidates
SIKE	Isogeny-based	It has relatively low communication costs. However, performance on embedded devices may be an issue because of the time to perform a single key encapsulation/decapsulation.

Table 4 presents a comparison of post-quantum cryptographic algorithms and their typical key sizes.

Larger key sizes result in the need for more storage space to store keys and increased bandwidth usage for transmitting cryptographic data. This can be problematic for devices with limited resources, such as IoT devices and mobile devices, where memory and bandwidth are at a premium. Larger key sizes can lead to increased computational overhead during encryption, decryption, and key generation operations. This can slow down cryptographic processes and impact system performance, especially on devices with limited processing power. Existing systems and protocols may not be designed to handle post-quantum key sizes, which could create compatibility issues when transitioning to post-quantum cryptographic solutions. Upgrading systems to support larger keys might require significant changes and updates. The complexity of handling large keys in software and hardware implementations can be challenging. Designing efficient and secure implementations for these algorithms might be more difficult compared to classical cryptographic algorithms.

3.6. Interoperability and Integration

Integrating post-quantum cryptographic algorithms into existing systems and protocols can be complex. Ensuring seamless interoperability between post-quantum algorithms and existing infrastructure is a challenging task.

The current cryptographic infrastructure of any company will need to be upgraded significantly to transition to post-quantum cryptography. Some of their current IT parts can become wholly unusable and need to be replaced. There may be a need to redesign and alter the protocol, software, and algorithms currently in use. Overall, the company will incur significant budget overhead and unavoidable complexity as a result of the conversion process [23].

The majority of the prospective post-quantum cryptography algorithms face a difficult problem with scalability. It is challenging to demonstrate the algorithm's difficulty on a large scale. For instance, one of the main methods for creating quantum-safe algorithms, lattice-based cryptography, scales well but only provides

average-case hardness. Scalability and toughness can be compromised. Either can be achieved, but not both.

This means that in the world of post-quantum cryptography, protocol designers need to be aware of the possibility of different trade-offs and choose systems matching their application scenario, taking into account how frequently public keys are sent relative to ciphertexts or signed messages using them and how important computation speed is relative to bandwidth. The choice of a post-quantum cryptographic algorithm should be driven by a careful analysis of the specific requirements and constraints of the application. Balancing security, efficiency, and resource limitations is key to successfully integrating post-quantum cryptography into various systems and protocols. As the field of post-quantum cryptography continues to evolve, more efficient and optimized algorithms may emerge, further enhancing the possibilities for secure and practical cryptographic solutions in the era of quantum computing [24, 25].

Table 4
Comparison of some post-quantum cryptographic algorithms

Algorithm	Type	Public Key, byte	Private Key, byte	Signature, byte
NTRU Encrypt	Lattice-based	1230	1590	—
Rainbow	Multivariate-based	124k	95k	—
SPHINCS	Hash-based	1k	1k	41k
SPHINCS+	Hash Signature-based	32	64	8k
Falcon-512	Lattice-based	897	1281	666
Falcon-1024	Lattice-based	1793	2305	1280
CRYSTALS-Dilithium	Lattice-based	2592	4864	—
CRYSTALS-KYBER	Lattice-based	1568	3168	—
BIKE	Code-based	5122	16494	—
HQC	Code-based	7245	7258	—
SIKE	Isogeny-based	564	48	—
BLISS-II	Lattice-based	7k	2k	5k
Goppa-based McEliece	Code-based	1M	11k	—
RLCE	Code-based	115k	3k	—
Quasi-cyclic MDPC-based McEliece	Code-based	1232	2464	—
SIDH	Isogeny-based	564	48	—
SIDH (compressed keys)	Isogeny-based	330	48	—

3.7. Future of Post-Quantum Algorithms

Cybersecurity of post-quantum algorithms is a key characteristic that adds significance to their development and integration into modern information systems. The fundamental concept of post-quantum cryptography is to design algorithms that remain resistant to attacks from both classical and quantum computers.

The primary requirement for post-quantum algorithms is their resistance to attacks from potential quantum computing systems. These algorithms are designed to remain secure even in the presence of powerful quantum computers. Post-quantum algorithms must also resist attacks from classical computing systems. This is important since new cryptographic algorithms can be vulnerable to attacks in the initial years after their introduction. Post-quantum algorithms should be designed to avoid vulnerabilities to new attack methods, including those that exploit quantum technologies. They should undergo scrutiny and security analysis to ensure their resistance to various types of attacks and vulnerabilities. Post-quantum algorithms should be ready for updates and adaptation since the cryptographic landscape is constantly evolving, and new attacks and methods may emerge over time.

In the face of the impending quantum computing era, it is imperative for every organization to swiftly take action. Outdated and

weakly quantum-resistant cryptographic methods must be promptly replaced with robust alternatives. This proactive transition to existing quantum-resistant cryptography, along with appropriate key sizes, should be a top priority wherever feasible. The urgency of this shift lies in the potential vulnerability of current cryptographic systems to quantum attacks. Quantum computers possess the capability to swiftly unravel traditional encryption, rendering sensitive data susceptible to exposure. By embracing quantum-resistant cryptography, organizations can fortify their defenses and ensure the longevity of their data security [26, 27].

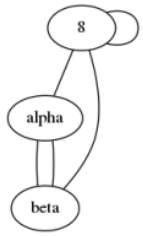

Figure 4: Four major post-quantum mitigation project stages

Most early quantum-involved systems are anticipated to adopt a hybrid approach, utilizing a combination of both quantum and classical technologies. This hybrid model is designed to harness the strengths of both quantum and classical computing to create more robust and efficient solutions for various applications [28]. Quantum computers, while holding the potential for certain types of computations, are still in their nascent stages of development and are not yet ready to completely replace classical computers [29]. Thus, the practical implementation of quantum computing is likely to involve integrating quantum capabilities into existing classical systems to address specific tasks where quantum advantages are prominent, such as cryptography, optimization, and simulations.

The hybrid approach offers organizations the opportunity to harness the emerging potential of quantum computing while maintaining compatibility with their established classical infrastructure. It also offers a gradual transition as quantum technologies continue to advance and become more applicable for broader usage. As the quantum computing field progresses and matures, it is expected that the integration of quantum and classical technologies will become more seamless and sophisticated, leading to the realization of more capable and efficient quantum-involved systems [30–32].

Fully quantum solutions refer to a future state where quantum computing technologies are not only fully developed but also integrated into various aspects of computing, cryptography, and problem-solving. Quantum-resistant cryptography will eliminate most of the risk from quantum cryptographic attacks, but quantum-based cryptography and devices are the ultimate protection.

4. Conclusion

Breaking current cryptographic algorithms using a quantum computer does indeed require a large-scale quantum computer with a significant number of qubits. The number of qubits needed to break specific algorithms depends on the algorithm's security strength and the chosen quantum attack method. However, the exponential growth in quantum computer technology's development shows that the storm is approaching very fast. The migration to post-quantum cryptographic algorithms is essential to ensure the long-term security of our digital infrastructure in the face of potential future quantum computing advancements. The transition to post-quantum cryptographic algorithms is a complex process that requires careful evaluation, standardization, and implementation. Cryptographers, researchers, and industry experts are working together to develop and test these algorithms to ensure their security and efficiency in real-world applications. While the timeline for the widespread deployment of large-scale quantum computers remains uncertain, the migration to post-quantum cryptographic algorithms is a prudent step to safeguard our digital security in the era of quantum computing.

Post-quantum cryptography brings significant changes to the field of cryptography and security, but it also opens up new opportunities for ensuring the resilience of digital infrastructure in the face of the growing threat of quantum computers.

5. References

[1] V. Buriachok, et al., Implementation of Active Cybersecurity Education in Ukrainian Higher School, Information Technology for Education, Science, and Technics, vol. 178 (2023) 533–551. doi:10.1007/978-3-031-35467-0_32

[2] V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master's Program on Cybersecurity, Advances in Computer Science for Engineering and Education II, vol. 938 (2020) 610-624. doi:10.1007/978-3-030-16621-2_57
[3] L. K. Grover, A Fast Quantum Mechanical Algorithm for Database Search, in 28th Annual ACM Symposium on Theory of Computing (1996).
[4] S. Yevseiev, et al., Development of Niederreiter Hybrid Crypto-Code Structure on Flawed Codes, Eastern-European Journal of Enterprise Technologies. Information and Controlling System 1, 9(97) (2019) pp. 27–38. doi: 10.15587/1729-4061.2019.156620
[5] A. Sahun, et al., Devising a Method for Improving Crypto Resistance of the Symmetric Block Cryptosystem RC5 using Nonlinear Shift Functions, Eastern-European J. of Enterprise Tech. 5(113) (2021) 17–29. doi: 10.15587/1729-4061.2021.240344
[6] I. Opirskyy, Y. Sovyn, O. Mykhailova, Heuristic Method of Finding Bitsliced-description of Derivative Cryptographic S-box, in IEEE 16th Int. Conf. on Advanced Trends in Radioelectronics, Telecommun. and Computer Engineering (2022) 104–109. doi: 10.1109/TCSET55632.2022.9766883
[7] D. J. Bernstein, J. Buchmann, E. Dahmen, Code-based Cryptography (2016).
[8] R. A. Grimes, Cryptography Apocalypse (2020).
[9] L. Chen, et al., Report on Post-Quantum Cryptography, NIST Publications (2016). doi: 10.6028/NIST.IR.8105
[10] G. Alagic, et al., Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Publications (2020). doi: 10.6028/NIST.IR.8309
[11] D. J. Bernstein. Visualizing Size-Security Tradeoffs for Lattice-based Encryption, IACR Cryptol. ePrint Arch. (2019) 655.
[12] A. Casanova, et al., A Great Multivariate Short Signature, Submission to NIST (2017).
[13] G. Alagic, et al., Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NIST Publications (2022). doi: 10.6028/NIST.IR.8413
[14] M. Kumar, Post-Quantum Cryptography Algorithm's Standardization and Performance Analysis. Array 15 (2022) 100242. doi: 10.1016/j.array.2022.100242
[15] M. Raavi, et al., Security Comparisons and Performance Analyses of Post-Quantum Signature Algorithms, in Applied Cryptography and Network Security (2021) 424–447. doi: 10.1007/978-3-030-78375-4_17
[16] U. Banerjee, S. Das, A. P. Chandrakasan, Accelerating Post-Quantum Cryptography using an Energy-Efficient TLS Crypto-Processor, in 2020 IEEE International Symposium on Circuits and Systems (2020). doi: 10.1109/iscas45731.2020.9180550
[17] F Borges, P. R. Reis, D. Pereira, A Comparison of Security and Its Performance for Key Agreements in post-Quantum Cryptography, IEEE Access 8 (2020) 142413–142422. doi: 10.1109/access.2020.3013250
[18] V. Pastushenko, D. Kronberg, Improving the Performance of Quantum Cryptography by Using the Encryption of the Error Correction Data, Entropy 25 (2023) 956. doi: 10.3390/e25060956
[19] 19 V. Sokolov, P. Skladannyi, H. Hulak, Stability Verification of Self-Organized Wireless Networks with Block Encryption, in: 5th International Workshop on Computer Modeling and Intelligent Systems, vol. 3137 (2022) 227–237.
[20] V. Grechaninov, et al., Decentralized Access Demarcation System Construction in Situational Center Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3188, no. 2 (2022) 197–206.
[21] V. Grechaninov, et al., Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center, in: Workshop on Emerging Technology Trends on the Smart Industry and the Internet of Things, vol. 3149 (2022) 107–117.
[22] R. Asif, Post-Quantum Cryptosystems for Internet-of-Things: a Survey on Lattice-based Algorithms, IoT 2(1) (2021) 71–91. doi: 10.3390/iot2010005
[23] M. Baldi, P. Santini, G. Cancellieri, Post-Quantum Cryptography based on Codes: State of the Art and Open Challenges, in AEIT International Annual Conference (2017). doi: 10.23919/aeit.2017.8240549
[24] P. Wallden, E. Kashefi, Cyber Security in the Quantum Era (2021).
[25] D. Bellizia, et al., Post-Quantum Cryptography: Challenges and Opportunities for Robust and Secure HW Design, in IEEE International Symposium on Defect and fault tolerance in VLSI and Nanotechnology

Systems (DFT) (2021) 1–6. doi: 10.1109/DFT52944.2021.9568301
[26] W. Buchanan, A. Woodward, Will Quantum Computers Be the End of Public Key Encryption? Journal of Cyber Security Technology 1(1) (2016) 1–22. doi: 10.1080/23742917.2016.1226650
[27] L. Chen, Cryptography Standards in Quantum Time: New Wine in an Old Wineskin? IEEE Security & Privacy 15(4) (2017) 51–57. doi: 10.1109/MSP.2017. 3151339
[28] C. Portmann, R. Renner, Security in Quantum Cryptography 94 (2022) 025008. doi: 10.1103/RevModPhys.94.025008
[29] W. Barker, W. Polk, M. Souppaya, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and using Post-Quantum Cryptographic Algorithms. NIST Cybersecurity White Paper (2021). doi: 10.6028/NIST.CSWP.04282021
[30] C. Bernhardt, Quantum Computing for Everyone. Cambridge, MIT Press (2019).
[31] P. Hauke, et al., Perspectives of Quantum Annealing: Methods and Implementations, Reports on Progress in Physics 83(5) (2020) 054401.
[32] A. Maitra, J. Samuel, S. Sinha, Likelihood Theory in a Quantum World: Tests with Quantum Coins and Computers, Pramana J Phys 94 (2019) 57. doi: 10.1007/s12043-020-1926-9