MANTECH Publications

Journal of Computer, Internet and Network Security
Volume 11, Issue 1, January-April 2026
ISSN: 2457-0176 (Online)

Post-Quantum Cryptography

Raman S. Patil[1], Kanika N. Deshmukh[2]

Associate Professor[1], Student[2]

Department of Computer Science Engineering

Loknete Shamrao Peje Government College of Engineering, Ratnagiri

Email ID: *Ramanspatil1@gmail.com[1], kanikand4d@yahoo.com[2]*

DOI: *https//doi.org/10.5281/zenodo.19281439*

ABSTRACT

The development of quantum computing is creating major concerns for modern cryptographic systems. Most widely used public-key cryptography algorithms such as RSA and Elliptic Curve Cryptography (ECC) rely on mathematical problems that can be solved efficiently using quantum algorithms like Shor's algorithm. As quantum computing technology advances, the security of these classical cryptographic methods may become vulnerable. Post-Quantum Cryptography (PQC) has emerged as a promising solution to protect digital communication against attacks from quantum computers. PQC refers to cryptographic algorithms that are designed to remain secure even in the presence of quantum computational capabilities. These algorithms are usually based on mathematical problems such as lattice structures, error-correcting codes, multivariate equations, and hash functions that are believed to be resistant to quantum attacks. Recently, international research communities and organizations such as the National Institute of Standards and Technology (NIST) have been actively working toward standardizing quantum-resistant cryptographic algorithms. This paper presents an overview of post-quantum cryptography including its motivation, types of PQC algorithms, architecture, implementation challenges, and real-world applications. A comparative discussion of different PQC approaches is also included. The study highlights how PQC can play an essential role in securing future communication networks, cloud computing platforms, financial transactions, and digital identity systems in the era of quantum computing.

KEYWORDS: *Post-Quantum Cryptography, Quantum Computing, Lattice-Based Cryptography, Digital Signatures, Quantum-Safe Security, Encryption Algorithms*

INTRODUCTION

Cryptography has been the backbone of secure communication systems for many decades. Modern internet protocols, online banking systems, cloud services, and government networks rely heavily on public-key cryptography for data protection. However, the emergence of quantum computing technology has raised serious concerns about the long-term security of these cryptographic methods.

Quantum computers operate based on quantum mechanical principles such as superposition and entanglement. These machines can perform certain computational tasks significantly faster than classical computers. For instance, Shor's algorithm allows efficient factorization of large numbers and computation of discrete logarithms, which are the mathematical foundations of widely used cryptographic algorithms such as RSA and Elliptic Curve Cryptography. If large-scale quantum computers become practical, they may break these encryption systems within a short time.

Because of this potential threat, researchers have started exploring cryptographic solutions that can remain secure even in the presence of quantum computing power. These solutions are collectively known as Post-Quantum Cryptography (PQC). PQC algorithms rely on mathematical problems that are believed to be hard for both classical and quantum computers to solve.

Over the past decade, significant research efforts have been carried out to develop and standardize quantum-resistant algorithms. In particular, the National Institute of Standards and Technology (NIST) initiated a global competition to identify suitable PQC algorithms that can replace traditional cryptographic schemes. The competition evaluated numerous candidate algorithms based on security, performance, and practical implementation considerations.

Post-Quantum Cryptography is expected to play a critical role in protecting future digital infrastructures including 5G networks, IoT systems, cloud platforms, and blockchain

applications. However, transitioning to PQC also introduces several technical and operational challenges such as larger key sizes, performance overhead, and compatibility with existing systems.

This paper provides a detailed review of PQC technologies and discusses the current progress, challenges, and future directions in this rapidly evolving field.

BACKGROUND OF QUANTUM THREATS

The motivation behind the development of **post-quantum cryptography (PQC)** mainly comes from the rapid advancement in **quantum computing technologies**. For several decades, modern digital security has depended on cryptographic algorithms whose security relies on certain mathematical problems that are very hard for classical computers to solve. However, the computational model used by quantum computers is fundamentally different from classical machines, and this difference can make some of these difficult mathematical problems much easier to solve.

Traditional public-key cryptographic systems such as RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are widely used for secure communication on the internet. These algorithms protect sensitive data such as online banking transactions; secure email communications, cloud storage access, and digital signatures used in software updates. The security of these systems depends on the assumption that solving certain mathematical problems requires extremely large computational effort on classical computers.

For example, the **RSA cryptosystem** depends on the difficulty of factoring very large integers into their prime factors. When RSA keys are generated, two large prime numbers are multiplied together to create a public modulus. While multiplying two numbers is easy, reversing the process—finding the original prime numbers from the product—is computationally difficult for classical machines when the numbers are large enough. Because of this difficulty, RSA has been widely trusted for decades.

Similarly, the **Diffie–Hellman key exchange protocol** depends on the discrete logarithm problem. In this case, computing exponentiation modulo a large prime number is easy, but reversing the operation to determine the original exponent is extremely difficult. This property

allows two communicating parties to establish a shared secret key over an insecure channel.

Another widely used technique is **Elliptic Curve Cryptography (ECC)**. ECC relies on the elliptic curve discrete logarithm problem, which is considered even harder than the traditional discrete logarithm problem for classical computers. Because of this property, ECC can provide the same level of security as RSA but with smaller key sizes, making it suitable for mobile devices, embedded systems, and Internet of Things (IoT) devices.

However, the emergence of quantum computing threatens the security of these classical cryptographic algorithms. Quantum computers use the principles of **quantum mechanics**, including superposition and entanglement, to perform computations in ways that are not possible for classical machines. Instead of processing information in bits that represent either 0 or 1, quantum computers use **qubits**, which can represent both states simultaneously. This allows quantum machines to explore many possible solutions to a problem at the same time.

One of the most significant breakthroughs in quantum algorithms is **Shor's algorithm**, proposed in 1994. This algorithm demonstrates that a sufficiently powerful quantum computer can factor large integers and compute discrete logarithms in polynomial time. In other words, the mathematical problems that currently protect RSA, Diffie-Hellman, and ECC can theoretically be solved efficiently by a quantum computer. If large-scale quantum computers become practical, they could break these widely used encryption systems within a short time.

Another quantum algorithm, known as **Grover's algorithm**, can accelerate brute-force attacks against symmetric cryptographic systems. Although symmetric algorithms such as AES are not completely broken by quantum computing, Grover's algorithm effectively reduces their security strength by roughly half. For example, a 128-bit symmetric key may offer security comparable to a 64-bit key against quantum attackers. As a result, larger key sizes may be required to maintain adequate security.

The potential impact of quantum computing on global cybersecurity infrastructure is therefore significant. Many security protocols used in the internet today rely on public-key cryptography. These include Transport Layer Security (TLS), Virtual Private Networks (VPNs), digital certificate infrastructures, secure software updates, and blockchain systems. If quantum

computers become capable of breaking these algorithms, a large portion of modern digital communication could become vulnerable.

Another important issue related to quantum threats is the concept known as **"harvest now, decrypt later."** In this attack strategy, malicious actors intercept and store encrypted data today, even if they cannot decrypt it immediately. Once powerful quantum computers become available in the future, they can use quantum algorithms to decrypt the previously collected data. This means that information transmitted today may become readable many years later.

This threat is particularly serious for data that must remain confidential for long periods of time. Examples include government documents, military communications, healthcare records, financial information, and intellectual property. In some cases, sensitive information must remain secure for decades. If encrypted data is stored by attackers today, future quantum computing capabilities could compromise that information.

In addition to communication security, quantum threats may also affect digital authentication systems. Many software update mechanisms and identity verification systems rely on digital signatures generated by algorithms such as RSA or ECC. If these signatures become breakable, attackers could forge digital identities or distribute malicious software updates that appear legitimate.

Because of these risks, governments, research institutions, and cybersecurity organizations around the world are actively working on developing cryptographic solutions that can resist quantum attacks. The field of **post-quantum cryptography** focuses on designing algorithms that remain secure even if large-scale quantum computers become available. These algorithms rely on mathematical problems that are believed to be hard for both classical and quantum machines to solve.

Several different approaches have been proposed in PQC research, including lattice-based cryptography, code-based cryptography, multivariate cryptography, and hash-based cryptographic schemes. These approaches are currently being evaluated and standardized to ensure that they provide strong security and practical performance for real-world applications. In summary, the background of quantum threats highlights the urgent need to rethink modern

cryptographic systems. While quantum computers are still in the early stages of development, the potential risks they pose to existing encryption technologies are significant. As a result, transitioning to quantum-resistant cryptographic methods is becoming an important priority for future cybersecurity infrastructure.

FUNDAMENTALS OF POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography (PQC) refers to a class of cryptographic algorithms that are designed to remain secure even in the presence of powerful quantum computers. As quantum computing research continues to progress, many of the cryptographic methods currently used for secure communication may become vulnerable. PQC aims to address this challenge by developing encryption and digital signature schemes that can resist both classical and quantum computational attacks.

Unlike **quantum cryptography**, which uses quantum mechanical properties such as photon transmission and quantum key distribution, PQC does not require specialized quantum hardware. Instead, it is implemented using traditional computing systems and standard digital communication networks. This makes PQC more practical for widespread adoption because it can be integrated into existing infrastructure such as internet protocols, cloud computing systems, and mobile devices.

The primary goal of post-quantum cryptography is to replace or upgrade existing public-key cryptographic algorithms that could be broken by quantum algorithms. Current systems like RSA, Diffie-Hellman, and Elliptic Curve Cryptography rely on mathematical problems that quantum computers can solve efficiently using algorithms such as Shor’s algorithm. PQC introduces new cryptographic methods that are based on different mathematical problems believed to remain difficult even for quantum computers.

One important aspect of PQC is that it must maintain **compatibility with existing digital systems**. Since the global internet infrastructure depends heavily on public-key cryptography, replacing these systems requires solutions that can operate efficiently on classical hardware. Therefore, PQC algorithms are designed to run on conventional processors while still providing quantum-resistant security.

Another fundamental requirement of PQC is **long-term security**. Cryptographic systems are often used to protect sensitive information that must remain confidential for many years. For example, financial records, government communications, and medical data require long-term protection. PQC algorithms are designed with the assumption that future adversaries may possess quantum computers, so they must remain secure even under these advanced attack models.

Post-Quantum Cryptography also aims to support the same core cryptographic functions as traditional systems. These functions include secure key exchange, public-key encryption, digital signatures, and authentication. By providing these capabilities, PQC algorithms can serve as direct replacements for existing cryptographic mechanisms in security protocols such as Transport Layer Security (TLS), secure email systems, and blockchain networks.

KEY CHARACTERISTICS OF POST-QUANTUM CRYPTOGRAPHY

Several important characteristics define the design and functionality of PQC algorithms.

Resistance against quantum algorithms

The most essential property of PQC algorithms is their resistance to known quantum attacks. The underlying mathematical problems used in these algorithms must remain computationally hard even when quantum algorithms are applied. Researchers carefully analyze these problems to ensure that no efficient classical or quantum algorithms exist for solving them.

Compatibility with classical computing systems

PQC solutions are designed to operate on traditional digital hardware such as CPUs and microcontrollers. This allows organizations to deploy quantum-resistant cryptography without requiring quantum computers or specialized communication channels.

Scalability for large-scale networks

Modern digital communication systems support billions of users and devices worldwide. PQC algorithms must therefore be capable of scaling efficiently in large networks. This includes handling high volumes of encrypted data, secure connections, and digital signatures without significant performance degradation.

Strong mathematical security assumptions

The security of PQC algorithms depends on well-studied mathematical problems that are believed to be difficult for both classical and quantum computers. Researchers analyze these problems using complexity theory and cryptanalysis to ensure their robustness against potential attacks.

Another important aspect of PQC is **efficiency**. In many cases, PQC algorithms require larger key sizes or produce larger digital signatures compared to traditional cryptographic methods. Therefore, researchers work to optimize these algorithms so they can be used in real-world systems without excessive computational overhead.

Cryptographic Operations in PQC Systems

Post-quantum cryptographic systems typically perform several fundamental operations that are essential for secure communication.

Key generation is the process of creating public and private keys that will be used for encryption and digital signatures. In PQC algorithms, this process often involves complex mathematical structures such as lattices or polynomial equations.

Encryption allows a sender to convert plaintext data into ciphertext using the recipient's public key. Only the corresponding private key can decrypt the message.

Decryption is the process of recovering the original plaintext from encrypted data using the private key.

Digital signatures provide authentication and data integrity. A sender signs a message using a private key, and the receiver verifies the signature using the public key. This ensures that the message has not been altered and that it comes from a legitimate source.

Classification of Post-Quantum Cryptographic Algorithms

PQC algorithms are generally classified based on the mathematical problems on which their security is based. These mathematical foundations determine how the algorithm operates and how resistant it is to quantum attacks.

Some of the major categories of PQC algorithms include lattice-based cryptography, code-based cryptography, hash-based cryptography, multivariate cryptography, and isogeny-based cryptography. Each category has its own advantages and limitations in terms of security, efficiency, and implementation complexity.

For example, lattice-based cryptography is currently one of the most promising PQC approaches because it offers strong security proofs and relatively efficient implementations. Code-based cryptography has a long history of research and is considered highly secure, although it may require very large public keys. Hash-based cryptography provides strong security guarantees but can produce large signatures. Multivariate cryptography offers fast signature generation but requires careful analysis to prevent vulnerabilities.

Importance of PQC in Future Cybersecurity

The development of post-quantum cryptography is becoming increasingly important as governments and technology companies prepare for the potential arrival of practical quantum computers. Transitioning to PQC will require updates to many security protocols, hardware devices, and software applications.

Researchers are currently working on optimizing PQC algorithms, improving their performance, and ensuring that they can be integrated smoothly into existing digital infrastructures. International standardization efforts are also underway to identify the most reliable and secure algorithms for global deployment.

In summary, the fundamentals of post-quantum cryptography focus on designing secure cryptographic methods that can withstand the computational capabilities of future quantum computers while remaining practical for use in current computing environments. PQC is expected to become a key component of next-generation cybersecurity systems, ensuring that digital communication remains secure even in the quantum era.

TYPES OF POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

1. Lattice-Based Cryptography

Lattice-based cryptography is currently considered one of the most promising approaches for post-quantum security. It relies on mathematical problems related to lattice structures in high-

dimensional spaces, which are extremely difficult to solve even with quantum computers. Common problems used in lattice-based cryptography include:

- Learning With Errors (LWE)
- Ring-LWE
- Short Integer Solution (SIS)

Several PQC algorithms are based on these lattice problems. Lattice-based cryptography offers good performance and relatively efficient implementations.

For example, algorithms such as CRYSTALS-Kyber and CRYSTALS-Dilithium are based on lattice structures and provide strong security and efficient operations.

2. Code-Based Cryptography

Code-based cryptography relies on error-correcting codes for encryption. The security of these systems depends on the difficulty of decoding random linear codes.

One of the earliest examples of code-based cryptography is the McEliece cryptosystem. Although it was proposed decades ago, it remains resistant to both classical and quantum attacks.

Advantages of code-based cryptography include strong security and long research history. However, the main disadvantage is the very large public key size, which can make implementation challenging in resource-constrained environments.

3. Hash-Based Cryptography

Hash-based cryptography uses cryptographic hash functions to construct digital signature schemes. These algorithms are considered highly secure because their security depends only on the collision resistance of hash functions.

SPHINCS+ is an example of a stateless hash-based signature scheme designed for post-quantum security. Hash-based signatures are simple and well-understood but sometimes produce larger signatures compared to other methods.

4. Multivariate Cryptography

Multivariate cryptographic systems are based on solving systems of multivariate polynomial equations over finite fields. These mathematical problems are believed to be computationally hard even for quantum computers.

Multivariate cryptography can offer fast signature generation and verification. However, some candidate algorithms have been broken during security evaluations, which shows the importance of thorough cryptanalysis.

5. Isogeny-Based Cryptography

Isogeny-based cryptography uses mathematical structures related to elliptic curve isogenies. These systems are relatively new and have attracted research interest because they produce smaller key sizes.

However, some isogeny-based algorithms have been broken recently, indicating that more research is needed before they can be widely adopted.

NIST STANDARDIZATION OF POST-QUANTUM CRYPTOGRAPHY

The National Institute of Standards and Technology (NIST) initiated a global effort to standardize PQC algorithms. After several rounds of evaluation and cryptanalysis, NIST selected a set of algorithms that provide strong quantum-resistant security.

The selected algorithms include:

- CRYSTALS-Kyber
- CRYSTALS-Dilithium
- SPHINCS+
- FALCON

These algorithms address key cryptographic functions such as encryption and digital signatures.

CRYSTALS-Kyber is designed for key encapsulation and secure key exchange, while CRYSTALS-Dilithium is used for digital signatures. SPHINCS+ provides a hash-based signature alternative, and FALCON offers another efficient signature scheme.

These algorithms were later standardized as federal security standards, including ML-KEM and ML-DSA, representing lattice-based encryption and digital signature mechanisms.

The standardization process is an important milestone toward deploying quantum-safe cryptography in real-world systems.

ARCHITECTURE OF A POST-QUANTUM CRYPTOGRAPHIC SYSTEM

A typical PQC-based security system consists of multiple layers that work together to protect digital communication.

1. Data Layer

The data layer stores and manages sensitive information that requires encryption and protection. This layer includes databases, communication logs, and digital records.

2. Cryptographic Algorithm Layer

This layer implements PQC algorithms such as lattice-based encryption and hash-based digital signatures.

The cryptographic operations performed in this layer include:

- Key generation
- Encryption
- Decryption
- Digital signatures
- Signature verification

3. Security Management Layer

This layer manages key distribution, authentication mechanisms, and policy enforcement. It ensures that cryptographic keys are securely generated and exchanged between communicating parties.

4. Application Layer

The application layer integrates PQC algorithms with real-world applications such as:

- Secure web communication
- Cloud computing platforms
- Blockchain systems
- Internet of Things (IoT) networks

COMPARISON OF MAJOR PQC ALGORITHMS

Table: 1

Algorithm	Category	Primary Function	Advantages	Limitations
CRYSTALS-Kyber	Lattice-based	Encryption	Fast performance and smaller keys	Moderate complexity
CRYSTALS-Dilithium	Lattice-based	Digital Signature	Strong security and efficient implementation	Larger signature sizes
SPHINCS+	Hash-based	Digital Signature	Very strong theoretical security	Large signatures
FALCON	Lattice-based	Digital Signature	Compact signatures	Complex implementation

These algorithms were selected after extensive evaluation of security, performance, and implementation feasibility.

APPLICATIONS OF POST-QUANTUM CRYPTOGRAPHY

1. Secure Internet Communication

PQC can be integrated into internet protocols such as TLS to secure web communication against future quantum attacks.

2. Cloud Security

Cloud service providers store large volumes of sensitive data. PQC can ensure long-term confidentiality of stored information.

3. Blockchain and Cryptocurrency

Blockchain systems rely heavily on cryptographic signatures. PQC algorithms can provide quantum-resistant authentication mechanisms for future blockchain platforms.

4. Internet of Things (IoT)

IoT devices often have limited computational resources. Implementing lightweight PQC algorithms can help secure IoT networks.

5. Government and Defense Systems

Government communication networks require extremely high levels of security. PQC will play an important role in protecting national infrastructure from future quantum threats.

CHALLENGES IN IMPLEMENTING PQC

Although PQC offers strong security advantages, its implementation introduces several challenges.

1. **Large Key Sizes**

Many PQC algorithms require larger public keys and signatures compared to traditional cryptography.

2. **Performance Overhead**

Some PQC algorithms require higher computational resources, which may affect system performance.

3. **Migration Complexity**

Transitioning from classical cryptography to PQC requires updating software, hardware, and communication protocols.

4. **Standardization and Interoperability**

Different organizations may adopt different PQC algorithms, which may create compatibility issues.

Despite these challenges, research continues to improve PQC efficiency and scalability.

FUTURE RESEARCH DIRECTIONS

Future research in post-quantum cryptography will focus on improving algorithm efficiency, reducing key sizes, and developing hybrid cryptographic systems.

Some promising research directions include:

- Hybrid classical and PQC encryption systems
- Hardware acceleration for PQC algorithms
- Lightweight PQC for IoT devices
- Integration with blockchain and distributed systems
- Development of quantum-secure authentication protocols

As quantum-computing technology continues to evolve, PQC research will remain an active and important field.

CONCLUSION

Post-Quantum Cryptography is becoming increasingly important as the world moves closer to practical quantum computing. Traditional cryptographic algorithms such as RSA and ECC are vulnerable to quantum algorithms that can efficiently solve their underlying mathematical problems. Therefore, there is a strong need for cryptographic techniques that can resist attacks from both classical and quantum computers.

This paper discussed the fundamental concepts, algorithms, architecture, and applications of PQC. Various approaches including lattice-based, code-based, hash-based, and multivariate cryptography were examined. The role of international standardization efforts, particularly by NIST, was also highlighted.

Although PQC introduces challenges such as large key sizes and implementation complexity, ongoing research is addressing these issues. With proper standardization and deployment strategies, PQC can provide a robust foundation for securing future digital communication systems.

In conclusion, post-quantum cryptography will be a critical component of next-generation cybersecurity infrastructure and will ensure the confidentiality, integrity, and authenticity of digital information in the quantum-computing era.

REFERENCES

1. Bernstein, D., Buchmann, J., & Dahmen, E. (2009). *Post-Quantum Cryptography*. Springer.
2. Chen, L., et al. (2016). Report on Post-Quantum Cryptography. NIST.
3. Shor, P. (1994). Algorithms for Quantum Computation: Discrete Logarithms and Factoring.
4. National Institute of Standards and Technology. Post-Quantum Cryptography Standardization.
5. NIST PQC Algorithm Announcement.
6. Post-Quantum Cryptography Standards Overview.
7. Demir, E., Bilgin, B., & Onbasli, M. (2025). Performance Analysis of PQC Algorithms.
8. Chen, A. C. H. (2024). Post-Quantum Cryptography Anonymous Scheme.

9. Dong, B., Feng, H., & Wang, Q. (2025). Optimization of HQC for PQC Systems.
10. TechRadar. Cyber resilience in the post-quantum era.

Cite as:

Raman S. Patil, Kanika N. Deshmukh (2026). Post-Quantum Cryptography. Journal of Computer, Internet and Network Security. 11(1), 31-46.

https//doi.org/10.5281/zenodo.19281439