5.3 POST-QUANTUM CRYPTOGRAPHY (PQC)

Introduction to Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to protect information against attacks from both classical computers and powerful quantum computers.

Traditional cryptographic algorithms such as RSA, ECC (Elliptic Curve Cryptography), and Diffie–Hellman rely on mathematical problems that are difficult for classical computers to solve. However, quantum algorithms, particularly Shor's Algorithm, can solve certain mathematical problems efficiently, threatening the security of these cryptographic systems.

Therefore, PQC develops new mathematical algorithms that are believed to remain secure even against quantum computer attacks.

Definition: Post-Quantum Cryptography is the study and development of cryptographic algorithms that are resistant to attacks from quantum computers while operating on classical computing devices.

Need for Post-Quantum Cryptography

Quantum computers use quantum mechanical principles such as superposition and entanglement to solve certain computational problems faster than classical computers.

The major reasons for developing PQC are:

1. Threat to RSA: Shor's algorithm can factor large integers efficiently, threatening RSA encryption.
2. Threat to ECC: Shor's algorithm can solve the discrete logarithm problem, threatening elliptic curve cryptography.
3. Data Confidentiality: Sensitive information must remain secure even in the quantum computing era.
4. Long-Term Security: Data encrypted today may be stored and decrypted in the future using quantum computers.
5. Secure Communication: PQC helps protect banking, healthcare, government and cloud communication systems.

Classical Cryptography vs Post-Quantum Cryptography

Classical Cryptography	Post-Quantum Cryptography
Uses conventional cryptographic algorithms.	Uses quantum-resistant mathematical algorithms.
RSA and ECC are commonly used.	Lattice-based, hash-based and code-based algorithms are used.
RSA and ECC are vulnerable to sufficiently powerful quantum computers.	Designed to resist known quantum attacks.

Relies on integer factorization and discrete logarithms.	Relies on alternative mathematical problems.
Used in traditional secure communication.	Used for future quantum-resistant communication.

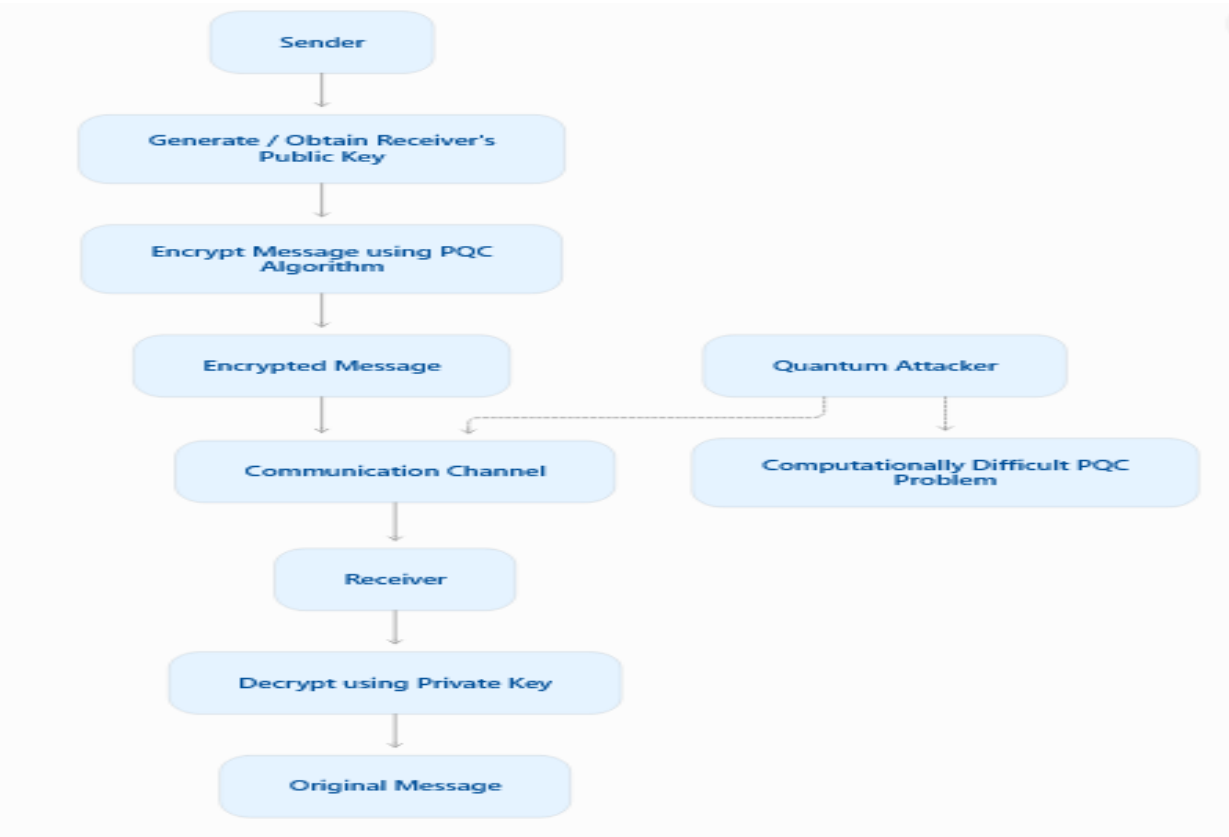
Working Principle of Post-Quantum Cryptography

PQC works similarly to classical public-key cryptography but uses mathematical problems that are considered difficult for both classical and quantum computers.

Steps involved:

1. Key Generation: The sender and receiver generate public and private keys using a post-quantum cryptographic algorithm.
2. Encryption: The sender uses the receiver's public key to encrypt the message.
3. Transmission: The encrypted message is transmitted through a communication channel.
4. Decryption: The receiver uses the corresponding private key to decrypt the message.
5. Security: Even if an attacker uses a quantum computer, the underlying mathematical problem is designed to remain computationally difficult.

Diagram 1: Working of Post-Quantum Cryptography



- The sender encrypts the original message using a PQC algorithm.
- The encrypted message travels through an insecure communication channel.
- The receiver decrypts it using the corresponding private key.
- An attacker attempting to break the encryption faces a difficult mathematical problem, even when using a quantum computer.

Types of Post-Quantum Cryptography

Post-Quantum Cryptography uses different mathematical approaches to provide security.

5.1 Lattice-Based Cryptography

Definition: Lattice-based cryptography is a cryptographic technique that uses mathematical structures called lattices to provide security against classical and quantum attacks.

Lattice: A lattice is a regular arrangement of points in a multidimensional space formed by integer combinations of basis vectors.

Important mathematical problems:

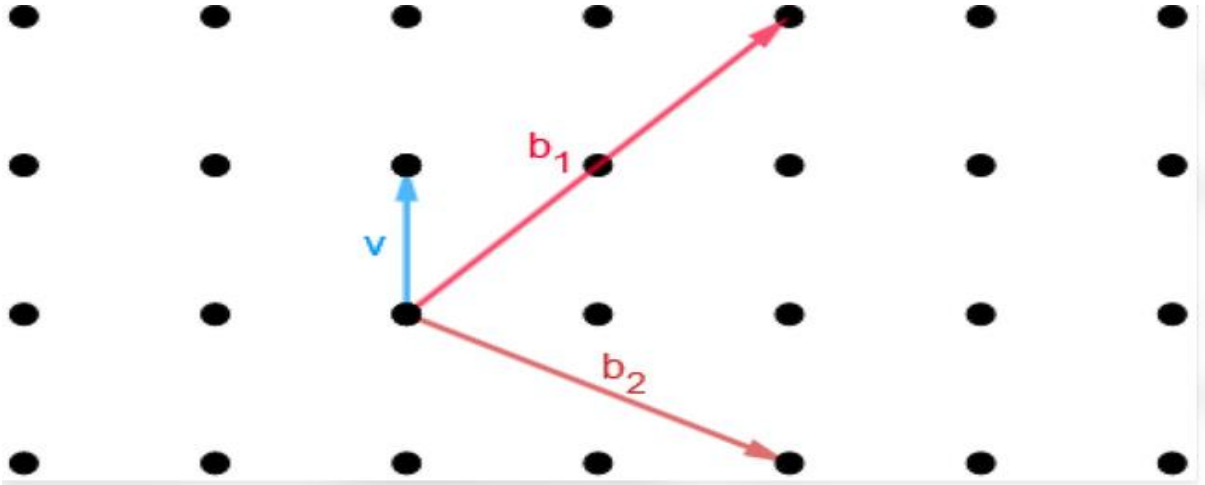
- Shortest Vector Problem (SVP)
- Closest Vector Problem (CVP)
- Learning With Errors (LWE)
- Module Learning With Errors (Module-LWE)

Working Principle:

1. A lattice structure is generated using mathematical basis vectors.
2. Public and private keys are generated from lattice-related mathematical problems.
3. The sender uses the public key to encrypt or encapsulate a secret.
4. The receiver uses the private key to recover the secret.

Examples:

- CRYSTALS-Kyber (now standardized as ML-KEM)
- CRYSTALS-Dilithium (now standardized as ML-DSA)



Applications: Secure key exchange, digital signatures, secure communication and cloud security.

5.2 Hash-Based Cryptography

Definition: Hash-based cryptography uses cryptographic hash functions to construct secure digital signatures.

A hash function converts an input message of any length into a fixed-length hash value.

Important concepts:

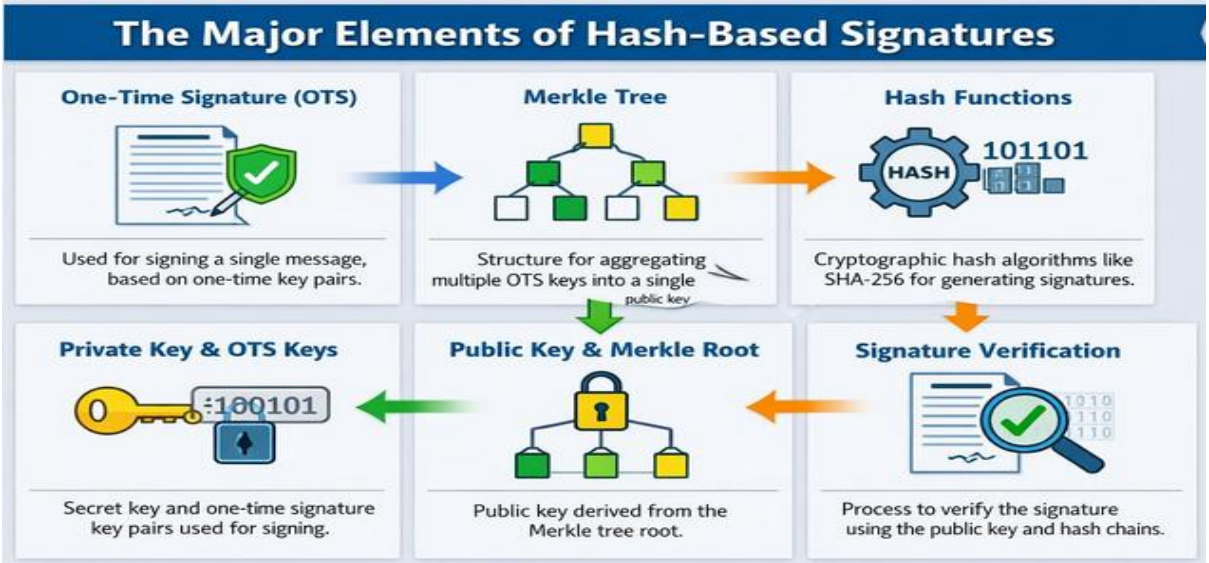
- Cryptographic Hash Functions
- One-Way Functions
- Collision Resistance
- Merkle Trees
- Digital Signatures

Working Principle:

1. The original message is passed through a hash function.
2. A fixed-length hash value is generated.
3. The hash-based signature scheme uses secret values to generate a digital signature.
4. The receiver verifies the signature using the corresponding public verification key.

Examples:

- SPHINCS+ (standardized as SLH-DSA)
- XMSS
- LMS



Applications: Software authentication, firmware verification, secure document signing and digital certificates.

5.3 Code-Based Cryptography

Definition: Code-based cryptography is a cryptographic technique that uses error-correcting codes and the difficulty of decoding a randomly generated linear code.

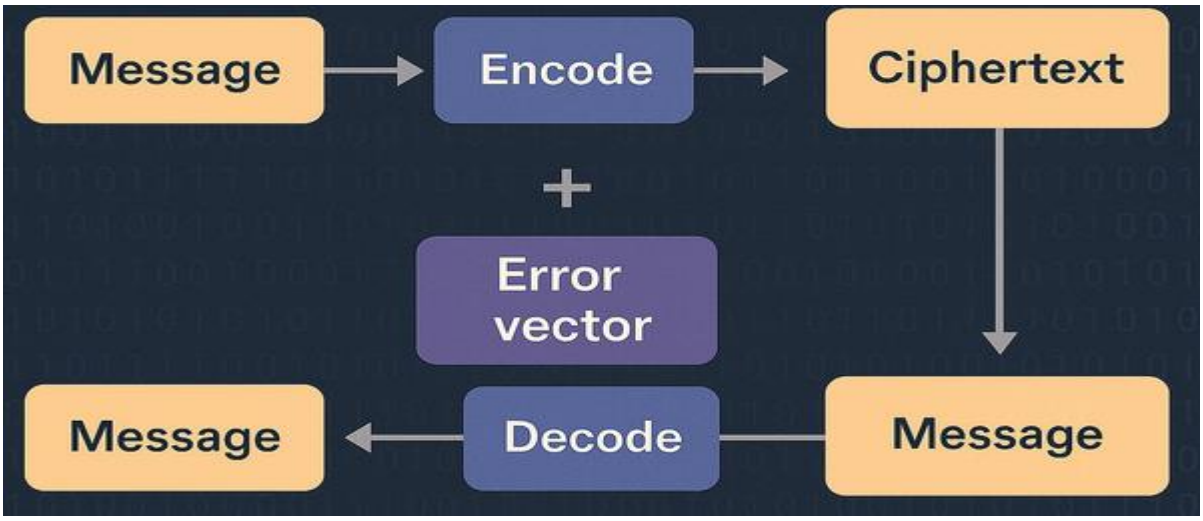
Important concepts:

- Error-Correcting Codes
- Linear Codes
- Syndrome Decoding Problem
- Generator Matrix
- Parity-Check Matrix

Working Principle:

1. A mathematical error-correcting code is generated.
2. Public and private keys are created based on the code.
3. The sender encrypts the message by introducing controlled errors.
4. The receiver uses the private key to correct the errors and recover the original message.

Example: McEliece Cryptosystem.



Applications: Secure communication, encryption and long-term data protection.

5.4 Multivariate Polynomial Cryptography

Definition: Multivariate polynomial cryptography uses systems of nonlinear polynomial equations over finite fields to construct cryptographic algorithms.

Important concepts:

- Multivariate Polynomial Equations
- Finite Fields
- Public and Private Keys
- Polynomial Mapping
- Multivariate Quadratic Problems

Working Principle:

1. A system of multivariate polynomial equations is generated.
2. The public key contains a set of polynomial equations.
3. The private key contains secret transformations that make solving the equations easier.
4. The receiver uses the private key to perform the required cryptographic operation.

Standardized Post-Quantum Cryptographic Algorithms

The following algorithms are important examples of post-quantum cryptography.

Algorithm	**Cryptographic technique**	**Purpose**
ML-KEM (Kyber)	Lattice-based	Secure key establishment
ML-DSA (Dilithium)	Lattice-based	Digital signatures
SLH-DSA (SPHINCS+)	Hash-based	Digital signatures

Classic McEliece	Code-based	Public-key encryption / key establishment

Important: ML-KEM, ML-DSA and SLH-DSA are NIST-standardized post-quantum algorithms.

Applications of Post-Quantum Cryptography

1. Banking and Finance: Protects online banking, financial transactions and sensitive customer information.
2. Healthcare: Secures electronic health records and medical data.
3. Government Communication: Protects confidential government information and military communication.
4. Cloud Computing: Provides quantum-resistant protection for cloud-stored data.
5. Internet Security: Protects secure websites, communication and network connections.
6. Digital Signatures: Provides authentication and integrity verification for digital documents.
7. IoT Security: Helps protect connected devices and smart systems.

Advantages of Post-Quantum Cryptography

1. Provides protection against known quantum computing attacks.
2. Supports secure communication in the quantum computing era.
3. Protects sensitive information for long periods.
4. Can be implemented on classical computers.
5. Supports digital signatures and secure key establishment.
6. Helps organizations migrate towards quantum-resistant security.

Challenges of Post-Quantum Cryptography

1. Large Key Sizes: Some PQC algorithms require larger public keys and signatures.
2. Performance: Certain algorithms require more memory and computational resources.
3. Implementation Complexity: Implementing and maintaining PQC algorithms requires specialized knowledge.
4. Compatibility: Existing systems may require modifications to support PQC.
5. Migration: Replacing traditional cryptographic systems with PQC requires time and planning.
6. Long-Term Security: New algorithms require continuous security analysis and testing.

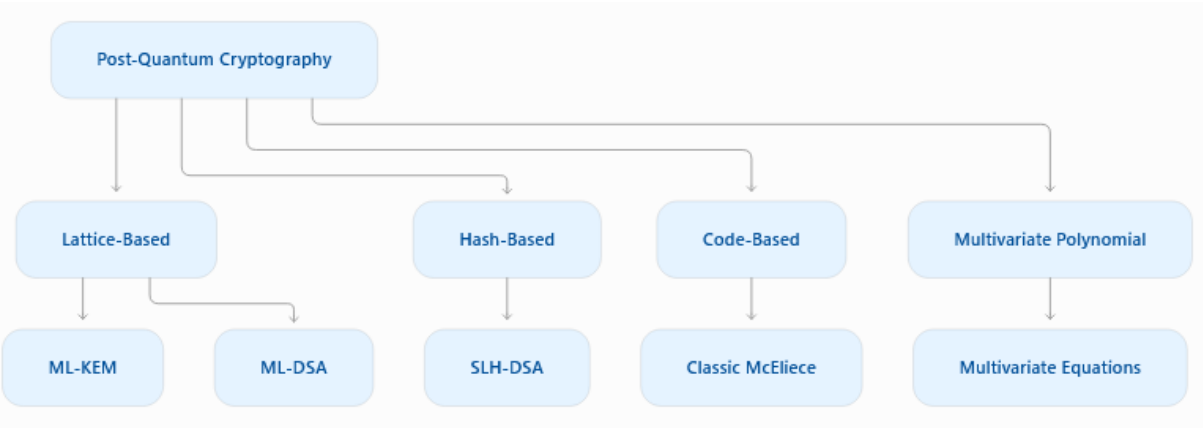
Classical Cryptography vs Post-Quantum Cryptography – Overall Comparison

Parameter	**Classical Cryptography**	**Post-Quantum Cryptography**
Security basis	Traditional mathematical problems	Quantum-resistant mathematical problems
Quantum resistance	RSA and ECC are vulnerable	Designed to resist known quantum attacks
Algorithms	RSA, ECC, AES	ML-KEM, ML-DSA, SLH-DSA
Computing platform	Classical computers	Classical computers

Key size	Generally smaller for RSA/ECC public keys	Often larger, depending on algorithm
Future security	Requires migration for quantum threats	Designed for the quantum era

Overall Architecture of Post-Quantum Cryptography

Diagram 2: Classification of PQC



Post-Quantum Cryptography is an important development in modern information security. It aims to protect communication and sensitive information from attacks performed using powerful quantum computers. It uses mathematical techniques such as lattice-based, hash-based, code-based and multivariate polynomial cryptography. Algorithms such as ML-KEM, ML-DSA and SLH-DSA provide standardized approaches for quantum-resistant key establishment and digital signatures. PQC plays an important role in developing secure communication systems for the future.