Post-Quantum Security: Comprehensive Study Notes

Table of Contents

Introduction and Overview

Post-Quantum Security represents one of the most critical challenges in modern cryptography. As quantum computers advance, they pose an existential threat to current public-key cryptographic systems that secure our digital infrastructure.

Current Cryptographic Landscape

Basic Cryptographic Primitives:

- **Integrity**: Hash functions (SHA-1, MD5, SHA-2, SHA-3)
- **Authenticity**: MACs and digital signatures (HMAC, RSA, DSA, ECDSA)
- **Confidentiality**: Symmetric-key encryption (SKE) and Public-key encryption (PKE/KEX/KEM)
  - Examples: DES, AES, Diffie-Hellman, ECDH, ECIES, ElGamal, RSA

Public-Key Cryptography Fundamentals

Public-key cryptography relies on two mathematically related keys:

- **Public key (pk)** and **Private key (sk)**
- **Encryption**: c = ENC(pk, m) → m = DEC(sk, c)
- **Signatures**: s = SIG(sk, m) → VER(pk, s, m) = 1

Core Security Assumptions:

- Given pk, it must be computationally infeasible to compute sk

- Based on mathematical problems believed to be hard:
  - **Integer factorization** (RSA)
  - **Discrete logarithm problem** (DH, DSA)
  - **Elliptic curve discrete logarithm** (ECDH, ECDSA)

The Quantum Threat to Cryptography

Shor's Algorithm (1994)

Revolutionary Impact:

- Factors an integer N in time $\tilde{O}(\log^3 N)$
- Computes discrete logarithm in a group of size N in time $\tilde{O}(\log^3 N)$
- **Completely breaks** current public-key cryptography

Affected Systems:

- RSA encryption/signature
- Diffie-Hellman key exchange
- Elliptic Curve Cryptography (ECC)
- All protocols dependent on these: Kerberos, IPSec, TLS, SSH, PGP, S/MIME

Grover's Algorithm (1996)

Effect on Symmetric Cryptography:

- Searches unsorted database of size N in time $O(\sqrt{N})$
- Proven optimal with lower bound $\Omega(\sqrt{N})$
- **Weakens but doesn't break** symmetric encryption
- **Mitigation**: Double key sizes (AES-128 → AES-256)

Quantum Threat Timeline

Expert Consensus (2021 Global Risk Institute Report):

- **High probability**: Quantum computers can break RSA-2048 within 24 hours in the next 25-30 years
- **Migration urgency**: Data encrypted today could be vulnerable in the future
- **"Harvest now, decrypt later"** attacks are a real concern

Critical Timeline Factors:

- **Migration time**: Time needed to transition to post-quantum systems
- **Shelf-life**: How long encrypted data must remain secure
- **Threat emergence**: When quantum computers become capable

---

Post-Quantum Cryptography Foundations

Definition and Requirements

Post-Quantum Cryptography (PQC):

- Cryptographic algorithms believed secure against both classical and quantum computers
- Can be efficiently implemented on classical computers
- Based on alternative mathematical foundations

Mathematical Foundations

1. Lattice-Based Cryptography

Core Problem: Learning with Errors (LWE) - Regev, 2005

- **Advantages**: Efficient, versatile, strong security proofs
- **Applications**: Encryption, signatures, advanced protocols
- **Key algorithms**: CRYSTALS-Kyber, CRYSTALS-Dilithium, NTRU

2. Code-Based Cryptography

Core Problem: Decoding linear codes - McEliece, Berlekamp et al., 1978

- **Advantages**: Long-standing security, well-understood
- **Disadvantages**: Large key sizes
- **Key algorithms**: Classic McEliece, HQC, BIKE

3. Multivariate Cryptography

Core Problem: Solving systems of multivariate polynomial equations

- **Advantages**: Fast signatures
- **Disadvantages**: Large key sizes, some recent attacks
- **Key algorithms**: Rainbow (broken), GeMSS, LUOV

4. Isogeny-Based Cryptography

Core Problem: Finding isogenies between elliptic curves

- **Status**: Severely weakened by recent attacks (2022)
- **Key algorithms**: SIDH/SIKE (broken), CSIDH (questionable)

5. Hash-Based Signatures

Core Problem: One-way functions and hash functions

- **Advantages**: Minimal assumptions, high security confidence
- **Disadvantages**: Stateful (traditional), large signatures
- **Key algorithms**: SPHINCS+, XMSS, LMS

NIST Standardization Process

Timeline and Phases

Project Launch: February 2016

- **Goal**: Standardize post-quantum algorithms for long-term security

Round 1 (November 2017):

- 82 submissions, 69 eligible
- 25 algorithms broken during evaluation

Round 2 (January 2019):

- 26 proposals advanced
- 8 additional algorithms broken

Round 3 (July 2020):

- **7 finalists**: Most promising algorithms
- **8 alternates**: Backup candidates

Final Selection (July 2022):

- Winners announced

Standards Release (August 2024):

- Final FIPS standards published

Round 3 Evaluation

Finalists (Key Exchange/Encryption)

- **CRYSTALS-Kyber**: Lattice-based, excellent performance
- **NTRU**: Lattice-based, alternative to Kyber
- **SABER**: Lattice-based, efficient implementation
- **Classic McEliece**: Code-based, large keys but mature

Finalists (Digital Signatures)

- **CRYSTALS-Dilithium**: Lattice-based, good balance
- **FALCON**: Lattice-based, compact signatures
- **Rainbow**: Multivariate, BROKEN by Beullens (2022)

Alternates

- **SPHINCS+**: Hash-based, high security confidence
- **Picnic**: Zero-knowledge proofs, innovative approach

Current Standards and Algorithms

NIST FIPS Standards (2024)

FIPS 203: ML-KEM (Module-Lattice Key Encapsulation Mechanism)

- **Based on**: CRYSTALS-Kyber
- **Purpose**: General encryption and key exchange
- **Security levels**: ML-KEM-512, ML-KEM-768, ML-KEM-1024
- **Status**: Primary standard for post-quantum encryption

FIPS 204: ML-DSA (Module-Lattice Digital Signature Algorithm)

- **Based on**: CRYSTALS-Dilithium
- **Purpose**: General digital signatures
- **Security levels**: ML-DSA-44, ML-DSA-65, ML-DSA-87
- **Status**: Primary standard for post-quantum signatures

FIPS 205: SLH-DSA (Stateless Hash-based Digital Signature Algorithm)

- **Based on**: SPHINCS+
- **Purpose**: High-assurance digital signatures
- **Advantages**: Minimal security assumptions
- **Status**: Conservative backup for signatures

FIPS 206: FN-DSA (FALCON Digital Signature Algorithm)

- **Based on**: FALCON
- **Purpose**: Compact digital signatures
- **Advantages**: Smaller signature sizes
- **Status**: Specialized applications requiring compact signatures

Round 4 and Future Directions

Ongoing Efforts:

- Additional signature algorithms (non-lattice-based)
- Alternative key exchange mechanisms
- Improved efficiency and security analysis

Migration Challenges

Technical Challenges

Algorithm Integration

- **Larger key sizes**: Most PQC algorithms have larger keys than current systems
- **Performance considerations**: Some algorithms are slower than current methods
- **Hybrid approaches**: Combining classical and post-quantum algorithms during transition

Protocol Updates

- **TLS/SSL**: Updating handshake protocols
- **PKI infrastructure**: Certificate authority systems
- **Embedded systems**: Resource-constrained devices

Strategic Considerations

Timing

- **Early adoption**: Risk of choosing eventually broken algorithms

- **Late adoption**: Risk of quantum computer emergence
- **Hybrid period**: Running both classical and post-quantum systems

Crypto-Agility

- **Design principle**: Systems should be able to quickly switch cryptographic algorithms
- **Implementation**: Modular cryptographic libraries
- **Testing**: Ensuring new algorithms work in existing systems

---

Practice Questions and Answers

Conceptual Questions

Q1: Why is RSA insecure against quantum computers? A1: Shor's algorithm allows efficient factoring of large integers in polynomial time, which is the mathematical foundation of RSA security. Classical computers require exponential time for factoring, but quantum computers can do it in $\tilde{O}(\log^3 N)$ time.

Q2: How does Grover's algorithm affect symmetric encryption? A2: Grover's algorithm reduces brute-force search time from O(n) to O(√n), effectively halving the security level. This means AES-256 provides only 128-bit security against quantum attacks, requiring larger key sizes for equivalent protection.

Q3: Which PQC approach is best for digital signatures with small size? A3: FALCON (now FN-DSA) offers the most compact signatures among practical post-quantum signature schemes, though CRYSTALS-Dilithium (ML-DSA) provides a good balance between size and performance.

Q4: Why is SPHINCS+ unique among signature schemes? A4: SPHINCS+ is based only on hash functions and makes minimal cryptographic assumptions. It's stateless and doesn't rely on structured mathematical problems, providing high confidence in post-quantum security.

Q5: What does the "shelf-life vs migration" timeline warn about? A5: Data encrypted today may be vulnerable if quantum computers emerge before migration to post-quantum systems is complete. This creates a window of vulnerability where previously secure data can be decrypted.

Multiple Choice Questions

Q1: Which quantum algorithm breaks RSA? a) Grover b) Shor ✅ c) AES d) BB84

Q2: Which post-quantum algorithm is hash-based? a) Dilithium b) Kyber c) SPHINCS+ ✅ d) McEliece

Q3: Which key exchange method is part of ML-KEM? a) FALCON b) Kyber ✅ c) RSA d) SIDH

Fill-in-the-Blanks

Q1: Shor's algorithm can break RSA by _______ large integers. **A1**: **factoring**

Q2: Grover's algorithm weakens symmetric-key crypto by reducing search time to _____. **A2**: **√n**

Q3: NIST selected CRYSTALS-Kyber as the basis for the _______ standard. **A3**: **ML-KEM**

Short Answer Questions

Q1: Why are lattice problems promising for PQC? A1: Lattice problems are believed to be hard even for quantum computers, offer efficient implementation, support diverse cryptographic constructions, and have strong security proofs connecting them to worst-case hardness assumptions.

Q2: How does SPHINCS+ avoid structural attacks? A2: SPHINCS+ uses only hash functions and avoids structured mathematical problems. It's stateless and resistant to structure-specific attacks that have affected other post-quantum schemes.

Q3: What makes quantum-safe migration urgent? A3: The "harvest now, decrypt later" threat means adversaries can collect encrypted data today and decrypt it when quantum computers become available, making immediate migration to post-quantum systems critical for long-term data protection.

Key Takeaways

Critical Points

1. **Quantum computers pose an existential threat** to current public-key cryptography
2. **Shor's algorithm breaks RSA, DH, and ECC** completely
3. **Grover's algorithm weakens symmetric crypto** but doesn't break it
4. **Post-quantum cryptography is essential** for future security
5. **NIST has standardized four algorithms** (ML-KEM, ML-DSA, SLH-DSA, FN-DSA)

Implementation Priorities

1. **Begin migration planning** immediately
2. **Implement crypto-agility** in new systems
3. **Consider hybrid approaches** during transition
4. **Focus on NIST standards** for mainstream adoption
5. **Prepare for larger key sizes** and performance impacts

Future Considerations

1. **Continued research** into new post-quantum approaches

2. **Analysis of standardized algorithms** for potential weaknesses
3. **Development of more efficient implementations**
4. **Integration with existing protocols and systems**
5. **Addressing the fundamental theoretical questions** about computational complexity

---

Note: This field is rapidly evolving. Stay updated with the latest research and NIST recommendations for current best practices.