Quantum-Resistant Cryptographic Algorithms

Created by Mehrnoush

- **Lattice-Based Cryptography**
  - Concept
    - Relies on the hardness of mathematical problems in lattice structures, such as:
      - **Shortest Vector Problem (SVP)**
      - **Learning With Errors (LWE) problem**
  - Features
    - Offers **strong security proofs** with worst-case to average-case reductions.
    - Supports advanced functionalities like f**ully homomorphic encryption.**
    - Provides **efficient and practical implementations.**
    - Security is based on **well-studied mathematical problems.**
  - Examples
    - **NTRUEncrypt**
    - **CRYSTALS-Kyber**
    - **CRYSTALS-Dilithium**
    - **FALCON**
  - Standardized by NIST
    - CRYSTALS-Kyber
      - CRYSTALS-Kyber (Standardized as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) in FIPS 203)
      - An IND-CCA2-secure Key Encapsulation Mechanism (KEM).
      - Security based on the hardness of solving the **LWE problem over module lattices**.
      - Parameter Sets and Security Levels:
        - ML-KEM-512: 128 bits (Security Category 1)
        - ML-KEM-768: 192 bits (Security Category 3)
        - ML-KEM-1024: 256 bits (Security Category 5)
      - Industry Adoption:
        - Cloudflare integrated Kyber into CIRCL (Cloudflare Interoperable Reusable Cryptographic Library).
        - Amazon AWS supports hybrid modes involving Kyber in their Key Management Service (KMS).
        - IBM introduced the "World's First Quantum Computing Safe Tape Drive" using Kyber and Dilithium.
    - CRYSTALS-Dilithium
      - **A digital signature scheme** secure under chosen message attacks.
      - Based on the hardness of lattice problems over module lattices.
      - Parameter Sets and Security Levels:
        - ML-DSA-44: 128 bits (Security Category 2)
        - ML-DSA-65: 192 bits (Security Category 3)
        - ML-DSA-87: 256 bits (Security Category 5)
      - Balances **security**, **efficiency**, and **key/signature sizes**.
    - FALCON
      - NIST plans to develop a FIPS that specifies a digital signature algorithm derived from FALCON.
      - Will provide an additional alternative for lattice-based digital signatures.
      - FALCON offers compact signatures and keys with high efficiency.
- **Code-Based Cryptography**
  - Concept
    - Based on the difficulty of decoding **general linear codes**, a problem hard even for quantum computers.
  - Features
    - Established security with a history dating back to the 1970s.
    - Typically results in **large public key sizes**.
    - Offers fast **encryption** and **decryption** operations.
    - Less practical for some applications due to key size.
  - Examples
    - McEliece cryptosystem.
      - Uses **binary Goppa codes**.
      - Strong security but **impractical key sizes**.
    - Classic McEliece
      - Selected as an alternate candidate in NIST's PQC standardization process.
- **Hash-Based Signatures**
  - Concept
    - Utilizes **cryptographic hash functions** to create digital signatures.
    - Two types:
      - **Stateful** Schemes: Require state management (e.g., **XMSS**, **LMS**).
      - **Stateless** Schemes: Do not require state (e.g., **SPHINCS+**).
  - Features
    - **Simple and robust security**, relying only on hash function properties.
    - **Large signature sizes** compared to classical schemes.
    - **Key management** can be complex for stateful schemes.
    - **Stateless schemes** are preferable when state management is challenging.
  - Examples
    - **Merkle Signature Scheme (MSS)**
    - **Leighton-Micali Signature (LMS)**
    - **SPHINCS+**
  - Standardized by NIST
    - **SPHINCS+** (Standardized as **Stateless** Hash-Based Digital Signature Algorithm (SLH-DSA) in FIPS 205)
      - A stateless hash-based digital signature scheme.
      - Provides strong security with minimal assumptions.
      - Parameter Sets and Security Levels:
        - SLH-DSA-SHA2-128[s/f], SLH-DSA-SHAKE-128[s/f]: 128 bits (Security Category 1)
        - SLH-DSA-SHA2-192[s/f], SLH-DSA-SHAKE-192[s/f]: 192 bits (Security Category 3)
        - SLH-DSA-SHA2-256[s/f], SLH-DSA-SHAKE-256[s/f]: 256 bits (Security Category 5)
      - Eliminates the need for state management.
    - **Stateful** Hash-Based Signatures (Specified in NIST SP 800-208)
      - **LMS** (Leighton-Micali Signature) and HSS (Hierarchical Signature System)
        - With SHA-256/192 or SHAKE256/192: 192 bits (Security Category 3)
        - With SHA-256 or SHAKE256: 256 bits (Security Category 5)
      - **XMSS** and **XMSSMT**
        - With SHA-256/192 or SHAKE256/192: 192 bits (Security Category 3)
        - With SHA-256 or SHAKE256: 256 bits (Security Category 5)
      - Note: Require careful state management to ensure security.
- **Multivariate Quadratic Equations**
  - Concept
    - Security based on the difficulty of solving systems of **multivariate quadratic (MQ) equations** over finite fields.
  - Features
    - Offers **efficient computation** in signature generation and verification.
    - Can have **large public key sizes**, affecting practicality.
    - **Security Analysis** is complex due to potential algebraic attacks.
    - Requires careful parameter selection to ensure security.
  - Examples
    - Rainbow scheme.
      - Known for fast operations.
      - Was a candidate in NIST's PQC process but was broken by cryptanalysis in 2022.
    - GeMSS
      - Parameters fell below claimed security levels, raising security concerns.
    - Note: NIST is evaluating other proposed digital signature algorithms through the Additional Signature Round for potential standardization.
- **Supersingular Isogeny-Based Cryptography**
  - Concept
    - Uses mathematical structures called **isogenies between supersingular elliptic curves**.
    - Security relies on the hardness of finding isogenies between such curves.
  - Features
    - Offers **small key sizes**, comparable to classical elliptic curve cryptography.
    - **Computationally intensive**, leading to slower operation speeds.
    - Considered **novel and under active research**.
    - Subject to recent **cryptanalysis breakthroughs.**
  - Examples
    - SIKE (Supersingular Isogeny Key Encapsulation).
      - Was a promising candidate but was broken in 2022 due to successful attacks.
      - Demonstrated vulnerabilities, emphasizing the need for further research.
- **Symmetric Key Approaches**
  - Concept
    - Enhancing existing symmetric algorithms to resist quantum attacks by:
      - **Increasing key sizes.**
      - Using quantum-resistant modes of operation.
  - Features
    - Symmetric algorithms like **AES** remain secure but require **larger key sizes** (e.g., AES-256).
    - **Grover's Algorithm** affects symmetric key security by effectively **halving the key length**.
    - **Key Distribution** remains a challenge since symmetric schemes require a shared secret key.
    - Pros:
      - **Efficient**, well-understood, and widely implemented.
      - Less impacted by quantum attacks compared to asymmetric schemes.
    - Note: NIST does not expect to need to transition away from these standards as part of the PQC migration.
  - Strategies
    - **Double the key size** to mitigate quantum threats (e.g., use AES-256 instead of AES-128).
    - Implement **quantum-resistant hash functions** (e.g., SHA-3 family).