Fact Sheet

Cogito Group

NIST PQC Algorithms

Overview

The **National Institute of Standards and Technology (NIST)** has been working on developing and standardising **Post-Quantum Cryptography (PQC)** algorithms to protect digital communications and data in a future where quantum computers can break traditional cryptographic systems like RSA and ECC. In July 2022, NIST announced the first set of quantum-resistant algorithms selected for standardisation, ensuring long-term security in the quantum era.

This factsheet covers the final algorithms chosen by NIST and their implications.

The Quantum Threat to Classical Cryptography

- **Quantum Computing:** Quantum computers, when fully developed, will be capable of solving problems that classical computers cannot, such as breaking widely-used public-key cryptography like RSA and ECC.
- **Cryptography at Risk:** RSA, DSA, and ECC, which are commonly used for secure communications, digital signatures, and key exchange, will no longer be secure against quantum attacks. A new set of cryptographic algorithms is required to safeguard information.

In order to compromise RSA and ECC (Elliptic Curve Cryptography) keys and transactions using a quantum computer, the required computational power depends on the size of the keys and the nature of the quantum algorithms that can be applied. The two primary quantum algorithms relevant here are Shor's Algorithm for factoring large integers (used in RSA) and solving the discrete logarithm problem (used in ECC).

- **RSA**: RSA relies on the difficulty of factoring large numbers. The security of RSA depends on the length of the modulus, typically 2048 or 4096 bits. With regards to the Quantum computer requirement, Shor's algorithm can factor large numbers exponentially faster than classical algorithms. To break a 2048-bit RSA key, a quantum computer would need about 4096 logical qubits (double the key size), factoring in the overhead for error correction, this could scale into millions of physical qubits depending on the error rates of the qubits used.

- **ECC**: ECC relies on the difficulty of solving the elliptic curve discrete logarithm problem, and is typically more secure per bit than RSA, meaning shorter key sizes provide similar security. With regards to the Quantum computer requirement, ECC is more vulnerable to quantum attacks than RSA for a given key size. For instance, a 256-bit ECC key can provide comparable security to a 3072-bit RSA key in classical terms. However, Shor's algorithm can also be applied to ECC, and it is estimated that breaking a 256-bit ECC key would require about 512 logical qubits, again potentially requiring millions of physical qubits after accounting for error correction.

- **Current State of Quantum Computers**: Current quantum computers are not yet close to having enough logical qubits to break RSA or ECC. The most advanced quantum computers today (as of 2024) have physical qubit counts in the hundreds, and logical qubit implementations remain in the early stages. Significant advancements in quantum error correction and scaling of qubit numbers are necessary to make quantum computers capable of breaking RSA or ECC. It is theorised that RSA 2048-bit requires around 4096 logical qubits to break and ECC 256-bit requires around 512 logical qubits to break. To achieve either, a quantum computer would likely need millions of physical qubits with low error rates. This level of quantum capability is still many years away, depending on advances in quantum computing technology.

NIST's Final Algorithms for Post-Quantum Cryptography

After rigorous evaluation and testing through several rounds, NIST selected the following algorithms as finalists for standardisation:

Public-Key Encryption & Key Establishment Algorithms

1. **Kyber (Lattice-Based Cryptography)**

- **Category:** Public-Key Encryption and Key Establishment
- **Description:** Kyber is a lattice-based algorithm chosen for its strong security, efficiency, and performance across a wide range of platforms. It is well-suited for encrypting data and establishing secure cryptographic keys.
- **Key Features:**
  - High security against quantum and classical attacks.
  - Efficient performance, particularly in embedded systems and low-power environments.
  - Scalable for various security levels.
- **Use Cases:**
  - Secure communication channels.
  - Key exchange in TLS (Transport Layer Security) protocols.
  - Protecting sensitive data in transit.

Digital Signature Algorithms

1. Dilithium (Lattice-Based Cryptography)

- **Category:** Digital Signatures
- **Description:** Dilithium is a lattice-based algorithm selected for its balance between security, efficiency, and scalability. It provides strong post-quantum security with fast verification times, making it ideal for systems that require high throughput.
- **Key Features:**
  - Strong security based on lattice problems.
  - Fast signature verification, making it suitable for large-scale applications.
  - Efficient performance across multiple platforms.
- **Use Cases:**
  - Digital signatures for authentication.
  - Code signing and document validation.
  - Public key infrastructure (PKI) systems.

2. Falcon (Lattice-Based Cryptography)

- **Category:** Digital Signatures
- **Description:** Falcon is another lattice-based signature algorithm selected for its compact signature sizes and robust security. It is particularly suited for environments with constrained resources, such as IoT devices.
- **Key Features:**
  - Compact signature size, ideal for resource-limited environments.
  - Strong security based on lattice problems.
  - Efficient verification process.

- **Use Cases:**
  - Digital certificates and signatures for secure communications.
  - IoT devices and embedded systems.
  - Systems requiring low bandwidth or storage overhead for signatures.

Other Algorithms Under Consideration

In addition to the finalised algorithms, NIST is still evaluating and considering other algorithms for potential standardisation in the future:

- **Sphincs+ (Hash-Based Cryptography):** A stateless hash-based signature scheme that offers post-quantum security but has larger signature sizes. It remains a candidate due to its different mathematical approach compared to lattice-based schemes.
- **Classic McEliece (Code-Based Cryptography):** Known for its strong security properties, particularly for public-key encryption, but not selected in the first round due to performance trade-offs.

Post-Quantum Cryptography Algorithm Categories

The NIST-selected algorithms are based on different mathematical foundations believed to be secure against quantum attacks. The main categories include:

- **Lattice-Based Cryptography:** This category forms the backbone of the chosen algorithms (Kyber, Dilithium, Falcon). Lattice problems are considered hard for both classical and quantum computers to solve, making these algorithms highly secure.

- **Hash-Based Cryptography:** Sphincs+ falls into this category, offering an alternative to lattice-based algorithms with a focus on hashing techniques that are resistant to quantum attacks.
- **Code-Based Cryptography:** Although not chosen for initial standardisation, Classic McEliece remains a strong candidate for public-key encryption due to its unique security properties.

Key Considerations for Implementing NIST PQC Algorithms

Organisations should start planning for the transition to quantum-safe cryptography by considering the following:

- **Cryptographic Agility:** Ensure systems are flexible enough to adopt new cryptographic algorithms without requiring a complete overhaul. This will allow smooth transitions to quantum-safe algorithms like Kyber and Dilithium.
- **Hybrid Cryptography:** During the transition period, organisations may use hybrid cryptographic approaches that combine classical and post-quantum algorithms to maintain security against both quantum and classical attacks.
- **Key Management:** Prepare for changes in key management processes. Quantum-resistant algorithms may require different key sizes and structures, so key management systems must adapt to support these new algorithms.
- **Long-Term Data Security:** Begin securing sensitive, long-lived data today using post-quantum algorithms, especially for information that must remain confidential for decades.

NIST's Next Steps in PQC Standardisation

- **Final Standardisation:** These standards will be integrated into protocols like TLS, VPNs, and secure email systems.
- **Continued Evaluation:** NIST will continue evaluating additional PQC candidates, such as Sphincs+ and Classic McEliece, and could standardise more algorithms in the future to offer a diverse range of post-quantum security solutions.
- **Global Adoption:** Governments, enterprises, and cryptographic libraries will need to adopt these quantum-safe algorithms to ensure the future security of their systems and data against quantum threats.

Preparing for Post-Quantum Cryptography

Organisations should take proactive steps to prepare for PQC implementation:

- **Monitor NIST Standards:** Stay updated on the finalisation of NIST standards and ensure your cryptographic systems are ready to implement Kyber, Dilithium, and Falcon when they become fully standardised.
- **Assess Cryptographic Dependencies:** Perform a comprehensive cryptographic audit to understand which systems, protocols, and applications rely on vulnerable algorithms like RSA and ECC.
- **Plan Migration Paths:** Develop a phased migration strategy to replace vulnerable cryptographic algorithms with PQC standards once they become available.
- **Collaborate with Vendors:** Engage with vendors to ensure they are integrating PQC algorithms into their products and services.

Conclusion

The NIST final algorithms—Kyber, Dilithium, and Falcon—are poised to become the cornerstone of post-quantum cryptography, ensuring the security of digital communications and data in the quantum era. As quantum computing advances, transitioning to these quantum-resistant algorithms will be essential for maintaining privacy and security in a post-quantum world.

Organisations should begin planning now for the adoption of NIST's post-quantum algorithms to ensure they remain secure as quantum computing evolves.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.