**NIST Internal Report, NIST IR 8547 ipd, *Transition to Post-Quantum Cryptography Standards*, November 2024[[1]](#footnote-1)**

NIST (National Institute of Standards and Technology) has a timeline for deprecating legacy encryption algorithms, with the goal of transitioning to post-quantum cryptography (PQC). RSA, ECDSA, EdDSA, DH, and ECDH are targeted for deprecation by 2030 and full phase-out by 2035. AES, including AES-256, is considered quantum-resistant. NIST has also selected five algorithms for post-quantum encryption, including Hamming Quasi-Cyclic (HQC).

Here's a summary with details below:

**2030**:

NIST plans to deprecate the use of RSA digital signature algorithms with 112 bits of security (2048-bit keys). Many widely used algorithms like RSA, ECDSA, EdDSA, DH, and ECDH are also targeted for deprecation by this year.

**2035**:

All RSA digital signature algorithms will be disallowed by NIST. This marks the full phase-out of the legacy algorithms listed above.

**Post-Quantum Cryptography (PQC):**

NIST has been working since 2016 to develop and standardize PQC algorithms to protect against attacks from quantum computers.

**NIST’s PQC Selection:**

NIST has selected five algorithms for post-quantum encryption: BIKE, Classic McEliece, HQC, and SIKE, with HQC being the latest addition.

**AES 256:**

AES with 256-bit keys is considered quantum-resistant and capable of withstanding brute-force attacks

**Post-Quantum Security Categories**

| **Security Category** | **Attack Type** | **Example** |
| --- | --- | --- |
| 1 | Key search on a block cipher with a 128-bit key | AES-128 |
| 2 | Collision search on a 256-bit hash function | SHA-256 |
| 3 | Key search on a block cipher with a 192-bit key | AES-192 |
| 4 | Collision search on a 384-bit hash function | SHA3-384 |
| 5 | Key search on a block cipher with a 256-bit key | AES-256 |

# **Digital Signatures**

The table below lists currently approved quantum-vulnerable digital signature algorithm standards.

**Quantum-vulnerable digital signature algorithms**

|  |  |  |
| --- | --- | --- |
| **Digital Signature Algorithm Family** | **Parameters** | **Transition** |
| **ECDSA**  [[FIPS186]](#_bookmark38) | 112 bits of security strength | ***Deprecated*** after 2030  ***Disallowed*** after 2035 |
| ≥ 128 bits of security strength | ***Disallowed*** after 2035 |
| **EdDSA**  [[FIPS186]](#_bookmark38) | ≥ 128 bits of security strength | ***Disallowed*** after 2035 |
| **RSA**  [[FIPS186]](#_bookmark38) | 112 bits of security strength | ***Deprecated*** after 2030  ***Disallowed*** after 2035 |
| ≥ 128 bits of security strength | ***Disallowed*** after 2035 |

NIST’s long-term cryptographic algorithm transition plans are outlined in SP 800-57pt1 (Part 1). These guidelines had projected that NIST would disallow public-key schemes that provide 112 bits of security on January 1, 2031. However, based on the need to migrate to quantum-resistant algorithms during this timeframe, NIST intends to instead deprecate classical digital signatures at the 112-bit security level. Organizations may continue using these algorithms and parameter sets as they migrate to the post-quantum signatures identified in the table below.

**Post-quantum digital signature algorithms**

|  |  |  |  |
| --- | --- | --- | --- |
| **Digital Signature Algorithm Family** | **Parameter Sets** | **Security Strength** | **Security Category** |
| **Module-Lattice-Based (ML-DSA)**  [[FIPS204]](#_bookmark42) | ML-DSA-44 | 128 bits | 2 |
| ML-DSA-65 | 192 bits | 3 |
| ML-DSA-87 | 256 bits | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Digital Signature Algorithm Family** | **Parameter Sets** | **Security Strength** | **Security Category** |
| **Stateless hash-based** **(SLH-DSA)**  [[FIPS205]](#_bookmark43) | SLH-DSA-SHA2-128[s/f] SLH-DSA-SHAKE-128[s/f] | 128 bits | 1 |
| SLH-DSA-SHA2-192[s/f] SLH-DSA-SHAKE-192[s/f] | 192 bits | 3 |
| SLH-DSA-SHA2-256[s/f] SLH-DSA-SHAKE-256[s/f] | 256 bits | 5 |
| **Leighton-Micali-Signature (LMS), Hierarchical Signature System (HSS)**  [[SP800208]](#_bookmark52) | With SHA-256/192 With SHAKE256/192 | 192 bits | 3 |
| With SHA-256 With SHAKE256 | 256 bits | 5 |
| **eXtended Merkle Signature Scheme** (**XMSS, XMSS*MT***)  [[SP800208]](#_bookmark52) | With SHA-256/192 With SHAKE256/192 | 192 bits | 3 |
| With SHA-256 With SHAKE256 | 256 bits | 5 |

# **Key Establishment**

[The](#_bookmark30) table below lists currently approved quantum-vulnerable key-establishment.

**Quantum-Vulnerable Key-Establishment Schemes**

|  |  |  |
| --- | --- | --- |
| **Key Establishment Scheme** | **Parameters** | **Transition** |
| **Finite Field DH and MQV** [[SP80056A]](#_bookmark46) | 112 bits of security strength | ***Deprecated*** after 2030  ***Disallowed*** after 2035 |
| ≥ 128 bits of security strength | ***Disallowed*** after 2035 |
| **Elliptic Curve DH and MQC** [[SP80056A]](#_bookmark46) | 112 bits of security strength | ***Deprecated*** after 2030  ***Disallowed*** after 2035 |
| ≥ 128 bits of security strength | ***Disallowed*** after 2035 |
| **RSA**  [[SP80056B]](#_bookmark47) | 112 bits of security strength | ***Deprecated*** after 2030  ***Disallowed*** after 2035 |
| ≥ 128 bits of security strength | ***Disallowed*** after 2035 |

Similar to the transition for digital signature algorithms, NIST intends to instead deprecate rather than fully disallow classical key-establishment schemes at the 112-bit security level. Organizations may continue using these algorithms and parameter sets as they migrate to Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) or other approved quantum-resistant techniques. However, in order to mitigate the risk of “harvest now, decrypt later” attacks on network communications, application-specific guidance, may require or recommend migration to quantum-resistant key establishment schemes before the classical schemes are generally disallowed.

[The](#_bookmark31) table below lists current quantum-resistant key establishment schemes. At this time, ML-KEM is the only approved post-quantum key-establishment scheme based on public key cryptography. Additional algorithms are still being considered as part of the fourth round of the NIST PQC Standardization process. NIST expects to select one or more alternatives to ML-KEM in the future.

**Post-quantum key-establishment schemes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Key Establishment Scheme** | **Parameter Sets** | **Security Strength** | **Security Category** |
| **ML-KEM**  [[FIPS203]](#_bookmark41) | ML-KEM-512 | 128 bits | 1 |
| ML-DSA-768 | 192 bits | 3 |
| ML-DSA-1024 | 256 bits | 5 |

# **Symmetric Cryptography**

NIST’s existing standards in symmetric cryptography — including hash functions, eXtendable-Output Functions (XOFs), block ciphers, key derivation functions (KDFs), and Deterministic Random Bit Generators (drbg) — are significantly less vulnerable to known quantum attacks than the public-key cryptography standards in SP 800-56A, SP 800-56B, and FIPS 186. In particular, all NIST-approved symmetric primitives that provide at least 128 bits of classical security are believed to meet the requirements of at least Category 1 security within the system of five security strength categories for evaluating parameter sets in the NIST PQC standardization process. NIST has a few symmetric cryptography standards at the 112-bit security level, which will be disallowed in 2030. Applications should move away from these when transitioning to post-quantum cryptography.

**Block ciphers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Block Cipher** | **Parameter Sets** | **Security Strength** | **Security Category** |
| **AES**  [[FIPS197]](#_bookmark39) | AES-128 | 128 bits | 1 |
| AES-192 | 192 bits | 3 |
| AES-256 | 256 bits | 5 |

**Hash functions and XOFs**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hash/XOF Algorithm Family** | **Variants** | **Collision Security Strength** | **Collision Security Category** | **Preimage Security Strength** | **Preimage Security Category** |
| **SHA-1**  [[FIPS180]](#_bookmark37) | SHA-1 | 80 bits | < 1 | 160 bits | 1 |
| **SHA-2**  [[FIPS180]](#_bookmark37) | SHA-224  SHA-512/224 | 112 bits | < 1 | 224 bits | 3 |
| SHA-256  SHA-512/256 | 128 bits | 2 | 256 bits | 5 |
| SHA-384 | 192 bits | 4 | 384 bits | 5 |
| SHA-512 | 256 bits | 5 | 512 bits | 5 |
| **SHA-3**  [[FIPS202]](#_bookmark40) | SHA3-224 | 112 bits | < 1 | 224 bits | 3 |
| SHA3-256 | 128 bits | 2 | 256 bits | 5 |
| SHAKE128 | 128 bits | 2 | 128 bits | 2 |
| SHA3-384 | 192 bits | 4 | 384 bits | 5 |
| SHA3-512 | 256 bits | 5 | 512 bits | 5 |
| SHAKE256 | 256 bits | 5 | 512 bits | 5 |

1. The information included in this document was extracted from NIST IR 8547 ipd. [↑](#footnote-ref-1)