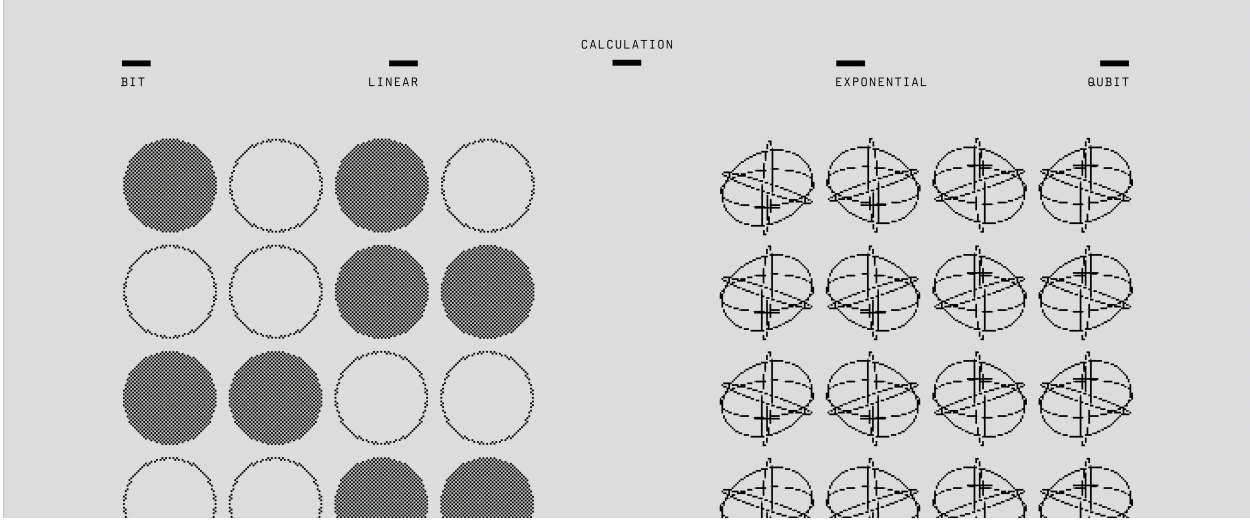


# Draft 04: NIST Standards for Quantum Computing and Algorithms.

**Author:** Jinay Shah

## Understanding NIST: The Guardian Of Standards.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

*For those who despise institutionalization, standardization, and formalization—bear with me.*

NIST stands for National Institute of Standards and Technology (NIST) a U.S. federal agency under the Department of Commerce responsible for advancing measurement science, standards, and technology.
NIST develops and maintains standards that ensure accuracy and reliability across

industries, from manufacturing and healthcare to cybersecurity and telecommunications. The agency conducts cutting-edge research in fields like quantum computing, cryptography, and materials science, providing the scientific foundation for innovation and commerce.
NIST also plays a critical role in protecting digital infrastructure by establishing cybersecurity standards and guidelines that government agencies and private organizations use worldwide.
Essentially, NIST ensures that measurements are accurate, technology is secure, and standards are consistent across the nation's economy and infrastructure. Think of NIST as the referee of the technology world: they don't play the game, but they make sure everyone's playing by the same rules. From ensuring your bathroom scale actually weighs things correctly to making sure your bank's encryption isn't child's play for hackers, NIST establishes the measurement science, standards, and technology that keep our modern world running.

---

# The Big 'Why?': Why Should Anyone Care About This?

→ Before diving into the technical depths, let's address the elephant in the room: Why does this matter? *And here's the answer to our **why**:*

## The Quantum Threat is Real and Imminent

Imagine if someone told you that in about ten years, every lock on every door in the world would become obsolete. You'd probably start thinking about new locks *now*, right? That's essentially where we are with quantum computing and encryption.
Quantum computers, once operational at scale, will be able to break virtually all current encryption methods that protect our digital world—from banking transactions and medical records to government communications and critical infrastructure. This isn't a distant sci-fi scenario; it's a recognized threat that security experts call "Y2Q" (Years to Quantum).
Even more concerning is the "harvest now, decrypt later" problem: adversaries are already collecting encrypted data today with the intention of decrypting it once quantum computers become powerful enough to crack it open like a piñata. *That sensitive email you encrypted in 2024? It might be perfectly readable in 2034.*

## NIST Provides Global Trust and Authority

When NIST standardizes cryptographic algorithms, it's far more than bureaucratic box-checking. NIST standards become the de facto global benchmark that governments, financial institutions, tech companies, and security professionals worldwide adopt. Their rigorous, transparent evaluation process—which involved cryptographers from around the world and spanned nearly eight years—ensures that these algorithms have been thoroughly vetted against both classical and quantum attacks. This gives organizations confidence that they're implementing genuinely secure solutions rather than rolling the dice with unproven alternatives.

## The Transition Takes Time and Must Start Now

Here's the uncomfortable truth: migrating the world's digital infrastructure to quantum-resistant cryptography is an enormous undertaking that could take a decade or more. Every system, device, protocol, and application that uses encryption needs to be updated. NIST's standardization provides the clear roadmap that industry needs to begin this transition immediately.
Think about it—your smartphone, your car's computer systems, your smart refrigerator (yes, even that), banking infrastructure, hospital networks, power grids. Each one needs to transition to quantum-resistant encryption. Without official standards, organizations face analysis paralysis: which algorithms to implement? Risk premature adoption of flawed solutions or dangerous delays in upgrading security? NIST's standardization provides the clear roadmap industry desperately needs.

## What are the NIST standards all about?

In response to the quantum threat, NIST initiated a comprehensive process to solicit, evaluate, and standardize quantum-resistant public-key cryptographic algorithms—algorithms that even future quantum computers can't crack.
Since, recently there has been a substantially valid and relevant research and development around quantum computing, with a recent and significant one being till date: Google’s historic breakthrough in quantum computing, achieving the first-ever verifiable quantum advantage using its Willow quantum chip. This milestone, published in Nature, demonstrates that the Willow chip can run the Quantum Echoes algorithm 13,000 times faster than the best classical supercomputers for a specific task, marking a significant step toward practical quantum applications.

To put that in perspective, imagine running a marathon in 13 seconds instead of 3 hours. That's the kind of computational leap we're talking about—and it's why NIST's work on quantum-resistant cryptography isn't just important, it's existential.

NIST was particularly concerned about **RSA (Rivest-Shamir-Adleman)** encryption, the cryptographic workhorse that has protected internet communications for decades. RSA's security relies on a seemingly simple principle: it's incredibly difficult to factor large numbers into their prime components.
For example, multiplying 89 × 97 to get 8,633 is trivial. But if I give you 8,633 and ask which two prime numbers multiply to create it, suddenly you're doing a lot more work. Now scale that up to numbers with hundreds of digits, and classical computers grind to a halt for years or centuries.
Quantum computers? They'll solve it over lunch. That's the problem.

Post-quantum cryptography (also called quantum-resistant cryptography) aims to develop cryptographic systems secure against *both* quantum and classical computers while remaining compatible with existing communications protocols

and networks.
The goal of *post-quantum cryptography* (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

---

## PQC Standardization Process: Meet the Candidates

After years of evaluation, NIST recommended a suite of algorithms for different use cases. Let's meet them:


### The Primary Duo: CRYSTALS-KYBER and CRYSTALS-Dilithium

NIST selected two primary algorithms for most use cases:

- CRYSTALS-KYBER for key establishment.
- CRYSTALS-Dilithium for digital signatures.

*Think of these as the Batman and Robin of post-quantum cryptography—your first line of defense.*

---

NIST recommended **two primary algorithms** to be implemented for most use cases: **CRYSTALS-KYBER (key-establishment)** and **CRYSTALS-Dilithium (digital**

**signatures)**.
In addition, the signature schemes **FALCON** and **SPHINCS+** will also be standardized. [July 5, 2022]

1. **CRYSTALS-KYBER → ML-KEM (FIPS 203)**
   **Official Name:** Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).
   **Purpose:** Key establishment - used to establish a shared secret key between two parties over a public channel.
   **Status:** Finalized and published on August 13, 2024.
   **Parameter Sets:** ML-KEM specifies three parameter sets in order of increasing security strength (and decreasing performance):

   - ML-KEM-512: Security Level 1 (equivalent to AES-128)
   - ML-KEM-768: Security Level 3 (equivalent to AES-192)
   - ML-KEM-1024: Security Level 5 (equivalent to AES-256)

   > As security increases, performance decreases—the eternal tradeoff. For most applications, ML-KEM-768 hits the sweet spot between security and speed.

---

2. **CRYSTALS-DILITHIUM → ML-DSA (FIPS 204)**
   **Official Name:** Module-Lattice-Based Digital Signature Algorithm (ML-DSA)
   **Purpose:** Generate and verify digital signatures to detect unauthorized modifications to data and authenticate the identity of the signatory.
   **Status:** Finalized and published on August 13, 2024.
   **Parameter Sets:** Three parameter sets are defined:

   - ML-DSA-44 (Dilithium 2): 128-bit security, Public key 1,312 bytes, Private key 2,560 bytes, Signature 2,420 bytes
   - ML-DSA-65 (Dilithium 3): 192-bit security, Public key 1,952 bytes, Private key 4,032 bytes, Signature 3,309 bytes
   - ML-DSA-87 (Dilithium 5): 256-bit security, Public key 2,592 bytes, Private key 4,866 bytes, Signature 4,627 bytes.

   **Two Variants:**

1. **ML-DSA (Standard):** Main algorithms include `ML-DSA.KeyGen`, `ML-DSA.Sign`, and `ML-DSA.Verify`.

2. **HashML-DSA (Pre-hash variant):** A closely related but domain-separated signature scheme that includes an additional pre-hashing step before signing, using `HashML-DSA.Sign` and `HashML-DSA.Verify` with the same key generation.

> **Note:** Yes, these signatures are significantly larger than current RSA signatures. A typical RSA signature might be 256 bytes; ML-DSA signatures range from 2,420 to 4,627 bytes. That's the cost of quantum resistance—like upgrading from a compact car to an SUV for better protection.

---

3. **FALCON → FN-DSA (FIPS 206)**
   `Official Name:` FFT (Fast-Fourier Transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA)
   `Purpose:` Digital signatures with smaller signature sizes than ML-DSA.
   `Status:` Draft standard (FIPS 206) was submitted to NIST for approval on August 28, 2025. Public review may last about a year, with final standard expected in late 2026 or early 2027.
   `Parameter Sets:` Two security levels:

   - **FN-DSA-512** (FALCON-512): 128-bit security (equivalent to RSA-2048), Public key 897 bytes, Private key 1,281 bytes, Signature 666-690 bytes.
   - **FN-DSA-1024** (FALCON-1024): 256-bit security, Public key 1,793 bytes, Private key 2,305 bytes, Signature 1,280-1,330 bytes.

> **Notice:** how FALCON's signatures are significantly smaller than ML-DSA's? That's its superpower. The tradeoff is complexity—FALCON is notoriously difficult to implement correctly, which is why NIST positioned it as a specialized tool rather than the primary recommendation.

---

4. **SPHINCS+ → SLH-DSA (FIPS 205)**
   `Official Name:` Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)
   `Purpose:` Digital signatures for detecting unauthorized modifications and authenticating identity, with non-repudiation.
   `Status:` Finalized and published on August 13, 2024.

**Parameter Sets:** FIPS 205 specifies 12 parameter options combining three security levels, two hash functions (SHA2 and SHAKE), and two optimization goals:

- **Security Levels:** 128-bit (Level 1), 192-bit (Level 3), 256-bit (Level 5)
- **Hash Functions:** SHA2 or SHAKE
- **Optimization:** "s" (small signatures) or "f" (fast signing)

> **The Catch:** SPHINCS+ signatures are *large*— really large. We're talking tens of kilobytes. But that's the price for its unique security guarantees and diversified mathematical foundation.

---

# Critical Updates and Recent Developments

## Fifth Algorithm Announcement:

On March 11, 2025, NIST announced the selection of **HQC (Hamming Quasi-Cyclic)** as a backup algorithm for general encryption. HQC uses code-based mathematics—completely different from ML-KEM's lattice-based approach.

**Why does this matter?**
Diversification. If researchers discover a critical weakness in lattice-based cryptography (the foundation of ML-KEM), HQC provides a mathematically independent fallback. It's like keeping both a deadbolt and a chain lock on your door—different mechanisms, double the protection.

## Additional Digital Signature Round:

In October 2024, NIST announced 14 candidates advancing to the second round of the Additional Digital Signatures process:

The second-round contenders: HAETAE, HAWK, Mayo, MIRA, MQ-Sign, PROV, SPHINCS-alpha, SQUIRRELS, UOV, Biscuit, CROSS, LESS, PERK, and TUOV. This second phase of evaluation and review is estimated to last 12-18 months, with NIST tentatively planning to hold a 6th PQC Standardization Conference from September 24-26, 2025.

NIST mathematician **Dustin Moody** encourages system administrators to start integrating the finalized standards into their systems immediately, because full integration will take time.

*→ In November 2024, NIST released draft NIST Internal Report 8547, "Transition to Post-Quantum Cryptography Standards," available for public comment through January 10, 2025.*

---

# References:


1. NIST Quantum Information Science: https://www.nist.gov/quantum-information-science
2. NIST Post Quantum Cryptography (PQC): https://csrc.nist.gov/projects/post-quantum-cryptography
3. Google's Quantum Echoes Algorithm [blog]: https://blog.google/technology/research/quantum-echoes-willow-verifiable-quantum-advantage
4. PQC Standardization Process: https://www.nist.gov/news-events/news/2022/07/pqc-standardization-process-announcing-four-candidates-be-standardized-plus#standardization
5. NIST PQC Release: https://www.quantum.gov/nist-releases-post-quantum-encryption-standards
6. Quantum Communications and Networking Project: https://www.nist.gov/publications/quantum-communications-and-networking-project-information-technology-laboratory-nist
7. Three Federal Information Processing Standards [FIPS] 203: https://csrc.nist.gov/pubs/fips/203/final

8. Three Federal Information Processing Standards [FIPS] 204: https://csrc.nist.gov/pubs/fips/204/final
9. Three Federal Information Processing Standards [FIPS] 205: https://csrc.nist.gov/pubs/fips/205/final
*FIPS 206: Expected late 2026/early 2027.*
10. Holland and Knight: https://www.hklaw.com/en/insights/publications/2024/08/nist-releases-three-post-quantum-cryptography-standards
11. NIST CSRC — PQC Publications & IR series: https://csrc.nist.gov/Projects/post-quantum-cryptography/publications