ETSI/IQC Quantum Safe Cryptography Conference 2026

NIST PQC: the road ahead

Presented by:

Dustin Moody

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

17/6/2026

NIST's Cryptographic Standards Program

- Research, develop, engineer, and produce standards, guidelines, recommendations, and best practices for cryptographic algorithms, methods, and protocols.
- Promote the use of validated cryptography, and inform federal cryptography procurement decisions, through the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP).

Program at a Glance

Research

- Circuit Complexity
- Threshold Crypto
- DLT & Consensus
- Privacy-Enhancing Crypto

Standards & Guidelines

- Block Ciphers
- Modes of Operation
- Random Number Generation
- Post-Quantum Crypto
- SHA3 & Keccak
- Lightweight Crypto

Applications

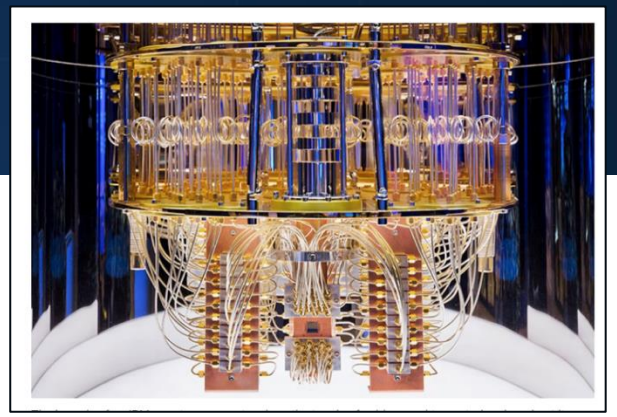
- TLS
- Roots of Trust
- App-specific KDFs
- Bluetooth/WiFi Guidelines

Testing

- FIPS 140
- CMVP
- CAVP

Nearly all commercial laptops, cellphones, Internet routes, VPN servers, and ATMs use NIST Cryptography

The Quantum Threat

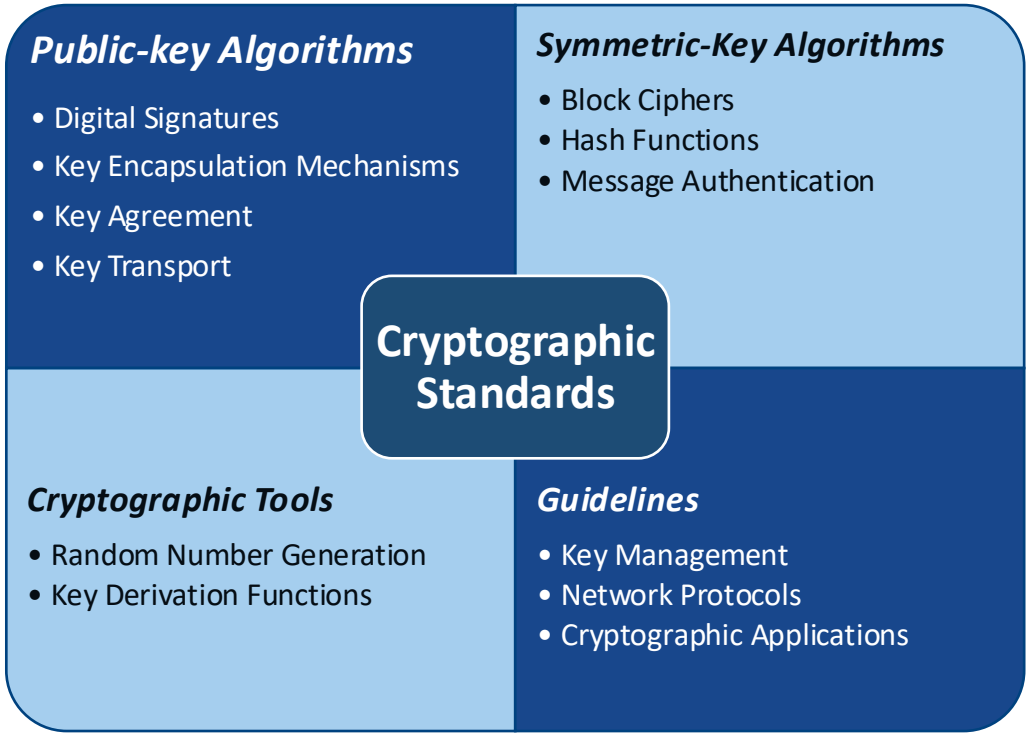


NIST public-key crypto standards

- **SP 800-56A**: Diffie-Hellman, ECDH
- **SP 800-56B**: RSA encryption
- **FIPS 186**: RSA, DSA, and ECDSA signatures

are all vulnerable to attacks from a (large-scale) quantum computer

- Symmetric-key crypto (AES, SHA) would also be affected (by Grover's algorithm), but less dramatically

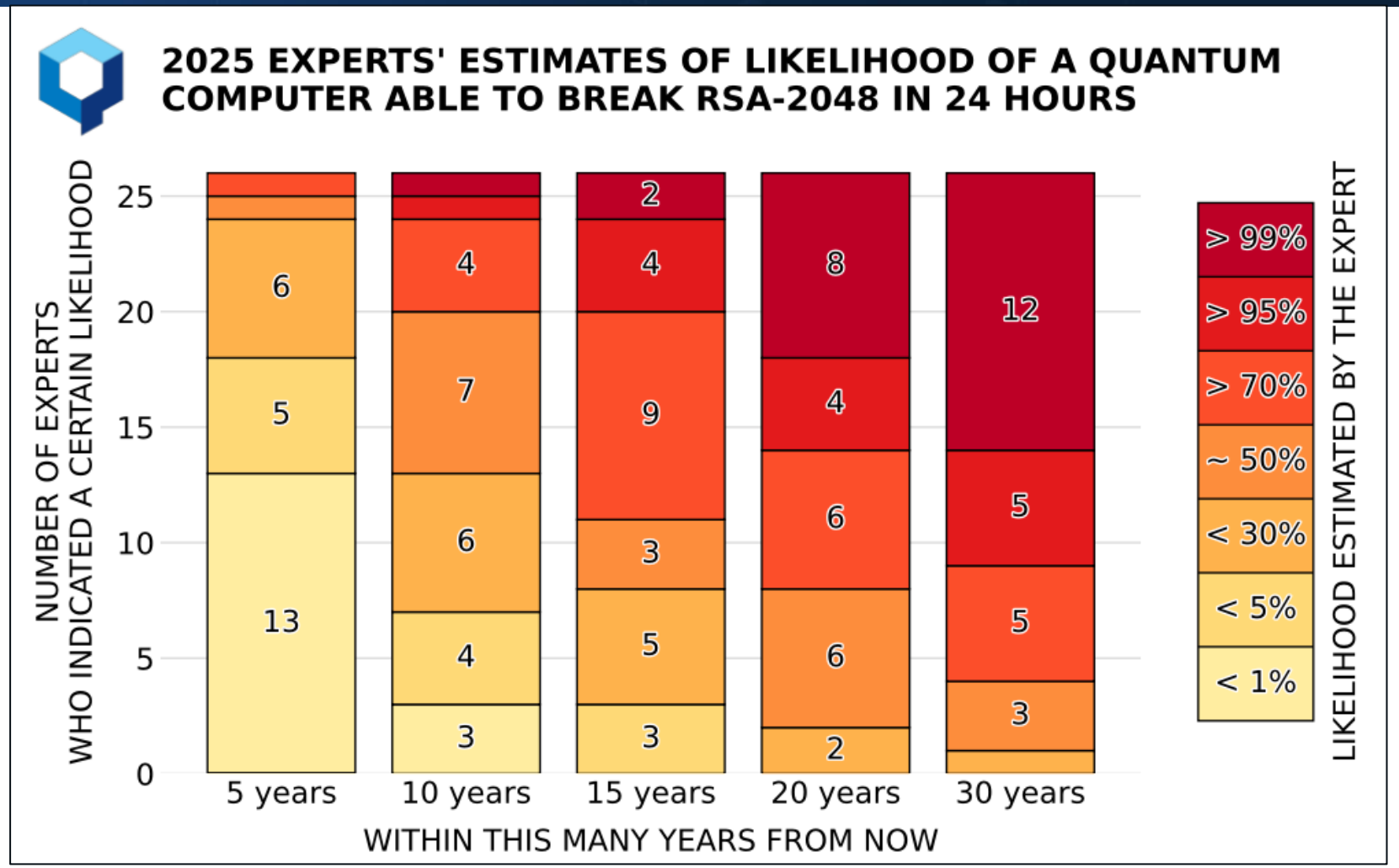


When will the threat be here?

- OPINIONS VARY
- THE ANSWER IS UNCLEAR

WHAT IS CLEAR?

- CYBER SYSTEMS WILL NEED TO MIGRATE TO QUANTUM-SAFE SOLUTIONS BEFORE THE THREAT IS REALIZED
- MIGRATIONS TAKE SEVERAL YEARS
- QUANTUM-SAFE SOLUTIONS NEED TO BE STANDARDIZED



Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2025
https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/

The First Set of NIST PQC Standards

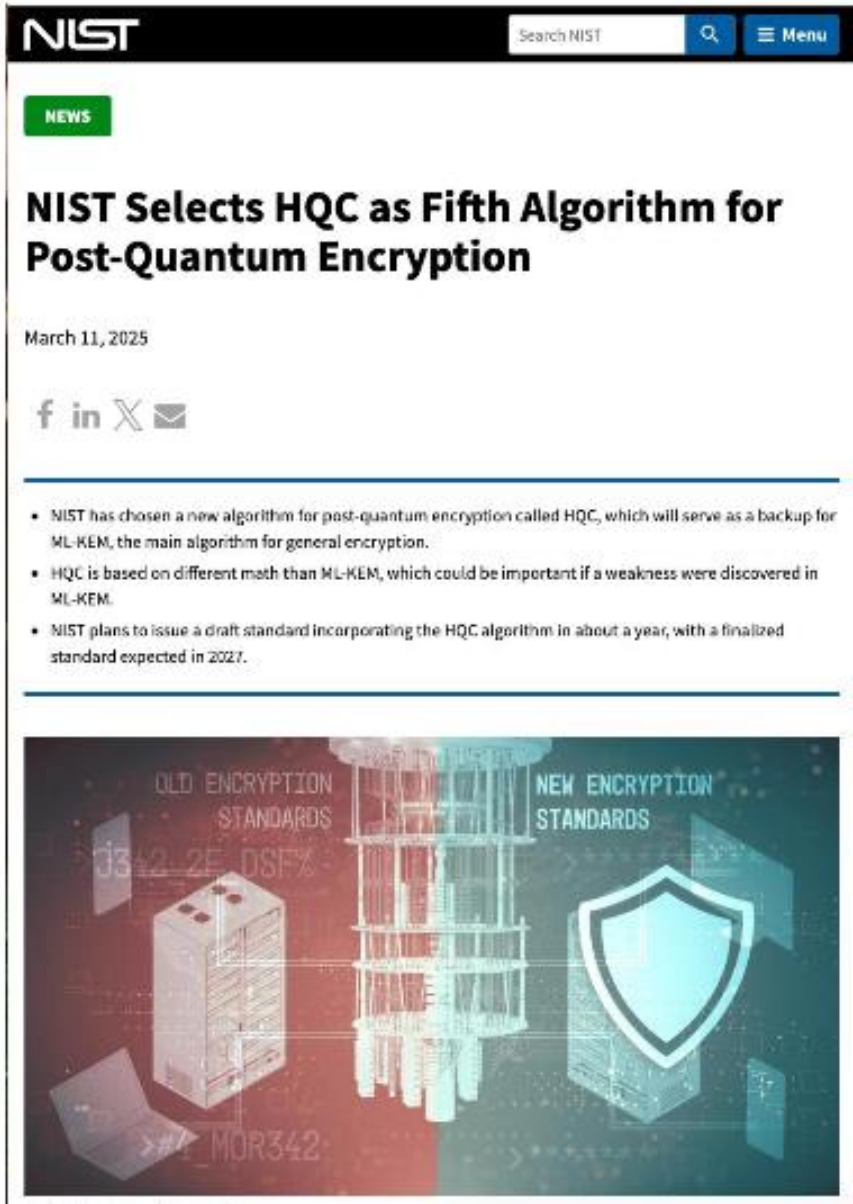
FIPS 203 ML-KEM (Based on CRYSTALS-Kyber)	FIPS 204 ML-DSA (Based on CRYSTALS-Dilithium)	FIPS 205 SLH-DSA (Based on SPHINCS+)	Draft FIPS 206 FN-DSA (Based on FALCON)
• A module learning with errors (MLWE)-based key encapsulation mechanism (KEM) • Good performance in different platforms • An algorithm for key establishment in security protocols	• A lattice-based digital signature algorithm based on the Fiat-Shamir paradigm • Good performance, simple implementation, moderate public-key and signature size, suitable for general applications	• Not require to keep track of any state between signatures • Solid security, signatures are longer compared with ML-DSA	• Hash and sign paradigm • Smaller bandwidth and fast verification but more complicated implementation • ***Under development*** • (hopefully soon)

Published August 2024!

Key Encapsulation Mechanisms (KEMs)

- KEMs are used to establish keys between two parties
  - ML-KEM already standardized in FIPS 203
    - Lattice-based
  - HQC selected in 2025 (draft FIPS 207 underway)
    - Code-based
  - No further KEMs under evaluation

- 800-227, Recommendations for KEMs
  - Describes the basic definitions, properties, and applications of KEMs
  - Provides recommendations for implementing and using KEMs in a secure manner
  - Contains some guidance on hybrid key establishment



NIST

Search NIST

Menu

NEWS

NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

March 11, 2025

- NIST has chosen a new algorithm for post-quantum encryption called HQC, which will serve as a backup for ML-KEM, the main algorithm for general encryption.
- HQC is based on different math than ML-KEM, which could be important if a weakness were discovered in ML-KEM.
- NIST plans to issue a draft standard incorporating the HQC algorithm in about a year, with a finalized standard expected in 2027.

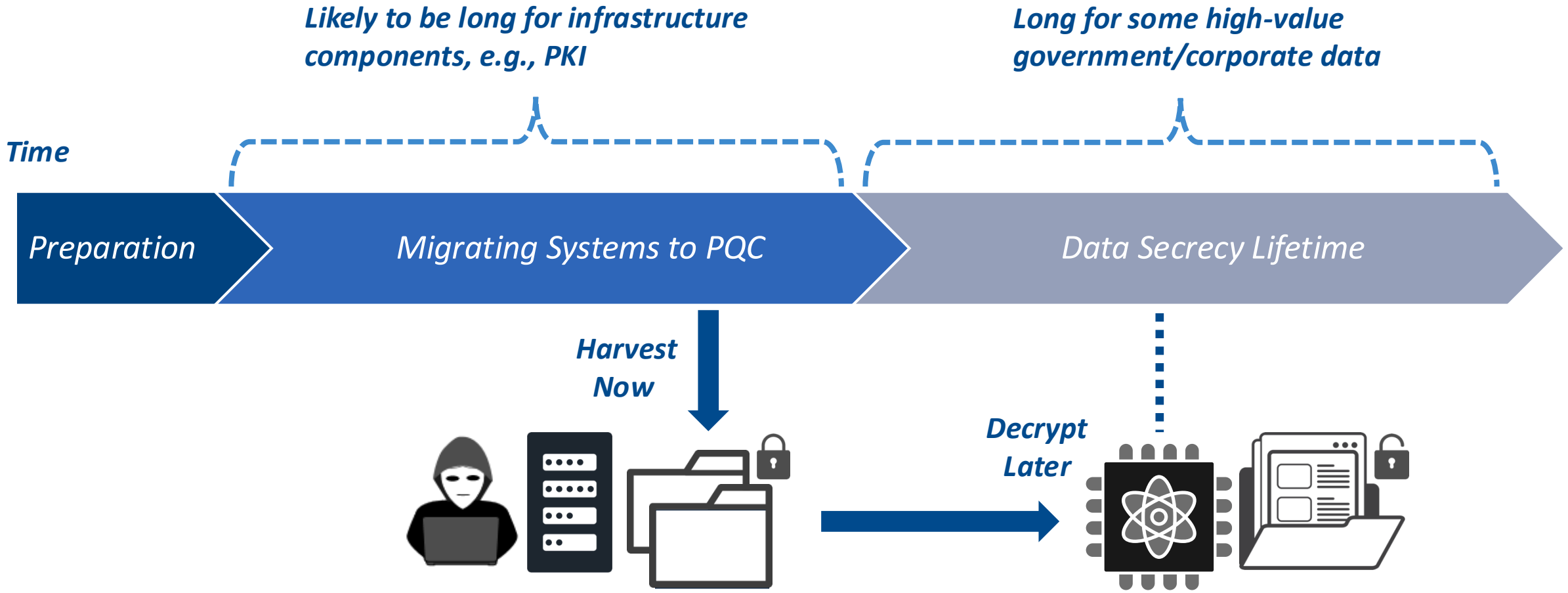
On-Ramp Signatures

- July 2022 – New Call for additional digital signatures
- June 2023 – Deadline for submission (40 candidates)
- Oct 2024 – 14 candidates in the 2nd round
- May 2026 – 9 candidates advance to the 3rd round

- Why did NIST call for additional post-quantum signatures?
  - NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.
  - NIST may also be interested in signature schemes that have short signatures and fast verification.

- No on-ramp for KEMs currently planned

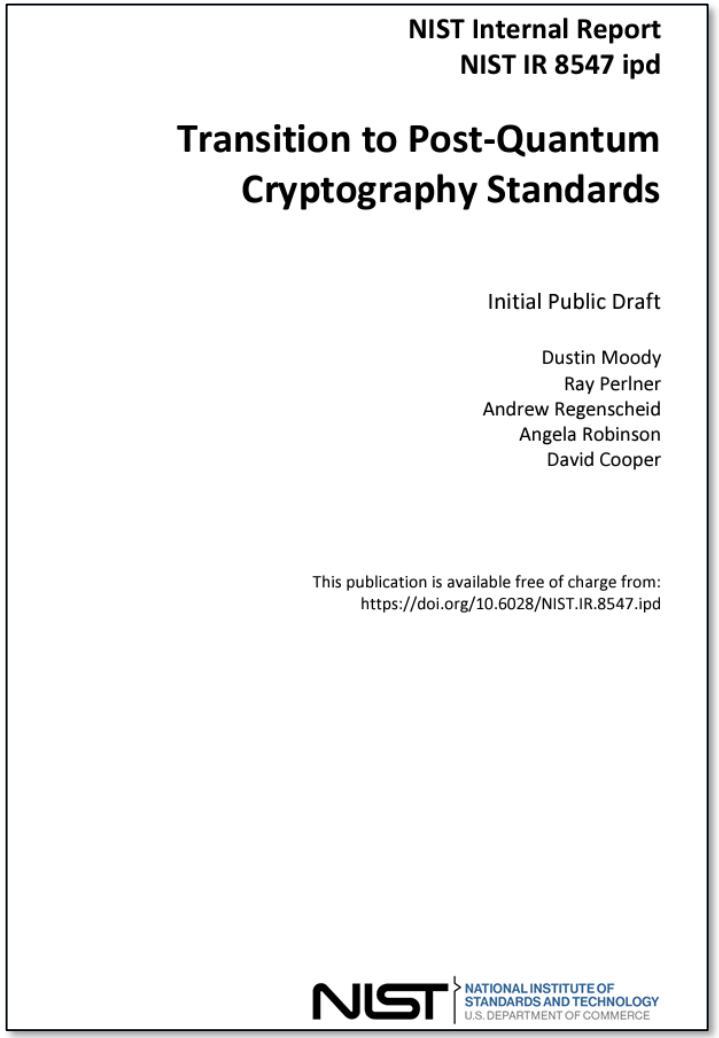
Migration Considerations



NIST IR 8547, Transition to PQC Standards

- Initial Public Draft released November 2024
- Identifies quantum-vulnerable and post-quantum standards
  - Vulnerable: RSA, (EC) Diffie-Hellman, MQV, ECDSA, EdDSA
  - PQC: ML-KEM, ML-DSA, SLH-DSA, LMS, XMSS
- Proposed transition timelines for quantum-vulnerable algorithms
  - 112-bit security strength – ***deprecated*** after 2030, ***disallowed*** after 2035
  - 128-bit and higher security strength – ***disallowed*** after 2035
- NIST-approved symmetric primitives providing at least 128 bits of classical security continue to be approved

NIST IR 8547 timeline supports NSM-10 goal of transitioning USG systems to PQC by 2035


NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

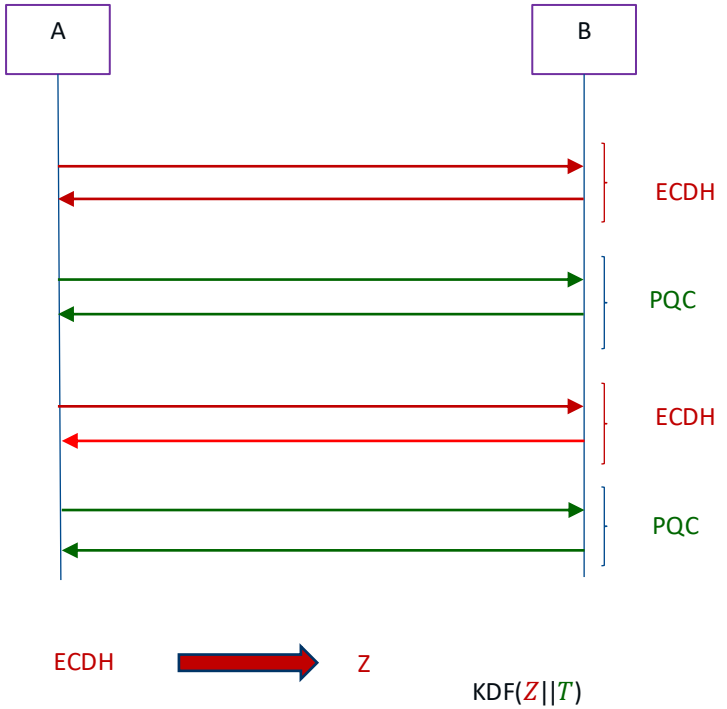
Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

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

Hybrid Schemes

- **Hybrid**: using classical and PQC algorithms together
  - A hybrid mode combines a classical algorithm with a PQC algorithm
  - Reduces risks from uncertainty if either is broken
  - More complexity / slower performance
  - Can get FIPS 140 validation
  - More guidance in SP 800-227 – order of schemes not important



- Several approaches to hybrid KEMs and certificates
  - Both composite and non-composite hybrid approaches
- Use of hybrid will depend on community and application-specific needs
  - NIST does not recommend for/against hybrid schemes
  - Implementers should consider complexity and migration issues
- Architectures /applications may support multiple algorithms

PQC Testing Under FIPS 140

Cryptographic Module Validation Program (CMVP)

- Joint program between NIST and Canadian Centre for Cyber Security (CCCS)

Automated Cryptographic Validation Testing System (ACVTS)

- Testing for algorithm standards to verify correct implementation of cryptographic standards
  - https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/how-to-access-acvts

Vendors, Labs, and CMVP

- Vendors use independent, **NVLAP-accredited Cryptographic and Security Testing (CST) laboratories** to test their modules. Over 20 labs worldwide.
- CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and other CMVP programmatic guidance to test conformance against FIPS 140-3.
- FIPS 140-3 and NIST SP 800-140 modify ISO/IEC 19790 and ISO/IEC 24759.

The PQC algorithms are testable today. No need to wait.

The NCCoE Migration to PQC Project

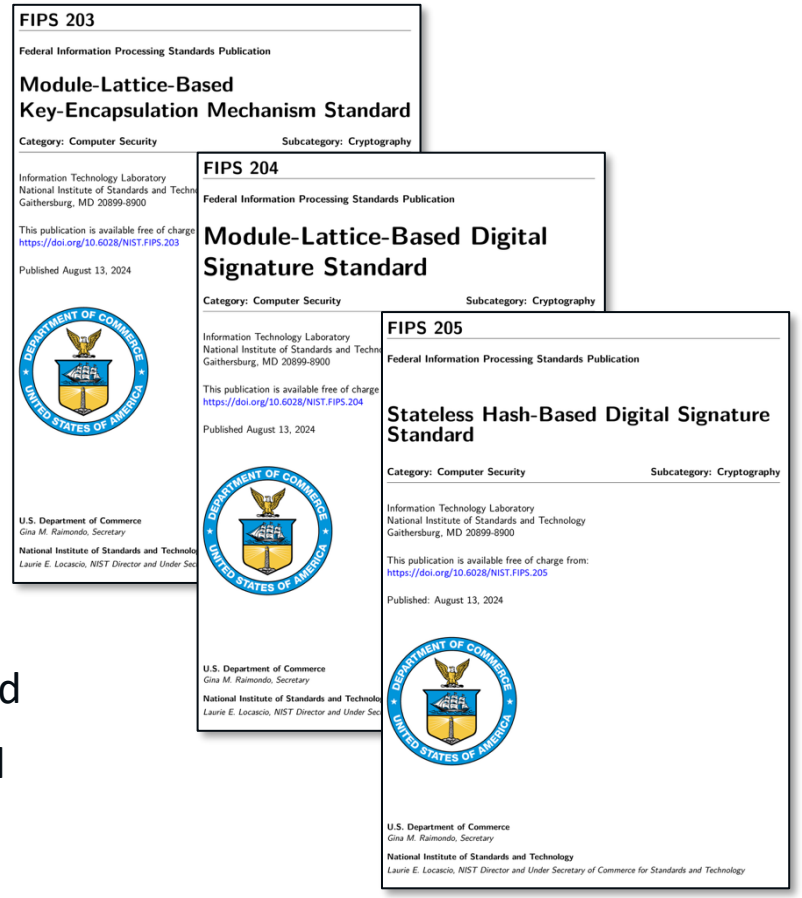
- At NIST's National Cybersecurity Center of Excellence (NCCoE), we are tackling challenges with ***adoption, implementation, and deployment*** of PQC in applications and protocols
- Engage with ***over 50*** industry and government partners to ***increase awareness*** and ***demonstrate practices*** that help organizations migrate to post-quantum algorithms
- Coordinate with ***standards developing organizations*** and ***government/industry*** to develop guidance to accelerate the migration
- Support ***US Government PQC initiatives***
  - NSM-10
  - Quantum Computing Cybersecurity Preparedness Act
  - NSA CNSA 2.0

See the Project FAQ

PQC Standards, Guidelines, and Next Steps

- ***ML-KEM***, ***ML-DSA***, & ***SLH-DSA*** finalized Aug, 2024
- Draft ***FN-DSA*** and ***HQC-KEM*** standards are under development

- **SP 800-227**, *Recommendations for key-encapsulation mechanisms*
- **CSWP 39** – Considerations for Achieving Cryptographic Agility: Strategies and Practices
- **NISTIR 8610** – End of the 2nd Round of the Onramp



- **SP 800-133**, *Recommendation for Cryptographic Key Generation*, being revised
- **SP 800-208**, *Recommendation for Stateful Hash-Based Signature Schemes*, being revised
- **SP 800-230**, *Additional SLH-DSA Parameter Sets and their Approved Uses,* being revised
  - Contains 6 additional parameter sets, with a maximum usage of 2^24 signatures

- Transition guidelines will be finalized in **NIST IR 8547**, with future ongoing revisions in SP 800-131A

Questions

Contact Information

Dustin Moody

Email: dustin.moody@nist.gov

NIST PQC standardization

www.nist.gov/pqcrypto
Email: pqc-comments@nist.gov

Sign up for ***pqc-forum*** mailing list

NCCoE PQC Migration Project

http://www.nccoe.nist.gov/applied-cryptography
Request to join Community of Interest
Email: applied-crypto-pqc@nist.gov