National Institute of Standards and Technology
U.S. Department of Commerce

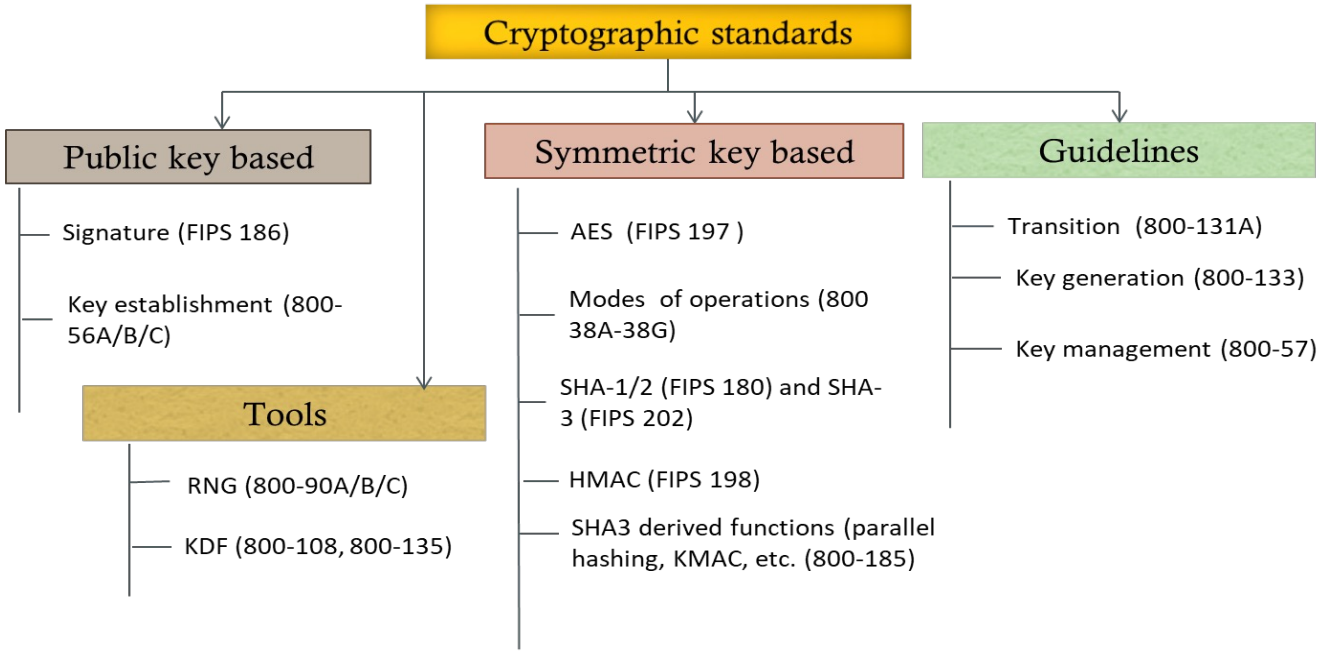
NIST PQC Standardization

Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

NIST Cryptographic Standards

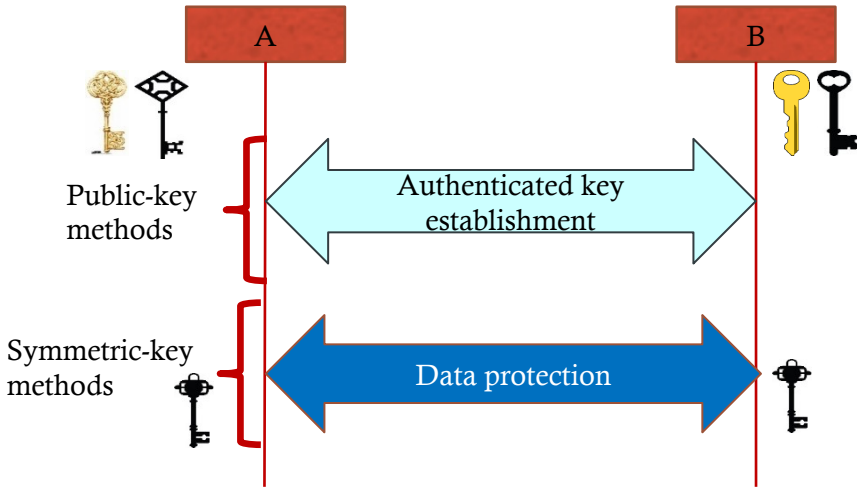
- NIST developed the first encryption standards in 1970s
  - Data Encryption Standard (DES), published 1977 as Federal Information Processing Standard (FIPS) 46
- Over 40 years, NIST continues to evolve its cryptographic standards
  - Enable to secure the emerging applications – Internet, digital communications, open platform, etc.
  - Enhance security strength to against more sophisticated attacks

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



Cryptography – The Cornerstone of Cybersecurity

- Protect information transmitted over the links and stored in the devices



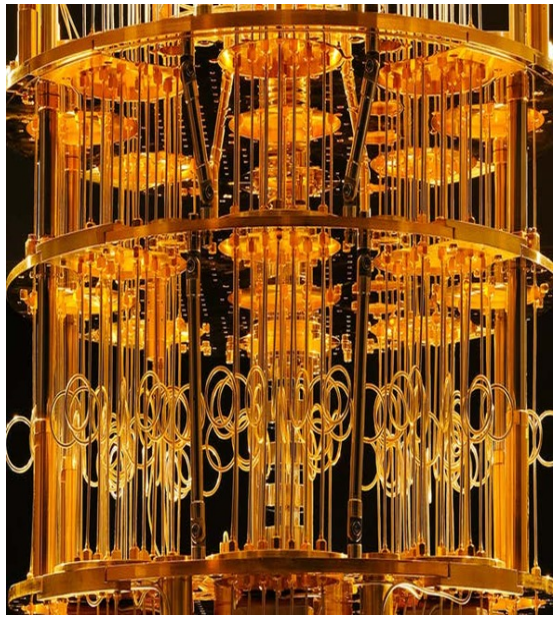
- Examples
  - Transport Layer Security (TLS)
  - Internet Key Exchange (IKE) + IPsec

- Prevent from malware and malicious software attacks

- Examples
  - Trusted Platform Module (TPM)
  - Code signing

Quantum Impact to Cybersecurity

- The security of public-key cryptography is based on hard problem assumptions for classic computers, e.g., integer factorization for RSA and discrete logarithm for DH and ECDSA
- Quantum computers changed what we have believed about the hardness
  - By Shor's algorithm, factorization and discrete logarithm problems can be solved by quantum computers in polynomial time
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms by Grover's algorithm – manageable by increasing key size if necessary

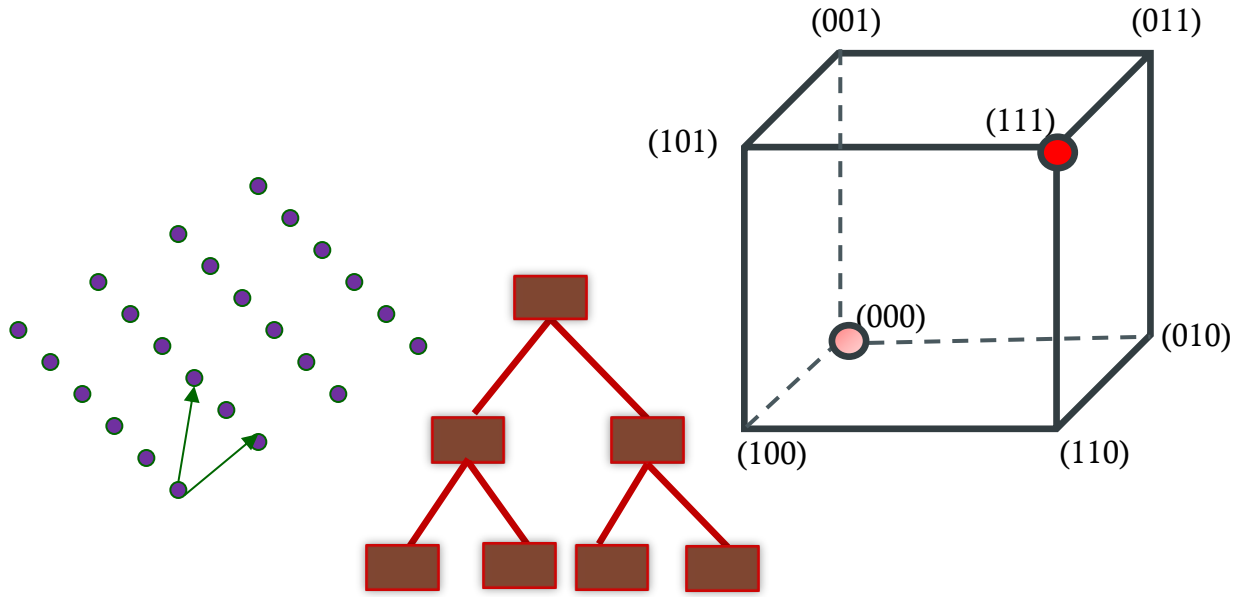


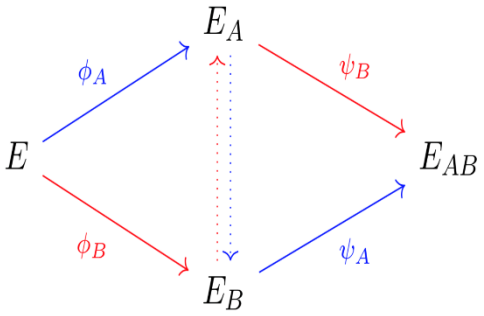
How to deal with quantum attacks

- Need to find cryptographic algorithms which are secure against attacks by both classical and quantum computers
  - The algorithms must be based on hard problems for both classical and quantum computers
- In other words, we need quantum resistant cryptography, named by the researchers as post-quantum cryptography (PQC)
- Clarification
  - Post-quantum cryptographic algorithms are supposed to be implemented in “classical” computers in the same way as RSA, DH, and ECDSA
  - It is different from Quantum Key Distribution (QKD), which relies on quantum mechanics to distribute keys

Post Quantum Cryptography (PQC)

- PQC has been a very active research area in the past two decades
- Some actively researched PQC categories include
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key-based signatures
  - Elliptic curve isogeny-based





$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

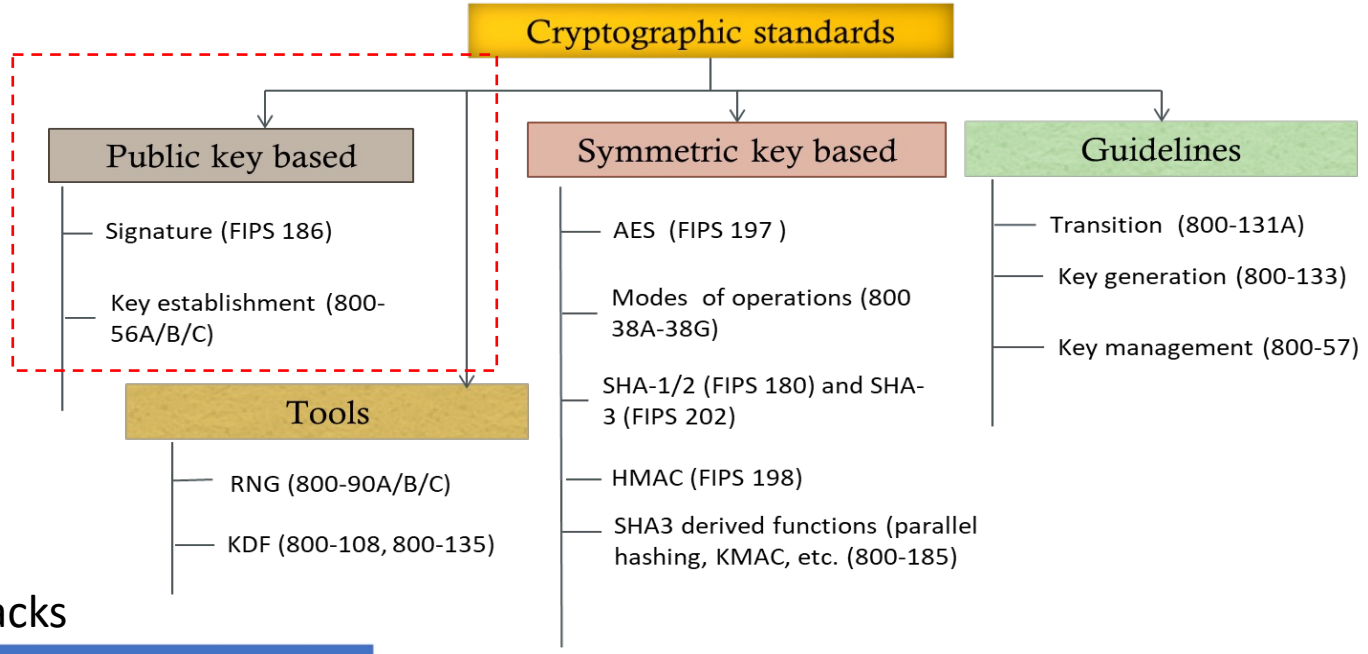
$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

NIST PQC Standards – Scope and security

- Key encapsulation mechanism (KEM)
- Digital signature



Security – against both classical and quantum attacks

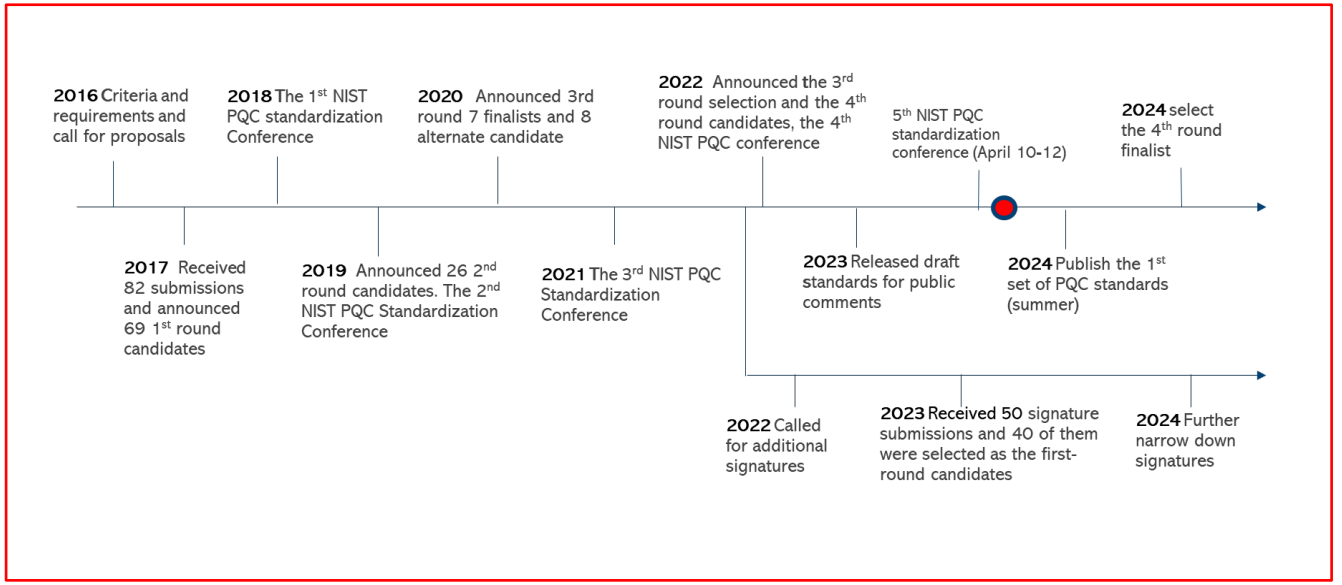
Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

Computational resources should be measured using a variety of metrics

1. Number of classical elementary operations, quantum circuit size, etc…
2. Consider realistic limitations on circuit depth (e.g. 2^{40} to 2^{80} logical gates)
3. May also consider expected relative cost of quantum and classical gates.

NIST PQC Standards – Milestones and Timeline

- NIST initiated PQC standardization process in 2016 by announcing call for proposals with requirements and criteria
- Before the deadline in 2017, NIST received 82 submissions from 25 countries in 6 continents
- NIST narrowed down the candidates three times and announced the first set of selection for standardization in 2022
- For each round, NIST published report for selection rationales and hosted conference for the experts and researchers to present their analysis and evaluation results



- NIST PQC standardization process has fully engaged with cryptography research and application community
- 2800+ individuals registered pqc-forum to discuss general and specific issues in PQC standardization

Current Status

- Selected algorithms are specified in draft FIPS and called for public comments
  - The received public comments are posted at NIST website under each of the draft FIPS
  - NIST team is actively working on the resolutions and decisions for the final publication
  - Major decisions have been presented at the 5th NIST PQC Standardization Conference and followed up in pqc-forum
- NIST plans to make the 4th round selection in 2024
- NIST called for additional signatures in 2022 to evaluate general-purpose signatures based on diversified math problems
  - Currently, 40 candidates are under consideration
  - Some candidates were presented by posters at the 5th NIST PQC Standardization Conference

Selected Algorithms and Draft FIPS

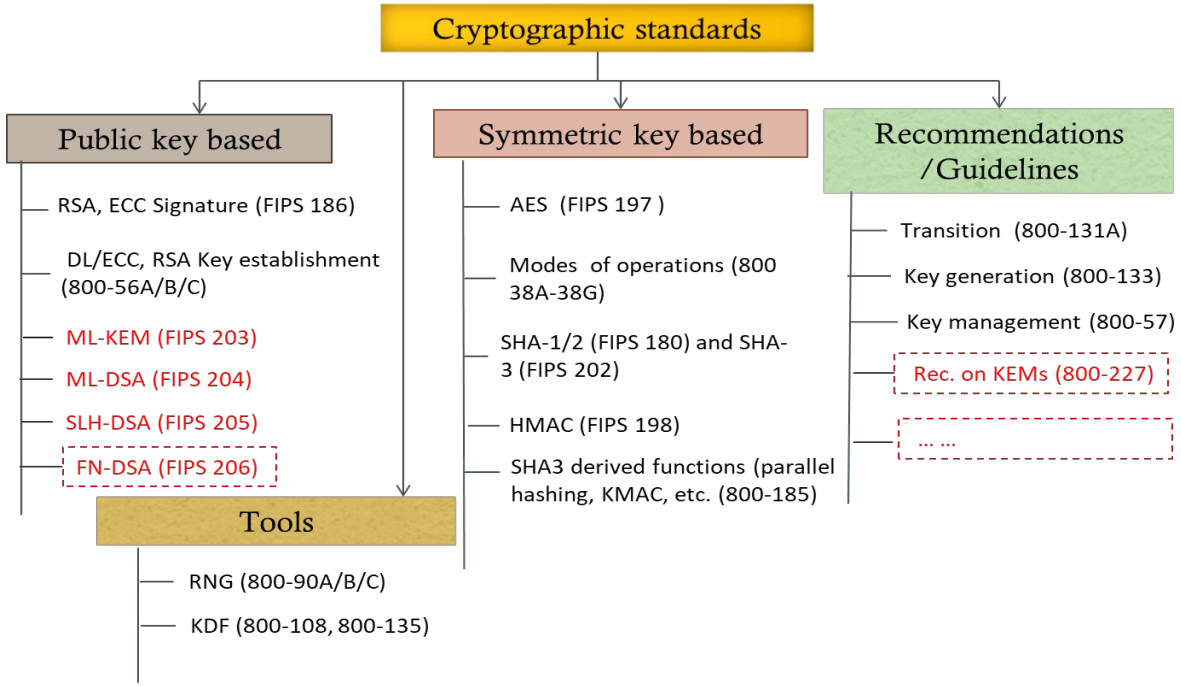
- Draft FIPS 203 “Module-Lattice-based Key-Encapsulation Mechanism Standard” (ML-KEM) (CRYSTALS-Kyber)
- Draft FIPS 204 “Module-Lattice-Based Digital Signature Standard” (ML-DSA) (CRYSTALS-Dilithium)
- Draft FIPS 205 “Stateless Hash-Based Digital Signature Standard” (SLH-DSA) (SPHINCS+)
- FALCON (Digital signature based on structured lattices) Will be specified in Draft FIPS 206, expected to be released in late 2024

The 4th round

- Classic McEliece
- BIKE
- HQC
- ~~SIKE~~

Recommendations, FIPS 140 Validations, Testing for PQC

- NIST is actively working on Special Publications to provide recommendations for the usage of PQC standards in applications, For example
  - "SP 800-227 Recommendations for key-encapsulation mechanisms" to use KEM in key establishment protocols
- NIST provided guidance for transition in the past (SP 800-131A) and will provide PQC transition guidance



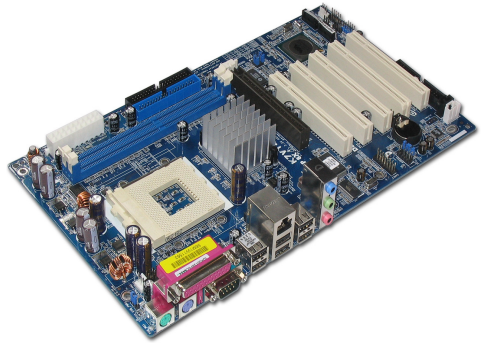
Next Generation of Cryptographic Standards

- Cryptographic standards must deal with
  - Extremely powerful attacking technologies such as quantum computers; and
  - Extremely constrained implementation environment such as IoT devices
- The PQC transition is beyond quantum vulnerable to quantum resistance
  - It is a transition to cryptographic schemes satisfying modern security concepts such as ciphertext indistinguishability under adaptive chosen ciphertext attack (IND-CCA2) for key encapsulation mechanisms (KEMs) and Existential Unforgeability under Chosen Message Attack (EUF-CMA)
- The advancement in cryptography research enables to
  - Introduce provably secure cryptographic schemes with quantum computing in mind such as under QROM model

Practical perspectives of PQC

- When deploying PQC to existing applications, performance of the new schemes must be considered
  - Performance in key generation, encapsulation/decapsulation, signing/verification
  - Bandwidth/space demanding for transmit/storage public key, signature, ciphertext
- For most selected PQC schemes, the performance is comparable or superior to currently well deployed public-key cryptography schemes such as RSA and ECC
- For PQC signatures, sizes of public-key or/and signature are significantly larger than RSA and ECC digital signatures

Scheme	Public Key (bytes)	Private Key (bytes)	Signature (bytes)	Security Level
RSA-3072	**384**	**384**	**384**	**Classical-128**
ECDSA-P256	**64**	**32**	**64**	**Classical-128**
ML-DSA-44 (Dilithium2)	**1312**	**2528**	**2420**	**PQC Category 2** *(SHA3-256)*



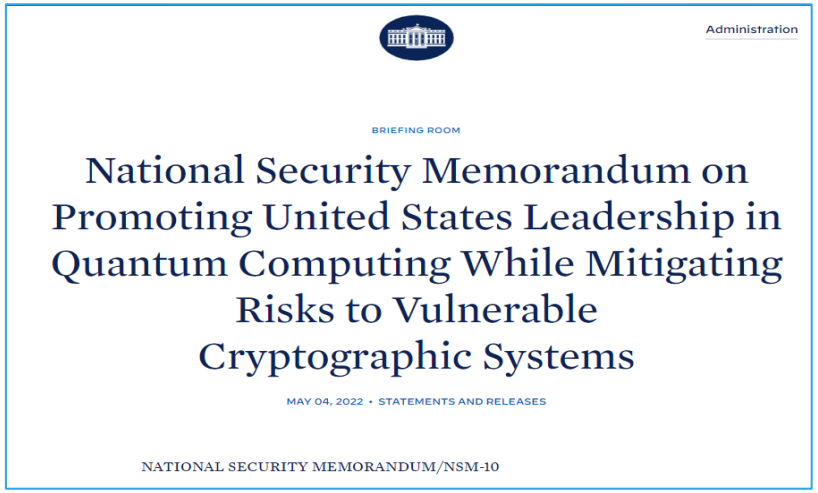
Challenges and Actions

- Billions of electronic digital devices use public key cryptography schemes such as RSA and ECC to protect communications and device integrity
  - Transition and migration must take place as soon as possible to prevent from “capturing now and decrypting later”, because some data must be protected for many years
  - It takes time to make transition in the product and introduce PQC to infrastructure
- Standards organizations and industry consortia take actions in preparing the transition
  - Discuss crypto-agility in communication protocols, software libraries, API, hardware, etc. through workshops and conferences
  - Introduce PQC to Internet protocols and public key infrastructure in IETF, e.g. exploring hybrid key establishment and dual signatures for certificate
- International Standards organizations such as ISO/IEC JTC1 SC27 initiated projects to standardize post-quantum cryptography

USG PQC migration

National Security Memo 10 (May 10, 2022)

- “The United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035.”



Administration

BRIEFING ROOM

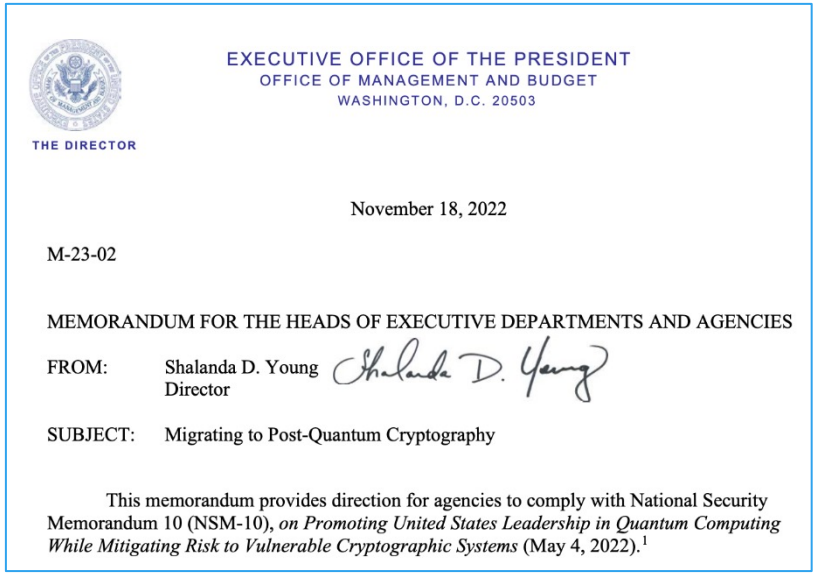
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

The OMB migration to PQC memo

- establishes requirements for agencies to inventory their active cryptographic systems, with a focus on High Value Assets (HVAs) and high impact systems.”
- requires annual assessment of funding required for migration, have already designated a migration lead, encourage testing pre-standardized pqc algorithms
- Nist will create a working group to develop best practices



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

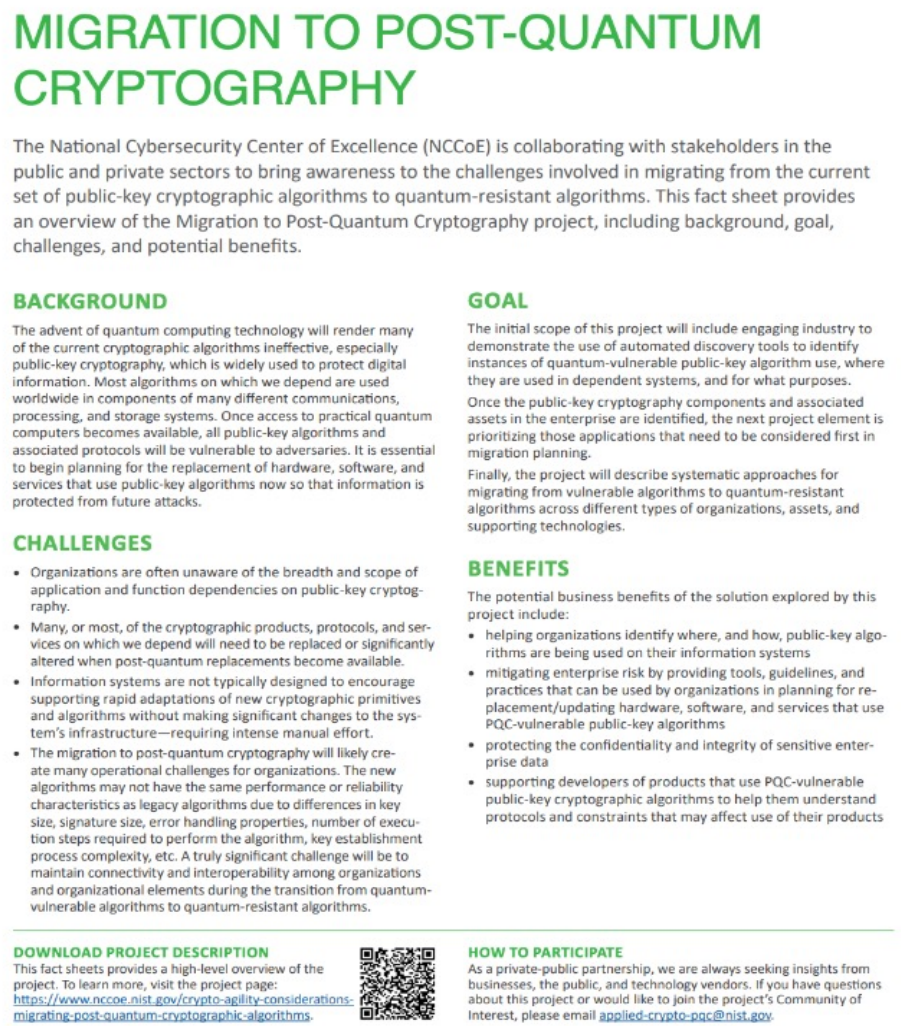
FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

NCCoE project - Migration to PQC

- National Cybersecurity Center of Excellence (NCCoE) Project for Migration to PQC
  - Collaboration with industry participants through CRADAs and a Community of Interest
- Project deliverables include
  - Draft NIST SP 1800-38B Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery
  - Draft NIST SP 1800-38C Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standard
- Testing development for PQC standards for FIPS 140 validation
  - Automated Cryptographic Validation Testing System (ACVTS)
  - Demo testing for draft algorithm standards to enable production/official testing once the standards are finalized



MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

The National Cybersecurity Center of Excellence (NCCoE) is collaborating with stakeholders in the public and private sectors to bring awareness to the challenges involved in migrating from the current set of public-key cryptographic algorithms to quantum-resistant algorithms. This fact sheet provides an overview of the Migration to Post-Quantum Cryptography project, including background, goal, challenges, and potential benefits.

BACKGROUND

The advent of quantum computing technology will render many of the current cryptographic algorithms ineffective, especially public-key cryptography, which is widely used to protect digital information. Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. Once access to practical quantum computers becomes available, all public-key algorithms and associated protocols will be vulnerable to adversaries. It is essential to begin planning for the replacement of hardware, software, and services that use public-key algorithms now so that information is protected from future attacks.

CHALLENGES

- Organizations are often unaware of the breadth and scope of application and function dependencies on public-key cryptography.
- Many, or most, of the cryptographic products, protocols, and services on which we depend will need to be replaced or significantly altered when post-quantum replacements become available.
- Information systems are not typically designed to encourage supporting rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure—requiring intense manual effort.
- The migration to post-quantum cryptography will likely create many operational challenges for organizations. The new algorithms may not have the same performance or reliability characteristics as legacy algorithms due to differences in key size, signature size, error handling properties, number of execution steps required to perform the algorithm, key establishment process complexity, etc. A truly significant challenge will be to maintain connectivity and interoperability among organizations and organizational elements during the transition from quantum-vulnerable algorithms to quantum-resistant algorithms.

GOAL

The initial scope of this project will include engaging industry to demonstrate the use of automated discovery tools to identify instances of quantum-vulnerable public-key algorithm use, where they are used in dependent systems, and for what purposes.

Once the public-key cryptography components and associated assets in the enterprise are identified, the next project element is prioritizing those applications that need to be considered first in migration planning.

Finally, the project will describe systematic approaches for migrating from vulnerable algorithms to quantum-resistant algorithms across different types of organizations, assets, and supporting technologies.

BENEFITS

The potential business benefits of the solution explored by this project include:

- helping organizations identify where, and how, public-key algorithms are being used on their information systems
- mitigating enterprise risk by providing tools, guidelines, and practices that can be used by organizations in planning for replacement/updating hardware, software, and services that use PQC-vulnerable public-key algorithms
- protecting the confidentiality and integrity of sensitive enterprise data
- supporting developers of products that use PQC-vulnerable public-key cryptographic algorithms to help them understand protocols and constraints that may affect use of their products

DOWNLOAD PROJECT DESCRIPTION

This fact sheets provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have questions about this project or would like to join the project's Community of Interest, please email applied-crypto-pqc@nist.gov.

Summary

- Cryptography has been the cornerstone for cybersecurity
- Cryptographic Relevant Quantum Computers (CRQC) will catastrophically break the well-deployed public-key cryptosystems
- NIST has been developing PQC standards for cybersecurity applications
- The first set of NIST PQC standards will be published in 2024
- It is time to prepare the migration to PQC for cybersecurity in quantum time

Thanks!

For NIST PQC standardization
Check out www.nist.gov/pqcrypto
Sign up for the pqc-forum for announcements & discussion
Contact us at: pqc-comments@nist.gov