NIST POST-QUANTUM CRYPTOGRAPHY UPDATE

Dustin Moody
Computer Security Division
NIST

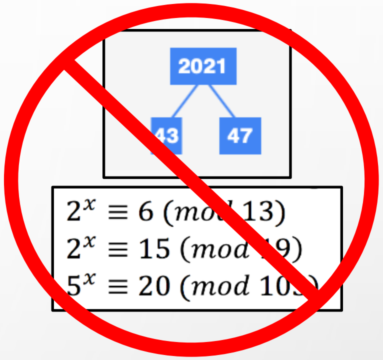
National Institute of Standards and Technology
U.S. Department of Commerce

THE QUANTUM THREAT

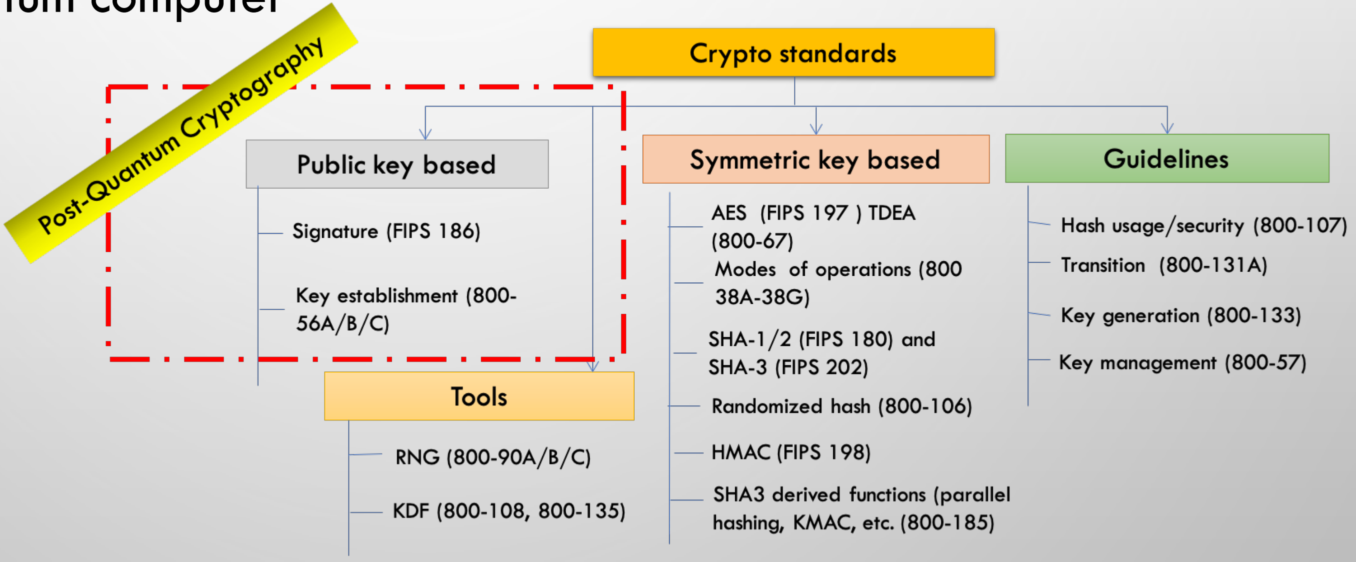
- NIST public-key crypto standards
  - **SP 800-56A**: Diffie-Hellman, ECDH
  - **SP 800-56B**: RSA encryption
  - **FIPS 186**: RSA, DSA, and ECDSA signatures

all vulnerable to attacks from

a (large-scale) quantum computer



2021
43
47
$2^x \equiv 6\ (mod\ 13)$
$2^x \equiv 15\ (mod\ 19)$
$5^x \equiv 20\ (mod\ 10$



Post-Quantum Cryptography

Crypto standards

Public key based
- Signature (FIPS 186)
- Key establishment (800-56A/B/C)

Symmetric key based
- AES (FIPS 197) TDEA (800-67)
- Modes of operations (800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- Randomized hash (800-106)
- HMAC (FIPS 198)
- SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)

Guidelines
- Hash usage/security (800-107)
- Transition (800-131A)
- Key generation (800-133)
- Key management (800-57)

Tools
- RNG (800-90A/B/C)
- KDF (800-108, 800-135)

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

THE NIST PQC "COMPETITION"

- IN 2016, NIST CALLED FOR QUANTUM-RESISTANT CRYPTOGRAPHIC ALGORITHMS FOR NEW PUBLIC-KEY CRYPTO STANDARDS
  - DIGITAL SIGNATURES
  - ENCRYPTION/KEY-ESTABLISHMENT
- OUR ROLE: MANAGING A PROCESS OF ACHIEVING COMMUNITY CONSENSUS IN A **TRANSPARENT** AND TIMELY MANNER
- DIFFERENT AND MORE COMPLICATED THAN PAST AES/SHA-3 COMPETITIONS
- THERE WOULD NOT BE A SINGLE "WINNER"
  - IDEALLY, SEVERAL ALGORITHMS WILL EMERGE AS 'GOOD CHOICES'

THE FIRST THREE ROUNDS

2016: NIST ANNOUNCES PROCESS FOR PQC STANDARDIZATION

2017: INITIAL SUBMISSIONS (64 ACCEPTED: 19 SIGS + 45 KEMS)

2019: 2ND ROUND START (26 SCHEMES: 9 SIGS + 17 KEMS)

2020: 3RD ROUND START (7 FINALISTS, 8 ALTERNATES):

	Finalists	Alternates
KEM	Kyber, NTRU, Saber, Classic McEliece	Bike, FrodoKEM, HQC, NTRUPrime, SIKE
Signature	Dilithium, Falcon, ~~Rainbow~~	~~GeMSS~~, Picnic, SPHINCS+

ROUND 3 RESULTS

ROUND 3 RESULTS

KEMs	Signatures
CRYSTALS-Kyber	**CRYSTALS-Dilithium, Falcon, SPHINCS+**

See NISTIR 8413, *Status Report on the 3rd Round of the NIST PQC Standardization Process*, for the rationale on the selections

4th round candidates (all KEMs) evaluated for 18-24 months

- ClassicMcEliece
- BIKE
- HQC
- ~~SIKE~~

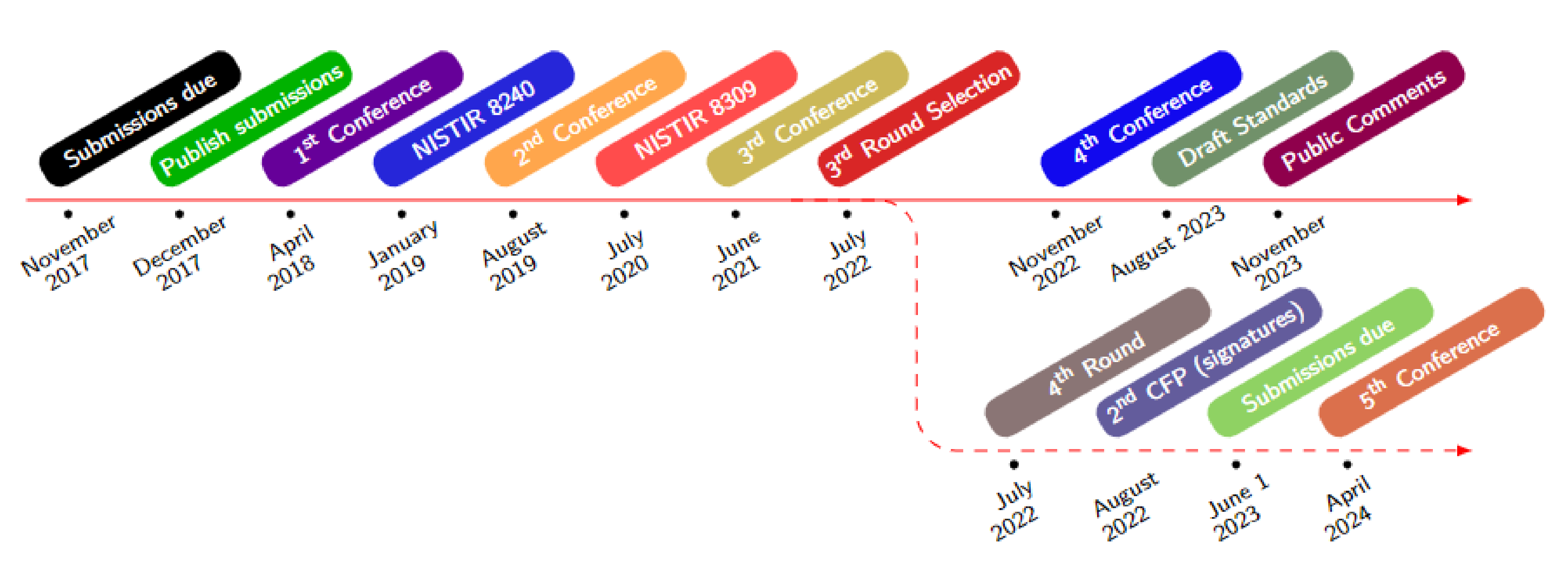
On-ramp signatures

- NIST issued a new call for additional signatures – preferably for signatures based on non-lattice problems

THE SELECTED ALGORITHMS

- CRYSTALS-KYBER
  - KEM BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY
- CRYSTALS-DILITHIUM
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY, RELATIVELY SIMPLE IMPLEMENTATION
  - NIST RECOMMENDS IT BE THE PRIMARY SIGNATURE ALGORITHM USED
- FALCON
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - SMALLER BANDWIDTH, BUT MUCH MORE COMPLICATED IMPLEMENTATION
  - THE FALCON STANDARD WILL COME OUT AFTER THE OTHERS
- SPHINCS+
  - DIGITAL SIGNATURE BASED ON STATELESS HASH-BASED CRYPTOGRAPHY
  - SOLID SECURITY, BUT PERFORMANCE NOT AS GOOD IN COMPARISON TO DILITHIUM/FALCON

TIMELINE



- The 5th NIST PQC Standardization Conference
  - April 10-12, 2024 in Rockville, Maryland

- Draft standards for public comment released Aug 2023
  - Deadline for comments: November 22, 2023

- **The first PQC standards should be published in 2024**

STANDARDIZATION

- THE 1ST PQC STANDARDS
    - FIPS 203: ML-KEM (KYBER)
    - FIPS 204: ML-DSA (DILITHIUM)
    - FIPS 205: SLH-DSA (SPHINCS+)
    - FN-DSA (FALCON) – UNDER DEVELOPMENT
  - WILL HAVE OTHER DOCS WITH MORE GUIDANCE/DETAILS
- SOME CHOICES MADE
  - WHICH PARAMETER SETS, WHICH HASH FUNCTIONS, OTHER SYMMETRIC PRIMITIVES, ETC
- PLEASE PROVIDE FEEDBACK
  - PQC-FORUM, EMAIL ETC

THE KEMS IN THE 4TH ROUND

- Classic McEliece
  - NIST is confident in the security
  - Smallest ciphertexts, but largest public keys
  - We'd like feedback on specific use cases for Classic McEliece

- BIKE
  - Most competitive performance of 4th round candidates
  - We encourage vetting of IND-CCA security
- HQC
  - Offers strong security assurances and mature decryption failure rate analysis
  - Larger public keys and ciphertext sizes than BIKE
- SIKE
  - The SIKE team acknowledges that SIKE (and SIDH) are insecure and should not be used

AN ON-RAMP FOR SIGNATURES

- Scope:
  - NIST is primarily interested in additional general-purpose signature schemes that are not based on structured lattices.

- (No on-ramp for KEMs currently planned)

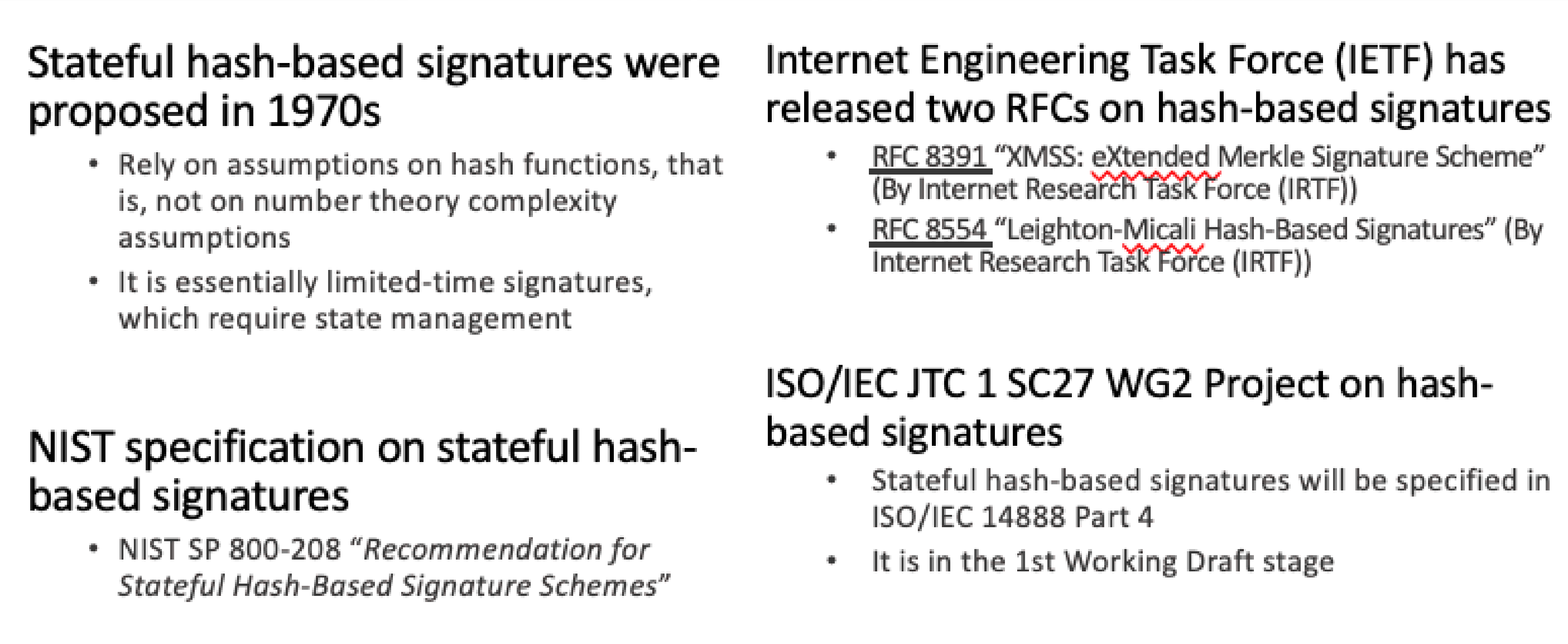
- July 2023: 40 submissions accepted
  - From 5 continents and 28 countries

- For complete specs (including code):

  see www.nist.gov/pqcrypto

Type	Number
Lattice	7
Code-based	6
Multivariate	11
MPC in the head	6
Symmetric	4
Isogeny	1
Other	5
Total	40

STATEFUL HASH BASED SIGNATURES FOR EARLY ADOPTION



Stateful hash-based signatures were proposed in 1970s

- Rely on assumptions on hash functions, that is, not on number theory complexity assumptions
- It is essentially limited-time signatures, which require state management

NIST specification on stateful hash-based signatures

- NIST SP 800-208 "*Recommendation for Stateful Hash-Based Signature Schemes*"

Internet Engineering Task Force (IETF) has released two RFCs on hash-based signatures

- RFC 8391 "XMSS: eXtended Merkle Signature Scheme" (By Internet Research Task Force (IRTF))
- RFC 8554 "Leighton-Micali Hash-Based Signatures" (By Internet Research Task Force (IRTF))

ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

- Stateful hash-based signatures will be specified in ISO/IEC 14888 Part 4
- It is in the 1st Working Draft stage

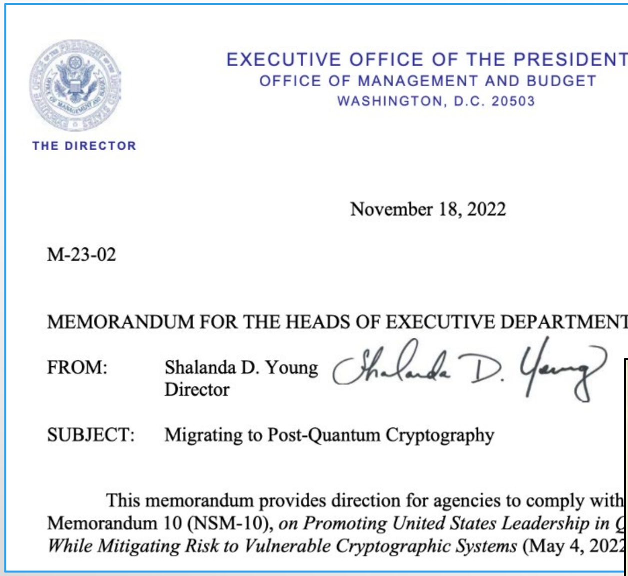
Stateful hash-based signatures from SP 800-208 are allowed for signing software/firmware updates in CNSA 2.0

OTHER STANDARDS ORGANIZATIONS

- WE ARE AWARE THAT MANY STANDARDS ORGANIZATIONS AND EXPERT GROUPS ARE WORKING ON PQC
  - ASC X9 HAS DONE STUDIES AND WRITTEN WHITE PAPERS
  - IEEE P1363.3 HAS STANDARDIZED SOME LATTICE-BASED SCHEMES
  - IETF HAS STANDARDIZED STATEFUL HASH-BASED SIGNATURES LMS/XMSS AND IS CURRENTLY DOING NEW WORK GEARED TO THE PQC MIGRATION
  - ETSI HAS RELEASED QUANTUM-SAFE CRYPTOGRAPHY REPORTS
  - EU EXPERT GROUPS PQCRYPTO AND SAFECRYPTO MADE RECOMMENDATIONS AND RELEASED REPORTS
  - ISO/IEC JTC 1 SC27 WG2 IS DEVELOPING A STANDARD TO SPECIFY PQC ALGORITHMS AS AN AMENDMENT TO ISO/IEC 18033-2
- NIST IS INTERACTING AND COLLABORATING WITH THESE ORGANIZATIONS AND GROUPS

- SOME COUNTRIES HAVE BEGUN STANDARDIZATION ACTIVITIES

RECENT GUIDANCE



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

THE DIRECTOR

November 18, 2022

M-23-02

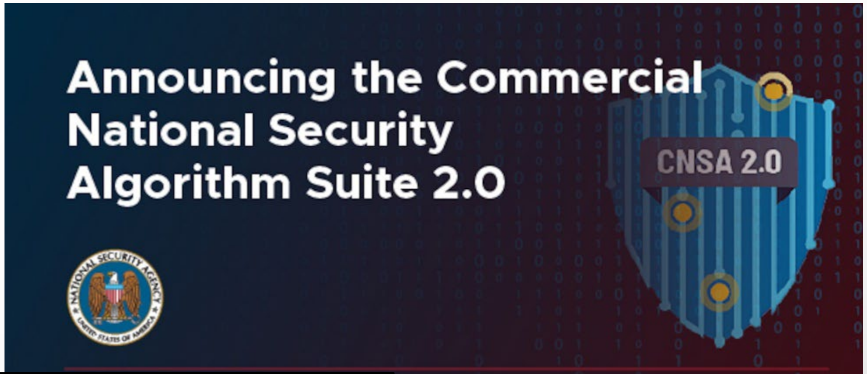
MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

Shalanda D. Young

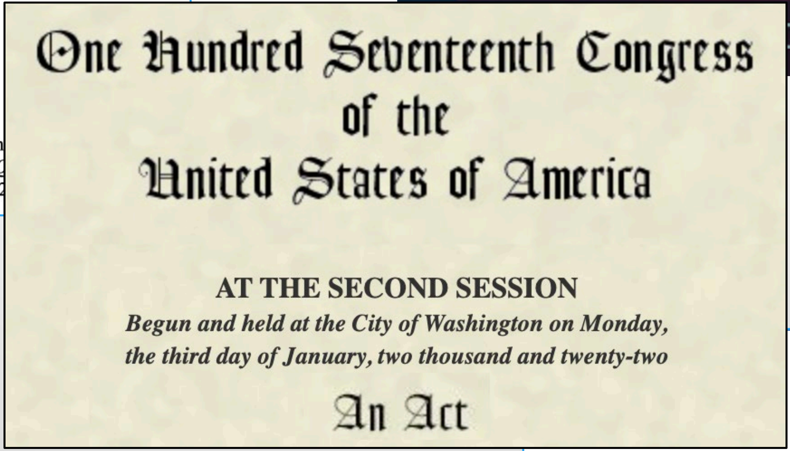
SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with
Memorandum 10 (NSM-10), *on Promoting United States Leadership in Q*
While Mitigating Risk to Vulnerable Cryptographic Systems (May 4, 2022



Announcing the Commercial National Security Algorithm Suite 2.0

DVISORY



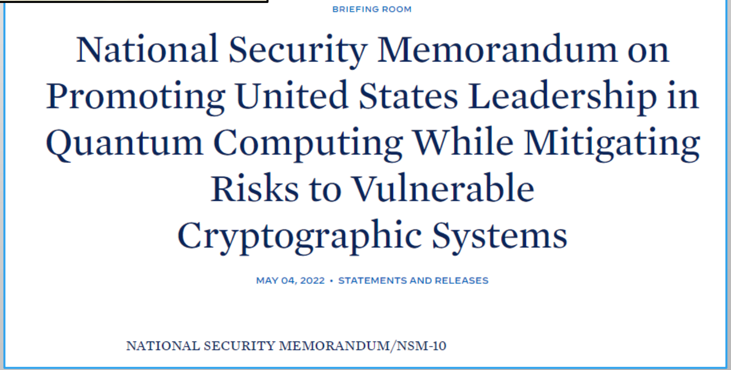
One Hundred Seventeenth Congress
of the
United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Monday,
the third day of January, two thousand and twenty-two

An Act

”The United States must prioritize the 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

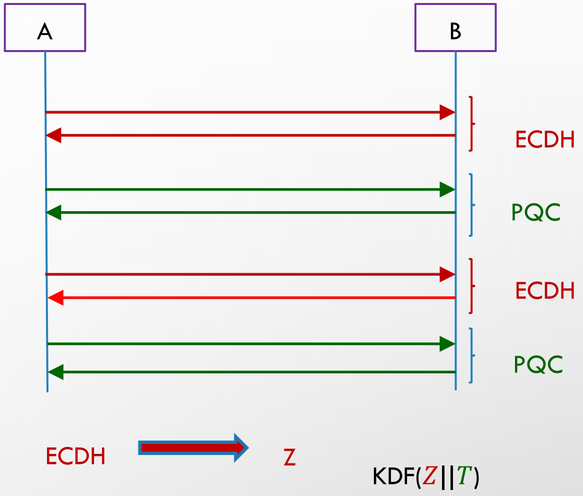
National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

TRANSITION AND MIGRATION

- THERE HAS BEEN MUCH DISCUSSION ON HYBRID/COMPOSITE MODES
    - NIST SP800-56C REV. 2 ALLOWS FOR A CERTAIN HYBRID MODE
- NIST WILL PROVIDE TRANSITION GUIDELINES TO PQC STANDARDS
    - NIST HAS PROVIDED SUCH GUIDANCE BEFORE
        - EXAMPLES: TRIPLE DES, SHA-1, KEYS < 112 BITS
- NEW CISA/NSA/NIST FACTSHEET: *QUANTUM READINESS – MIGRATION TO POST-QUANTUM CRYPTOGRAPHY*
    - CRYPTOGRAPHIC INVENTORY
    - DISCUSS POST-QUANTUM ROADMAP W/ TECHNOLOGY VENDORS
    - SUPPLY CHAIN QUANTUM-READINESS



A

B

ECDH

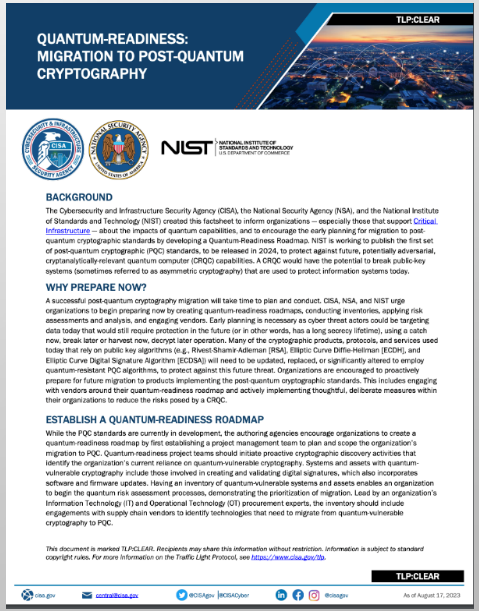
PQC

ECDH

PQC

ECDH → Z

$KDF(Z||T)$



TLP:CLEAR

QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

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

BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and the National Institute of Standards and Technology (NIST) created this factsheet to inform organizations — especially those that support Critical Infrastructure — about the impacts of quantum capabilities, and to encourage the early planning for migration to post-quantum cryptographic standards by developing a Quantum-Readiness Roadmap. NIST is working to publish the first set of post-quantum cryptographic (PQC) standards, to be released in 2024, to protect against future, potentially adversarial, cryptanalytically-relevant quantum computer (CRQC) capabilities. A CRQC would have the potential to break public-key systems (sometimes referred to as asymmetric cryptography) that are used to protect information systems today.

WHY PREPARE NOW?

A successful post-quantum cryptography migration will take time to plan and conduct. CISA, NSA, and NIST urge organizations to begin preparing now by creating quantum-readiness roadmaps, conducting inventories, applying risk assessments and analysis, and engaging vendors. Early planning is necessary as cyber threat actors could be targeting data today that would still require protection in the future (or in other words, has a long secrecy lifetime), using a catch now, break later or harvest now, decrypt later operation. Many of the cryptographic products, protocols, and services used today that rely on public key algorithms (e.g., Rivest-Shamir-Adleman [RSA], Elliptic Curve Diffie-Hellman [ECDH], and Elliptic Curve Digital Signature Algorithm [ECDSA]) will need to be updated, replaced, or significantly altered to employ quantum-resistant PQC algorithms, to protect against this future threat. Organizations are encouraged to proactively prepare for future migration to products implementing the post-quantum cryptographic standards. This includes engaging with vendors around their quantum-readiness roadmap and actively implementing thoughtful, deliberate measures within their organizations to reduce the risks posed by a CRQC.

ESTABLISH A QUANTUM-READINESS ROADMAP

While the PQC standards are currently in development, the authoring agencies encourage organizations to create a quantum-readiness roadmap by first establishing a project management team to plan and scope the organization's migration to PQC. Quantum-readiness project teams should initiate proactive cryptographic discovery activities that identify the organization's current reliance on quantum-vulnerable cryptography. Systems and assets with quantum-vulnerable cryptography include those involved in creating and validating digital signatures, which also incorporates software and firmware updates. Having an inventory of quantum-vulnerable systems and assets enables an organization to begin the quantum risk assessment processes, demonstrating the prioritization of migration. Lead by an organization's Information Technology (IT) and Operational Technology (OT) procurement experts, the inventory should include engagements with supply chain vendors to identify technologies that need to migrate from quantum-vulnerable cryptography to PQC.

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

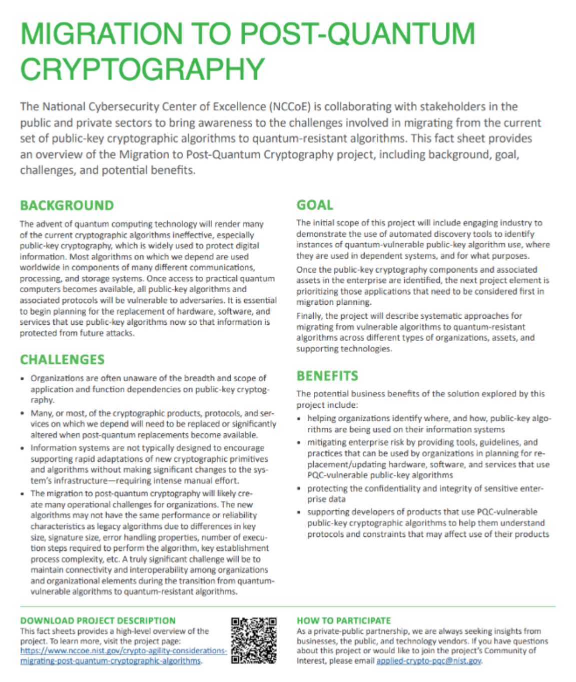
TLP:CLEAR

cisa.gov central@cisa.gov @CISAgov |@CISACyber @cisagov As of August 17, 2023

THE NCCOE MIGRATION TO PQC PROJECT

- COMPLEMENT STANDARDIZATION AND TACKLE CHALLENGES WITH ADOPTION, IMPLEMENTATION AND DEPLOYMENT TO PQC
    - COORDINATE WITH SDO'S AND INDUSTRY COLLABORATORS
- PRODUCT DELIVERABLES
    - PRACTICE GUIDES, PLAYBOOKS, REFERENCE ARCHITECTURES, AUTOMATED TOOLS, PROOF OF CONCEPT CODE, ETC
    - DRAFT SP 1800-38 VOLUME A
- OUTREACH AND ENGAGEMENT
    - COMMUNITY OF INTEREST, WEBINARS, PUBLIC EVENTS
    - IN PERSON MEETING – AUG 15 AT NCCOE
    - APPLIED-CRYPTO-PQC@NIST.GOV

NCCoE
NATIONAL
CYBERSECURITY
CENTER OF
EXCELLENCE



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

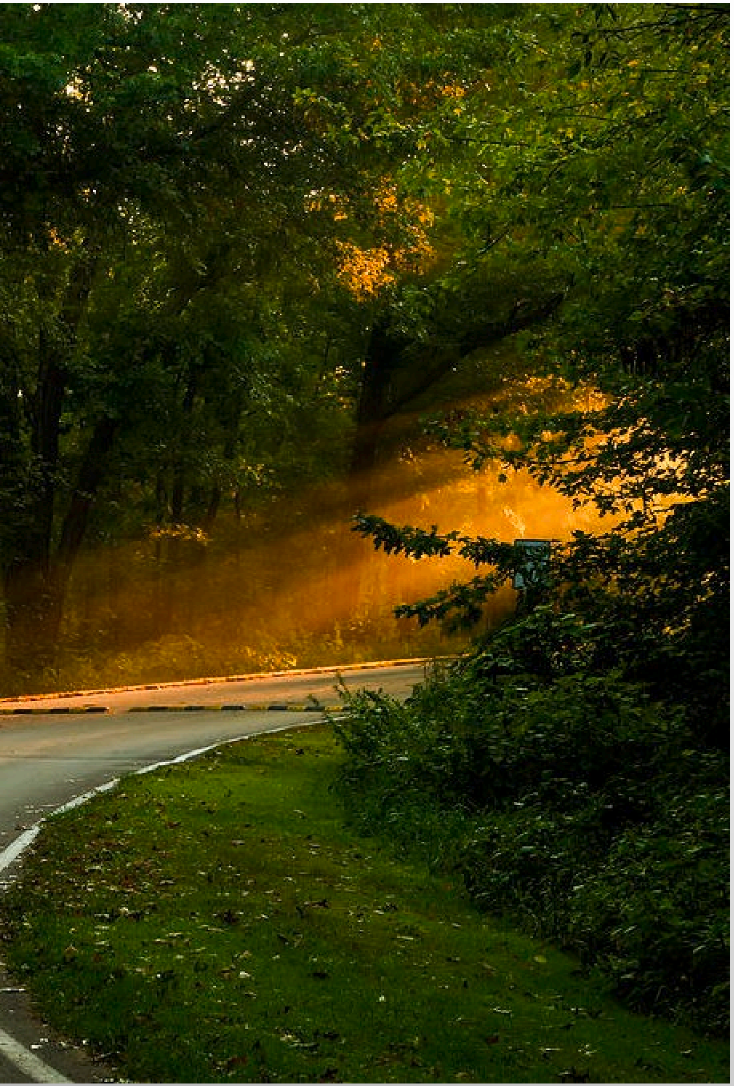
DOWNLOAD PROJECT DESCRIPTION

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.

CONCLUSION



- THE BEGINNING OF THE END IS HERE!
- OR IS IT THE END OF THE BEGINNING?

- NIST IS GRATEFUL FOR EVERYBODY’S EFFORTS

- CHECK OUT WWW.NIST.GOV/PQCRYPTO
  - SIGN UP FOR THE PQC-FORUM FOR ANNOUNCEMENTS & DISCUSSION
  - SEND E-MAIL TO PQC-COMMENTS@NIST.GOV