ARE WE THERE YET?

AN UPDATE ON THE NIST PQC STANDARDIZATION PROJECT

Dustin Moody
Computer Security Division
NIST PQC

THE QUANTUM THREAT

FIPS 186-5

FEDERAL INFORMA

(Supersedes FIPS 186-4)

Digital Signatur

CATEGORY: COMPUTER

ST Special Publication 800-56B
Revision 2

endation for Pair-Wise
lishment Using Integer
rization Cryptography

T Special Publication 800-56A
Revision 3

endation for Pair-Wise
shment Schemes Using
garithm Cryptography

- Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically

POST-QUANTUM CRYPTOGRAPHY

- Need to find cryptographic algorithms that 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*, also known 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 cryptography or quantum key distribution (QKD)

HOW SOON SHOULD WE WORRY?

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
Memorandum 10 (NSM-10), *on Promoting United States Leadership in Q*
While Mitigating Risk to Vulnerable Cryptographic Systems (May 4, 2022

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

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'

ROUND 3 RESULTS

3rd round selection (KEM)	3rd round selection (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

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

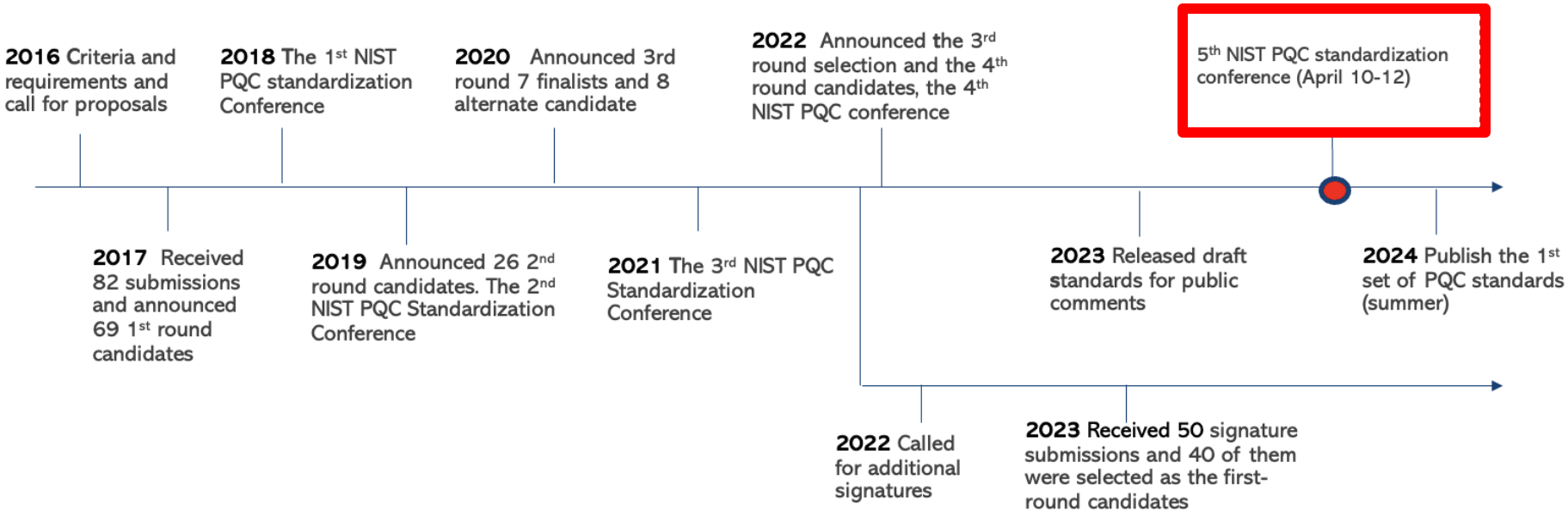
On-ramp signatures

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

STANDARDIZATION

- THE 1ST PQC DRAFT 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

- 90 DAY COMMENT PERIOD (AUG-NOV 2023)
  - SEE COMMENTS AT WWW.NIST.GOV/PQCRYPTO
  - LOTS OF DISCUSSION ON PQC-FORUM

WRITING THE STANDARDS

- FOLLOW THE 3RD ROUND SPECIFICATIONS
  - THESE HAVE BEEN THOROUGHLY ANALYZED
- MINOR TWEAKS
  - TO ENSURE THAT THE STANDARDS CAN BE IMPLEMENTED SUCCESSFULLY BY A VARIETY OF USERS IN DIFFERENT SITUATIONS
  - SPECIFY WHAT NEEDS TO BE SPECIFIED, ALLOW FLEXIBILITY WHEN APPROPRIATE
  - PLAY NICELY WITH OTHER PARTS OF THE CYBERSECURITY ECOSYSTEM:
    - OUR STANDARDS FOR RNGS AND HASH FUNCTIONS
    - HIGHER-LEVEL PROTOCOLS
    - PROCEDURES FOR TESTING AND VALIDATION
  - GET FEEDBACK FROM IMPLEMENTERS, THINKING THROUGH ALL ISSUES BEFORE THE FINAL STANDARD

THE PATH TO THE FINAL STANDARDS

- WE ARE FINISHING OUR REVISIONS BASED ON THE PUBLIC COMMENTS
- NIST WILL DESCRIBE THE RESOLUTIONS LATER TODAY
  - WE'LL ALSO POST ON THE PQC-FORUM
  - WE WILL SOLICIT QUICK FEEDBACK ON SOME POINTS
- WE WILL THEN HAVE IT REVIEWED INTERNALLY AND PREPARED FOR PUBLICATION
  - **THE GOAL FOR PUBLICATION IS SUMMER 2024**
- THE FINAL VERSIONS WILL BE SUBMITTED TO THE SECRETARY OF COMMERCE FOR APPROVAL
  - THERE WILL BE A FEDERAL REGISTER NOTICE (FRN) ANNOUNCING THE PUBLICATION
  - THE FRN WILL ALSO INCLUDE A SUMMARY OF THE PUBLIC COMMENTS AND OUR RESPONSES, INCLUDING IF WE MADE ANY CHANGES

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

The 4th Round will likely end in the fall of 2024

AN ON-RAMP FOR SIGNATURES

- Scope:
  - 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 with short signatures and fast verification.
  - Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.

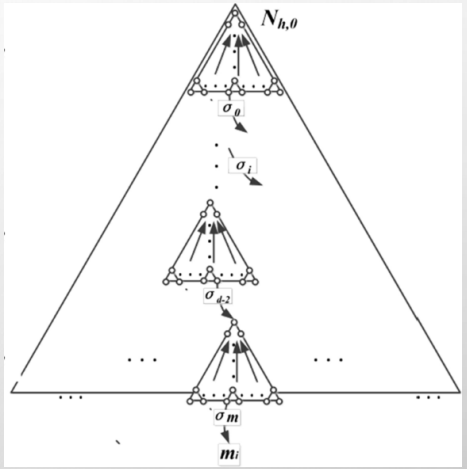
- 40 Signature candidates currently in Round 1
  - Poster session later today and tomorrow

- Selections for Round 2 will be within a few months
- Any standardization will not be for a few years

No on-ramp for KEMs currently planned.

STATEFUL HASH BASED SIGNATURES FOR EARLY ADOPTION

- Stateful hash-based signatures have been around since the 1970s
  - Security only relies on hash functions, and not number theory assumptions
  - It is critical to manage the state to not allow key re-use



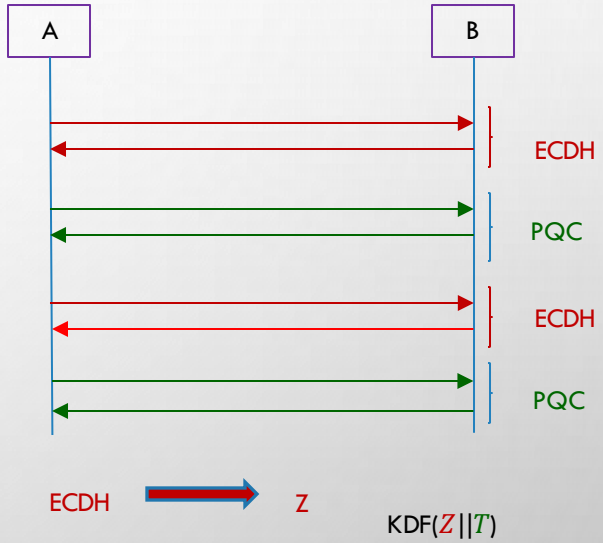
- Standardized and ready to use for certain applications
  - IETF: RFCs 8391 and 8554
  - NIST: SP 800-208
  - ISO/IEC JTC 1 SC 27 WG2 (in 1st working draft stage)

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

- SP 800-208 is being revised, based on industry feedback
  - How to allow backups for HSMs w/o allowing re-use of one-time keys?

TRANSITION AND MIGRATION

- THERE HAS BEEN MUCH DISCUSSION ON HYBRID MODES
  - NIST SP800-56C REV. 2 ALLOWS FOR A CERTAIN HYBRID MODE
    - SP 800-227 SHOULD HAVE MORE TO SAY
  - WE WILL WORK WITH THE COMMUNITY IN DIFFERENT STAGES OF MIGRATION TO ASSURE SECURITY
- NIST WILL PROVIDE TRANSITION GUIDELINES TO PQC STANDARDS
  - NIST HAS PROVIDED SUCH GUIDANCE BEFORE
    - EXAMPLES: TRIPLE DES, SHA-1, KEYS < 112 BITS
  - TIMEFRAME WILL BE BASED ON RISK ASSESSMENT OF QUANTUM ATTACKS

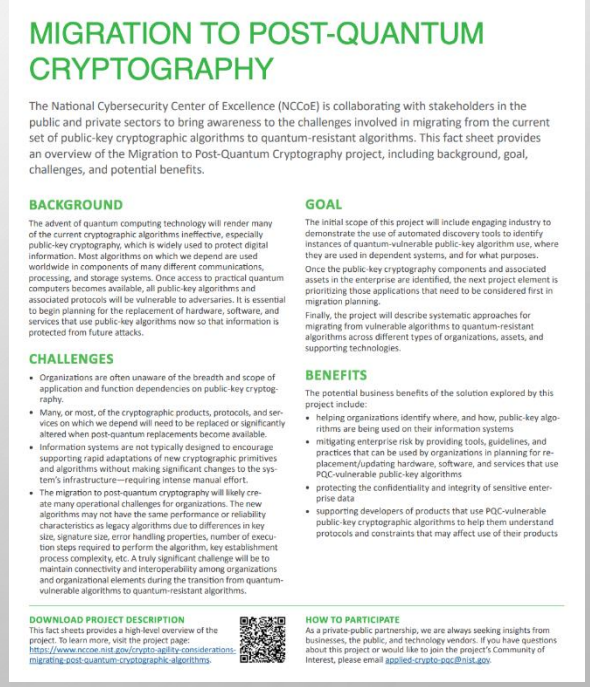


THE NCCOE MIGRATION TO PQC PROJECT

- COMPLEMENT STANDARDIZATION AND TACKLE CHALLENGES WITH ADOPTION, IMPLEMENTATION AND DEPLOYMENT TO PQC
  - COORDINATE WITH SDO'S AND INDUSTRY COLLABORATORS
  - DRAFT SP 1800-38 VOLUMES A, B, AND C

- WORKSTREAMS
  - DISCOVERY, INTEROPERABILITY, PERFORMANCE

- OUTREACH AND ENGAGEMENT
  - SEE THE PROJECT PANELS ON THURSDAY, FRIDAY
  - COMMUNITY OF INTEREST, WEBINARS, PUBLIC EVENTS
  - APPLIED-CRYPTO-PQC@NIST.GOV



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
  - WE ARE COLLABORATING WITH OTHER STANDARDIZATION ACTIVITIES

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