THE FIRST NIST PQC STANDARDS

Dustin Moody
Computer Security Division
NIST

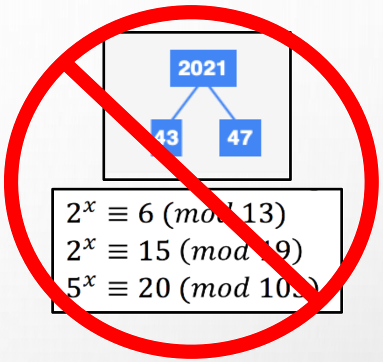
NIST National Institute of Standards and Technology
U.S. Department of Commerce

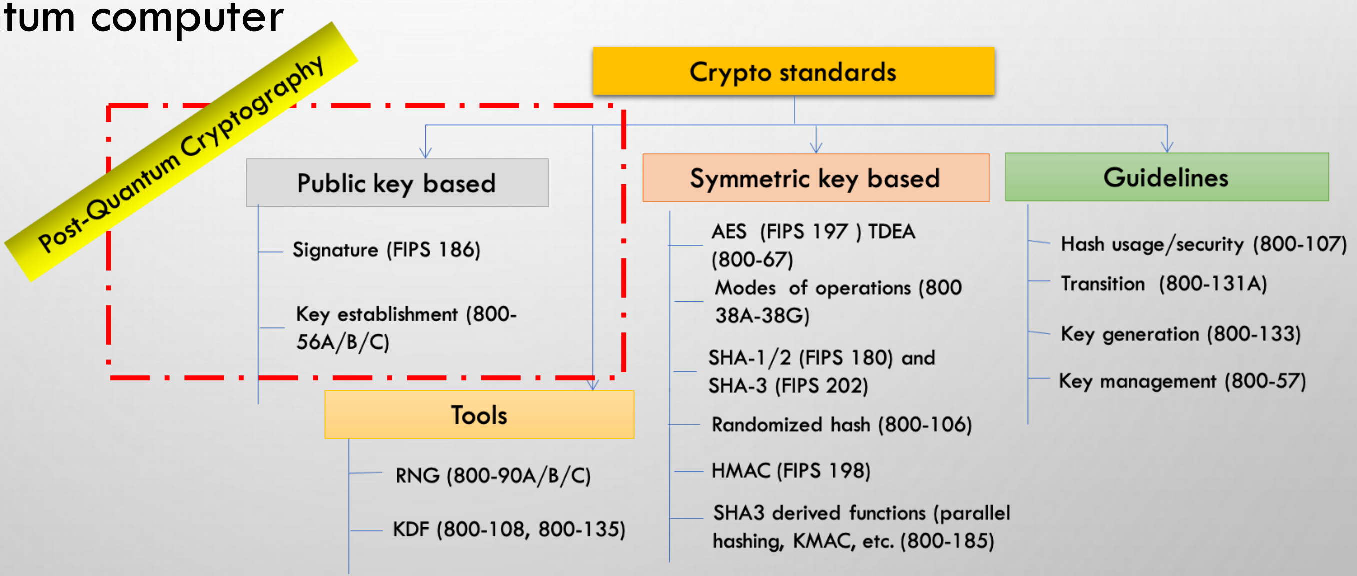
THE QUANTUM THREAT

- 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





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

HOW SOON SHOULD WE WORRY?

NIST

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

Announcing the Commercial National Security Algorithm Suite 2.0

CNSA 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

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 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.”

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'

Credit: Pixabay

ROUND 3 RESULTS

ROUND 3 RESULTS

3rd round selection (KEM)	3rd round selection (Signatures)
CRYSTALS-Kyber	**CRYSTALS-Dilithium, Falcon, SPHINCS+**

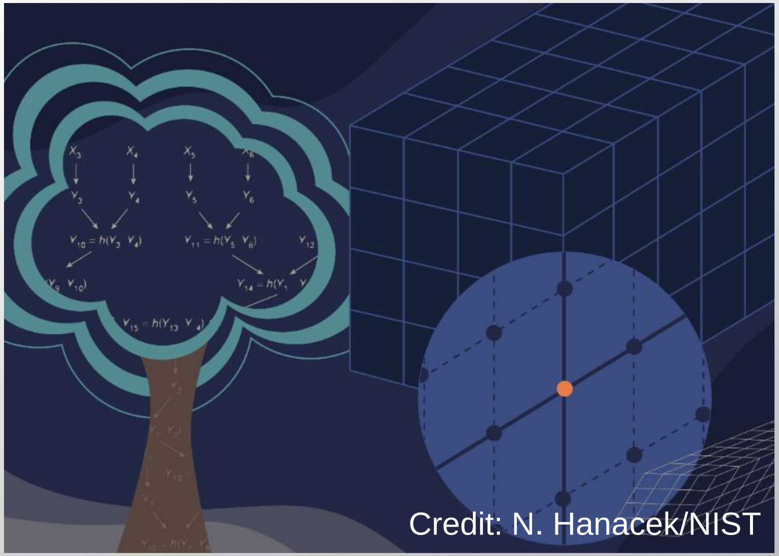
See NISTIR 8413, *Status Report on the 3rd Round of the NIST PQC Standardization Process*, for the rationale on the selections

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

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

On-ramp signatures

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



Credit: N. Hanacek/NIST

STANDARDIZATION

- THE 1ST PQC STANDARDS (AUG 2024)
    - FIPS 203: ML-KEM (KYBER)
    - FIPS 204: ML-DSA (DILITHIUM)
    - FIPS 205: SLH-DSA (SPHINCS+)
    - FIPS 206: FN-DSA (FALCON) – UNDER DEVELOPMENT
  - WILL HAVE OTHER DOCS WITH MORE GUIDANCE/DETAILS
  - TESTING/VALIDATION ALREADY POSSIBLE

- SOME SMALL TWEAKS, CHOICES MADE
    - WHICH PARAMETER SETS, WHICH HASH FUNCTIONS, OTHER SYMMETRIC PRIMITIVES, ETC

- SEE COMMENTS AT WWW.NIST.GOV/PQCRYPTO
- LOTS OF DISCUSSION ON PQC-FORUM

Credit: Pixabay

FIPS 203: ML-KEM

- KEY-ENCAPSULATION MECHANISM BASED ON CRYSTALS-KYBER
- COMPLETE SPECIFICATION
  - ALL ALGORITHMS NEEDED TO IMPLEMENT KEYGEN, ENCAPS, AND DECAPS
- SOME REQUIREMENTS, BUT MORE TO COME IN SP 800-227
  - SP 800-227 WILL DISCUSS HYBRID KEMS
- PARAMETER SETS INCLUDED: SECURITY CATEGORIES 1, 3, AND 5
- DIFFERENCES FROM THE ROUND 3 SUBMISSION
  - KEY IS FIXED TO 256 BITS
  - FO TRANSFORM TWEAKED
  - ENCAPS RANDOMNESS NOT HASHED
  - SOME INPUT VALIDATION STEPS ADDED
  - DOMAIN SEPARATION ADDED

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security — Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Table 2. Approved parameter sets for ML-KEM

	n	q	k	η_1	η_2	d_u	d_v	required RBG strength (bits)
ML-KEM-512	256	3329	2	3	2	10	4	128
ML-KEM-768	256	3329	3	2	2	10	4	192
ML-KEM-1024	256	3329	4	2	2	11	5	256

Table 3. Sizes (in bytes) of keys and ciphertexts of ML-KEM

	encapsulation key	decapsulation key	ciphertext	shared secret key
ML-KEM-512	800	1632	768	32
ML-KEM-768	1184	2400	1088	32
ML-KEM-1024	1568	3168	1568	32

FIPS 204: ML-DSA

NIST

- SIGNATURE SCHEME BASED ON CRYSTALS-DILITHIUM
- COMPLETE SPECIFICATION
  - ALL ALGORITHMS NEEDED TO IMPLEMENT KEYGEN, SIGN, VERIFY
  - NO FLOATING POINT ARITHMETIC
  - ALSO INCLUDES PRE-HASH VERSION: HASH ML-DSA
- SOME REQUIREMENTS (SEE ALSO SP 800-89)
- PARAMETER SETS INCLUDED: SECURITY CATEGORIES 2, 3, AND 5
- DIFFERENCES FROM THE ROUND 3 SUBMISSION
  - A FEW VARIABLE SIZES CHANGED TO INCREASE SECURITY
  - RANDOMIZED VERSION ALSO, NOT JUST DETERMINISTIC
  - DOMAIN SEPARATION ADDED

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.204

Published August 13, 2024

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

U.S. Department of Commerce
Gina M. Raimondo, Secretary

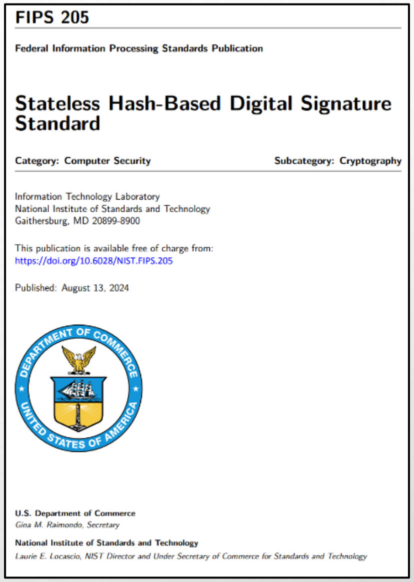
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Table 2. Sizes (in bytes) of keys and signatures of ML-DSA

	Category	Private Key	Public Key	Signature Size
ML-DSA-44	2	2560	1312	2420
ML-DSA-65	3	4032	1952	3309
ML-DSA-87	5	4896	2592	4627

FIPS 205: SLH-DSA

- SIGNATURE SCHEME BASED ON SPHNICS+
- COMPLETE SPECIFICATION
  - ALL ALGORITHMS NEEDED TO IMPLEMENT KEYGEN, SIGN, VERIFY
  - BASED ON HASH-BASED CRYPTOGRAPHY
  - HAS ”SMALL”, “FAST”, SHA2, AND SHAKE VERSIONS
  - ALSO INCLUDES PRE-HASH VERSION: HASH SLH-DSA
- SOME REQUIREMENTS (SEE ALSO SP 800-89)
- PARAMETER SETS INCLUDED: SECURITY CATEGORIES 1, 3, AND 5
- DIFFERENCES FROM THE ROUND 3 SUBMISSION:
  - SMALLER NUMBER OF PARAMETER SETS
  - MITIGATION AGAINST MULTI-KEY ATTACKS
  - MITIGATION AGAINST PRE-IMAGE ATTACKS
  - USE SHA-512 INSTEAD OF SHA-256 IN PLACES



FIPS 205

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205

Published: August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Table 2. SLH-DSA parameter sets

	n	h	d	h'	a	k	lg_w	m	security category	pk bytes	sig bytes
SLH-DSA-SHA2-128s SLH-DSA-SHAKE-128s	16	63	7	9	12	14	4	30	1	32	7 856
SLH-DSA-SHA2-128f SLH-DSA-SHAKE-128f	16	66	22	3	6	33	4	34	1	32	17 088
SLH-DSA-SHA2-192s SLH-DSA-SHAKE-192s	24	63	7	9	14	17	4	39	3	48	16 224
SLH-DSA-SHA2-192f SLH-DSA-SHAKE-192f	24	66	22	3	8	33	4	42	3	48	35 664
SLH-DSA-SHA2-256s SLH-DSA-SHAKE-256s	32	64	8	8	14	22	4	47	5	64	29 792
SLH-DSA-SHA2-256f SLH-DSA-SHAKE-256f	32	68	17	4	9	35	4	49	5	64	49 856

FIPS 206: FN-DSA

- SIGNATURE SCHEME BASED ON FALCON
- DRAFT FIPS TO BE PUBLISHED BY END OF 2024 (HOPEFULLY ☺)
  - WILL HAVE 90 DAYS FOR PUBLIC COMMENTS
- WILL HAVE A PRE-HASH VERSION
- PARAMETER SETS INCLUDED: SECURITY CATEGORIES 1 AND 5
- HEAVY USE OF FLOATING POINT ARITHMETIC
- DIFFERENCES FROM THE ROUND 3 SUBMISSION:
  - KEYGEN ALGORITHM FROM HAWK (TO AVOID FLOATING POINT)
  - WILL ALLOW EMULATED FLOATING POINT

	Private Key	Public Key	Signature Size
FN-DSA-512	1281	897	666
FN-DSA-1024	2305	1793	1280

Table 2. Sizes (in bytes) of keys and signatures of FN-DSA.

UPDATES ON
FIPS 140 VALIDATION PROGRAM

NIST

August 2024

Cryptographic Algorithm Validation Program Demo Server

ML-KEM
ML-DSA
SLH-DSA

- **Cryptographic Algorithm Validation Program**
  - Automated Cryptographic Validation Testing System (ACVTS) https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/how-to-access-acvts
  - Testing for algorithm standards to enable production/official testing
    https://github.com/usnistgov/ACVP-Server
    Test vectors are available:
    https://github.com/usnistgov/ACVP-Server/tree/master/gen-val/
- FIPS 140 implementation guidance on self-test requirements are developed in collaboration with the Cryptographic Module User https://www.cmuf.org/
- **FIPS 203 ML-KEM**
  - Key Generation, Encapsulation, Decapsulation
- **FIPS 204 ML-DSA**
  - Key Generation, Signature Generation, Signature Verification
- **FIPS 205 SLH-DSA**
  - Key Generation, Signature Generation, Signature Verification

https://pages.nist.gov/ACVP/#module-lattice-algorithms

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

Credit: iStock

- 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 be over by the end of 2024

AN ON-RAMP FOR SIGNATURES

NIST

- 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.

Credit: Pixabay

- 40 Signature candidates currently in Round 1
  - Poster session at our April conference
- For complete specs (including code): see www.nist.gov/pqcrypto
- Selections for Round 2 will be in the fall/winter of 2024

No on-ramp for KEMs currently planned.

IMPACT AND WIDER ADOPTION

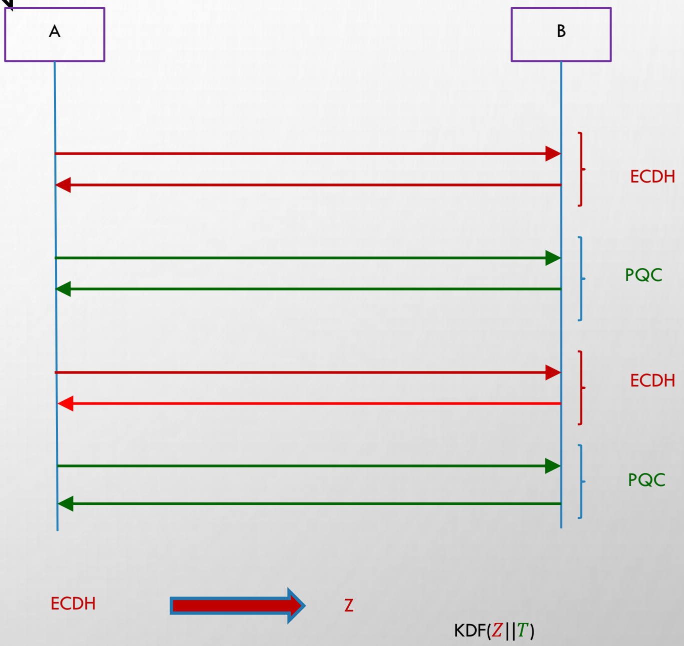
NIST

- 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
    - HTTPS://GITHUB.COM/IETF-WG-PQUIP/STATE-OF-PROTOCOLS-AND-PQC
  - 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

TRANSITION AND MIGRATION

- **HYBRID**: USING CLASSICAL AND PQC ALGORITHMS TOGETHER
  - REDUCES RISKS FROM UNCERTAINTY IF EITHER IS BROKEN
  - MORE COMPLEXITY / SLOWER PERFORMANCE
  - SEVERAL POSSIBLE APPROACHES
  - CAN GET FIPS 140 VALIDATION
    - NIST SP800-56C REV. 2 ALLOWS FOR A CERTAIN HYBRID MODE
  - MORE GUIDANCE TO COME IN SP 800-227

- USE OF HYBRID WILL DEPEND ON COMMUNITY AND APPLICATION-SPECIFIC NEEDS
  - NIST DOES NOT INTEND TO RECOMMEND FOR/AGAINST HYBRID SCHEMES
  - IMPLEMENTERS SHOULD CONSIDER COMPLEXITY AND MIGRATION ISSUES
  - ARCHITECTURES /APPLICATIONS MAY SUPPORT MULTIPLE ALGORITHMS



TRANSITION AND MIGRATION

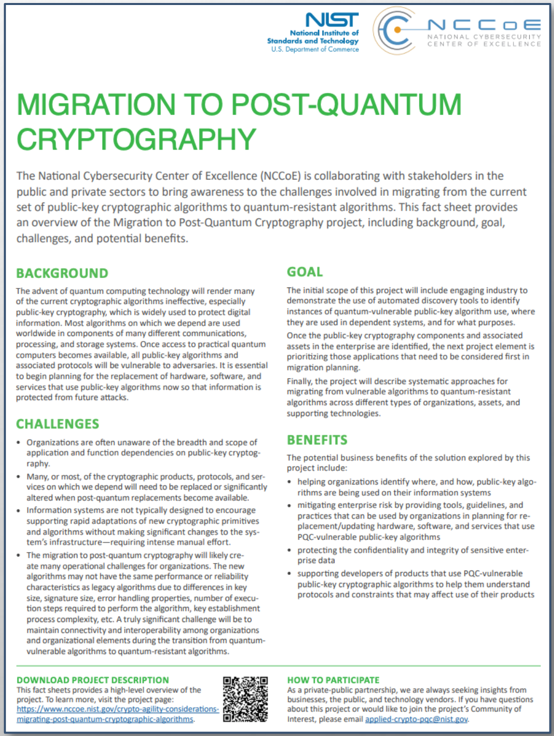
- NIST WILL PROVIDE TRANSITION GUIDANCE TO PQC
  - NIST HAS PROVIDED SUCH GUIDANCE BEFORE
    - EXAMPLES: TRIPLE DES, SHA-1, KEYS < 112 BITS
  - NSM 10: "*WITHIN 90 DAYS OF THE PQC STANDARDS, NIST SHALL RELEASE A PROPOSED TIMELINE FOR THE DEPRECATION OF QUANTUM-VULNERABLE CRYPTOGRAPHY IN STANDARDS*"
  - TRANSITION GUIDELINES AND DEPRECATION TIMELINES
    - TIMEFRAME WILL BE BASED ON RISK ASSESSMENT OF QUANTUM ATTACKS
- DOCUMENTS BEING UPDATED

SP 800-227	SP 800-89
SP 800-208	SP 800-57 Part 1
SP 800-185	SP 800-230
SP 800-175B	SP 800-131A

NCCOE MIGRATION TO PQC PROJECT

- Tackle challenges with ***adoption, implementation, and deployment*** of PQC
- Engage with ***industry and government*** to raise awareness of the issues involved in migrating to post-quantum algorithms
- Coordinate with ***standards developing organizations*** and ***government/industry*** to develop guidance to accelerate the migration
  - Draft NIST SP 1800-38B *Quantum Readiness: Cryptographic Discovery*
  - Draft NIST SP 1800-38C *Quantum Readiness: Testing Draft Standards for Interoperability and Performance*
- Support ***US Government PQC initiatives***
  - White House NSM-10 (M-23-02)
  - NSA CNSA 2.0

Contact: 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.

ASPECTS OF CRYPTOGRAPHIC AGILITY

NIST

May 2024

NIST Started the discussion with the NIST PQC consortium to develop guidance to support migration use cases

- **Motivations** for crypto-agility in migration (designers, developers, implementers, users, etc.)

- Crypto-agility **guiding principles**
  - Independence to applications
  - Simplicity
  - Abstraction
  - Exchangeability
  - Manageability
  - Portability

- **Security** considerations
  - Attack surface
  - Downgrade attacks

- **Maturity model**
  - Measurements, testing, and validation

- A **framework** approach
  - Modularity and abstraction
  - Dynamic configuration and management
  - Algorithm adaptability and standardization

- Crypto-agility **technical mechanisms**
  - Protocol level negotiation
  - API abstraction for applications
  - Libraries for algorithms
  - Hardware accelerators

- **Resource and performance**
  - Hardware, firmware, software, and communication protocols
  - Microcontrollers to clouds

- **Legal** and **regulatory** considerations

- **Use cases** driven demonstrations to inform development of practical guidance

CONCLUSION

NIST

- 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

- THE NCCOE MIGRATION TO PQC PROJECT
  - HTTPS://WWW.NCCOE.NIST.GOV/CRYPTO-AGILITY-CONSIDERATIONS-MIGRATING-POST-QUANTUM-CRYPTOGRAPHIC-ALGORITHMS
  - CONTACT EMAIL: APPLIED-CRYPTO-PQC@NIST.GOV