Post-Quantum Cryptography

Andy Regenscheid, Manager
Cryptographic Technology Group, NIST

Tuesday, October 3rd, 2023

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

PQC– Much Work Remains

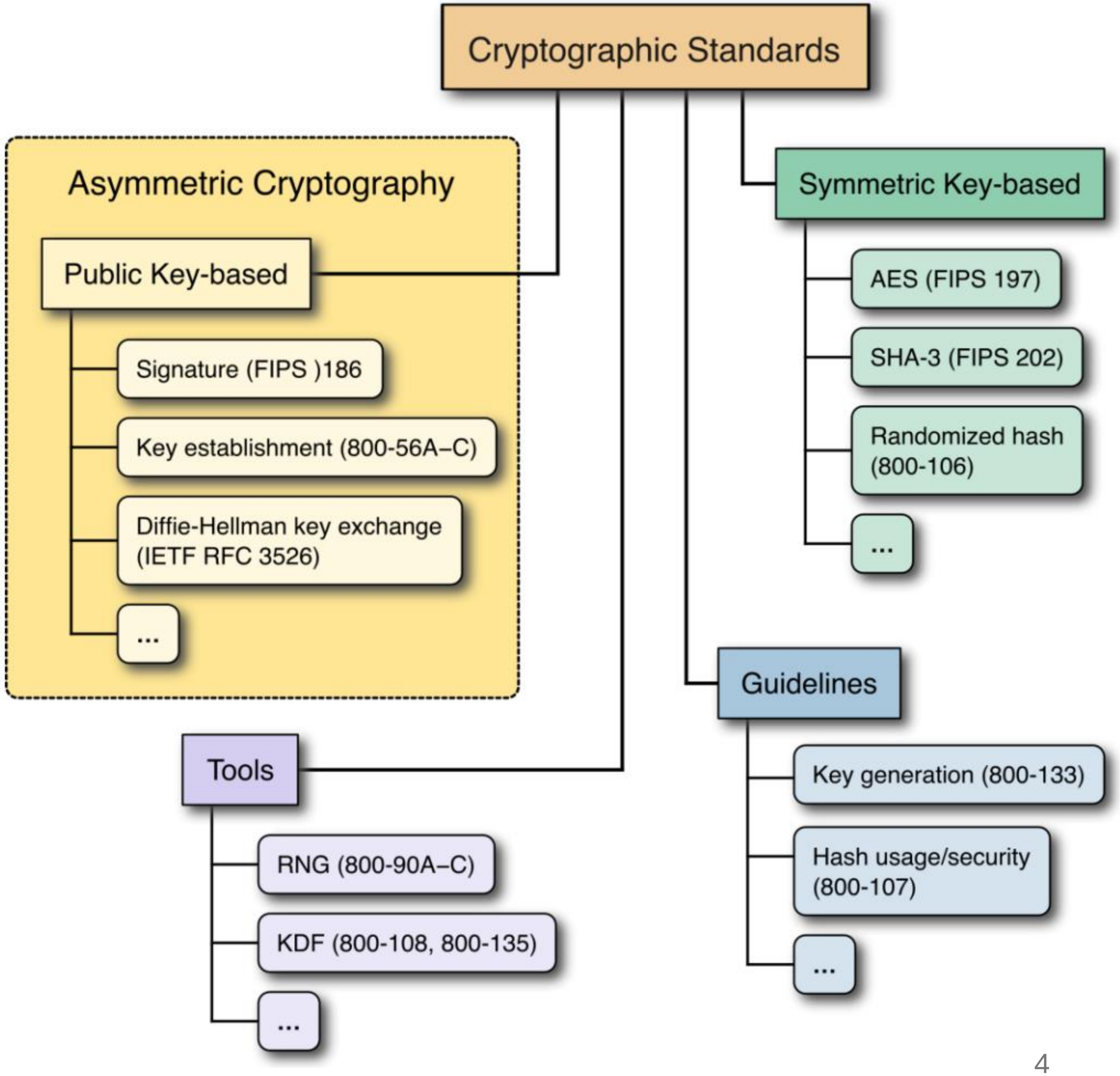
- Operations
- Infrastructure Modernization
- PQC Adoption in Software/Systems
- Hardware Acceleration/Support
- Implementation in Cryptographic Libraries
- Protocol/Application Standards
- $\mathbb{Z}_q[X]$ Algorithm Standards

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

PQC Algorithms

PQC Selection Process

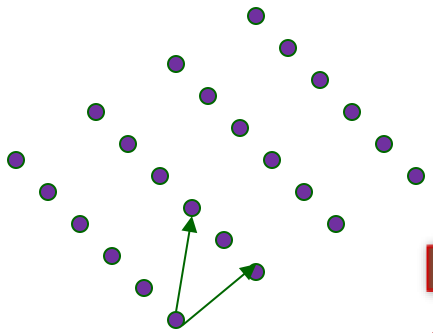
- **Quantum computers threaten the security of current, widely-deployed public key cryptosystems**
  - *Signatures*– ECDSA, RSA
  - *Key Establishment*–Diffie-Hellman, RSA
- Quantum computers changed what we have believed about the hardness
  - By Shor’s algorithm, factorization and discrete logarithm problems can be solved by quantum computers in polynomial time
- Quantum computing also impacts security strength of symmetric key based cryptography algorithms – manageable by increasing key size
  - Grover’s algorithm provides quadratic speedup

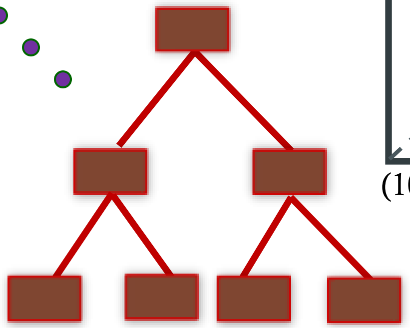


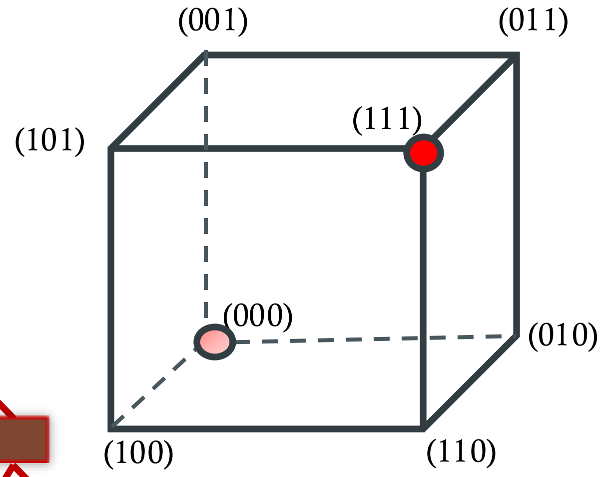
Post Quantum Cryptography (PQC)

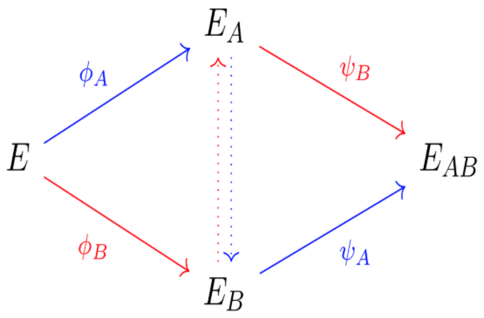
- PQC has been a very active research area in the past two decades

- 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 – Milestones and Timeline

NIST

2010-2015– NIST PQC project team builds & First PQC Conference

2016– Determined criteria and requirements, Call for proposals

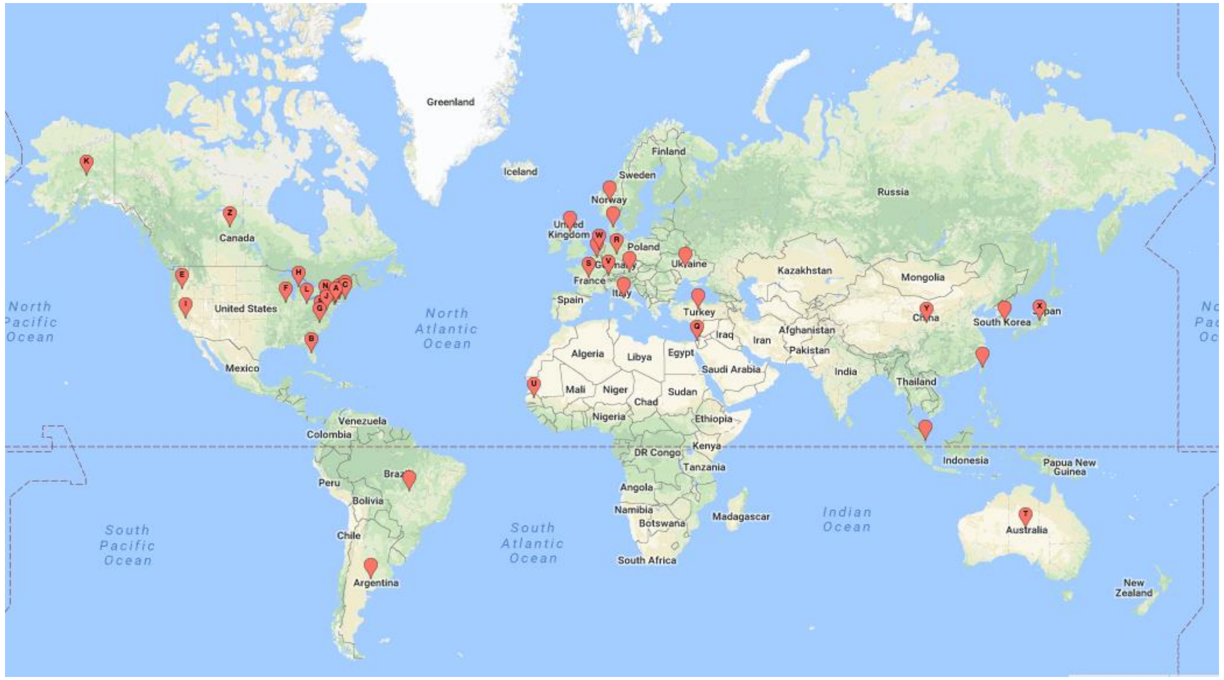
2017– Received 82 submissions, ***69 First Round candidates***

2018– 1st NIST PQC Standardization Conference

2019 – Announced ***26 Second Round candidates***
Released NISTIR 8240
Held the 2nd NIST PQC Standardization Conference

2020– Announced ***7 finalists & 8 alternate candidates***
Released NISTIR 8309

2021– Hold 3rd NIST PQC Standardization Conference



2022– ***Announced Initial Selections for Standardization & 4th Round Candidates***
Held 4th NIST PQC Standardization Conference

2023 Release draft standards and call for public comments

2024- Release Initial Final Standards

NIST PQC Algorithm Standards

Key Encapsulation	Digital Signatures
Lattice-Based: • **CRYSTALS-Kyber** → ML-KEM (FIPS 203)	***Lattice-Based*** • **CRYSTALS-Dilithium** → ML-DSA (FIPS 204) • **FALCON** → FN-DSA *(Standard forthcoming)* ***Hash-Based*** • **SPHINCS+** → SLH-DSA (FIPS 205)

4th round KEMs

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

Onramp signatures

40 new signature algorithm candidates received in response to a call for algorithms based on different hardness assumptions.

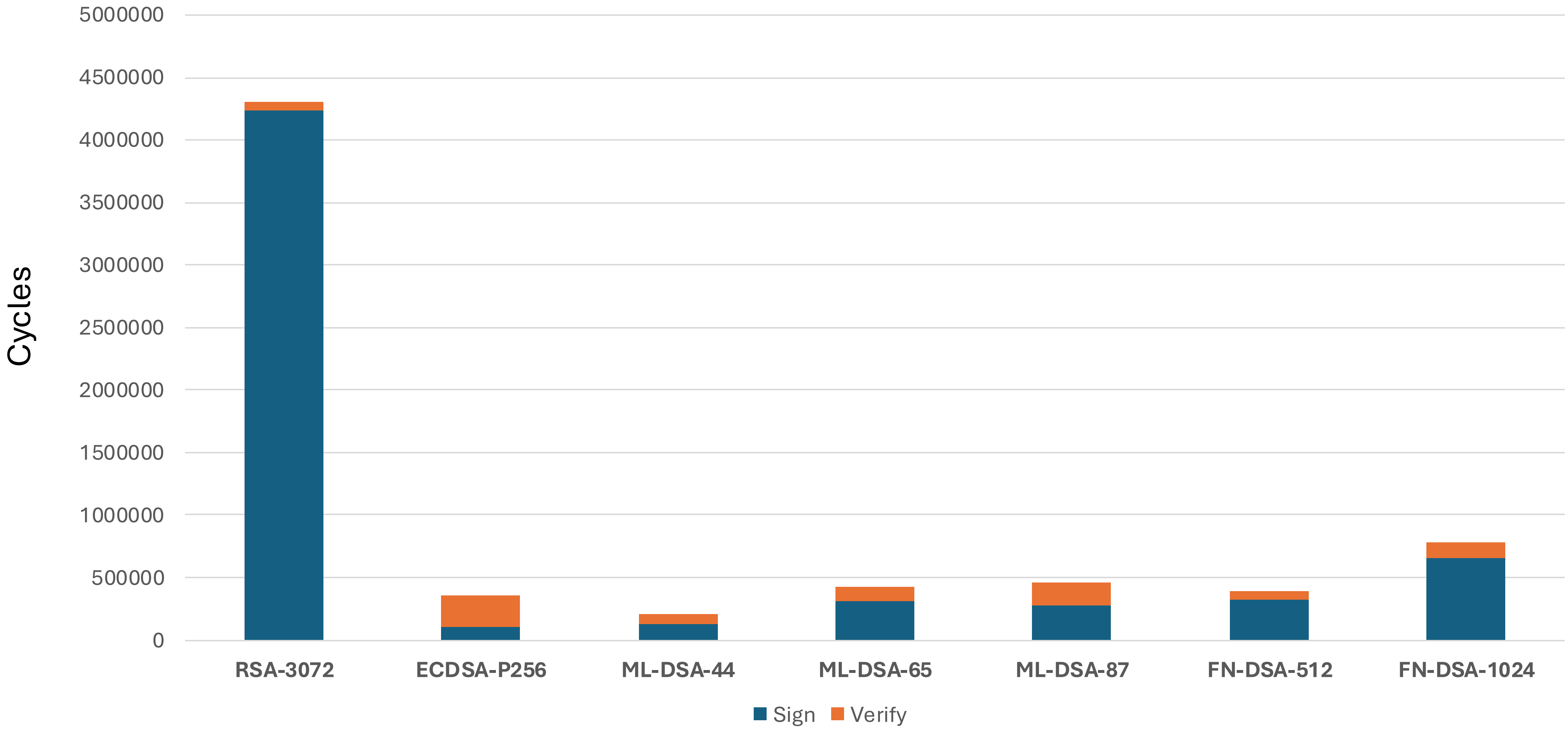
PQC Signatures- Security

- Both ML-DSA (*Dilithium*) and FN-DSA (*Falcon*) are based on lattices
  - ML-DSA is based on module-LWE, FN-DSA is based on SIS over NTRU lattices
  - Best known attacks amount to applying generic algorithms for finding short vectors in lattices
  - During the third round, some results improving the dual attack
- ML-DSA offers parameter sets for security categories 2, 3, and 5
- FN-DSA offers parameter sets for security categories 1 and 5
- Both ML-DSA and FN-DSA have similar levels of core SVP hardness
- The complex FN-DSA implementation may make side-channel attack protection difficult

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

Standards

PQC Signatures– Performance

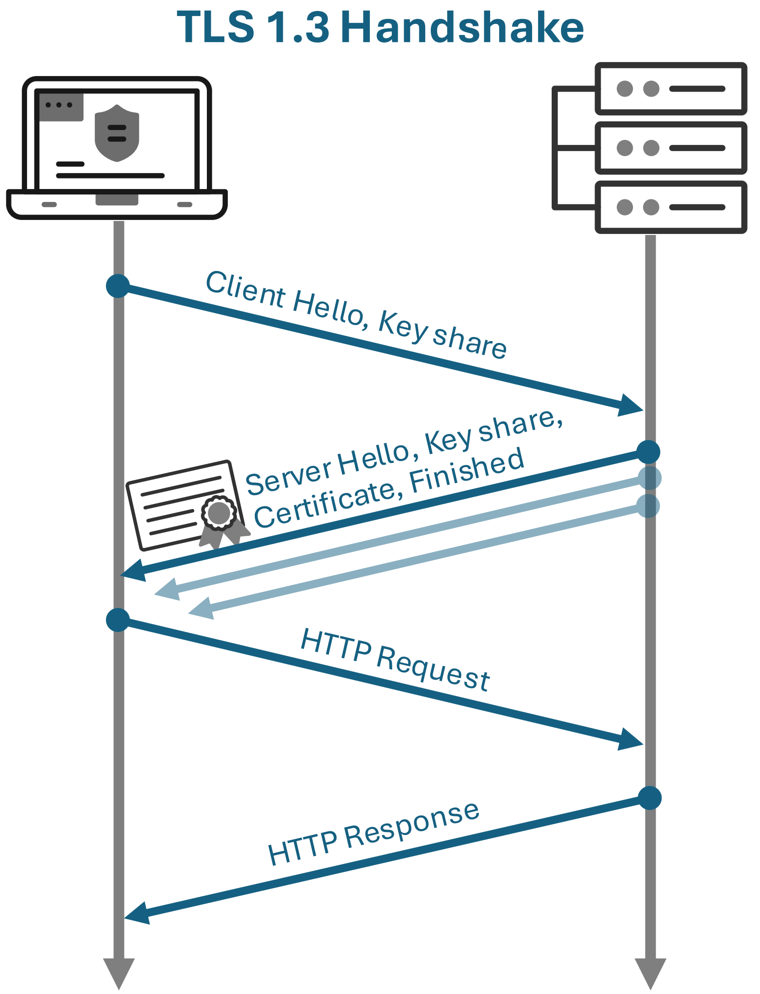


PQC Key and Signature Sizes

Scheme	Public Key (bytes)	Private Key (bytes)	Signature (bytes)	Security Level
RSA-3072	**384**	**384**	**384**	**Classical-128**
ECDSA-P256	**64**	**32**	**256**	**Classical-128**
ML-DSA-44 (Dilithium2)	**1312**	**2528**	**2420**	**PQC Category 2** *(SHA3-256)*
ML-DSA-65 (Dilithium3)	**1952**	**4000**	**3293**	**PQC Category 3** *(AES-192)*
ML-DSA-87 (Dilithium5)	**2592**	**4864**	**4595**	**PQC Category 5** *(AES-256)*
FN-DSA-512 (Falcon512)	**897**	**7553**	**666**	**PQC Category 1** *(AES-128)*
FN-DSA-1024 (Falcon1024)	**1793**	**13953**	**1280**	**PQC Category 5** *(AES-256)*

A bit much to chew?

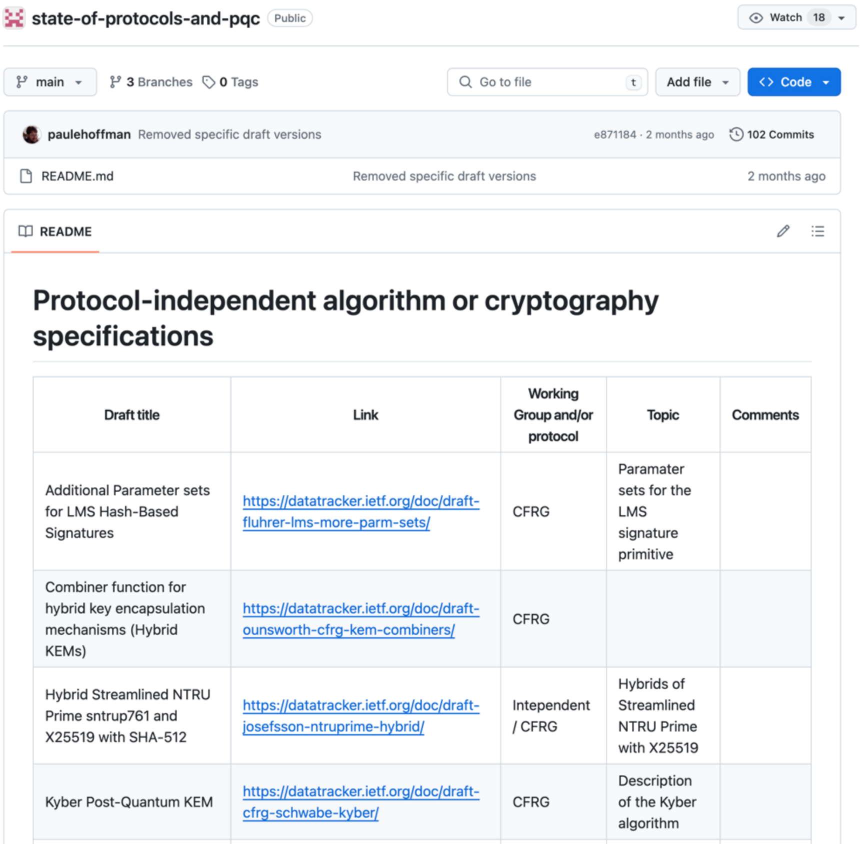
- TLS & WebPKI Certificate Signatures
  - *Server Certificate*: 1 public key and signature, 2 SCT signatures
  - *Intermediate CA Certificate*: 1 public key and signature
  - *TLS Handshake*: 1 signature
  - ML-DSA-44 → **14,724 bytes**
  - Current Quantum-Vulnerable → **1,248 bytes**
- ML-KEM-768 key shares
  - Client → Server: 1,184 bytes
  - Server → Client: **1,088 bytes**
- Why does this matter?
  - *TCP initial congestion window* limits the first wave of messages
  - Typical default: **~14,600 bytes**
- Without protocol/implementation changes, this could slow web connection establishment



Standards Efforts

NIST

- **Internet Engineering Task Force**
  - *Algorithms*: Crypto Forum Research Group (CFRG)
  - *Protocol WGs*: e.g., TLS, IPSec
  - *Mechanisms*: LAMPS, COSE, etc.
  - *PQUIP WG*: PQC transition support
- **ISO/IEC**
  - ML-KEM being incorporated into ISO/IEC 18033-2 with Classic McEliece and Fodo
  - ML-DSA, SLH-DSA expected to follow
  - Will serve as references for future system/protocol standards
- **ETSI/SAGE**
  - TC Cyber Working Group for Quantum-Safe Cryptography
  - Recommendations on PQC algorithms and hybrid protocols
  - Will support PQC migration of 3GPP/5G standards



Protocol-independent algorithm or cryptography specifications

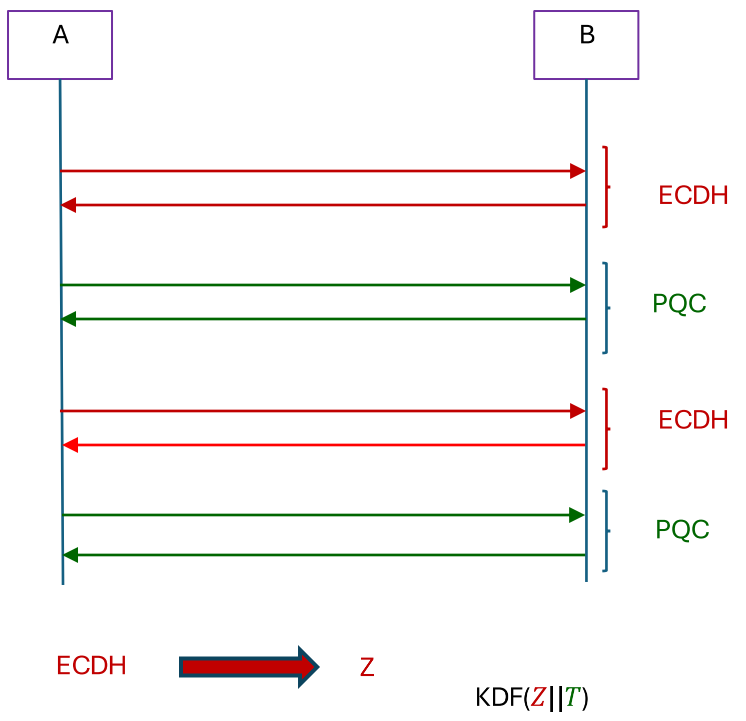
Draft title	Link	Working Group and/or protocol	Topic	Comments
Additional Parameter sets for LMS Hash-Based Signatures	https://datatracker.ietf.org/doc/draft-fluhrer-lms-more-parm-sets/	CFRG	Paramater sets for the LMS signature primitive	
Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)	https://datatracker.ietf.org/doc/draft-ounsworth-cfrg-kem-combiners/	CFRG		
Hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512	https://datatracker.ietf.org/doc/draft-josefsson-ntruprime-hybrid/	Independent / CFRG	Hybrids of Streamlined NTRU Prime with X25519	
Kyber Post-Quantum KEM	https://datatracker.ietf.org/doc/draft-cfrg-schwabe-kyber/	CFRG	Description of the Kyber algorithm	

IETF PQUIP WG

https://github.com/ietf-wg-pquip/state-of-protocols-and-pqc

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 to come in SP 800-227
- Several approaches to hybrid KEMs and certificates
  - Composite approaches
  - Non-composite hybrid approaches
  - Chameleon certificates
- 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



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

Migration

USG Migration

NIST

MAY 04, 2022

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

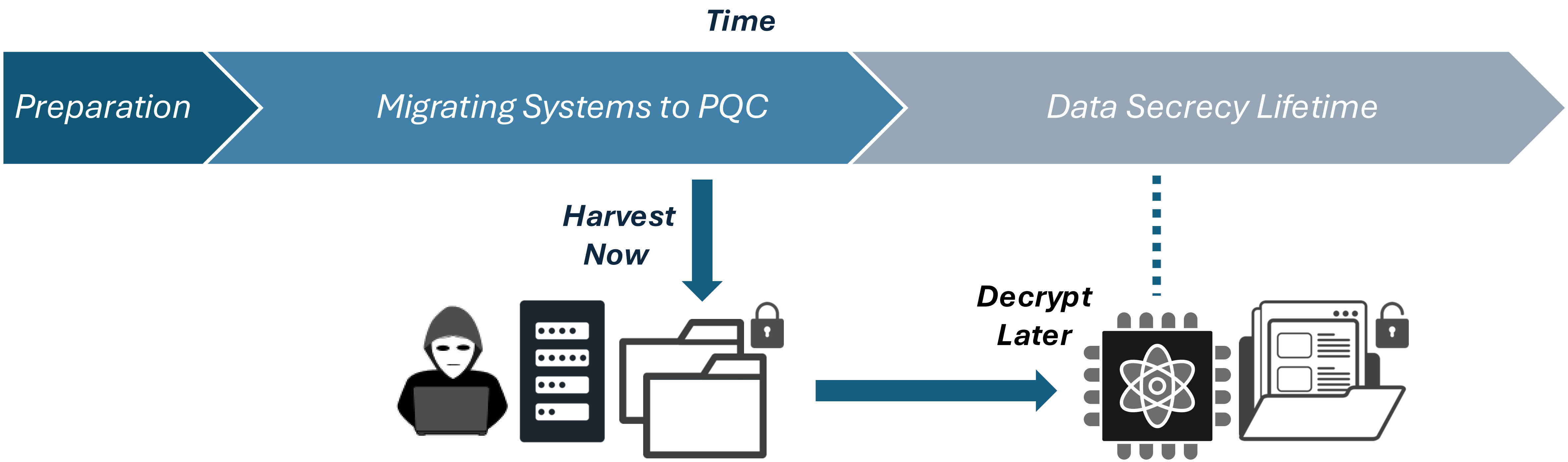
BRIEFING ROOM ▸ STATEMENTS AND RELEASES

Excerpt from NSM-10:

"Mitigating the Risks to Encryption. ... To mitigate this risk, 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."***

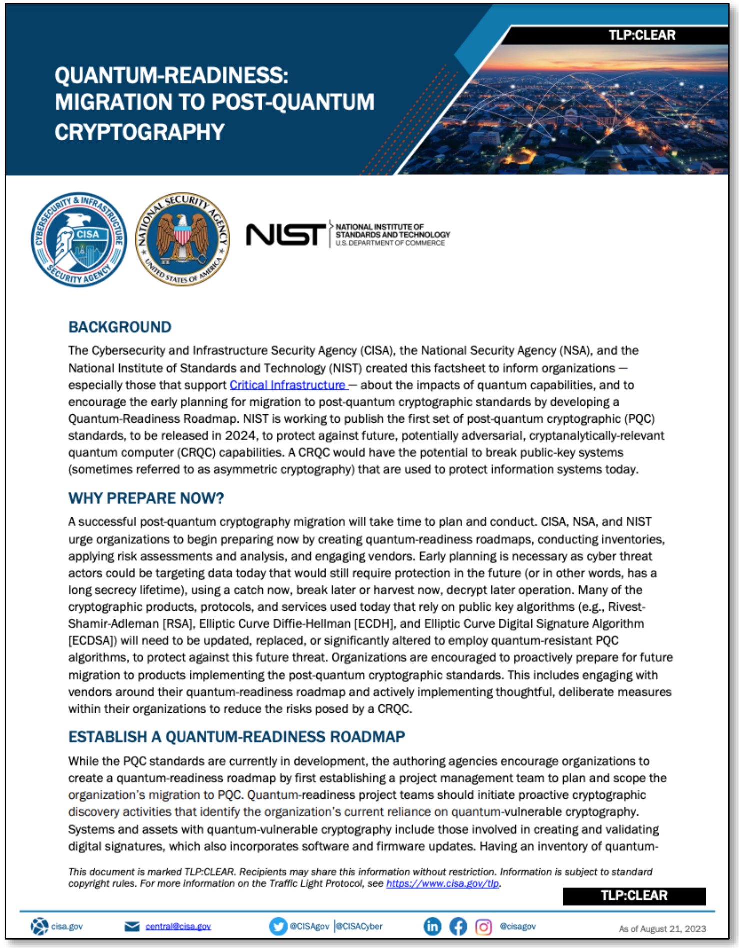
Migration Considerations

Mosca's Theorem



Migration– What can you do

- **Establish a Quantum-Readiness Roadmap**
  - Project management team to plan and scope the migration to PQC
- **Prepare an Inventory of Cryptography and Assets**
  - Identity protocols/applications/devices that use vulnerable cryptography
  - Identify high-value data requiring long-term secrecy
- **Discuss PQC Roadmaps with Vendors**
- **Develop a Migration Strategy**
  - Prioritize high-impact systems, ICSs, and those requiring long-term secrecy
  - Integrate with technology modernization/refresh efforts
  - Prepare to rearchitect, rebuild, or replace legacy applications/systems
- **Validate and Test Systems**
- **Educate and Train Staff**



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-

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

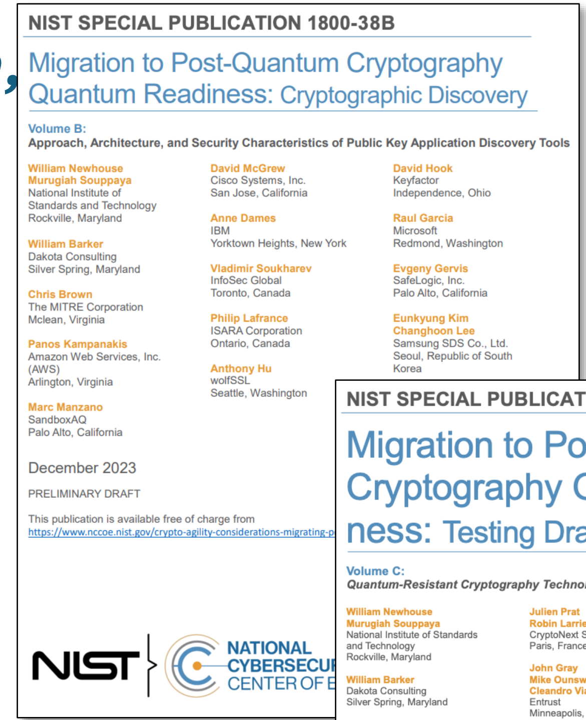
cisa.gov central@cisa.gov @CISAgov |@CISACyber @cisagov As of August 21, 2023

Migration to Post-Quantum Cryptography Project

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Migration to PQC Project– Goals

- 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
- Support ***US Government PQC initiatives***
  - NSM-10
  - Quantum Computing Cybersecurity Preparedness Act
  - NSA CNSA 2.0



NIST SPECIAL PUBLICATION 1800-38B

Migration to Post-Quantum Cryptography Quantum Readiness: Cryptographic Discovery

Volume B:
Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools

William Newhouse
Murugiah Souppaya
National Institute of Standards and Technology
Rockville, Maryland

William Barker
Dakota Consulting
Silver Spring, Maryland

Chris Brown
The MITRE Corporation
Mclean, Virginia

Panos Kampanakis
Amazon Web Services, Inc. (AWS)
Arlington, Virginia

Marc Manzano
SandboxAQ
Palo Alto, California

David McGrew
Cisco Systems, Inc.
San Jose, California

Anne Dames
IBM
Yorktown Heights, New York

Vladimir Soukharev
InfoSec Global
Toronto, Canada

Philip Lafrance
ISARA Corporation
Ontario, Canada

Anthony Hu
wolfSSL
Seattle, Washington

David Hook
Keyfactor
Independence, Ohio

Raul Garcia
Microsoft
Redmond, Washington

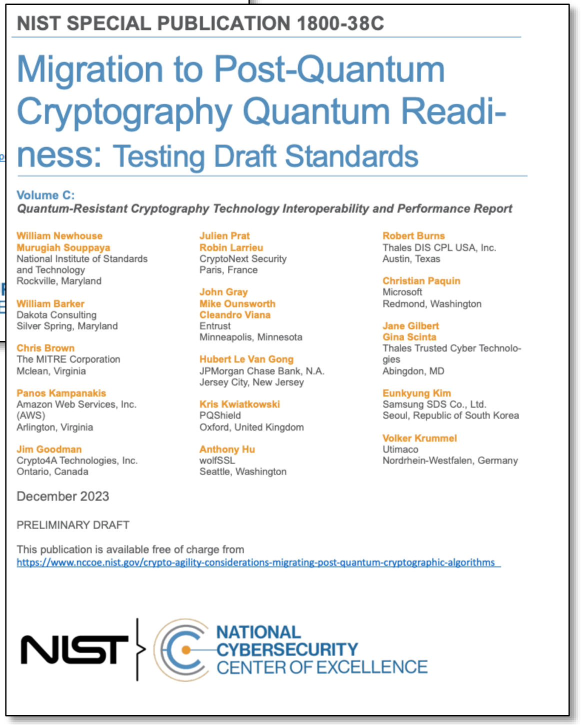
Evgeny Gervis
SafeLogic, Inc.
Palo Alto, California

Eunkyung Kim
Changhoon Lee
Samsung SDS Co., Ltd.
Seoul, Republic of South Korea

December 2023

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-p



NIST SPECIAL PUBLICATION 1800-38C

Migration to Post-Quantum Cryptography Quantum Readiness: Testing Draft Standards

Volume C:
Quantum-Resistant Cryptography Technology Interoperability and Performance Report

William Newhouse
Murugiah Souppaya
National Institute of Standards and Technology
Rockville, Maryland

William Barker
Dakota Consulting
Silver Spring, Maryland

Chris Brown
The MITRE Corporation
Mclean, Virginia

Panos Kampanakis
Amazon Web Services, Inc. (AWS)
Arlington, Virginia

Jim Goodman
Crypto4A Technologies, Inc.
Ontario, Canada

Julien Prat
Robin Larrieu
CryptoNext Security
Paris, France

John Gray
Mike Ounsworth
Cleandro Viana
Entrust
Minneapolis, Minnesota

Hubert Le Van Gong
JPMorgan Chase Bank, N.A.
Jersey City, New Jersey

Kris Kwiatkowski
PQShield
Oxford, United Kingdom

Anthony Hu
wolfSSL
Seattle, Washington

Robert Burns
Thales DIS CPL USA, Inc.
Austin, Texas

Christian Paquin
Microsoft
Redmond, Washington

Jane Gilbert
Gina Scinta
Thales Trusted Cyber Technologies
Abingdon, MD

Eunkyung Kim
Samsung SDS Co., Ltd.
Seoul, Republic of South Korea

Volker Krummel
Utimaco
Nordrhein-Westfalen, Germany

December 2023

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

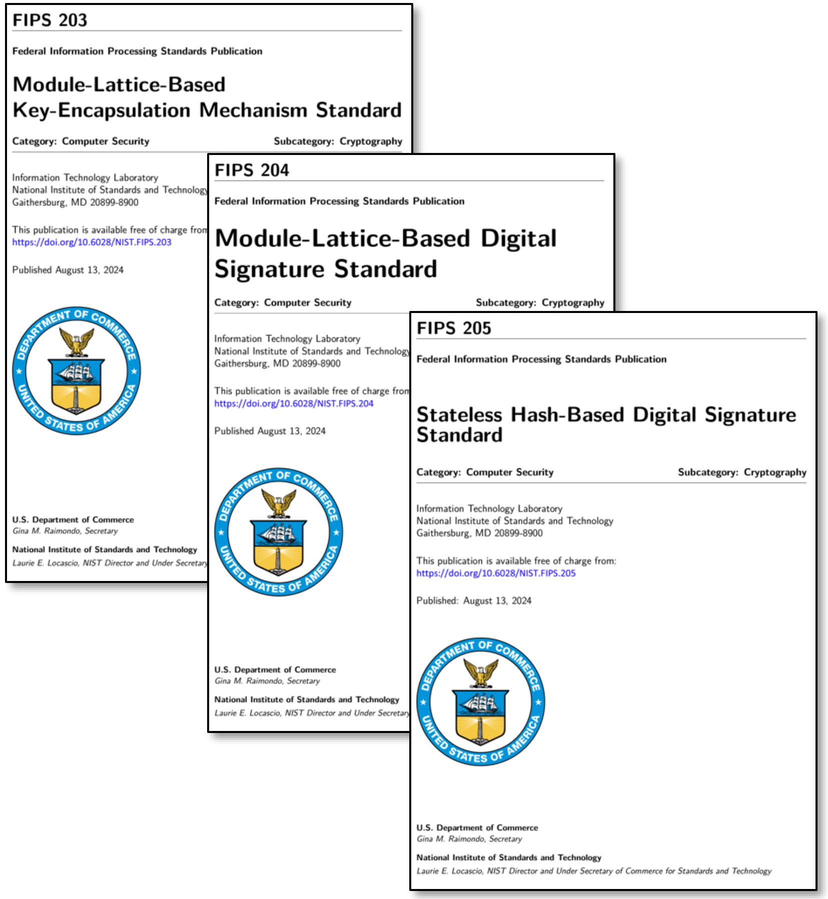
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

Next Steps

PQC Standards- Next Steps

- ***ML-KEM***, ***ML-DSA***, & ***SL-DSA*** finalized on August 13
- Draft ***FN-DSA*** (Falcon) standard under development
- NIST plans to make 4th round KEM selection in 2024
  - Classic McEliece
  - BIKE
  - HQC
  - ~~SIKE~~
- 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 at the 5th NIST PQC Standardization Conference

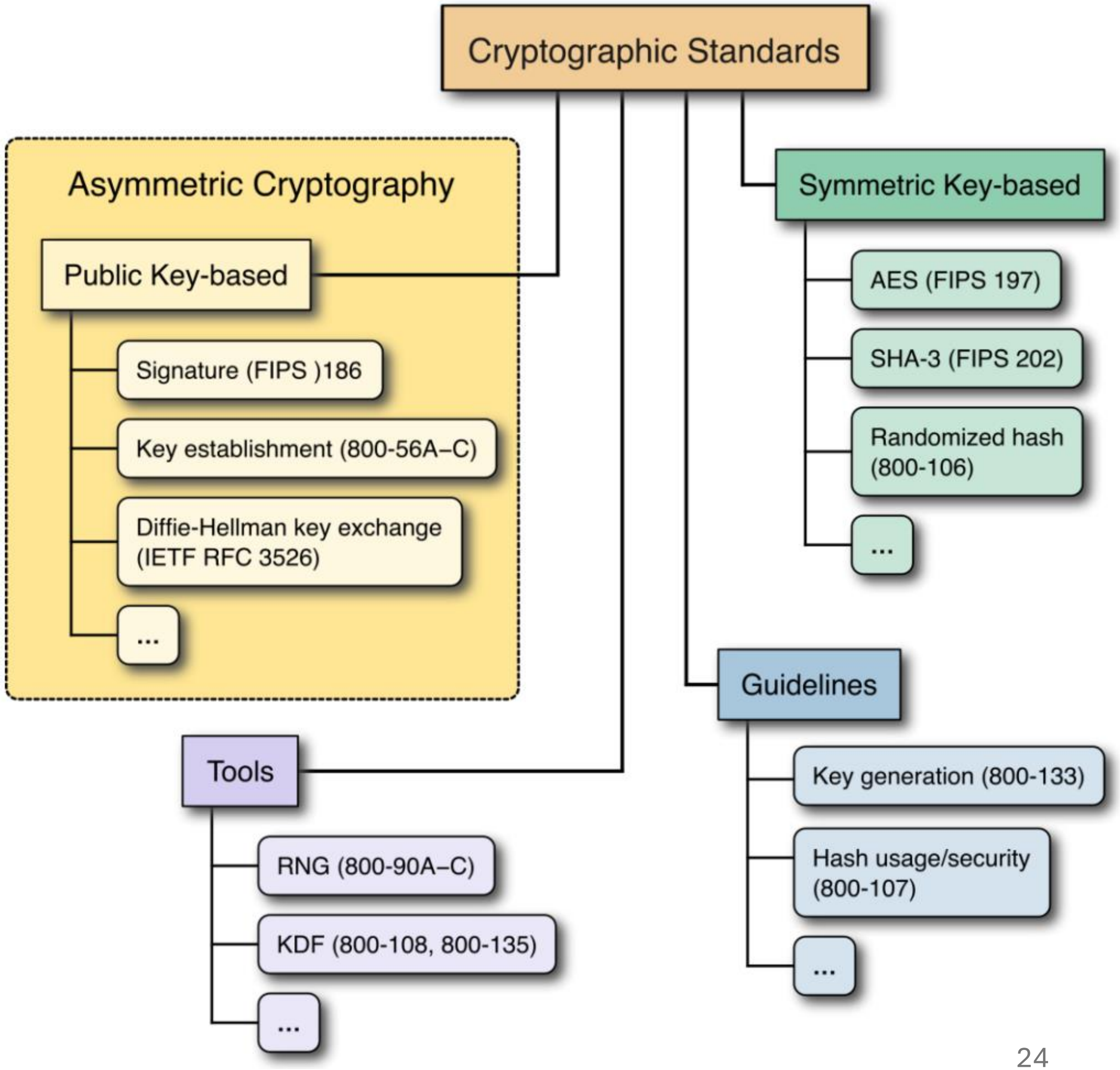

FIPS 203
Federal Information Processing Standards Publication
Module-Lattice-Based Key-Encapsulation Mechanism Standard
Category: Computer Security Subcategory: Cryptography
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900
This publication is 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

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
U.S. Department of Commerce
Gina M. Raimondo, Secretary
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary

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

Recommendations & FIPS 140 Testing

- 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
- NIST CAVP is already testing new PQC algorithms for FIPS 140 validation



Questions

Contact Information

Andrew Regenscheid, Cryptographic Technology Group

Email: Andrew.Regenscheid@nist.gov

NIST PQC standardization

www.nist.gov/pqcrypto

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

Email: pqc-comments@nist.gov

NCCoE PQC Migration Project

www.nccoe.nist.gov/applied-cryptography

Request to join Community of Interest

Email: applied-crypto-pqc@nist.gov