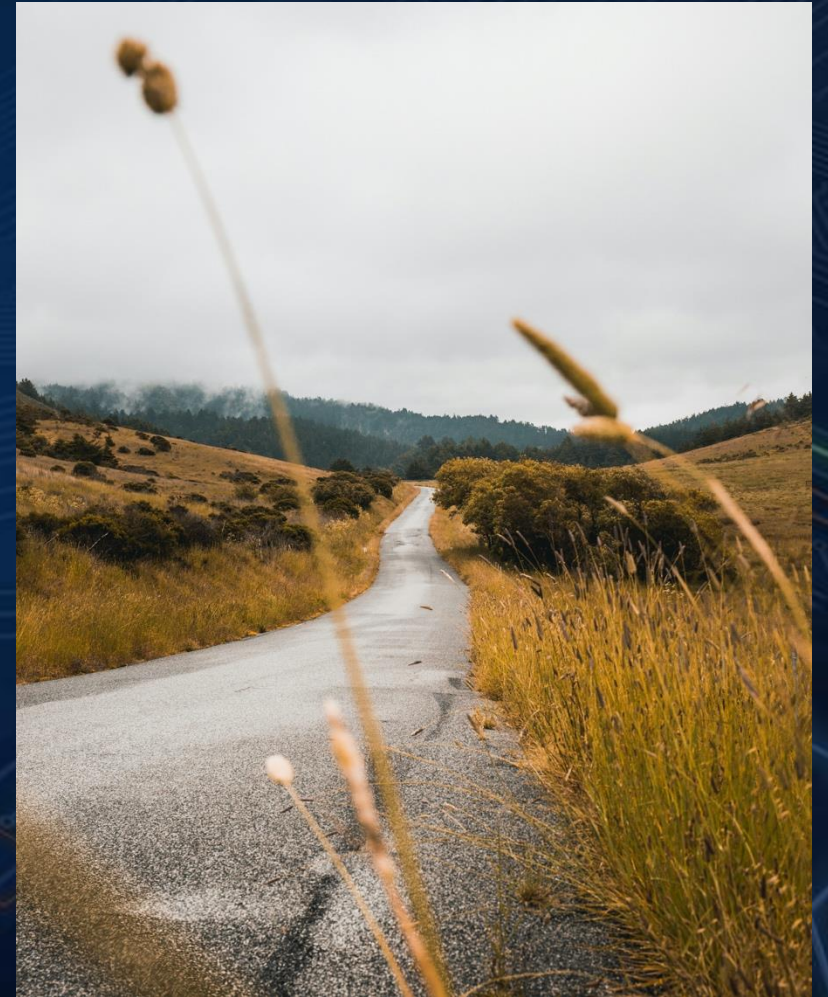


NIST PQC

The Road Ahead

Dustin Moody
Cryptographic Technology Group

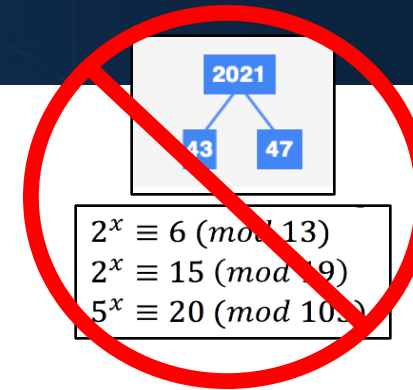


Tuesday, October 3rd, 2023

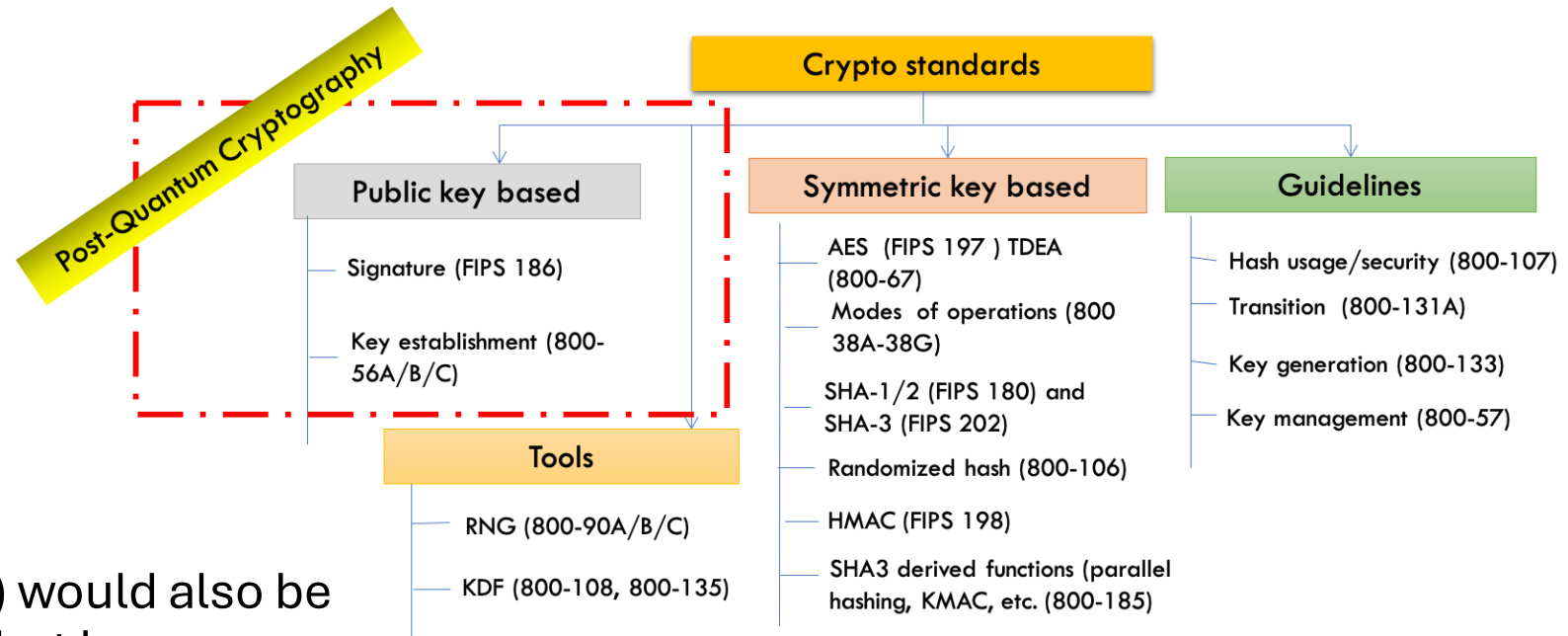
The Quantum Threat

- 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




(Prior to 2024)



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

Taking Action in the U.S.




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 *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 Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).

Announcing the Commercial National Security Algorithm Suite 2.0



ADVISORY

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
- Selection Criteria
 - Security, performance, and other characteristics

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)

The First Set of NIST PQC Standards



FIPS 203

ML-KEM

(Based on CRYSTALS-Kyber)

- A module learning with errors (MLWE)-based key encapsulation mechanism (KEM)
- Good performance in different platforms
- An algorithm for key establishment in security protocols

FIPS 204

ML-DSA

(Based on CRYSTALS-Dilithium)

- A lattice-based digital signature algorithm based on the Fiat-Shamir paradigm
- Good performance, simple implementation, moderate public-key and signature size, suitable for general applications

FIPS 205

SLH-DSA

(Based on SPHINCS+)

- Not require to keep track of any state between signatures
- Solid security, signatures are longer compared with ML-DSA
- Limited version w/ smaller parameter sets being developed (see Quynh's talk tomorrow)

Draft FIPS 206

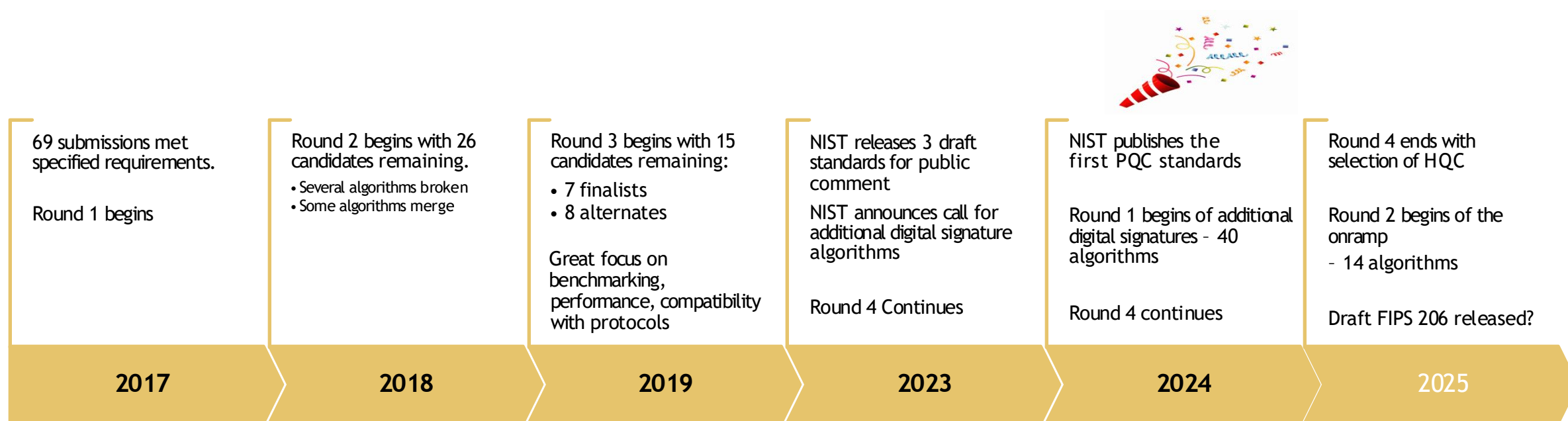
FN-DSA

(Based on FALCON)

- Hash and sign paradigm
- Smaller bandwidth and fast verification but more complicated implementation
- ***Under development***
- ***(hopefully soon)***

Published August 2024!

Milestones and Timeline



- **March 2025 - NISTIR 8545**

- [Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process](#)

BIKE or HQC?

- No clear winner for performance
 - HQC faster for KeyGen, Decaps
 - BIKE a bit faster for Encaps
 - BIKE has smaller key/ciphertext sizes
- Both need low DFR for IND-CCA2
 - Recent results for BIKE
 - Analysis is more mature for HQC

- HQC selected

Classic McEliece or not?

- Public keys from 260K to 1M bytes
- Small ciphertext sizes
- Fast Encaps/Decaps, slow KeyGen
- Would it be used?
 - Limited interest
- ISO standardization

- Not selected

NIST SP 800-227, Recommendations for KEMs



- **Published:** September 18, 2025
 - 1st Draft available for comments: January 2025
- Describes the basic definitions, properties, and applications of KEMs
- Provides recommendations for implementing and using KEMs in a secure manner
- Contains some guidance on hybrid key establishment
- ***NIST Workshop on Guidance for KEMs***
 - Held on February 25-26th
 - Intended to facilitate discussions on draft guidance for KEMs
 - Slides and video available at:
<https://csrc.nist.gov/Events/2025/workshop-on-guidance-for-kems>

NIST Special Publication 800
NIST SP 800-227

Recommendations for Key-Encapsulation Mechanisms

Gorjan Alagic
Elaine Barker
Lily Chen
Dustin Moody
Angela Robinson
Hamilton Silberg
Noah Waller

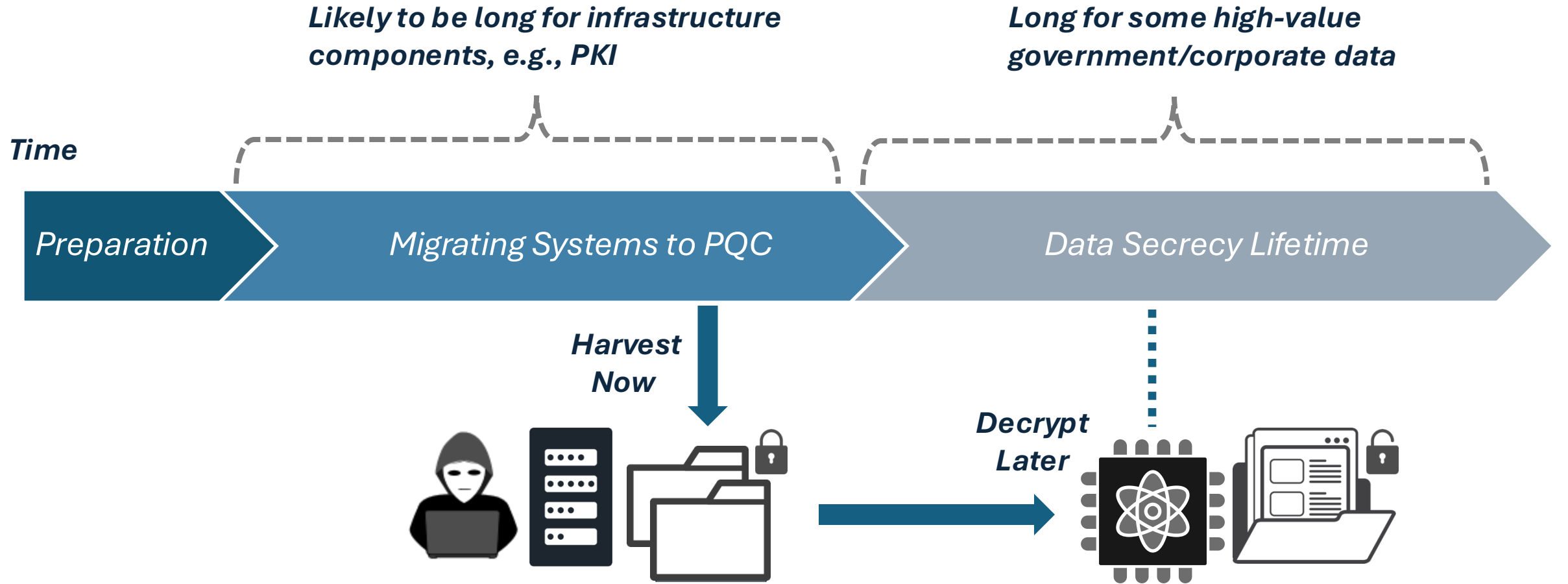
This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-227>

On-Ramp Signatures

- July 2022 – New Call for additional digital signatures
- June 2023 – Deadline for submissions
 - 40 candidates
- Why did NIST call for additional post-quantum signatures?
 - 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 that have short signatures and fast verification.
 - Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.
- No on-ramp for KEMs currently planned



Migration Considerations



FIPS 140 Validation and Testing

- **Cryptographic Algorithm Validation Program**

- Automated Cryptographic Validation Testing System (ACVTS)

<https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/how-to-access-acvts>

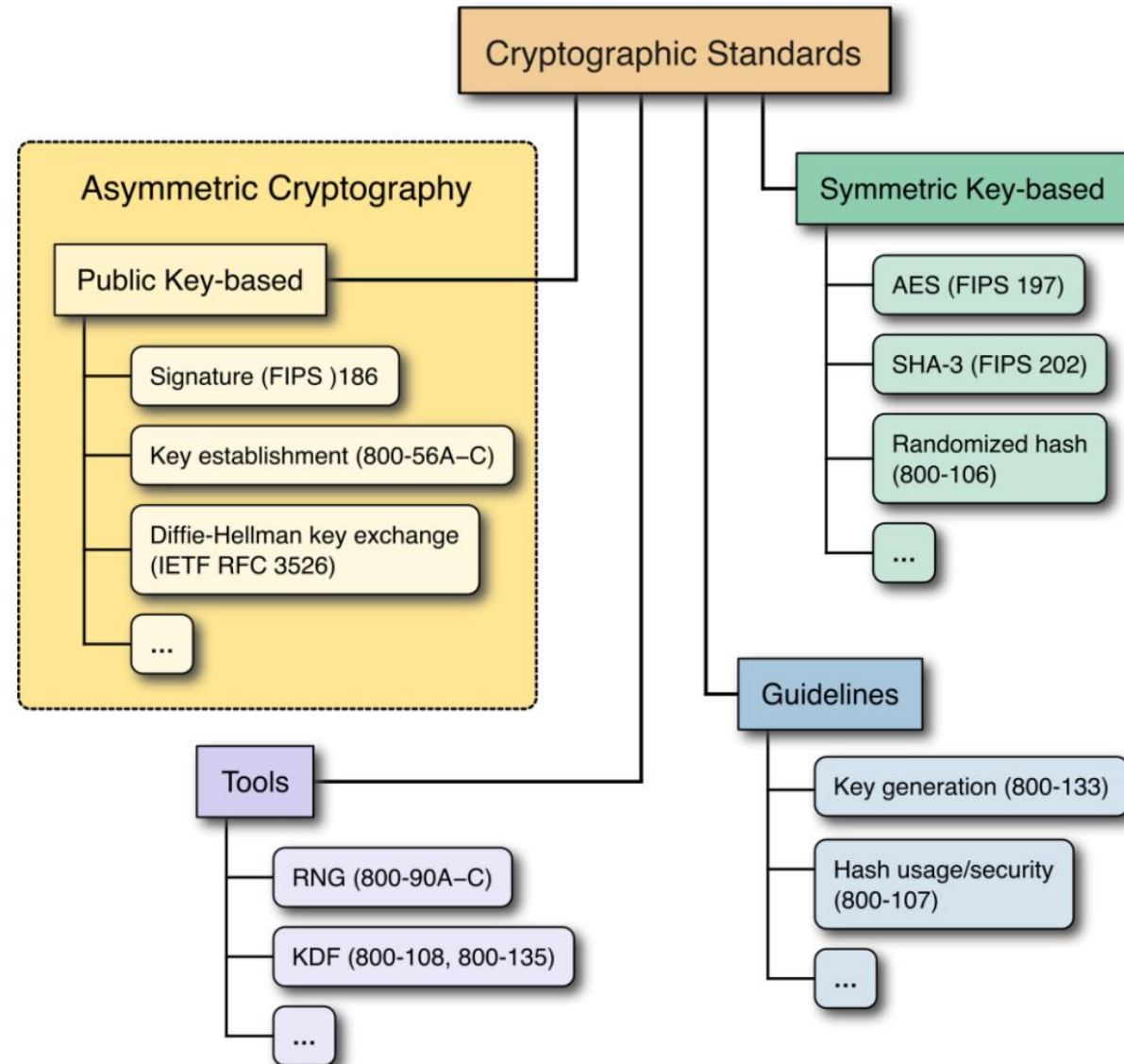
- Testing for algorithm standards to enable production/official testing

<https://github.com/usnistgov/ACVP-Server>

- Test vectors are available:

<https://github.com/usnistgov/ACVP-Server/tree/master/gen-val/>

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



NIST IR 8547, Transition to PQC Standards



- Initial Public Draft released November 12th
 - Comments received are posted online
- Describes NIST's expected approach to the PQC migration
- Identifies quantum-vulnerable standards
 - Key establishment: Diffie-Hellman and MQV over finite field and elliptic curves (SP 800-56A), RSA-based (SP 800-56B)
 - Digital signatures: RSA, ECDSA, EdDSA (FIPS 186-5)
- Identifies the PQC standards
 - Key establishment: ML-KEM (FIPS 203)
 - Digital signatures: XMSS, LMS (SP 800-208), ML-DSA (FIPS 204), SLH-DSA (FIPS 205)
- Includes some migration considerations for use cases
 - Code signing, user and machine authentication, network security protocols, email and document signing and encryption
 - Touches on PQC/classical hybrids

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8547.ipd>



NIST IR 8547, Transition to PQC Standards



- Proposed transition timelines for quantum-vulnerable algorithms
 - 112-bit security strength – **deprecated** after 2030, **disallowed** after 2035
 - *Organizations may continue using public key algorithms at the 112 bit security level as they migrate to post-quantum cryptography.*
 - 128-bit and higher security strength – **disallowed** after 2035
- NIST-approved symmetric primitives providing at least 128 bits of classical security continue to be approved
- System migration timelines will depend on use case or application
- Priorities:
 - Systems with long-term confidentiality needs– *e.g., VPN, TLS*
 - Broad, long-lived cryptographic infrastructures– *e.g., PKI, PIV, code signing*

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft



Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8547.ipd>

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



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.

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.

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.


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 sheet 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.

- **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 FrodoKEM
 - The document is the DIS ballot. The ballot ends May 14, 2025.
- ML-DSA and SLH-DSA are proposed to be standardized in ISO/IEC 14888-5 and 14888-6 respectively as new work items
 - PWI 25542 Inclusion of digital signature schemes for Post-Quantum Cryptography in ISO/IEC standards is the proposed work item which will ask for further questions.

- **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

The screenshot shows a GitHub repository page for 'state-of-protocols-and-pqc'. The repository is public and has 102 commits. The README file is open, displaying a table titled 'Protocol-independent algorithm or cryptography specifications'. The table lists four draft titles with their corresponding links, working groups, topics, and comments.

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	Parameter 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>



NIST PQC standardization

www.nist.gov/pqcrypto

Email: pqc-comments@nist.gov

Sign up for the *pqc-forum* mailing list

Next steps:

- FIPS 206 – soon
- SP 800-133 update – soon
 - allow for seeds to come from a KDF (instead of an approved DRBG)
- FIPS 207 – in 2026
- SP 800-208 update – in 2026
 - provide a way to do private key export
- SP 800-230 (smaller SLH-DSA) – in 2026
- 3rd Round of the onramp – in 2026

And migrate by 2035!