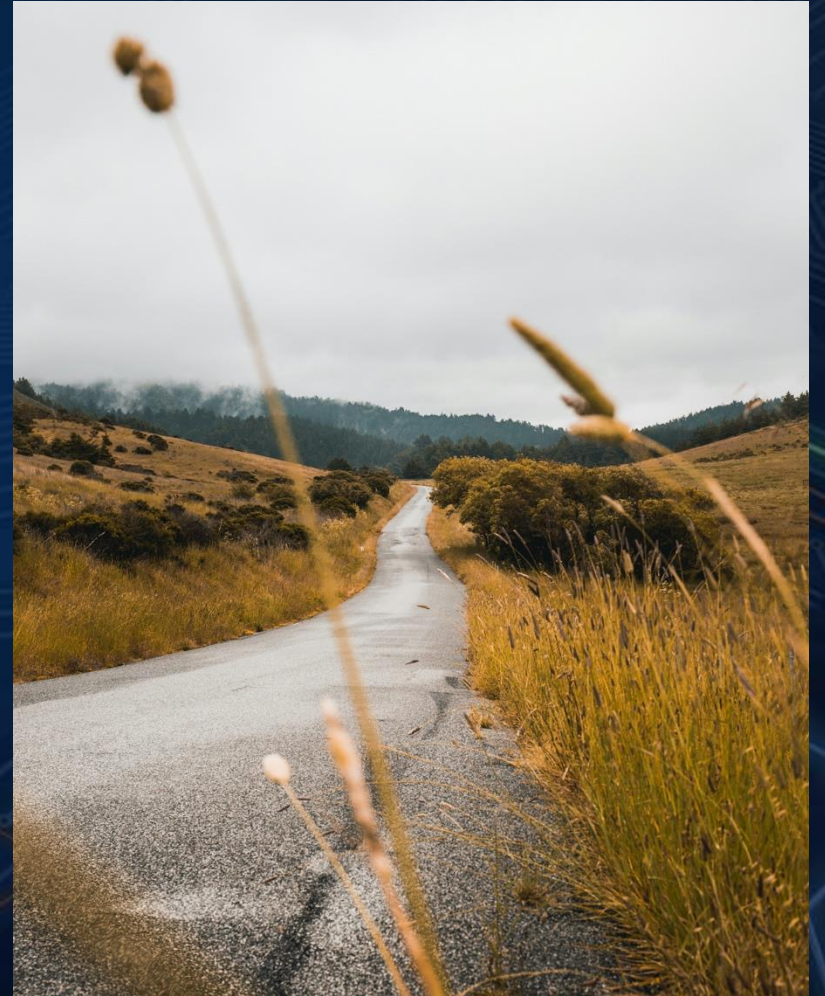


NIST PQC

The Road Ahead

Dustin Moody
Cryptographic Technology Group



Tuesday, October 3rd, 2023

Here we are now

- March 11, 2025 – Selection of HQC marks the end of the 4th Round of the (main) NIST PQC process
- The process began in February 2016
- Some numbers
 - 82 submission packages
 - 278 submitters involved, from 25 countries in 6 continents
 - Over 3000 members on the pqc-forum and over 5000 posts
 - NIST has held 7 workshops, with over 2000 attendees
 - 11 NIST documents published (reports and standards)
 - Over 100 commenters on our first three PQC Standards

March 2025

NIST Search NIST Menu

NEWS

NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

March 11, 2025

f in X

- NIST has chosen a new algorithm for post-quantum encryption called HQC, which will serve as a backup for ML-KEM, the main algorithm for general encryption.
- HQC is based on different math than ML-KEM, which could be important if a weakness were discovered in ML-KEM.
- NIST plans to issue a draft standard incorporating the HQC algorithm in about a year, with a finalized standard expected in 2027.

OLD ENCRYPTION STANDARDS

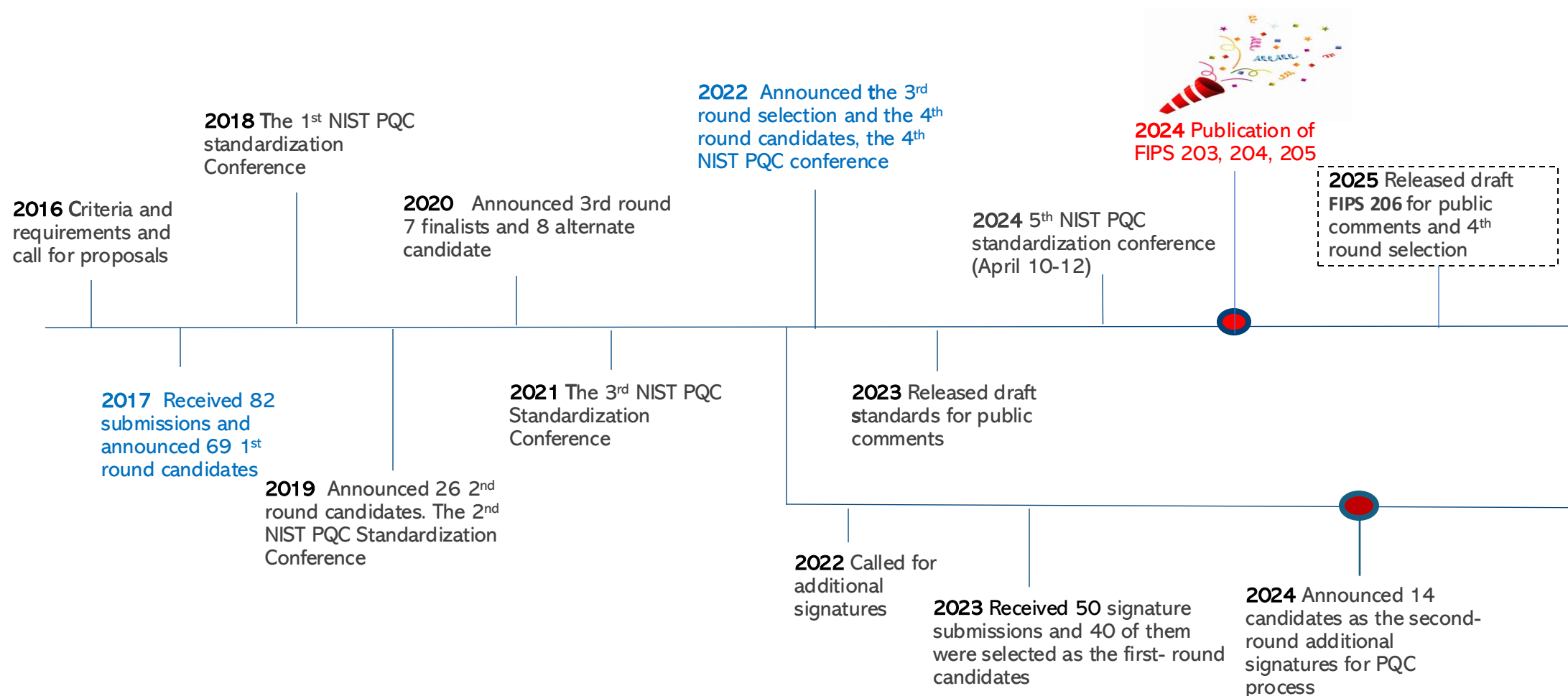
NEW ENCRYPTION STANDARDS

U342 2E DSF%

>#1 MOR342

>*****

Milestones and Timeline in 8 Years



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

FIPS 206

FN-DSA

(Based on FALCON)

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

Published August 2024!

- **Classic McEliece**

- Code-based KEM that uses a binary Goppa code
- Confidence in the security of the 1978 scheme
- Small ciphertext but very large public key and relatively slow key generation

- **HQC (Hamming Quasi-Cyclic)**

- KEM based on QC-MDPC code
- Offers strong security assurances and mature decryption failure rate analysis
- Larger public keys and ciphertext sizes than BIKE

- **BIKE (Bit Flipping Key Encapsulation)**

- KEM based on binary linear quasi-cyclic moderate density parity check (QC-MDPC) codes
- Public-key and ciphertext comparable to lattice-based schemes
- Competitive performance for non-lattice-based KEMs
- Announced a new decoder in the 5th NIST Conference
 - Reduce impact of new weak key classes in Crypto 2023 paper

- ~~SIKE~~

- Based on isogenies of elliptic curves
- The SIKE team acknowledges that SIKE is insecure and should not be used

- **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

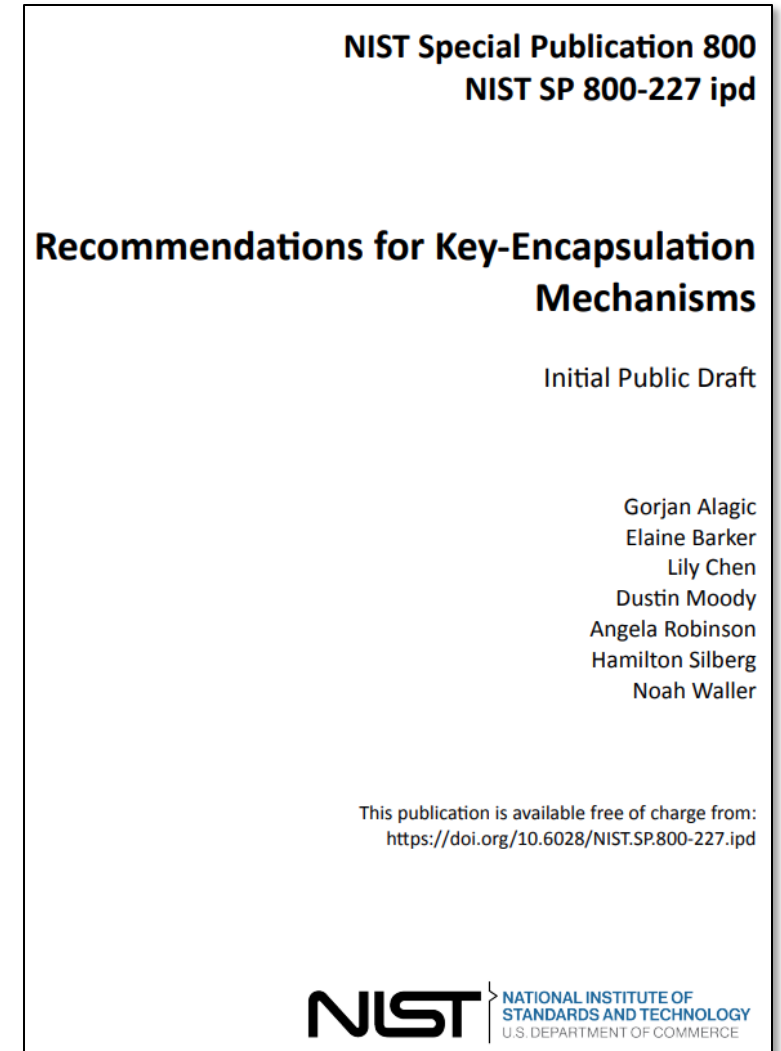
Classic McEliece or not?

- 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

Draft NIST SP 800-227, Recommendations for KEMs



- **Released:** January 7, 2025
 - Comment period ended: March 7th, 2025
- Draft 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 available at:
<https://csrc.nist.gov/Events/2025/workshop-on-guidance-for-kems>



On-Ramp Signatures

- July 2022 – New Call for additional digital signatures
- June 2023 – Deadline for submissions
- 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

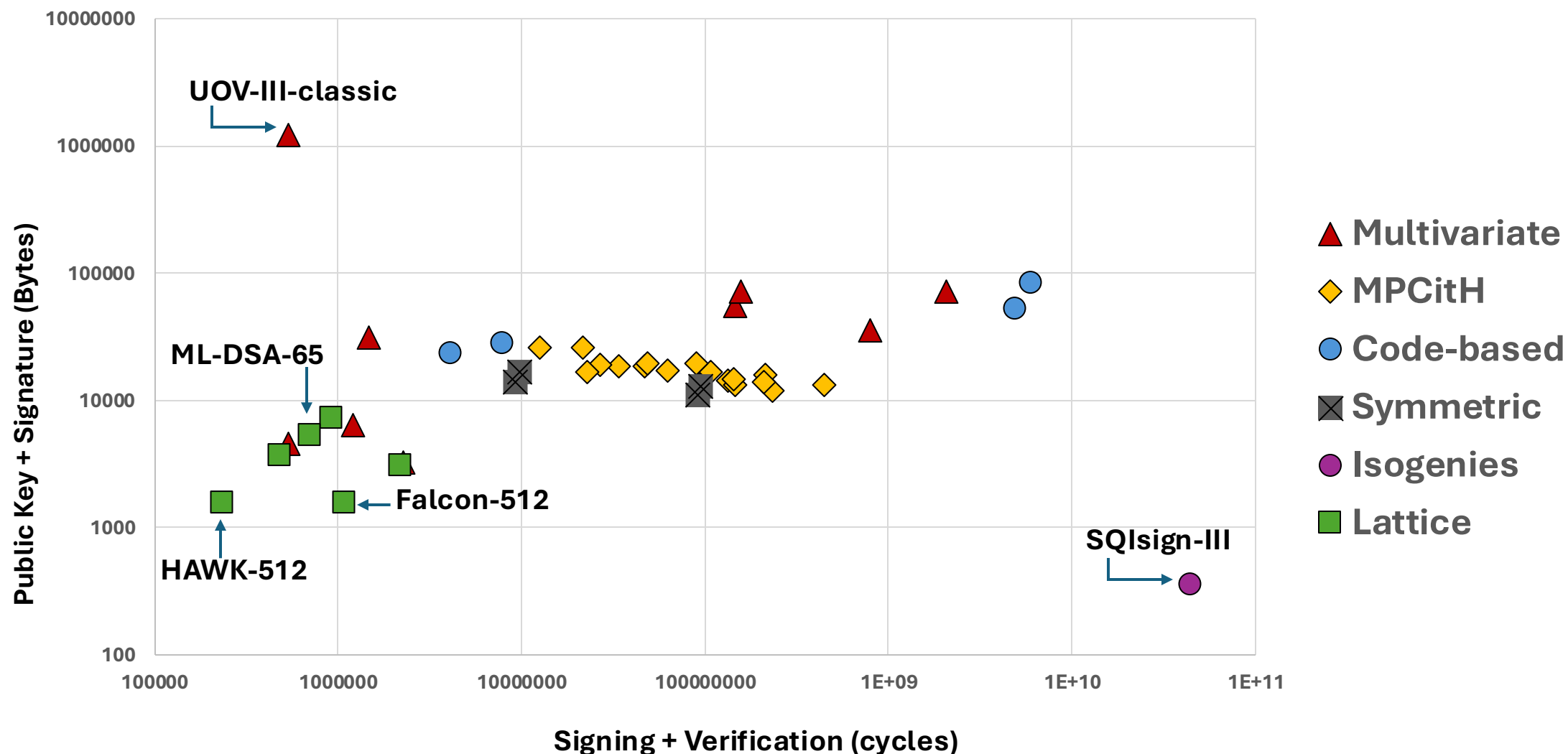


The 2nd Round candidates

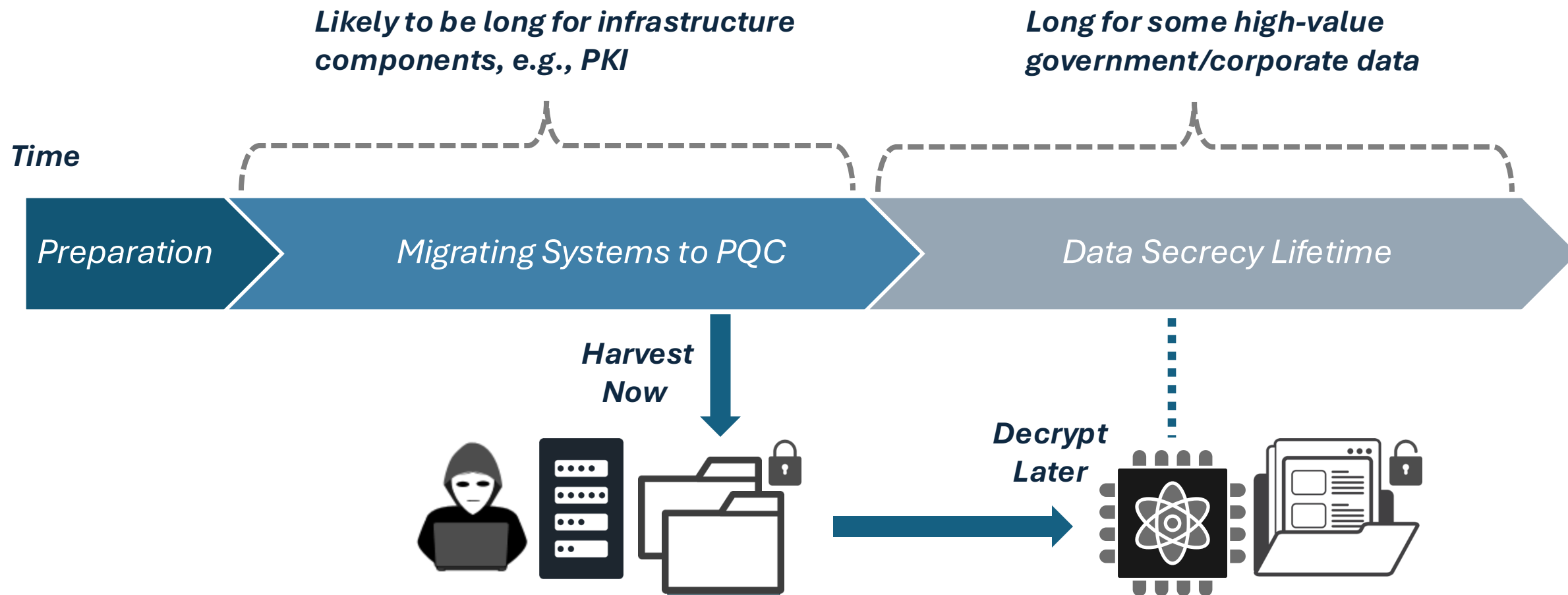


Multivariate		MPC in-the-head			Lattice	Code	Symmetric	Isogeny
<i>UOV</i>	<i>MinRank</i>	<i>SD/Rank-SD</i>	<i>PKP</i>	<i>MQ</i>				
Mayo	Mirath	Ryde	Perk	MQOM	Hawk	Cross	FAEST	SQLsign
QR-UOV		SDitH				LESS		
SNOVA								
UOV								

Performance Summary (log scale)



Migration Considerations



NIST IR 8547, Transition to PQC Standards



- Initial Public Draft released November 12th
 - Comment period ended **January 10th**
 - pqc-transition@nist.gov
- Identifies quantum-vulnerable standards
 - Key establishment based on Diffie-Hellman and MQV over finite field and elliptic curves (SP 800-56A)
 - Key establishment based on RSA (SP 800-56B)
 - Digital signatures include RSA, ECDSA, EdDSA (FIPS 186-4)
- Proposed transition timelines for quantum-vulnerable algorithms
 - 112-bit security strength – **deprecated** after 2030, **disallowed** after 2035
 - 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

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>



Quantum-Vulnerable Algorithms



Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	Disallowed after 2035
RSA [FIPS186]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035

Key Establishment Scheme	Parameters	Transition
Finite Field DH and MQV [SP80056A]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
Elliptic Curve DH and MQC [SP80056A]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035
RSA [SP80056B]	112 bits of security strength	Deprecated after 2030 Disallowed after 2035
	≥ 128 bits of security strength	Disallowed after 2035

Organizations may continue using public key algorithms at the 112 bit security level as they migrate to post-quantum cryptography.

Post-Quantum Algorithms



Digital Signature Algorithm Family	Parameter Sets	Security Strength	Security Category
ML-DSA [FIPS204]	ML-DSA-44	128 bits	2
	ML-DSA-65	192 bits	3
	ML-DSA-87	256 bits	5
SLH-DSA [FIPS205]	SLH-DSA-SHA2-128[s/f]	128 bits	1
	SLH-DSA-SHAKE-128[s/f]		
	SLH-DSA-SHA2-192[s/f]	192 bits	3
	SLH-DSA-SHAKE-192[s/f]		
	SLH-DSA-SHA2-256[s/f]	256 bits	5
	SLH-DSA-SHAKE-256[s/f]		
LMS, HSS [SP800208]	With SHA-256/192	192 bits	3
	With SHAKE256/192		
	With SHA-256	256 bits	5
	With SHAKE256		
XMSS, XMSS^{MT} [SP800208]	With SHA-256/192	192 bits	3
	With SHAKE256/192		
	With SHA-256	256 bits	5
	With SHAKE256		

Key Establishment Scheme	Parameter Sets	Security Strength	Security Category
ML-KEM [FIPS203]	ML-KEM-512	128 bits	1
	ML-DSA-768	192 bits	3
	ML-DSA-1024	256 bits	5

NIST IR 8547– Timeline and Priorities



- NIST IR 8547 timeline supports NSM-10 goal of transition USG systems to PQC by 2035
- 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 will develop/update application-specific guidance throughout the transition, e.g.,
 - **FIPS 201**– *Personal Identity Verification (PIV) of Federal Employees and Contractors*
 - **NIST SP 800-52**– *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
 - **NIST SP 800-77**– *Guide to IPsec VPNs*
 - **NIST SP 800-57 Part 3** – *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*

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>



- **Hybrid Constructions**

- Order of schemes
- Allowed combinations before and after PQC transition
- More guidance on hybrid signatures and certificates

- **Timeline**

- May be too fast
- May be too slow
- Distinguish KEMs from signatures

- **Transition guidance**

- Prioritization
- More on use cases- firmware signing, KEMs
- What about quantum-vulnerable cryptography with no PQC alternative?
- Call out other federal workstreams/activities

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

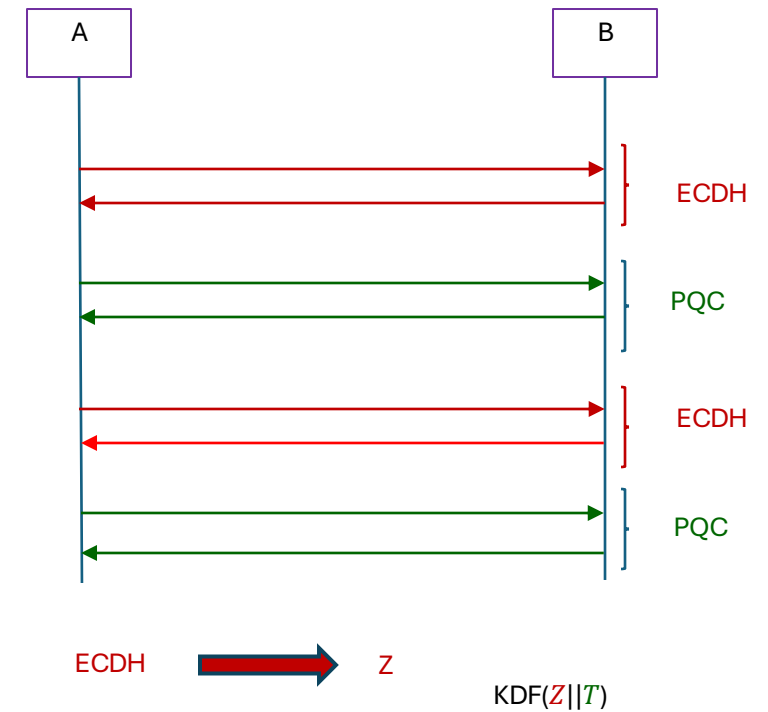
Initial Public Draft

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>

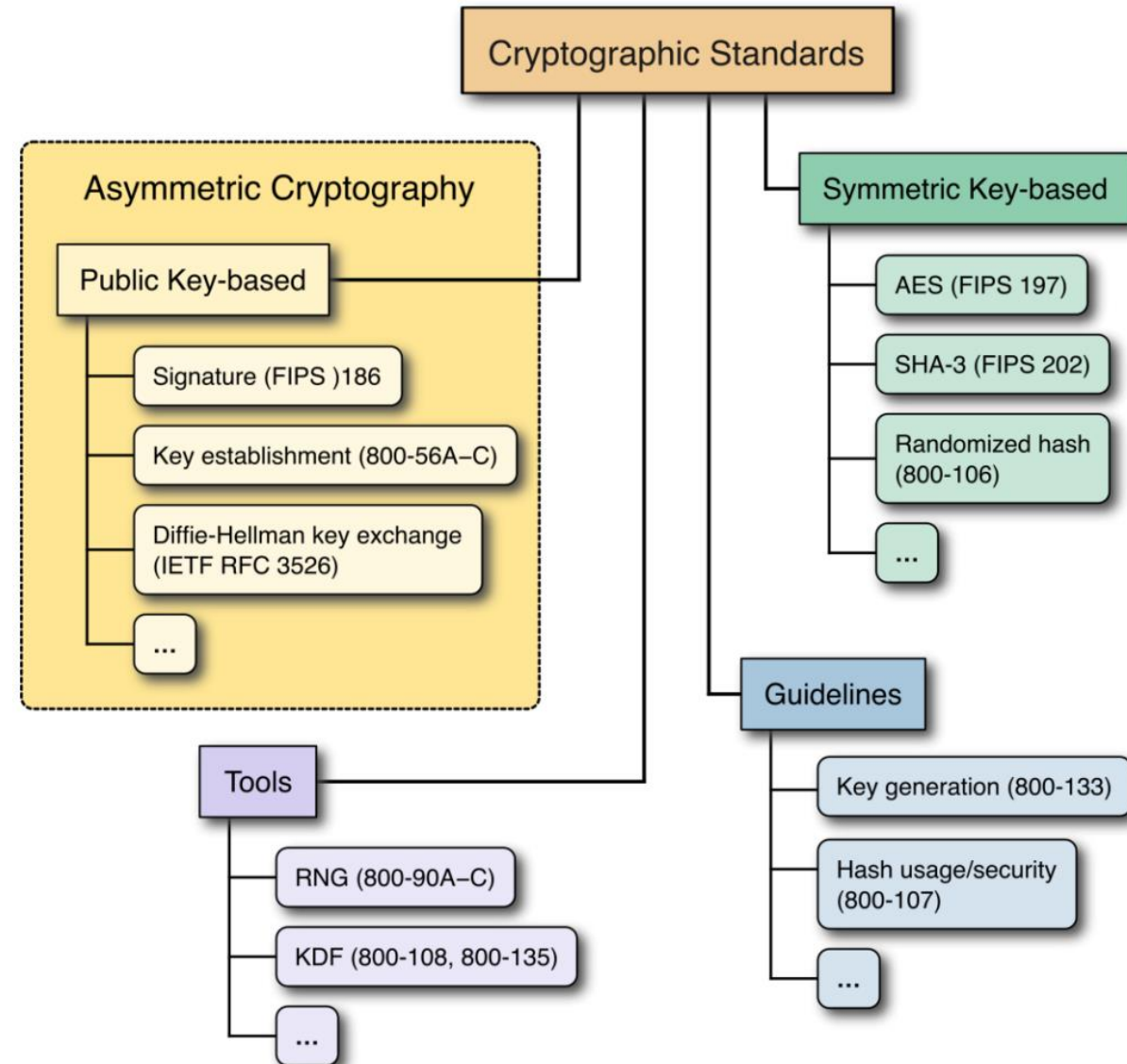
Hybrid Schemes

- **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 in SP 800-227 – order of schemes not important
- Several approaches to hybrid KEMs and certificates
 - Composite approaches
 - Non-composite hybrid approaches
- 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



Recommendations & FIPS 140 Testing



- NIST provided guidance for transition in the past (SP 800-131A) and will provide PQC transition guidance
- **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 new PQC algorithms for FIPS 140 validation



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



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.

Migration to PQC Project– Draft Publications



Draft NIST SP 1800-38B

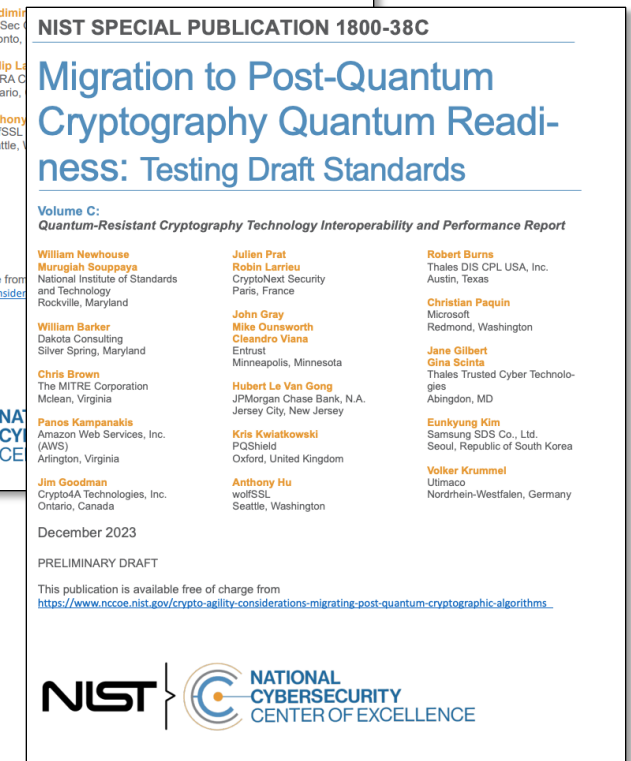
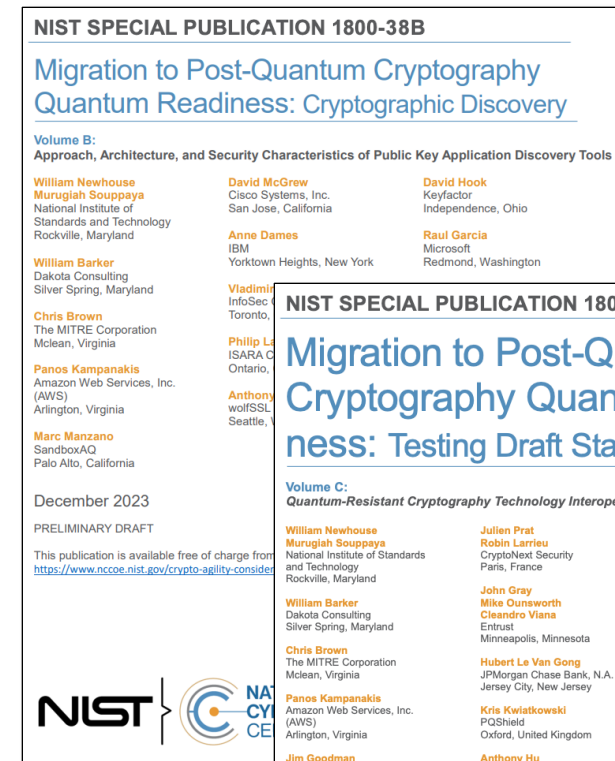
Quantum Readiness: Cryptographic Discovery

- Functional test plan that exercises the cryptographic discovery tools to determine baseline capabilities
- Describes a use case to provide context and scope
- Identifies threats addressed in this demonstration
- Provides a multifaceted approach to start the discovery process
- Describes the high-level architecture that integrates contributed discovery tools in our lab

Draft NIST SP 1800-38C

Quantum Readiness: Testing Draft Standards for Interoperability and Performance

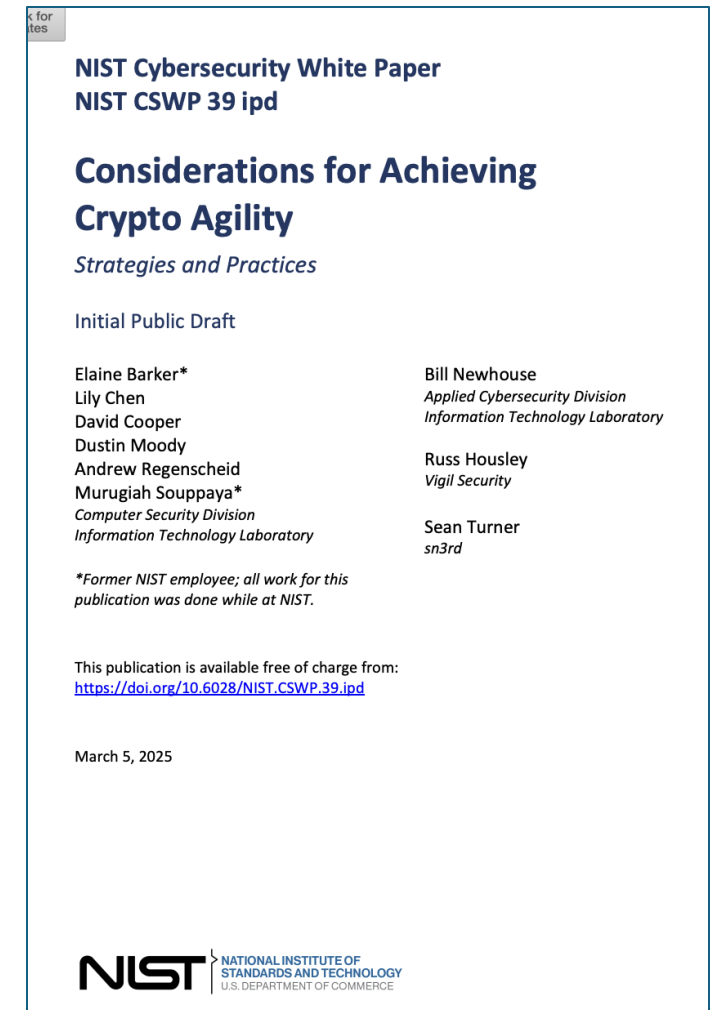
- Identification of compatibility issues between quantum-ready algorithms
- Explore interoperability issues in a controlled, non-production environment
- Reduction of time spent by individual organizations performing similar interoperability testing for their own PQC migration efforts



Aspects of Cryptographic Agility



- **Crypto agility** describes the capabilities needed to replace and adapt cryptographic algorithms for protocols, applications, software, hardware, and infrastructures without interrupting the flow of a running system to achieve resiliency
- NIST Cybersecurity White Paper [Considerations for Achieving Cryptographic Agility: Strategies and Practices](#) is to survey the current practice and inspire sector specific approaches
 - Bring crypto agility awareness for different players
 - Accommodate communications between cryptographers, developers, and practitioners
 - Explore operational mechanisms in each implementation environment to achieve crypto agility
 - Encourage developing sector/standards specific guidelines
- NIST will hold a virtual crypto agility workshop April 17-18, 2025
<https://csrc.nist.gov/Events/2025/crypto-agility-workshop>
Submission due March 31, 2025



Standards Efforts

- **Internet Engineering Task Force**

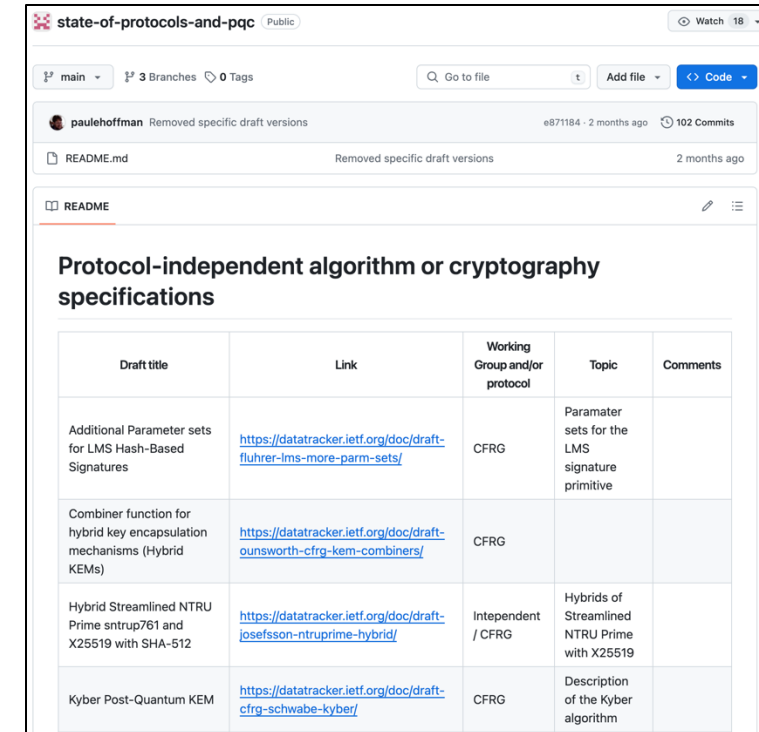
- *Algorithms*: Crypto Forum Research Group (CFRG)
- *Protocol WGs*: e.g., TLS, IPsec
- *Mechanisms*: LAMPS, COSE, etc.
- *PQUIP WG*: PQC transition support

- **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



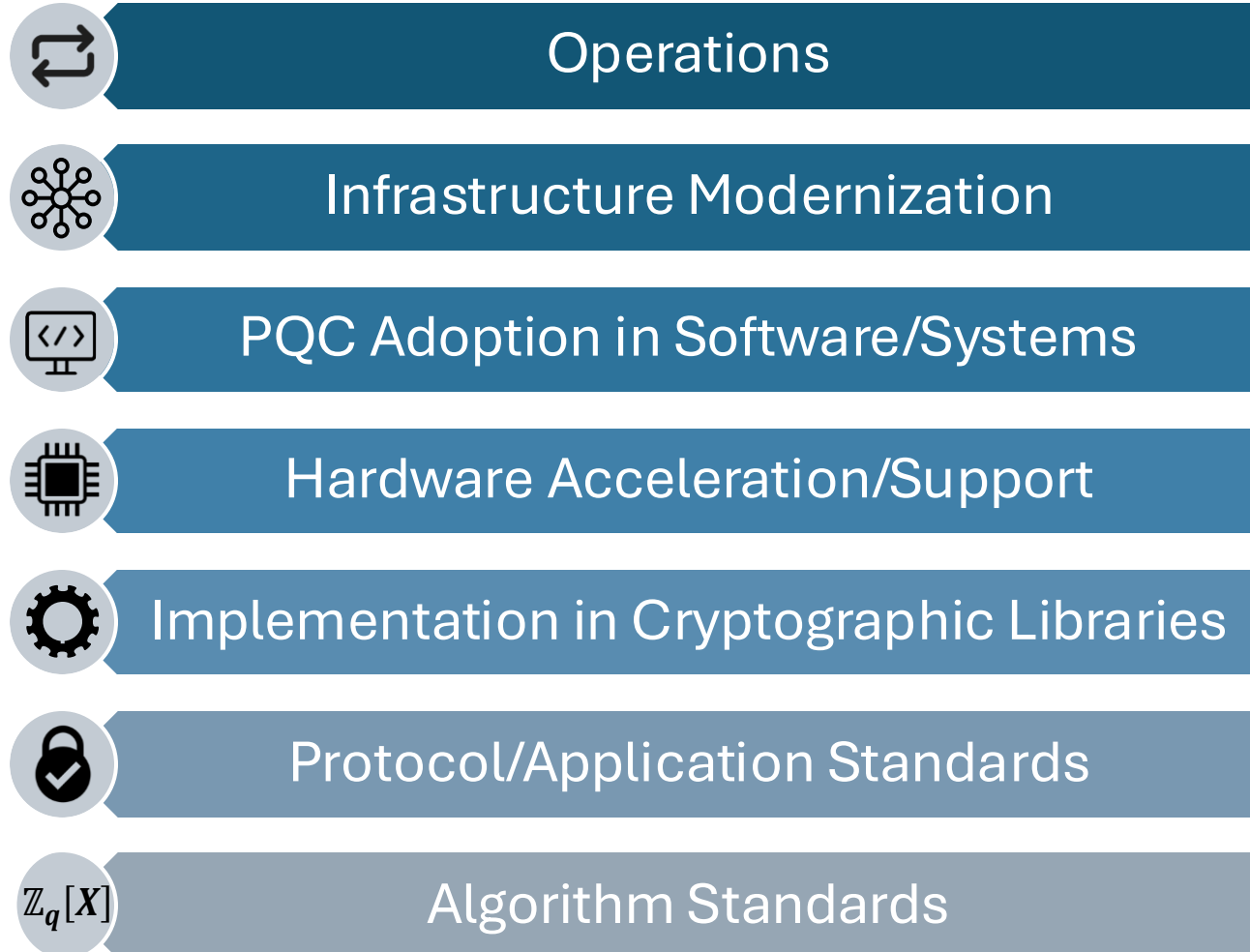
The screenshot shows a GitHub repository page for 'state-of-protocols-and-pqc'. The repository is public and has 102 commits. The README file is open, displaying a table titled 'Protocol-independent algorithm or cryptography specifications'. The table lists four draft titles with their corresponding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

PQC– Much Work Remains



PQC Standards- Next Steps



- ***ML-KEM***, ***ML-DSA***, & ***SLH-DSA*** finalized on August 13
- Draft ***FN-DSA*** (Falcon) standard under development
- NIST made 4th round KEM selection in 2025
 - Classic McEliece
 - BIKE
 - **HQC**
 - ~~SIKE~~
- NIST called for additional signatures in 2022 to evaluate general-purpose signatures based on diversified math problems
 - 14 algorithms were selected for a second round





Contact Information

Dustin Moody, Cryptographic Technology Group

Email: dustin.moody@nist.gov

NIST PQC standardization

www.nist.gov/pqcrypto

Email: pqc-comments@nist.gov

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

NCCoE PQC Migration Project

www.nccoe.nist.gov/applied-cryptography

Request to join Community of Interest

Email: applied-crypto-pqc@nist.gov