Post-Quantum Cryptography

Update on NIST Standard/Guidelines

Convening to Act

Accelerating U.S. Post-Quantum Cryptography Adoption: From Standards to Deployment

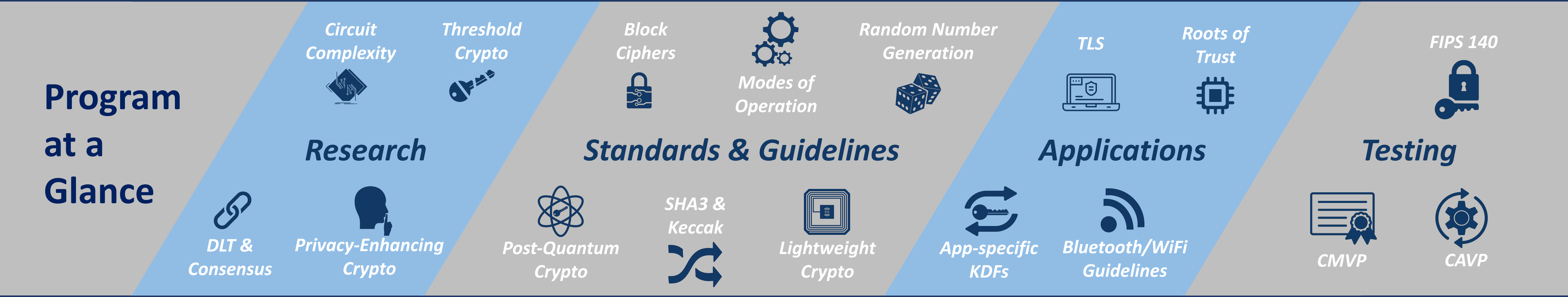
Andy Regenscheid
Cryptographic Technology Group
Computer Security Division, NIST

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

March 2026

Cryptographic Standards Program

- Research, develop, engineer, and produce standards, guidelines, recommendations, and best practices for cryptographic algorithms, methods, and protocols.
- Promote the use of validated cryptography, and inform federal cryptography procurement decisions, through the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP).



Program at a Glance

Research: *Circuit Complexity*, *Threshold Crypto*, *DLT & Consensus*, *Privacy-Enhancing Crypto*

Standards & Guidelines: *Block Ciphers*, *Modes of Operation*, *Random Number Generation*, *Post-Quantum Crypto*, *SHA3 & Keccak*, *Lightweight Crypto*

Applications: *TLS*, *Roots of Trust*, *App-specific KDFs*, *Bluetooth/WiFi Guidelines*

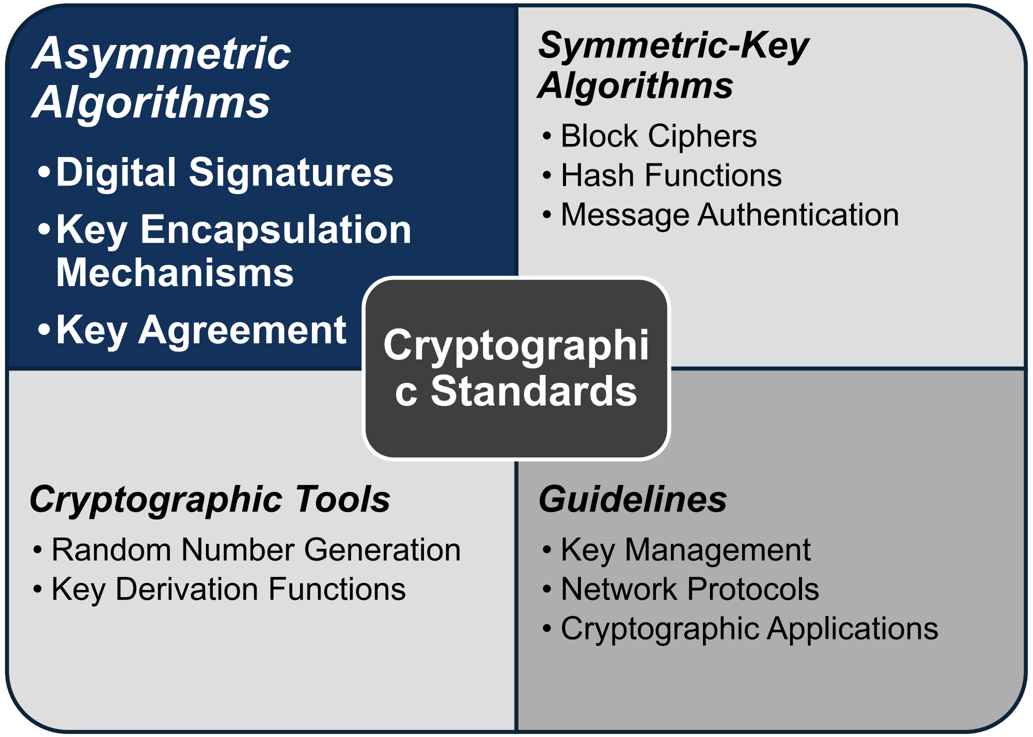
Testing: *FIPS 140*, *CMVP*, *CAVP*

Quantum Threat

- **Quantum computers threaten the security of widely-deployed public key cryptosystems**
    - *Signatures*– ECDSA, RSA
    - *Key Establishment*–Diffie-Hellman, RSA

- Need for new cryptographic algorithms and standards based on different mathematical problems that can withstand attacks by quantum computers

- Quantum algorithms have a much smaller impact on the security of symmetric-key cryptography



Asymmetric Algorithms

- **Digital Signatures**
- **Key Encapsulation Mechanisms**
- **Key Agreement**

Symmetric-Key Algorithms

- Block Ciphers
- Hash Functions
- Message Authentication

Cryptographi c Standards

Cryptographic Tools

- Random Number Generation
- Key Derivation Functions

Guidelines

- Key Management
- Network Protocols
- Cryptographic Applications

The First Set of NIST PQC Standards

Published August 2024

FIPS 203

Module-Lattice-Based
Key-Encapsulation Mechanism
Standard

(CRYSTALS-Kyber)

- A module learning with errors (MLWE)-based key encapsulation mechanism (KEM)
- Good performance on different platforms
- Moderate public-key and ciphertext size
- Suitable for applications requiring key establishment for encryption

FIPS 204

Module-Lattice-Based Digital
Signature Standard

(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 requiring digital signatures

FIPS 205

Stateless Hash-Based Digital
Signature Standard

(SPHINCS+)

- Conservative design based on security of well-understood cryptographic hash functions
- Does not state management by signers compared to earlier LMS/XMSS standards
- Solid security, signatures are longer compared with ML-DSA

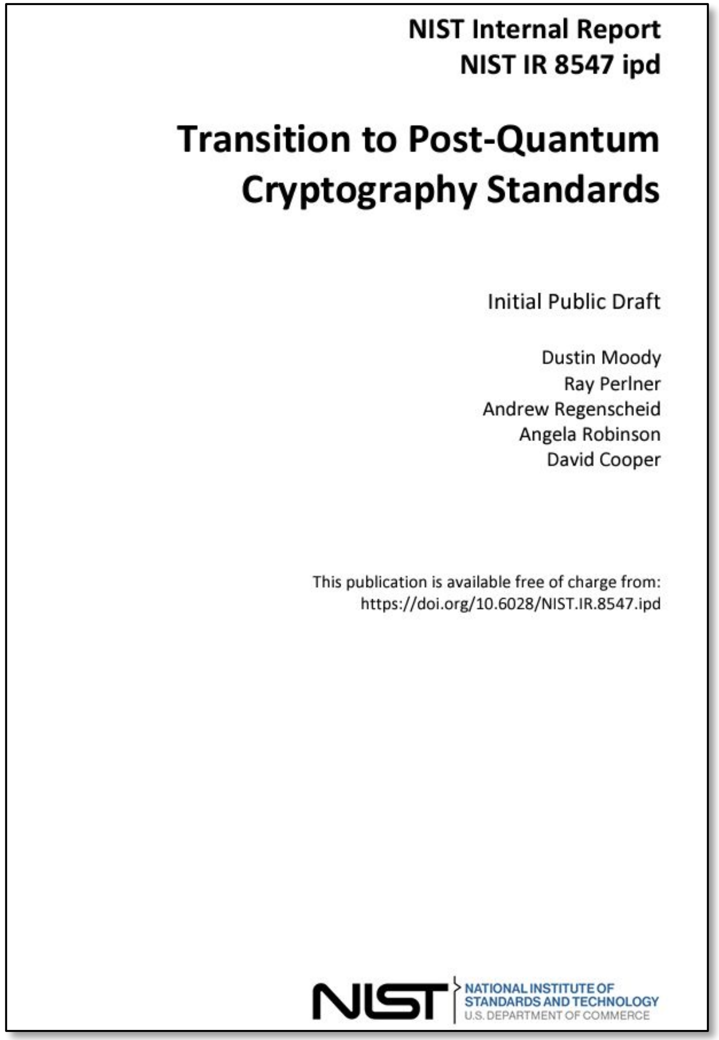
Practical Considerations for Adoption

- **Performance of PQC algorithms:**
  - Performance in key generation, encapsulation/decapsulation, signing/verification
  - Bandwidth/space demanding for transmit/storage public key, signature, ciphertext
- **PQC performance is comparable to commonly-deployed algorithms**
- **Public key and signature sizes are significantly larger than RSA and ECC signatures**
  - May lead to significant challenges in bandwidth-constrained use cases, e.g., GPS, Vehicle-to-Vehicle Communication.

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-87 *(Dilithium5)*	**2592**	**4864**	**4595**	**PQC Category 5** *(AES-256)*

NIST IR 8547, Transition to PQC Standards

- Initial Public Draft released November 2024
  - Comment period ended ***January 10th***
- 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 186-5)
- Proposed transition timelines for quantum-vulnerable algorithms
  - Deprecation after 2030
  - 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

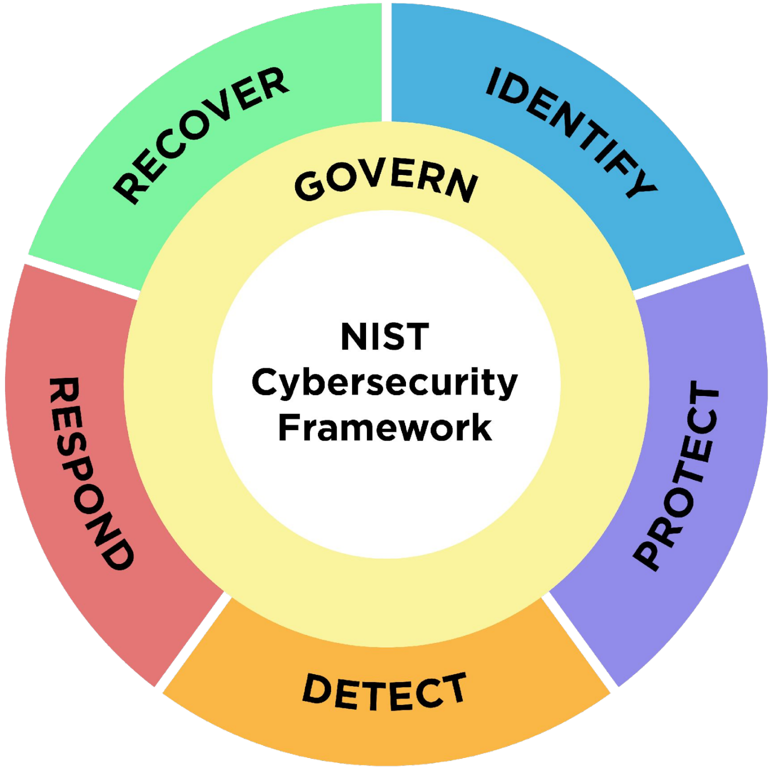
Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

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

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

Cryptography in the CSF 2.0

Public key cryptography is a foundational tool for implementing security objectives and controls



Data Security (PR.DS): Data are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information

- **PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected
- **PR.DS-02:** The confidentiality, integrity, and availability of data-in-transit are protected
- **PR.DS-10:** The confidentiality, integrity, and availability of data-in-use are protected
- **PR.DS-11:** Backups of data are created, protected, maintained, and tested

SP 800-53 Security Controls

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: Protect the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

SC-13 CRYPTOGRAPHIC PROTECTION

Control: a. Determine the [*Assignment: organization-defined cryptographic uses*]; and b. Implement the following types of cryptography required for each specified cryptographic use: [*Assignment: organization-defined types of cryptography for each specified cryptographic use*].

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: a. Issue public key certificates under an [*Assignment: organization-defined certificate policy*] or obtain public key certificates from an approved service provider; and b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

SC-28 PROTECTION OF INFORMATION AT REST

Control: Protect the [*Selection (one or more): confidentiality; integrity*] of the following information at rest: [*Assignment: organization-defined information at rest*].

SP 800-171– Controlled Unclassified Information

NIST SPECIAL PUBLICATION

SP 800-171r3

171

REVISION 3

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

03.05.08 Transmission and Storage Confidentiality

Implement cryptographic mechanisms to prevent the unauthorized disclosure of CUI during transmission and while in storage.

03.13.10 Cryptographic Key Establishment and Management

Establish and manage cryptographic keys in the system in accordance with the following key management requirements: [*Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction*].

03.13.11 Cryptographic Protection

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

PQC Testing Under FIPS 140

Cryptographic Module Validation Program (CMVP)

- Joint program between NIST and Canadian Centre for Cyber Security (CCCS)

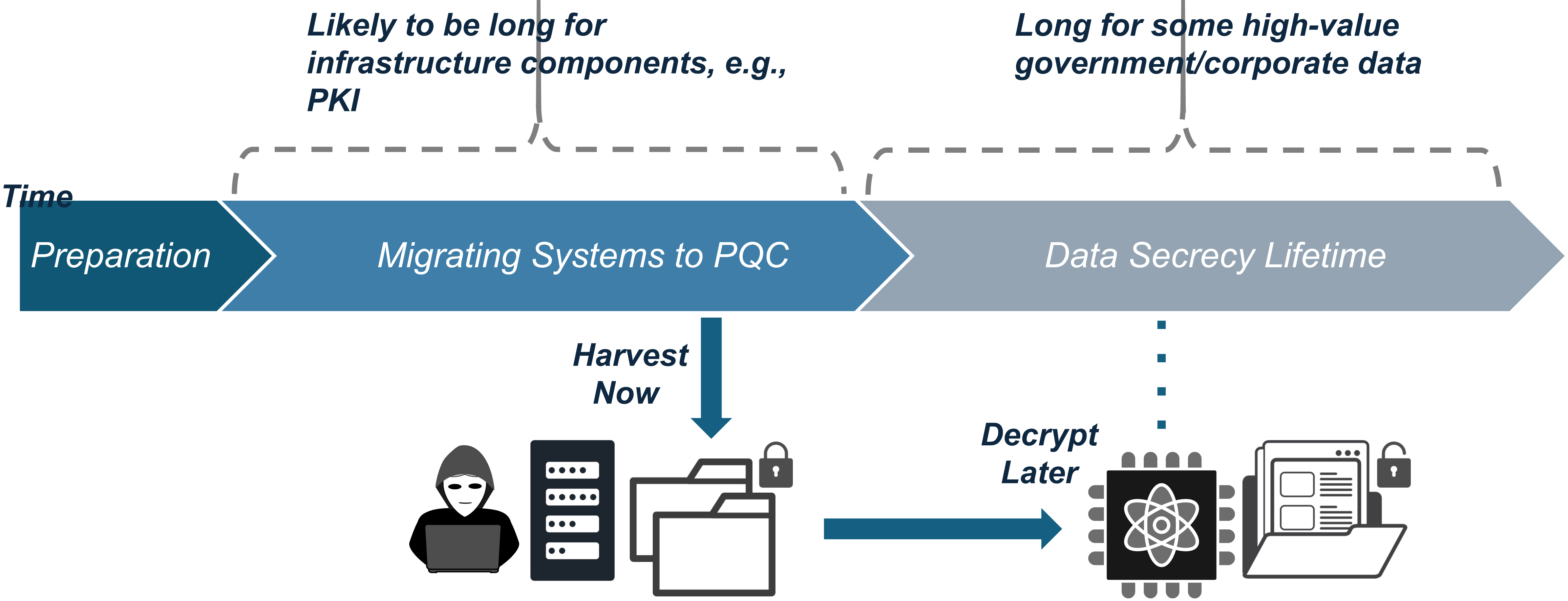
Automated Cryptographic Validation Testing System (ACVTS)

- Testing for algorithm standards to verify correct implementation of cryptographic standards
- Validated 81 implementations of ***ML-DSA***, 33 of ***SLH-DSA***, and 91 of ***ML-KEM***

Vendors, Labs, and CMVP

- Vendors use independent, **NVLAP-accredited Cryptographic and Security Testing (CST) laboratories** to test their modules. Over 20 labs worldwide.
- CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and other CMVP programmatic guidance to test conformance against FIPS 140-3.
- FIPS 140-3 and NIST SP 800-140 modify ISO/IEC 19790 and ISO/IEC 24759.

Migration Considerations



Likely to be long for infrastructure components, e.g., PKI

Long for some high-value government/corporate data

Time

Preparation

Migrating Systems to PQC

Data Secrecy Lifetime

Harvest Now

Decrypt Later

Standards– State of Migration

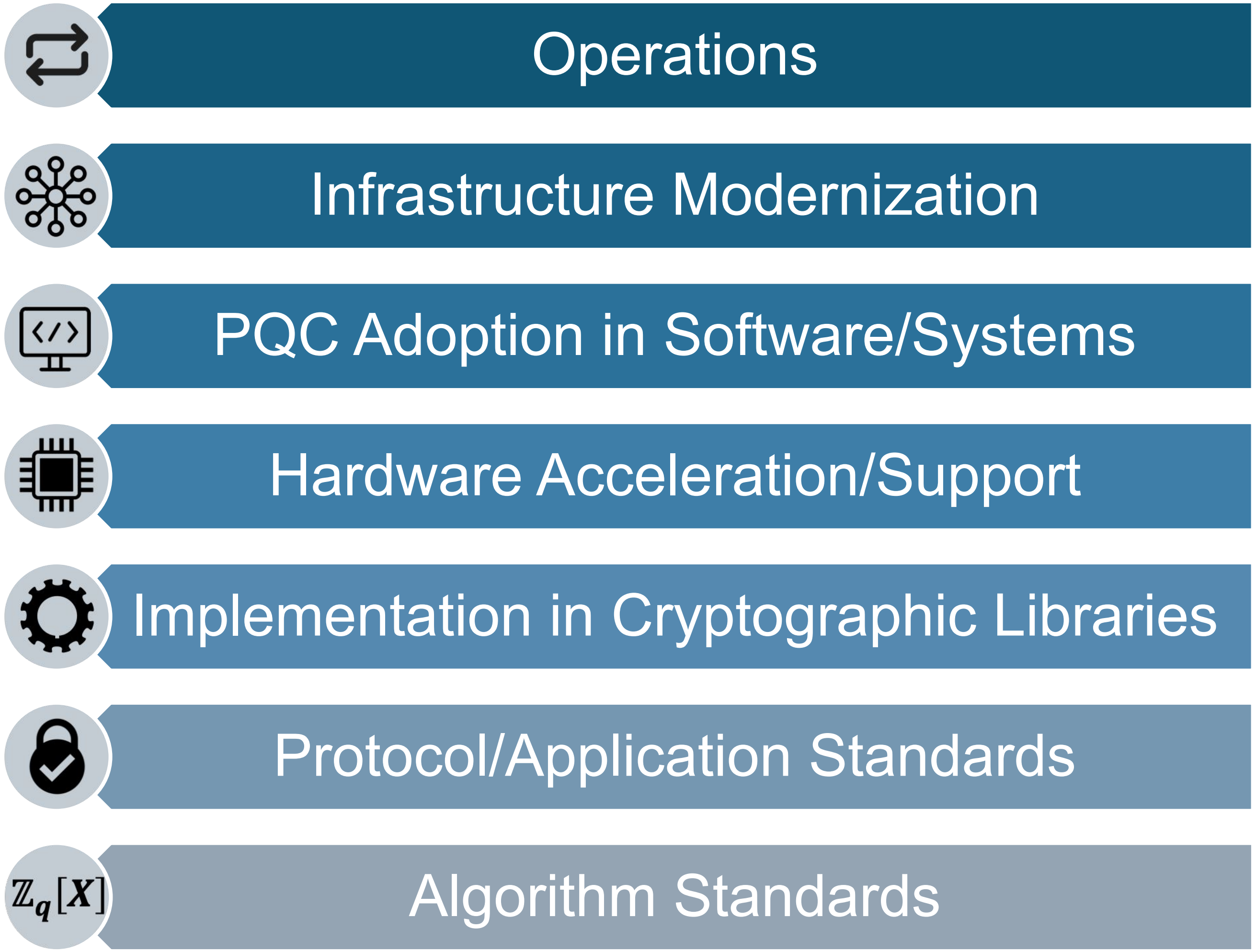
Standard	Pure PQC encrypt	Hybrid PQ encrypt	Pure PQ sig	Hybrid PQ sig
SSH	*Drafts*	**Some Adoption**	*Drafts*	*Drafts*
TLS 1.2	**-**	**-**	**-**	**-**
TLS 1.3	**Integrated**	**Broad Adoption**	**Integrated**	*Drafts*
X.509	**Integrated**	Finalization	**Integrated**	**Finalization**
S/MIME	**Finalized**	*Drafts*	**Integrated**	*Drafts*
OpenPGP	*In-Progress*	**Finalization**	**Finalization**	**Finalization**
IKE/IPSec	**Some Adoption**	**Some Adoption**	*Drafts*	*In-Progress*
MLS	**Finalization**	**Finalization**	**Finalization**	*In-Progress*
DNSSec	**-**	**-**	*Stalled*	*Stalled*

Source: Post-Quantum Cryptography Coalition: https://pqcc.org/

Prioritization

- **High-Impact Systems and Data Assets**
  - Accelerate PQC deployment – particularly for key agreement
  - Consider mitigating architectures/controls
- **Network Infrastructure**
  - Web Services – cloud services and locally-hosted
  - VPN clients/gateways and remote access
- **Identity & Trust Infrastructures**
  - Code Signing – support and usage
  - Authentication and Authorization Systems
- **Operational Technology with Long Lifecycles**
  - Integrate PQC into procurement, modernization, and refresh cycle
- **Legacy Systems**
  - Prepare to update or migrate systems and software

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

Questions

NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
UNITED STATES DEPARTMENT OF COMMERCE
100 Bureau Drive

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