Post-Quantum

Cryptography Conference

# Status update from NIST


## Bill Newhouse

Cybersecurity Engineer & Project Lead, National Cybersecurity Center of Excellence (NCCoE) at NIST

## Dustin Moody

Mathematician &
Project Lead, Post-Quantum Cryptography at NIST

# Post-Quantum Cryptography
## - Status Update from NIST

**Dustin Moody**
**Bill Newhouse**

Tuesday, October 3rd, 2023

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

# QUANTUM ALGORITHMS

- 1994 – SHOR'S ALGORITHM
  - A QUANTUM ALGORITHM GIVING AN EXPONENTIAL SPEED-UP OVER CLASSICAL COMPUTERS
    - FACTORING LARGE INTEGERS
    - FINDING DISCRETE LOGARITHMS

**Algorithms for Quantum Computation: Discrete Logarithms and Factoring**

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

**Abstract**

*A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)*

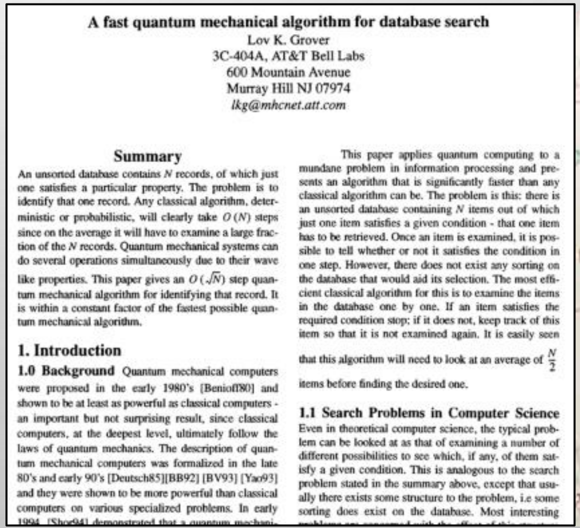
**1 Introduction**

Since the discovery of quantum mechanics, people have found the behavior of the laws of probability in quantum mechanics counterintuitive. Because of this behavior, quantum mechanical phenomena behave quite differently than the phenomena of classical physics that we are used

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of problems which can be solved by efficient algorithms is known as P. This classification has several nice properties. For one thing, it does a reasonable job of reflecting the performance of algorithms in practice (although an algorithm whose running time is the tenth power of the input size, say, is not truly efficient). For another, this classification is nice theoretically, as different reasonable machine models

- 1996 - GROVER'S ALGORITHM
  - POLYNOMIAL SPEED-UP IN UNSTRUCTURED SEARCH, FROM O($N$ ) TO O($\sqrt{N}$)



**A fast quantum mechanical algorithm for database search**

Lov K. Grover
3C-404A, AT&T Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
*lkg@mhcnet.att.com*

**Summary**

An unsorted database contains $N$ records, of which just one satisfies a particular property. The problem is to identify that one record. Any classical algorithm, deterministic or probabilistic, will clearly take $O(N)$ steps since on the average it will have to examine a large fraction of the $N$ records. Quantum mechanical systems can do several operations simultaneously due to their wave like properties. This paper gives an $O(\sqrt{N})$ step quantum mechanical algorithm for identifying that record. It is within a constant factor of the fastest possible quantum mechanical algorithm.

**1. Introduction**

**1.0 Background** Quantum mechanical computers were proposed in the early 1980's [Benioff80] and shown to be at least as powerful as classical computers - an important but not surprising result, since classical computers, at the deepest level, ultimately follow the laws of quantum mechanics. The description of quantum mechanical computers was formalized in the late 80's and early 90's [Deutsch85][BB92] [BV93] [Yao93] and they were shown to be more powerful than classical computers on various specialized problems. In early

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing $N$ items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of $\frac{N}{2}$ items before finding the desired one.

**1.1 Search Problems in Computer Science** Even in theoretical computer science, the typical problem can be looked at as that of examining a number of different possibilities to see which, if any, of them satisfy a given condition. This is analogous to the search problem stated in the summary above, except that usually there exists some structure to the problem, i.e some sorting does exist on the database. Most interesting

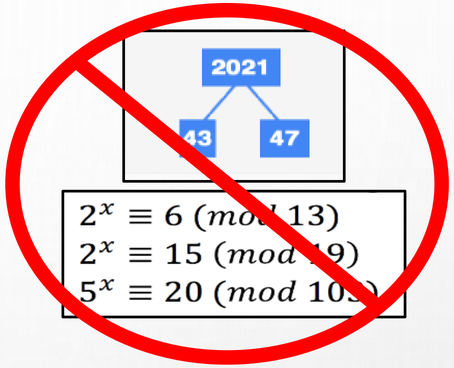
# THE QUANTUM THREAT

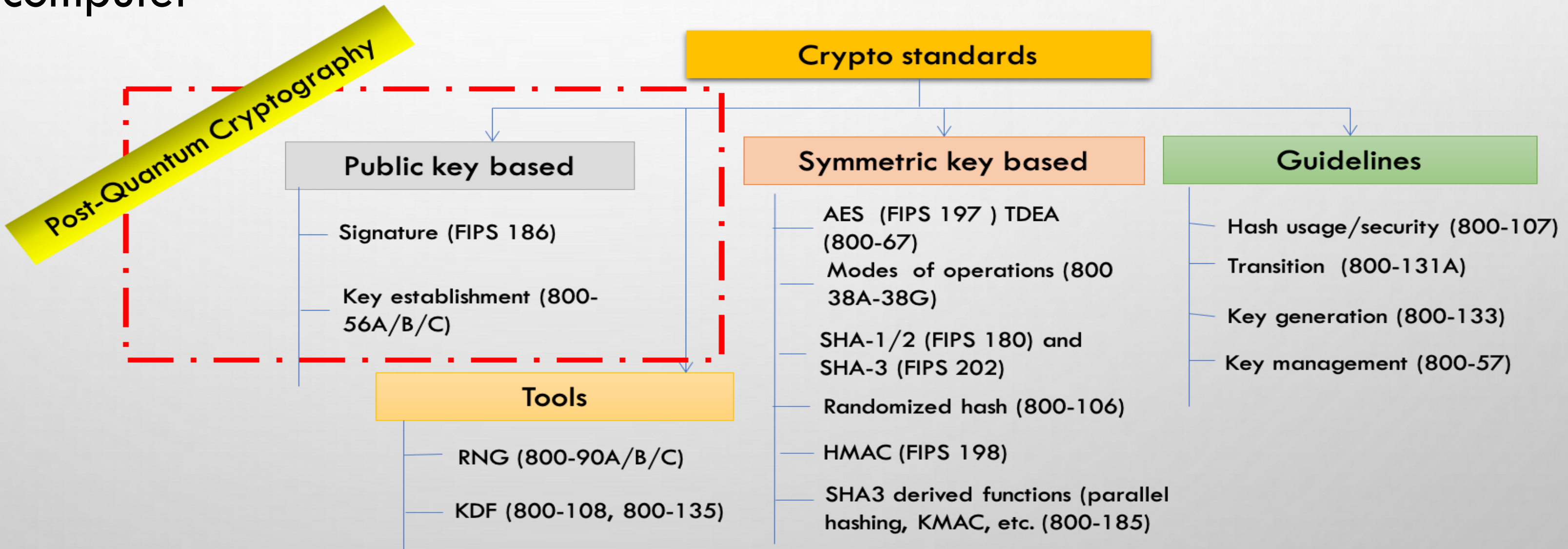
NIST

- 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

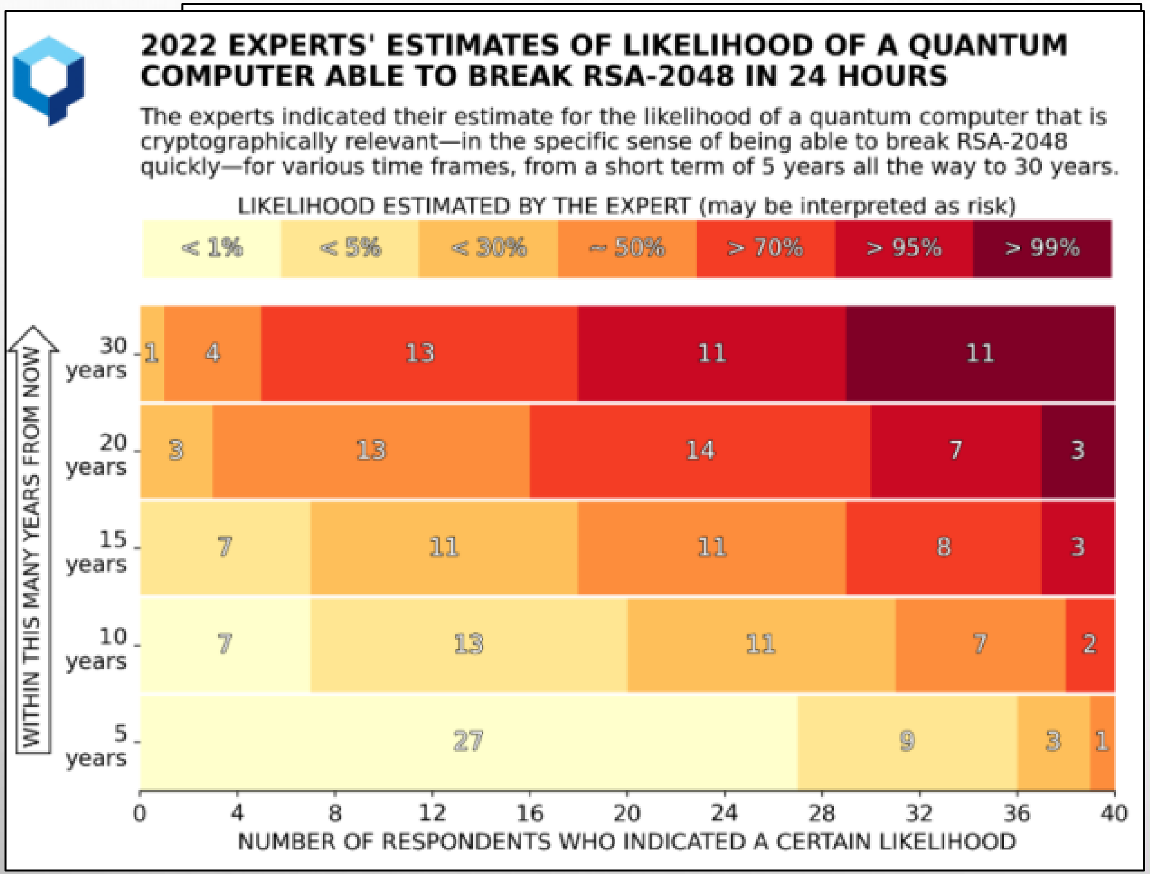


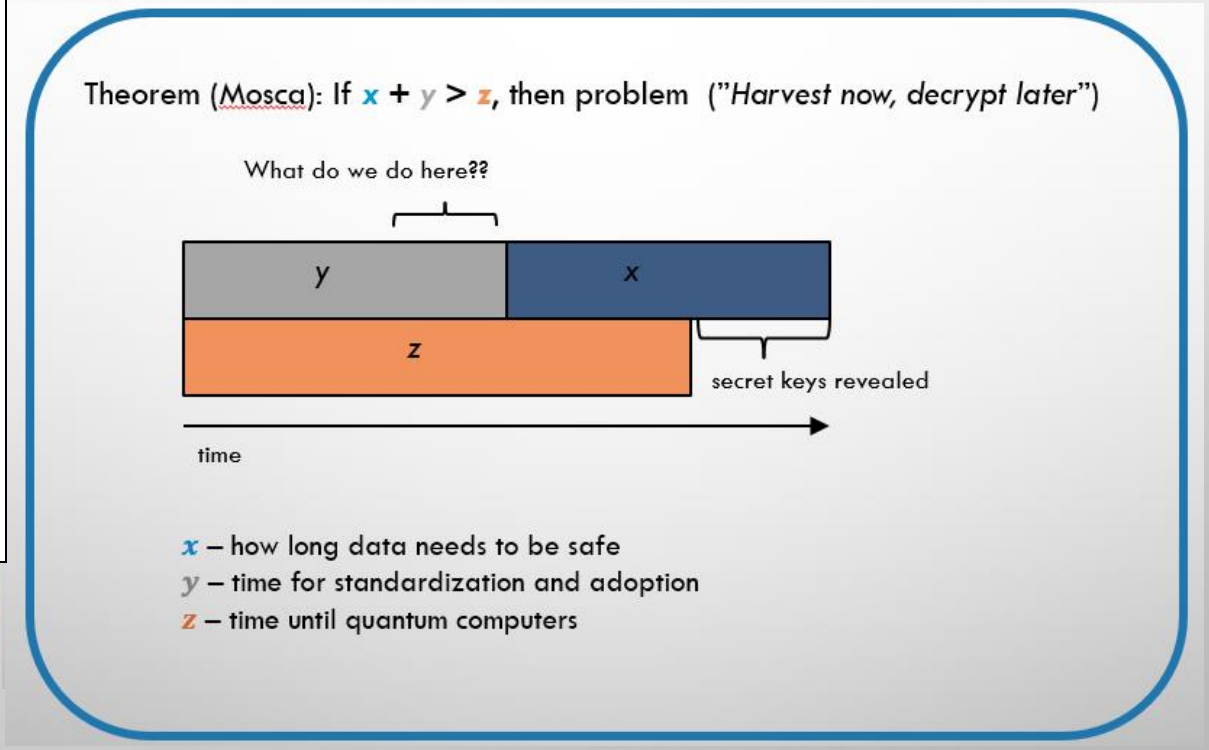

- Symmetric-key crypto (AES, SHA) would also be affected (by Grover's algorithm), but less dramatically

# HOW SOON DO WE NEED TO WORRY?

# HOW SOON DO WE NEED TO WORRY?




Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2022
https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/



# 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 AGE

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with National Sec
Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Comp While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

Administ

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

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

"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**."

Announcing the Commercial National Security Algorithm Suite 2.0

CNSA 2.0

CYBERSECURITY ADVISORY

# 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'

# SELECTION CRITERIA

## 1. **SECURE** AGAINST BOTH CLASSICAL AND QUANTUM ATTACKS

| 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) |

## 2. **PERFORMANCE** - MEASURED ON VARIOUS "CLASSICAL" PLATFORMS

## 3. **OTHER PROPERTIES**

- DROP-IN REPLACEMENTS - COMPATIBILITY WITH EXISTING PROTOCOLS AND NETWORKS
- PERFECT FORWARD SECRECY
- RESISTANCE TO SIDE-CHANNEL ATTACKS
- SIMPLICITY AND FLEXIBILITY
- MISUSE RESISTANCE, ETC…

# THE FIRST THREE ROUNDS

NIST

## ROUND 1 (DEC '17 – JAN '18)

- 69 CANDIDATES AND 278 DISTINCT SUBMITTERS
- SUBMITTERS FROM >25 COUNTRIES, ALL 6 CONTINENTS
- APR 2018, 1ST NIST PQC CONFERENCE
- ALMOST 25 SCHEMES BROKEN/ATTACKED
- NISTIR 8240, NIST REPORT ON THE 1ST ROUND

| | Signatures | KEM/Encryption | Overall |
|---|---|---|---|
| Lattice-based | 5 | 21 | 26 |
| Code-based | 2 | 17 | 19 |
| Multi-variate | 7 | 2 | 9 |
| Symmetric based | 3 | | 3 |
| Other | 2 | 5 | 7 |
| Total | **19** | **45** | **64** |

## ROUND 2 (JAN '18 – JUL '20)

- 26 CANDIDATES
- AUG 2019 – 2ND NIST PQC CONFERENCE
- 7 SCHEMES BROKEN/ATTACKED
- NISTIR 8309, NIST REPORT ON THE 2ND ROUND

| | Signatures | KEMs/Encryption | Total |
|---|---|---|---|
| Lattice-based | 3 | 9 | 12 |
| Code-based | 0 | 7 | 7 |
| Multi-variate | 4 | 0 | 4 |
| Symmetric-based | 2 | | 2 |
| Other | 0 | 1 | 1 |
| | | | |
| Total | **9** | **17** | **26** |

## ROUND 3 (JUL '20 – JUL '22)

- 7 FINALISTS AND 8 ALTERNATES
- JUNE 2021 – 3RD NIST PQC CONFERENCE
- NISTIR 8413, NIST REPORT ON THE 3RD ROUND

| | Signatures | KEMs/Encryption | Total |
|---|---|---|---|
| Lattice-based | 2 | 5 | 7 |
| Code-based | 0 | 3 | 3 |
| Multi-variate | 2 | 0 | 2 |
| Symmetric-based | 2 | 0 | 2 |
| Other | 0 | 1 | 1 |
| | | | |
| Total | **6** | **9** | **15** |

# ROUND 3 RESULTS

NIST

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~~

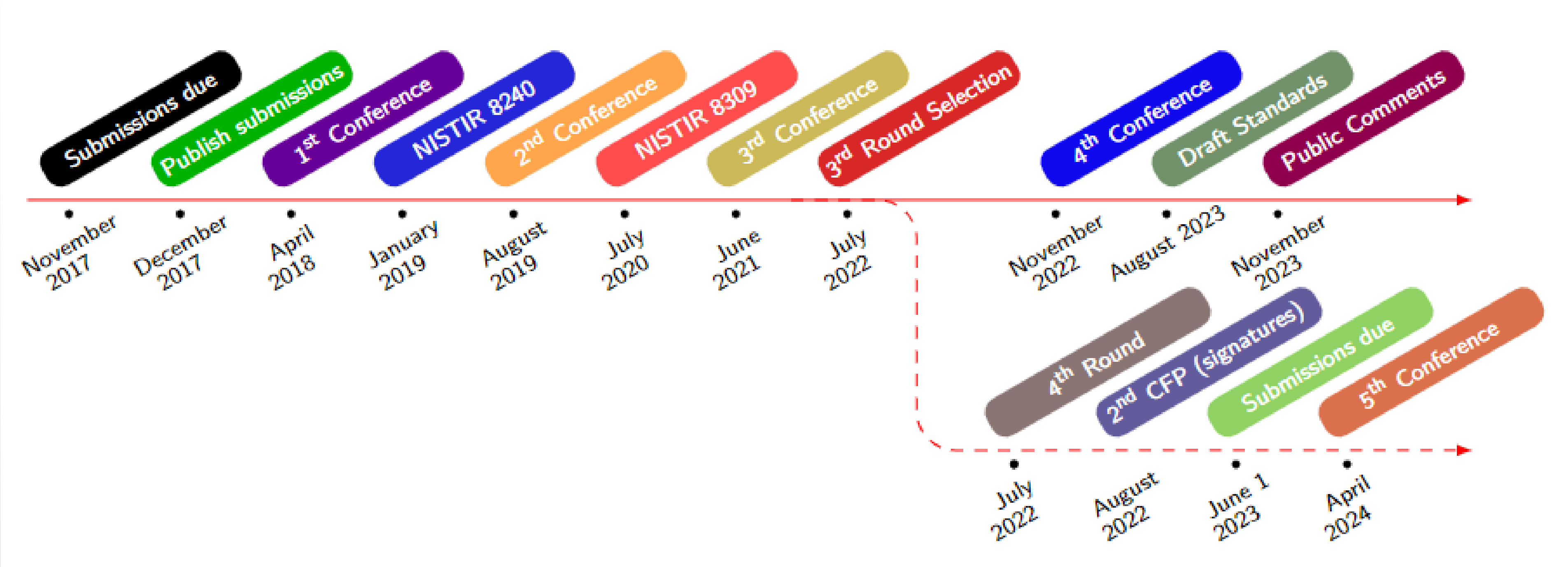
**On-ramp signatures**

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

# THE SELECTED ALGORITHMS

- CRYSTALS-KYBER
  - KEM BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY
- CRYSTALS-DILITHIUM
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY, RELATIVELY SIMPLE IMPLEMENTATION
  - NIST RECOMMENDS IT BE THE PRIMARY SIGNATURE ALGORITHM USED
- FALCON
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - SMALLER BANDWIDTH, BUT MUCH MORE COMPLICATED IMPLEMENTATION
  - THE FALCON STANDARD WILL COME OUT AFTER THE OTHERS
- SPHINCS+
  - DIGITAL SIGNATURE BASED ON STATELESS HASH-BASED CRYPTOGRAPHY
  - SOLID SECURITY, BUT PERFORMANCE NOT AS GOOD IN COMPARISON TO DILITHIUM/FALCON

# TIMELINE




- The 5th NIST PQC Standardization Conference
  - April 10-12, 2024 in Rockville, Maryland
- Draft standards for public comment released Aug 2023
  - Deadline for comments: November 22, 2023
- **The first PQC standards should be published in 2024**

# STANDARDIZATION


- THE 1ST PQC STANDARDS
    - FIPS 203: ML-KEM (KYBER)
    - FIPS 204: ML-DSA (DILITHIUM)
    - FIPS 205: SLH-DSA (SPHINCS+)
    - FN-DSA (FALCON) – UNDER DEVELOPMENT
  - WILL HAVE OTHER DOCS WITH MORE GUIDANCE/DETAILS
- SOME CHOICES MADE
    - WHICH PARAMETER SETS, WHICH HASH FUNCTIONS, OTHER SYMMETRIC PRIMITIVES, ETC
- PLEASE PROVIDE FEEDBACK
    - PQC-FORUM, EMAIL ETC

# THE KEMS IN THE $4^{\text{TH}}$ 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
- BIKE
  - Most competitive performance of $4^{\text{th}}$ 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

# AN ON-RAMP FOR SIGNATURES

- 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 that have short signatures and fast verification.

- The more mature the scheme, the better.
- NIST will decide which (if any) of the received schemes to focus attention on

- Currently ongoing - See my talk tomorrow for more details!

No on-ramp for KEMs currently planned.

# STATEFUL HASH BASED SIGNATURES FOR EARLY ADOPTION

## Stateful hash-based signatures were proposed in 1970s

- Rely on assumptions on hash functions, that is, not on number theory complexity assumptions
- It is essentially limited-time signatures, which require state management

## NIST specification on stateful hash-based signatures

- NIST SP 800-208 "*Recommendation for Stateful Hash-Based Signature Schemes*"

## Internet Engineering Task Force (IETF) has released two RFCs on hash-based signatures

- RFC 8391 "XMSS: eXtended Merkle Signature Scheme" (By Internet Research Task Force (IRTF))
- RFC 8554 "Leighton-Micali Hash-Based Signatures" (By Internet Research Task Force (IRTF))

## ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

- Stateful hash-based signatures will be specified in ISO/IEC 14888 Part 4
- It is in the 1st Working Draft stage

Stateful hash-based signatures from SP 800-208 are allowed for signing software/firmware updates in CNSA 2.0 (Commercial National Security Algorithms suite)

# OTHER STANDARDS ORGANIZATIONS

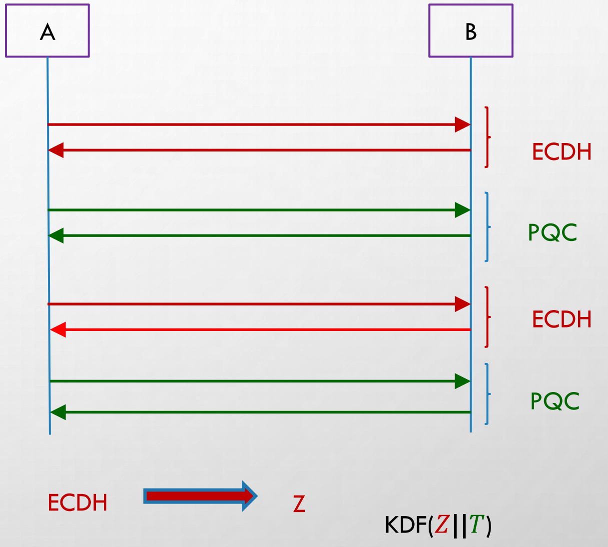
- WE ARE AWARE THAT MANY STANDARDS ORGANIZATIONS AND EXPERT GROUPS ARE WORKING ON PQC
  - ASC X9 HAS DONE STUDIES AND WRITTEN WHITE PAPERS
  - IEEE P1363.3 HAS STANDARDIZED SOME LATTICE-BASED SCHEMES
  - IETF HAS STANDARDIZED STATEFUL HASH-BASED SIGNATURES LMS/XMSS AND IS CURRENTLY DOING NEW WORK GEARED TO THE PQC MIGRATION
  - 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

- THERE HAS BEEN MUCH DISCUSSION ON HYBRID/COMPOSITE MODES
  - NIST SP800-56C REV. 2 ALLOWS FOR A CERTAIN HYBRID MODE
  - WE WILL WORK WITH THE COMMUNITY IN DIFFERENT STAGES OF MIGRATION TO ASSURE SECURITY

- NIST WILL PROVIDE TRANSITION GUIDELINES TO PQC STANDARDS
  - NIST HAS PROVIDED SUCH GUIDANCE BEFORE
    - EXAMPLES: TRIPLE DES, SHA-1, KEYS < 112 BITS
  - TIMEFRAME WILL BE BASED ON RISK ASSESSMENT OF QUANTUM ATTACKS



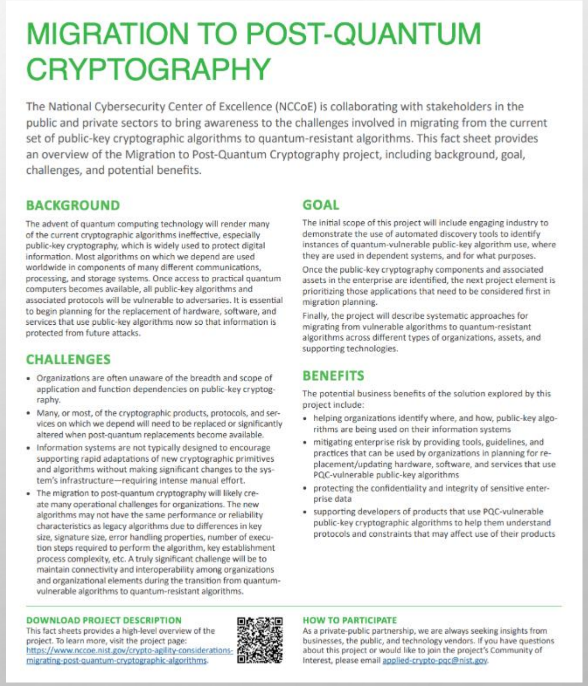
# THE NCCOE MIGRATION TO PQC PROJECT

- COMPLEMENT STANDARDIZATION AND TACKLE CHALLENGES WITH ADOPTION, IMPLEMENTATION AND DEPLOYMENT TO PQC
  - COORDINATE WITH SDO'S AND INDUSTRY COLLABORATORS

- PRODUCT DELIVERABLES
  - PRACTICE GUIDES, PLAYBOOKS, REFERENCE ARCHITECTURES, AUTOMATED TOOLS, PROOF OF CONCEPT CODE, ETC
  - DRAFT SP 1800-38 VOLUME A: EXEC SUMMARY

- OUTREACH AND ENGAGEMENT
  - COMMUNITY OF INTEREST, WEBINARS, PUBLIC EVENTS
  - IN PERSON MEETING – AUG 15 AT NCCOE
  - APPLIED-CRYPTO-PQC@NIST.GOV

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



## 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

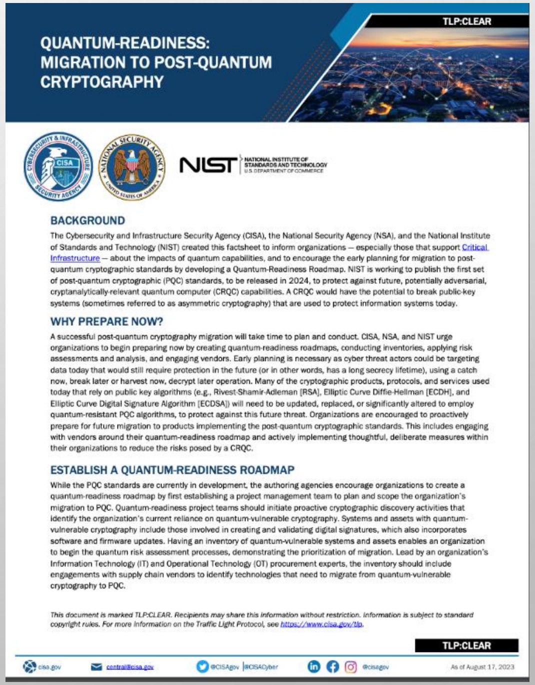
This fact sheets provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

### 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.

# WHAT CAN ORGANIZATIONS DO NOW?

- (FOLLOW GUIDANCE IN THE OMB MEMO)
- NEW CISA/NSA/NIST FACTSHEET: *QUANTUM READINESS – MIGRATION TO POST-QUANTUM CRYPTOGRAPHY*
  - CRYPTOGRAPHIC INVENTORY
  - DISCUSS POST-QUANTUM ROADMAP W/ TECHNOLOGY VENDORS
  - SUPPLY CHAIN QUANTUM-READINESS
- DEVELOP A KNOWLEDGE BASE AND TRACK DEVELOPMENTS IN THE FIELD
  - TESTING THE ALGORITHMS ENCOURAGED
- ESTABLISH A ROADMAP TO QUANTUM READINESS FOR YOUR ORGANIZATION
- ACT NOW – IT WILL BE LESS EXPENSIVE, LESS DISRUPTIVE, AND LESS LIKELY TO HAVE MISTAKES CAUSED BY RUSHING AND SCRAMBLING



TLP:CLEAR

QUANTUM-READINESS: MIGRATION TO POST-QUANTUM CRYPTOGRAPHY

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

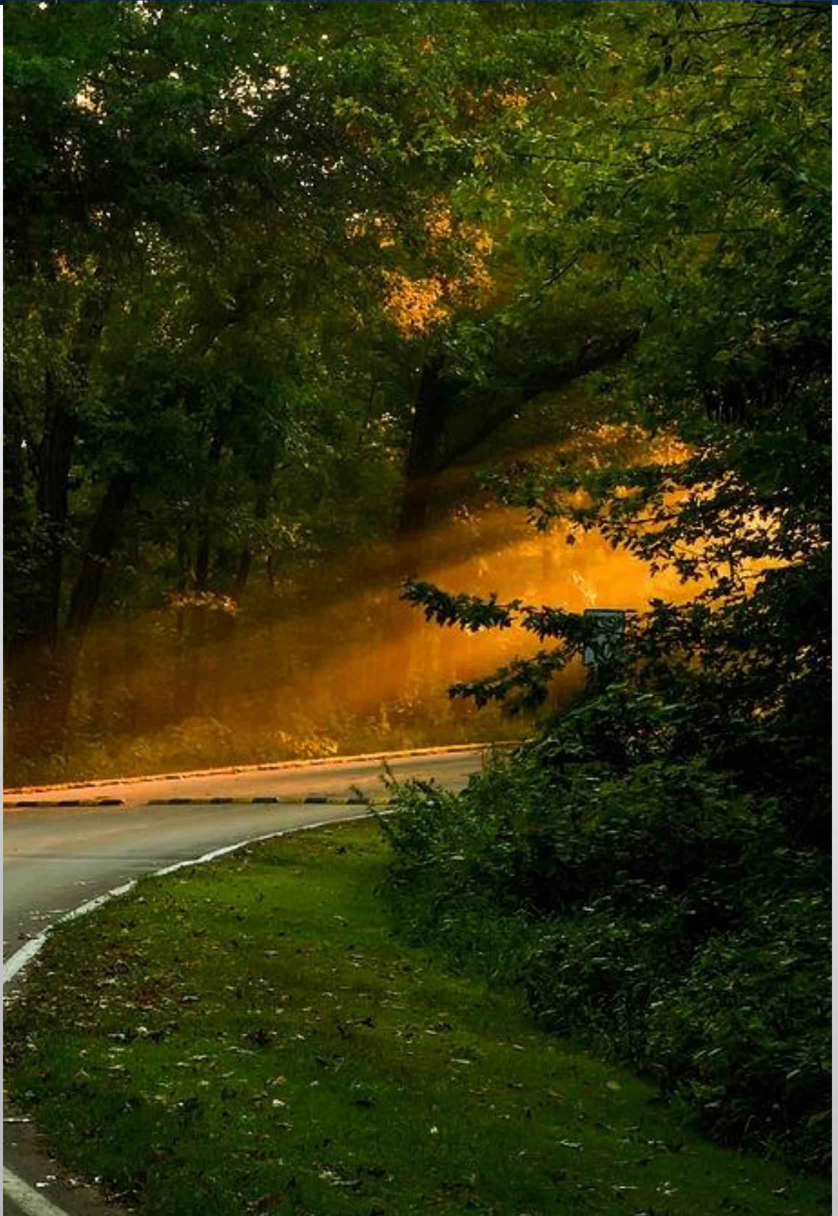
While the PQC standards are currently in development, the authoring agencies encourage organizations to create a quantum-readiness roadmap by first establishing a project management team to plan and scope the organization's migration to PQC. Quantum-readiness project teams should initiate proactive cryptographic 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-vulnerable systems and assets enables an organization to begin the quantum risk assessment processes, demonstrating the prioritization of migration. Lead by an organization's Information Technology (IT) and Operational Technology (OT) procurement experts, the inventory should include engagements with supply chain vendors to identify technologies that need to migrate from quantum-vulnerable cryptography to PQC.

*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 17, 2023

# THE NIST PQC STANDARDIZATION PROJECT



- THE BEGINNING OF THE END IS HERE!
- OR IS IT THE END OF THE BEGINNING?

- NIST APPRECIATES EVERYBODY'S EFFORTS

- CHECK OUT WWW.NIST.GOV/PQCRYPTO
  - SIGN UP FOR THE PQC-FORUM FOR ANNOUNCEMENTS & DISCUSSION
  - SEND E-MAIL TO PQC-COMMENTS@NIST.GOV

# NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

## Migration to Post-Quantum Cryptography Project

2nd hybrid Post-Quantum Cryptography (PQC) Conference in Amsterdam

Bill Newhouse, NIST NCCoE

November 7, 2023

# NCCOE OVERVIEW

NIST

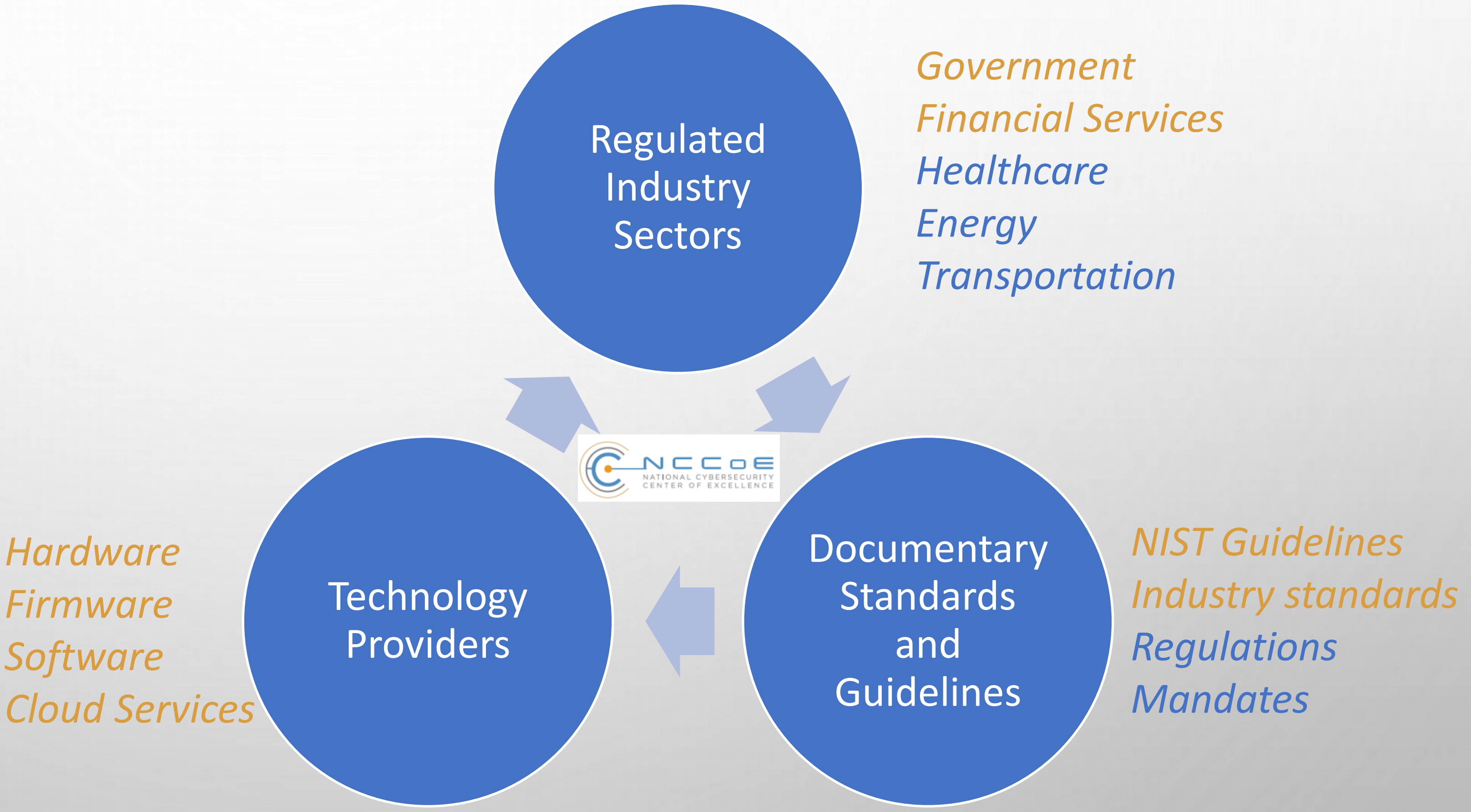
## National Cybersecurity Center of Excellence (NCCoE)

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

- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

**Practice Guide SP 1800**

## Engagement Model




https://www.nccoe.nist.gov/

# NCCOE PROJECT DELIVERABLES

## NIST Special Publication 1800 – Practice Guide

- **C-Suite**: executive summary
- **Architects and Infosec**: reference architecture, demonstration use cases, and security documentation
- **Operators and engineers**: implementation guide, bills of material, scripts, codes, tools, etc.

## Other documents

- Playbooks
- Cybersecurity papers
- Update existing standards, guidelines, protocols, etc.

## Open-source code

- Proof of concept code
- Infrastructure as code
- Sample applications

## Outreach and Engagement

- Community of interest
- Webinars
- Public events

# Migration to Post-Quantum Cryptography (PQC) Project Goal

Initiating the development of practices to ease migration from the current set of public-key cryptographic algorithms to replacement algorithms that are resistant to quantum computer-based attacks

# MIGRATION TO PQC PROJECT TIMELINE

NIST

**September 2018**

Plan for Migration to PQC

**May 2020**

Draft cybersecurity paper "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms"

**October 2020**

Virtual workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms

**April 2021**

Final cybersecurity paper "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms"

**June 2021**

Draft NCCoE project description "Migration to Post-Quantum Cryptography"

**October 2021**

Final NCCoE project description "Migration to Post-Quantum Cryptography" and the Federal Register Notice soliciting industry collaborators

**May 2022**

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems - NSM 10

**June 2022**

Kick-off project with industry and government participants

**June 2022 - Today**

Add Collaborators

**April 2023**

Published Preliminary Draft SP 1800 Volume A

**August 2023**

Host In-Person Event

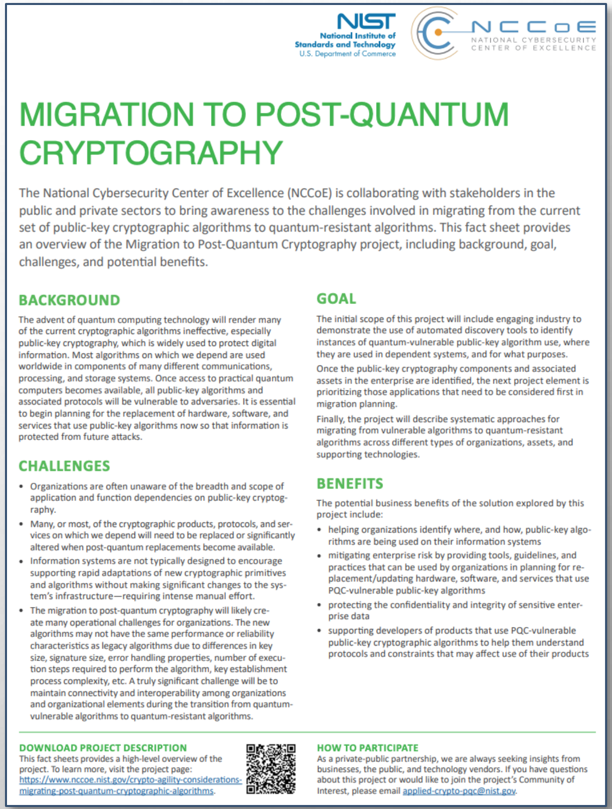
# Migration to PQC Project Collaborators

- Amazon Web Services, Inc. (AWS)
- Cisco Systems, Inc.
- Cybersecurity and Infrastructure Security Agency (CISA)
- Cloudflare, Inc.
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Dell Technologies
- DigiCert
- Entrust
- HP, Inc.
- IBM
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- *Keyfactor*
- *Microsoft*
- *National Security Agency (NSA)*
- *PQShield*
- *QuantumXChange*
- *SafeLogic, Inc.*
- *Samsung SDS Co., Ltd.*
- *SandboxAQ*
- *Santander*
- *SSH Communications Security Corp*
- *Thales DIS CPL USA, Inc.*
- *Thales Trusted Cyber Technologies*
- *Utimaco*
- *Verizon*
- *VMware, Inc.*
- *wolfSSL*

# MIGRATION TO PQC PROJECT FOCUS

NIST

- **Complement NIST PQC standardization effort**
- Support US Government PQC initiatives (White House NSM-10 (M-23-02), CISA, NSA CNSA 2.0, etc.)
- Tackle challenges with adoption, implementation, and deployment of PQC
- Engage with the community including industry collaborators and across government to bring awareness to the issues involved in migrating to post-quantum algorithms
- Coordinate with standard developing organizations and government and industry sectors community to develop guidance to accelerate the migration



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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

## 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

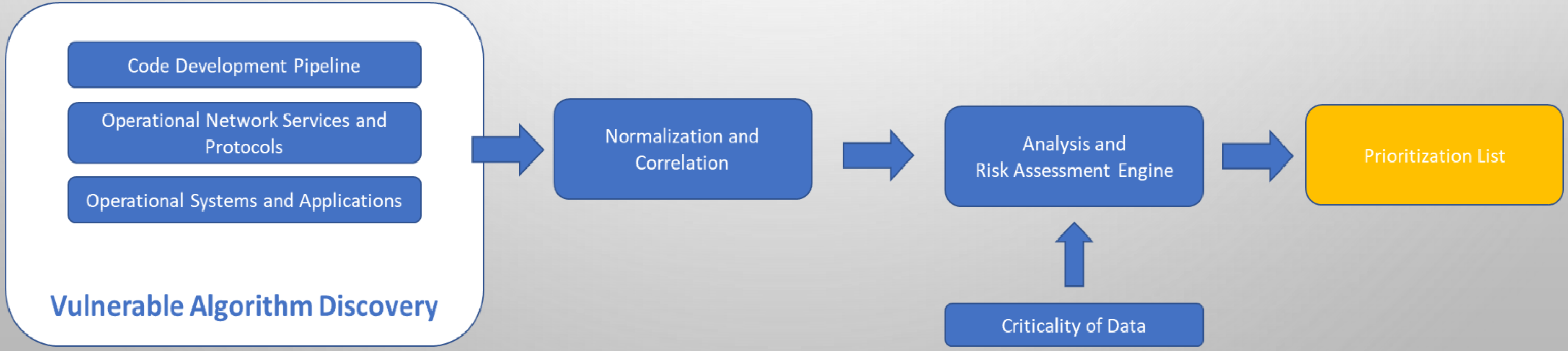
This fact sheets provides a high-level overview of the project. To learn more, visit the project page: https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

### 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.

# MIGRATION TO POST-QUANTUM CRYPTOGRAPHY DISCOVERY WORKSTREAM

- Exploring the use of discovery tools to detect and report the presence and use of quantum vulnerable cryptography in systems and services, and the use of output from the tools to inform risk analysis for prioritizing actions to move away from quantum-vulnerable cryptography.



# TABLE OF CONTENTS

# MIGRATION TO POST-QUANTUM CRYPTOGRAPHY INTEROPERABILITY & PERFORMANCE

- Identifying interoperability and performance challenges that applied cryptographers face as they implement quantum-resistant algorithms.
  - QUIC, Transport Layer Security (TLS)
  - Secure Shell (SSH)
  - X.509 post-quantum certificate hybrid profiles to support traditional and post-quantum algorithms
  - post-quantum-related operations of next-generation Hardware Security Modules (HSMs).

# INTEROPERABILITY AND PERFORMANCE WORKSTREAM WORKSTREAM

- **INTEROPERABILITY**
  - DEMONSTRATE INTEROPERABILITY BETWEEN COLLABORATORS' SOFTWARE AND HARDWARE COMPONENTS IMPLEMENTING THE SAME ALGORITHM OR STANDARD
  - DEVELOP AND DEMONSTRATE KNOWN ANSWER TESTS (KATS) AND TEST VECTORS FOR THE NIST STANDARDIZED ALGORITHMS
- **PERFORMANCE**
  - IDENTIFY METRICS TO MEASURE (TIME, MEMORY, ETC.)
  - VARY THE DEMONSTRATION CONDITIONS (OPERATIONAL ENVIRONMENT SUCH AS ON-PREM, CLOUDS, DEVICES, VIRTUAL MACHINES, CONTAINERS, ETC.)
  - VARY THE DEMONSTRATION CRYPTO MODES SUCH AS PQC-ONLY AND HYBRID
- **WORK IN PROGRESS**
  - DRAFT PUBLICATION SHOWING INTEROP AND PERFORMANCE DEMONSTRATION PLANS FOR TLS, SSH, HSM, AND X.509 CERTIFICATE FORMAT (COORDINATION WITH IETF HACKATHON PQC CERTIFICATES)
  - DOCUMENT ISSUES AND GAPS TO REPORT BACK TO THE DEVELOPERS' STANDARDS AND PROTOCOLS TO RESOLVE THE PROBLEMS.

NIST SP 1800-38 VOLUME C
MIGRATION TO PQC

*QUANTUM RESISTANT CRYPTOGRAPHY TECHNOLOGY INTEROPERABILITY AND PERFORMANCE REPORT*

# TABLE OF CONTENTS

# REFERENCES

- **PROJECT WEBSITE**
  - HTTPS://WWW.NCCOE.NIST.GOV/CRYPTO-AGILITY-CONSIDERATIONS-MIGRATING-POST-QUANTUM-CRYPTOGRAPHIC-ALGORITHMS
- **PROJECT COMMUNITY OF INTEREST (COI)**
  - REQUEST TO JOIN EMAIL: APPLIED-CRYPTO-PQC@NIST.GOV
- **CONTACT THE PQC PROJECT TEAM**
  - APPLIED-CRYPTO-PQC@NIST.GOV
- **BILL NEWHOUSE**
  - WILLIAM.NEWHOUSE@NIST.GOV

Post-Quantum

Cryptography Conference

PKI Consortium