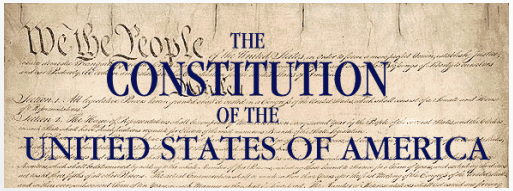
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

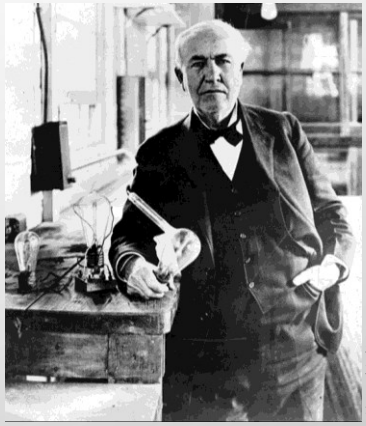
- Non-regulatory federal agency within U.S. Department of Commerce.
- Founded in 1901, known as the National Bureau of Standards (NBS) prior to 1988.
  - Origins in the Constitution: "Congress shall have power to …. fix the standard of weights and measures…"
- Headquarters in Gaithersburg, Maryland, and laboratories in Boulder, Colorado.
- Employs around 6,000 employees and associates.
- At least 5 Nobel prizes

THE IMPORTANCE OF STANDARDS



Article I, Section 8: The Congress shall have the power to…*fix the standard of weights and measures*

- NATIONAL BUREAU OF STANDARDS ESTABLISHED BY CONGRESS IN 1901
- EIGHT DIFFERENT "AUTHORITATIVE" VALUES FOR THE GALLON
- ELECTRICAL INDUSTRY NEEDED STANDARDS
- AMERICAN INSTRUMENTS SENT ABROAD FOR CALIBRATION
- CONSUMER PRODUCTS AND CONSTRUCTION MATERIALS UNEVEN IN QUALITY AND UNRELIABLE



National Archives

Estimated that 80% of global merchandise trade is influenced by testing and other measurement-related requirements of regulations and standards

NIST has…

…four joint institutes

JILA

NIST + University of Colorado

Institute for Bioscience and Biotechnology Research

NIST + University of Maryland College Park + The University of Maryland Baltimore

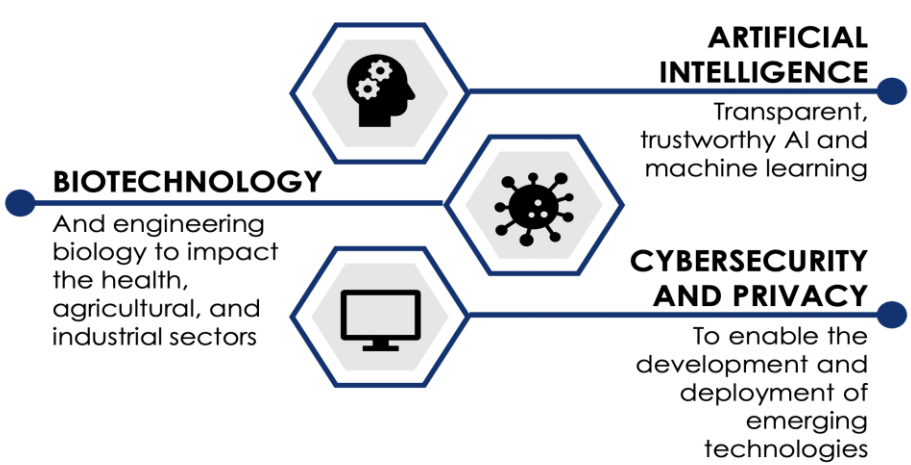
Joint Quantum Institute

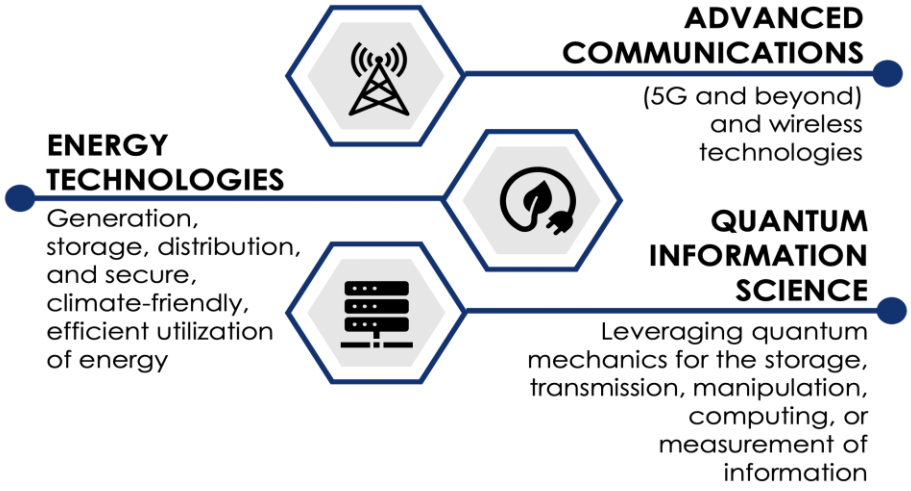
NIST + University of Maryland + NSA

Hollings Marine Laboratory

NIST + NOAA + South Carolina + College of Charleston + Medical University of South Carolina

NIST WIDE R&D FOCUS AREAS





HOW WE WORK ON THESE PROBLEMS

Transparent

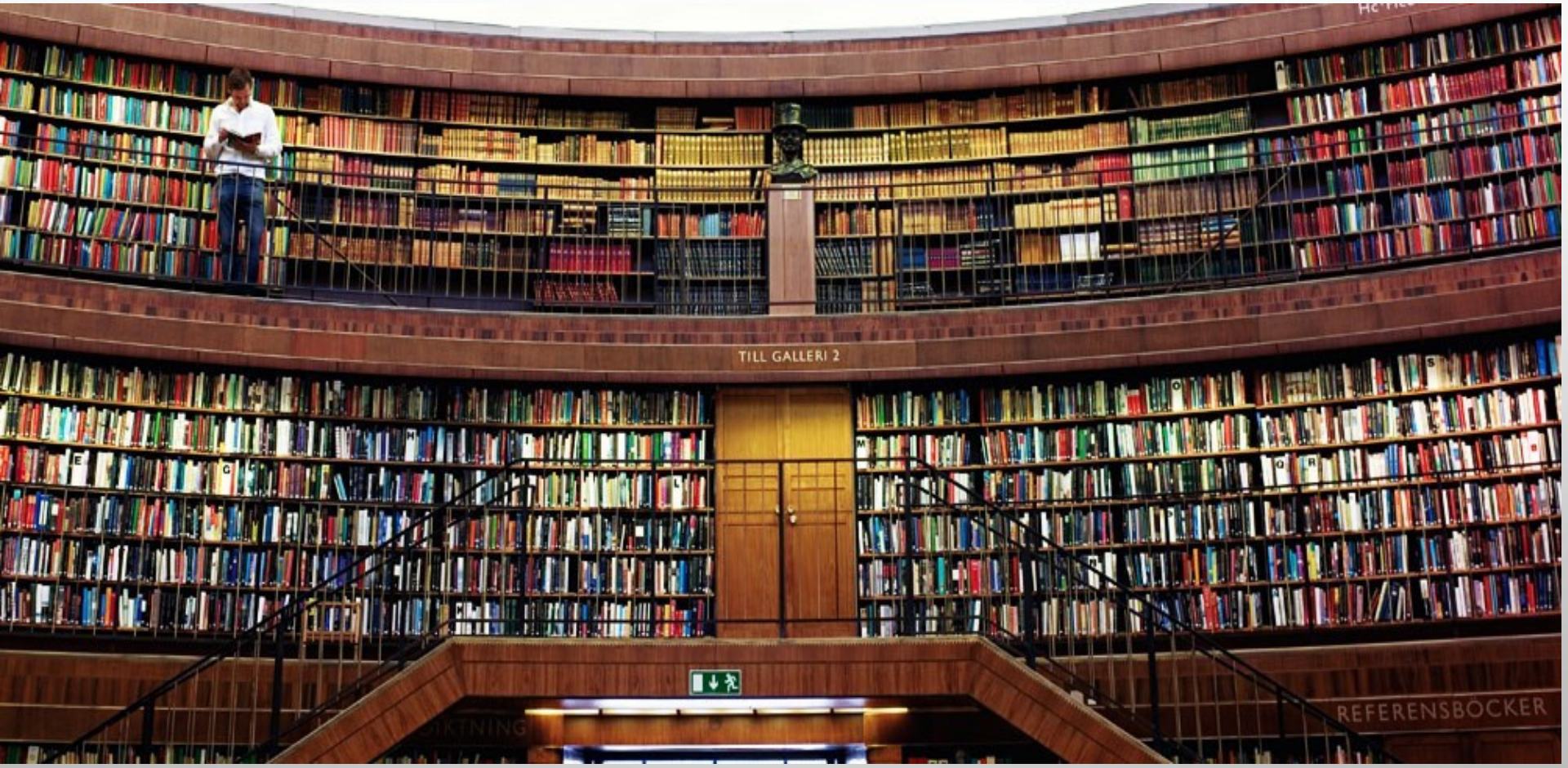
Traceable

Open

Inclusive

Cultivating Trust in IT and Metrology

Documents, Documents, Documents, also Data

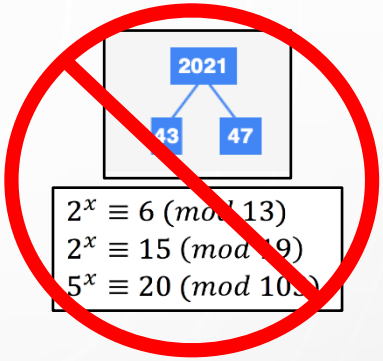


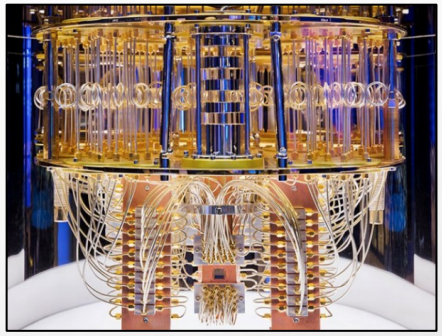
THE QUANTUM THREAT

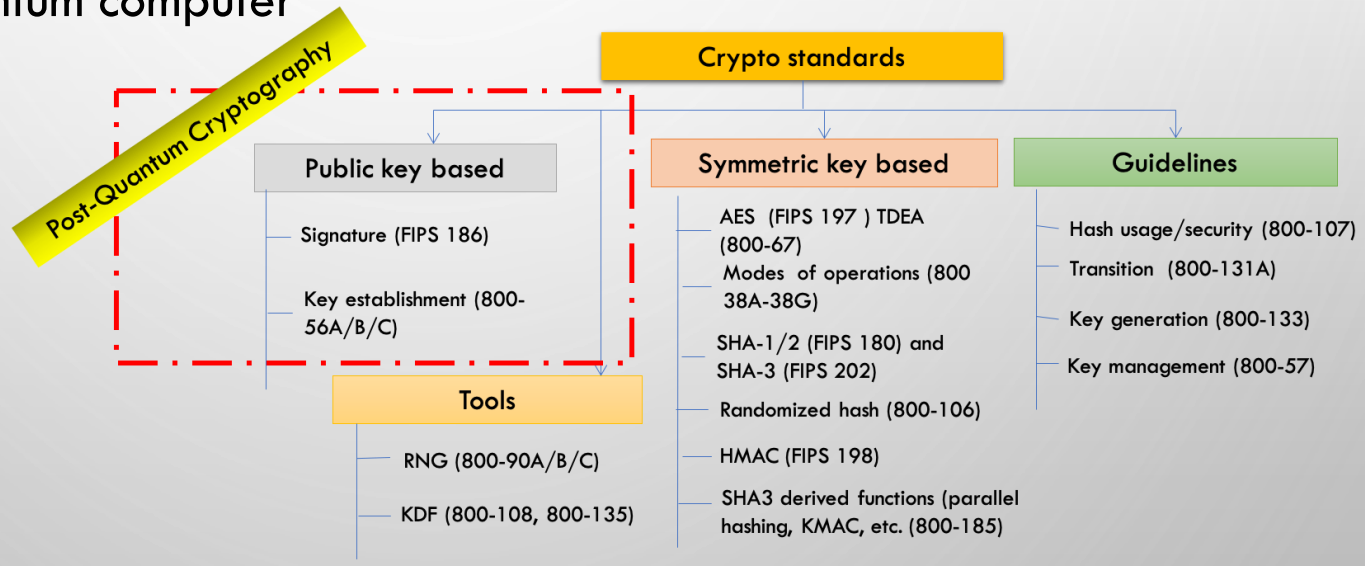
- NIST public-key crypto standards
  - **SP 800-56A**: Diffie-Hellman, ECDH
  - **SP 800-56B**: RSA encryption
  - **FIPS 186**: RSA, DSA, and ECDSA signatures

all vulnerable to attacks from

a (large-scale) quantum computer







- Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically

THE PQC "COMPETITION"

- 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 AN OPEN, 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…

SUBMISSIONS

37 PRELIMINARY SUBMISSIONS (EARLY DEADLINE SEP 2017)

82 TOTAL SUBMISSIONS RECEIVED

69 ACCEPTED AS "COMPLETE AND PROPER" (5 SINCE WITHDRAWN)

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

25 COUNTRIES, 16 STATES, 6 CONTINENTS

THE FIRST THREE ROUNDS

ROUND 1 (DEC '17 – JAN '18)

- 69 CANDIDATES AND 278 DISTINCT SUBMITTERS
- SUBMITTERS FROM >25 COUNTRIES, 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-v			
Symme			
Other			
Total			

	Signatures	KEMs/Encryption	Total
Lattice-based	3	9	12
Code-based	0	7	7
Multi-variate	4	0	4
Symm			
Other			
Total			

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	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 (JUL '20 – JUL '22)

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

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

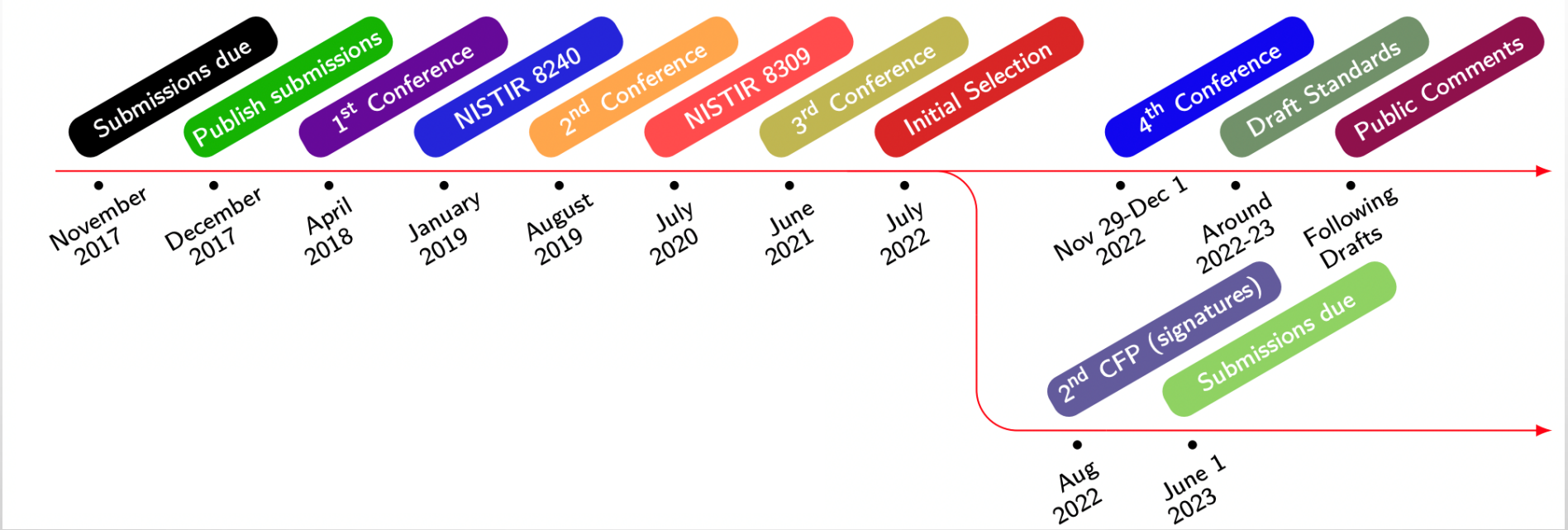
4th round candidates (all KEMs) evaluated for 18-24 months

- ClassicMcEliece
- BIKE
- HQC
- ~~SIKE~~

On-ramp signatures

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

TIMELINE



- Draft standards for public comment were posted in July 2023
- **The first 3 PQC standards should be published in 2024**

THE KEMS IN THE 4TH 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 4th 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

- NIST issued a new Call for Signatures
  - Deadline for submission: June 1, 2023
  - This will be much smaller in scope than main NIST PQC effort
  - The main reason for this call is to diversify our signature portfolio
  - These signatures will be on a different track than the candidates in the 4th round
- We are **most interested** in a general-purpose digital signature scheme which is not based on structured lattices
  - We may be interested in other signature schemes targeted for certain applications. For example, a scheme with very short signatures.
- The more mature the scheme, the better.
- NIST will decide which (if any) of the received schemes to focus attention on

No on-ramp for KEMs currently planned.

STANDARDIZATION

- THE PQC STANDARDS WILL BE FIPS
  - EACH ALGORITHM WILL BE ITS OWN DOCUMENT
  - MIGHT HAVE SOME SP'S WHICH CONTAIN MORE TECHNICAL DETAILS
  - ALL THE ALGORITHMS WILL BE GIVEN A STANDARDIZED NAME
    - SOMETHING LIKE MLWE-KEM (KYBER), MLWE-SIG (DILITHIUM), NSIS-SIG (FALCON) AND SHBS-SIG (SPHINCS+)
- SOME CHOICES NEED TO BE MADE
  - WHICH PARAMETER SETS TO INCLUDE
  - WHICH HASH FUNCTIONS, OTHER SYMMETRIC PRIMITIVES, ETC?
  - HOW TO ALLOW FOR ANY POTENTIAL CHANGES FROM THE ROUND 3 SPECIFICATIONS?
    - SUBMISSION TEAMS MAY SUBMIT SUGGESTED CHANGES
    - ANY CHANGES BY NIST (OR SUGGESTED BY TEAMS) WILL BE DISCUSSED PUBLICLY
- PLEASE PROVIDE FEEDBACK
  - PQC-FORUM, EMAIL ETC

STANDARDIZATION

CRYSTALS - KYBER

- SELECTED FOR ITS STRONG SECURITY AND PERFORMANCE
- WE ARE PLANNING TO STANDARDIZE BOTH KYBER-768 AND KYBER-1024
- WHAT ABOUT KYBER-512?
  - THE SECURITY MARGIN FOR KYBER-512 IS CLOSE IN THE GATE METRIC
  - NIST IS CURRENTLY LEANING IN THE DIRECTION OF INCLUDING KYBER-512 IN THE STANDARD
- NIST IS NOT PLANNING ON STANDARDIZING THE 90'S VERSION OF KYBER

STANDARDIZATION

CRYSTALS - KYBER

- WE ARE STILL LEANING TOWARDS INCLUDE KYBER-512
  - THE RECOMMENDED DEFAULT OPTION WOULD BE KYBER-768

- SOME TOPICS DISCUSSED ON PQC-FORUM
  - LEAVE DOMAIN SEPARATION AS WAS SPECIFIED IN THE ROUND 3 SPEC (USE FIPS 202 FUNCTIONS WITH INTERNAL DOMAIN SEPARATION)
  - NIST NOTED THAT IT WILL **NOT** BE USING TURBOSHAKE
  - STILL TO BE DECIDED: SHOULD THE FO TRANSFORM BE SLIGHTLY TWEAKED FOR ADDITIONAL SECURITY PROPERTIES?

IP UPDATE

- THE LICENSE AGREEMENTS MENTIONED IN NISTIR 8413 HAVE BEEN SIGNED BY ALL PARTIES
  - NIST APPRECIATES THE EFFORTS OF THOSE WHO HELPED OBTAIN THIS OUTCOME AND THE COOPERATION OF THIRD PARTIES
- THE (RELEVANT) TEXT OF THE LICENSE IS AVAILABLE ON OUR WEBSITE
- **SUMMARY:** THE LICENSE ALLOWS FOR ROYALTY-FREE USE (FROM THE THIRD PARTIES LISTED ABOVE) OF IMPLEMENTATIONS WHICH FOLLOW THE NIST STANDARD
  - *DISCLAIMER: I'M NOT A LAWYER. SEE THE LICENSE TEXT FOR DETAILS*

STANDARDIZATION

CRYSTALS – DILITHIUM

- SELECTED BASED ON ITS SECURITY, HIGH EFFICIENCY, AND RELATIVELY SIMPLE IMPLEMENTATION
- WE RECOMMEND IT BE THE PRIMARY SIGNATURE ALGORITHM USED
- WE WILL STANDARDIZE THE PARAMETER SETS FOR DILITHIUM CORRESPONDING TO SECURITY CATEGORIES 2, 3, AND 5
- PRE-HASH VERSION ALLOWED, BUT NOT THE DEFAULT
- ALLOWING FOR A RANDOMIZED VERSION OF DILITHIUM
- (WE'RE NOT CONSIDERING THE AES VARIANT)

STANDARDIZATION

- SELECTED FOR ITS SMALL BANDWIDTH, FAST VERIFICATION AND SECURITY
- THE IMPLEMENTATION MAY BE COMPLICATED FOR SOME APPLICATIONS

- WE ARE PLANNING TO STANDARDIZE THE PARAMETER SETS FOR FALCON CORRESPONDING TO SECURITY CATEGORIES 1 AND 5

- THE STANDARD WILL COME AFTER THE DILITHIUM STANDARD

STANDARDIZATION

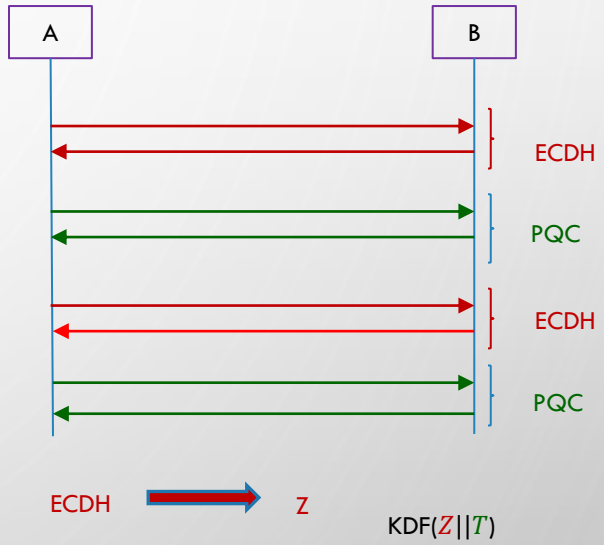
SPHINCS+

- SELECTED FOR ITS SOLID SECURITY
- BASED ON A DIFFERENT SET OF ASSUMPTIONS FROM LATTICES

- THERE ARE MANY PARAMETER SETS INCLUDED IN THE SUBMISSION
  - WE WILL INCLUDE PARAMETER SETS FOR SECURITY CATEGORIES 1, 3, AND 5
  - NIST IS PLANNING ON CONSIDERING THE SIMPLE VERSION (NOT THE ROBUST VERSION)
  - NIST PLANS TO INCLUDE BOTH THE FAST AND SMALL VERSIONS
  - ALLOWED HASH FUNCTIONS: SHAKE AND SHA-2
    - BY SHA-2 WE MEAN SHA-256 FOR CATEGORY 1 AND A MIX OF SHA-512 AND SHA-256 FOR CATEGORIES 3 AND 5

TRANSITION AND MIGRATION

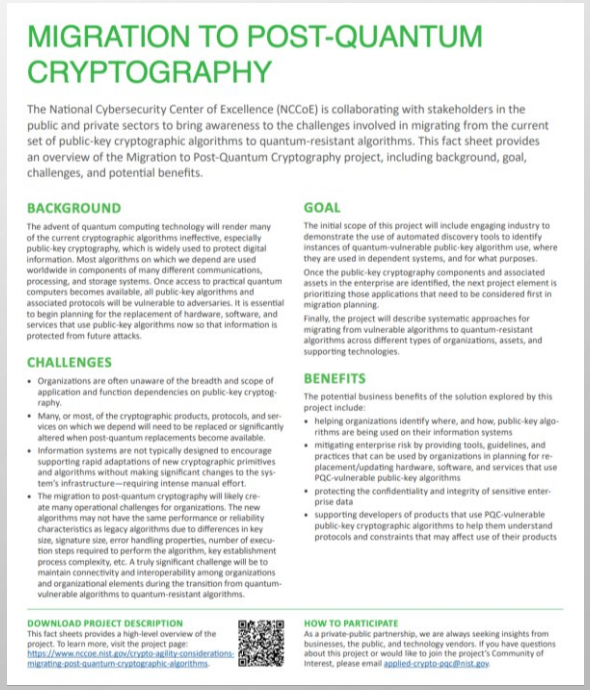
- THERE HAS BEEN MUCH DISCUSSION ON HYBRID/COMPOSITE MODES
  - NIST SP800-56C REV. 2 ALLOWS FOR A CERTAIN HYBRID MODE
  - WE WILL WORK WITH THE COMMUNITY IN DIFFERENT STAGES OF MIGRATION TO ASSURE SECURITY
- NIST WILL PROVIDE TRANSITION GUIDELINES TO PQC STANDARDS
  - NIST HAS PROVIDED SUCH GUIDANCE BEFORE
    - EXAMPLES: TRIPLE DES, SHA-1, KEYS < 112 BITS
  - TIME FRAME 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
- OUTREACH AND ENGAGEMENT
  - COMMUNITY OF INTEREST, WEBINARS, PUBLIC EVENTS
  - 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

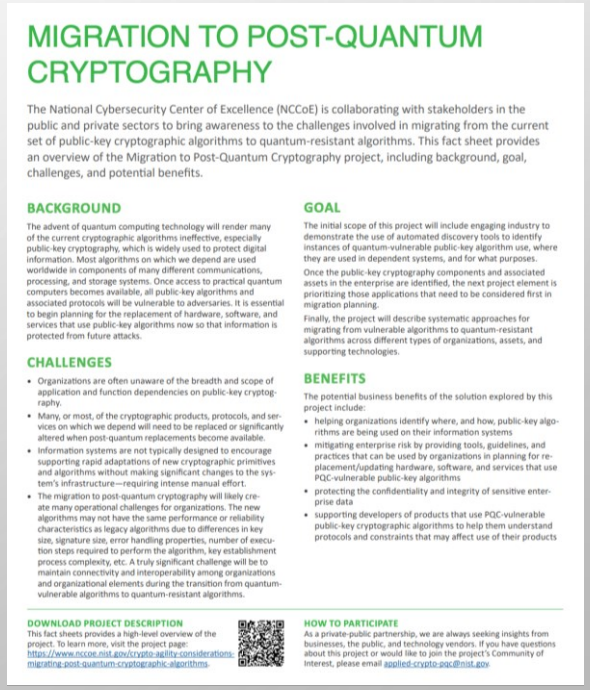
HOW TO PARTICIPATE

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.

THE NCCOE MIGRATION TO PQC PROJECT

- DISCOVERY WORKSTREAM
  - DEFINE COMMON DATA ELEMENTS FOR PQC
  - BUILD THE NCCOE LAB ENVIRONMENT WITH CLASSICAL AND PQC SYSTEMS AND APPLICATIONS
  - START DEPLOYMENT OF THE COLLABORATORS' CONTRIBUTED DISCOVERY TOOLS AND COLLECT THE ASSESSMENT REPORTS
- INTEROPERABILITY AND PERFORMANCE WORKSTREAM
  - DEMONSTRATE INTEROPERABILITY BETWEEN COLLABORATORS' SOFTWARE AND HARDWARE COMPONENTS
  - DEVELOP KNOWN ANSWER TESTS (KATS) AND TEST VECTORS
  - IDENTIFY METRICS TO MEASURE (TIME, MEMORY, ETC.)
  - VARY DEMONSTRATION CONDITIONS AND CRYPTO MODES
  - DEVELOP INTEROP AND PERFORMANCE DEMONSTRATION PLAN FOR TLS, SSH, HSM, AND X.509 CERTIFICATE FORMAT
  - DOCUMENT ISSUES AND GAPS TO REPORT BACK TO THE DEVELOPERS' STANDARDS AND PROTOCOLS

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

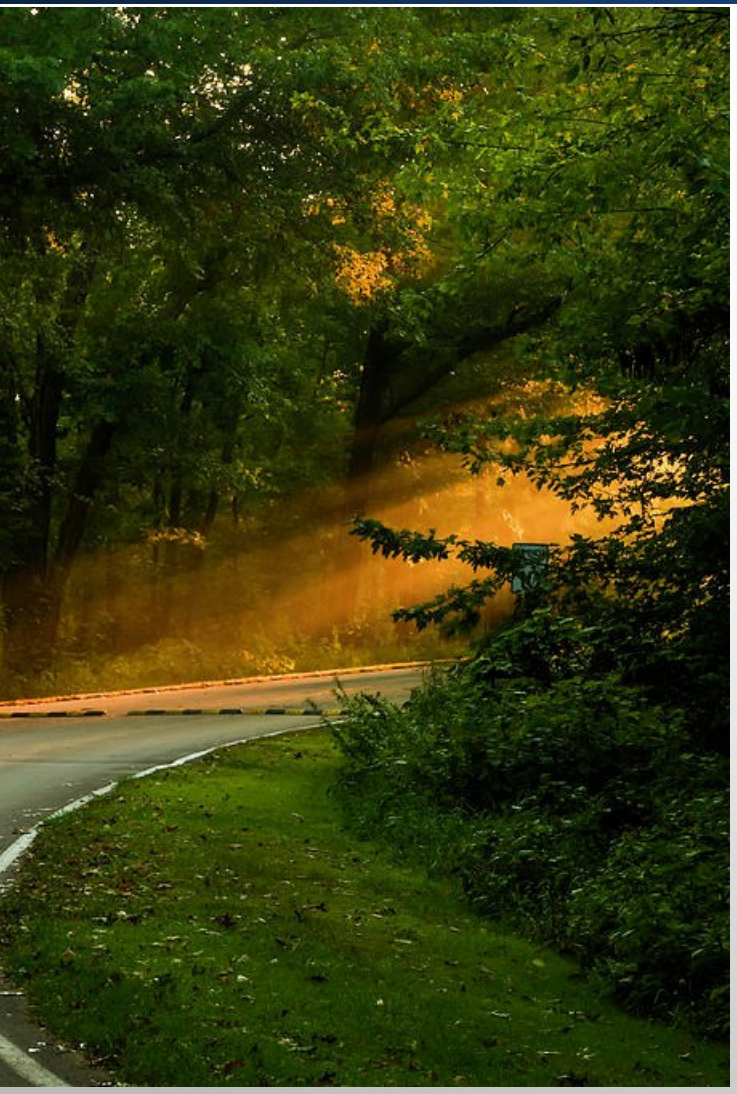
DOWNLOAD PROJECT DESCRIPTION

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.

CONCLUSION



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

- NIST IS GRATEFUL FOR EVERYBODY'S EFFORTS

- *PLEASE PROVIDE US WITH FEEDBACK!*

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