# THE NIST PQC STANDARDS: LIGHT AT THE END OF THE TUNNEL

Dustin Moody
Computer Security Division
NIST

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

# NIST CRYPTOGRAPHIC STANDARDS

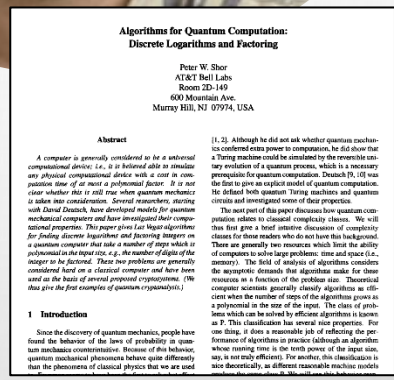
- NIST DEVELOPED THE FIRST ENCRYPTION STANDARDS IN 1970S
  - DATA ENCRYPTION STANDARD (DES), PUBLISHED 1977 AS FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 46

Nearly all commercial laptops, cellphones, Internet routes, VPN servers, and ATMs use NIST Cryptography

- OVER 40 YEARS, NIST CONTINUES TO EVOLVE ITS CRYPTOGRAPHIC STANDARDS
  - ENABLE TO RESPOND THE GROWING APPLICATION DEMAND
  - ENHANCE SECURITY STRENGTH TO AGAINST MORE SOPHISTICATED ATTACKS

# 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 fast 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.)*

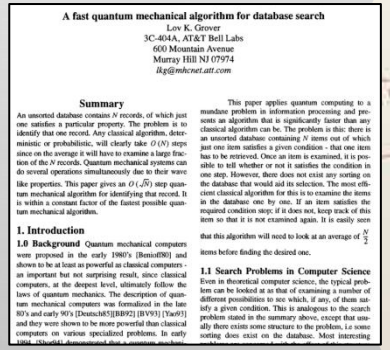
**1 Introduction**

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 in 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 then 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 algorithm 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 really 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-step; 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.

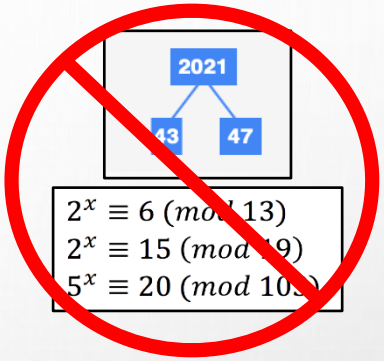
**1.1 Search Problems in Computer Science** Even in theoretical computer science, the typical problem can be looked at as that of examining a number of different possibilities to see which, if any, of them satisfy a given condition. This is analogous to the search problem stated in the summary above,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

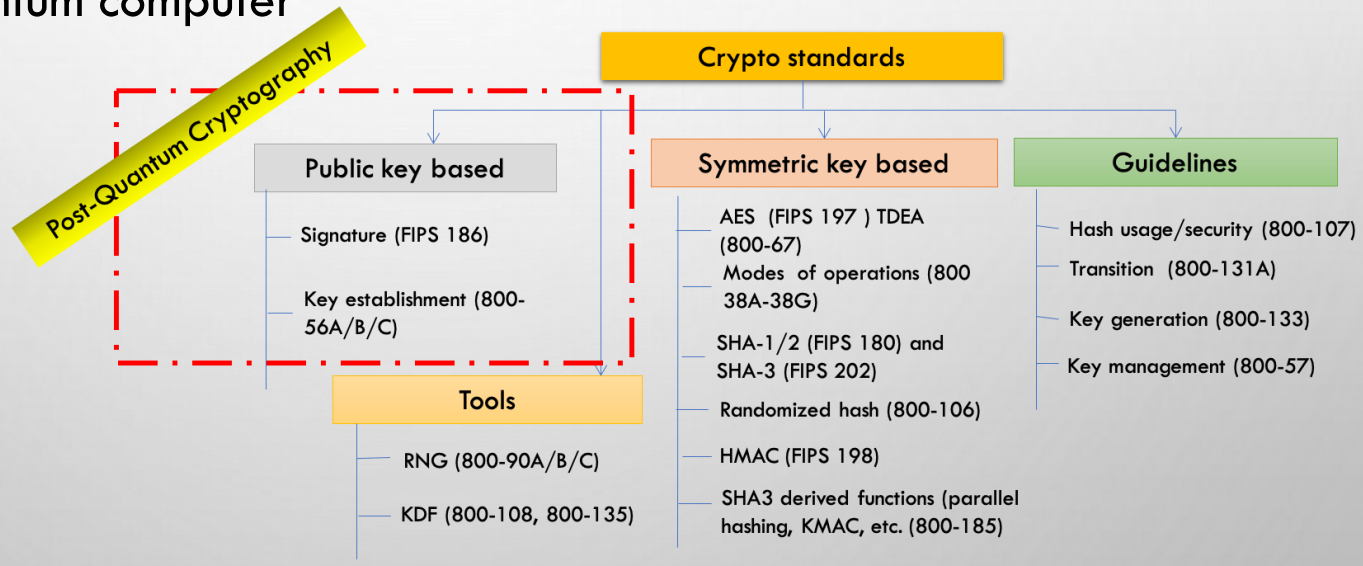
# THE QUANTUM THREAT

- NIST 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

# HOW SOON DO WE NEED TO WORRY?

# HOW SOON SHOULD WE WORRY?

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with
Memorandum 10 (NSM-10), *on Promoting United States Leadership in Q*
*While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022


One Hundred Seventeenth Congress
of the
United States of America

AT THE SECOND SESSION
*Begun and held at the City of Washington on Monday, the third day of January, two thousand and twenty-two*

An Act

Administration

BRIEFING ROOM

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

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

”The United States must prioritize the transition of cryptographic systems to *quantum-resistant cryptography*, with the goal of mitigating as much of the quantum risk as is feasible by 2035.”

# THE OMB 'MIGRATING TO PQC' MEMO

- PRIORITIZE INVENTORY OF CRYPTOGRAPHIC SYSTEMS
  - FOCUS ON HIGH VALUE ASSETS AND HIGH IMPACT SYSTEMS
  - ANNUALLY SUBMIT RESULTS TO ONCD AND CISA UNTIL 2035
    - ONCD/CISA WILL RELEASE TOOLS AND PROCEDURES FOR INVENTORY
  - MORE SPECIFICS PROVIDED…..
- ANNUAL ASSESSMENT OF FUNDING REQUIRED FOR MIGRATION
- AGENCIES SHOULD HAVE ALREADY DESIGNATED A MIGRATION LEAD
  - OMB WILL COORDINATE GOVERNMENT-WIDE RESPONSE
- TESTING PRE-STANDARDIZED PQC ALGORITHMS ENCOURAGED
- NIST WILL CREATE A WORKING GROUP TO DEVELOP BEST PRACTICES

"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."

# CNSA - COMMERCIAL NATIONAL SECURITY ALGORITHM SUITE 2.0

- IN SEPT 2022, NSA ANNOUNCED CNSA 2.0 ADVISORY TO PREPARE NATIONAL SECURITY SYSTEMS FOR THE TRANSITION TO PQC

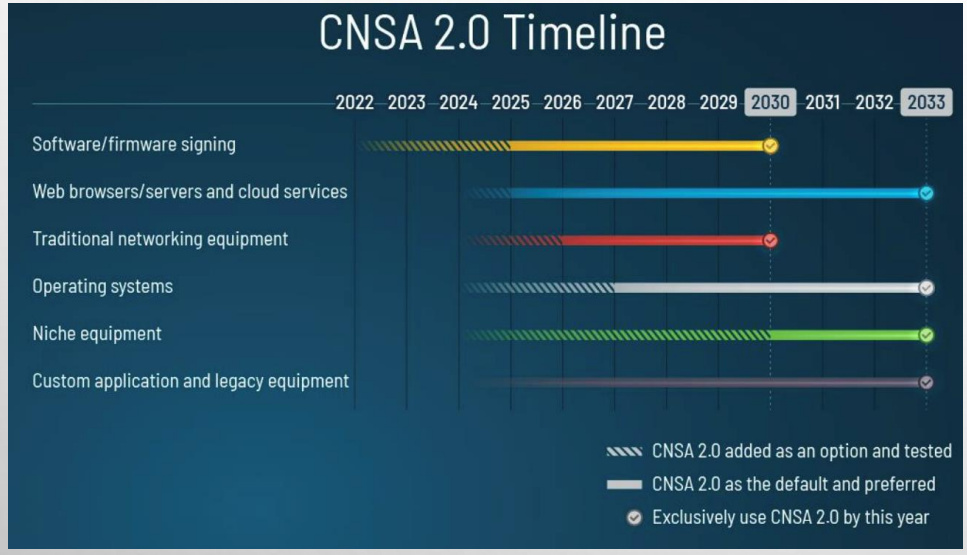



*Table IV: CNSA 2.0 algorithms*

| Algorithm | Function | Specification | Parameters |
|---|---|---|---|
| Advanced Encryption Standard (AES) | Symmetric block cipher for information protection | FIPS PUB 197 | Use 256-bit keys for all classification levels. |
| CRYSTALS-Kyber | Asymmetric algorithm for key establishment | TBD | Use Level V parameters for all classification levels. |
| CRYSTALS-Dilithium | Asymmetric algorithm for digital signatures | TBD | Use Level V parameters for all classification levels. |
| Secure Hash Algorithm (SHA) | Algorithm for computing a condensed representation of information | FIPS PUB 180-4 | Use SHA-384 or SHA-512 for all classification levels. |
| Leighton-Micali Signature (LMS) | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels. SHA256/192 recommended. |
| Xtended Merkle Signature Scheme (XMSS) | Asymmetric algorithm for digitally signing firmware and software | NIST SP 800-208 | All parameters approved for all classification levels. |

- NSA EXPECTS THE TRANSITION TO QR ALGORITHMS FOR NSS TO BE COMPLETE BY 2035 IN LINE WITH NSM-10.

# 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

## 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

| 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

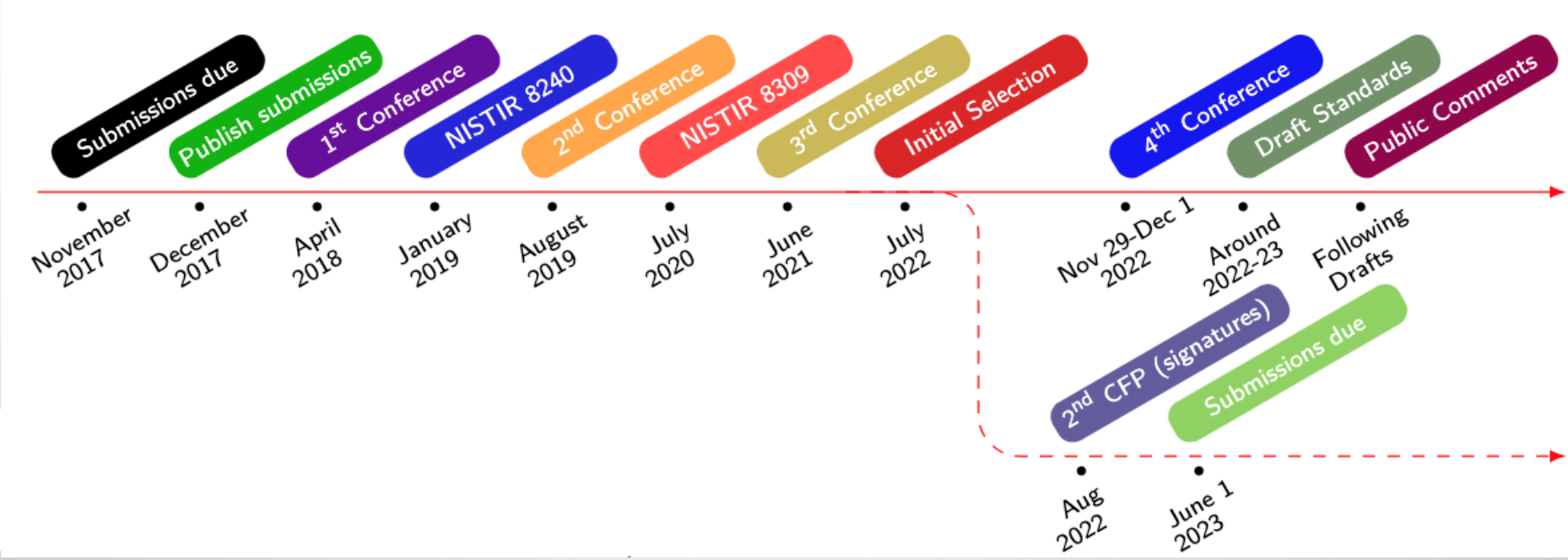
**On-ramp signatures**

- 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 will be in summer 2023
- **The first 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

- 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.
  - Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.

- 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.

# THE ONRAMP NUMBERS

- 50 submissions received by the final deadline
  - There were 23 signatures (and 59 KEMs) submitted in 2017
  - 262 distinct submitters

- 40 submissions accepted as 'complete and proper'
  - From 5 continents and 28 countries

- For complete specs (including code):

  see www.nist.gov/pqcrypto

| Type | Number |
|---|---|
| Lattice | 7 |
| Code-based | 6 |
| Multivariate | 11 |
| MPC in the head | 6 |
| Symmetric | 4 |
| Isogeny | 1 |
| Other | 5 |
| Total | 40 |

# STANDARDIZATION


- THE PQC STANDARDS WILL BE FIPS
  - EACH ALGORITHM WILL BE ITS OWN DOCUMENT
  - WILL HAVE SOME SP'S WHICH CONTAIN MORE GUIDANCE/DETAILS
  - ALL THE ALGORITHMS WILL BE GIVEN A STANDARDIZED NAME
    - ML-KEM (KYBER), ML-DSA (DILITHIUM), NL-DSA (FALCON) AND SLH-DSA (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

# 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))

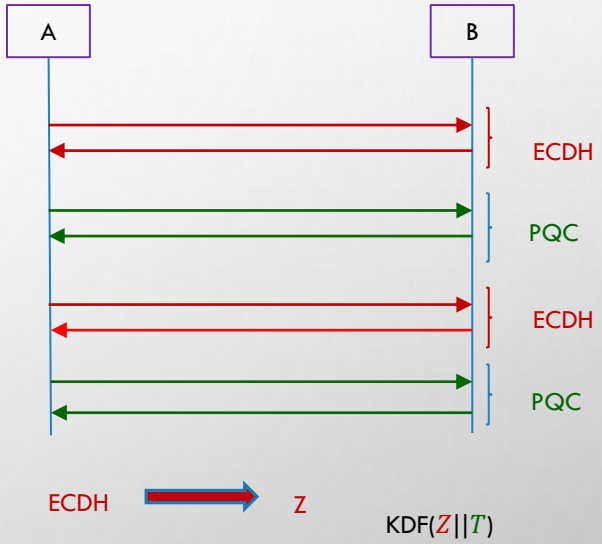
## ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

- 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

# 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



# OTHER STANDARDS ORGANIZATIONS

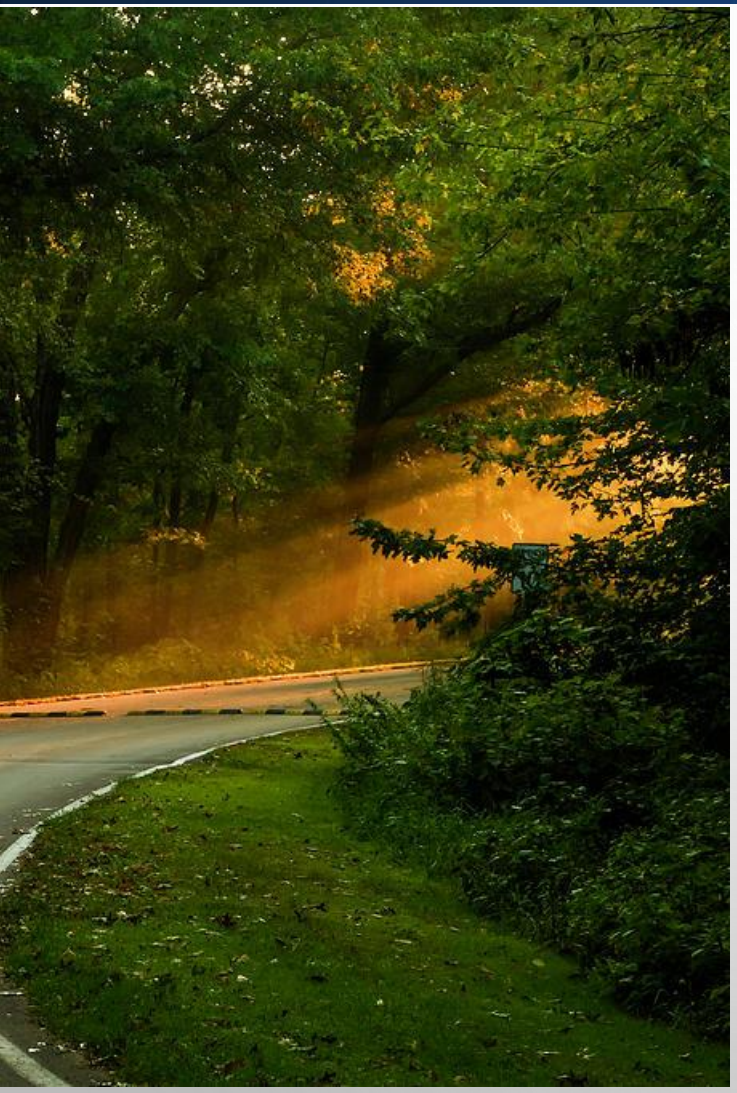
- WE ARE AWARE THAT MANY STANDARDS ORGANIZATIONS AND EXPERT GROUPS ARE WORKING ON PQC
  - ASC X9 HAS DONE STUDIES AND WRITTEN WHITE PAPERS
  - IEEE P1363.3 HAS STANDARDIZED SOME LATTICE-BASED SCHEMES
  - IETF HAS STANDARDIZED STATEFUL HASH-BASED SIGNATURES LMS/XMSS AND IS CURRENTLY DOING NEW WORK GEARED 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 HAD A STUDY PERIOD FOR QUANTUM-RESISTANT CRYPTOGRAPHY AND RELEASED A STANDING DOCUMENT (SD)
- NIST IS INTERACTING AND COLLABORATING WITH THESE ORGANIZATIONS AND GROUPS
- SOME COUNTRIES HAVE BEGUN STANDARDIZATION ACTIVITIES

# WHAT CAN ORGANIZATIONS DO NOW?

- PERFORM A QUANTUM RISK ASSESSMENT WITHIN YOUR ORGANIZATION
  - INVENTORY INFORMATION ASSETS AND THEIR CURRENT CRYPTO PROTECTION
  - IDENTIFY WHAT 'X', 'Y', AND 'Z' MIGHT BE FOR YOU – DETERMINE YOUR QUANTUM RISK
  - PRIORITIZE ACTIVITIES REQUIRED TO MAINTAIN AWARENESS, AND TO MIGRATE TECHNOLOGY TO QUANTUM-SAFE SOLUTIONS
- EVALUATE VENDOR PRODUCTS WITH QUANTUM SAFE FEATURES
  - KNOW WHICH PRODUCTS ARE NOT QUANTUM SAFE
  - ASK VENDORS FOR QUANTUM SAFE FEATURES IN PROCUREMENT TEMPLATES
- DEVELOP AN INTERNAL KNOWLEDGE BASE AMONGST IT STAFF
- TRACK DEVELOPMENTS IN QUANTUM COMPUTING AND QUANTUM SAFE SOLUTIONS
- 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

# CONCLUSION



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

- NIST IS GRATEFUL FOR 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