THE FIRST NIST PQC STANDARDS:
AN UPDATE

Dustin Moody

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

The National Institute of Standards and Technology

- 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.
- 5 Nobel prizes

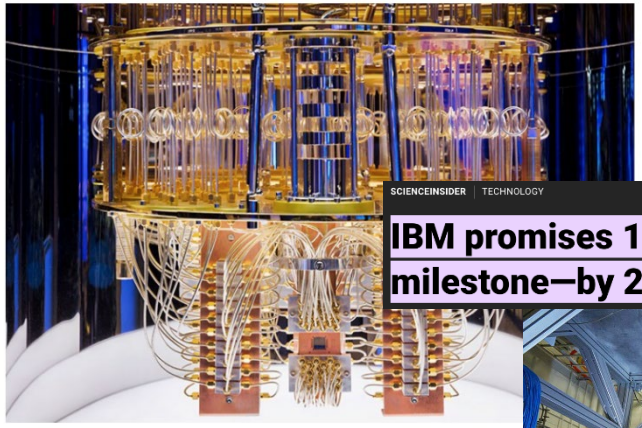
PROGRESS OF QUANTUM COMPUTING

NIST

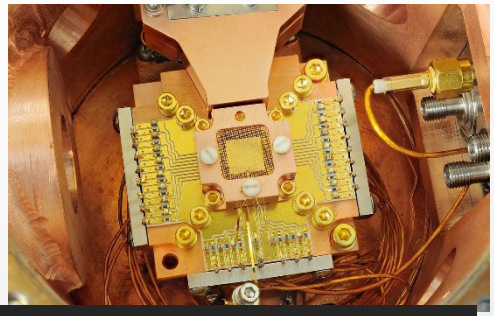
First quantum computer to pack 100 qubits enters crowded race

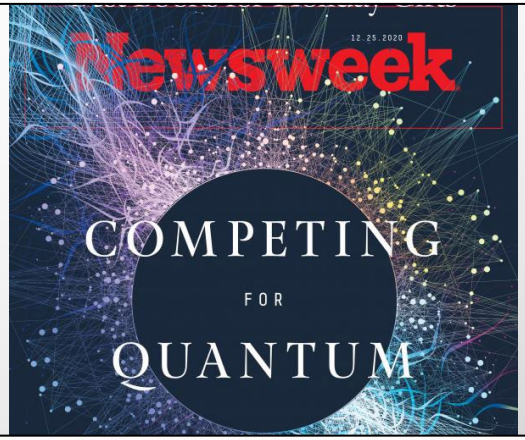
But IBM's latest quantum chip and its competitors face a long path towards making the machines useful.

Philip Ball



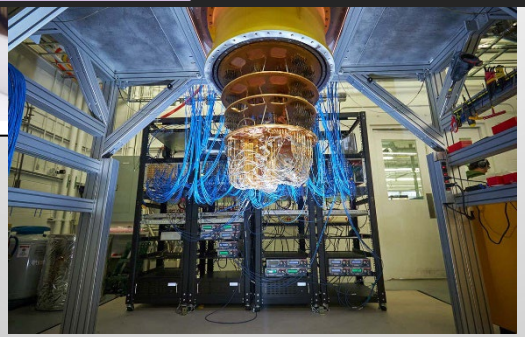
Quantum computers may be able to break Bitcoin sooner than you think





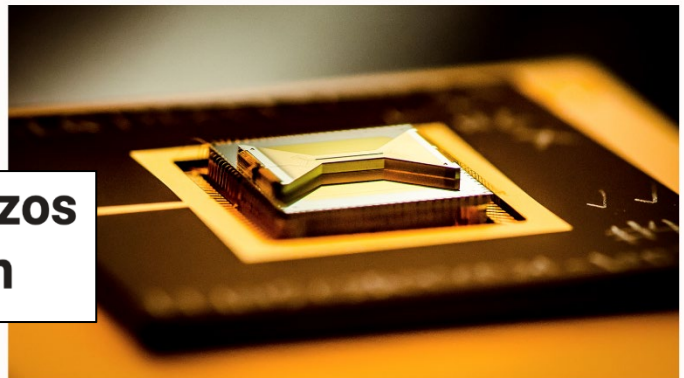
SCIENCEINSIDER | TECHNOLOGY

IBM promises 1000-qubit quantum computer—a milestone—by 2023



Scientists are one step closer to error-correcting quantum computers

Multiple quantum bits were combined into one 'logical qubit' to detect mistakes



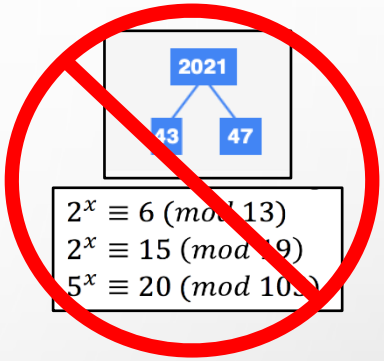
Quantum computing venture backed by Jeff Bezos will leap into public trading with $1.2B valuation

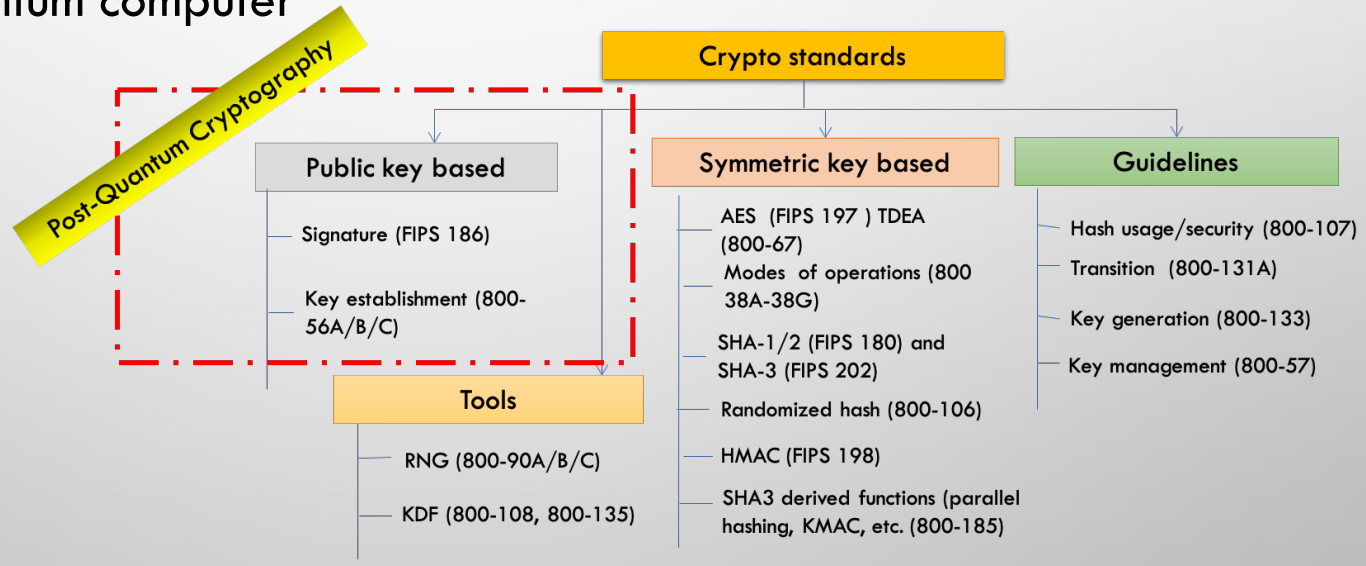
THE QUANTUM THREAT

- 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



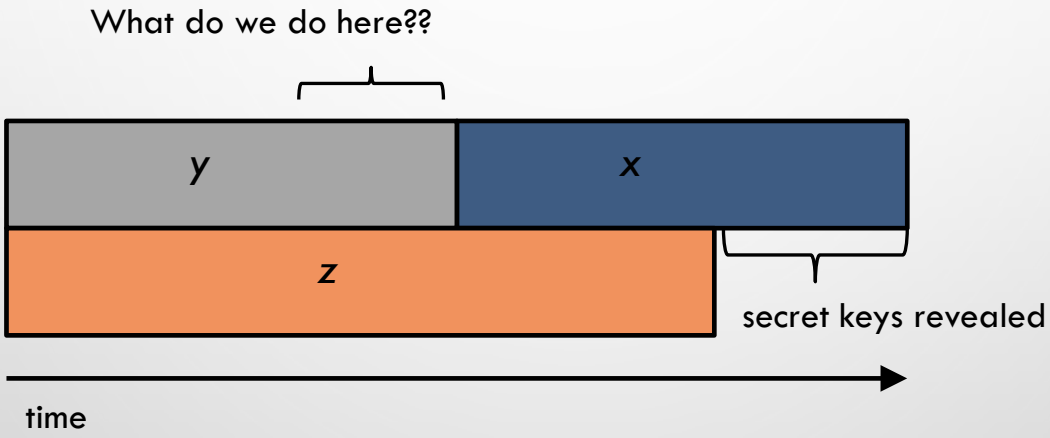


- Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically

HOW SOON DO WE NEED TO WORRY?

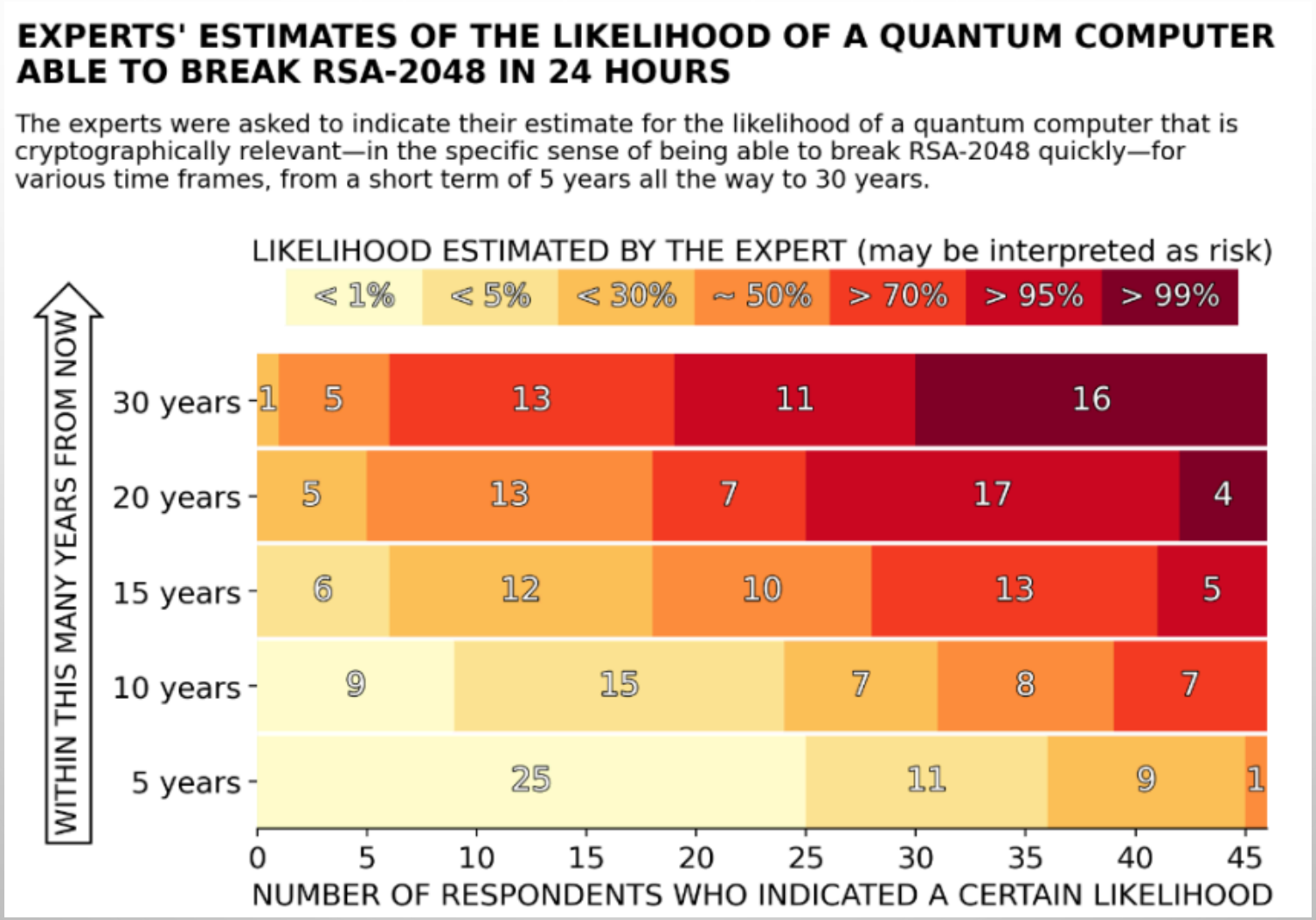
HOW SOON DO WE NEED TO WORRY?

Theorem (Mosca): If $x + y > z$, then problem ("*Harvest now, decrypt later*")



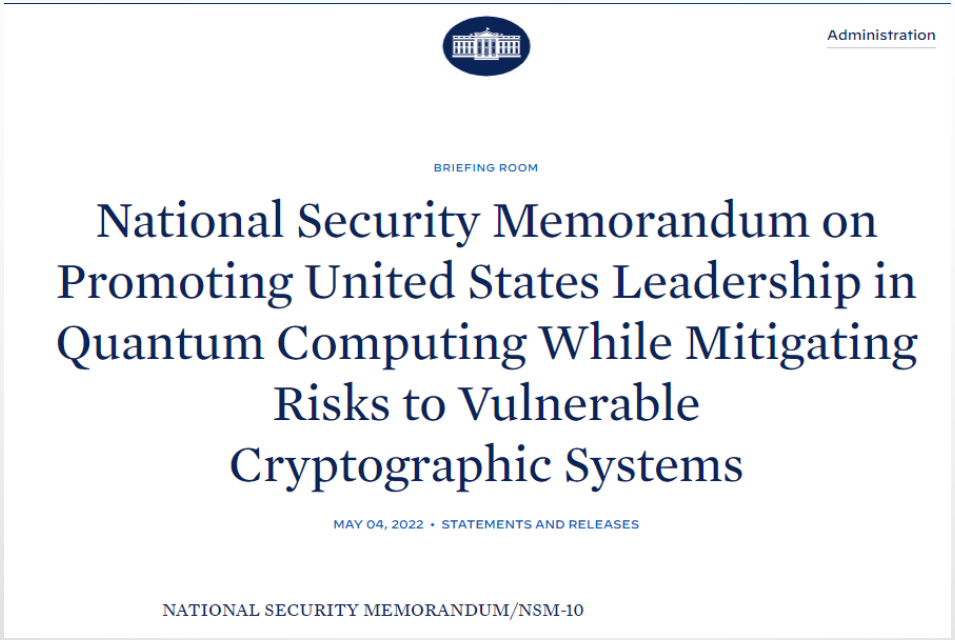
x – how long data needs to be safe
y – time for standardization and adoption
z – time until quantum computers

WHEN WILL A QUANTUM COMPUTER BE BUILT?



Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2021
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report//

U.S. WHITE HOUSE NATIONAL SECURITY MEMO



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

"WITHIN 1 YEAR OF THE RELEASE OF THE FIRST SET OF NIST STANDARDS FOR QUANTUM-RESISTANT CRYPTOGRAPHY …, THE DIRECTOR OF OMB … SHALL ISSUE A POLICY MEMORANDUM REQUIRING FCEB AGENCIES TO DEVELOP A PLAN TO UPGRADE THEIR NON-NSS IT SYSTEMS TO QUANTUM-RESISTANT CRYPTOGRAPHY."

NIST PQC MILESTONES AND TIMELINES

2010-2015
NIST PQC project team builds

First PQC conference

2016

Determined criteria and requirements, published NISTIR 8105

Announced call for proposals

2017

Received 82 submissions

Announced 69 1st round candidates

2018

Held the 1st NIST PQC standardization Conference

2019

Announced 26 2nd round candidates, NISTIR 8240

Held the 2nd NIST PQC Standardization Conference

2020

Announced 3rd round 7 finalists and 8 alternate candidates. NISTIR 8309

2021

Hold the 3rd NIST PQC Standardization Conference

2022 Make 3rd round selection NISTIR 8413, and draft standards

2023 Release draft standards and call for public comments

PAST COMPETITIONS

BLOCK CIPHER

AES – 15 CANDIDATES, 2 ROUNDS, 5 FINALISTS, 3 YEARS + 1 YEAR FOR STANDARD

HASH FUNCTION

SHA-3 – 64 SUBMISSIONS, 51 ACCEPTED, 3 ROUNDS, 14 2ND ROUND CANDIDATES, 5 FINALISTS, 5 YEARS + 3 YEARS FOR STANDARD

POST-QUANTUM CRYPTOGRAPHY

NO NAME? – 82 SUBMISSIONS, 69 ACCEPTED, 3-4 ROUNDS, 26 2ND ROUND CANDIDATES, 15 3RD ROUND FINALISTS/ALTERNATES, 2017-2022 + 2? YEARS FOR STANDARD

LIGHTWEIGHT CRYPTO

57 SUBMISSIONS, 3 ROUNDS, 32 2ND ROUND CANDIDATES, 10 FINALISTS, 2019-2022ISH

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**

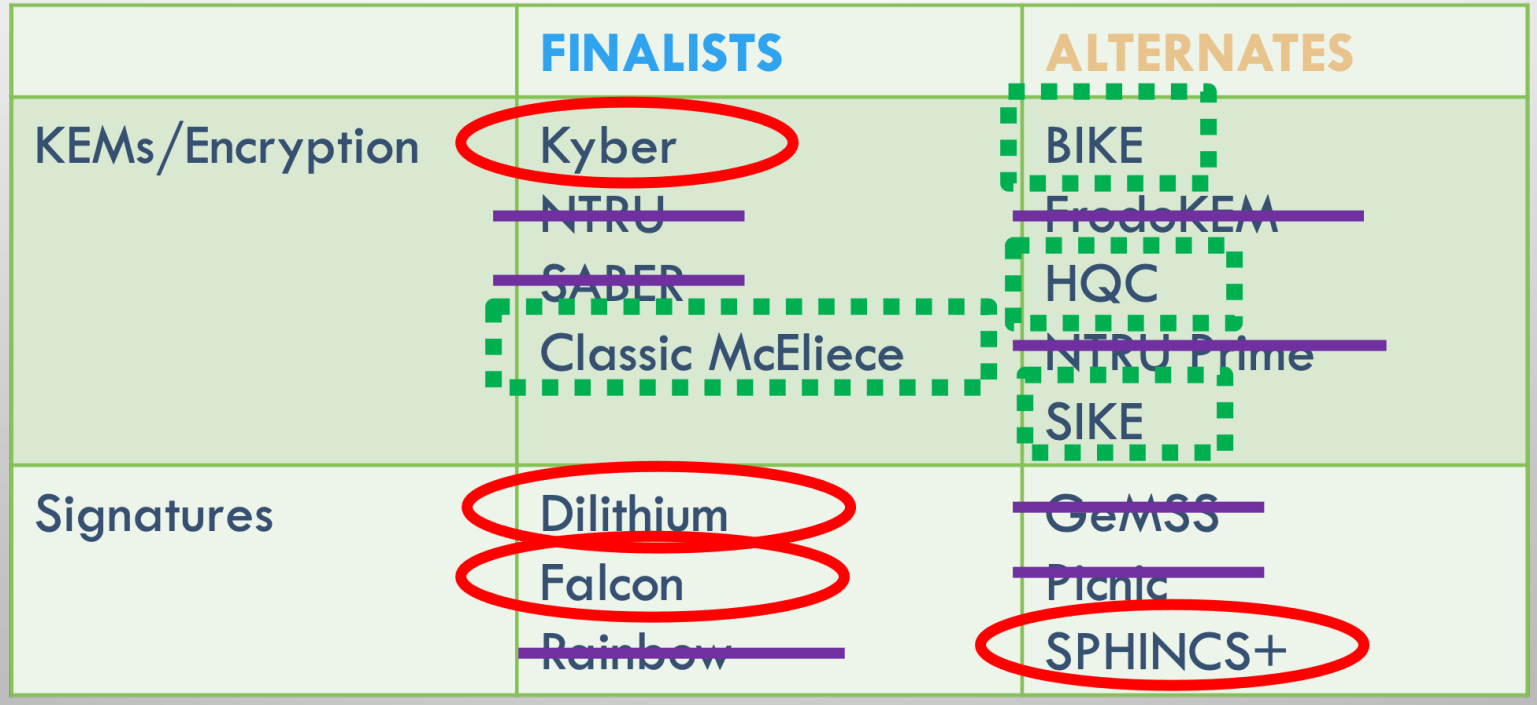
THE ROUND 3 CANDIDATES

- NIST SELECTED 7 **FINALISTS** AND 8 **ALTERNATES**
  - **FINALISTS**: MOST PROMISING ALGORITHMS WE EXPECT TO BE READY AT END OF 3RD ROUND
  - **ALTERNATES**: CANDIDATES FOR POTENTIAL STANDARDIZATION, MOST LIKELY AFTER ANOTHER (4TH) ROUND

	FINALISTS	ALTERNATES
KEMs/Encryption	Kyber NTRU SABER Classic McEliece	BIKE FrodoKEM HQC NTRU Prime SIKE
Signatures	Dilithium Falcon Rainbow	GeMSS Picnic SPHINCS+

WHAT WE PICKED

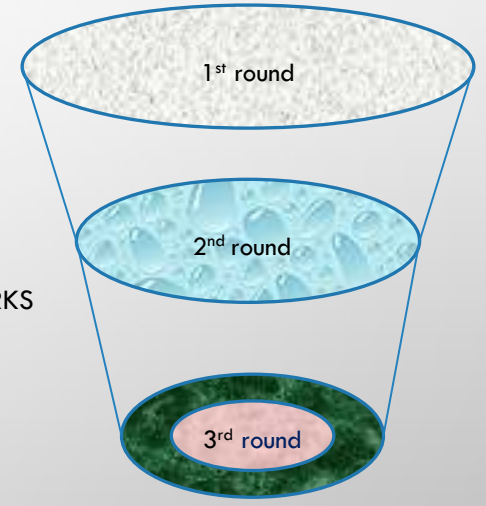
- NIST SELECTED 7 **FINALISTS** AND 8 **ALTERNATES**
  - **FINALISTS**: MOST PROMISING ALGORITHMS WE EXPECT TO BE AT END OF 3RD ROUND
  - **ALTERNATES**: CANDIDATES FOR POTENTIAL STANDARDIZATION, MOST LIKELY AFTER ANOTHER (4TH) ROUND



DECISION TIME

- HOW AND WHY DID NIST MAKE THESE HARD DECISIONS?
  - NISTIR 8413: STATUS REPORT ON THE 3RD ROUND OF THE NIST PQC STANDARDIZATION PROCESS

- EVALUATION CRITERIA
  1. **SECURE** AGAINST BOTH CLASSICAL AND QUANTUM ATTACKS
  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
     - ANY FACTOR WHICH COULD HINDER ADOPTION (I.E. PATENTS)
     - MISUSE RESISTANCE
     - ETC…



THE SIGNATURES

- BOTH DILITHIUM AND FALCON ARE BASED ON LATTICES
  - TRADEOFFS: FALCON'S COMPLEX IMPLEMENTATION VS ITS SMALLER KEY AND SIGNATURE SIZES

- NIST SELECTED DILITHIUM AS THE PRIMARY SIGNATURE ALGORITHM
  - NIST WILL PRIORITIZE ITS STANDARDIZATION
  - NIST SELECTED FALCON FOR APPLICATIONS WHICH NEED SMALLER BANDWIDTH AND CAN HANDLE A MORE COMPLEX IMPLEMENTATION

- SPHINCS+ IS A STATELESS HASH-BASED SIGNATURE SCHEME
  - SPHINCS+ WAS SELECTED TO COMPLEMENT THE LATTICE SIGNATURES, BEING BASED ON A DIFFERENT SECURITY PROBLEM
  - MUCH HIGHER COST AND PERFORMANCE IN COMPARISON TO DILITHIUM AND FALCON

THE KEMS

- THE LATTICE-BASED ALGORITHM KYBER WAS THE ONLY KEM SELECTED FOR STANDARDIZATION AT THIS POINT
  - STRONG SECURITY AND GREAT PERFORMANCE

- THERE ARE STILL 4 KEMS UNDER CONSIDERATION IN THE 4TH ROUND
  - CLASSIC MCELIECE
    - CODE-BASED, CONSERVATIVE SECURITY
    - VERY LARGE PUBLIC KEYS MEAN IT MAY NOT BE SUITABLE FOR MOST SETTINGS
  - BIKE AND HQC
    - BASED ON STRUCTURED CODES
    - BOTH HAVE PERFORMANCE PROFILES THAT WOULD BE SUITABLE FOR MOST USES
  - SIKE
    - BASED ON ISOGENIES
    - SMALL KEY/CIPHERTEXT SIZE, BUT NOT AS PERFORMANT

TIMELINE

- The 3rd Round has ended!!
  - NIST is currently writing draft standards for the selected algorithms
- The 4th Round has begun
  - BIKE, Classic McEliece, HQC, and SIKE to be further studied
    - Tweaks due October 1, 2022
  - The 4th round will likely be 18-24 months
- The 4th NIST PQC Standardization Conference
  - Nov 29-Dec 1, 2022, held virtually
- Draft standards for public comment should be in 2023
- The first PQC standards should be published around 2024

STANDARDIZATION

- NIST'S PUBLIC-KEY CRYPTO IS STANDARDIZED IN:
  - FIPS 186-5, DIGITAL SIGNATURES
  - SP 800-56A, 800-56B, ENCRYPTION/KEY-ESTABLISHMENT

- NIST WILL CREATE NEW STANDARDS, IN CONSULTATION WITH THE CANDIDATE TEAMS
  - NIST WILL DETERMINE WHICH SPECIFIC PARAMETER SETS TO INCLUDE, AND GIVE THEIR SECURITY STRENGTH
  - NIST WILL SEEK FEEDBACK FROM COMMUNITY, IF NEEDED

- THE DRAFT STANDARDS WILL BE PUT OUT FOR PUBLIC COMMENT
  - FEEDBACK RECEIVED WILL BE MADE PUBLIC
  - NIST WILL MAKE ANY NECESSARY REVISIONS AND THEN PUBLISH THE STANDARD

AN ON-RAMP FOR SIGNATURES

- NIST will issue a new Call for Signatures
  - There will be a deadline for submission, likely Jan 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

RECENT CRYPTANALYSIS

- THERE WERE SEVERAL CRYPTANALYTIC RESULTS IN THE 3RD ROUND
- EXAMPLES: (SEE THE REPORT FOR CITATIONS)
  - ADVANCES ON THE MINRANK PROBLEM LEADING TO ATTACKS ON GEMSS AND RAINBOW
  - IMPROVEMENTS IN THE DUAL LATTICE ATTACK
  - ATTACKS ON SOME PARAMETER SETS OF SPHINCS+
  - WORK ON THE COST OF ATTACKS THAT REQUIRE LARGE MEMORY
  - LATTICE ALGORITHMS LIKE TWISTED-PHS AND S-UNIT ATTACKS

- NIST IS AWARE OF THESE DEVELOPMENTS AND TAKES THEM INTO ACCOUNT
- MORE RECENTLY, THE 4TH ROUND CANDIDATE SIKE WAS BROKEN

PATENT ISSUES

- NIST BELIEVES IT IS CRITICAL THAT THIS PROCESS LEADS TO CRYPTOGRAPHIC STANDARDS THAT CAN BE FREELY IMPLEMENTED IN SECURITY TECHNOLOGIES AND PRODUCTS
- NTRU HAD PATENTS THAT HAVE EXPIRED, AND ARE NOW DEDICATED TO THE PUBLIC
- NIST WAS AWARE OF (3RD PARTY) PATENTS THAT COULD POTENTIALLY APPLY TO KYBER AND SABER
- NIST ENGAGED WITH THE PARTIES THAT OWNED THESE PATENTS AND HAS REACHED AGREEMENTS SO THAT THESE PATENTS WILL NOT BE ASSERTED AGAINST IMPLEMENTERS (OR END-USERS) OF THE NIST PQC STANDARD
- NIST APPRECIATES THE EFFORTS OF THOSE WHO HELPED OBTAIN THIS OUTCOME, PARTICULARLY THE COOPERATION OF THE PARTIES

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))

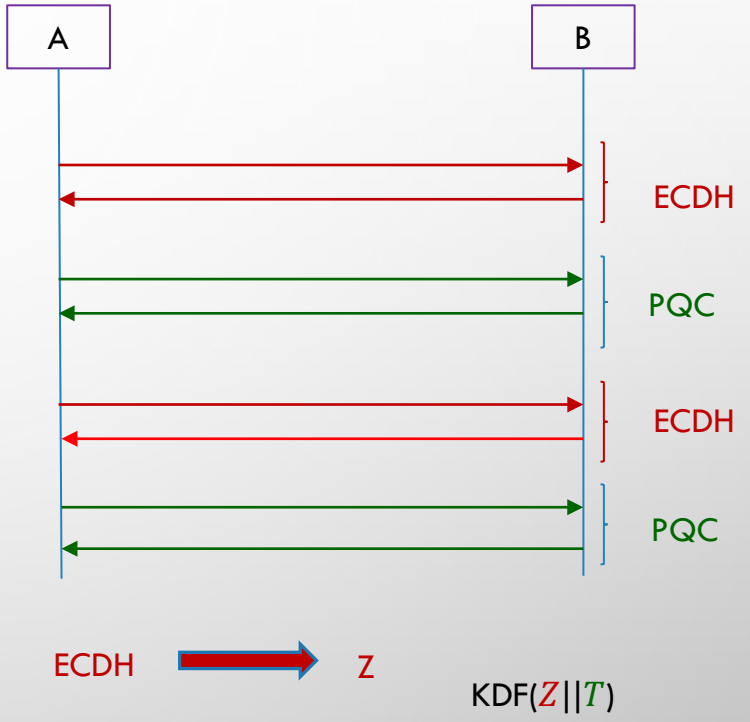
ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

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

HYBRID MODE – AN APPROACH FOR MIGRATION

NIST SP800-56C Rev. 2
Recommendation for Key-Derivation Methods in Key-Establishment Schemes
August 2020

> "In addition to the currently approved techniques for the generation of the shared secret Z … this Recommendation permits the use of a "hybrid" shared secret of the form $Z' = Z \,||\, T$, a concatenation consisting of a "standard" shared secret Z that was generated during the execution of a key-establishment scheme (as currently specified in [SP 800-56A] or [SP 800-56B]) followed by an auxiliary shared secret T that has been generated using some other method"



The above is just an illustration. The actual combination of two schemes will depend on the protocol specifications.

CRYPTO TRANSITIONS

NIST has published transition guidelines for algorithms and key lengths

NIST SP 800-131A Revision 2 "Transitioning the Use of Cryptographic Algorithms and Key Lengths" - Examples

- Three-key Triple DES
  - Encryption - Deprecated through 2023 Disallowed after 2023
  - Decryption - Legacy use
- SHA-1
  - Digital signature generation - Disallowed, except where specifically allowed by NIST protocol-specific guidance
  - Digital signature verification - Legacy use
  - Non-digital signature applications – Acceptable
- Key establishment methods with strength < 112 bits (e.g. DH mod p, $|p| < 2048$)
  - Disallowed

NIST will provide transition guidelines to PQC standards

- The timeframe will be based on a risk assessment of quantum attacks

GETTING READY FOR PQC

NIST

- The National Cybersecurity Center of Excellence (NCCoE) has a project for Migration to PQC . The goals:
  - Align and complement the NIST PQC standardization activities
  - Raise awareness and develop practices to ease the migration to PQC algorithms
  - Deliver white papers, playbooks, and demonstrable implementations for organizations
  - Target organizations that provide cryptographic standards and protocols and enterprises that develop, acquire, implement, and service cryptographic products
- NCCoE recently teamed up with the Dept. of Homeland Security in this effort.
- If you are interested in joining the project team as a collaborator, please review the requirements identified in the Federal Register Notice which is based on the final project description.
  - Questions and comments: applied-crypto-pqc@nist.gov

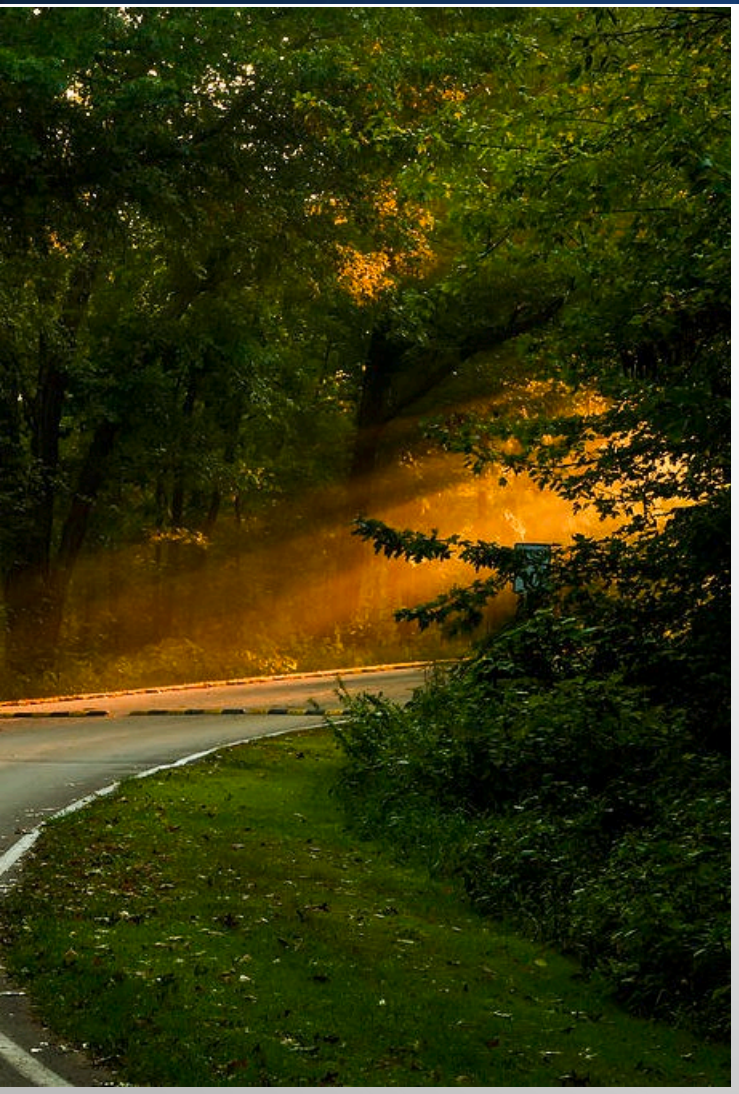
OTHER STANDARDS ORGANIZATIONS

- 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
  - 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
  - IDENTIFY 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, AND TO 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!
- 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