



ETSI/IQC Quantum Safe Cryptography Event

The first NIST PQC Standards

(Lily Chen and) Dustin Moody



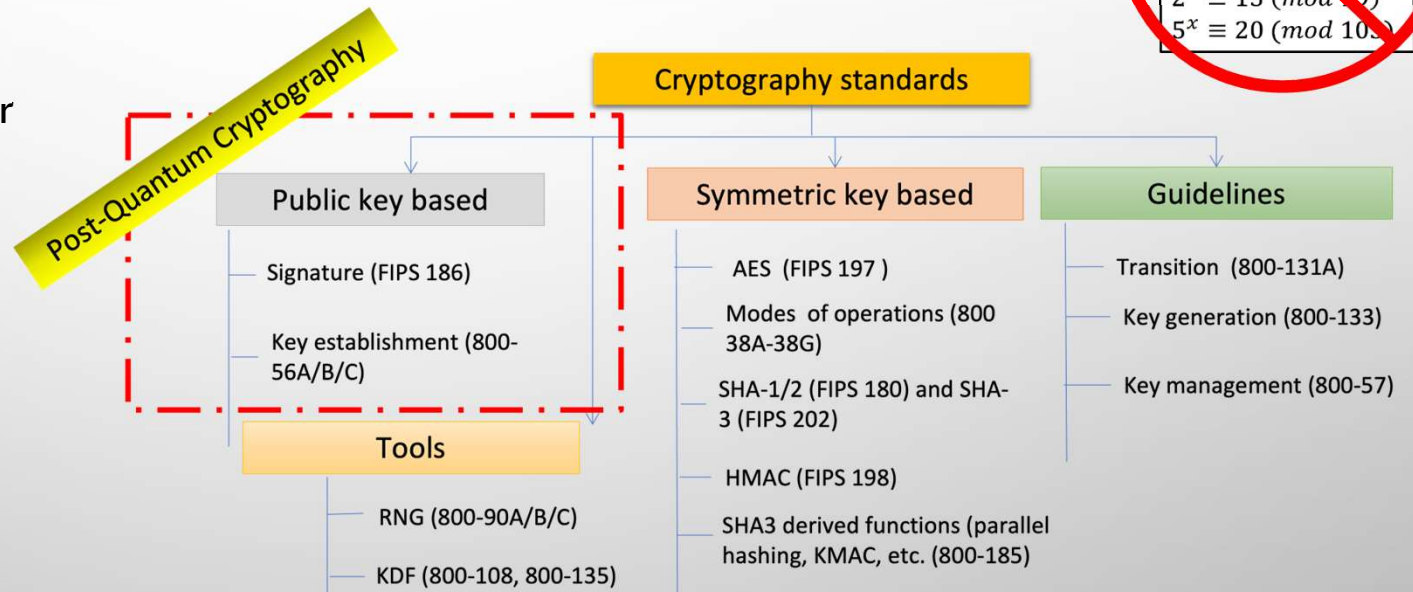
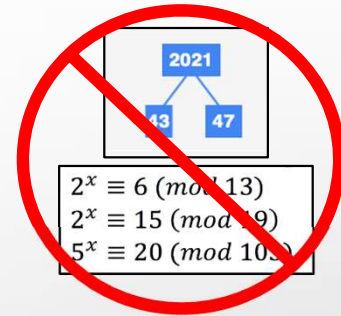
14/2/2023



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 SHOULD WE WORRY?



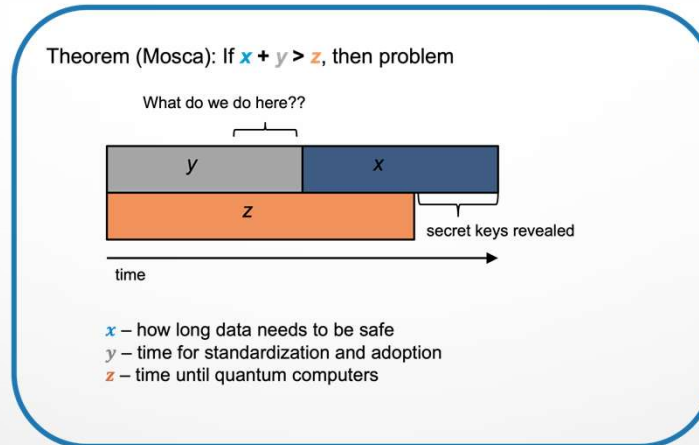
Administration

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



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.”

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 *Shalanda D. Young*
Director

SUBJECT: Migrating to Post-Quantum Cryptography

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

Announcing the Commercial National Security Algorithm Suite 2.0

CNSA 2.0

CYBERSECURITY ADVISORY

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

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

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	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric based	3		3

Other	Signatures	KEMs/Encryption	Total	
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	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**

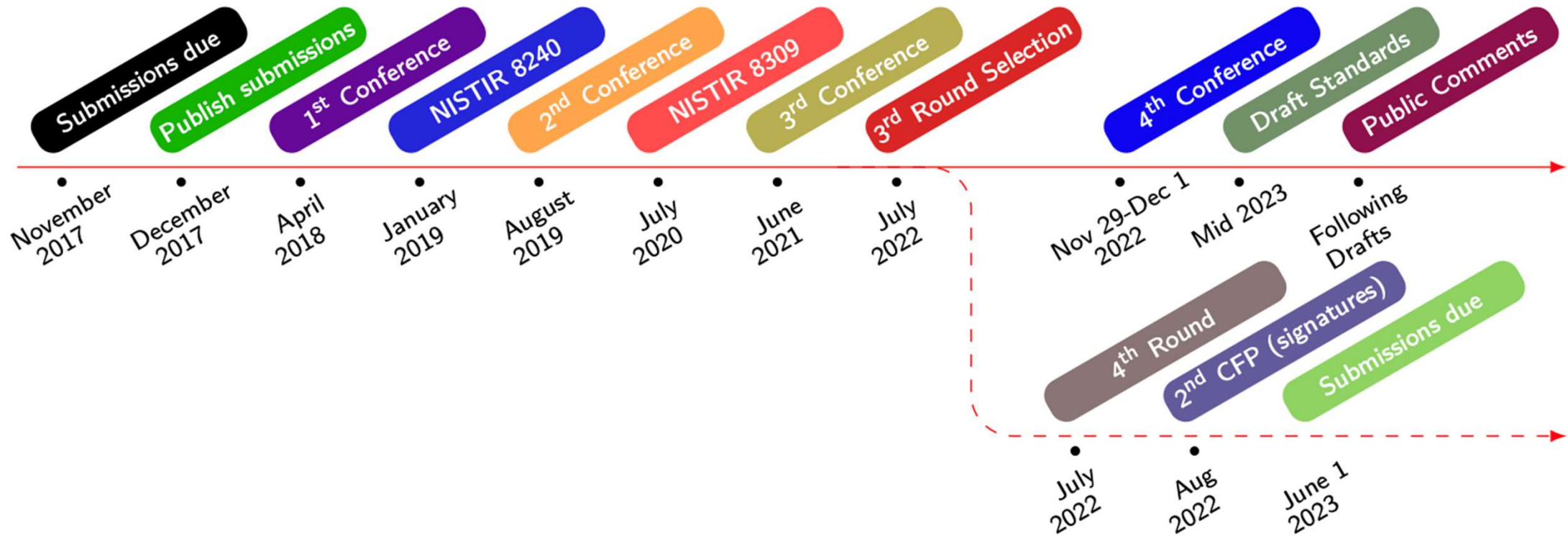
- ClassicMcEliece
- BIKE
- HQC
- SIKE

On-ramp signatures

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



TIMELINE



- The 4th Round is ongoing, and a new call for additional PQC signatures was made
- Draft standards for public comment will be in 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

- 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

- WE ARE WRITING THE PQC STANDARDS AS 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, HASH FUNCTIONS, SYMMETRIC PRIMITIVES, ETC. TO INCLUDE?
 - NIST INDICATED WHICH PARAMETER SETS THEY ARE THINKING OF STANDARDIZING
 - IN PARTICULAR, WE ARE LEANING TO INCLUDE KYBER-512
 - HOW TO ALLOW FOR ANY POTENTIAL CHANGES FROM THE ROUND 3 SPECIFICATIONS?
 - ANY CHANGES BY NIST (OR SUGGESTED BY TEAMS) WILL BE DISCUSSED PUBLICLY
 - WE DO NOT PLAN TO SUPPORT A 12-ROUND VERSION OF KECCAK AS WAS PROPOSED
- PLEASE PROVIDE FEEDBACK
 - PQC-FORUM, SLACK, ETC



IP UPDATE

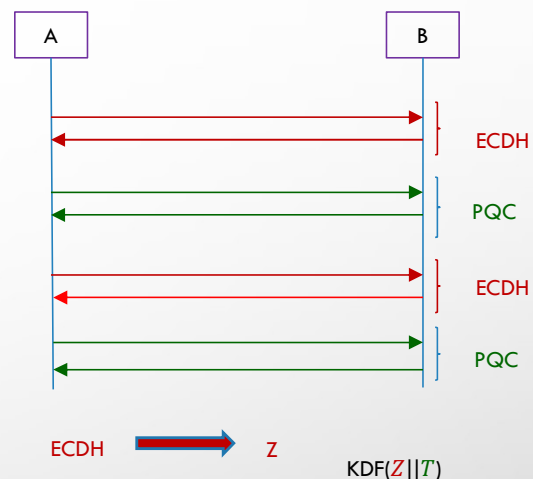
- THE LICENSE AGREEMENTS MENTIONED IN NISTIR 8413 HAVE BEEN SIGNED BY ALL PARTIES
 - NIST APPRECIATES THE EFFORTS OF THOSE WHO HELPED OBTAIN THIS OUTCOME AND THE COOPERATION OF THIRD PARTIES
 - CNRS, THE UNIVERSITY OF LIMOGES, THE LABORATORY XLIM, AND JINTAI DING
- THE (RELEVANT) TEXT OF THE LICENSE 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*



WE ARE **NOT** CONSIDERING NTRU FOR STANDARDIZATION

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 NATIONAL CYBERSECURITY CENTER OF EXCELLENCE (NCCOE) HAS A PROJECT FOR [MIGRATION TO PQC](#).



CONCLUSION

NIST



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

- NIST IS GRATEFUL FOR EVERYBODY'S EFFORTS

- WE WELCOME FEEDBACK

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