NIST PQC Standards

IETF 120-PQUIP
Vancouver Canada, July 22 2024.

Quynh Dang
Cryptographic Technology Group, NIST

Tuesday, October 3rd, 2023

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.
- AT LEAST 5 NOBEL PRIZES

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

THE QUANTUM THREAT

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

All vulnerable to attacks from a (large-scale) quantum computer.

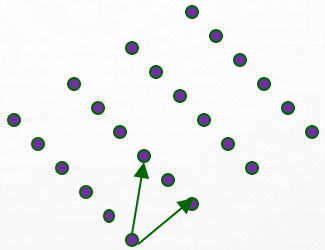
- Symmetric-key crypto (AES, SHA) would also be affected (by Grover's algorithm), but less dramatically.

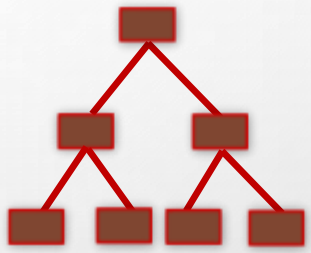
POST-QUANTUM CRYPTOGRAPHY

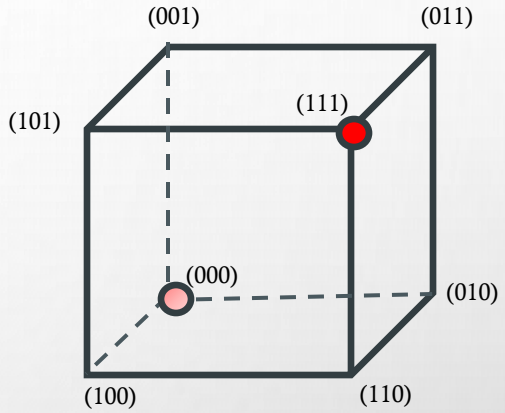
- Need to find cryptographic algorithms which are secure against attacks by both classical and quantum computers
  - The algorithms must be based on hard problems for both classical and quantum computers
- In other words, we need *quantum resistant cryptography*, also known as as *post-quantum cryptography* (PQC)

POST QUANTUM CRYPTOGRAPHY (PQC)

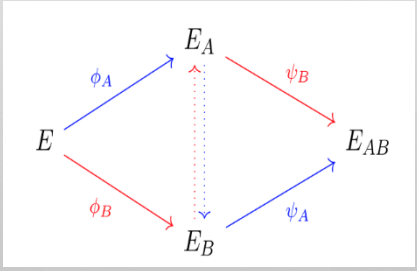
- PQC has been a very active research area in the past few decades
- Some actively researched PQC categories include
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key-based signatures
  - Elliptic curve isogeny-based







$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(m)}\cdot x_i + p_0^{(m)}
\end{aligned}
$$



THE NIST PQC SELECTION PROCESS

- 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 ALGORITHM SELECTIONS 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

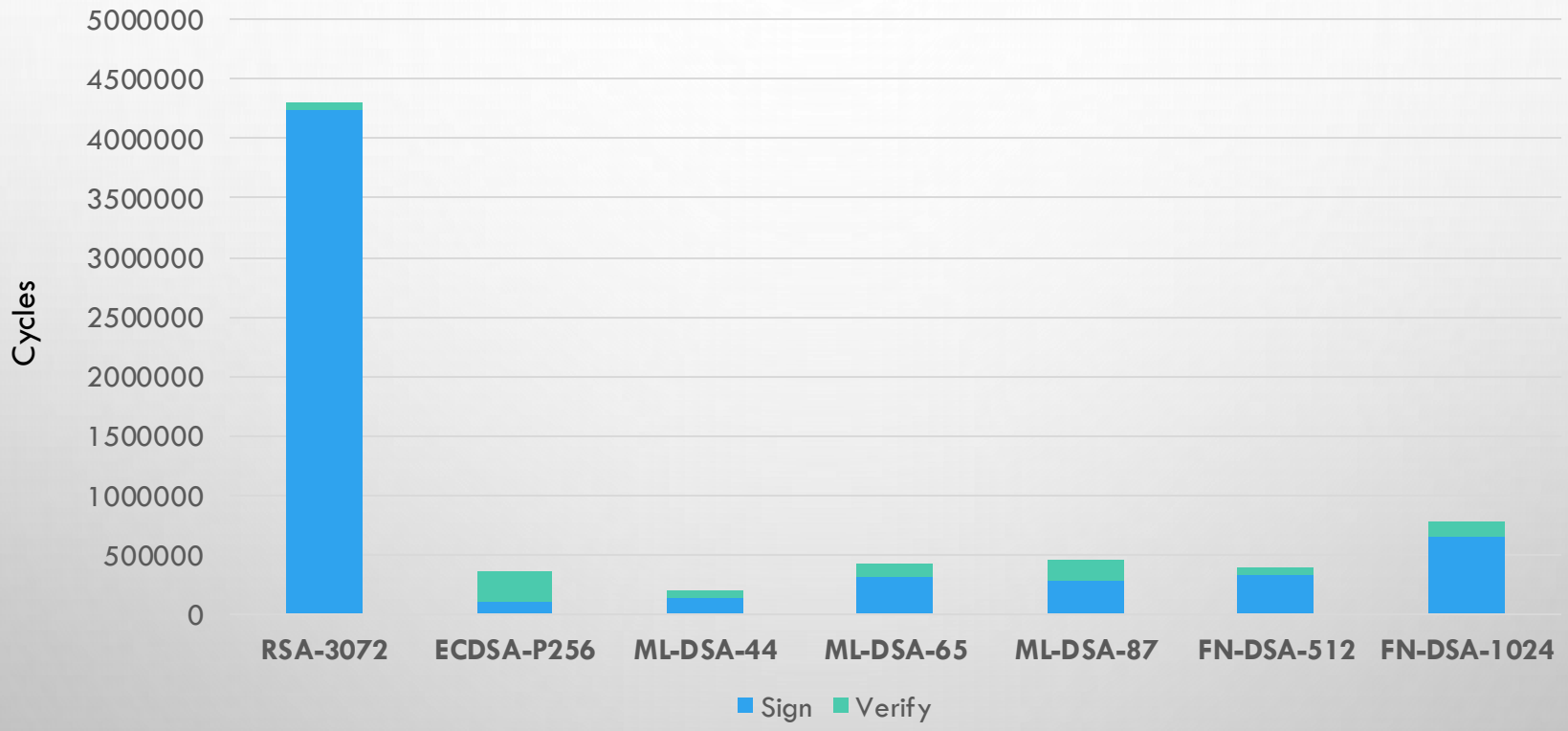
- NIST issued a new call for additional signatures – preferably for signatures based on non-lattice problems (2022).

THE SELECTED ALGORITHMS

- ML-KEM (CRYSTALS-KYBER)
  - KEM BASED ON STRUCTURED LATTICES
  - GOOD ALL-AROUND PERFORMANCE AND SECURITY

- ML-DSA (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
- FN-DSA (FALCON)
  - DIGITAL SIGNATURE BASED ON STRUCTURED LATTICES
  - SMALLER BANDWIDTH, BUT MUCH MORE COMPLICATED IMPLEMENTATION
  - THE FALCON STANDARD WILL COME OUT AFTER THE OTHERS
- SLH-DSA (SPHINCS+)
  - DIGITAL SIGNATURE BASED ON STATELESS HASH-BASED CRYPTOGRAPHY
  - SOLID SECURITY, BUT PERFORMANCE NOT AS GOOD IN COMPARISON TO DILITHIUM/FALCON

PQC SIGNATURES– PERFORMANCE



PQC KEY AND SIGNATURE SIZES

Scheme	Public Key (bytes)	Private Key (bytes)	Signature (bytes)	Security Level
RSA-3072	**384**	**384**	**384**	**Classical-128**
ECDSA-P256	**64**	**32**	**256**	**Classical-128**
ML-DSA-44 (Dilithium2)	**1312**	**2528**	**2420**	**PQC Category 2** *(SHA3-256)*
ML-DSA-65 (Dilithium3)	**1952**	**4000**	**3293**	**PQC Category 3** *(AES-192)*
ML-DSA-87 (Dilithium5)	**2592**	**4864**	**4595**	**PQC Category 5** *(AES-256)*
FN-DSA-512 (Falcon512)	**897**	**7553**	**666**	**PQC Category 1** *(AES-128)*
FN-DSA-1024 (Falcon1024)	**1793**	**13953**	**1280**	**PQC Category 5** *(AES-256)*

ML-KEM

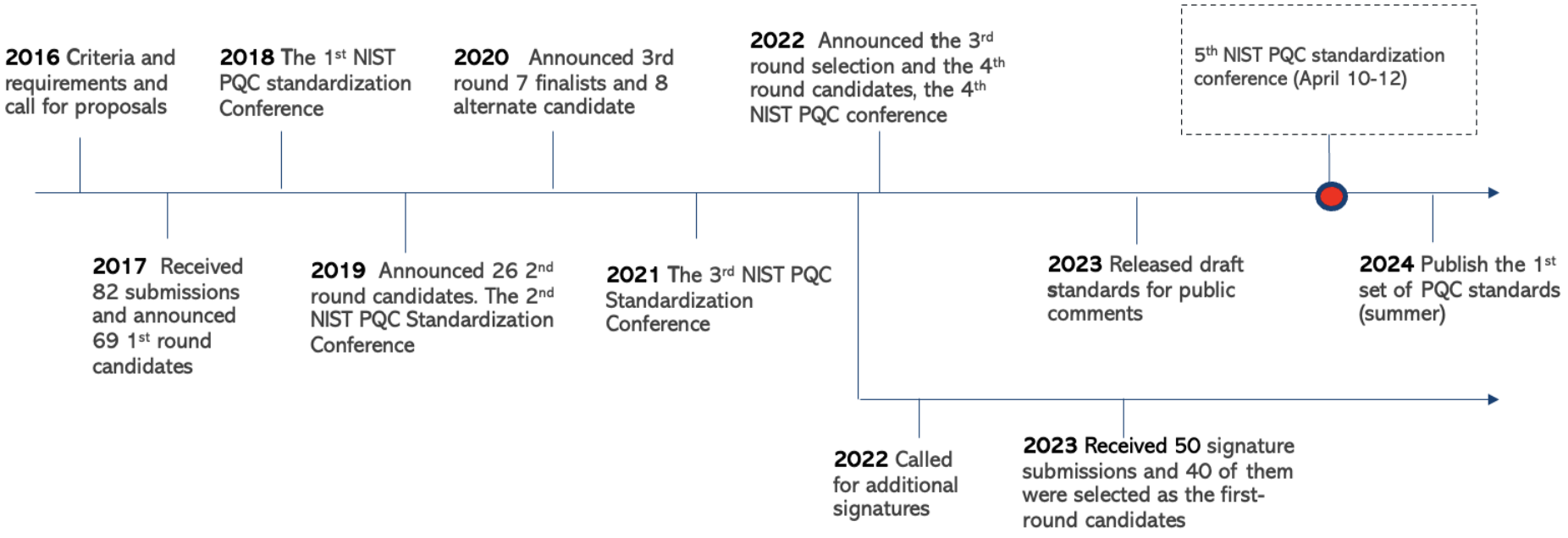
Scheme	Encap Key (bytes)	Decap Key (bytes)	Ciphertext (bytes)	Security Level
ML-KEM-512	800	1632	768	1
ML-KEM-768	1184	2400	1088	3
ML-KEM-1024	1568	3168	1568	5

ML-KEM

Scheme	Encap Key (bytes)	Decap Key (bytes)	Ciphertext (bytes)	Security Level
ML-KEM-512	**800**	**1632**	**768**	**1**
ML-KEM-768	**1184**	**2400**	**1088**	**3**
ML-KEM-1024	**1568**	**3168**	**1568**	**5**

We plan to allow key expansion from a seed of 64 bytes (d, z) so that Decap key can be derived from the seed whenever needed.

TIMELINE



- **The first PQC standards will be published very soon.**

STANDARDIZATION

- THE 1ST PQC DRAFT STANDARDS
  - FIPS 203: ML-KEM (KYBER)
  - FIPS 204: ML-DSA (DILITHIUM)
  - FIPS 205: SLH-DSA (SPHINCS+)
  - FN-DSA (FALCON) – UNDER DEVELOPMENT

- WE ARE FINISHING OUR REVISIONS BASED ON THE COMMENTS
  - **FIPS 203, 204, 205 ARE COMING SOON.**

- SEE COMMENTS AT WWW.NIST.GOV/PQCRYPTO
- LOTS OF DISCUSSION ON PQC-FORUM

THE PATH TO THE FINAL STANDARDS

THE FINAL VERSIONS WILL BE SUBMITTED TO THE SECRETARY OF COMMERCE FOR APPROVAL SOON!

- THERE WILL BE A FEDERAL REGISTER NOTICE (FRN) ANNOUNCING THE PUBLICATION
- THE FRN WILL ALSO INCLUDE A SUMMARY OF THE PUBLIC COMMENTS AND OUR RESPONSES, INCLUDING MANY MAIN CHANGES THAT WE MADE.

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 acknowledged that SIKE (and SIDH) are insecure and should not be used

The 4th Round will likely end in the fall of 2024

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 with short signatures and fast verification.
  - Any lattice signature would need to significantly outperform CRYSTALS-Dilithium and FALCON and/or ensure substantial additional security properties.
- 40 Signature candidates currently in Round 1
  - Poster session at our April conference
- We expect to make selections for Round 2 in 2024.

No on-ramp for KEMs currently planned.

OTHER UP COMING PQC PUBLICATIONS

- SP 800-208 is being revised, based on industry feedback. How to allow backups for HSMs while minimizing the risk of key reuse.
- SP 800-227 Recommendations for Key Encapsulation Mechanisms is expected to be available for public comments soon after FIPS 203 is finalized and published.
- A draft SP specifies Small SLH-DSA Parameter Sets is expected in Fall 2024.

KEM KDFS

- NIST SP800-56C REV. 2 ALLOWS HYBRID MODE KDFS WHERE Z' = Z || T. Z IS A CLASSICAL SHARED SECRET AND T IS ANOTHER SHARED SECRET/SECRET KEY.
- THE KDFS IN SP 800-108 ARE ALLOWED TO DERIVE KEYS FROM ML-KEM SHARED SECRET KEY.
- WE PLAN TO ALLOW THE KDFS IN SP 800-56C TO DERIVE KEYS FROM ML-KEM SHARED SECRET KEY.
- THE KDFS IN SP 800-108 ARE ALLOWED TO DERIVE KEYS FROM MULTIPLE PSEUDORANDOM KEYS BY SP 800-133.

CONTACT & FEEDBACK

- NIST IS GRATEFUL FOR EVERYBODY'S EFFORTS
  - WE ARE COLLABORATING WITH OTHER STANDARDIZATION ACTIVITIES

NIST PQC Standardization

www.nist.gov/pqcrypto

Sign up for ***pqc-forum*** mailing list, pqc-forum@list.nist.gov

EMAIL: pqc-comments@nist.gov (only go to NIST PQC team members)