

NIST PQC Standardization

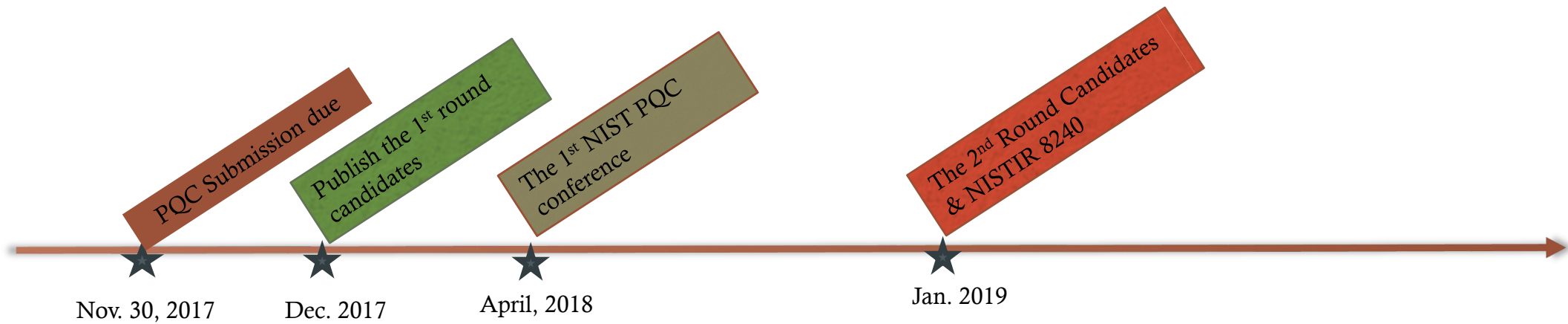
- The second round candidates

Lily Chen

Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

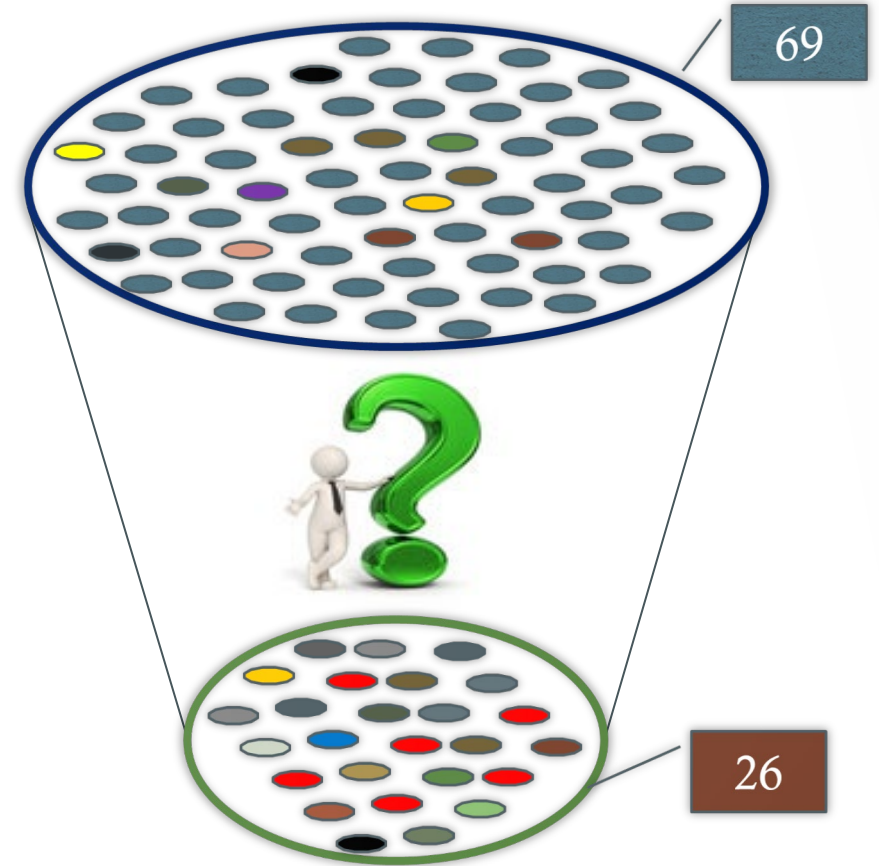
Where are we?

- The 69 first round candidates were announced December 2017
- NIST held the 1st PQC Standardization Conference in April 2018
- After about 12 months of evaluation and analysis, 26 candidates were announced as the second round candidates in January 2019 and we also published NISTIR 8240



Outline

- Evaluation of the 1st round candidates
- The selection of the 2nd round candidates
- What to expect in second round evaluation
 - Important factors to consider
- What industry can do to prepare for transition and migration
- Next step plan



The 1st Round Candidates

- 82 submissions received.
- 69 accepted as “complete and proper” (5 withdrew)

	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

Evaluation of the 1st Round

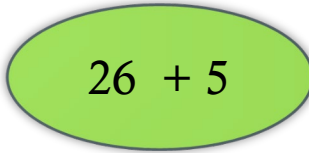
- NIST team had seminars to present each candidate by team members to understand how it works, look into security analysis provided by the submitters, raise questions, discuss pros and cons, etc.
- Security analysis
 - Research publications at conferences and journals (e.g. PQCrypto)
 - Official comments - Over 300 official comments
 - E-mail discussions at pqc-forum – 926 posts
- Performance
 - Evaluation resources include
 - NIST's internal testing with submitters' code
 - Preliminary benchmarks – SUPERCOP, OpenQuantumSafe, etc.

Selection of second round candidates

- Security
 - Candidates which were broken, significantly attacked, or difficult to establish confidence in their security were left out
 - Candidates which provided clear design rationale and reasonable security proofs to established reasonable confidence in security are advanced
- Performance
 - Candidates with obvious performance or key/signature/ciphertext size issues for existing applications were not advanced - even though they might have been well prepared with good ideas

More on selections

- We wanted to keep algorithm diversity and promote research, but had to reduce the number of candidates to a manageable size for the community
 - It is hard to make comparison among candidates in different categories
 - Sometimes even in the same category, it is not always possible to rank them
- Some candidates were merged as NIST encouraged
 - Round5 = Round2 + Hila5
 - Rollo = Lake + Locker + Ouroboros-R
 - NTRU = NTRUEncrypt + NTRU-HRSS-KEM
 - LEDAcrypt = LEDAkem + LEDApkc
- We encouraged members from the teams whose submitted algorithms were not advanced to join the relevant submission teams in the second round
 - It has been a community effort and all together we can get the best out of it



26 + 5

The 2nd round candidates

KEM/Enc

Lattice –based (9):

Crystals-Kyber; FrodoKEM; LAC;
NewHope; NTRU; NTRU Prime; Round 5;
Saber; Three Bears

Code –based (7):

Classic McEliece; NTS-KEM; BIKE; HQC;
Rollo; LEDAcrypt; RQC

Isogeny –based (1):

SIKE

Signature

Lattice –based (3):

Crystals-Dilithium; Falcon; qTESLA

Symmetric –based (2) :

Sphincs+; Picnic

Multivariate (4):

GeMSS; LUOV; MQDSS; Rainbow

* See NISTIR 8240 for a summary of each of the 2nd round candidates

Review of the 2nd round candidates

- The 2nd round candidates cover algorithms in the most researched categories for post quantum cryptography
- In the same category, candidates are designed with different ideas and mathematical structures, e.g.
 - Lattice-based includes LWE, RLWE, MLWE, Rounding, Error Correction, NTRU, etc.
 - Code-based category includes some candidates of rank-based variations, which are evaluated with significant different cryptanalysis approaches
 - Multivariate signature schemes include the Hidden Field Equations (HFEv-) family and also the Unbalanced Oil Vinegar (UOV) family
 - Signature schemes are either in hash-and-sign or in Fiat-Shamir format
- The 2nd round includes candidates with relatively conservative as well as more aggressive/optimized designs
- The 2nd round candidates provide a full spectrum for investigation

Second round evaluation

- NIST will hold the 2nd PQC Standardization Conference August 22-24, 2019 in Santa Barbara (right after crypto 2019)
- Security is very critical and we have a lot to understand, e.g.
 - Generic vs. structured (e.g. LWE vs. R-LWE) – Structured have smaller key sizes and/or are more efficient
 - Security impact on optimized versions – how far an optimization can go to maintain security
 - Newer security assumptions
- Performance evaluation is important to make the future standards useable
 - Performance (hardware + software) will play much more of a role in the second round
 - More benchmarks through different platforms and implementations
 - Evaluate how candidates fit into applications/protocols and identify show stoppers

Tradeoffs among second round candidates

- For signature
 - Public key size vs. signature size
 - Signature generation vs. verification
- For encryption
 - Public key size vs. ciphertext size
 - Key generation, encryption and decryption
 - Decryption failure rate vs. parameter size, etc.

Tradeoff preference in applications

- For secure boot
 - The time for signature verification is most important - signature generation may not impact the speed of booting
 - The key size may not be important if it can be stored externally with integrity protection
- For key establishment protocols e.g. IKE, TLS
 - The time on key generation is important when a one-time public key is used
 - Public-key size is also important when it needs to be transmitted
 - Signature size and ciphertext size are important in order to avoid message segmentation
- We need to look into more applications to see different preferences

Preparation for Migration

- Enable crypto agility for each function (public key encryption/key encapsulation, signature) when it is possible
- Understand implementation costs and required bandwidth/space for transmitting and storing keys, signatures and ciphertext
- Discuss tradeoff preferences in each application – identify special restrictions, limitations, and show stoppers
- Gain first-hand experience through trial implementations e.g. hybrid mode or dual signatures as a temporary solution
- Do not commit to a specific candidate for long-term products until NIST makes its selection for standardization

Future plans

- The 2nd PQC Standardization Conference will be held in August 2019
- Spend 12-18 months to analyze and evaluate the 2nd round candidates
- Start a 3rd round and/or select algorithms to standardize 2020-2021
- Release draft standards in 2022-2023 for public comments



Information on NIST PQC Standardization

- For NIST PQC project, please follow us at <https://www.nist.gov/pqcrypto>
- To submit a comment, send e-mail to pqc-comments@nist.gov
- Join discussion mailing list pqc-forum@nist.gov