NIST PQC Standardization
- The first round candidates

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

Where we are?

- The first round candidates were announced December 2017
  - A Christmas gift to cryptographers to play during holidays
- Since then some have been broken, wounded, or scratched and some are remain sound and health
- We, together with the whole community, are conducting analysis and evaluation
- NIST team will announce the second round candidates in early spring of 2019

Submissions to NIST Call for Proposals

- 82 total submissions received from 26 Countries, 6 Continents
- 69 accepted as "complete and proper" (5 since withdrawn)
- 2 candidates merged (*) and an encryption and a signature recently announced "merging"

	Signatures	KEM/Encryption	Overall
Lattice-based	5	20*	25
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash-based/Symmetric based	3	Merge?	3
Other	2	5	7
Total	**19**	**45**	**63**

General on the first round candidates

- Most submitted schemes (or early versions) have been published at the conferences or released through IACR eprint – In general, no big surprise
- Most submissions include proofs/discussions on the CCA/CPA security for Encryption/KEM and EUF-CMA for signatures
- Most submissions addressed the rationale for the selected parameters and mathematics structures as well as pros and cons of the schemes

Diversities and Tradeoffs

- Related to the security assumptions
  - Generic vs. structured (e.g. LWE vs. R-LWE) – Some submissions include both versions
- Auxiliary functions
  - Uniform sampling vs. Gaussian sampling
- Encryption/key exchange
  - Ciphertext size vs. public key size
  - Decryption failure vs. techniques to reduce the probability, including to increase the module
- Signature
  - Signature size vs. public key size
  - Hash-and-sign vs. Fiat-Shamir
- etc.

The 1st NIST PQC Standardization Conference

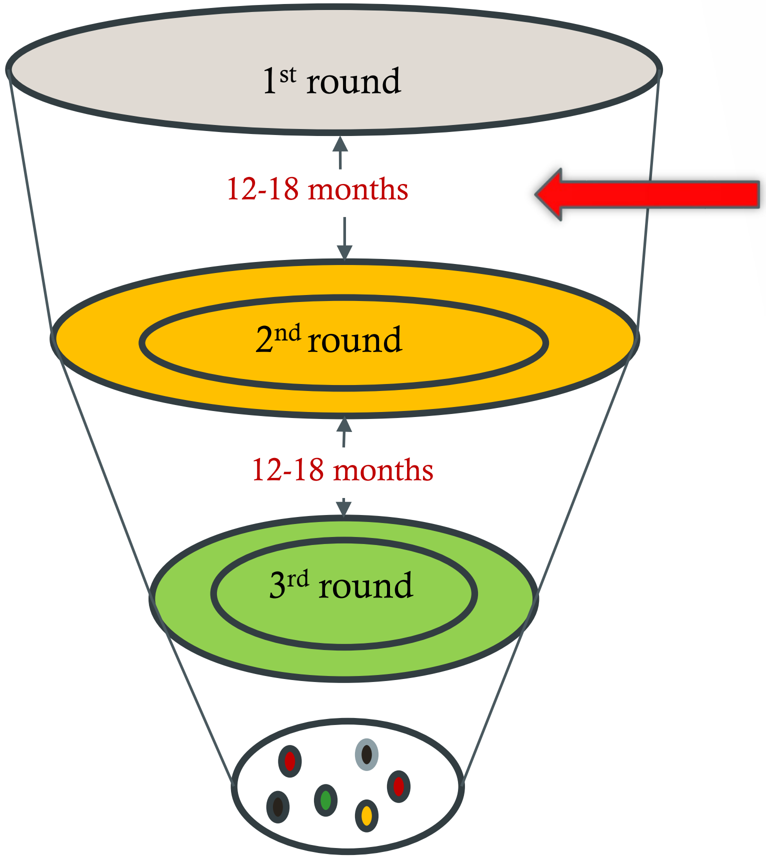
- The 1st NIST PQC Standardization Conference was held in Ft. Lauderdale April 11-13, collocated with PQCrypto2018
- The conference accommodated 52 presentations covering 60 algorithms, attracted 345 attendees
- We held a discussion session at the workshop on the following topics
  - measuring the complexity of quantum attacks
  - classical attack with super high memory
  - the way to handle similar submissions, and
  - what constitutes unacceptable key sizes or performance

Analysis and official comments

- Security analysis on submitted PQC schemes and related research topics have been active
  - Results have been published at conferences like PQCrypto 2018 and also release through IACR eprint
  - More analysis results have been announced through "Official Comments", which may lead to future publications
- About 313 "Official Comments" received upon October 22nd, 2018
- Comments are questions to submitters, attacks, or tweaks for their own submissions
  - 51 submissions have official comments among the initial 69 submissions

NIST Timeline (from April 2018)

- Initial analysis phase 12-18 months
- Announce second round candidates in the spring of 2019
- Hold the second conference in August 2019 (Collocate with Crypto 2019)
- Second analysis phase 12-18 months
- May take third analysis phase if needed
- Expect draft standards in 2022-2023



Information on NIST PQC Standardization

- For NIST PQC project, please follow us at
  https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- To submit a comment, send e-mail to pqc-comments@nist.gov
- Join discussion mailing list pqc-forum@nist.gov