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

Towards PQC Standardization and Migration

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

Why Post-Quantum Cryptography (PQC) is needed?

The security of well deployed public key cryptosystems is based on the hardness of

- Factorization
  - e.g. RSA signature and RSA public key encryption
- Discrete Logarithm Problem
  - E.g. Diffie-Hellman Key Agreement over finite fields and elliptic curves

Emerging quantum computers, when in full size, changes what we believed about the hardness of discrete log and factorization problems

- Using quantum computers, the factorization and discrete logarithm problem are not hard any more
- Shor's algorithm can solve them in polynomial time
  - RSA and Diffie-Hellman will not be secure!

We need to look for quantum-resistant counterparts for these cryptosystems

- The category is called post-quantum cryptography (PQC)
  - a.k.a. quantum resistant cryptography or quantum-safe cryptography

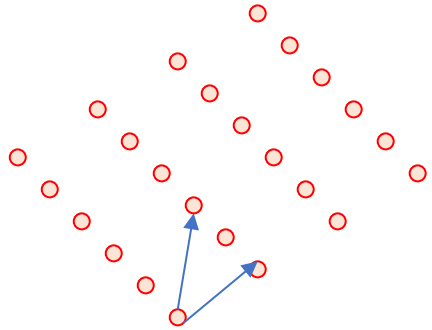
Quantum computing also impacted security strength of symmetric key based cryptography algorithms

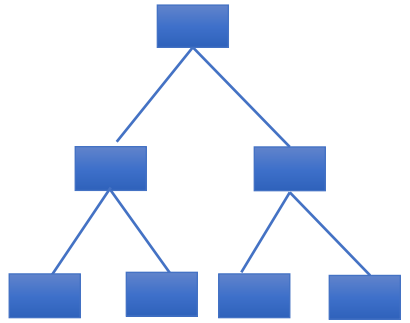
- Grover's algorithm can find AES128 key with approximately $\sqrt{2^{128}} = 2^{64}$ operations
- The quantum impact to symmetric key algorithms can be dealt with by increasing the key size

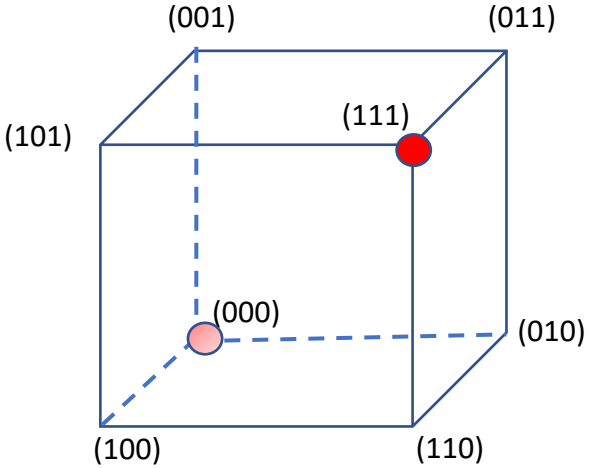
Post-Quantum Cryptography (PQC)

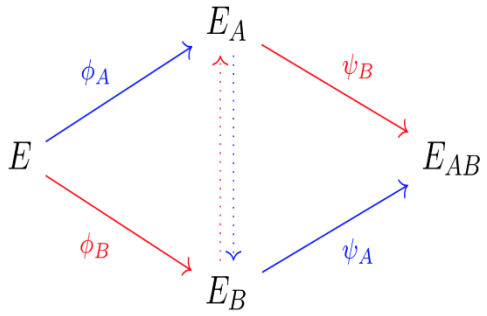
Some actively researched PQC categories

- Lattice-based
- Code-based
- Multivariate
- Hash based signatures
- Isogeny-based schemes



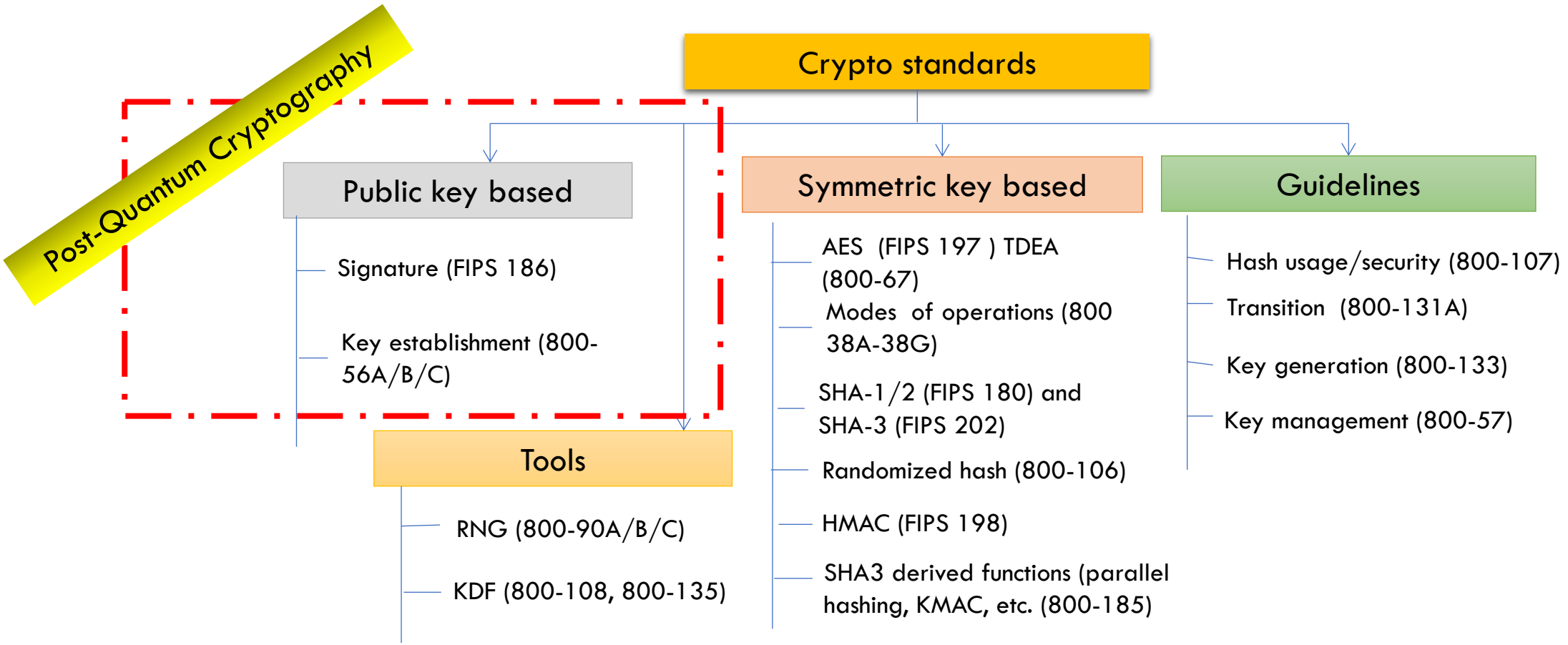






$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)} \\
&\vdots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

NIST Post-Quantum Cryptography Standards



NIST PQC Milestones

2016

Determined criteria and requirements

Announced call for proposals

2017

Received 82 submissions

Announced 69 1st round candidates

2018

1st round analysis

Held the 1st NIST PQC standardization Conference

2019

Announced 26 2nd round candidates

Held the 2nd NIST PQC Standardization Conference

2020

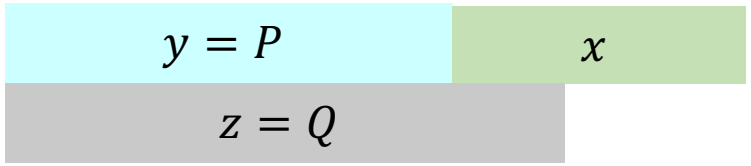
Announced 3rd round 7 finalists and 8 alternate candidates (new!)

P and Q Timeline – P stands for PQC while Q Quantum Computers

2022-2023
Release drafts standards for public comments

2024 -
Start to publish standards

If $y + x > z$, then we should worry.
- Michele Mosca



y – time for PQC standardization and adoption

x – time of maintaining data security

z – time for quantum computers to be developed

What is z?

- **2014**, D. Mariantoni: $1 billion dollars, 15 years, small nuclear power plant
- **2015**, M. Mosca: There is a 1 in 7 chance that RSA-2048 will be broken by 2026, and a 1 in 2 chance by 2031
- **2017**, S. Benjamin: 15-25 years at current spending. 6-12 years if somebody "goes Manhattan-level"
- **2017**, D. Bernstein: Private bet on twitter that quantum computers break RSA-2048 by 2033.
- **2020**, M. Mosca: "There is a 1 in 5 chance that some fundamental public-key crypto will be broken by quantum by 2029."

Quantum Threat Timeline

See survey at
https://globalriskinstitute.org/publications/quantum-threat-timeline/

Security Strength and Definitions for PQC Standards

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)

Security definitions (proofs recommended, but not required) used to judge whether an attack is relevant

- IND-CPA/IND-CCA2 for encryptions and KEMs
- EUF-CMA for signatures

Submissions to NIST Call for Proposals and the 1st Round Candidates

Before submission deadline (Nov. 30, 2017), 82 total submissions received from 25 Countries, 6 Continents

- The submitters in USA are from 16 States

69 accepted as "complete and proper" (5 since withdrawn)

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash or Symmetric based	3		3
Other	2	5	7
Total	19	45	64

The 2nd Round Candidates

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

	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-variate	4		4
Stateless Hash or Symmetric based	2		2
Isogeny		1	1
Total	10	16	26

The 3rd Round Finalists and Alternate Candidates

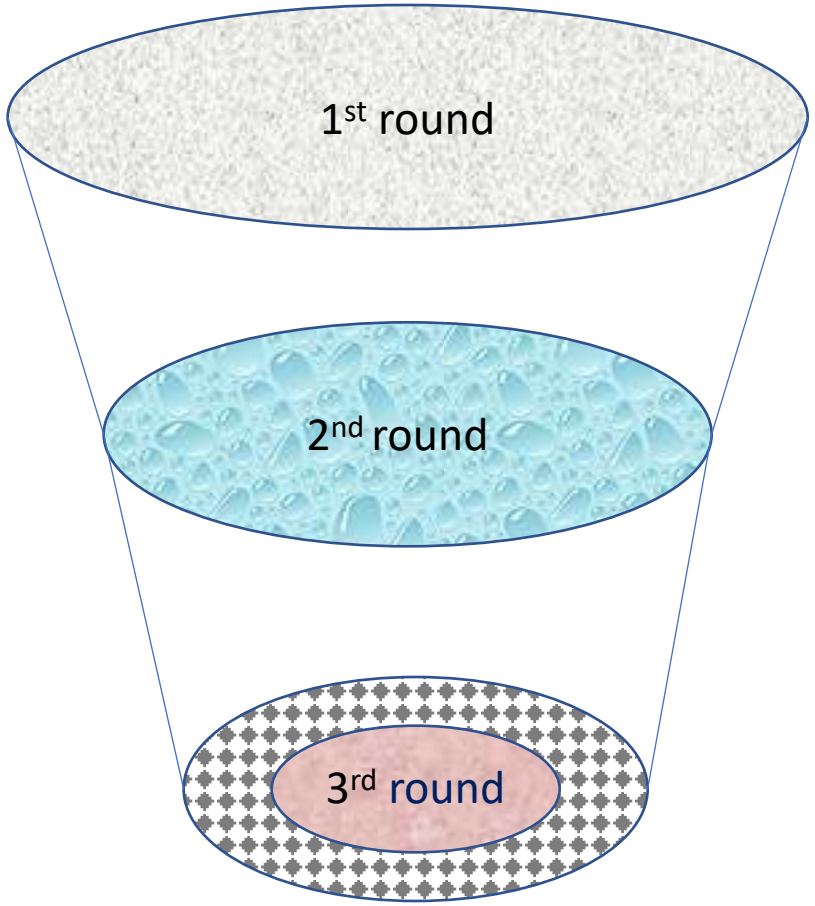
The 3rd round consists of 7 finalists and 8 alternate candidates

- The set of finalists are algorithms that NIST considers to be the most promising to fit the majority of use cases and most likely to be ready for standardization soon after the end of the third round.
- The alternate candidates are regarded as potential candidates for future standardization, most likely after another round of evaluation

	Signatures		KEM/Encryption		Overall	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	3	4	5	7	8

Challenges in Selecting Algorithms

- Understand classical security for numerous new designs
- Understand quantum security with different complexity models and numerous possibilities of new discovery
- Look into performance on multiple platforms and for numerous applications
- Understand tradeoff preferences for practical applications



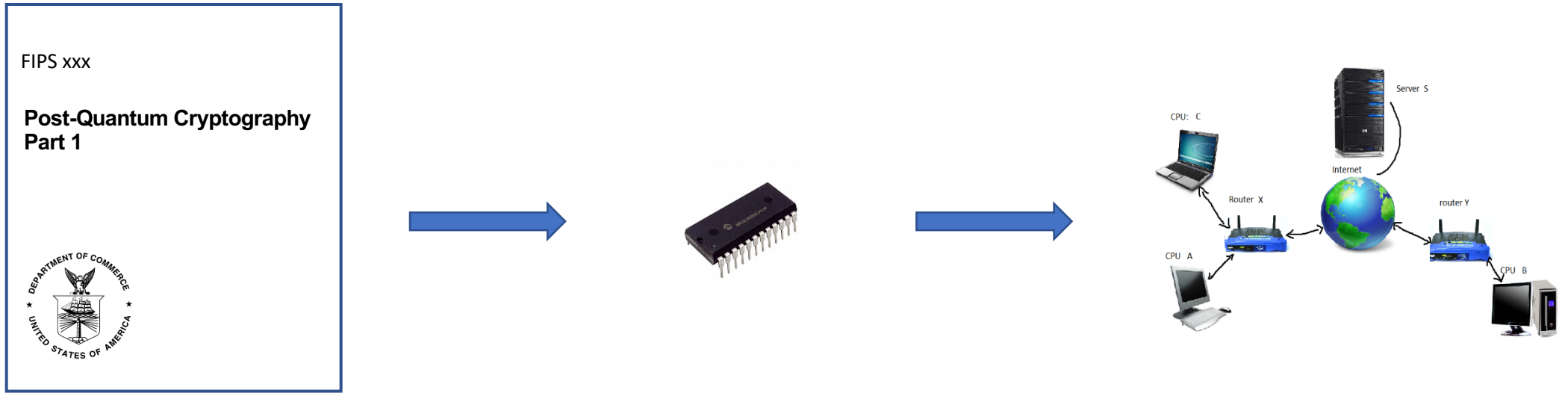
More challenges ahead – Transition and Migration

Public key Cryptography has been used everywhere and two most important usages are for

- Communication security; and
- Trusted platforms

Transition and migration is going to be a long journey and full of exciting adventures

- Understand new features, characters, implementation challenges
- Identify barriers, issues, show-stoppers, needed justifications, etc.
- Reduce the risk of disruptions in operation and security



More about migration strategies

Enable crypto agility – A capability to adopt new and sunset insecure algorithms

- Replacing or changing crypto libraries
- Introduce authenticated negotiation of cipher suite in protocols

Obtain firsthand experience through prototype

- See how they work on different platforms and in different applications

Understand product cycle and plan ahead

- Make algorithm change into a phased schedule
- Do not commit to a specific candidate for long-term products until NIST makes its selection for standardization

Understand implementation costs and required bandwidth/space for transmitting and storing keys, signatures and ciphertext

- Identify any needs to make adaption to existing protocols

Timeline and contact information

Hold the 3rd NIST PQC Standardization Conference in spring 2021

Release draft standards in 2022-2023 for public comments

We will continue open for suggestions and encourage discussions

- 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