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

Cryptography in Quantum Era

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

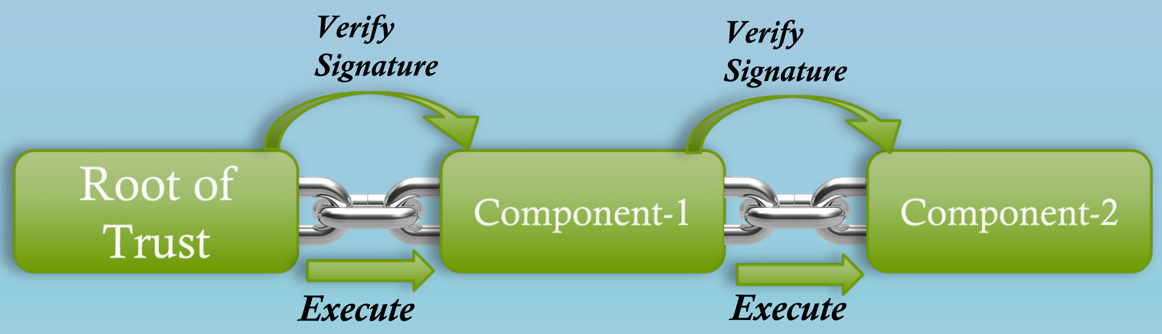
Cryptography in Hardware-Enabled Security

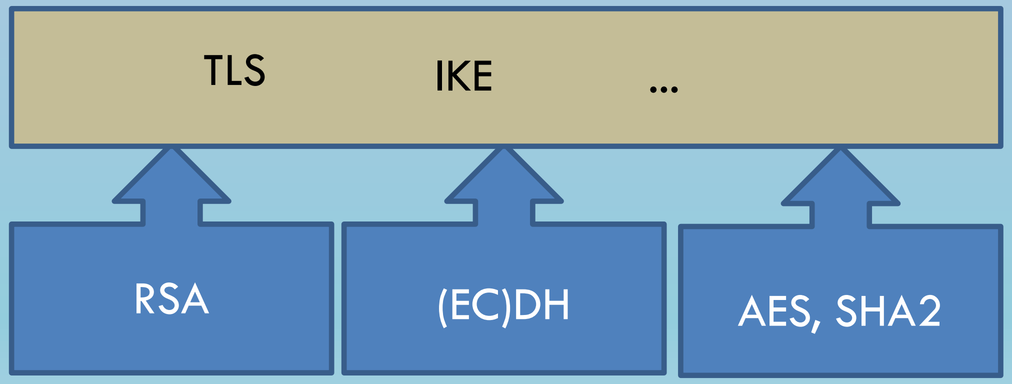
All security controls must have a root of trust (RoT) – A start point for a chain of trust

- Secure boot - verify integrity and trustworthy of the firmware
- The basic idea behind secure boot is to sign executables using a public-key cryptography scheme – digital signatures

Cryptography algorithms are implemented in hardware to accelerate the operations

- Hardware libraries provide cryptographic functions for applications
    - Dedicated cryptographic hardware





Quantum Impact

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

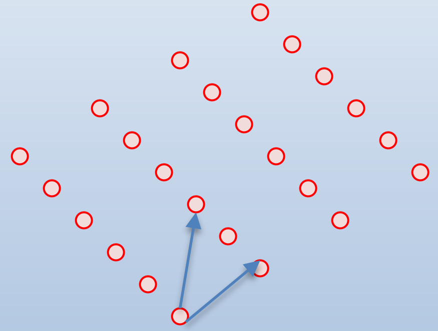
Quantum computing also impacted security strength of symmetric key based cryptography algorithms

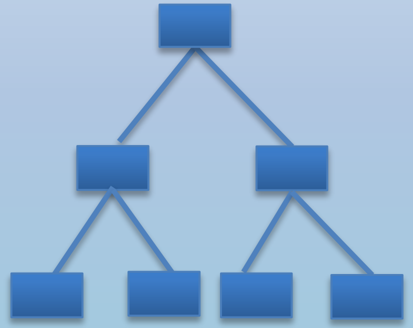
- Grover's algorithm can find AES128 key with approximately $\sqrt{2^{128}} = 2^{64}$ operations
- The quantum impact to symmetric key algorithms can be dealt with by increasing the key size

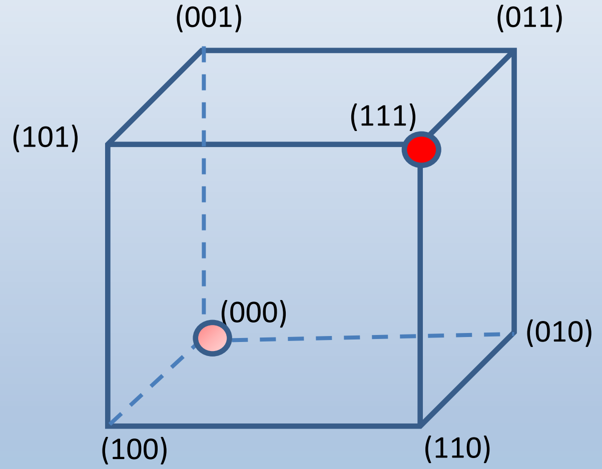
Post-Quantum Cryptography (PQC)

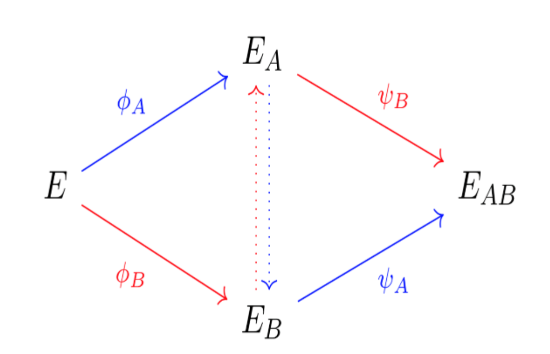
Some actively researched PQC categories

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









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

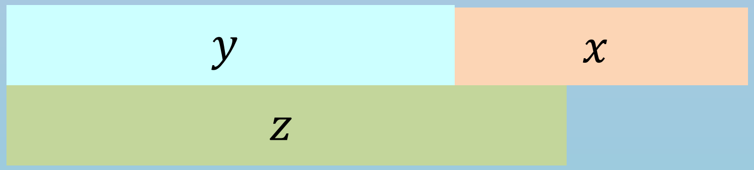
When should we get ready?

NIST Plan

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

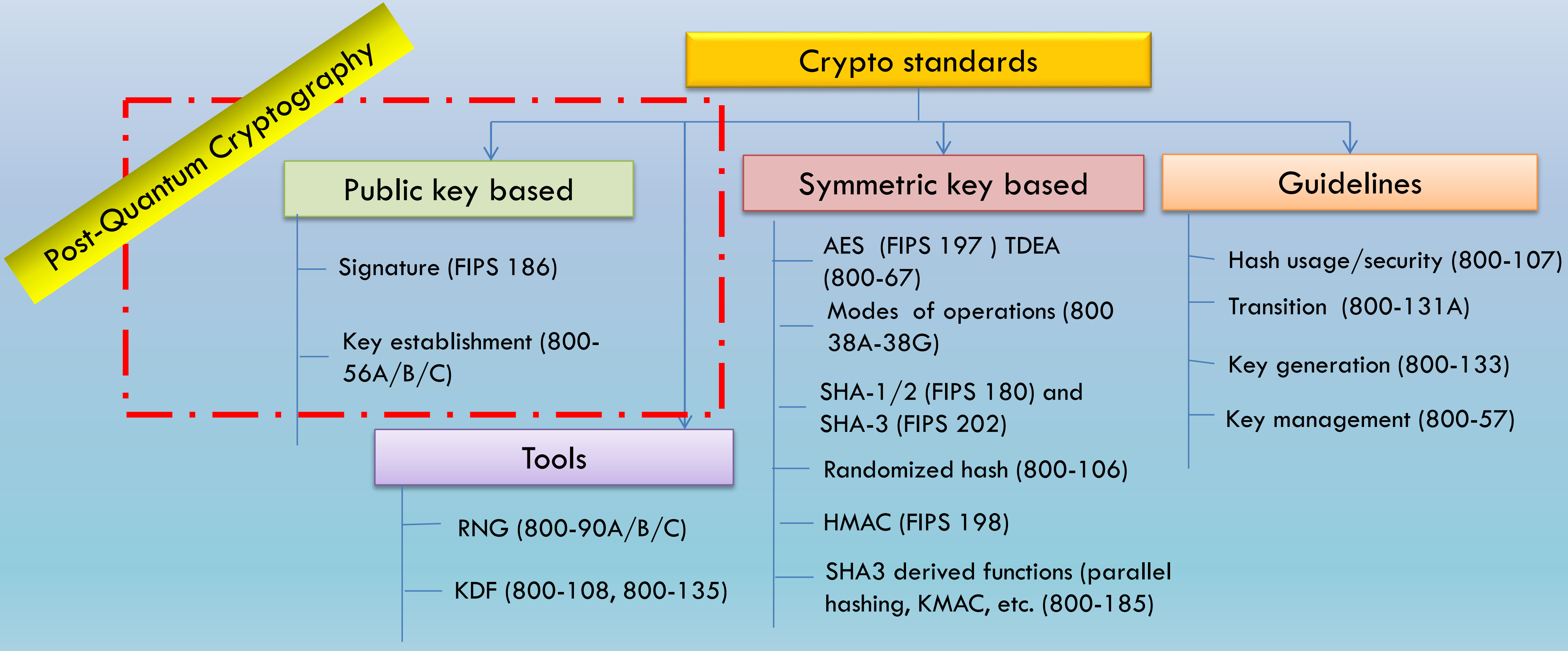
What is z?

- **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/

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

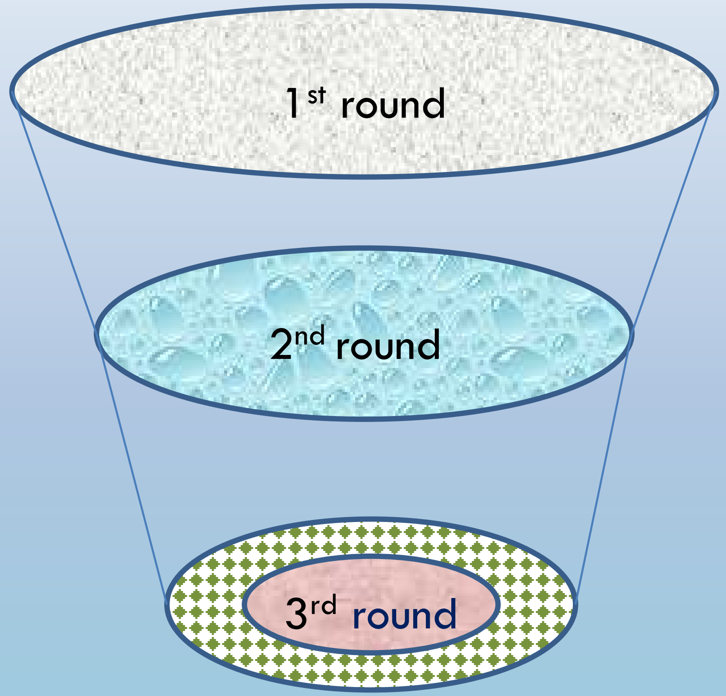
2019

Announced 26 2nd round candidates

Held the 2nd NIST PQC Standardization Conference

2020

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



Migration strategies

Understand product cycle and plan ahead

- Make algorithm change into a phased schedule
- Plan for next generation of hardware cryptographic libraries and accelerators

Obtain firsthand experience through prototype

- See how they work on different platforms
- Understand implementation costs and required areas, power consumption, etc.

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.

Timeline, resource, and contact information

Hold the 3rd NIST PQC Standardization Conference in spring 2021

Release draft standards in 2022-2023 for public comments

We hope to heard from hardwre community

- 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