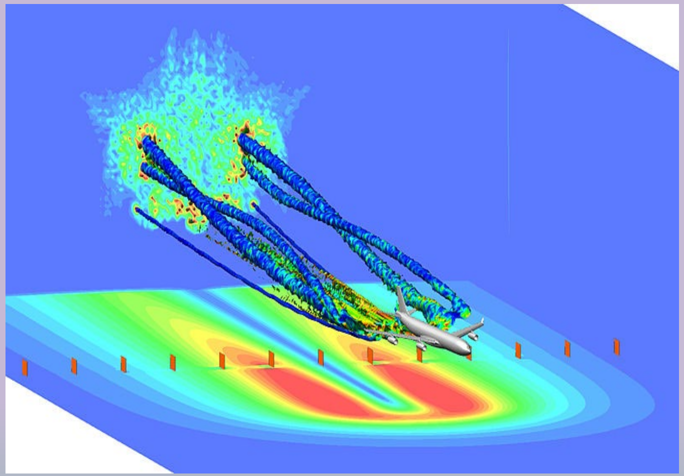
Quantum and Cryptography

— NIST Effort on PQC Standardization

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

Quantum Computers – New Paradigm

Design new materials and drugs



Simulation and data processing

Sensing and measuring

- Known to solve many problems previously thought to be intractable

Quantum Impact

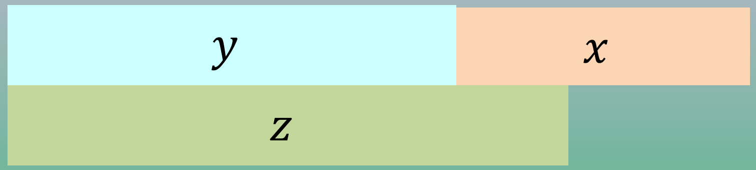
- Emerging quantum computers changed what we believed about the hardness of discrete log and factorization problems
  - Using quantum computers, an integer *n* can be factored in polynomial time using Shor's algorithm
  - The discrete logarithm problem can also be solved by Shor’s algorithm in polynomial time
- As a result, the public key cryptosystems deployed since the 1980s will need to be replaced
  - RSA signatures, DSA and ECDSA (FIPS 186-4)
  - Diffie-Hellman Key Agreement over finite fields and elliptic curves(NIST SP 800-56A)
  - RSA encryption (NIST SP 800-56B)
- We have to look for quantum-resistant counterparts for these cryptosystems
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms
  - Grover’s algorithm can find AES key with approximately $\sqrt{2^n}$ operations where n is the key length
  - Intuitively, we should double the key length, if 2^{64} quantum operations cost about the same as 2^{64} classical operations
    - Based on current understanding about the cost of Grover’s attack, we will probably not need such a large key length increase in practice

Why we need to develop PQC standards now?

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

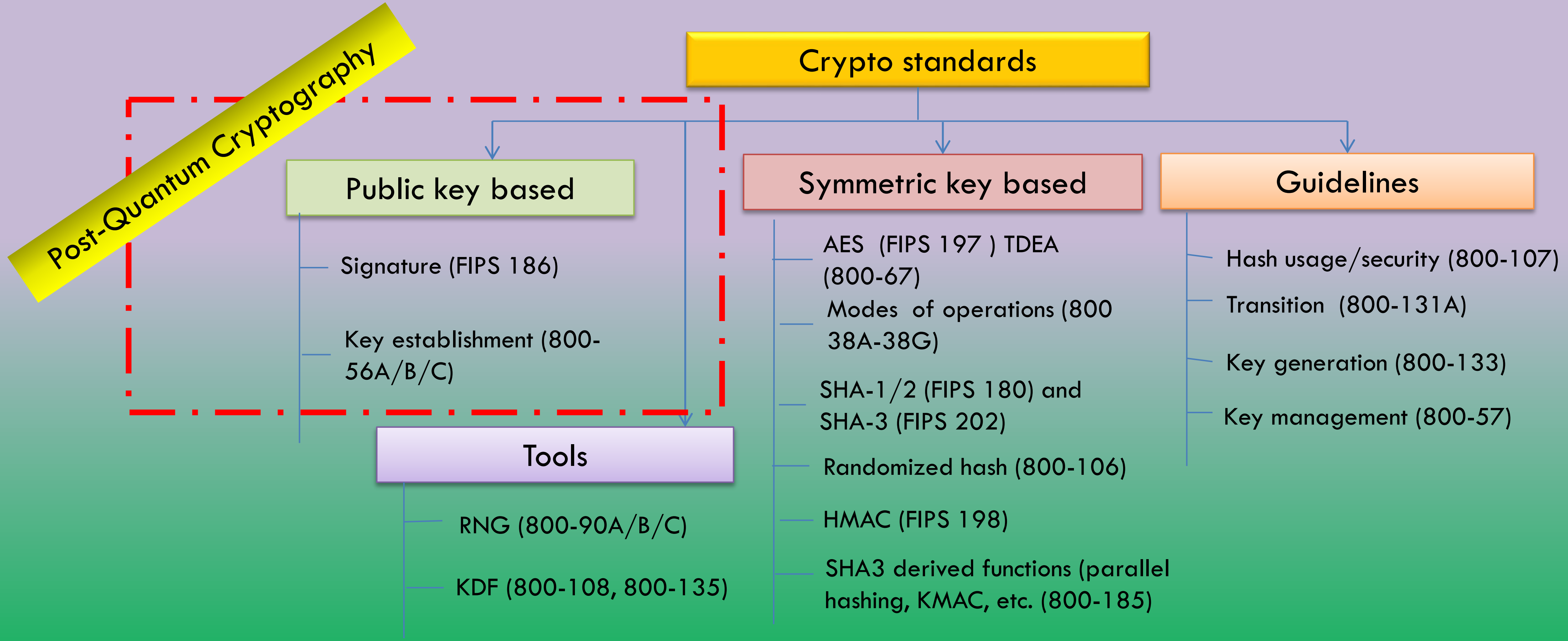
What is z?

- **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



Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC)

QKD uses quantum technology to distribute cryptographic keys

- Theoretically unconditional security guaranteed by the laws of physics if used as one-time pad
- Practically, it cannot be used as one-time pad because the data rate in real communication is much higher than what the QKD can achieve

Limitations of QKD

- Can do encryption, but not authentication
- Quantum networks are not very scalable
- Transmission distance is limited and need trusted relay
- Expensive and need special hardware

Security of PQC is based on hard mathematics problems, hard for classical and quantum computers

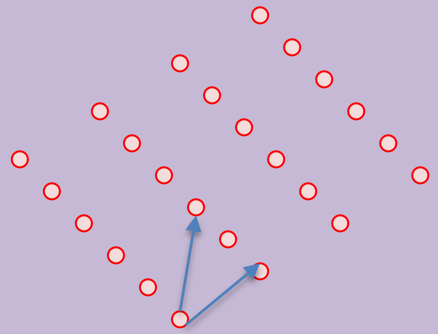
- It works in the same way as the current well deployed cryptographic mechanisms in the Internet and other applications

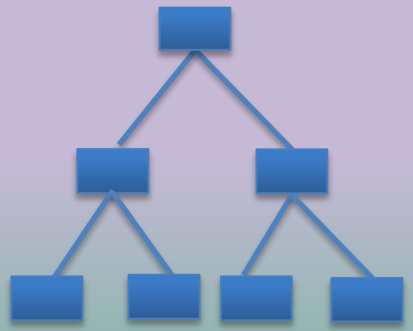
Post-Quantum Cryptography (PQC)

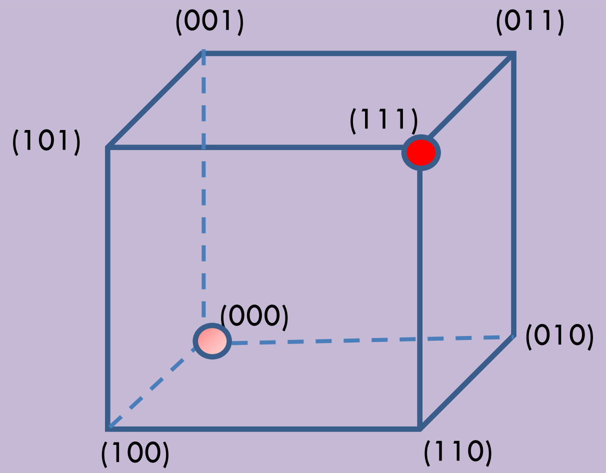
Some actively researched PQC categories

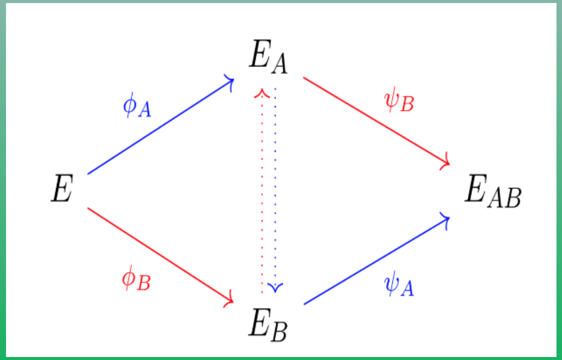
- Lattice-based
- Code-based
- Multivariate
- Hash/Symmetric key based signatures
- Isogeny-based schemes

NIST team has started conducting research on PQC since 2011









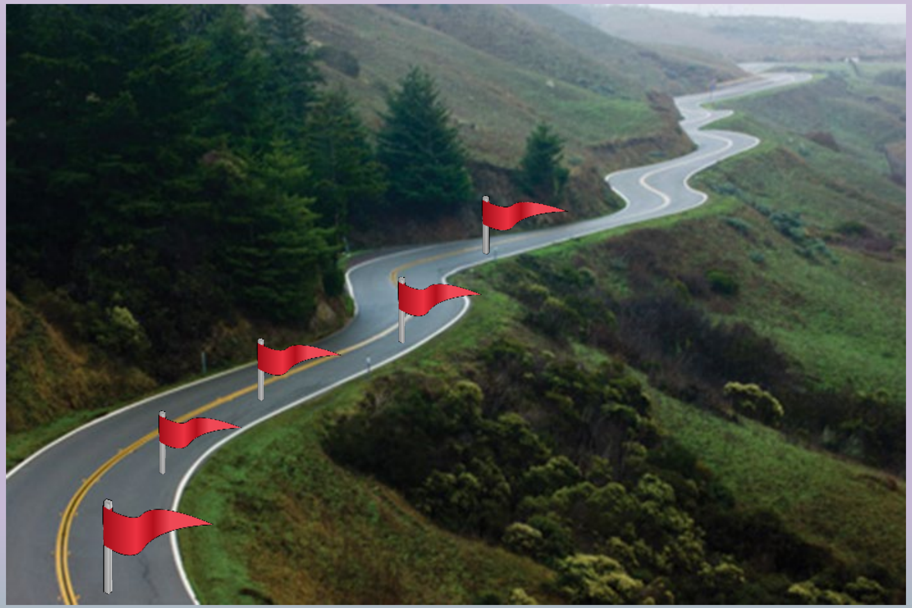
$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

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

$$\vdots$$

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

NIST PQC Milestones and Timelines



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

2021

Hold the 3rd NIST PQC Standardization Conference

2022-2023

Release draft standards and call for public comments

Summary

- Quantum computers, when available, will break the well deployed public-key cryptography in Internet and other applications
- Quantum resistant cryptography (a.k.a. post-quantum cryptography) is needed to provide cybersecurity in quantum time
- NIST has led a process to select and develop PQC standards since 2016
- It is planned to release draft standards in 2022-2023