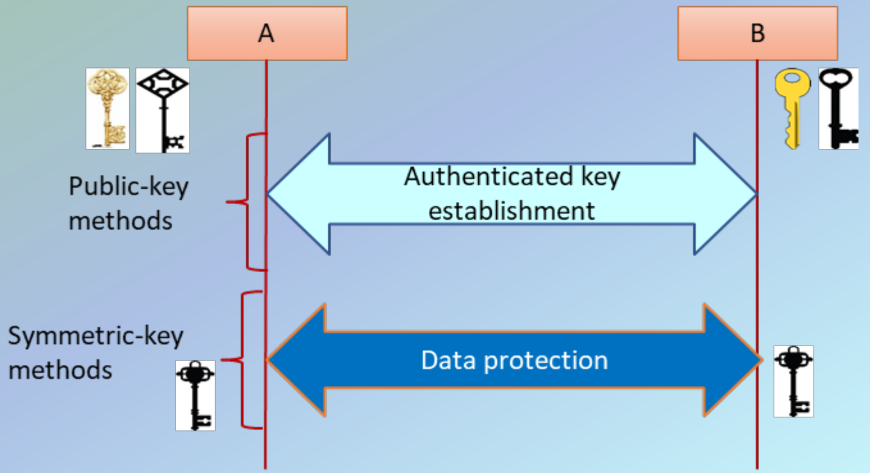
NIST Post-Quantum Cryptography Standardization

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

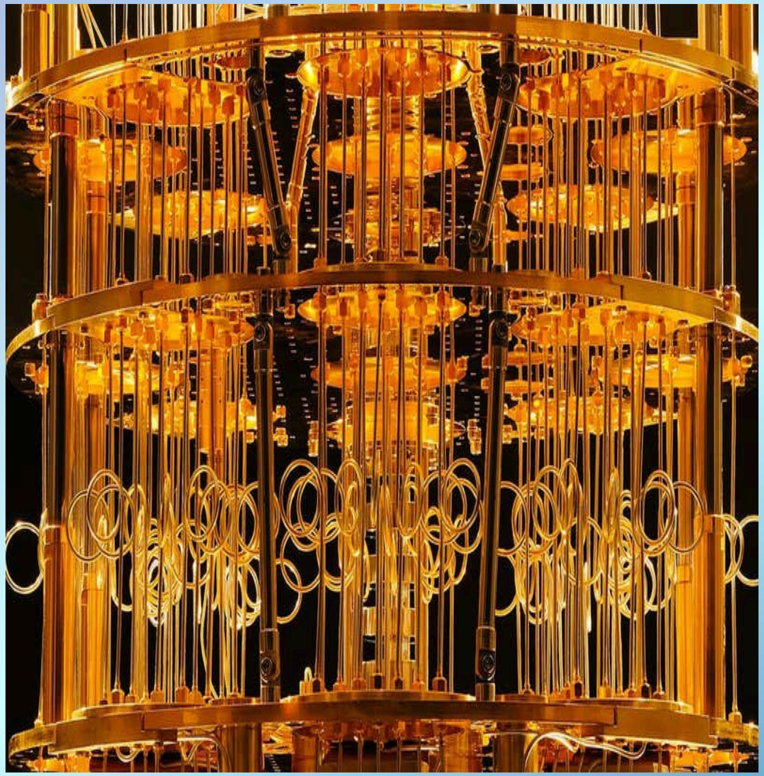
Cryptography – The Cornerstone of Cybersecurity

- Protect information transmitted over the links and stored in the devices
- Prevent from malware and malicious software attacks



Quantum Impact to Cybersecurity

- The security of public-key cryptography is based on hard problem assumptions, e.g., integer factorization for RSA
- Quantum computing changed what we have believed about the hardness
  - By Shor's algorithm, factorization problem can be solved by quantum computers in polynomial time
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms – manageable by increasing key size

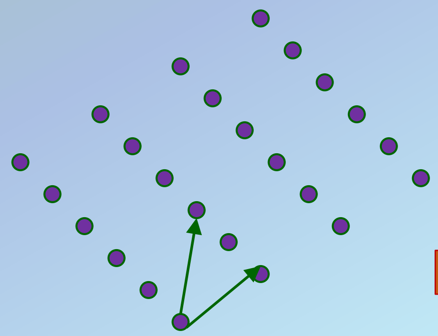


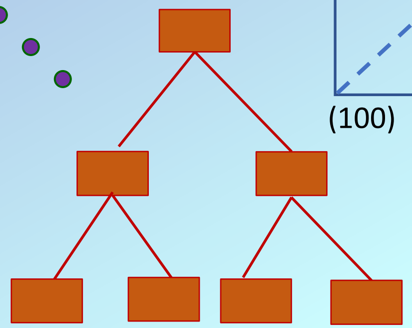
How to Deal with Quantum Attacks?

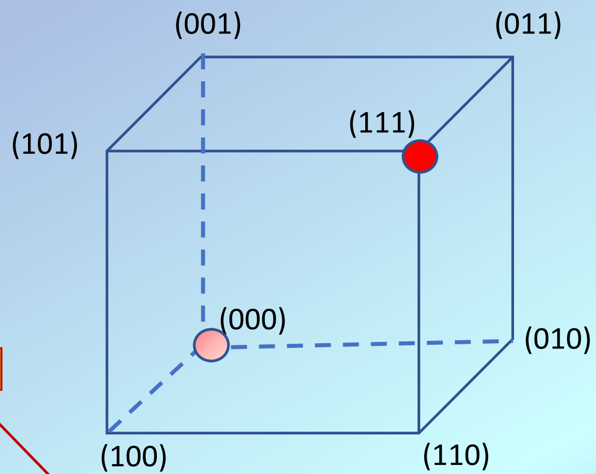
- Need to find cryptographic algorithms which are secure against attacks by both classical and quantum computers
  - The algorithms must be based on hard problems which are hard for both classical and quantum computers
- In other words, we need quantum resistant cryptography, named by the researchers as post-quantum cryptography (PQC)
- Clarification
  - Post-quantum cryptographic algorithms are supposed to be implemented in "classical" computers in the same way as RSA
  - It is different from Quantum Key Distribution (QKD), which relies on quantum mechanics to distribute keys

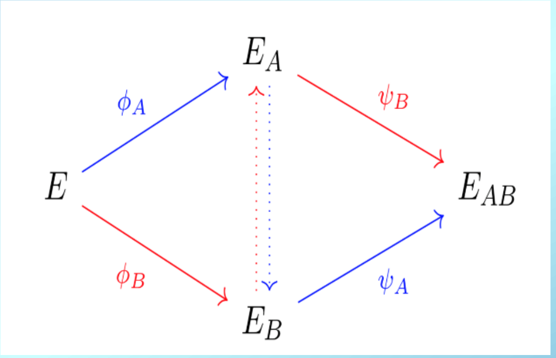
Post Quantum Cryptography (PQC)

- PQC has been a very active research area in the past decade
- Some actively researched PQC categories include
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key -based signatures
  - Isogeny-based schemes









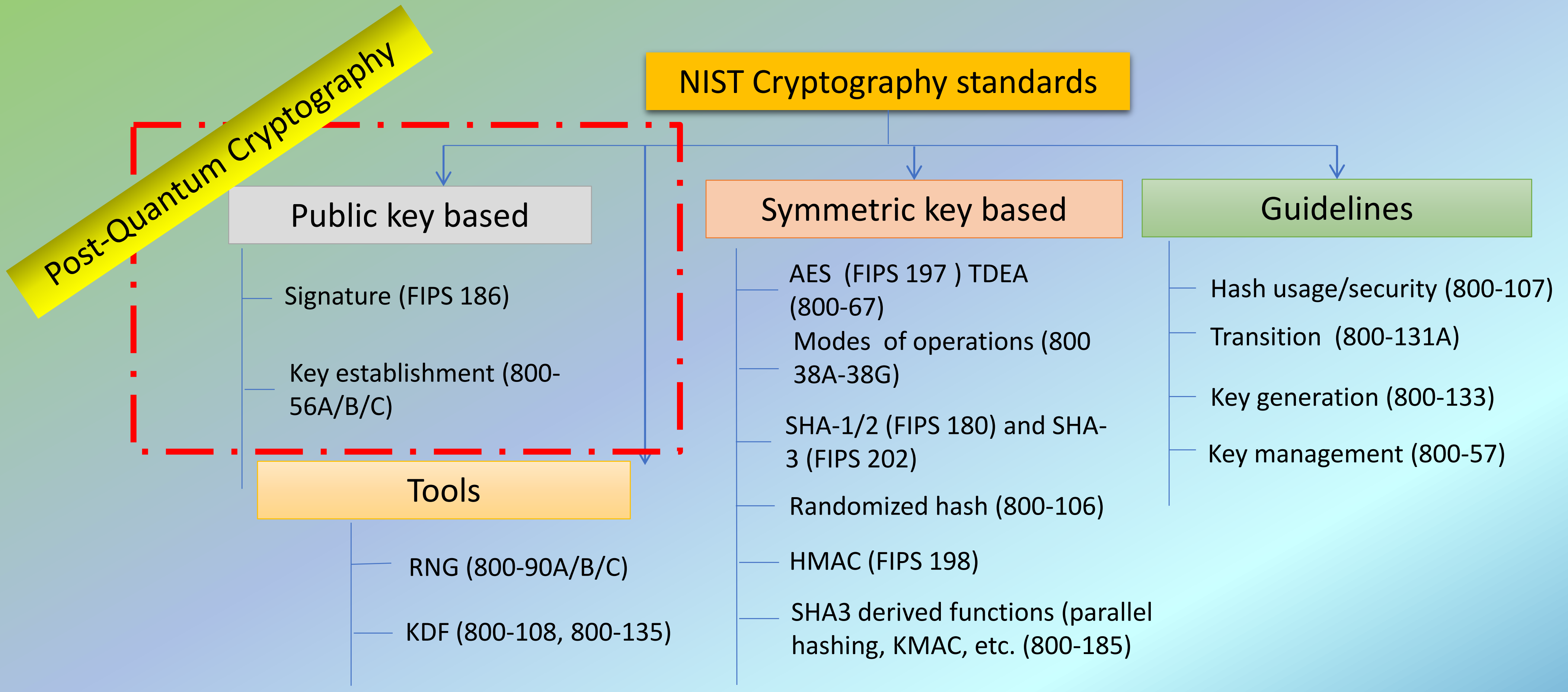
$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

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

$$\vdots$$

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

NIST PQC Standards - Scope



NIST PQC Standards – Milestones and Timeline

2016 Criteria and requirements and call for proposals

2017 Received 82 submissions and announced 69 1st round candidates

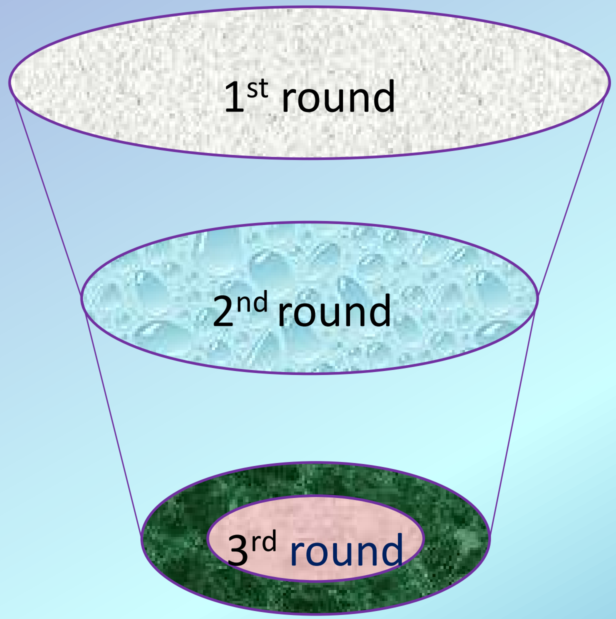
2018 The 1st NIST PQC standardization Conference

2019
Announced 26 2nd round candidates

The 2nd NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidate

2021
The 3rd NIST PQC Standardization Conference



2022-2023 Release draft standards and call for public comments

2024 Publish PQC Standards

Transition to PQC

- Quantum computers, once in a full scale, will crash cryptographic schemes used today, reveal yesterday's secret, and attack tomorrow's transaction
  - PQC is the cornerstone of cybersecurity in quantum time
- PQC standardization and migration are in a pipeline
  - Standardization: NIST PQC standardization process www.nist.gov/pqcrypto
  - Migration and adoption: The National Cybersecurity Center of Excellence (NCCoE) has a project for Migration to PQC to support a head start on executing migration roadmap in collaboration with industry partners
- The clock is ticking – We need to be well prepared before full scale quantum computers become available