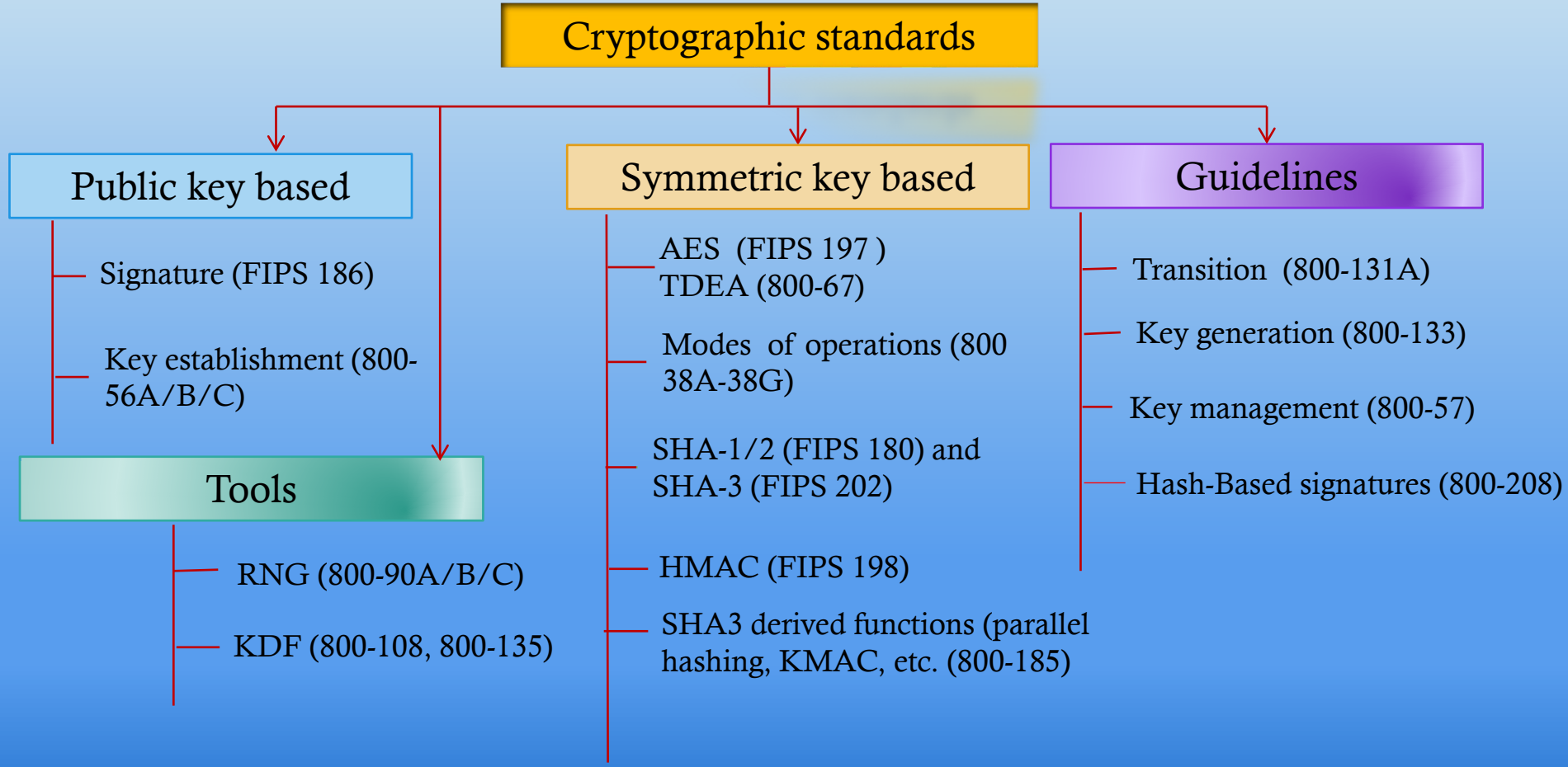
Update on PQC and Cryptographic Transitions

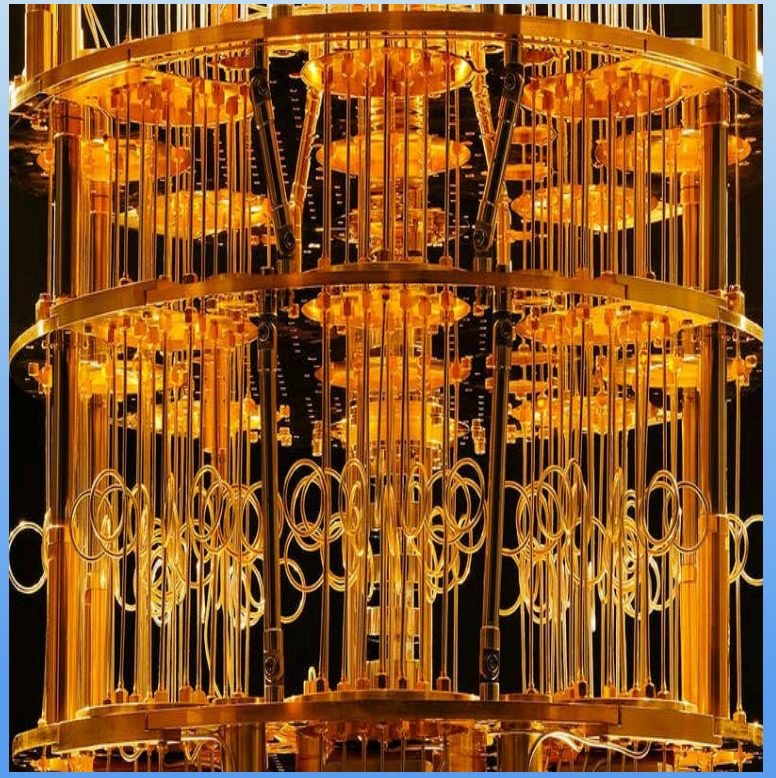
Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

NIST Cryptographic Standards



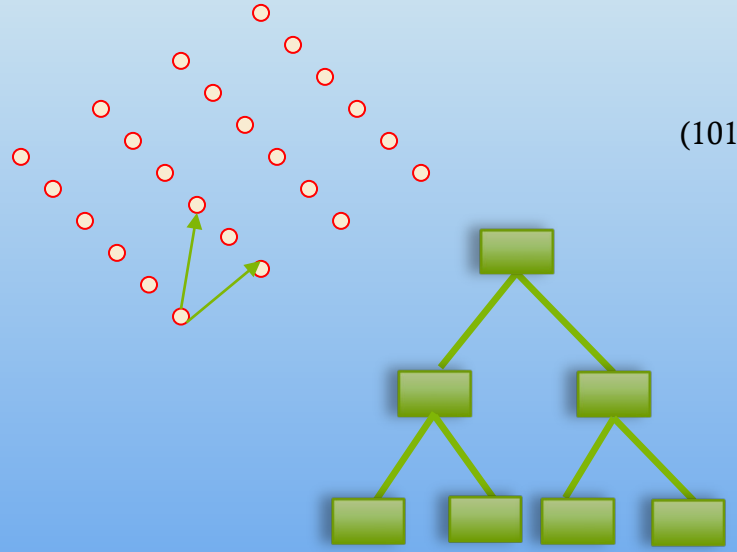
Quantum Impact

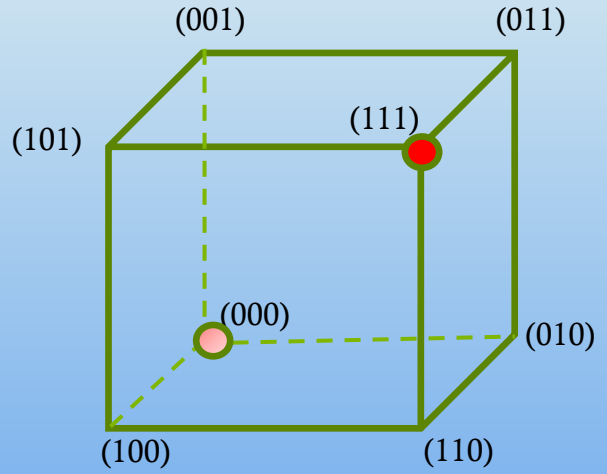
- Quantum computing changed what we have believed about the hardness of discrete log and factorization problems
  - By Shor's algorithm, they can be solved by quantum computers in polynomial time
- The well-deployed public - key cryptosystems, RSA, Diffie-Hellman, ECDSA, will need to be replaced to prepare for quantum era
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms – manageable by increasing key size

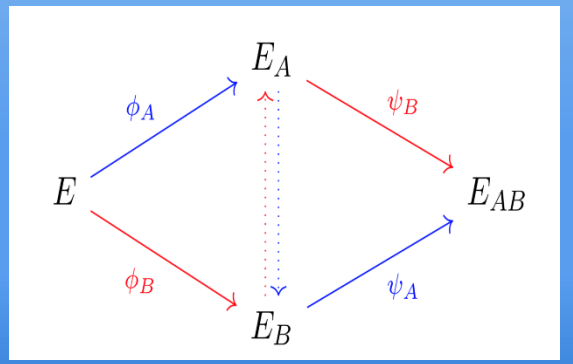


Post-Quantum Cryptography (PQC)

- Some actively researched PQC categories
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key -based signatures
  - Isogeny-based schemes







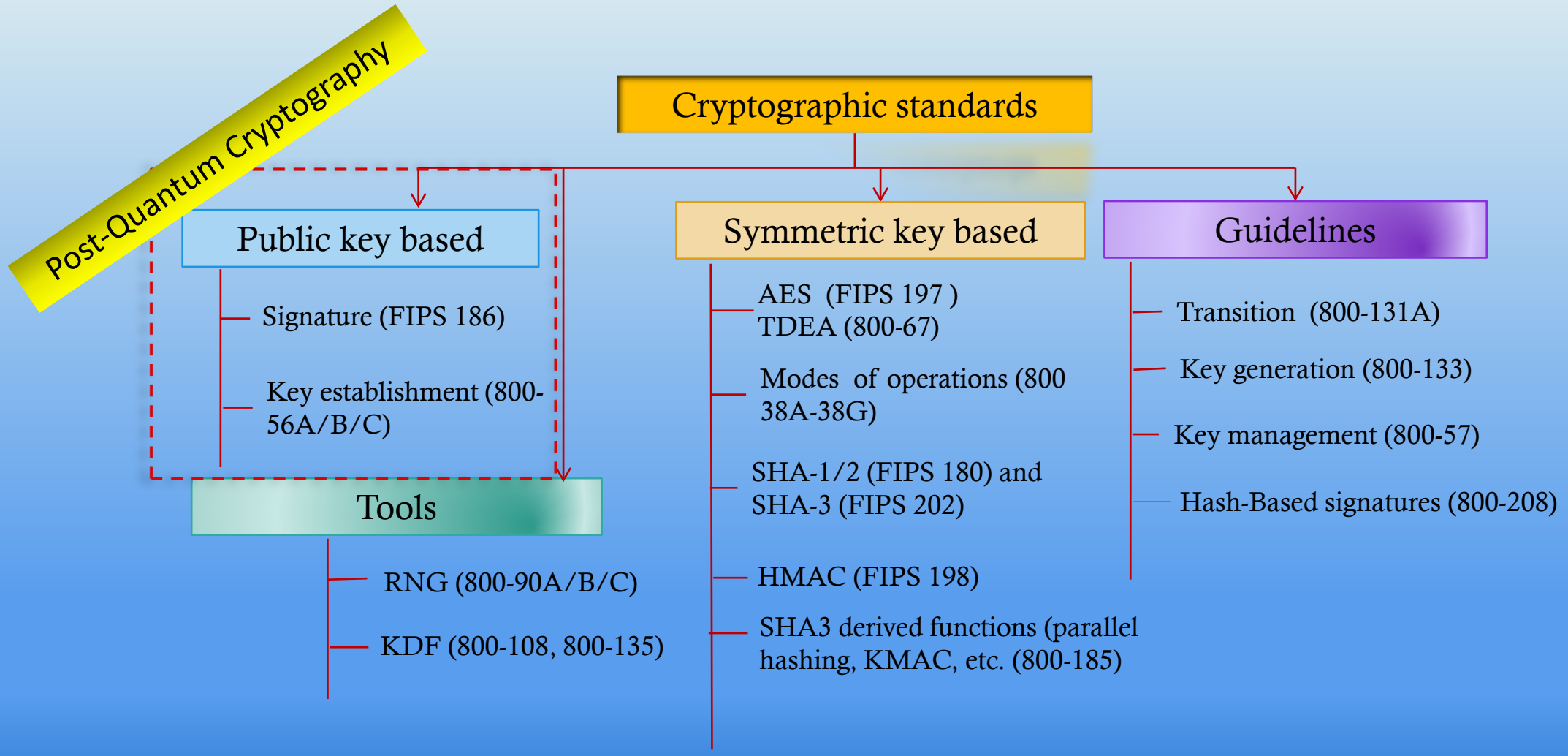
$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

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

$$\vdots$$

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

NIST PQC Standards - Scope



NIST PQC Process Update: Milestones and Timeline

- **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** Held the 3rd NIST PQC Standardization Conference (Virtual)
- **2022** Made the 1st set selection, the 4th NIST PQC standardization conference Nov. 29 – Dec. 1
  - A new call for additional signatures
- **2023** Release draft standards and call for public comments
- **2024** Publish the first set of PQC standards

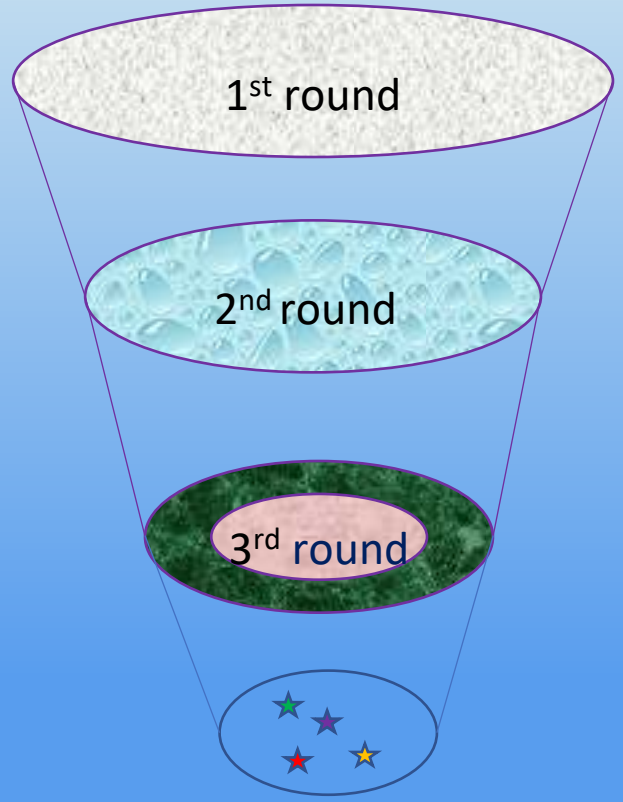
4th round candidates (all KEMs) 18-24 months

- ClassicMcEliece
- BIKE
- HQC
- ~~SIKE~~

The 3rd round selection

- Key Encapsulation Mechanism (KEM)
  - **Crystals-Kyber**: module learning with errors (MLWE)-based
- Signatures
  - **Crystals-Dilithium**: module learning with errors (MLWE)-based
    - Fiat-Shamir signature
  - **Falcon**: based on SIS over NTRU lattices
    - Hash and sign
  - **SPHINCS+**: Stateless hash-based signature

    (Stateful hash-based signatures are specified in SP 800-208)



The 4th round candidates

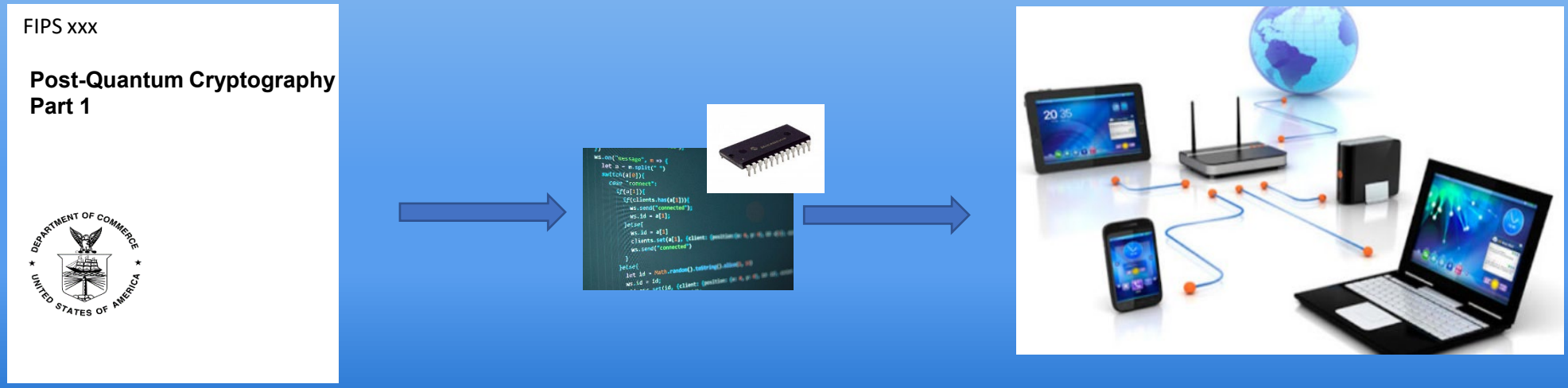
- Key Encapsulation Mechanism (KEM)
  - **ClassicMcEliece**: Code-based, original design was proposed in 1978, very large public-key and small ciphertext
    - Confident about the security. Very large PK may be a problem for common usage
  - **BIKE**: based on binary linear quasi-cyclic moderate density parity check (QC-MDPC) codes
    - The most competitive performance among the non-lattice-based KEMs
  - **HQC**: based on QC-MDPC codes
    - Strong security assurances and a mature decryption failure rate analysis
  - ~~**SIKE**:~~ based on isogenies of elliptic curves
    - SIKE is broken!
    - Isogeny-based category is relatively new but worth to investigate
- NIST intends to select at least one additional KEM for standardization at the end of the fourth round
- The estimated timeframe for the 4th round is 18-24 months

Call for Additional Signatures

- Most interested in a general-purpose digital signature scheme which is not based on structured lattice to diversify the underlying security assumptions
  - Also consider signature schemes targeted for certain applications, e.g., a scheme with very short signatures
  - Look for mature designs, i.e. the more mature the scheme, the better.
  - The deadline is June 1, 2023
  - A different track than the candidates in the 4th round
  - Planned to spend 12-18 months to evaluate the candidates

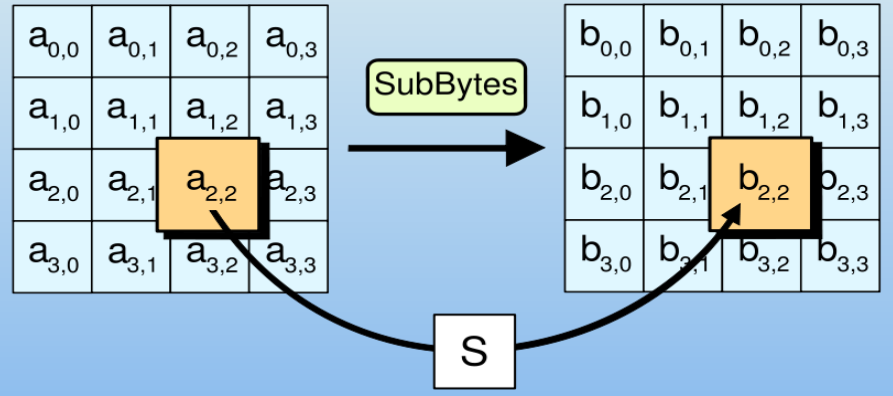
PQC Migration

- NCCoE initiated project partnership for migration to Post-Quantum Cryptography
- Industry participants and other interested parties are invited to participate in the Migration to Post-Quantum Cryptography project
- Work with standards organizations to explore issues, concerns, implementation details in different applications
- Accommodate migration needs, e.g., hybrid KEM and dual signatures



Cryptographic Publication Review

- NIST has about 45+ years of history of publishing cryptographic standards
- It is critical to improve the scientific quality and useability to match advanced technology and meet the requirements of emerging applications
- In NISTIR 7977
  - *"Review standards and guidelines regularly. … FIPS are reviewed at least every five years or more frequently if issues arise."*
- NIST Cryptographic Technology Group established Review Board in 2021
  - Assign internal reviewers, solicit public comments, and propose review decisions
- Completed 4 publication reviews
- 8 publications are under review



- AES has published for 20 years!
- The 1st round of public comments (May 10, 2021 – June 11, 2021)
- NISTIR 8319 Review of the Advanced Encryption Standard (July 2021)
  - A list of proposed changes

Cryptographic Transition

- Transition to stronger cryptography is constantly required because
  - Increased computing power by Moore's Law
  - New computing technologies such as quantum computers
  - More sophisticated cryptoanalysis techniques
- NIST has guided many transitions (see SP 800-131A), e.g.
  - Block ciphers: DES → Triple DES → AES
  - Hash functions: SHA-1 → SHA-2 and SHA-3 families
  - RSA signature and encryption: modulus 1024 bits → ≥ 2048 bits (80 bit to minimum 112-bit security)
- Technology advanced and new trends emerged, e.g.,
  - Using authenticated encryption, instead of encryption only modes
- Work with application community for interoperability and backward compatibility

- After 2023 (SP 800-131A Rev. 2)
  - Disallow 3key triple DES (SP 800-67)
  - Disallow PKCS1-v1_5 padding for RSA encryption (SP 800-56B)

Thanks!

Questions?

lily.chen@nist.gov