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

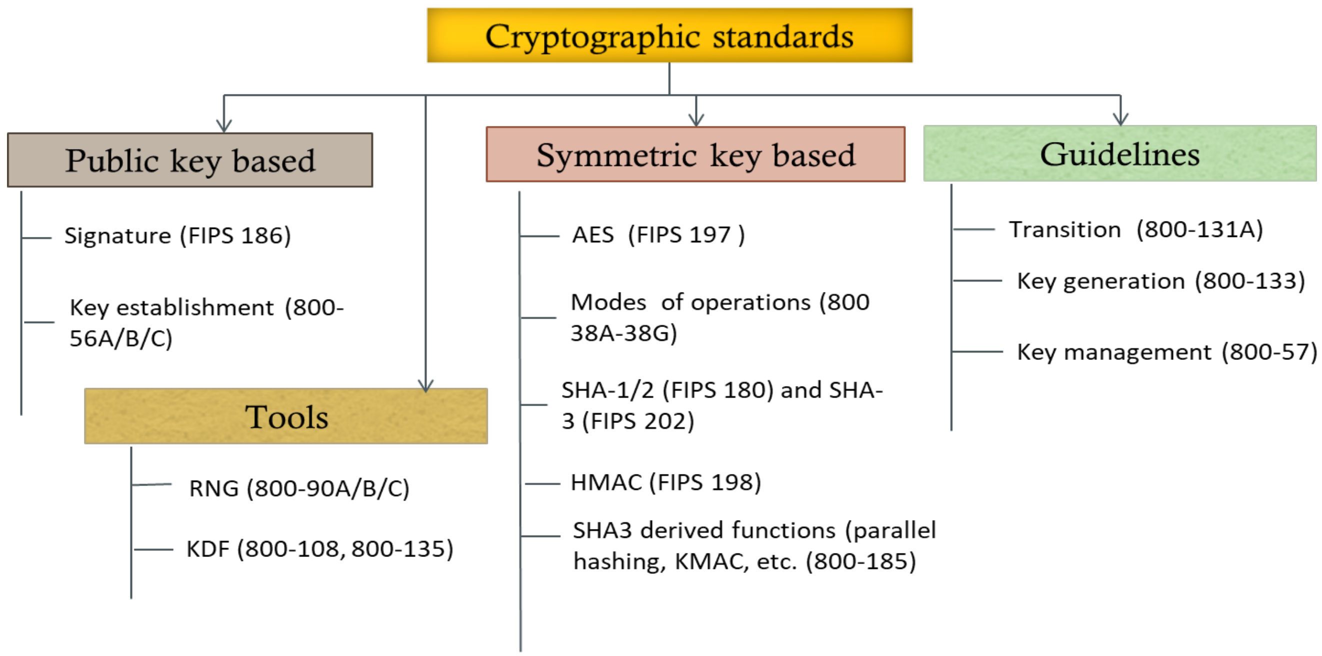
Post-Quantum Cryptography Standards

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

NIST Cryptographic Standards

- NIST developed the first encryption standards in 1970s
  - Data Encryption Standard (DES), published 1977 as Federal Information Processing Standard (FIPS) 46
- Over 40 years, NIST continues to evolve its cryptographic standards
  - Enable to secure the emerging applications – Internet, digital communications, open platform, etc.
  - Enhance security strength to against more sophisticated attacks

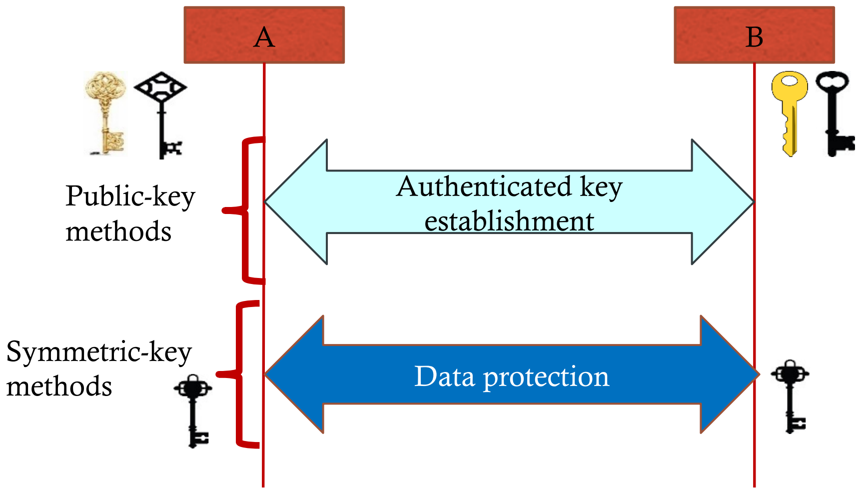
- Nearly all commercial laptops, cellphones, Internet routes, VPN servers, and ATMs use NIST Cryptography



Cryptography for Secure Communications

NIST

- Use public key cryptography to establish keys and authenticate users through signatures
  - (EC) Diffie-Hellman Key Exchange
  - RSA and ECDSA signatures
- Use symmetric key cryptography to encrypt and authenticate bulk data
  - AES (CCM, GCM, etc.)
  - HMAC (SHA-2, SHA-3)

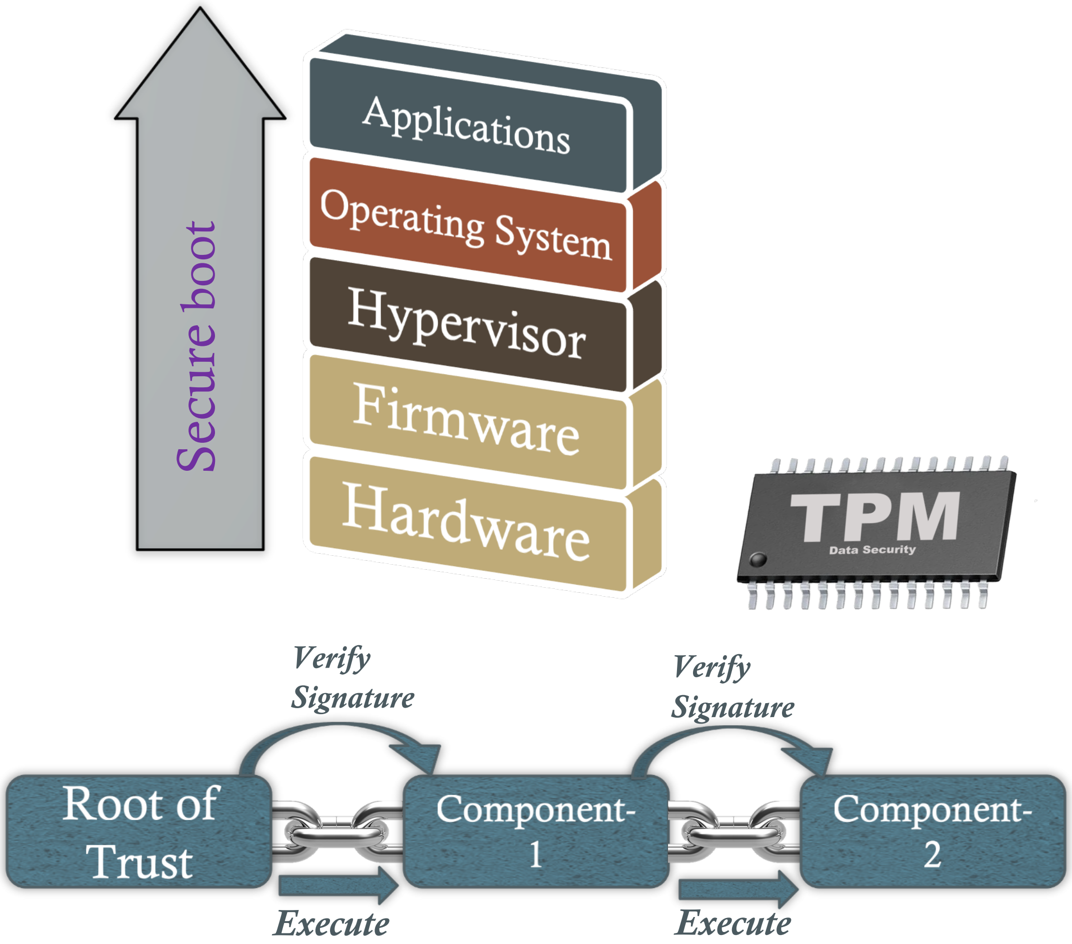


- Examples
  - Transport Layer Security (TLS)
  - Internet Key Exchange (IKE) + IPsec

Cryptography for Trusted Platform

NIST

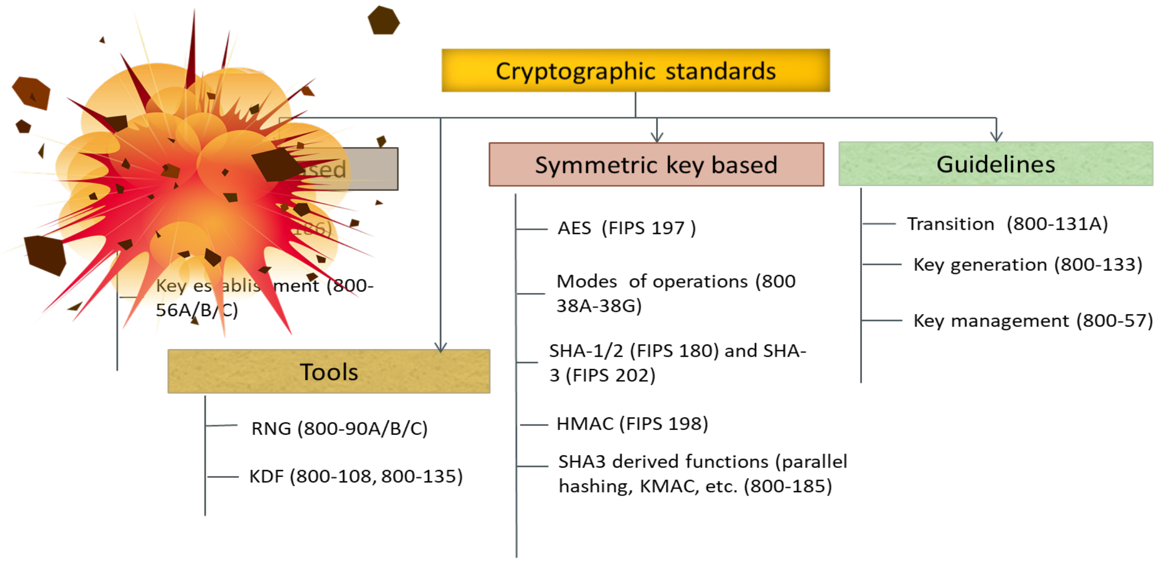
- Today's digital devices adopt open-platforms and allow constant update and installation
- Public-key based digital signatures are used for establishing trusted platform – root of trust and code signing-protect devices from malware
- Symmetric-key algorithms are used to protect data stored in the devices



Quantum Impact to Cybersecurity

- 1994, Peter Shor created a quantum algorithm giving an exponential speed up over classical computers on
  - Factoring large integers
  - Finding discrete logarithms

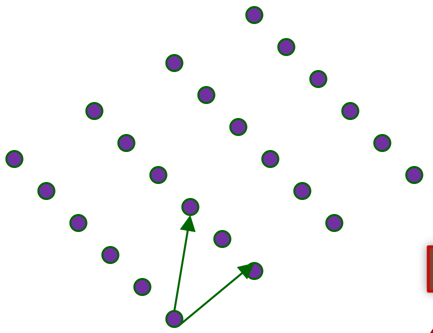
- The well-deployed public - key cryptosystems, RSA, Diffie-Hellman, ECC, will need to be replaced to prepare for quantum era

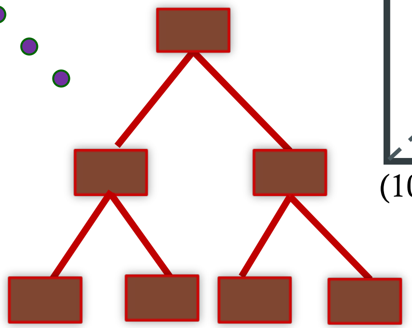


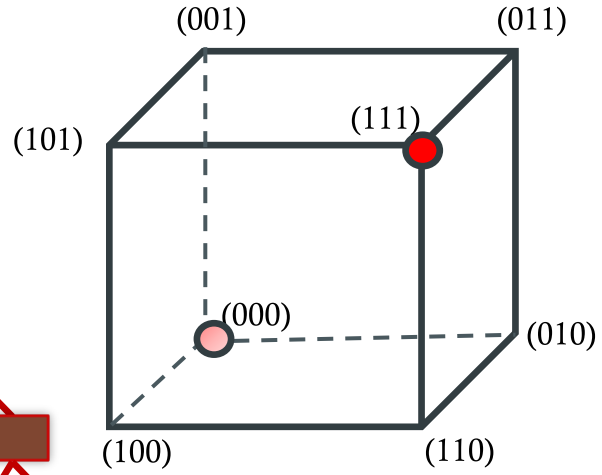
- Grover's algorithm (1996) – polynomial speed-up in unstructured search, from $O(N)$ to $O(\sqrt{N})$, e.g. AES 128 from 2^{128} to 2^{64}.
- Quantum computing impact on security of symmetric-key based cryptography algorithms is manageable by increasing key size

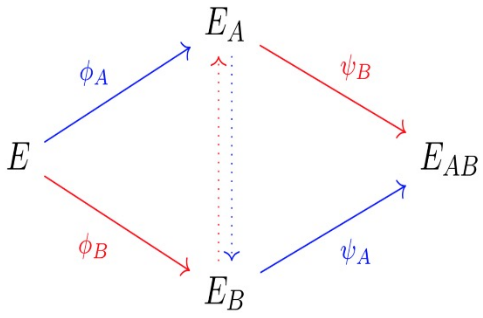
Post Quantum Cryptography (PQC)

- PQC has been a very active research area in the past two decades
- Some actively researched PQC categories include
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key-based signatures
  - Elliptic curve isogeny-based









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

NIST PQC Standards – 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 Announced the 3rd round selection and the 4th round candidates, the 4th NIST PQC conference

2023 Released draft standards for public comments

5th NIST PQC standardization conference (April 10-12)

2024 Publish the 1st set of PQC standards (summer)

2022 Called for additional signatures

2023 Received 50 signature submissions and 40 of them were selected as the first-round candidates

- The Fifth NIST PQC Standardization Conference
- April 10-12, 2024
- Rockville, MD, In-person only
- Register before April 3, 2024!

Current Status

Approved

- SP 800-208 Stateful Hash-Based Signature (LMS, XMSS)

*not in submissions but based on IETF work

Selected Algorithms and Draft FIPS

Will be published in 2024

- Draft FIPS 203 "Module-Lattice-base… Encapsulation Mechanism Standa… …EM) (CRYSTALS-Kyber)
- Draft FIPS 204 "Module-… …ased Digital Signature Standard" (… (CRYSTALS-Dilithium)
- Draft FIPS 205 "… Hash-Based Digital Signature Sta… (SLH-DSA) (SPHINCS+)
- FALCON … signature based on structured lattices) Will … …ied in Draft FIPS 206, expected to be re… …n late 2024

The 4th round

Will be selected in 2024

Continue to evaluate … …alysis the candidates, expect to make s… …n in later 2024

- Classic M…
- BIKE
- HQ…

Onramp signatures

Will be narrowed down in 2024

- NIST is primarily interested in ad… general-purpose signature schemes that are n… on structured lattices
- NIST may also be inte… signature schemes that have short signatu… …ast verification
- Any lattice sign… …uld need to significantly outperform … …cted ones
- Among … …ubmissions, 40 of them are selected as the … …d candidates

Challenges and Actions

NIST

- Billions of electronic digital devices use public key cryptography schemes such as RSA and ECC to protect communications and device integrity
  - Transition and migration must take place as soon as possible to prevent from "capturing now and decrypting later", because some data must be protected for many years
  - It takes time to make transition in the product and introduce PQC to infrastructure
- Standards organizations and industry consortia take actions in preparing the transition
  - Discuss crypto-agility in communication protocols, software libraries, API, hardware, etc. through workshops and conferences
  - Introduce PQC to Internet protocols and public key infrastructure in IETF, e.g. exploring hybrid key establishment and dual signatures for certificate
- International Standards organizations such as ISO/IEC JTC1 SC27 initiated projects to standardize post-quantum cryptography

Transition and Migration to PQC

- NIST provided guidance for transition in the past (SP 800-131A)
  - DES → Triple DES →AES
  - SHA1 →SHA2/3
  - …
- NIST will provide PQC transition guidance
- NIST CAVP is actively developing testing for PQC standards for FIPS 140 validation
- National Cybersecurity Center of Excellence (NCCoE) Project for Migration to PQC

Check out www.nist.gov/pqcrypto
Sign up for the pqc-forum for announcements & discussion
Contact us at: pqc-comments@nist.gov

National Security Memorandum 10 on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

Sec. 3. Mitigating the Risks to Encryption. (a) Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a CRQC. To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035.