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

NIST Cryptographic Standards

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

National Institute of Standards and Technology

- Non-regulatory federal agency within U.S. Department of Commerce.
- Founded in 1901, known as the National Bureau of Standards (NBS) prior to 1988.
- Origins in the Constitution: “Congress shall have power to …. fix the standard of weights and measures…”
- Headquarters in Gaithersburg, Maryland, and laboratories in Boulder, Colorado.
- Around 6,000 employees and associates.
- At least 5 Nobel prizes

Mission of NIST Cryptographic Standards

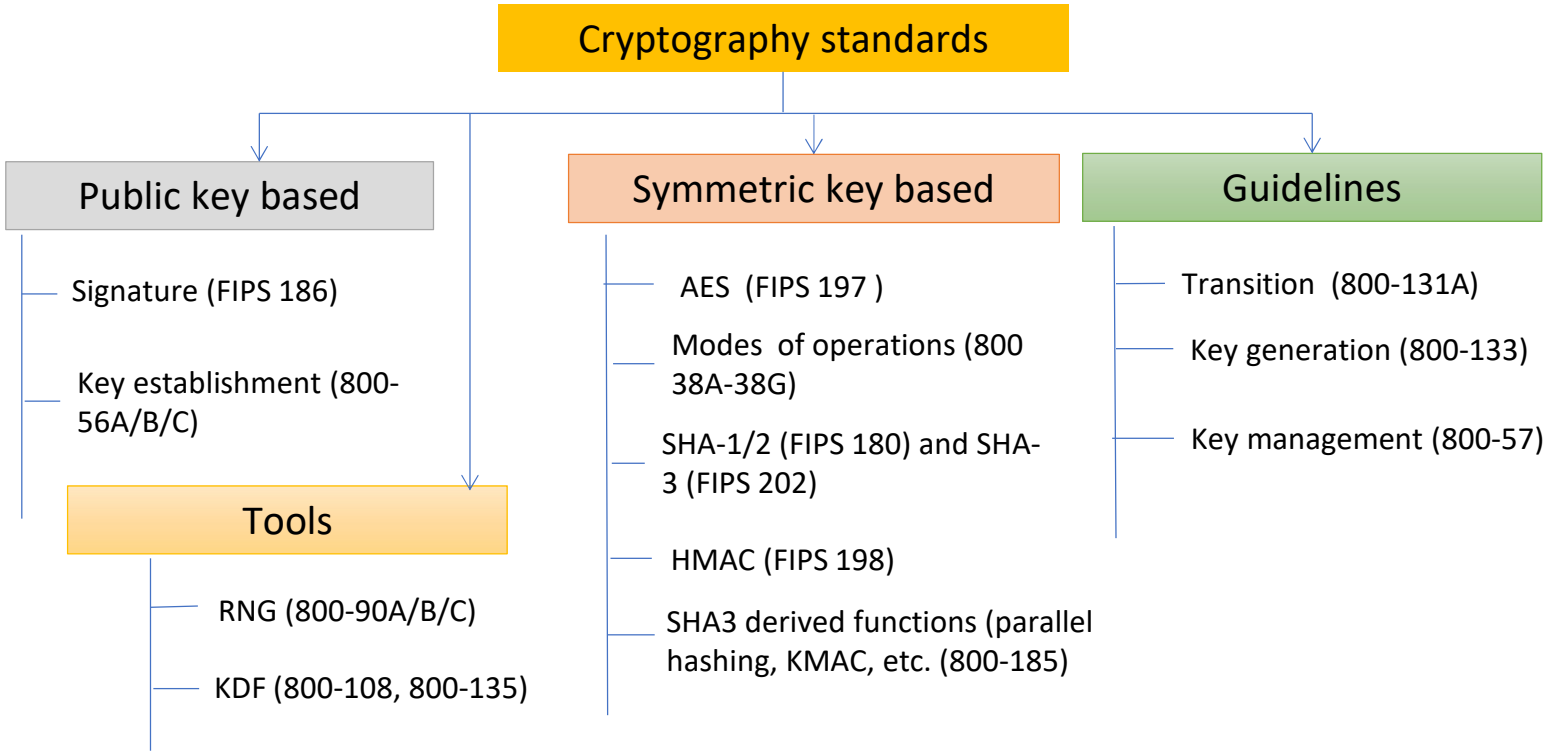
NIST is responsible for developing standards (Federal Information Processing Standards, or “FIPS”) and guidelines to protect non-national security federal information system

Outside the Federal Government, these publications are voluntarily relied upon across many sectors to promote economic development and protect sensitive personal and corporate

NIST Cryptographic Standards Evolution

- NIST developed the first encryption standard 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

Published Standards (Not a complete list)



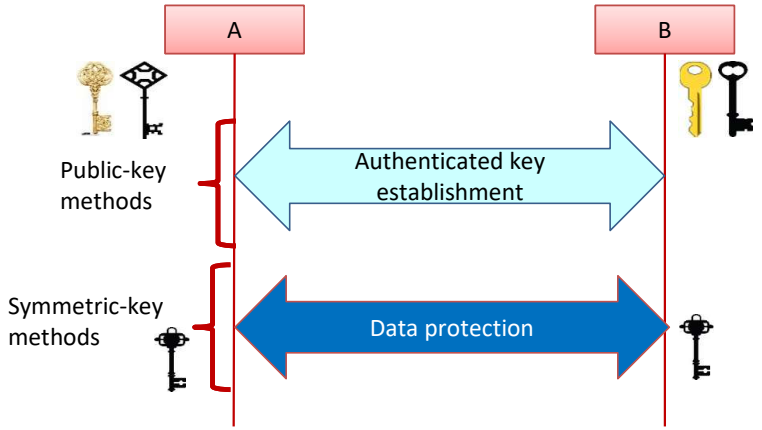
Cryptography for Secure Communications

Use public key cryptography to establish keys and authenticate users through signatures

- Diffie-Hellman Key Exchange
- RSA and ECDSA signatures

Use symmetric key cryptography to encrypt and authenticate bulk data

- AES (CBC, GCM, etc.)
- HMAC (SHA-2, SHA-3)



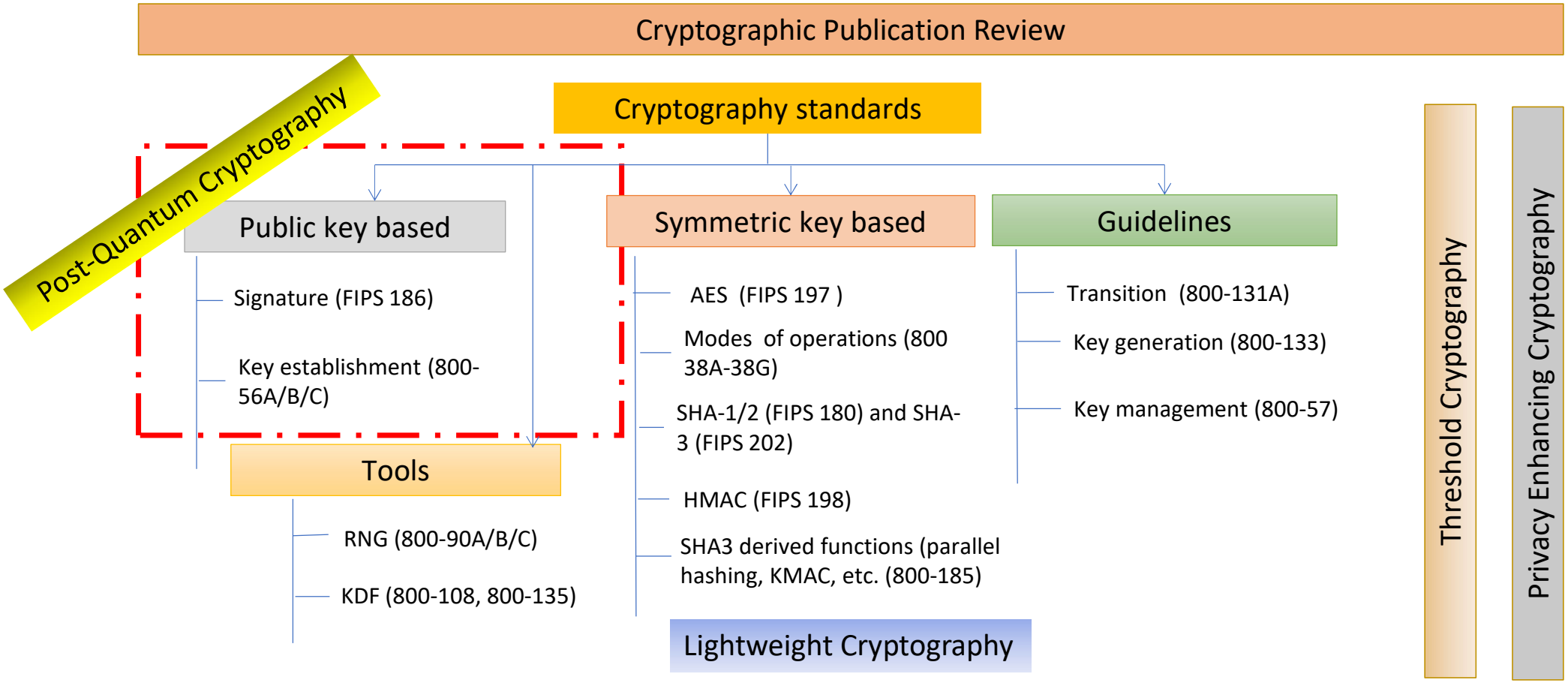
Examples

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

Challenges in 5G and Beyond

- 5G takes advantages of public-key cryptography
  - Cryptographic relevant quantum computers will break well-deployed public key cryptography such as RSA and ECC
- 5G provides connections for Internet of Things (IoT)
  - Cryptographic protection must be applied to constrained implementation environment
- 5G demands interoperability, and backward compatibility
  - Increase key size, length of hash values, etc.
  - Introduce new algorithms in the protocols (e.g., post-quantum cryptography)
- 5G must target on extended security objectives and features
  - Deal with more sophisticated cryptanalysis methods, e.g., side-channel attacks, multiple-key/target attacks, etc.
  - Demand useable features, e.g., misuse resistance
- 5G requires privacy protection for connected user devices
  - User information is transmitted through multiple media formats with different protection levels

New Directions to meet challenges



Post-quantum cryptography

New public-key cryptographic algorithms to resist quantum computers

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

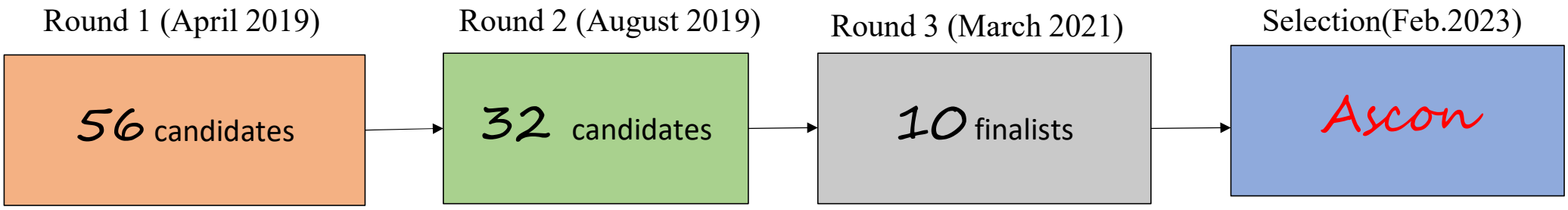
2022 Announced the 3rd round selection and the 4th round candidates + Call for additional signatures

2023 Release draft standards for public comments + Evaluate 4th round and additional signatures

2024 Publish the 1st set of PQC Standards

Lightweight cryptography

- Scope: Authenticated Encryption with Additional Data (AEAD) with optional hashing functionality for constrained implementation environment
- Security analysis and maturity assessment were mainly provided by the design teams and independent third parties
- The performance is evaluated in software and hardware
  - Targeted devices, optimized implementations
  - Hardware benchmarks on different platforms
- Expect to publish the standard in 2023



Standards and validation

Cryptographic Module Validation Program will be introduced in the next presentation