The Cornerstone for Cybersecurity – Cryptographic Standards

Lily Chen

Computer Security Division, Information Technology Lab

National Institute of Standards and Technology (NIST)

History and Fact Sheet

- 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 respond the growing application demand
  - Enhance security strength to against more sophisticated attacks

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

Published Standards

Cryptography standards

Public key based

- Signature (FIPS 186)
- Key establishment (800-56A/B/C)

Tools

- RNG (800-90A/B/C)
- KDF (800-108, 800-135)

Symmetric key based

- AES (FIPS 197) TDEA (800-67)
- Modes of operations (800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- Randomized hash (800-106)
- HMAC (FIPS 198)
- SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)

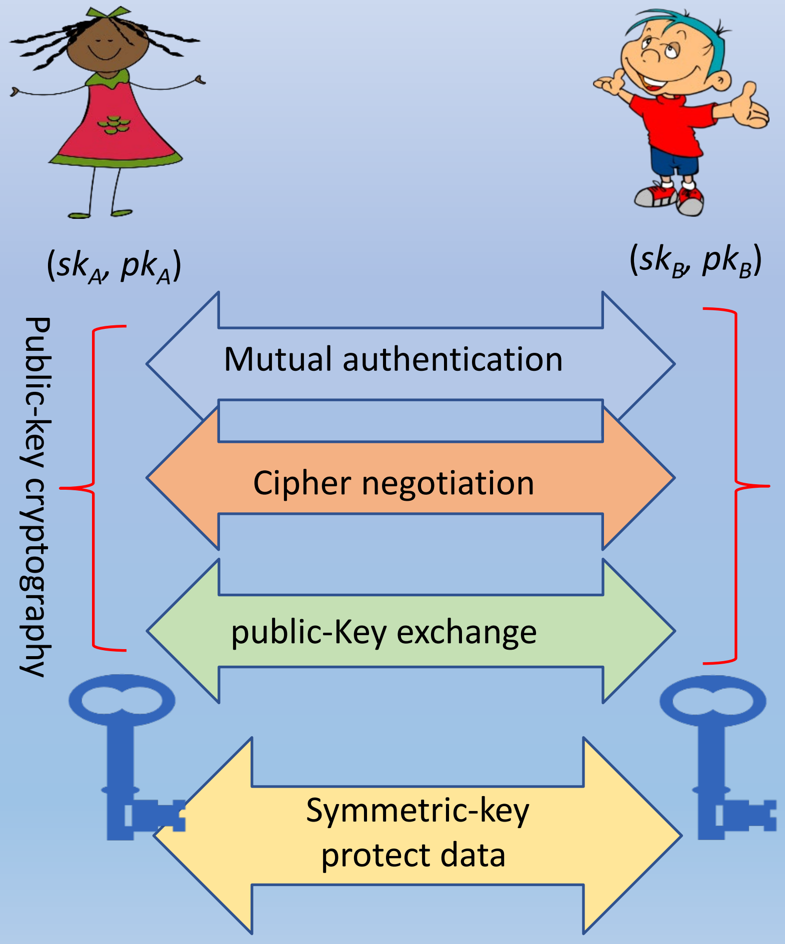
Guidelines

- Hash usage/security (800-107)
- Transition (800-131A)
- Key generation (800-133)
- Key management (800-57)

NIST Cryptographic Standards Approaches

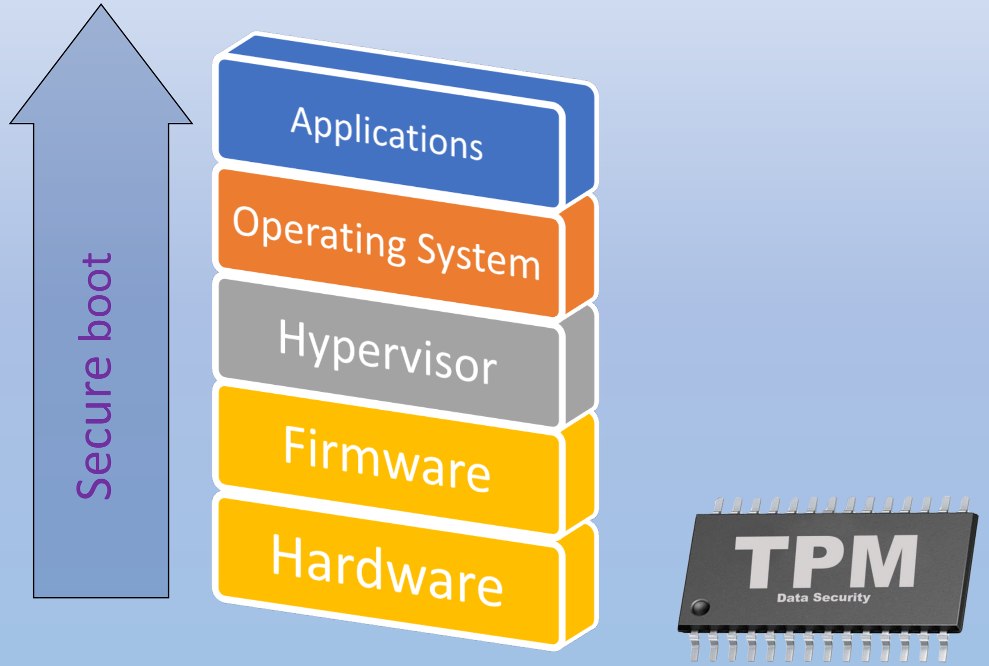
- Cryptographic algorithm competitions (AES, SHA-3)
- Adoption of standards developed in other standards organizations
  - IETF, IEEE, X9F1, etc.
- Develop new standards
  - based on well accepted research results
  - selected among submissions (e.g. modes of operations)

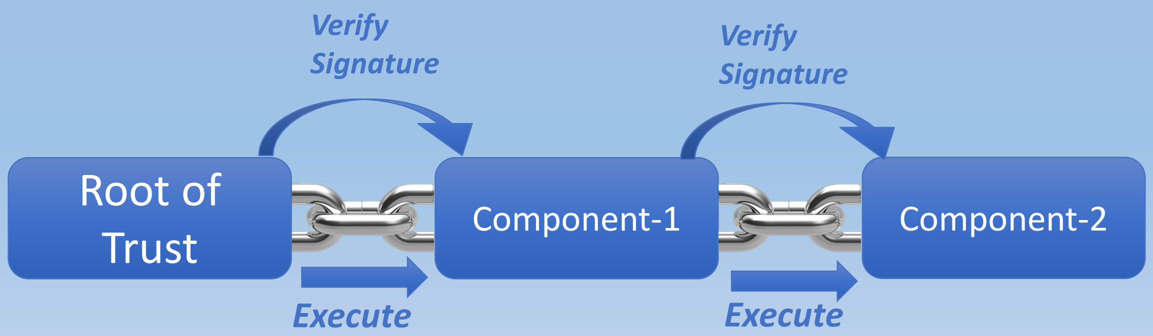
NIST Cryptographic Standards Usage – Over the link



- Public-key cryptography has been used to establish a secure and protected link, e.g.
  - Internet Key Exchange (IKE) Protocol
  - Transport Layer Security (TLS) protocol
- Symmetric-key algorithms are used to protect data, e.g.
  - Advanced Encryption Standard (AES)
  - Keyed Hash Message Authentication Code (HMAC)
  - Authenticated encryption, GCM, CCM, etc.

NIST Cryptographic Standards Usage – Inside the device





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

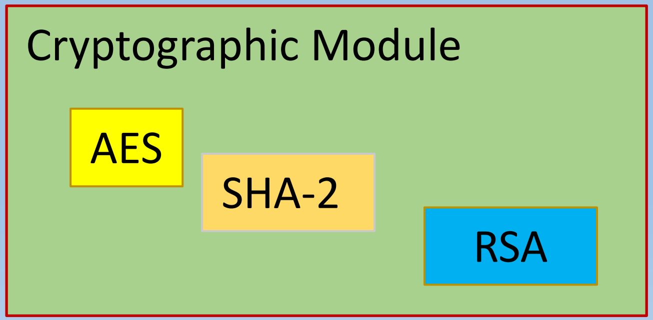
NIST Cryptographic Standards

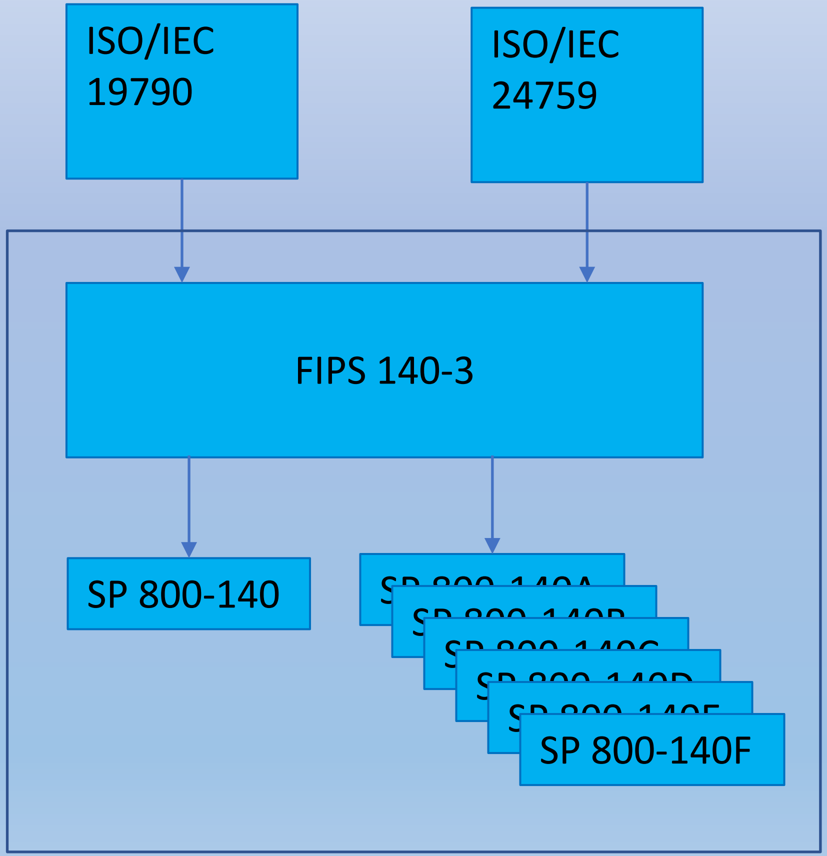
- NIST is responsible for developing standards and guidelines to protect non-national security federal information systems
  - Federal Information Processing Standards (FIPS), e.g.
  - Special Publications (SPs), e.g.
  - NIST Internal or Interagency Reports (NISTIRs), e.g.

- "Approved" is defined as
  - FIPS-**approved** or NIST-Recommended

Cryptographic Module Validation Program

- Cryptographic Module
- Cryptographic Module Validation Program
- Cryptographic Algorithm Validation Program
    - a prerequisite of cryptographic module validation.





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
- Historically, 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)
- More transitions are expected
  - Post-Quantum Cryptography
- Cryptographic agility is very important for future transitions
  - Allow to make smooth transition between algorithms and configurations

Challenges in Next Generation of Crypto Standards

- Deal with extremes
  - Extremely powerful attacks, quantum computers
  - Extremely constrain environment, sensors
- Transition and backward compatibility
- Diversified portfolio and interoperability
- Special usage vs. general purpose standards
- Synchronize with industry best practice
- Promote international adoption

New Initiatives – Deal with Extremes

Post-Quantum Cryptography

Cryptography standards

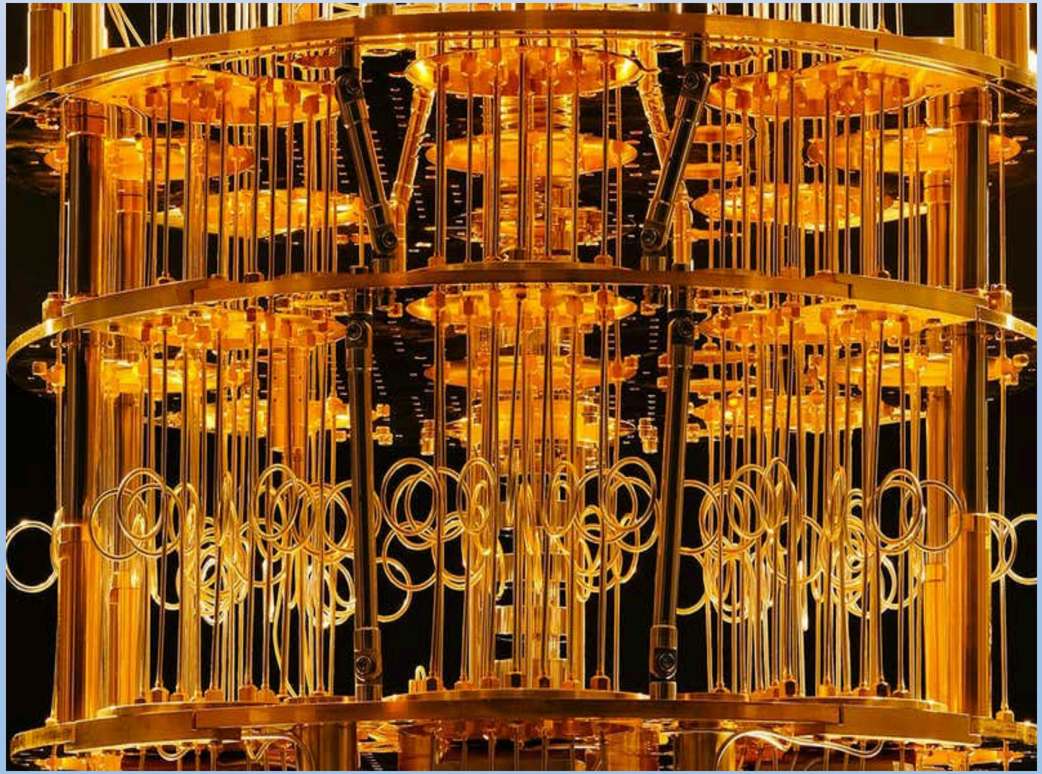
- Public key based
  - Signature (FIPS 186)
  - Key establishment (800-56A/B/C)
- Tools
  - RNG (800-90A/B/C)
  - KDF (800-108, 800-135)
- Symmetric key based
  - AES (FIPS 197) TDEA (800-67)
  - Modes of operations (800 38A-38G)
  - SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
  - Randomized hash (800-106)
  - HMAC (FIPS 198)
  - SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)
- Guidelines
  - Hash usage/security (800-107)
  - Transition (800-131A)
  - Key generation (800-133)
  - Key management (800-57)

Lightweight Cryptography

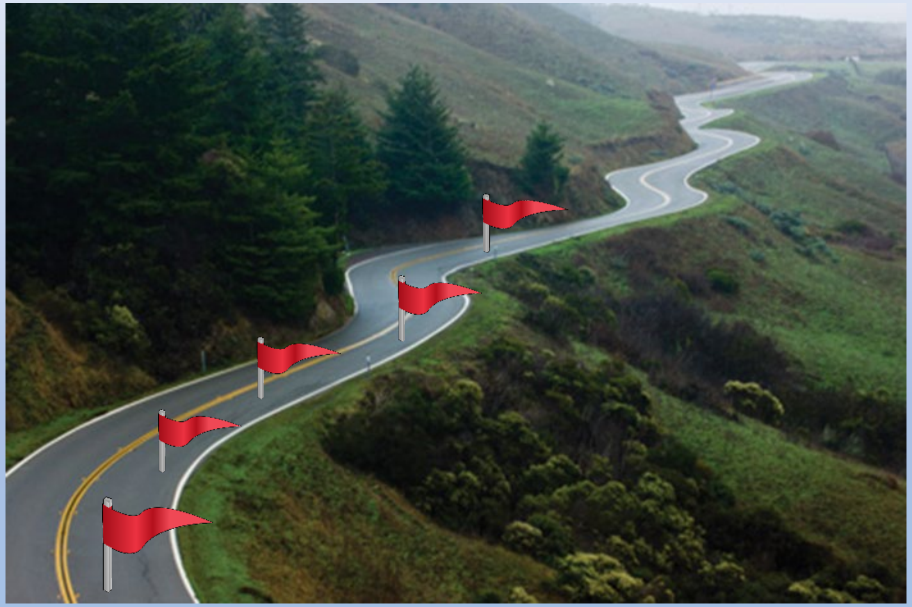
Post-Quantum Cryptography

Quantum Impact

- Quantum computing changed what we have believed about the hardness of discrete log and factorization problems
- The well-deployed public - key cryptosystems, RSA, Diffie-Hellman, ECDSA, will need to be replaced
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms – manageable by increasing key size



NIST 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

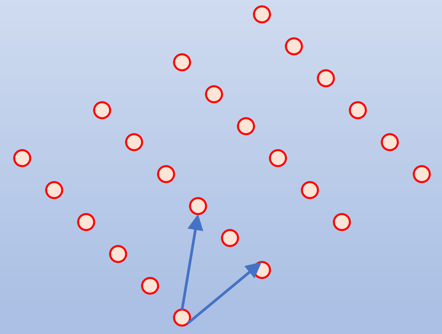
2020 Announced 3rd round 7 finalists and 8 alternate candidates

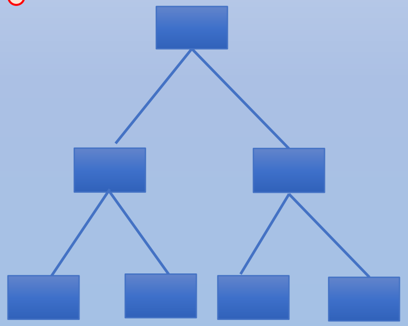
June 7-9, 2021
Hold the 3rd NIST PQC Standardization Conference

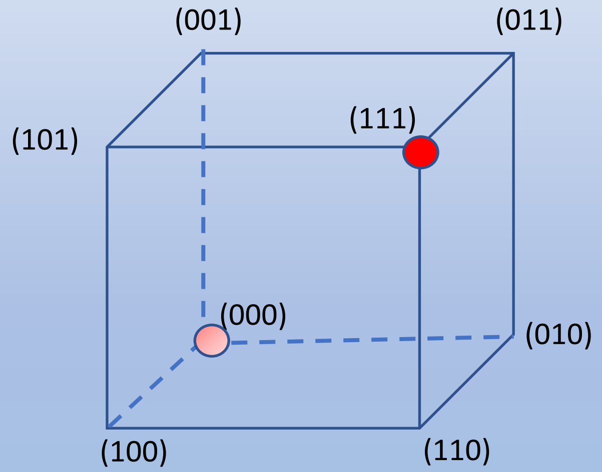
2022-2023
Release draft standards and call for public comments

Post-Quantum Cryptography

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







$$\begin{tikzcd} & E_A \arrow[dr, "\psi_B"] \arrow[dd, dotted, shift left] & \\ E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_{AB} \\ & E_B \arrow[ur, "\psi_A"'] \arrow[uu, dotted, shift left] & \end{tikzcd}$$

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

Scope, Security Definitions, Strength Levels

- The scope of submissions
  - Public key encryption /key encapsulation mechanism (KEM)
  - Digital signature
- Definitions (proofs recommended, but not required) used to judge whether an attack is relevant
  - IND-CPA/IND-CCA2 for encryptions and KEMs
  - EUF-CMA for signatures
- Security strength is defined at 5 levels

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

First, Second, and Third Round Candidates

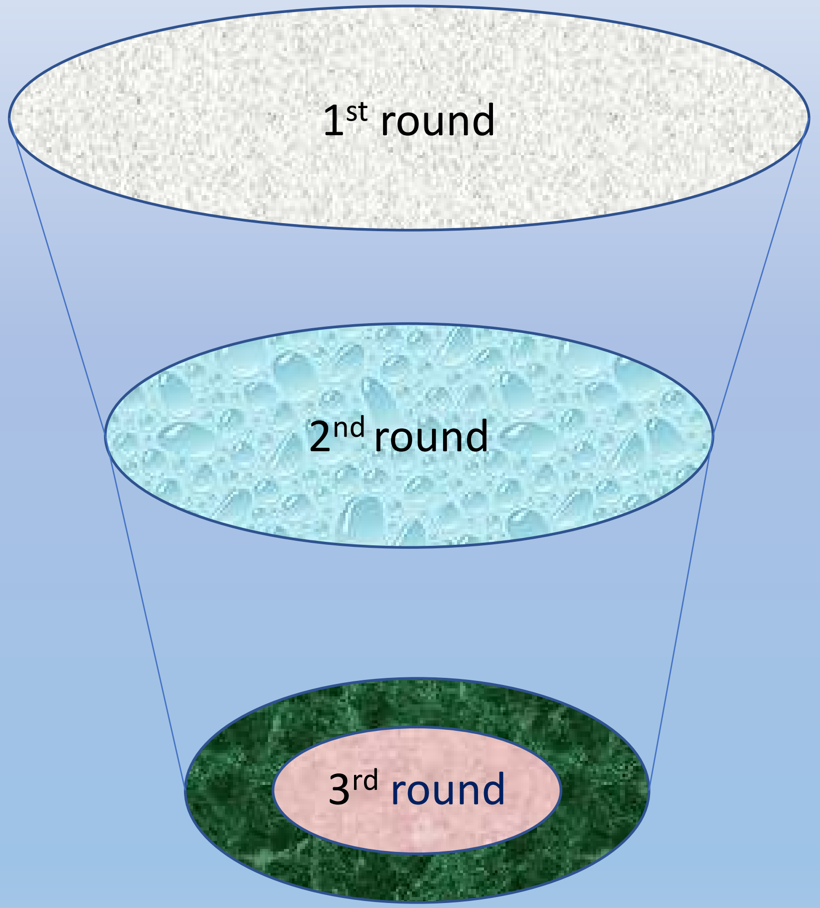
1st round	**Signatures**	**KEM/Encryption**	**Overall**
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate			
Stateless Hash/Symme			
Other			
Total			

2nd round	**Signatures**	**KEM/Encryption**	**Overall**
Lattice-based	3	9	12
Code-based		7	7
Multi-			
Statele based			
Isogen			
Total			

3rd round	**Signatures**		**KEM/Encryption**		**Overall**	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	3	4	5	7	8

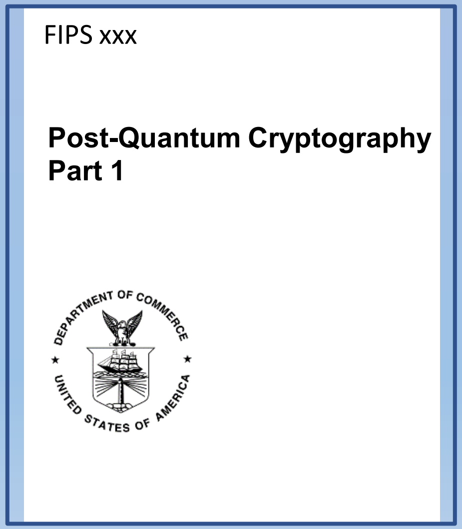
Challenges and Considerations in Selecting Algorithms

- Security
  - Security levels offered
  - (confidence in) security proof
  - Any attacks
  - Classical/quantum complexity
- Performance
  - Size of parameters
  - Speed of KeyGen, Enc/Dec, Sign/Verify
  - Decryption failures
- Algorithm and implementation characteristics
  - IP issues
  - Side channel resistance
  - Simplicity and clarity of documentation
  - Flexible

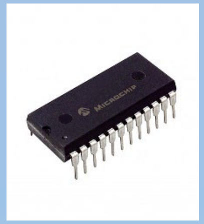


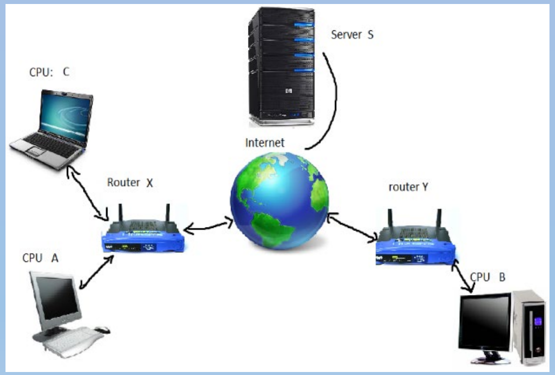
Transition and Migration

- Public key Cryptography has been used everywhere
- Transition and migration are going to be a long journey full of exciting adventures


FIPS xxx

Post-Quantum Cryptography Part 1





Lightweight Cryptography

Lightweight Cryptography Needs Heavy Lifting

- Recognize the need for cryptographic standards for applications in constrained environment that are not well-served by existing NIST standards
- The task is not light – more challenging in the design to satisfy all security requirements and performance for different platforms
- It has been a difficult decision for NIST to initiate a call for proposals
  - Held two workshops in 2015 and 2016 to get industry feedback and published NISTIR 8144 in 2017
  - The scope and criteria were finalized in 2018 – Call for contributions

Lightweight Cryptography Candidates

- Scope: Symmetric-key based Authenticated Encryption with Additional Data (AEAD) with optional hashing functionality
- The candidates include (tweakable) block ciphers, stream ciphers, permutation, …
  - The designs reflected the technology advance in the past 20 years
  - Most designs are based on the primitives used in the standardized algorithms
  - Many candidates claimed additional security features

Round 1 (April 2019): 56 candidates → Round 2 (August 2019): 32 candidates → Round 3 (March 2021): 10 finalists →

Towards Lightweight Cryptography Standards

- Security analysis and maturity assessment were provided by the design team and independent third parties
- The performance is evaluated in software and hardware
  - Targeted devices, optimized implementations
  - Hardware API. FPGA, ASIC
- Expect to announce final winners in about 12 months

Summary

- NIST Cryptographic Standards have been a cornerstone for cybersecurity
  - Provide protection on communication links; and
  - Establish trusted platforms
- NIST Cryptographic Standards are developed for non-national security applications
  - Cryptographic Module Validation Program provide Federal agencies with a security metric
- Next generation cryptography standards will deal with
  - Quantum threats — Post-quantum Cryptography
  - Protection demand for constrained environment — Lightweight Cryptography

Thanks!

lily.chen@nist.gov

For more information on NIST cryptographic standards and validations, please visit
http://csrc.nist.gov