Information Security in Quantum Time

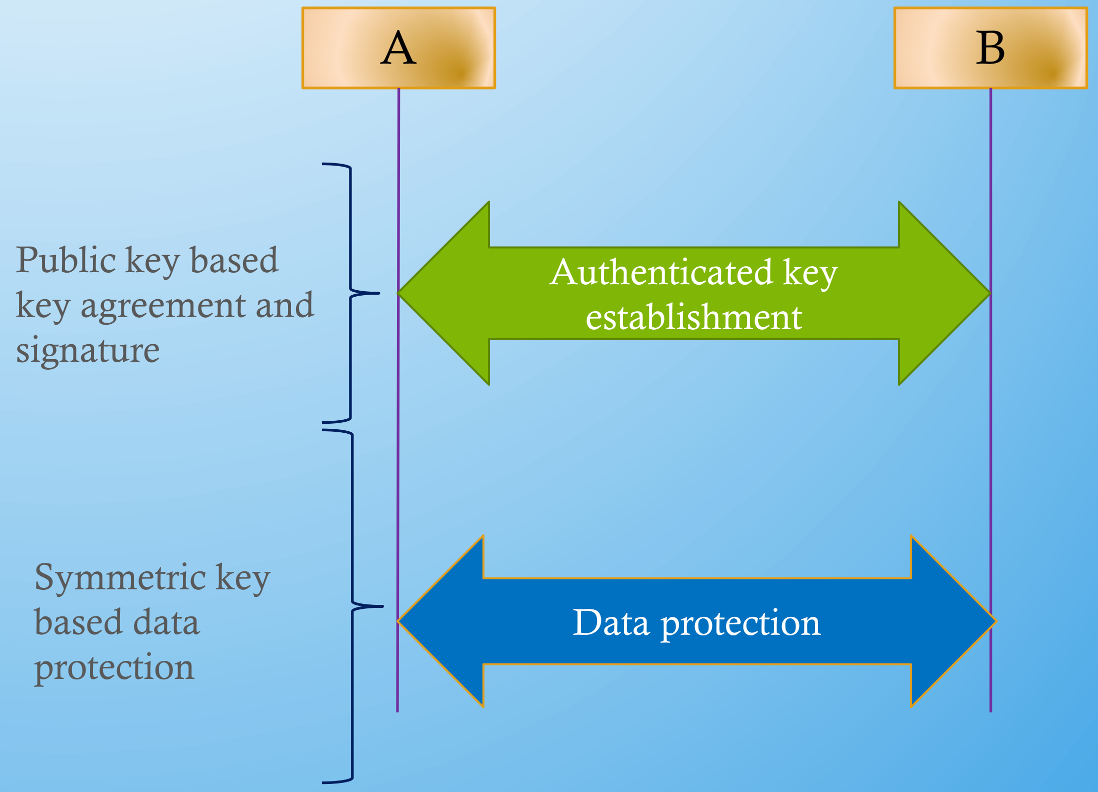
Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

Cryptography and Information Security

- In 1970s, cryptography was solely used for encryption
  - NIST published the first block cipher standard, FIPS 46 Data Encryption Standard (DES), in 1977 with 64-bit block size and 56-bit key size
- The public key cryptography was invented in 1976 - enable automated key establishment through public channel and digital signatures
- Internet accelerated adoption of public-key cryptography
  - Automated peer to peer key establishment - manual key distribution would not work in a many-to-many communication network
  - Authentication with non-repudiation - verifiable by any one without protected key distribution
- Today, cryptography has gone from an art for secret communication to a science which apply to every aspect of people’s life

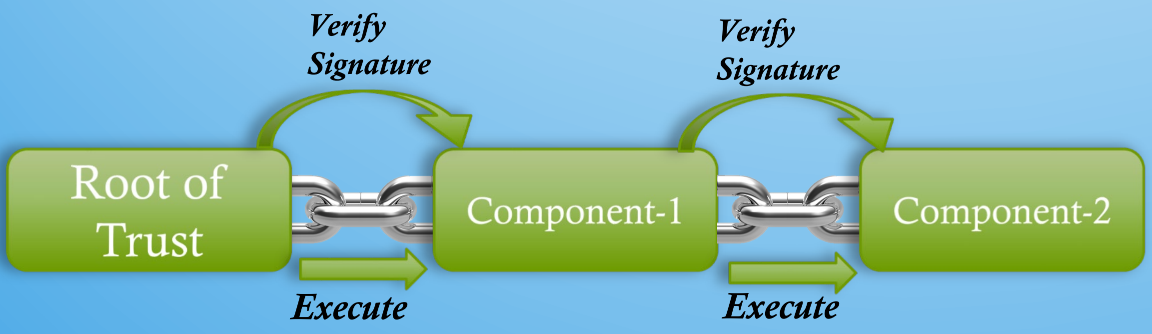
Cryptography in Network Security

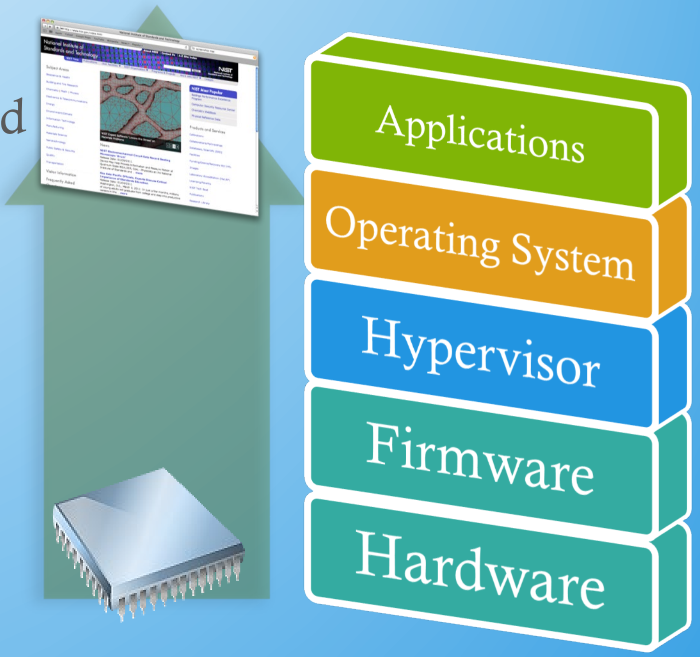
- In communication protocols, public key and symmetric key cryptography schemes are used together, e.g. TLS, IKE/IPsec, etc.
  - Use public key cryptography to establish keys and conduct entity authentication
  - Use symmetric key cryptography to encrypt and authenticate bulk data



Cryptography in Trusted Computing Platform

- Open platform introduces trust issues on the firmware and software update
- In trusted platform technologies,
  - Use public key to establish root of trust
  - Use signatures to authenticate/authorize firmware, software and applications
  - Use symmetric key crypto to protect data
- Public key cryptography enables to establish a trust chain





Public-Key Cryptography (PKC) Standardizations

- Two classes of PKC schemes have been widely deployed
  - Discrete log based (e.g. DH, DSA, ECDH, ECDSA)
  - Integer factorization based (RSA encryption, RSA signature)
- NIST has specified digital signatures in FIPS 186-4, discrete log based key agreement like DH in SP 800-56A, and RSA key transport in SP 800-56B
  - These standards are developed for government non-classified applications
- The major schemes are standardized by many standards organizations, ISO, IEEE, IETF, ANSI, etc.
- We have been relying on PKC to protect data in transmit and in storage
  - For protect Internet traffic as in Internet Key Exchange (IKE)
  - For protect Internet applications as in Transport Layer Security (TLS)

NIST Cryptography Standards

Crypto 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)

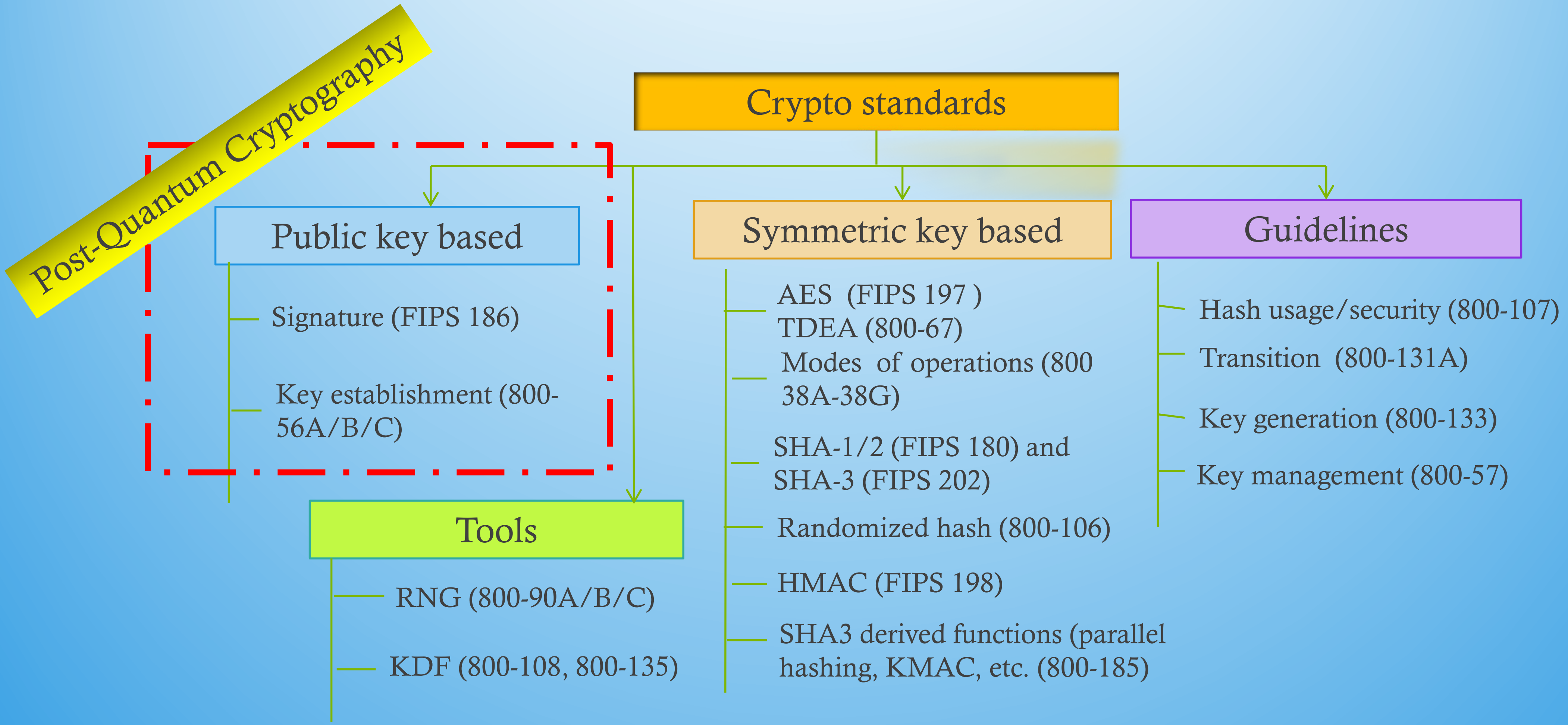
Guidelines

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

Quantum Impact

- Emerging quantum computers changed what we believed about the hardness of discrete log and factorization problems
  - Using quantum computers, an integer n can be factored in polynomial time using Shor's algorithm
  - The discrete logarithm problem can also be solved by Shor’s algorithm in polynomial time
- As a result, the public key cryptosystems deployed since the 1980s will need to be replaced
  - RSA signatures, DSA and ECDSA (FIPS 186-4)
  - Diffie-Hellman Key Agreement over finite fields and elliptic curves (NIST SP 800-56A)
  - RSA encryption (NIST SP 800-56B)
- We have to look for quantum-resistant counterparts for these cryptosystems
- Quantum computing will also impact security strength of symmetric key based cryptography algorithms
  - Grover’s algorithm can find AES key with approximately $\sqrt{2^n}$ operations where n is the key length
  - Intuitively, we should double the key length, if 2^{64} quantum operations cost about the same as 2^{64} classical operations
    - Based on current understanding about the cost of Grover’s attack, we will probably not need such a large key length increase in practice

NIST Post-Quantum Cryptography Standards



Understand Challenges

- Security analysis against classical computers
  - When introducing new schemes, many details must be scrutinized even for provably security schemes
- Security analysis against quantum computers
  - Estimation of the quantum security strength for a given set of parameters must consider many factors – processing complexity, memory requirement, etc.
- Performance assessment and improvement for practical usage
  - Acceptable key size, ciphertext size, and signature size
- Smooth migration to quantum resistant PKC schemes in the existing applications
  - How to adapt them in the existing applications – timeline and cost

NIST PQC Milestones

- 2009 – NIST Survey paper on Post-Quantum Cryptography
- 2012 – NIST began PQC project: build NIST team on PQC research
- April 2015 – 1st NIST PQC workshop
- Feb 2016 – NIST Report on PQC (NISTIR 8105)
- Feb 2016 – NIST preliminary announcement of standardization plan
- Dec 2016 – Announcement of finalized requirements and criteria(Federal Register Notice)
- Nov. 30, 2017 – Submission deadline, received 82 submissions
- Dec. 24, 2017 – Announced the first round 69 algorithms, as "complete and proper"
- April 11-13, 2018 – The 1st NIST PQC Standardization Conference (Fort Lauderdale, FL)
- January 30, 2019 – Announcement of the 2nd round 26 candidates
- August 22-24, 2019 – The 2nd NIST PQC Standardization Conference (Santa Barbara, CA)

Scope of NIST PQC Standardization

- Digital signature
  - Replace the schemes specified in FIPS 186-4 (RSA, ECDSA)
- Public Key Encryption/Key Encapsulation
  - Replace key establishment specified in
    - SP 800-56A (DH/ECDH, MQV/ECMQV)
    - SP 800-56B (RSA public key secret value transport and encryption OAEP)

The Selection Criteria

- Security - against both classical and quantum attacks
- Performance - measured on various "classical" platforms
- Other properties
  - Drop-in replacements - Compatibility with existing protocols and networks
  - Perfect forward secrecy
  - Resistance to side-channel attacks
  - Simplicity and flexibility
  - Misuse resistance, and
  - More
- The draft requirements and criteria were announced in August 2016 to call for public comments

Quantum Security

- Uncertainties
  - The possibility that new quantum algorithms will be discovered, leading to new attacks
  - The performance characteristics of future quantum computers, such as their cost, speed and memory size
- For PQC standardization, need to specify concrete parameters with security estimates, that is,
  - A selected parameter set maps to a specific security level

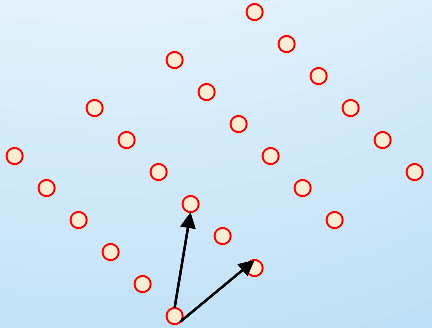
Security Strength Categories

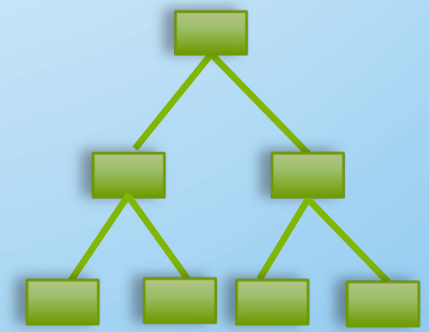
Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256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

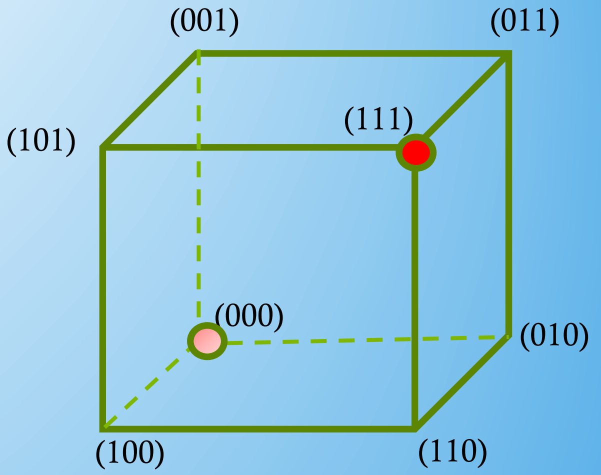
- Computational resources should be measured using a variety of metrics
- NIST asked submitters to focus on levels 1,2, and 3
  - Levels 4 and 5 for high security
- Security definitions (proofs recommended, but not required) used to judge whether an attack is relevant
  - IND-CPA/IND-CCA2 for encryptions and KEMs
  - EUF-CMA for signatures

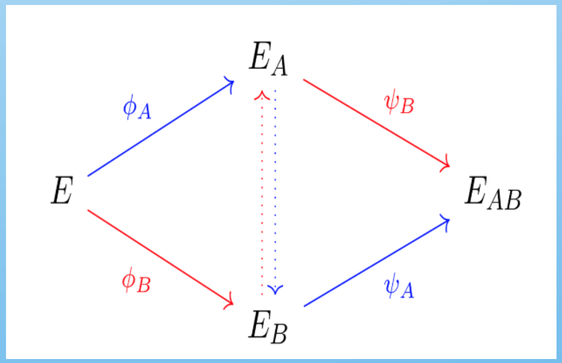
Post-Quantum Cryptography (PQC)

- The 1st PQCrypto Conference was held in 2006 in Leuven, Belgium
  - It has become an annual conference since 2016
  - PQC has become a very active research area
- Some actively researched PQC categories
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash based signatures
  - Isogeny-based schemes









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

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

$$\vdots$$

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

Submissions and the 1st Round Candidates

- Before submission deadline (Nov. 30, 2017), 82 total submissions received from 25 Countries, 6 Continents
  - The submitters in USA are from 16 States
- 69 accepted as "complete and proper" (5 since withdrawn)

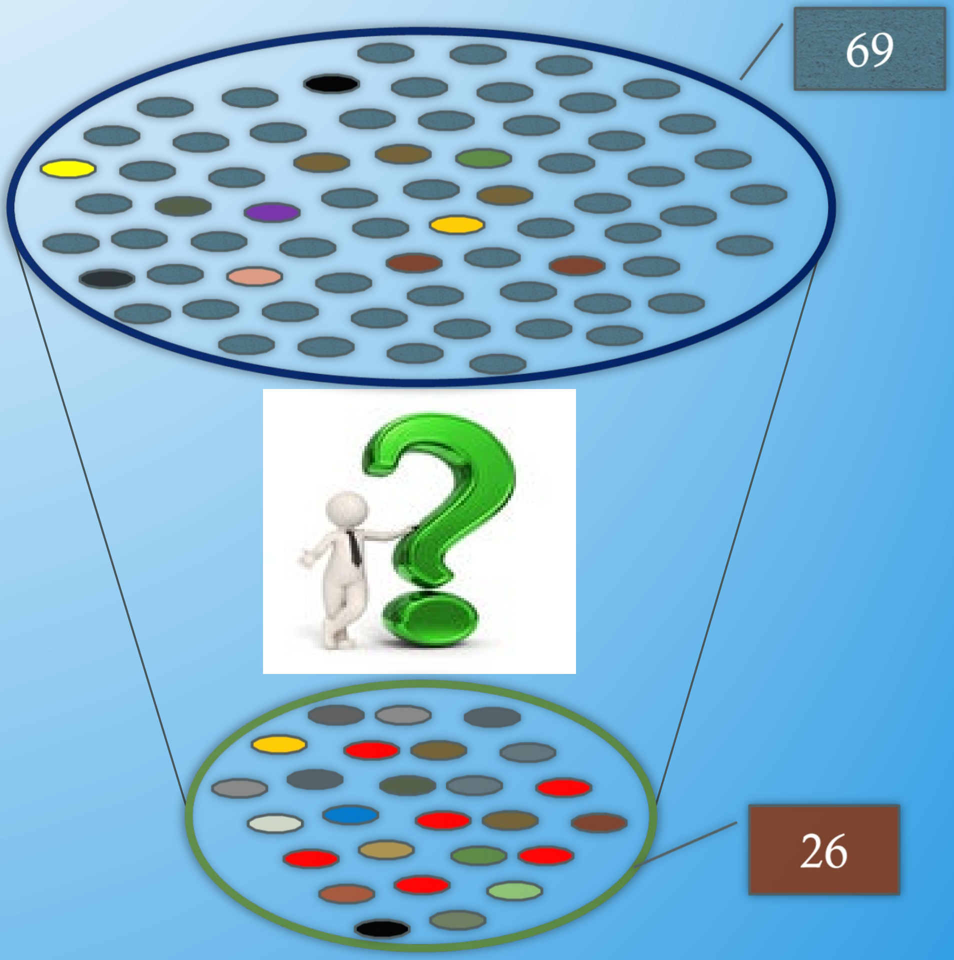
	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash or Symmetric based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

Evaluation of the 1st Round

- NIST team held internal seminars to present each candidate to understand how it works, look into security analysis provided by the submitters, raise questions, discuss pros and cons, etc.
- Security analysis
  - Research publications at conferences and journals (e.g. PQCrypto)
  - Official comments - Over 300 official comments in the first round evaluation
  - E-mail discussions at pqc-forum – 926 posts
- Performance
  - Evaluation resources include
    - NIST’s internal testing with submitters’ code
    - Preliminary benchmarks – SUPERCOP, OpenQuantumSafe, etc.

Selection of 2nd Round Candidates

- Security
  - Candidates which were broken, significantly attacked, or difficult to establish confidence in their security were left out
  - Candidates which provided clear design rationale and reasonable security proofs to establish reasonable confidence in security are advanced
- Performance
  - Candidates with obvious performance or key/signature/ciphertext size issues for existing applications were not advanced - even though they might have been well prepared with good ideas
- Diversity
  - Candidates with good security and performance were kept if their security is based on alternative security assumptions or offer unique performance tradeoffs
  - Some candidates were very similar and NIST encouraged mergers and advance only the most promising few



The 2nd Round Candidates

- We wanted to keep algorithm diversity and promote research, but had to reduce the number of candidates to a manageable size for the community
  - It is hard to make comparison among candidates in different categories
  - Sometimes even in the same category, it is not always possible to rank them
- Some candidates were merged as NIST encouraged

	Signatures	**KEM/Encryption**	**Overall**
Lattice-based	3	9	12
Code-based		7	7
Multi-variate	4		4
Stateless Hash or Symmetric based	2		2
Isogeny		1	1
Total	**10**	**16**	**26**

Review of the 2nd Round Candidates

- The 2nd round candidates cover algorithms in the most researched categories in post quantum cryptography
- In the same category, candidates are designed with different ideas and mathematical structures, e.g.
  - Lattice-based includes unstructured LWE, RLWE, MLWE, NTRU using Rounding, Error Correction, etc.
  - Code-based includes schemes based on rank metric and Hamming metric, as well as the original 1979 McEliece cryptosystem based on Goppa codes
  - Multivariate signature schemes include the Hidden Field Equations (HFEv-) family and also the Unbalanced Oil Vinegar (UOV) family
  - Signature schemes are either in hash-and-sign or in Fiat-Shamir format
- The 2nd round includes candidates with relatively conservative approaches as well as more aggressive/optimized designs
- The 2nd round candidates provide a full spectrum for investigation

Security Topics

- Security proofs – whether the proof is correct
  - Security reduction under random oracle model (ROM) and quantum random oracle model (QROM) for IND-CPA or IND-CCA2
- Security strength estimation – whether the estimation is precisely close
  - Classical security strength is sometimes estimated, e.g. in lattice based schemes, by a combination of theory and heuristics and based on different models – closer investigations may be needed for more precise estimations
  - Quantum security strength is estimated by
    - Quantum algorithms on a specific problem
    - Grover's algorithm to speed up search
- Practical security
  - Security against side-channel attacks
  - Security to deal with decryption failure, incorrect error distribution, improper implementation of auxiliary functions/transitions, etc.

Performance Evaluation

- Benchmarks on different platforms and implementation environments
  - For hardware, NIST emphasizes to focus on Cortex M4 (with all options) and Artix-7
    - Researchers also explored Cortex-A53 and UltraScale+ for high performance
    - Identify different speed up technologies and also essential barriers in enabling hardware speed up for specific algorithms
  - Performance in software only or limited available hardware environment
  - RAM + Flash required for the implementation in constrained environments
- Performance in protocols and applications
  - Signature verification in secure boot, software update, application authorizations
  - Impact of key size on latency for real time protocols like TLS and IKE
- Power consumption and other costs
  - Get more precise estimation

Transition Strategies

- Enable crypto agility for public key encryption/key encapsulation, signature
  - Allow introduction of new algorithms in existing applications and removal of algorithms vulnerable to attacks, classical and/or quantum
  - Assess implementation costs, e.g. required bandwidth/space
  - Adapt protocols and applications to accommodate new algorithms
- Understand tradeoff preferences in each application
  - Identify restrictions, limitations, and show stoppers
- Gain first-hand experience through trial implementations
  - Eliminate security pitfalls and explore implementation optimizations
- Introduce hybrid mode and/or dual signature in the current protocols and applications
  - Prevent crashing from single security failure

Timeline

- Spend 12-18 months to analyze and evaluate the 2nd round candidates
- Announce the 3rd round candidates in June 2020
- Hold the 3rd NIST PQC Standardization Conference in winter 2020 or early 2021
- Release draft standards in 2022-2023 for public comments

Summary – Road ahead

- We will have many decisions to make
  - When can we tell the security analysis is sufficient?
  - Shall we start from the most conservative algorithms?
  - How much to weigh security proofs?
  - When shall we finalize the standards?

- We will continue open for suggestions and encourage discussions
  - For NIST PQC project, please follow us at
    https://www.nist.gov/pqcrypto
  - To submit a comment, send e-mail to pqc-comments@nist.gov
  - Join discussion mailing list pqc-forum@nist.gov