Post-Quantum Cryptography and Standardization

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

NIST

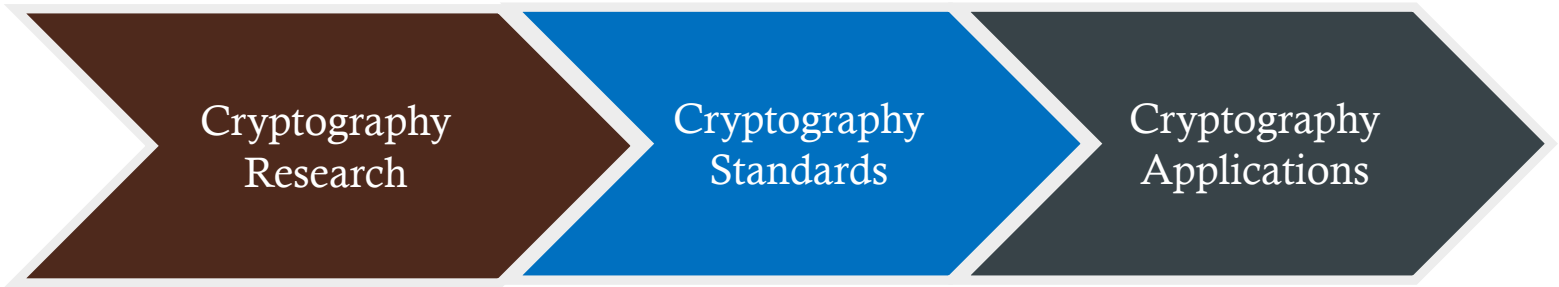
NIST Mission:
To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Information Technology Laboratory Mission:
Cultivating trust in IT and metrology.

Computer Security Division Mission:
Conduct research, development and outreach necessary to provide standards and guidelines, mechanisms, tools, metrics and practices to protect information and information systems.

Crypto Technology Group Mission:
Research, develop, engineer, and standardize cryptographic algorithms, methods, and protocols.

NIST Cryptography Program



Cryptography: Fact Sheet

NIST is the worldwide leader for strong, trusted cryptography standards and guidelines.

Nearly all commercial laptops, cellphones and ATMs use NIST Cryptography

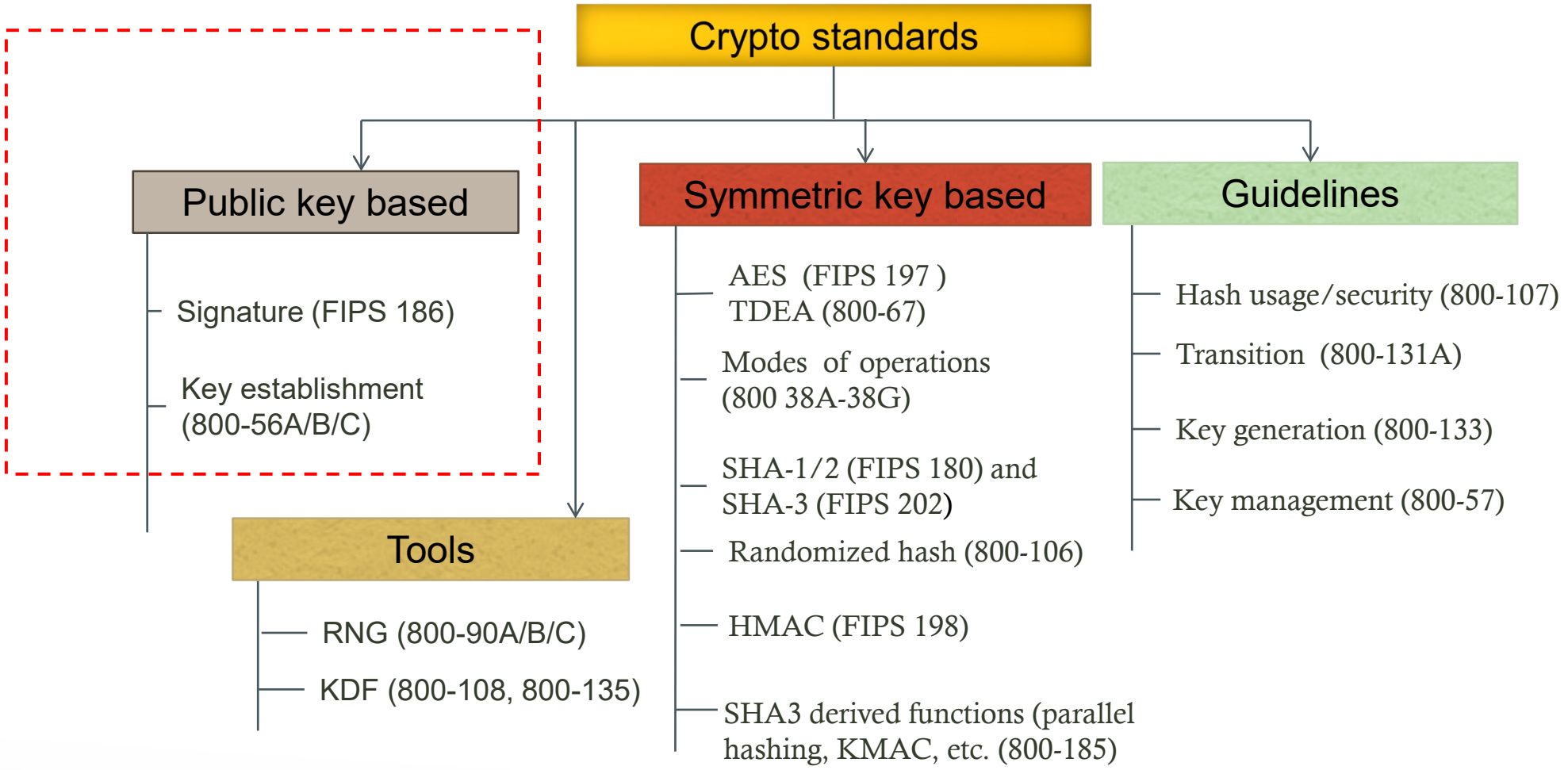
24,000 cryptographic algorithms have been validated by NIST

4,000 implementations of the Advanced Encryption Standard have been validated.

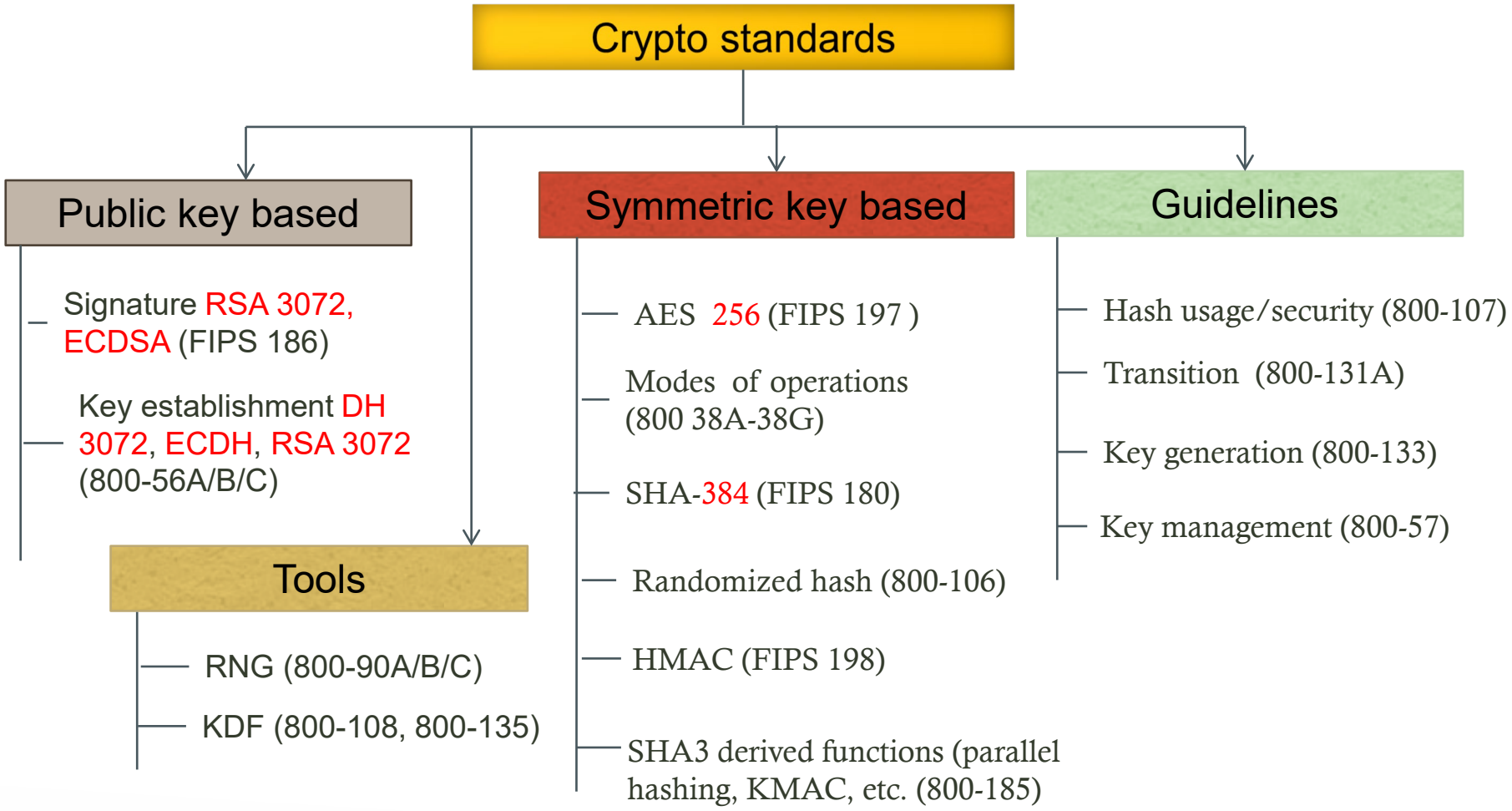
69 submissions received in response to NIST's request for nominations for public-key quantum-resistant cryptographic algorithms

4

NIST Cryptographic Standards



Commercial National Security Algorithm Suite (replacing Suite B)



NIST Public Key Cryptography Standards

- NIST standardized public key cryptographic schemes are based two "hard problems"

Integer Factorization

- RSA encryption (SP 800-56B for key establishment)
- RSA signatures (FIPS 186)

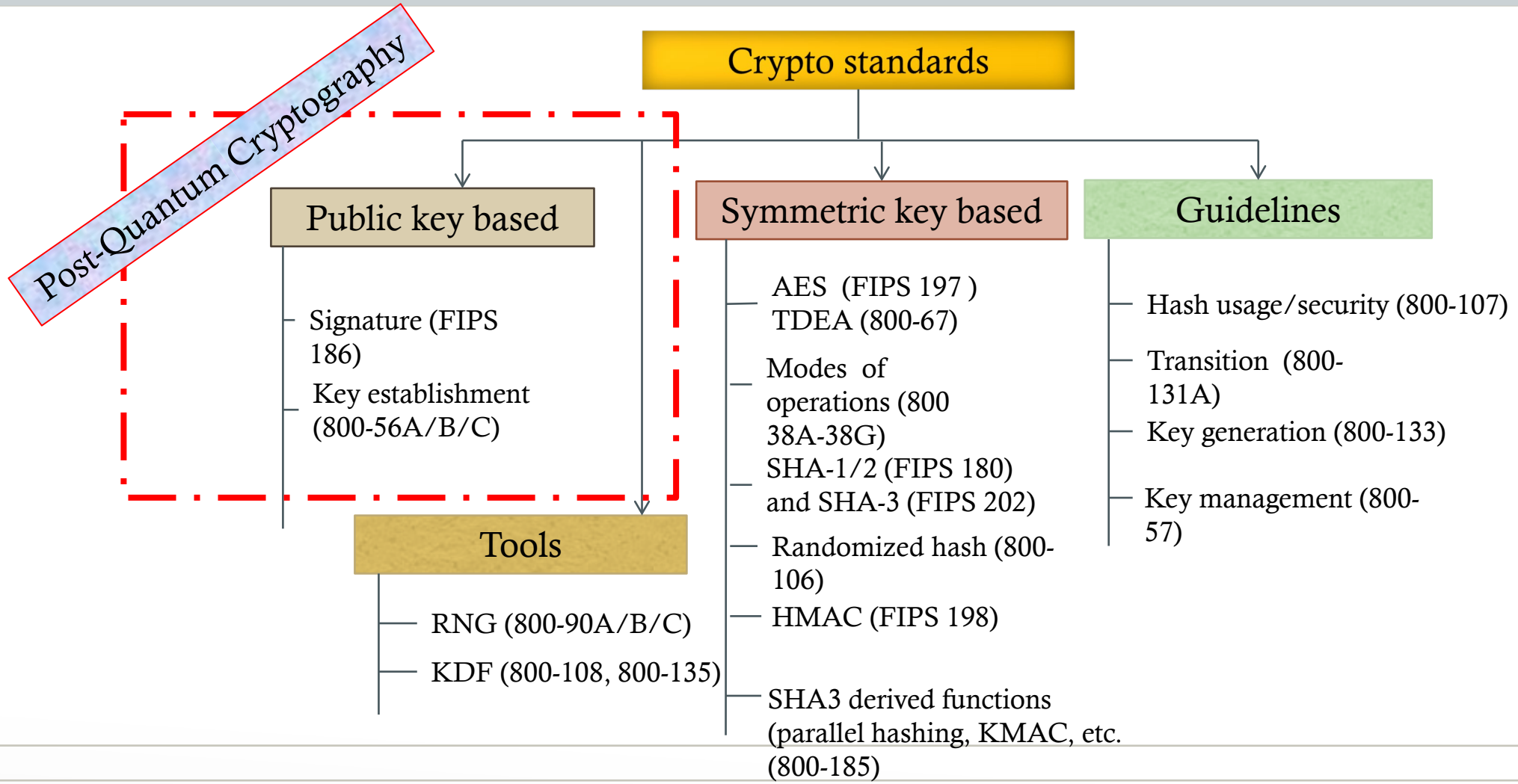
Discrete Logarithm

- DH/ECDH and MQV/ECMQV (SP 800-56A for key establishment)
- DSA and ECDSA (FIPS 186)

Quantum Impact

- Emerging quantum computers changed what we have 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 also impacted 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

Quantum Impact to NIST Standards



NIST PQC Milestones

- 2009 – NIST Survey paper on Post-Quantum Cryptography
- 2012 – NIST begin PQC project
  - Research and build NIST team
- April 2015 – 1st NIST PQC workshop
- Feb 2016 – NIST Report on PQC (NISTIR 8105)
- Feb 2016 – NIST preliminary announcement of standardization plan
- Aug 2016 – Draft submission requirements and evaluation criteria released for public comments
- Sep 2016 – Comment period ends
- Dec 2016 – Announcement of finalized requirements and criteria(Federal Register Notice)

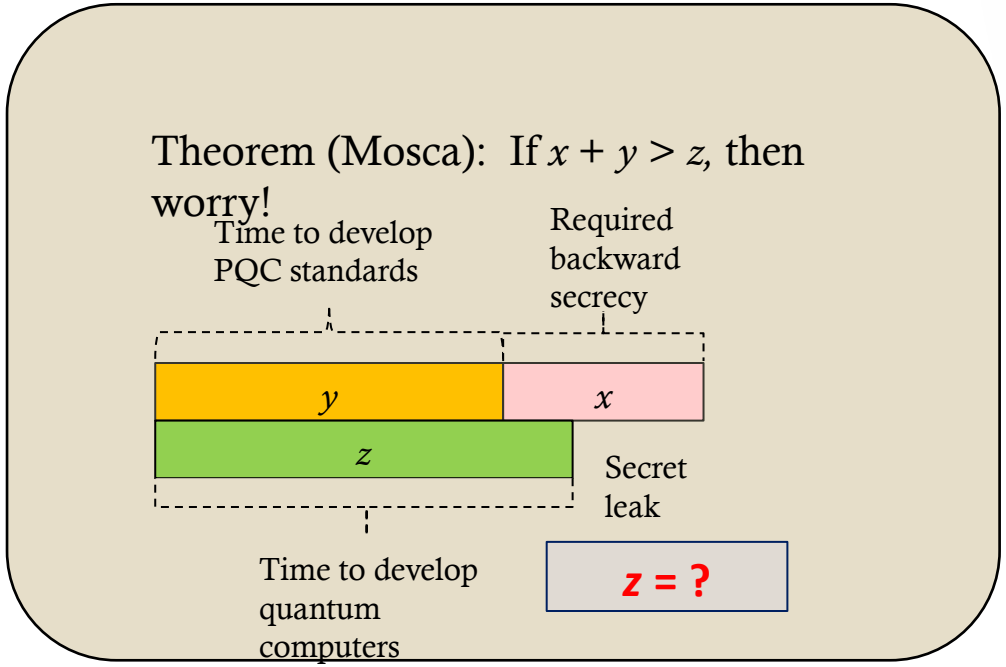
- Nov. 30, 2017 – Submission deadline, received 82 submissions
- Dec. 24, 2017 – Announced the first round 69 algorithms, as "complete and proper"
- April 11-13, 2018 – The 1st NIST PQC Standardization Conference

Is it too early to start?

"There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."

– Dr. Michele Mosca, (April 2015)

- It takes time to develop and deploy PQC standards (y years)
- Considering backward secrecy and product cycle, it is the time to start



NSA IAD Announcement August 2015

- NSA's Information Assurance Directorate updated its list of Suite B cryptographic algorithms
  - "IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."
- Standardization is the first step towards the transition

Scope

- Digital signature
  - Replace the schemes specified in FIPS 186-4 (RSA, DSA, ECDSA)
- Encryption
  - Replace key transport specified in SP 800-56B (currently using RSA encryption like OAEP and Key-Encapsulation Mechanism)
- Key agreement
  - Replace DH/ECDH, MQV/ECMQV in SP 800-56A
  - If no good replacement, use public key encryption to exchange selected secret values (as in 56B)
  - For perfect forward secrecy, use one-time public key to encrypt the selected secret values, assuming key pair generation is fast

Understand the Challenges

- Much broader scope – three crypto primitives, compared to AES and SHA-3 – single primitive
- Both classical and quantum attacks
  - Security strength assessment on specific parameter selections
- Consider various theoretical security models and practical attacks
  - Provably security and security against instantiation or implementation related security flaws and pitfalls
- Multiple tradeoff factors
  - Security, performance, key size, signature size, side-channel attack countermeasures
- Migrations into new and existing applications
  - TLS, IKE, code signing, PKI infrastructure, and much more

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

- The comments received on draft requirements and criteria focused on quantum security
  - No clear consensus on best way to measure quantum attacks
- 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

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 encryption, KEMS
  - EUF-CMA for signatures

Submissions to NIST Call for Proposals

- 82 total submissions received from 26 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**

Security Analysis and Evaluations

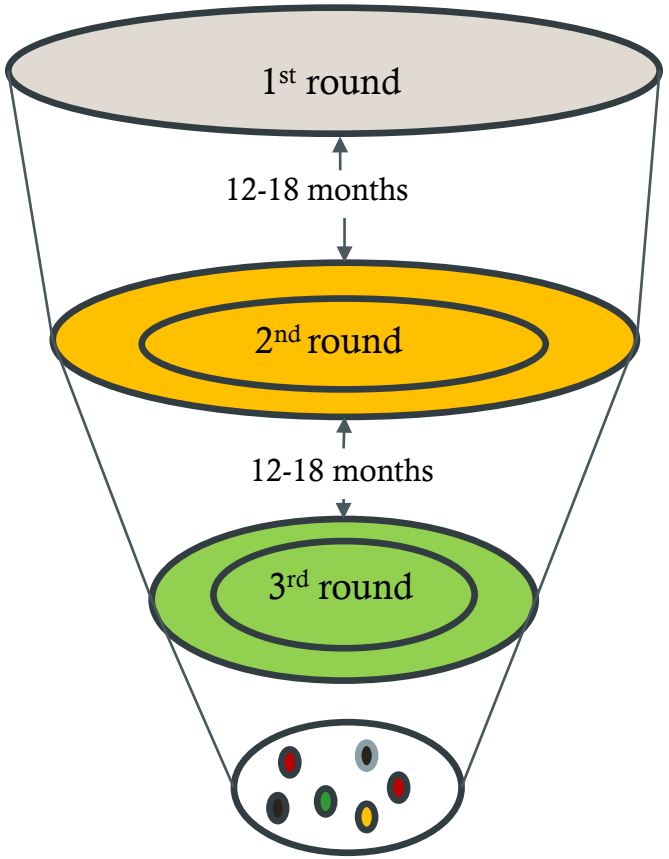
- NIST team has been reviewing and evaluating the first round candidates through internal seminars
- NIST team members monitored and participated in the discussions on pqc-forum
- The NIST PQC Standardization has greatly promoted research
  - Analysis results on candidates have been published at conferences like PQCrypto 2018 and also released through IACR eprint
  - More analysis results were announced through “Official Comments”, which will lead to future publications
- Each design team submitted reference implementations and preliminary estimations on the performance
  - NIST team has verified the reference implementations as the first round review
  - At this stage, even performance considerations will not play a major role in the evaluation process, need to understand extreme cases and show stoppers

The 1st NIST PQC Standardization Conference

- The 1st NIST PQC Standardization Conference was held in Ft. Lauderdale April 11-13, collocated with PQCrypto2018
- The conference accommodated 52 presentations covering 60 algorithms, attracted 345 attendees
- Topics discussed
  - measuring the complexity of quantum attacks
  - classical attack with super high memory
  - the way to handle similar submissions, and
  - what constitutes unacceptable key sizes or performance

NIST Timeline (from April 2018)

- Initial analysis phase 12-18 months
- Narrow the pool and hold the second workshop in August 2019
- Second analysis phase 12-18 month
- May take third analysis phase if needed
- Expect draft standards in 2022-2023



Tough Job Ahead

- Secure analysis against both classical and quantum attacks
- Secure against side-channel attacks
- Performance evaluation, including
  - Computational efficiency
  - Key size, signature size, ciphertext expansion
  - Handling decryption failure, auxiliary functions, padding, etc.
- Drop-in exercise to existing applications, check whether an algorithm can work (and how well it can work) in
  - a protocol like Internet Key Exchange (IKE) and Transport Layer Security (TLS)
  - an application like software authentication (code signing)
  - etc.

Transition and Migration

- NIST will update guidance when PQC standards are available
  - Before that, follow the transition guideline as specified in NIST SP 800-131A
  - The future PQC transition shall not be an excuse to stay on weak crypto
  - The classical attacks can be efficient and can break your system – the pre-quantum security is equally important and more urgent
- A "hybrid mode" has been proposed as a transition/migration step towards PQC
  - Such a mode combines a classical algorithm with a post-quantum one
  - Besides "quantum resistant", it can provide some user experience for selected post quantum cryptography
  - Current FIPS 140 validation will validate the NIST-approved (classical) component
  - It is vendors/users decision whether to implement hybrid mode
- NIST plans to consider stateful hash-based signatures as an early candidates for standardization, but only for specific applications like code signing
  - Please let us know whether it is suitable for your application and how likely you will deploy it

Input from Application Community

- We need input from the application community about PQC candidates
- Tell us what you can or cannot handle in your applications with regard to key size, ciphertext size, signature size, key generation, decryption failure, processing complexity, etc.
- Discuss what is the possible barrier to migrate to post-quantum cryptography in your application
- Tell us your concerns with regard to the product cycle for implementing new cryptography algorithms
- Raise issues you can see on deploying post-quantum cryptography in your application environment
- Ask questions if you have any

Summary

- Quantum computers can break the public-key cryptography systems currently in use
- Cybersecurity in quantum-time demands quantum resistant cryptosystems
- NIST is leading a new initiative to develop post-quantum cryptography standards

Information on NIST PQC Standardization

- For NIST PQC project, please follow us at
  https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

- Join discussion mailing list pqc-forum@nist.gov