NIST Post-Quantum Cryptography Standardization

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

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

NIST Cryptographic 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

Quantum computing 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

Post-Quantum Cryptography

- **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)

NIST Team has been in action

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”

PQC Families - Actively Researched as Examples

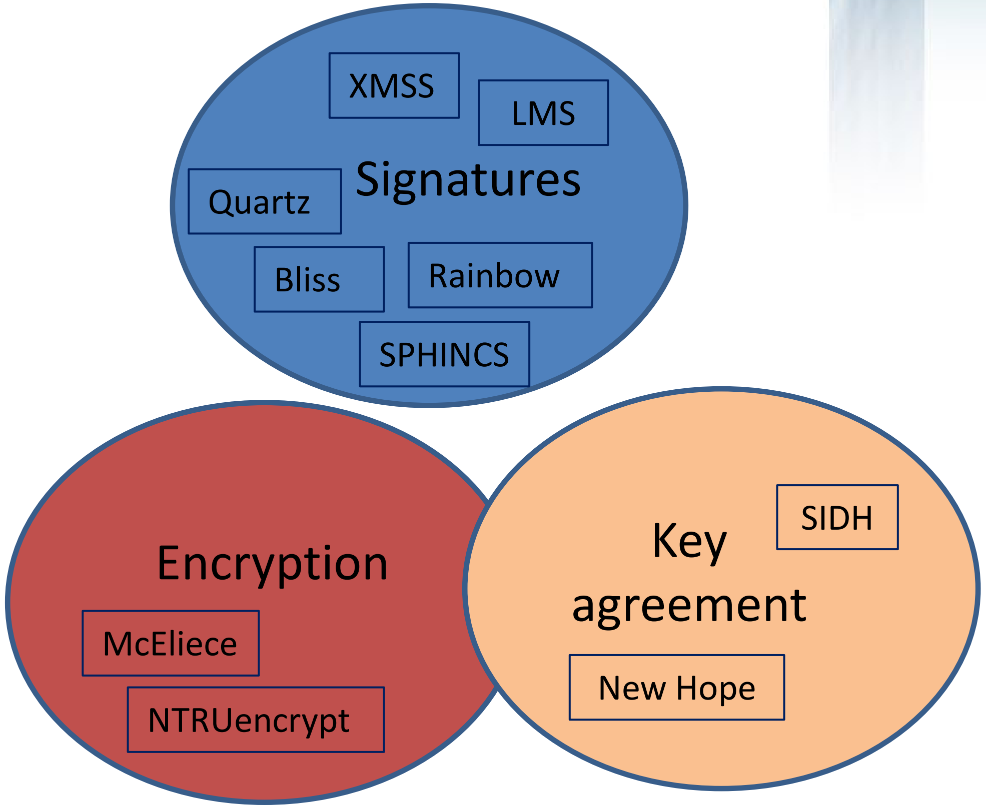
Lattice-based
- NTRUencrypt
- Signature, e.g. Bliss
- (Ring-based) Learning with Errors (e.g. Key Agreement - New Hope)

Code-based
- McEliece encryption and the variants

Multivariate
- Rainbow (signature), Quartz (signature), etc.

Hash-based signatures
- LMS, XMSS, SPHINCS

Isogeny-based schemes
- Supersingular isogeny Diffie–Hellman key exchange (SIDH)



NIST Timeline

NIST will hold the first PQC Standardization Workshop in April 12-13, 2018

Initial analysis phase 12-18 months

Narrow the pool and hold the second workshop in late 2019

Second analysis phase 12-18 month

May take third analysis phase if needed

Expect draft standards in 2022-2023

Submissions to NIST Call for Proposals

Upon the submission deadline (Nov. 30, 2017), NIST received 82 submissions from 26 countries and 6 continents

After an initial review, 69 submissions are considered as complete and proper

At the time of this presentation, 3 of them have been confirmed as “broken” and 66 remains as the first round submissions

46 Key Establishment schemes

- 24 lattice-based
- 17 code-based
- 5 other (2 multi-variate, 1 RSA, 1 random walk, 1 isogeny-based)

20 Signature schemes

- 7 multi-variate
- 5 lattice
- 3 code-based
- 3 hash-based (or symmetric based)
- 2 other (1 RSA, 1 braids)

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

Tough Jobs 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 drop in

- a protocol like Internet Key Exchange (IKE) and Transport Layer Security (TLS)
- an application like software authentication (code signing)
- etc.

Join Us for 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