Towards Post-Quantum Cryptography Standardization

Lily Chen and Dustin Moody
National Institute of Standards and Technology
USA

First mile - Towards PQC standardization

- After about four years of preparation, NIST published a Federal Register Notice (FRN) August 2, 2016
  - Requesting comments on a proposed process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms
- Comment period closed September 16, 2016
  - Received comments from N individuals/teams
- What have we observed in the first mile?

Overview of NIST call for proposals

- Requirements for Submission Packages
  - Cover sheet, supporting documentation, media, IP statement
- Minimum Acceptability Requirements
  - Scope – Public-key crypto algorithms for digital signature, encryption, key establishment
  - Basic requirements for each function
- Evaluation Criteria
  - Security definitions, targeted security strength (classical and quantum), costs, etc.
- Plans for the Evaluation Process

Complexities of PQCS

- Much broader scope with three main cryptographic primitives
- Both classical attacks and quantum attacks
- Both theoretical and practical aspect to assess security and judge whether a set of results can be considered as attacks
- Multiple factor tradeoffs (security, key sizes, signature sizes, ciphertext expansion, speed, space, etc.)
- Migrations in new applications and existing applications
- Many aspects which we have never handled in the previous standards

Scope of NIST PQCS

- Encryption/key establishment
  - Encryption scheme is used for
    - key transport from one party to another, like RSA-OAEP or
    - exchanging encrypted secret values between two parties to establish a shared secret value
  - Key establishment scheme like Diffie-Hellman key exchange
- Signature
  - Signature schemes for generating and verifying digital signatures

Security notions

- Signature
  - Existentially unforgeable with respect to adaptive chosen message attack (EUF-CMA)
  - Assume the attacker has access to no more than 2^{64} signatures for chosen messages
- Encryption
  - Semantically secure with respect to adaptive chosen ciphertext attack (IND-CCA2)
  - Assume the attacker has access to no more than 2^{64} decryptions for chosen ciphertexts
- These definitions specify security against attacks which use classical (rather than quantum) queries – 2^{64} online queries are probably beyond realistic
- These definitions are used to judge whether an attack is relevant

Target classical and quantum security

- The following metrics are considered as the minimum security strength at different levels to enable transition from one security level to another
- For a given parameter set, the algorithm may provide a different ratio as listed between classical security and quantum security (e.g. 131 classical and 119 quantum)
- For a given algorithm, with different parameter sets, it is expected to provide different security levels

	Classical Security	Quantum Security	Examples
I	128 bits	64 bits	AES128 (brute force key search)
II	128 bits	80 bits	SHA256/SHA3-256 (collision)
III	192 bits	96 bits	AES192 (brute force key search)
IV	192 bits	128 bits	SHA384/SHA3-384 (collision)
V	256 bits	128 bits	AES256 (brute force key search)

Quantum security

- The best quantum attack against most proposed post-quantum schemes seems to either be a classical attack or something similar to Grover's algorithm
- Further studies are needed regarding the best way to measure quantum attacks
  - Scaling up is a difficult engineering problem
  - Too early to predict: anything like Moore's law for quantum devices?
  - Need the empirical performance of quantum cryptanalytic attacks, e.g. running them on classical simulators or small quantum computers
- Additional factors to consider:
  - Parallel attacks
    - Note that Grover's algorithm parallelizes very poorly (a million times as many processors only a thousand times as fast.)
    - Our way of measuring quantum security explicitly considers this.
  - Limited (but easier to implement) models of computation
    - E.g. classical computing, hybrid classical-quantum attacks, adiabatic computing etc.

Drop-in replacement

- For a given primitive, in order to be used in an existing protocol, we need to consider the following aspects
  - Parameter set
  - Key generation time
  - Key length
  - Ciphertext expansion/signature size
  - Auxiliary functions (hash functions, key derivation functions, random number generation, sampling, etc.)

- For an existing protocol, in order to use a specific PQC primitive, we might need to consider whether a special feature might have security or performance issues, e.g.
  - Public-key reuse - for some new primitives public-key reuse can bring about a security problem which would not be suitable for public-key cache in TLS
  - Decryption failure – some encryption algorithms, even occasionally, produce ciphertexts which cannot be properly decrypted

Transition and migration

- Transition and migration are important to assure that security will be maintained and services are not interrupted

- NIST guidance will be updated when PQC standards are available
  - NIST SP 800-57 Part 1 specifies "classical" security strength levels 128, 192, and 256 bits acceptable through 2030 or beyond 2031

- Even foreseeing the upcoming transition to quantum-resistant cryptographic schemes, it is still required to move away from weak algorithms/short key sizes as specified in 800-131A, i.e.
  - Anything with a "classical" security strength less than 112 bits should not be used any more

Some initial actions

- Hybrid mode has been proposed as a transition/migration to PQC cryptography
  - Current FIPS 140 validation will only validate the approved component
  - NIST PQC standardization will focus on the quantum-resistant component
  - Hybrid mode may not be considered as a long term quantum resistant solution for its implementation burden (a double edge sword)
- Stateful hash-based signatures
  - IETF has taken actions in specifying stateful hash based signatures
  - NIST will coordinate with IETF and possibly other standard organizations
  - NIST may consider stateful hash-based signatures as an early candidates for standardization, but just for specific applications like code signing

Summary

- Post-quantum cryptography standardization is going to be a long journey
- After the first mile, we have observed complexities and challenges
- NIST acknowledges all the feedbacks received on the call for proposals
- NIST will continue to work with the community towards PQC standardization