NIST PQC Standardization

– Process, Issues and Strategies

Lily Chen
NIST, USA
March 22, 2017

PQC Asia Forum

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

NIST PQC Standardization Milestones

- 2012 – PQC project begins
- 2015 – 1st NIST PQC workshop
- Feb 2016 –NISTIR 8105 published
- Feb 2016 – Preliminary plan on PQC standardization announced
- Aug 2016 – Call for public comments on draft submission requirements and evaluation criteria
- Sep 2016 – Comment period ends
- Dec. 2016 – Finalize Call for Proposals

NIST PQC Standardization Plan

Nov. 30, 2017	Submission deadline
April 2018	Workshop – Submitters' presentations
3-5 years	Analysis phase - NIST reports on findings and more workshops/conferences
2 years later	Draft standards available for public comments

- NIST will post "complete and proper" submissions
- NIST PQC Standardization Conference (with PQCrypto, Apr 2018)
- Initial phase of evaluation (12-18 months)
  - Internal and public review
  - No modifications allowed
- Narrowed pool will undergo a second round (12-18 months)
  - Second conference to be held
  - Minor changes allowed
- Possible third round of evaluation, if needed
- NIST will release reports on progress and selection rationale

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

Overview of NIST Call For Proposals

- Requirements for Submission Packages
  - Cover sheet, supporting documentation, implementations, IP statements
- Minimal Acceptability Requirements
  - Scope – public key signatures, encryption, key-exchange
  - Basic requirements for each function
- Evaluation Criteria
  - Security: security models, target security strengths,
  - Performance: key sizes, computational efficiency
  - Flexibility
- Plans for the Evaluation Process

Scope and Current NIST Standards

- The scope is determined by the NIST current standards.
  - Signatures
    - Public-key signature schemes for generating and verifying digital signatures (FIPS 186-4)
  - Encryption/key-establishment
    - Encryption scheme used for
      - Key transport from one party to another
      - Exchanging encrypted secret values between two parties to establish shared secret value (see SP 800-56B)
    - Key-establishment
      - Schemes like Diffie-Hellman key exchange (see SP 800-56A)
- We plan to standardize the PQC algorithms in new standards, i.e.
  - PQC signatures will not be a revision of FIPS 186
  - PQC key exchange will not be a revision of NIST SP 800-56A

Requirements

- Minimal acceptability requirements
  - Provide description on at least one of functionalities:
    - Public-key encryption, KEM scheme, Digital signatures
  - Publicly disclosed and available for public review
  - Not incorporate components insecure against quantum computers
  - Concrete values for parameters claiming to meet security properties
- Required support materials
  - Performance analysis (implementations + documentation)
  - Known Answer Test values
  - Security analysis (with preliminary security strength categories)
  - Signed Intellectual Property statements and disclosures

Security Notions

- Signatures
  - 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
- Ephemeral key-agreement
  - Semantic security with respect to chosen plaintext attack (IND-CPA security)

Other Desirable Security Properties

- Perfect Forward Secrecy
  - A feature of key agreement protocols which gives assurances that past session keys will not be compromised even if the private key of the server is compromised, e.g. Ephemeral Diffie-Hellman
- Side Channel Resistance
  - Cost assessment on applying countermeasures to against side-channel attack
- Resistance to multi-key attacks
  - No significant advantage by attacking multiple keys
- Misuse Resistance
  - No catastrophic failure by improper operations or mishaps on key generation, random number selection, etc.

Target Security Levels (in Draft CFP)

- Submissions are required to specify parameters and map each specified parameter set to one of 5 security strength categories
  - Allows for more meaningful performance comparisons
  - Helps us make decisions on transition to longer keys

	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)

Classical Security

- Science for assessing classical security is better developed than that for assessing quantum security
- The most effective and practical attacks may be classical attacks, even if quantum attacks work better "on paper"
- Classical cryptanalysis can improve our understanding of the structure underlying the primitive, which is also the basis for quantum cryptanalysis
- Submitters should at least share their understanding of classical security of the proposal(s)

Quantum Security

- Quantum security levels specified in the draft requirements and evaluation criteria received many comments
- Comments were inconsistent or even controversial
- Uncertainties on quantum security
  - 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
- Concerns on hurting performance to satisfy the security levels

Target Security Levels (in Final CFP)

- Computational resources should be measured using a variety of metrics
  - Number of classical elementary operations, quantum circuit size, etc.
  - Should consider realistic limitations on circuit depth (e.g. 2^{40} to 2^{80} logical gates)
  - May also consider expected relative cost of quantum and classical gates.
- Submitters need not provide parameters for all 5 categories
- These are understood to be preliminary estimates

	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)

Hypothetical Scenario on Security Strength

- Assume no quantum attacks (like Shor's on factorization), beside generic ones (i.e. Grover-based to speed up classical attack)
- To achieve security strengths 1, 3, 5, set parameters for classical security to (at least) 128, 192, 256 bits respectively
- To achieve security strengths 2 and 4
  - If there is no quantum speedup, 128 bits and 192 bits of classical security, respectively, will be enough.
  - If there is a quantum speedup, more classical security will be needed to achieve the required quantum security.

Competing Factors in a Non-Competition

- Secure 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

Cost and Performance

- Standardized post-quantum cryptography will be implemented in “classical” platforms
- Diversified applications require different properties from extremely processing constrained device to limited communication bandwidth
- May need to standardize more than one algorithm for each function to accommodate different application environments
- Allowing parallel implementation for improving efficiency is certainly a plus
- If an algorithm is not a good performer on all platforms, then it would be very helpful to understand where it is a good performer

Drop-in Replacements

- We're looking for Quantum resistant drop-in replacements for existing applications, e.g. Internet Key Exchange (IKE) and Transport Layer Security (TLS)
  - Key establishment
    - Schemes similar to Diffie-Hellman key exchange
    - Public key encryption (maybe one time public key)
  - Signatures
    - Reasonable public key size, signature size, and- fast signature verification
- For an algorithm, the evidence of compatibility with the current existing protocols will be valuable, while knowing how to modify the protocols to make it work is also extremely helpful

Security Implementation Issues

- Properly handling security implementation issues are critical to make an algorithm a strong candidate for standardization, e.g.
  - Public key validation
    - How efficient or inefficient it can be
    - What is the risk of not doing it
  - Decryption failure
    - Probability
    - How to prevent security flaws brought about by decryption failure
  - Countermeasures to side-channel attack
    - Methods and costs
  - Auxiliary functions
    - Requirements and efficiency, e.g. Gaussian simulation
  - Misuse resistance, e.g.
    - If public key reuse is a security issue, how to prevent it
- Details determine success or failure – General strategy to win

Summary

- NIST acknowledges all the feedback received, which has improved the submission requirements and evaluation criteria
- Submission deadline is November 30, 2017
- Next NIST PQC workshop will be held
  - April 12- 13, 2018, Fort Lauderdale, Florida
  - Co-locate with PQCrypto 2018
- See also: www.nist.gov/pqcrypto
  - Sign up for the pqc-forum for announcements and discussion