NIST
Post-Quantum Cryptography Standardization

Lily Lidong Chen
National Institute of Standards and Technology
USA

AWACS 2016

Outline

- Introduction
- NIST Plan on PQC Standardization
- Challenges and Strategies
- Discussions

Introduction

- Quantum computers would completely break widely deployed public key cryptosystems
  - RSA, DSA, and elliptic curve cryptosystems (FIPS 186, SP 800-56A/B)
- These schemes have been used in major security protocols
  - TLS, IKE, SSH, and many other protocols
- To prepare for cyber security in a quantum time, quantum resistant cryptography standards are needed
  - Active research in this area and many publications
- We are working toward a timeline of 2023 - 2025
  - It takes time to research, standardize, and implement in products
  - Backward secrecy and smooth migration/transition also require an early deployment

NIST Initial Activities

- Since 2012
  - Bi-weekly post-quantum cryptography seminars
  - Guest researchers and invited speakers
  - Research publications and presentations
  - Participation in international projects and activities
- Held our first workshop in April 2015
  - Cyber-security in a Post Quantum World
- Published Interagency Report NISTIR 8105
  - Report on Post-Quantum Cryptography
- Announced NIST preliminary plan to develop post-quantum standards at PQCrypto 2016

Tentative Timeline

- Spring/Summer 2016 – Release the draft of "call for proposals"
- Fall 2016 – Release Federal Notice on call for proposals
- Late 2017 – Deadline for Submissions
- Spring 2018 – The first PQC standardization workshop
- 2018-2023 – Analysis stage
  - Hold more workshops
  - Narrow the selection pool
  - Release reports periodically
  - Release draft standards for public comments

Scope of NIST PQC Standardization

- 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, MQV 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

Similar to SHA-3 competition

- It will be an open procedure and we hope to engage with research communities, implementers and practitioners
- NIST will encourage public analysis on the submitted algorithms and make the results available
- NIST will hold conferences for researchers to share analysis and evaluation results
- NIST will release reports periodically and summarize the rationale for each selection

Different from SHA-3 competition

- Post-quantum cryptography is more complicated than hash function
- The algorithms are based on very different mathematical structures and security assumptions
  - Straight forward comparison might be impossible
- We may not be able to select one single "winner" for each function (signature, encryption, key agreement)
  - For interoperability reasons, we do not want to select too many algorithms for each function
  - NIST will standardize a limited number of algorithms for each function category, instead of introducing a portfolio

Different from SHA-3 competition

- We may not select all the “winners” in one pass
  - For a submission not to be selected may not mean it’s out of the game
- We may adopt algorithms specified in other standard organizations
- Some submissions may be merged or revised
- The timeline and some selection criteria may change based on developments in the field

Security

- Security definitions
  - Signature
    - Existentially unforgeable with respect to adaptive chosen message attack (EUF-CMA)
  - Encryption
    - Semantically secure with respect to adaptive chosen ciphertext attack (IND-CCA2)
- These definitions specify security against attacks which use classical (rather than quantum) queries
- These definitions are used to judge whether an attack is relevant
- Security proofs are not required but will be considered as evidence supporting security claims
- We expect each submission specify certain parameter sets corresponding to various classical and quantum security levels
  - See next slide

Target 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

- 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
  - Limited (but easier to implement) models of computation
    - E.g. classical computing, hybrid classical-quantum attacks, adiabatic computing etc.

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

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
    - Ideally, we'd like to have something to replace Diffie-Hellman key exchange
    - Practically, we have to look into some schemes such as encryption with one-time public key, which are not quite drop-in replacements
  - Signatures
    - We'd like to have signatures with reasonable public key size, signature size, and fast signature verification
    - Practically, we shall prepare to handle probably larger public keys, or/and larger signatures
- We need to be realistic about what we can get for the quantum resistant counterpart for the existing applications

Transition and Migration

- NIST will provide transition and migration guidance when the standards are ready for post quantum cryptography
- In particular, security strength requirements may be updated to include quantum security strength besides algorithm transition
  - NIST SP 800-57 Part 1 specifies "classical" security strength levels 128, 192, and 256 bits acceptable through 2030 or beyond 2031
- Even foreseeing upcoming transition to quantum resistant cryptographic schemes, it is still required to move away from the weak algorithms/short key sizes as specified in 800-131A, i.e.
  - Anything with "classical" security strength less than 112 bits should not be used any more

Hybrid Mode

- Hybrid mode has been proposed as a transition/migration to PQC cryptography
  - Encryption: two shares of secret value S_1 and S_2 are encrypted separately as $E_1(S_1)$ and $E_2(S_2)$ with
    - currently standardized algorithm $E_1()$, e.g. RSA, and
    - a PQC algorithm $E_2()$, e.g. NTRU, separately
  - Signature: message M is signed as $Sig_1(M)$ and $Sig_2(M)$ and the signature on M is valid if and only if $Sig_1(M)$ and $Sig_2(M)$ are both valid
    - Sig_1 () is a currently standardized algorithm, e.g. RSA,
    - Sig_2 () is a PQC algorithm, e.g. XMSS.

- NIST can validate hybrid mode with certain modification on key derivation in SP 800-56A and SP 800-56B
  - Cryptographic Algorithm Validation Program (CAVP) will validate the "currently" approved portion and consider another portion as a constant

- But it is the decision for each applications considering the performance burden and
  - Submissions of hybrid modes are not in the purview of the post-quantum standardization process

Interaction with Standards Organizations

- We are aware that many international/industry standards organizations and expert groups are working on or planning to work on post quantum cryptography standards/recommendations
  - IETF
  - ETSI
  - PQCrypto
  - ISO/IEC JTC 1 SC27
- NIST is interacting and collaborating with these organizations and groups
- NIST will standardize algorithms for general usage, not for specific applications
  - NIST may consider 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
- We may not understand everything now
- Our plan is based on what we know at this point
- In the long run, we will learn together with the community and adapt our plan as we learn

Remarks and Acknowledgement

- Stay tuned for NIST formal announcement of call for proposals
- Thank NIST PQC team for review and valuable comments
- I am responsible for the opinions in this presentation