Post-Quantum Cryptography and NIST Standardization

Lily Chen and Dustin Moody

Computer Security Division, Information Technology Lab

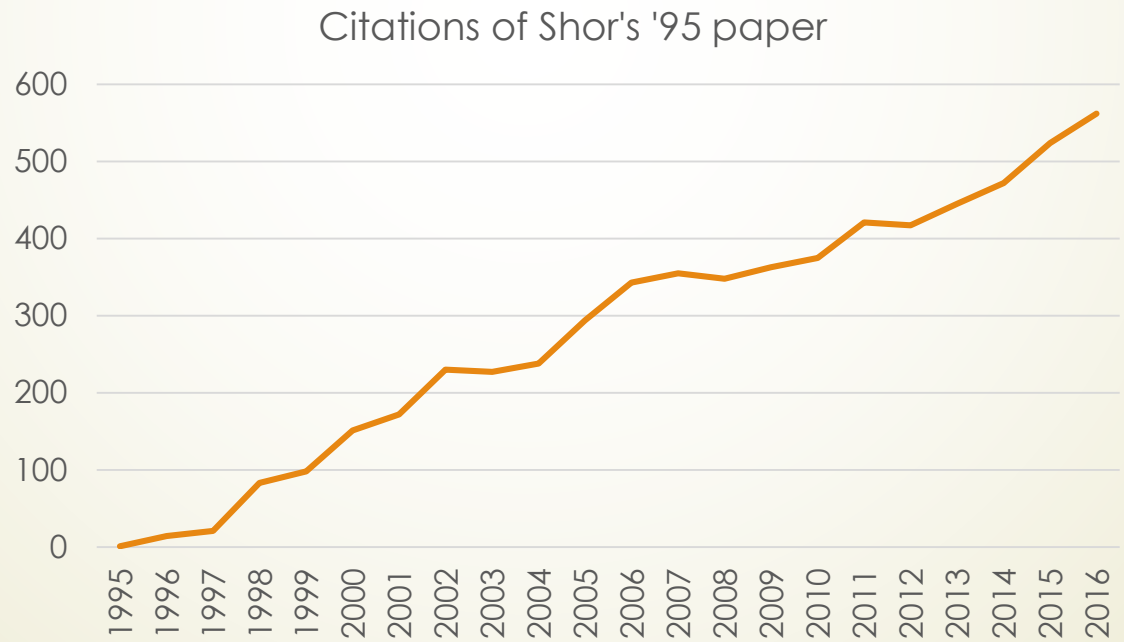
National Institute of Standards and Technology (NIST)

Background

- Quantum computing – a gamechanger?
  - An integer *n* can be *factored* in polynomial time using Shor's algorithm
  - Shor's algorithm also solves *the discrete logarithm problem* in polynomial time
- Public-key crypto deployed since the 1980s will need to be replaced
  - Signatures: RSA, DSA and ECDSA (FIPS 186-4)
  - Key Agreement: Diffie-Hellman over finite field and elliptic curves (NIST SP 800-56A)
  - Encryption: RSA (NIST SP 800-56B)
- Impact for symmetric-key crypto:
  - 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 (assuming 2^{64} quantum operations cost about the same as 2^{64} classical operations)

Post-Quantum Cryptography (PQC)

- Cryptosystems which run on classical computers, and are considered to be resistant to quantum attacks
  - Also known as “quantum-safe” or “quantum-resistant” crypto
- Focus is on public-key crypto



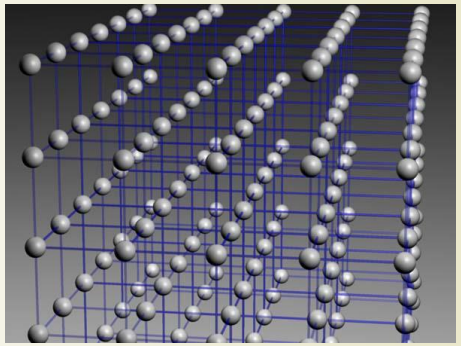
What we have done so far – The first mile in a long journey

- 2012 – NIST begins PQC project
  - Research and build NIST team
- April 2015 – 1st NIST PQC workshop
- Aug 2015 – NSA statement
- 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)

NIST PQC team – The most significant in the first mile

- Consists of 10+ NIST researchers in cryptography, quantum information, quantum algorithms
- Hold bi-weekly seminars (internal and invited speakers)
- Publish results at PQcrypto and other journals/conferences
- Engage with research community (presentations and discussion forums)
- Work with industry and standards organizations (ETSI, IETF, ISO/IEC SC27)
- Reach government agencies for raising awareness of upcoming cryptography transition
- Collaborate with QuiCS (Joint Center for Quantum Information and Computer Science), University of Maryland

Post-Quantum Cryptography- What has been in the standards and research?



- The main categories of PQC schemes
  - **Lattice based** (e.g. NTRUencrypt, New Hope)
  - **Code based** (e.g. McEliece)
  - **Multivariate** (e.g. Rainbow)
  - **Other** (e.g. isogenies on supersingular elliptic curves SIDH)
  - **Hash based** signatures (e.g. XMSS and SPHINCS)
- Research has been rapidly advancing in the past five years
  - Many schemes are proposed and analyzed. Some are broken under classical attacks
- Industry has been moving towards quantum resistant cryptosystems
- Some standards organizations have considered specific schemes (e.g. IETF, hash-based signature) and some expert groups (e.g. EU PQcrypto) made recommendations

PQC Standardization – Is it too early?

- It has been a long debate among researchers and practitioners on whether it is too early to look into PQC standardization

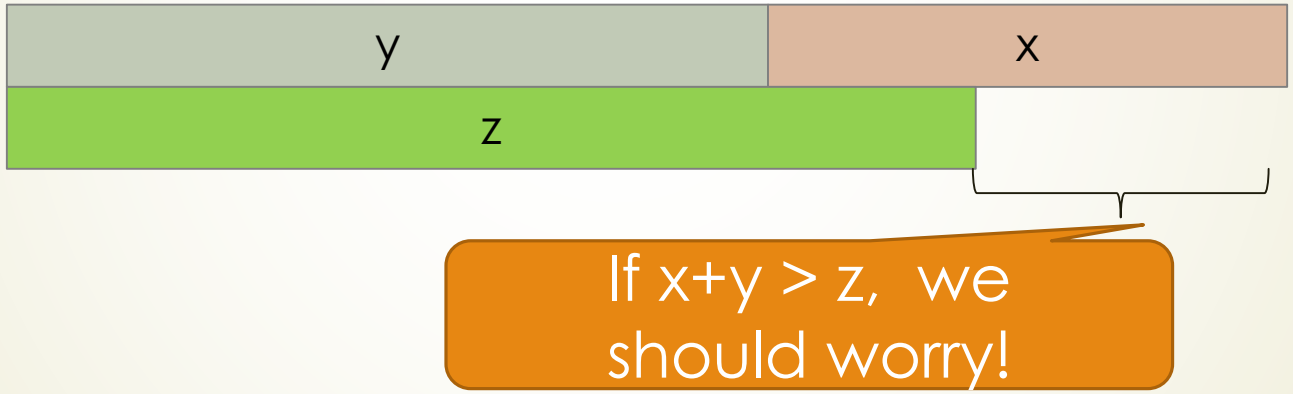
- "A 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."

  – Dr. Michele Mosca, U. of Waterloo

- Our experience tells that we need at least several years to developing and deploying PQC standards

Mosca's Theorem

- y is the time taken for developing and deploying PQC standards
- x is the time for "backward secrecy" (maintain secrecy for information encrypted x years ago)
- z is the time before quantum computers are available



- If we require 5-year backward secrecy, we certainly need to start standardization

Post-Quantum Cryptography Standardization – A big decision to move forward

- Considering the time to develop/deploy PQC standards and the backward secrecy required for information, **it is the time** to look into standardization
- NIST sees its role as managing a process of achieving community consensus in a transparent and timely manner
- NIST announced its preliminary plan of developing PQC standards at PQCrypto 2016
  - The announcement received strong support from research community
- NIST released draft of call for proposals in August 2016
  - Scope – public key signatures, encryption, key-exchange
  - Evaluation Criteria
    - Security: security models, target security strengths – classic and quantum
    - Performance: key size, signature size, computational efficiency, and flexibility
  - Plans for the Evaluation Process

PQC Standardization Plan

Timeline	
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

The selection criteria

- 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

Complexities of PQC Standardization

- Much broader scope – three crypto primitives
- Both classical and quantum attacks
- Both a theoretical and practical aspect to assess security
- Multiple tradeoff factors
- Migrations into new and existing applications
- Many challenges which we haven't dealt with in previous standards
- Field is still undergoing active research
  - Requirements and timeline could change
- Not exactly a competition – it is and it isn't

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
- These definitions specify security against attacks which use classical (not quantum) queries

Quantum Security – How to assess it?

- Currently, NIST cryptography standards specify parameters for classical security levels at 112, 128, 192, 256 bits
- For PQC standardization, need to specify concrete parameters with security estimates
  - Led to the bits of quantum security requirements in the draft CFP
- 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

Quantum Security Strength Categories

	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
  - Number of classical elementary operations, quantum circuit size, etc…
  - 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.
- These are understood to be preliminary estimates

Challenges

- A quantum security strength assessment is just one of the objectives, while the first and the foremost is classical security
  - Most of PQC schemes are relatively new
  - It takes years to understand their classical security – more so for quantum security
  - Best practical attacks may be classical, even if quantum ones are asymptotically better
- We need to deal with new situations which we haven't considered before, e.g.
  - Decryption failure
  - Public-key encryption vs. key-exchange issues
    - Validation/Ephemeral key exchange (no key-pair reuse, consider passive attacks, IND-CPA)
  - Auxiliary functions/algorithms, e.g.
    - Gaussian simulation
- We have to move away from many things we have been using with existing schemes

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

- Preliminary conclusions: efficiency likely OK, but key sizes may pose a significant challenge

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, (and to handle a stateful situation)
- We need to be realistic about what we can get for the quantum-resistant counterpart for existing applications

Transition and Migration

- NIST will update guidance when PQC standards are available
  - SP 800-57 Part I specifies "classical" security strength levels 128, 192, and 256 bits are acceptable through 2030
- Even with the upcoming PQC transition, still required to move away from weak algorithms/key sizes:
  - Anything with "classical" security strength less than 112 bits should NOT be used anymore

Hybrid Mode

- A "hybrid mode" has been proposed as a transition/migration step towards PQC cryptography
  - Key establishment by two schemes:
    - A current approved schemes to obtain S_1 and
    - A post-quantum scheme to obtain S_2
    - The keying material is derived from S_1 and S_2
  - 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.
- Current FIPS 140 validation will only validate the approved component
- The PQC standardization will only consider the post-quantum component

Interactions 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
  - IEEE P1363.3 has standardized some lattice-based schemes
  - IETF is taking action in specifying stateful hash-based signatures
  - ETSI released quantum-safe cryptography report
  - EU expert groups PQCrypto and SafeCrypto made recommendations and released reports
  - ISO/IEC JTC 1 SC27 has already had three six months study periods for quantum-resistant cryptography
- NIST is interacting and collaborating with these organizations and groups
- NIST plan to consider hash-based signatures as an early candidates for standardization, but probably just for specific applications like code signing

Summary

- Post-quantum cryptography standardization is going to be a long journey
- Be prepared to transition to new algorithms in 10 years
- After the first mile, we have observed many complexities and challenges
- NIST acknowledges all the feedback received, which has improved the submission requirements and evaluation criteria
- We will continue to work with the community towards PQC standardization
- See also: www.nist.gov/pqcrypto
  - Sign up for the pqc-forum for announcements and discussion