Challenges in Post Quantum Cryptography Standardization

(Lily) Lidong Chen
National Institute of Standards and Technology
USA

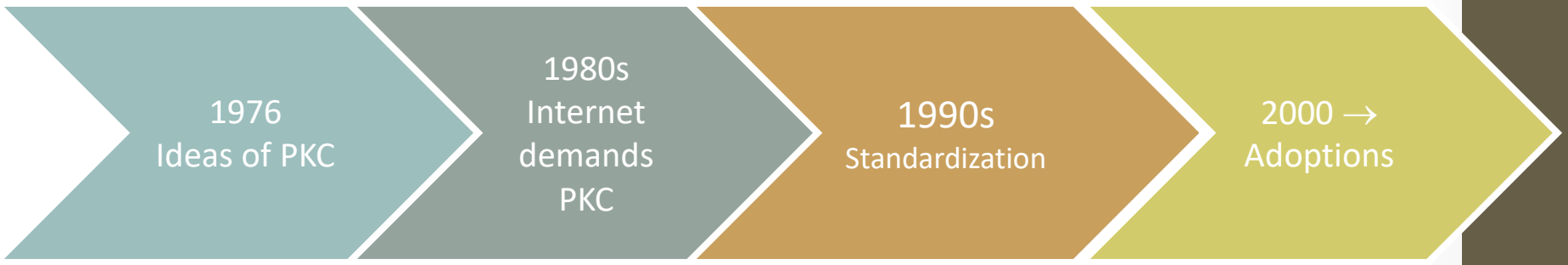
Outline

- History of public key cryptography (PKC) standardization
- Post quantum cryptography (PQC) families
- Challenges in PQC standardization
- Moving forward - Strategies

2016 – 40 Year Anniversary of Public Key Cryptography

- 40 years ago, public key cryptography was presented as a fascinating research idea
- Today, public key cryptography has become the corner stone of information and communication security
  - Public key cryptography schemes have been specified in the standards (IEEE P1363, IETF, NIST, X9, ISO/IEC, TCG, etc.) for different applications
    - Signatures
    - Encryption
    - Key agreement
  - Public key cryptography is used in every dimension of the cyber space, e.g.
    - Web browsing
    - VPN

Recapture the History



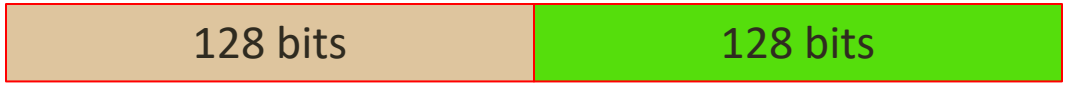
Public Key Cryptography

- Most widely deployed public key cryptography schemes are based on either
  - Factorization problem, e.g.
    - RSA encryption and RSA signature
  - Discrete logarithm problem (CDH problem, DDH problem, etc.) e.g.
    - DSA, DH, MQV
- These problems are hard under the conventional computing techniques

Quantum Computing Technology and Its Implications

- Quantum computing changed what we have believed about the hardness of discrete log and factorization problems
  - Using quantum computers, to factor an integer *n*, Shor's algorithm runs in polynomial time
  - The discrete logarithm problem can be solved in the same scale of complexity
- With such results, all the public key cryptosystems deployed since the 1980s must be replaced with the quantum-resistant counterparts in the quantum computing era

- Grover's search algorithm proffers a quadratic speedup on search problems
  - The impact to the symmetric key cryptography system is to push for larger key/hash size (≈2 times larger)



- In order to protect the information and communication systems in a quantum era, we need to introduce cryptographic schemes which are quantum computing resistant

Post Quantum Cryptography

- The main categories of PQC schemes
  - Lattice based (e.g. NTRUencrypt)
  - Hash based signatures (e.g. XMSS)
  - Code based (e.g. McEliece)
  - Multivariate (e.g. Rainbow)
  - Other
- Not all of the schemes were proposed recently for quantum resistant purposes
  - Some of the schemes were proposed as early as in 1978 (about the same time when RSA and DH were proposed)
  - Reconsidered recently for their quantum computing resistant property

Moving Towards PQC Standardization

- We have more than 20 years experience in PKC standardization
- Will the experience be sufficient for developing PQC standards?
- In other words, do we know what we think we know?

Lattice Based Cryptosystem
- Early proposed schemes

- Shortest Vector Problem (SVP) is NP-hard under randomized reductions
  - There are other related problems in lattice based on which cryptosystems can be built
- Ajtai and Dwork (1997) described a lattice-based public key cryptosystem with worst-case to average case reduction
  - The security proof showed that every instance of the unique shortest vector problem could be transformed into a random instance of their cryptosystem with high probability
  - It encrypts one bit for each operation, not practical
- Goldreich, Goldwasser, and Halevi (1997) proposed a more practical lattice-based cryptosystem (GGH)
  - GGH is fast, but requires megabyte-size public keys to be secure
- NTRU was presented in 1996 by Hoffstein, Pipher and Silverman
- NTRU includes two algorithms
  - NTRUencrypt
  - NTRUsign
    - the early version has been found vulnerable to attacks

NTRUencrypt

- It is typically described using the ring of convolution polynomials
  - Polynomial ring R = Z[X]/(X^n-1), where each element is an n-1 degree polynomial over Z
- Convolution products of polynomials can also be expressed as multiplication with a circulant matrices
  - It is possible to describe NTRU using lattices
  - Its security is related to the hardness of lattice problems in a very special class of lattices
- NTRUencrypt has been standardized in
  - IEEE P1363.1 -2008
  - ANSI X9.98 - 2010
- NTRUencrypt has been introduced in IETF
  - as a ciphersuite for TLS (2001) (not moved forward)
  - as a hybrid mode for TLS
    - draft-whyte-qsh-tls12-00 (2015)
- At the same security strength, the key size is larger than that of RSA but it is manageable
- The performance is comparable with RSA in encryption operation but much faster in decryption operation
- Provably secure version of NTRU encryption is less efficient
  - It is proved to be as secure as worst-case problems over ideal lattice

Lattice Based Cryptosystem

- More lattice based cryptosystems have been proposed based on different hard problems in lattices
- In 2006, Regev introduced a PKE cryptosystem based on the LWE problem
- Lattice based signatures have been proposed with improved security and efficiency in recent years e.g.
  - Lattice-based signature schemes based on short integer solution (SIS) (2012) by Lyubashevsky et al.
  - BLISS (Bimodal Lattice Signature Scheme) (2013) by Ducas et al.
- DH-like key exchange schemes and key encapsulation mechanisms (KEM) based on Learning With Error (LWE) problem
  - First proposal by Ding et. al in 2012
  - KEM by Peikert in 2014
  - Integration to TLS by Bos et.al 2015
- Lattices have been used to construct fully homomorphic encryption and other cryptographic schemes beyond encryption and signature

Hash Based Signatures -1

- The original idea was presented as Merkle signature scheme (MSS) in 1979
- The keys are represented as a tree
  - The one time public/private keys are represented as the leaves while the master public key is the root
- A Merkle tree can be used to sign a limited number of messages
- It is stateful because each private key can be used only once
- Hash based signatures are based on well understood assumption on hash functions

Hash Based Signatures - 2

- The improved versions are more efficient with regard to the signature size and the maximum number of signatures each tree can be used to generate
- Some stateless versions of hash based signatures were proposed
  - SPHINCS by Bernstein et. al
- The signature size is usually much larger than RSA, depending on the size of the tree, which determines the number of messages a tree can be used to sign
- Encryption schemes cannot be built based on hash functions
- IETF has internet drafts on hash based signatures
  - XMSS: Extended Hash-Based Signatures (draft-irtf-cfrg-xmss-hash-based-signatures-01)
  - Hash-Based Signatures (draft-mcgrew-hash-sigs-03)

Code Based Cryptosystems

- The McEliece cryptosystem was proposed in 1978
- It is built on (binary) Goppa codes and its security is based on the syndrome decoding problem
- The original version of the McEliece cryptosystem has a key length of million of bits
  - Probably, this is the reason for not being adopted at the time it was proposed
- The security has stood the test of time
- Some optimized versions have been proposed to reduce the key size to less than 10K/20K (public/private keys), e.g.
  - quasi-cyclic (QC) moderate density parity check (MDPC) and
  - quasi-cyclic (QC) low rank Parity check (LRPC)
- The signature schemes are less mature and inefficient in this family
- So far, no known standard organization has approached Code based cryptosystems

Multivariate Cryptographic Schemes

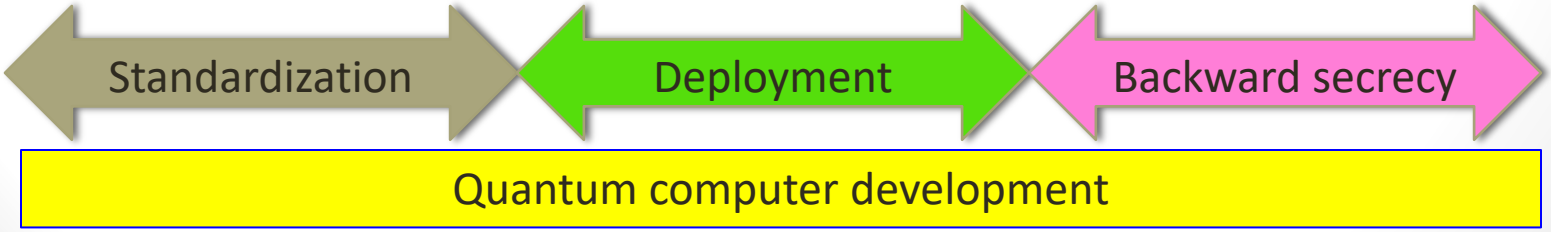
- This family of cryptographic schemes is based on the problem of solving a system of quadratic equations
- The first scheme C* in this family was proposed in 1988, which was broken in 1995
  - In the same family, SFLASH was proposed as C*_ and then a repaired version was proposed as pFLASH
- In 1996, Patarin proposed cryptosystems using Hidden Fields Equations (HFE) trapdoor functions
- The research on multivariate cryptosystems has been motivated by its property of resisting quantum computing
- The structure is considered more suitable for signatures e.g.
  - Rainbow signatures - public key is large while signature size can be reduced
  - HFE and HFEv- variants - comparable in signature size to schemes like RSA and ECC
- The family has evolved very rapidly with many variants
- No standard organizations have considered multivariate cryptosystems*
  - * SFLASH was selected by New European Schemes for Signatures, Integrity and Encryption (NESSIE 2000-2003) but was broken in 2007

Standard Related Activities on PQC

- Three ETSI Quantum-Safe Workshops since 2013
- ETSI quantum-safe cryptography white paper - 2014
- NIST Workshop on Cybersecurity in a Post-Quantum World 2015
- ISO/IEC JTC 1 SC27 Study Period on Quantum Computing Resistant Cryptography April – October 2015
  - Received contributions from Japan and Russia
  - The study period is extended to April 2016
- PQCRYPTO project in EU
  - Initial recommendation September 2015
    - Public key encryption - McEliece with binary Goppa codes (with parameter specification)
      - Other choice under evaluation: (1) Quasi-cyclic MDPC (2) Stehlé – Steinfeld provably secure version NTRU
    - Signature – hash based XMSS (stateful) and SPHINCS-256 (Stateless)

Challenges on Starting up

- How far are we from the quantum era?
  - Engineers predict that within the next 20 or so years sufficiently large quantum computers will be built to break essentially all public key schemes currently in use
- At least, it takes five years to come up with generally acceptable standards
- Another five years are needed to deliver the products to the market and also to make the transition
- To provide 5-10 years backward “confidentiality”, it is already not too early to consider standardization



Challenges on Selection Criteria

- Compared with 20-30 years ago, more security concepts have been introduced
  - How much to weigh security proofs
  - Which security definitions shall we use
- New research results appear constantly on PQC, e.g. break an existing system and/or propose an improved version
  - What will happen on the way to standardize, if
    - Weaknesses are discovered, or
    - An improved version is significantly better

Challenges on Migration

- Key size and signature size are significantly larger than currently deployed cryptosystems, e.g.
  - McEliece has millions of bits in its public key
  - Hash based signature XMSS has a signature size 19k bits (for 2^{20} signs)
- Signature and encryption may not be from the same family, not like RSA, considering the current promising candidates
  - Encryption (Code based and lattice based)
  - Signature (hash based and multivariate)
- To provide perfect forward secrecy for key establishment
  - Use one time public key
    - Need at least three messages
  - Use R-LWE key agreement
    - Not as symmetric as Diffie-Hellman

Challenges on Industry Involvement

- Academic community has been more enthusiastic on PQC than industry
  - Many conferences/workshops
  - Active research on the existing and new schemes
  - Recommendations on potential PQC standardization candidates
- Possible reasons
  - Replacing the old system implies investing many resource
  - The urgency is not clear because quantum computers are not available
  - No outstanding winners among the candidates
  - Some proprietary development is not ready to share yet
- Industry involvement is critical
  - Standardization needs input from industry to understand
    - impact on current applications
    - issues with any specific implementation environment

Moving Forward – Start Now

- There is a long way to go from the research literature to standards
  - Concrete details in algorithms specifications
    - Parameters (e.g. mathematics structures, key length)
    - Padding methods
    - Components (e.g. hash functions, key derivation functions, etc.)
- A lot of issues cannot be identified without actually developing standards
- A possible path is to
  - Start from specifying cryptography primitives
  - Integrate to protocols (like IKE, TLS)

Moving Forward – Security Criteria

- Compared with 30 years ago, we are more vulnerable to security failures
  - Advanced infrastructure
  - Pervasive network connection and information flow
- Security must be the first consideration
  - Security proof adds confidence but should not be the solely considered criteria
    - Still need to look into weak cases and physical attacks, like side channel attacks
  - Assess security based on basic security definitions, e.g.
    - IND-CCA2 for encryption
    - EUF-CMA for signature

Moving Forward - Migration

- Adapt the existing protocols for
  - Large keys/signatures
  - New key agreement schemes
- Test implementation for different schemes
- Introduce cryptographic agility in new designs

Moving Forward – Engage Industry

- Provide educational opportunities and raise awareness of quantum computing threats
  - Presentations and panels in the industry forums, standard organizations, etc.
- Make clear recommendations on
  - A smaller pool of potential candidates (e.g. EU PQcrypto project)
- Promote research on PQC implementations to identify impacts and issues
  - Prototype implementations and benchmarks

Summary

- It is the time to move forward on post-quantum cryptography standardization
- Security should be the basic and essential selection criteria
- The situation is different from that of developing the first generation public key cryptography standards
- What we learnt in the past 40 years is still useful but not sufficient
- Many new situations to handle and we still need to learn!

Acknowledgement

- Thank NIST PQC team for review and valuable comments
- I am responsible for the opinions in this presentation