Next Generation Cryptographic Standards

– Challenges and Solutions

Lily Chen
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

History and Fact Sheet

- NIST developed the first encryption standards in 1970s, Data Encryption Standard (DES), and published as Federal Information Processing Standard (FIPS) 46
- Over 40 years, NIST continues to evolve its cryptographic standards
  - Enable the usage of new cryptographic technologies to respond the growing application demand
  - Enhance security strength to deal with advanced and more sophisticated cryptanalysis methods

Nearly all commercial laptops, cellphones, Internet routes, VPN servers, and ATMs use NIST Cryptography

NIST Cryptographic Standards

NIST

- Cryptographic standards
  - Public key based
    - Signature (FIPS 186)
    - Key establishment (800-56A/B/C)
  - Tools
    - RNG (800-90A/B/C)
    - KDF (800-108, 800-135)
  - Symmetric key based
    - AES (FIPS 197)
    - TDEA (800-67)
    - Modes of operations (800 38A-38G)
    - SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
    - Randomized hash (800-106)
    - HMAC (FIPS 198)
    - SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)
  - Guidelines
    - Hash usage/security (800-107)
    - Transition (800-131A)
    - Key generation (800-133)
    - Key management (800-57)

Challenges in Next Generation of Crypto Standards

- Deal with extremes
  - Extremely powerful attack technologies, e.g. using quantum computers
  - Extremely constrained implementation environment, e.g. sensors
- Transition, forward secrecy, and backward compatibility
  - Increased key sizes, stronger hash functions
  - Post-quantum cryptography
- Extended security objectives and features
  - Deal with more sophisticated cryptanalysis methods, e.g. side-channel attacks, multiple-key/target attacks, etc.
  - Demand useable features, e.g. misuse resistance
- Special usage vs. general purpose standards
  - Some standards are developed for special usage, e.g. lightweight cryptography
- Synchronize with industry best practice and promote international adoption
  - Organizations tend to create standards divergent from existing ones

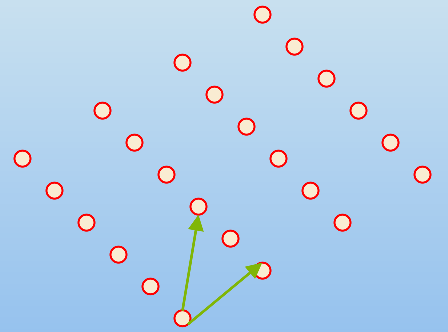
Post-Quantum Cryptography

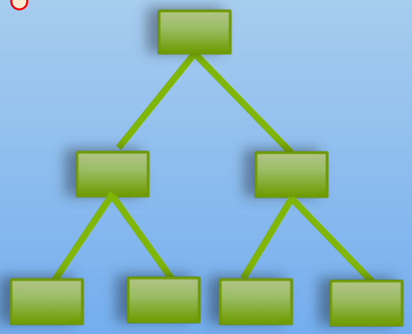
Quantum Impact

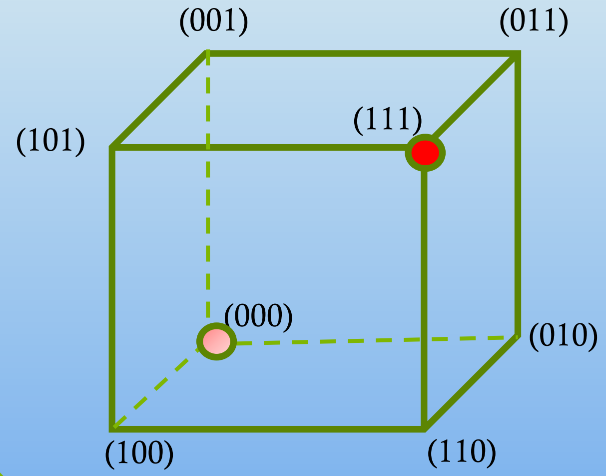
- Quantum computing changed what we have believed about the hardness of discrete log and factorization problems
  - Shor's algorithm with full scale quantum computers can solve integer factorization and discrete logarithm problems in polynomial time
- As a result, the public key cryptosystems deployed since the 1980s will need to be replaced
  - RSA signatures and ECDSA (FIPS 186-4)
  - Diffie-Hellman Key Agreement over finite fields and elliptic curves (NIST SP 800-56A)
  - RSA encryption (NIST SP 800-56B)
- Quantum computing also impacts security strength of symmetric key based cryptographic algorithms
  - Grover's algorithm can find n - bit AES key with approximately $\sqrt{(2^n)}$ operations – It can be mitigated by increasing the key size

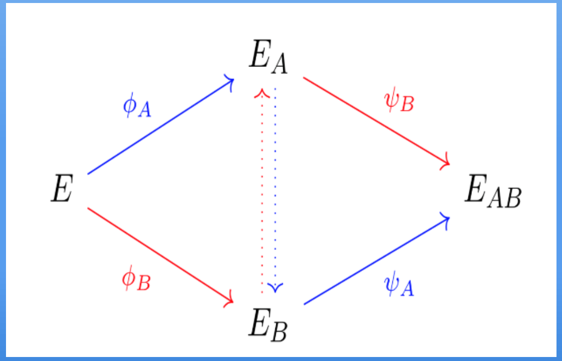
Post-Quantum Cryptography (PQC)

- Some actively researched PQC categories
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key -based signatures
  - Isogeny-based schemes









$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$
$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$
$$\vdots$$
$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j \;+\; \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

NIST PQC Process Update: Milestones and Timeline

- **2016** Determined criteria and requirements
  Announced call for proposals
- **2017** Received 82 submissions
  Announced 69 1st round candidates
- **2018** 1st round analysis
  Held the 1st NIST PQC standardization Conference
- **2019** Announced 26 2nd round candidates
  Held the 2nd NIST PQC Standardization Conference
- **2020** Announced 3rd round 7 finalists and 8 alternate candidates
- **2021** Held the 3rd NIST PQC Standardization Conference (Virtual)
- **2022** Make the 1st set selection
- **2022-2023** Release draft standards and call for public comments

Scope, Security Definitions, Strength Levels for PQC

- The scope of NIST PQC standardization
  - Public key encryption / Key establishment
  - Digital signature
- Definitions (proofs recommended, but not required) used to judge whether an attack is relevant
  - IND-CPA/IND-CCA2 for encryptions and KEMs
  - EUF-CMA for signatures
- Security strength is defined at 5 levels

Level	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)

First, Second, and Third Round PQC Candidates

NIST

1st round	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variat			
Stateless Hash/Symm based			
Other			
Total			

2nd round	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-			
Statel Hash/			
Isogen			
Total			

3rd round	Signatures		KEM/Encryption		Overall	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	3	4	5	7	8

Challenges and Considerations in Selecting Algorithms

Security

- Security levels offered
- (confidence in) security proof
- Any attacks
- Classical/quantum complexity

Performance

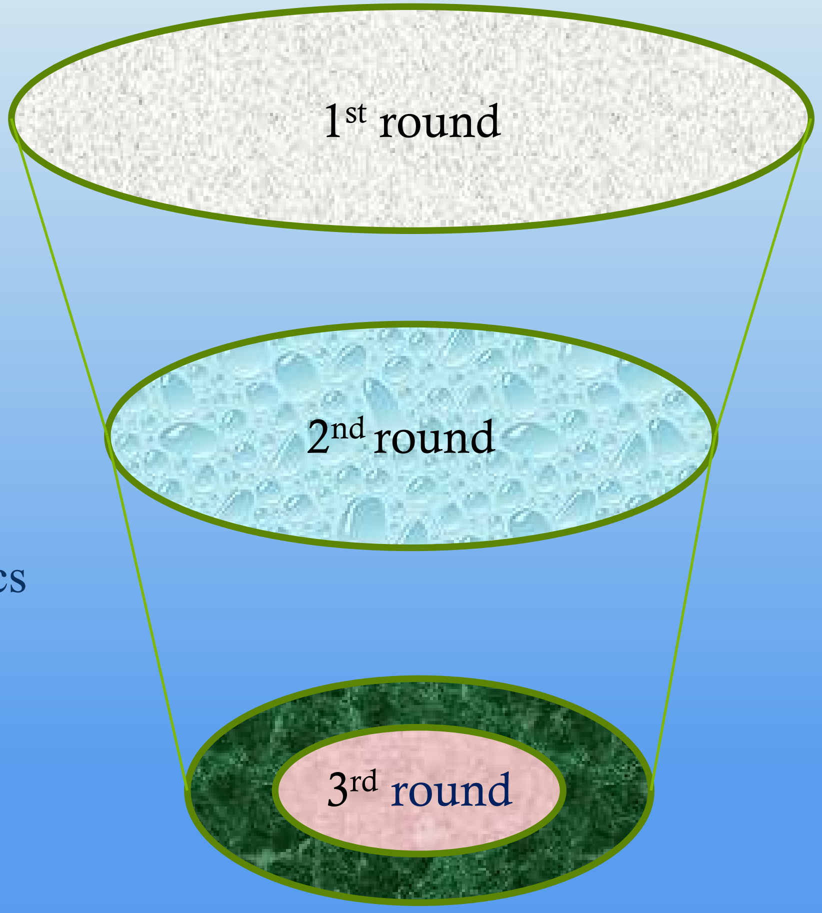
- Size of keys, signature, ciphertext
- Speed of KeyGen, Enc/Dec, Sign/Verify
- Decryption failures

Algorithm and implementation characteristics

- IP issues
- Side channel resistance
- Simplicity and clarity of documentation
- Flexibility

Other

- Official comments/pqc-forum discussion
- Papers published/presented



PQC Transition and Migration

- Public key Cryptography has been used everywhere; two most important usages:
  - Communication security; and
  - Trusted platforms
- Transition and migration are full of exciting adventures
  - Understand new features, characters, implementation challenges
  - Identify barriers, issues, show-stoppers, needed justifications, etc.
  - Reduce the risk of disruptions in operation and security
- For early adoption in code-signing, NIST specified stateful hash-based signature in SP 800-208 (LMS, XMSS)
- Accommodate hybrid mode, e.g. PQC+ECDH, in SP 800-56C key derivation
  - Enable current NIST approved mechanisms, e.g. ECDH, to obtain FIPS 140 validation

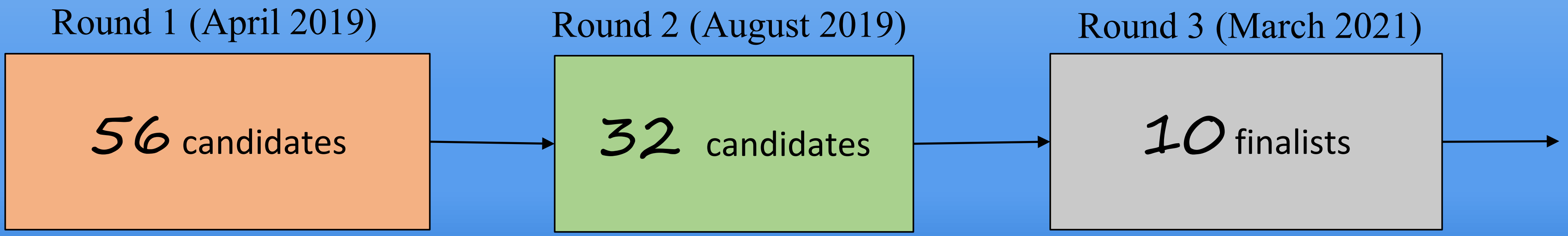
Lightweight Cryptography

Lightweight Cryptography (LWC)

- Recognize the need for cryptographic standards for applications in constrained environment that are not well-served by existing NIST standards
  - Internet of Things (IoT), pervasive computing, healthcare monitoring systems, automated management of supply chain, public transportation, telephone cards
- The task is not light – more challenging in the design to satisfy all security requirements and performance for different platforms
  - Achieve security goals with limited resource – The attackers are not constrained
  - Different applications/constraints – Industry presented needs are either very broad or too specific
- It has been a difficult decision for NIST to initiate a call for proposals
  - Held two workshops in 2015 and 2016 to get industry feedback and published NISTIR 8144 in 2017
  - The scope and criteria were finalized in 2018 – Call for contributions

Lightweight cryptography candidates

- Scope: Authenticated Encryption with Additional Data (AEAD) with optional hashing functionality
- The candidates include (tweakable) block ciphers, stream ciphers, permutation, …
  - The designs reflected the technology advance in the past 20 years
  - Most designs are based on the primitives used in the standardized algorithms such as AES, Keccak, PHOTON, SKINNY, SPONGENT, etc.
  - Many candidates claimed additional security features: Nonce misuse security, releasing unverified plaintext (RUP) security, post-quantum security, side-channel resistance, etc.



Towards Lightweight Cryptography Standards

- Security analysis and maturity assessment were mainly provided by the design teams and independent third parties
- The performance is evaluated in software and hardware
  - Targeted devices, optimized implementations
  - Hardware API. FPGA, ASIC
- Expect to announce final winner(s) in summer of 2022

Exploratory Projects and Long-term Strategy

Special Efforts

- Next generation crypto standards shall provide additional features, e.g.
  - Threshold cryptography – Prevent from single failure point through secure multiparty computation
  - Privacy enhanced cryptography – Enable processing collected and protected data
- Continue to enhance open and transparency and improve scientific quality and useability of cryptographic standards
- Engage with application community and enable crypto agility for smooth transition
- Adopt industry best practice and work with standards organizations to promote global acceptance

Threshold Cryptography - Eliminate single-point of failure

NIST

- Multi-party threshold schemes for key-based cryptographic primitives
  - Key-generation (e.g., RSA, ECC, AES)
  - Signing (e.g., RSA, ECDSA, EdDSA)
  - Enciphering (e.g., AES, lightweight ciphers)
  - Decryption (e.g., RSA)
  - Random number generation
  - Post-Quantum Cryptography (emerging standards)
- Towards guidelines on threshold implementations
- 2019-2020: Two workshops
  - Threshold schemes and implementations
  - Feedbacks from the community

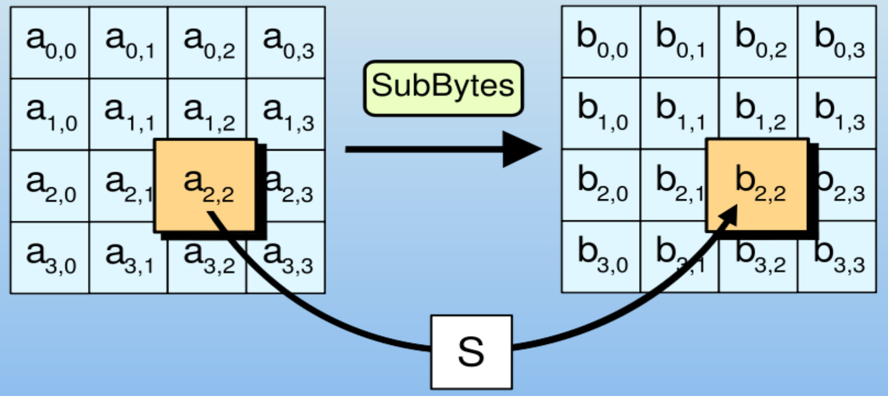
- NISTIR 8214 Threshold Schemes for Cryptographic Primitives: Challenges and Opportunities in Standardization and Validation of Threshold Cryptography
- NISTIR 8214a NIST Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives – Call for public comments (July 2 – September 13, 2021)

Privacy Enhancing Cryptography (PEC)

- Privacy enhancing cryptography is highly demanded in modern applications
- Some academic and industry initiatives approached various cryptographic tools for standardization, e.g.
  - Zero-knowledge proof (ZKProof)
  - Fully homomorphic encryption
- NIST researchers participated in and contributed to the initiatives
  - Evaluate potentials to standardize PEC tools
- NIST has organized "Special Topics on Privacy and Public Auditability" (STPPA) series" since January 2020
- NIST researchers conducted research on privacy solutions in Covid-19 contact tracing
  - Measure aggregate levels of encounters in a population while preserving the privacy of individuals

Cryptographic Publication Review

- NIST has about 40+ years of history of publishing cryptographic standards
- It is critical to improve their scientific quality and useability to match advanced technology and meet the requirements of emerging applications
- In NISTIR 7977
  - *“Review standards and guidelines regularly. … FIPS are reviewed at least every five years or more frequently if issues arise.”*
- NIST Cryptographic Technology Group established Review Board
  - Assign internal reviewers, solicit public comments, and propose review decisions



- AES has published for 20 years!
- The 1st round of public comments (May 10, 2021 – June 11, 2021)
- NISTIR 8319 Review of the Advanced Encryption Standard (July 2021)
  - A list of proposed changes

Cryptographic Transition

- Transition to stronger cryptography is constantly required because
  - Increased computing power by Moore's Law
  - New computing technologies such as quantum computers
  - More sophisticated cryptoanalysis techniques
- Historically, NIST has guided many transitions (see SP 800-131A), e.g.
  - Block ciphers: DES → Triple DES → AES
  - Hash functions: SHA-1 → SHA-2 and SHA-3 families
  - RSA signature and encryption: modulus 1024 bits → ≥ 2048 bits (80 bit to minimum 112-bit security)
- Cryptographic agility is very important for future transitions
  - Allow to make smooth transition between algorithms and configurations

- NCCoE initiated project partnership for migration to Post-Quantum Cryptography
- Industry participants and other interested parties are invited to participate in the Migration to Post-Quantum Cryptography project. (See NCCoE announcement)

Summary

- It is full of challenges and opportunities in developing next generation cryptography standards
- Future technologies will shape the trends of cryptography applications
- Next generation cryptography standards will deal with
  - Quantum threats with Post-quantum Cryptography
  - Protection demand for constrained environment with Lightweight Cryptography
- Transition will be constantly required
  - Cryptographic agility is the key
- Please join discussions through different mailing list (information is provided at each project website)
- Comments, questions, suggestions always help NIST to improve cryptographic standards – communication is the key

Thanks!

lily.chen@nist.gov

For more information on NIST cryptographic standards, please visit http://csrc.nist.gov