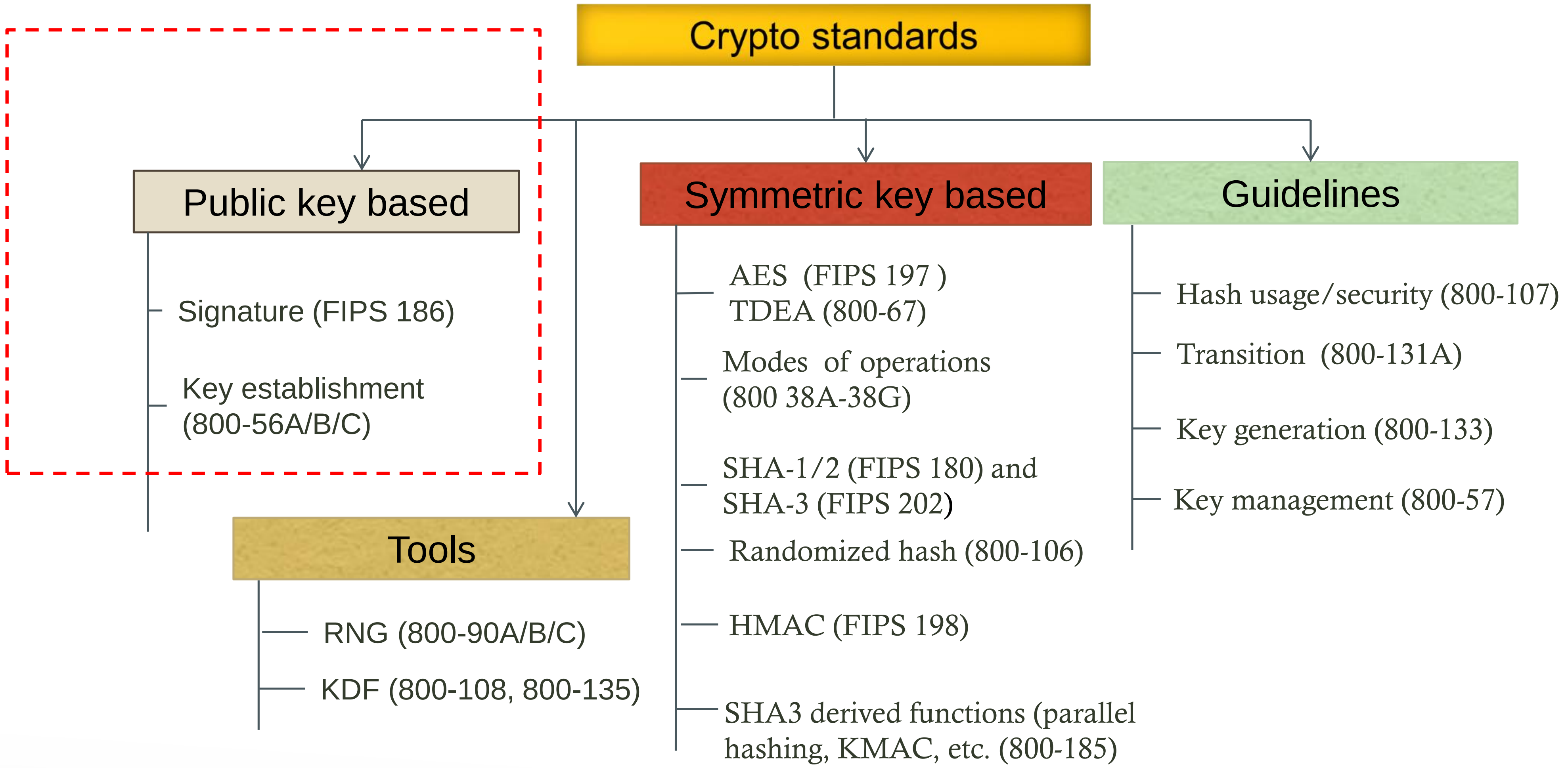
NIST Cryptographic Standards for Trusted Platform in Quantum Era

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

NIST Cryptographic Standards



NIST Public Key Cryptography Standards

- NIST standardized public key cryptographic schemes are based on two "hard problems" and some of these algorithms are used in today's TPM

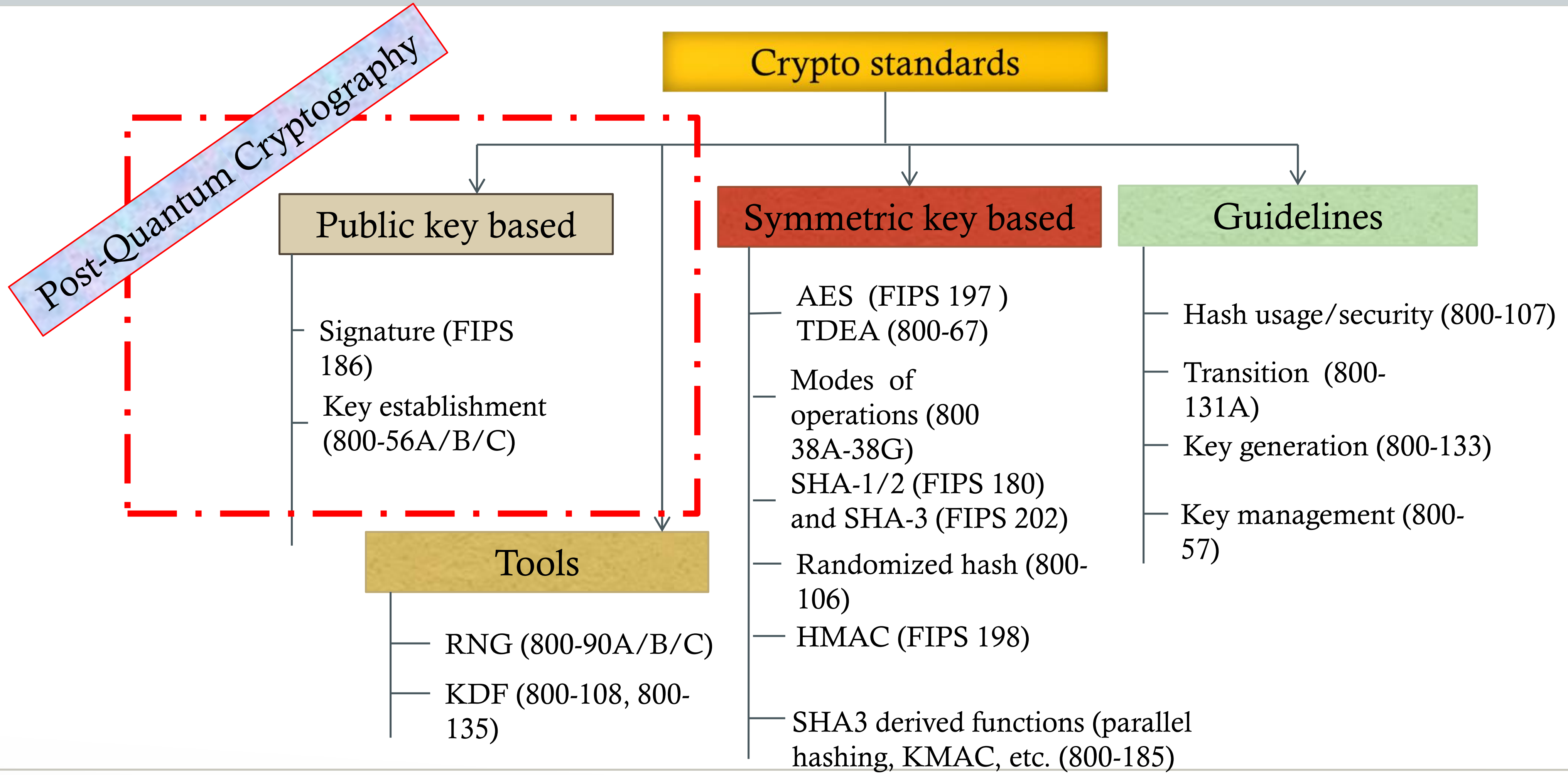
Integer Factorization
- RSA encryption (SP 800-56B) for key establishment)
- RSA signatures (FIPS 186)

Discrete Logarithm
- DH/ECDH and MQV/ECMQV (SP 800-56A for key establishment)
- DSA and ECDSA (FIPS 186)

Quantum Impact

- Emerging quantum computers changed what we have believed about the hardness of discrete log and factorization problems
  - Using quantum computers, an integer $N = p \cdot q$ can be factored in polynomial time using Shor's algorithm
  - The discrete logarithm problem, find x, given y can such that $g^x = y \bmod p$, also be solved by Shor's algorithm in polynomial time
- As a result, the public key cryptosystems deployed since the 1980s will need to be replaced
  - RSA signatures, DSA 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)
- We have to look for quantum-resistant counterparts for these cryptosystems
- Quantum computing also impacted security strength of symmetric key based cryptography algorithms
  - 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, if 2^{64} quantum operations cost about the same as 2^{64} classical operations

Quantum Impact to NIST Standards



NIST PQC Initiative

- NIST Crypto program started to build a research team since 2012
  - Today NIST PQC team consists of a dozen of researchers with background in cryptography, quantum algorithms, crypto standards, etc.
- In 2015 -2016, we started to prepare for PQC standardization
  - The first workshop was held in April 2015
  - Published NIST IR 8105 in 2016
- NIST announced call for proposals in Dec. 2016

The Selection Criteria

- Security - 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 for key establishment
  - Resistance to side-channel attacks
  - Simplicity and flexibility
  - Misuse resistance, and
  - More
- The draft requirements and criteria were announced in August 2016 to call for public comments

Understand the Challenges

- Much broader scope – three crypto primitives
- Both classical and quantum attacks
  - Security strength assessment on specific parameter selections
- Consider various theoretical security models and practical attacks
  - Provably security and security against instantiation or implementation related security flaws and pitfalls
- Multiple tradeoff factors
  - Security, performance, key size, signature size, side-channel attack countermeasures
- Migrations into new and existing applications
  - TLS, IKE, TPM/code signing, PKI infrastructure, and much more
- Not exactly a competition – it is and it isn't

Differences with Past Competitions

- Post-quantum cryptography is far more complicated than AES/SHA-3
  - No silver bullet – not exact "drop in replacement"
  - Not enough research on quantum algorithms to ensure confidence on quantum security for some schemes
- We do not expect to "pick a single winner"
  - Ideally, several algorithms will emerge as "good choices"
- We will narrow our focus at some point
  - This does not mean algorithms are "out"
- Requirements/timeline could potentially change based on developments in the field

Submissions to NIST Call for Proposals

- 82 total submissions received from 26 Countries, 6 Continents
- 69 accepted as "complete and proper" (5 since withdrawn)
- 2 of them announced to "merge" to one (*)

	Signatures	KEM/Encryption	Overall
Lattice-based	5	20*	25
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash-based/Symmetric based	3		3
Other	2	5	7
Total	**19**	**45**	**63**

Stateful Hash-Based Signatures

- Stateful hash-based signature is out of the scope of NIST call for proposals but it is in the scope for PQC standardization
- Two versions of stateful hash-based signatures have been proposed in IETF
  - XMSS – RFC 8391 "XMSS: eXtended Merkle Signature Scheme"
  - LMS – "Hash-Based Signatures" (draft-mcgrew-hash-sigs-13)
- Input/feedback was solicited on whether NIST shall standardize any or both hash-based signatures
  - About 20 responses were received and, in general, support NIST to standardize hash-based signatures
- NIST plans to initiate the project to develop a special publication on stateful hash-based signatures
- Further question will be how much to limit hash-based signature, e.g. for code signing only or also allowing for root/intermediate certificates
- Potential usage in TPM?
  - hash-based digital signature schemes are space-intensive, requiring trusted key state management and producing large signatures (some research appears in this area)

General on first round candidates

- Most submitted schemes (or early versions) have been published at the conferences or released through IACR eprint – In general, no big surprise
- Most submissions include proofs/discussions on the CCA/CPA security for Encryption/KEM and EUF-CMA for signatures
- Most submissions addressed the rationale for the selected parameters and mathematics structures as well as pros and cons of the schemes

Diversities and Tradeoffs

- Related to the security assumptions
  - Generic vs. structured (e.g. LWE vs. R-LWE) – Some submissions include both versions
- Auxiliary functions
  - Uniform sampling vs. Gaussian sampling
- Encryption/key exchange
  - Ciphertext size vs. public key size
  - Decryption failure vs. techniques to reduce the probability, including increase the module
- Signature
  - Signature size vs. public key size
  - Hash-and-sign vs. Fiat-Shamir
- etc.

Specific aspects for TPM

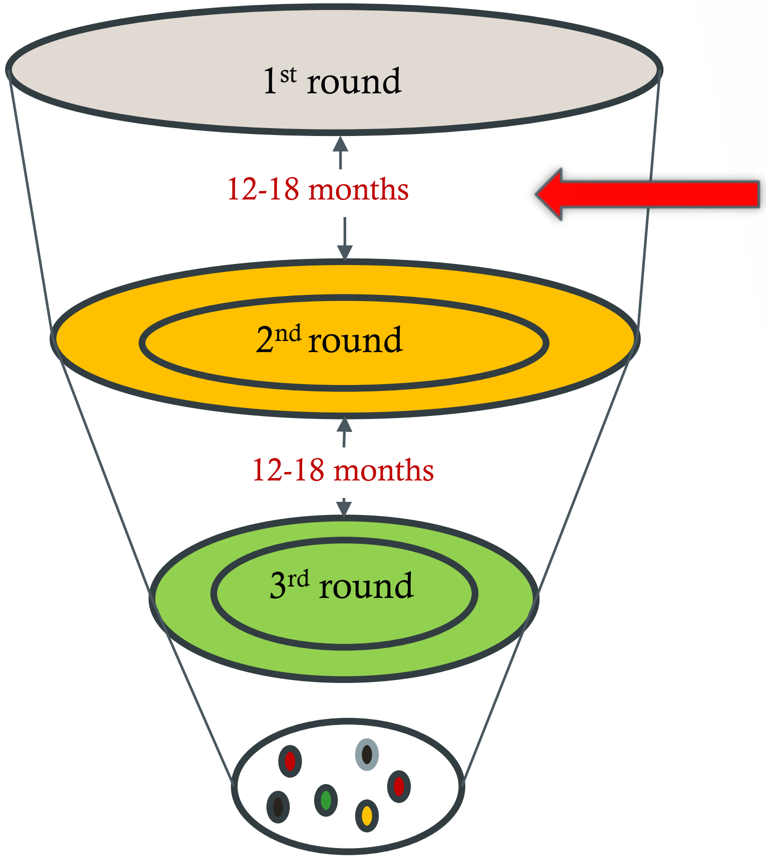
- Feedback from application community is important
  - Is there a limit on public key size, ciphertext size, signature size for TPM?
  - Is there a limit on internal memory?
  - Is decryption failure, even with 2^{-160} probability, an issue?
  - How important is it for encryption and signature to use the same primitive/operation (e.g. lattice, coding etc.)?
- Look into the first round candidates and voice application special needs
  - Tell what can potentially become a problem
- Which underlying operations among PQC primitives will be in favor of DAA?

Transition and Migration

- Is it a problem for TPM protocols between old and new, how to handle it?
- Is it possible to facilitate crypto agility?
- Is dual signature or hybrid mode a transition solution in TPM applications?

NIST Timeline (from April 2018)

- Initial analysis phase 12-18 months
- Narrow the pool and hold the second workshop in August 2019
- Second analysis phase 12-18 months
- May take third analysis phase if needed
- Expect draft standards in 2022-2023



Information on NIST PQC Standardization

- For NIST PQC project, please follow us at
  https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- To submit a comment, send e-mail to pqc-comments@nist.gov
- Join discussion mailing list pqc-forum@nist.gov