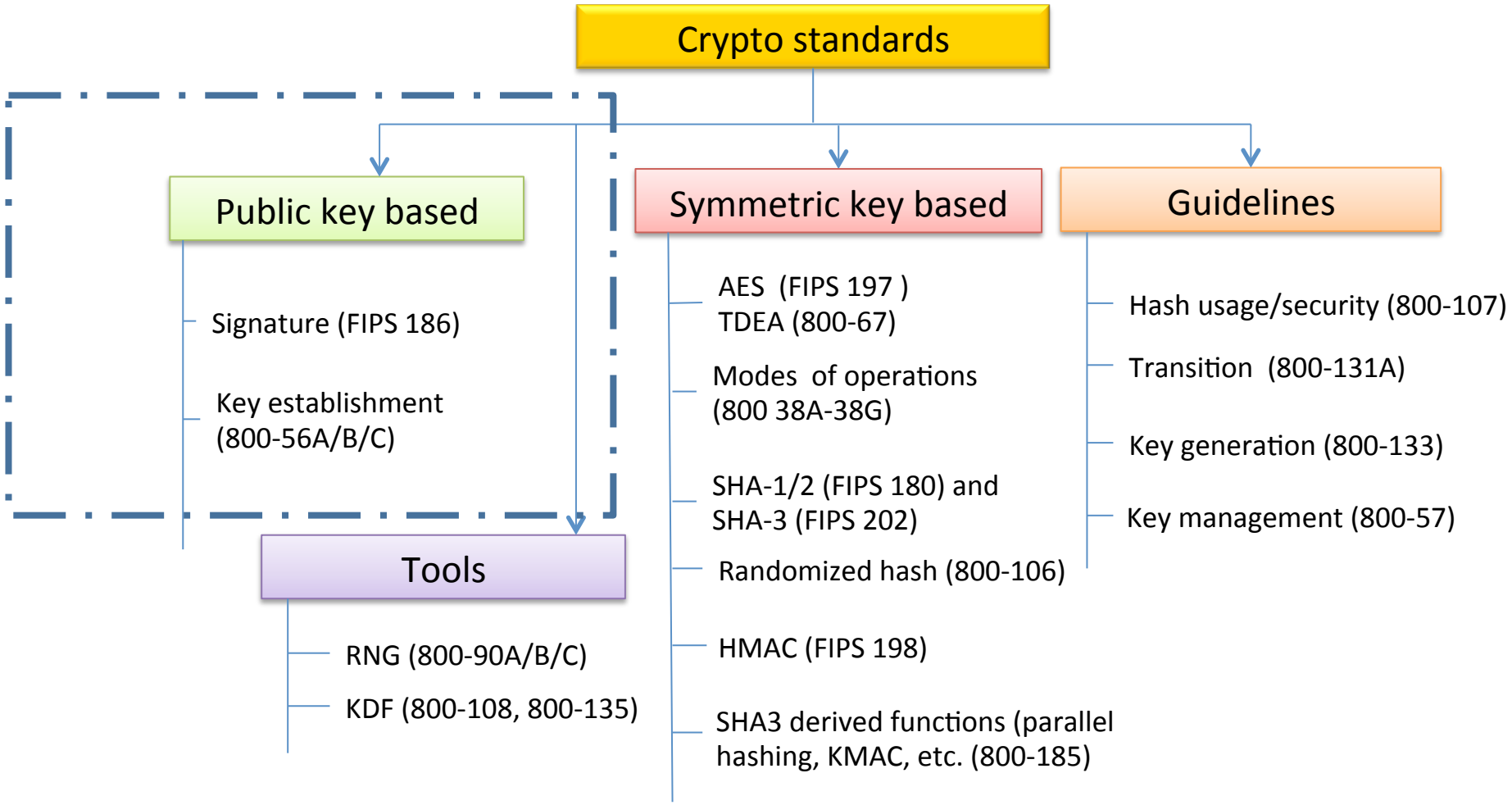
NIST Post-Quantum Cryptography Standardization

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

NIST Crypto Standards - Overview



Public (Asymmetric) Key Cryptography

Digital Signatures

- FIPS 186-4
  - DSA and ECDSA (Discrete Logarithm-Based)
  - RSA (Factorization-Based)

Key Establishment Schemes

- NIST SP 800-56A (Discrete Logarithm-Based)
  - DHs, MQVs (over a finite field or Elliptic curve)
- NIST SP 800-56B (Factorization-Based)
  - RSA based key transport and key agreement

Impact of Quantum Computers on RSA and DH

Quantum computing changed what we have believed about the hardness of discrete log and factorization problems

- Using quantum computers, an integer *n* can be factored in polynomial time using Shor's algorithm
- The discrete logarithm problem can 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

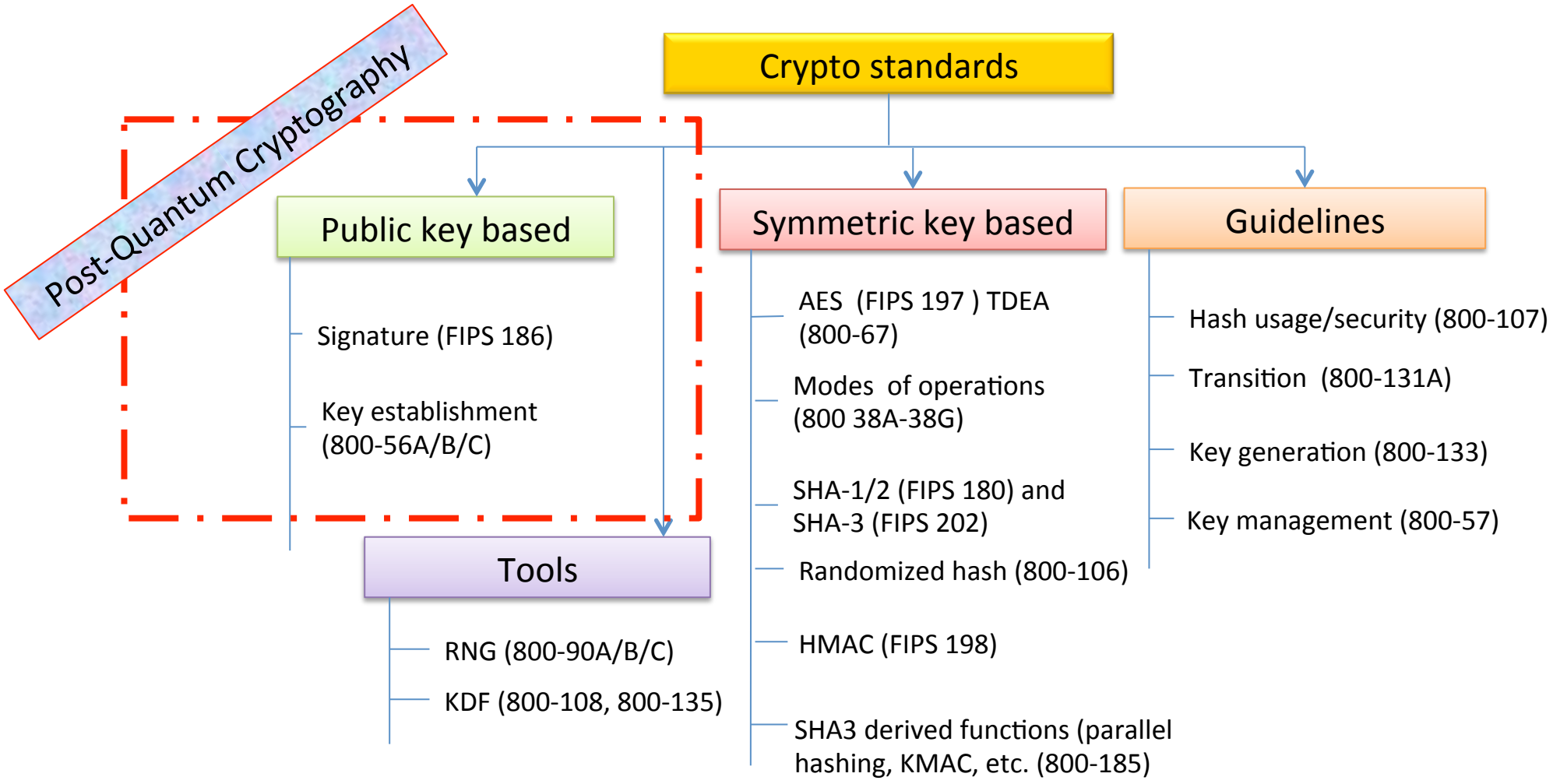
- RSA signatures, DSA and ECDSA (FIPS 186-4)
- Diffie-Hellman Key Agreement over finite fields and elliptic curves(NIST SP 800-56A)
- RSA encryption (NIST SP 800-56B)

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

Look for Quantum Resistant Counterparts for RSA and DH



What we have done – Milestones in a Long Journey

2012 – NIST begins PQC project

- Research and build NIST team

April 2015 – 1st NIST PQC workshop

Feb 2016 – NIST Report on PQC (NISTIR 8105)

Feb 2016 – NIST preliminary announcement of standardization plan

Aug 2016 – Draft call for proposals,

- 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)

Nov 2017 – Submission Deadline

NIST PQC Standardization Plan

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 (co-locate with PQCrypto, April 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

NIST PQC Standardization – Multiparty Process

NIST has fully engaged with

- Research community – for algorithm design, security analysis, performance assessment, etc.
- Standard organizations – for collaboration and interoperability
- Standards user community – for application and implementation requirements, for migration/transition
  - Hardware/software venders, system designers, government agencies, testing labs, etc.
  - Compared with 20-30 years ago, we have a much more mature user community on cryptography applications

What can the standards users expect for this process?

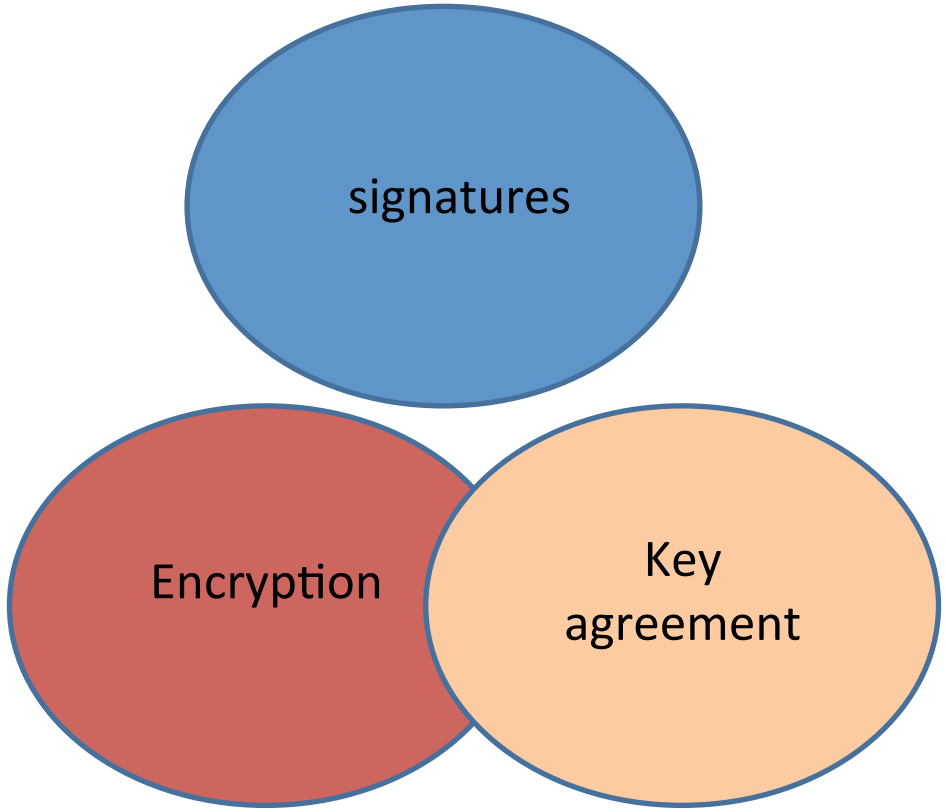
Post-Quantum Cryptography Standardization Scope

The scope is determined by the NIST current standards

- Signatures
  - Public-key signature schemes for generating and verifying digital signatures (FIPS 186-4)
- Encryption/key-establishment
  - Encryption scheme used for
    - Key transport from one party to another (See SP 800-56B)
    - Exchanging encrypted secret values between two parties to establish shared secret value (see SP 800-56B)
  - Key-agreement
    - Schemes like Diffie-Hellman key exchange (see SP 800-56A)

We plan to standardize the PQC algorithms in new standards

- That is, they will not be revisions or additional parts of the existing standards



PQC Families - Actively Researched as Examples

Lattice-based

- NTRUencrypt
- Signature, e.g. Bliss
- (Ring-based) Learning with Errors (e.g. Key Agreement - New Hope)

Code-based

- McEliece encryption and the variants

Multivariate

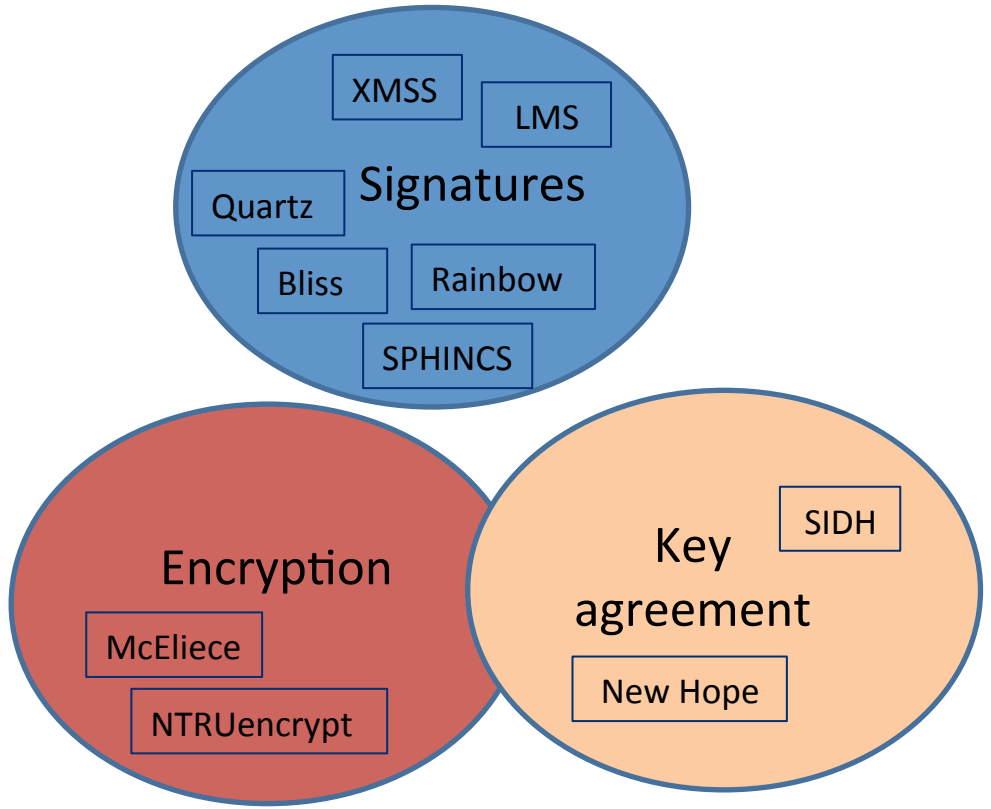
- Rainbow (signature), Quartz (signature), etc.

Hash-based signatures

- LMS, XMSS, SPHINCS

Isogeny-based schemes

- Supersingular isogeny Diffie–Hellman key exchange (SIDH)



The Selection Criteria for PQC Standardization

Secure against both classical and quantum attacks

- Security notions: encryption (IND-CCA2), key agreement (ephemeral, IND-CPA), and signatures (EUF-CMA)
- Classical security strength
- Quantum security strength

Performance on "classical" platforms

- key size, signature size, computational efficiency, and flexibility

Other properties

- Drop-in replacements - Compatibility with existing protocols and networks such as TLS, IKE, etc.
- Perfect forward secrecy, like ephemeral Diffie-Hellman
- Resistance to side-channel attacks
- Misuse resistance, and
- More

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

Ephemeral key-agreement

- Semantic security with respect to chosen plaintext attack (IND-CPA security)

Quantum security

Currently NIST cryptography standards specify parameters for classical security levels at 112, 128, 192, 256 bits

- For RSA public module n, $|n|$ = 2048 bits, the estimated “classical” security strength is 112 bits
- For ECDH, key agreement over curve P-256 is estimated to support “classical” security of 128 bits

For PQC standardization, need to specify concrete parameter sets with security estimates

The bits of quantum security requirements in the draft call for proposals (CFP) received many comments

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

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

Complexities of PQC Standardization

Much broader scope – three crypto primitives

- Signatures, Encryption, Key agreement

Against both classical and quantum attacks

- Security strength assessment on specific parameter selections

Consider various theoretical security models and practical attacks

- Provably security vs. security against instantiation or implementation related security flaws and pitfalls

Multiple tradeoff factors

- Security, performance, key size, signature size, side-channel resistance countermeasures

Migrations into new and existing applications

- TLS, IKE, code signing, PKI infrastructure, and much more

Not exactly a competition – it is and it isn’t

Similar to SHA-3 competition

It will be an open procedure and we will 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 with many choices

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

The timeline and some selection criteria may change based on developments in the field

NIST Looks for Input from Standards User Community

Feedback on special requirements on PQC for different applications

- Applications in Internet protocols like TLS, IKE are better understood
- Requirements for applications in processing and/or bandwidth constrained environment need to be explored
- Different trust models also propose special requirements, for example, multiple signer scenarios when using stateful hash-based signatures

Application specific secure implementation issues

- In some applications, error or failure handling can be an issue
- Performance impact when applying countermeasure to side-channel attacks

Transition issues

- The application specific life cycle
- Possibility to add new cryptographic algorithms without replacing the equipment
- Capability or limitation to support crypto agility
- Backward compatibility support requirement

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 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 initiated a study period for quantum-resistant cryptography since 2015

NIST is interacting and collaborating with these organizations and groups

Summary

Post-quantum cryptography standardization is going to be a long journey

Input from standards user community is extremely important

- Early stage engagement is critical

See also: www.nist.gov/pqcrypto

- Sign up for the pqc-forum for announcements and discussion