Update on NIST Post-Quantum Cryptography Standardization

Lily Chen
National Institute of Standards and Technology
USA

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Where we are?

Dec 2016 – NIST Announcement of Call for Proposals on post-quantum cryptography

- Public key encryption
- Key agreement
- Digital signature

Preliminary deadline:

- Sept. 30, 2017

ssions received by this dat will
ete les and we
ncies by the end of October

Final Deadline

- November 30, 2017

16 Days Left

77 Days Left

Overview of NIST call for proposals

Requirements for Submission Packages

- Cover sheet, supporting documentation, media, IP statement

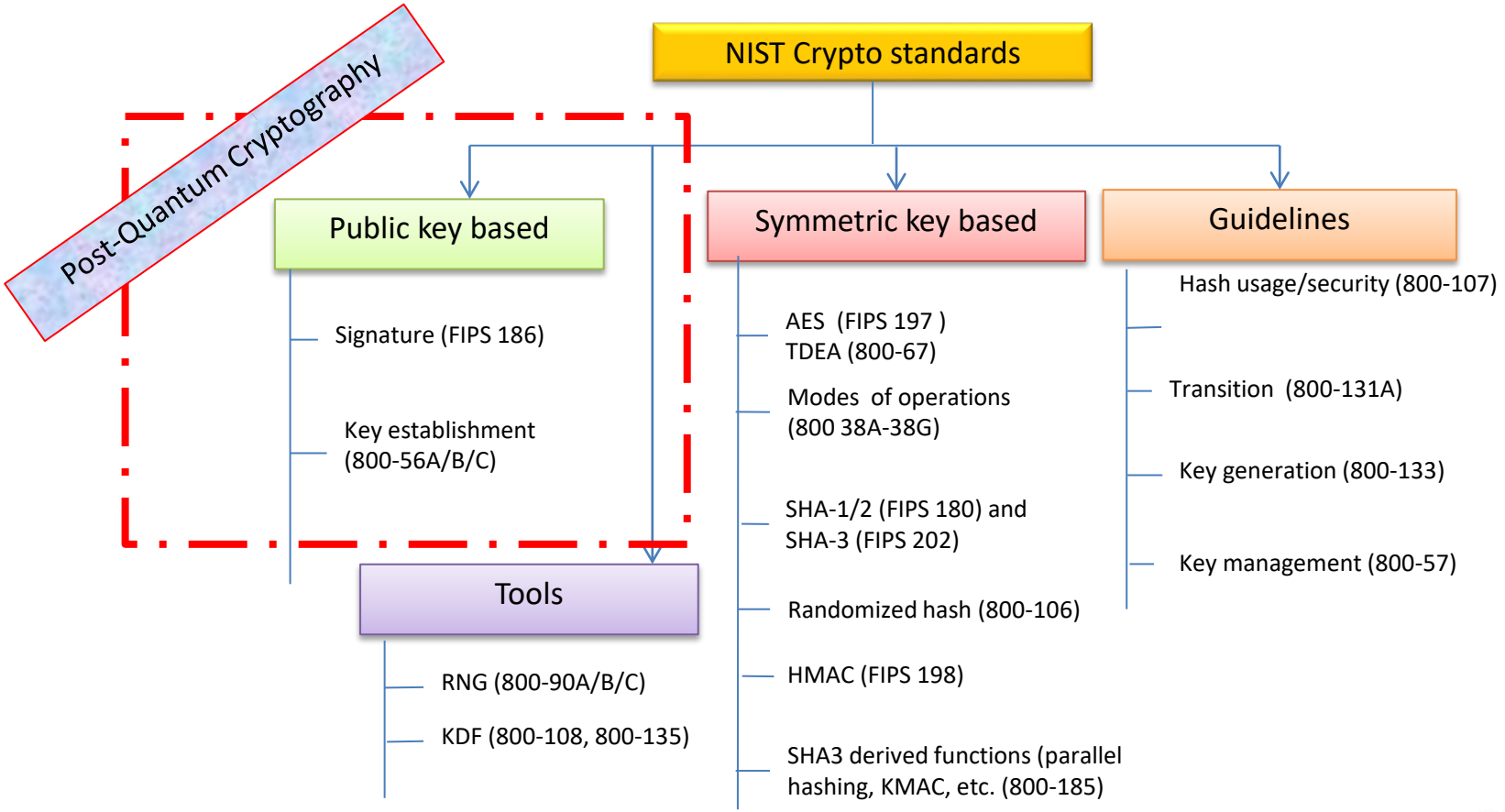
Minimum Acceptability Requirements

- Scope – Public-key crypto algorithms for digital signature, encryption, key establishment
- Basic requirements for each function

Evaluation Criteria

- Security definitions, targeted security strength (classical and quantum), cost and performance, etc.

Post-Quantum Cryptography and NIST Standards



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Major Updates in Requirements and Criteria

The draft Call for proposals with requirements and criteria was released for public comments in August 2016

Comment period closed September 16, 2016 (Right before ETSI/IQC workshop 2016)

Major updates in resolving comments and concerns at the final release of call for proposals

1. Description of quantum security strength levels
   - NIST continues to specify five security strength categories in terms of the computational resources, classical and quantum, required to break a selected parameter set for a cryptographic primitive
   - Submitters are not required to provide different parameters for all five security categories
2. Notions for public-key encryption, key exchange/key agreement
   - Introduce notion of key encapsulation mechanism (KEM)
   - For KEM with ephemeral keys, use IND-CPA security notion instead of IND-CCA2

*"Summary of Draft Call for Proposals Comments and Changes" can be found at http://www.nist.gov/pqcrypto

Discussions and Questions

Since the draft call for proposals was announced, NIST team has actively interacted with potential submitters and researchers

The questions include

- APIs to support different ancillary functions
- Using third party libraries
- Submission format
- etc.

The topics discussed at pqc-forum@nist.gov include

- Quantum vs. classical security strength
- Security notions (IND-CCA2, IND-CPA, etc.)
- Random number generator
- Key exchange vs. key encapsulation
- etc.

Answers to the common questions and summaries on the major discussion topics were added to FAQs at www.nist.gov/pqcrypto

Observations and Strategies

- Post-Quantum Cryptography standardization is going to be much more complicated, compared with AES and SHA3 competitions
- Some PQC schemes require different subroutines from existing public key cryptography schemes and need to handle new issues, e.g.
  - decryption failure, and
  - signature compression, etc.
- The potential submitters have expressed great concerns on performance, which has triggered many questions on using libraries and different programming languages
- PQC standardization is a new direction for NIST team and also for the community
- NIST team will continue to work with the community, including submitters, researchers, and practitioners, to learn from handling new issues as they appear

What to expect next?

NIST will post “complete and proper” submissions for security and performance analysis at www.nist.gov/pqcrypto , that is,

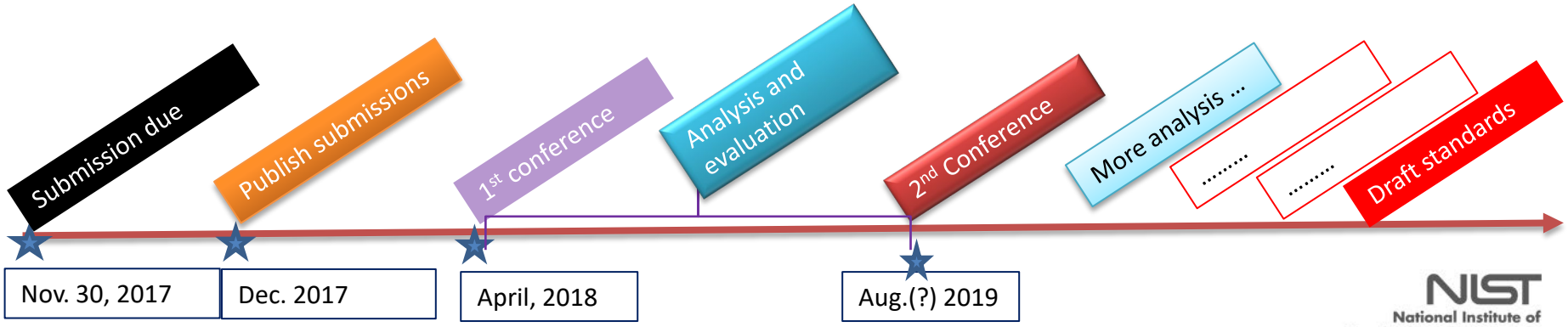
- The submitted candidates are publicly available for scrutinizing and evaluating

The First NIST PQC Standardization Conference (co-located with PQCrypto, April 2018)

- For submitters to present the algorithms and design rationale
- For researchers and practitioners to ask questions on the submitted algorithms

Evaluation and analysis continue after The First NIST PQC Standardization Conference (~16 months)

The Second NIST PQC Standardization Conference is planning to be held in the second half of 2019 (tentative Aug. 2018 to be confirmed)



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Summary

We learnt a lot through questions and discussions when the potential submitters prepare submissions

We are prepared to handle new issues in the procedure

Please follow the discussions at pqc-forum@nist.gov

Questions to NIST team should be sent to pqc-comments@nist.gov

See future updates at www.nist.gov/pqcrypto