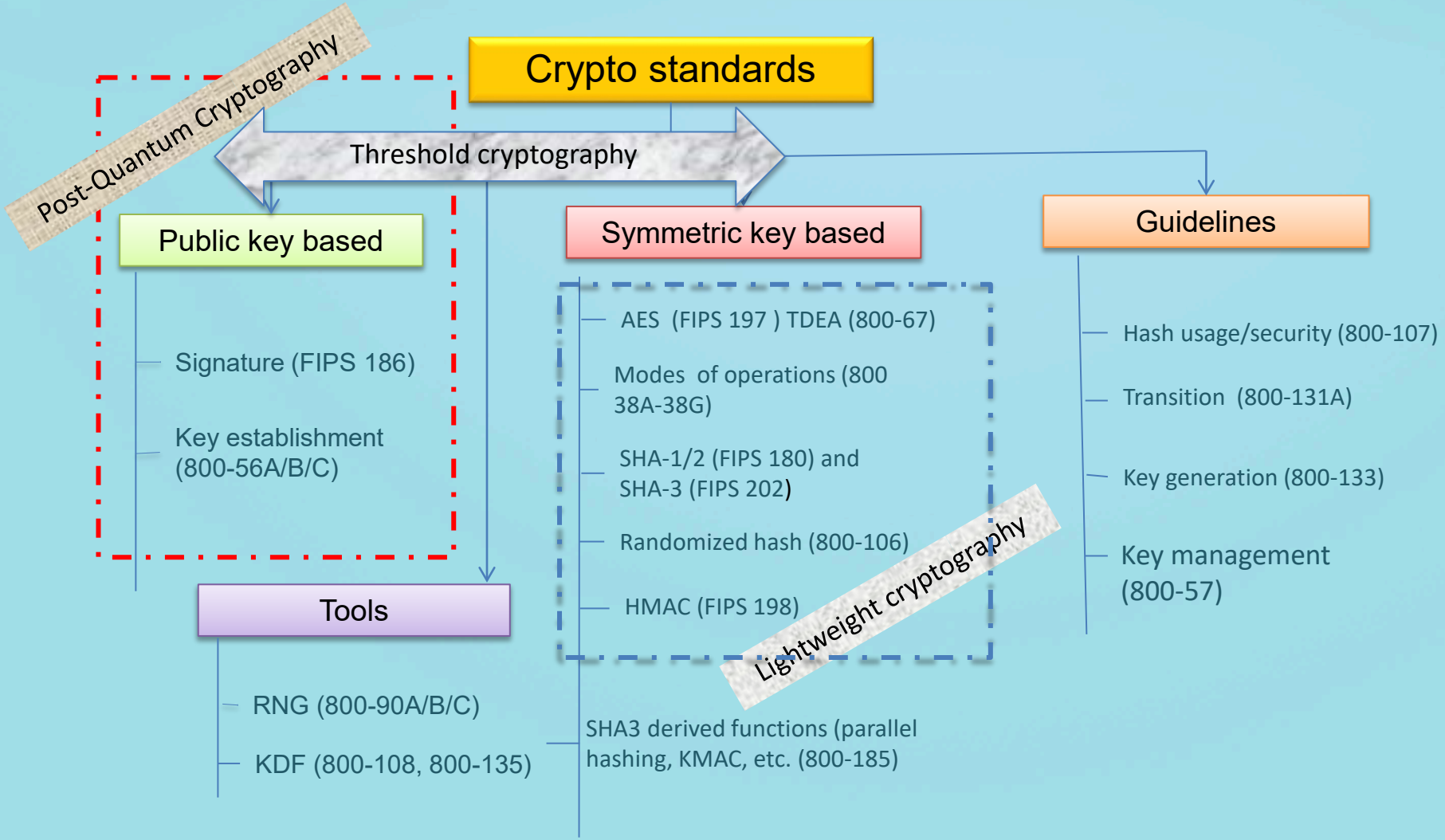

Cryptography Research
Cryptography Standards
Cryptography Applications

NIST Cryptographic Standards



New directions

- Post-Quantum Cryptography
- Lightweight Cryptography
- Threshold Cryptography

The PQC "Competition"

- Similar to our past competitions (AES/SHA-3), but more complicated
  - More than one primitive
  - Still an active research area – especially quantum algorithms and security
  - No easy drop-in replacement -- Multiple trade-off factors
- We anticipate selecting more than one algorithm
  - Probably 2 or 3 more years until selection(s) made
- We will narrow our focus throughout the process, and release reports explaining our decisions

**Requirements/timeline subject to change, depending on developments in the field

The Submissions

- 82 total submissions received from 25 Countries, 6 Continents (and 16 states)
  - A total of 278 submitters
- 69 accepted as "complete and proper" (5 have withdrawn)
- Most submitted schemes (or previous versions) have been published previously – In general, no big surprises

	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Stateless Hash-based/symmetric key	3		3
Other	2	5	7
Total	**19**	**45**	**64**

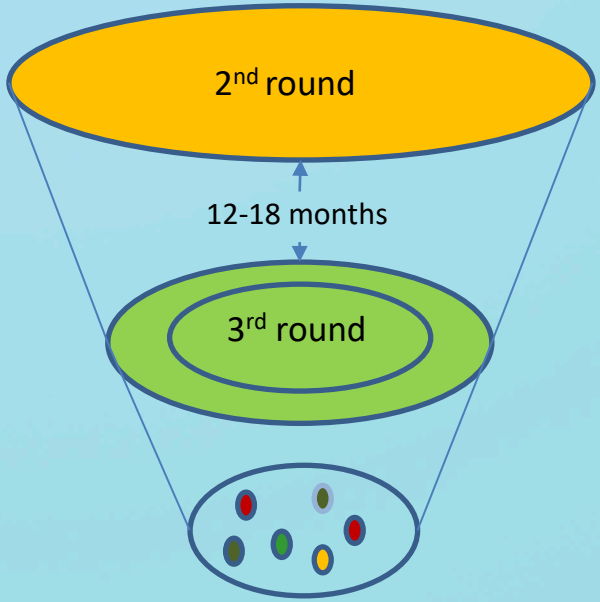
The 2nd Round Candidates

- Used evaluation criteria: Security, Cost and Performance, Algorithm and Implementation characteristics
- Overall quantity, quality and maturity of analysis on each scheme
- Attacks that called security into question
- Size of keys, signatures, ciphertexts, benchmarks (multiple sources)
- unique and elegant designs for diversity

	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based	0	7	7
Multivariate	4	0	4
Stateless hash-based/symmetric key	2	0	2
Other	0	1	1
Total	9	17	26

What will be the next?

- Analyze and evaluate the PQC candidates
  - Second analysis phase 12-18 month from January of 2019
- May take third analysis phase if needed
- Make selections and release draft standards in 2022-2023



NIST Lightweight Cryptography Project

Aim: Standardize lightweight cryptographic algorithms that are suitable for constrained environments when the performance of current NIST standards is not acceptable.

Call: Authenticated Encryption with Associated Data (AEAD) schemes to be used in constrained environments. Optional hashing functionality that shares design components with AEAD scheme.

Contact: lightweight-crypto@nist.gov
Mailing list: lwc-forum@list.nist.gov
Webpage: https://csrc.nist.gov/Projects/Lightweight-Cryptography

Timeline and Status

Timeline

July 2015	First workshop
October 2016	Second workshop
March 2017	NISTIR 8113
August 27, 2018	Call for submissions
January 4, 2019	Early submission deadline
February 25, 2019	Submission deadline
March 29, 2019	Amendment deadline
November 4-6, 2019	Third workshop

Status

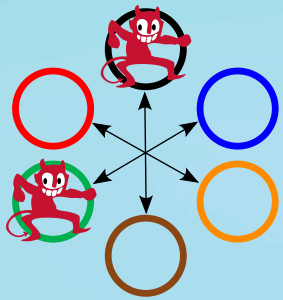
57 submissions received

- 36 AEAD only
- 21 AEAD and hashing

NIST will post round 1 candidates after March deadline

Threshold Cryptography

Threshold Schemes:
Use redundancy & diversity to mitigate the compromise of some (up to a threshold number f of) components



(*f*-out-of-*n*)

Cryptographic Primitives:

- Signatures, encryption, key-gen, ciphers
- Operation needs several parties
- Secret key is never at one place
- Resistance against side-channel attacks

NIST-CSD's goal: to standardize Threshold Schemes for Cryptographic Primitives

NISTIR 8214 (report)

Initiates discussion about standardization:

- How to characterize threshold schemes
- What criteria to call for/select standards?
- How to validate implementations?

(Draft July 2018 → Public feedback → Published March 2019)

https://doi.org/10.6028/NIST.IR.8214

NISTIR 8214 (report)

Initiates discussion about standardization:

- How to characterize threshold schemes
- What criteria to call for/select standards?
- How to validate implementations?

(Draft July 2018 → Public feedback → Published March 2019)

https://doi.org/10.6028/NIST.IR.8214