NIST PQC Standardization
- An Update

Dustin Moody

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

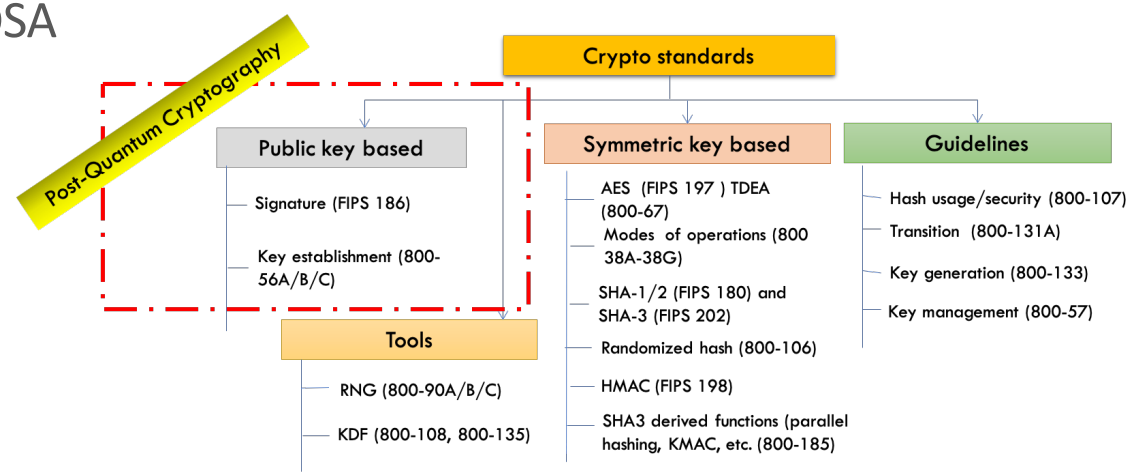
Crypto Technology Group
Computer Security Division
Information Technology Lab

The Quantum Threat

- NIST public-key crypto standards
  - **SP 800-56A**: *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*
  - **SP 800-56B**: *Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography*
  - **FIPS 186**: *The Digital Signature Standard*

  would be vulnerable to attacks from a (large-scale) quantum computer
  - Shor's algorithm would break RSA, ECDSA, (EC)DH, DSA

- Symmetric-key crypto standards would also be affected, but less dramatically

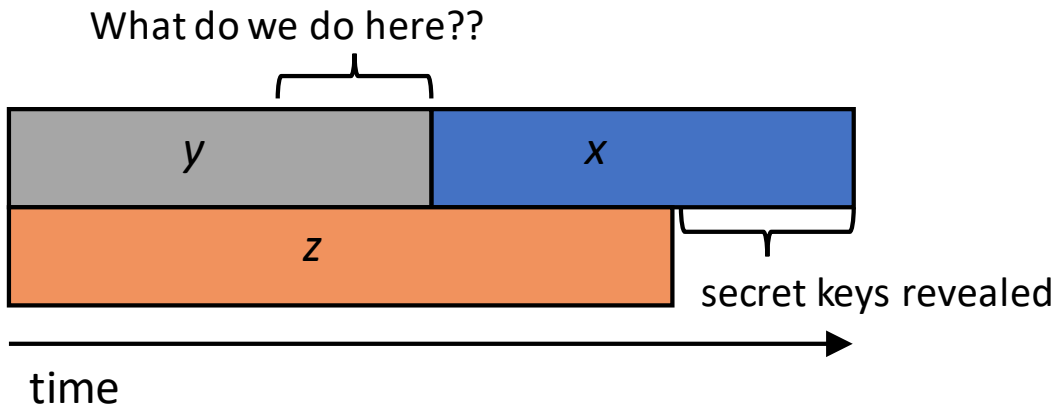


Post-Quantum Cryptography

- Post-Quantum Cryptography (PQC)
  - Cryptosystems which run on classical computers, and are believed to be resistant to attacks from both classical and quantum computers

- How soon do we need to worry?

Theorem (Mosca): If $x + y > z$, then worry



x – time of maintaining data security
y – time for PQC standardization and adoption
z – time for quantum computer to be developed

NIST PQC Milestones and Timelines

2016

Determined criteria and requirements, published NISTIR 8105

Announced call for proposals

2017

Received 82 submissions

Announced 69 1st round candidates

2018

Held the 1st NIST PQC standardization Conference

2019

Announced 26 2nd round candidates, NISTIR 8240

Held the 2nd NIST PQC Standardization Conference

2020

Announced 3rd round 7 finalists and 8 alternate candidates. NISTIR 8309

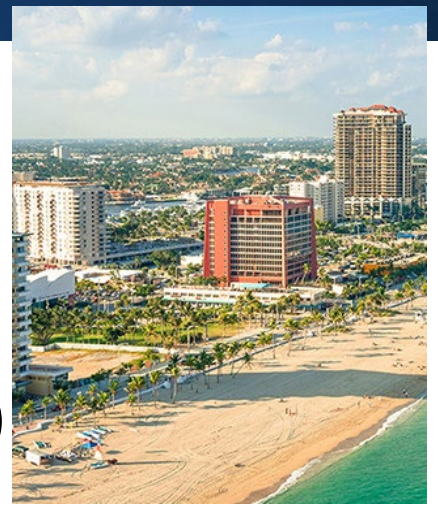
2021

Hold the 3rd NIST PQC Standardization Conference

2022-2023

Release draft standards and call for public comments

The 1st Round



- A lot of schemes quickly attacked!
- Many similar schemes (esp. lattice KEMs)
- 1st NIST PQC Standardization workshop
- Over 300 ”official comments” and 900 posts on the pqc-forum
- Research and performance numbers

- After a year: 26 schemes move on

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

The 2nd Round

- 4 merged submissions
- Maintained diversity of algorithms
- Cryptanalysis continues
- LAC, LEDAcrypt, RQC, Rollo, MQDSS, qTESLA, LUOV all broken
- 2nd NIST PQC Standardization workshop
- More benchmarking and real world experiments

- After 18 months: 15 submissions move on

	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-variate	4		4
Stateless Hash or Symmetric based	2		2
Isogeny		1	1
Total	**10**	**16**	**26**

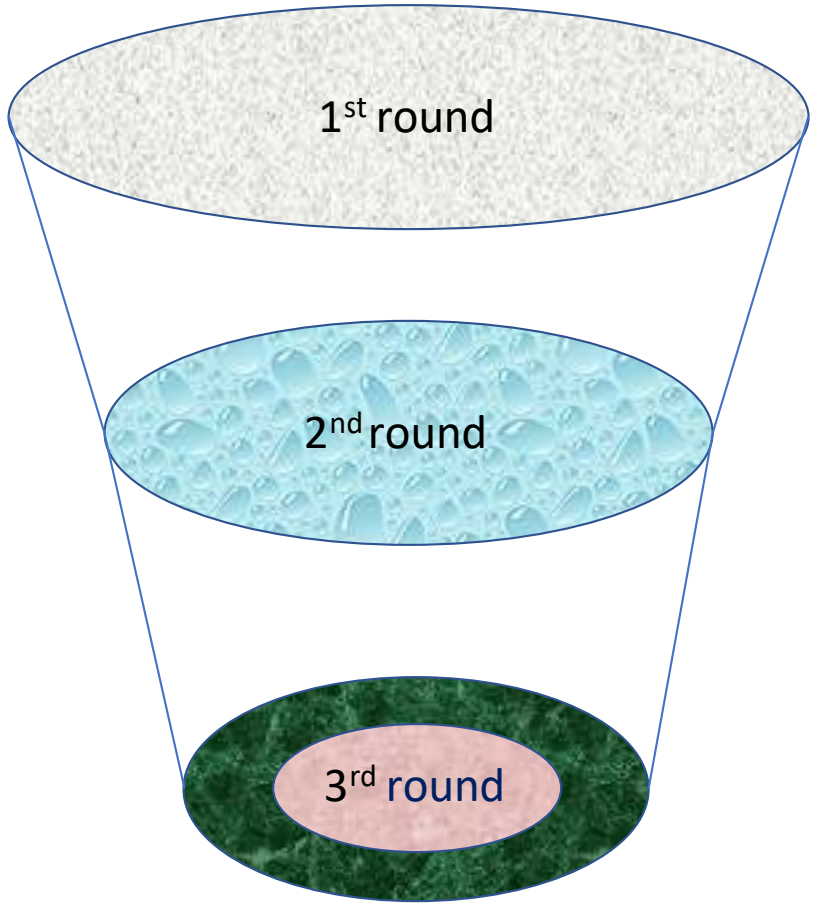
Challenges and Considerations in Selecting Algorithms

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

Performance
- Size of parameters
- Speed of KeyGen, Enc/Dec, Sign/Verify
- Decryption failures

Algorithm and implementation characteristics
- IP issues
- Side channel resistance
- Simplicity and clarity of documentation
- Flexible

Other
- Round 2 changes
- Official comments/pqc-forum discussion
- Papers published/presented



The 3rd Round Finalists and Alternates

- NIST selected 7 Finalists and 8 Alternates
  - Finalists: most promising algorithms we expect to be ready for standardization at end of 3rd round
  - Alternates: candidates for potential standardization, most likely after another (4th) round
- KEM finalists: Kyber, NTRU, SABER, Classic McEliece
- Signature finalists: Dilithium, Falcon, Rainbow

- KEM alternates: Bike, FrodoKEM, HQC, NTRUprime, SIKE
- Signature alternates: GeMSS, Picnic, Sphincs+

	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**

Timeline

- The 3rd round will last 12-18 months
  - NIST will then select which finalist algorithms to standardize
  - NIST will also select which alternates to keep studying in a 4th round (*)
  - The 4th round will similarly be 12-18 months
  - NIST may decide to consider new schemes – details to come
- NIST will hold a 3rd PQC Standardization workshop ~ spring 2021
- We expect to release draft standards for public comment in 2022-2023
- The finalized standard will hopefully be ready by 2024

Stateful Hash Based Signatures for Early Adoption

Stateful hash-based signatures were proposed in 1970s

- Rely on assumptions on hash functions, that is, not on number theory complexity assumptions
- It is essentially limited-time signatures, which require state management

Internet Engineering Task Force (IETF) has released two RFCs on hash-based signatures

- RFC 8391 "XMSS: eXtended Merkle Signature Scheme" (By Internet Research Task Force (IRTF))
- RFC 8554 "Leighton-Micali Hash-Based Signatures" (By Internet Research Task Force (IRTF))

NIST specification on stateful hash-based signatures

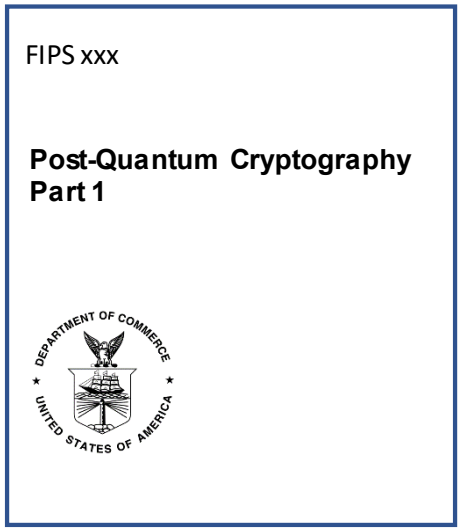
- Draft NIST SP 800-208 "*Recommendation for Stateful Hash-Based Signature Schemes*" was released for public comments December 2019
- It is in the process for final publication

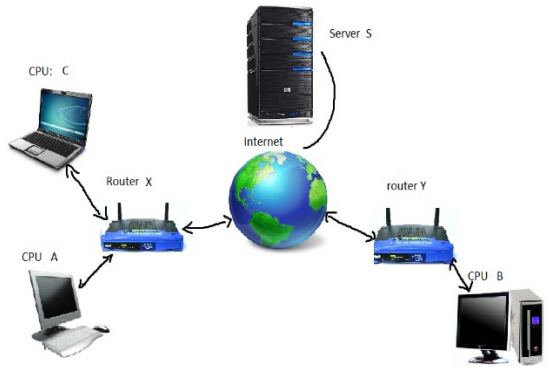
ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

- Stateful hash-based signatures will be specified in ISO/IEC 14888 Part 4
- It is in the 1st Working Draft stage

Transition and Migration

- Public key Cryptography has been used everywhere; 2 important uses:
  - Communication security; and
  - Trusted platforms
- Transition and migration are going to be a long journey 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

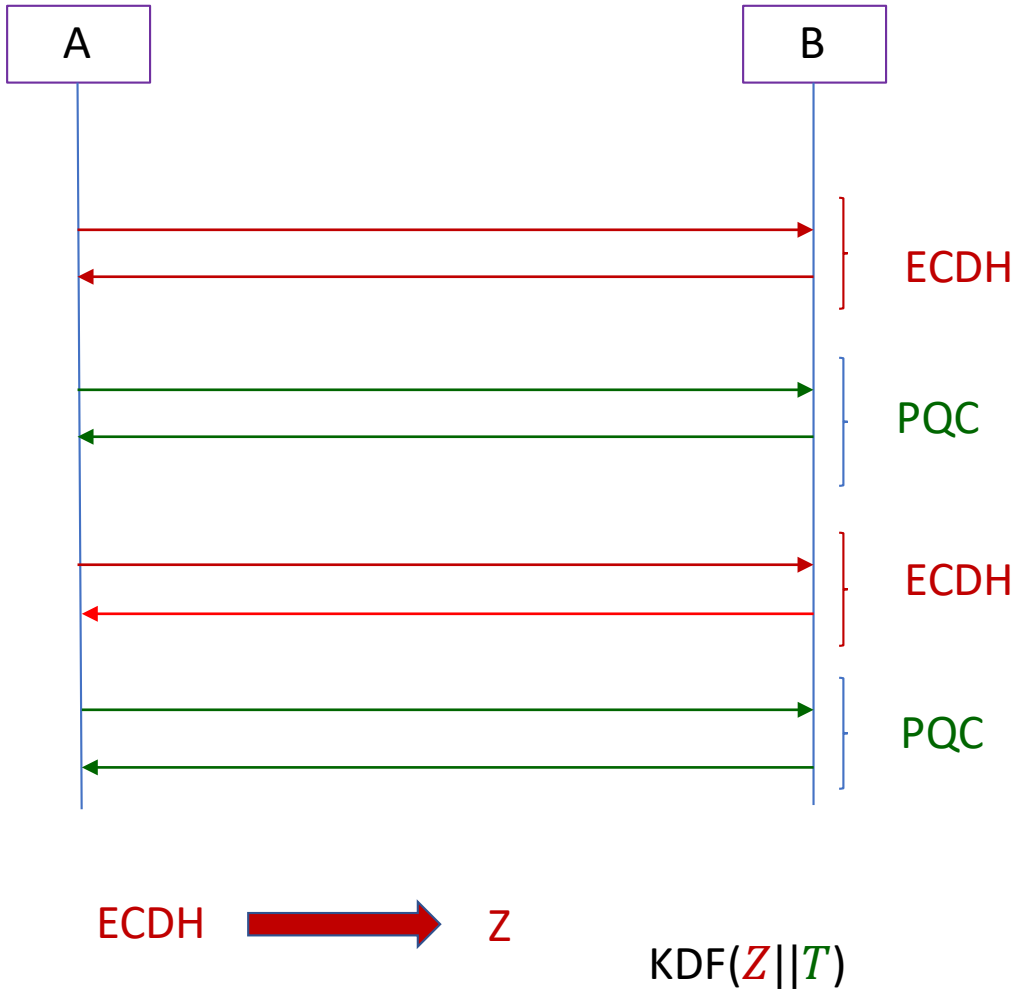




Hybrid mode – An approach for migration

NIST SP800-56C Rev. 2
Recommendation for Key-Derivation Methods in Key-Establishment Schemes
August 2020

> "In addition to the currently approved techniques for the generation of the shared secret *Z* … this Recommendation permits the use of a "hybrid" shared secret of the form Z' = *Z* || *T*, a concatenation consisting of a "standard" shared secret *Z* that was generated during the execution of a key-establishment scheme (as currently specified in [SP 800-56A] or [SP 800-56B]) followed by an auxiliary shared secret *T* that has been generated using some other method"



NIST Transition Guideline for PQC?

NIST has published transition guidelines for algorithms and key lengths

NIST SP 800-131A Revision 2 "Transitioning the Use of Cryptographic Algorithms and Key Lengths" - Examples

- Three-key Triple DES
  - Encryption - Deprecated through 2023 Disallowed after 2023
  - Decryption - Legacy use
- SHA-1
  - Digital signature generation - Disallowed, except where specifically allowed by NIST protocol-specific guidance
  - Digital signature verification - Legacy use
  - Non-digital signature applications – Acceptable
- Key establishment methods with strength < 112 bits (e.g. DH mod p, $|p| < 2048$)
  - Disallowed

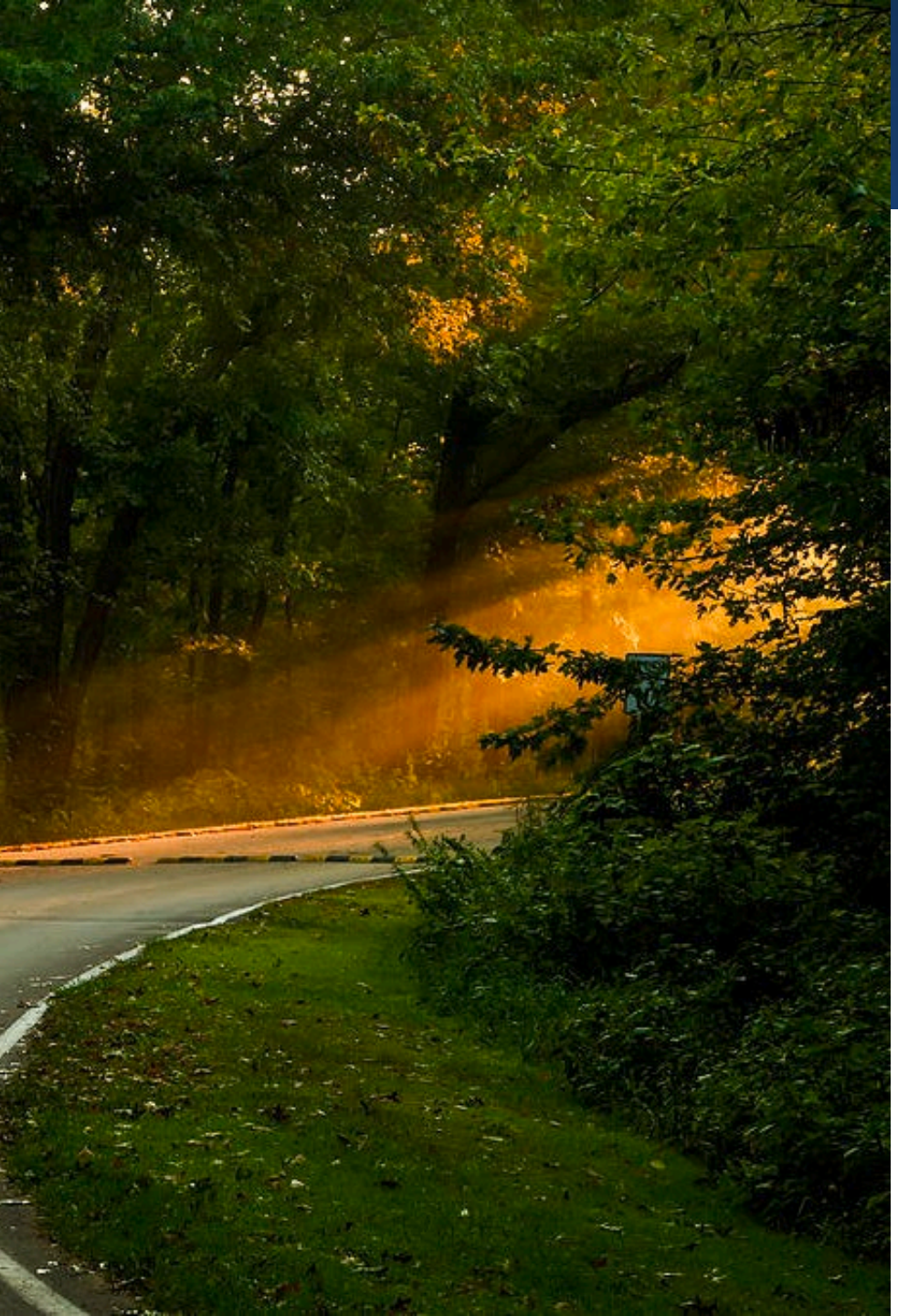
NIST will provide transition guidelines to PQC standards

The timeframe will be based on a risk assessment of quantum attacks

What can you do now?

- Perform an internal quantum risk assessment
  - Identify information assets and their current crypto protection
  - Identify what ‘x’, ‘y’, and ‘z’ might be for you – determine your quantum risk
  - Prioritize activities required to maintain awareness, and to migrate technology to quantum-safe solutions
- Evaluate vendor products with quantum safe features
  - Know which products are not quantum safe
  - Ask vendors for quantum safe features in procurement templates
- Develop an internal knowledge base amongst IT staff
- Track developments in quantum computing and quantum safe solutions, and to establish a roadmap to quantum readiness for your organization

- Act now – it will be less expensive, less disruptive, and less likely to have mistakes caused by rushing and scrambling



Conclusion

- We can start to see the end?
- NIST is grateful for everybody's efforts
- Check out www.nist.gov/pqcrypto
  - Sign up for the pqc-forum for announcements & discussion
  - send e-mail to pqc-comments@nist.gov