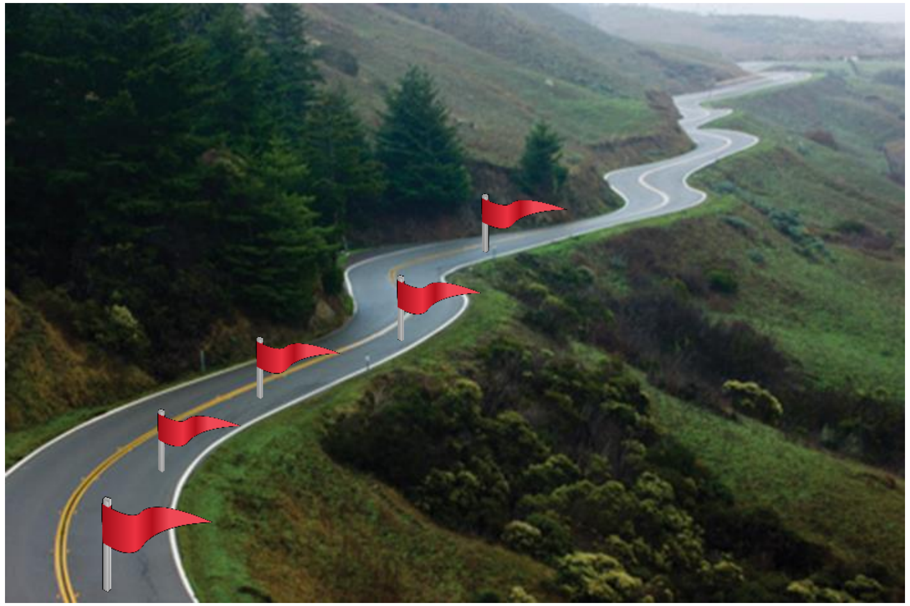
National Institute of Standards and Technology
U.S. Department of Commerce

Post-Quantum Cryptography
- Standardization and Transition

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

NIST Process Update: Milestones and Timeline



2016

Determined criteria and requirements

Announced call for proposals

2017

Received 82 submissions

Announced 69 1st round candidates

2018

1st round analysis

Held the 1st NIST PQC standardization Conference

2019

Announced 26 2nd round candidates

Held the 2nd NIST PQC Standardization Conference

2020 Announced 3rd round 7 finalists and 8 alternate candidates

2021

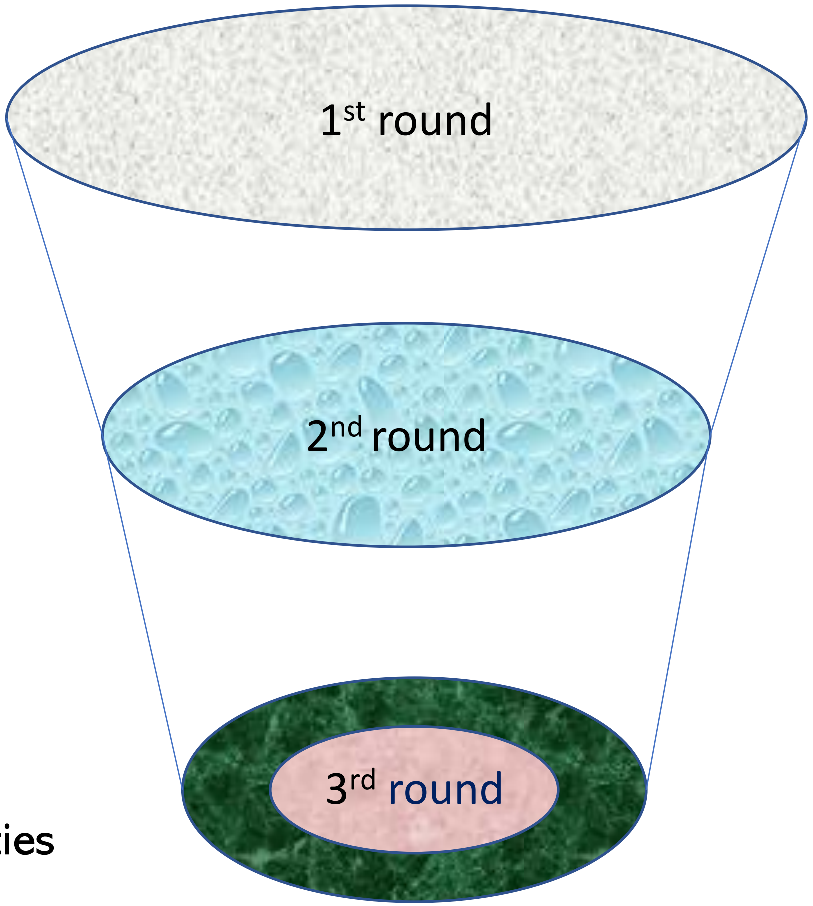
Hold the 3rd NIST PQC Standardization Conference

2022-2023

Release draft standards and call for public comments

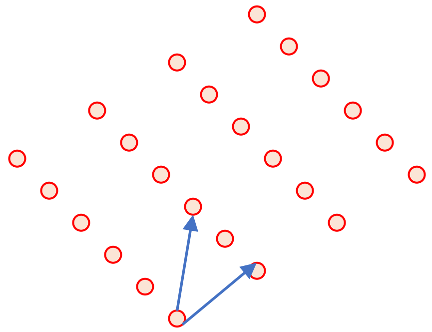
Considerations in Selecting Algorithms

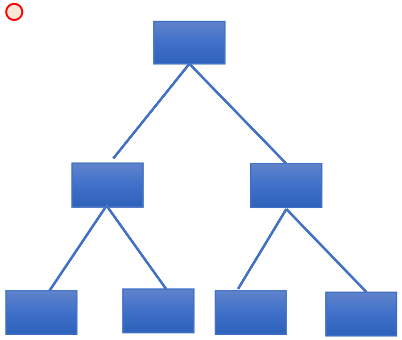
- Security
  - Security levels offered
  - (confidence in) security proof
  - Any attacks
  - Classical/quantum complexity
- Performance
  - Size of pk, ciphertext, signature, etc.
  - Speed of KeyGen, Enc/Dec, Sign/Verify
  - Decryption failures
- Algorithm and implementation characteristics
  - IP issues
  - Side-channel resistance
  - Simplicity and clarity of documentation
  - Flexible for different platforms and applications
- Diversity
  - Based on different assumptions and/or with different properties
- Other
  - Official comments/pqc-forum discussion
  - Papers published/presented

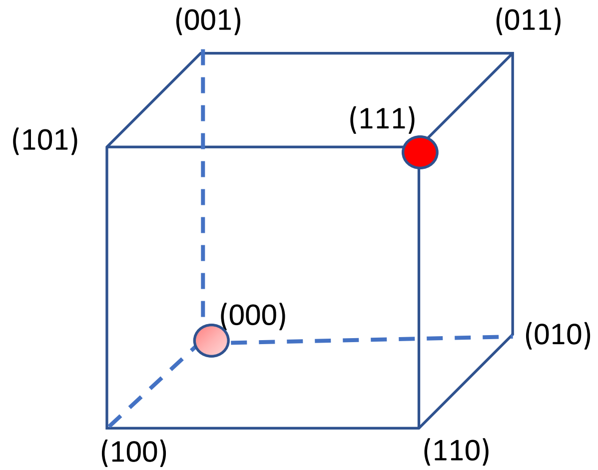


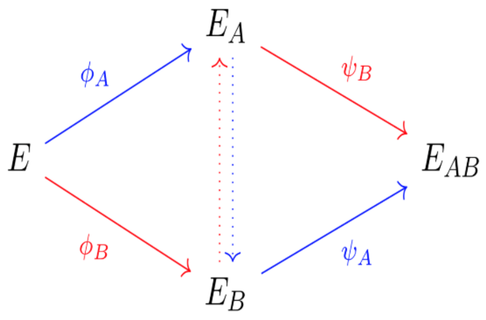
Post-Quantum Cryptography

- Some actively researched PQC categories
  - Lattice-based
  - Code-based
  - Multivariate
  - Hash/Symmetric key -based signatures
  - Isogeny-based schemes









$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$

$$\vdots$$

$$p^{(m)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

First, Second, and Third Round Candidates

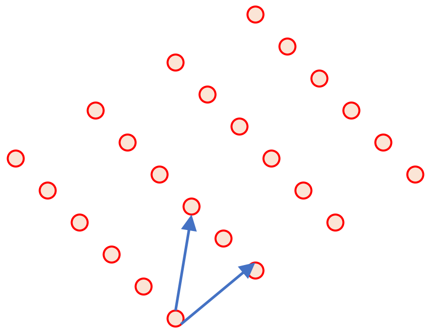
1st round	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate			
Stateless Hash/Symme			
Other			
Total			

2nd round	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-			
Statele based			
Isogen			
Total			

3rd round	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

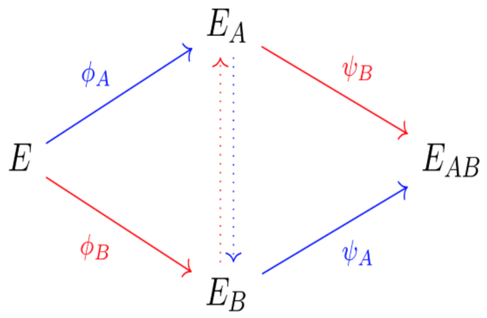
Third Round – Lattice Based KEM

- Crystals-Kyber and Saber
  - Great performance all-around → Finalists
- FrodoKEM
  - Conservative/Backup → Alternate
- NTRU
  - Not quite as efficient, but long & established history, existing standards → Finalist
- NTRUprime
  - Different design choice and security model → Alternate

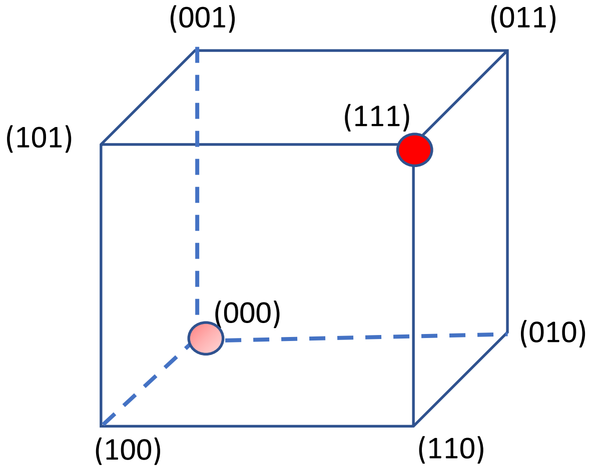


Third Round – Isogeny and Code-based KEMs

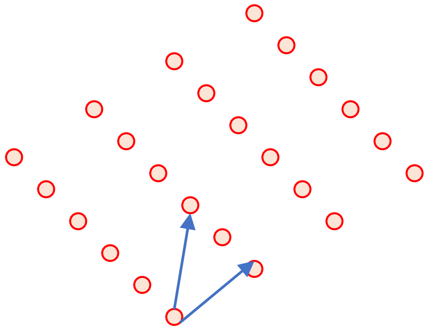
- SIKE
  - Newer security problem, an order slower → Alternate



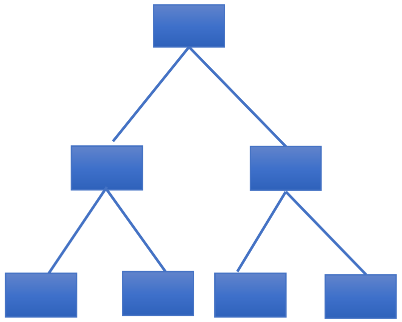
- Classic McEliece
  - Oldest design, large public keys but small ciphertexts→ Finalist
- BIKE
  - Good performance, made some changes → Alternate
- HQC
  - Better security analysis/larger keys (than BIKE) → Alternate



Third Round – Signatures (Lattice, Hash/Symmetric Key-Based, Multivariate)



- Dilithium and Falcon
  - Both balanced, efficient lattice-based signatures
  - Manageable pk and sig sizes → Finalists



- SPHINCS+ and Picnic
  - SPHINCS+ is stateless hash-based signatures, relatively stable, conservative security, larger sig/slower → Alternate
  - Picnic is based on symmetric-based primitive, not stable yet, but has lots of potential → Alternate

- Rainbow and GeMMS
  - Both have large pk, very small sig
  - Rainbow a bit better → Finalist
  - GeMMS → Alternate

$$p^{(1)}(x_1,\dots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$

$$p^{(2)}(x_1,\dots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$

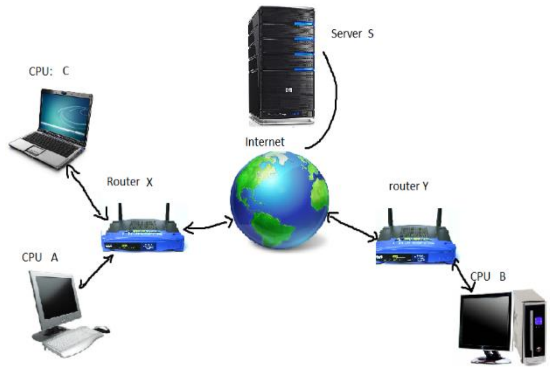
$$\vdots$$

$$p^{(m)}(x_1,\dots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}$$

Challenges and Strategies in Transition to PQC

NIST

- Public key Cryptography has been used everywhere and two most important usages are for
  - Communication security (IPsec, TLS, etc)
  - Trusted platforms (Code signing)
- Transition is going to be a long journey and full of exciting adventures
  - New features, characters, implementation challenges
  - Not quite drop-in replacements
  - Risk of disruptions in operation and security
- Enable crypto agility is the key for smooth migration
  - A capability allowing to remove some algorithms and to introduce new algorithms in the existing applications and implementations



Initiatives in Transition to PQC

NIST

- Prototype PQC candidates in TLS and other protocols
- Stateful Hash Based Signatures for Early Adoption
  - 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 SP 800-208 "Recommendation for Stateful Hash-Based Signature Schemes" published in October 2020
  - ISO/IEC JTC 1 SC27 WG2 Project: Stateful hash-based signatures will be specified in ISO/IEC 14888 Part 4
- Hybrid mode as an approach for migration to PQC
  - Use an existing public key standard, e.g. Diffie-Hellman Key Agreement and a PQC mechanism
  - Each of them establishes a "shared secret value"
  - Derive session keys from both secret values
  - NIST SP 800-56C rev. 2 has incorporated the additional shared secret to key derivation

Transition Preparation and Outreach

- NIST National Center of Cybersecurity of Excellence (NCCoE) released white paper "Getting Ready for Post-Quantum Cryptography - Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms" in May 2020 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.05262020-draft.pdf
  - The paper discussed what we can do now as the first step to prepare for the transition

- NCCoE held a Virtual Workshop on Considerations in Migrating to Post-Quantum Cryptographic Algorithms on October 7, 2020
  - About 300 researchers, practitioners, implementers, and policy makers participated workshop
  - Covered experiment implementations on protocols, like TLS, IKE, DNSSEC, and applications like code signing using PQC algorithms
  - Shared transition timeline for specific application community, e.g. financial service
  - Identified some strategies on smooth transition, e.g. dual-signature for PKI
  - Explored hybrid mode in various of protocols e.g. Hybrid mode in TLS 1.3

  Presentations/records can be found at https://www.nccoe.nist.gov/events/virtual-workshop-considerations-migrating-post-quantum-cryptographic-algorithms

Summary and Contact

- NIST announced the 3rd round 7 finalists and 8 alternate candidates in July 2020
- NIST plans to release draft standards for public comments in 2022-2023
- It is the time to prepare for transition and migration

- We will continue open for suggestions and encourage discussions
  - For NIST PQC project, please follow us at https://www.nist.gov/pqcrypto
  - To submit a comment, send e-mail to pqc-comments@nist.gov
  - Join discussion mailing list pqc-forum@nist.gov