Cryptography in a Post-Quantum World

Dustin Moody

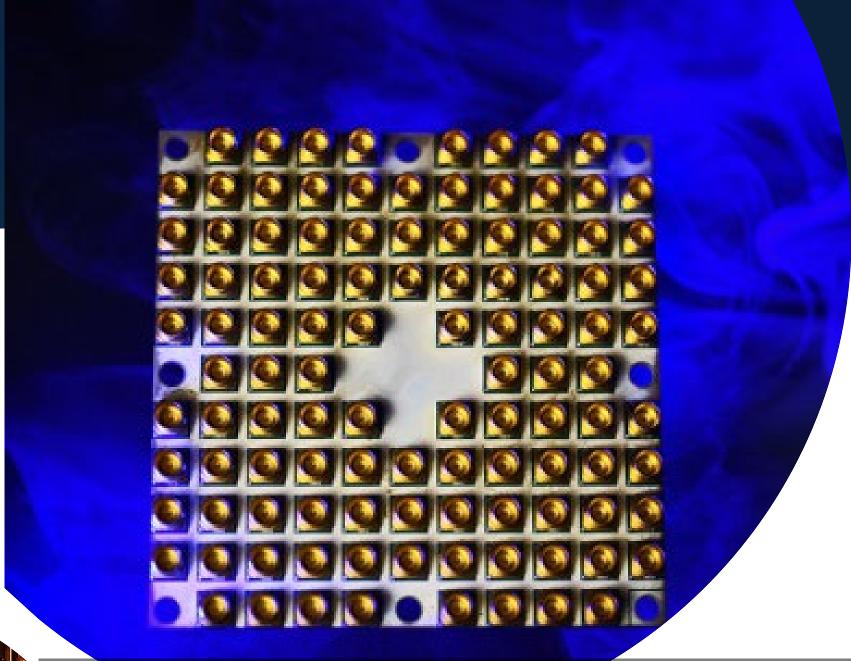
National Institute of Standards and Technology
U.S. Department of Commerce

Crypto Technology Group
Computer Security Division
Information Technology Lab

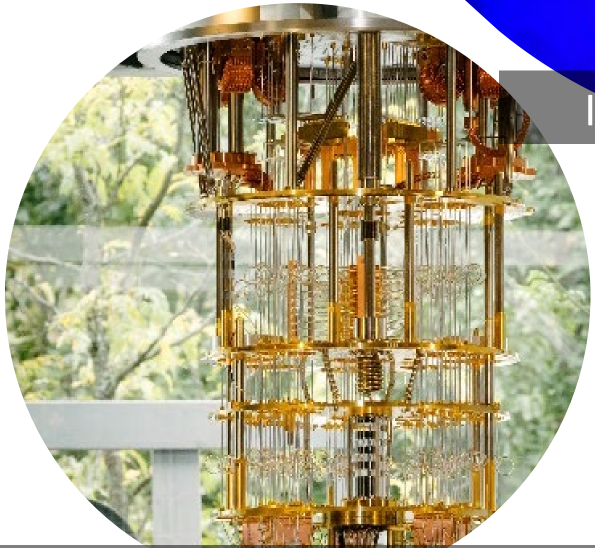
Quantum Computers

- Exploit quantum mechanics to process information
- ”Qubits” instead of bits
- Potential to vastly increase computational power beyond classical computing limit

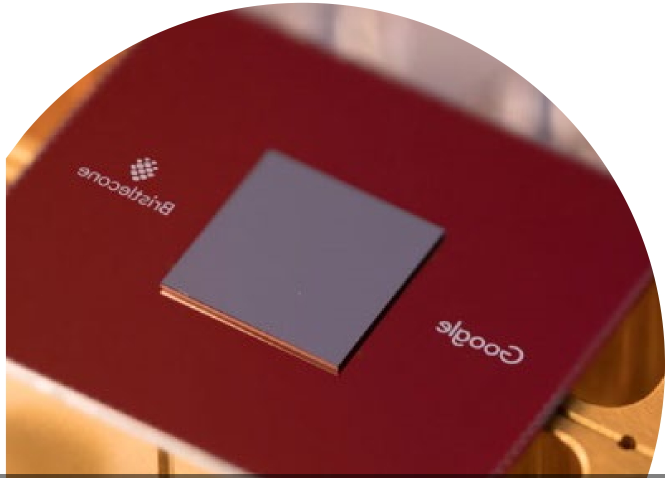
- Limitations:
  - When a measurement is made on quantum system, superposition collapses
  - Only good at certain problems
  - Quantum states are very fragile and must be extremely well isolated



Intel’s 49-qubit chip “Tangle-Lake”



IBM’s 50-qubit quantum computer

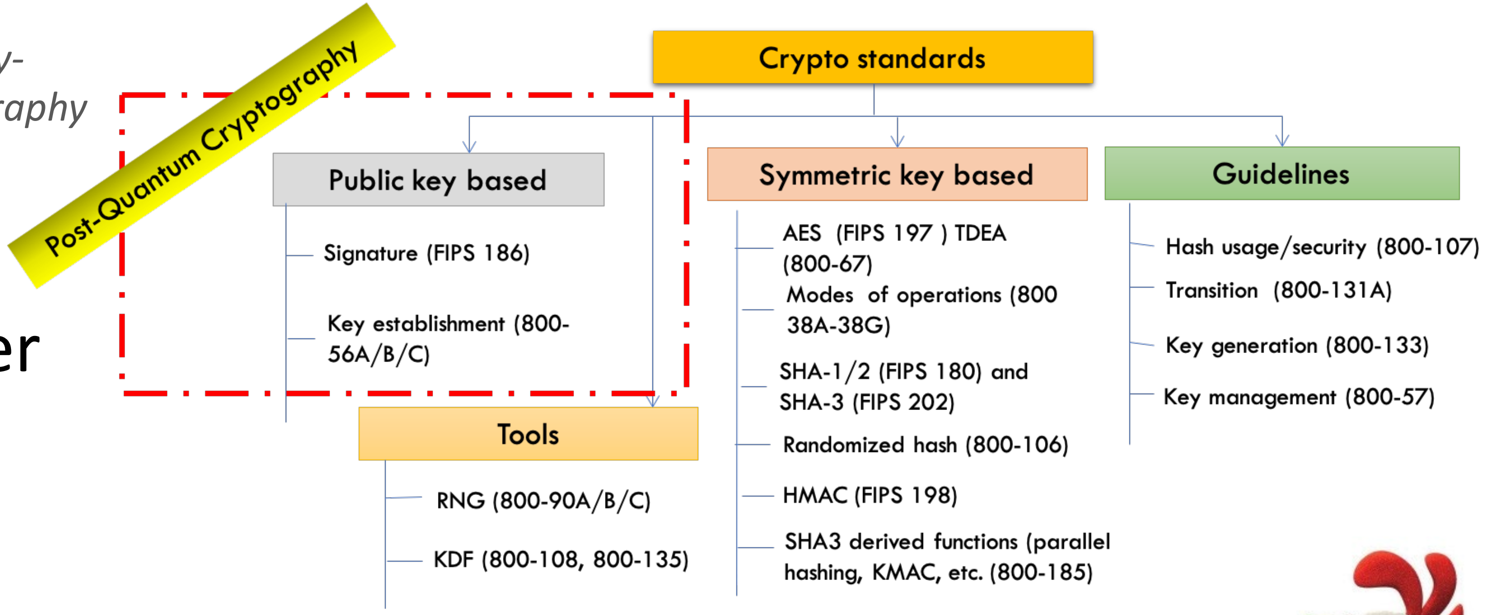


Google’s 72-qubit chip “Bristlecone”

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*

  vulnerable to attacks from a (large-scale) quantum computer



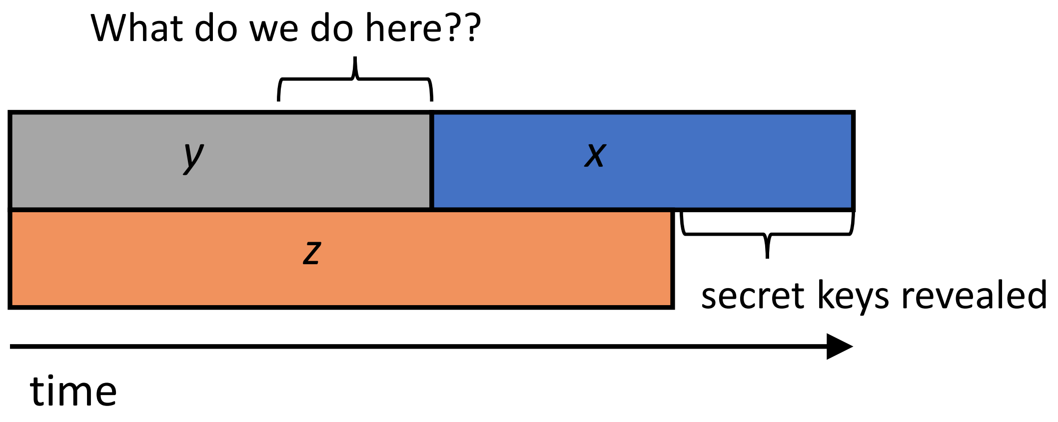
- Shor's algorithm would break RSA, ECDSA, (EC)DH, DSA
- Symmetric-key crypto standards would also be affected, but less dramatically

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?

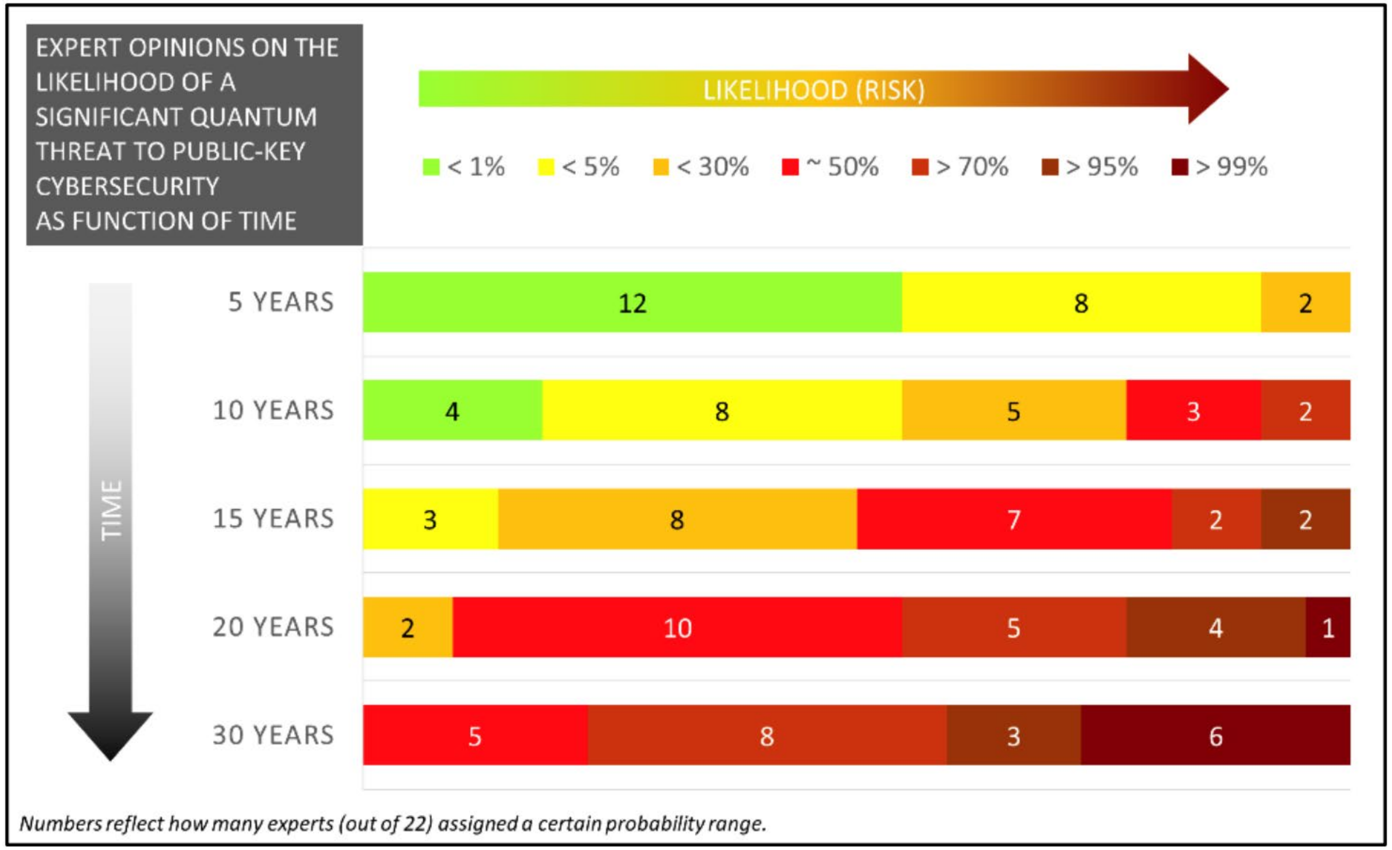
Theorem (Mosca): If $x + y > z$, then worry



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

When will a Quantum Computer be Built?

NIST



Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, Oct 2019

available at: https://globalriskinstitute.org/publications/quantum-threat-timeline/

Quantum Cryptography aka QKD

Using quantum technology to build cryptosystems

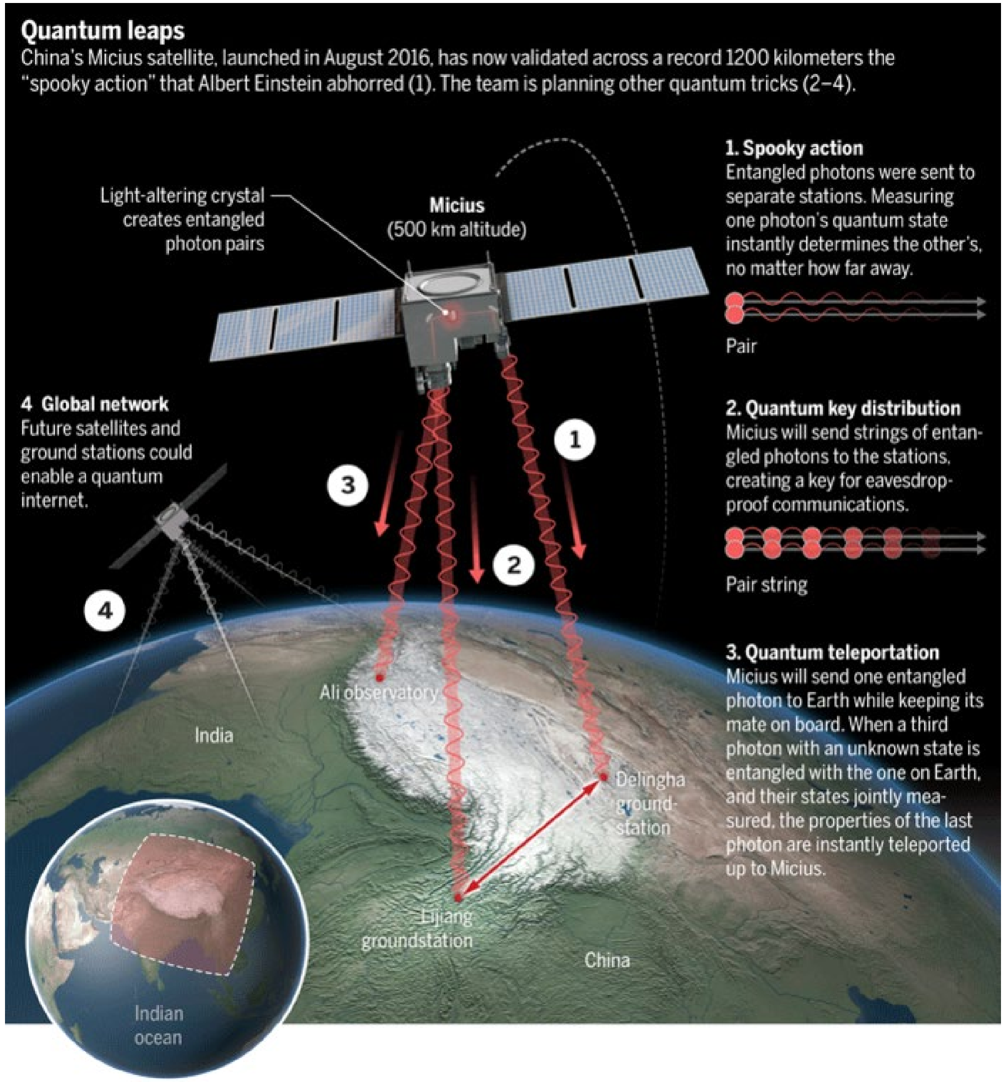
- Theoretically unconditional security guaranteed by the laws of physics

Limitations

- Can do encryption, but not authentication
- Quantum networks not very scalable
- Expensive and needs special hardware

Lots of money being spent on “quantum”

This is <u>NOT</u> our focus



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

Evaluation Criteria

NIST

Security – against both classical and quantum attacks

Level	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)

NIST asked submitters to focus on levels 1,2, and 3. (Levels 4 and 5 are for very high security)

Performance – measured on various classical platforms

Other properties: Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, etc.

A Worldwide Effort

25 Countries

16 States

6 Continents

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

NIST

- 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

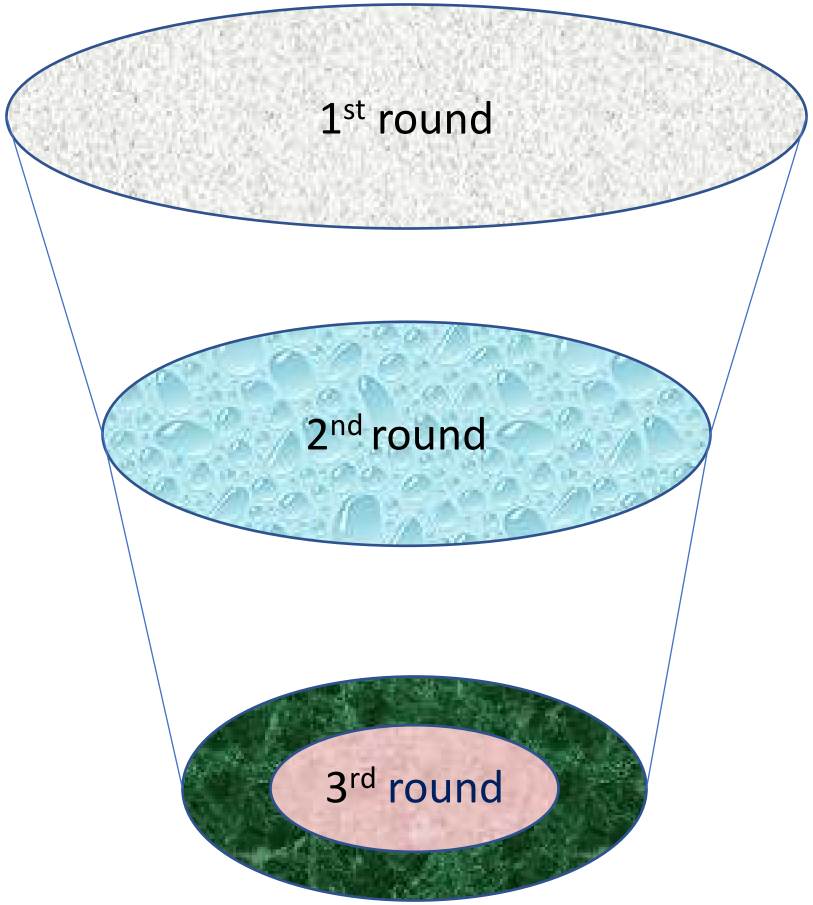
NIST

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

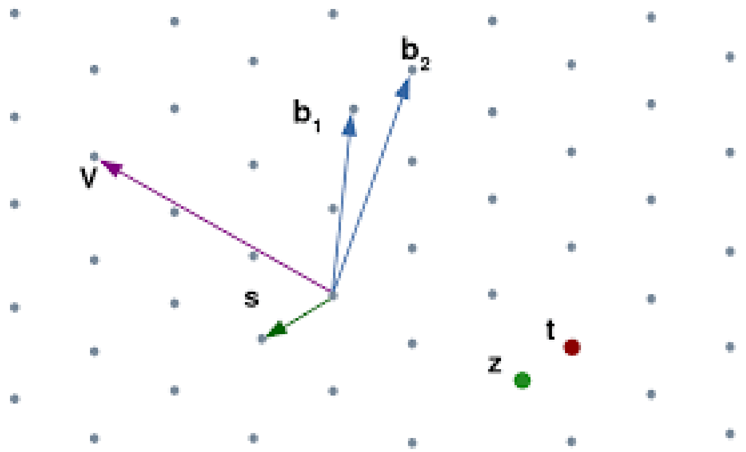
- KEM alternates: Bike, FrodoKEM, HQC, NTRUprime, SIKE
- Signature alternates: GeMSS, Picnic, Sphincs+

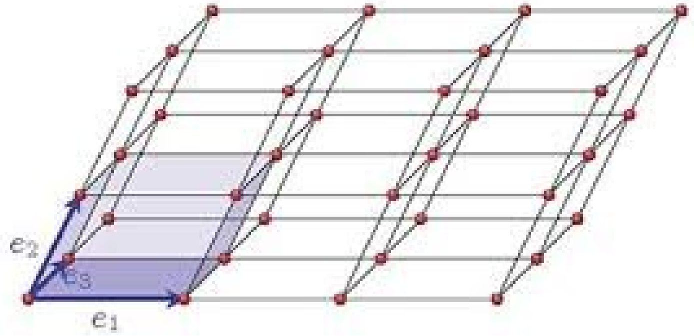
	Signatures		KEM/Encryption		Overall	
Lattice-based	2		3	2	5	2
Code-based			1	2	1	2
Multi-variate	1	1			1	1
Stateless Hash or Symmetric based		2				2
Isogeny				1		1
Total	3	**3**	4	**5**	7	**8**

Lattice-based KEMs

NIST

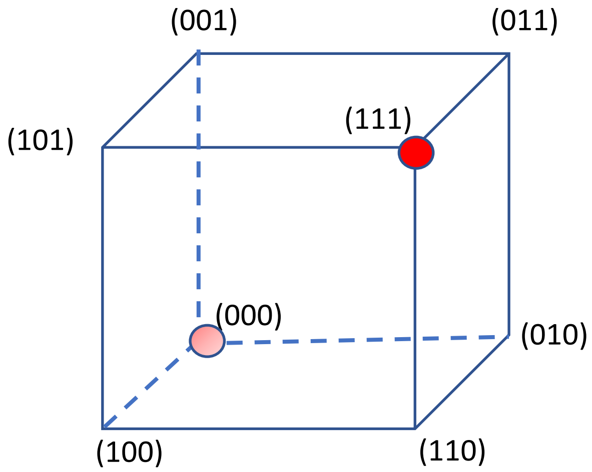
- Crystals-Kyber
  - Great all-around → Finalist
- Saber
  - Great all-around → Finalist
- NTRU
  - Not quite as efficient, but older, IP situation → Finalist
- NTRUprime
  - Different design choice and security model → Alternate
- FrodoKEM
  - Conservative/Backup → Alternate

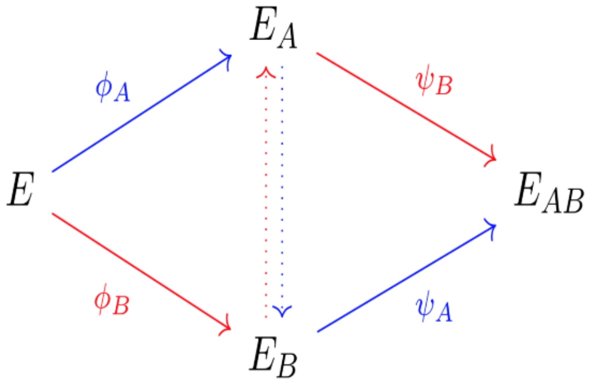




Isogeny- and Code-based KEMs

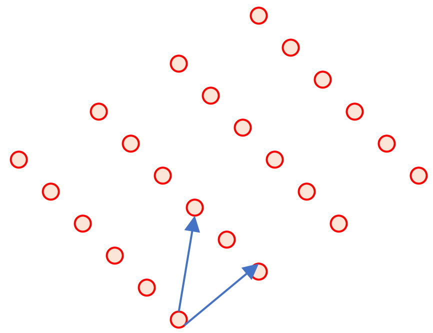
- Classic McEliece
  - Oldest submission, large public keys but small ciphertexts→ Finalist
- BIKE
  - Good performance, CCA security?, more time to be stable → Alternate
- HQC
  - Better security analysis/larger keys (than BIKE) → Alternate
- SIKE
  - Newer security problem, an order slower → Alternate

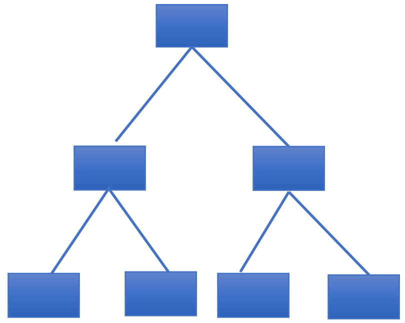




The Signatures

- Dilithium and Falcon
  - Both balanced, efficient lattice-based signatures
  - coreSVP security higher?
  - → Finalists
- SPHINCS+ and Picnic
  - SPHINCS+ is stable, conservative security, larger/slower → Alternate
  - Picnic not stable yet, but has lots of potential → Alternate
- Rainbow and GeMMS
  - Both have large public keys, small signatures. Rainbow a bit better → Finalist, GeMMS → Alternate





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

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

$$\vdots$$

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

Timeline

NIST

- 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

Research Challenges

NIST

- Many important topics to be studied:
  - Security proofs in both the ROM and QROM
  - Does the specific ring/module/field choice matter for security?
    - Or choice of noise distribution?
    - Does “product” or “quotient” style LWE matter?
  - Finer-grained metrics for security of lattice-based crypto (coreSVP vs. real-world security)
  - Are there any important attack avenues that have gone unnoticed?
  - Side-channel attacks/resistant implementations for finalists and alternates
  - More hardware implementations
  - Ease of implementations – decryption failures, floating point arithmetic, noise sampling, etc.

- Specific algorithm questions
  - Decoding analysis for BIKE, category 1 security levels for Kyber/Saber/Dilithium, algebraic cryptanalysis of cyclotomics for lattices, etc…

Other Challenges

- Many other challenges to work on
  - IP issues
  - Continued performance benchmarking in different platforms and environments
    - For hardware – NIST suggested Artix-7 and Cortex M4 (with all options) for easier comparison
  - Real world experiments
    - How do these algorithms work in actual protocols and applications.
      - Are some key sizes too large?

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

NIST specification on stateful hash-based signatures

- NIST SP 800-208 "*Recommendation for Stateful Hash-Based Signature Schemes*"

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

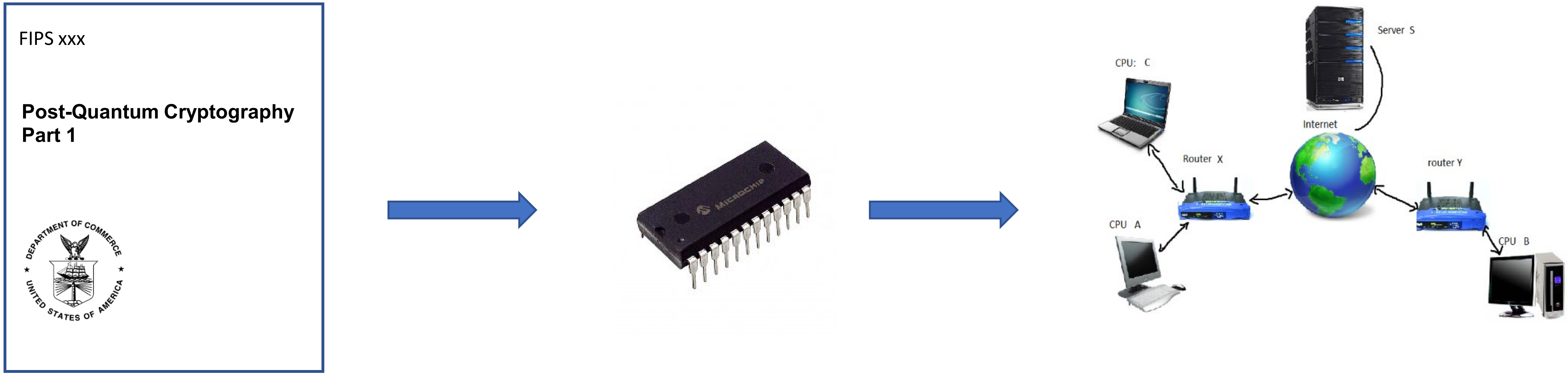
- RFC 8391 "XMSS: eXtended Merkle Signature Scheme" (By Internet Research Task Force (IRTF))
- RFC 8554 "Leighton-Micali Hash-Based Signatures" (By Internet Research Task Force (IRTF))

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

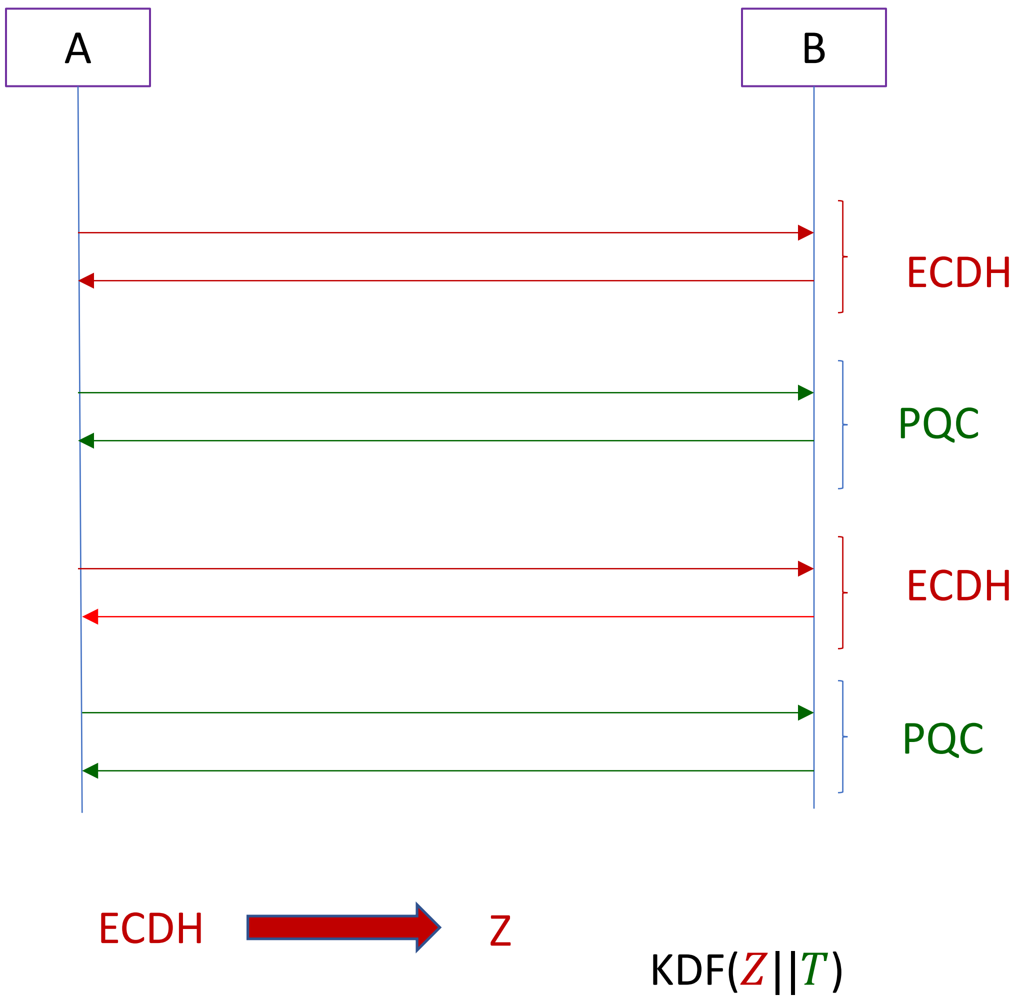
- Public key Cryptography has been used everywhere; 2 important uses:
  - Communication security; and
  - Trusted platforms
- Transition and migration are going to be a long journey full of exciting adventures
  - Understand new features, characters, implementation challenges
  - Identify barriers, issues, 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

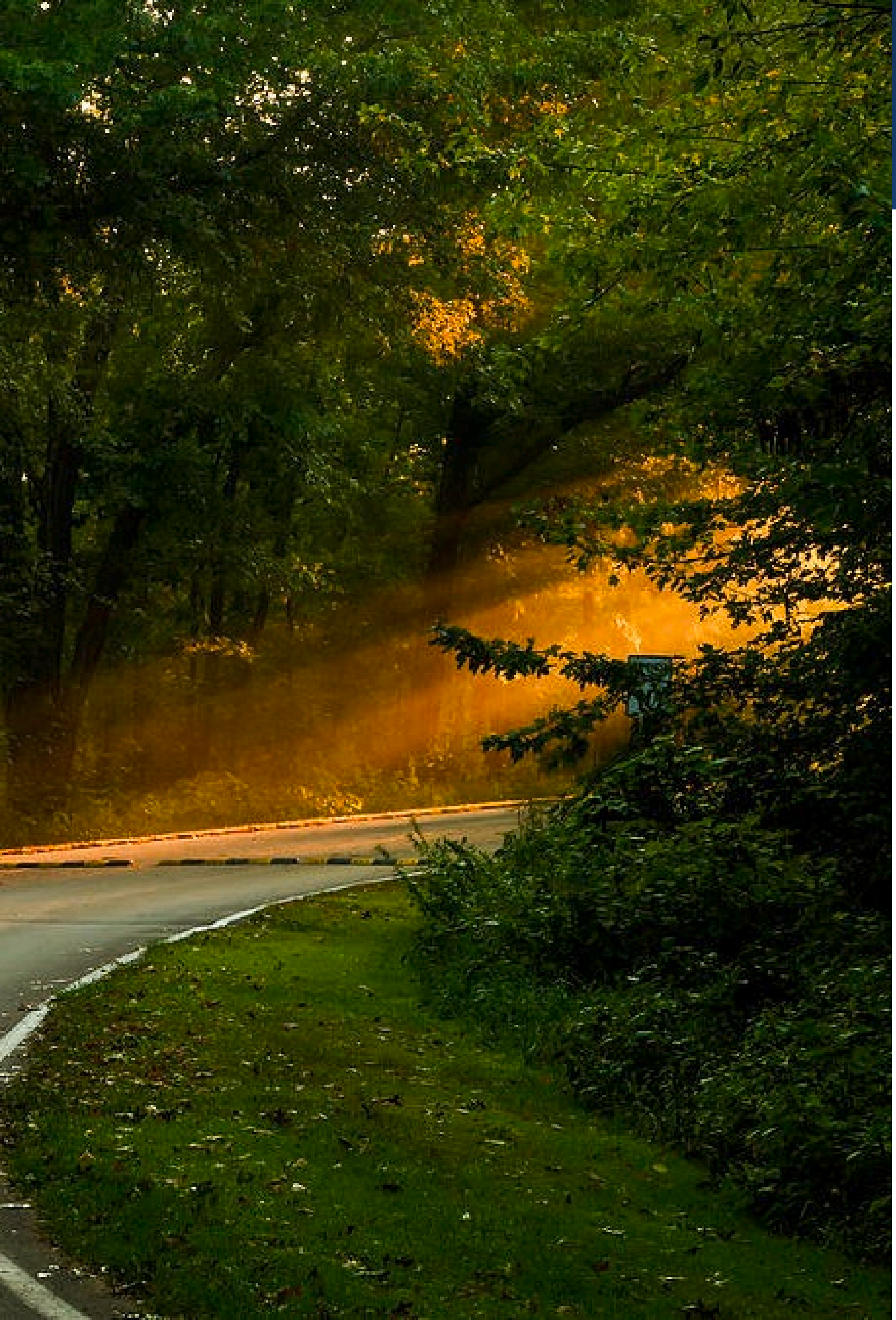
- The timeframe will be based on a risk assessment of quantum attacks
- NCCoE hosted a workshop on *Considerations in Migrating to Post-Quantum Cryptographic Algorithms* on October 7

What can organizations do now?

NIST

- Perform a quantum risk assessment within your organization
  - 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