Cryptography in a Post-Quantum World

Dustin Moody

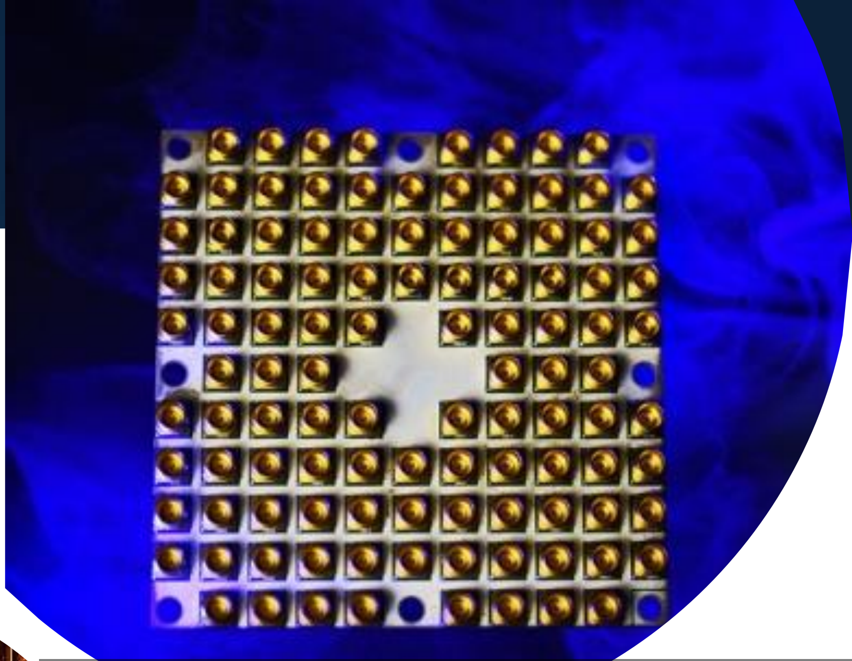
National Institute of Standards and Technology
U.S. Department of Commerce

Crypto Technology Group
Computer Security Division
Information Technology Lab

Quantum Computers

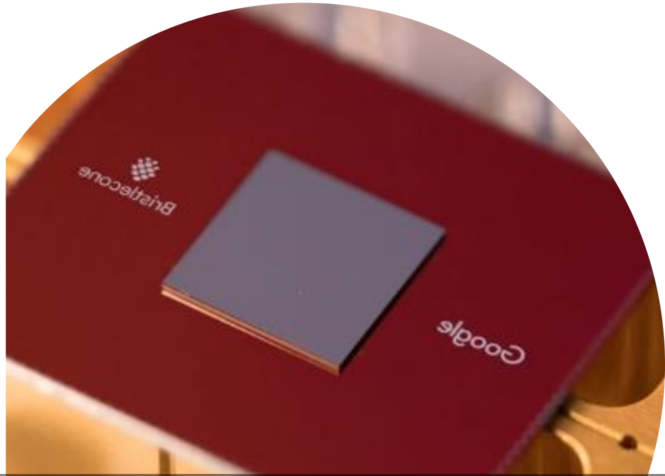
- Exploit quantum mechanics to process information
- ”Qubits” instead of bits
- Potential to vastly increase computational power beyond classical computing limit

- 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



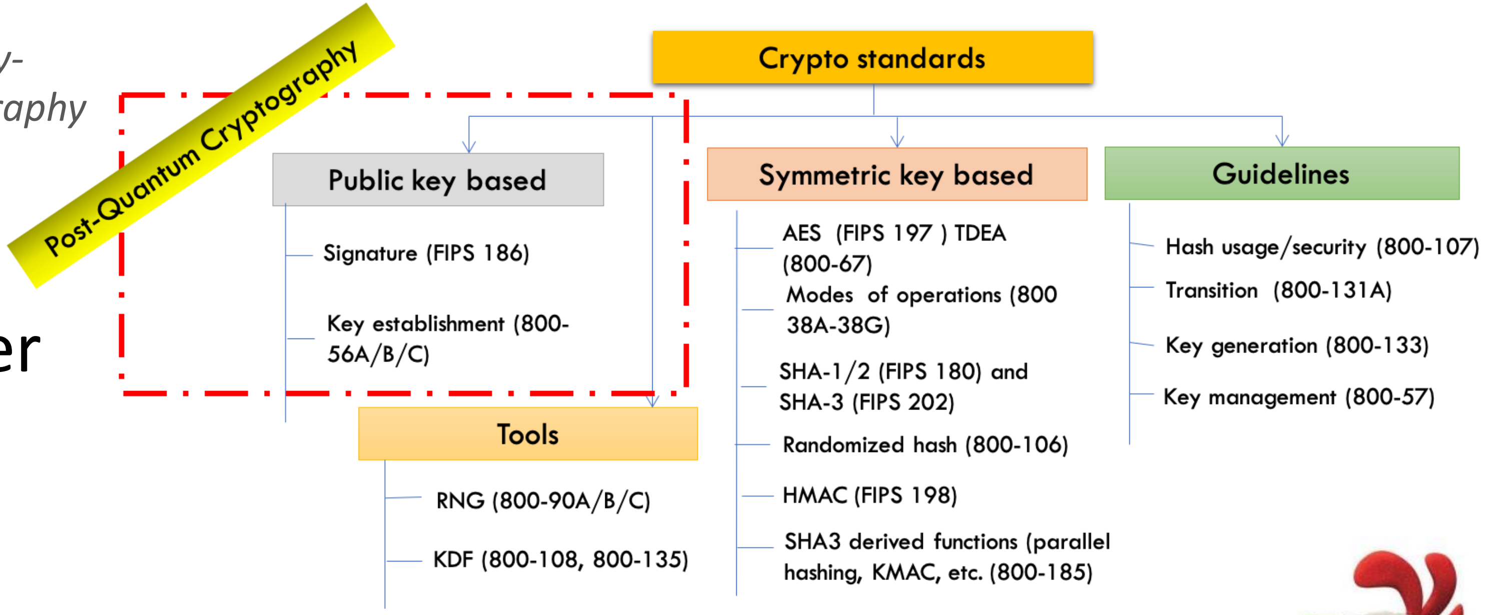
Google’s 72-qubit chip “Bristlecone”

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

Crypto standards

Public key based
- Signature (FIPS 186)
- Key establishment (800-56A/B/C)

Tools
- RNG (800-90A/B/C)
- KDF (800-108, 800-135)

Symmetric key based
- AES (FIPS 197) TDEA (800-67)
- Modes of operations (800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
- Randomized hash (800-106)
- HMAC (FIPS 198)
- SHA3 derived functions (parallel hashing, KMAC, etc. (800-185)

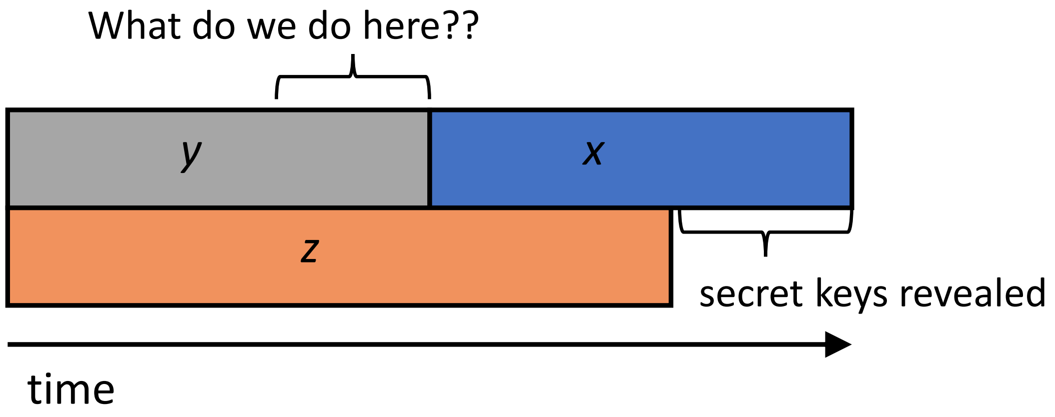
Guidelines
- Hash usage/security (800-107)
- Transition (800-131A)
- Key generation (800-133)
- Key management (800-57)

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

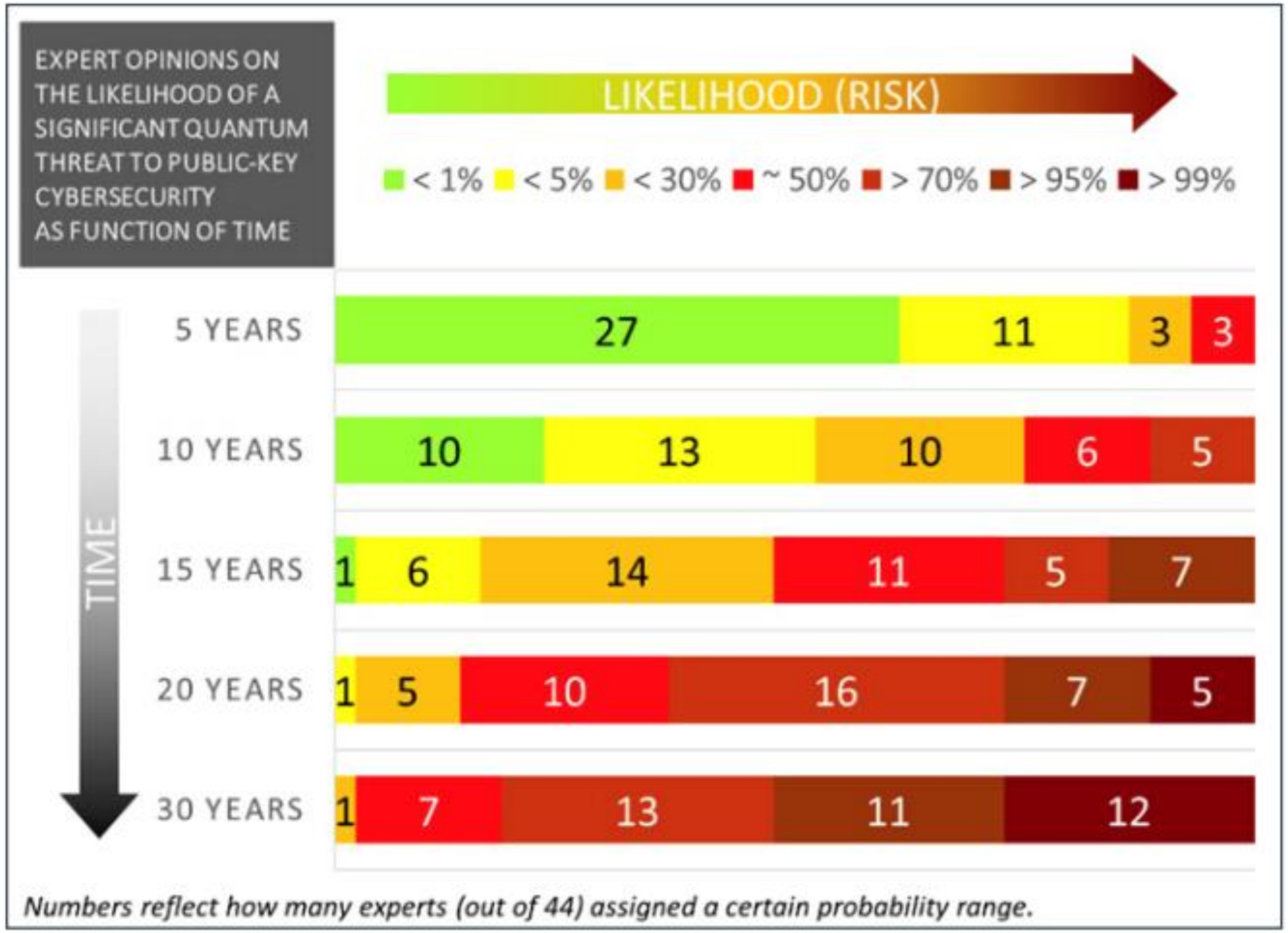


x – time of maintaining data security

y – time for PQC standardization and adoption

z – time for quantum computer to be developed

When will a Quantum Computer be Built?



Numbers reflect how many experts (out of 44) assigned a certain probability range.

Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2020

available at: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

Quantum Cryptography aka QKD

Using quantum technology to build cryptosystems

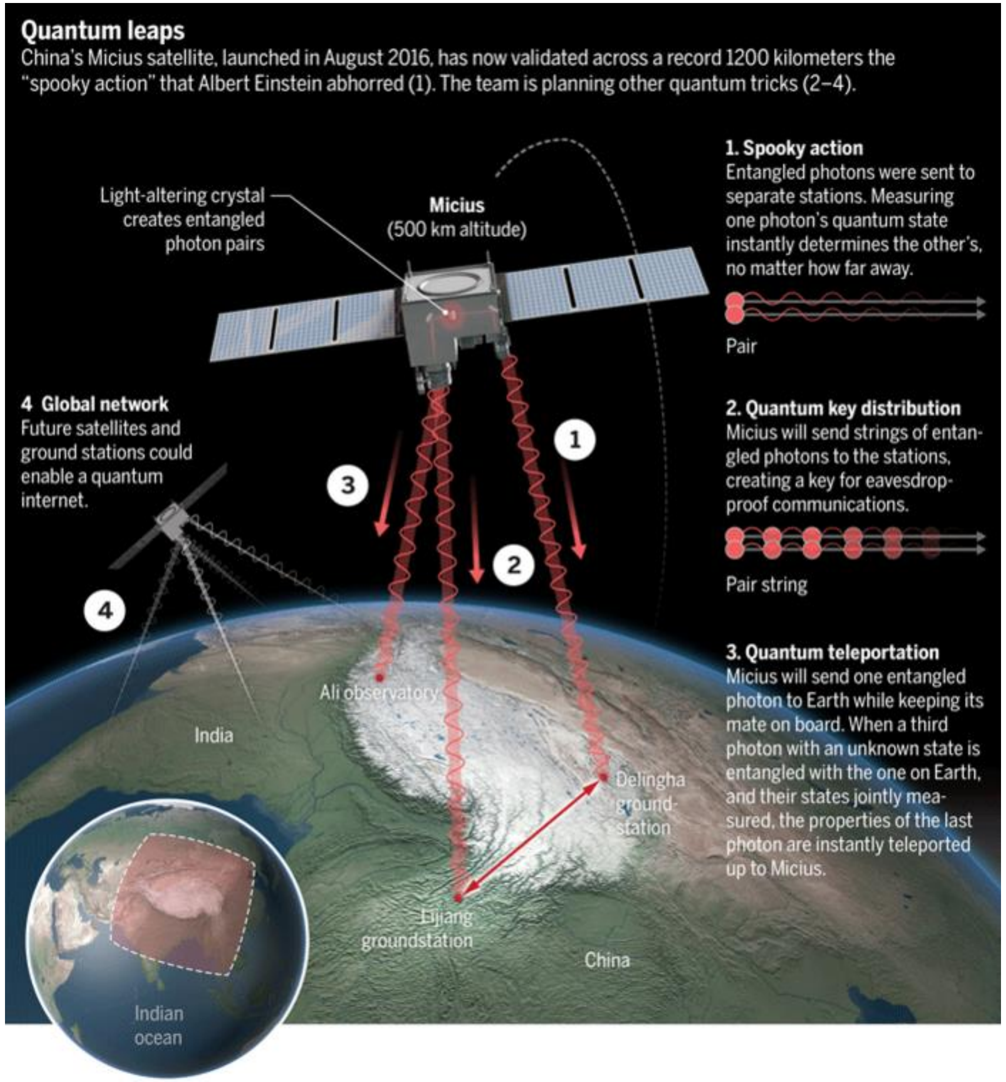
- Theoretically unconditional security guaranteed by the laws of physics

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



Quantum leaps

China's Micius satellite, launched in August 2016, has now validated across a record 1200 kilometers the “spooky action” that Albert Einstein abhorred (1). The team is planning other quantum tricks (2–4).

1. Spooky action
Entangled photons were sent to separate stations. Measuring one photon's quantum state instantly determines the other's, no matter how far away.

2. Quantum key distribution
Micius will send strings of entangled photons to the stations, creating a key for eavesdrop-proof communications.

3. Quantum teleportation
Micius will send one entangled photon to Earth while keeping its mate on board. When a third photon with an unknown state is entangled with the one on Earth, and their states jointly measured, the properties of the last photon are instantly teleported up to Micius.

4 Global network
Future satellites and ground stations could enable a quantum internet.

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

Security – against both classical and quantum attacks

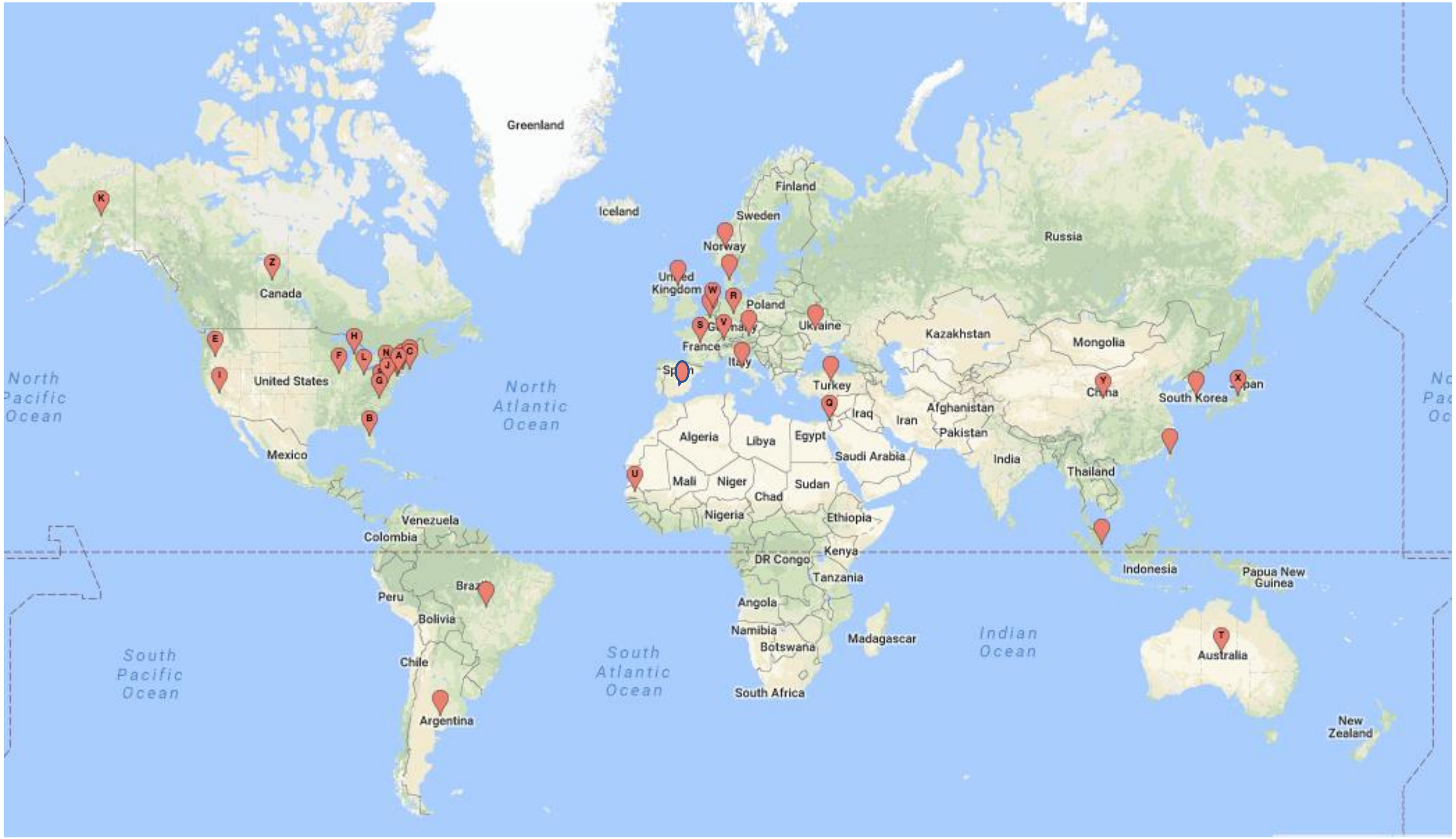
Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (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**

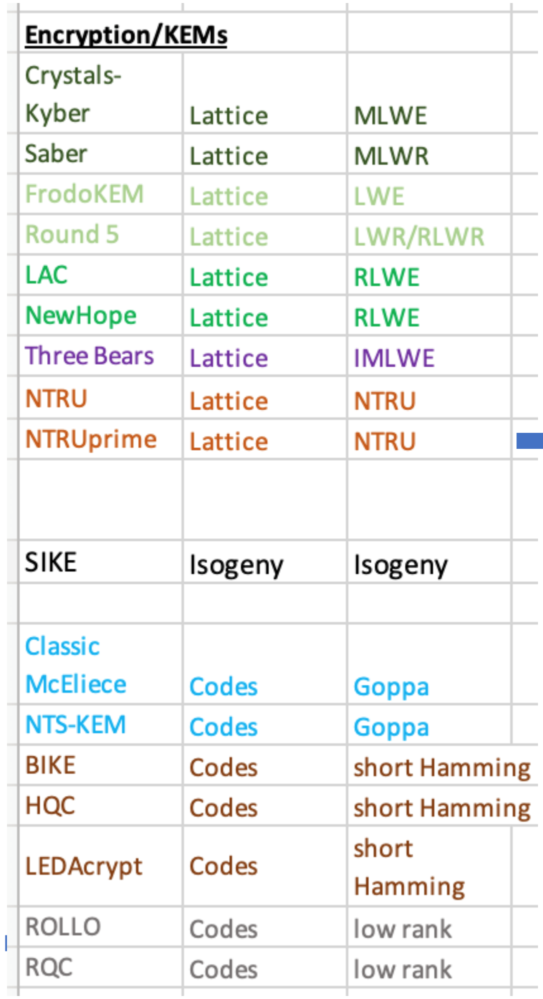
The 2nd Round

- 4 merged submissions
- Maintained diversity of algorithms
- Cryptanalysis continues

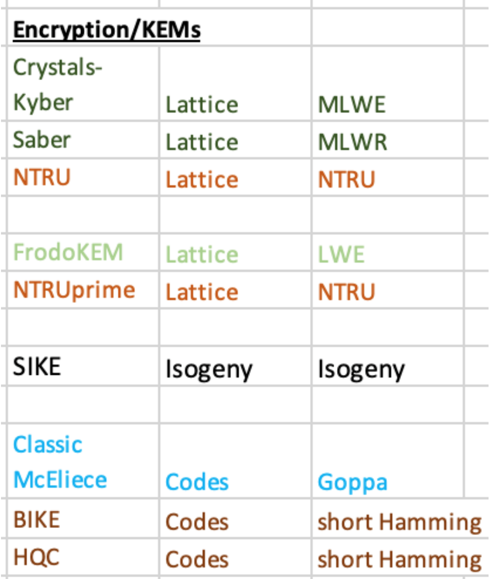
  LAC, LEDAcrypt, RQC, Rollo, MQDSS, qTESLA, LUOV all broken
- 2nd NIST PQC Standardization workshop
- More benchmarking and real world experiments
- After 18 months: 15 submissions move on

	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**

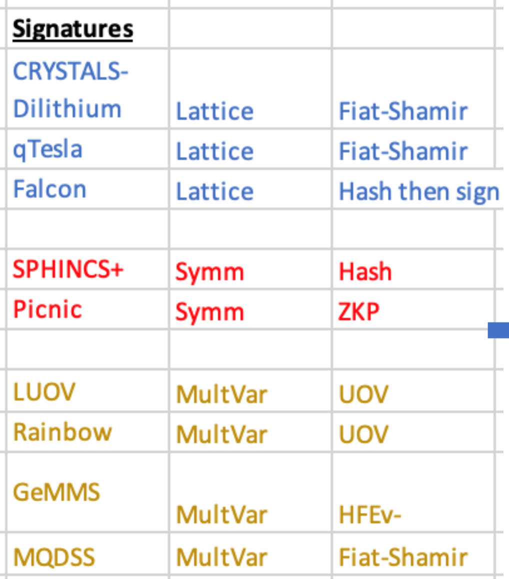
Biting the Bullet



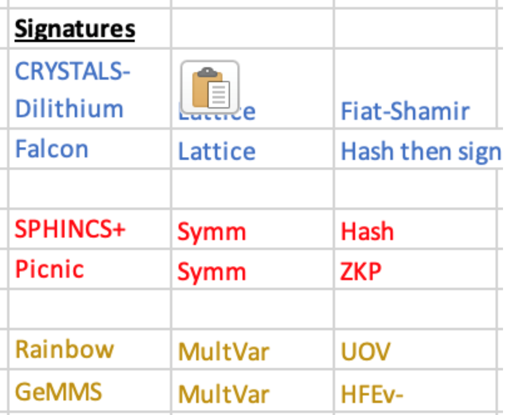
Encryption/KEMs		
Crystals-Kyber	Lattice	MLWE
Saber	Lattice	MLWR
FrodoKEM	Lattice	LWE
Round 5	Lattice	LWR/RLWR
LAC	Lattice	RLWE
NewHope	Lattice	RLWE
Three Bears	Lattice	IMLWE
NTRU	Lattice	NTRU
NTRUprime	Lattice	NTRU
SIKE	Isogeny	Isogeny
Classic McEliece	Codes	Goppa
NTS-KEM	Codes	Goppa
BIKE	Codes	short Hamming
HQC	Codes	short Hamming
LEDAcrypt	Codes	short Hamming
ROLLO	Codes	low rank
RQC	Codes	low rank



Encryption/KEMs		
Crystals-Kyber	Lattice	MLWE
Saber	Lattice	MLWR
NTRU	Lattice	NTRU
FrodoKEM	Lattice	LWE
NTRUprime	Lattice	NTRU
SIKE	Isogeny	Isogeny
Classic McEliece	Codes	Goppa
BIKE	Codes	short Hamming
HQC	Codes	short Hamming



Signatures		
CRYSTALS-Dilithium	Lattice	Fiat-Shamir
qTesla	Lattice	Fiat-Shamir
Falcon	Lattice	Hash then sign
SPHINCS+	Symm	Hash
Picnic	Symm	ZKP
LUOV	MultVar	UOV
Rainbow	MultVar	UOV
GeMMS	MultVar	HFEv-
MQDSS	MultVar	Fiat-Shamir



Signatures		
CRYSTALS-Dilithium	Lattice	Fiat-Shamir
Falcon	Lattice	Hash then sign
SPHINCS+	Symm	Hash
Picnic	Symm	ZKP
Rainbow	MultVar	UOV
GeMMS	MultVar	HFEv-

The 3^{rd} Round Finalists and Alternates

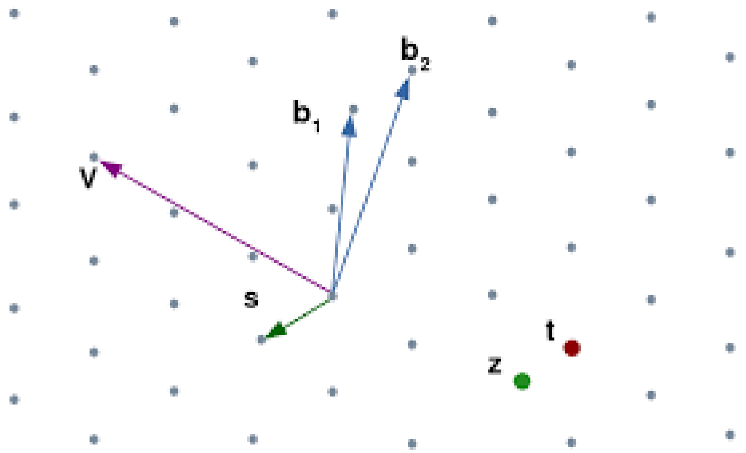
- NIST selected 7 Finalists and 8 Alternates
  - Finalists: most promising algorithms we expect to be ready for standardization at end of 3^{rd} round
  - Alternates: candidates for potential standardization, most likely after another (4th) round
- KEM finalists: Kyber, NTRU, SABER, Classic McEliece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

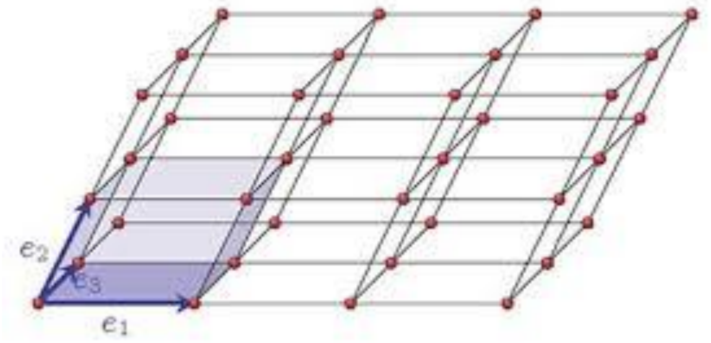
- KEM alternates: Bike, FrodoKEM, HQC, NTRUprime, SIKE
- Signature alternates: GeMSS, Picnic, Sphincs+

	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

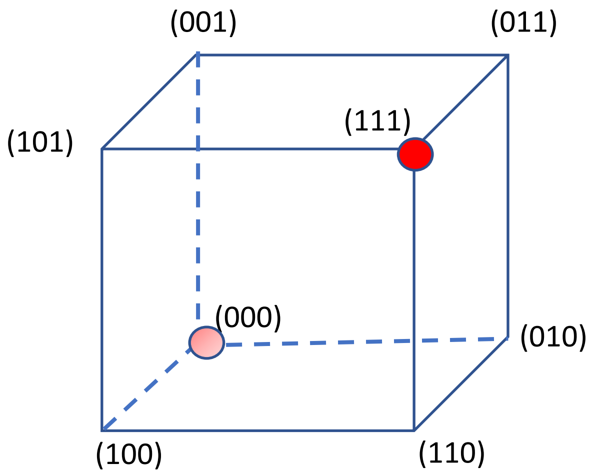
- Crystals-Kyber
  - Great all-around → Finalist
- Saber
  - Great all-around → Finalist
- NTRU
  - Not quite as efficient, but older, IP situation → Finalist
- NTRUprime
  - Different design choice and security model → Alternate
- FrodoKEM
  - Conservative/Backup → Alternate





Isogeny- and Code-based KEMs

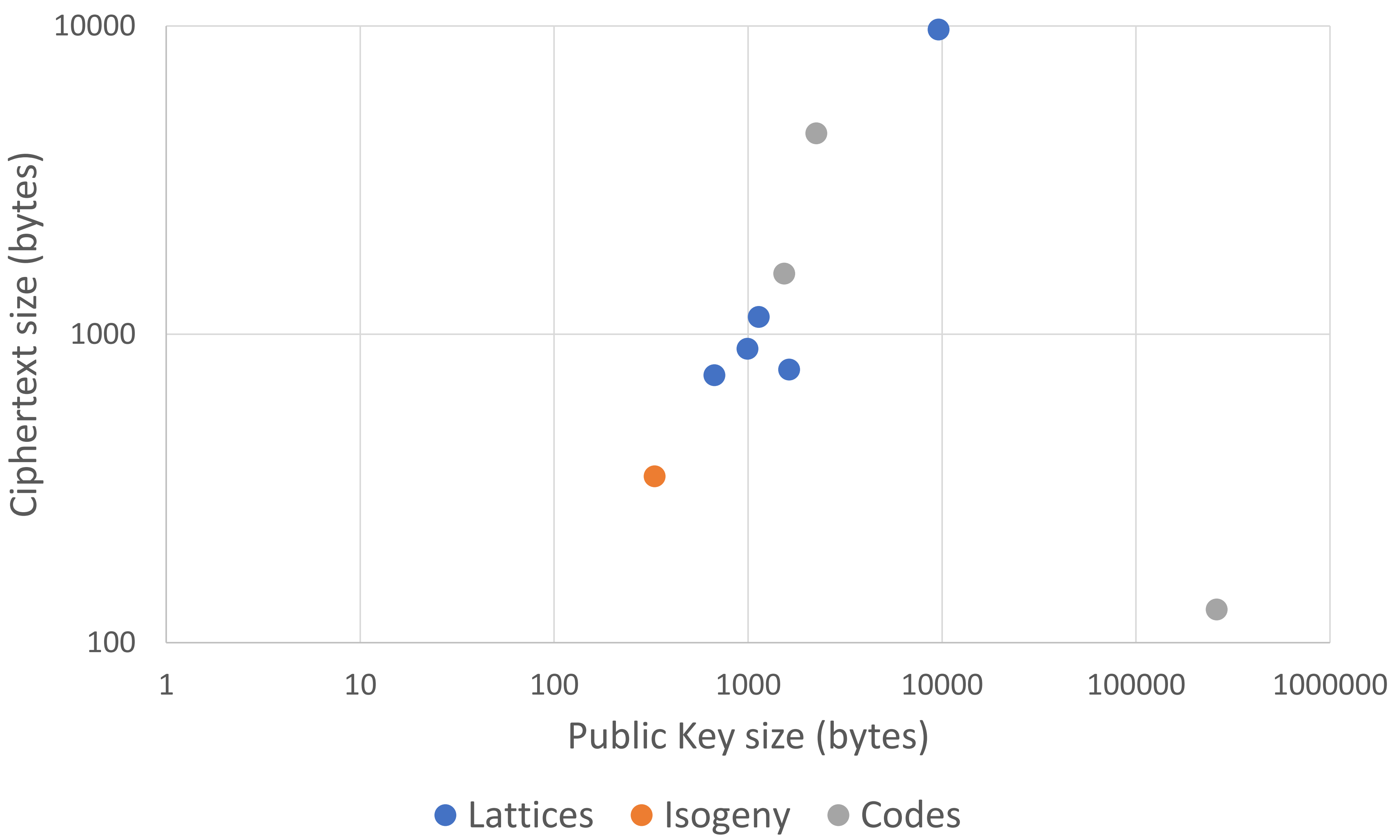
- Classic McEliece
  - Oldest submission, large public keys but small ciphertexts→ Finalist
- BIKE
  - Good performance, CCA security?, more time to be stable → Alternate
- HQC
  - Better security analysis/larger keys (than BIKE) → Alternate
- SIKE
  - Newer security problem, an order slower → Alternate



$$\begin{tikzcd}
 & E_A \arrow[dr, "\psi_B"] \arrow[dd, dotted, shift left] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_{AB} \\
 & E_B \arrow[ur, "\psi_A"'] \arrow[uu, dotted, shift left] &
\end{tikzcd}$$

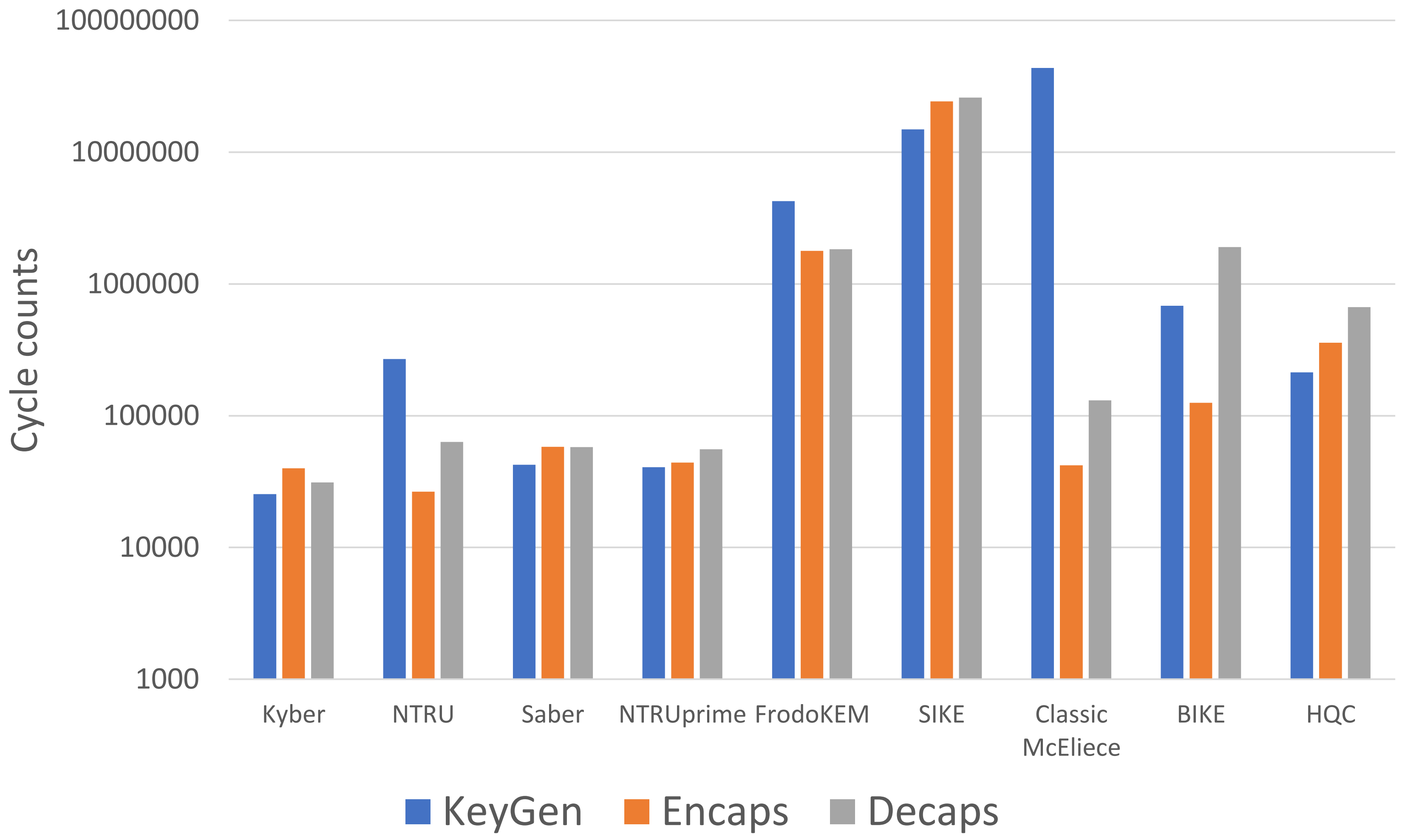
KEM Key sizes (category 1)

Note: Both axes have logarithmic scale



KEM Performance graph (category 1)

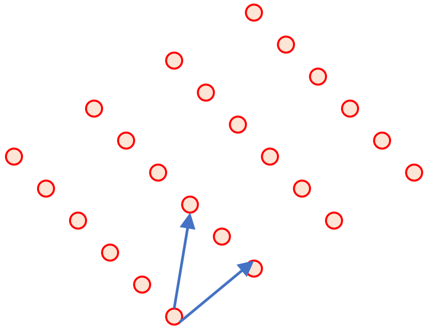
Note: The cycle count axis has logarithmic scale

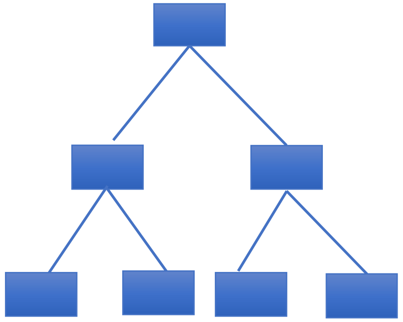


Benchmarks on a Haswell avx2

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
  - 3rd round cryptanalytic results call into question the security for both

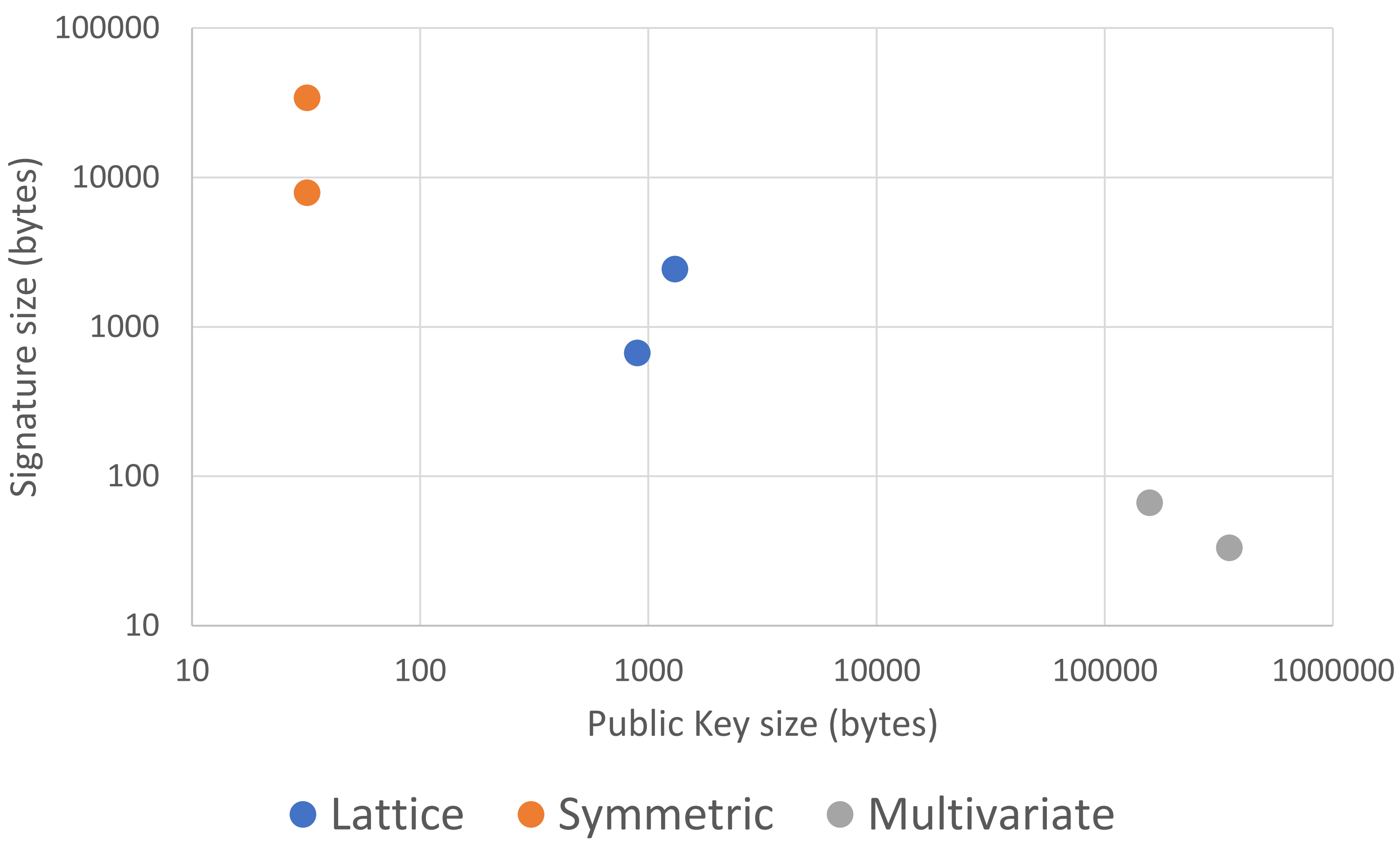




$$\begin{aligned}
p^{(1)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1,\dots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(m)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(m)} \cdot x_i + p_0^{(m)}
\end{aligned}$$

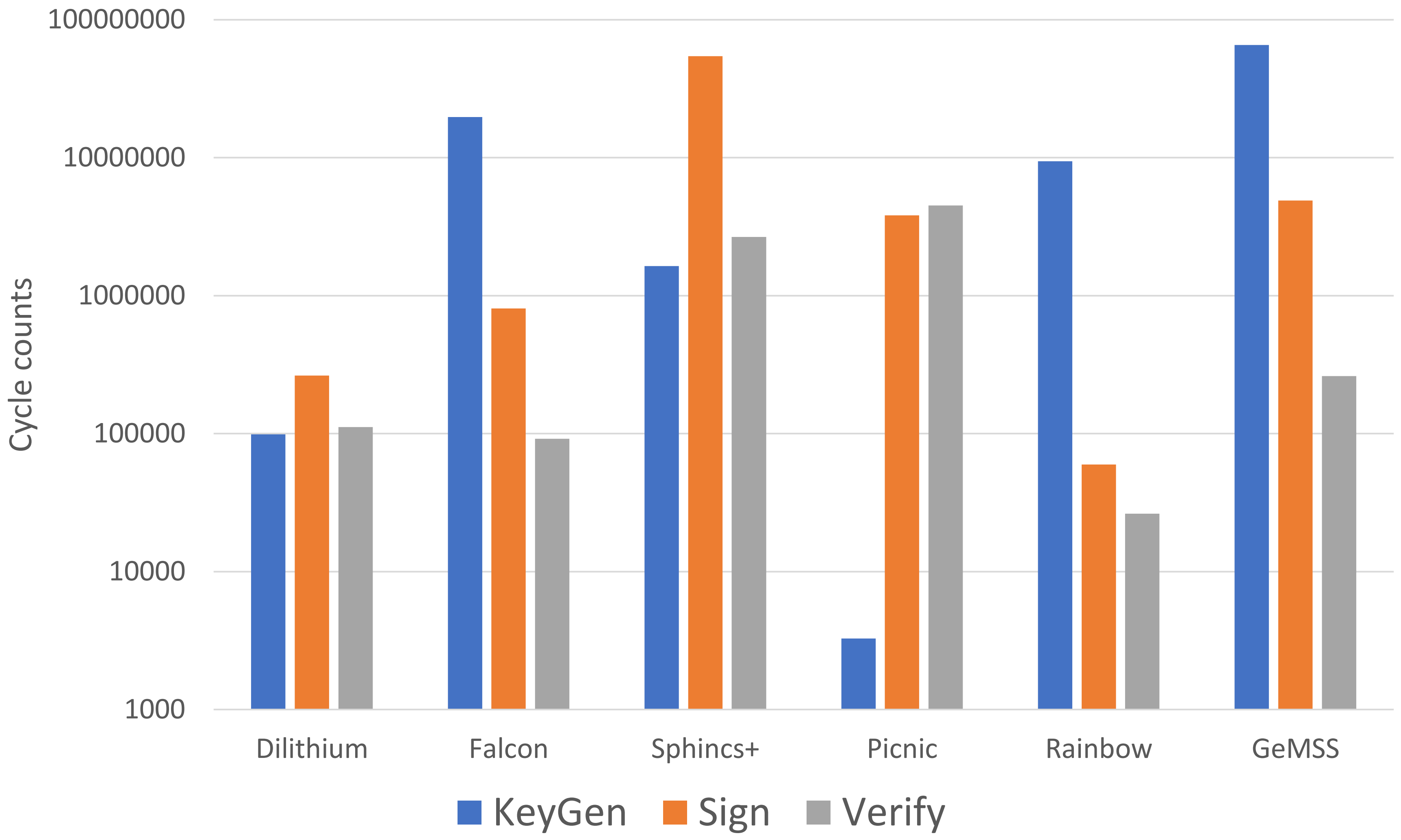
Signature key sizes (category 1)

Note: Both axes have logarithmic scale



Signature Performance graph (category 1)

Note: The cycle count axis has logarithmic scale



Benchmarks on a Haswell avx2

Timeline

- The 3rd Round will end sometime in end of 2021/beginning of 2022
  - NIST will announce which finalist algorithms it will standardize
    - Including potentially SPHINCS+
  - This will include algorithms which will be able to be used by most applications
  - NIST will issue a Report on the 3rd Round to explain our decisions

- NIST will also announce any candidates advancing to 4th round
  - The 4th round will similarly be 12-18 months
  - These algorithms will be for a diversified portfolio, or for applications with different performance needs

- We expect to release draft standards for public comment in 2022-2023
- The first set of standards will hopefully be finalized by 2024

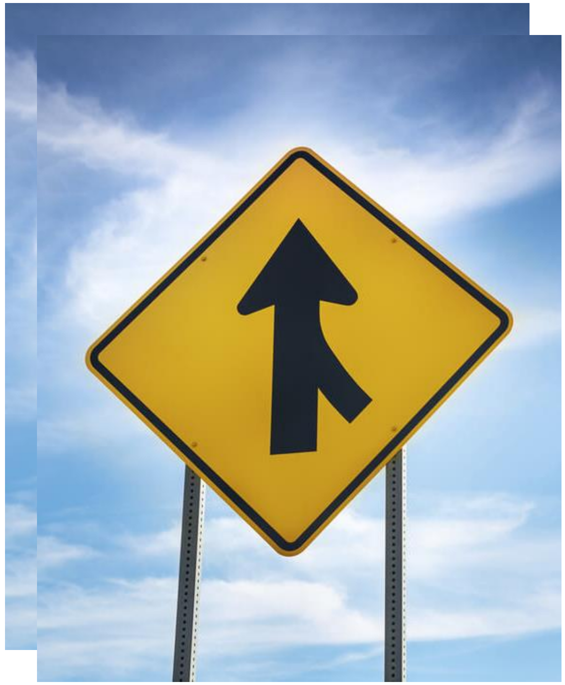
An on-ramp for signatures

- At the conclusion of the 3rd Round, NIST will issue a new Call for Signatures
  - There will be a deadline for submission, likely 6 months – 1 year
  - This will be much smaller in scope than main NIST PQC effort
  - The main reason for this call is to diversify our signature portfolio
  - These signatures will be on a different track than the candidates in the 4th round

- We are **most interested** in a general-purpose digital signature scheme which is not based on structured lattices
  - We may be interested in other signature schemes targeted for certain applications. For example, a scheme with very short signatures.

- The more mature the scheme, the better.

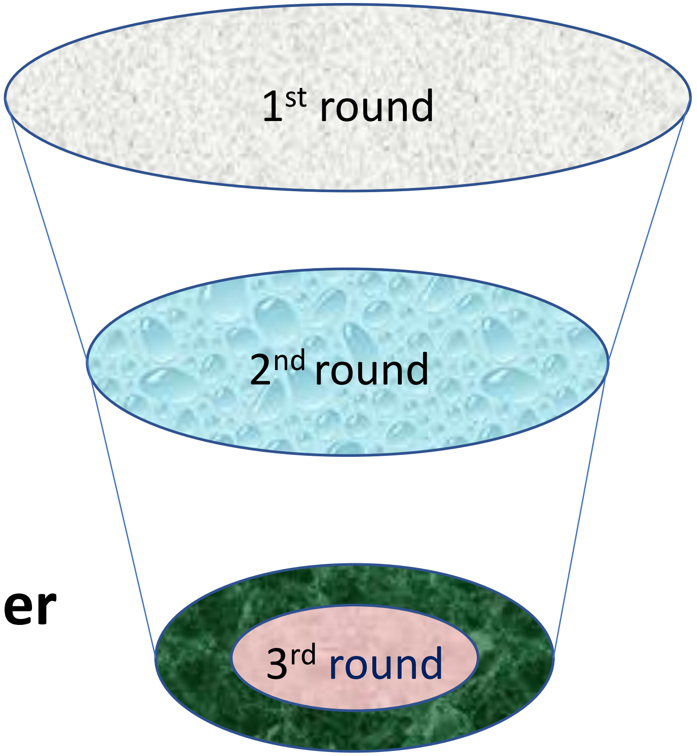
- NIST will decide which (if any) of the received schemes to focus attention on



How will NIST make its decisions?

- **Using the evaluation criteria:**
  - Security
    - Security levels offered, (confidence in) security proof, known 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

- For the lattice KEMs, the main decision will be **Kyber/NTRU/Saber**
- Similarly for lattice signatures, the main decision will be **Dilithium/Falcon**
- Any other algorithms selected will be their own distinct decision



Patent and IPR issues

- This is a very complicated area
- We acknowledge the impact of encumbered technology on adoption

- NIST is actively engaging to try to resolve known IPR issues on the candidates
- When we have something concrete, we will share it

Note: it may not be possible for NIST to resolve all IP concerns

- In light of the above, NIST believes the discussion should be around the impact of IP, and how we should factor these issues into our decision-making
  - *NIST would very much appreciate feedback on the impact of potentially selecting algorithms which may be encumbered*

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))

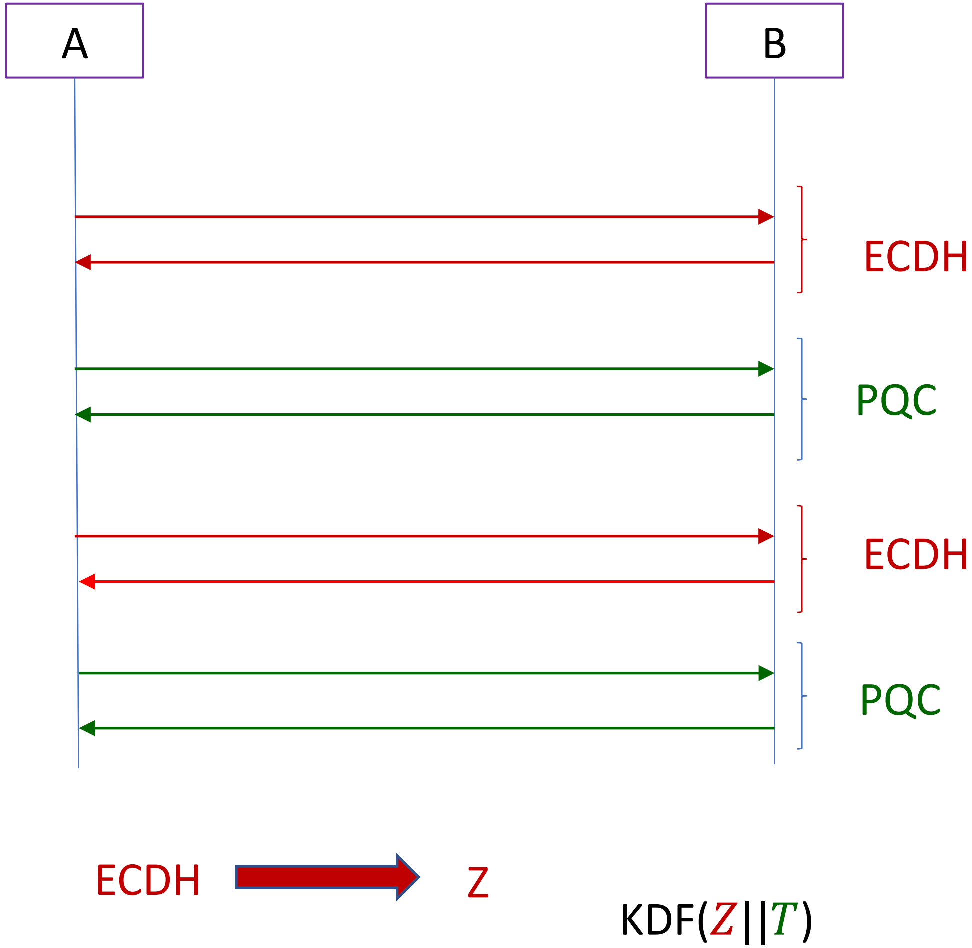
ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

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

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"



The above is just an illustration. The actual combination of two schemes will depend on the protocol specifications.

Crypto transitions

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

Getting ready for PQC

NCCoE
NATIONAL
CYBERSECURITY
CENTER OF
EXCELLENCE

- The National Cybersecurity Center of Excellence (NCCoE) has a project for Migration to PQC . The goals:
  - Align and complement the NIST PQC standardization activities
  - Raise awareness and develop practices to ease the migration to PQC algorithms
  - Deliver white papers, playbooks, and demonstrable implementations for organizations
  - Target organizations that provide cryptographic standards and protocols and enterprises that develop, acquire, implement, and service cryptographic products

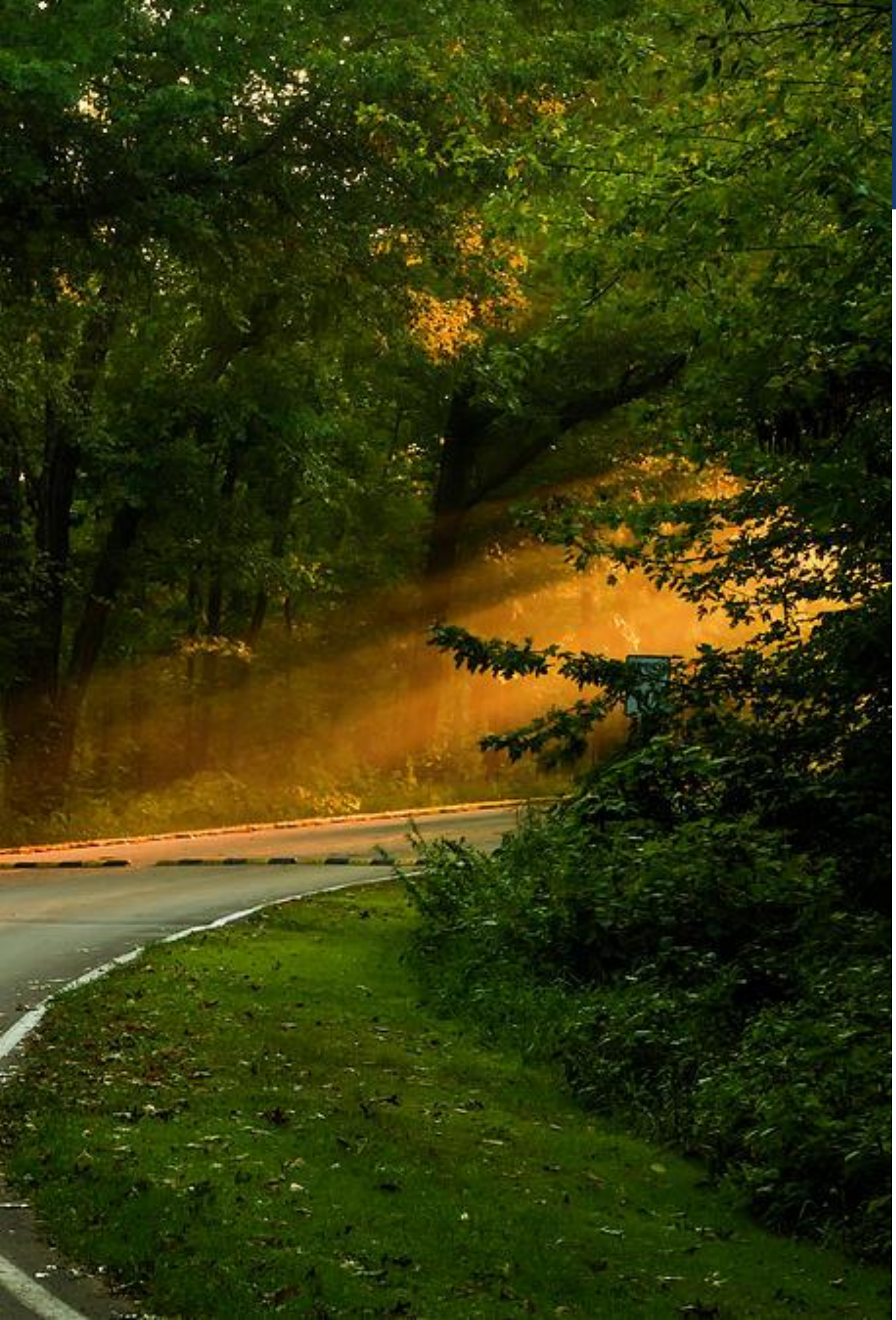
- NCCoE hosted a workshop on *Considerations in Migrating to Post-Quantum Cryptographic Algorithms* in October 2020

- If you are interested in joining the project team as a collaborator, please review the requirements identified in the Federal Register Notice which is based on the final project description.
  - Questions and comments: applied-crypto-pqc@nist.gov

What can organizations do now?

- 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