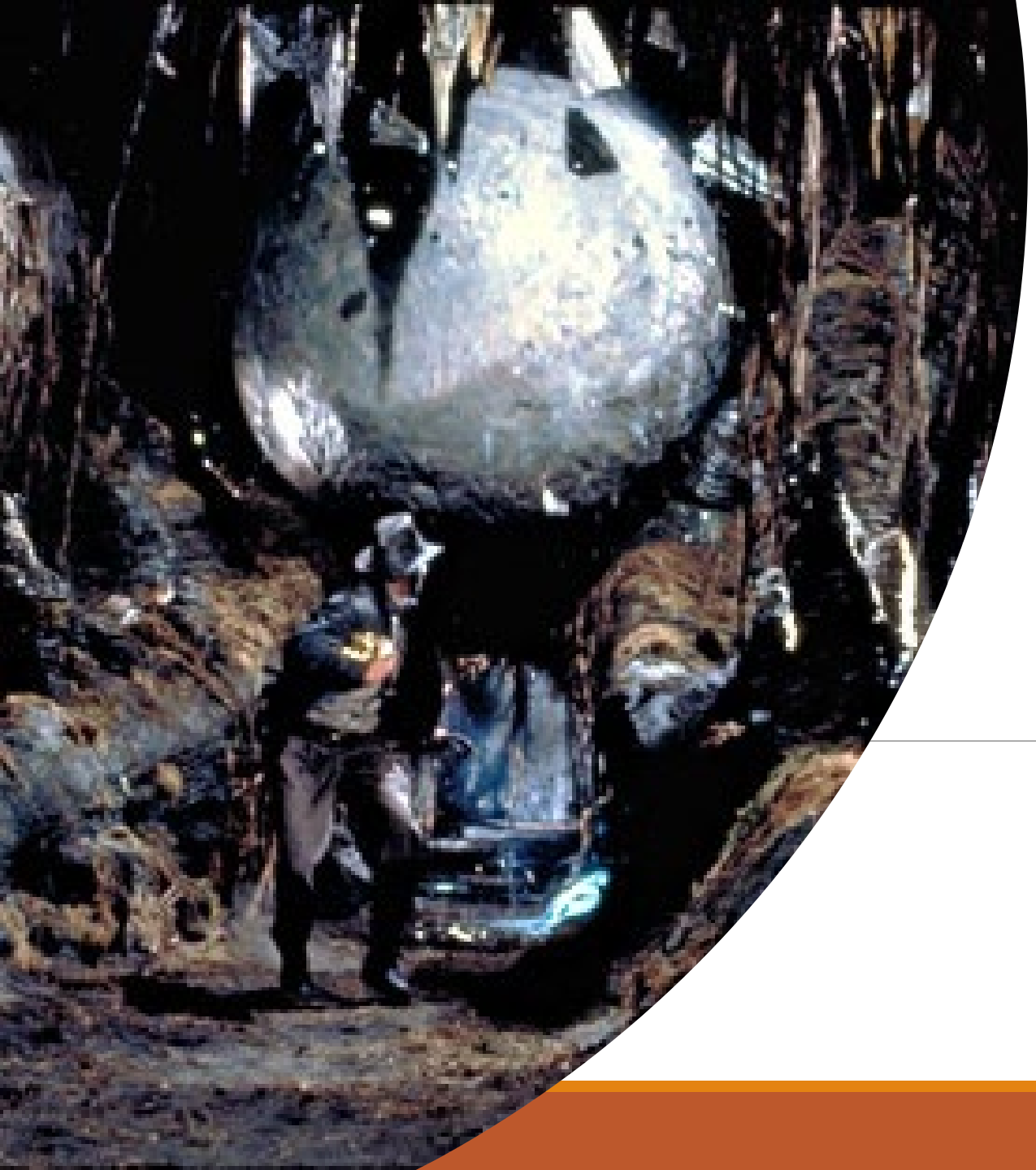


Cryptography in a Post-Quantum World

DUSTIN MOODY

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

Cryptography

Alice and Bob want to communicate
- Beware of Eve

Symmetric-key crypto
- Alice and Bob have a shared key
- Example: AES (encryption)

Public-key crypto
- Alice has never met Bob, but wants to send him a message
- Example: RSA (encryption and signatures)

NIST Crypto Standards

Areas:

- Block ciphers
- Hash functions
- Message authentication codes (MACs)
- Digital signatures
- Key-establishment
- Post-quantum crypto (signatures + key establishment)
- Random bit generation
- etc…

FIPS, SP's, and NISTIRs

NISTIR 7977 – NIST's process for developing crypto standards

Cooperation with other SDO's

Principles:

Transparency, openness, balance, integrity, technical merit, global acceptability, usability, continuous improvement, innovation and intellectual property

Stakeholders:

Primarily the US federal government, broader industry and public/private organizations

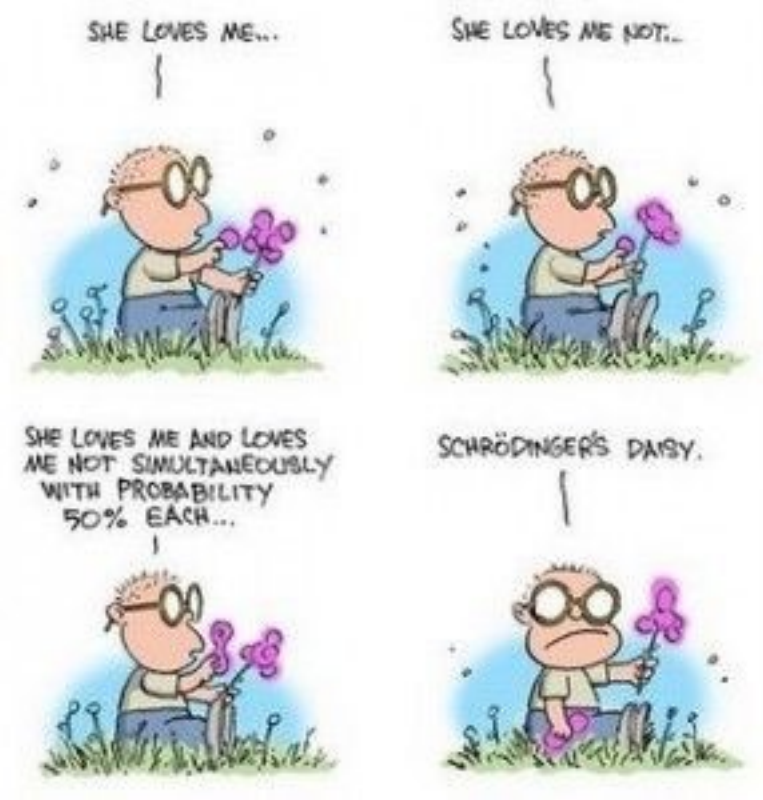
Classical vs Quantum Computers

The security of crypto relies on intractability of certain problems to modern computers

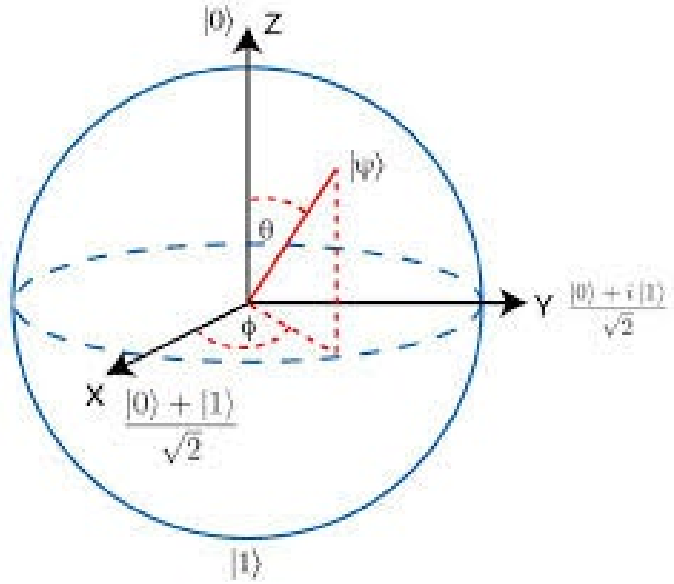
- Example: RSA and factoring

Quantum computers

- Exploit quantum mechanics to process information
- Use quantum bits = “qubits” instead of 0’s and 1’s
- Superposition – ability of quantum system to be in multiples states at the same time
- Entanglement – “spooky action at a distance”
- Potential to vastly increase computational power beyond classical computing limit



Qubits = “Quantum Bits”



Classical bits are either a 0 or a 1

A qubit can be represented by a vector $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex numbers with $\alpha^2 + \beta^2 = 1$.

Measuring $|\Psi\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis yields $\{|0\rangle$ with probability $|\alpha|^2$, and $\{|1\rangle$ with probability $|\beta|^2$

Two qubits:

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

again with complex α_{ij} with $\sum|\alpha_{ij}|^2 = 1$.

Quantum computation

Quantum computation = superposition + interference

Quantum Gates

X Gate
Bit–flip, Not

$$\boxed{X} \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Z Gate
Phase–flip

$$\boxed{Z} \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle$$

H Gate
Hadamard

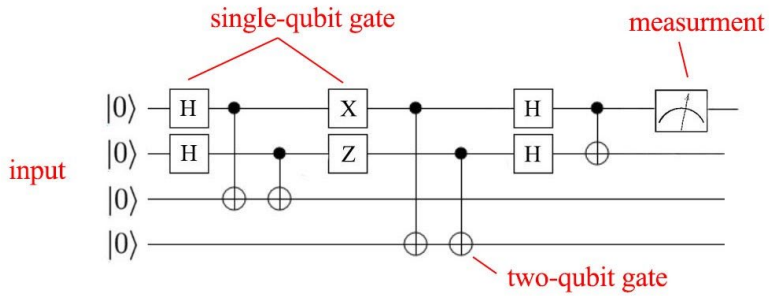
$$\boxed{H} \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{\alpha+\beta|0\rangle + \alpha-\beta|1\rangle}{\sqrt{2}}$$

T Gate

$$\boxed{T} \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$$

Run a circuit of elementary gates creating the right interference, so the final state has most of its weight on the solution to your problem

Measure the final state to get the solution



Quantum Computers

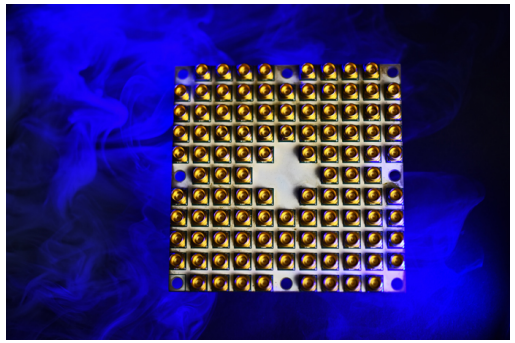
Exploit quantum mechanics to process information

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

IBM's 50-qubit quantum computer



Intel's 49-qubit chip "Tangle-Lake"

Google's 72-qubit chip "Bristlecone"

Google AI Blog

The latest news from Google AI

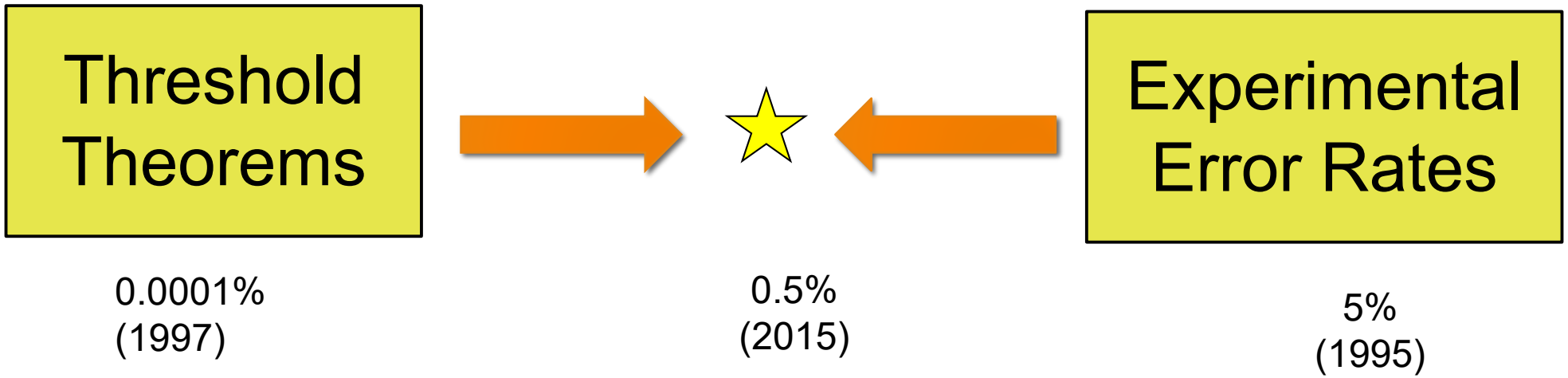
Quantum Supremacy Using a Programmable Superconducting Processor

Wednesday, October 23, 2019

Posted by John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum

Threshold Theorem

If error per quantum computation can be brought below (roughly) 0.5%, arbitrarily long quantum computations can be performed by correcting errors as you go

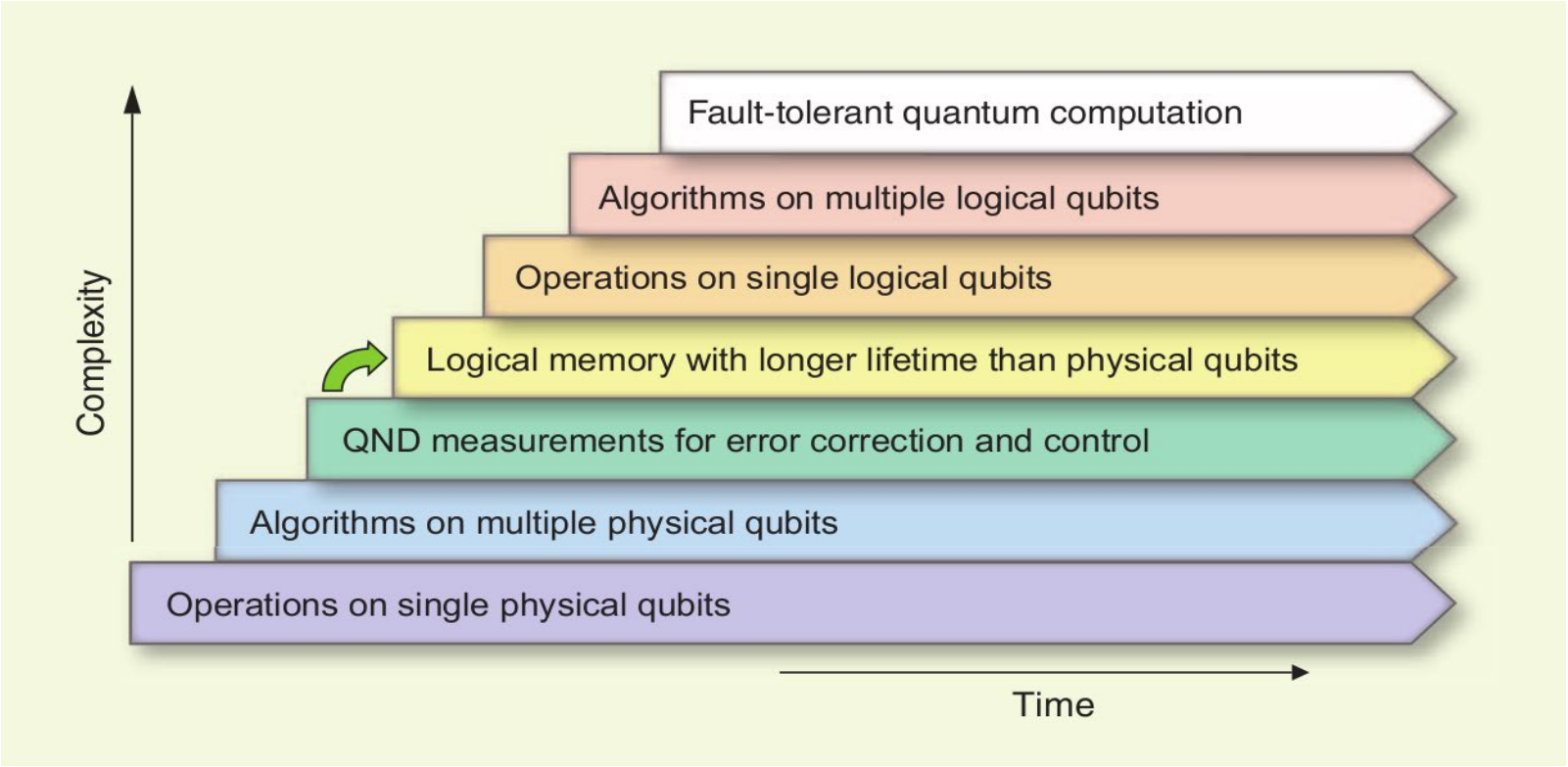


Theorists improve error correction schemes to tolerate higher error rates

Experimentalists achieve lower error rates

Quantum Computing Progress

A lot of progress, but still a long way to go



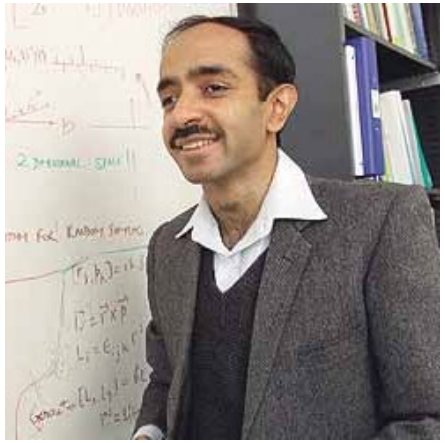
[Image credit: M. Devoret and R. Schoelkopf (Yale)]

Quantum Algorithms

1994, Peter Shor created a quantum algorithm that would give an exponential speed-up over classical computers

- Factoring large integers
- Finding discrete logarithms

Grover's algorithm – polynomial speed-up in unstructured search, from O(N) to O($\sqrt{N}$)



Simulating the dynamics of molecules, superconductors, photosynthesis, among many, many others

- see http://math.nist.gov/quantum/zoo

Quantum Cryptography

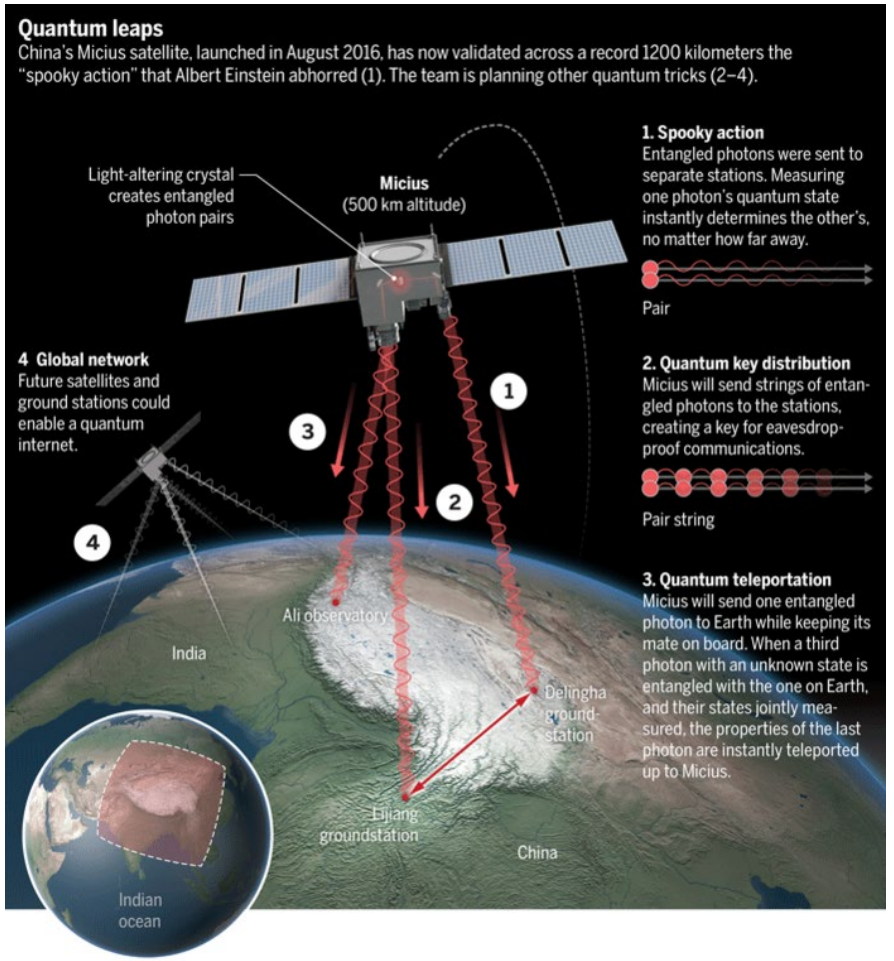
Using quantum technology to build cryptosystems

- Theoretically unconditional security guaranteed by the laws of physics

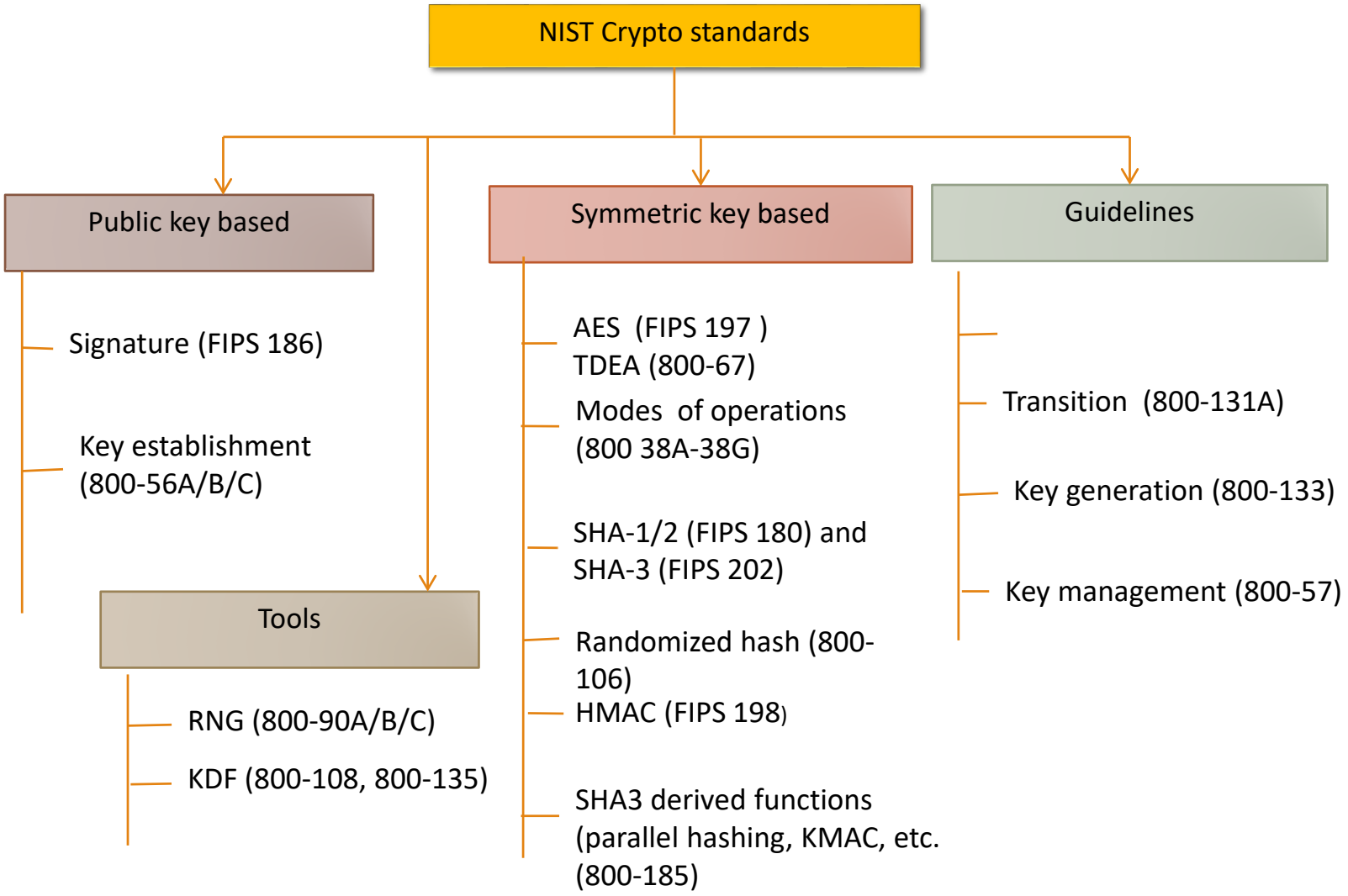
Limitations

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

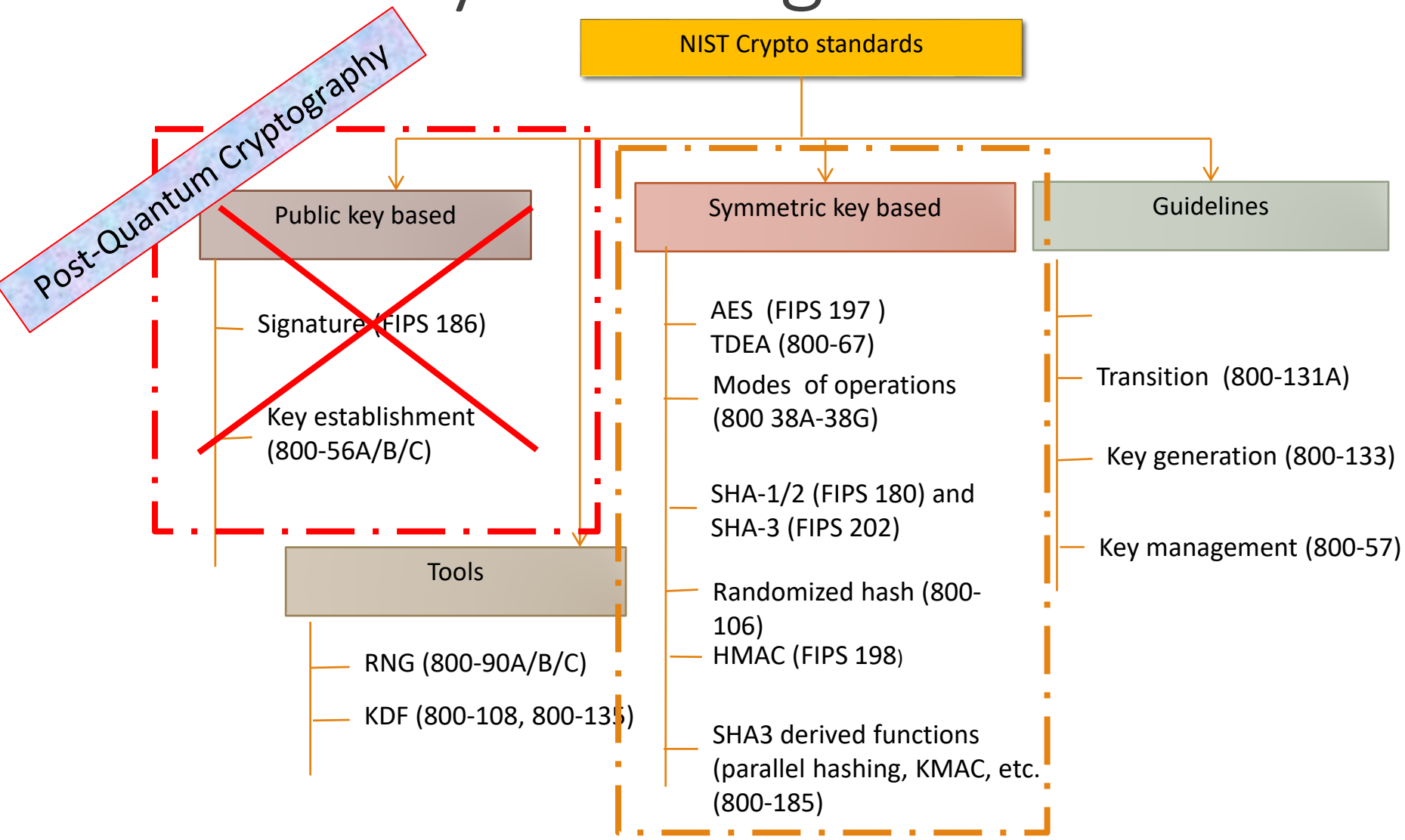
Lots of money being spent on “quantum”



The Sky is Falling?



The Sky is Falling?



When will a Quantum Computer be Built?

Quantum computers are 20 years in the future and always will be

“There is a 1 in 5 chance that some fundamental public-key crypto will be broken by quantum by 2029.”

– Dr. Michele Mosca, U. of Waterloo (2020)

See also: https://globalriskinstitute.org/publications/quantum-threat-timeline/

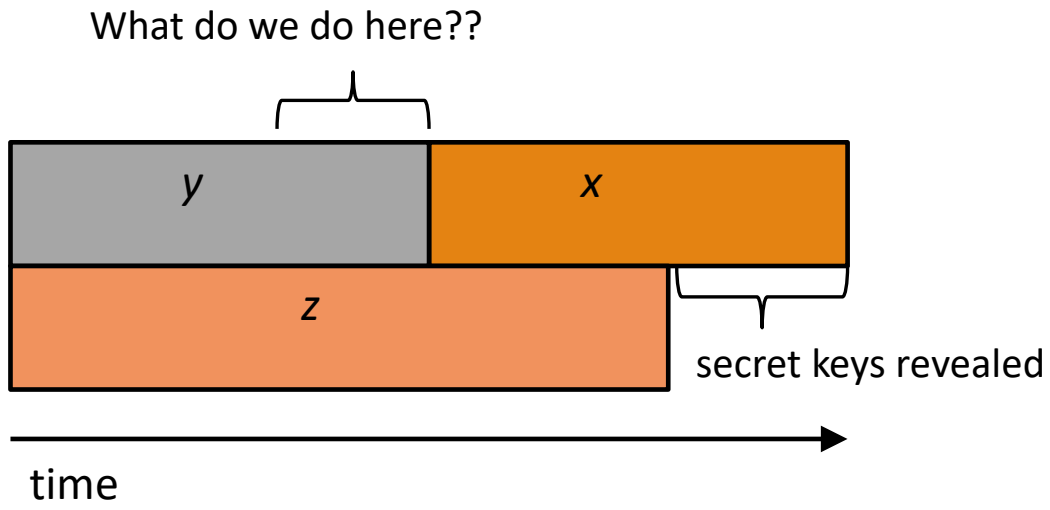
How soon do we need to worry?

How long does your information need to be secure (*x* years)

How long to re-tool existing infrastructure with quantum safe solution (*y* years)

How long until large-scale quantum computer is built (*z* years)

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



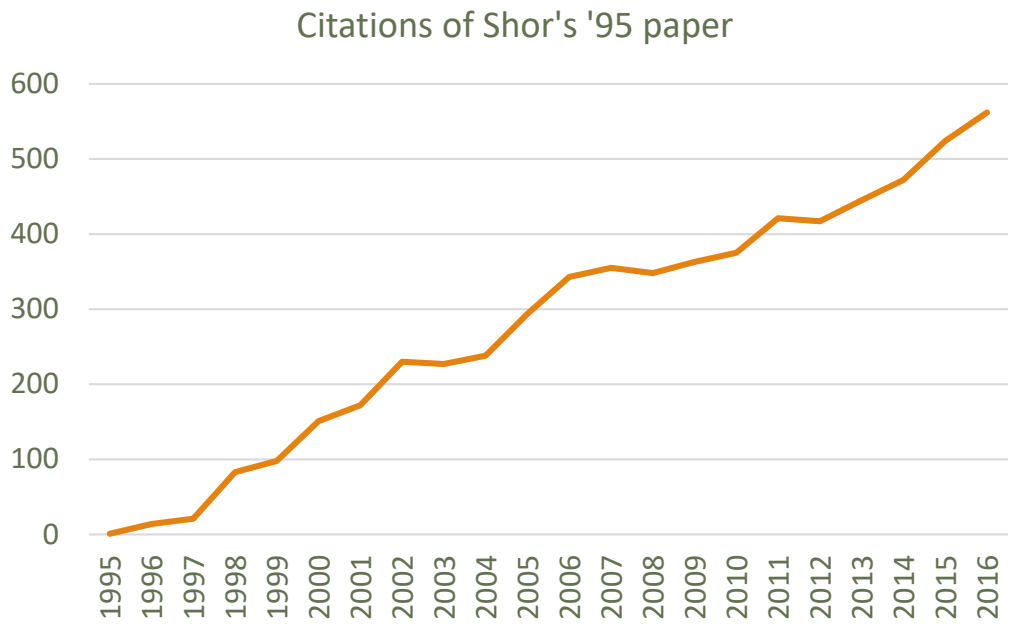
Post-Quantum Cryptography (PQC)

Cryptosystems which run on classical computers, and are considered to be resistant to quantum attacks

PQC needs time to be ready for applications

- Efficiency
- Confidence – cryptanalysis
- Standardization
- Usability and interoperability

  (IKE, TLS, etc… use public key crypto)



The NIST PQC Project

- 2009 – NIST publishes a PQC survey
  - Quantum Resistant Public Key Cryptography: A Survey
    [D. Cooper, R. Perlner]
- 2012 – NIST begins PQC project
  - Research and build team
  - Work with other standards organizations
    (ETSI, IETF, ISO/IEC SC 27)
- April 2015 – 1st NIST PQC Workshop

NSA Announcement

Aug 2015 - NSA's Information Assurance Directorate updated its list of Suite B cryptographic algorithms

- **"IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms."**

Feb 2016 - NIST published NISTIR 8105, *Report on Post-Quantum Cryptography*

Standardization is the first step towards the transition

The NIST PQC “Competition”

Announced: Feb 2016, along with NIST Report on PQC (NISTIR 8105)

Scope:

- Digital Signatures
  - Replace the signatures specified in FIPS 186-4 (RSA, DSA, ECDSA)
- Public-key Encryption / Key-Encapsulation Mechanisms (KEMs)
  - Replace the key-establishment algorithms specified in SP 800-56 A/B (DH, ECDH, MQV, RSA OAEP)

Open and transparent process

Unlike previous AES and SHA-3 competitions, there will not be a single “winner”

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

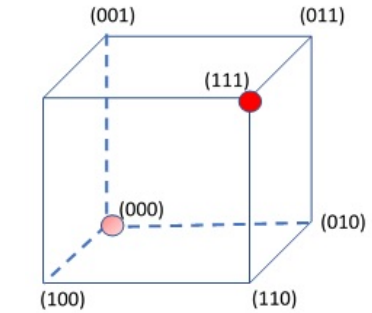
Other properties: Drop-in replacements, Perfect forward secrecy, Resistance to side-channel attacks, Simplicity and flexibility, Misuse resistance, etc.

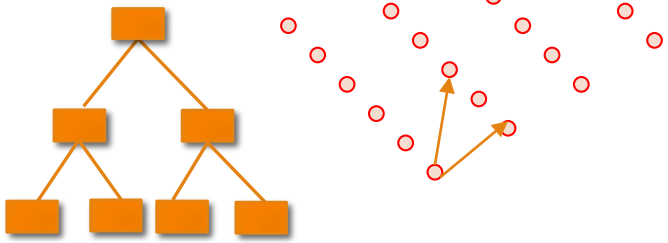
The 1st Round Candidates

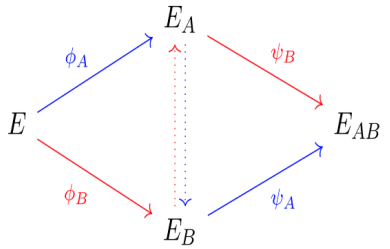
$$p^{(1)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} \cdot x_i + p_0^{(1)}$$
$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} \cdot x_i + p_0^{(2)}$$
$$\vdots$$
$$p^{(m)}(x_1,\ldots,x_n)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

- Nov 2017 - 82 submissions received.
- 69 accepted as "complete and proper" (5 withdrew)

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







BIG QUAKE
BIKE
CFPKM
Classic McEliece
Compact LWE
CRYSTALS-DILITHIUM
CRYSTALS-KYBER
DAGS
Ding Key Exchange
DME
DRS
DualModeMS
Edon-K
EMBLEM/R.EMBLEM
FALCON
FrodoKEM
GeMSS
Giophantus
Gravity-SPHINCS
Guess Again
Gui
HILA5
HiMQ-3
HK-17
HQC
KCL
KINDI
LAC
LAKE
LEDAkem
LEDApkc
Lepton
LIMA
Lizard
LOCKER
LOTUS
LUOV
McNie
Mersenne-756839
MQDSS
NewHope
NTRUEncrypt
NTRU-HRSS-KEM
NTRU Prime
NTS-KEM
Odd Manhattan
Ouroboros-R
Picnic
Post-quantum RSA Encryption
Post-quantum RSA Signature
pqNTRUSign
pqsigRM
QC-MDPC-KEM
qTESLA
RaCoSS
Rainbow
Ramstake
RankSign
RLCE-KEM
Round2
RQC
RVB
SABER
SIKE
SPHINCS+
SRTPI
Three Bears
Titanium
WalnutDSA

A Worldwide Effort

25 Countries

16 States

6 Continents

Overview of the 1st Round

Began Dec 2017 – 1st Round Candidates published

Resources:

- Internal and external cryptanalysis
  - 21 of the 69 schemes had been broken/attacked by April
- The 1st NIST PQC Standardization Workshop
- Research publications
- Performance benchmarks
  - NIST's internal numbers based on submitter's code
  - Preliminary benchmarks – SUPERCOP, OpenQuantumSafe
- Official comments
- The pqc-forum mailing list

Announced 2nd Round candidates – Jan 30, 2019

- NISTIR 8240 – Status Report on the 1st Round

A brief intermission

Dec 4 – pqc-forum post saying we are close to end of 1st round

Dec 13 – NIST decided to announce 2nd Round candidates at Real World Crypto Conference

Dec 22 – US government shutdown begins

- NIST employees cannot work in any way, shape or form

Jan 9-11 – Real World Crypto in San Jose, CA

- NIST did not attend and announce as planned

Jan 28 – NIST is back at work!

Jan 30 – 2nd Round Announcement

- 1st Round Report, NISTIR 8240 (https://doi.org/10.6028/NIST.IR.8240)

The 2nd Round Candidates

We wanted to keep algorithm diversity and promote research, but had to reduce the number of candidates to a manageable size for the community

- It is hard to make comparisons among candidates in different categories
- Sometimes even in the same category, it is not always possible to rank them

Some candidates were merged as NIST encouraged

	Signatures	KEM/Encryption	Overall
Lattice-based	3	9	12
Code-based		7	7
Multi-variate	4		4
Symmetric based	2		2
Isogeny		1	1
Total	**9**	**17**	**26**

The 2nd Round Candidates

Encryption/KEMs (17)

- BIKE
- Classic McEliece
- CRYSTALS-KYBER
- FrodoKEM
- HQC
- LAC
- LEDAcrypt (merger of LEDAkem/pkc)
- NewHope
- NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM)
- NTRU Prime
- NTS-KEM
- ROLLO (merger of LAKE/LOCKER/Ouroboros-R)
- Round5 (merger of Hila5/Round2)
- RQC
- SABER
- SIKE
- Three Bears

Digital Signatures (9)

- CRYSTALS-DILITHIUM
- FALCON
- GeMSS
- LUOV
- MQDSS
- Picnic
- qTESLA
- Rainbow
- SPHINCS+

Review of the 2nd Round Candidates

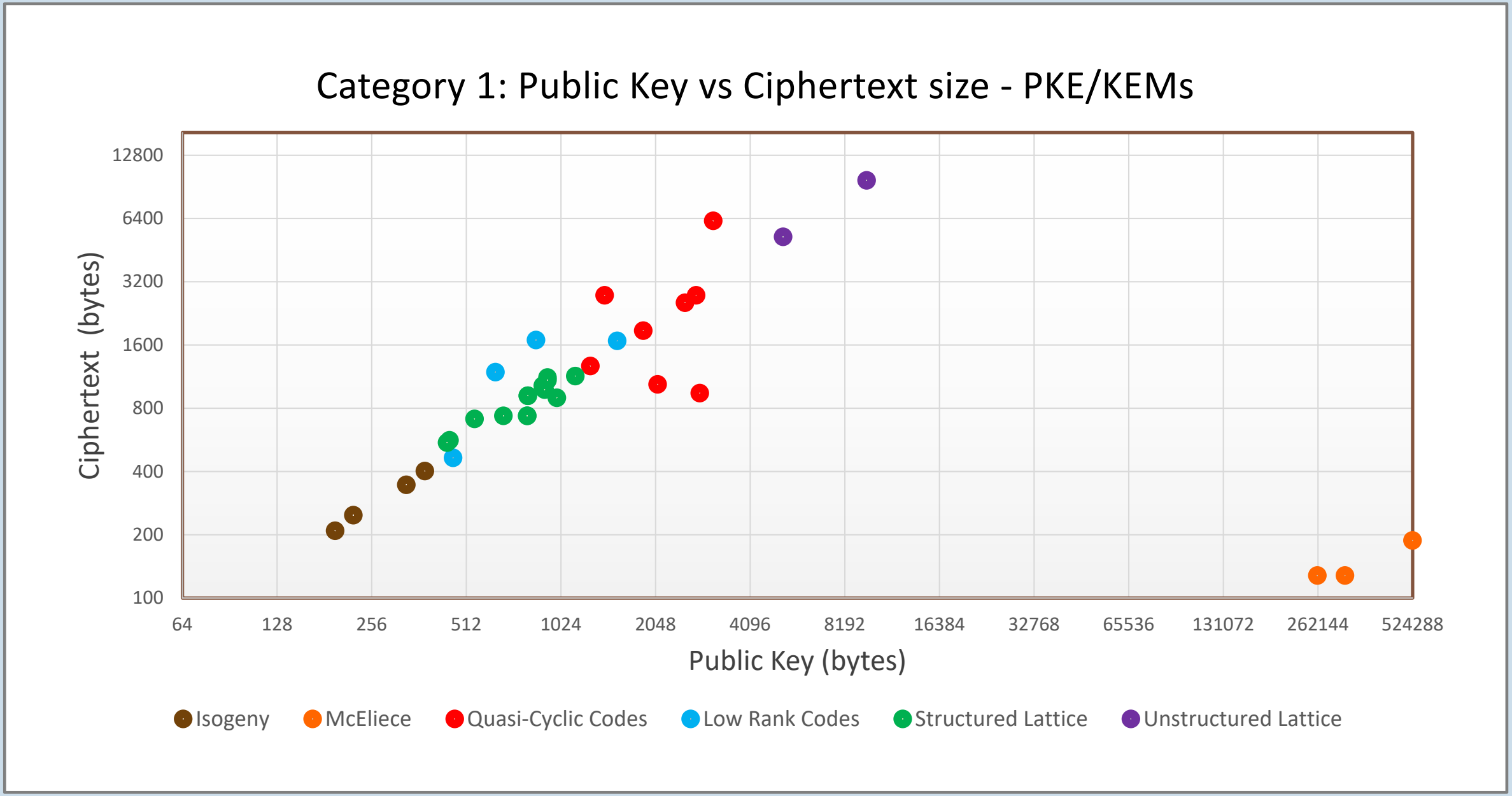
The 2nd Round candidates cover algorithms in the most researched categories of PQC

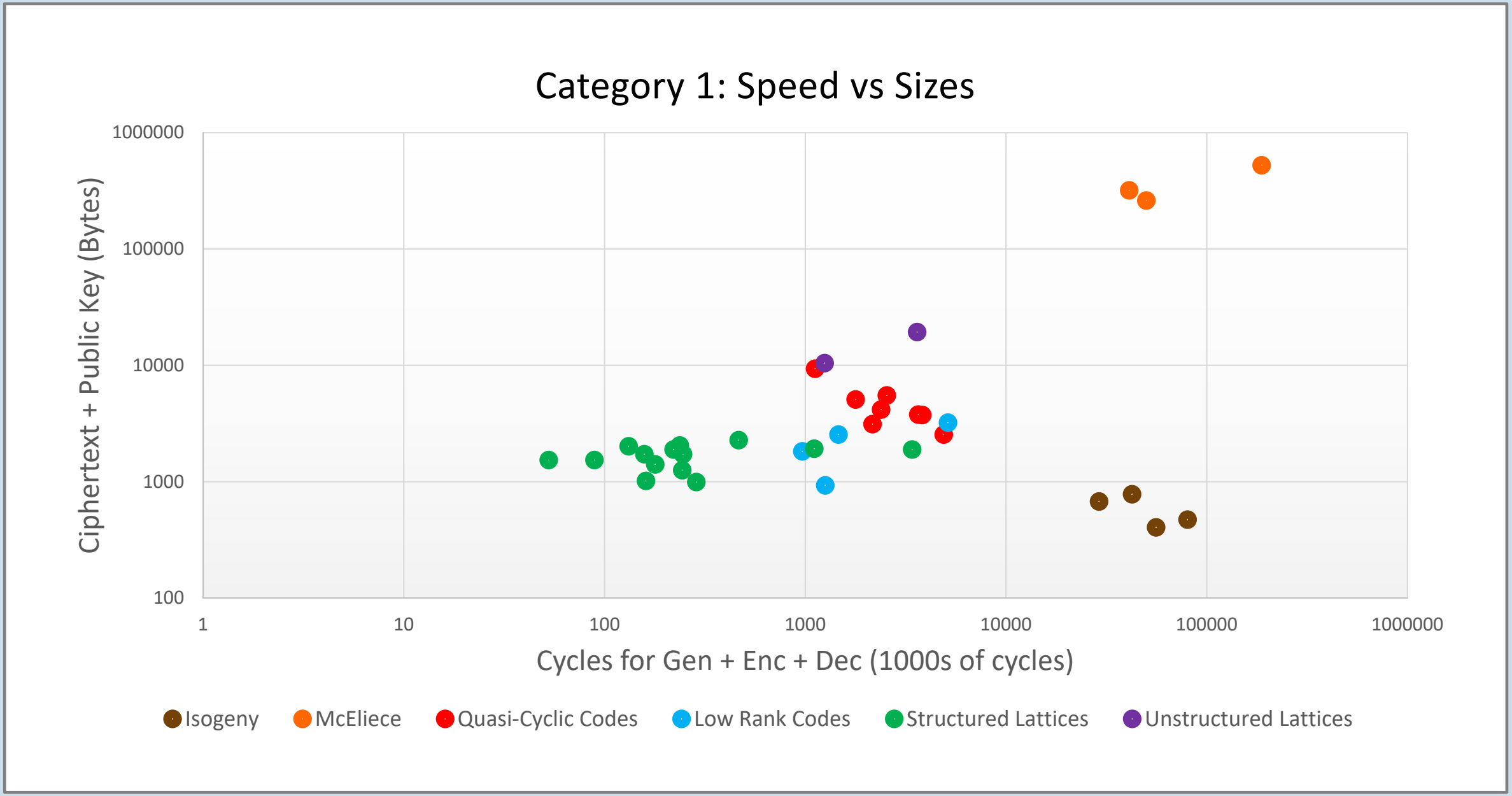
In the same category, candidates are designed with different ideas and mathematical structures, e.g.

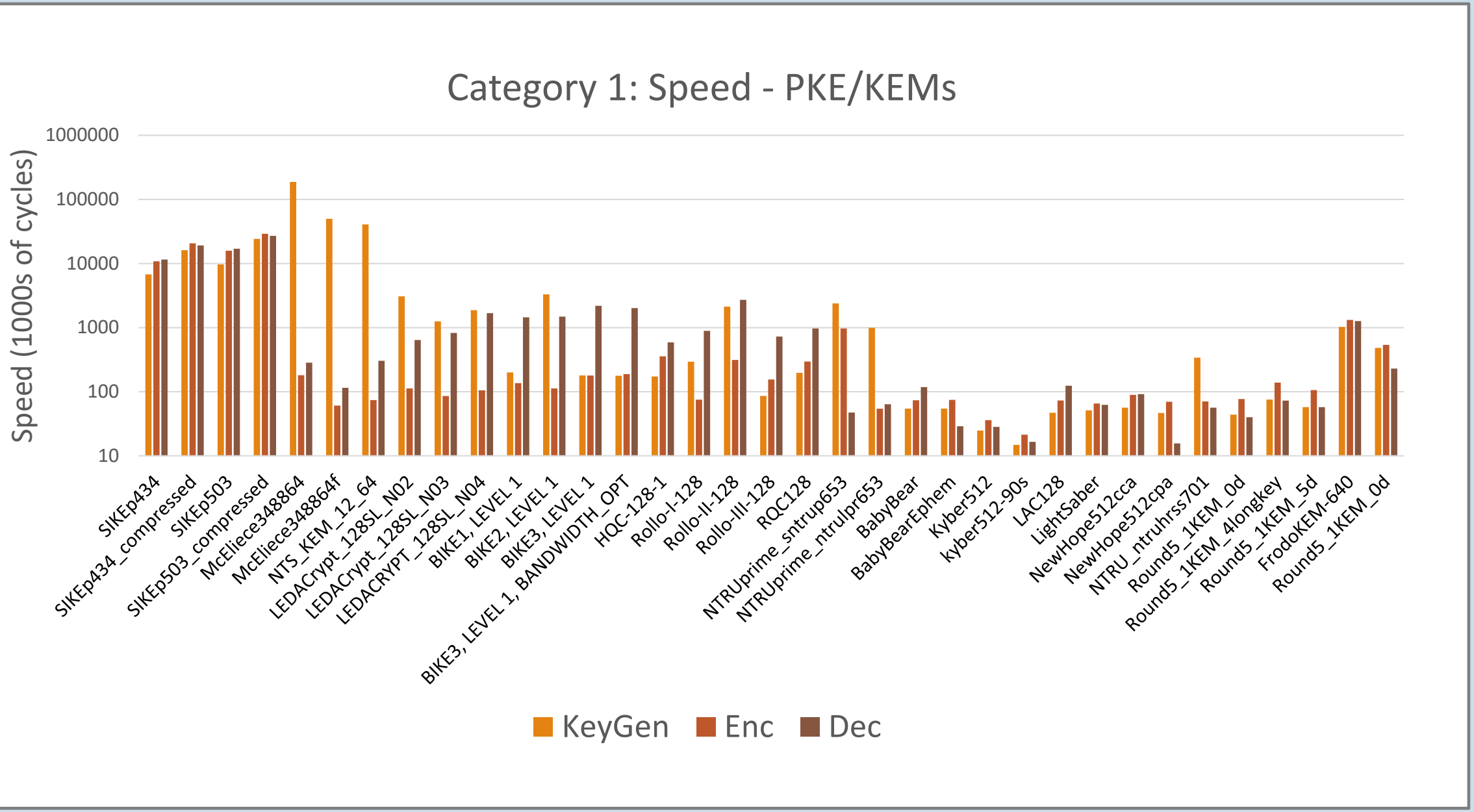
- Lattice-based includes unstructured LWE, RLWE, MLWE, NTRU using rounding, error correction, etc.
- Code-based includes schemes based on Hamming and rank metrics, and the original 1979 McEliece cryptosystem based on Goppa codes
- Multivariate signature schemes include the Hidden Field Equations (HFEv-) family and also the Unbalanced Oil Vinegar (UOV) family
- Signature schemes are either in hash-and-sign or in the Fiat-Shamir format
- There are also candidates based on novel designs with isogenies and symmetric-key primitives

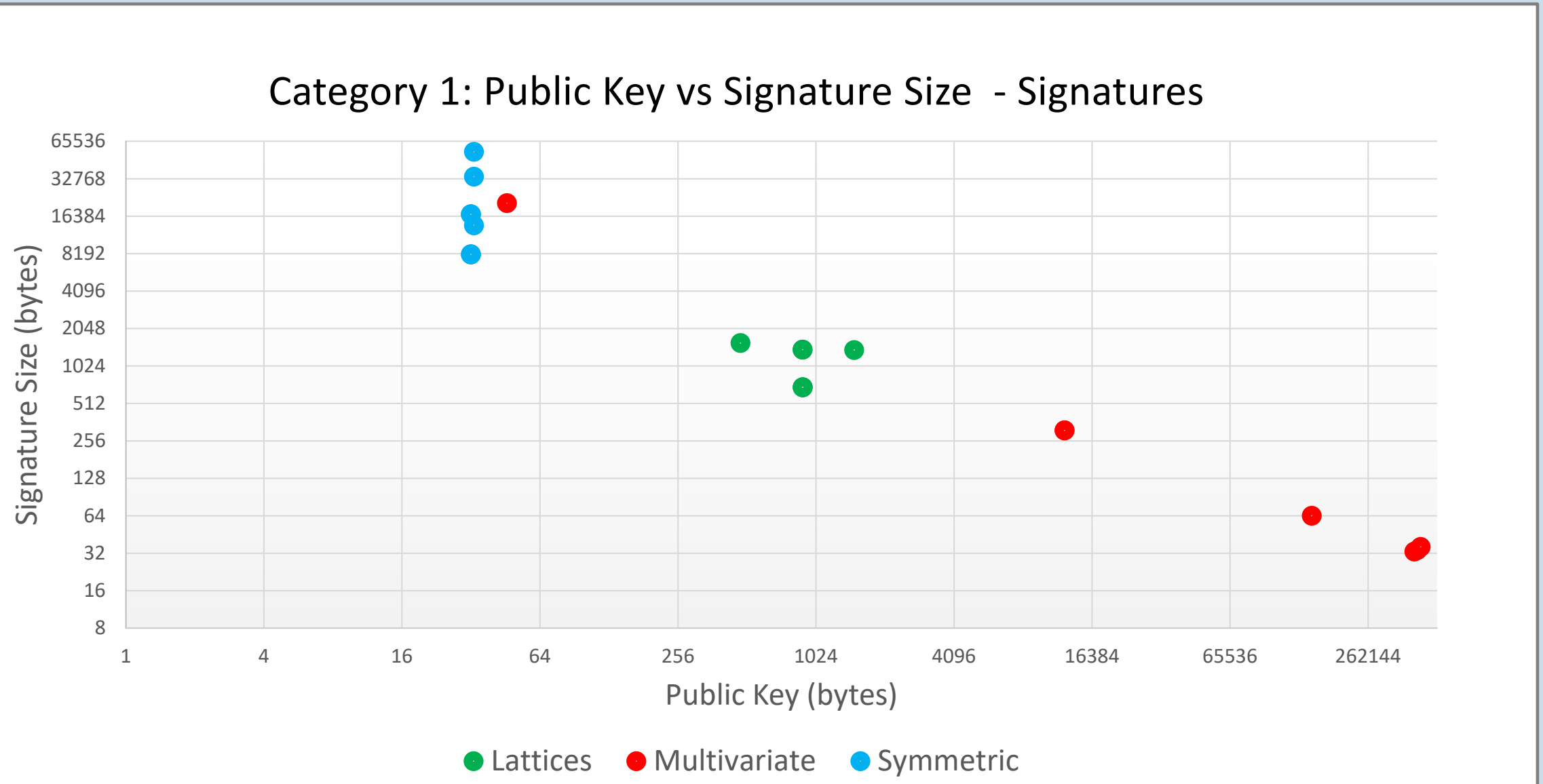
The 2nd round includes candidates with relatively conservative approaches as well as more aggressive/optimized designs

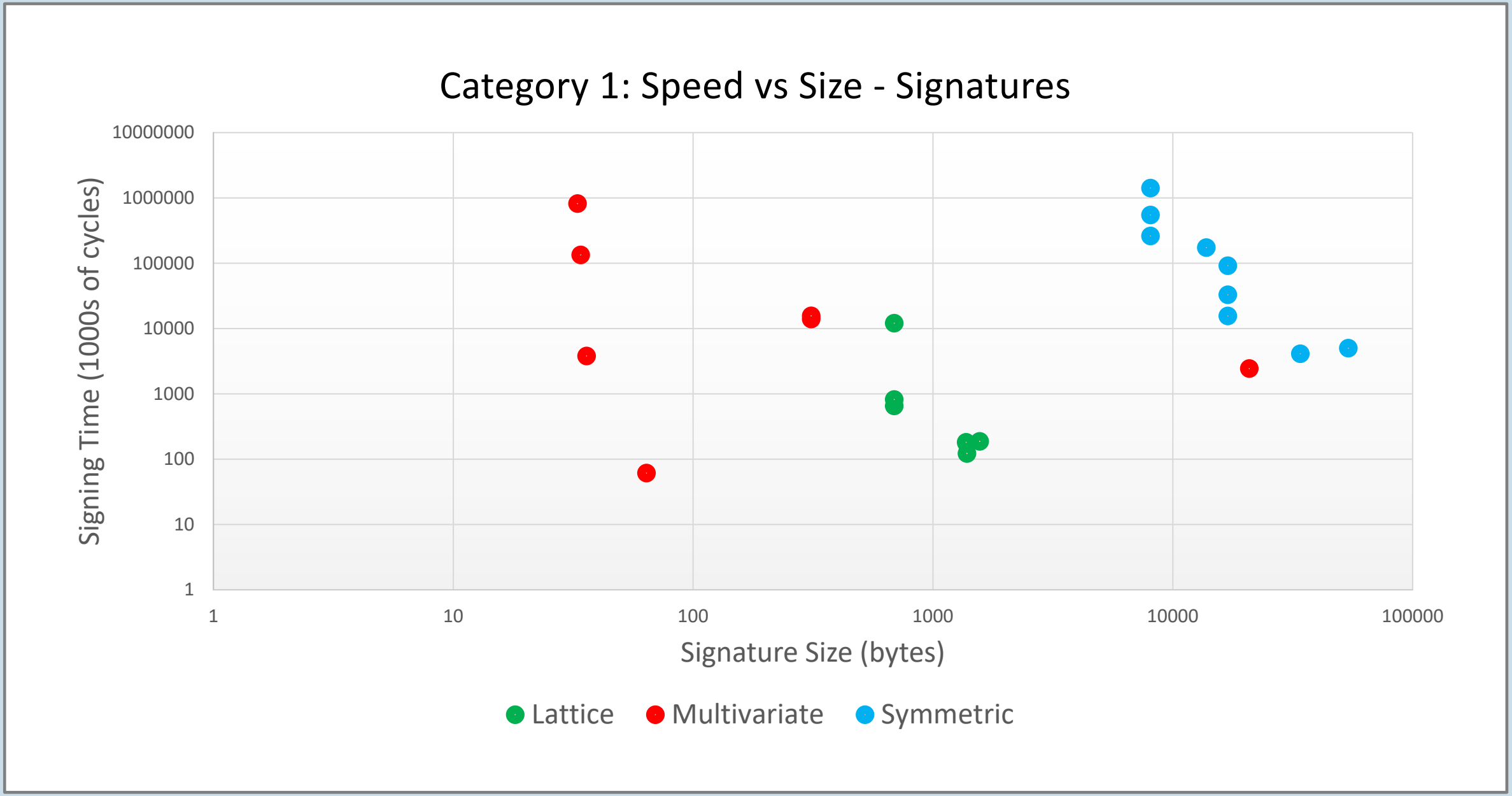
- LAC, LEDAcrypt, RQC, Rollo, MQDSS, qTESLA, LUOV have all been broken

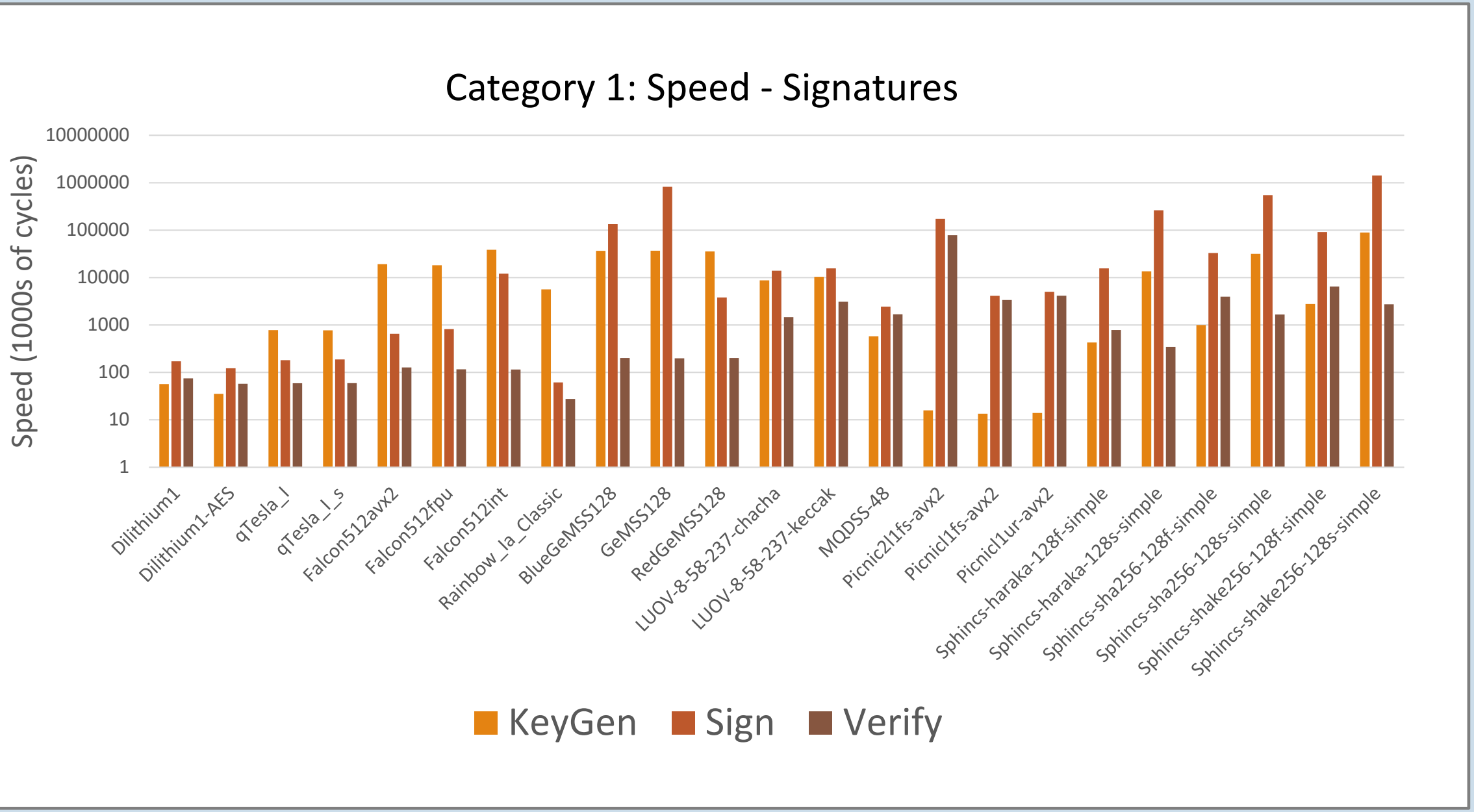

Category 1: Public Key vs Ciphertext size - PKE/KEMs
Ciphertext (bytes)
12800
6400
3200
1600
800
400
200
100
64
128
256
512
1024
2048
4096
8192
16384
32768
65536
131072
262144
524288
Public Key (bytes)
Isogeny
McEliece
Quasi-Cyclic Codes
Low Rank Codes
Structured Lattice
Unstructured Lattice


Category 1: Speed vs Sizes
Ciphertext + Public Key (Bytes)
1000000
100000
10000
1000
100
1
10
100
1000
10000
100000
1000000
Cycles for Gen + Enc + Dec (1000s of cycles)
Isogeny
McEliece
Quasi-Cyclic Codes
Low Rank Codes
Structured Lattices
Unstructured Lattices


Category 1: Speed - PKE/KEMs
Speed (1000s of cycles)
1000000
100000
10000
1000
100
10
SIKEp434
SIKEp434_compressed
SIKEp503
SIKEp503_compressed
McEliece348864
McEliece348864f
NTS_KEM_12_64
LEDACrypt_128SL_N02
LEDACrypt_128SL_N03
LEDACRYPT_128SL_N04
BIKE1, LEVEL 1
BIKE2, LEVEL 1
BIKE3, LEVEL 1
BIKE3, LEVEL 1, BANDWIDTH_OPT
HQC-128-1
Rollo-I-128
Rollo-II-128
Rollo-III-128
RQC128
NTRUprime_sntrup653
NTRUprime_ntrulpr653
BabyBear
BabyBearEphem
Kyber512
kyber512-90s
LAC128
LightSaber
NewHope512cca
NewHope512cpa
NTRU_ntruhrss701
Round5_1KEM_0d
Round5_1KEM_4longkey
Round5_1KEM_5d
FrodoKEM-640
Round5_1KEM_0d
KeyGen
Enc
Dec


Category 1: Public Key vs Signature Size - Signatures
Signature Size (bytes)
65536
32768
16384
8192
4096
2048
1024
512
256
128
64
32
16
8
1
4
16
64
256
1024
4096
16384
65536
262144
Public Key (bytes)
Lattices
Multivariate
Symmetric


Category 1: Speed vs Size - Signatures
Signing Time (1000s of cycles)
10000000
1000000
100000
10000
1000
100
10
1
1
10
100
1000
10000
100000
Signature Size (bytes)
Lattice
Multivariate
Symmetric


Category 1: Speed - Signatures
Speed (1000s of cycles)
10000000
1000000
100000
10000
1000
100
10
1
Dilithium1
Dilithium1-AES
qTesla_I
qTesla_I_s
Falcon512avx2
Falcon512fpu
Falcon512int
Rainbow_Ia_Classic
BlueGeMSS128
GeMSS128
RedGeMSS128
LUOV-8-58-237-chacha
LUOV-8-58-237-keccak
MQDSS-48
Picnic2l1fs-avx2
Picnicl1fs-avx2
Picnicl1ur-avx2
Sphincs-haraka-128f-simple
Sphincs-haraka-128s-simple
Sphincs-sha256-128f-simple
Sphincs-sha256-128s-simple
Sphincs-shake256-128f-simple
Sphincs-shake256-128s-simple
KeyGen
Sign
Verify

Next Steps - Security

Security proofs – whether the proof is correct

- Security reduction under random oracle model (ROM) and quantum random oracle model (QROM) for IND-CPA or IND-CCA2

Security strength estimation – whether the estimation is precise

- Classical security strength is sometimes estimated, e.g. in lattice based schemes, by a combination of theory and heuristics – closer investigations may be needed for more precise estimations
- Quantum security strength is estimated by
  - Quantum algorithms on a specific problem
  - Grover's algorithm to speed up search

Practical security

- Security against side-channel attacks
- Security to deal with decryption failure, incorrect error distribution, improper implementation of auxiliary functions/transitions, etc.

Next Steps - Performance

Benchmarks on different platforms and implementation environments

- For hardware, NIST asks to focus on Cortex M4 (with all options) and Artix-7
  - Researchers also explored Cortex-A53 and UltraScale+ for high performance
  - Identify different speed up technologies and also essential barriers in enabling hardware speed up for specific algorithms
- Performance in software only or limited available hardware environment
- RAM + Flash required for the implementation in constrained environments

Performance in protocols and applications

- Signature verification in secure boot, software update, application authorizations
- Impact of key size on latency for real time protocols like TLS and IKE

Power consumption and other costs

- Get more precise estimation
- Need constant time implementations

Next Steps - Transition

Enable crypto-agility for public key encryption/key encapsulation, signatures

- Allow introduction of new algorithms in existing applications and removal of algorithms vulnerable to attacks, classical and/or quantum
- Assess implementation costs and required bandwidth/space
- Adapt protocols and applications to accommodate new algorithms

Understand tradeoff preferences in each application

- Identify restrictions, limitations, and show stoppers

Gain first-hand experience through trial implementations

- Eliminate security pitfalls and explore implementation optimizations
- Amazon, Cisco, Google, Cloudflare, and others have done experiments with PQC algorithms in real-world protocols

Introduce hybrid mode and/or dual signatures in current protocols and applications

- Prevent crashing from a single security failure

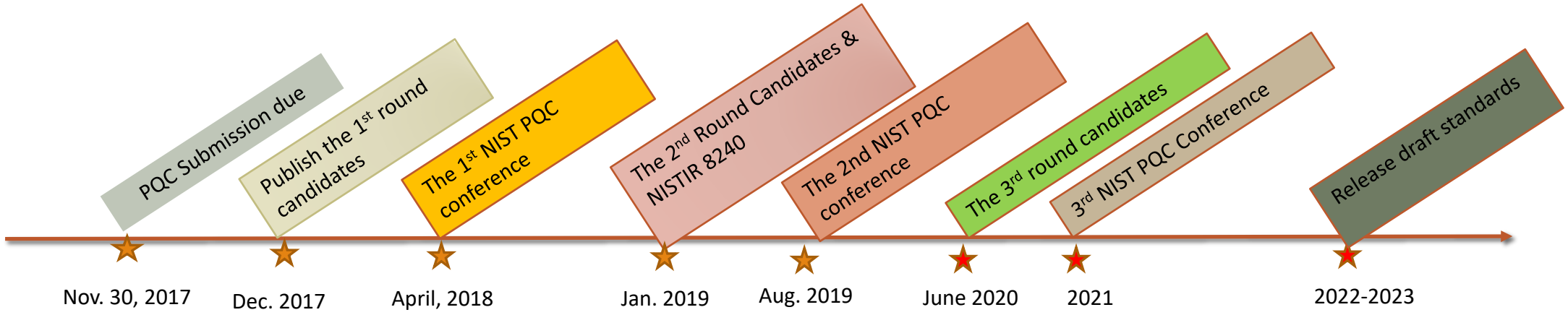
Timeline

Round 2 began on January 30, 2019

We'll announce the 3rd round candidates in a month (or two)

Hold the 3rd NIST PQC Standardization Conference in the first half of 2021

Release draft standards in 2022-2023 for public comments



Stateful Hash-based signatures

NIST plans to approve stateful hash-based signatures

- 1) XMSS, specified in RFC 8931
- 2) LMS, specified in RFC 8554
  - Will include their multi-tree variants, XMSS^MT and HSS

Will recommend HBS schemes limited to scenarios in which a digital signature scheme needs to be deployed soon, but where risks of accidental one-time key reuse can be minimized

NIST issued draft SP 800-208 for public feedback. Comments due by Feb 28, 2020

What can your organization 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

What NIST wants

Performance (hardware+software) will play more of a role

- More benchmarks
- For hardware, NIST asks to focus on Cortex M4 (with all options) and Artix-7
  - pqc-hardware-forum
- How do schemes perform on constrained devices?
- Side-channel analysis (concrete attacks, protection, etc…)

Continued research and analysis on **ALL** of the candidates

See how submissions fit into applications/procotols. Any constraints?

Other NIST projects

Lightweight cryptography “competition”

- 56 submissions (for AEAD + optional hash function)
- Workshop on Nov 4-6, 2019

Threshold Cryptography

- Workshop on March 11-12, 2019

FIPS 186-5 (Digital Signature Standard)

- Expected very, very soon
- New elliptic curves, signature algorithms to be added

Summary

Quantum computers have HUGE potential

Post-quantum crypto standardization will be a long journey

Check out www.nist.gov/pqcrypto

- Sign up for the pqc-forum for announcements & discussion
- send e-mail to pqc-comments@nist.gov