Round 2 of the NIST PQC “Competition”

What was NIST thinking?

Dustin Moody

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

NIST Crypto Standards

- Areas:
  - Block ciphers, hash functions, message authentication codes (MACs), digital signatures, key-establishment, post-quantum (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

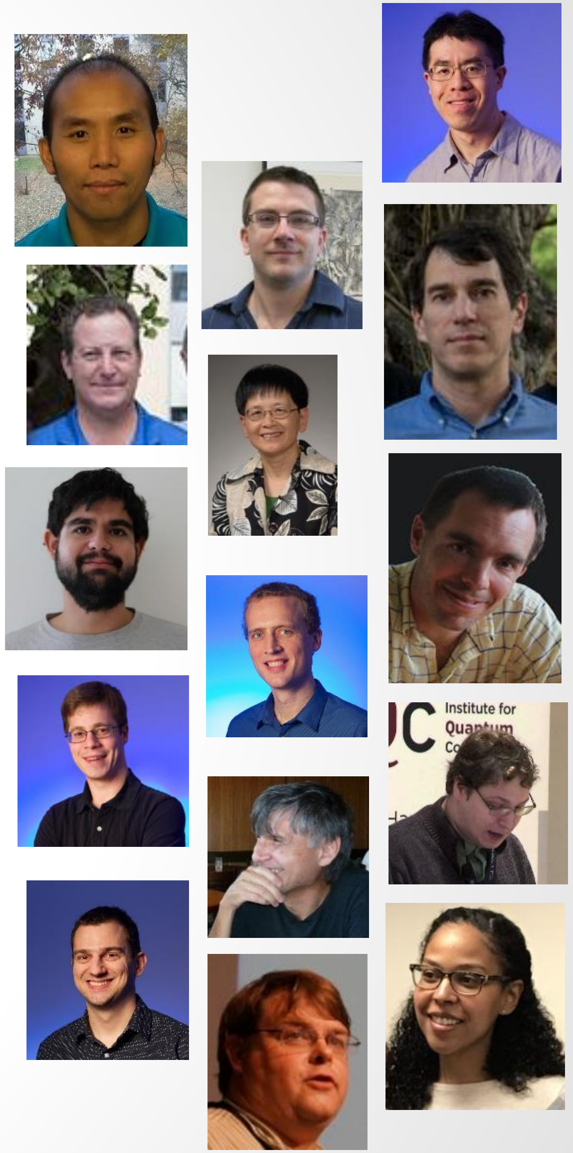
NIST Competitions*

- Block Cipher
  - AES – 15 candidates, 2 rounds, 5 finalists, 3 years + 1 year for standard
- Hash Function
  - SHA-3 – 64 submissions, 51 accepted, 3 rounds, 14 2nd round candidates, 5 finalists, 5 years + 3 years for standard

- *Post-Quantum Cryptography*
  - No Name? – 82 submissions, 69 accepted, 2 (or 3) rounds, 26 2nd round candidates, 2017-2020ish + 2? Years for standard
- Lightweight Crypto
  - 57 submissions, 2019-2022ish

The NIST PQC Project

- 2009 – NIST publishes a PQC survey
  - Quantum Resistant Public Key Cryptography: A Survey [R. Perlner, D. Cooper]
- 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



A competition by any other name

- Feb 2016 – NIST Report on PQC (NISTIR 8105)
- Feb 2016 – NIST announcement at PQCrypto in Japan
- Dec 2016 – Final requirements and evaluation criteria published
- Nov 2017 – Deadline for submissions

- Scope:
  - Digital Signatures (FIPS 186)
  - Public-key encryption/KEMs (SP 800-56A and SP 800-56B)

- Expected outcome: a few different algorithms

Targeted Functionalities/ Security Definitions

- Digital Signature
  - EUF-CMA up to 2^{64} signature queries
- PKE/KEM (first option)
  - IND-CCA up to 2^{64} decryption/decapsulation queries
  - Necessary in situations requiring key reuse
- PKE/KEM (second option)
  - IND-CPA
  - Needs usage restrictions to prevent key reuse
  - May be worth standardizing in addition to IND-CCA schemes if it comes with significant performance benefits

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

- 82 submissions received.
- 69 accepted as “complete and proper” (5 withdrew)

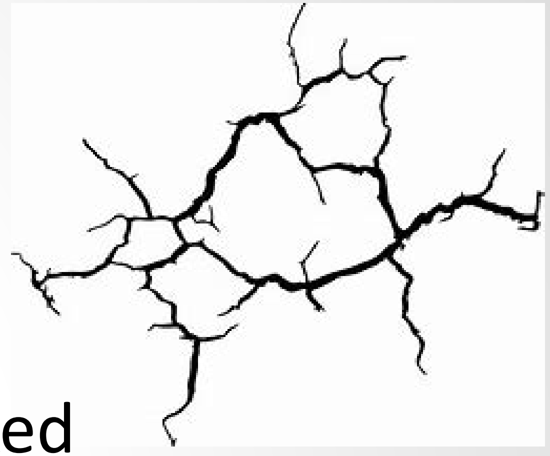
	Signatures	KEM/Encryption	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multi-variate	7	2	9
Symmetric-based	3		3
Other	2	5	7
Total	**19**	**45**	**64**

- 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

Overview of the 1st Round

- Began Dec 2017 – 1st Round Candidates published
- Resources:
  - Internal and external cryptanalysis
  - The 1st NIST PQC Standardization Workshop
  - Research publications
  - Performance benchmarks
  - Official comments
  - The pqc-forum mailing list
- Ended Jan 30, 2019 – 2nd Round Candidates Announced

Breaks and attacks



- Dec 21 – Submissions publicly posted
- 3 weeks later – 12 schemes broken or significantly attacked
- 5 withdrawals
  - Edon-K, HK17, RankSign, RVB, SRTPI
- April 2018 – 4 more schemes broken/attacked

- NIST lacked full confidence in security of:
  - CFPKM, Compact-LWE, DAGS, DME, DRS, GuessAgain, Giophantus, Lepton, McNie, pqsigRM, RaCoSS, RLCE, Walnut-DSA

Performance considerations

- “*Performance considerations will NOT play a major role in the early portion of the evaluation process*.”

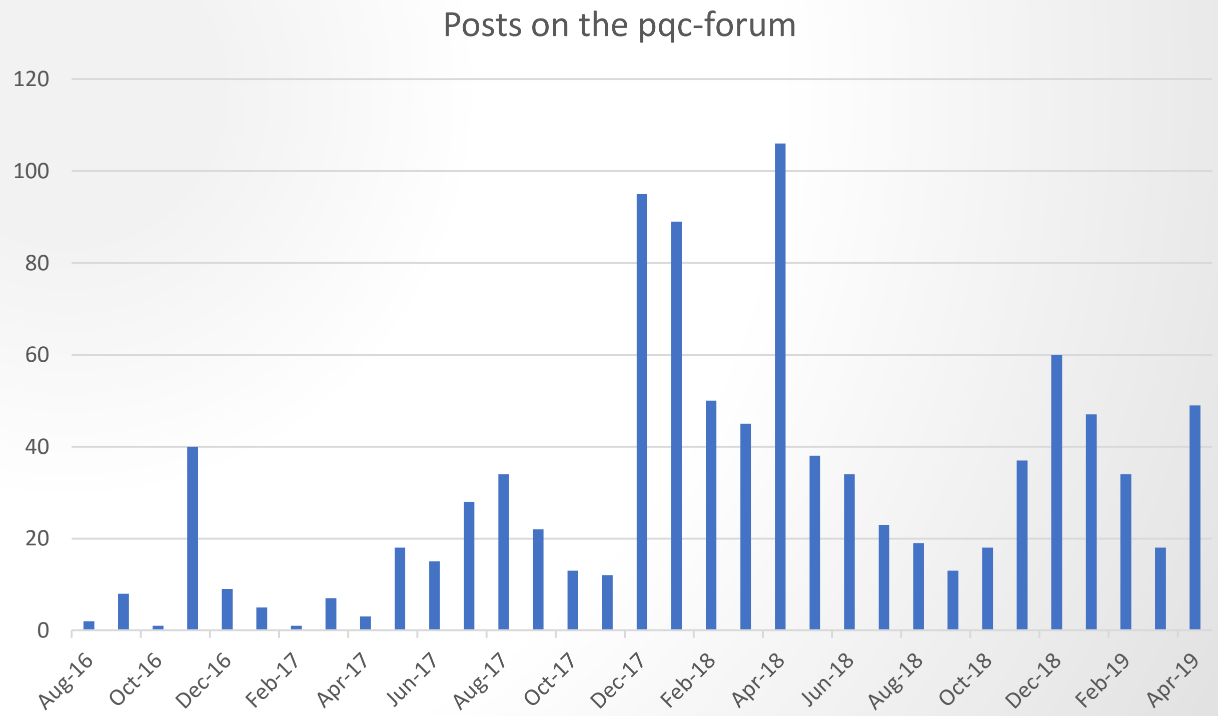
- PQRSA and DualModeMS were too inefficient

- Evaluation resources
  - NIST’s internal numbers
  - Preliminary benchmarks – SUPERCOP, OpenQuantumSafe, etc…
  - We hope to get more benchmarks for Round 2

The PQC-forum

- Sign up at www.nist.gov/pqcrypto
- Official channel for announcements and discussion of NIST PQC

- 1300 members
- 1002 posts



Official Comments

- Can be submitted on pqc-forum or our website
- Way to keep track of comments on particular submission

- Round 1 - Over 300 official comments
  - 60% of comments on about 10 submissions
  - About half of submissions had 2 or fewer comments

- Round 2 – official comments “start over”
  - So far, 7 submissions have a total of 48 comments

The 1st NIST PQC Standardization Conference

- April 11-13, 2018 in Ft. Lauderdale, Florida co-located with PQCrypto 2018

- There were 52 presentations, covering 60 algorithms, with 345 attendees
  - Most presentations were only 15 minutes
  - Slides available at https://csrc.nist.gov/events/2018/first-pqc-standardization-conference

Intellectual Property

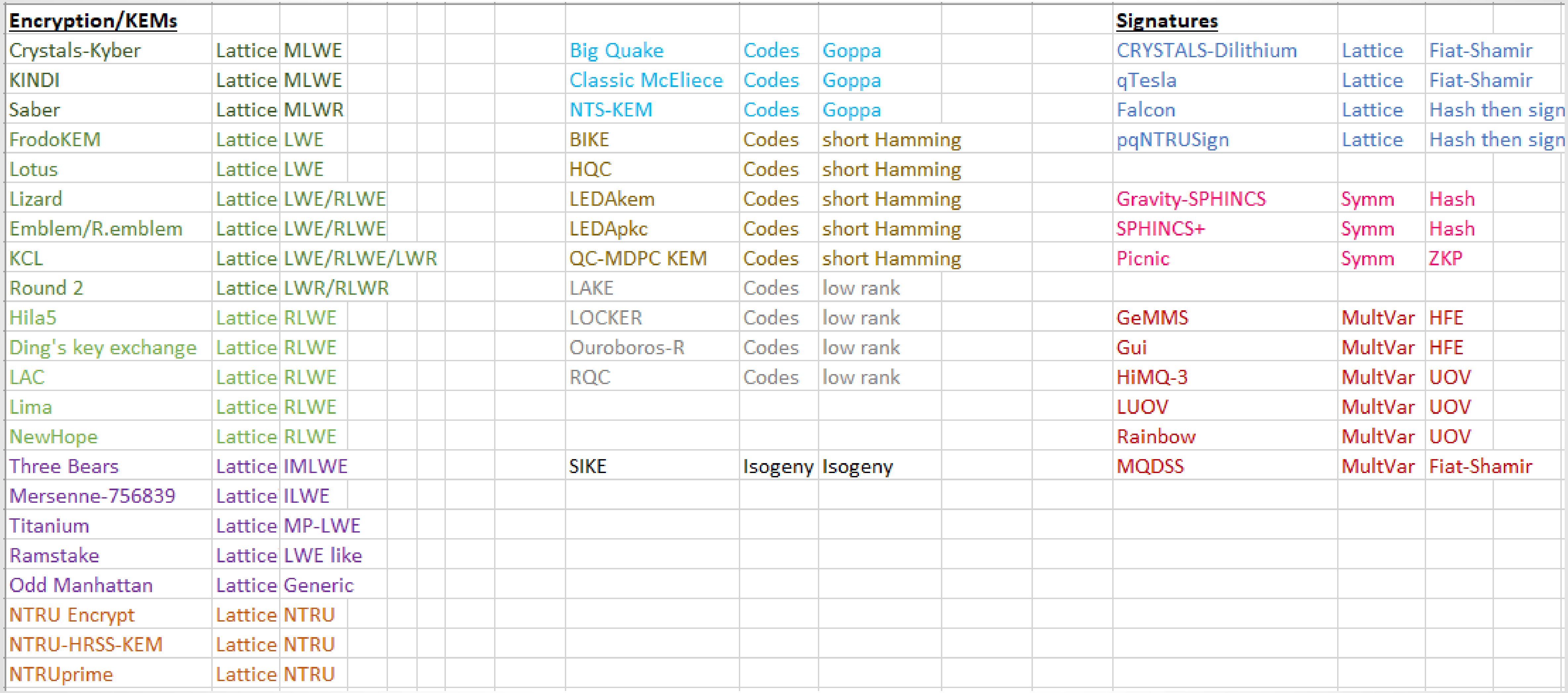
- Signed statements required from submitters (posted on our webpage)
- From the CFP:

  "NIST does not object in principle to algorithms or implementations which may require the use of a patent claim, where technical reasons justify this approach, but will consider any factors which could hinder adoption in the evaluation process."
- For Round 1 – schemes evaluated on their technical merits
  - Later on in process, IP concerns may play a larger role
- For Round 2 – only need new IP statements if new team members, or if IP status has changed.

NIST’s Process

- Dec 2017 – Check submissions for completeness
- Jan to Sep 2018 – Detailed internal presentations on submissions
- Apr 2018 – 1st Workshop – submitter’s presentations
- Sep to Nov 2018 – Review and make preliminary decisions
  - Compare similar type schemes to each other
- Dec 2018 – Final decision and start report (NISTIR 8240)
  - Very hard decisions
  - Report focused on candidates that advanced on

Apples and Oranges



Encryption/KEMs						Signatures		
Crystals-Kyber	Lattice	MLWE	Big Quake	Codes	Goppa	CRYSTALS-Dilithium	Lattice	Fiat-Shamir
KINDI	Lattice	MLWE	Classic McEliece	Codes	Goppa	qTesla	Lattice	Fiat-Shamir
Saber	Lattice	MLWR	NTS-KEM	Codes	Goppa	Falcon	Lattice	Hash then sign
FrodoKEM	Lattice	LWE	BIKE	Codes	short Hamming	pqNTRUSign	Lattice	Hash then sign
Lotus	Lattice	LWE	HQC	Codes	short Hamming			
Lizard	Lattice	LWE/RLWE	LEDAkem	Codes	short Hamming	Gravity-SPHINCS	Symm	Hash
Emblem/R.emblem	Lattice	LWE/RLWE	LEDApkc	Codes	short Hamming	SPHINCS+	Symm	Hash
KCL	Lattice	LWE/RLWE/LWR	QC-MDPC KEM	Codes	short Hamming	Picnic	Symm	ZKP
Round 2	Lattice	LWR/RLWR	LAKE	Codes	low rank			
Hila5	Lattice	RLWE	LOCKER	Codes	low rank	GeMMS	MultVar	HFE
Ding's key exchange	Lattice	RLWE	Ouroboros-R	Codes	low rank	Gui	MultVar	HFE
LAC	Lattice	RLWE	RQC	Codes	low rank	HiMQ-3	MultVar	UOV
Lima	Lattice	RLWE				LUOV	MultVar	UOV
NewHope	Lattice	RLWE				Rainbow	MultVar	UOV
Three Bears	Lattice	IMLWE	SIKE	Isogeny	Isogeny	MQDSS	MultVar	Fiat-Shamir
Mersenne-756839	Lattice	ILWE						
Titanium	Lattice	MP-LWE						
Ramstake	Lattice	LWE like						
Odd Manhattan	Lattice	Generic						
NTRU Encrypt	Lattice	NTRU						
NTRU-HRSS-KEM	Lattice	NTRU						
NTRUprime	Lattice	NTRU						

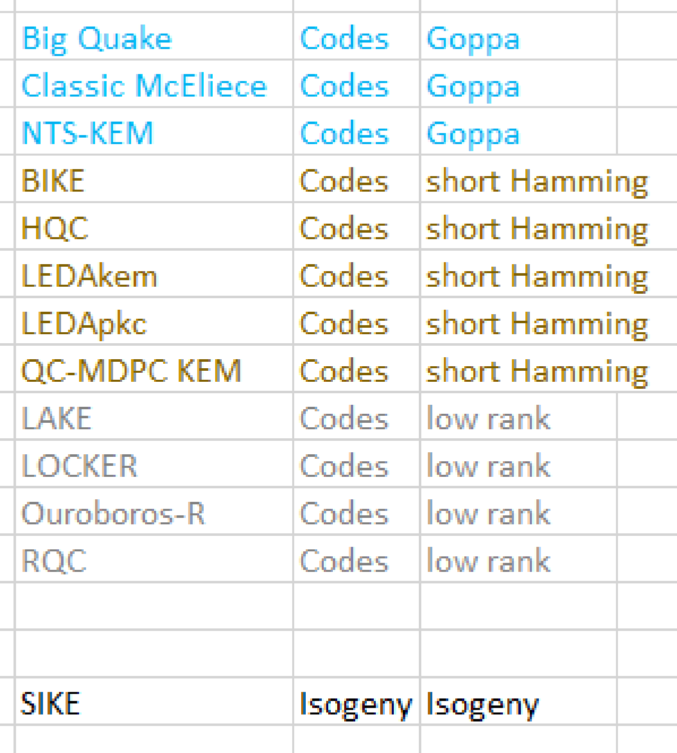
Mergers

- NIST encouraged mergers of similar submissions
  - Round5 = Round2 + Hila5
  - Rollo = Lake + Locker + Ouroboros-R
  - NTRU = NTRUEncrypt + NTRU-HRSS-KEM
  - LEDAcrypt = LEDAkem + LEDApkc

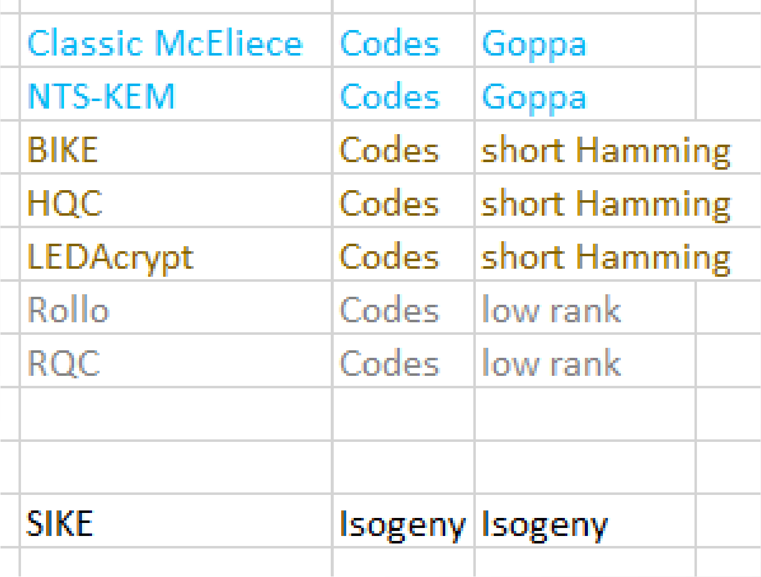
- NIST is still open to future mergers

Biting the Bullet (1)

- NIST wanted to keep diversity, but reduce numbers



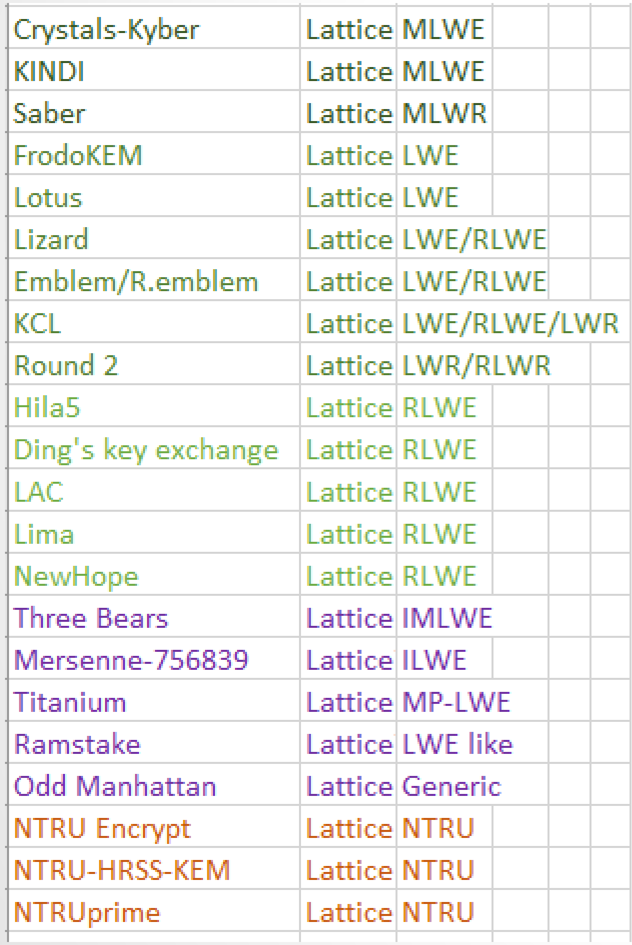
Big Quake	Codes	Goppa
Classic McEliece	Codes	Goppa
NTS-KEM	Codes	Goppa
BIKE	Codes	short Hamming
HQC	Codes	short Hamming
LEDAkem	Codes	short Hamming
LEDApkc	Codes	short Hamming
QC-MDPC KEM	Codes	short Hamming
LAKE	Codes	low rank
LOCKER	Codes	low rank
Ouroboros-R	Codes	low rank
RQC	Codes	low rank
SIKE	Isogeny	Isogeny



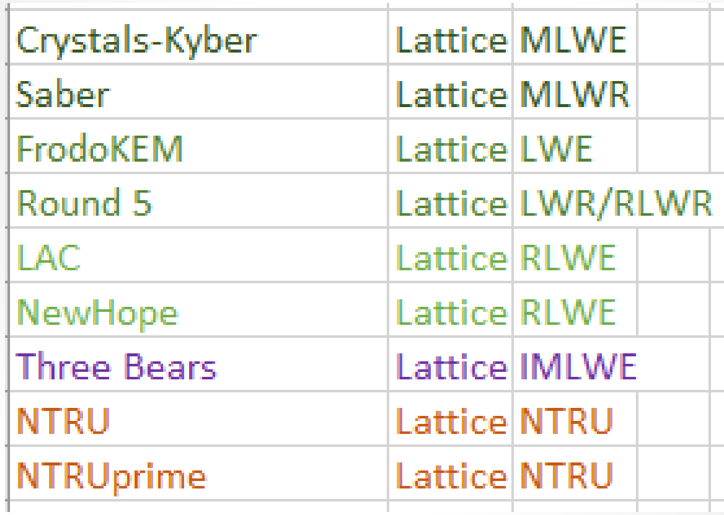
Classic McEliece	Codes	Goppa
NTS-KEM	Codes	Goppa
BIKE	Codes	short Hamming
HQC	Codes	short Hamming
LEDAcrypt	Codes	short Hamming
Rollo	Codes	low rank
RQC	Codes	low rank
SIKE	Isogeny	Isogeny

Biting the Bullet (2)

- NIST wanted to keep diversity, but reduce numbers



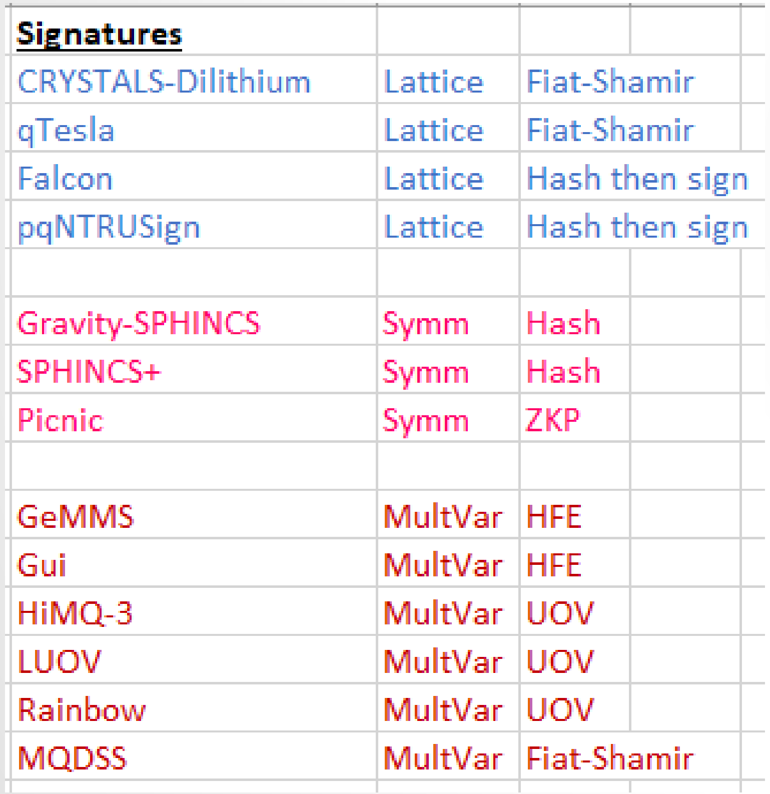
Crystals-Kyber	Lattice	MLWE
KINDI	Lattice	MLWE
Saber	Lattice	MLWR
FrodoKEM	Lattice	LWE
Lotus	Lattice	LWE
Lizard	Lattice	LWE/RLWE
Emblem/R.emblem	Lattice	LWE/RLWE
KCL	Lattice	LWE/RLWE/LWR
Round 2	Lattice	LWR/RLWR
Hila5	Lattice	RLWE
Ding's key exchange	Lattice	RLWE
LAC	Lattice	RLWE
Lima	Lattice	RLWE
NewHope	Lattice	RLWE
Three Bears	Lattice	IMLWE
Mersenne-756839	Lattice	ILWE
Titanium	Lattice	MP-LWE
Ramstake	Lattice	LWE like
Odd Manhattan	Lattice	Generic
NTRU Encrypt	Lattice	NTRU
NTRU-HRSS-KEM	Lattice	NTRU
NTRUprime	Lattice	NTRU



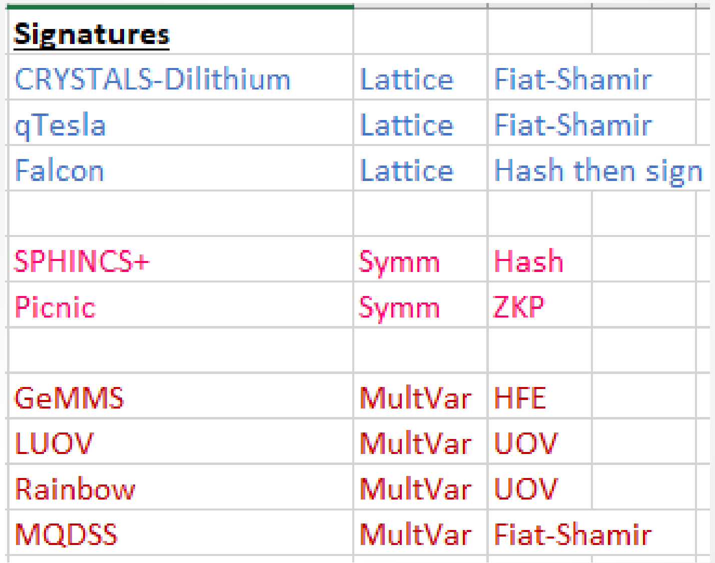
Crystals-Kyber	Lattice	MLWE
Saber	Lattice	MLWR
FrodoKEM	Lattice	LWE
Round 5	Lattice	LWR/RLWR
LAC	Lattice	RLWE
NewHope	Lattice	RLWE
Three Bears	Lattice	IMLWE
NTRU	Lattice	NTRU
NTRUprime	Lattice	NTRU

Biting the Bullet (3)

- NIST wanted to keep diversity, but reduce numbers



Signatures		
CRYSTALS-Dilithium	Lattice	Fiat-Shamir
qTesla	Lattice	Fiat-Shamir
Falcon	Lattice	Hash then sign
pqNTRUSign	Lattice	Hash then sign
Gravity-SPHINCS	Symm	Hash
SPHINCS+	Symm	Hash
Picnic	Symm	ZKP
GeMMS	MultVar	HFE
Gui	MultVar	HFE
HiMQ-3	MultVar	UOV
LUOV	MultVar	UOV
Rainbow	MultVar	UOV
MQDSS	MultVar	Fiat-Shamir



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

A brief intermission

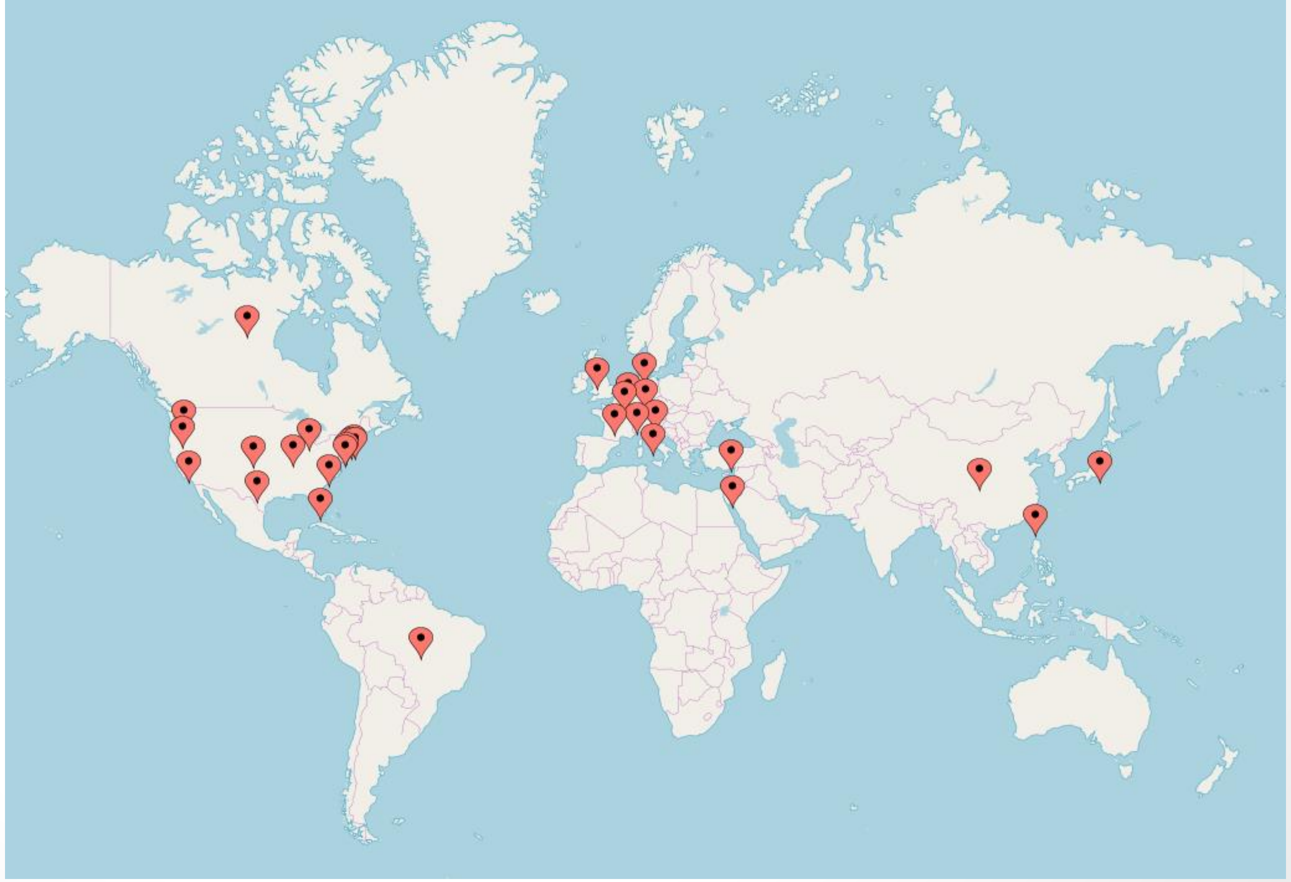
- Dec 4 – pqc-forum post saying we are close to end of 1st round
- Dec 13 – NIST decided to announce 2nd Round candidates at RWC
- Dec 22 – US government shutdown begins
    - NIST employees cannot work in any way, shape or form
- Jan 9-11 – Real World Crypto in San Jose, CA
    - NIST did not attend 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)

CLOSED
We're sorry. Due to the shutdown of the Federal Government, the Washington, DC, facility is closed.
Please check www.archives.gov for updated information.

Numbers

- For Round 2, there are a total of 157 submitters
  - Distribution: [114,22,10,10,0,0,1]

- 17 Countries
- 13 States
- 4 Continents



Tweaks

- Submission teams had until March 15 to send us their revised/merged submission
  - No major re-designs, must meet all the same acceptance criteria
  - NIST to decide whether tweaks are acceptable (working with the submitters)
- Many teams asked for more time, so 2 week extension granted
- Mostly parameter updates, better implementations, compression

The Round 2 Candidates

- KEMs/Encryption: Lattices
  - Crystals-Kyber
    - Based on Module LWE over power-of-2 cyclotomic ring. Easy to scale. Good performance. Security proof might not cover actual scheme.
    - Tweaks: Updated parameters (decreased *q*), removed compression, "90s" version
  - FrodoKEM
    - Uses algebraically unstructured lattices, relies on standard LWE. Results in larger key sizes, and slightly slower performance than other (ring-based) lattice schemes.
    - Tweaks: Added level 5 parameter set, updated parameters, simplified transform
  - LAC
    - Based on poly-variant of LWE. Uses modulus q=251. Good performance. Category 5 parameters have problems. Needs constant-time implementation.
    - Tweaks: Updated parameters, changed distribution, added error-correcting code, made constant-time
  - NewHope
    - Based on ring LWE, with power-of-2 cyclotomic ring. Good performance.
    - Tweaks: Added Lima team, very minor corrections

The Round 2 Candidates

- KEMs/Encryption: Lattices
  - NTRU
    - Merger of 2 good submissions. Been around longer than other submissions. Based on “NTRU assumption”. NTRU lattices have more structure than other lattice schemes.
    - Tweaks: New transform, some parameter sets from both teams in common framework
  - NTRU Prime
    - 2 versions (streamlined and LPRime). Uses irreducible, non-cyclotomic polynomials and inert prime *q*. Good performance. Different cost model used than other submissions. Only level 5 parameters.
    - Tweaks: Added more parameter sets, implicit rejection, expanded discussion in spec
  - Round 5
    - Merger, mostly based on Round2. Uses prime cyclotomic rings, based on (ring) LWR. Good performance and low bandwidth.   Previous issue with decryption failure.
    - Tweaks: Uses ECC from Hila5, updated parameters and implementation
  - Saber
    - Based on module LWR, and power-of-2 cyclotomic ring. Good performance and low bandwidth. Parameters may not fit known security reductions.
    - Tweaks: Slight changes for efficiency and security reductions, cleaner spec
  - Three Bears
    - Novel design (variant of module LWE over the integers). Fast arithmetic. Newer security assumption.
    - Tweaks: Updated parameters, new security proof, added failure analysis (lower failure rate)

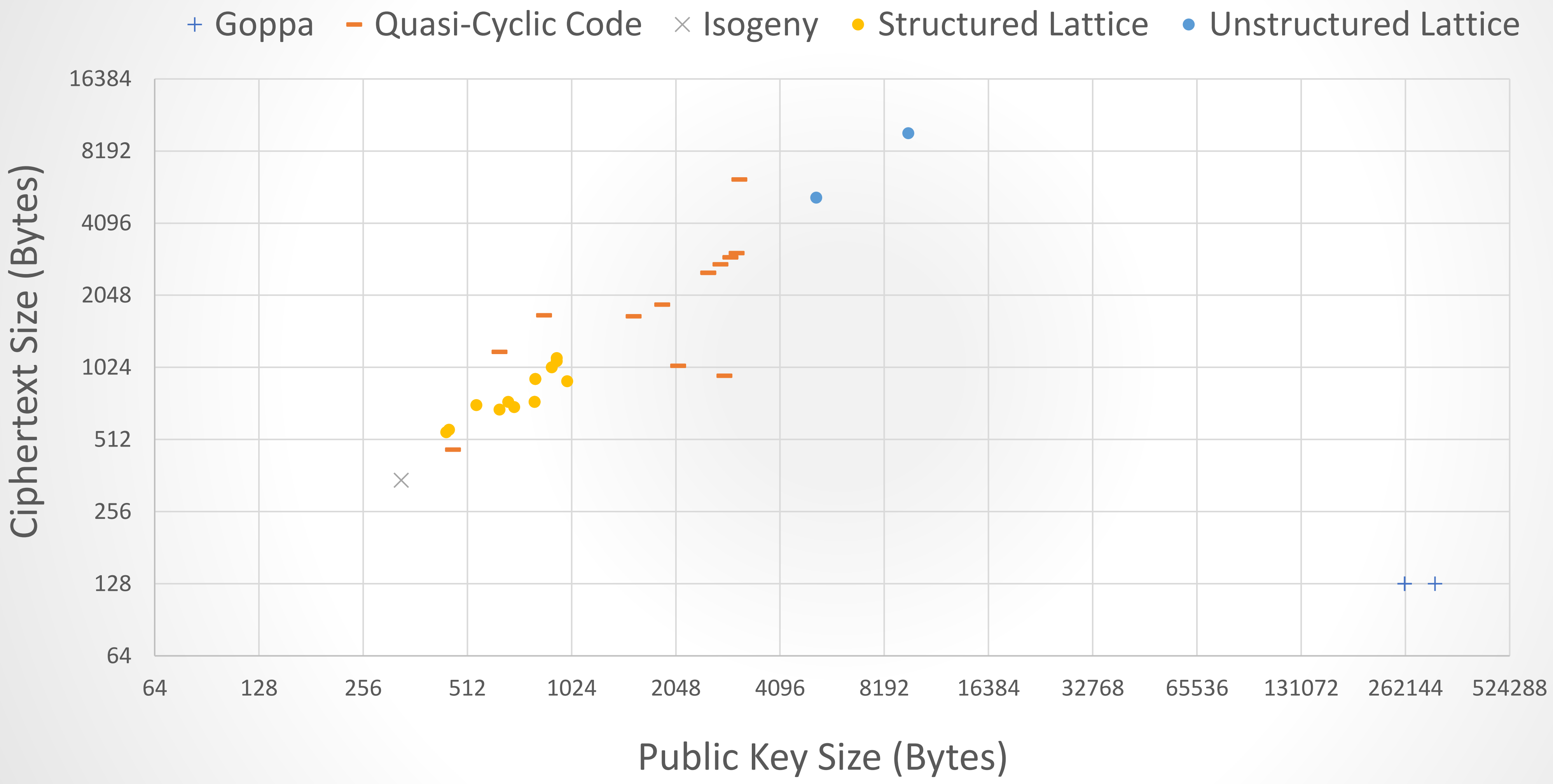
The Round 2 Candidates

- KEMs/Encryption: Code-based
  - Classic McEliece
    - Based on established McEliece cryptosystem (binary Goppa codes). Lots of analysis of security problem. No decryption failures. Short ciphertexts. Okay performance. Very large public keys. Only level 5 parameters given.
    - Tweaks: More parameter sets/security levels, future proposal with 2x faster keygen algorithm
  - NTS-KEM
    - Very, very similar to Classic McEliece, but with some different design choices. Needs constant time implementation.
    - Tweaks: Uses implicit rejection
  - BIKE
    - 3 versions. Based on quasi-cyclic MDPC codes. Ephemeral use only. Similar key size and performance to lattice schemes. More analysis needed of particular security assumption.
    - Tweaks: New decoder yielding smaller error rates, new CCA version
  - HQC
    - Low decryption failure rate (necessary for CCA security). As a result, slightly larger key and ciphertext sizes. More analysis needed of particular security assumption.
    - Tweaks: dropped some parameter sets, updated implementation

The Round 2 Candidates

- KEMs/Encryption: Code-based (and Isogeny)
  - LEDAcrypt
    - Merger. Based on quasi-cyclic LDPC codes, which have more structure than QC-MDPC codes. New parameters with low decryption rates. Needs more analysis.
    - Tweaks: Updated parameters, CCA version, better failure rates, new transform
  - Rollo
    - Merger of 3 rank-based schemes using LRPC codes. 2 schemes are ephemeral, 1 targets CCA security. Newer security assumption.
    - Tweaks: Uses ideal codes instead of quasi-cyclic ones (Rollo-3), updated parameters
  - RQC
    - Rank-based scheme. No decryption failures. As a result, slower speeds and ciphertext size. Security problem needs more analysis, as it is newer.
    - Tweaks: Uses ideal codes (not quasi-cyclic), updated parameters, updated implementation
  - SIKE
    - Uses isogenies of supersingular elliptic curves. Very low key sizes. Can leverage ECC knowledge and code. Security problem is relatively new. Performance a concern.
    - Tweaks: New parameter sets, new quantum security analysis, optional key compression

Public Key vs Ciphertexts, Category 1



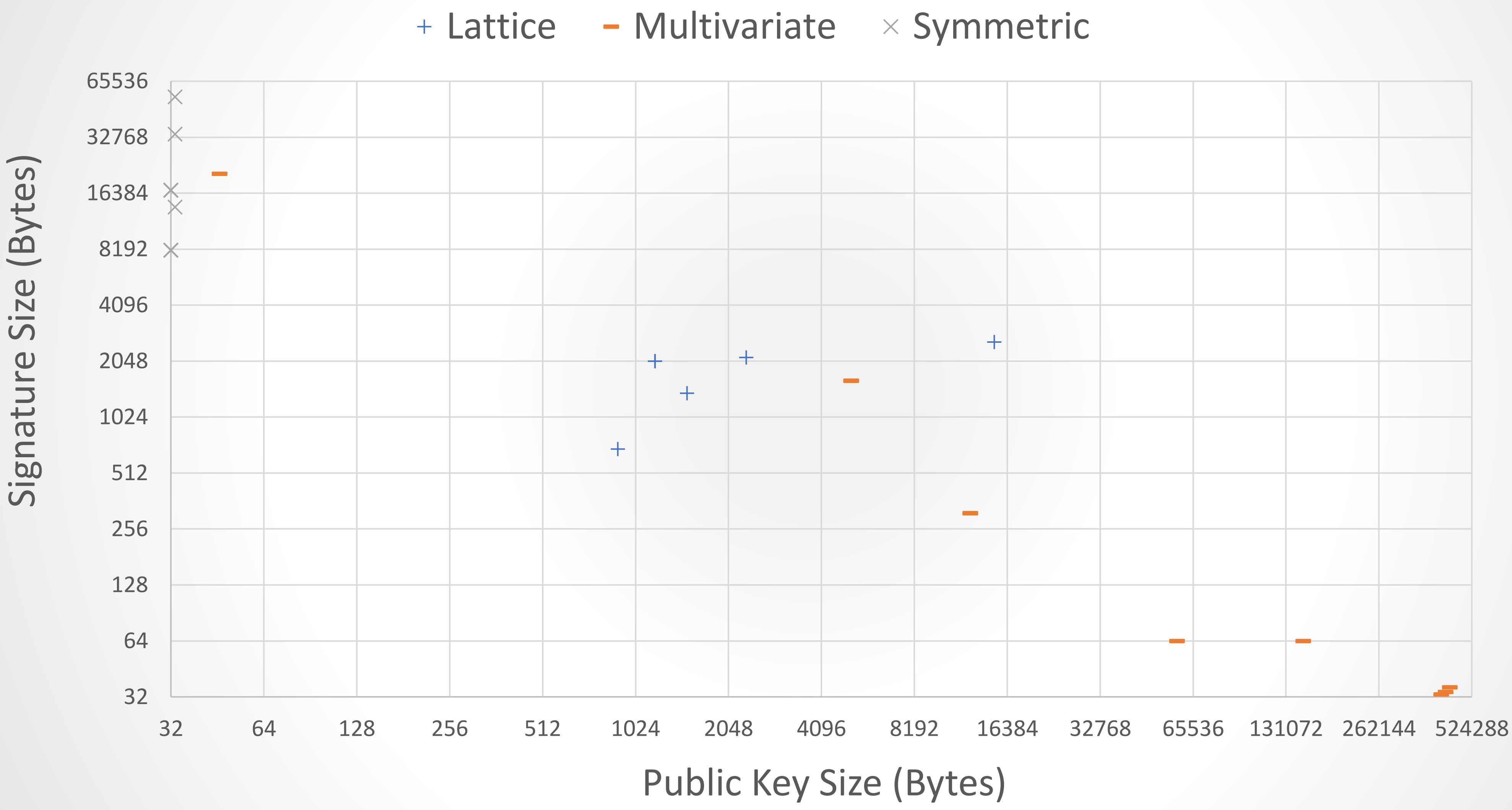
The Round 2 Candidates

- Signatures: Lattices
  - Crystals-Dilithium
    - Fiat-Shamir idea, based on module LWE. Good performance.
    - Tweaks: randomized signing option, some optimizations
  - Falcon
    - Uses the NTRU lattice. Good performance. Complicated to implement.
    - Tweaks: removed parameter set, key-recovery mode
  - qTesla
    - Based on ring LWE. Good performance. More analysis needed of particular security assumption.
    - Tweaks: updated parameters, randomized signatures, optional compressed version
- Symmetric-based
  - Sphincs+
    - Stateless hash-based scheme. Security well understood, relying only on pre-image resistance of the hash function. Small public keys, but large signatures. Signing is slower.
    - Tweaks: use tweakable hash, some optimizations
  - Picnic
    - Novel design, based on hash functions, block ciphers, and zero-knowledge proofs. Small public keys, but larger signatures. Slower performance. Very modular scheme. Needs more analysis.
    - Tweaks: Updated parameter sets, different MPC system, protection from multi-target attacks

The Round 2 Candidates

- Signatures: Multivariate
  - GeMSS
    - An HFEv- “big-field” scheme. Very small signatures. As a result, some performance sizes/times are larger. Better tradeoffs may be found.
    - Tweaks: Updated parameter sets, better performance, updated implementation
  - LUOV
    - “Small-field” scheme based on UOV. Low bandwidth. Some of the techniques introduced need more analysis.
    - Tweaks: Updated parameters (smaller security margin), more side-channel protection
  - MQDSS
    - Based on provably secure reduction to MQ problem, using Fiat-Shamir. (Actual parameters don’t fit the reduction). Smaller public keys, and larger signature sizes.   Needs more research and optimization.
    - Tweaks: Updated parameters, updated security analysis
  - Rainbow
    - Generalization of UOV, adding in structure to be more efficient. Somewhat well-studied. The implementation could be improved.
    - Tweaks: Updated (and fewer) parameter sets, improved KeyGen, variant with smaller keys

Public Key By Signature (Category 1)



Cryptanalysis continues….

- LAC
    - D’ Anvers, Tiepelt, Vercauteren, Verbauwhede: eprint.iacr.org/2019/292
        - “It is able to retrieve LAC’s secret for all security levels in under 2 hours using less than 2^{21} decryption queries…”
    - Round 2 spec counters this timing attack by using (almost) constant time BCH decoding algorithm
- qTesla
    - Optional key compressed version broken by Lyubashevsky and Schwabe

The Second Round (and beyond)

- Aug 22-24, 2019 – 2nd NIST PQC Standardization workshop, co-located with CRYPTO in Santa Barbara, CA
  - Deadline for paper submission: May 31, 2019
  - Registration is already open
- Expected to last 12-18 months, after possibly a 3rd Round
- Overall timeline: we still expect draft standards around 2022ish
  - (but reserve the right to change this!)

Stateful Hash-based signatures

- NIST plans to approve stateful hash-based signatures
  - 1) XMSS, specified in RFC 8931
  - 2) LMS, specified in RFC 8554

- In Feb 2019, NIST issued a request for public input on how to mitigate the potential misuse of stateful HBS schemes.
  - See comments received here

- NIST expects to have a Special Publication (SP) published in 2019

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

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
- Continued research and analysis on **ALL** of the 2nd round candidates
- See how submissions fit into applications/procotols. Any constraints?

Summary

- Round 2 has started
  - 26 candidate algorithms (17 encryption/KEM, 9 signatures)
- We will continue to work in an open and transparent manner with the crypto community for PQC standards
- Check out: www.nist.gov/pqcrypto
  - Sign up for the pqc-forum
- Talk to us: pqc-comments@nist.gov