NIST PQC Standardization Update
- Round 2 and Beyond

Dustin Moody
and the NIST PQC team

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

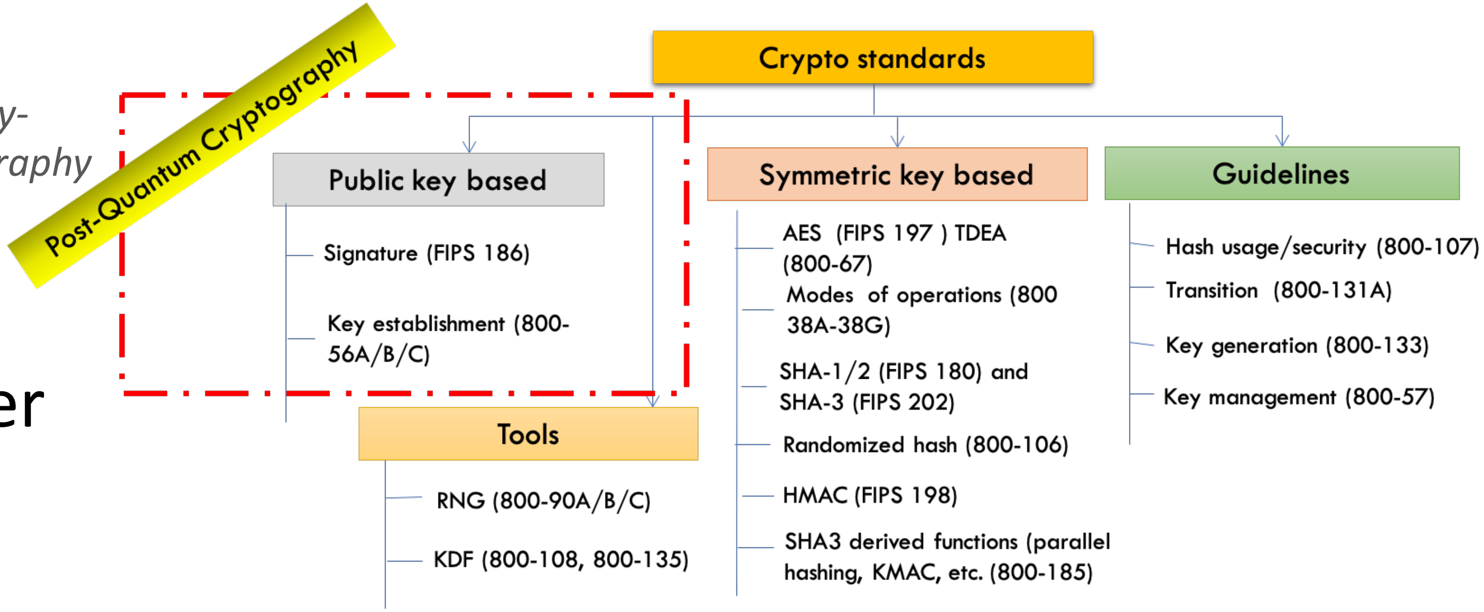
Crypto Technology Group
Computer Security Division
Information Technology Lab

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)

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)

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

NIST Crypto Standards

- FIPS, SP’s, and NISTIRs

- NISTIR 7977 – *NIST Cryptographic Standards and Guidelines Development Process*
  - Cooperation with other SDO’s
  - Section 7 discusses competitions as a standards vehicle
- 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 PQC Milestones

- Apr 2015 – NIST Workshop on PQC
- Feb 2016 – published report on PQC: NISTIR 8105
- – announced "competition-like" process to select PQC standards
- Dec 2016 – finalized evaluation criteria and submission requirements

---

- Nov 2017 – received 82 submissions, yielding 69 first round candidates
- Apr 2018 – 1st NIST PQC Standardization workshop

- Jan 2019 – 26 algorithms advance to the 2nd round
  - – Published Status report on the 1st round: NISTIR 8240
- Aug 2019 – 2nd NIST PQC Standardization workshop

- July 2020 – announced 7 finalists and 8 alternates for the 3rd round
  - – Published Status report on the 2nd round: NISTIR 8309

NIST PQC Milestones

- Apr 2015 – NIST Workshop on PQC
- Feb 2016 – published report on PQC: NISTIR 8105
- – announced “competition-like” process to select PQC standards
- Dec 2016 – finalized evaluation criteria and submission requirements
- Nov 2017 – received 82 submissions, yielding 69 first round candidates
- Apr 2018 – 1st NIST PQC Standardization workshop
- Jan 2019 – 26 algorithms advance to the 2nd round

  – Published Status report on the 1st round: NISTIR 8240
- Aug 2019 – 2nd NIST PQC Standardization workshop
- July 2020 – announced 7 finalists and 8 alternates for the 3rd round

  – Published Status report on the 2nd round: NISTIR 8309

NIST PQC Milestones

- Apr 2015 – NIST Workshop on PQC
- Feb 2016 – published report on PQC: NISTIR 8105
- – announced "competition-like" process to select PQC standards
- Dec 2016 – finalized evaluation criteria and submission requirements
- Nov 2017 – received 82 submissions, yielding 69 first round candidates
- Apr 2018 – 1st NIST PQC Standardization workshop
- Jan 2019 – 26 algorithms advance to the 2nd round

  – Published Status report on the 1st round: NISTIR 8240
- Aug 2019 – 2nd NIST PQC Standardization workshop
- July 2020 – announced 7 finalists and 8 alternates for the 3rd round

  – Published Status report on the 2nd round: NISTIR 8309

NIST PQC Milestones

- Apr 2015 – NIST Workshop on PQC
- Feb 2016 – published report on PQC: NISTIR 8105
- – announced "competition-like" process to select PQC standards
- Dec 2016 – finalized evaluation criteria and submission requirements
- Nov 2017 – received 82 submissions, yielding 69 first round candidates
- Apr 2018 – 1st NIST PQC Standardization workshop
- Jan 2019 – 26 algorithms advance to the 2nd round

  – Published Status report on the 1st round: NISTIR 8240
- Aug 2019 – 2nd NIST PQC Standardization workshop
- July 2020 – announced 7 finalists and 8 alternates for the 3rd round

  – Published Status report on the 2nd round: NISTIR 8309

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

- 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 1st Round Candidates

- 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

The 2nd Round Candidates

~~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~~

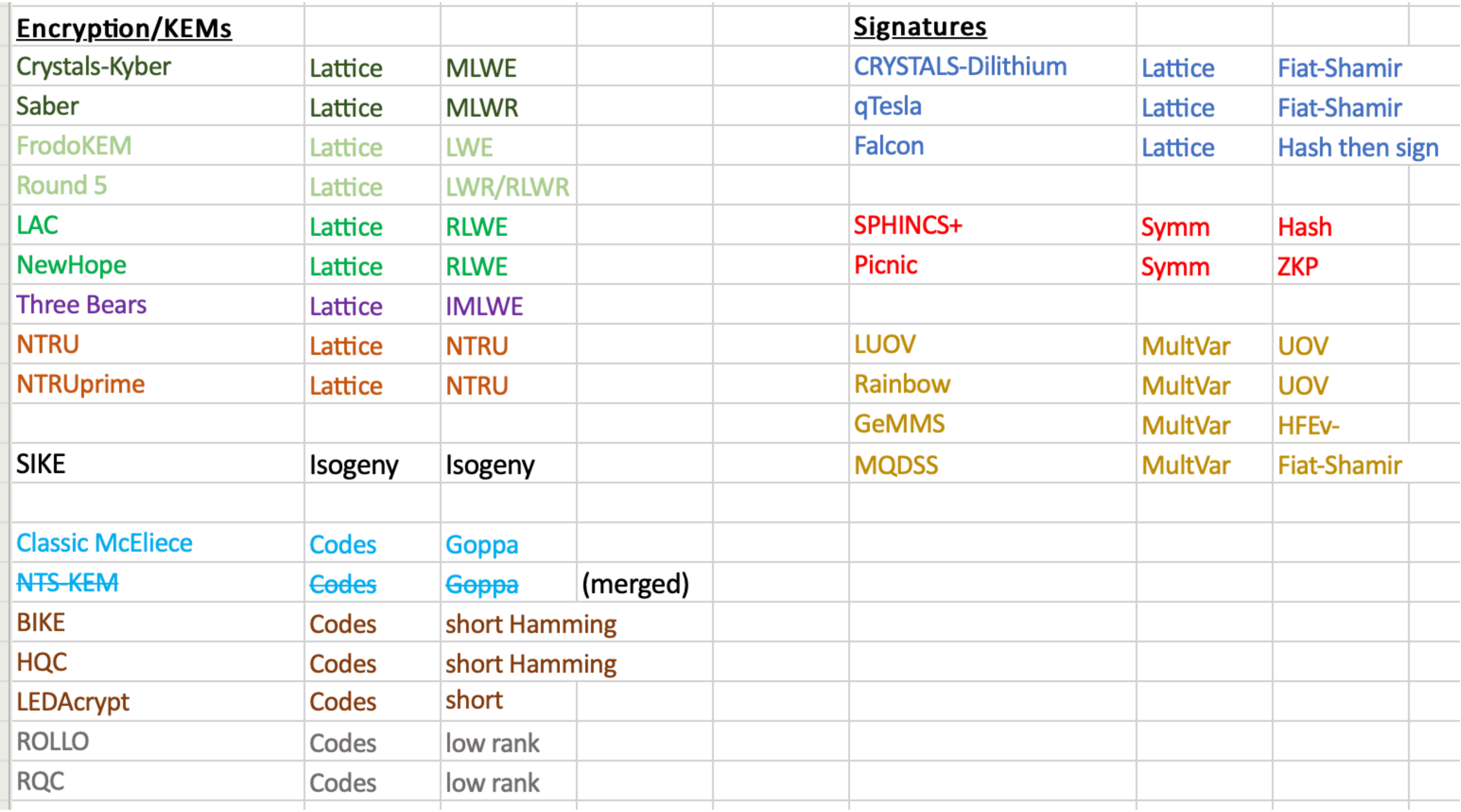
LEDAcrypt

NTRU

Rollo

Round5

The 2nd Round Candidates sorted



Encryption/KEMs					**Signatures**		
Crystals-Kyber	Lattice	MLWE			CRYSTALS-Dilithium	Lattice	Fiat-Shamir
Saber	Lattice	MLWR			qTesla	Lattice	Fiat-Shamir
FrodoKEM	Lattice	LWE			Falcon	Lattice	Hash then sign
Round 5	Lattice	LWR/RLWR					
LAC	Lattice	RLWE			SPHINCS+	Symm	Hash
NewHope	Lattice	RLWE			Picnic	Symm	ZKP
Three Bears	Lattice	IMLWE					
NTRU	Lattice	NTRU			LUOV	MultVar	UOV
NTRUprime	Lattice	NTRU			Rainbow	MultVar	UOV
					GeMMS	MultVar	HFEv-
SIKE	Isogeny	Isogeny			MQDSS	MultVar	Fiat-Shamir
Classic McEliece	Codes	Goppa					
~~NTS-KEM~~	~~Codes~~	~~Goppa~~	(merged)				
BIKE	Codes	short Hamming					
HQC	Codes	short Hamming					
LEDAcrypt	Codes	short					
ROLLO	Codes	low rank					
RQC	Codes	low rank					

Overview of the 2nd Round

- 4 merged submissions
  - NTRU, LEDAcrypt, ROLLO, Round5
- Maintained diversity of algorithms
- 158 forum posts and 180 "official comments"
- Cryptanalysis continues
  - LAC, LEDAcrypt, RQC, Rollo, MQDSS, qTESLA, LUOV all attacked or broken
- 2nd NIST PQC Standardization workshop
- More research, 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**

The 2nd NIST PQC Workshop

- Aug 22-25, 2020 – co-located with CRYPTO in Santa Barbara, CA
- 23 papers accepted and an Industry Panel
  - Implementations, experiments, benchmarking, cryptanalysis, security proofs and evaluation,
- Round 2 updates from each team
- NIST also surveyed the attendees and held a feedback session
  - **Don’t rush**, focus on cryptanalysis, more education/outreach, questions about after round 3, civility on the pqc-forum, time estimate on when quantum computers will threaten crypto, etc.
  - In response, NIST clarified about the 3rd round and asked for results which might impact the 3rd round decision by April 15, 2019

The Selection Process

- Throughout the 2nd round, NIST regularly met and reviewed the submissions and research results
- Starting in April 2020, we began more frequently meeting to review each submission in detail and start to make decisions
- By around the end of May 2020, we'd made our decisions and began writing the 2nd Round Report
    - Long discussions and back and forth. Changed our minds often.
    - A lot of debate about the 2 track approach "finalists" and "alternates"
- We were essentially done by the end of June 2020, and then went through the process to get NISTIR 8309 reviewed and published
- July 22nd, 2020 – we announced the 3rd round Finalists and Alternates

Other Inputs

- Round 2 ”tweaks” from each submission team
- Official comments and pqc-forum discussion
- Papers published/presented in journals and workshops
- Engagement with community and stakeholders
    - This includes feedback we received from many, including the NSA.
    - We keep everyone out of our internal standardization meetings and the decision process
    - The feedback received (from the NSA) did not change any of our decisions and did not substantively change our 2nd Round Report.
    - NIST encouraged the NSA to provide comments publicly
    - NIST alone makes the PQC standardization decisions, based on publicly available information, and stands by those decisions

Reminder - Evaluation Criteria

1. Security
   - Security categories
   - (confidence in) security proof
   - Any attacks
   - Classical/quantum complexity

2. Performance
   - Size of parameters
   - Speed of KeyGen, Enc/Dec, Sign/Verify
     - Software and Hardware
   - Decryption failures

3. Algorithm and implementation characteristics
   - Advantages and disadvantages
   - IP issues
   - Side channel resistance
     - Constant time code?
   - Simplicity and clarity of documentation
   - Flexible

The First Cuts

Security Concerns

1. LEDAcrypt
2. ROLLO
3. RQC
4. qTESLA
5. LUOV
6. MQDSS

7. To a lesser extent: LAC (and Round5)

LEDAcrypt

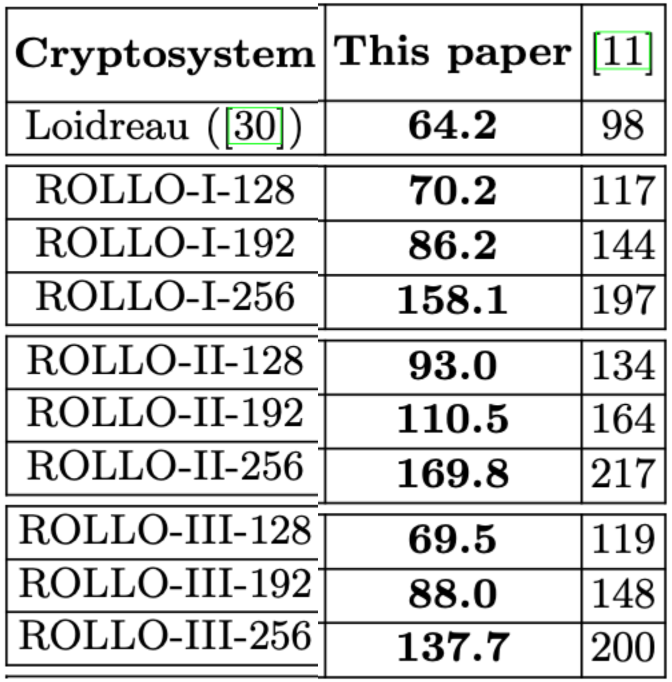
- Oct 2019 – Attack by Apon, Perlner, Robinson, Santini

- “For $2^{49.22}$ AES-256 operations, we recover 1 in $2^{47.79}$ Category-5 keys”
- “We think we can recover nearly all of the keys for LEDAcrypt (CPA, Category 5, $n_0 = 2$) for about 2^{240} classical AES operations”
- “Our attack shows that LEDAcrypt’s product structure is a security problem not just asymptotically, but **concretely”**

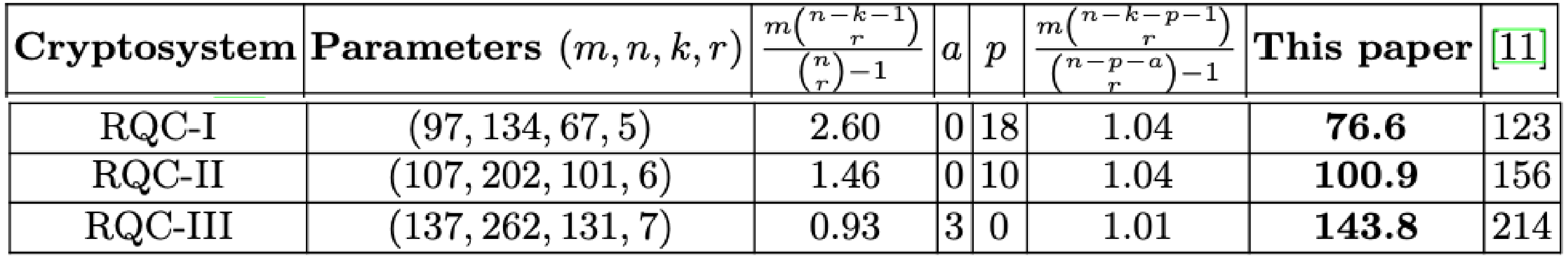
- LEDAcrypt team acknowledges.

ROLLO and RQC

- March 11, from Gaborit, Perlner, Smith-Tone, et. al.
  - Improves earlier attack paper from Gaborit, et. al.
  - "…our new attacks show that ROLLO parameters are broken and need to be changed."
  - "Moreover, unlike that previous attack, the new one does not rely on Grobner basis computations and thus does not require any assumption concerning the behavior of the so-called solving degree. "
- New parameters proposed – new key sizes approximately doubled



Cryptosystem	**This paper**	[11]
Loidreau ([30])	**64.2**	98
ROLLO-I-128	**70.2**	117
ROLLO-I-192	**86.2**	144
ROLLO-I-256	**158.1**	197
ROLLO-II-128	**93.0**	134
ROLLO-II-192	**110.5**	164
ROLLO-II-256	**169.8**	217
ROLLO-III-128	**69.5**	119
ROLLO-III-192	**88.0**	148
ROLLO-III-256	**137.7**	200



Cryptosystem	**Parameters** (m, n, k, r)	$\frac{m\binom{n-k-1}{r}}{\binom{n}{r}-1}$	a	p	$\frac{m\binom{n-k-p-1}{r}}{\binom{n-p-a}{r}-1}$	**This paper**	[11]
RQC-I	$(97, 134, 67, 5)$	2.60	0	18	1.04	**76.6**	123
RQC-II	$(107, 202, 101, 6)$	1.46	0	10	1.04	**100.9**	156
RQC-III	$(137, 262, 131, 7)$	0.93	3	0	1.01	**143.8**	214

qTESLA

- April 2019 comment by Vadim Lyubashevsky and Peter Schwabe
  - A “complete break” of qTESLA parameters for compressed public-keys (which had an incorrect security proof)
  - They can sign messages faster than that qTESLA implementation w/o knowing the secret key
  - For their main (heuristic) parameters, “there is no reasoning…as to why their parameters have the concrete hardness of SIS they claim”
  - “provably secure” parameters still okay (but much larger key sizes than Frodo)
- qTESLA confirmed attack worked on compressed key version. Drops those parameter sets. They disagree about the rest.
- Aug 2019 – qTESLA agrees with Vadim about security gap for the heuristic parameters. They drop those parameters sets, leaving only the provably secure version.

LUOV

- June 2019 – Subfield differential attack by Ding, et. al.
  - Lowered security for level 2 from 147 bits to 107 and from 147 to 135
  - Lowered security for level 4 from 210 bits to 144.5 and from 214 to 202
  - Lowered security for level 5 from 272 bits to 184 and from 273 to 244.
  - Implemented it on level 2 parameter set and it worked
- LUOV didn’t dispute, and proposed dropping lifting technique to use just UOV; we said no.
- In Sept, they gave new parameters (with prime degree extensions). About the same size and w/ same efficiency.
- More recently, Ding, et al. showed how to forge a LUOV signature in 210 minutes of real-world computation (massive break)

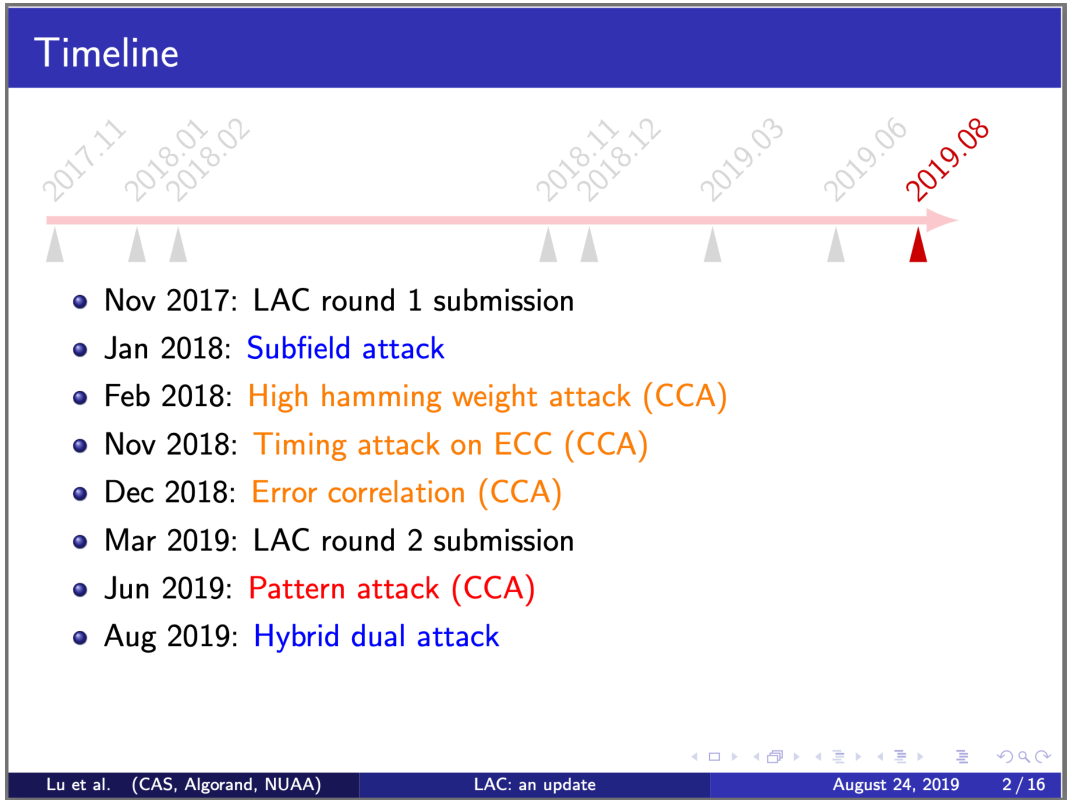
MQDSS

- Aug 2019 – Greg Zaverucha and Daniel Kales announce attack
  - “Concretely, forging a signature for the L1 instance of MQDSS, which should provide 128 bits of security, can be done in ≈ 2^95 hash function calls with high probability. We verify the validity of the attack by implementing it for round reduced versions of MQDSS, and show that we can forge a signature for 40 rounds of MQDSS with ≈ 2^29 hash function calls.

    Even though a security proof of the scheme exists and we did not find a flaw in it, the proof is not tight enough to rule out these attacks. Our attack does not break the MQDSS design, rather the proposed parameter sets.”
  - MQDSS team confirms attack, proposes new parameters.
    - Need to have 1.4x more rounds. Security proof still valid (just not tight). Key sizes almost 50% bigger
    - This appears to make the scheme worse in performance than SPHINCS+…

LAC

- LAC has had attacks since Aug as well:
  - CCA attack using decryption failures
  - Attack on LAC in misuse situation
- None outright break it, but LAC has had to adjust parameters



Timeline

- Nov 2017: LAC round 1 submission
- Jan 2018: Subfield attack
- Feb 2018: High hamming weight attack (CCA)
- Nov 2018: Timing attack on ECC (CCA)
- Dec 2018: Error correlation (CCA)
- Mar 2019: LAC round 2 submission
- Jun 2019: Pattern attack (CCA)
- Aug 2019: Hybrid dual attack

Lu et al. (CAS, Algorand, NUAA) LAC: an update August 24, 2019 2 / 16

Round5

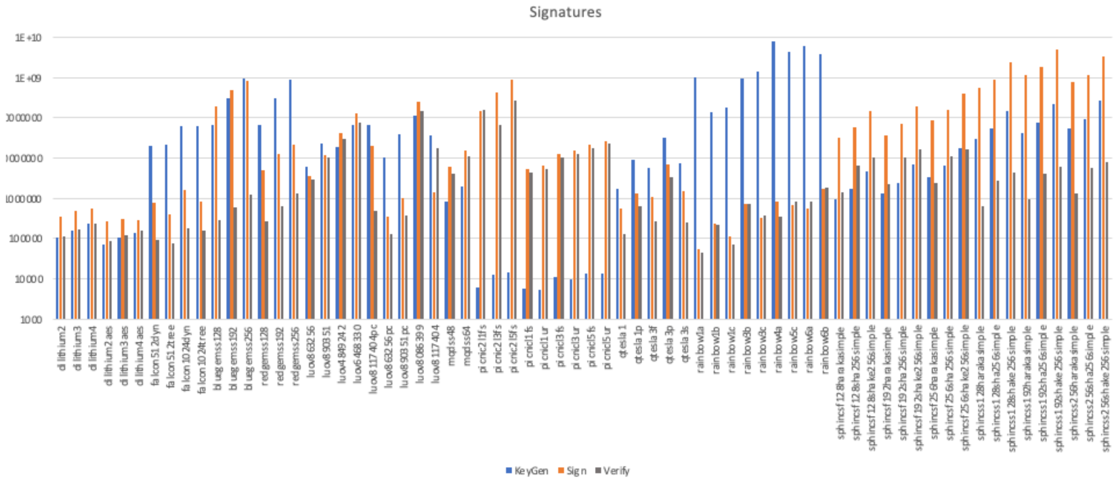
- Round5 had a minor attack announced in Aug 2019
  - Response: “Tighter concrete security analysis of small secret attacks. After having many discussions, the main conclusion is that the original security estimates hardly change, and thus, we are not suggesting any change of parameters.”
  - Also provided an improved implementation
  - Minor attack. Complicated spec.
  - Not more promising than the 3 lattice KEM finalists

Performance Hits

Too slow in some way??

- SPHINCS+
- PICNIC
- MQDSS
- Classic McEliece
- SIKE
- GeMSS
- Rainbow
- LUOV
- Others …

- ## Key Sizes too big?
- Classic McEliece
  - PK size up to a million bytes
- Frodo and Round5N1
  - PK and CT size large (10-20K bytes)



- Performance wasn’t the *primary* factor in our decisions, but we stayed aware of it

The other ones

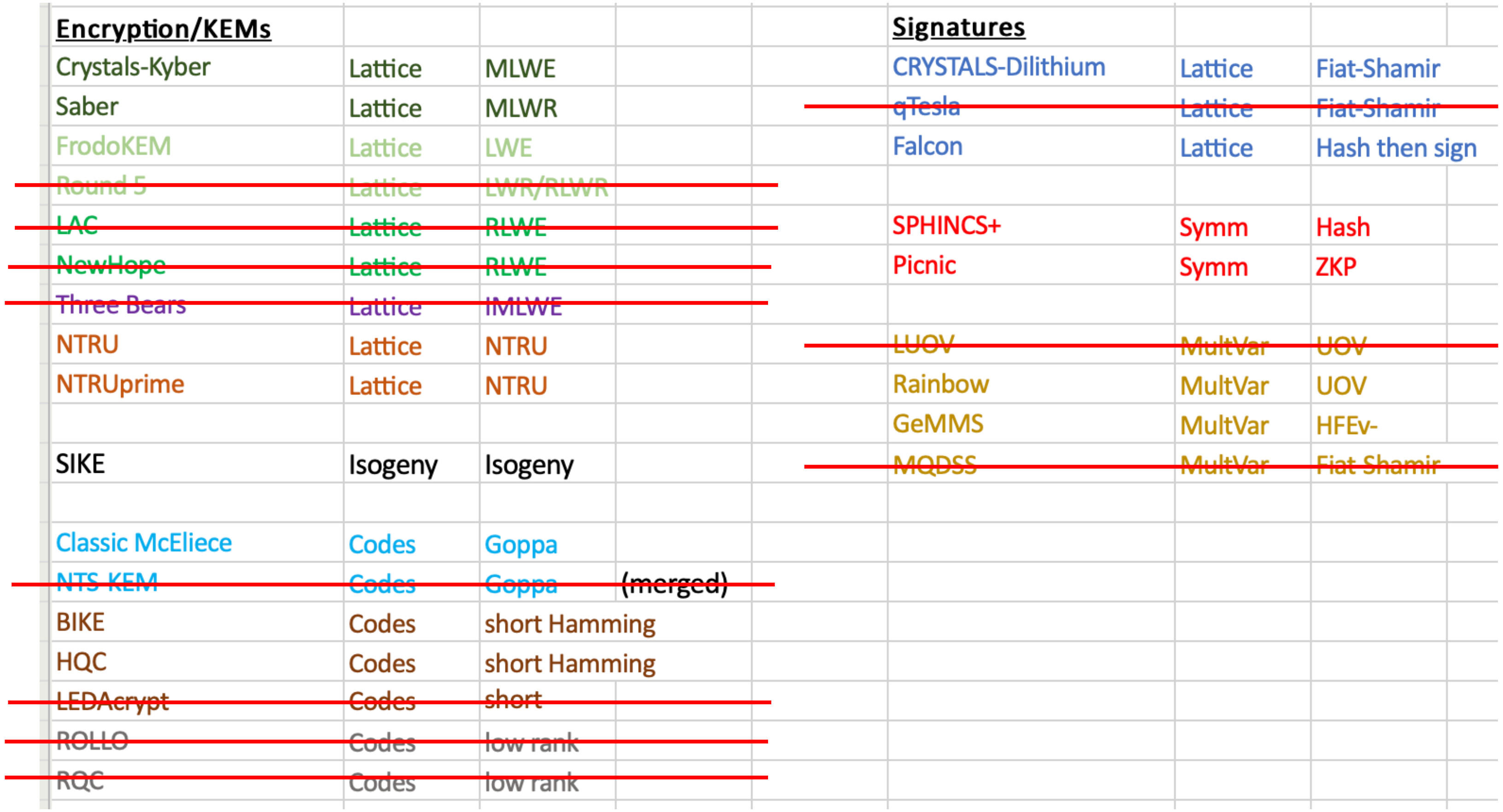
- NTS-KEM
  - Merged with Classic McEliece

- Three Bears
  - A very good scheme
  - Not enough independent analysis
  - I-MLWE

- New Hope
  - A very good scheme
  - Security reduction (MLWE is ~always at least as good as RLWE)
  - NIST needed to make hard decisions for the lattice KEMs

Two Tracks

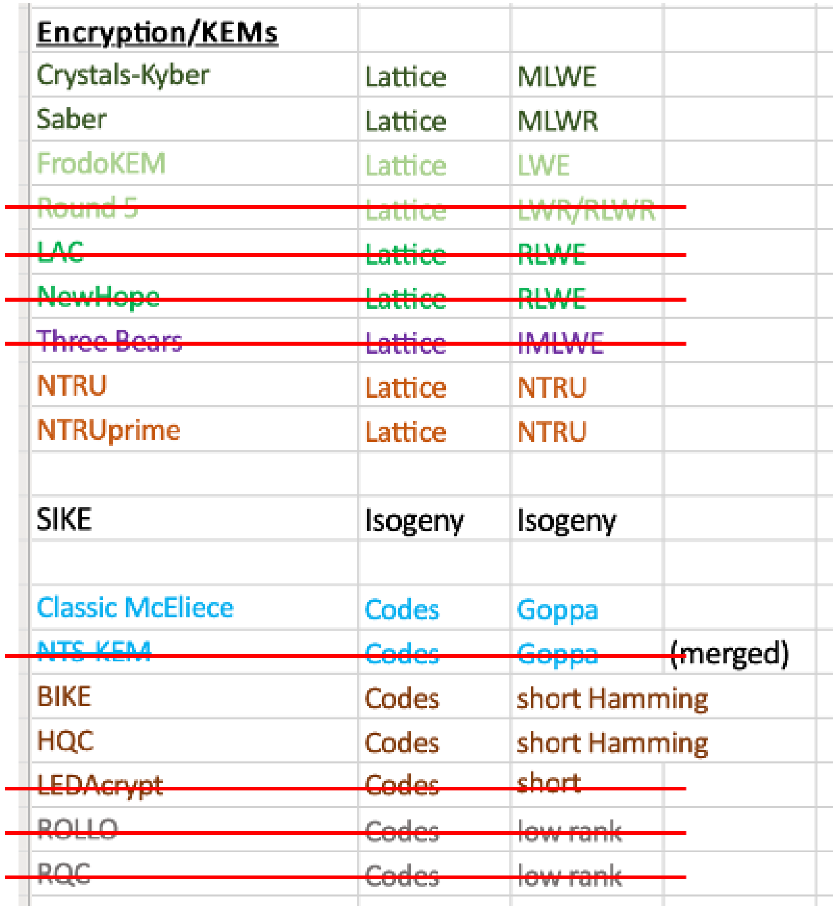
- Finalists
  - Algorithms that could be ready to be standardized at the end of the 3rd round
  - Most promising to fit the majority of use cases
- The 2nd track: Alternates
  - Crucial point – had to have potential for standardization
  - not just be of interest for future research



Encryption/KEMs				**Signatures**		
Crystals-Kyber	Lattice	MLWE		CRYSTALS-Dilithium	Lattice	Fiat-Shamir
Saber	Lattice	MLWR		~~qTesla~~	~~Lattice~~	~~Fiat-Shamir~~
FrodoKEM	Lattice	LWE		Falcon	Lattice	Hash then sign
~~Round 5~~	~~Lattice~~	~~LWR/RLWR~~				
~~LAC~~	~~Lattice~~	~~RLWE~~		SPHINCS+	Symm	Hash
~~NewHope~~	~~Lattice~~	~~RLWE~~		Picnic	Symm	ZKP
~~Three Bears~~	~~Lattice~~	~~IMLWE~~				
NTRU	Lattice	NTRU		~~LUOV~~	~~MultVar~~	~~UOV~~
NTRUprime	Lattice	NTRU		Rainbow	MultVar	UOV
				GeMMS	MultVar	HFEv-
SIKE	Isogeny	Isogeny		~~MQDSS~~	~~MultVar~~	~~Fiat Shamir~~
Classic McEliece	Codes	Goppa				
~~NTS-KEM~~	~~Codes~~	~~Goppa~~	~~(merged)~~			
BIKE	Codes	short Hamming				
HQC	Codes	short Hamming				
~~LEDAcrypt~~	~~Codes~~	~~short~~				
~~ROLLO~~	~~Codes~~	~~low rank~~				
~~RQC~~	~~Codes~~	~~low rank~~				

Lattice-based KEMs

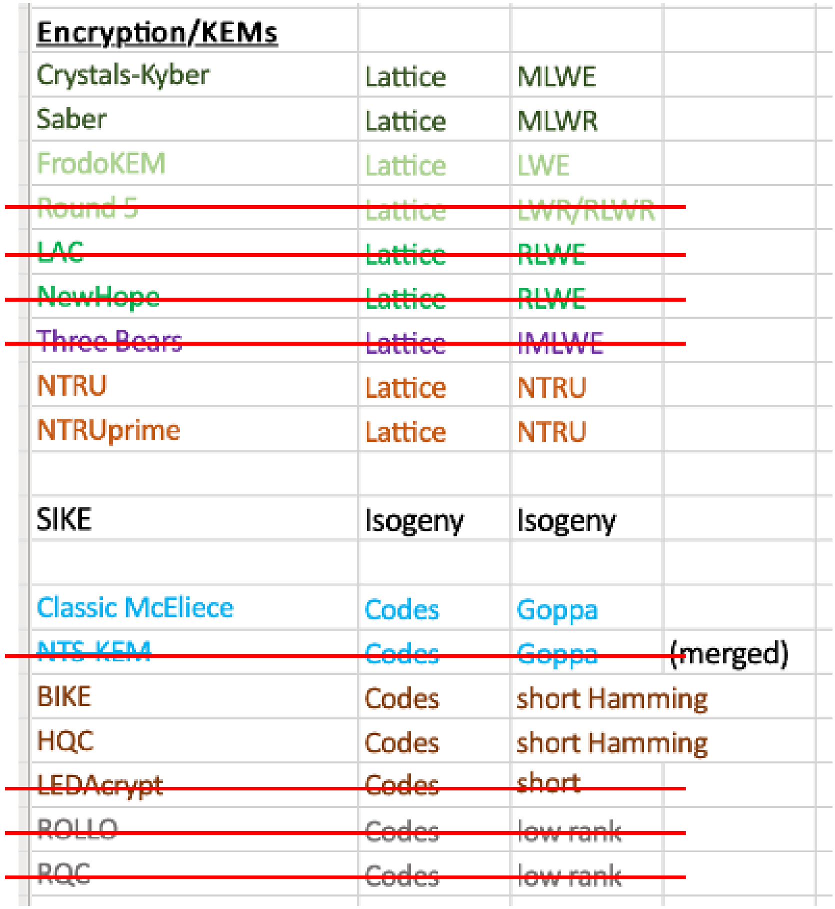
- Crystals-Kyber
  - Great all-around → Finalist
- Saber
  - Great all-around → Finalist
- FrodoKEM
  - Conservative/Backup → Alternate
- NTRU
  - Not quite as efficient, but older, IP situation → Finalist
- NTRUprime
  - Different design choice and security model → Alternate



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~~	(merged)
BIKE	Codes	short Hamming	
HQC	Codes	short Hamming	
~~LEDAcrypt~~	~~Codes~~	~~short~~	
~~ROLLO~~	~~Codes~~	~~low rank~~	
~~RQC~~	~~Codes~~	~~low rank~~	

Isogeny- and Code-based KEMs

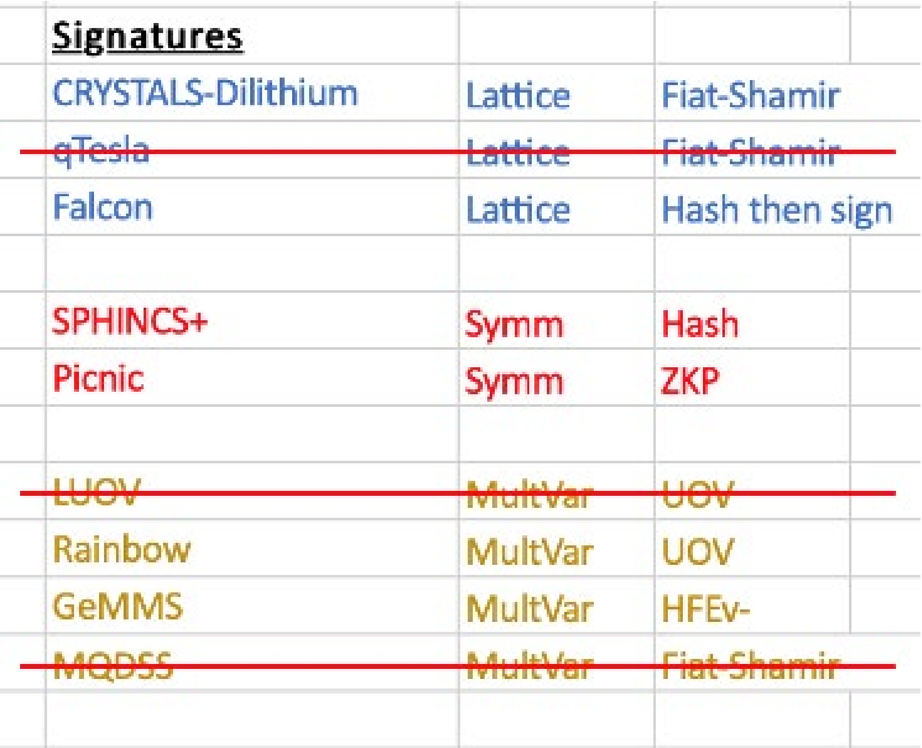
- SIKE
  - Newer security problem, an order slower → Alternate
- Classic McEliece
  - Oldest submission, large public keys but small ciphertexts→ Finalist
- BIKE
  - Good performance, CCA security?, more time to be stable → Alternate
- HQC
  - Better security analysis/larger keys (than BIKE) → Alternate



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~~	(merged)
BIKE	Codes	short Hamming	
HQC	Codes	short Hamming	
~~LEDAcrypt~~	~~Codes~~	~~short~~	
~~ROLLO~~	~~Codes~~	~~low rank~~	
~~RQC~~	~~Codes~~	~~low rank~~	

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



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~~

The Overall Picture

- KEM finalists: Kyber, NTRU, SABER, Classic McEliece
- KEM alternates: Bike, FrodoKEM, HQC, NTRUprime, SIKE

- Signature finalists: Dilithium, Falcon, Rainbow
- Signature alternates: GeMSS, Picnic, Sphincs+

- NIST expects to standardize **at most one** of
  - (Encryption/KEM) Kyber or NTRU or Saber
  - (Signature) Dilithium or Falcon

Timeline

- 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
- Tweaks are due by October 1st, 2020
- 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

Stateful Hash-based Signature (HBS)

- NIST plans to approve stateful hash-based signatures

  1) XMSS, specified in RFC 8931

  2) LMS, specified in RFC 8554

     It 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

- Draft SP 800-208 should be published very shortly

Research Challenges

- 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…

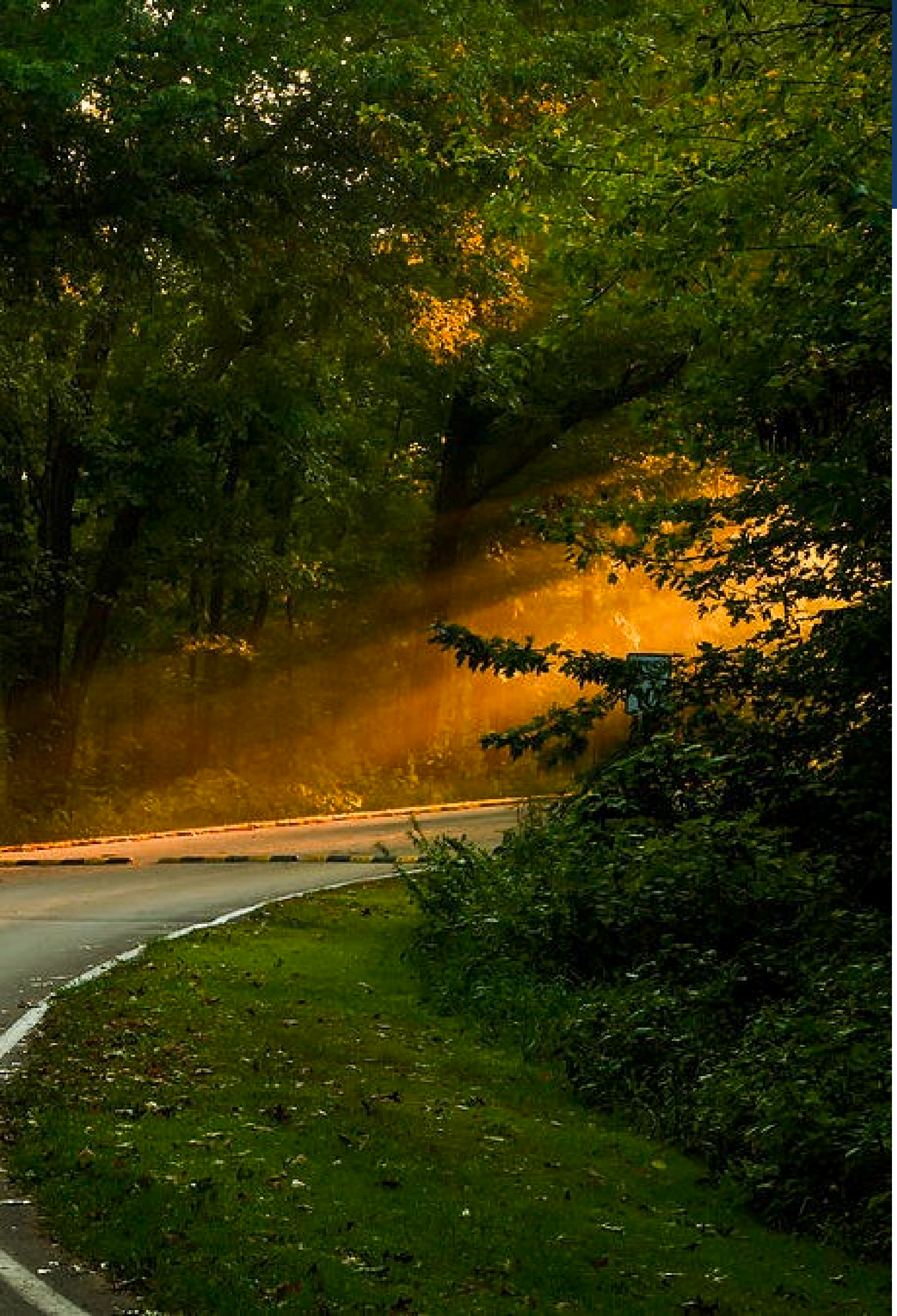
Other Challenges

- 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?
  - Transition
    - Hybrid solutions – combining classical and PQC algorithms. Allowed in SP 800-56C, Rev. 2 (Aug 2020)
    - NIST will issue more guidance in the coming years
    - NCCoE is hosting a workshop on *Considerations in Migrating to Post-Quantum Cryptographic Algorithms* on October 7

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