THE FIRST NIST PQC STANDARDS

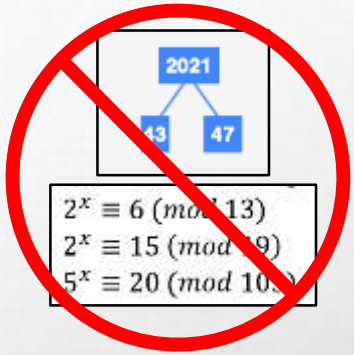
DUSTIN MOODY

(AND THE PQC TEAM)

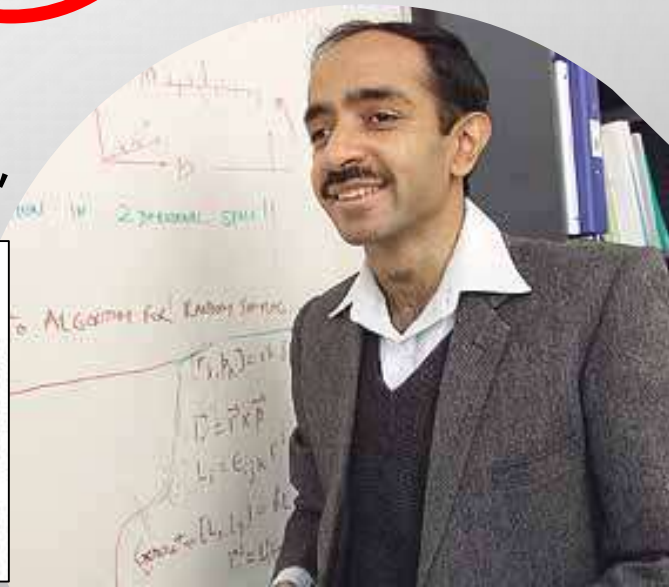
National Institute of Standards and Technology
U.S. Department of Commerce

MOTIVATION

- 1994 – SHOR'S ALGORITHM
  - A QUANTUM ALGORITHM GIVING AN EXPONENTIAL SPEED-UP OVER CLASSICAL COMPUTERS
    - FACTORING LARGE INTEGERS
    - FINDING DISCRETE LOGARITHMS



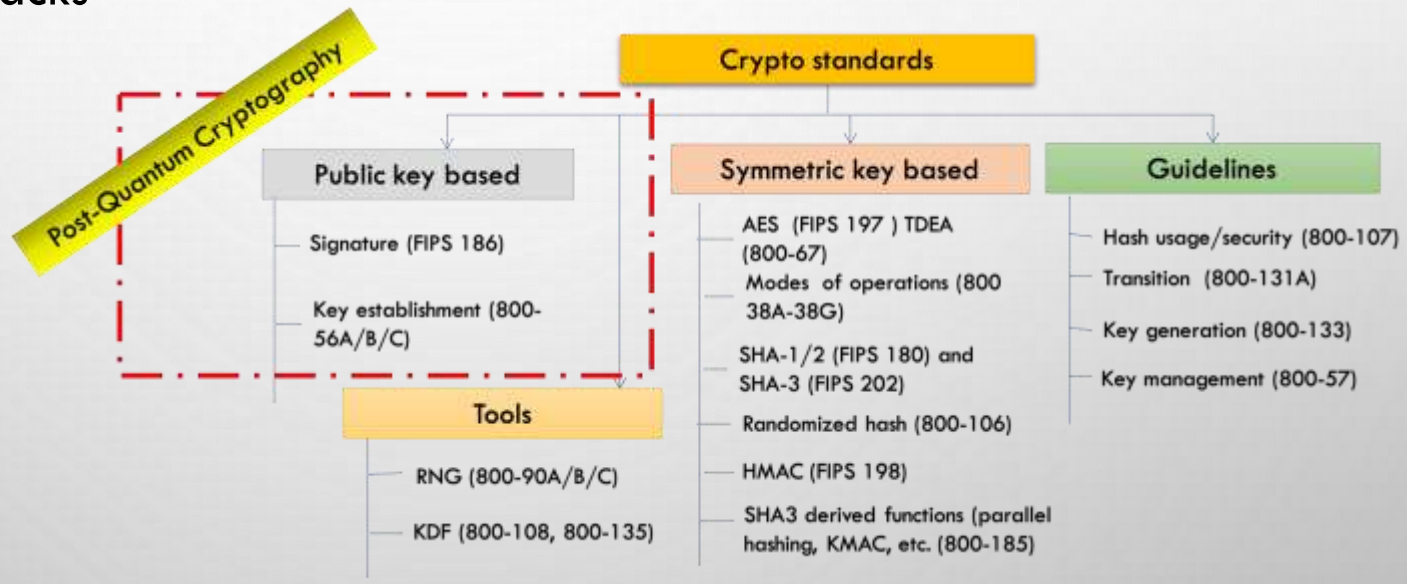
- 1996 - GROVER'S ALGORITHM
  - POLYNOMIAL SPEED-UP IN UNSTRUCTURED SEARCH, FROM O(N) TO O($\sqrt{N}$)



THE QUANTUM THREAT

- NIST public-key crypto standards
  - **SP 800-56A**: Diffie-Hellman, ECDH
  - **SP 800-56B**: RSA encryption
  - **FIPS 186**: RSA, DSA, and ECDSA signatures

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

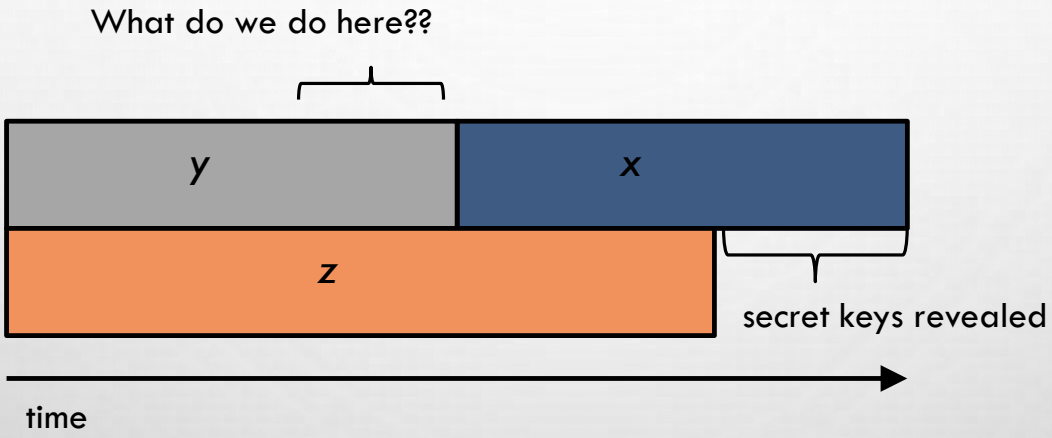


- Symmetric-key crypto (AES, SHA) would also be affected, but less dramatically

HOW SOON DO WE NEED TO WORRY?

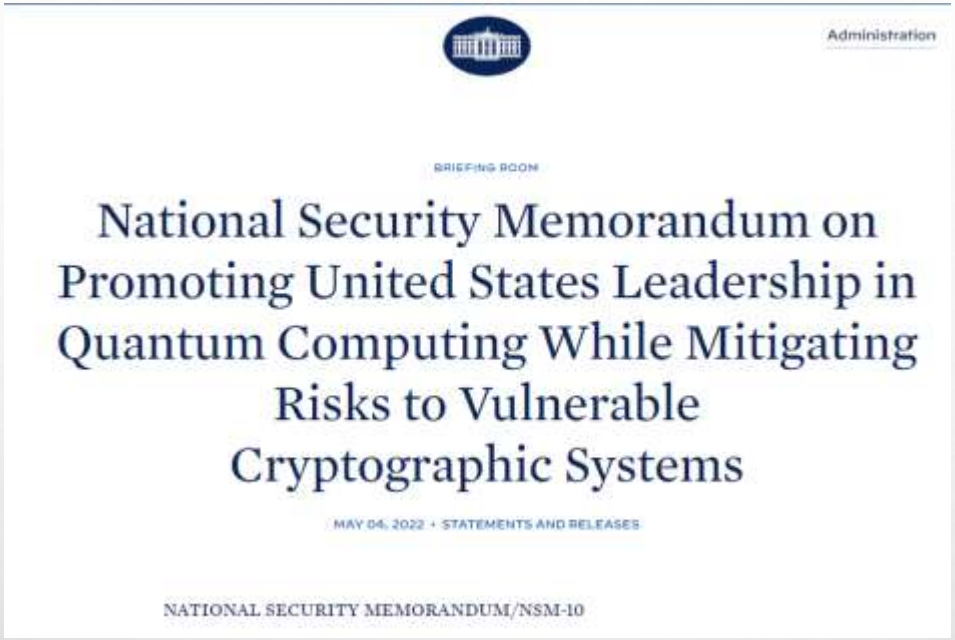
HOW SOON DO WE NEED TO WORRY?

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



x – how long data needs to be safe
y – time for standardization and adoption
z – time until quantum computers

WHITE HOUSE NATIONAL SECURITY MEMO



Administration

BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

"WITHIN 1 YEAR OF THE RELEASE OF THE FIRST SET OF NIST STANDARDS FOR QUANTUM-RESISTANT CRYPTOGRAPHY …, THE DIRECTOR OF OMB … SHALL ISSUE A POLICY MEMORANDUM REQUIRING AGENCIES TO DEVELOP A PLAN TO UPGRADE THEIR NON-NSS IT SYSTEMS TO QUANTUM-RESISTANT CRYPTOGRAPHY."

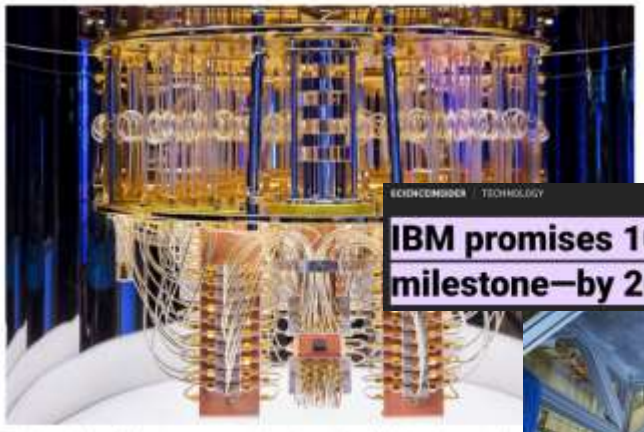
PROGRESS OF QUANTUM COMPUTING

NIST

First quantum computer to pack 100 qubits enters crowded race

But IBM's latest quantum chip and its competitors face a long path towards making the machines useful.

Philip Ball



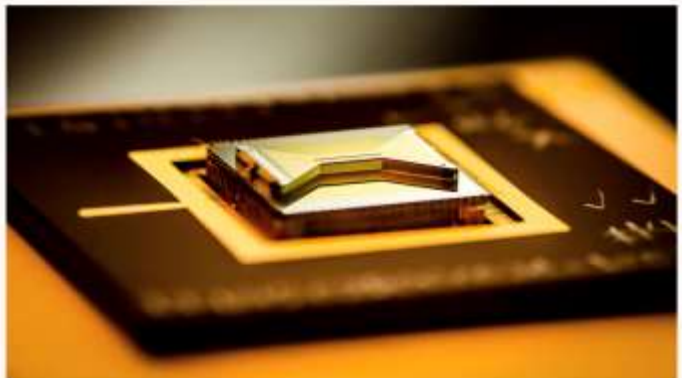
Quantum computers may be able to break Bitcoin sooner than you think

ECOMCONSIDER / TECHNOLOGY

IBM promises 1000-qubit quantum computer—a milestone—by 2023

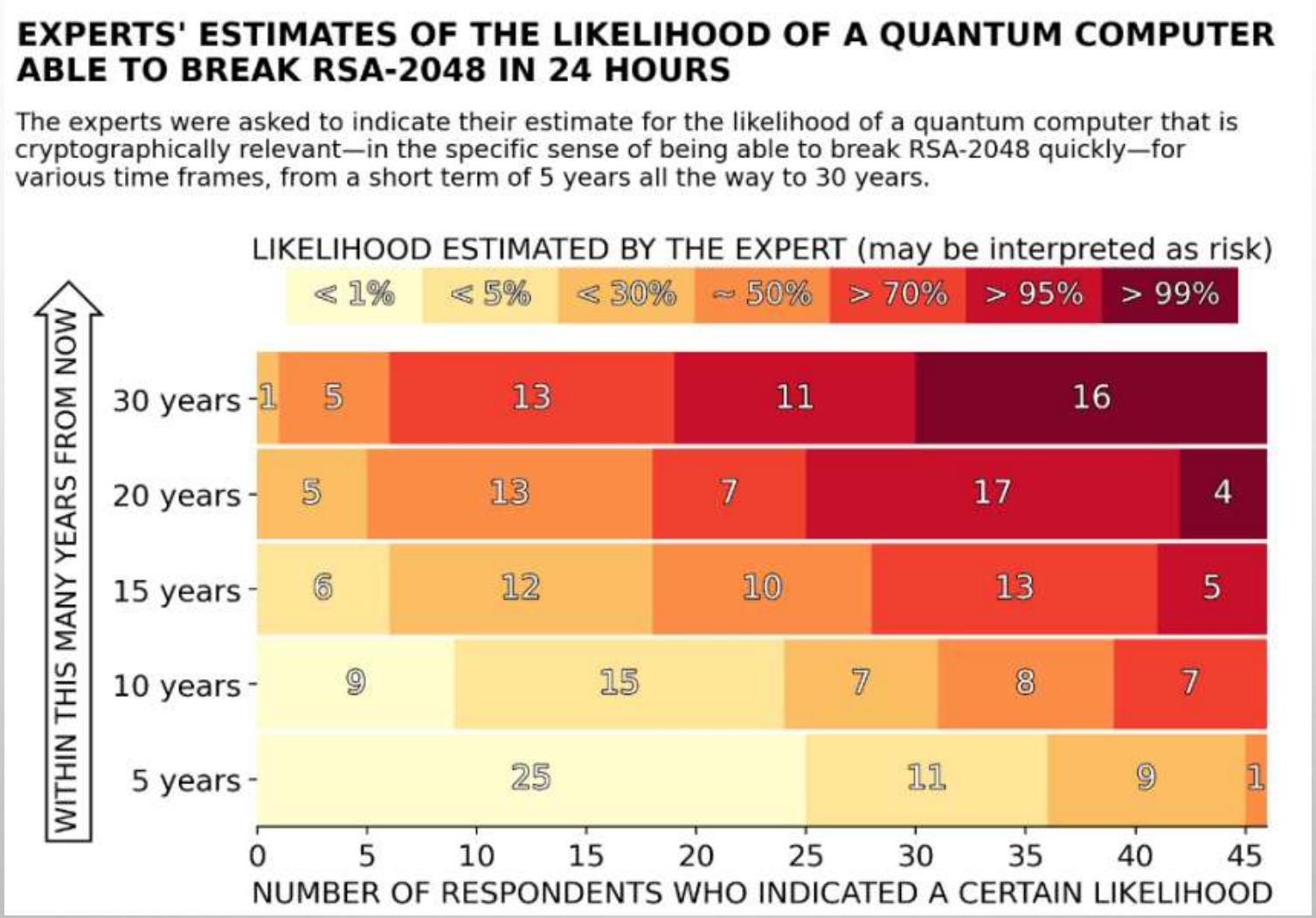
Scientists are one step closer to error-correcting quantum computers

Multiple quantum bits were combined into one 'logical qubit' to detect mistakes



Quantum computing venture backed by Jeff B will leap into public trading with $1.2B valuatic

WHEN WILL A QUANTUM COMPUTER BE BUILT?



Source: M. Mosca, M. Piani, Quantum Threat Timeline Report, 2021
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

QUANTUM CRYPTOGRAPHY AKA QKD

USING QUANTUM TECHNOLOGY TO BUILD CRYPTOSYSTEMS

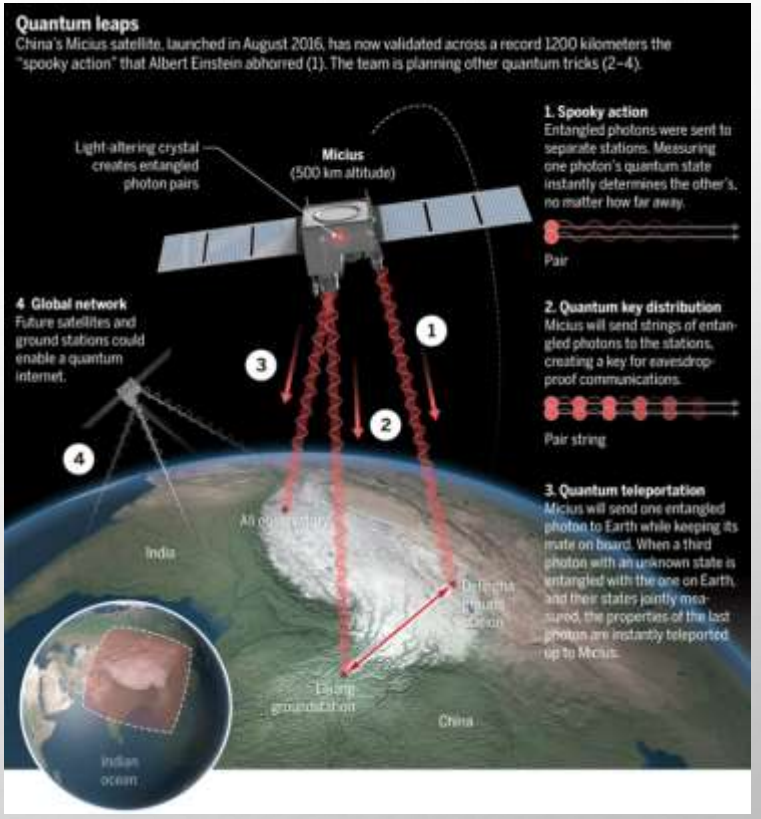
- THEORETICALLY UNCONDITIONAL SECURITY GUARANTEED BY THE LAWS OF PHYSICS

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 NOT OUR FOCUS



NIST PQC MILESTONES AND TIMELINES

2010-2015
NIST PQC project team builds
First PQC conference

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 Make 3rd round selection and draft standards

2023 Release draft standards and call for public comments

THE NIST PQC TEAM

PAST 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, 3-4 ROUNDS, 26 2ND ROUND CANDIDATES, 15 3RD ROUND FINALISTS/ALTERNATES, 2017-2022 + 2? YEARS FOR STANDARD

LIGHTWEIGHT CRYPTO

57 SUBMISSIONS, 3 ROUNDS, 32 2ND ROUND CANDIDATES, 10 FINALISTS, 2019-2022ISH

CALL FOR PROPOSALS

- NIST CALLED FOR QUANTUM-RESISTANT CRYPTOGRAPHIC ALGORITHMS FOR NEW PUBLIC-KEY CRYPTO STANDARDS
  - **DIGITAL SIGNATURES**
  - **ENCRYPTION/KEY-ESTABLISHMENT**
- OUR ROLE: MANAGING A PROCESS OF ACHIEVING COMMUNITY CONSENSUS IN A **TRANSPARENT** AND TIMELY MANNER
- DIFFERENT AND MORE COMPLICATED THAN PAST AES/SHA-3 COMPETITIONS
- WE WILL NOT PICK A SINGLE "WINNER"
  - IDEALLY, SEVERAL ALGORITHMS WILL EMERGE AS 'GOOD CHOICES'

COMPLEXITIES

- MUCH BROADER SCOPE – THREE CRYPTO PRIMITIVES
- BOTH CLASSICAL AND QUANTUM ATTACKS
- BOTH A THEORETICAL AND PRACTICAL ASPECT TO ASSESS SECURITY
- MULTIPLE TRADEOFF FACTORS (SECURITY, KEY SIZE, SIGNATURE SIZE, CIPHTERTEXT EXPANSION, SPEED, ETC.)
- MIGRATIONS INTO NEW AND EXISTING APPLICATIONS
- MANY ASPECTS WHICH WE HAVEN'T HANDLED IN PREVIOUS STANDARDS
- NOT EXACTLY A COMPETITION

SELECTION CRITERIA

1. **SECURE** AGAINST BOTH CLASSICAL AND QUANTUM ATTACKS
   - PKE/KEMS -SEMANTICALLY SECURE WITH RESPECT TO ADAPTIVE CHOSEN CIPHERTEXT ATTACK (IND-CCA2)
   - SIGNATURES - EXISTENTIALLY UNFORGEABLE WITH RESPECT TO ADAPTIVE CHOSEN MESSAGE ATTACK (EUF-CMA)

2. **PERFORMANCE** - MEASURED ON VARIOUS "CLASSICAL" PLATFORMS

3. **OTHER PROPERTIES**
   - DROP-IN REPLACEMENTS - COMPATIBILITY WITH EXISTING PROTOCOLS AND NETWORKS
   - PERFECT FORWARD SECRECY
   - RESISTANCE TO SIDE-CHANNEL ATTACKS
   - SIMPLICITY AND FLEXIBILITY
   - MISUSE RESISTANCE, AND
   - MORE

SECURITY CATEGORIES

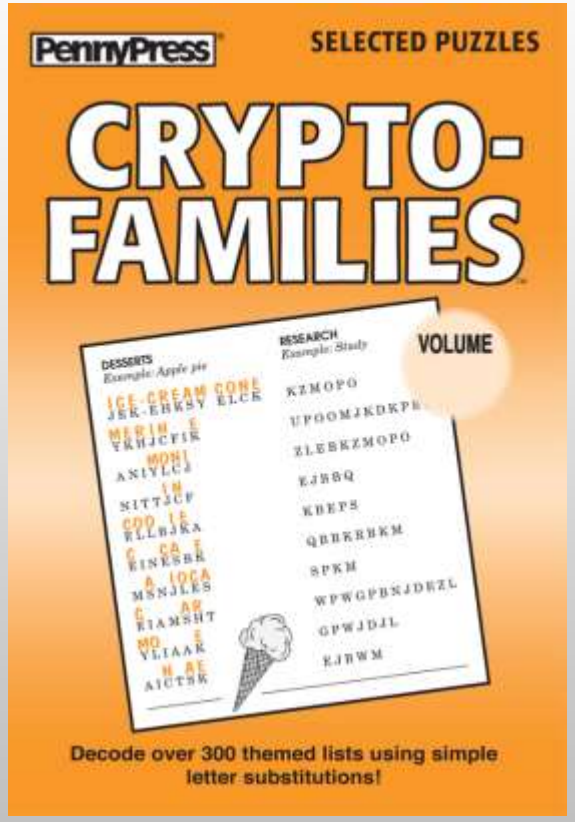
Security – against both classical and quantum attacks

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)

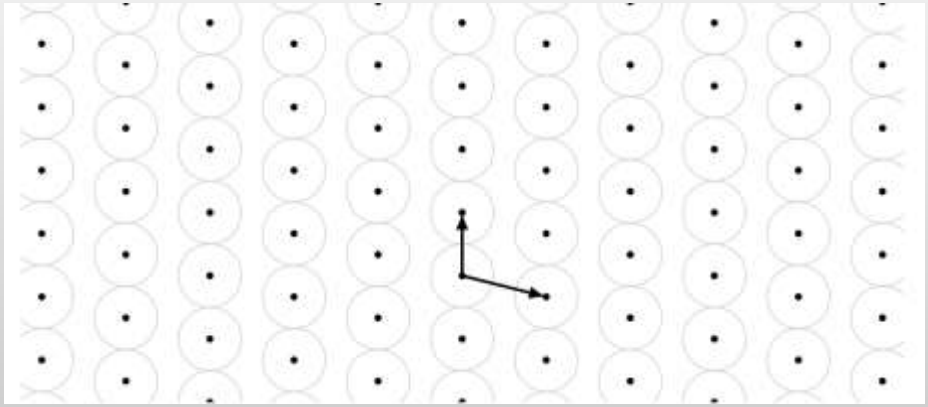
- Computational resources should be measured using a variety of metrics
  - Number of classical elementary operations, quantum circuit size, etc…
  - Consider realistic limitations on circuit depth (e.g. 2^{40} to 2^{80} logical gates)
  - May also consider expected relative cost of quantum and classical gates.

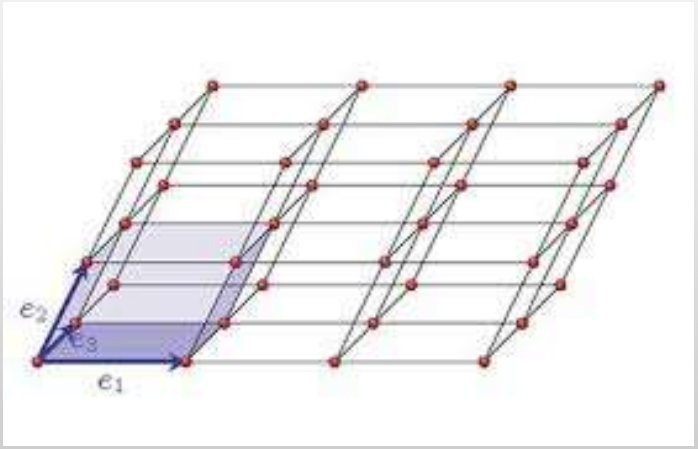
THE MAIN FAMILIES

- LATTICE-BASED CRYPTO
- CODE-BASED CRYPTO
- MULTIVARIATE CRYPTO
- ISOGENY-BASED CRYPTO
- HASH-BASED CRYPTO
- OTHER….



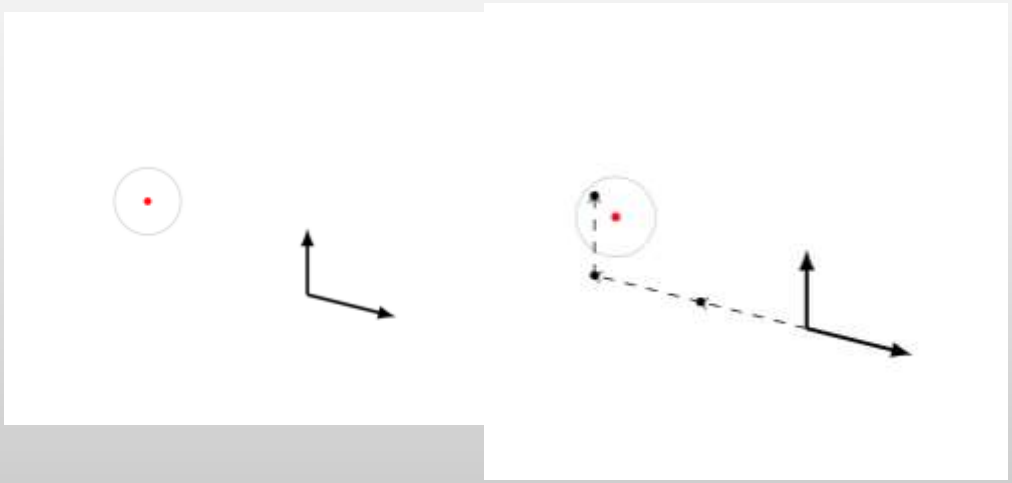
INTRO TO LATTICES

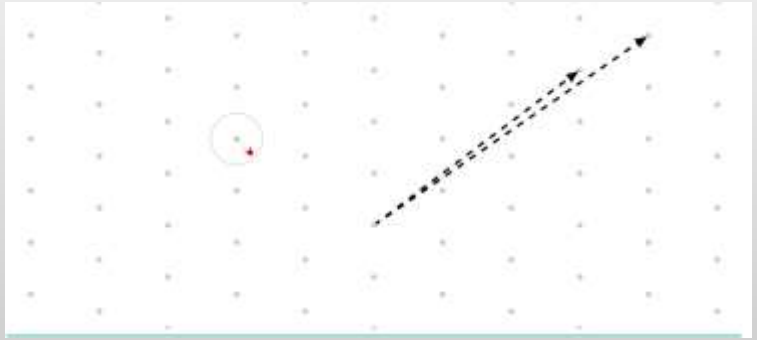




Basis vectors

GOOD AND BAD BASES





- Closest Vector Problem: Given a point, and a basis, find the closest lattice point
- The problem is much easier with a “good” basis

LINEAR ALGEBRA

- We can represent the basis vectors of a lattice as a matrix
- Writing a lattice point as a linear combination of basis vectors is then linear algebra

Solving linear systems is easy

(use Gaussian elimination, polynomial time)

- Given

$$
\begin{aligned}
1s_1 + 2s_2 + 5s_3 + 2s_4 &= 9 \, mod \, 13 \\
12s_1 + 1s_2 + 1s_3 + 6s_4 &= 7 \, mod \, 13 \\
6s_1 + 10s_2 + 3s_3 + 6s_4 &= 1 \, mod \, 13 \\
10s_1 + 4s_2 + 12s_3 + 8s_4 &= 0 \, mod \, 13 .
\end{aligned}
$$

- Find s_1, s_2, s_3, s_4

CLOSEST VECTOR PROBLEM

- Given an arbitrary point – how do find the closest lattice point?

Solving linear systems with errors is hard

- Given

$$1s_1 + 2s_2 + 5s_3 + 2s_4 \approx 9 \, mod \, 13$$
$$12s_1 + 1s_2 + 1s_3 + 6s_4 \approx 7 \, mod \, 13$$
$$6s_1 + 10s_2 + 3s_3 + 6s_4 \approx 1 \, mod \, 13$$
$$10s_1 + 4s_2 + 12s_3 + 8s_4 \approx 0 \, mod \, 13 .$$

- Find s_1, s_2, s_3, s_4 , knowing that the solution is incorrect by ± 1 ...
- The problem is called Learning With Errors (LWE)
- The associated one-way function is

$$f(s, e) = sA + e$$

Where $s = (s_1, \dots, s_4)$, A is the coefficient matrix, e is a vector of small errors

A (SIMPLIFIED) LWE CRYPTOSYSTEM

- **KEYGEN()**
  - LET *A* BE A MATRIX FOR A LATTICE. EVERYTHING HERE IS MOD Q (FOR SOME PRIME Q)
  - CHOOSE SECRET "SHORT" VECTOR *S* AND "SHORT" VECTOR *E*. COMPUTE $b = As + e$
  - THE PUBLIC KEY IS *A* AND *B*. THE SECRET KEY IS *S*
- **ENCRYPT()**
  - CHOOSE "SHORT" S' AND E',E''. COMPUTE $u = A^T s' + e'$ AND $v = b^T s' + e'' + m * [q/2]$
  - CIPHERTEXT IS (*U, V*)
- **DECRYPT()**
  - ALICE COMPUTES $v - s^T u = b^T s' + e'' + m * [q/2] - s^T(As' + e')$

$$= (As + e)^T s' + e'' + m * \left[\frac{q}{2}\right] - s^T A^T s' + s^T e'$$

$$= s^T A^T s' + e^T s' + e'' + m * \left[\frac{q}{2}\right] - s^T A^T s' + s^T e'$$

$$= m * \left[\frac{q}{2}\right] + e^T s' + e'' + s^T e'$$

  - THE ERROR IS "SMALL" SO *M* CAN BE RECOVERED

LATTICE-BASED CRYPTOSYTEMS

- A LOT OF RESEARCH WORK ON LATTICES
- A NUMBER OF CRYPTO FUNCTIONALITIES CAN BE IMPLEMENTED VIA LATTICES
- FORMAL SECURITY PROOFS TO HARD MATHEMATICAL PROBLEMS
  - THOUGH NOT FOR PARAMETERS USED IN CRYPTOSYSTEMS!
- CAN ADD STRUCTURE TO LATTICES TO REDUCE KEY SIZES
  - INCREASED AVENUE FOR ATTACKS
  - *STRUCTURED LATTICES ARE THE MOST PROMISING GENERAL-PURPOSE POST-QUANTUM CRYPTOSYSTEMS*
- EFFICIENT TO IMPLEMENT IN PRACTICE

INTRO TO CODE-BASED CRYPTO

- ERROR-CORRECTING CODES ARE USED IN TELECOMMUNICATIONS TO CORRECT ERRORS
- REPETITION CODE: ENCODE A MESSAGE $M = 10110010$ AS

$$11110000111111110000000011110000$$

- THIS CODE CAN CORRECT UP TO 1 ERROR (PER ENCODED MESSAGE BIT)
- HOW COULD WE MODIFY THE ENCODING SO IT CORRECTS MORE ERRORS?

GENERATOR MATRICES

- FOR THE REPETITION CODE, A GENERATOR MATRIX IS

- $G = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$

- REPRESENT THE MESSAGE AS A VECTOR $m = [1\ 0\ 1\ 1\ 0\ 0\ 1\ 0]$

- THEN

$$mG = [1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0]$$

- THERE EXIST MUCH MORE EFFICIENT CODES: GOPPA CODES, REED-SOLOMON CODES, ETC

- CODES HAVE DECODING ALGORITHMS, WHICH TAKE AN ARBITRARY VECTOR, AND FIND THE CLOSEST CODEWORD.

A (SIMPLIFIED) CODE-BASED ENCRYPTION SYSTEM

- **KEYGEN()**
  - ALICE CHOOSES A CODE, I.E. A GENERATOR MATRIX G WITH AN EFFICIENT DECODING ALGORITHM
  - SHE HIDES IT BY SETTING HER PUBLIC KEY TO BE $\hat{G} = SGP$, WHERE S IS INVERTIBLE, AND P IS A PERMUTATION MATRIX
- **ENCRYPT()**
  - BOB ENCRYPTS A MESSAGE M BY COMPUTING $m\hat{G}$
  - BOB SELECTS AN ERROR VECTOR E, AND THE CIPHERTEXT IS $c = m\hat{G} + e$
- **DECRYPT()**
  - ALICE COMPUTES $cP^{-1} = m\hat{G}P^{-1} + eP^{-1}$

    $= mSG + e'$
  - ALICE CAN CORRECT FOR E', OBTAINING MSG. SHE THEN DECODES TO OBTAIN MS. AS SHE KNOWS S^{-1}, SHE CAN RECOVER M

- AN ATTACKER HAS TO TRY AND FIND A DECODING ALGORITHM FROM THE SCRAMBLED GENERATOR MATRIX, WHICH APPEARS TO LOOK LIKE A RANDOM MATRIX

CODE-BASED CRYPTOSYSTEMS

- OLD: THE MCELIECE CRYPTOSYSTEM WAS PROPOSED IN 1979, AND IS STILL UNBROKEN
- MCELIECE HAS LARGE PUBLIC KEYS, BUT SMALL CIPHERTEXTS
- CAN ADD MORE STRUCTURE TO THE CODES, AND GET SMALLER KEYS
  - RUN A RISK OF ADDITIONAL STRUCTURE LEADS TO A NEW ATTACK SURFACE
- ALMOST ALL CODE-BASED SIGNATURE SCHEMES HAVE BEEN BROKEN
- IMPLEMENTATIONS ARE EFFICIENT, SINCE EVERYTHING IS LINEAR ALGEBRA
- THE IDEAS BEHIND CODE-BASED SCHEMES ARE VERY SIMILAR TO THE IDEAS IN LATTICE-BASED CRYPTO

MULTIVARIATE CRYPTO

Solving a system of m multivariate polynomial equations in n variables over $\mathbb{F}_q$.

This is called the

MP Problem

the MP problem is an *NP-Complete* problem even for multivariate *quadratic* system and $q = 2$

Example with $m = 3, n = 3$:

$$5x_1^3x_2x_3^2 + 17x_2^4x_3 + 23x_1^2x_2^4 + 13\,x_1 + 12x_2 + 5 = 0$$

$$12x_1^3x_2^3x_3 + 15x_1x_3^3 + 25x_2x_3^3 + 5\,x_1 + 6x_3 + 12 = 0$$

$$28x_1x_2x_3^4 + 14x_2^3x_3^2 + 16x_1x_3 + 32\,x_2 + 7x_3 + 10 = 0$$

It is very easy to evaluate multivariate functions

A MULTIVARIATE SIGNATURE SCHEME

- **Keygen()**
  - Choose a "random" multivariate *f* such that f^{-1} is secretly known
  - The public key is *f*. The secret key is f^{-1}
- **Signing()**
  - Given a message *m*, compute $s = f^{-1}(m)$
  - The signature is *s*
- **Verifying()**
  - Given *s*, compute $f(s) = f\left(f^{-1}(m)\right) = m$
  - Accept if you get *m* and reject otherwise

- How to choose such an *f* ?
  - Many failed attempts
  - Over $\mathbb{F}_{q^n}$, the map induced by $x \to x^q$ is a linear map. Can show $g: x \to x^{q^\alpha+1}$ is invertible for certain α. You then scramble *g* by composing it with invertible maps on the left and right.

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 CANDIDATES (1ST ROUND)

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

BREAKS AND ATTACKS

- DEC 21, 2017 – 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

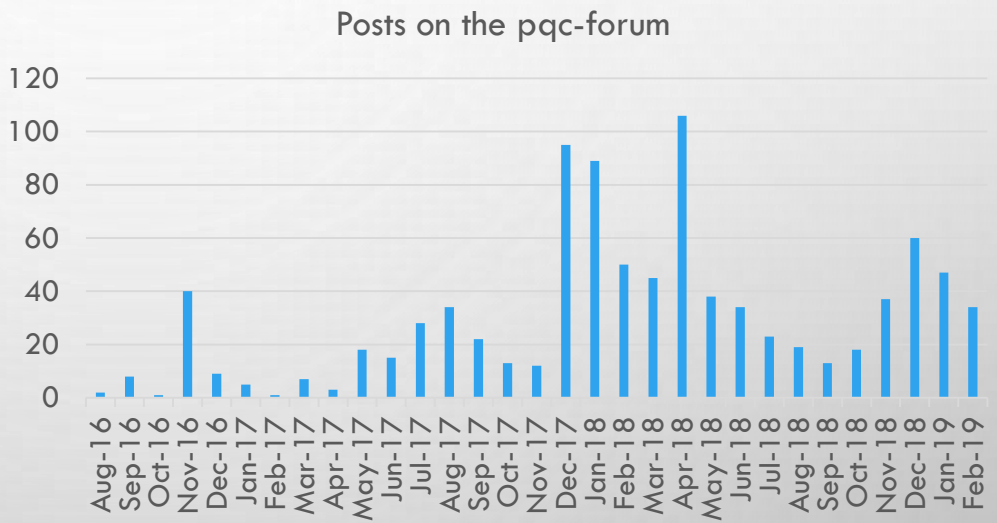
- NIST LACKED FULL CONFIDENCE IN SECURITY OF:
  - CFPKM, COMPACT-LWE, DAGS, DME, DRS, GUESSAGAIN, GIOPHANTUS, LEPTON, MCNIE, PQSIGRM, RACOSS, RLCE, WALNUT-DSA

THE PQC-FORUM

SIGN UP AT WWW.NIST.GOV/PQCRYPTO

OFFICIAL CHANNEL FOR ANNOUNCEMENTS AND DISCUSSION OF NIST PQC

- 2000+ MEMBERS
- 1000'S OF POSTS
  - SOME WITH OVER 5000 VIEWS
- VERY, VERY ACTIVE



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						

THE 2ND ROUND

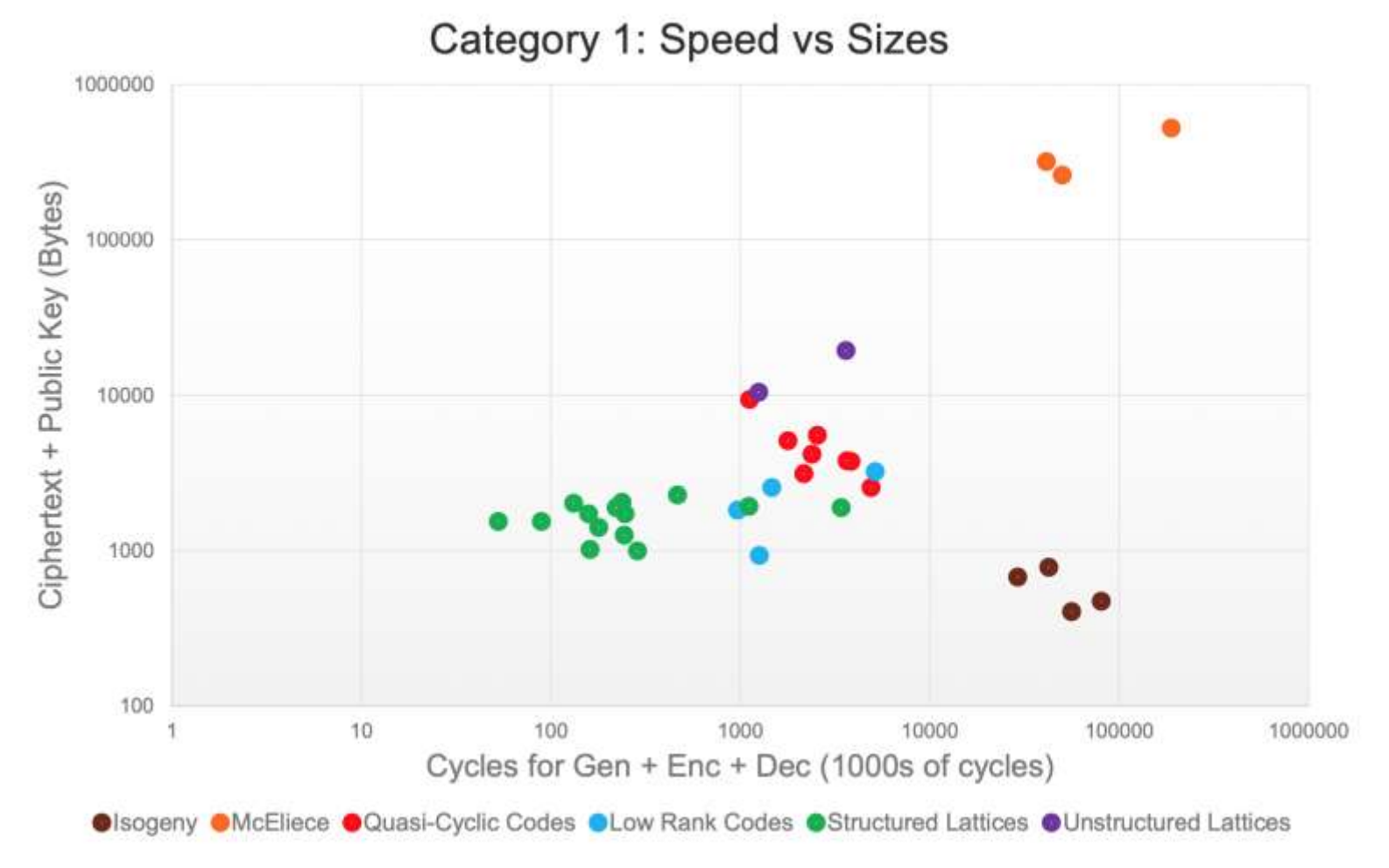
- 4 MERGED SUBMISSIONS
- MAINTAINED DIVERSITY OF ALGORITHMS
- CRYPTANALYSIS CONTINUES
- LEDACRYPT, RQC, ROLLO, MQDSS, QTESLA, LUOV, LAC: ALL BROKEN
- 2ND NIST PQC STANDARDIZATION WORKSHOP
- MORE BENCHMARKING AND REAL WORLD EXPERIMENTS

- AFTER 18 MONTHS:

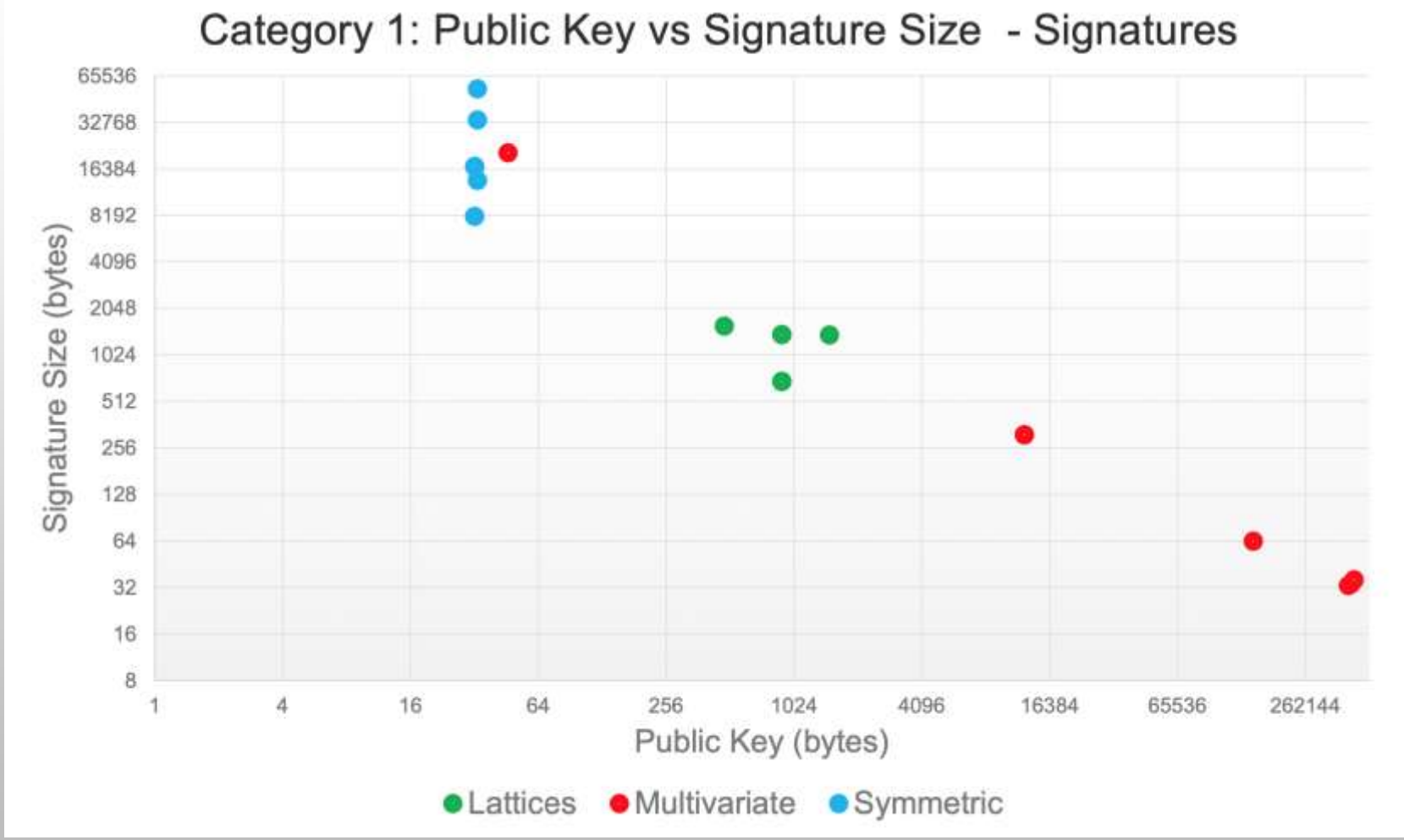
  15 SUBMISSIONS MOVE ON

	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	**9**	**17**	**26**

ANY KEMS TOO SLOW?



LARGE PUBLIC KEYS OR SIGNATURES



THE ONES MOVING ON

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~~

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~~

Eliminated in RED
Alternates in ORANGE
Finalists w/ arrows

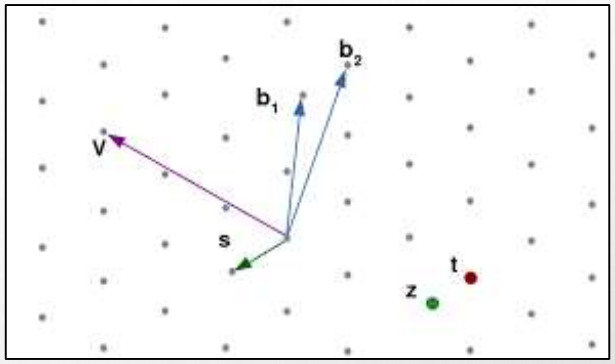
THE 3RD ROUND FINALISTS AND ALTERNATES

- NIST SELECTED 7 FINALISTS AND 8 ALTERNATES
  - **FINALISTS**: MOST PROMISING ALGORITHMS WE EXPECT TO BE READY FOR STANDARDIZATION AT END OF 3RD ROUND
  - **ALTERNATES**: CANDIDATES FOR POTENTIAL STANDARDIZATION, MOST LIKELY AFTER ANOTHER (4TH) ROUND

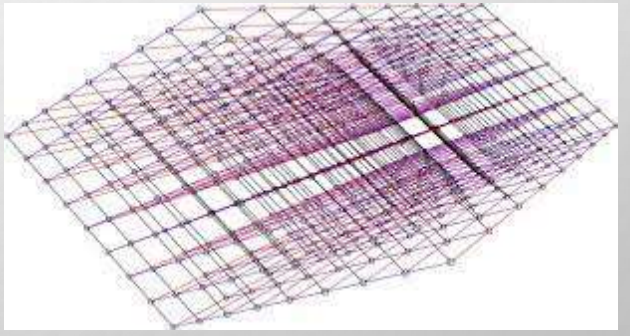
	FINALISTS	ALTERNATES
KEMs/Encryption	Kyber NTRU SABER Classic McEliece	BIKE FrodoKEM HQC NTRU Prime SIKE
Signatures	Dilithium Falcon Rainbow	GeMSS Picnic SPHINCS+

THE LATTICE KEMS

- THE FINALISTS **KYBER, NTRU, SABER** ARE BASED ON STRUCTURED LATTICES
  - KYBER AND SABER ARE BASED ON MODULE-LWE/LWR
  - NTRU IS BASED ON THE NTRU PROBLEM
  - ALL THREE HAVE GOOD PERFORMANCE (IN TERMS OF EFFICIENCY AND KEY/CIPHERTEXT SIZES)
  - *NIST EXPECTS TO SELECT AT MOST ONE FOR STANDARDIZATION*

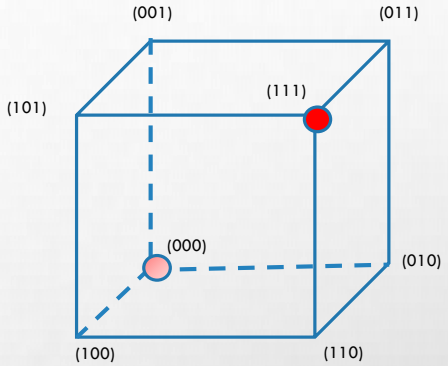


- THE ALTERNATES **NTRU PRIME** AND **FRODOKEM** ARE BASED ON LATTICES
  - NTRUPRIME USES STRUCTURED LATTICES, WHILE FRODOKEM DOES NOT



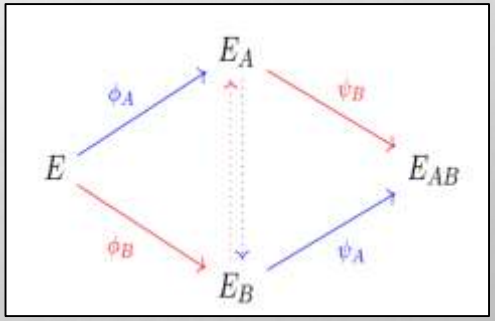
THE OTHER KEMS

- **CLASSIC MCELIECE**, THE OTHER FINALIST, IS CODE-BASED
  - BEEN AROUND SINCE 1978
  - VERY LARGE PUBLIC KEYS, BUT VERY SMALL CIPHERTEXTS



- THE ALTERNATES **BIKE** AND **HQC** ARE BASED ON STRUCTURED CODES
  - BOTH HAVE MUCH SMALLER KEY SIZES THAN CLASSIC MCELIECE

- THE FINAL ALTERNATE **SIKE** IS BASED ON ISOGENIES OF ELLIPTIC CURVES
  - SMALL KEY/CIPHERTEXT SIZES, SLOWER THAN OTHER CANDIDATES



THE SIGNATURES

- THE FINALISTS **DILITHIUM** AND **FALCON** ARE BOTH BASED ON STRUCTURED LATTICES
  - DILITHIUM IS FIAT-SHAMIR STYLE, WHILE FALCON IS HASH THEN SIGN
  - BOTH HAVE GOOD PERFORMANCE

- THE ALTERNATE **PICNIC** IS BASED ON ZERO-KNOWLEDGE PROOFS AND A BLOCK CIPHER
- THE ALTERNATE **SPHINCS+** IS BASED ON THE SECURITY OF HASH FUNCTIONS
  - THE SECURITY OF SPHINCS+ IS VERY WELL UNDERSTOOD
  - SPHINCS+ IS STATELESS

- THERE ARE TWO MULTIVARIATE SCHEMES: THE FINALIST **RAINBOW**, AND THE ALTERNATE **GEMSS**
  - BOTH HAVE LARGE PUBLIC KEYS, AND VERY SMALL SIGNATURE SIZES

THE STATE OF THE SIGNATURES

- CRYPTANALYTIC RESULTS DURING THE 3RD ROUND HAVE CREATED SOME CONCERNS ABOUT THE SECURITY OF BOTH MULTIVARIATE SCHEMES **RAINBOW** AND **GEMSS**

- BEULLENS RECENTLY POSTED A NEW ATTACK ON **RAINBOW**
  - BREAKS CATEGORY 1 PARAMETERS IN "A WEEKEND ON A LAPTOP"
  - SERVES AS A REMINDER TO NOT PUT CANDIDATES INTO PRODUCTS UNTIL THE STANDARD IS DONE

- IN JAN 2021, NIST ASKED FOR FEEDBACK ON TWO TOPICS:
  - STANDARDIZING SPHINCS+ AFTER 3RD ROUND
  - INTRODUCING A MECHANISM TO CONSIDER NEW SIGNATURE SCHEMES

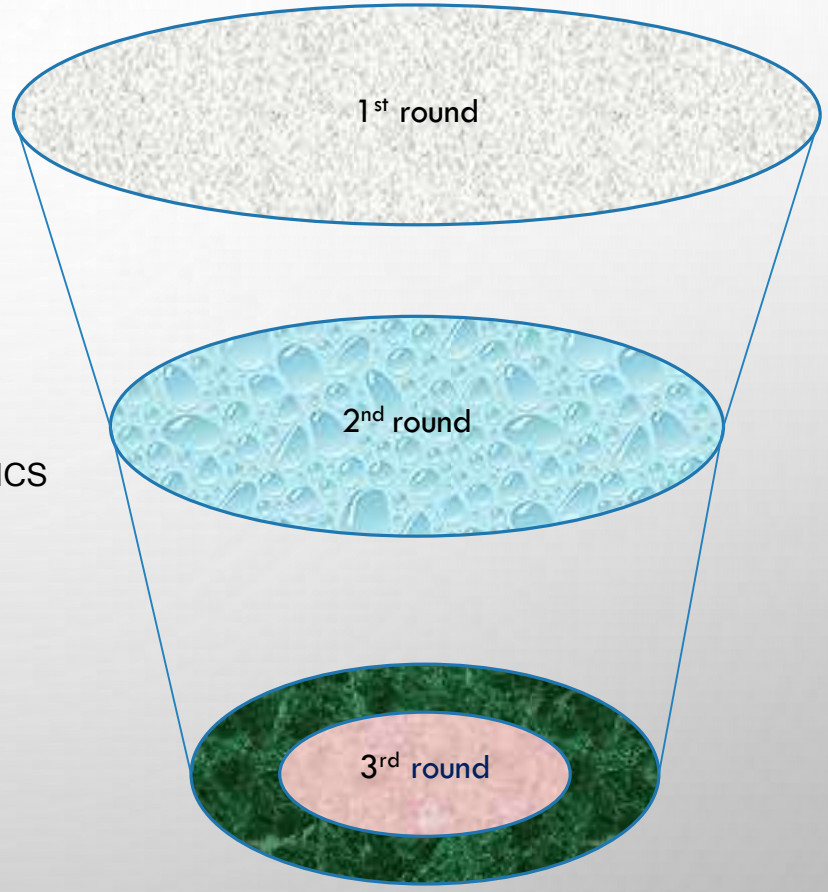
ATTACKS IN THE 3RD ROUND

- NOV 2020 – GEMSS ATTACK
  - ALL PARAMETER SETS FALL BELOW SECURITY LEVEL 1
- FEB 2022 – RAINBOW ATTACK
  - "BREAKING RAINBOW TAKES A WEEKEND ON A LAPTOP" (FOR CATEGORY 1)
- APR 2022 – ATTACK ON STRUCTURED LATTICE SCHEMES
  - RELEVANT TO KYBER, SABER, DILITHIUM, AND LIKELY NTRU
- APR 2022 – ATTACK ON SPHINCS+
  - AFFECTS CATEGORY 5 PARAMETERS USING SHA-256

HOW WILL NIST MAKE ITS DECISIONS?

USING THE EVALUATION CRITERIA:

- SECURITY
  - SECURITY LEVELS OFFERED
  - (CONFIDENCE IN) SECURITY PROOF
  - ANY ATTACKS
  - CLASSICAL/QUANTUM COMPLEXITY
- PERFORMANCE
  - SIZE OF PARAMETERS
  - SPEED OF KEYGEN, ENC/DEC, SIGN/VERIFY
  - SOFTWARE AND HARDWARE BENCHMARKS
- ALGORITHM AND IMPLEMENTATION CHARACTERISTICS
  - IP ISSUES
  - DECRYPTION FAILURES
  - SIDE CHANNEL RESISTANCE
  - SIMPLICITY AND CLARITY OF DOCUMENTATION
  - FLEXIBLE
- OTHER
  - OFFICIAL COMMENTS/PQC-FORUM DISCUSSION
  - PAPERS PUBLISHED/PRESENTED



HOW WILL NIST MAKE ITS DECISIONS?

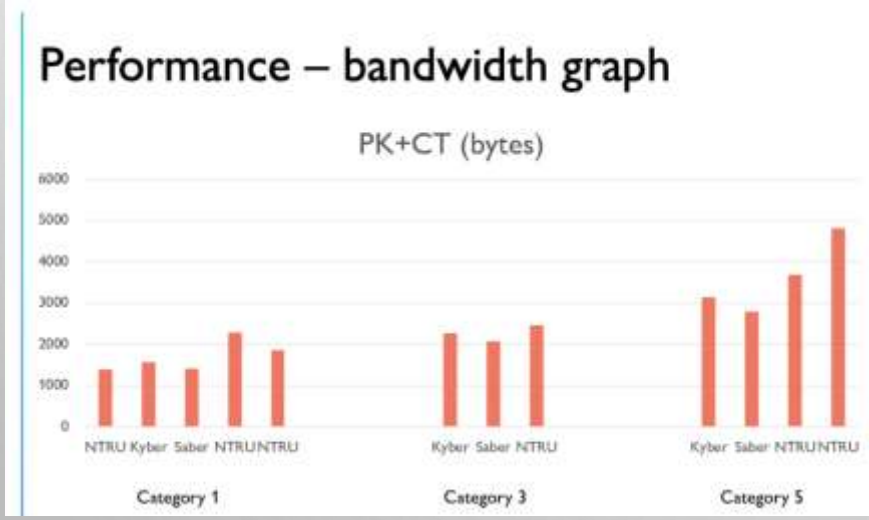
- FOR THE LATTICE KEMS, THE MAIN DECISION WILL BE **KYBER/NTRU/SABER**
- SIMILARLY FOR LATTICE SIGNATURES, THE MAIN DECISION WILL BE **DILITHIUM/FALCON**
- ANY OTHER ALGORITHMS SELECTED WILL BE THEIR OWN DISTINCT DECISION
  - OTHER FINALISTS: CLASSIC MCELIECE AND RAINBOW
  - KEM ALTERNATES: BIKE, HQC, FRODOKEM, NTRUPRIME, SIKE
  - SIGNATURE ALTERNATES: GEMSS, PICNIC, SPHINCS+

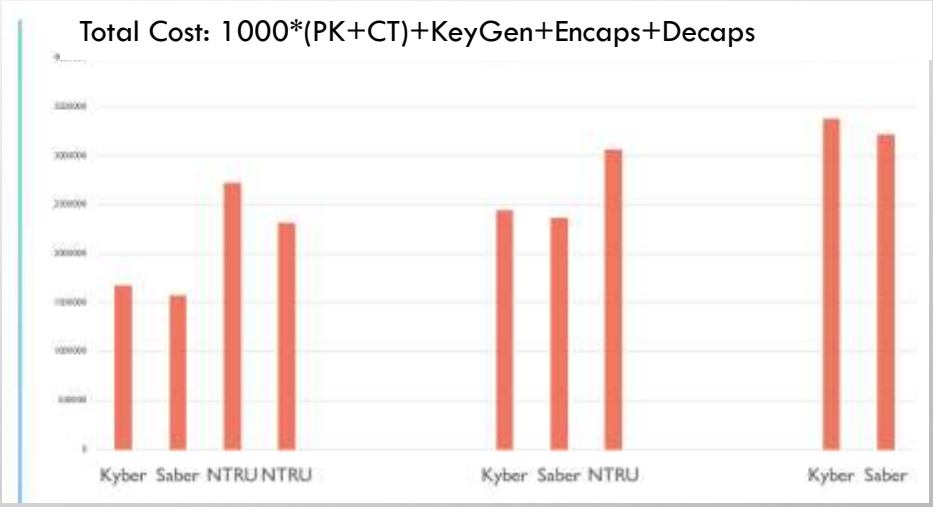
KYBER VS NTRU VS SABER

- Kyber and Saber based on Module-Learning With Errors/Rounding
- NTRU is based on NTRU problem

- Each has an IND-CCA2 proof, constructed from PKEs using some type of Fujisaka-Okamoto transform
  - Kyber and Saber have decryption failure, NTRU does not

- Kyber, Saber use modules with ring $\mathbb{Z}_q[x]/\left\langle x^{2^k}+1\right\rangle$, NTRU uses ring $\mathbb{Z}_q[x]/\langle x^p-1\rangle$

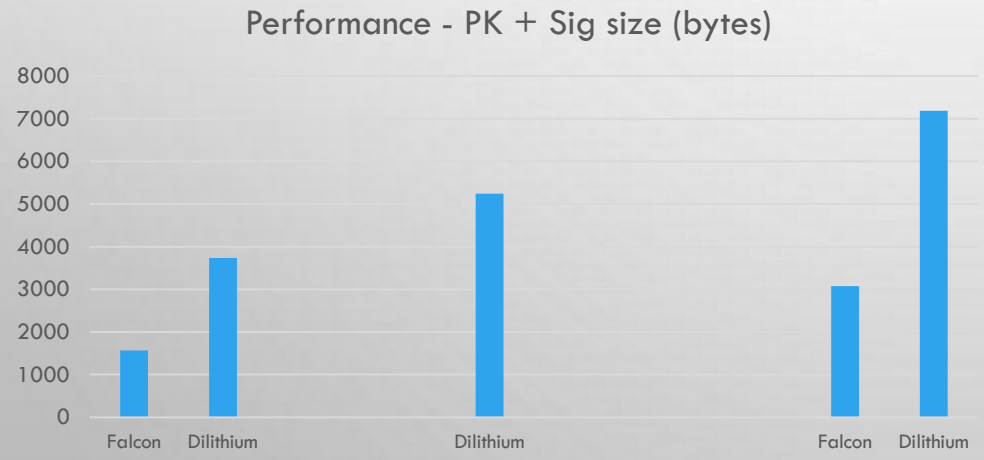




Software – AVX2 processor

DILITHIUM VS FALCON

- DILITHIUM IS BASED ON MODULE-LWE, FALCON IS BASED ON SIS OVER NTRU LATTICES
- DILITHIUM USES FIAT-SHAMIR WITH ABORTS, UNIFORM SAMPLING
- FALCON USES HASH-THEN-SIGN PARADIGM, GAUSSIAN SAMPLING.
  - FALCON HAS A VERY COMPLEX IMPLEMENTATION, KEYGEN IS COMPARATIVELY SLOW
- BOTH USE RINGS OF THE FORM $\mathbb{Z}_q[x]/\langle x^{2^k}+1\rangle$
- EACH HAS AN EUF-CMA PROOF



Software – AVX2 processor

PATENT AND IPR ISSUES

- **"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.*"**

- 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

TIMELINE

- The 3rd Round will end any day now!
  - NIST will announce which finalist algorithms it will standardize
    - Including potentially the alternate 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 18-24 months
  - These algorithms will be for a diversified portfolio
- We'll likely hold a workshop in winter 2022
- We plan to release draft standards for public comment in 2022-2023
- The first set of standards should be finalized by 2024

STANDARDIZATION

- NIST'S PUBLIC-KEY CRYPTO IS STANDARDIZED IN:
  - FIPS 186-5, DIGITAL SIGNATURES
  - SP 800-56A, 800-56B, ENCRYPTION/KEY-ESTABLISHMENT
- NIST WILL CREATE NEW STANDARDS, IN CONSULTATION WITH THE CANDIDATE TEAMS
  - NIST WILL DETERMINE WHICH SPECIFIC PARAMETER SETS TO INCLUDE, AND GIVE THEIR SECURITY STRENGTH
  - NIST WILL SEEK FEEDBACK FROM COMMUNITY, IF NEEDED
- THE DRAFT STANDARDS WILL BE PUT OUT FOR PUBLIC COMMENT
  - FEEDBACK RECEIVED WILL BE MADE PUBLIC
  - NIST WILL MAKE ANY NECESSARY REVISIONS AND THEN PUBLISH THE STANDARD

AN ON-RAMP FOR SIGNATURES

- After the conclusion of the 3rd Round, NIST will issue a new Call for Signatures
  - There will be a deadline for submission, in early 2023
  - 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

RESEARCH CHALLENGES

- MANY IMPORTANT TOPICS 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)
    - MORE GENERALLY, WHAT COST MODELS SHOULD WE BE USING TO MEASURE ATTACKS?
  - ARE THERE ANY IMPORTANT ATTACK AVENUES THAT HAVE GONE UNNOTICED?
  - SIDE-CHANNEL ATTACKS/RESISTANT IMPLEMENTATIONS
  - MORE HARDWARE IMPLEMENTATIONS
  - EASE OF IMPLEMENTATIONS – DECRYPTION FAILURES, FLOATING POINT ARITHMETIC, NOISE SAMPLING, ETC.
  - ALGEBRAIC CRYPTANALYSIS OF CYCLOTOMICS FOR LATTICES

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))

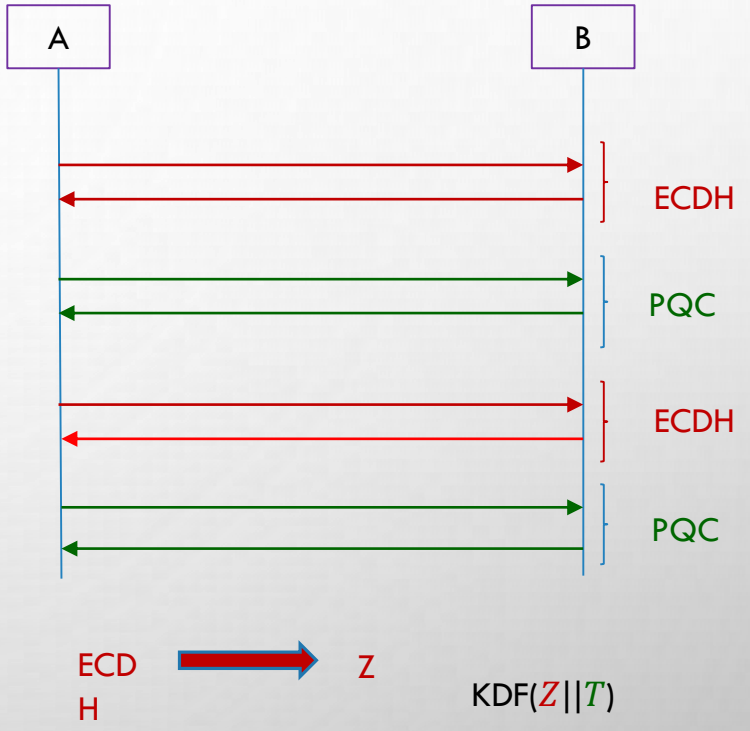
ISO/IEC JTC 1 SC27 WG2 Project on hash-based signatures

- 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

- 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 recently teamed up with the Dept. of Homeland Security in this effort.
- 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

OTHER STANDARDS ORGANIZATIONS

- WE ARE AWARE THAT MANY STANDARDS ORGANIZATIONS AND EXPERT GROUPS ARE WORKING ON PQC
  - IEEE P1363.3 HAS STANDARDIZED SOME LATTICE-BASED SCHEMES
  - IETF HAS STANDARDIZED STATEFUL HASH-BASED SIGNATURES LMS/XMSS
  - ETSI HAS RELEASED QUANTUM-SAFE CRYPTOGRAPHY REPORTS
  - EU EXPERT GROUPS PQCRYPTO AND SAFECRYPTO MADE RECOMMENDATIONS AND RELEASED REPORTS
  - ISO/IEC JTC 1 SC27 HAD A STUDY PERIOD FOR QUANTUM-RESISTANT CRYPTOGRAPHY AND RELEASED A STANDING DOCUMENT (SD)
- NIST IS INTERACTING AND COLLABORATING WITH THESE ORGANIZATIONS AND GROUPS
- SOME COUNTRIES HAVE BEGUN STANDARDIZATION ACTIVITIES

CONCLUSION

- THE BEGINNING OF THE END IS HERE!
- 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