Post-Quantum Cryptography Standardization, As Driven by NIST, Summarized

Kris Gaj

George Mason University

CERG
Cryptographic Engineering Research Group
cryptography.gmu.edu

Thank You!

Great thanks to

Prof. Bertrand Cambou

& the entire VICEROY Symposium Organizing Committee

for the kind invitation

to give this talk!

CERG: Cryptographic Engineering Research Group

CERG
Cryptographic Engineering
Research Group

- 3 faculty members
- 7 Ph.D. students
- 5 MS students
- 10 affiliated scholars

Recent and Current CERG Group Members supporting PQC

Recent Graduates

Farnoud

SW/HW Codesign

RTL Accelerators

Experimental Setup for Timing Measurements

CAD Tools

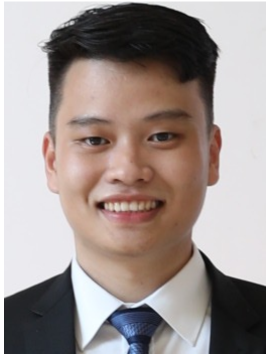
Apple

Bakry

Experimental Setup for Side-Channel Analysis

Lightweight Architectures

PQSecure



Viet

RTL Design of HW Accelerators for Lattice-based & Code-based PQC

Qualcomm

PhD Students

Duc

HLS Design of HW Accelerators for Lattice-based PQC

NEON-based SW implementations

Kamyar

RTL Design of HW Accelerators for Lattice-based PQC

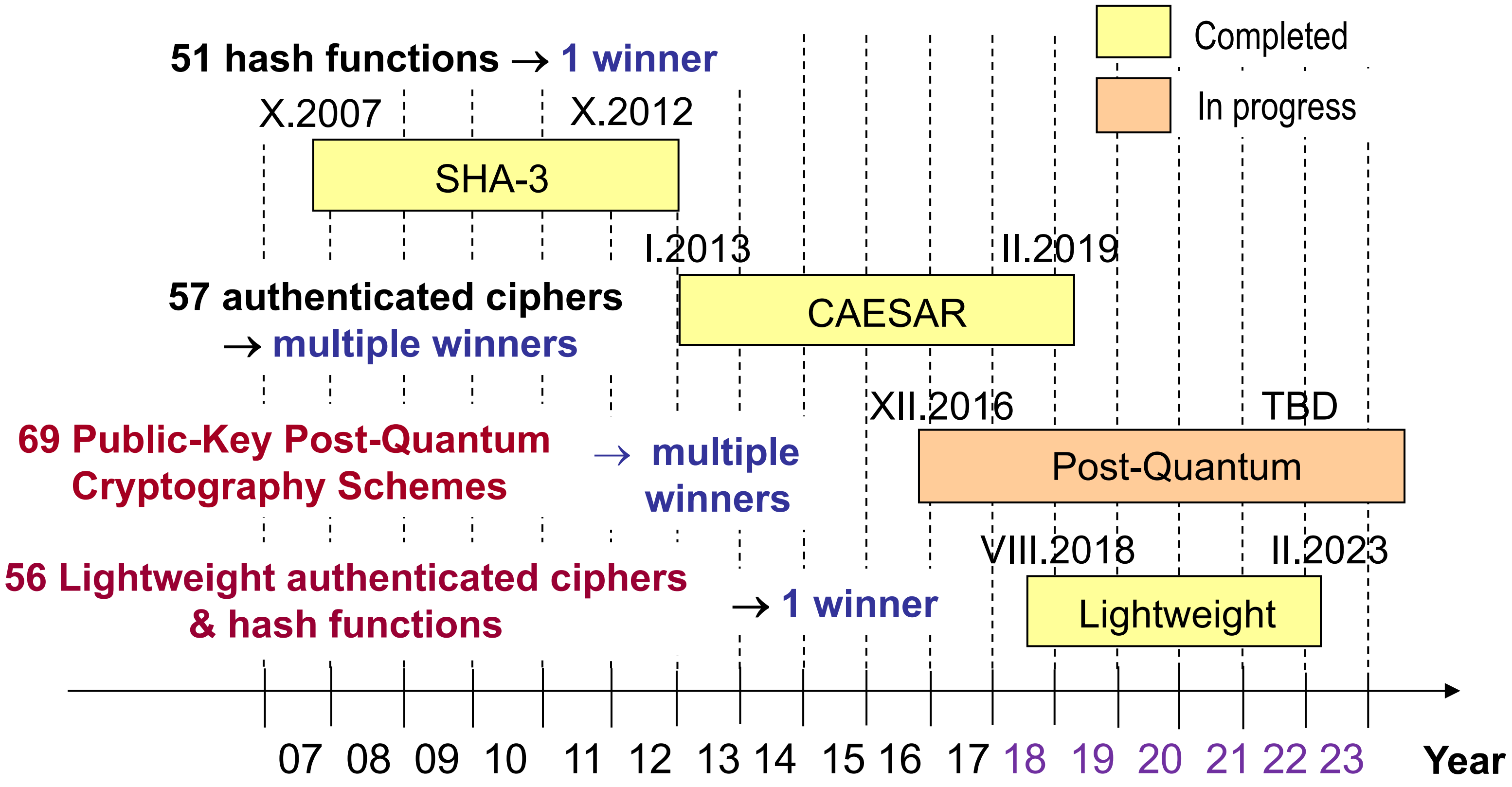
Side-Channel Analysis

Luke

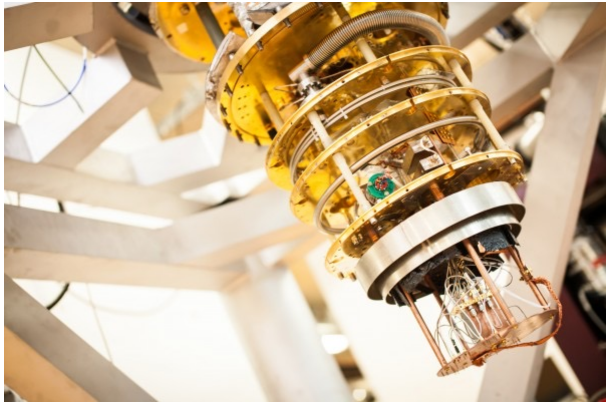
RTL Design of HW Accelerators for Lattice-based PQC

Power & Energy Measurements

CERG Participation in Cryptographic Contests 2007-Present



Quantum Computers



- Substantial investments by: Google, IBM, Intel, Microsoft, and governments of multiple countries

- Jan 2018: Intel’s 49-qubit “Tangle Lake” processor
- Mar 2018: Google’s 72-qubit “Bristlecone” processor
- 2020-2021: Three quantum computers developed at the University of Science and Technology of China reach quantum supremacy
- Nov 2022: IBM’s 433-qubit “Ospray” processor

Photos: https://www.technologyreview.com

Source: https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication

Development Roadmap | Executed by IBM ✓ On target

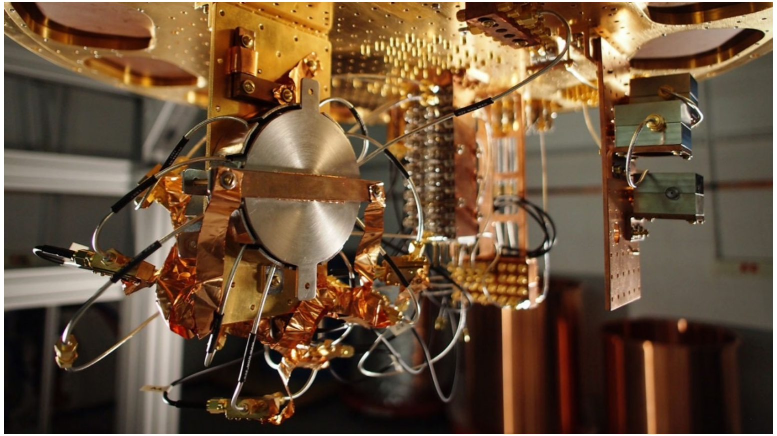
IBM 2022Roadmap

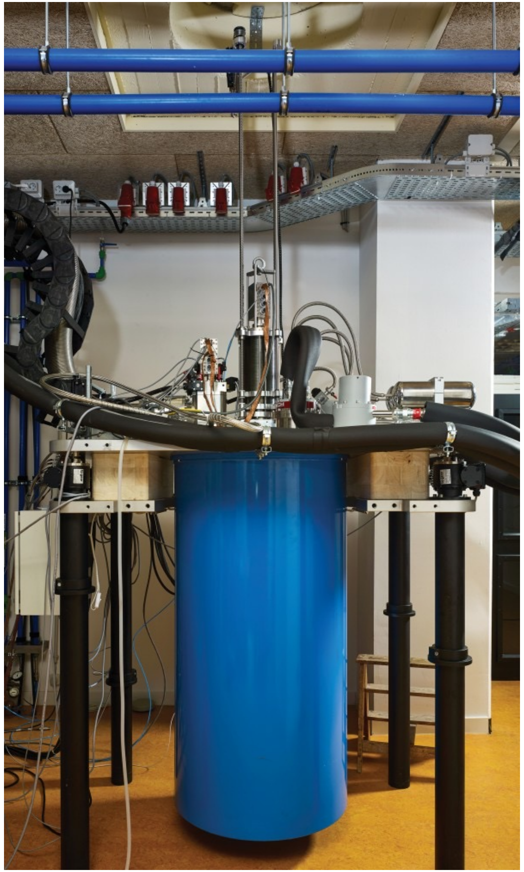
IBM **Quantum**

	2019 ✓	2020 ✓	2021 ✓	2022 ✓	2023	2024	2025	2026+
	Run quantum circuits on the IBM cloud	Demonstrate and prototype quantum algorithms and applications	Run quantum programs 100x faster with Qiskit Runtime	Bring dynamic circuits to Qiskit Runtime to unlock more computations	Enhancing applications with elastic computing and parallelization of Qiskit Runtime	Improve accuracy of Qiskit Runtime with scalable error mitigation	Scale quantum applications with circuit knitting toolbox controlling Qiskit Runtime	Increase accuracy and speed of quantum workflows with integration of error correction into Qiskit Runtime
Model Developers					Prototype quantum software applications →		Quantum software applications Machine learning | Natural science | Optimization	
Algorithm Developers		Quantum algorithm and application modules ✓ Machine learning | Natural science | Optimization			Quantum Serverless	Intelligent orchestration	Circuit Knitting Toolbox	Circuit libraries
Kernel Developers	Circuits ✓		Qiskit Runtime ✓	Dynamic circuits ✓	Threaded primitives	Error suppression and mitigation		Error correction
System Modularity	Falcon ✓ 27 qubits	Hummingbird ✓ 65 qubits	Eagle ✓ 127 qubits	Osprey ✓ 433 qubits	Condor 1,121 qubits	Flamingo 1,386+ qubits	Kookaburra 4,158+ qubits	Scaling to 10K-100K qubits with classical and quantum communication
					Heron 133 qubits x p	Crossbill 408 qubits		

Source: https://www.ibm.com/quantum/roadmap

Progress in Quantum Computing



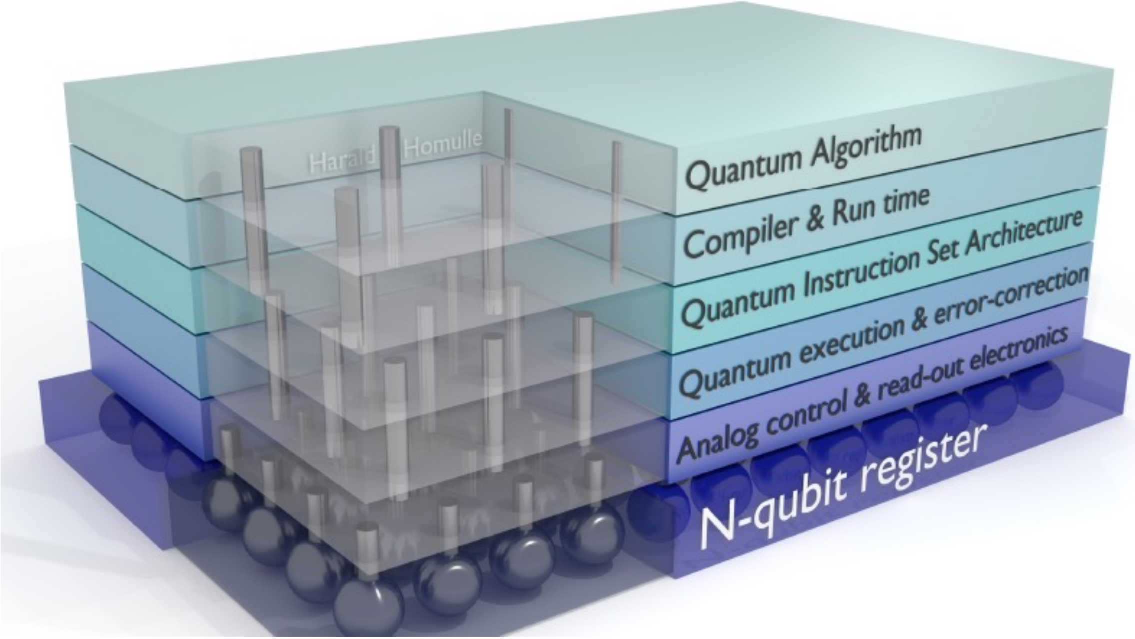


Google and IBM quantum computers based on superconducting circuits operating in the temperature close to absolute 0 (~0.01 K)

Photos: https://www.technologyreview.com

System Layer Approach

Challenges in each layer **Layers are highly interrelated**



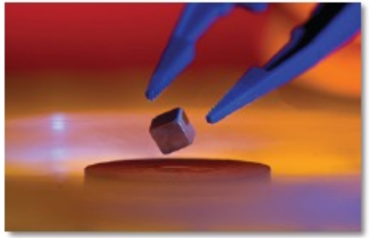
Source: Vandersypen, PQCrypto 2017

What Quantum Computers Can Do?

Model complex molecules

Health: Quantum chemistry for medicine

Model complex materials



Energy: Room-temperature superconductivity

Solve complex math problems

Security: factoring and code breaking

Nobel 2012 citation: *"The quantum computer may **change our everyday lives** in this century in the same radical way as the classical computer did in the last century."*

Source: Vandersypen, PQCrypto 2017

Best known attack using quantum computers

1996: Grover's Algorithm, reduces the time of the exhaustive-key search for secret key ciphers

from 2^k to $2^{k/2}$ operations, for a k-bit key,

e.g., from 2^{128} to 2^{64} operations, for a 128-bit key or

from 2^{256} to 2^{128} operations, for a 256-bit key

assuming

a sufficiently powerful and reliable quantum computer available

Easy Countermeasure: Double the size of a key

Effect on Public-Key Cryptography

1994: Shor's Algorithm, breaks major public key cryptosystems based on

Factoring:	RSA
Discrete logarithm problem (DLP):	DSA, Diffie-Hellman
Elliptic Curve DLP:	Elliptic Curve Cryptosystems

independently of the key size

assuming

a sufficiently powerful and reliable quantum computer available

Bases of the traditional public cryptosystems security

	Factorization	**Discrete Logarithm**	**Elliptic Curve Discrete Logarithm**
Given:	$\mathbf{N} = p \cdot q$	$\mathbf{y} = \mathbf{g}^x \bmod \mathbf{p} =$ $= \underbrace{g \cdot g \cdot g \cdot \ldots \cdot g}_{x \text{ times}}$ constants **p, g**	$\mathbf{Q} = x \cdot \mathbf{P} =$ $= \underbrace{P+P+\ldots+P}_{x \text{ times}}$ **P** - point of an elliptic curve
Unknown:	**p, q**	**x**	**x**

Underlying Mathematical Problem - RSA

N =P*Q (P, Q random primes)

214032465024074496126442307283933356300861471514475501779775492
088141802344714013664334551909580467961099285187247091458768739
626192155736304745477052080511905649310668769159001975940569345
7452230589325976697471681738069364894699871578494975937497937

=

641352894770715802787901901705773890848250147429434472081168596
32024532344630238623598752668347708737661925585694639798853367

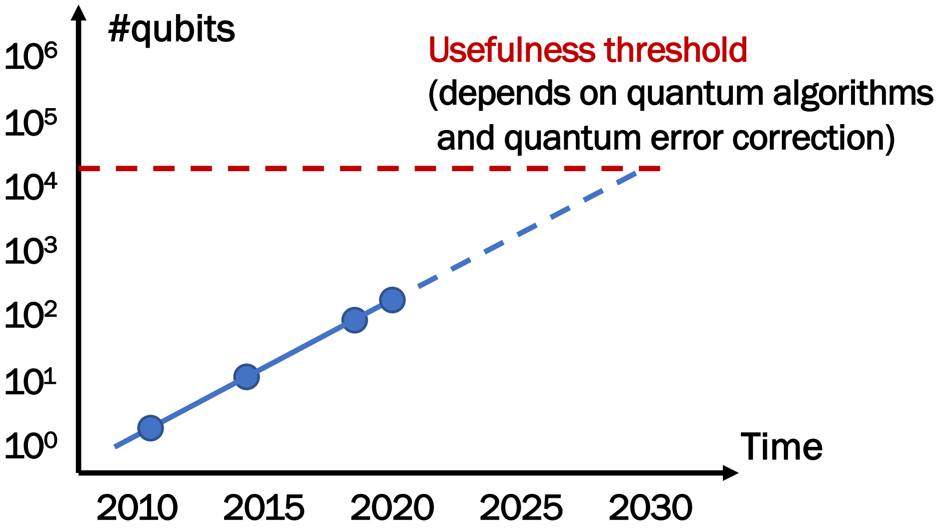
*

333720275949781565562260106053551142279407603447675546667845209
87023841729210037080257448673296881877565718986258036932062711

Record Using Classical Computers, 250 decimal digits, 829 bits

Announced on February 28, 2020

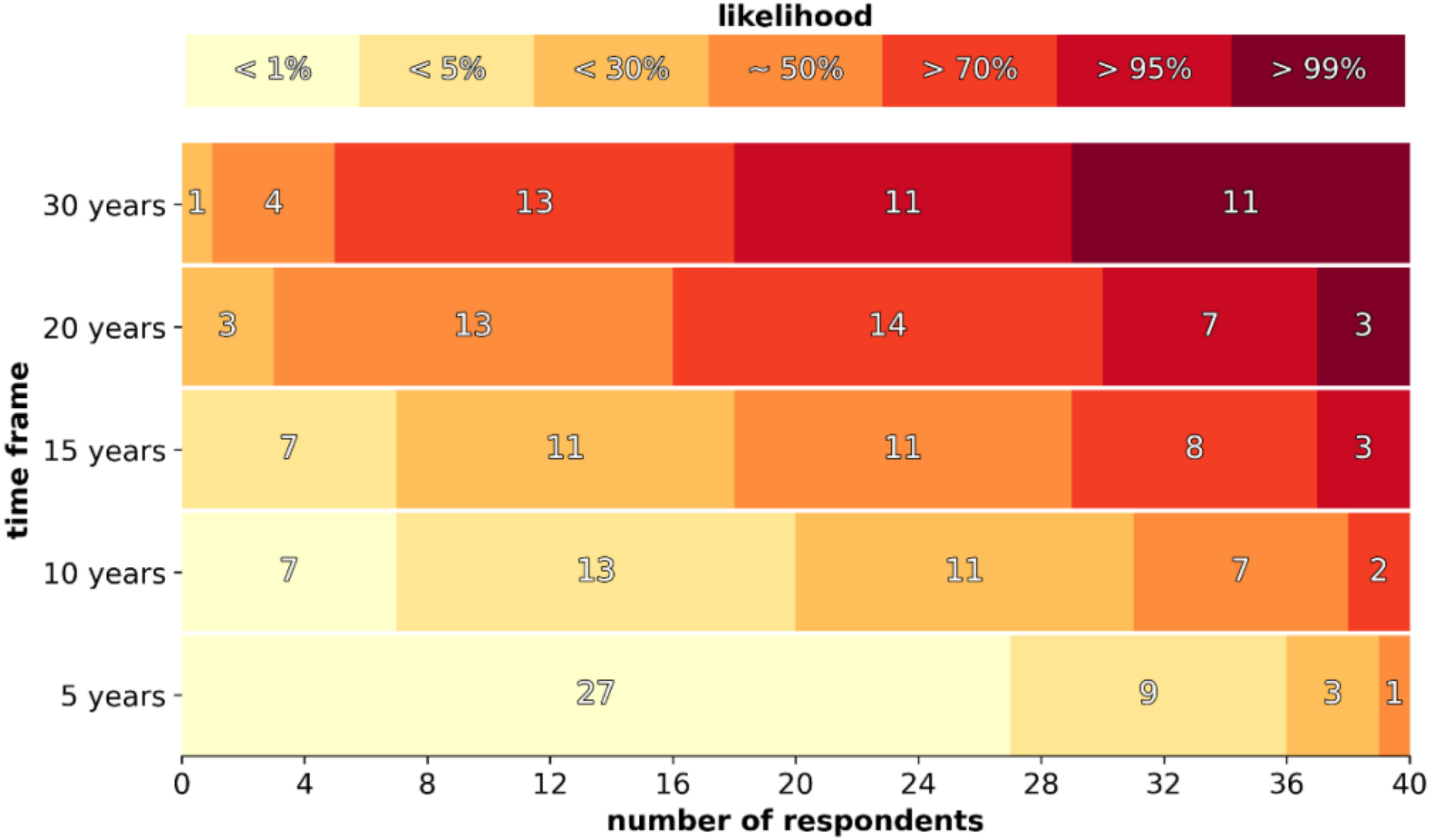
How Real Is the Danger?



"There is a 1 in 5 chance that some fundamental public-key crypto will be broken by quantum by 2029."
Dr. Michele Mosca
Deputy Director of the Institute for Quantum Computing, University of Waterloo
2020

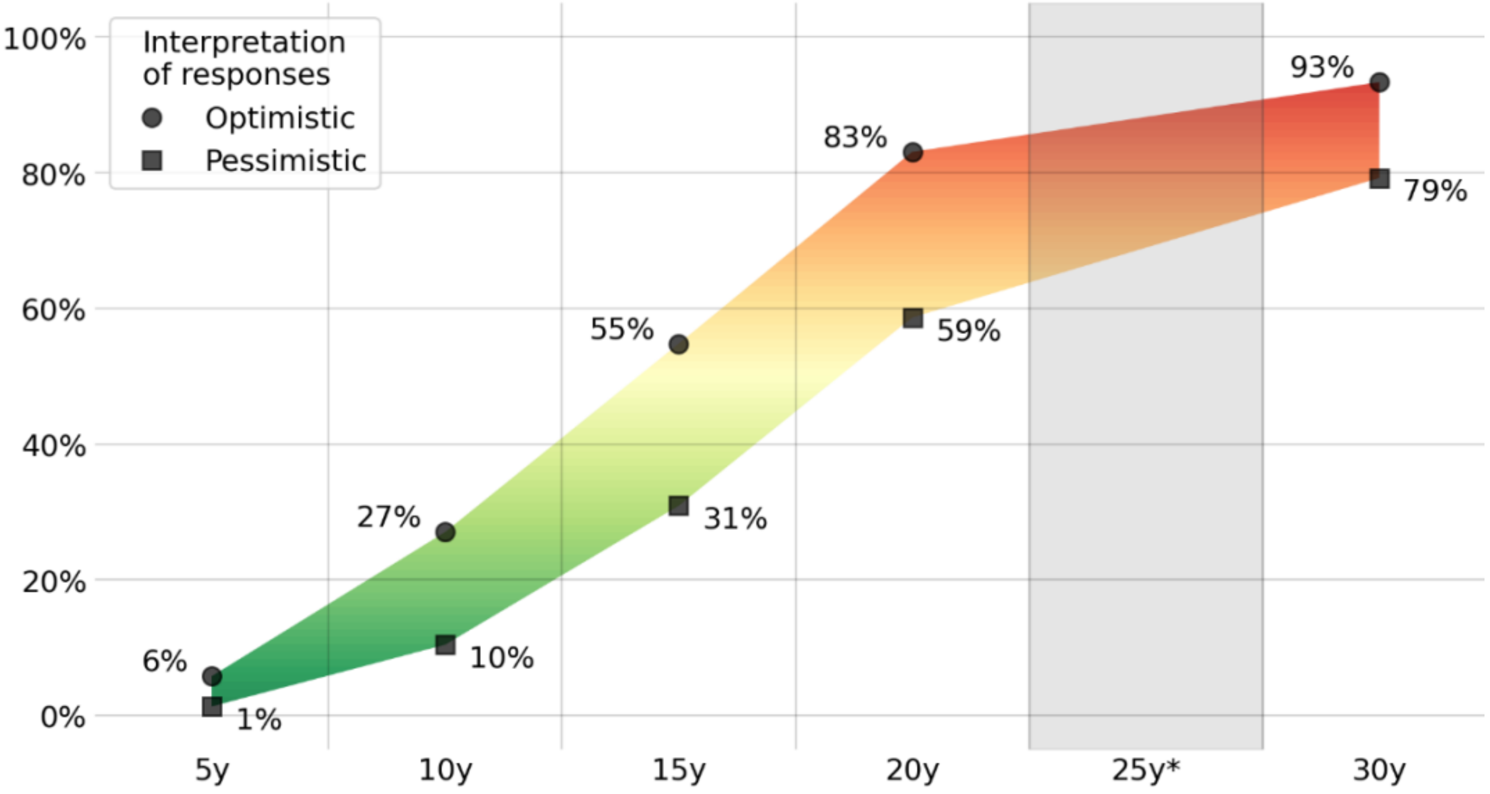
Source: Vandersypen, PQCrypto 2017; Lily Chen, seminar, 2020

2022 Experts' Estimates of Likelihood of a Quantum Computer Able to Break RSA-2048 in 24 hours



Source: 2022 Quantum Threat Timeline Report, https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report

2022 Opinion-Based Estimates of the Probability of a Quantum Computer Being Able to Break RSA-2048 in 24 hours



Source: 2022 Quantum Threat Timeline Report, https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report

“Theorem” by Mosca

If $z < y + x$, then worry!

y – Time to Develop & Deploy New Standards

x – Time Information Must Remain Protected

z – Time to Build Quantum Computers

Encrypted Data Stored by Powerful Adversaries

No Announcement when Quantum Computer Available to NSA, Foreign Governments, or Organized Crime

Post-Quantum Cryptography (PQC)

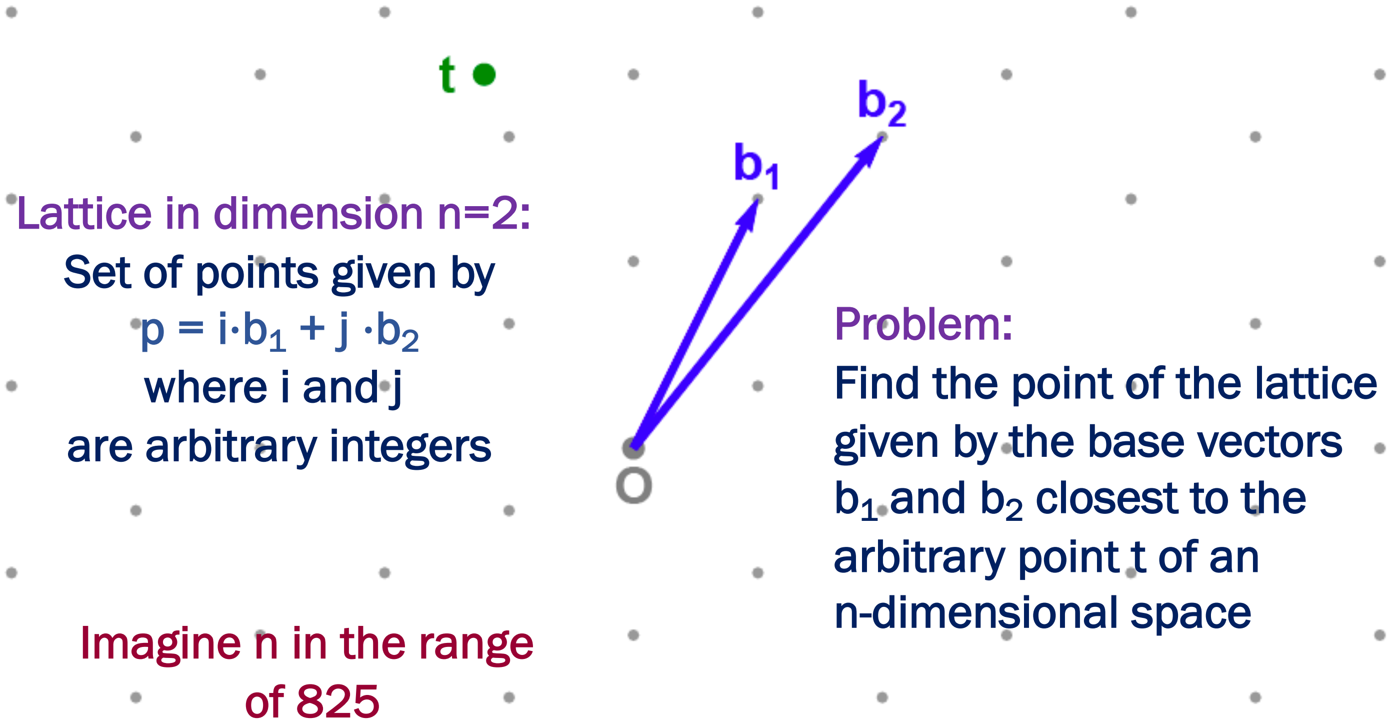
- Public-key cryptographic algorithms for which there are no known attacks using quantum computers

  - Capable of being implemented using any traditional methods, including software and hardware
  - Running efficiently on any modern computing platforms: PCs, tablets, smartphones, servers with FPGA accelerators, etc.

- Based entirely on traditional semiconductor VLSI technology!

The biggest revolution in cryptography, since the invention of public-key cryptography in 1970s!!!

Closest Vector Problem



Lattice in dimension n=2:

Set of points given by

$p = i \cdot b_1 + j \cdot b_2$

where i and j

are arbitrary integers

Problem:

Find the point of the lattice given by the base vectors b_1 and b_2 closest to the arbitrary point t of an n-dimensional space

Imagine n in the range of 825

Underlying Mathematical Problem – Multivariate PQC

Solving a system of *m* quadratic equations with *n* unknowns

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

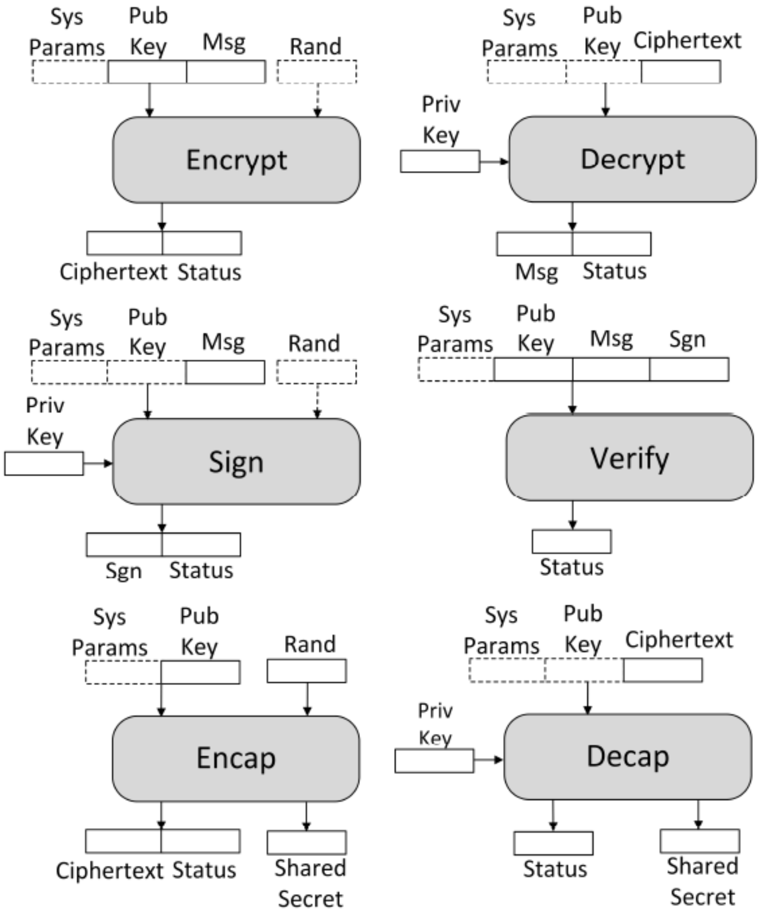
$$p^{(2)}(x_1,\ldots,x_n) = \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)} \cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)} \cdot x_i \left(+p_0^{(2)}\right)$$

$$\vdots$$

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

Imagine *m* and *n* in the range of 70 and above

Three Types of PQC Schemes



1. Public Key Encryption

2. Digital Signature

3. Key Encapsulation Mechanism (KEM)

Five Security Levels

Level	Security Description
1	At least as hard to break as AES-128 using exhaustive key search
2	At least as hard to break as SHA-256 using collision search
3	At least as hard to break as AES-192 using exhaustive key search
4	At least as hard to break as SHA-384 using collision search
5	At least as hard to break as AES-256 using exhaustive key search

Leading PQC Families

Family	Encryption/ KEM	Signature
Symmetric-based		XX
Code-based	XX	X
Lattice-based	XX	XX
Multivariate	X	XX
Isogeny-based	X	

XX – high-confidence candidates, X – medium-confidence candidates

Two Major Types of Schemes & Corresponding Families

Post-Quantum
Public Key Exchange

Post-Quantum
Digital Signatures

Lattice-based

Code-based

Symmetric-based

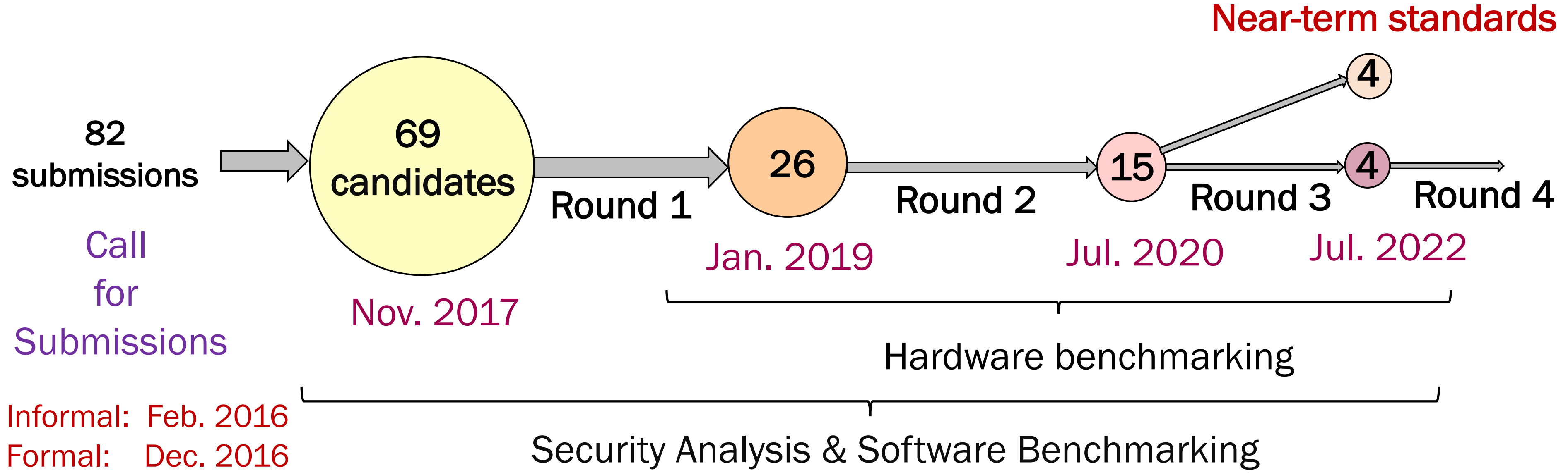
Isogeny-based

Multivariate

Informal Call for Submissions – PQCrypto 2016

Fukuoka, Japan, February 24-26, 2016

NIST PQC Standardization Process



Round 1 Submissions as of May 2018

- 69 Submissions accepted to Round 1, 26 Countries, 278 co-authors

BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. DAGS. Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. 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. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqNTRUSign. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some attack scripts already posted causing **total break** or **serious tweaks**. Many more receiving detailed analysis.

Round 1 Candidates

69 accepted as complete, 5 withdrawn within the first 6 months

Family	Signature	Encryption/KEM	Overall
Lattice-based	5	21	26
Code-based	2	17	19
Multivariate	7	2	9
Symmetric-based	3		3
Isogeny-based		1	1
Other	2	4	6
Total	19	45	64

Round 2 Candidates (announced Jan. 30, 2019)

- Lattice-based
- Code-based
- Isogenies

- Encryption/KEMs (17)

- CRYSTALS-KYBER
- FrodoKEM
- LAC
- NewHope
- NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM)
- NTRU Prime
- Round5 (merger of Hila5/Round2)
- SABER
- Three Bears

9

- BIKE
- Classic McEliece
- HQC
- LEDAcrypt (merger of LEDAkem/pkc)
- NTS-KEM
- ROLLO (merger of LAKE/LOCKER/Ouroboros-R)
- RQC

7

- SIKE

1

- Digital Signatures (9)

- Lattice-based
- Symmetric-based
- Multivariate

- CRYSTALS-DILITHIUM
- FALCON
- qTESLA

3

- Picnic
- SPHINCS+

2

- GeMSS
- LUOV
- MQDSS
- Rainbow

4

NIST Report on the 1st Round: https://doi.org/10.6028/NIST.IR.8240

Sources: Moody, PQCrypto May 2019

Round 3 Candidates (announced July 22, 2020)

FINALISTS

Encryption/KEM

- Lattice-based
  - CRYSTALS-KYBER
  - NTRU
  - SABER
- Code-based
  - Classic McEliece

Digital Signature

- Lattice-based
  - CRYSTALS-DILITHIUM
  - FALCON
- Multivariate
  - Rainbow

ALTERNATE

Encryption/KEM

- Lattice-based
  - FrodoKEM
  - NTRU Prime
- Code-based
  - BIKE
  - HQC
- Isogeny-based
  - SIKE

Digital Signature

- Symmetric-based
  - Picnic
  - SPHINCS+
- Multivariate
  - GeMSS

NSA’s Cybersecurity Perspective on PQC
July 29, 2020

- Strong preference for Lattice-Based Cryptography
  - “fairly well-studied”
  - “secure when well-parameterized”
  - “among the most efficient”

- Lattice-based KEM and digital signature scheme
  to be approved for National Security Systems (NSS)

- Stateful signature schemes, LMS and XMSS,
  - “have a limited number of allowable signatures per key”
  - “require the signer to maintain an internal state”

  to be approved for NSS solutions for certain niche applications

- NSA CSD does not anticipate the need to approve other
  PQC schemes for NSS usage
  - “circumstances could change”

Classical Attack on Rainbow

When: Feb. 25, 2022

Who:

Ward Beullens
Postdoc
IBM Research,
Zurich, Switzerland

Time of the attack on 8 cores of
an Intel i9-10885H CPU, running at 2.5 GHz:

Claimed security level 1: 53 hours

Paper: Cryptology ePrint Archive,
Report 2022/214

Sage Code:
https://github.com/WardBeullens/BreakingRainbow

Developments During Round 3

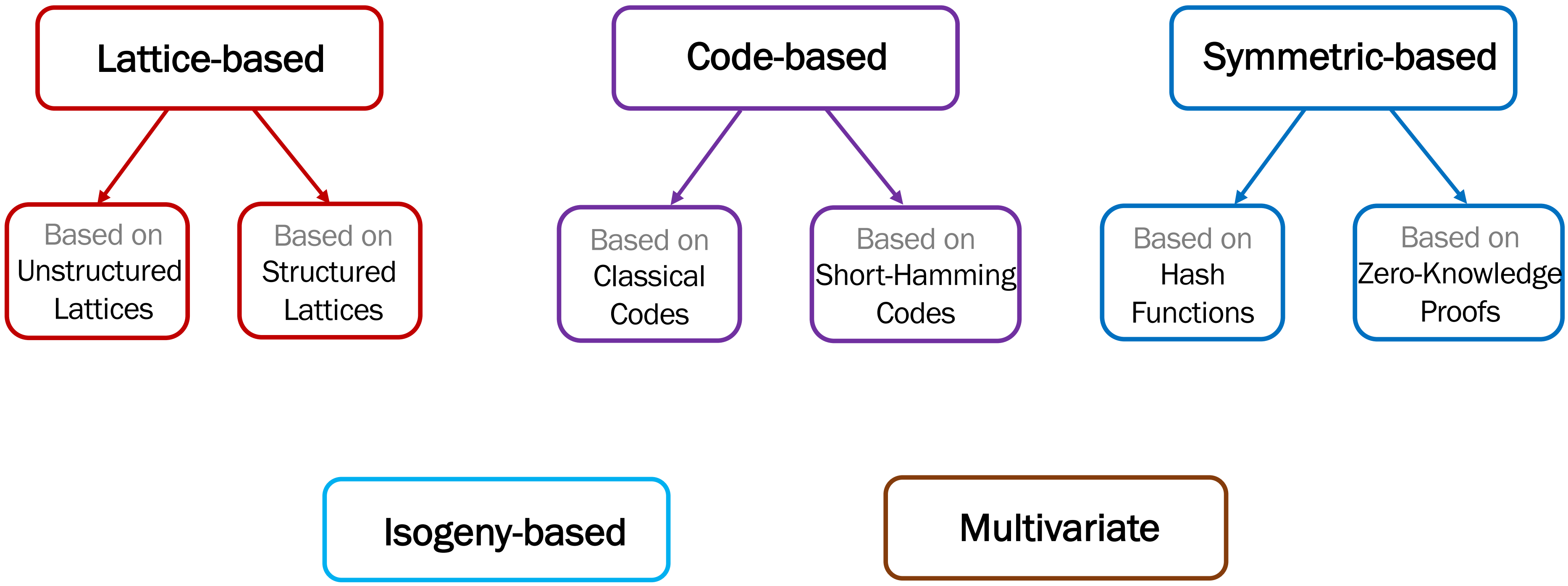
Round 3 Candidates

FINALISTS	**Encryption/KEM**	Lattice-based ├ CRYSTALS-KYBER ├ NTRU └ SABER	Code-based └ Classic McEliece	
	Digital Signature	Lattice-based ├ CRYSTALS-DILITHIUM └ FALCON	Multivariate └ Rainbow	
ALTERNATE	**Encryption/KEM**	Lattice-based ├ FrodoKEM └ NTRU Prime	Code-based ├ BIKE └ HQC	Isogeny-based └ SIKE
	Digital Signature	Symmetric-based ├ Picnic └ SPHINCS+	Multivariate └ GeMSS	

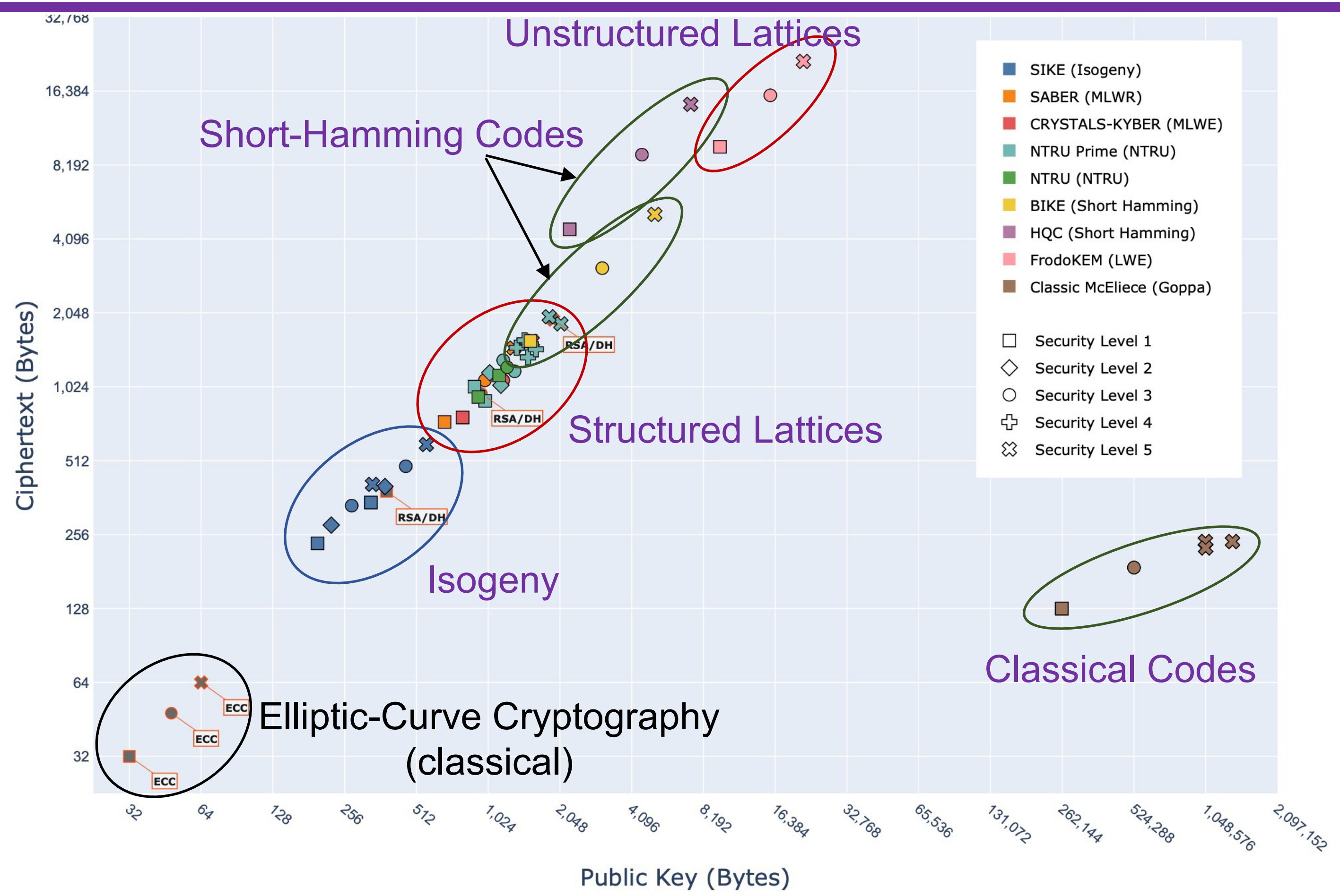
Breaking Rainbow Takes a Weekend on a Laptop

by Ward Beullens, https://eprint.iacr.org/2022/214, received 21 Feb 2022

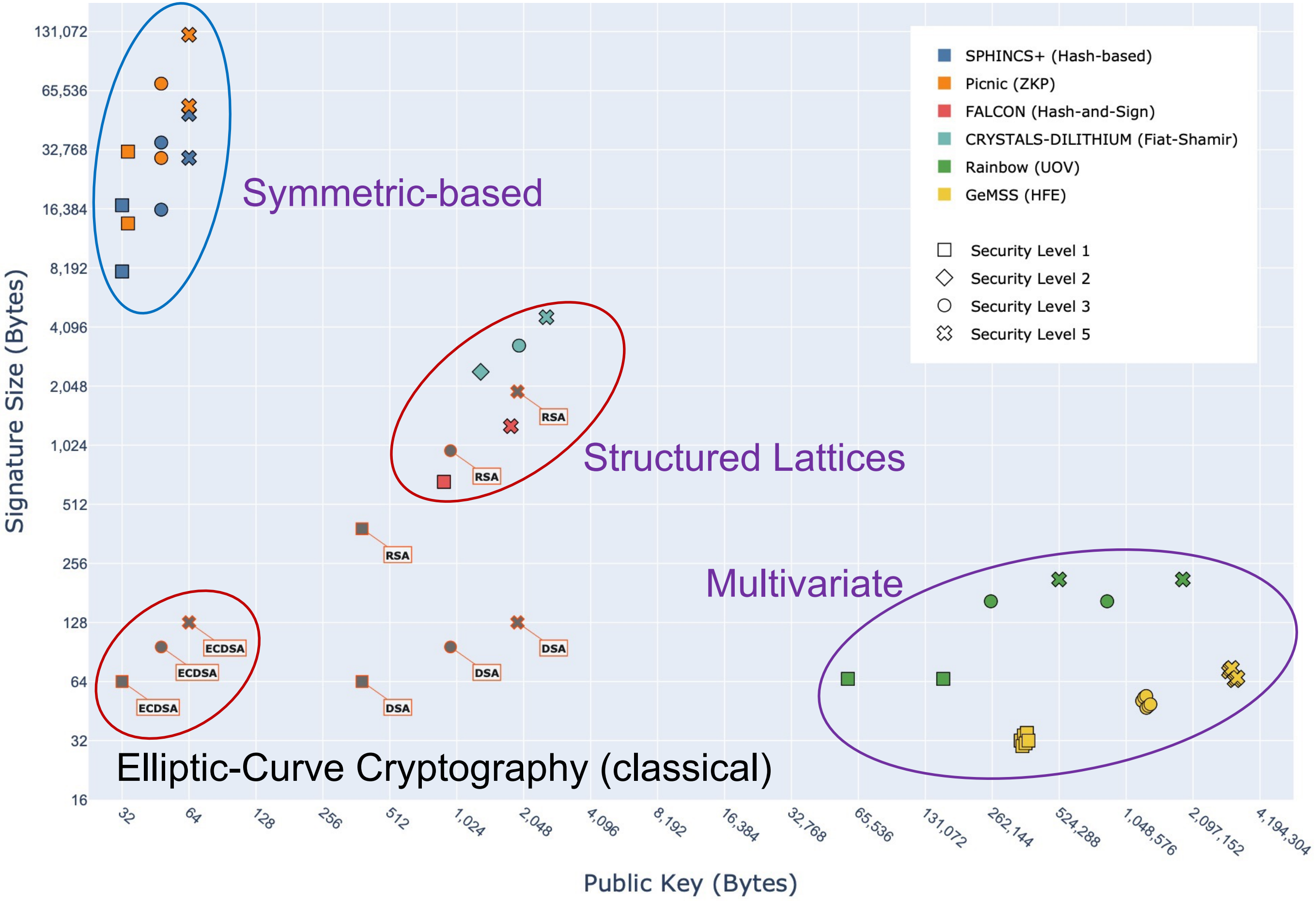
PQC Families and Subfamilies



Round 3 PQC Key Exchange + Classical PKE



Round 3 + Classical Digital Signature Schemes



Favorites for first-generation standards

Key Exchange (Key Encapsulation Mechanism – KEM)

Based on structured lattices	CRYSTALS-KYBER	SABER	NTRU
Based on classical codes	Classic McEliece		

Digital Signatures

Based on structured lattices	CRYSTALS-DILITHIUM	FALCON
Symmetric-based (hash-based)	SPHINCS+	

Certificate Size Ratio

Client **Server**

Request →

Certificate={Public_Key$_{Server}$, Signature$_{CA}$} ←

Ciphertext →

Certificate Size Ratio

$$\frac{\text{Classic McEliece + SPINCS+}}{\text{CRYSTALS-KYBER + CRYSTALS DILITHIUM}} > 100$$

Evaluation Criteria

Size of Keys, Ciphertext, and Signatures

Security

Patent Issues

Software Efficiency

Hardware Efficiency

Simplicity

Flexibility

Evaluation Criteria – Other Desired Properties

- Drop-in replacements
  Compatibility with existing protocols and networks
- Perfect forward secrecy
- Resistance to side-channel attacks
- Misuse resistance
- Ease of implementation (challenging features: decryption failures, floating-point arithmetic, Gaussian sampling)

CERG Major Contributions

High-Speed Hardware Implementations of KEMs:

- NTRU (first)
- CRYSTALS-Kyber (fastest)
- Saber (fastest)

High-Speed Hardware Implementations of Digital Signatures:

- CRYSTALS-Dilithium (2^{nd} fastest)
- Falcon (verification only) (first)

Lightweight Hardware Implementations of KEMs Resistant Against Side-Channel Attacks

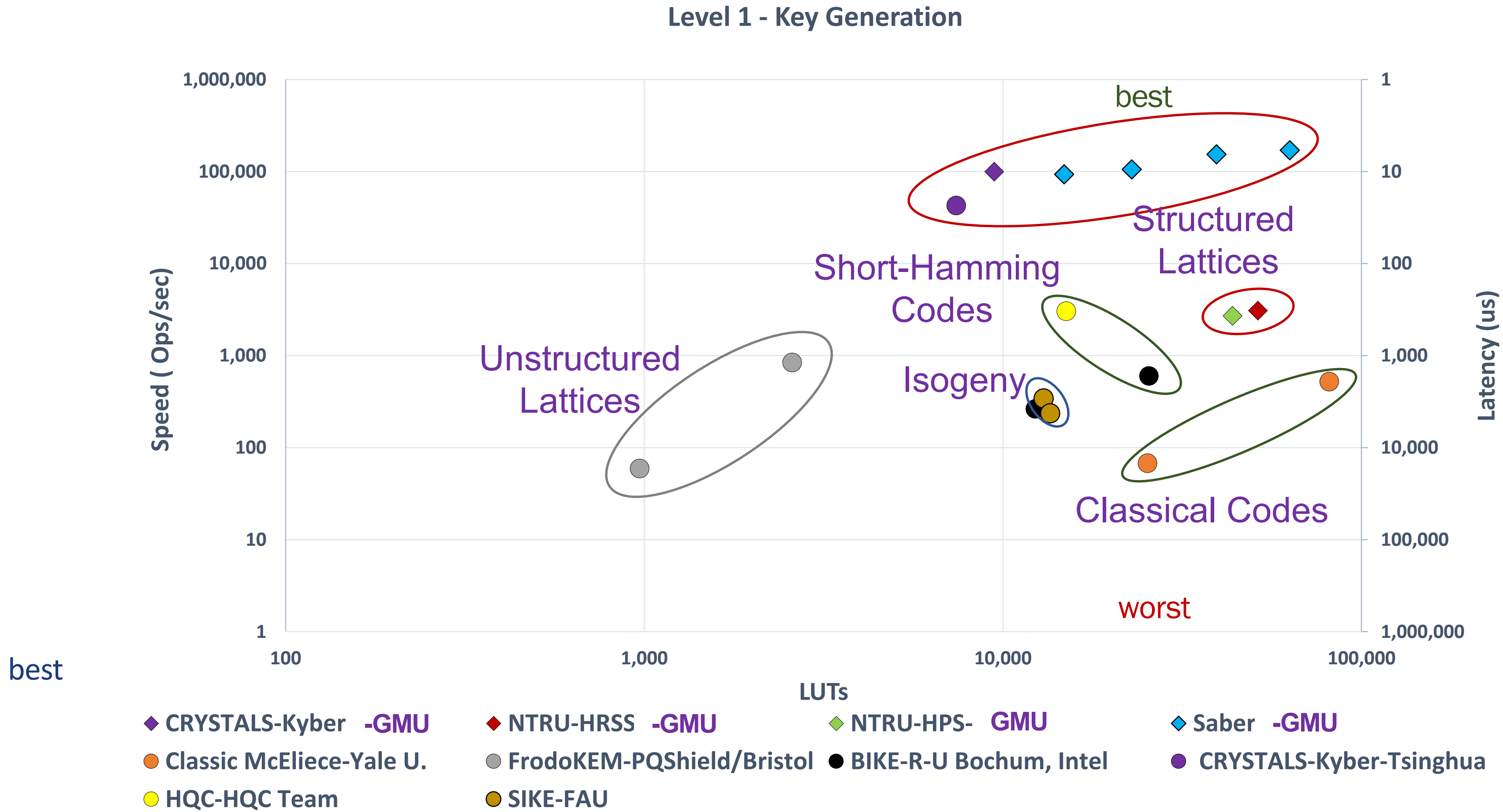
- Saber (first)

NEON-Based Software Implementations

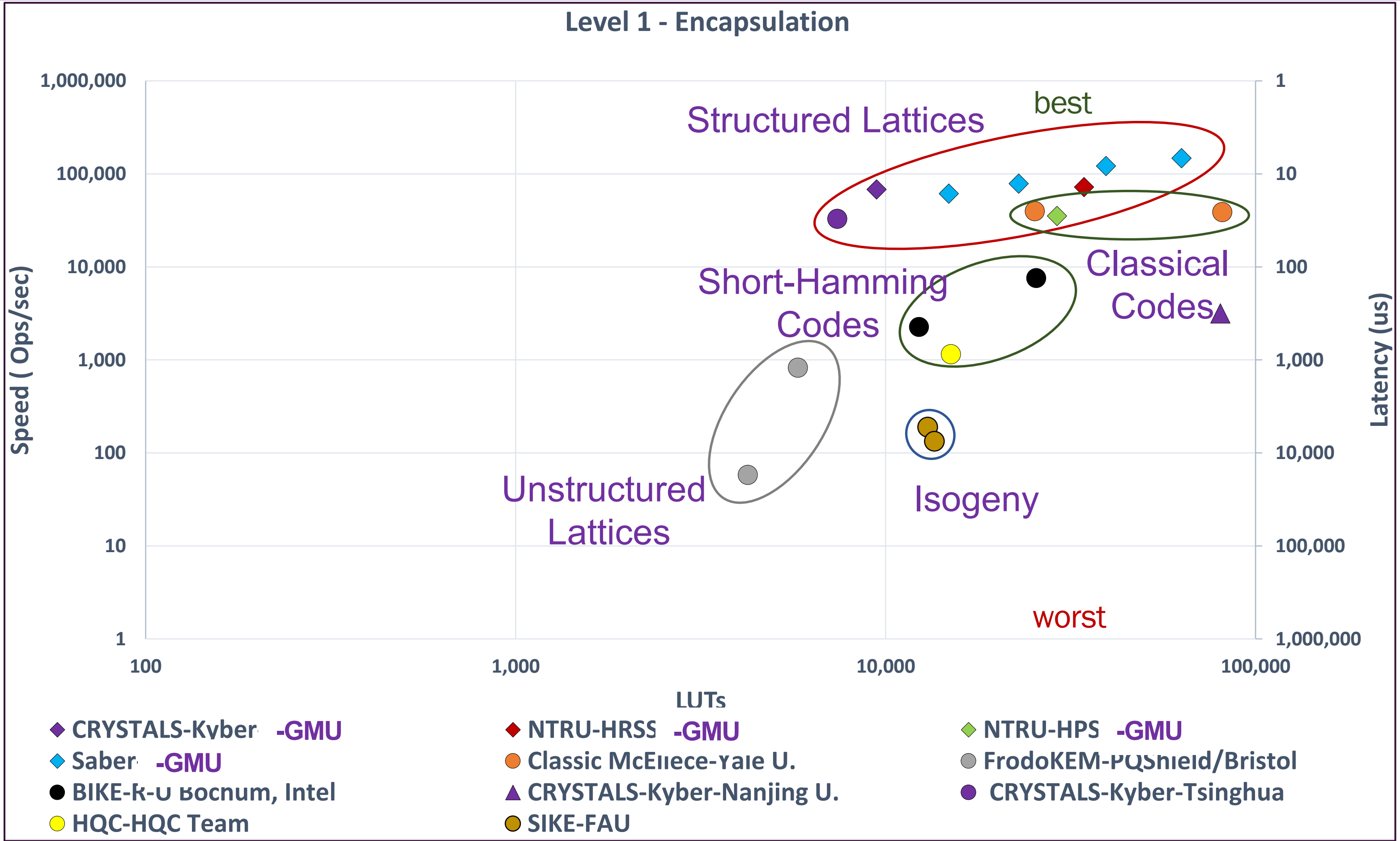
- NTRU (first)
- CRYSTALS-Kyber (first)
- Saber (first)
- Falcon (first)

Results for KEMs in Hardware

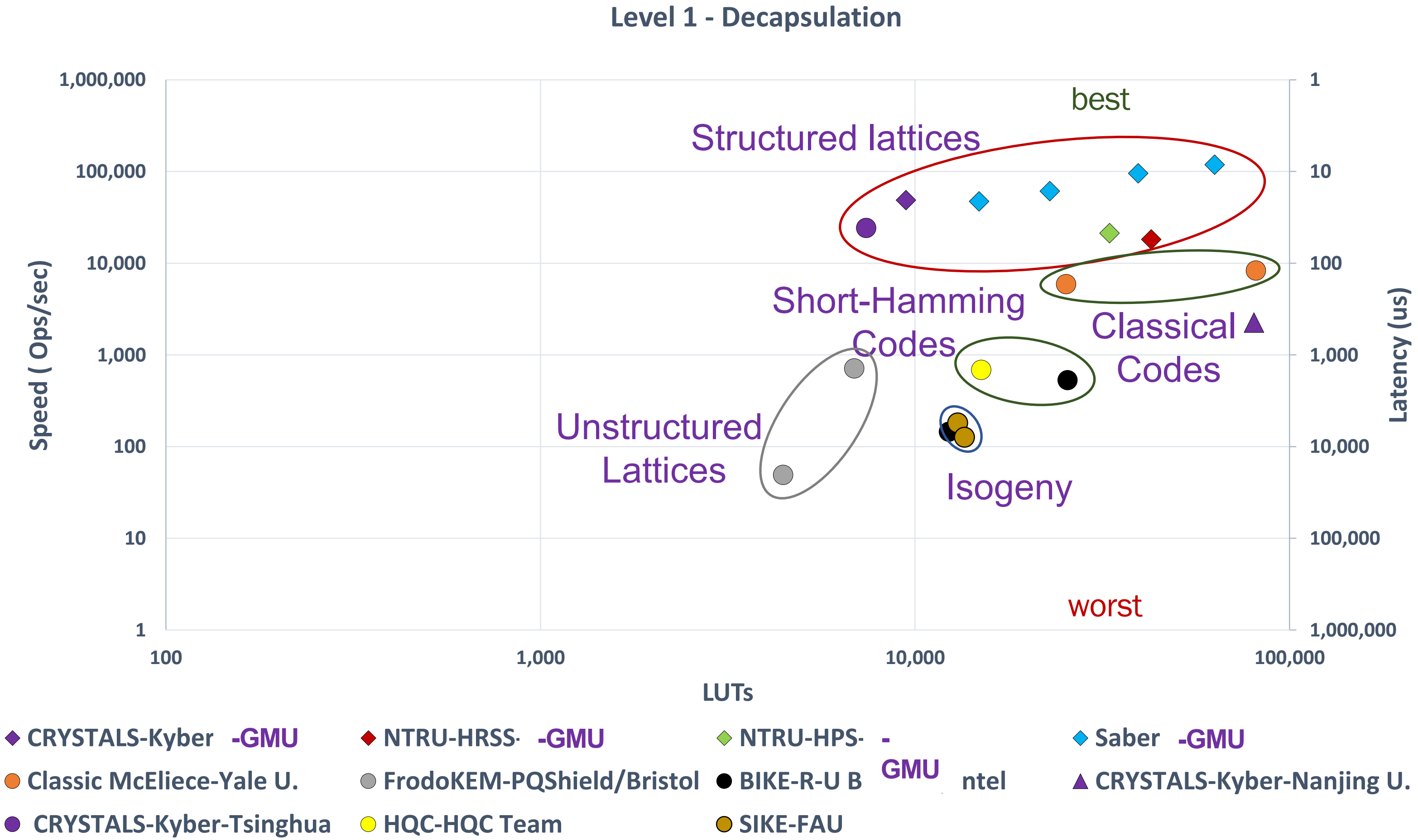
Level 1: Key Generation on Artix-7



Level 1: Encapsulation on Artix-7

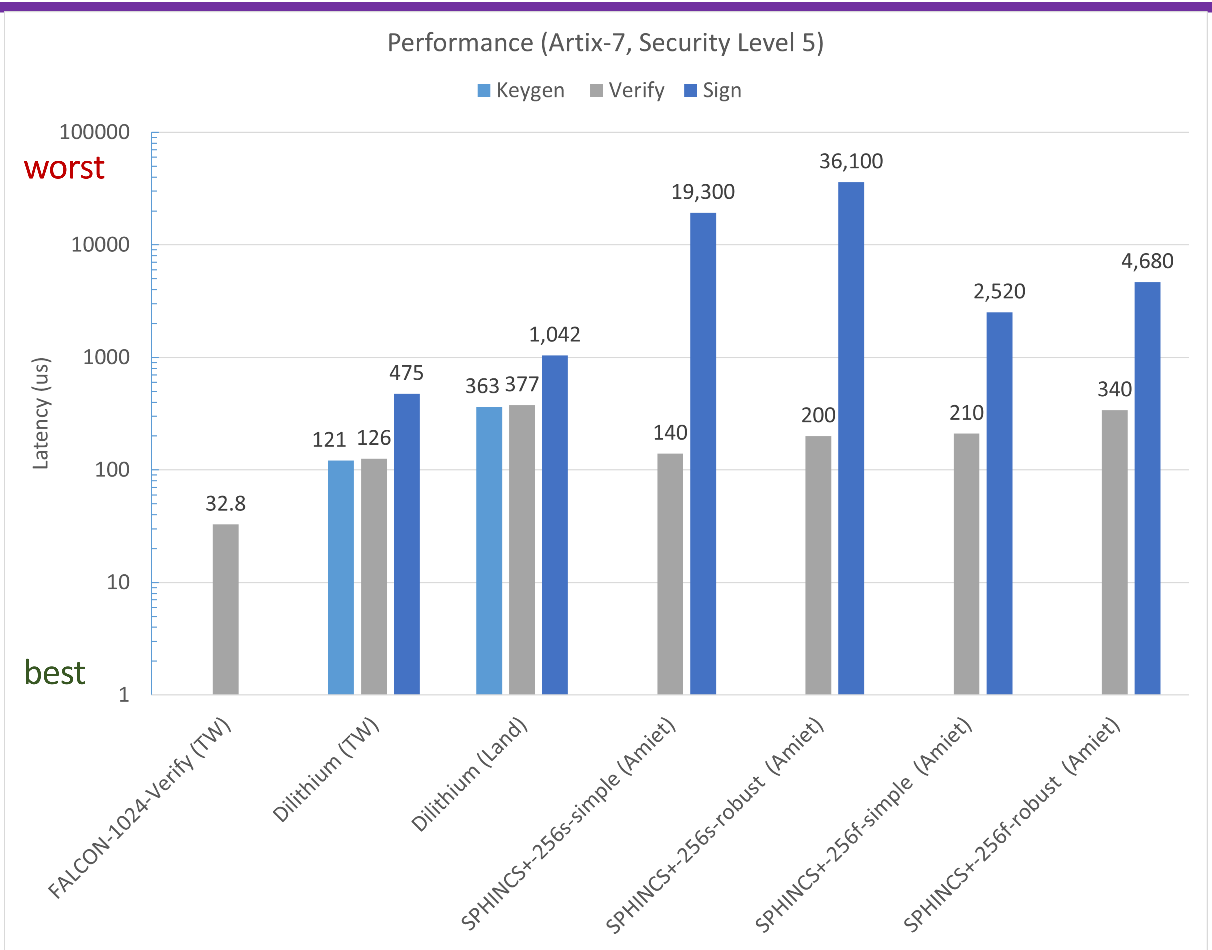


Level 1: Decapsulation on Artix-7



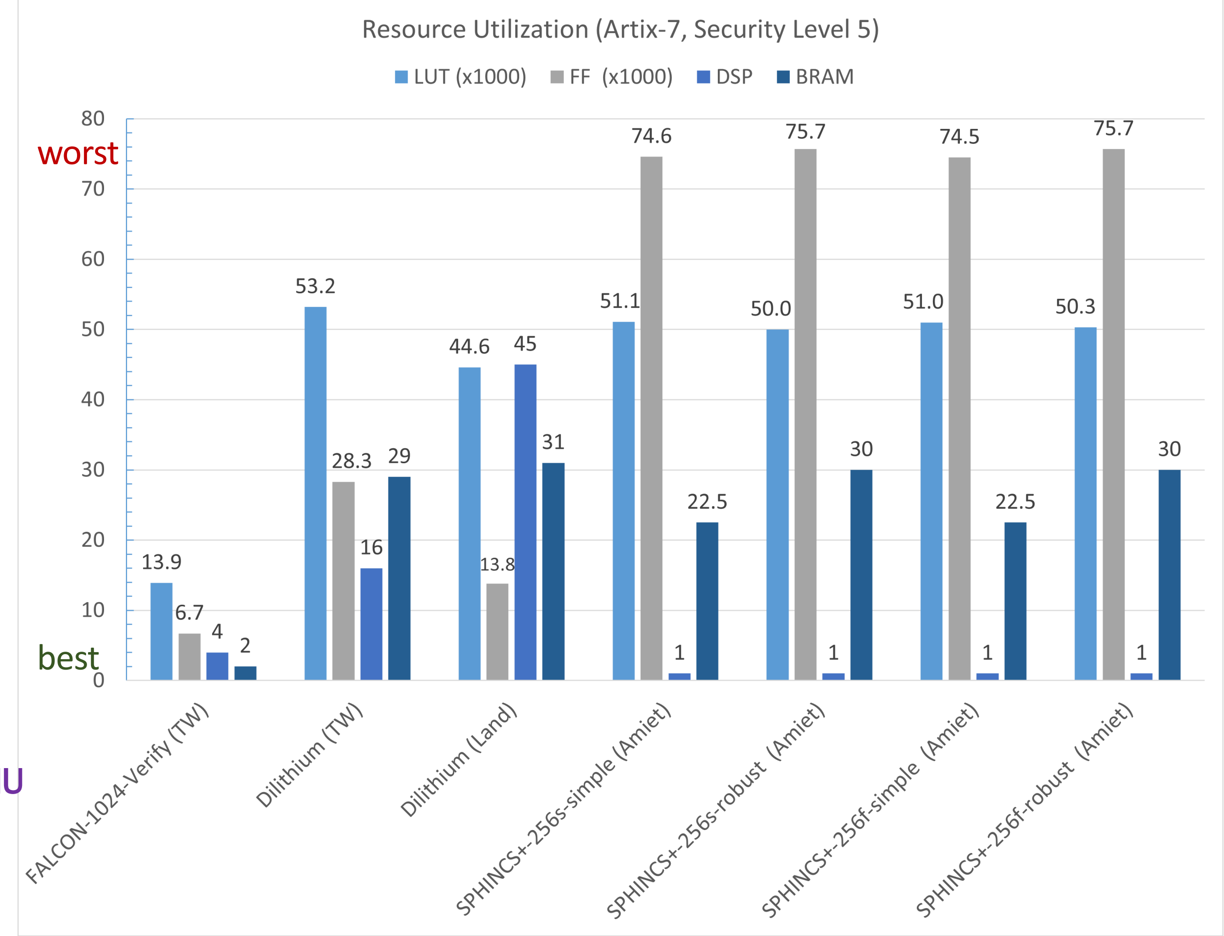
Results for Digital Signatures in Hardware

Level 5: All Operations on Artix-7: Latency



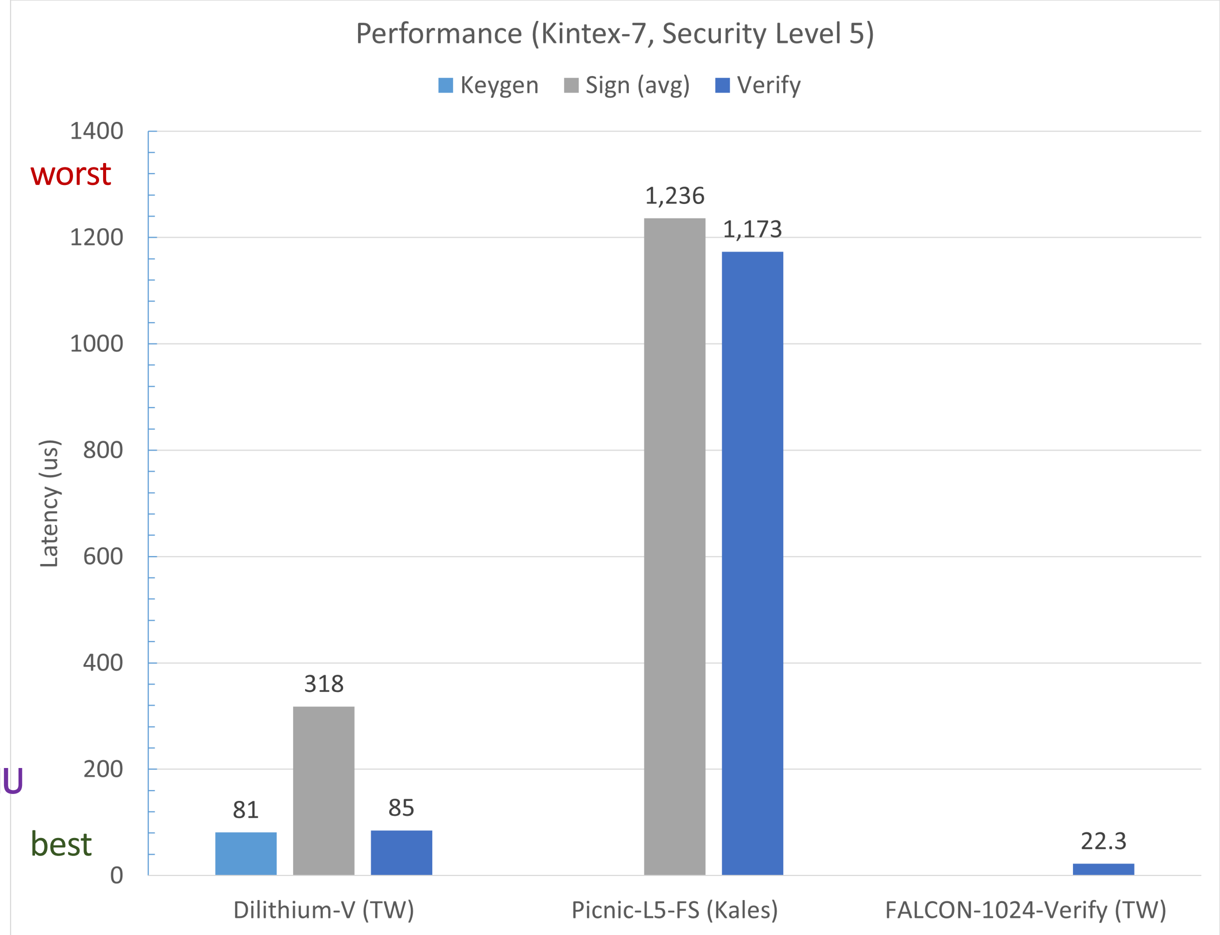
TW– This Work = GMU

Level 5: All Operations on Artix-7: Resource Utilization



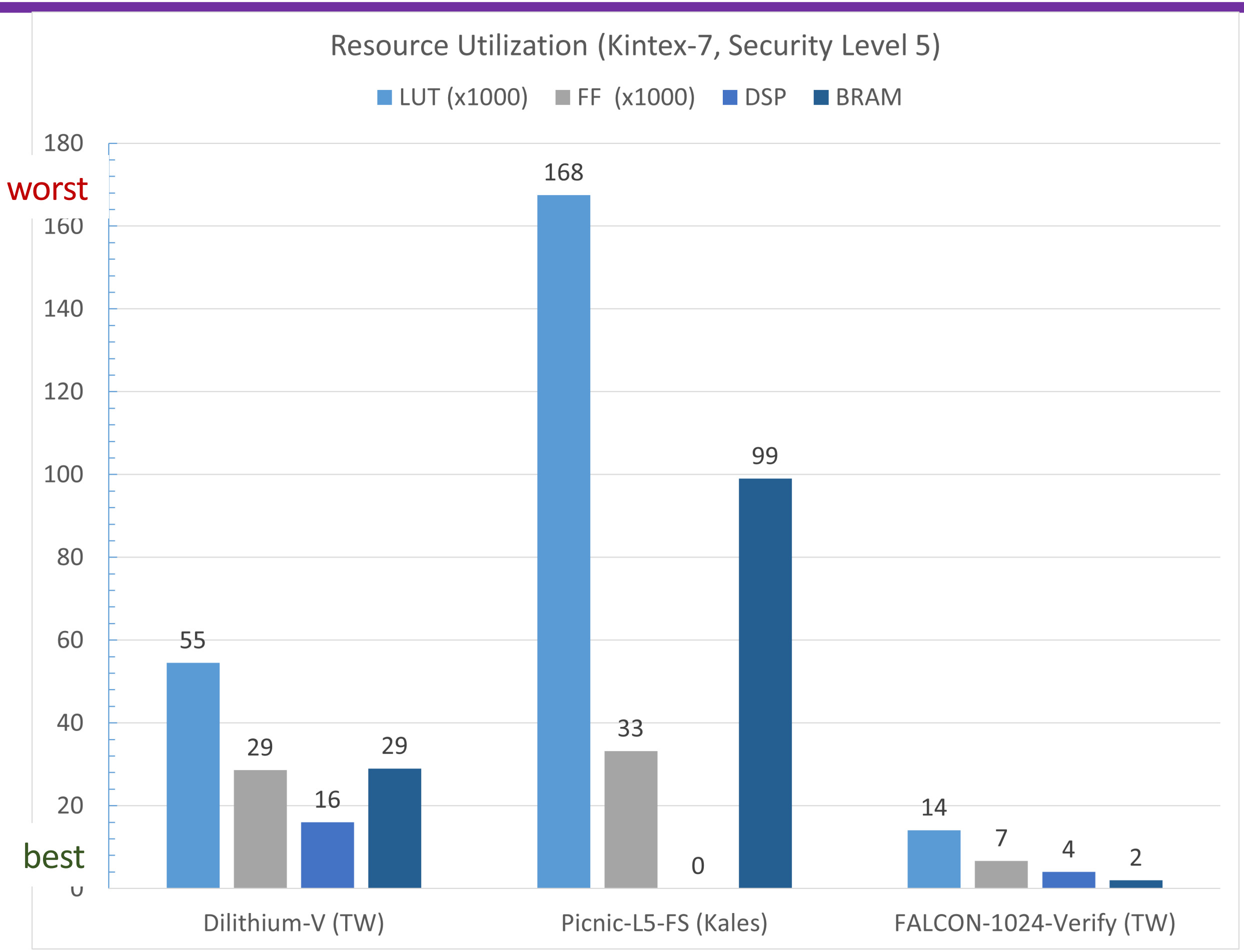
TW– This Work = GMU

Level 5: All Operations on Kintex-7: Latency



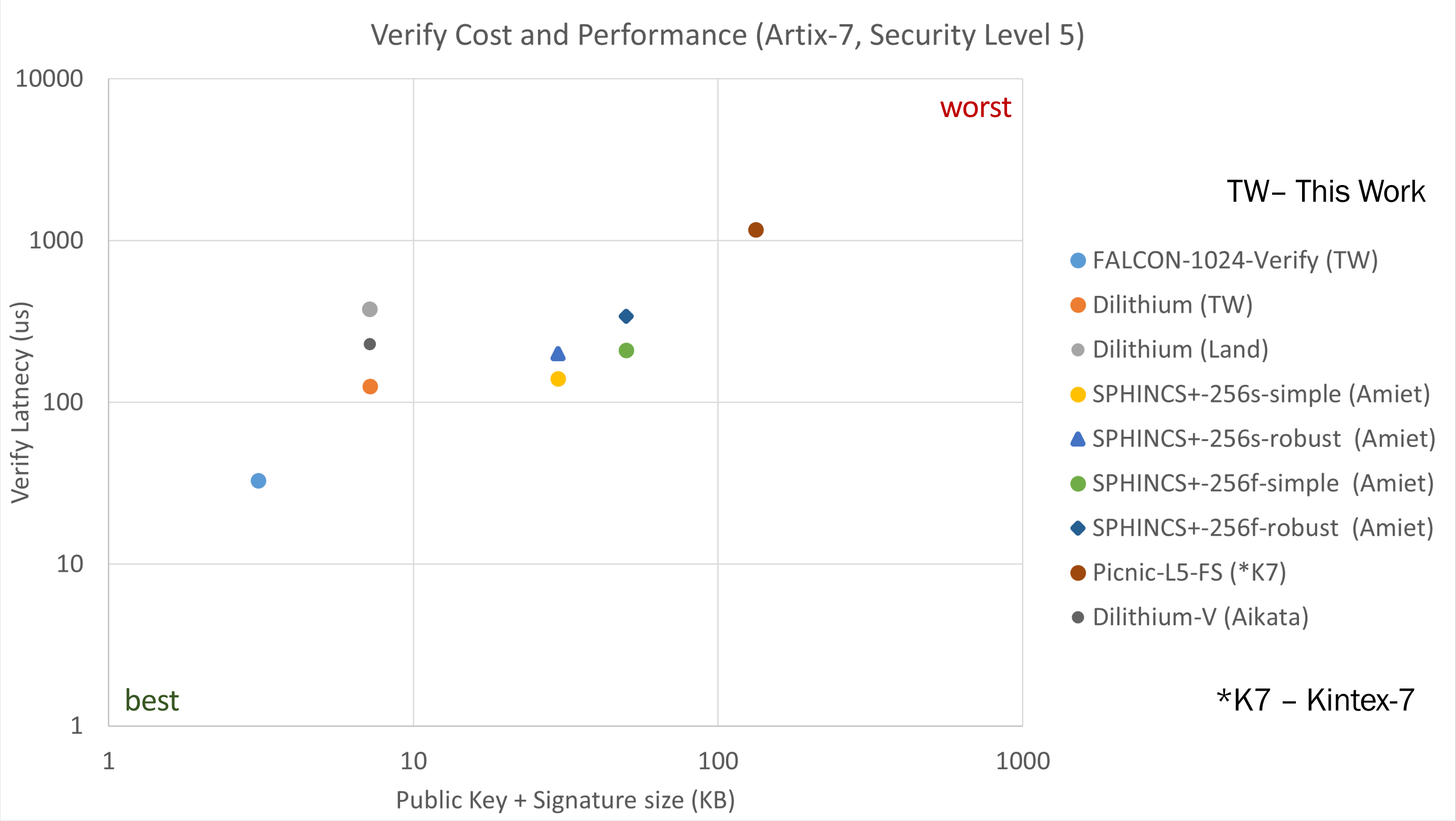
TW– This Work = GMU

Level 5: All Operations on Kintex-7: Resource Utilization



TW– This Work = GMU

Level 5: Signature Verification: Artix-7: Latency vs. Certificate Size



Hardware Benchmarking Summary

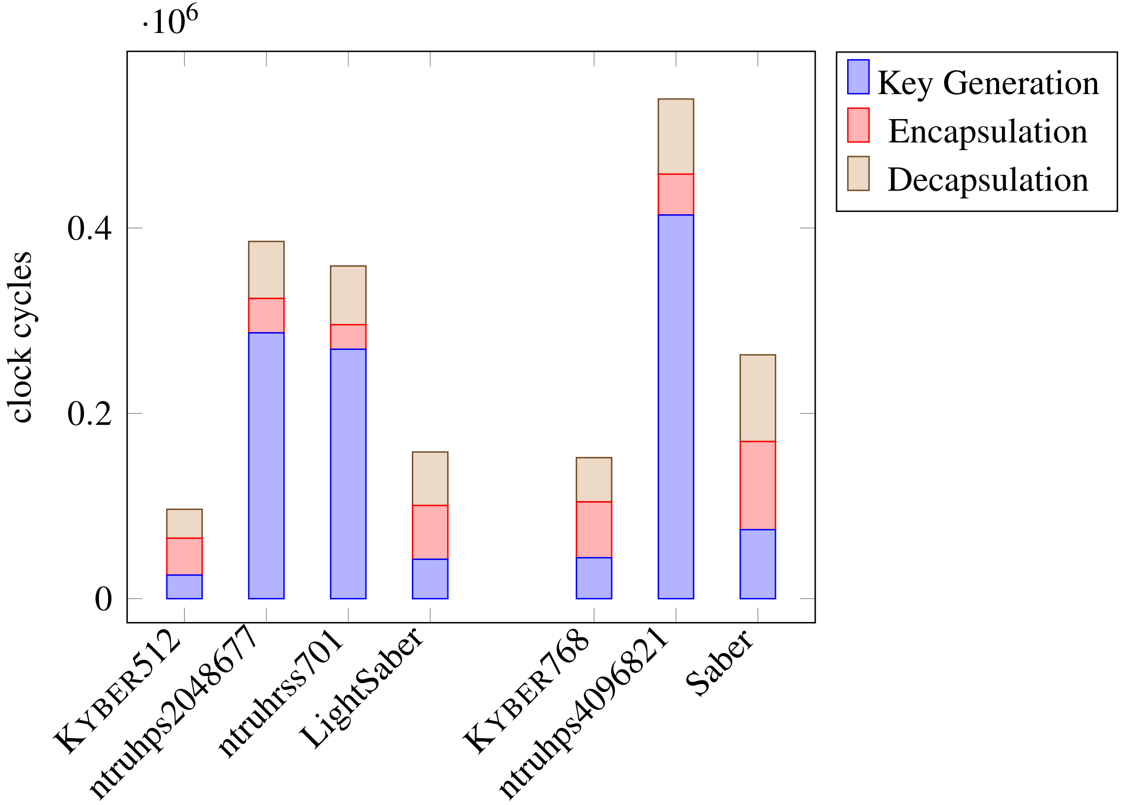
Summary

- **High-speed hardware for KEMs:**
  - CRYSTALS-Kyber and Saber comparable; Saber more flexible
  - NTRU and Classic McEliece significantly slower for key generation and somewhat slower for decapsulation and encapsulation
  - SIKE, BIKE, HQC, and FrodoKEM orders of magnitude slower

- **High-speed hardware for Digital Signatures:**
  - CRYSTALS-Dilithium efficient and easy to implement
  - FALCON Verify operation the fastest, but KeyGen and Sign prohibitively complicated
  - SPHINCS+ and Picnic outperformed by CRYSTALS-Dilithium

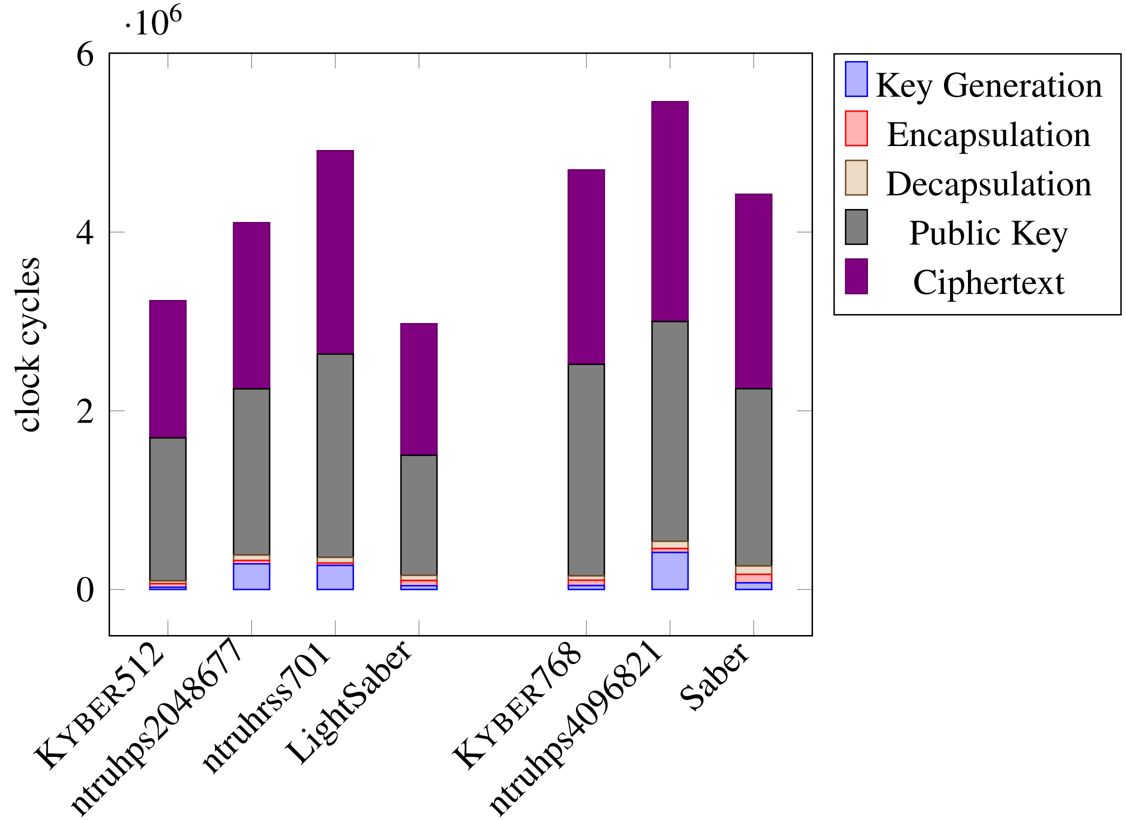
Software Benchmarking Summary

KEM Benchmarks on x86-64 processors with AVX2



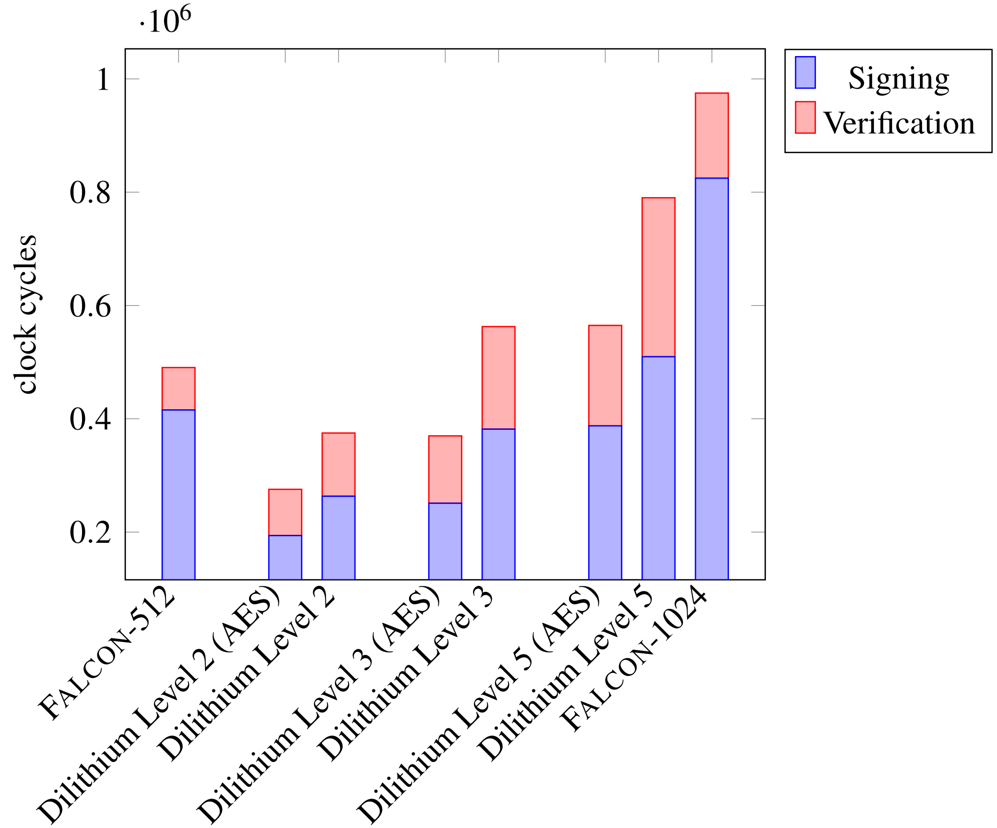
Source: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

KEM Benchmarks on x86-64 processors with AVX2 with 2000 cycles/byte transmission costs



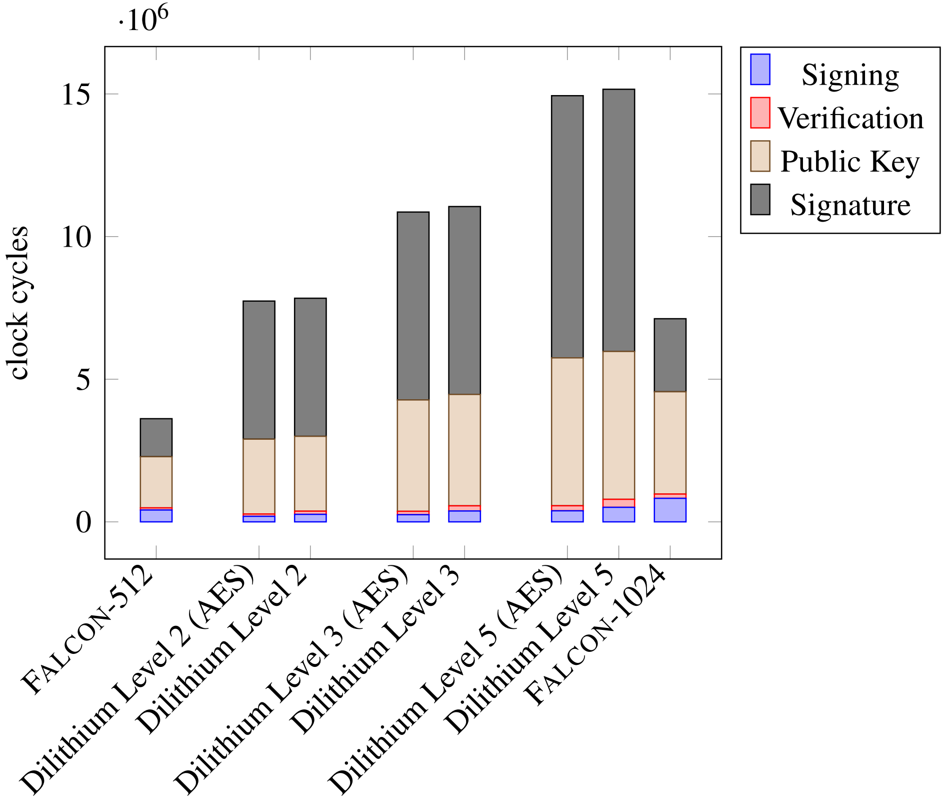
Source: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Digital Signature Benchmarks on x86-64 processors with AVX2



Source: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Digital Signature Benchmarks on x86-64 processors with AVX2 with 2000 cycles/byte transmission costs



Source: Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

NIST The-end-of-Round 3 Announcement

Before the End of Round 3

Round 3 Candidates

FINALISTS	**Encryption/KEM**	Lattice-based: CRYSTALS-KYBER, NTRU, SABER	Code-based: Classic McEliece	
	Digital Signature	Lattice-based: CRYSTALS-DILITHIUM, FALCON	Symmetric-based: SPHINCS+	
ALTERNATE	**Encryption/KEM**	Lattice-based: FrodoKEM, NTRU Prime	Code-based: BIKE, HQC	Isogeny-based: SIKE
	Digital Signature	Symmetric-based: Picnic	Multivariate: GeMSS, Rainbow	

NIST Decision Published on July 5, 2022

TO BE STANDARDIZED FIRST (2023-2024)

Encryption/KEM

Lattice-based
- CRYSTALS-KYBER
- ~~NTRU~~
- ~~SABER~~

Code-based
- Classic McEliece

Digital Signature

Lattice-based
- CRYSTALS-DILITHIUM
- FALCON

Symmetric-based
- SPHINCS+

ROUND 4 (2022-2023)

Encryption/KEM

~~Lattice-based~~
- ~~FrodoKEM~~
- ~~NTRU Prime~~

Code-based
- BIKE
- HQC

Isogeny-based
- SIKE

NEW ON-RAMP PROCESS FOR SIGNATURES (2023-2025)

Digital Signature

~~Symmetric-based~~
- ~~Picnic~~

~~Multivariate~~
- ~~GeMSS~~
- ~~Rainbow~~

Complete Break of SIKE

Classical Attack on SIKE (1)

When: July 30, 2022

Who:

Wouter Castryck
Research Fellow
COSIC, KU Leuven
2007-present

Thomas Decru
Postdoc
COSIC, KU Leuven
2022-present

Classical Attack on SIKE (2)

Time of the attack using Magma code and Intel Xeon CPU @ 2.60GHz:

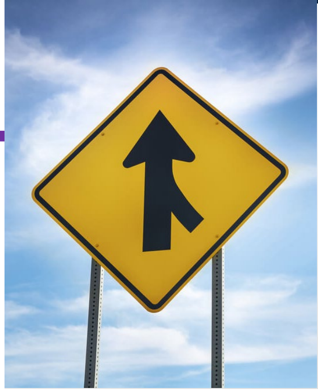
SIKEp434 (claimed security level 1):	1 hours 02 minutes
SIKEp503 (claimed security level 2):	2 hours 19 minutes
SIKEp610 (claimed security level 3):	8 hours 15 minutes
SIKEp751 (claimed security level 5):	20 hours 37 minutes

Paper: Cryptology ePrint Archive, Report 2022/975

Magma code: https://homes.esat.kuleuven.be/~wcastryc

NIST Call for New Signature Schemes

An On-Ramp for Signatures



Call for Additional Digital Signature Schemes
issued on Sep. 6, 2022; updated in Oct. 2022

- Deadline: June 1, 2023
- Main reason: diversify signature portfolio
- Candidates on a different track than Round 4 KEMs
- Focus on general-purpose signatures that are not based on structured lattices (e.g., code-based signatures)
- Schemes with certain unique features may be considered as well, e.g., schemes with very short signatures
- The more mature the scheme, the better

Standardization in Other Countries

Countries with Independent Standardization Efforts

Germany:

At the beginning of 2020, the Federal Office for Information Security (BSI) recommended:

- FrodoKEM – based on unstructured lattices
- Classic McEliece – based on classical codes

China:

The Chinese Association for Cryptologic Research (CACR) held a national cryptographic algorithm design competition in 2018-2019. 79 candidates.

Winners announced in January 2020:

Digital signatures: Aigis-sig
Public-key encryption: LAC-PKE and Aigis-enc

Transition Plans for National Security Systems

Informal Definition & Recent Developments

Most systems run by the Department of Defense or Intelligence Community fall under the “National Security System” classification.

May 2022:

National Security Memo 10 (NSM-10) signed making it an aim of US to be off quantum vulnerable crypto by 2035

- Calls out to several cybersecurity agencies across the US Government to work in their area of responsibility to ensure a timely transition:
- Calls out NSA to make standards for NSS and give a timeline for deprecation of quantum vulnerable systems

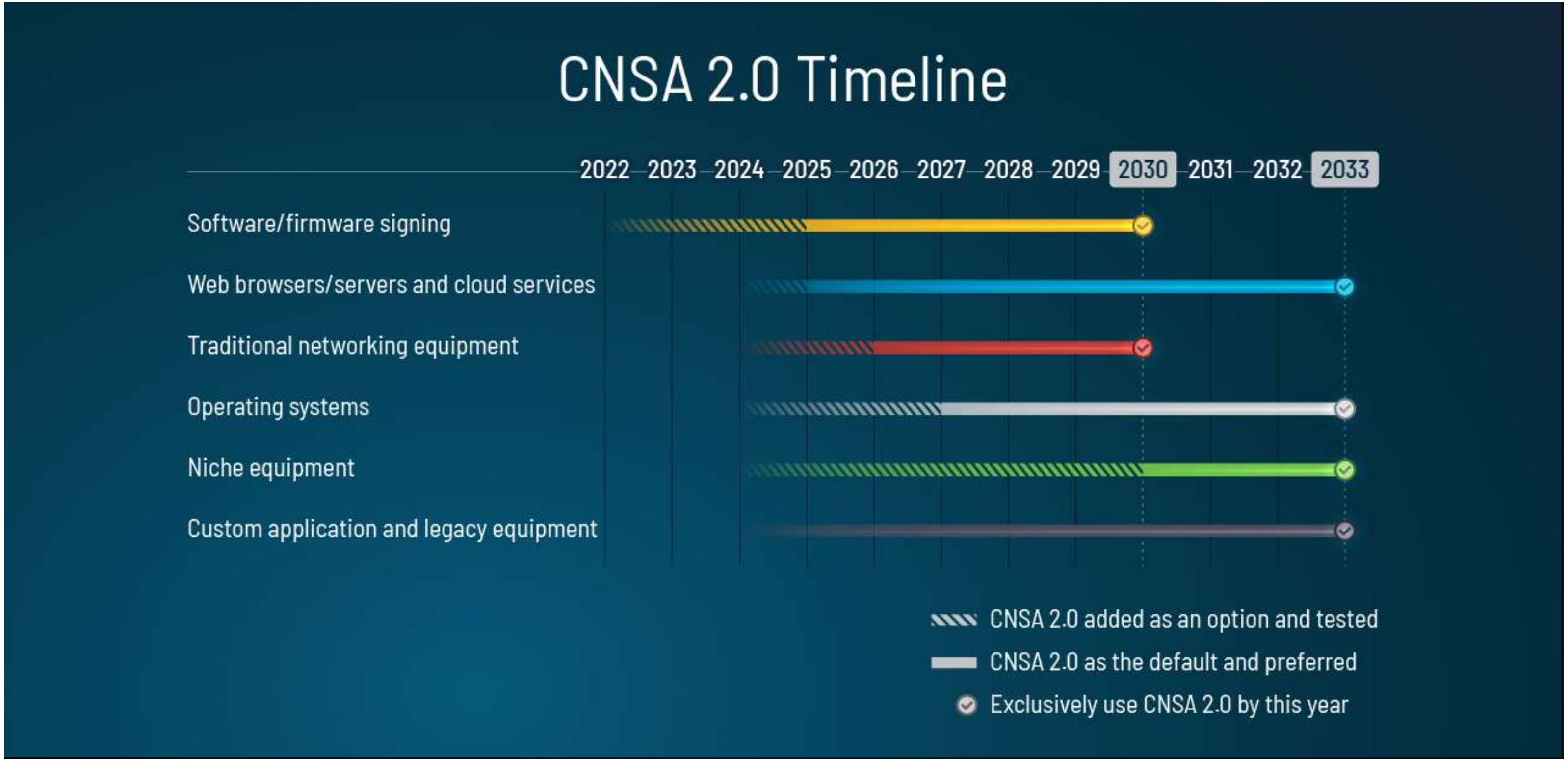
September 2022:

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) released laying out how to achieve quantum resistance in NSS

Commercial National Security Algorithm (CNSA) 2.0 Suite

Function	Algorithm	Specification
Symmetric block cipher for information protection	AES-256	FIPS 197
Cryptographic hash	SHA-384 or SHA-512	FIPS 180-4
Asymmetric algorithm for key establishment	CRYSTALS-Kyber	TBD
Asymmetric algorithm for digital signature	CRYSTALS-Dilithium	TBD
Asymmetric algorithm for digitally signing firmware and software	Leighton-Micali Signature (LMS) with SHA-256/192, Xtended Merkle Signature Scheme (XMSS)	NIST SP 800-208

CNSA 2.0 Transition Timeline



Source: Morgan Stern (NSA), Transitioning National Security Systems to a Post-Quantum Future, Fourth PQC Standardization Conference, Nov. 29-Dec. 1, 2022

Last Thoughts

PQC Opportunities and Challenges

- The biggest revolution in cryptography since the invention of public-key cryptography in 1970s
- Very fast changing field
- A lot of work remaining to be done in terms of developing new standards and practical validation procedures and labs
- New candidates for future standardization still in the pipeline
- Long and laborious transition period (easily 10-15 years)
- Many applications require resistance to side-channel and fault attacks
- Likely extensions to Instruction Set Architectures of multiple major microprocessors
- Excellent employment opportunities, especially for U.S. Citizens
- Start-up and new-product opportunities

Once in a life-time opportunity! Get involved!

Q&A

CERG
Cryptographic Engineering Research Group

Thank You!

Questions?  Comments?

CERG: http://cryptography.gmu.edu

ATHENa: http://cryptography.gmu.edu/athena
Menu Field: PQC

CERG
Cryptographic Engineering Research Group