THE NIST POST-QUANTUM CRYPTOGRAPHY STANDARDIZATION PROJECT

Angela Robinson

AGENDA

Analyzing the quantum threat

Overview of PQC

Observations and experiences

Future of PQC

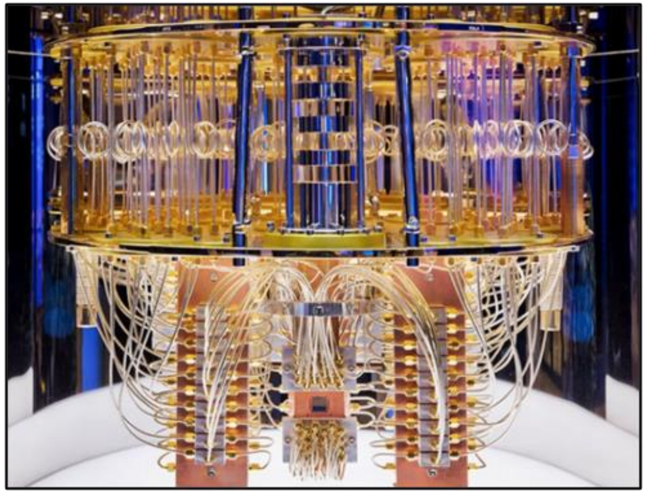
Impact

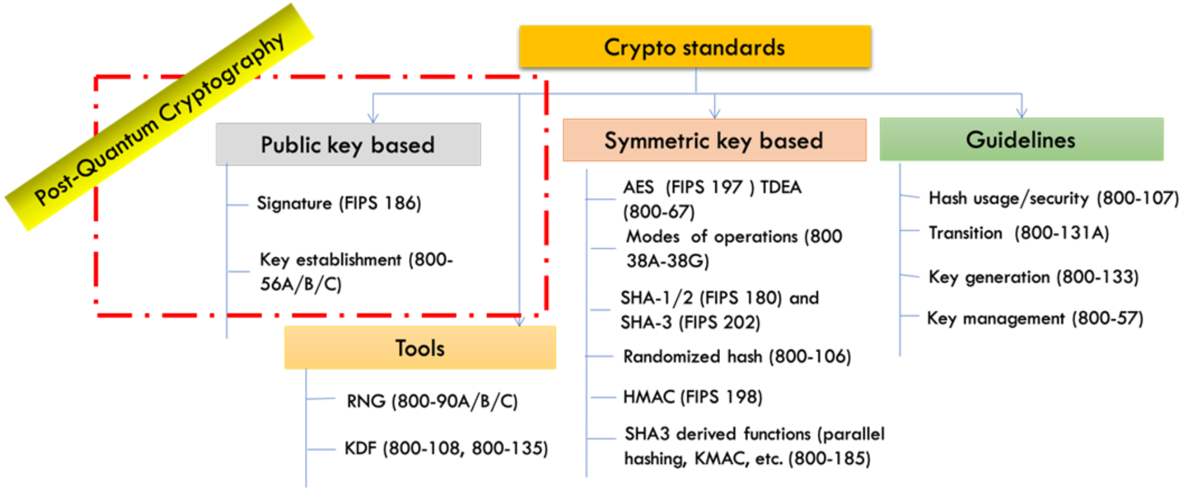
THE QUANTUM THREAT

All NIST public-key cryptographic standards are vulnerable to attacks from a large-scale quantum computer:

- SP 800-56A: Diffie-Hellman, ECDH
- SP 800-56B: RSA encryption
- FIPS 186: RSA, DSA, ECDSA signatures

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



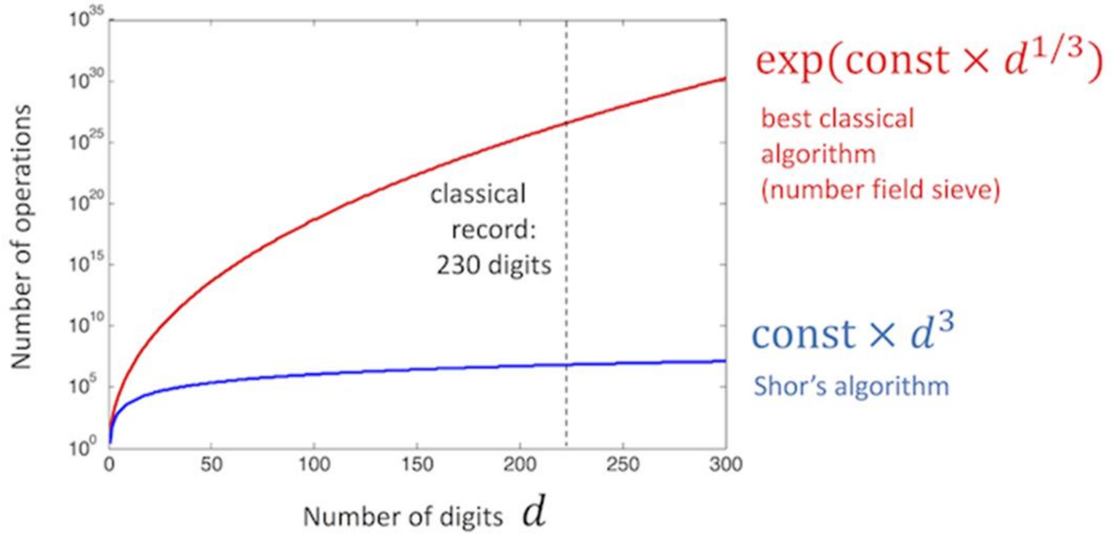


Post-Quantum Cryptography
Crypto standards
Public key based
Signature (FIPS 186)
Key establishment (800-56A/B/C)
Tools
RNG (800-90A/B/C)
KDF (800-108, 800-135)
Symmetric key based
AES (FIPS 197) TDEA (800-67)
Modes of operations (800 38A-38G)
SHA-1/2 (FIPS 180) and SHA-3 (FIPS 202)
Randomized hash (800-106)
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)

QUANTIFYING THE QUANTUM THREAT

Rough quantum timeline

- 1994 – Shor's algorithm
- 1998 – First experimental demonstration of a quantum algorithm, 2 physical qubits



Classical vs. quantum factoring algorithms

Image credit: https://quantum-computing.ibm.com/composer/docs/iqx/guide/shors-algorithm

QUANTIFYING THE QUANTUM THREAT

Rough quantum timeline

- 1994 – Shor's algorithm
- 1998 – First experimental demonstration of a quantum algorithm, 2 physical qubits
- 2010's – reports of ~10-100 physical qubit computations
- 2020's – reports of ~128 – 1,180 physical qubit computations

Millions needed to break today's cryptosystems

	Logical qubits	Physical qubits
RSA-1024	4098	6-11 million
RSA-2048	8194	8-22 million
RSA-3072	12,290	19-44 million

Approximating quantum resources required to **break** RSA cryptosystem using Shor's algorithm

"A Resource Estimation Framework for Quantum Attacks Against Cryptographic Functions: Recent Developments" Global Risk Institute, March 2021

WHEN WILL THE THREAT BE REALIZED?

- Opinions vary
- The answer is unclear

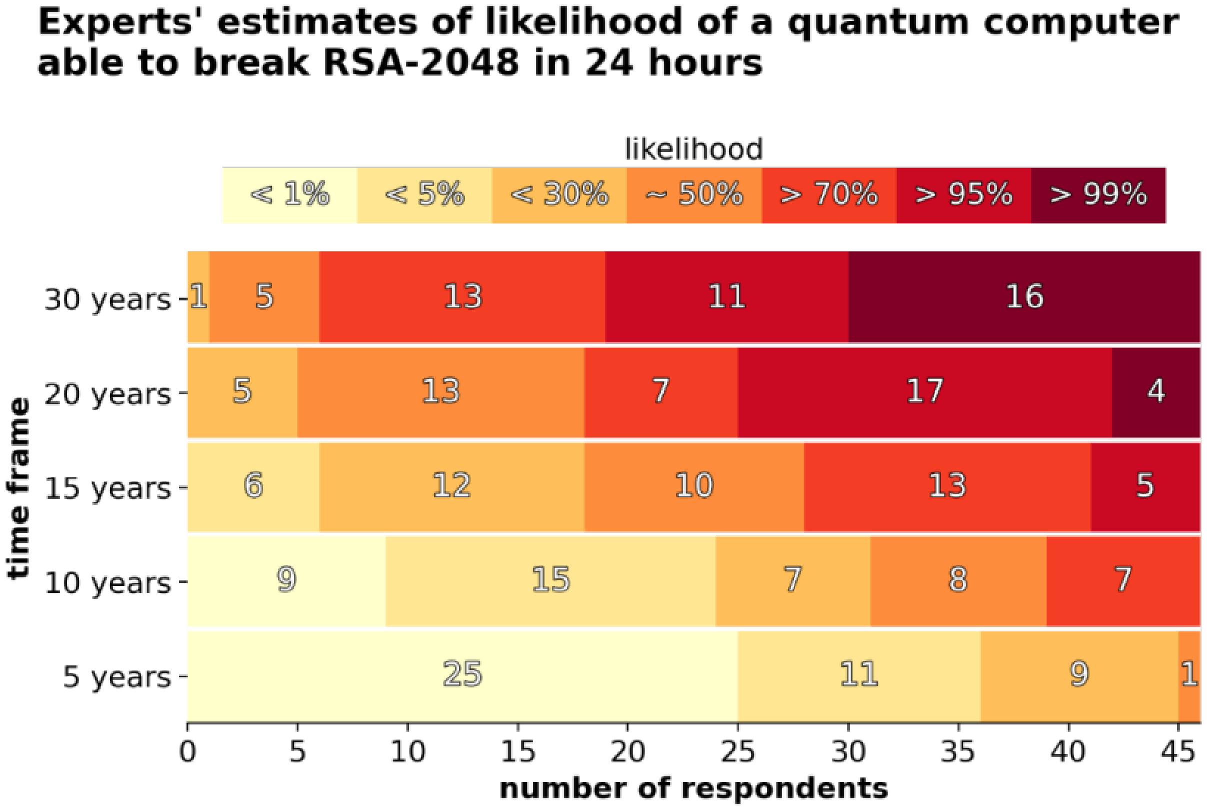


Figure 10 This figure illustrates the central information collected through our survey. The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specified sense of being able to break RSA-2048 in 24 hours—for various time frames, from a short term of 5 years all the way to 30 years.

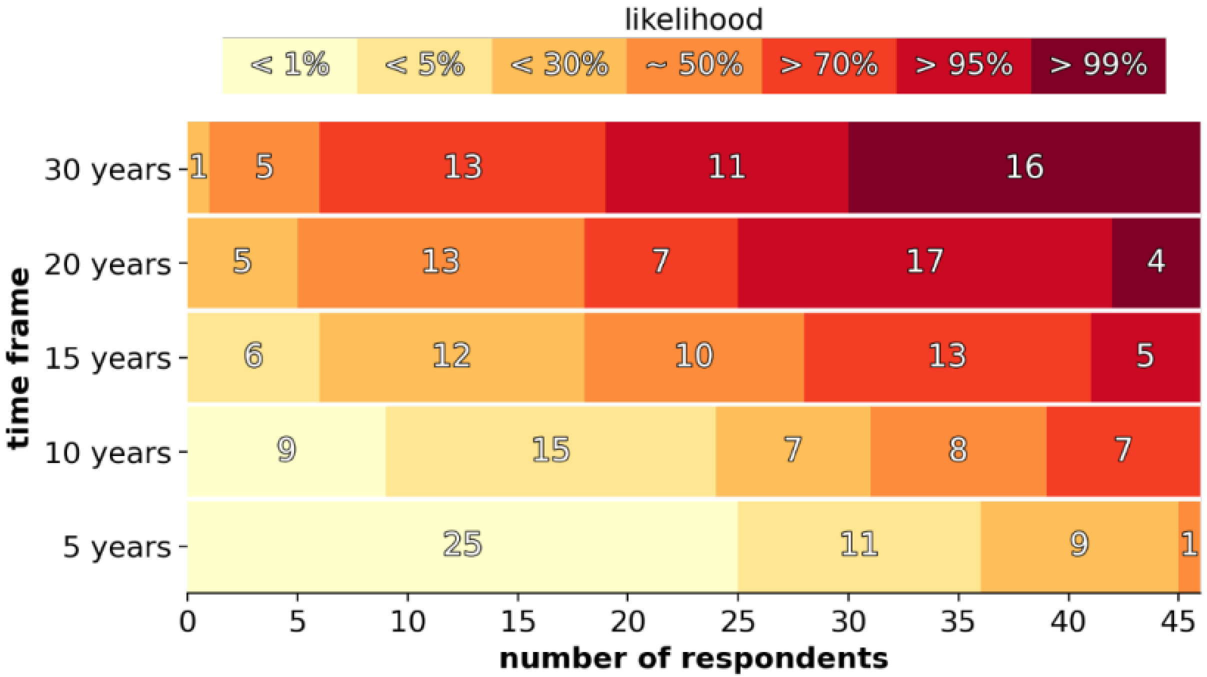
Quantum Threat Timeline Report, 2021
Global Risk Institute

WHEN WILL THE THREAT BE REALIZED?

- Opinions vary
- The answer is unclear

What is clear?

- Cyber systems will need to migrate to quantum-safe solutions before the threat is realized
- Migrations take several years
- Quantum-safe solutions need to be standardized



Experts' estimates of likelihood of a quantum computer able to break RSA-2048 in 24 hours

Figure 10 This figure illustrates the central information collected through our survey. The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specified sense of being able to break RSA-2048 in 24 hours—for various time frames, from a short term of 5 years all the way to 30 years.

Quantum Threat Timeline Report, 2021
Global Risk Institute

NIST PQC STANDARDIZATION PROCESS

Call for quantum-resistant cryptographic algorithms for new public-key standards

- Digital signatures
- Encryption/key establishment

Expectations:

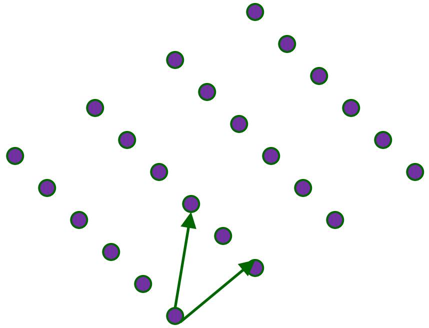
- NIST's role: manage process of achieving community consensus in an open, transparent, and timely manner
- Different and more complicated than past NIST standardization competitions
- There would not be a single "winner"

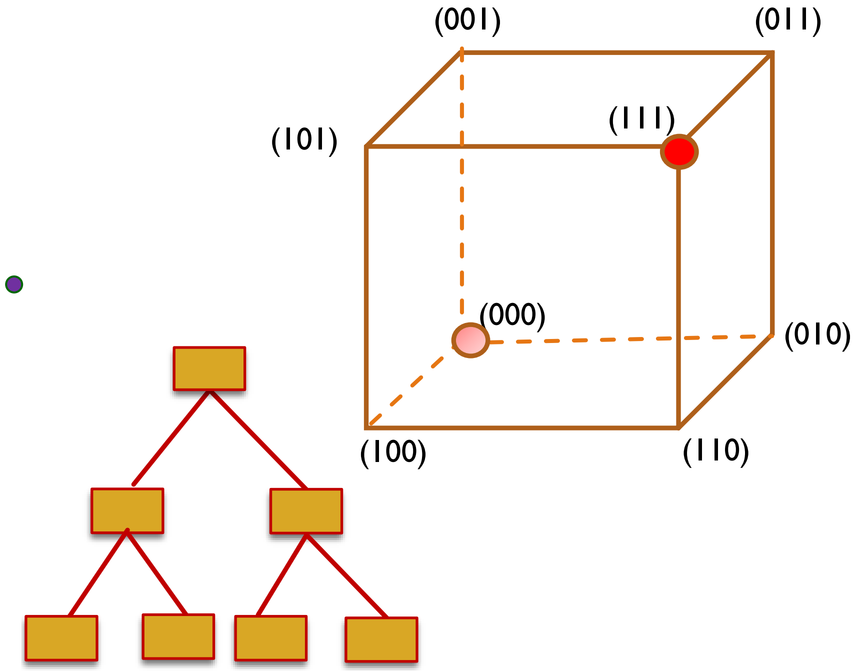
POST QUANTUM CRYPTOGRAPHY (PQC)

PQC has been a very active research area in the past decade

Some actively researched PQC categories include

- Lattice-based
- Code-based
- Multivariate
- Hash/Symmetric key -based signatures
- Isogeny-based





$$\begin{tikzcd}
 & E_A \arrow[dr, "\psi_B"] \arrow[dd, dotted, shift left] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_{AB} \\
 & E_B \arrow[ur, "\psi_A"'] \arrow[uu, dotted, shift left] &
\end{tikzcd}$$

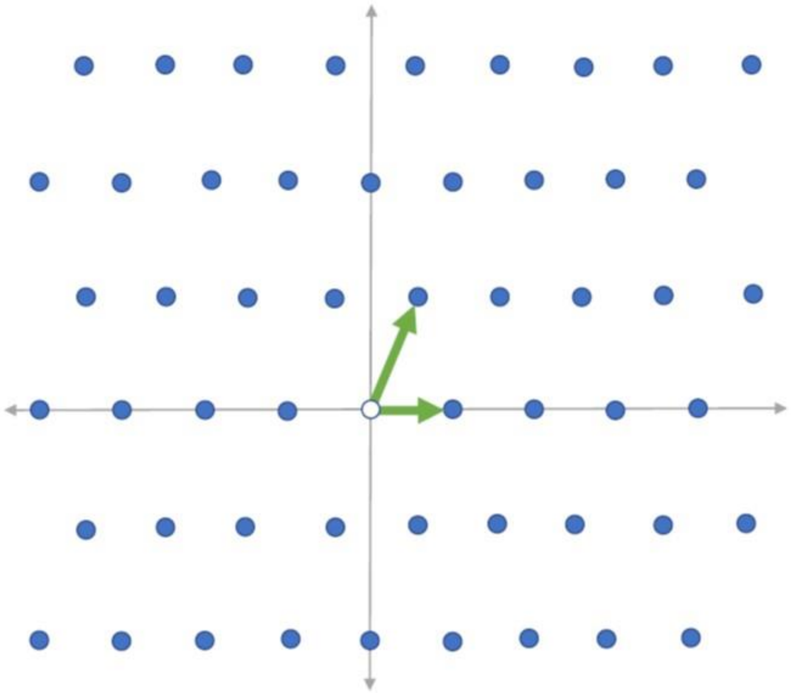
$$\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(1)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(1)}\cdot x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=i}^{n} p_{ij}^{(2)}\cdot x_i x_j \quad + \quad \sum_{i=1}^{n} p_i^{(2)}\cdot x_i + p_0^{(2)}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

LATTICES

A lattice is a set of evenly spaced points in some space S.

A lattice L is generated by a finite number of vectors $\{b_0, b_1, \dots, b_{n-1}\}$.

These n vectors are known as the basis of the lattice, where n is the dimension of the lattice

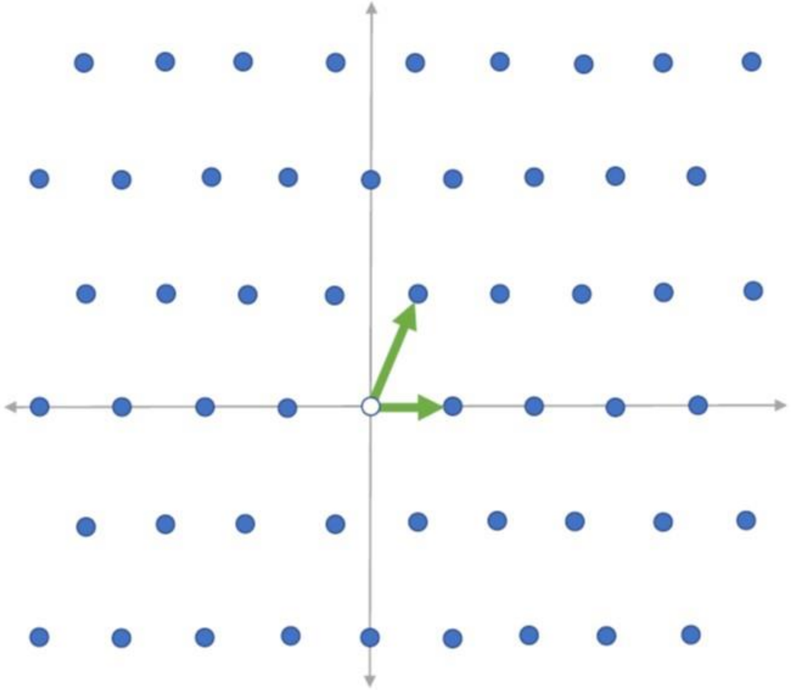


Example in $\mathbb{R}^2$. Basis elements

LATTICES

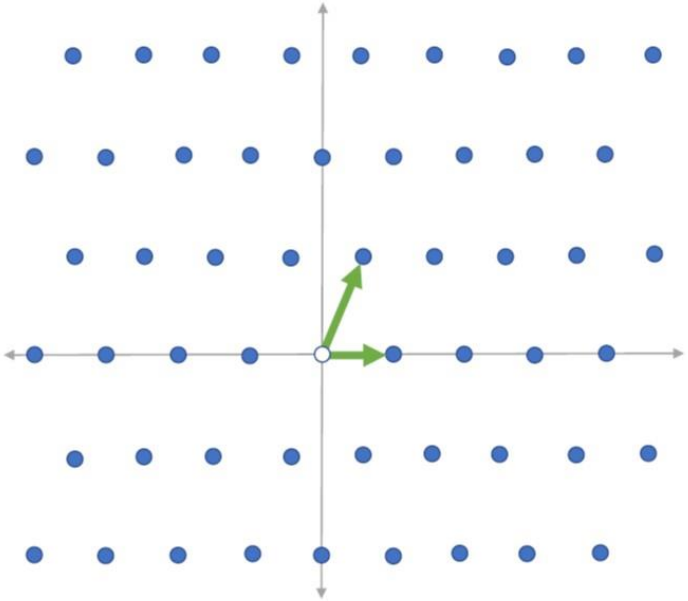
Shortest vector problem (SVP)

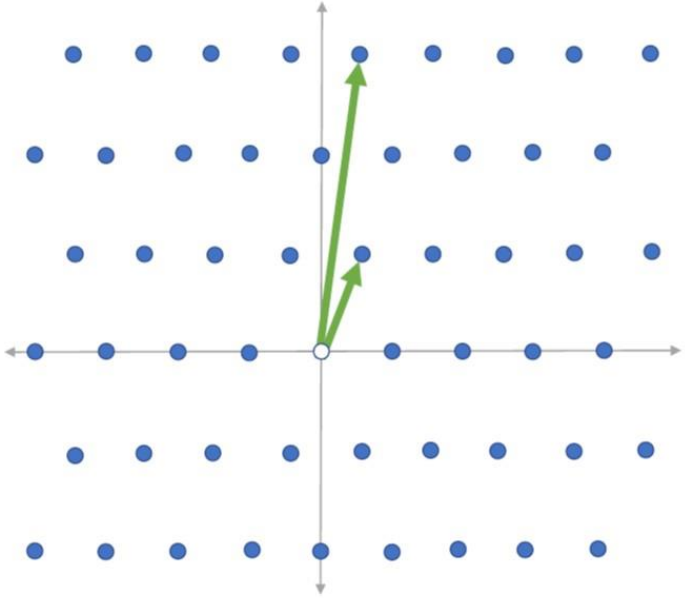
given a lattice L, one must find (one of) the shortest nonzero vector(s) in L



LATTICES

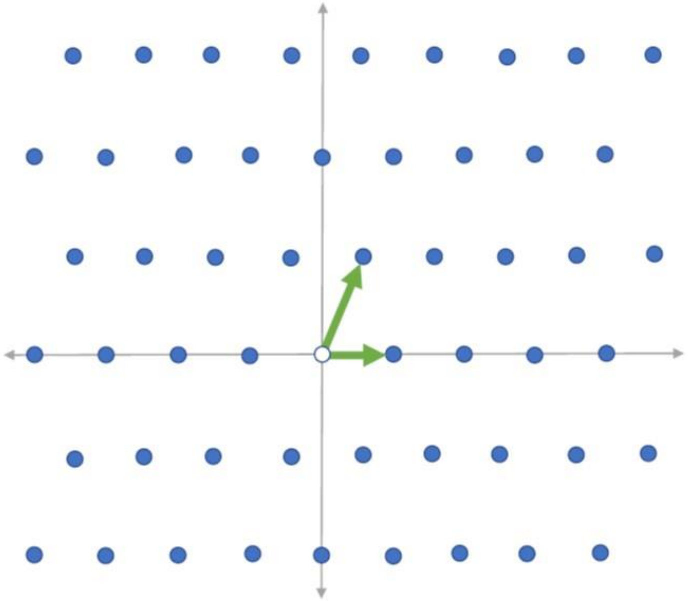
Shortest vector problem (SVP): given a lattice L, one must find (one of)   the shortest nonzero vector(s) in L



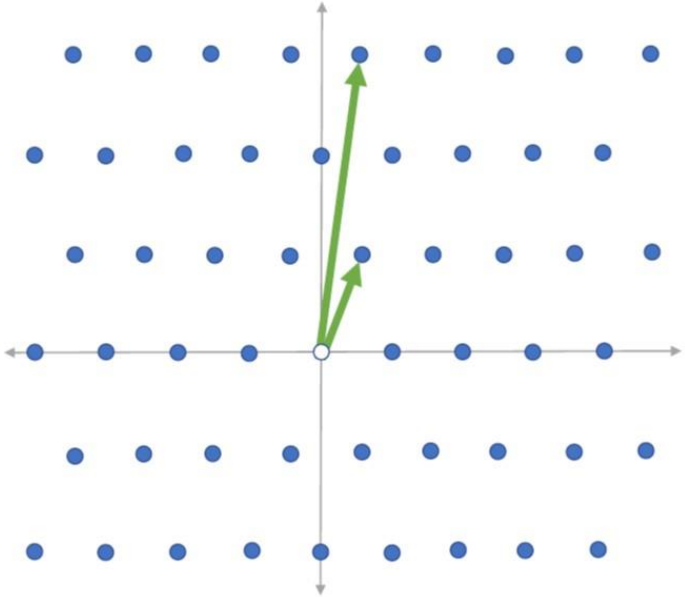


LATTICES

Shortest vector problem (SVP): given a lattice L, one must find (one of) the shortest nonzero vector(s) in L



"good" basis – Private key



"bad" basis – Public key

SYSTEMS OF MULTIVARIATE QUADRATIC EQS

Recall systems of linear equations:

$$4x_1 - x_2 = 1$$
$$-3x_1 + 2x_2 = 8$$

System of 2 equations in 2 variables.

SYSTEMS OF MULTIVARIATE QUADRATIC EQS

Recall systems of linear equations:

$$4x_1 - x_2 = 1$$
$$-3x_1 + 2x_2 = 8$$

System of 2 equations in 2 variables.

Coefficients $\{4, -1, -3, 2\}$ and solutions $\{2,7\} \in \mathbb{R}$

SYSTEMS OF MULTIVARIATE QUADRATIC EQS

Recall systems of linear equations:

$$4x_1 - x_2 = 1$$
$$-3x_1 + 2x_2 = 8$$

System of 2 equations in 2 variables.

Coefficients $\{4, -1, -3, 2\}$ and solutions $\{2,7\} \in \mathbb{R}$

A general system of multivariate quadratic (MQ) equations involves m equations in n variables with coefficients and solutions (if any) in some field.

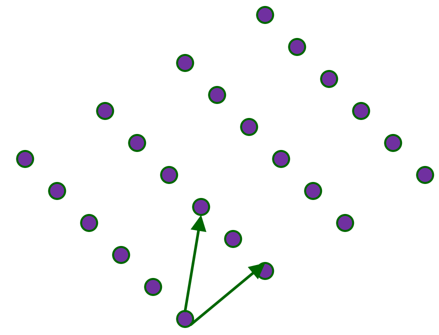
MQ Cryptosystems can generically be constructed by

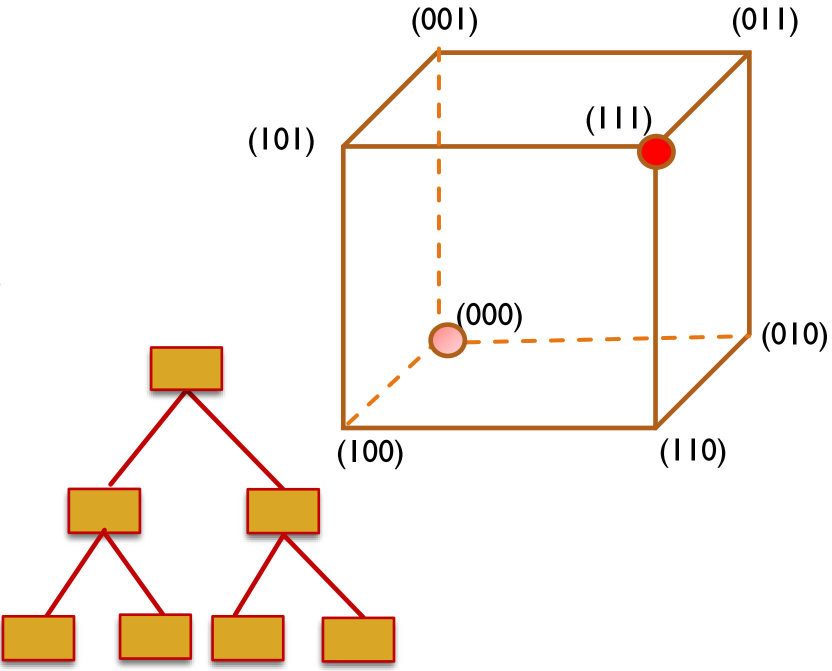
- Making public the matrix of coefficients and the right-hand side of equations and
- Incorporating the solution vector into the shared secret

POST QUANTUM CRYPTOGRAPHY (PQC)

Areas of mathematics comprising PQC and cryptanalysis:

- Probability theory
- Lattice theory
- Coding theory
- Algebraic geometry
- Group theory
- …





$$\begin{tikzcd}
 & E_A \arrow[dr, "\psi_B"] \arrow[dd, dotted, shift left] & \\
E \arrow[ur, "\phi_A"] \arrow[dr, "\phi_B"'] & & E_{AB} \\
 & E_B \arrow[ur, "\psi_A"'] \arrow[uu, dotted, shift left] &
\end{tikzcd}$$

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

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

$$\vdots$$

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

KEY CHALLENGES IN POST-QUANTUM CRYPTOGRAPHY

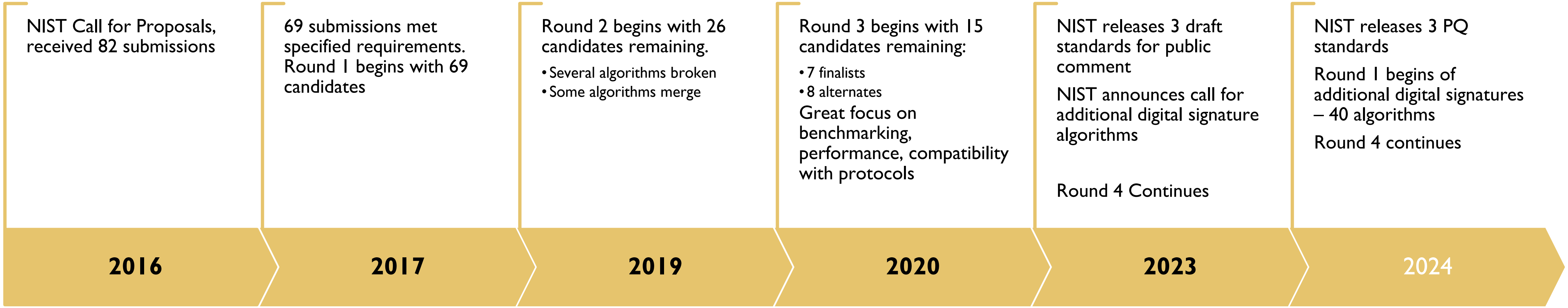
- Security vs. performance tradeoff
- Example of remaining algorithms under consideration for post-quantum key establishment

Classical vs PQ	Algorithm	Public key size (bytes)	Ciphertext size (bytes)	KeyGen (kilocycles)	Encaps (kilocycles)	Decaps (kilocycles)
PQ	BIKE	1,540	1,572	589	97	1,135
PQ	HQC	2,249	4,497	87	204	362
PQ	mceliece348864f	261,120	96	35,978	38	128
PQ – standard	Kyber-512	800	768	123	155	289
Classical – standard	ECDH NIST P-256	64	64	187	187	187

SELECTION CRITERIA

- Secure against both classical and quantum attacks
- Performance
- Other properties:
  - Compatibility with existing protocols and networks
  - Resistance to side-channel attacks
  - Perfect forward secrecy
  - Simplicity and flexiblity
  - Misuse resistance, etc.

TIMELINE



NIST Call for Proposals, received 82 submissions

2016

69 submissions met specified requirements. Round 1 begins with 69 candidates

2017

Round 2 begins with 26 candidates remaining.

- Several algorithms broken
- Some algorithms merge

2019

Round 3 begins with 15 candidates remaining:

- 7 finalists
- 8 alternates

Great focus on benchmarking, performance, compatibility with protocols

2020

NIST releases 3 draft standards for public comment

NIST announces call for additional digital signature algorithms

Round 4 Continues

2023

NIST releases 3 PQ standards

Round 1 begins of additional digital signatures – 40 algorithms

Round 4 continues

2024

OBSERVATIONS AND EXPERIENCES

Security analysis of cryptographic algorithms

- Benefits from community effort

Greenland
Iceland
Finland
Sweden
Norway
Russia
United Kingdom
Poland
Ukraine
France
Spain
Italy
Kazakhstan
Mongolia
Canada
United States
North Pacific Ocean
North Atlantic Ocean
Mexico
Turkey
Iraq
Iran
Afghanistan
Pakistan
China
South Korea
Japan
Algeria
Libya
Egypt
Saudi Arabia
India
Thailand
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Venezuela
Colombia
DR Congo
Kenya
Tanzania
Indonesia
Papua New Guinea
Peru
Brazil
Bolivia
Angola
Namibia
Botswana
Madagascar
Indian Ocean
South Pacific Ocean
South Atlantic Ocean
Chile
South Africa
Australia
Argentina
New Zealand

OBSERVATIONS AND EXPERIENCES

Security analysis of cryptographic algorithms

- Benefits from community effort
- Often relies on previous cryptanalytic experience

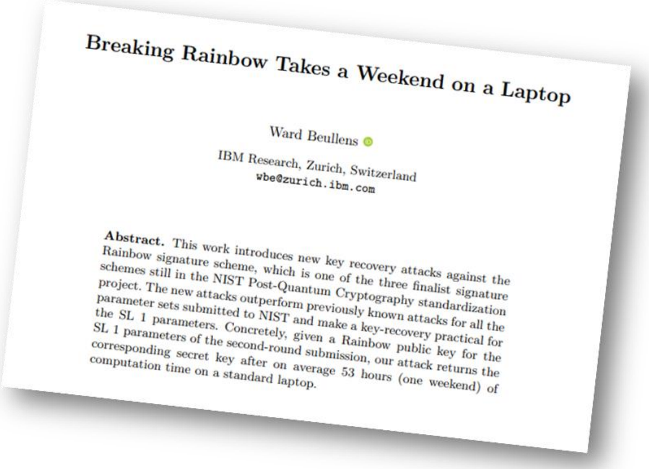
Greenland
Iceland
Finland
Sweden
Norway
Russia
United Kingdom
Poland
Germany
Ukraine
France
Italy
Spain
Kazakhstan
Mongolia
Canada
United States
Mexico
North Pacific Ocean
North Atlantic Ocean
Turkey
Iraq
Iran
Afghanistan
Pakistan
China
South Korea
Japan
India
Thailand
Algeria
Libya
Egypt
Saudi Arabia
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Venezuela
Colombia
Kenya
DR Congo
Tanzania
Indonesia
Papua New Guinea
Peru
Brazil
Bolivia
Angola
Namibia
Botswana
Madagascar
Indian Ocean
Australia
South Pacific Ocean
South Atlantic Ocean
Chile
South Africa
Argentina
New Zealand
K
Z
E
I
H
F
L
N
A
C
J
G
B
W
R
S
V
Q
U
Y
X
T

OBSERVATIONS AND EXPERIENCES

Security analysis of cryptographic algorithms

- Benefits from community effort
- Often relies on previous cryptanalytic experience
- Takes time

Greenland
Iceland
Finland
Sweden
Norway
United Kingdom
Poland
Ukraine
France
Spain
Italy
Russia
Kazakhstan
Mongolia
Turkey
Canada
United States
Mexico
North Pacific Ocean
North Atlantic Ocean
Algeria
Libya
Egypt
Iraq
Iran
Afghanistan
Pakistan
China
South Korea
Japan
Saudi Arabia
India
Thailand
Mali
Niger
Chad
Sudan
Nigeria
Ethiopia
Venezuela
Colombia
Kenya
DR Congo
Tanzania
Indonesia
Papua New Guinea
Peru
Brazil
Bolivia
Angola
Namibia
Botswana
Madagascar
Indian Ocean
South Pacific Ocean
South Atlantic Ocean
Chile
Argentina
South Africa
Australia
New Zealand



Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

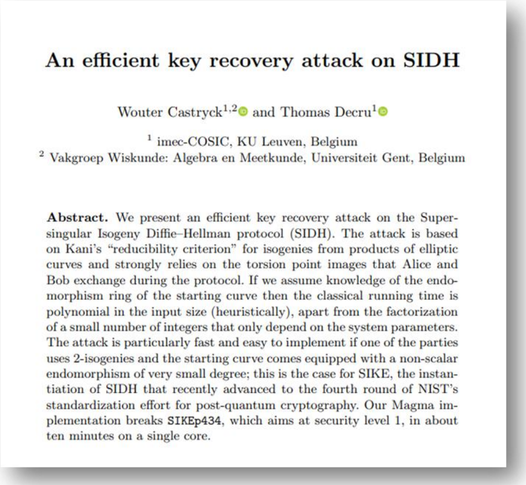
IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

OBSERVATIONS AND EXPERIENCES

Security analysis of cryptographic algorithms

- Benefits from community effort
- Often relies on previous cryptanalytic experience
- Takes time
- Can result in unexpected outcomes

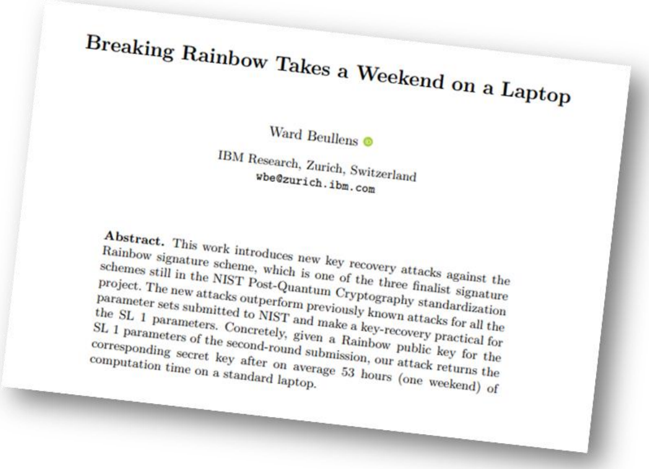


An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
[2] Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

Abstract. We present an efficient key recovery attack on the Supersingular Isogeny Diffie–Hellman protocol (SIDH). The attack is based on Kani's "reducibility criterion" for isogenies from products of elliptic curves and strongly relies on the torsion point images that Alice and Bob exchange during the protocol. If we assume knowledge of the endomorphism ring of the starting curve then the classical running time is polynomial in the input size (heuristically), apart from the factorization of a small number of integers that only depend on the system parameters. The attack is particularly fast and easy to implement if one of the parties uses 2-isogenies and the starting curve comes equipped with a non-scalar endomorphism of very small degree; this is the case for SIKE, the instantiation of SIDH that recently advanced to the fourth round of NIST's standardization effort for post-quantum cryptography. Our Magma implementation breaks SIKEp434, which aims at security level 1, in about ten minutes on a single core.



Breaking Rainbow Takes a Weekend on a Laptop

Ward Beullens

IBM Research, Zurich, Switzerland
wbe@zurich.ibm.com

Abstract. This work introduces new key recovery attacks against the Rainbow signature scheme, which is one of the three finalist signature schemes still in the NIST Post-Quantum Cryptography standardization project. The new attacks outperform previously known attacks for all the parameter sets submitted to NIST and make a key-recovery practical for the SL 1 parameters. Concretely, given a Rainbow public key for the SL 1 parameters of the second-round submission, our attack returns the corresponding secret key after on average 53 hours (one weekend) of computation time on a standard laptop.

CONSIDERATIONS AND IMPACT

Threat to long-term security

- What data do you need to protect?
- How long does this data need to be stored?
- "Harvest now, decrypt later" threat
- Lower risk tolerance requires more urgent transition to PQC

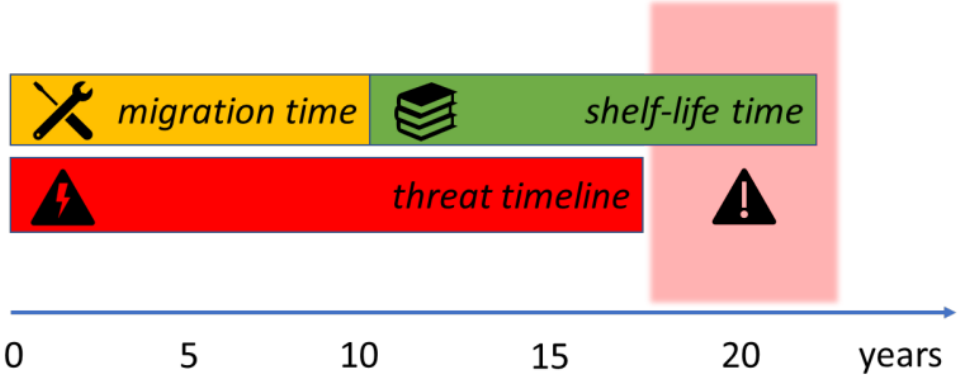


Figure 1 The timeline for the development of quantum computers that may pose a threat to cybersecurity should be compared with the time needed to migrate the cyber-system to post-quantum security combined with the shelf-life time of the data to be protected. See main text for details.

Quantum Threat Timeline Report, 2021
Global Risk Institute

CONSIDERATIONS AND IMPACT

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Threat to long-term security

- What data do you need to protect?
- How long does this data need to be stored?
- "Harvest now, decrypt later" threat
- Lower risk tolerance requires more urgent transition to PQC

PQC Migration

- Migrating to new cryptographic algorithms takes time
  - Historical examples: 3DES to AES, transition to ECC, transition to SHA1, etc.
- National Cybersecurity Center of Excellence (NCCoE) PQC Migration project
  - https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
  - Initiating the development of practices to aid in transition away from quantum-vulnerable algorithms and adopt PQC standards

NEXT STEPS FOR NIST PQC

Release 4th Standard

- Public comment period on 3 draft standards: FIPS 203, 204, 205 closed November 22, 2023
- NIST released FIPS 203, 204, 205 in August 2024
- NIST to release 4th draft standard in early 2025

Additional Digital Signatures

- NIST received 50 submissions and deemed 40 to be complete and proper candidates
- 40 candidate packages posted on July 17, 2023 to NIST webpage. NIST encourages
  - Security analysis
  - Implementations
  - Benchmarking

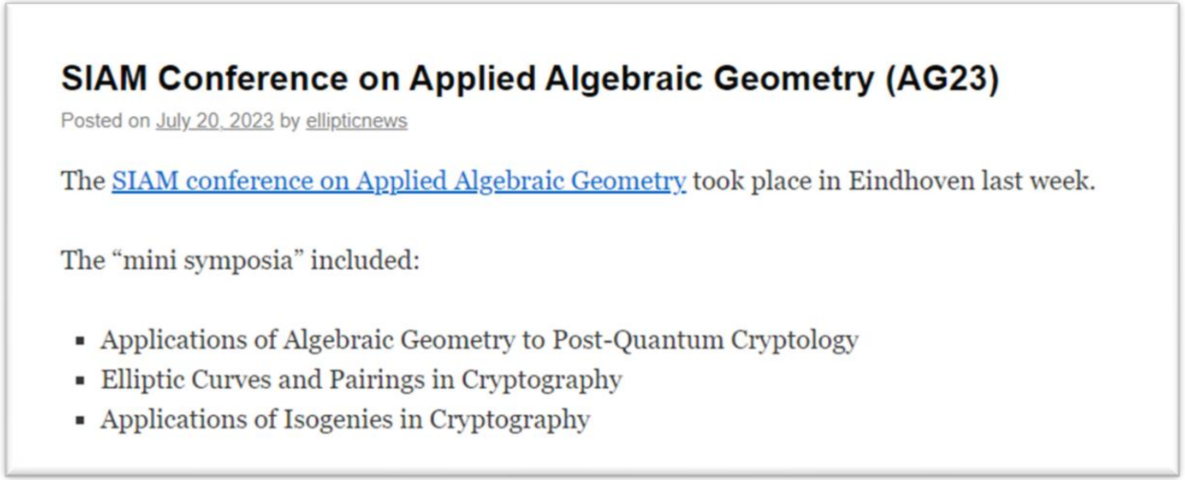
Round 4

- 4 remaining candidates in Round 4
  - SIKE was broken and no longer under consideration
- NIST encourages
  - Security analysis
  - Implementations
  - Benchmarking

FUTURE OF PQC

Research

- Implementations of algorithms
  - Secure optimizations in hardware, software, …
  - Protections against side-channel attacks
- Development of new algorithms
  - Key agreement
  - Digital signatures
  - Homomorphic encryption
  - Secure multiparty computation
- Cryptanalysis



SIAM Conference on Applied Algebraic Geometry (AG23)

Posted on July 20, 2023 by ellipticnews

The SIAM conference on Applied Algebraic Geometry took place in Eindhoven last week.

The "mini symposia" included:

- Applications of Algebraic Geometry to Post-Quantum Cryptology
- Elliptic Curves and Pairings in Cryptography
- Applications of Isogenies in Cryptography

Workforce development

- Curriculum expansion
  - Course offerings and availability
  - Interdisciplinary coursework
- Internships
- Summer/Winter schools

NIST PQC RESOURCES

https://csrc.nist.gov/projects/post-quantum-cryptography

- NIST PQC Standardization Conference Series
- NIST PQC Seminar
  - Videos, slides available
- Subscribe to PQC Forum
- Submission packages from all NIST PQC rounds

Angela Robinson:

Angela.robinson@nist.gov

NIST PQC Technical Inquiries:

pqc-comments@nist.gov