The State of Post-Quantum Cryptography

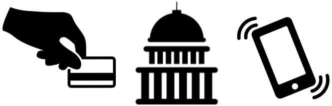
Valerie Gilchrist

Université Libre de Bruxelles and FRIA, Brussels, Belgium

July 6, 2023

What is cryptography?

From Wikipedia: "Cryptography...is the practice and study of techniques for secure communication in the presence of adversarial behaviour."



Cryptography is essential in industries such as banking, communications, and government.

What is cryptography?

Cryptosystems rely on *hard problems* (a.k.a *one-way function* or *cryptographic functions*).

These are mathematical functions that are easy to compute but hard to undo.

$$\text{e.g. } p, q \mapsto p \cdot q = N$$

$$N \not\mapsto p, q$$

What is cryptography?

Cryptosystems rely on *hard problems* (a.k.a *one-way function* or *cryptographic functions*).

These are mathematical functions that are easy to compute but hard to undo.

$$\text{e.g. } p, q \mapsto p \cdot q = N$$
$$N \not\mapsto p, q$$

This was the first ever hard problem, and it was used for a system called *RSA*.

Many banks, emails, computers, and messaging apps use RSA, and thus depend on the hardness of integer factorization.

Other classical hard problems

Classical Diffie-Hellman uses the *Discrete Log Problem (DLP)*:

$$g, x \mapsto g^x$$

$$g, g^x \not\mapsto x$$

Other classical hard problems

Classical Diffie-Hellman uses the *Discrete Log Problem (DLP)*:

$$g, x \mapsto g^x$$

$$g, g^x \not\mapsto x$$

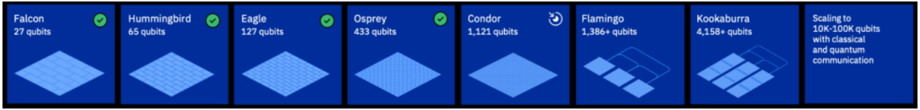
A commonly used variant of DLP is the *Elliptic Curve Discrete Log Problem (ECDLP)*:

$$n, P \mapsto nP$$

$$nP, P \not\mapsto n$$

The quantum threat

A sufficiently large quantum computer could break the RSA hard problem using *Shor's algorithm*.



Post-quantum crypto

We need new hard problems that are still hard for quantum computers.

- If the hard problem runs on a **quantum** computer it is called *quantum cryptography*.
- If the hard problem runs on a **classical** computer it is called *post-quantum cryptography* (PQC).

Post-quantum crypto

We need new hard problems that are still hard for quantum computers.

- If the hard problem runs on a **quantum** computer it is called *quantum cryptography*.
- If the hard problem runs on a **classical** computer it is called *post-quantum cryptography* (PQC).

A *key exchange mechanism (KEM)* is a system that allows to parties to agree on a shared secret.

A *digital signature* is a system that allows a user to authenticate messages.

NIST competition

In 2016 the American National Institute of Standards and Technology (NIST) began a competition to standardize post-quantum cryptographic protocols.

NIST competition

In 2016 the American National Institute of Standards and Technology (NIST) began a competition to standardize post-quantum cryptographic protocols.

Currently there are 5 main branches of post-quantum cryptography:

- lattice-based
- code-based
- multivariate
- hash-based
- isogeny-based

NIST competition

Round 1		
Type	KEMs	sigs
Lattices	22 21	5 4
Codes	19 15	3 1
Multivariate	4 2	7
Hash	0	2
Isogenies	1	0
Other	4 1	2 1

NIST competition

Round 1		
Type	KEMs	sigs
Lattices	22 21	5 4
Codes	19 15	3 1
Multivariate	4 2	7
Hash	0	2
Isogenies	1	0
Other	4 1	2 1

Round 2		
Type	KEMs	sigs
Lattices	9	3
Codes	7	0
Multivariate	0	4
Hash	0	1
Isogenies	1	0
Other	0	1

NIST competition

NIST continued with rounds 3 and 4.

NIST competition

NIST continued with rounds 3 and 4.

Two finalists, *Rainbow* and *SIKE*, were fully broken during this time.

NIST competition

NIST continued with rounds 3 and 4.

Two finalists, *Rainbow* and *SIKE*, were fully broken during this time.

The following have been fully stanardized so far:

- CRYSTALS-Kyber (lattice KEM)
- CRYSTALS-Dilithium (lattice sig)
- FALCON (lattice sig)
- SPHINCS+ (hash sig)

NIST competition

NIST continued with rounds 3 and 4.

Two finalists, *Rainbow* and *SIKE*, were fully broken during this time.

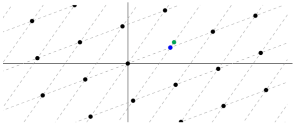
The following have been fully stanardized so far:

- CRYSTALS-Kyber (lattice KEM)
- CRYSTALS-Dilithium (lattice sig)
- FALCON (lattice sig)
- SPHINCS+ (hash sig)

NIST called for new round of signature submissions on June 2, 2023.

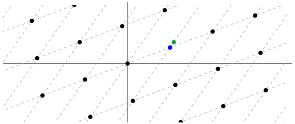
Lattices

A *lattice* can be thought of as a grid, where the points are whole numbers.



Lattices

A *lattice* can be thought of as a grid, where the points are whole numbers.

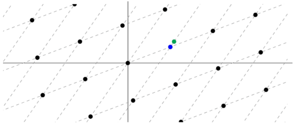


Some hard problems include:

- Finding the shortest vector in a lattice (SVP)
- Finding the vector closest to some other vector (CVP)

Lattices

A *lattice* can be thought of as a grid, where the points are whole numbers.



Some hard problems include:

- Finding the shortest vector in a lattice (SVP)
- Finding the vector closest to some other vector (CVP)

Lattice-based cryptography has proven (so far) to be the fastest, but requires a lot of memory.

Crystals-Kyber (KEM), Crystals-Dilithium (sig), and Falcon (sig) have all been selected for standardization by NIST.

Codes

A *code* is a set of sequences of symbols, where the symbols belong to a particular alphabet.
e.g. binary strings whose digits sum to an even number

Codes

A *code* is a set of sequences of symbols, where the symbols belong to a particular alphabet. e.g. binary strings whose digits sum to an even number

The *Syndrome Decoding (SD) Problem* says that given a matrix, H, and vector $\mathbf{s}$, it is hard to find a "small" vector $\mathbf{x}$ such that

$$H\mathbf{x}^T = \mathbf{s}^T.$$

Codes

A *code* is a set of sequences of symbols, where the symbols belong to a particular alphabet. e.g. binary strings whose digits sum to an even number

The *Syndrome Decoding (SD) Problem* says that given a matrix, H, and vector $\mathbf{s}$, it is hard to find a "small" vector $\mathbf{x}$ such that

$$H\mathbf{x}^T = \mathbf{s}^T.$$

Classic McEliece (KEM), HQC (KEM), and BIKE (KEM) have advanced to the fourth round of the NIST standardization competition.

Multivariate

Multivariate polynomials are polynomials in more than one variable, generally defined over a finite field.

Multivariate

Multivariate polynomials are polynomials in more than one variable, generally defined over a finite field.

Let P, S, T be easily invertible multivariate polynomials.
It is hard to invert the composition

$$M := P \circ S \circ T.$$

Multivariate

Multivariate polynomials are polynomials in more than one variable, generally defined over a finite field.

Let P, S, T be easily invertible multivariate polynomials.
It is hard to invert the composition

$$M := P \circ S \circ T.$$

Multivariate signature schemes have very small signature sizes, relative to other types of PQC.
Signature schemes based on multivariate hard problems have been submitted to NIST for review.

Rainbow

Rainbow was a multivariate signature scheme, and a finalist in the NIST competition.

Ward Beullens (IBM Zurich) published a full key recovery attack titled *Breaking Rainbow Takes a Weekend on a Laptop*.

The attack used differentials to recover the secret key in 53 hours on a laptop.

Hash

A *hash function* maps inputs of variable size to outputs of fixed size.

Hash

A *hash function* maps inputs of variable size to outputs of fixed size.

Let H be a hash function.
Given $H(x)$ it is hard to recover x.

Hash

A *hash function* maps inputs of variable size to outputs of fixed size.

Let H be a hash function.
Given $H(x)$ it is hard to recover x.

Hash functions have been studied for longer than PQC, so they offer more confidence in their security compared to younger fields.

SPHINCS+ (sig) was selected for standardization by NIST.

Isogenies

An *elliptic curve* can be written as

$$E : y^2 = x^3 + ax + b.$$

An *isogeny* is a mapping between two elliptic curves

$$\phi : E \to E'.$$

Given two elliptic curves it is hard to find an isogeny between them.

Isogenies

An *elliptic curve* can be written as

$$E : y^2 = x^3 + ax + b.$$

An *isogeny* is a mapping between two elliptic curves

$$\phi : E \to E'.$$

Given two elliptic curves it is hard to find an isogeny between them.

Isogeny-based cryptography is very slow, but has small key sizes.
Isogeny signature schemes appear promising and have been submitted to NIST for review.

SIKE

SIKE was an isogeny-based key exchange scheme that had made it to round 4 in the NIST standardization competition.

SIKE

SIKE was an isogeny-based key exchange scheme that had made it to round 4 in the NIST standardization competition.

In July 2022, a full key recovery attack was published about SIKE from Wouter Castryck and Thomas Decru (KU Leuven).

SIKE

SIKE was an isogeny-based key exchange scheme that had made it to round 4 in the NIST standardization competition.

In July 2022, a full key recovery attack was published about SIKE from Wouter Castryck and Thomas Decru (KU Leuven).

This serves as a reminder that cryptography, and in particular PQC, is a very fast-paced field. Hard problems are hard computationally, but security can't be proven mathematically.

Looking to the future

Are we ready to convert fully to PQC?

Looking to the future

Are we ready to convert fully to PQC?
No. But hybrid approaches are a good compromise (for now).

Looking to the future

Are we ready to convert fully to PQC?
No. But hybrid approaches are a good compromise (for now).

Is the NIST competition over?

Looking to the future

Are we ready to convert fully to PQC?
No. But hybrid approaches are a good compromise (for now).

Is the NIST competition over?
No... it might never be.

Looking to the future

Are we ready to convert fully to PQC?
No. But hybrid approaches are a good compromise (for now).

Is the NIST competition over?
No... it might never be.

Can I do my masters/PhD on a PQC topic?

Looking to the future

Are we ready to convert fully to PQC?
No. But hybrid approaches are a good compromise (for now).

Is the NIST competition over?
No... it might never be.

Can I do my masters/PhD on a PQC topic?
Yes! There is still lots to do both in the way of theory and implementation.

Looking to the future

Are we ready to convert fully to PQC?
No. But hybrid approaches are a good compromise (for now).

Is the NIST competition over?
No... it might never be.

Can I do my masters/PhD on a PQC topic?
Yes! There is still lots to do both in the way of theory and implementation.