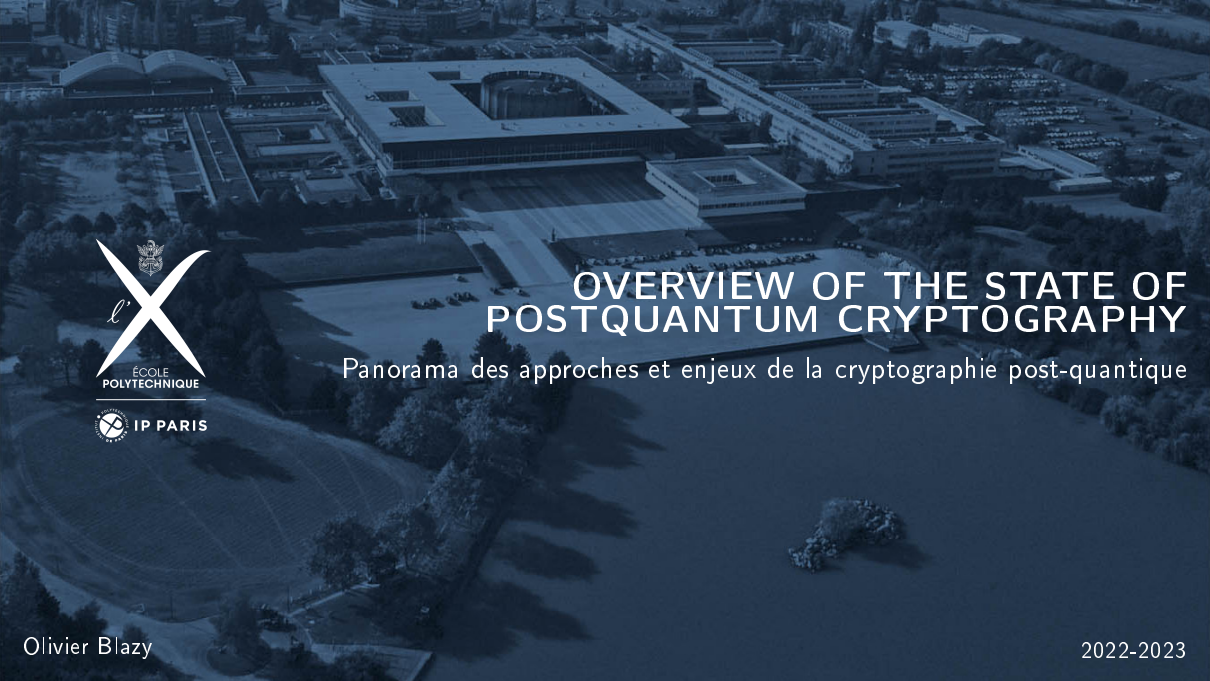


# OVERVIEW OF THE STATE OF POSTQUANTUM CRYPTOGRAPHY

## Panorama des approches et enjeux de la cryptographie post-quantique

Olivier Blazy

2022-2023

# 1
# QUICK REMINDERS ON CRYPTO

# CRYPTOGRAPHY GOALS

Ensure communication security over a public channel with adversaries

- Passive: The adversaries listen to the conversation (Eavesdropper)
- Active: They can write, alter, remove communications over the channel

What is the secret ingredient?

# QUICK TIMELINE





- Artisanal Age: ($\sim$ 1900)
  - Caesar: Each letter is replaced by one 3 steps after
  - Generalized in basic permutation / substitution (Vigenere, Hill, ...)
- Mechanical Age: ($\sim$ 1900 $\rightarrow$ 1970)
  - Substitution and permutation are done by machines (Hagelin, Enigma (2nd WW))
- Paradoxical Age: (Since 1970)
  - Doing impossible things: Zero-Knowledge Proofs, Anonymous Authentication, Machine Learning on Encrypted Data

# QUICK TIMELINE

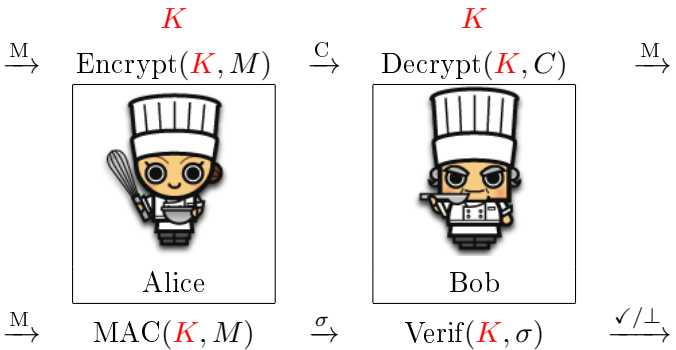




- Artisanal Age: ($\sim$ 1900)
  - Caesar: Each letter is replaced by one 3 steps after
  - Generalized in basic permutation / substitution (Vigenere, Hill, ...)
- Mechanical Age: ($\sim$ 1900 $\rightarrow$ 1970)
  - Substitution and permutation are done by machines (Hagelin, Enigma (2nd WW))
- Paradoxical Age: (Since 1970)
  - Doing impossible things: Zero-Knowledge Proofs, Anonymous Authentication, Machine Learning on Encrypted Data
  - Post-Quantum Cryptography

# SYMMETRIC CRYPTOGRAPHY

The key $K$ used to encrypt / sign is the same used to decrypt / verify




Security (Enc): Without knowing $K$ one cannot recover $M$. (DES, AES, ...)
Security (Auth): Without knowing $K$ one cannot authenticate $M$.

# ASYMMETRIC CRYPTOGRAPHY

There is a set of keys, a public key $P_B$ accessible by everyone to encrypt, and a secret key $K_B$ to decrypt possessed only by Bob.

$\xrightarrow{M}$ Encrypt$(P_B, M)$ $\xrightarrow{C}$ Decrypt$(K_B, C)$ $\xrightarrow{M}$



$\xrightarrow{M}$ Sign$(K_A, M)$ $\xrightarrow{\sigma}$ Verif$(P_A, \sigma)$ $\xrightarrow{\checkmark/\perp}$

Security (Enc): Without knowing $K_B$ one cannot recover $M$ even when knowing $P_B$. (RSA, ElGamal, ...)

Security (Auth): Without knowing $K_A$ one cannot sign $M$ even when knowing $P_A$.

# PARAMETERS





- With current computers, we consider that $2^{64}$ operations is within reach of an adversary.
- Birthday paradox says that 128 bits of security is de-facto the minimum requirement. (256, or even 512 are more and more recommended)
- For asymmetric cryptography, one may want at least 1536 bits for RSA, et 256 for Elliptic Curves.

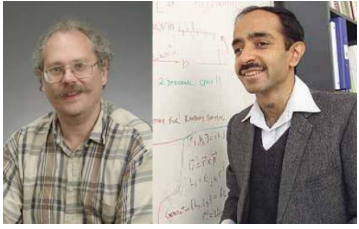
# 2
# THE QUANTUM MENACE

# QUANTUM AGAINST CRYPTOGRAPHY



1994 Peter Shor proposed a quantum algorithm breaking discrete logarithm and factorisation assuming enough qubits.

1996 Grover proposed a quantum algorithm allowing to search unstructured sets of size $N$ in $O(\sqrt{N})$



# A BRIEF SUMMARY

| | Symmetric | Asymmetric |
|---|---|---|
| Encryption | Grover | Shor |
| Authentication | Grover | Shor |

**Encryption:** Save now, attack later
**Signature:** Need a live attack

# A DANGER, NOT SO CLOSE



Applying Shor algorithm requires:

- a huge number of qubits
- even more quantum gates

Estimates show that for the 256 bits of security, we need **2330** qubits to break the discrete logarithm on elliptic curves, and **3072** to factor an RSA modulus.

Current best quantum computer claims... **256** qubits with some restriction.

# 3
# A POSTQUANTUM WORLD

# WHAT WOULD REMAIN AFTER THE QUANTUM TSUNAMI?





| | |
|---|---|
| Cryptography based on isogenies? | Probably |
| Lattice-based / Code-based cryptography? | Quite likely |
| Multivariate cryptography? | Quite likely too |
| Hash-based cryptography? | Yes! (but no encryption) |

# *NEW* HYPOTHESES: CODES/LATTICES





**Syndrome Decoding / Short Integer Solution**

Given $\mathbf{A}$, $\mathbf{s}$ find a *small* $\mathbf{x}$ such that $\mathbf{Ax} = \mathbf{s}$

**Learning With Error**

Given $\mathbf{A}$, and $\mathbf{c}$, decide whether $\mathbf{c}$ is *close* to the span of $\mathbf{A}$. (ie $\mathbf{c} = \mathbf{As} + \mathbf{e}$)

Warning Depending on the underlying ring/field, the noise sampling, the metric used, this can go very poorly

# NEW HYPOTHESES, SAME TECHNIQUES: ISOGENIES





## Random walks on graph

$$\begin{array}{ccc} E & \xrightarrow{\phi_1} & E_1 \\ \downarrow \phi_2 & & \downarrow \phi_2 \\ E_2 & \xrightarrow{\phi_1} & E_{12} \end{array}$$

## Computation Supersingular Diffie-Hellman

Given $E, E_1, E_2$, find $E_{12}$.

Warning The main problem (SIDH) was broken this summer (few seconds on a laptop). But CSIDH using group action remains safe.

**The MQ Problem**

Given

- A finite field of $q$ elements $\mathbb{F}_q$;
- $m$ quadratic polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n]$ in $n$ variables.

Find a solution $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$ to the system of equations $p_i(X_1, \ldots, X_n) = 0$.

Warning Finding the right balance between efficiency and security is complex, and lead to attacks.

# ENTER THE NIST PQ COMPETITION





- International Call in 2016
- 69 proposals at Round 1 (16 Fr)
- Round 2, only 26 remains
  - 9 Signatures (**Lattices, MV, Hash**) (3 Fr)
  - 17 KEM (**Lattices, Codes, Isogenies**) (6 Fr)
- Round 3, 7 finalists, 8 alternates:
  - 3 (+3) Signatures (**Lattices, MV, Hash**) (3 + 1 Fr)
  - 4 (+5) KEM (**Lattices, Codes, Isogenies**) (2 + 2 Fr)
- Standardisation of 3 Signatures, and 1 KEM all **Lattices** (2,1 Fr)
  - Round 4, for 4 KEM (**Codes, Isogenies**) (2 Fr) For October'22, then Summer'23?
  - New call for other kind of signatures For June'23

Pros: Many research papers, new attacks, tested in the wild (TLS 1.3...)

Cons: A lot of noise, and non scientific disruptions

# RESULTS OF NIST

A PostQuantum world



## Standardized* (Lattices)

E/$\sigma$ **CRYSTAL-Kyber/ Dilithium**: ENS Lyon, ARM, NXP, CWI, RUB, SRI, IBM, Waterloo, Radboud

$\sigma$ **FALCON**: Rennes 1, Thales, Brown, IBM, NCC, OnBoard Security

$\sigma$ **SPHINCS$^+$**: Taurus, RUB, KUL, Graz, Genua, Eindhoven, G, Infineon, Cisco, USD, Radboud, Cloudflare

## 4th Round, Encryption

- **Classic McEliece**: Inria, RHUL, RUB, Sinica, Okinawa, ETHZ, Eindhoven, G, FAU, MPI, Yale, PQSolutions
- **HQC**: Rennes, Worldline, Enac, U.Toulon, U.Limoges, U.Bordeaux, Polytechnique, G, FAU
- **BIKE**: Rennes, Wordline, Enac, U.Limoges, Supaero, Inria, Bordeaux, Polytechnique, UoW, Intel, Haifa, RUB, G, FAU
- **SIKE**: IBM, Infosec Global, Louisian Tech, Linkedin, NRC, TI, Radboud, Toronto, Waterloo, FAU, A,M

# RESULTS OF NIST





## Standardized* (Lattices)

E/$\sigma$ **CRYSTAL-Kyber/ Dilithium**: ENS Lyon, ARM, NXP, CWI, RUB, SRI, IBM, Waterloo, Radboud

$\sigma$ **FALCON**: Rennes 1, Thales, Brown, IBM, NCC, OnBoard Security

$\sigma$ **SPHINCS$^+$**: Taurus, RUB, KUL, Graz, Genua, Eindhoven, G, Infineon, Cisco, USD, Radboud, Cloudflare

## 4th Round, Encryption

- **Classic McEliece**: Inria, RHUL, RUB, Sinica, Okinawa, ETHZ, Eindhoven, G, FAU, MPI, Yale, PQSolutions
- **HQC**: Rennes, Worldline, Enac, U.Toulon, U.Limoges, U.Bordeaux, Polytechnique, G, FAU
- **BIKE**: Rennes, Wordline, Enac, U.Limoges, Supaero, Inria, Bordeaux, Polytechnique, UoW, Intel, Haifa, RUB, G, FAU

? **SIKE**: IBM, Infosec Global, Louisian Tech, Linkedin, NRC, TI, Radboud, Toronto, Waterloo, FAU, A,M

# AND NOW?

## Should we switch to PQC?

ANSSI, and other agencies are warning that switching to PQC only is probably risky, an hybrid design (**Vanilla+PQC**) seems safer and wiser.
Schemes that were in the final stages were broken on classical computers. It is still **too early** to trust them completely

Classical **hybrid** design would be only slightly less efficient than PQC only (Increase by 10%). It is also an interesting path of research to explore this hybrid aspect and see if there are further optimizations possible between the standards/finalists and classical schemes.

NIST and NSA have been very elliptical about this...

# WRAPPING UP

**Quantum Computers!**
Will annihilate classical cryptography...
some day

**4 main kind of hypotheses exist**
Lattice and codes are the safest choice for now, as they have been extensively studied

**Encryption**
Can still be meaningful in 20 years, so we need to update today

**France**
Is well represented, 25% of the submission, 75% of the standards/finalists