

# Quantum Computing and Cryptography

Damien, Théo, Matthieu

University

February 12, 2025

- 1 Intro
- 2 RSA
- 3 Quantum computing
  - Introduction to the quantum world
  - Quantum algorithms
- 4 Post-Quantum cryptography
  - Intro to PQ cryptography
  - Lattice cryptography
  - Limits of PQ cryptography
- 5 Conclusion

# Introduction

- Cryptography=TODO
- TODO: secret

# Introduction

- Cryptography=TODO
  - TODO: secret
- Science of secret



## Classical bit

$$b \in \{0, 1\}$$

## Classical bit

$$b \in \{0, 1\}$$

- 0

## Classical bit

$b \in \{0, 1\}$

- 0
- 1



## Classical bit

$$b \in \{0, 1\}$$

- 0
- 1

## Quantum bit

$$|\psi\rangle \in \mathbb{C}^2$$

## Classical bit

$$b \in \{0, 1\}$$

- 0
- 1

## Quantum bit

$$|\psi\rangle \in \mathbb{C}^2$$

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

## Classical bit

$$b \in \{0, 1\}$$

- 0
- 1

## Quantum bit

$$|\psi\rangle \in \mathbb{C}^2$$

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

## Classical bit

$$b \in \{0, 1\}$$

- 0
- 1

## Quantum bit

$$|\psi\rangle \in \mathbb{C}^2$$

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

- $|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

## Classical bit

$$b \in \{0, 1\}$$

- 0
- 1

## Quantum bit

$$|\psi\rangle \in \mathbb{C}^2$$

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

- $|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
- $|-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

- $\langle 0| \Rightarrow 0$  (100%)

- $\langle 0 | \Rightarrow 0$  (100%)
- $\langle 1 | \Rightarrow 1$  (100%)

- $\langle 0| \Rightarrow 0$  (100%)
- $\langle 1| \Rightarrow 1$  (100%)
- $\langle +| \Rightarrow 0$  (50%),  $1$  (50%)



- $\langle 0| \Rightarrow 0$  (100%)
- $\langle 1| \Rightarrow 1$  (100%)
- $\langle +| \Rightarrow 0$  (50%),  $1$  (50%)
- $\langle -| \Rightarrow 0$  (50%),  $1$  (50%)

- Gate  $X$

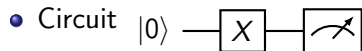
- Gate  $X$ 
  - $X|0\rangle \rightarrow |1\rangle$

- Gate  $X$

- $X|0\rangle \rightarrow |1\rangle$
- $X|1\rangle \rightarrow |0\rangle$

- Gate  $X$

- $X|0\rangle \rightarrow |1\rangle$
- $X|1\rangle \rightarrow |0\rangle$



- Gate  $H$

- Gate  $H$ 
  - $H|0\rangle \rightarrow |+\rangle$

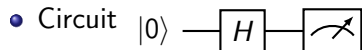
- Gate  $H$

- $H|0\rangle \rightarrow |+\rangle$
- $H|1\rangle \rightarrow |-\rangle$



- Gate  $H$

- $H|0\rangle \rightarrow |+\rangle$
- $H|1\rangle \rightarrow |-\rangle$



# Problème B.V

Given the oracle of a function  $f$  :

$$f : \{0, 1\}^n \rightarrow \{0, 1\} \quad f(x) = x \cdot s$$

Find  $s$  in the few request possible.

# Algo classique - Slide 1

with  $n = 2$  try :

- $f(10) = s_0$

2 requests.

with  $n = 2$  try :

- $f(10) = s_0$
- $f(01) = s_1$

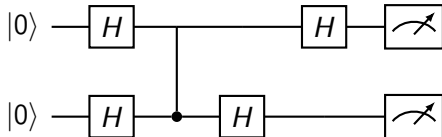
2 requests.

in general :  $\mathcal{O}(n) \rightarrow$  Try every  $x$  that contains one bit to 1. At each query, we get the value of that bit in  $s$

$\mathcal{O}(1) \rightarrow$  Just try every  $x$  at the same time.

Not only the  $x$  with only one bit at one but every possible  $x$ .

# Algo Quantique - Slide 2



- Gain de complexité :  $\mathcal{O}(e^b) \rightarrow \mathcal{O}(b)$



- Gain de complexité :  $\mathcal{O}(e^b) \rightarrow \mathcal{O}(b)$
- combien de qubit il faut

- Gain de complexité :  $\mathcal{O}(e^b) \rightarrow \mathcal{O}(b)$
- combien de qubit il faut
- combien de cubit on as

# What is PQ cryptography

- Based on (other) mathematical problems
- Considered unsolvable by a quantum computer

What it is not :

- Cryptography **using** quantum technologies

# The problems

- Codes
- Hash functions
- Multivariate polynomials systems
- Isogenies
- Lattices

# The problems

- Codes
- Hash functions
- Multivariate polynomials systems
- Isogenies
- **Lattices**

# Why lattices ?

- Well spread
- Good results

Encryption/Key encapsulation	
Crystals-Kyber	Lattices
Signatures	
Crystals-Dilithium	Lattices
Falcon	Lattices
Sphincs+	Hash

# What is a lattice ?

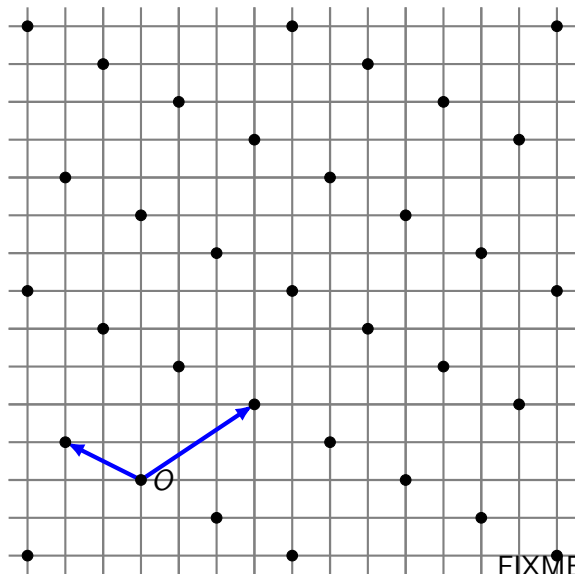
- A discrete subgroup of  $\mathbb{R}^n$

abc akpqzsfkeokf akoczckdp kpzqkfs pkzapqfkpkde pzkpkd czqks qkp  
kfsdkvoesd, okpze kswkw k

Like vector spaces, we have :

- Vectors and matrices
- Linear combination

# What is a lattice ? (cont'd)



FIXME : Basis:



TODO

# (Fully) homomorphic encryption

TODO

Size 

TODO	
------	--

# Not necessarily robust to classical computer

- Example : Supersingular isogenies Diffie-Hellman key exchange

# Conclusion