Quantum Computing and Cryptography

Damien, Théo, Matthieu

University

February 12, 2025

Outline

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

Outline

Introduction

- Cryptography=TODO
- TODO: secret

Introduction

- Cryptography=TODO
- TODO: secret

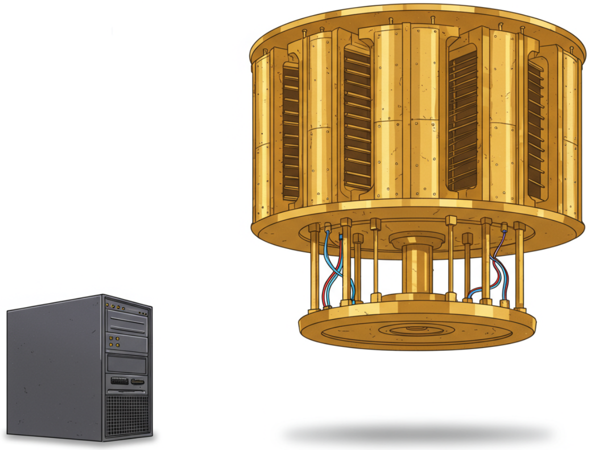
$\rightarrow$ Science of secret

Outline

RSA

Outline

Quantum computing



Outline

Qubits

Classical bit

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

Qubits

Classical bit

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

- 0

Qubits

Classical bit

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

- 0
- 1

Qubits

Classical bit

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

- 0
- 1

Quantum bit

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

Qubits

Classical bit

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

- 0
- 1

Quantum bit

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

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

Qubits

Classical bit

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

- 0
- 1

Quantum bit

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

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

Qubits

Classical bit

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

- 0
- 1

Quantum bit

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

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

Qubits

Classical bit

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

- 0
- 1

Quantum bit

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

- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
- $|-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

Measurements

Why measuring ?

We cannot read superposition. When we look at a qubit, it collapses to a classical bit.

Measurements

Why measuring ?

We cannot read superposition. When we look at a qubit, it collapses to a classical bit.

What do we get ?

We measure 0 or 1 with a probability that depends on the state of the qubit.

Measurements

Why measuring ?

We cannot read superposition. When we look at a qubit, it collapses to a classical bit.

What do we get ?

We measure 0 or 1 with a probability that depends on the state of the qubit.

- $|0\rangle \to 0$ (100%)

Measurements

Why measuring ?

We cannot read superposition. When we look at a qubit, it collapses to a classical bit.

What do we get ?

We measure 0 or 1 with a probability that depends on the state of the qubit.

- $|0\rangle \rightarrow 0$ (100%)
- $|1\rangle \rightarrow 1$ (100%)

Measurements

Why measuring ?

We cannot read superposition. When we look at a qubit, it collapses to a classical bit.

What do we get ?

We measure 0 or 1 with a probability that depends on the state of the qubit.

- $|0\rangle \rightarrow 0$ (100%)
- $|1\rangle \rightarrow 1$ (100%)
- $|+\rangle \rightarrow 0$ (50%), 1 (50%)

Measurements

Why measuring ?

We cannot read superposition. When we look at a qubit, it collapses to a classical bit.

What do we get ?

We measure 0 or 1 with a probability that depends on the state of the qubit.

- $|0\rangle \rightarrow 0$ (100%)
- $|1\rangle \rightarrow 1$ (100%)
- $|+\rangle \rightarrow 0$ (50%), 1 (50%)
- $|-\rangle \rightarrow 0$ (50%), 1 (50%)

NOT gate

X gate

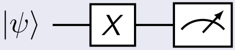
- $X\left|0\right\rangle \to \left|1\right\rangle$
- $X\left|1\right\rangle \to \left|0\right\rangle$

NOT gate

X gate

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

Circuit representation



Hadamard gate

H gate

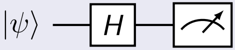
- $H\left|0\right\rangle \rightarrow \left|+\right\rangle$
- $H\left|1\right\rangle \rightarrow \left|-\right\rangle$

Hadamard gate

H gate

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

Circuit representation



Outline

Problème B.V

Given the oracle of a function f :
$f : \{0,1\}^n \to \{0,1\}$ $f(x) = x \cdot s$
Find s in the few request possible.

with $n = 2$ try :

- $f(10) = s_0$

2 requests.

with $n = 2$ try :

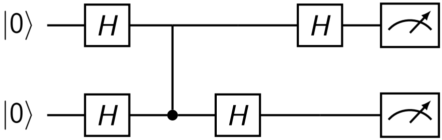
- $f(10) = s_0$
- $f(01) = s_1$

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



Shor

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

Shor

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

Shor

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

Outline

Outline

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
- Multivariates polynomials systems
- Isogenies
- Lattices

The problems

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

Why lattices ?

- Well spread
- Good results

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

Outline

What is a lattice ?

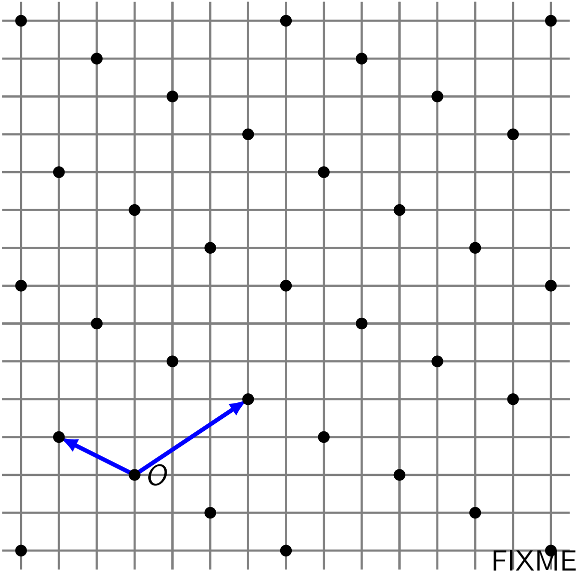
- A discret subgroup of RR^n

abc akpqzsfkeokf akozckdp 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:

Learning with error problem

TODO

(Fully) homomorphic encryption

TODO

Outline

Size	TODO	

Not necessary robust to classical computer

- Example : Supersingular isogenies Diffie-Hellman key exchange

Outline

Conclusion