Quantum Computing and Cryptography

Damien, Théo, Matthieu

University

February 12, 2025

Outline

Introduction

RSA

Qubits

- Classical bit $\rightarrow$ 0 or 1

Qubits

- Classical bit $\rightarrow$ 0 or 1
- Qubit $\rightarrow$ vector $\in \mathbb{C}^2$

Qubits

- Classical bit $\rightarrow$ 0 or 1
- Qubit $\rightarrow$ vector $\in \mathbb{C}^2$
- $\langle 0| = \begin{bmatrix} 1 & 0 \end{bmatrix}$

Qubits

- Classical bit $\rightarrow$ 0 or 1
- Qubit $\rightarrow$ vector $\in \mathbb{C}^2$
- $\langle 0| = \begin{bmatrix} 1 & 0 \end{bmatrix}$
- $\langle 1| = \begin{bmatrix} 0 & 1 \end{bmatrix}$

Qubits

- Classical bit $\rightarrow$ 0 or 1
- Qubit $\rightarrow$ vector $\in \mathbb{C}^2$
- $\langle 0| = \begin{bmatrix} 1 & 0 \end{bmatrix}$
- $\langle 1| = \begin{bmatrix} 0 & 1 \end{bmatrix}$
- $\langle +| = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \end{bmatrix}$

Qubits

- Classical bit $\rightarrow$ 0 or 1
- Qubit $\rightarrow$ vector $\in \mathbb{C}^2$
- $\langle 0| = \begin{bmatrix} 1 & 0 \end{bmatrix}$
- $\langle 1| = \begin{bmatrix} 0 & 1 \end{bmatrix}$
- $\langle +| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \end{bmatrix}$
- $\langle -| = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -1 \end{bmatrix}$

Mesures

- $\langle 0|$ => 0 (100%)

Mesures

- $\langle 0|$ => 0 (100%)
- $\langle 1|$ => 1 (100%)

Mesures

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

Mesures

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

Gates - Slide 1

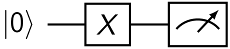
- Gate X

Gates - Slide 1

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

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

Gates - Slide 1

- Gate X
  - $X\ket{0} \to \ket{1}$
  - $X\ket{1} \to \ket{0}$
- Circuit 

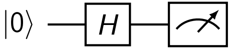
Gates - Slide 2

- Gate H

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

Gates - Slide 2

- Gate H
  - $H|0\rangle \to |+\rangle$
  - $H|1\rangle \to |-\rangle$

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

Problème B.V

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

Algo classique - Slide 1

with $n = 2$ try :

- $f(10) = s_0$

2 requests.

Algo classique - Slide 1

with $n = 2$ try :

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

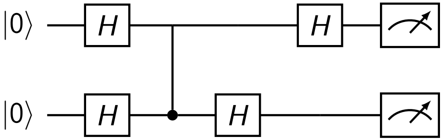
2 requests.

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

Algo Quantique - Slide 1

$\mathcal{O}(1) \rightarrow$ 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 : $\mathcal{O}(e^b) \rightarrow \mathcal{O}(b)$

Shor

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

Shor

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

Post-quantique

Conclusion