

De la quantique en cryptographie

Élie Besnard, Malo Leroy,
Yun Marcola–da-Cunha Macedo

Lycée Chateaubriand

26 juin 2022

Motivation

- Qu'est-ce que la cryptographie?

Motivation

- Qu'est-ce que la cryptographie?
- Ancrage au thème

Principes de quantique

■ Fonction d'état

Principes de quantique

- Fonction d'état
- États propres : $|0\rangle$, $|1011\rangle$, etc.

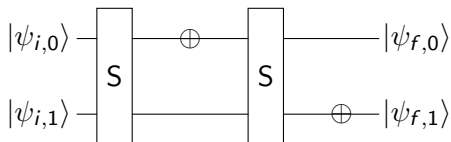
Principes de quantique

- Fonction d'état
- États propres : $|0\rangle$, $|1011\rangle$, etc.
- États superposés, amplitudes : $|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$

Principes de quantique

- Fonction d'état
- États propres : $|0\rangle$, $|1011\rangle$, etc.
- États superposés, amplitudes : $|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$
- Probabilité

Un exemple



$$(I_2 \otimes X) \cdot S \cdot (X \otimes I_2) \cdot S = I_4$$

Application : tests de parité

Oracles

- Phase : $U_f |x\rangle = (-1)^{f(x)} |x\rangle$
- Somme : $U_f |x, y\rangle = |x, y \oplus f(y)\rangle$

Calcul formel

- Valeurs exactes : $\frac{2}{5}$, $\sqrt{2}$, $e^{\frac{i\pi}{7}}$, $\pi + 3^{2/3}$, etc.

Calcul formel

- Valeurs exactes : $\frac{2}{5}$, $\sqrt{2}$, $e^{\frac{i\pi}{7}}$, $\pi + 3^{2/3}$, etc.
- Produit de Kronecker, produit matriciel, etc.

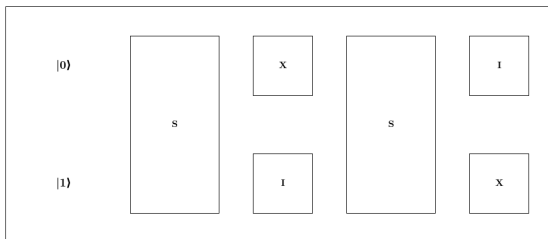
Calcul formel

- Valeurs exactes : $\frac{2}{5}$, $\sqrt{2}$, $e^{\frac{i\pi}{7}}$, $\pi + 3^{2/3}$, etc.
- Produit de Kronecker, produit matriciel, etc.
- Efficacité algorithmique

Interface graphique

Ordinateur Quantique

Exécuter

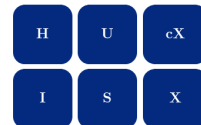


Dimensions du circuit

Nombre de qubits : 2

Nombre d'étapes : 5

Portes



Oracle

☒ Somme

$$U_f|x, y\rangle = |x, y \oplus f(y)\rangle$$

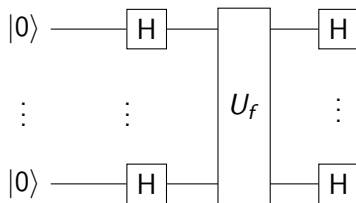
☐ Phase

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$

Éditeur de fonction

 $f(x) =$

Deutsch-Jozsa et Bernstein-Vazirani

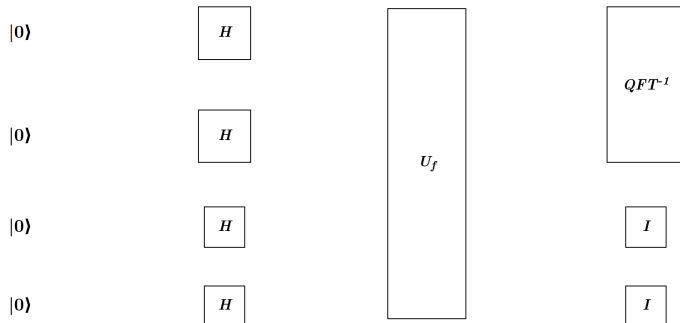


Application : Bernstein-Vazirani, $f(x_1, \dots, x_n) = \sum_{i=0}^n x_i \cdot a_i \in \mathbb{F}_2$

Shor : principe

- 1 a pseudo-aléatoire
- 2 Algorithme d'Euclide
- 3 Recherche de période

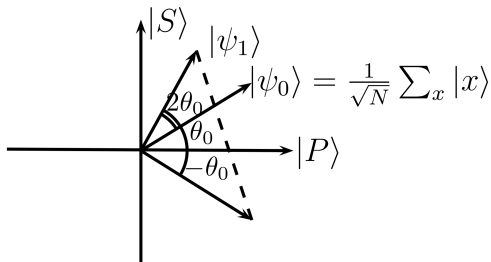
Shor : circuit



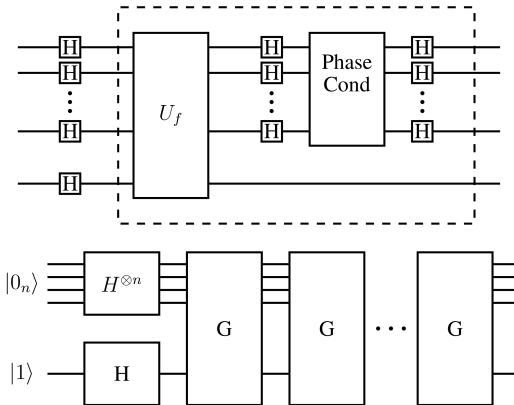
Fonction d'oracle : $f(x) = a^x \bmod N$

Grover : principe

Équation : $f(x_1, \dots, x_n) = 1$, résolution par rotations successives

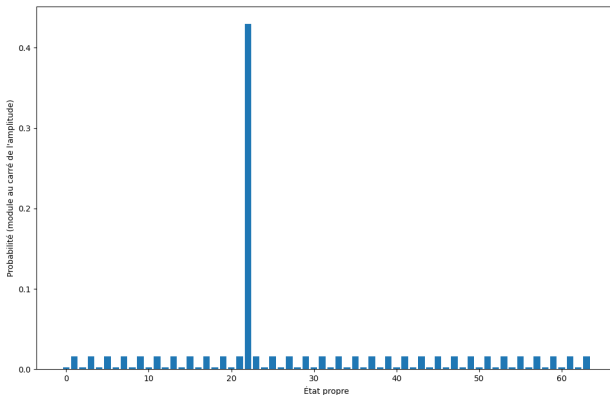


Grover : circuit



Grover : résultats

Exemple : la seule solution est (0, 1, 0, 1, 1, 0) soit 22



Protocoles

■ Protocole E91

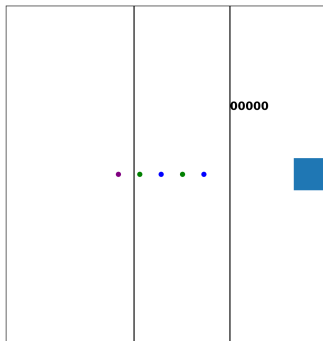
Protocoles

- Protocole E91
- Tentative de création d'un protocole

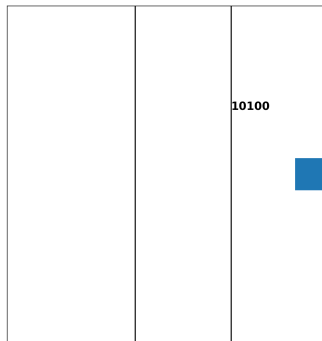
Protocoles

- Protocole E91
- Tentative de création d'un protocole
- Expérience : loi de Malus

Travaux sur la polarisation



Avant mesure



Après mesure