

De la quantique en cryptographie

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

Lycée Chateaubriand

24 juin 2022

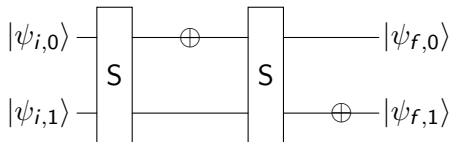
Motivation

- Qu'est-ce que la cryptographie ?

Motivation

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

Un exemple



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

Calcul formel

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

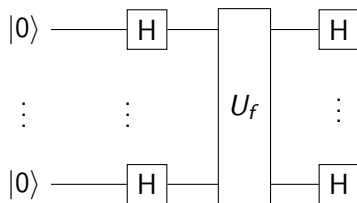
Calcul formel

- 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

Deutsch-Jozsa et Bernstein-Vazirani



Exemples : oracles

- de phase

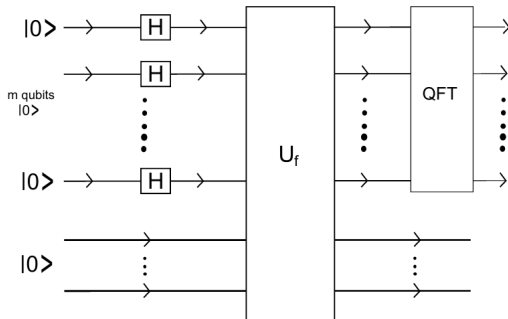
$$U_f |x\rangle = (-1)^{f(x)} |x\rangle$$

- par somme

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

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

Shor



Exemple :

Grover

Interface graphique

Cryptographie quantique

- Le protocole E91
 - Expérience
 - Simulation

Cryptographie quantique

- Le protocole E91
 - Expérience
 - Simulation
- Tentative de création d'un protocole