

# INTRODUCTION À L'ALGORITHMIQUE QUANTIQUE



---

Roxane LEDUC  
Oct. 2023 – Jan. 2024

# SOMMAIRE



1. Introduction

2. Un premier  
circuit quantique

3. Qubits, portes et  
mesures

4. Algorithmes de  
Deutsch/Grover

5. Algorithme  
de Shor

6. Circuit quantique  
de l'algorithme de  
Shor

7. Implémentation  
avec Qiskit

8. Conclusion



# INTRODUCTION

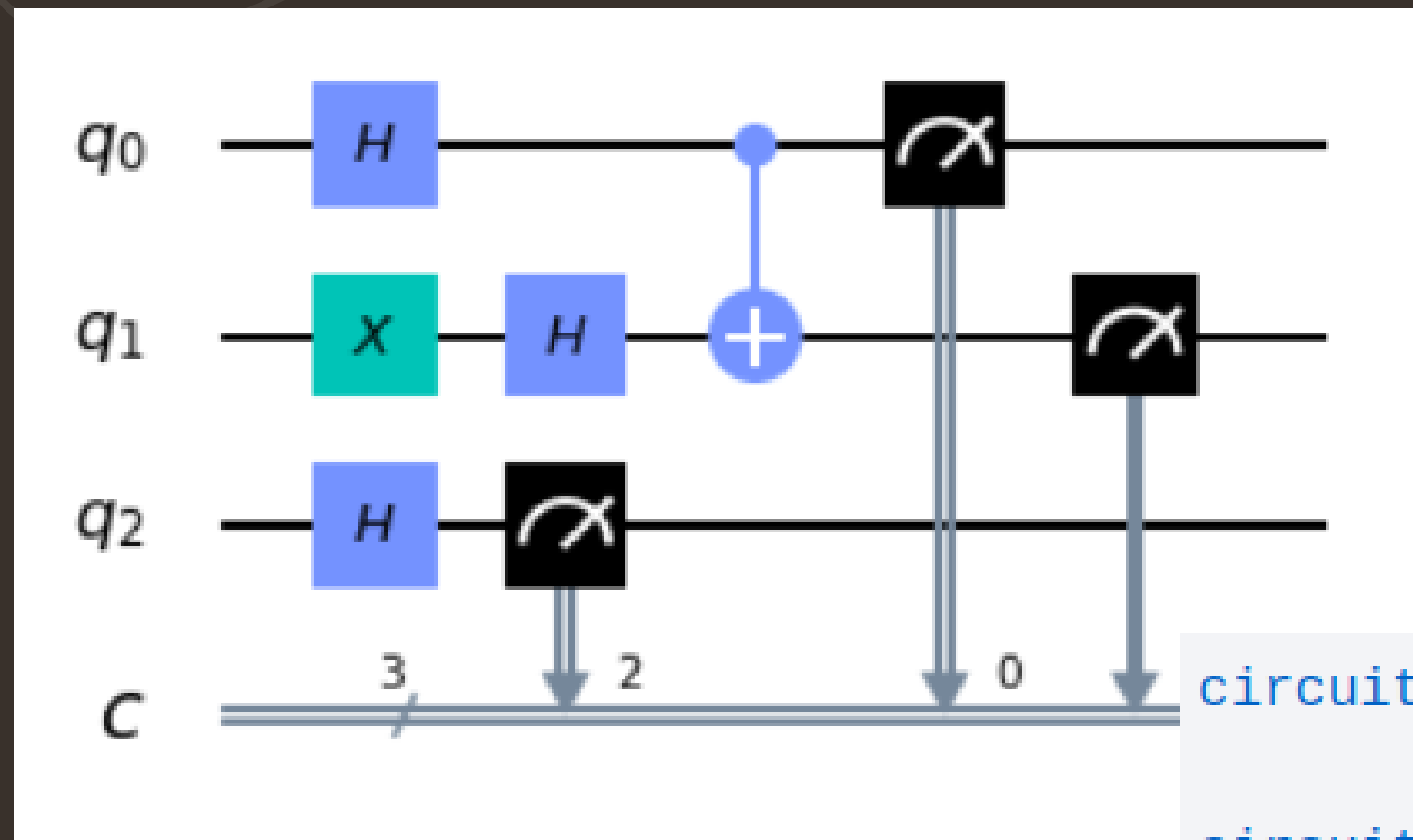


- Projet de Fin d'Études à l'INSA Rouen Normandie en collaboration avec le CEA.



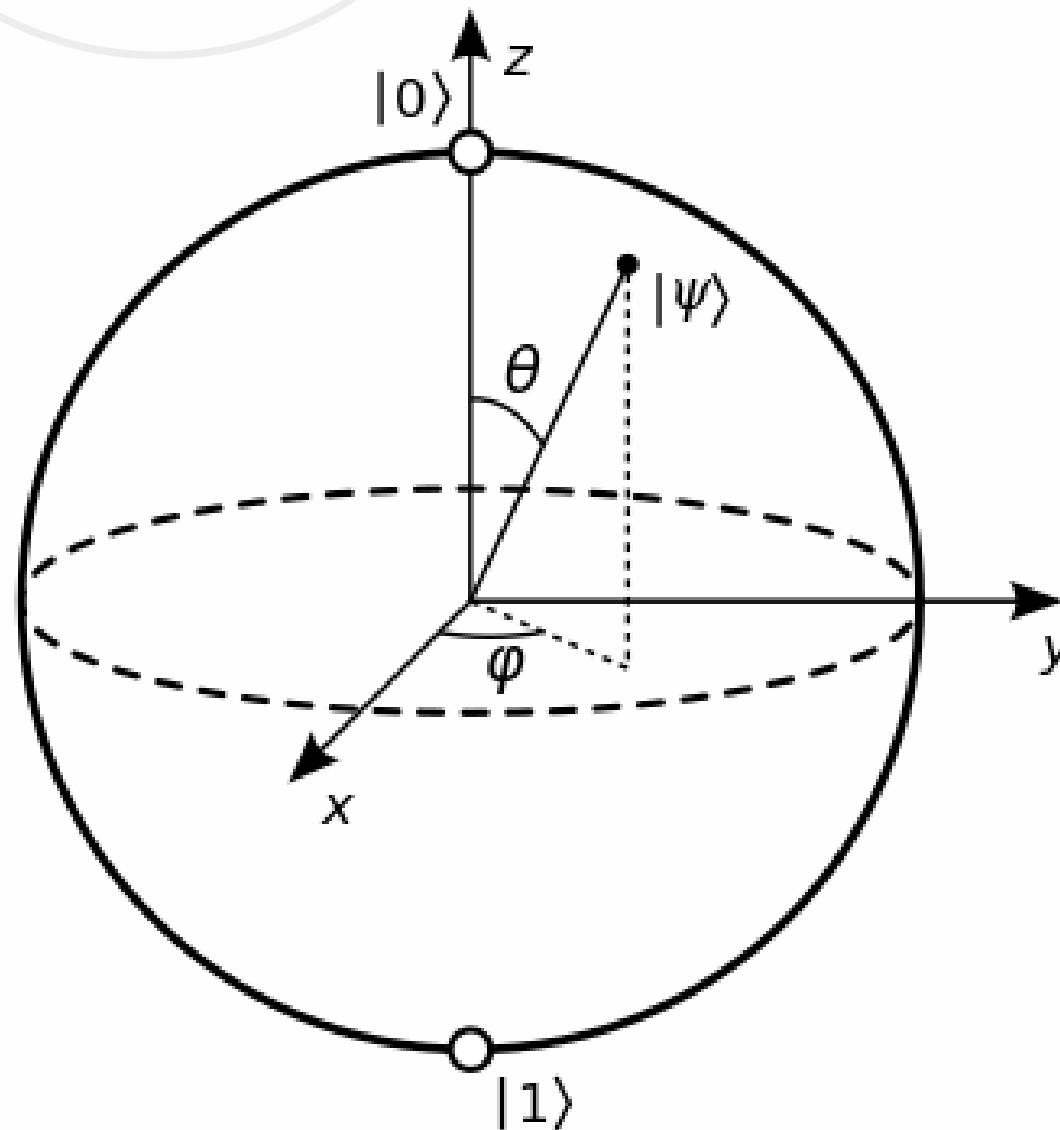
- Découvrir les grands principes de l'algorithmique quantique.
- Comprendre et implémenter l'algorithme de Shor.

# CIRCUIT



```
circuit = QuantumCircuit(3, 3)

circuit.x(1)
circuit.h(range(3))
circuit.cx(0, 1)
circuit.measure(range(3), range(3))
```



$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

$$|\psi\rangle \equiv \cos\left(\frac{\theta}{2}\right) |0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\phi} |1\rangle$$

$$\begin{array}{ll} \text{ket de } \Psi & \langle \Psi| = [\bar{\alpha}, \bar{\beta}] \\ |\Psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} & \end{array}$$

produit scalaire (inner product)

$$\langle \Psi | \Psi \rangle = [\bar{\alpha}, \bar{\beta}] \times \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha^2 + \beta^2 = 1$$

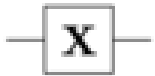



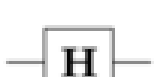
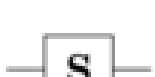


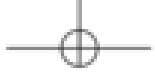




produit externe (outer product)

$$|\Psi\rangle\langle\Psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \times [\bar{\alpha}, \bar{\beta}] = \begin{bmatrix} \alpha\bar{\alpha} & \alpha\bar{\beta} \\ \beta\bar{\alpha} & \beta\bar{\beta} \end{bmatrix}$$

produit tensoriel (tensor product)

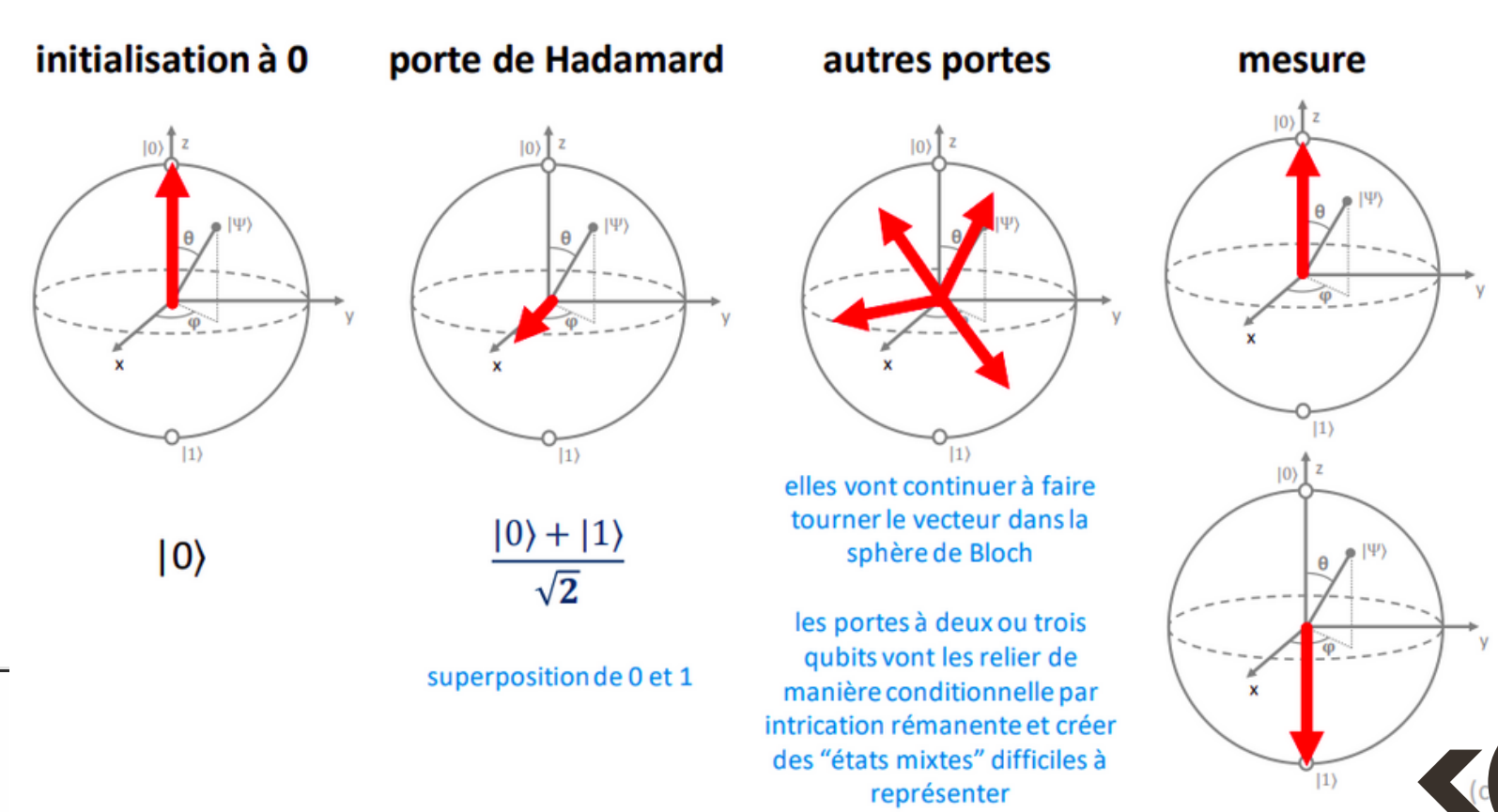
$$|\psi.\phi\rangle = |\psi\rangle \otimes |\phi\rangle$$

$$\begin{array}{ll} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \\ \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{array}$$

Operator	Gate(s)		Matrix
Pauli-X (X)			$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)			$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)			$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)			$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)			$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)			$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
SWAP			$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)			$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

# Grands principes de l'informatique quantique:

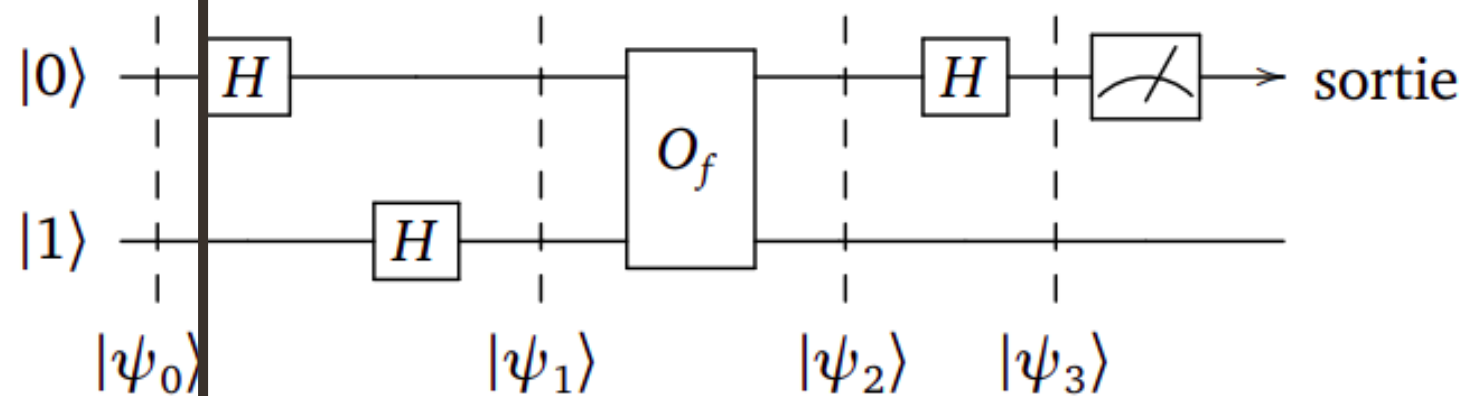
- Intrication
- Interférence
- Non-déterminisme
- Non-clonabilité



la mesure va retourner un |0> avec une probabilité  $\alpha^2$  dépendant de l'état évalué et l'état du qubit deviendra |0>

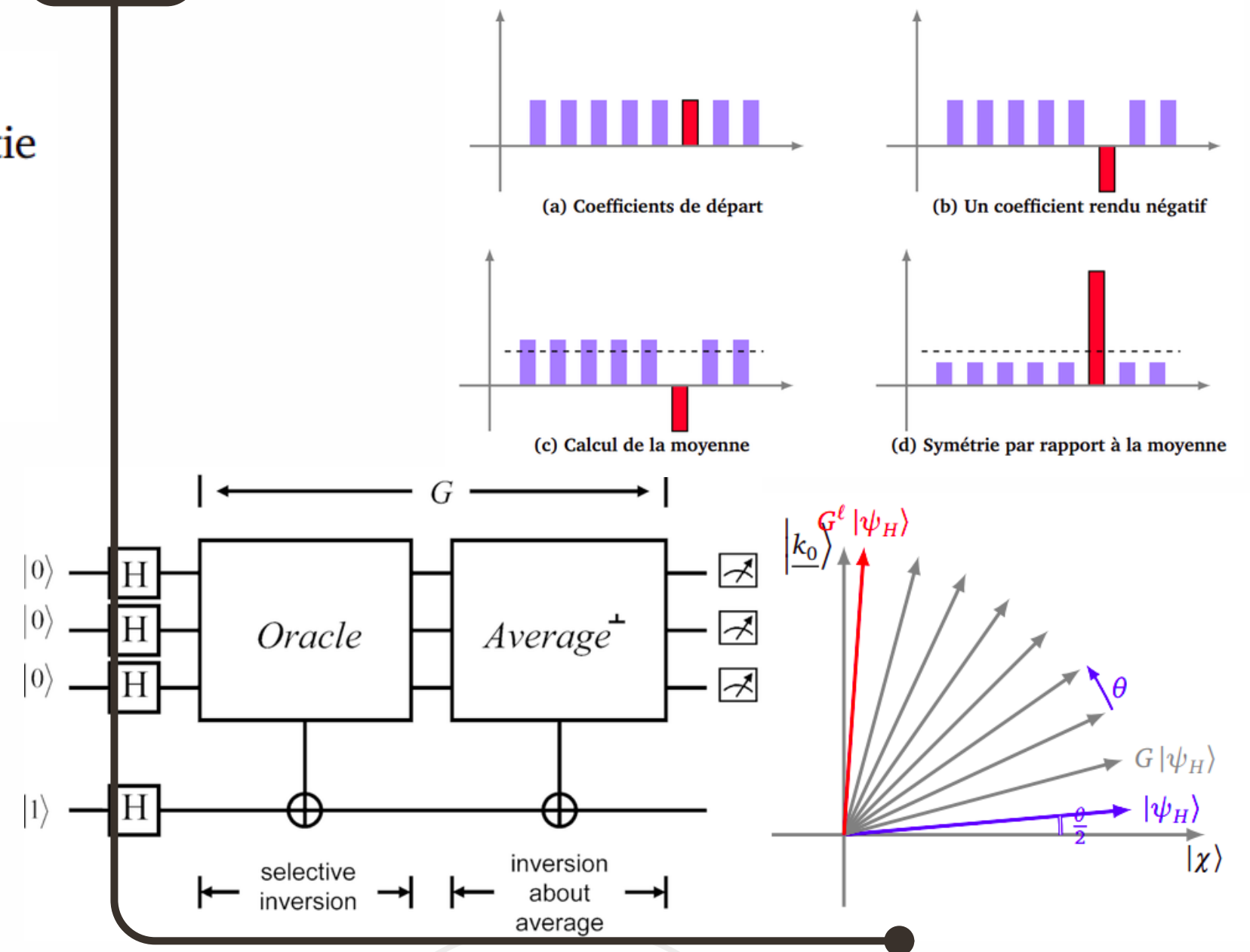
la mesure va retourner un |1> avec une probabilité  $\beta^2$  dépendant de l'état évalué et l'état du qubit deviendra |1>

## 01 Deutsch



$$|\psi_3\rangle \equiv \begin{aligned} &((-1)^{f(0)} + (-1)^{f(1)}) 0.0 \\ &+ (-(-1)^{f(0)} - (-1)^{f(1)}) 0.1 \\ &+ ((-1)^{f(0)} - (-1)^{f(1)}) 1.0 \\ &+ (-(-1)^{f(0)} + (-1)^{f(1)}) 1.1 \end{aligned}$$

## 02 Grover

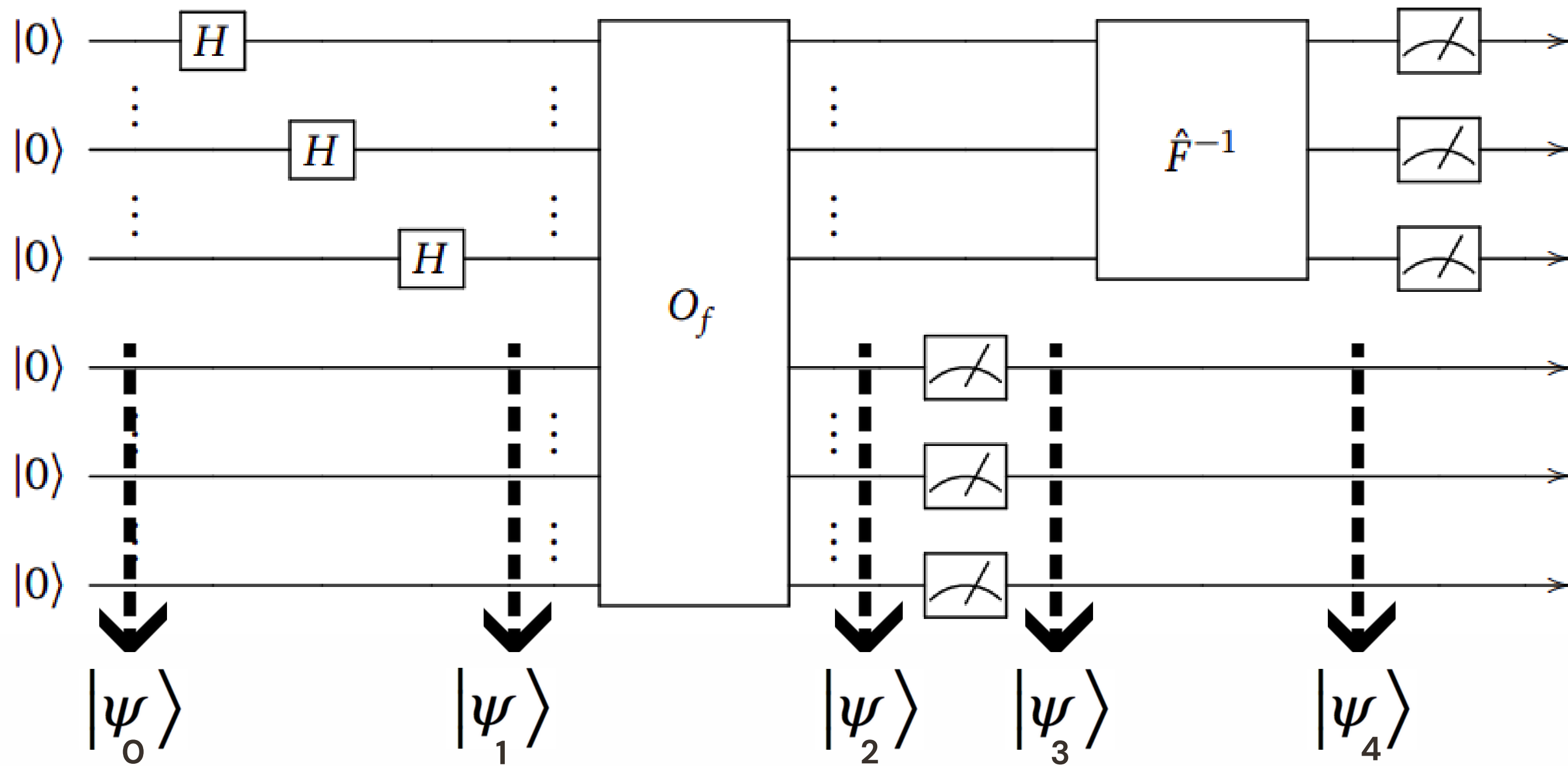


# ALGORITHME DE SHOR

1. Vérifier que  $N$  n'est pas un nombre pair, premier ou une puissance d'un nombre premier.
2. Choisir aléatoirement  $1 < a < N$ .
3. Si  $b = \text{pgcd}(a, N) > 1$ , renvoyer  $b$  (facteur non trivial).
4. Sinon, trouver l'ordre de  $a$  modulo  $N$ ... nécessité d'utiliser un circuit quantique !
5. Si  $r$  est impair, retourner à l'étape 1.
6. Sinon, calculer  $x \equiv a^{r/2} + 1[N]$  et  $y \equiv a^{r/2} - 1[N]$ . Si  $x \equiv 0[N]$ , retourner à l'étape 2.
7. Calculer :  $p = \text{pgcd}(x, N)$  et  $q = \text{pgcd}(y, N)$ . Au moins l'un d'entre eux sera un facteur non trivial de  $N$ .



# CIRCUIT/FEI 1



1. Initialisation :  $|\psi_0\rangle = |\underline{0}\rangle \otimes |\underline{0}\rangle$
2. Transformation de Hadamard :  $|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle \otimes |\underline{0}\rangle$
3. Passage de l'oracle :  $|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle \otimes |\underline{a^k[N]}\rangle$
4. Qubit du premier registre, obtenu après mesure du second registre :  $|\bar{\psi}_3\rangle = \frac{1}{\sqrt{A}} \sum_{\alpha=0}^{A-1} |\underline{\alpha r + \beta_0}\rangle$
5. Transformation de Fourier Inverse :  $|\bar{\psi}_4\rangle = \hat{F}^{-1} |\bar{\psi}_3\rangle = \frac{1}{\sqrt{A}\sqrt{2^n}} \sum_{j=0}^{2^n-1} (\sum_{\alpha=0}^{A-1} e^{-2i\pi \frac{\alpha j}{2^n/r}}) e^{-2i\pi \frac{\beta_0 j}{2^n}} |\underline{j}\rangle$

**r divise  $2^n$**

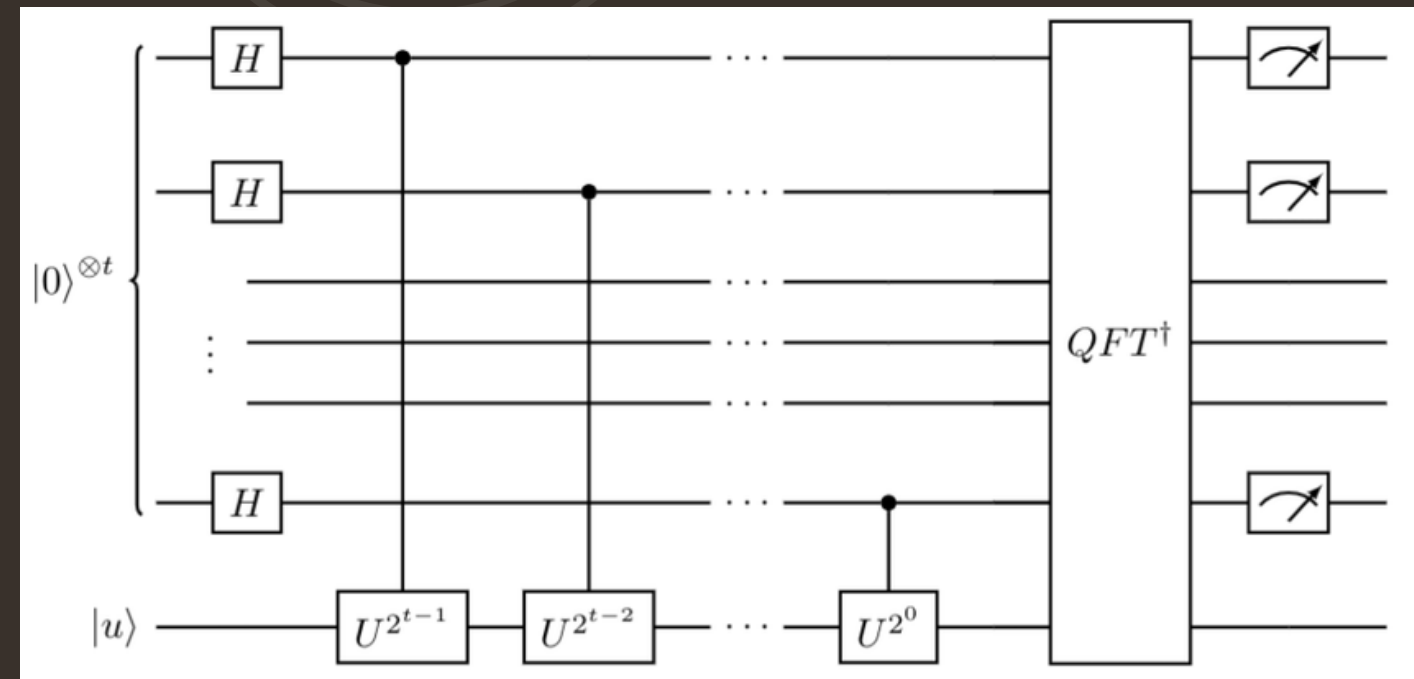
$$|\bar{\psi}_4\rangle = \frac{1}{\sqrt{r}} \sum_{\substack{j=0, \dots, 2^n-1 \\ \text{avec } \frac{j}{2^n/r} \text{ entier}}} e^{-2i\pi \frac{\beta_0 j}{2^n}} |\underline{j}\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2i\pi \beta_0 \frac{\ell}{r}} |\underline{\frac{2^n \ell}{r}}\rangle$$

La mesure fournit un entier  $(2^n)/r$

**r pair mais ne divise pas  $2^n$**

La mesure conduit à un entier proche de  $(2^n)/r$ , fraction non-entière...  $\rightarrow$   
Développement en fraction continue

## Estimation quantique de phase

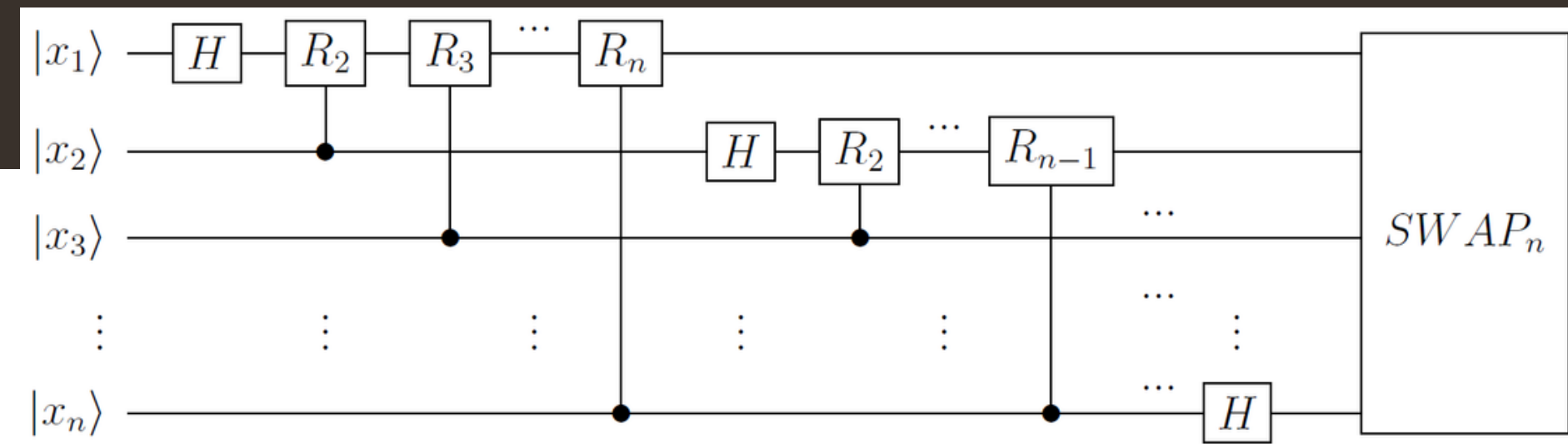


Exponentiation modulaire

$$U^{2^x} = a^{2^x} [N]$$

## Transformée de Fourier

$$\begin{aligned} \hat{F} |\underline{k}\rangle &= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{kj}{2^n}} |\underline{j}\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \prod_{l=1}^n e^{2i\pi \frac{kj_l}{2^l}} |j_1 j_2 \dots\rangle \\ &= \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2i\pi \frac{k}{2^1}} |1\rangle) \otimes (|0\rangle + e^{2i\pi \frac{k}{2^2}} |1\rangle) \otimes \dots (|0\rangle + e^{2i\pi \frac{k}{2^n}} |1\rangle) \end{aligned}$$



```
# Creation du circuit
qc = QuantumCircuit(n1 + n2, n1)

for q in range(n1):
    qc.h(q)

qc.x(3+n1)

for q in range(n1):
    qc.append(apmod15(a,2**q), [q]+[i+n1 for i in range(n2)])

qc.append(tfi(n1), range(n1))
qc.measure(range(n1), range(n1))
qc.draw(fold=-1)
```

```
# Transformee de Fourier quantique Inverse
def tfi(n):
    qc = QuantumCircuit(n)

    for qubit in range(n//2):
        qc.swap(qubit, n-qubit-1)

    for j in range(n):
        qc.h(j)
        for m in range(j+1, n):
            qc.cp(-np.pi/float(2**(j-m)), m, j)

    qc.name = "Transformee de Fourier Inverse"

    return qc
```

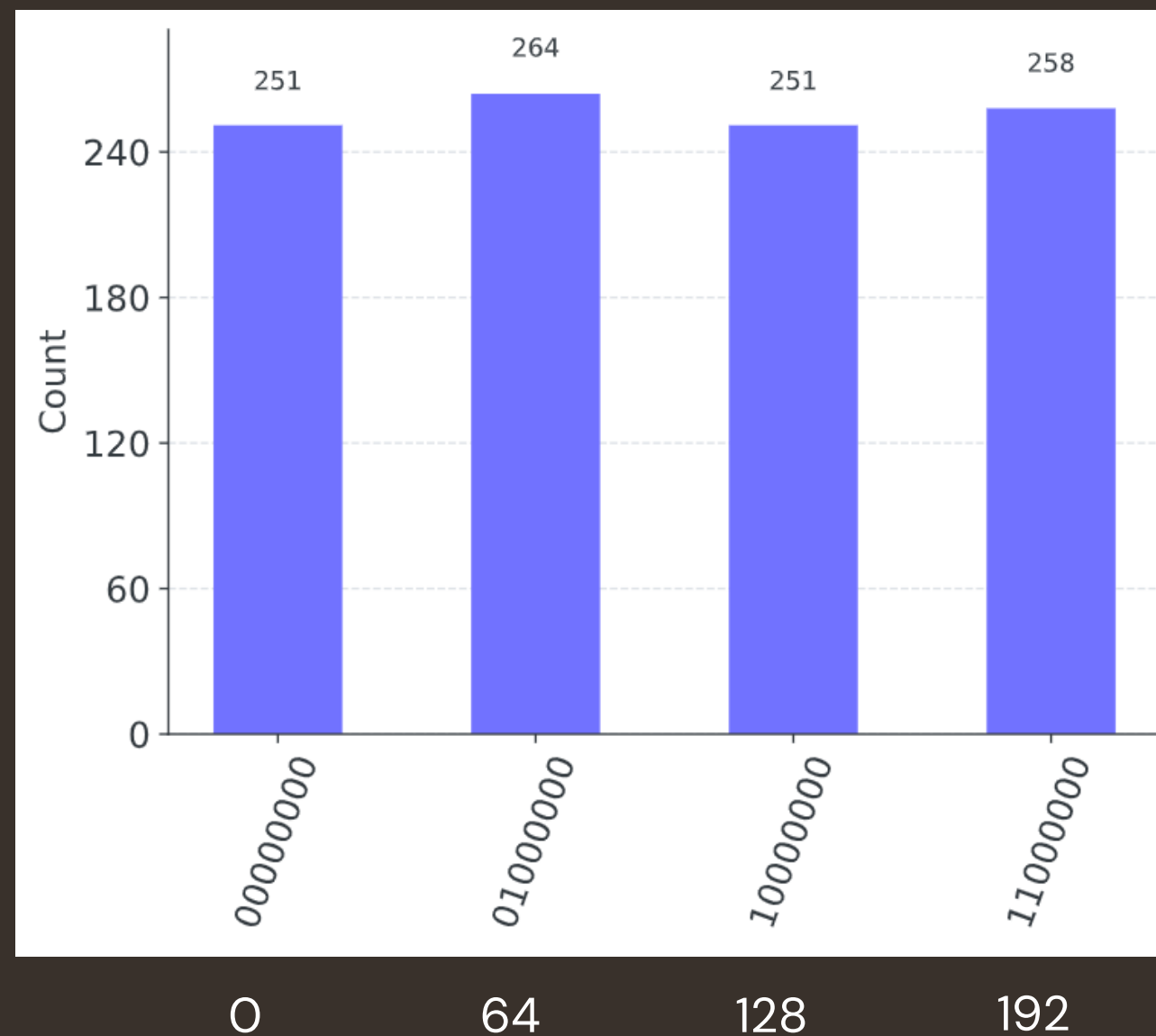
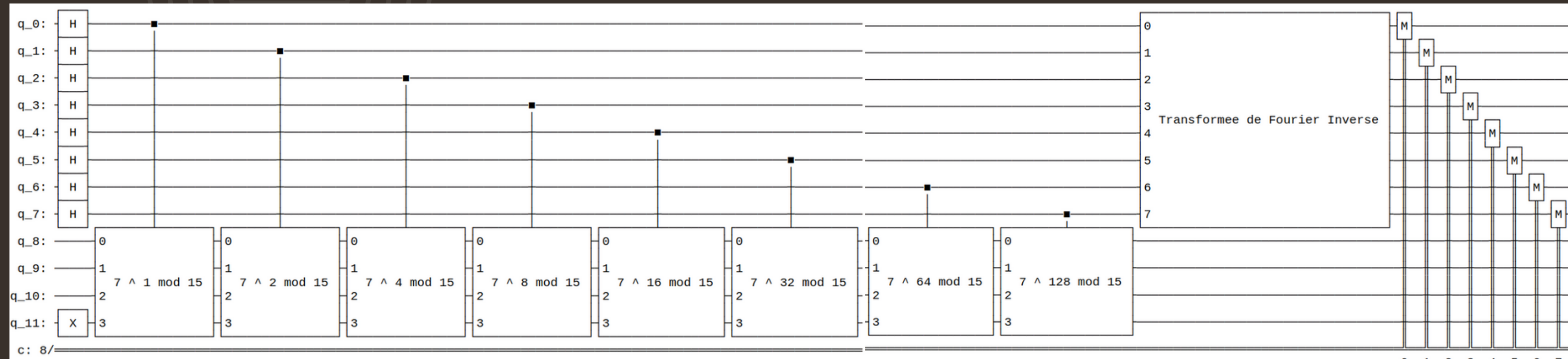
	Init.	2 <-> 3	1 <-> 2	0 <-> 1	X
p=1	0001	0010	0100	1000	0111
p=2	0111	0111	0111	1011	0100

```
# Exponentiation modulaire
def apmod15(a, power):
    U = QuantumCircuit(4)

    for iteration in range(power):
        U.swap(2,3)
        U.swap(1,2)
        U.swap(0,1)
        for q in range(4):
            U.x(q)

    U = U.to_gate()
    U.name = "%i ^ %i mod 15" %(a,power)
    c_U = U.control()

    return c_U
```



On détermine la période...

0	00000000(bin)	=	0(dec)	0/256	=	0.00
1	11000000(bin)	=	192(dec)	192/256	=	0.75
2	10000000(bin)	=	128(dec)	128/256	=	0.50
3	01000000(bin)	=	64(dec)	64/256	=	0.25

Fractions irréductibles,  $r = 4$  ou  $2$

Finalemment:  
 $p = \text{PGCD}(7^2 - 1, 15) = 3$   
 $q = \text{PGCD}(7^2 + 1, 15) = 5$



## Conclusion

- Introduction approfondie au calcul quantique, révélant son potentiel révolutionnaire.
- Exploration détaillée de trois algorithmes quantiques de renom.
- Implémentation de l'un de ces algorithmes via la manipulation de simulateurs quantiques et l'apprentissage de Quiskit, un langage de programmation dédié.
- Collaboration enrichissante avec un expert du domaine.





**MERCI POUR  
VOTRE  
ATTENTION !**

**Roxane LEDUC**

Oct. 2023 – Fev. 2024

---



## Transformation de Hadamard

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\underline{0}\rangle = |0.0\rangle \xrightarrow{H^{\otimes 2}} \frac{1}{2}(|0+1\rangle|0+1\rangle) = \frac{1}{2}(|0.0\rangle + |0.1\rangle + |1.0\rangle + |1.1\rangle) = \frac{1}{2}(|\underline{0}\rangle + |\underline{1}\rangle + |\underline{2}\rangle + |\underline{3}\rangle)$$

$$H^{\otimes n}|\underline{0}\rangle = \frac{1}{\sqrt{2^n}}(|0\dots 0.0\rangle + |0\dots 0.1\rangle + |0\dots 1.0\rangle + \dots + |1\dots 1.1\rangle)$$

$$H^{\otimes n}|\underline{0}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\ell=0}^{2^n-1} |\underline{\ell}\rangle$$

## Développement en fractions continues

$$x = \frac{427}{512} = [0, 1, 5, 42, 2] = 0 + \frac{1}{1 + \frac{1}{5 + \frac{1}{42 + \frac{1}{2}}}}$$

## Transformée de Fourier Inverse

$$|\bar{\psi}_4\rangle = \hat{F}^{-1}|\bar{\psi}_3\rangle$$

$$= \hat{F}^{-1}\left(\frac{1}{\sqrt{A}} \sum_{\alpha=0}^{A-1} |\underline{\alpha r + \beta_0}\rangle\right)$$

$$= \frac{1}{\sqrt{A}} \sum_{\alpha=0}^{A-1} \hat{F}^{-1}(|\underline{\alpha r + \beta_0}\rangle)$$

$$= \frac{1}{\sqrt{A}} \sum_{\alpha=0}^{A-1} \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2i\pi \frac{(\alpha r + \beta_0)j}{2^n}} |\underline{j}\rangle$$

$$= \frac{1}{\sqrt{A}\sqrt{2^n}} \sum_{j=0}^{2^n-1} \left( \sum_{\alpha=0}^{A-1} e^{-2i\pi \frac{\alpha j}{2^n/r}} \right) e^{-2i\pi \frac{\beta_0 j}{2^n}} |\underline{j}\rangle$$



$$\begin{aligned}
 |\psi_2\rangle = \frac{1}{4} & \left( |\underline{0}\rangle |\underline{1}\rangle + |\underline{1}\rangle |\underline{2}\rangle + |\underline{2}\rangle |\underline{4}\rangle + |\underline{3}\rangle |\underline{8}\rangle \right. \\
 & + |\underline{4}\rangle |\underline{1}\rangle + |\underline{5}\rangle |\underline{2}\rangle + |\underline{6}\rangle |\underline{4}\rangle + |\underline{7}\rangle |\underline{8}\rangle \\
 & + |\underline{8}\rangle |\underline{1}\rangle + |\underline{9}\rangle |\underline{2}\rangle + |\underline{10}\rangle |\underline{4}\rangle + |\underline{11}\rangle |\underline{8}\rangle \\
 & \left. + |\underline{12}\rangle |\underline{1}\rangle + |\underline{13}\rangle |\underline{2}\rangle + |\underline{14}\rangle |\underline{4}\rangle + |\underline{15}\rangle |\underline{8}\rangle \right)
 \end{aligned}$$

$$\begin{aligned}
 |\psi_2\rangle = \frac{1}{4} & \left( |\underline{0}\rangle + |\underline{4}\rangle + |\underline{8}\rangle + |\underline{12}\rangle \right) |\underline{1}\rangle \\
 & + \frac{1}{4} \left( |\underline{1}\rangle + |\underline{5}\rangle + |\underline{9}\rangle + |\underline{13}\rangle \right) |\underline{2}\rangle \\
 & + \frac{1}{4} \left( |\underline{2}\rangle + |\underline{6}\rangle + |\underline{10}\rangle + |\underline{14}\rangle \right) |\underline{4}\rangle \\
 & + \frac{1}{4} \left( |\underline{3}\rangle + |\underline{7}\rangle + |\underline{11}\rangle + |\underline{15}\rangle \right) |\underline{8}\rangle
 \end{aligned}$$

Qubit du premier registre obtenu  
après mesure du  
second registre...

### Mesure du second registre.

Une mesure sur le second registre renvoie de façon équiprobable :

1 ou 2 ou 4 ou 8.

Le qubit  $|\bar{\psi}_3\rangle$  du premier registre dépend alors de cette mesure :

- si la mesure du second registre est 1 alors  $|\bar{\psi}_3\rangle = \frac{1}{2} \left( |\underline{0}\rangle + |\underline{4}\rangle + |\underline{8}\rangle + |\underline{12}\rangle \right)$
- si la mesure du second registre est 2 alors  $|\bar{\psi}_3\rangle = \frac{1}{2} \left( |\underline{1}\rangle + |\underline{5}\rangle + |\underline{9}\rangle + |\underline{13}\rangle \right)$