Encryption (e.g. RSA)

- Trust me bro thm (garrohan) (*)
- Left as an exercise to the reader (**).

Alice ⟶ Bob

$C = E(M, Pub)$

↑
Facile

Pub

Priv

$M = D(C, Priv)$

↖ Difficile sans Priv

Moralement Pub = "p q"
↙ prime ↘ prime

connu
↓ ~ poly time ~ super poly.

Facile de multiplier, difficile de factoriser.

ex $23 \times 17 = 400 - 9 = 391$ (*)

Problème de factorisation peut ê mappé sur un autre problème d'arithmétique modulaire.

ex : $\mathbb{Z}/_{\mathbb{Z}N}$ ⟶ entiers modulo N

$N = 15$	2	4	8	16	32	64	128
↓	2	4	8	1	2	4	8 ⟶

période 4.

Marche aussi avec d'autres nombres.

3	9	27	81	243
3	9	12	6	3

$r = 5$

Il s'avère que cette période est liée au problème de factorisation.

Prop $x^2 = 1 \ [N]$ $x \neq \pm 1 \ [N]$.

Alors N divisible par $PGCD(x-1, N)$

Preuve $x^2 = 1 \ [N]$

$x^2 - 1 = uN \quad u \in \mathbb{Z}$

$(x-1)(x+1) = uN$.

$d := PGCD(x-1, N)$.

d non trivial $\neq \{1, N\}$.

$d = 1$

↳ $x-1$ & N premiers entre eux.

↳ $x+1$ divise N

$x = -1 \ [N]$ → contradiction.

$d = N$

↳ N divisible par $x-1$

$x = 1 \ [N]$. contradiction.

Maintenant Supposons qu'on a trouvé a et r pair tels que

$$a^r = 1 \ [N]$$

$$x^2 := a^r$$

↳ $PGCD(a^{r/2} - 1, N)$ et $PGCD(a^{r/2} + 1, N)$

Sont des facteurs non triviaux de N qu'on

peut calculer facilement avec l'algorithme d'Euclide

<u>Algo d'Euclide</u> pour le PGCD de (A,B),

$$(A,B) \to (A, B-A) \to$$
$B \geq A$ répète

Si q divise A & B alors il divise aussi $(A, B-A)$

<u>ex:</u> $(4,15) \to (4,11) \to (4,7) \to (3,4) \to (4,1)$
$\dots \to (1,1)$

$$(3,15) \to (3,12) \to (3,9) \to (3,6) \to (3,3).$$

<u>ex de cette idée</u>

$N = 15 \quad a = 2 \quad r = 4$

$PGCD\,(a^{r/2} - 1, N) = PGCD\,(4-1, 15) = 3$

$PGCD\,(a^{r/2} + 1, N) = PGCD\,(5, 15) = 5$

$15 = 3 \times 5.$

En pratique on prend a au hasard et on espère tomber sur un r pair $\to$ arrive avec une proba "respectable" (*)

Problème $\to$ difficile en général de calculer r (*)

C'est ce problème que résout l'ordinateur quantique

Rappel mécanique quantique. $\to$ r qubits. $\to$ produit tensoriel

Qbit espace vectoriel $\{|0\rangle, |1\rangle\}$ sur $\mathbb{C}$ comme $\to$: . . .
Base.

$n = \lceil \log_2 N \rceil$ Choisis t tel que $Q := 2^t \geq N^2$

Registre de comptage t qubits

Registre de travail n qubits.

État initial. $|\psi_0\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x, 1\rangle$

Applique l'unitaire d'exponentiation modulaire

$U : |x, y\rangle \longrightarrow |x, y\, a^x [N]\rangle$

↗ Permutation sur les N éléments.

Ex: $N = 15$ $a = 3$ $x = 14$

$x = 2^3 + 2^2 + 2^1$ $a^x = 3^{14} = ((3^2)^2)^2 (3^2)^2 (3^2)$.

$3^2 = 9$; $9 \times 9 = 81$; $81 = 6$; $6 \times 6 = 36$; $36 = 6$; $6 \times 9 = 54$; $54 = 9$; $9 \times 9 = 9$

$$U|\psi_0\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x, a^x [N]\rangle$$

Intérêt de cet état → Si on mesure le registre de travail on obtient avec une certaine proba a^{x_0}

L'état est projeté sur.

projection operator.

$\Pi_{x_0} U|\psi_0\rangle \quad \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |x_0 + j r\rangle \qquad M = \left\lceil \frac{Q - x_0}{r} \right\rceil$

↳ de TF de g on intuitionne constructivement

pour le nombre d'onde $\sim \pi$.

$\omega \times h$.

Quantum Fourier Transform

$$|\tilde{h}\rangle = \frac{1}{\sqrt{Q}} \sum_{h=0}^{Q-1} e^{\frac{i 2\pi x h}{Q}} |x\rangle$$

QFT: $$|x\rangle := \frac{1}{\sqrt{Q}} \sum_{k=0}^{Q-1} e^{\frac{i 2\pi x k}{Q}} |\tilde{k}\rangle$$

$$QFT\,(U|\psi_0\rangle) = \frac{1}{\sqrt{MQ}} \sum_{k=0}^{Q-1} e^{i 2\pi x_0 k/Q} \underbrace{\sum_{j=0}^{M-1} e^{i 2\pi j x k/Q}}_{\text{Very high weight on } k \sim m\frac{Q}{\pi}} |\tilde{k}\rangle$$

QFT with quantum circuits

j nombre $|j\rangle$ encodé en binaire sur des qubits

ex $j = 3$ $\quad |j\rangle = |11\rangle = |j_2, j_2\rangle \cdots$

Pour 1 qbit

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

$e^{\frac{i 2\pi j h}{2}} \to 0$ ou 1.

$$|\tilde{1}\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Pour 2 qbits. $e^{\frac{i 2\pi j h}{4}} \to 1 \; -1 \; i \; -i$

$$|\tilde{00}\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

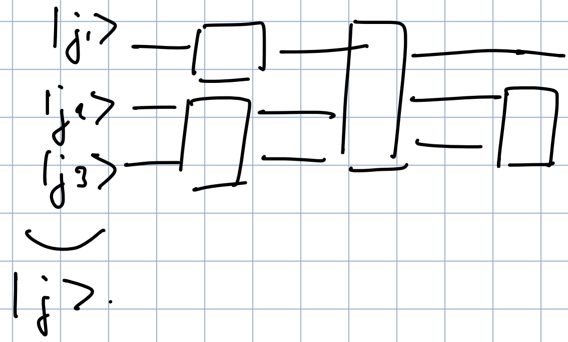
$$|\tilde{01}\rangle = \frac{1}{2} (|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$$

$$\vdots$$

ctz.

(**) → il y a un pattern général.

Circuit quantique.



Portes quantiques élémentaires → construire unitaires donc n'importe quel unitaire.

1 qbit.

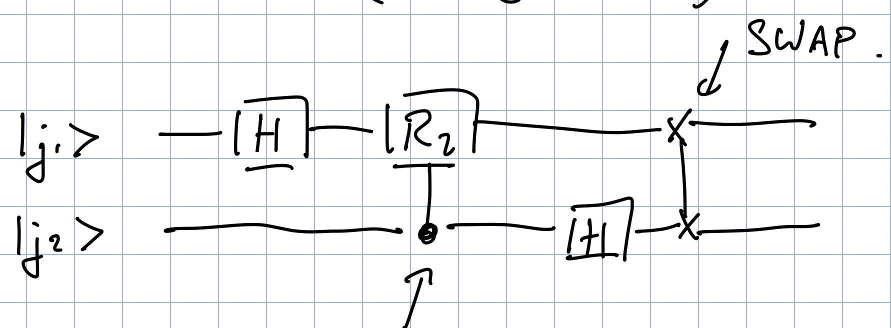
Hadamard. —[H]— $= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

QFT

$|0\rangle$ —[H]— $\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$

$|1\rangle$ —[H]— $\frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$.

2 qbits. $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$ $R_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$



applique R_2 si l'état est 1

$|00\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{R_2} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{H} \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

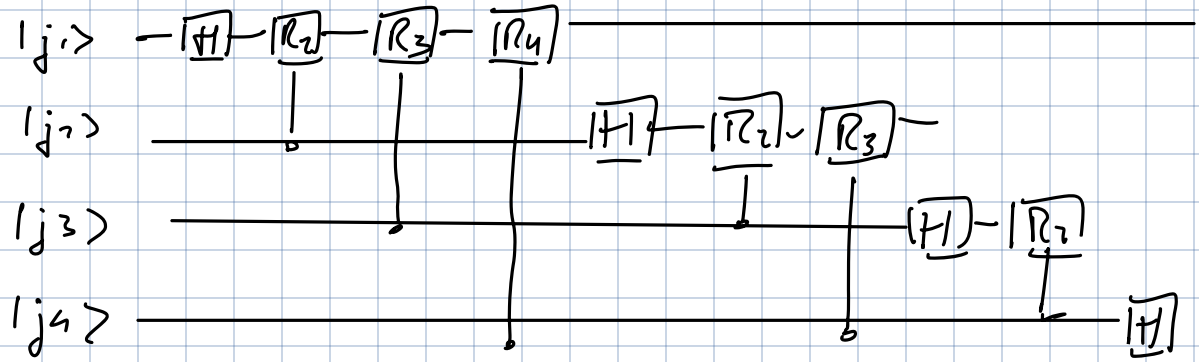
$|01\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \xrightarrow{R_2} \frac{1}{\sqrt{2}}(|01\rangle + i|11\rangle)$

$\xrightarrow{H} \frac{1}{2}(|00\rangle - |01\rangle + i|10\rangle - i|11\rangle)$

$\xrightarrow{\times} \frac{1}{2}(|00\rangle - |10\rangle + i|01\rangle - i|11\rangle)$

$n=4$

(4)



↳ $O(n^2)$ portes. → efficace.

FFT classique $O(n2^n)$.