L'algoritmo di fattorizzazione di Shor e la crittografia quantistica

Laureando: Giovanni Varutti
Relatore: Fabio Benatti

16/09/2022

Università degli studi di Trieste

Indice

La crittografia RSA e il problema della fattorizzazione

L'algoritmo RSA

Generazione delle chiavi

1. Scegliere due numeri primi p e q, per esempio 5 e 11, e calcolare $N = pq = 55$.
2. Calcolare la funzione di Eulero, $\phi(N) = (p-1)(q-1) = 40$.
3. Scegliere un intero $e < N$ coprimo di $\phi(N)$, e trovare un numero d tale che: $ed = k\phi(N) + 1$. Nel caso in esempio $e = 3$ e $d = 27$.
4. Chiave pubblica: $(e, N) = (3, 55)$. Chiave privata: $(d, N) = (27, 55)$.

Si vuole trasmettere un messaggio $M = 47$.

- Si **cifra** usando la chiave pubblica del destinatario:
  $C = M^e \pmod N = 47^3 \pmod{55} = 38$
- Il destinatario **decifra** con la chiave privata:
  $C^d \pmod N = 38^{27} \pmod{55} = 47 = M$

Caso classico vs caso quantistico

Operazioni richieste per fattorizzare un numero RSA-2048:

- Algoritmo classico: $O(\exp(cL^{1/3}\log^{2/3}L)) \approx O(e^{82}) \approx O(10^{35})$
- Algoritmo quantistico: $O(L^2 \log L \log\log L) \approx O(10^8)$

Vantaggi della computazione quantistica

- sovrapposizione quantistica dei **qubit:**

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathbb{C}^2 \ \text{ con } \alpha, \beta \in \mathbb{C}\ ;\ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\ ,\ |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- sistema di n qubits $\in \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n} \implies 2^n$ ampiezze di probabilità
- Gates quantistici: operatori unitari che agiscono su uno o più qubits

L'algoritmo di fattorizzazione di Shor

Riduzione della fattorizzazione all'order-finding

1. Si sceglie un intero $m < N$ e coprimo di N. Si definisce la funzione $f(x) = m^x \pmod N \implies m^x = kN + f(x),\ k \in \mathbb{N}$

2. L'ordine r è il più piccolo intero tale che $f(r) = 1$, ossia $m^r = kN + 1$

3. Se r è pari $\implies \left(m^{r/2} + 1\right)\left(m^{r/2} - 1\right) = kN$

4. Calcolando $\gcd(m^{r/2} - 1, N)$ e $\gcd(m^{r/2} + 1, N)$ si ottengono i fattori di N

Trasformata di Fourier quantistica

Si considera un sistema di 2 qubits. Lo spazio di Hilbert associato è $\mathbb{C}^4$.

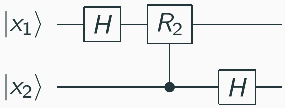
La base computazionale è l'insieme dei vettori:
$\{|x_1\rangle \otimes |x_2\rangle \equiv |x_1 x_2\rangle\}$ con $x_1, x_2 = 0, 1$

Si può passare alla **forma decimale**:
$x = x_1 2^1 + x_2 2^0 \implies |x_1 x_2\rangle \to |x\rangle$ con $x = 0, \ldots, 2^2 - 1 = 3$

Definizione

La *QFT* è l'operatore che agisce sulla base ortonormale nel modo seguente:

$$QFT(|x_1 x_2\rangle) = \frac{1}{\sqrt{2^2}} \underbrace{\left(|0\rangle + e^{2\pi i x/2^1} |1\rangle\right)}_{\text{primo qubit}} \otimes \underbrace{\left(|0\rangle + e^{2\pi i x/2^2} |1\rangle\right)}_{\text{secondo qubit}}$$



$\implies 2 + 1 = 3$ gates

Generalizzando per n qubits:

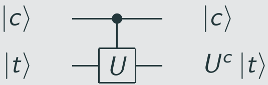
$$n + (n-1) + \cdots + 1 = \frac{n(n+1)}{2} = \frac{n^2}{2} + \frac{n}{2} = O(n^2) \text{ gates}$$

Gates quantistici

- Hadamard:

$$\implies \begin{cases} H\left|0\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \left|1\right\rangle\right) \\ H\left|1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right) \end{cases}$$

- Control-U:



$$\implies \begin{cases} \left|0\right\rangle\left|t\right\rangle \to \left|0\right\rangle\left|t\right\rangle \\ \left|1\right\rangle\left|t\right\rangle \to \left|1\right\rangle U\left|t\right\rangle \end{cases}$$

Quantum phase estimation

Definizione

Si considera un operatore unitario $U : \mathbb{C}^{2^L} \mapsto \mathbb{C}^{2^L}$ su L qubits. Si suppone di conoscere un autovettore $|u\rangle$ di U, da cui:

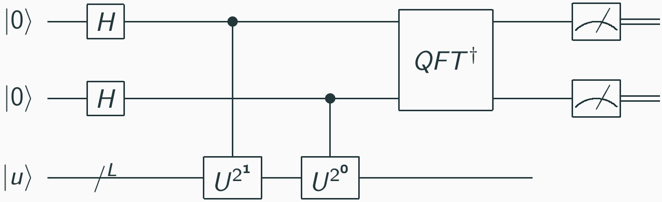
$$U\,|u\rangle = e^{2\pi i \varphi_u}\,|u\rangle$$

con $\varphi_u \in [0, 1)$. Lo scopo della QPE è determinare la fase φ_u.

Si prepara un circuito quantistico a due registri:

- Il numero di qubits nel primo registro dipende dalla precisione con cui si vuole stimare φ_u
- L'autovettore $|u\rangle$ può essere espresso come prodotto tensore di L qubits nel secondo registro

Quantum phase estimation



$$|Reg1\rangle\,|Reg2\rangle = |0\rangle^{\otimes 2}\,|u\rangle \xrightarrow{H} \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes 2} |u\rangle \xrightarrow{CU^{2^j}}$$

$$\rightarrow \frac{1}{\sqrt{2^2}} \underbrace{\left(|0\rangle + e^{2\pi i 2^1 \varphi_u}|1\rangle\right)}_{\text{primo qubit}} \otimes \underbrace{\left(|0\rangle + e^{2\pi i 2^0 \varphi_u}|1\rangle\right)}_{\text{secondo qubit}} |u\rangle$$

$$\xrightarrow{QFT^\dagger} |2^2\varphi_u\rangle\,|u\rangle = |2^2 \times 0.\varphi_1\varphi_2\rangle\,|u\rangle = \boxed{|\varphi_1\varphi_2\rangle\,|u\rangle}$$

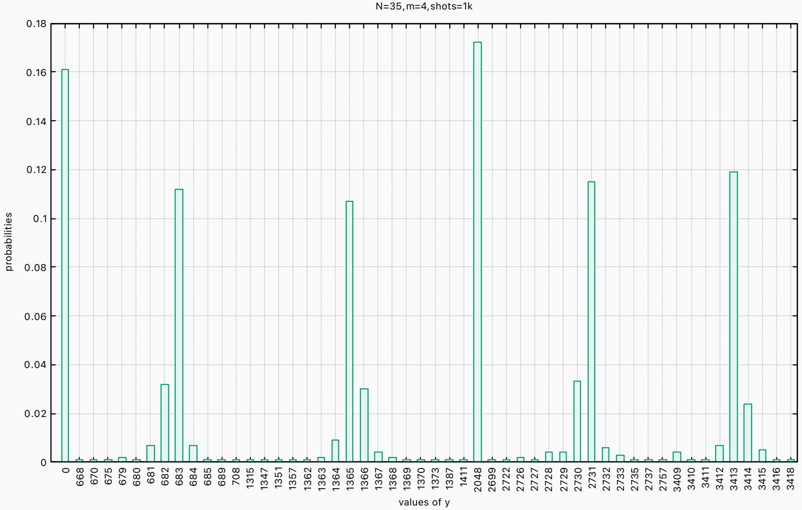
Order-finding

Introduzione

Lo scopo è trovare l'ordine della funzione $f(x) = m^x \pmod N$, ossia il più piccolo intero r tale che $f(r) = 1$

1. Si utilizza la QPE con il gate: $U_{m,N} |x\rangle = |mx \pmod N\rangle$
   $|x\rangle \in \{|0\rangle, \ldots, |N-1\rangle\}$ base di $\mathbb{C}^N \longrightarrow \mathbb{C}^{2^L}$ con $L = \lceil \log_2 N \rceil$
2. Gli autovettori sono definiti dalla combinazione lineare:
$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{-2\pi i x s/r} |m^x \pmod N\rangle, \ \text{con } 0 \leq s \leq r-1$$
$$U_{m,N} |u_s\rangle = e^{2\pi i s/r} |u_s\rangle = e^{2\pi i \varphi_s} |u_s\rangle, \ \text{con } \varphi_s = s/r < 1$$
3. Per inizializzare il secondo registro si utilizza l'uguaglianza:
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle = |\underbrace{0\ldots0}_{L-1}1\rangle$$

Simulazioni



Conclusioni

La crittografia quantistica

Protocolli di scambio quantistico della chiave

Permettono a due utenti di generare una chiave crittografica comune sfruttando lo scambio di qubits. Cifratura e decifratura avvengono utilizzando la stessa chiave.

La sicurezza si basa su leggi quantistiche:

- **Teorema no-cloning:** non è sempre possibile copiare lo stato quantistico di un qubit sconosciuto a priori.
- **Teorema di non discriminazione quantistico:** non è possibile distinguere fra due stati quantistici non ortogonali senza perturbarli.

$\Longrightarrow$ ogni azione sui qubits inviati produce un effetto di disturbo misurabile ed individuabile.