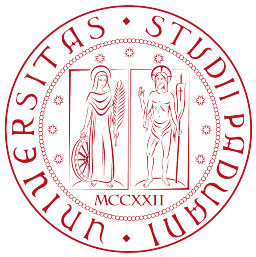


Università degli Studi di Padova

Dipartimento di Fisica e Astronomia

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea Triennale in

Fisica

Tesi di Laurea

Computazione quantistica e dimostrazioni sperimentali del modello circuitale

Relatore
Giuseppe Vallone

Laureando
Daniele Guarrera

ANNO ACCADEMICO
2014-2015

Indice

1 Introduzione alla computazione quantistica **4**
1.1 Il qubit 4
1.2 Sfera di Bloch 5
1.3 Modello circuitale 7
1.4 Porte logiche a singolo qubit 9
1.5 Porte logiche controllate 10

2 Algoritmo di Shor **12**
2.1 Trasformata di Fourier quantistica 13
2.2 Come trovare il periodo 15
2.3 Fattorizzazare 91 17
2.4 Protocollo RSA 19

3 Dimostrazione sperimentale del modello circuitale **20**
3.1 Requisiti per la computazione quantistica 20
3.2 Tecnologie per realizzare un computer quantistico 21
3.3 Computazione con fotoni su chip al silicio 23
3.4 Algoritmo di Shor su un chip con tecnologia a fotoni 27
3.5 Realizzazione di una porta C-NOT a fotoni 29

4 Conclusioni **34**

5 Bibliografia **35**

ABSTRACT

Questo lavoro ha lo scopo di approfondire il tema della computazione quantistica, con particolare attenzione alla definizione di qubit e ai modelli teorici di computazione. Verrà trattato in dettaglio l'algoritmo di Shor di fattorizzazione, ponendo l'attenzione sui limiti del protocollo RSA se tale algoritmo fosse implementato su larga scala. Infine, dopo aver parlato delle principali tecnologie che si attestano come le possibili per un'implementazione fisica del modello circuitale, verranno descritte due tecniche sperimentali di codifica di informazione quantistica, per dimostrare tale modello. Queste si basano sulla computazione con fotoni su chip al silicio: la prima con codifica "dual-rail", la seconda con codifica in polarizzazione.

1 Introduzione alla computazione quantistica

Il campo della computazione quantistica è stato avviato dai lavori di Yuri Manin, Richard Feyman e David Deutsch negli anni '80 del Novecento. Oggi il reale sviluppo di un computer quantistico è ancora nella sua infanzia, tuttavia sia la ricerca sperimentale che teorica continuano, in quanto molti governi nazionali ed agenzie militari private finanziano tali studi per questioni d'affari, commercio e sicurezza nazionale.
Un computer quantistico sarebbe in grado di risolvere molto più rapidamente alcuni problemi rispetto a qualsiasi computer classico. Inoltre permetterebbe la simulazione di sistemi quantistici complessi e fondamentali, con forti ricadute sulla ricerca nel campo di molti settori scientifici.
Il divario a livello computazionale tra un computer classico ed un computer quantistico risiede nell'unità di misura dell'informazione che lo caratterizza: il *qubit*, oggetto matematico, la cui implementazione fisica sarà trattata nell'ultimo capitolo.

1.1 Il qubit

In Teoria dell'Informazione classica, l'unità di misura dell'informazione è il bit, rappresentabile in due forme distinte come 0 o 1. Analogamente il quibit (bit quantistico) è l'unità dell'informazione quantistica.
Il qubit[5] è un vettore appartenente ad uno spazio di Hilbert bidimensionale, dove

$$|\,0>\equiv \begin{pmatrix}1\\0\end{pmatrix} \quad , \quad |\,1>\equiv \begin{pmatrix}0\\1\end{pmatrix} \tag{1}$$

rappresentano una base ortonormale, chiamata "base computazionale".
Per il principio di sovrapposizione lo stato di un qubit è descritto dal vettore

$$|\,\psi>=\alpha\,|\,0>+\beta\,|\,1> \qquad \alpha,\beta\in\mathbb{C} \tag{2}$$

Il qubit può trovarsi in uno stato di sovrapposizione, tuttavia in meccanica quantistica quando si effettua una misura nella base computazionale, lo stato viene proiettato su una delle sue componenti con probabilità

$$P_0=|<0\,|\,\psi>|^2=|\alpha|^2 \tag{3}$$

$$P_1=|<1\,|\,\psi>|^2=|\beta|^2 \tag{4}$$

Poiché la probabilità totale è pari alla somma delle due probabilità si deve imporre che $P_0+P_1=|\alpha|^2+|\beta|^2=1$.

Il medesimo stato si può rappresentare con

$$|\psi>=\cos\tfrac{\theta}{2}\,|0>+e^{i\phi}\sin\tfrac{\theta}{2}\,|1> \qquad 0\leq\theta\leq\pi\ ,\ 0\leq\phi<2\pi \tag{5}$$

che soddisfa la condizione di normalizzazione.

Essendo α, β, θ e ϕ variabili continue, sono permessi un numero infinito di stati. Questo va contro l'intuizione classica secondo cui un ente debba assumere uno stato ben definito come 0 o 1 in modo esclusivo. Tuttavia per i sistemi quantistici è possibile che un qubit, prima di essere misurato, si trovi in uno stato di sovrapposizione.

Una rappresentazione geometrica ed intuitiva dello stato di un quibit è quella della *Sfera di Bloch*.

1.2 Sfera di Bloch

Il qubit può essere rappresentato dalle coordinate di un punto sulla superficie di una sfera di raggio unitario, centrata nell'origine di un sistema di assi cartesioni tridimensionale. Questa prende il nome di *Sfera di Bloch*[5] ed è utilizzata per interpretare geometricamente sia lo stato di un qubit che le trasformazioni su di questo. Una trasformazione unitaria non farà altro che far migrare lo stato del qubit da un punto ad un altro della superficie sferica.

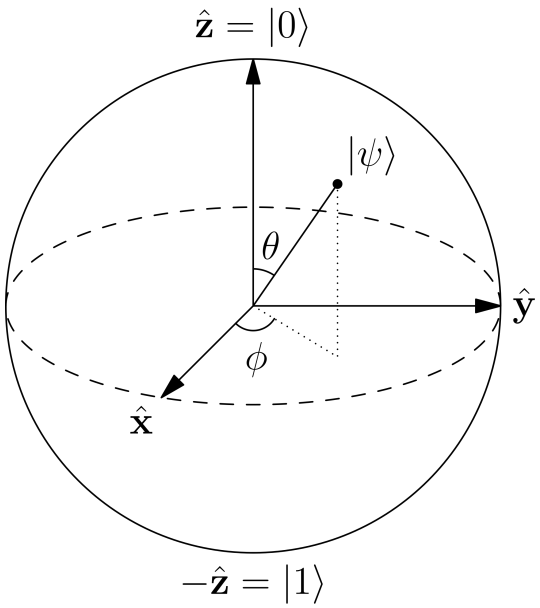


FIGURA 1

Lo stato $|0>$ è rappresentato dal versore $\hat{z}$ del sistema cartesiano, mentre lo stato $|1>$ è rappresentato dal suo opposto. Tutte le possibili sovrapposizioni dei due stati della base computazionale sono rappresentate dagli altri punti sulla superficie grazie alle coordinate sferiche.

$$\begin{cases} x = \sin\theta\ \cos\phi \\ y = \sin\theta\ \sin\phi \\ z = \cos\theta \end{cases} \qquad 0 \leq \theta \leq \pi\ ,\ 0 \leq \phi < 2\pi \tag{6}$$

Per sapere lo stato del qubit corrispondente al generico punto della sfera di coordinate $(\theta,\, \phi)$ basta sostituire tale coppia nella rappresentazione

$$|\psi_{(\theta,\,\phi)}> = \cos\tfrac{\theta}{2}\,|0> + e^{i\phi}\sin\tfrac{\theta}{2}\,|1> \tag{7}$$

Ad esempio il versore $\hat{x} = (\pi/2,\, 0)$ ed il versore $\hat{y} = (\pi/2,\, \pi/2)$ rappresentano rispettivamente gli stati

$$|\psi_{\hat{x}}> = \cos\tfrac{\pi}{4}\,|0> + e^{i0}\sin\tfrac{\pi}{4}\,|1> = \frac{1}{\sqrt{2}}\,(|0> + |1>) \tag{8}$$

$$|\psi_{\hat{y}}> = \cos\tfrac{\pi}{4}\,|0> + e^{i\frac{\pi}{2}}\sin\tfrac{\pi}{4}\,|1> = \frac{1}{\sqrt{2}}\,(|0> + i\,|1>) \tag{9}$$

Per compiere una trasformazione sullo stato di un qubit si utilizzano gli *operatori unitari*. Un operatore U si definisce unitario se soddisfa la seguente condizione, dove $U^\dagger$ è l'operatore autoaggiunto di U

$$UU^\dagger = \mathbb{I} \tag{10}$$

da cui

$$U^\dagger = U^{-1} \tag{11}$$

condizione di reversibilità della trasformazione.

Applicare un operatore unitario a due vettori di uno spazio di Hilbert preserva il loro prodotto scalare.

$$|\psi_1'> = U|\psi_1> \qquad |\psi_2'> = U|\psi_2> \tag{12}$$

$$<\psi_1'|\psi_2'> = <U\psi_1|U\psi_2> = <\psi_1|U^\dagger U|\psi_2> = <\psi_1|\psi_2> \tag{13}$$

Tali operatori agiscono in modo analogo alle rotazioni nello spazio euclideo, preservando lunghezze ed angoli fra vettori.

Degli esempi importanti di operatori unitari sono le *matrici di Pauli*[5].

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{14}$$

La matrice σ_x, ad esempio si comporta come un operatore NOT, infatti

$$\sigma_x |\, 0 > = |\, 1 > \quad , \quad \sigma_x |\, 1 > = |\, 0 > \tag{15}$$

Come vedremo l'operatore σ_x corrisponde ad una rotazione di un angolo π della Sfera di Bloch intorno all'asse x, invertendo l'orientazione dell'asse z.

1.3 Modello circuitale

Un computer quantistico può essere pensato come un insieme di n qubit. Tale insieme viene definito *registro quantistico*[5] di dimensione n.
Lo stato di n qubit si può rappresentare come un vettore appartenente ad uno spazio di Hilbert H 2^n-dimensionale:

$$|\, \psi > = \sum_{i=0}^{2^n-1} c_i |\, i > = \sum_{i_{n-1}=0}^{1} \cdots \sum_{i_1=0}^{1} \sum_{i_0=0}^{1} c_{i_{n-1},\cdots,i_1,i_0} \bigotimes_{k=0}^{n-1} |\, i_k > \tag{16}$$

dove

$$|\, i_k > \in H_k \quad , \quad |\psi > \in H = \bigotimes_{k=0}^{n-1} H_k \tag{17}$$

inoltre, per la condizione di normalizzazione, deve valere $\sum_{i=0}^{2^n-1} |c_i|^2 = 1$.

Ad esempio lo stato di 2 qubit di un registro quantistico 2-dimensionale può essere descritto da

$$|\, \psi > = c_0 |\, 0 > + c_1 |\, 1 > + c_2 |\, 2 > + c_3 |\, 3 > = \tag{18}$$

$$= c_{0,0} |\, 0 > \otimes |\, 0 > + c_{0,1} |\, 0 > \otimes |\, 1 > + c_{1,0} |\, 1 > \otimes |\, 0 > + c_{1,1} |\, 1 > \otimes |\, 1 > = \tag{19}$$

$$= c_{00} |\, 00 > + c_{01} |\, 01 > + c_{10} |\, 10 > + c_{11} |\, 11 > \tag{20}$$

quindi il numero di stati della base computazionale risulta pari a 2^n, in questo caso 4. È possibile notare che il numero di stati disponibili cresce esponenzialmente con il numero di qubit grazie al principio di sovrapposizione. A differenza dei bit classici che contengono l'informazione di solo un numero intero i, lo stato di n qubit può essere preparato nello stato $|\, i >$ della base computazionale o nei suoi stati di sovrapposizione.
In questo modo, rispetto ad un computer classico che elabora input differenti separatamente, un computer quantistico può lavorare in *parallelo* elaborando più input contemporaneamente.

Il modello prevede tre fasi[5] per portare a termine un processo di computazione quantistica:

1. preparare il computer quantistico in uno stato iniziale ben definito, per esempio $|0\cdots00>$ (lo stato fiduciario del computer);
2. trasformare la funzione d'onda del computer quantistico tramite operatori unitari, corrispondenti alle porte logiche quantistiche: $|\psi_f> = U|\psi_i>$;
3. alla fine dell'algoritmo, compiere una misura nella base computazionale che mi fornisca il valore di σ_z di ogni qubit.

Per misurare lo stato di un singolo qubit bisogna misurare le coordinate x, y e z della sua rappresentazione sulla Sfera di Bloch.
Il valore atteso delle matrici di Pauli risulta essere la rispettiva coordinata:

$$<\psi|\sigma_x|\psi> = <\psi| \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |\psi> = \sin\theta\,\cos\phi = x \tag{21}$$

$$<\psi|\sigma_y|\psi> = <\psi| \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} |\psi> = \sin\theta\,\sin\phi = y \tag{22}$$

$$<\psi|\sigma_z|\psi> = <\psi| \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} |\psi> = \cos\theta = z \tag{23}$$

Come risulta evidente gli autovalori di σ_z sono 1 e -1, relativi agli autostati $|0>$ e $|1>$.
La probabilità $p_{0,z}$ di aver misurato il valore logico 0 per la componente z risulta essere $|<0|\psi>|^2 = \cos^2\frac{\theta}{2}$, mentre la probabilità $p_{1,z}$ di aver misurato il valore logico 1 risulta essere $|<1|\psi>|^2 = \sin^2\frac{\theta}{2}$. Di conseguenza si nota che $p_{0,z} - p_{1,z} = \cos^2\frac{\theta}{2} - \sin^2\frac{\theta}{2} = \cos\theta$.
Se ho un numero N abbastanza grande di dispositivi uguali, preparati nello stesso stato, sarà possibile stimare il valore di z come $N_0/N - N_1/N$, dove N_0 ed N_1 sono il numero di volte che ottengo 0 o 1.

Per misurare la componente x e la componente y, analogamente alla componente z, è possibile compiere delle misure di σ_z sugli stati $|\psi_x> = U_1|\psi>$ e $|\psi_y> = U_2|\psi>$ rispettivamente, dove

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad , \quad U_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \tag{24}$$

infatti

$$<\psi_x|\sigma_z|\psi_x> = <U_1\psi|\sigma_z|U_1\psi> = <\psi|U_1^\dagger\sigma_z U_1|\psi> = <\psi|\sigma_x|\psi> \tag{25}$$

$$<\psi_y|\sigma_z|\psi_y> = <U_2\psi|\sigma_z|U_2\psi> = <\psi|U_2^\dagger\sigma_z U_2|\psi> = <\psi|\sigma_y|\psi> \tag{26}$$

1.4 Porte logiche a singolo qubit

Le operazioni su singoli qubit devono preservare la normalizzazione e sono rappresentate da operatori unitari 2×2. Le porte utili per compiere qualsiasi trasformazione su singolo qubit sono la porta *Hadamard*[5] e la porta *phase-shift*[5].

La porta Hadamard si definisce come

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{27}$$

Questa matrice trasforma la base computazionale $\{|\,0>, |\,1>\}$ in una nuova base dove gli stati sono la sovrapposizione degli stati della base computazionale:

$$H|\,0> = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|\,0> + |\,1>\right) \equiv |+> \tag{28}$$

$$H|\,1> = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(|\,0> - |\,1>\right) \equiv |-> \tag{29}$$

La porta phase-shift si definisce come

$$R_z(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \tag{30}$$

Questa porta cambia la fase dello stato di δ con una rotazione della Sfera di Bloch intorno l'asse z.

$$R_z(\delta)|\,\psi> = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i(\phi+\delta)}\sin\frac{\theta}{2} \end{pmatrix} \tag{31}$$

L'operatore che permette di raggiungere un punto generico di coordinate (θ_2, ϕ_2) a partire da un punto generico di coordinate (θ_1, ϕ_1) è combinazione dei due precedenti:

$$|\,\psi_{(\theta_2,\phi_2)}> = R_z\left(\tfrac{\pi}{2} + \phi_2\right) H R_z(\theta_2 - \theta_1) H R_z(-\tfrac{\pi}{2} - \phi_1)|\,\psi_{(\theta_1,\phi_1)}> \tag{32}$$

Per avere una visione più generale del problema consideriamo il fatto che la trasformazione, che porta il generico stato da un punto (θ_1, ϕ_1) ad un punto (θ_2, ϕ_2), si può interpretare come una rotazione intorno ad un particolare asse della Sfera di Bloch.

Sia Σ un operatore tale che $\Sigma^k = \mathbb{I}$ per k pari e $\Sigma^k = \Sigma$ per k dispari. Allora è possibile sviluppare in serie di Taylor l'esponenziale

$$e^{-i\alpha\Sigma} = [1 - \tfrac{\alpha^2}{2!} + ...]\mathbb{I} - i[\alpha - \tfrac{\alpha^3}{3!} + ...]\Sigma = \cos\alpha\,\mathbb{I} - i\sin\alpha\,\Sigma \tag{33}$$

É possibile notare che si ottine l'operatore phase-shift ponendo $\alpha = \frac{\delta}{2}$ e $\Sigma = \sigma_z$

$$e^{-i\frac{\delta}{2}\sigma_z} = \begin{pmatrix} \cos\frac{\delta}{2} - i\sin\frac{\delta}{2} & 0 \\ 0 & \cos\frac{\delta}{2} + i\sin\frac{\delta}{2} \end{pmatrix} = \begin{pmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{pmatrix} = e^{-i\frac{\delta}{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \equiv R_z(\delta) \quad (34)$$

analogamente si possono ricavare gli operatori di rotazione intorno l'asse x ed y della Sfera di Bloch

$$e^{-i\frac{\delta}{2}\sigma_x} \equiv R_x(\delta) \qquad e^{-i\frac{\delta}{2}\sigma_y} \equiv R_y(\delta) \quad (35)$$

In generale, definiti $n = (n_x, n_y, n_z)$ un generico asse e $\sigma = (\sigma_x, \sigma_y, \sigma_z)$, la rotazione di un angolo δ intorno all'asse n della Sfera di Bloch può avvenire tramite l'operatore

$$R_n(\delta) = \cos\tfrac{\delta}{2}\,\mathbb{I} - i\sin\tfrac{\delta}{2}\,(n \cdot \sigma) \quad (36)$$

A questo punto si può notare che ponendo $\tilde{n} = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ e $\delta = \pi$

$$R_{\tilde{n}}(\pi) = -\frac{i}{\sqrt{2}}(\sigma_x + \sigma_z) \sim \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H \quad (37)$$

risulta che la porta Hadamard ruota un punto della Sfera di Bloch intorno all'asse $\tilde{n}$ di π, scambiando la coordinata x con la z e viceversa.

1.5 Porte logiche controllate

Sia $H = H_1 \otimes H_2$ con $\{|\,0>_1, |\,1>_1\}$ e $\{|\,0>_2, |\,1>_2\}$ le rispettive basi di H_1 ed H_2. Per definizione uno stato di H è detto *entangled* se non può essere scritto come un semplice prodotto tensore di uno stato $|\,\alpha_1>$ di H_1 e uno stato $|\,\beta_2>$ di H_2. Al contrario se possiamo scrivere $|\,\psi> = |\,\alpha_1> \otimes |\,\beta_2>$ allora $|\,\psi>$ si dice *separabile*.

$$|\,\psi_1> = \frac{1}{\sqrt{2}}(|\,00> + |\,10>) = \frac{1}{\sqrt{2}}(|\,0> + |\,1>) \otimes |\,0> \quad \rightarrow \quad \textit{separabile} \quad (38)$$

$$|\,\psi_2> = \frac{1}{\sqrt{2}}(|\,00> + |\,11>) \quad \rightarrow \quad \textit{entangled} \quad (39)$$

Porte a singolo qubit non possono generare stati entangled in un sistema a n qubit. Partendo da uno stato separato $|\,\psi> = |\,\psi_{n-1}> \otimes \cdots \otimes |\,\psi_0>$ possiamo muovere i singoli qubit sulla propria Sfera di Bloch ottenendo $|\,\psi'> = |\,\psi'_{n-1}> \otimes \cdots \otimes |\,\psi'_0>$. Per preparare stati entangled c'è bisogno di interazioni, cioè una porta logica a 2 qubit.

Prendiamo in considerazione un registro di 2 qubit con base computazionale $\{|\,i_1 i_0> = |\,00>, |\,01>, |\,10>, |\,11>\}$.

Si definisce porta *C-NOT*[5] il seguente operatore unitario 2×2

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{40}$$

Come si può si notare che $CNOT|\, i_1 i_0 >$ cambia il valore di i_0 se $i_1 = 1$, se $i_1 = 0$ il valore di i_0 non cambia.

$$CNOT|\, 00 >= |\, 00 > \qquad CNOT|\, 01 >= |\, 01 > \tag{41}$$

$$CNOT|\, 10 >= |\, 11 > \qquad CNOT|\, 11 >= |\, 10 > \tag{42}$$

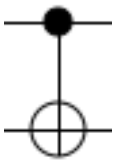
Il primo è un qubit di *controllo*, il secondo invece è il qubit *bersaglio*.

Questa porta logica permette di trasformare uno stato separabile in uno stato entangled.

$$CNOT(\alpha|\, 0 > + \beta|\, 1 >)|\, 0 >= CNOT(\alpha|\, 00 > + \beta|\, 10 >) = \alpha|\, 00 > + \beta|\, 11 > \tag{43}$$

Questa è una delle proprietà, dimostrata sperimentalmente, che sarà discussa nelle sezioni successive.

La seguente figura è la rappresentazione circuitale della porta C-NOT di tipo A. Le due righe orizzontali indicano l'evoluzione dei singoli qubit che da sinistra verso destra incontrano le porte logiche. Il simbolo "$\oplus$" rappresenta il NOT del secondo qubit se il primo è nello stato $|\, 1 >$, rappresentato da "$\bullet$".



Una seconda porta logica quantistica a due qubit è la porta *C-PHASE*[5] che cambia la fase del qubit bersaglio solo se il qubit di controllo si trova nello stato $|1 >$. L'operatore che permette questa trasformazione di definisce come segue

$$CPHASE(\delta) := R_z(\delta) \otimes \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\delta} & 0 \\ 0 & 0 & 0 & e^{i\delta} \end{pmatrix} \tag{44}$$

L'implementazione di queste porte logiche permette di processare *algoritmi quantistici*. Uno dei più famosi è l'algoritmo di Shor che sarà discritto in dettaglio nel possimo capitolo.

2 Algoritmo di Shor

Nel 1994 Peter Shor propone un algoritmo quantistico per fattorizzare i numeri interi in numeri primi. La parte dell'algoritmo che richiede più tempo computazionale è quella relativa alla "modular exponentiation"[2]: questo problema si può risolvere grazie all'algoritmo di Schönhage-Strassen[1]. Infatti, nell'articolo del 1971, i due matematici presentarono un algoritmo processabile in un tempo polinomiale.

Dato N, numero intero, l'algoritmo si svolge nei seguenti passaggi:

1. Scegliere in modo casuale un intero $1 < x < N$ e, attraverso l'algoritmo di Euclide, calcolare il massimo comune divisore $MCD(N, x)$.
   Se $MCD(N, x) \neq 1$ allora è stato trovato un fattore di N.
   Se invece $MCD(N, x) = 1$ procedere allo step 2.

2. Trovare l'*ordine* di x mod N, ovvero il più piccolo valore di r tale che x^r mod $N = 1$ (modular exponentiation). In questo caso r corrisponde al periodo della funzione $f_{x,N} : \mathbb{N} \to \mathbb{N}$ definita da $f_{x,N} : a \to x^a$ mod N.
   Se r è dispari tornare allo step 1.
   Se r è pari calcolare $x^{r/2}$ mod N.
   Se $x^{r/2}$ mod $N = -1$ tornare allo step 1.
   Se $x^{r/2}$ mod $N \neq -1$ procedere allo step 3.

3. Calcolare, attraverso l'algoritmo di Euclide, il massimo comune divisore $MCD(x^{r/2}+1, N)$ e $MCD(x^{r/2} - 1, N)$.
   Entrambi sono fattori non banali di N.

Si dimostra la validità dello step 3[3]:

Essendo x^r mod $N = 1$ allora $(x^r - 1)$ mod $N = 0$, quindi, essendo r pari,

$$(x^{r/2} - 1)(x^{r/2} + 1) \mod N = 0 \tag{45}$$

Tuttavia essendo r per definizione il più piccolo r tale che x^r mod $N = 1$, allora $x^{r/2}$ mod $N \neq 1$, ossia $(x^{r/2} - 1)$ mod $N \neq 0$.
Inoltre vale la condizione $x^{r/2}$ mod $N \neq -1$, ossia $(x^{r/2} + 1)$ mod $N \neq 0$. Questo significa che N divide il prodotto $(x^{r/2} - 1)(x^{r/2} + 1)$, ma non $(x^{r/2} - 1)$ e $(x^{r/2} + 1)$ singolarmente.
Da ciò si deduce che N deve avere fattori in comune con entrambi: alcuni con $(x^{r/2} - 1)$ altri con $(x^{r/2} + 1)$.

Questi fattori sono non banali, infatti se $MCD(x^{r/2} \pm 1, N) = N$ allora sarebbe vero che $(x^{r/2} \pm 1)$ mod $N = 0$, contro le ipotesi fatte.

Lemma di Bèzout
Siano $a, b \in \mathbb{N}$ e sia $d = MCD(a, b)$. Allora esistono $u, v \in \mathbb{N}$ tali che $au + bv = d$.

Se invece $MCD(x^{r/2} \pm 1, N) = 1$ allora per il *lemma di Bézout* devono valere le identità $(x^{r/2} \pm 1)u + Nv = 1$ con $u, v \in \mathbb{N}$.

$$(x^{r/2} \mp 1)(x^{r/2} \pm 1)u + N(x^{r/2} \mp 1)v = (x^{r/2} \mp 1) \tag{46}$$

$$(x^r - 1)u + N(x^{r/2} \mp 1)v = (x^{r/2} \mp 1) \tag{47}$$

Tuttavia essendo $(x^r - 1) \bmod N = 0$ allora per la (47) deve valere $(x^{r/2} \mp 1) \bmod N = 0$, contro le ipotesi fatte.

Il primo e il terzo step sono processabili in modo efficiente anche da un computer classico, tuttavia un computer quantistico riesce a trovare più facilmente il periodo della funzione $f_{x,N}$ allo step 2. Ciò è possibile grazie all'implementazione della Trasformata di Fourier quantistica, che all'interno dell'algoritmo svolge un ruolo fondamentale. È possibile implementare la trasformata tramite porte *Hadamard* e *phase-shift controllate*.

2.1 Trasformata di Fourier quantistica

La Trasformata di Fourier quantistica[5] è un operatore unitario F che agisce su un registro di n qubit. Se $|\, j >$ è uno stato della base computazionale, allora

$$F(|\, j >) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} |\, k > \tag{48}$$

Se si considera un generico stato $|\, \psi >= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} f(j) |\, j >$, allora si avrà che

$$F(|\, \psi >) = \sum_{k=0}^{2^n-1} \tilde{f}(k) |\, k > \tag{49}$$

dove

$$\tilde{f}(k) = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} f(j) \tag{50}$$

Quindi la Trasformata di Fourier

$$\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} f(j) |\, j > \longrightarrow \sum_{k=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi i \frac{jk}{2^n}} f(j) \right) |\, k > \tag{51}$$

si applica attraverso una matrice unitaria $2^n \times 2^n$, i cui elementi (j, k) sono dati da $(e^{2\pi i/2^n})^{jk}$.

È possibile modificare l'espressione della Trasformata di Fourier per ridurre il numero di operazioni che permettono di implementarla in un circuito quantistico. Innanzitutto si scrivono j e k nella loro espansione binaria.

$$j = j_{n-1} \cdot 2^{n-1} + \cdots + j_1 \cdot 2^1 + j_0 \cdot 2^0 \tag{52}$$

$$k = k_{n-1} \cdot 2^{n-1} + \cdots + k_1 \cdot 2^1 + k_0 \cdot 2^0 \tag{53}$$

Facendo il prodotto $jk/2^n$ si scartano le potenze di 2 maggiori o uguali di n, che non darebbero contributo agli elementi di matrice.

$$\frac{jk}{2^n} = k_{n-1}(.j_0) + k_{n-2}(.j_1 j_0) + \cdots + k_0(.j_{n-1} j_{n-2} \cdots j_0) \tag{54}$$

$$(.j_{m-1} j_{m-2} \cdots j_0) := \sum_{l=1}^{m} \frac{j_{m-l}}{2^l} = a_{m-1} \tag{55}$$

$$F(|\, j >) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp\left(2\pi i \frac{jk}{2^n}\right) |\, k > \tag{56}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_{n-1}=0}^{1} \cdots \sum_{k_1=0}^{1} \sum_{k_0=0}^{1} \exp\left[2\pi i \sum_{m=1}^{n} (k_{n-m}\, a_{m-1})\right] |\, k_{n-1} k_{n-2} \cdots k_0 > \tag{57}$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{m=1}^{n} \left[\sum_{k_{n-m}=0}^{1} \exp\left(2\pi i\, k_{n-m}\, a_{m-1}\right) |\, k_{n-m} >\right] \tag{58}$$

$$= \frac{1}{\sqrt{2^n}} \bigotimes_{m=1}^{n} [|\, 0 > + \exp\left(2\pi i\, a_{m-1}\right) |\, 1 >] \tag{59}$$

dunque l'm-esimo qubit dovrà trovarsi nello stato

$$\frac{1}{\sqrt{2}} \left(|\, 0 > + \exp\left(2\pi i \sum_{l=1}^{m} \frac{j_{m-l}}{2^l}\right) |\, 1 >\right) = \frac{1}{\sqrt{2}} \left(|\, 0 > + \prod_{l=1}^{m} \exp\left(2\pi i\, \frac{j_{m-l}}{2^l}\right) |\, 1 >\right) \tag{60}$$

Per raggiungere tale stato basta utilizzare una porta logica *Hadamard* e delle porte logiche R_l controllate, dove

$$R_l = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^l} \end{pmatrix} \tag{61}$$

Applicando H a $|\, j_{m-1} >$ si ottiene

$$\frac{1}{\sqrt{2}} \left(|\, 0 > + \exp\left(2\pi i\, \frac{j_{m-1}}{2}\right) |\, 1 >\right) \tag{62}$$

Applicando ora R_2 controllata sull'$(m-2)$-esimo qubit si ottiene

$$\frac{1}{\sqrt{2}}\left(|\,0>+\prod_{l=1}^{2}\exp\left(2\pi i\,\frac{j_{m-l}}{2^l}\right)|\,1>\right) \tag{63}$$

Continuando ad applicare R_l controllate sull' $(m-l)$-esimo qubit, finché $l=m$, si ottiene lo stato

$$\frac{1}{\sqrt{2}}\left(|\,0>+\prod_{l=1}^{m}\exp\left(2\pi i\,\frac{j_{m-l}}{2^l}\right)|\,1>\right) \tag{64}$$

Tale circuito va implementato in successione per ogni qubit del registro.

2.2 Come trovare il periodo

Per trovare il periodo richiesto allo step 2 dell'algoritmo di Shor si procede come segue[3]. Sia $f_{x,N}(a) = x^a \bmod N$, con $x, N \in \mathbb{N}$ ed $x < N$. L'obiettivo è trovare il più piccolo r tale che $f(a+r) = f(a)$. Per fare ciò si necessita di due registri di n qubit affinché $N^2 < 2^n < 2N^2 \Rightarrow 2^n/r > N$. Lo stato del sistema inizialmente dovrà trovarsi nello stato fiduciario

$$|\,\psi> = |0,0> \tag{65}$$

Successivamente si applica una trasformazione unitaria H ad ogni qubit del primo registro, ottenendo lo stato

$$|\,\psi> = \frac{1}{\sqrt{2^n}}\sum_{a=0}^{2^n-1}|\,a,0> \tag{66}$$

Scelto x è necessario calcolare la funzione $f_{x,N}$ applicando la seguente trasformazione

$$|\,a,0> \longrightarrow |\,a, x^a \bmod N> \tag{67}$$

implementabile in modo efficiente anche da un computer classico.
Preparato lo stato

$$|\,\psi> = \frac{1}{\sqrt{2^n}}\sum_{a=0}^{2^n-1}|\,a, x^a \bmod N> \tag{68}$$

si esegue una misura nella base computazionale sul secondo registro, ottenendo lo stato

$$|\,\psi> = \frac{1}{\sqrt{M}}\sum_{a\in A}|\,a,b> \tag{69}$$

dove A è un insieme di a tali che $x^a \bmod N = b$.

$$A = \{a_0, a_0+r, a_0+2r, ..., a_0+(M-1)r\} \tag{70}$$

$$|\psi> = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |a_0 + jr, b> \tag{71}$$

A questo punto si applica la Trasformata di Fourier al primo registro, ottenendo

$$|\psi> = \frac{1}{\sqrt{2^n M}} \sum_{k=0}^{2^n-1} \sum_{j=0}^{M-1} \exp\left(2\pi i \, \frac{k(a_0 + jr)}{2^n}\right) |k, b> \tag{72}$$

$$|\psi> = \frac{1}{\sqrt{2^n M}} \sum_{k=0}^{2^n-1} \exp\left(2\pi i \, \frac{k a_0}{2^n}\right) \sum_{j=0}^{M-1} \Omega^j |k, b> \qquad \Omega := \exp\left(2\pi i \, \frac{kr}{2^n}\right) \tag{73}$$

Ora si effettua una misura del primo registro nella base computazionale. Si osserva il sistema in uno stato $|k>$ con una probabilità pari a

$$Pr(k) = \frac{1}{2^n M} \left| \sum_{j=0}^{M-1} \Omega^j \right|^2 \tag{74}$$

È facile notare che per $kr/2^n \approx \lambda$, con $\lambda \in \mathbb{N}$, ovvero per $\Omega \to 1$, si ha il massimo della probabilità di osservare lo stato $|k>$. La probabilità per $\Omega \neq 1$ tende ad annullarsi per un fenomeno di interferenza distruttiva.

Conoscendo k ed n è possibile trovare quale frazione approssima meglio il valore di $k/2^n$, ottenendo così sia il valore di r che di λ. Per fare ciò si usa il metodo delle frazioni continue, facendo convergere λ/r a $k/2^n$.
A questo punto è importante sottolineare che le frazioni corrispndenti a quella cercata possono essere scritte come segue.

$$\frac{k}{2^n} \approx \frac{\lambda}{r} = \frac{2\lambda}{2r} = \frac{3\lambda}{3r} = ... \tag{75}$$

Per trovare il vero periodo sarà quindi necessario effettuare un'ultima verifica calcolando $x^r \bmod N$ per i primi multipli di r finché non si ottiene un valore pari ad 1. Il primo valore di r soddisfacente questa condizione sarà il periodo cercato.

Come si è visto il risultato ottenuto dipende dalla probabilità di successo nell'osservare un buon stato $|k>$ del primo registro. Per questo motivo per avere una maggiore confidenza sul risultato ottenuto è necessario ripetere l'algoritmo, calcolando la probabilità di successo come il rapporto fra i casi favorevoli sul numero di prove effettuate.

2.3 Fattorizzazare 91

Si propone un esempio numerico di fattorizzazione usando l'algoritmo di Shor. Si prende in considerazione il caso particolare in cui un numero N intero sia tale che $N = pq$ con p e q numeri primi. Questo esempio è propedeutico per capire successivamente come sia possibile violare facilmente il sistema di criptazione RSA con questo algoritmo.

$N = 91$

1. Si sceglie con un algoritmo di generazione di numeri casuali un numero intero $1 < x < 91$. Sia $x = 4$.

   Applico l'algoritmo di Euclide per calcolare $MCD(91, 4)$

   $$91 \mod 4 = 3$$
   $$4 \mod 3 = 1$$
   $$3 \mod 1 = 0$$
   $$MCD(91, 4) = 1$$

   $x = 4$ è un buon intero e si può passare allo step successivo.

2. Si fissa il numero n di qubit per due registri affinché $N^2 < 2^n < 2N^2 \Rightarrow Q/r > N$: $n = 14$.
   Partendo dallo stato fiduciario $|\,0, 0>$ si applica una trasformazione unitaria H ai 14 qubit del primo registro, ottenendo lo stato

   $$|\,\psi> = \frac{1}{\sqrt{16384}}\left(|\,0, 0> + |\,1, 0> + |\,2, 0> + |\,3, 0> + \cdots + |\,16383, 0>\right)$$

   Successivamente di applica $f_{4,91} : |\,a, 0> \longrightarrow |\,a, 4^a \bmod 91>$ ottenendo lo stato

   $$|\,\psi> = \frac{1}{\sqrt{16384}}\left(|\,0, 1> + |\,1, 4> + |\,2, 16> + |\,3, 64> + \cdots + |\,16383, 64>\right)$$

   Ora si effettua un'osservazione del secondo registro, ottenendo con circa uguale probabilità uno degli stati possibili. Supponiamo lo stato $|\,16>$.

   $$|\,\psi> = \frac{1}{\sqrt{456}}\left(|\,2, 16> + |\,8, 16> + |\,14, 16> + \cdots + |\,16382, 16>\right)$$

   Il passo successivo è l'applicazione della Trasformata di Fourier al primo registro.

   $$|\,\psi> = \frac{1}{\sqrt{7470192}} \sum_{k=0}^{16383} \exp\left(2\pi i \,\frac{2k}{16384}\right) \sum_{j=0}^{455} \Omega^j |k, 16>, \quad \Omega := \exp\left(2\pi i \,\frac{kr}{16384}\right)$$

Si effettua una misura sul primo registro, ottenendo come risultato uno stato corrispondente al valore di $k = 8193$. Di seguito si applica il metodo delle frazioni continue per trovare qualche frazione λ/r approssima meglio 8193/16384.

$$\frac{8193}{16384} = \frac{1}{\frac{16384}{8193}} = \frac{1}{1 + \frac{8191}{8193}}$$
$$\frac{8191}{8193} = \frac{1}{\frac{8193}{8191}} = \frac{1}{1 + \frac{2}{8191}}$$
$$\frac{8193}{16384} = \frac{1}{1 + \frac{1}{1 + \frac{2}{8191}}}$$

dunque si effettua la seguente approssimazione

$$\frac{8193}{16384} \approx \frac{1}{1 + \frac{1}{1}} = \frac{1}{2}$$

Si ottiene così un valore di $\lambda = 1$ ed $r = 2$. Tuttavia il giusto valore di r è il primo numero s multiplo di 2 che soddisfa $4^s \bmod 91 = 1$.

$$4^2 \mod 91 = 16$$
$$4^4 \mod 91 = 74$$
$$4^6 \mod 91 = 1 \quad \Rightarrow \quad r = 6$$

3. Si calcolano $MCD(4^{6/2} - 1 = 63, 91)$ e $MCD(4^{6/2} + 1 = 65, 91)$ con l'algoritmo di Euclide

$$91 \mod 63 = 28$$
$$63 \mod 28 = 7$$
$$28 \mod 7 = 0$$
$$p = MCD(63, 91) = 7$$

$$91 \mod 65 = 26$$
$$65 \mod 26 = 13$$
$$26 \mod 13 = 0$$
$$q = MCD(65, 91) = 13$$

$91 = 7 \times 13$

2.4 Protocollo RSA

Il protocollo RSA[5] è un sistema crittografico a chiave pubblica che permette ad oggi la trasmissione di messaggi in modo sicuro.

Questo funziona come segue:

1. Bob sceglie due numeri primi abbastanza grandi p e q e calcola $N = pq$

2. Bob genera un numero casuale d tale che $MCD[\,d, (p-1)(q-1)] = 1$

3. Bob calcola $e = 1/[\,d \bmod (p-1)(q-1)]$

4. Bob pubblica la coppia (e, N). Questa è la chiave pubblica con cui si può criptare un messaggio.

5. (d, N) è la chiave privata che possiede solo Bob. Solo con questa chiave si può decriptare il messaggio.

6. Alice divide il messaggio da inviare a Bob in blocchi. Ogni blocco uguale corrisponde ad un numero $b_i < N$. Ogni b_i è criptato calcolando $b'_i = b_i^e \bmod N$.

7. Bob decripta il messaggio calcolando $b_i = b_i'^{\,d} \bmod N$.

Questo algoritmo si basa sull'impossibilità per un computer classico di fattorizzare in tempi brevi un numero N a 1024 bit o maggiori. Infatti potendo risalire ai fattori p e q sarebbe possibile ottenere la chiave privata (d, N).
Come si è mostrato in precedenza, un computer quantistico sarebbe in grado di risolvere tale problema in tempi brevi. Dunque il protocollo RSA è un sistema crittografico che non può garantire la segretezza di un messaggio a lungo termine, ma fino a quando non sarà costruito un computer quantistico capace di processare l'algoritmo di Shor.

3 Dimostrazione sperimentale del modello circuitale

Molti ricercatori in tutto il mondo stanno lavorando per raggiungere il medesimo obiettivo: costruire un computer quantistico.
Per questo motivo vediamo quali sono gli aspetti più importanti di cui tener conto per una computazione efficiente e quali sistemi fisici siano i più sviluppati per raggiungere tale obiettivo tecnologico.
In particolare, per dimostrare il modello circuitale, si trattano due esperimenti basati sulla computazione con fotoni: il primo con codifica "dual-rail", il secondo con codifica in polarizzazione.

3.1 Requisiti per la computazione quantistica

L'aspetto più critico per la realizzazione di un computer quantistico è la necessità di isolare le operazioni interne di questo dal resto dell'Universo. In particolare le funzioni d'onda quantistiche non devono essere disturbate dall'ambiente esterno: l'interazione con esso porterebbe ad un processo di "*decoerenza*"[8].
Tale processo comporta lo svanimento del termine di interferenza costruttiva degli stati di sovrapposizione, con una conseguente introduzione di errori nei processi di computazione.
Per questo motivo un computer quantistico deve essere dotato della capacità di preservare lo stato quantistico durante la preparazione dello stato iniziale ed il processo di misura, evitando l'aumento di entropia introdotta dal mondo esterno e cercando di ridurla il più possibile.

Inoltre per effettuare una computazione non banale è necessario che il computer quantistico sia "*scalabile*"[8]. Tale proprietà permette di operare in uno spazio di Hilbert le cui dimensioni possono crescere esponenzialmente senza un esponenziale costo in termini di spazio, tempo ed energia.
Tuttavia dichiarare un computer quantistico scalabile non è banale, in quanto le risorse utilizzate per controllare i qubit (spazio su microcip, refrigeratori, appositi laser, etc.) devono essere a loro volta scalabili; questo comporta problemi di ingegneria complessi da superare.

Infine, per realizzare un computer quantistico, bisogna concentrarsi nella realizzazione di un set di porte logiche quantistiche che permetta di implementare una *logica universale*[8].
Affinché ciò sia possibile si può dimostrare che è sufficiente costruire porte a singolo qubit e porte C-NOT[5].

3.2 Tecnologie per realizzare un computer quantistico

Per realizzare l'unità d'informazione della computazione quantistica si ricorre a diversi sistemi fisici. Di seguito elencheremo una serie di metodi utilizzati per realizzare sperimentalmente un qubit e le porte logiche quantistiche[5,8].

Fotoni

Uno dei metodi più interessanti per realizzare un qubit è l'utilizzo della polarizzazione del fotone. Infatti è possibile considerare tale metodo uno dei pochi in cui la decoerenza affligge relativamente poco lo stato del sistema quantistico. Un computer quantistico scalabile è realizzabile seguendo lo schema KLM (Knill-Laflamme-Milburn) che prevede di usare solo sorgenti e rivelatori di fotone singolo, e circuiti ottici lineari.
Per i singoli fotoni sono usati rivelatori che, utilizzando nanofili superconduttori di NbN, raggiungono un'alta efficienza.
Uno dei tipi di sorgente utilizzabile può essere una cavità ottica che emette un singolo fotone dalla transizione da uno stato eccitato allo stato fondamentale.
Per realizzare le porte logiche si utilizzano circuiti a guida d'onda in silicio.
Si dimostrerà nelle sezioni successive il modello circuitale con una tecnologia basata su fotoni.

Atomi intrappolati

Eccellenti proprietà di coerenza sono raggiunte dai livelli energetici degli atomi. Per questo motivo i livelli energetici di sistemi atomici intrappolati ed isolati sono usati come qubit.
Apposite interazioni fra gli atomi permettono la realizzazione di stati entangled e delle relative porte logiche.
Lo stato iniziale è preparato tramite pompaggio ottico, mentre la misura dello stato è fatto tramite la rivelazione di fluorescenza ottica.
L'hardware è costituito da una stringa di ioni confinati da campi elettrici, o da un array di atomi neutri, confinati nello spazio da un reticolo di raggi laser incrociati. La seconda soluzione risulta migliore per quanto riguarda l'efficienza di controllo dello stato iniziale, dell'interazione e della misura dei quibit atomici. Il vero aspetto critico di questa tecnologia è la scalabilità dell'hardware che richiedere un'architettura più complessa per preservare il controllo dei qubit per sistemi atomici sempre più grandi: è in questa direzione che si concentreranno i futuri lavori di ricerca per questa tecnologia.

Risonanza magnetica nucleare

In questo caso l'hardware è costituito da un liquido contenente un gran numero di molecole (dell'ordine di 10^{18}), immeserso in un forte campo magnetico statico. Un qubit è lo spin di un nucleo di una molecola, mentre le porte quantistiche sono implementate mediante campi magnetici oscillanti risonanti (impulsi Rabi), utilizzando tecniche di risonanza magnetica nucleare (NMR). Le interazioni spin-spin fra atomi vicini sono alla base delle porte logiche a più qubit. Le molecole sono preparate in equilibrio termico e i singoli qubit non sono nè preparati nè misurati: si misura lo stato medio degli spin di tutte le molecole, considerate indipendenti le une dalle altre in quanto le interazioni, a causa del moto caotico, si mediano a zero nell'arco di tempo richiesto per implementare una porta quantistica. Con esperimenti NMR, è stato possibile dimostrare sperimentalmente diversi algoritmi quantistici. Purtroppo però, allo stato liquido la computazione NMR non è scalabile.

Stato solido

Riguardo alla computazione quantistica dello stato solido sono state avanzate diverse proposte. Infatti nel corso degli anni si è sviluppata una sofisticata tecnologia volta alla creazione di strutture artificiali e dispositivi su scala nanometrica. Uno degli aspetti più promettenti di questa tecnologia è l'offerta di una soluzione naturale al problema della scalabilità: si può beneficiare delle tecniche di fabbricazione della microelettronica.

Punti quantici: sono strutture fabbricate con i semiconduttori, in cui i potenziali elettrostatici confinano elettroni. La dimensione dei punti quantici è fra i dieci nanometri ed un micron. Il qubit è rappresentato dallo spin di un elettrone confinato in un punto quantico. Le operazioni quantistiche fra due qubit avvengono tramite "gating" della barriera elettrostatica fra due punti quantici. L'abbassamento o l'innalzamento di questa barriera corrisponde rispettivamente alla modalità "on-off" di interazione di due qubit. In linea di principio la scalabilità è possibile per la produzione di arrey di punti quantici. Tuttavia il vero problema è la varietà di processi di decoerenza che avvengono in questi dispositivi: la ricerca per questo tipo di tecnologia è principalmente concentrata sulla soluzione di tale problema.

Spin nei semiconduttori: una proposta di Bruce Kane concilia le tecniche NMR dello stato solido con la tecnologia dei microchip al silicio. L'idea è di mettere un singolo atomo di forsforo in una matrice di silicio. Il qubit sarebbe rappresentato dallo spin nucleare di un singolo atomo di fosforo. L'interazione iperfine fra qubit ed elettroni circostanti permette l'interazione fra diversi qubit. Le operazioni logiche sono implementate da campi magnetici (impulsi Rabi). Per disporre di tale tecnologia è necessaria la nanofabbricazione a scale atomiche. Tuttavia tali sfide tecnologiche sono affrontate da un campo di ricerca sempre più in rapido sviluppo.

Superconduttori

Utilizzando circuiti microelettronici superconduttori ci sono stati notevoli progressi sperimentali nella computazione quantistica. Infatti, nei superconduttori, coppie di elettroni, chiamate *Coppie di Cooper*, sono legate insieme per formare oggetti di carica doppia quella dell'elettrone. Potenziali elettrostatici possono confinare tali coppie in "box" micrometrici. I due stati di un qubit sono rappresentati da due stati di carica differenti di un "box" contente questa coppia. Lo stato del qubit è controllato da una giunzione Josephson. Tale giunzione prevede che due "boxes" siano separati da un sottile isolante e che una coppia di Cooper possa passare da uno all'altro tramite effetto tunnel quantistico. È possibile indurre oscillazioni Rabi tra questi due stati, implementando così porte logiche a singolo qubit. In un altro approccio un flusso magnetico viene applicato ad un anello superconduttore: i due stati di un qubit corrispondono al senso orario ed antiorario delle correnti circolanti. Con entrambi gli approcci è stato possibile osservare oscillazioni Rabi e controllare lo stato del qubit mediante impulsi a microonde Rabi.

Come risultato degli ultimi due decenni di informazione quantistica, la comunità scientifica può iniziare a impegnarsi seriamente nella progettazione di tali tecnologie al fine di un confronto delle diverse architetture. Solo così si potrà capire quale hardware sarà il migliore per una progettazione di computer quantistici su larga scala.
È necessario uno sforzo per spostarsi verso la realizzazione di dispositivi basati su principi quantistici, affinché possano essere più potenti, più efficienti e meno costosi di quelli classici.
Nelle prossime sezioni vedremo come due gruppi di ricerca hanno contribuito allo sviluppo della tecnologia che permette la computazione quantistica utilizzando fotoni.

3.3 Computazione con fotoni su chip al silicio

Alberto Politi ed il suo gruppo di ricerca ha dimostrato i circuiti quantistici a fotoni usando guide d'onda di SiO_2 su un chip di silicio[6].
La natura monlitica di questo dispositivo ha permesso di implementare sofisticati circuiti quantistici in modo semplice: infatti è stato possibile costruirne centinaia su un singolo wafer, verificandone il funzionamento e la ripetibilità delle misure.
Un tipico circuito quantistico a fotoni mette insieme diversi percorsi ottici in una rete ottica lineare, composta da interferometri classici e quantistici. In un'implementazione di rete ottica standard, i fotoni si propagano in aria e il circuito è costituito da specchi, beam splitter (BSS), o specchi semi-riflettenti che dividono e ricombinano i modi ottici, dando origine a fenomei di interferenza classica e quantistica. La visibilità di inteferenza e la quantità di fotoni persi sono i parametri che caratterizzano meglio le prestazioni del circuito quantistico.

Nel caso in questione, invece, i percorsi ottici dei fotoni attraverso le guide d'onda trasportano lo stato del qubit: gli stati $|0>$ e $|1>$ corrispondono a due possibili percorsi del fotone. Per correlare i due stati si sono avvicinante sufficientemente due guide d'onda: questa operazione è conosciuta come "*directional coupling*" (Fig. 2)[6]. La tecnologia più promettente per la computazione quantistica con fotoni sembra essere quella a singolo fotone: è stato necessario, quindi, realizzare delle guide apposite.

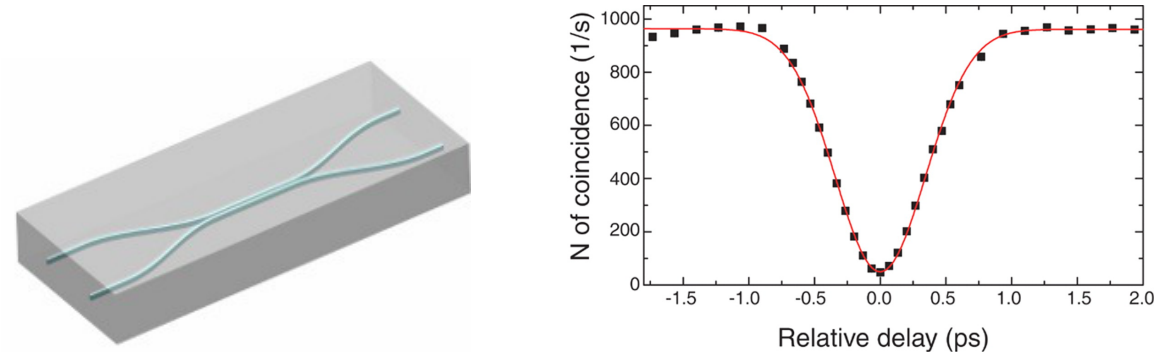


FIGURA 2: "Directional coupler" (a sinistra) e grafico interferenza (a destra)

Facendo passare due fotoni attraverso le guide d'onda è stato possibile misurare il fenomeno d'interferenza quantistica che il dispositivo produce in output. Costruendo la curva che mette in relazione il tasso di rilevazione di due fotoni ed il ritardo di arrivo relativo, è stato osservato un minimo caratteristico del fenomeno d'interferenza, come si vede in Fig. 2.
Per dimostrare che il comportamento quantistico dei fotoni in questa architettura ottica è molto buono, si calcola la visibilità come $V = (max - min)/max$, dove max e min sono gli estremanti della curva descritta, ottenendo $V = (94.8 \pm 0.5)\%$.

A questo punto il funzionamento di tale dispositivo è stato verificato costruendo una porta C-NOT in cui il qubit di controllo C ed il qubit bersaglio T sono sono entrambi codificati da un fotone in due guide d'onda. L'implementazione di questa porta è permessa dalla costruzione di due "directional couplers" di tipo 1/2 e tre di tipo 1/3 (le frazioni 1/2 ed 1/3 corrispondono al valore rispettivo di trasmittività del "directional coupler" considerato), secondo lo schema teorico (Fig. 3) presentato da T. C. Ralph, N. K. Langford, T. B. Bell, A. G. White[4].

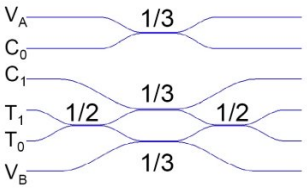


FIGURA 3: schema porta C-NOT con "directional couplers"

Sono stati impostati come input le quattro basi computazionali $|0>_C |0>_T$, $|0>_C |1>_T$, $|1>_C |0>_T$ e $|1>_C |1>_T$, misurando la probabilità di rilevare ogni base computazionale in output[6]. Come si vede dalla Fig. 4-A le probabilità misurate per le diverse basi computazionali sono in accordo con quelle previste. In particolare si può notare che in presenza di $|0>_C$ (misura di interferenza classica) si ha un accordo eccellente, prova della stabilità delle guide d'onda. Il valore di fedeltà, ottenuto dalla ricostruzione della tabella di verità della porta C-NOT (come stima della compatibilità dello stato misurato con lo stato atteso), risulta pari a $(94.3 \pm 0.2)\%$.

Per confermare direttamente la coerenza degli stati quantistici ed il fenomeno di entanglement dei dispositivi[6], sono state lanciate coppie di fotoni nelle guide d'onda T_0 e T_1. Il primo "directional coupler" 1/2 dovrebbe trasformare lo stato quantistico come segue:

$$|11>_{T_0T_1} \rightarrow \frac{1}{\sqrt{2}} (|20>_{T_0T_1} - |02>_{T_0T_1}) \tag{76}$$

cioè uno stato di sovrapposizione nelle due guide d'onda. Rilevare un basso tasso di fotoni alle uscite C_1 e V_A, ed un alto tasso di due fotoni in una di queste uscite, conferma che lo stato era composto in predominanza da $|02>$ e $|20>$. Il secondo "directional coupler" 1/2 dovrebbe compiere la trasformazione inversa della (76) se lo stato di sovrapposizione esiste. Ciò è confermato dall'alto tasso di fotoni rilevati alle uscite T_0 e T_1, ed un basso tasso di due fotoni rilevati in uno di questi output.

La matrice di densità di uno stato si definisce come

$$\rho = \sum_i p_i |\psi_i><\psi_i| \tag{77}$$

dove la p_i è la probabilità di misurare la base i-esima $|\psi_i>$ che compone lo stato.
In questo caso quindi la matrice di densità dello stato $\frac{1}{\sqrt{2}}(|20> - |02>)$, tenendo conto anche della probabilità nulla di osservare lo stato iniziale $|11>$, risulta essere

$$\begin{pmatrix} 1/2 & 0 & -1/2 \\ 0 & 0 & 0 \\ -1/2 & 0 & 1/2 \end{pmatrix} \tag{78}$$

È possibile confrontare tale risultato con la Fig. 4-D, in cui è riportata la ricostruzione tomografica, teorica e sperimentale, della matrice di densità in questione.
Il valore di fedeltà ottenuto, come stima della compatibilità degli stati misurati con lo stato teorico $\frac{1}{\sqrt{2}}(|20> - |02>)$, risulta $> 92\%$.

Infine sono stati testati i circuiti rappresentati in Fig. 4-(B e C)[6], costituiti da una porta C-NOT e porte Hadarmard (ognuna implementata con un "directional coupler" 1/2 fra C_0 e C_1). Le porte Hadamard implementano rispettivamente le trasformazioni (28) e (29).

Nel primo caso la trasformazione implementata corrisponde all'operatore

$$B = (H \otimes I)(CNOT)(H \otimes I) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix} \tag{79}$$

Per cui il circuito dovrebbe produrre quattro stati come segue

$$B|00>= \tfrac{1}{\sqrt{2}}(|00> +|01> +|10> -|11>) \tag{80}$$

$$B|01>= \tfrac{1}{\sqrt{2}}(|00> +|01> -|10> +|11>) \tag{81}$$

$$B|10>= \tfrac{1}{\sqrt{2}}(|00> -|01> +|10> +|11>) \tag{82}$$

$$B|11>= \tfrac{1}{\sqrt{2}}(-|00> +|01> +|10> +|11>) \tag{83}$$

Nel secondo caso la trasformazione implementata corrisponde all'operatore

$$C = (CNOT)(H \otimes I) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \tag{84}$$

Per cui il circuito dovrebbe produrre i quattro stati di Bell come segue

$$C|00>= \tfrac{1}{\sqrt{2}}(|00> +|11>) = \Phi^+ \tag{85}$$

$$C|01>= \tfrac{1}{\sqrt{2}}(|01> +|10>) = \Psi^+ \tag{86}$$

$$C|10>= \tfrac{1}{\sqrt{2}}(|00> -|11>) = \Phi^- \tag{87}$$

$$C|11>= \tfrac{1}{\sqrt{2}}(|01> -|10>) = \Psi^- \tag{88}$$

In entrambi i casi si è osservato un'ottima compatibilità con le operazioni ideali, quantificata da un valore di fedeltà pari rispettivamente a (97.9 $\pm$ 0.4)% e (91.5 $\pm$ 0.2)%.

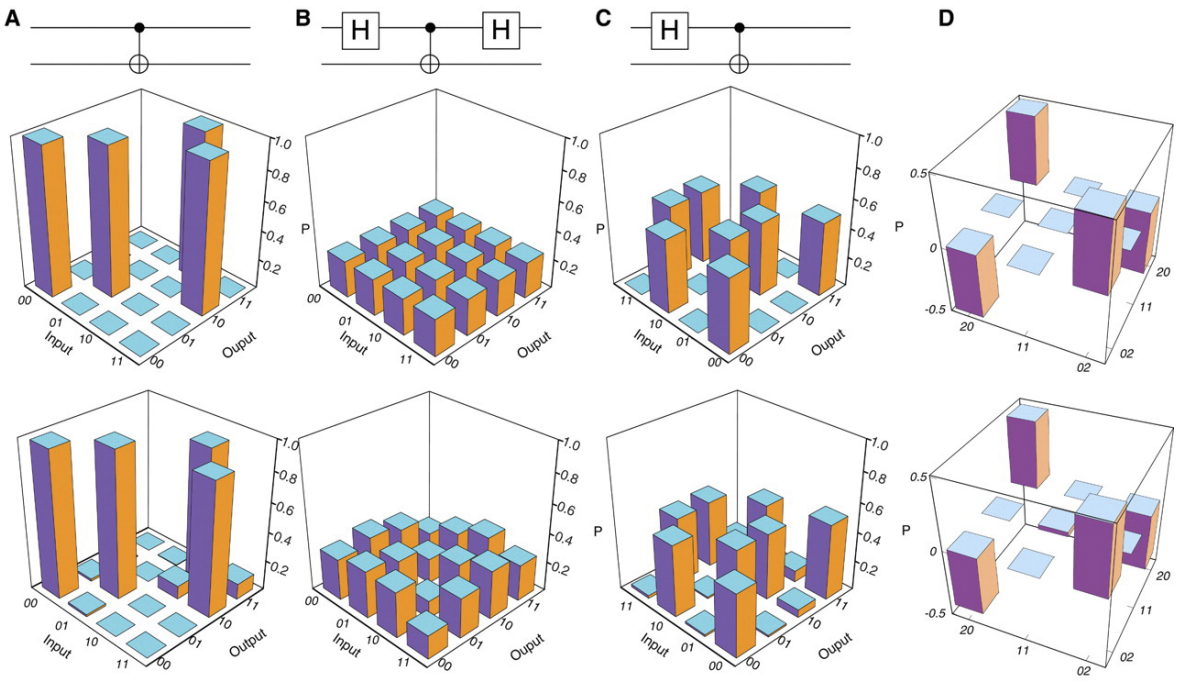


FIGURA 4

È stato dunque dimostrato come i componenti chiave per la computazione quantistica siano integrati su dispositivi a guide d'onda su silicio con un'alta fedeltà, senza la necessità di utilizzo di interferometri complicati. Questo lavoro ha permesso di aprire la strada alla scalabilità dei circuiti quantistici con fotoni e a futuri metodi di codifica dell'informazione, relativi all'utilizzo di tale tecnologia.

3.4 Algoritmo di Shor su un chip con tecnologia a fotoni

Un'applicazione dei dispositivi per costruire circuiti quantistici a fotoni, con guide d'onda al silicio, è l'implementazione dell'algoritmo di Shor[7]. La scalabilità di tale tecnologia ha permesso di dimostrare una versione compilata di questo algoritmo su quattro qubit.
Come si è visto, tale algoritmo risulta il migliore per la scomposizione dei numeri in fattori primi. Tuttavia il dispositivo che vediamo è stato realizzato per scomporre il numero 15.

Il circuito[7] utilizza cinque qubit, uno dei quali (x_0) risulta *ausiliario*, rimanendo sempre in uno stato separato.
L'implementazione fisica, come si può vedere dalla Fig. 5-B, consiste nella realizzazione di due porte C-PHASE (CZ) e sei porte Hadamard (H).

La computazione procede come segue: quattro fotoni sono introdotti nelle guide d'onda "0" o "1" per preparare lo stato iniziale $|\psi_{in}> = |0>_{x_1} |0>_{x_2} |0>_{f_1} |1>_{f_2}$ (questo non rappresenta 15 ma l'inizializzazione dell'algoritmo compilato per calcolare i fattori di 15). Le porte H, implementate da dei "directional coupler" 1/2, preparano ogni qubit nella sovrapposizione degli stati 0 e 1, affinchè l'intero stato sia una sovrapposizione di tutti i possibili 4 bit di partenza (questo parallelismo permette in parte l'aumento di velocità del calcolo). Il cuore del processo è dato da due porte CZ indipendenti, grazie ad una rete di "directional coupler" 1/3. Queste, combinate con le porte H implementano le porte C-NOT necessarie per l'algoritmo.
Successivamente la misura dei qubit x_1 e x_2 permette di processare la parte classica dell'algoritmo per calcolare i fattori di 15.

Come si vede dalla Fig. 5-C, in output sono stati osservati gli stati $x_2x_1x_0 = 000$, 010, 100, 110. Gli output 010 e 110 corrispondono al corretto calcolo per trovare l'ordine $r = 4$, che permette di calcolare con una computazione classica i fattori 3 e 5; 100 e 000 corrispondono a due valori errati inerenti all'algoritmo di Shor, in particolare il primo contiene l'informazione dei fattori banali 1 e 15. La fedeltà dei dati misurati con la distribuzione di probabilità ideale (linea tratteggiata) è pari a $(99 \pm 1)\%$.

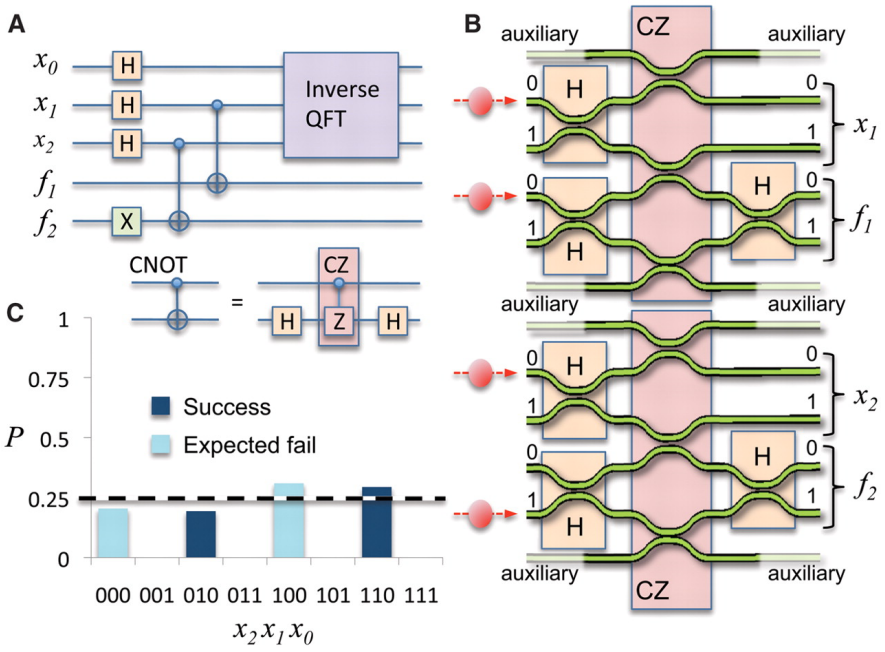


FIGURA 5

La dimostrazione dell'algoritmo di Shor implementato su piccola scala mostra le promettenti capacità dei circuiti quantistici a fotoni con guide d'onda. La possibilità di implementare interferometri così complessi in un architettura miniaturizzata e stabile è un passaggio cruciale per la futura realizzazione di algoritmi quantistici su larga scala.

3.5 Realizzazione di una porta C-NOT a fotoni

Per quanto riguarda la realizzazioni di circuiti quantistici con fotoni finora abbiamo visto un esempio in cui i qubit sono codificati in due percorsi ottici, per rappresentare la base computazionale ($|0>, |1>$). Tuttavia uno studio, condotto da Andrea Crespi ed il suo gruppo di ricerca, ha integrato a tali dispositivi la possibilità di codificare i qubit tramite la polarizzazione dei fotoni stessi[9].
Per fare ciò è stato utilizzato un laser a femtosecondi che ha permesso la realizzazione diretta di "directional couplers" capaci di avere un controllo accurato e indipendente del rapporto di scissione fra polarizzazione orizzontale (H) e verticale (V) dei fotoni.

"Directional coupler" come "partially polarized beam splitters"

Un "directional coupler" è composto da due distinte guide d'onda poste vicine per una certa lunghezza, chiamata lunghezza d'interazione, affinchè i due modi di propagazione si possano accoppiare attraverso la sovrapposizione del campo evanescente. È possibile fare un'analogia fra i "beam splitters" (BSs) e i "directional couplers" (DCs)[9]. In analogia con i BSs, i rapporti di riflettività e trasmissività dei DCs possono essere definiti come

$$R = \frac{P_{OUT1}}{P_{OUT1} + P_{OUT2}} \qquad T = 1 - R = \frac{P_{OUT2}}{P_{OUT1} + P_{OUT2}} \tag{89}$$

rispettivamente, quando la luce passa dalla porta $IN1$, (P indica la potenza ottica). Scambiando gli indici si ottengono le rispettive relazioni per la porta $IN2$ (Fig. 6-a).

In presenza di un analogo della birifrangenza per le guide d'onda, il coefficiente di accoppiamento, e quindi il periodo di oscillazione della legge sinusoidale che mette in relazione la potenza ottica trasferita da una guida d'onda e un'altra con la lunghezza di interferenza, cambia per diverse polarizzazioni.
Tuttavia un'alta birifrangenza può portare a processi di decoerenza degli stati dei fotoni accoppiati. Pertanto una guida d'onda ottimale è caratterizzata dal miglior compromesso fra la birifrangenza, che dovrebbe essere sufficientemente bassa per preservare la coerenza tra fotoni, e sufficientemente elevata da consentire il processo dipendente dalla polarizzazione. Tale compromesso è realizzabile grazie a guide d'onda incise su un verto borosilicato (con bassa birifrangenza) da un laser a femtosecondi.
Questo approccio ha portato alla costruzione di "partially polarized beam splitters" (PPBSs) integrati da "partially polarized directional couplers" (PPDCs).

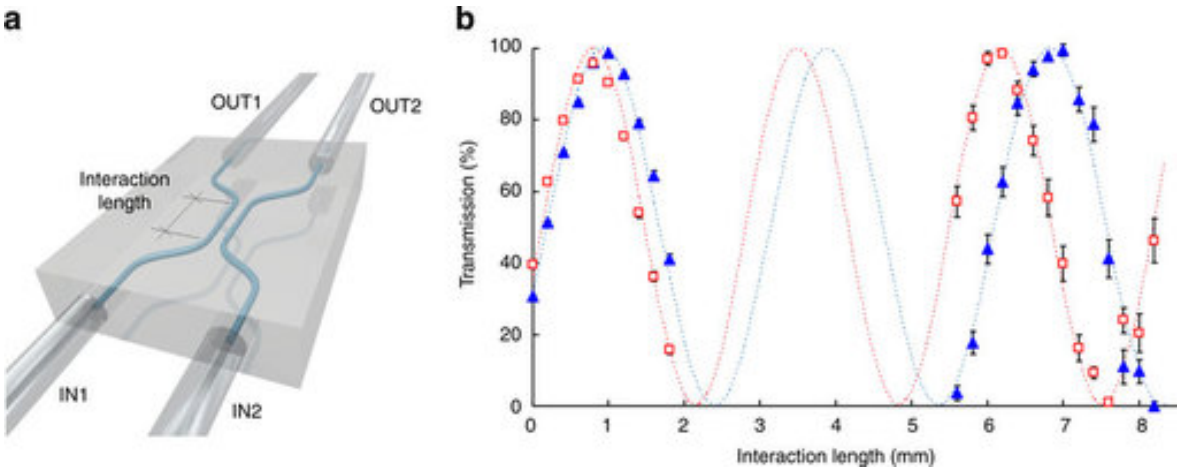


FIGURA 6

Codifica in polarizzazione dei qubit per realizzare porte quantistiche

Questa tecnologia può essere sfruttata per la costruzione di porte logiche quantistiche basate sulla codifica in polarizzazione dei qubit. In particolare un qubit potrà essere implementato come la sovrapposizione coerente degli stati di polarizzazione H e V: $\alpha|H> + \beta|V>$.

Come abbiamo detto, per ottenere una computazione quantistica universale sono sufficienti porte logiche a singolo qubit e porte logiche a due qubit. Per implementare trasformazioni su singolo qubit si usano delle lamine quarto d'onda birifrangenti. Mentre la porta a due qubit più usata è la C-NOT. Obiettivo dello studio condotto gruppo di ricerca è la caratterizzazione del comportamento quantistico di una porta C-NOT, realizzata con la tecnologia basata sulla codifica in polazizzazione dei qubit.

Una porta C-NOT permette di correlare e separare lo stato dei due qubit di input. Ad esempio se come input si hanno gli stati $|\pm>_C |0>_T$ e $|\pm>_C |1>_T$, con $|\pm> = \frac{1}{\sqrt{2}}(|0> \pm |1>)$, allora come output di una porta C-NOT si avranno rispettivamente gli stati correlati di Bell.

$$CNOT|\pm 0> = \Phi^{\pm} \tag{90}$$

$$CNOT|\pm 1> = \Psi^{\pm} \tag{91}$$

Un computer quantistico scalabile è realizzabile utilizzando solo circuiti ottici lineari, composti prevalentemente da BSs. Lo schema più semplice per implementare una porta C-NOT con codifica in polarizzazione presenta tre PPBSs con codifica in polarizzazione. Nella descrizione del setup sperimentale vedremo che per la sua implementazione sono stati utilizzati tre PPDCs.

Il setup sperimentale

Il setup sperimentale[9] utilizzato può essere concettualmente diviso in tre parti come si vede dalla Fig. 7.

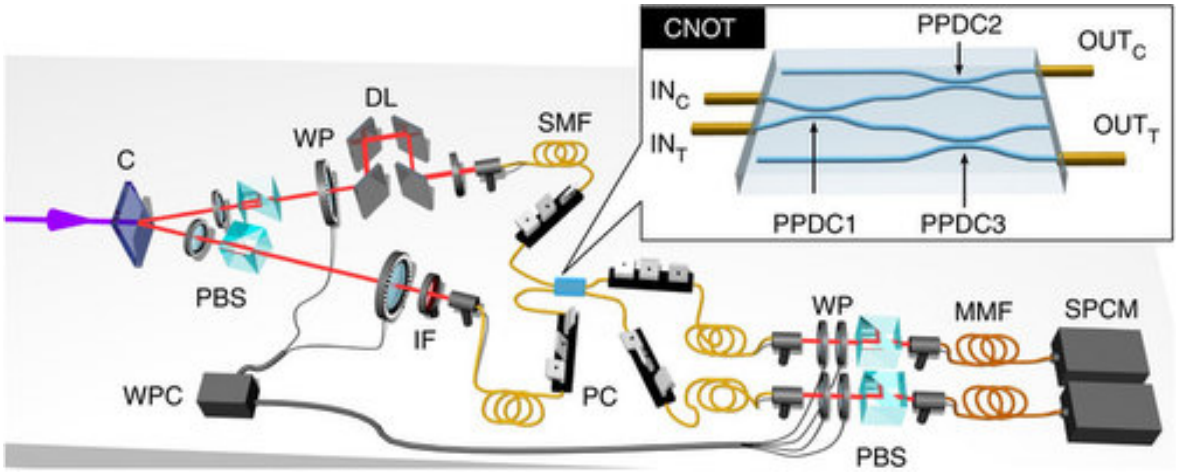


FIGURA 7

La prima è la sorgente: fotoni di lunghezza d'onda $\lambda = 806\,nm$ sono generati dalla conversione parametrica spontanea attraverso un cristallo di β-bario borato (C). Lo stato di polarizzazione dei fotni è preparato usando "polarizing beam splitters" (PBSs) e lamine quarto d'onda (WPs). La corrispondenza fra qubit logici e stati fisici è data dalle seguenti relazioni: $|0>_C \equiv |V>$, $|1>_C \equiv |H>$, $|0>_T \equiv \frac{1}{\sqrt{2}}(|H> + |V>)$, $|1>_T \equiv \frac{1}{\sqrt{2}}(|H> - |V>)$. Una "delay line" (DL) controlla la sovrapposizione temporale dei fotoni che sono poi accoppiati a fibre ottiche monomodali (SMFs) e iniettati nella porta C-NOT. I filtri di interferenza (IFs) determinano la larghezza di banda dei fotoni $\Delta\lambda = 6\,nm$.

La seconda parte mostra la porta C-NOT realizzata con la tecnica di incisione del laser a femtosecondi. Per ottenere il dispositivo con miglior prestazione è stato costruita una porta C-NOT di calibrazione. Questa è costituita da un primo PPDC (1), con trasmissività $T_H^{(1)} = 0$ e $T_V^{(1)} = \frac{2}{3}$ rispettivamente per la polarizzazione orizzontale e verticale, dove il qubit di controllo ed il qubit bersaglio interferisco. Di seguito ci sono altri due PPDC (2 e 3) con $T_H^{(2,3)} = \frac{1}{3}$ e $T_V^{(2,3)} = 1$.
I PPDC sono stati costruiti tenendo le guide d'onda ad una distanza costante di $7\,\mu m$. Per ottenere la trasmittività desiderata, il primo PPDC è caratterizzato da una lunghezza di interazione $L_1 \simeq 7.4\,mm$, per i secondi due $L_{2,3} \simeq 7\,mm$.

Successivamente, costruendo diversi dispositivi con lunghezze di interazione intorno L_1 ed L_2, la porta C-NOT con miglior pestrazione risultava caratterizzata dai seguenti parametri di trasmettività: $T_H^{(1)} < 1\%$, $T_V^{(1)} = (64 \pm 1)\%$, $T_H^{(2)} = (43 \pm 1)\%$, $T_V^{(2)} = (98 \pm 1)\%$, $T_H^{(3)} < (27 \pm 1)\%$, $T_V^{(3)} = (93 \pm 1)\%$.

La terza parte è costituita dalla strumentazione per l'analisi: lo stato di polarizzazione dei qubit uscenti dal chip viene misurata mediante un setup standard d'analisi (WP e PBS). I fotoni poi raggiungono i moduli di conteggio di fotoni singoli (SPCM) attraverso fibre multimodali (MMF) e sono misurate le coincidenze tra i due canali. Controlli di polarizzazione (PC) sono effettuati prima e dopo il dispositivo C-NOT, per compensare eventuali rotazioni di polarizzazione indotte dalle fibre. Infine è presente un dispositivo di controllo delle lamine quarto d'onda (WPC) per automatizzare le misurazioni.

Caratterizzazione della porta C-NOT

Il primo esperimento condotto sulla porta C-NOT è stato quello di determinare la sua tabella di verità[9].
Una volta ottenuto lo stato di sovrapposizione dei fotoni nel PPDC1, sono state prepareta come input per il chip le basi computazionali $|0>_C |0>_T$, $|0>_C |1>_T$, $|1>_C |0>_T$, $|1>_C |1>_T$ e sono state misurate le probabilità di ottenere ognuna di esse in output. La tabella di verità ottenuta è riportata nella Fig. 8-a.
La fedeltà delle basi logiche è stata calcolata come 0.940 ± 0.004. Tenendo conto dei parametri di trasmissività dei PPDCs, la fedeltà attesa risulta pari a 0.975 ± 0.007. Questa discrepanza è stata attribuita sia alla parziale distinguibilità dei pacchetti d'onda dei fotoni, che alla non perfetta comprensione della rotazione della polarizzazione nelle fibre ottiche monomodali.

La porta C-NOT è stata sfruttata anche per verificare il suo comportamento di "entangling gate", che permette di correlare stati separati[9]. A tal fine sono stati preparati come input gli stati $|\pm>_C |0>_T$ e $|\pm>_C |1>_T$ per ottenere in uscita gli stati di Bell. In particolare in Fig. 8-b è riportata una ricostruzione tomografica della matrice di densità dello stato Φ^+, in ottimo accordo con quella teorica

$$\begin{pmatrix} 1/2 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 1/2 \end{pmatrix} \tag{92}$$

Come si può vedere dalla Fig. 8-c è stata misurata la probabilità di ottenere come output gli stati di Bell corrispondenti alla trasformazione C-NOT degli stati iniziali, ottenendo un valore di fedeltà medio pari a 0.912 ± 0.005; analogamente sono state misurate anche le probabilità di ottenere come output gli stati iniziali a partire dagli stati di Bell come input (Fig. 8-d): in questo caso la probabilità di discriminazione dei quattro output ortogonali risulta pari a 0.877 ± 0.007, leggermente più bassa delle fedeltà precedenti. Questo è dovuto ad imperfezioni della sorgente degli stati correlati[9].

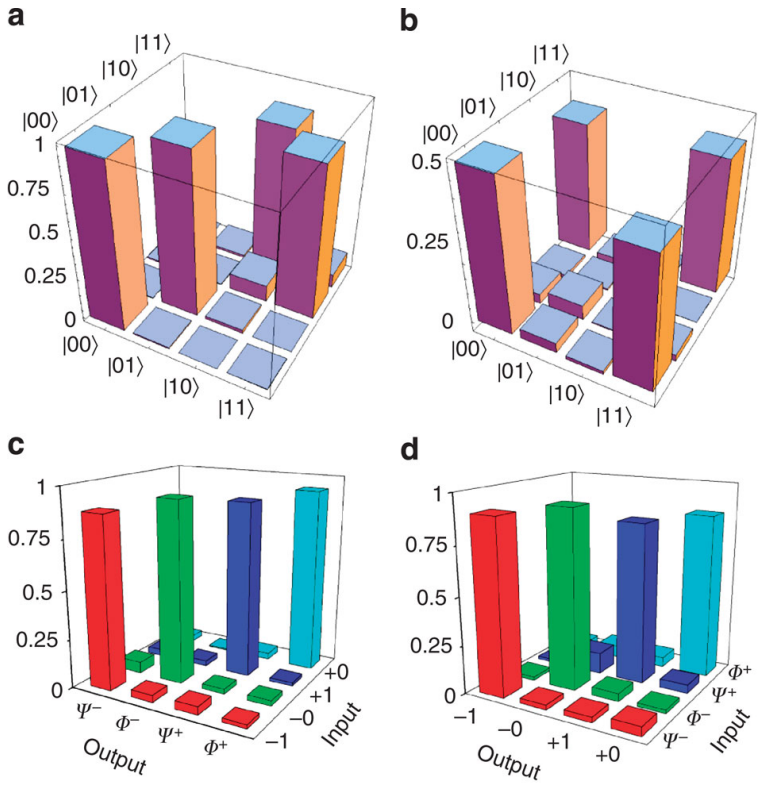


FIGURA 8

Lo studio condotto dal gruppo di ricerca ha permesso la dimostrazione della prima porta C-NOT a fotoni basata sulla codifica in polarizzazione. Questo successo è stato possibile grazie all'uso del laser a femtosecondi, uno strumento che ha permesso la realizzazione di dispositivi a guida d'onda sensibili alla polarizzazione, arricchendo la quantità di applicazioni che possono essere affrontate con questa semplice e flessibile tecnica di fabbricazione.
Questo lavoro è stato sicuramente un passo importante verso lo sviluppo di un una tecnologia a fotoni integrata per fornire una valida soluzione all'elaborazione dell'informazione quantistica. Tale tecnologia spiana la strada ad una vasta gamma di algoritmi quantistici basati sulla polarizzazione dei fotoni, a beneficio anche il campo della simulazione quantistica di fenomeni fisici complessi.

4 Conclusioni

L'obiettivo di questo lavoro è stato quello di approfondire le basi teoriche del modello circuitale della computazione quantistica. Grazie a questo studio è stato possibile descrivere in dettaglio uno degli algoritmi quantistici più famosi: l'algoritmo di Shor. Così si è potuto mettere in luce una delle applicazioni dell'implementazione del modello circuitale, con le sue implicazioni sulla vulnerabilità del protocollo di sicurezza RSA.
Dopo la contestualizzazione teorica è stato possibile porre l'attenzione su uno degli sviluppi recenti della computazione quantistica. Infatti, come abbiamo visto, la tecnologia a fotoni, ha permesso l'implementazione di porte logiche a singolo qubit e porte logiche controllate, dimostrando, con un alto grado di attendibilità, il modello circuitale.
In conclusione, questi lavori aprono le porte alla realizzazione di una logica universale, definendo la strada per la futura scalabilità del computer quantistico con la tecnologia a fotoni.

5 Bibliografia

1. A. Schönhage, V. Strassen, Schnelle Multiplikation grosser Zahlen, *Computing* **7**, 281-292 (1971)

2. P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM J. Computing* **26**, 1484-1509 (1997)

3. J. Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation*, California Institute of Technology (1998);

4. T. C. Ralph, N. K. Langford, T. B. Bell, A. G. White in *Phys. Rev.* A **65**, 062324 (2002)

5. G. Benenti, G. Casati, G. Strini, *Principles of Quantum Computation and Information - Volume 1: Basic concepts*, World Scientific Publishing Co. Pte. Ltd., Singapore (2004);

6. A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, J. L. O'Brien, Silica-on-Silicon Waveguide Quantum Circuits, *Science* **320**, 646-649 (2008);

7. A. Politi, J. C. F. Matthews, J. L. O'Brien, Shor's Quantum Factoring Algorithm on a Photonic Chip, *Science* **325**, 1221 (2009);

8. T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J. L. O'Brien, Quantum Computers, *Nature* **464**, 45-53 (2010);

9. A. Crespi, R. Ramponi, R. Osellame, L. Sansoni, I. Bongioanni, F. Sciarrino, G. Vallone, P. Mataloni, Integrated photonic quantum gates for polarization qubits, *Nature Communications* **566**, 1-6 (2011);