Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

Crittografia quantistica e algoritmo di Shor

Tesi di laurea in crittografia

Relatore:
Chiar.mo Prof.
Davide Aliffi

Presentata da:
Michele Bandini

V sessione
Anno Accademico 2017-2018

A Toski, per il supporto morale;
A Flap, per il supporto intellettuale.

Introduzione

Un problema classico su cui sono basati molti degli algoritmi crittografici odierni, è il problema della fattorizzazione: una volta trovata una soluzione, è facile verificarla, facendolo ricadere nella categoria di problemi detta *NP*; tuttavia, trovare effettivamente una soluzione sembra molto difficile. Per capire meglio di cosa stiamo parlando, può essere utile dare una definizione:

Definizione 0.1. Dati due numeri $(x, y) \in \mathbb{N}^2$, chiamiamo f_{mult} la funzione

$$f_{mult}(x, y) = \begin{cases} 1 & \text{se } x = 1 \vee y = 1 \\ x \cdot y & \text{altrimenti} \end{cases}$$

Invertire questa funzione significa trovare i valori (x, y) che moltiplicati insieme restituiscono un dato N: si noti che f_{mult} dà come risultato 1, nel caso in cui uno dei due fattori sia 1. Questo serve per impedire che il problema di fattorizzare un numero N sia facilmente risolto con la fattorizzazione banale, ossia fattorizzando $N = 1 \cdot N$.

Per apprezzare le implicazioni crittografiche, e per capire come sia possibile che un calcolatore quantistico sia capace di risolvere un tale problema in minor tempo di un calcolatore classico, bisogna fare prima alcune considerazioni.

Il problema di fattorizzare primi non sarebbe così studiato se non fosse che uno dei metodi più usati dai sistemi crittografici odierni, il metodo RSA di crittografia a chiave pubblica, "sfrutta" la sua difficoltà come forma di sicurezza. Un sistema a chiave pubblica funziona come segue: un utente, che chiameremo Alice, genera due chiavi, una segreta, che chiameremo k_s, e una pubblica, che chiameremo k_p, in modo che si possa codificare un messaggio con k_p, ma che sia necessaria k_s per decifrarlo. A quel punto, rende pubblica la chiave k_p: chiunque voglia mandare messaggi ad A può cifrarli con essa, mentre solo A conosce k_s per decifrarli. Affinché un sistema del genere funzioni, è necessario trovare una classe di funzioni che corrisponda alla descrizione appena fatta, ossia che si possa calcolare con una chiave ma che necessiti di un'altra per essere invertita. Una delle più usate fu pubblicata da Rivest, Shamir e Adleman, e prende il nome dalle loro iniziali: è detta *classe di funzioni RSA*, e si definisce come segue:

Definizione 0.2. Sia $\mathbf{RSA} = \{f_i : D_i \to R_i\}_{i \in I}$, dove

$$\begin{aligned} I &= \{(N,e) | N = p \cdot q \quad \text{t.c.} \quad p,q \in \Pi_n \text{e} e \in \mathbb{Z}_{\Phi(N)}*\} \\ D_i &= \{x | x \in \mathbb{Z}_N*\} \\ R_i &= \mathbb{Z}_N* \\ f_{N,e}(x) &= x^e \mod N \end{aligned}$$

Senza entrare troppo nei dettagli, un avversario che vuole decifrare un testo cifrato codificato tramite RSA, deve invertire un'elevazione a potenza modulo N, e si può dimostrare che problema diventa "facile" se questo avversario conosce i valori dei fattori di N.

Va sottolineato che fattorizzare N non è sempre così difficile: lo diventa quando N è il prodotto di due primi. Se Alice vuole utilizzare il sistema RSA cercherà quindi prima due numeri primi (ad esempio usando il criterio di Rabin), e poi li moltiplicherà tra loro per generare N. A questo punto, può distribuire (N,e) come chiave pubblica, tenendo segreti i due primi che compongono N.

Fin oggi, non è ancora stato mostrato che il problema non è risolubile in tempo polinomiale; tuttavia, l'algoritmo più veloce conosciuto ad oggi impiega $O\left(\exp \sqrt[3]{\frac{64}{9} n (\log n)^2}\right)$ operazioni, dove n è il numero di cifre del numero da fattorizzare: un tempo quindi subesponenziale, cioè molto più lento di qualsiasi algoritmo polinomiale, per n grande. Molte aree della matematica sono state chiamate in causa per trovare algoritmi più veloci per computer classici, o perlomeno per dimostrare che non ne esisteva uno. Nel 1994, Peter Shor pubblicò un articolo che mostrava un algoritmo capace di scomporre qualsiasi numero composto in tempo polinomiale, utilizzando un calcolatore quantistico. Il resto di questo elaborato si impegnerà nello spiegare come funziona un calcolatore quantistico, come si possono utilizzare le sue peculiarità per velocizzare i calcoli, e come funziona l'algoritmo di Shor.

Indice

Capitolo 1

Il computer quantistico

I fenomeni che avvengono a livello quantistico sono spesso difficili da comprendere, perché buona parte della nostra esperienza quotidiana non è applicabile. Una spiegazione completa della meccanica quantistica esula dagli obiettivi di questo lavoro; tuttavia, non è necessario conoscere profondamente l'argomento per utilizzare le sue qualità nella computazione quantistica.

Una cosa da sapere è che la fisica quantistica è una teoria, in senso matematico: ci sono degli assiomi che la governano. Questi postulati riescono a descrivere il comportamento di sistemi quantistici. Gli assiomi in questione portano a molti fenomeni apparentemente paradossali: nell'effetto Compton, un'azione sembra precedere la sua causa; l'esperimento EPR fa supporre la possibilità di un'azione che si propaga a una velocità maggiore di quella della luce. Molti di questi esperimenti richiedono strumenti molto sofisticati e portano solo a misurazioni indirette. Tuttavia, è possibile fare un esperimento che richiede solo strumentazione facilmente ottenibile e può aiutare a comprendere alcuni aspetti chiave della fisica quantistica necessari per i calcolatori quantistici.

1.1 Polarizzazione dei fotoni

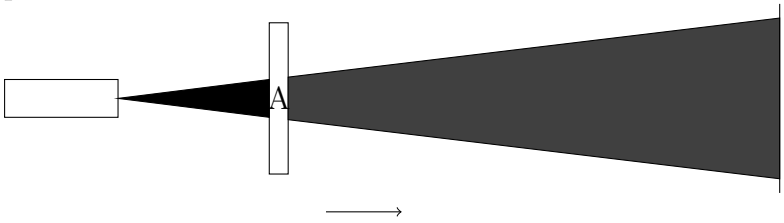
I fotoni sono le uniche particelle che si possono osservare direttamente. L'esperimento seguente necessita di una strumentazione ridotta: una fonte di luce potente, come un puntatore laser, e tre filtri polarizzatori, che possono essere comprati in qualsiasi negozio di strumentazione fotografica. Questo esperimento mostra alcuni dei principi della meccanica quantistica attraverso i fotoni e la loro polarizzazione.

1.1.1 L'esperimento.

Un raggio di luce viene sparato contro uno schermo o un muro. I filtri A, B e C sono polarizzati orizzontalmente, a 45° e verticalmente, rispettivamente, e verranno piazzati

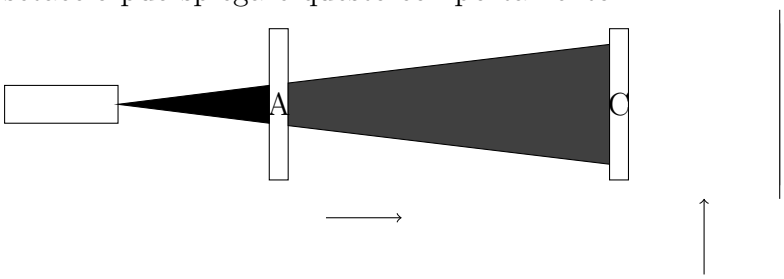
tra la fonte di luce e lo schermo.

Posizioniamo il filtro A. Se ipotizziamo che la luce sia polarizzata in maniera casuale, l'intensità della luce che raggiunge lo schermo sarà metà dell'intensità della luce che esce dalla nostra fonte. I fotoni che hanno attraversato il filtro sono ora tutti orizzontalmente polarizzati.

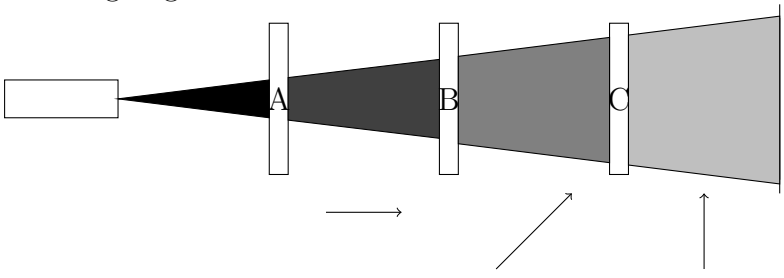


La funzione del filtro A non può essere spiegata come un "setaccio" che fa passare solo i fotoni che incidentalmente avevano già una polarizzazione orizzontale. Se fosse così, soltanto alcuni dei fotoni polarizzati avrebbero avuto polarizzazione orizzontale, e ci aspetteremmo un'attenuazione molto maggiore della luce passando attraverso il filtro.

Successivamente, inseriamo il filtro C: notiamo come l'intensità della luce che colpisce lo schermo diventa nulla. Nessuno dei fotoni polarizzati orizzontalmente riesce a passare attraverso il filtro verticale. In questo caso, diversamente che in precedenza, l'idea di un setaccio può spiegare questo comportamento.



Per ultimo, posizioniamo il filtro B tra A e C, e vediamo che un piccolo ammontare di luce giunge allo schermo: esattamente un ottavo della luce che fuoriesce dalla fonte.



Questo è un effetto controintuitivo. L'esperienza ci suggerirebbe che aggiungere un filtro può solo diminuire il numero di fotoni che arrivano allo schermo. Come può aumentarli?

1.1.2 La spiegazione.

Lo stato di polarizzazione di un fotone può essere rappresentato con un vettore di norma unitaria orientato nella direzione appropriata. Qualsiasi polarizzazione può essere espressa da una combinazione lineare $a|\uparrow\rangle + b|\rightarrow\rangle$ dei due vettori della base[1] $|\rightarrow\rangle$ (polarizzazione orizzontale) e $|\uparrow\rangle$ (polarizzazione verticale).

Dal momento che siamo solo interessati alla direzione della polarizzazione (la nozione di "modulo" non ha significato qui), il vettore di stato avrà norma unitaria, ossia $|a|^2 + |b|^2 = 1$. In generale, la polarizzazione di un fotone può essere espressa come $a|\uparrow\rangle + b|\rightarrow\rangle$ dove a e b sono numeri complessi[2] tali che $|a|^2 + |b|^2 = 1$. Si noti che la scelta della base per questa rappresentazione è completamente arbitraria: qualsiasi coppia di vettori ortonormali va bene (ad esempio $\{|\nwarrow\rangle, |\nearrow\rangle\}$).

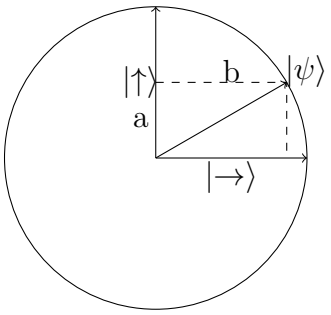


Figura 1.1: La misurazione è una proiezione sulla base

I postulati della meccanica quantistica ci dicono che qualsiasi dispositivo che misura un sistema 2-dimensionale ha una base ortonormale associata in relazione alla quale la misura quantistica viene effettuata. La misurazione di uno stato lo trasforma in uno dei vettori della base associata al dispositivo che effettua la misura. La probabilità che lo stato venga misurato come il vettore della base $|u\rangle$ è il quadrato della norma dell'ampiezza probabilistica dei componenti dello stato originale nella direzione del vettore della base $|u\rangle$, dove l'ampiezza probabilistica è un numero complesso. Per esempio, dato uno strumento per misurare la polarizzazione dei fotoni con base associata $\{|\uparrow\rangle, |\rightarrow\rangle\}$, lo stato $\psi = a|\uparrow\rangle + b|\rightarrow\rangle$ è misurato come $|\uparrow\rangle$ con probabilità $|a|^2$ e come $|\rightarrow\rangle$ con probabilità $|b|^2$ (si veda la figura 1.1). Si noti che a diversi strumenti di misura corrispondono diverse basi associate, e misure che utilizzano strumenti diversi avranno risultati diversi. Dal momento che le misurazioni vengono sempre fatte rispetto a una base ortonormale, per il resto del testo tutte le basi saranno ritenute ortonormali.

Inoltre, la misurazione dello stato quantico cambierà lo stato del sistema misurato al risultato della misura. Ovvero, se la misurazione di $a|\uparrow\rangle + b|\rightarrow\rangle$ restituisce $|\uparrow\rangle$, allora lo

[1] Rimandiamo a dopo la definizione rigorosa della notazione $|\rightarrow\rangle$.

[2] Coefficienti immaginari corrispondono a una polarizzazione circolare.

stato ψ diventa $|\uparrow\rangle$ e una seconda misurazione rispetto alla stassa base restituirà $|\uparrow\rangle$ con probabilità 1. Quindi, a meno che lo stato originale fosse incidentalmente uno dei vettori della base, una misurazione cambierà quello stato, e renderà impossibile determinare quale fosse lo stato originale.

La meccanica quantistica può spiegare l'esperimento della polarizzazione come segue. Un filtro polarizzante misura lo stato quantico dei fotoni rispetto alla base che consiste nel vettore corrispondente alla sua polarizzazione insieme a quello perpendicolare ad esso. I fotoni che, dopo essere stati misurati dal filtro, combaciano con la polarizzazione del filtro vengono fatti passare. Gli altri sono riflessi e ora hanno una polarizzazione perpendicolare a quella del filtro. Per esempio, il filtro A misura la polarizzazione dei fotoni rispetto al vettore base $|\rightarrow\rangle$, che corrisponde alla sua polarizzazione. I fotoni che passano attraverso il filtro A hanno tutti polarizzazione $|\rightarrow\rangle$. Quelli che sono riflessi dal filtro hanno tutti polarizzazione $|\uparrow\rangle$.

Ipotizzando che la fonte di luce produca fotoni con polarizzazioni uniformemente casuali, il filtro A misurerà il 50% di tutti i fotoni come polarizzati orizzontalmente. Questi fotoni passeranno attraverso il filtro e il loro stato sarà $|\rightarrow\rangle$. Il filtro C misurerà questi fotoni rispetto a $|\uparrow\rangle$. Ma lo stato $|\rightarrow\rangle = 0|\uparrow\rangle + 1|\rightarrow\rangle$ sarà proiettato su $|\uparrow\rangle$ con probabilità 0 e nessun fotone passerà il filtro C.

Infine, il filtro B misura lo stato quantico rispetto alla base

$$\{\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle), \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)\}$$

che scriviamo come $\{|\nearrow\rangle, |\nwarrow\rangle\}$. Si noti che $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\nwarrow\rangle)$ e $|\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\nwarrow\rangle$). Quei fotoni che sono misurati come $|\nearrow\rangle$ passano attraverso il filtro. I fotoni che passano attraverso A con stato $|\rightarrow\rangle$ saranno misurati da B come $|\nearrow\rangle$ con probabilità 1/2 e quindi il 50% dei fotoni che passano attraverso A passeranno attraverso B e saranno nello stato $|\nearrow\rangle$. Come prima, questi fotoni saranno misurati dal filtro C come $|\uparrow\rangle$ con probabilità 1/2. Quindi solo un ottavo dei fotoni usciti dalla fonte di luce riusciranno a passare attraverso la sequenza di filtri A, B e C.

1.2 Spazio degli stati e notazione Bra/Ket

Lo spazio degli stati di un sistema quantistico, che consiste nelle posizioni, quantità di moto, polarizzazioni, spin, ecc. delle varie particelle, è modellizzato da uno spazio di Hilbert di funzioni onda. Non si andrà nel dettaglio di queste funzioni onda. Per la computazione quantistica bisogna avere a che fare solo con sistemi quantistici finiti ed è sufficiente considerare spazi vettoriali complessi finito-dimensionali con un prodotto interno che sono generati da funzioni onda astratte come $|\rightarrow\rangle$.

Gli spazi degli stati quantici e le trasformazioni che agiscono su di essi possono essere descritti in termini di vettori e matrici o nella più compatta notazione bra/ket inven-

tata da Dirac. I ket come $|x\rangle$ denotano vettori colonna e sono solitamente usati per descrivere stati quantici. Il corrispondente bra, $\langle x|$, denota il trasposto coniugato di $|x\rangle$. Per esempio, la base ortonormale $\{|0\rangle, |1\rangle\}$ può essere espressa come $\{(1,0)^T, (0,1)^T\}$. Qualsiasi combinazione lineare complessa di $|0\rangle$ e $|1\rangle$, $a|0\rangle + b|1\rangle$, può essere scritta come $(a,b)^T$. Si noti che la scelta dell'ordine dei vettori della base è arbitraria. Per esempio, rappresentare $|0\rangle$ come $(0,1)^T$ e $|1\rangle$ come $(1,0)^T$ può andar bene, a patto che sia fatto coerentemente.

Combinare $\langle x|$ e $|y\rangle$ nella forma $\langle x||y\rangle$, anche scritto come $\langle x|y\rangle$, denota il prodotto interno fra i due vettori. Per esempio, essendo $|0\rangle$ un vettore unitario abbiamo $\langle 0|0\rangle = 1$ e dal momento che $|0\rangle$ e $|1\rangle$ sono ortogonali abbiamo $\langle 0|1\rangle = 0$.

La notazione $|x\rangle\langle y|$ è il prodotto esterno di $|x\rangle$ e $\langle y|$. Per esempio, $|0\rangle\langle 1|$ è la trasformazione che manda $|1\rangle$ in $|0\rangle$ e $|0\rangle$ in $(0,0)^T$ poiché

$$|0\rangle\langle 1||1\rangle = |0\rangle\langle 0|1\rangle = |0\rangle$$

$$|0\rangle\langle 1||0\rangle = |0\rangle\langle 1|0\rangle = 0|0\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Equivalentemente, $|0\rangle\langle 1|$ può essere scritto in forma matriciale dove $|0\rangle = (1,0)^T$, $\langle 0| = (1,0), |1\rangle = (0,1)^T$, e $\langle 1| = (0,1)$. Allora

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}(0,1) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Questa notazione ci fornisce un modo conveniente di specificare trasformazioni di stati quantici in termini di cosa accade ai vettori della base (questo argomento sarà approfondito in seguito). Per esempio, la trasformazione che scambia $|0\rangle$ e $|1\rangle$ è fornita dalla matrice

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|.$$

In questo elaborato si preferirà la notazione lievemente più intuitiva

$$\begin{aligned} X : |0\rangle &\to |1\rangle \\ |1\rangle &\to |0\rangle \end{aligned}$$

che specifica esplicitamente il risultato di una trasformazione dei vettori della base.

1.3 Bit quantistici

Un bit quantistico, o qubit, è un vettore di norma unitaria in uno spazio vettoriale complesso due-dimensionale per cui una base particolare, denotata da $\{|0\rangle, |1\rangle\}$, è stata

fissata. La base ortonormale $|0\rangle$ e $|1\rangle$ può corrispondere rispettivamente alle polarizzazioni $|\uparrow\rangle$ e $|\rightarrow\rangle$ di un fotone, o alle polarizzazioni $|\nearrow\rangle$ e $|\nwarrow\rangle$. Oppure $|0\rangle$ e $|1\rangle$ potrebbero corrispondere agli stati di spin-up e spin-down di un elettrone. Quando si parla di qubit, e computazione quantistica in generale, una base fissata rispetto alla quale tutte le affermazioni vengono fatte è stata scelta in precedenza. In particolare, tranne se specificato diversamente, tutte le misurazioni saranno fatte rispetto alla base standard per l'informatica quantistica, $\{|0\rangle, |1\rangle\}$.

Per lo scopo della computazione quantistica, gli stati base $|0\rangle$ e $|1\rangle$ si intende che rappresentino i valori dei bit classici 0 e 1 rispettivamente. A differenza dei bit classici, tuttavia, i qubit possono essere in una sovrapposizione di $|0\rangle$ e $|1\rangle$ come $a|0\rangle + b|1\rangle$ dove a e b sono numeri complessi tali che $|a|^2 + |b|^2 = 1$. Come nel caso della polarizzazione dei fotoni, se una tale sovrapposizione è misurata rispetto alla base $\{|0\rangle, |1\rangle\}$, la probabilità che il valore misurato sia $|0\rangle$ è $|a|^2$ e la probabilità che il valore misurato sia $|1\rangle$ è $|b|^2$.

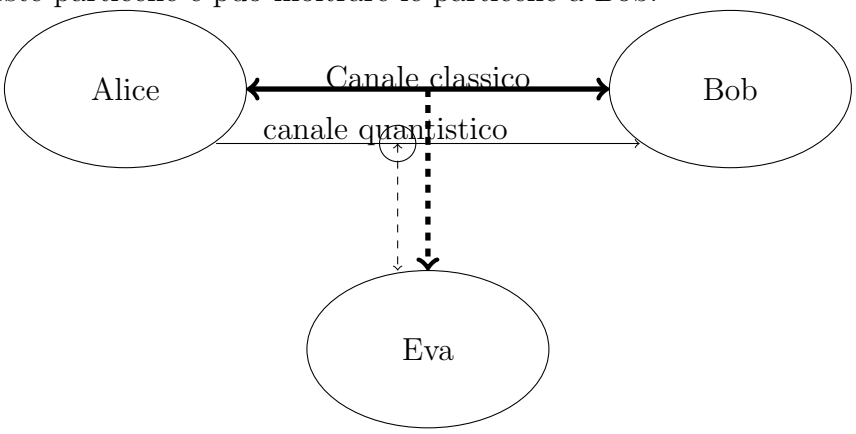
Malgrado un bit quantistico possa essere messo in infiniti stati di sovrapposizione diversi, è possibile estrarre solo una quantità pari ad un singolo bit classico di informazione da un singolo bit quantistico. La ragione per cui nessun altra informazione può essere ottenuta da un qubit che in un bit classico è che l'informazione può essere ottenuta solo da una misurazione. Quando un qubit è misurato, la misura cambia lo stato ad uno degli stati base nella maniera vista nell'esperimento della polarizzazione dei fotoni. Visto che ogni misura può restituire solo uno di due stati, ossia uno dei vettori della base associati allo strumento di misura, allora ci sono solo due possibili risultati, proprio nel caso classico. Essendo che la misurazione cambia lo stato, non si può misurare lo stato di un qubit in due basi differenti. Inoltre, come vedremo più avanti, gli stati quantici non possono essere clonati e quindi non è possibile misurare un qubit in due maniere, nemmeno indirettamente, ad esempio, clonando il qubit e misurando la copia in una base diversa dall'originale.

1.3.1 Distribuzione quantistica della chiave

Sequenze di singoli qubit possono essere usate per trasmettere chiavi private su canali insicuri. Nel 1984 Bennett e Brassard descrissero il primo schema di distribuzione quantistica della chiave: nel 2004, venne istituito Qnet. Classicamente, tecniche di crittografia a chiave pubblica, ad esempio RSA, sono usati per distribuire le chiavi: questo metodo, detto QKD, può essere usato sia per aumentare la sicurezza di sistemi già esistenti, sia per prevenire eventuali attacchi che sfruttano proprio le potenzialità del computer quantistico, perché si basa su un principio fisico.

Si consideri la situazione in cui Alice e Bob vogliano avere una chiave segreta in comune così da comunicare privatamente. Sono connessi da un ordinario canale bidirezionale aperto e un canale quantistico unidirezionale, entrambi osservabili da Eva, che vuole intercettare la loro conversazione. Questa situazione è illustrata nella figura in basso. Il canale quantistico permette ad Alice di inviare particelle individuali (ad esempio fotoni)

a Bob che può misurare il loro stato quantico. Eva può provare a misurare lo stato di queste particelle e può inoltrare le particelle a Bob.



Per cominciare il processo, Alice invia una sequenza di bit a Bob codificando ogni bit nello stato quantico di un fotone come segue. Per ogni bit, Alice sceglie casualmente una delle seguenti due basi:

$$0 \rightarrow |\uparrow\rangle$$
$$1 \rightarrow |\rightarrow\rangle$$

oppure:

$$0 \rightarrow |\nwarrow\rangle$$
$$1 \rightarrow |\nearrow\rangle$$

Bob misura lo stato dei fotoni che riceve scegliendo casualmente ciascuna base. Dopo che i bit sono stati trasmessi, Bob e Alice comunicano la base che hanno usato per codificare e decodificare ogni bit attraverso il canale aperto. Con questa informazione entrambi possono determinare quali bit sono stati trasmessi correttamente, identificando quei bit per cui la base di invio e di ricezione corrispondono. Useranno questi bit come chiave e scarteranno tutti gli altri. In media, Alice e Bob avranno una corrispondenza del 50% su tutti i bit trasmessi.

Si supponga che Eva intercetti la comunicazione, misuri lo stato dei fotoni trasmessi da Alice, e rimandi nuovi fotoni aventi lo stesso stato che ha misurato. In questo processo, lei userà la base sbagliata circa il 50% delle volte, e ognuna di quelle volte inoltrerà a Bob il bit con la base sbagliata. Quindi quando Bob misurerà uno dei qubit mandati da Eva con la base "corretta" (ossia la stessa che ha usato Alice) ci sarà una probabilità del 25% che egli misuri il valore sbagliato. Quindi un attacco sul canale quantistico introdurrà una quantità di errori che Alice e Bob possono individuare comunicando una quantità

sufficiente di bit di parità della loro chiave sul canale aperto. Quindi, non solo è probabile che la versione di Eva della chiave sia sbagliata del 25%, ma il fatto che qualcuno abbia effettuato un attacco sarà palese ad Alice e Bob.

1.3.2 Qubit multipli

Si immagini un oggetto fisico macroscopico spaccarsi, e molteplici pezzi volare via in diverse direzioni. Lo stato di questo sistema può essere descritto completamente descrivendo lo stato di ognuno dei suoi componenti separatamente. Un aspetto sorprendente e poco intuitivo dello spazio degli stati di un sistema quantistico composto da n particelle è che lo stato del sistema non sempre può essere descritto in termini dello stato dei suoi componenti. È esaminando sistemi di più di un qubit che si riesce a intravedere da dove può arrivare il potere computazionale di un computer quantistico.

Come si è visto, lo stato di un qubit può essere rappresentato da un vettore nello spazio vettoriale complesso due dimensionale generato da $|0\rangle$ e $|1\rangle$. Nella fisica classica, se si hanno n particelle, ognuna delle quali può essere descritta da un vettore in uno spazio vettoriale due-dimensionale, gli stati possibili del sistema saranno rappresentati da un vettore in uno spazio di dimensione $2n$. Tuttavia, in un sistema quantico lo spazio degli stati risultante è molto più grande; un sistema di n qubit ha uno spazio degli stati a 2^n dimensioni. È questa crescita esponenziale dello spazio degli stati rispetto al numero di particelle che suggerisce una possibile velocizzazione esponenziale dei calcoli in un computer quantistico rispetto un computer classico.

Spazi degli stati individuali di n particelle si combinano classicamente attraverso il prodotto cartesiano. Gli stati quantici, tuttavia, si combinano tramite il prodotto tensoriale. Vediamo brevemente alle distinzioni tra il prodotto cartesiano e quello tensoriale che saranno cruciali per capire la computazione quantistica.

Siano V e W due spazi vettoriali complessi 2-dimensionali con basi $\{v_1, v_2\}$ e $\{w_1, w_2\}$ rispettivamente. Il prodotto cartesiano di questi due spazi può prendere come base l'unione delle basi dei suoi spazi componenti $\{v_1, v_2, w_1, w_2\}$. Si noti che l'ordine delle basi è stato scelto arbitrariamente. In particolare, la dimensione dello spazio degli stati di molteplici particelle classiche cresce linearmente con il numero delle particelle, perché $\dim(X \times Y) = \dim(X) + \dim(Y)$. Il prodotto tensoriale di V e W ha base $\{v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_1 \otimes w_2\}$. Si noti che l'ordine dei vettori della base è, di nuovo, arbitrario. Quindi lo spazio degli stati per due qubit, ognuno con base $\{|0\rangle, |1\rangle\}$, ha base $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$ che può essere scritto in maniera più compatta come $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Più generalmente, scriviamo $|x\rangle$ per esprimere $|b_n b_{n-1} \dots b_0\rangle$ dove b_i sono le cifre binarie del numero x.

Una base per un sistema a tre qubit è

$$\{|000\rangle, |000\rangle, |000\rangle, |000\rangle, |000\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

e in generale un sistema di n qubit ha 2^n vettori che formano la base. Possiamo ora vedere la crescita esponenziale dello spazio degli stati con il numero delle particelle quantistiche. Il prodotto tensoriale $X \otimes Y$ ha dimensione $\dim(X) \times \dim(Y)$.

Lo stato $|00\rangle + |11\rangle$ è un esempio di uno stato quantico che non può essere descritto in funzione degli stati di ognuna delle sue componenti (qubits) separatamente. In altre parole, non si possono trovare a_1, a_2, b_1, b_2 tali che $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = |00\rangle + |11\rangle$ perché

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

e $a_1b_2 = 0$ implica che o $a_1a_2 = 0$ o $b_1b_2 = 0$. Gli stati che non possono essere scomposti in questa maniera sono chiamati stati di correlazione quantistica o *entanglement*. Questi stati rappresentano situazioni che non hanno una controparte classica, e dei quali non abbiamo intuizione. Questi sono anche gli stati che forniscono la crescita esponenziale degli spazi di stato quantici con il numero di particelle.

Si noti che servirebbero grandi risorse per simulare anche un sistema quantico piccolo in computer tradizionali. L'evoluzione dei sistemi quantici è esponenzialmente più veloce delle loro simulazioni classiche. Il potere dei computer quantistici sta nella possibilità di sfruttare l'evoluzione di uno stato quantico come meccanismo di calcolo.

1.3.3 Misurazione

L'esperimento nella sezione 1.1.1 spiega come la misurazione di un singolo qubit proietti lo stato quantico su uno degli stati della base associati con il dispositivo di misurazione. Il risultato di una misura è probabilistico e il processo di misurazione cambia lo stato a quello misurato.

Si guardi ad un esempio di misurazione in un sistema di due qubit. Qualsiasi stato di due qubit può essere espresso come $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, dove a, b, c, e d sono numeri complessi tali che $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. Si supponga che vogliamo misurare il primo qubit rispetto alla base standard $\{|0\rangle, |1\rangle\}$. Per facilitare i calcoli si riscriverà lo stato come segue:

$$\begin{aligned} a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle =& |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle) \\ =& u|0\rangle \otimes (a/u|0\rangle + b/u|1\rangle) + \\ & v|1\rangle \otimes (c/v|0\rangle + d/v|1\rangle). \end{aligned}$$

Per $u = \sqrt{|a|^2 + |b|^2}$ e $v = \sqrt{|c|^2 + |d|^2}$ i vettori $a/u|0\rangle + b/u|1\rangle$ e $c/v|0\rangle + d/v|1\rangle$ sono di lunghezza unitaria. Una volta che lo stato è stato riscritto come sopra, come prodotto tensoriale del bit misurato e un secondo vettore di lunghezza unitaria, il risultato probabilistico di una misura è facile da leggere. Una misurazione del primo bit ritornerà

$|0\rangle$ con probabilità $u^2 = |a|^2+|b|^2$ proiettando lo stato a $|0\rangle\otimes(a/u|0\rangle+b/u|1\rangle)$ o restituirà $|1\rangle$ con probabilità $v = |c|^2 + |d|^2$ proiettando lo stato a $|1\rangle \otimes (c/v|0\rangle + d/v|1\rangle)$. Poiché $|0\rangle \otimes (a/u|0\rangle + b/u|1\rangle)$ e $|1\rangle \otimes (c/v|0\rangle + d/v|1\rangle)$ sono entrambi vettori unitari, nessun ridimensionamento è necessario. Per misurare il secondo bit si agisce in maniera simile.

Per gli scopi della computazione quantistica, una misurazione multi-bit può essere trattata come una serie di misurazioni a bit singolo nella base standard. Altri tipi di misurazioni sono possibili, come misurare se due qubit hanno lo stesso valore senza dedurre l'effettivo valore dei due qubit. Ma siffatte misurazioni sono equivalenti a trasformazioni unitarie seguite da una misura standard dei qubit individuali, ed è quindi sufficiente considerare solo misurazioni standard.

Nell'esempio a due qubit, lo spazio degli stati è un prodotto cartesiano del sottospazio che consiste in tutti gli stati tali che il primo qubit sia nello stato $|0\rangle$ e il sottospazio ad esso ortogonale, quello degli stati tali che il primo qubit sia nello stato $|1\rangle$. Qualsiasi stato quantico può essere scritto come somma di due vettori, uno in ognuno dei sottospazi. Una misurazione di k qubit nella base standard ha 2^k possibili risultati m_i. Qualsiasi dispositivo che misura k qubit di un sistema n-qubit spezza lo spazio degli stati 2^n dimensionale $\mathcal{H}$ in un prodotto cartesiano di sottospazi ortogonali $S_1, \ldots, S_{2^k}$ con $\mathcal{H} = S_1 \times \ldots \times S_{2^k}$, tali che il valore dei k qubit che vengono misurati sia m_i e lo stato dopo la misurazione è nello spazio S_i per qualche i. Il dispositivo sceglie casualmente uno dei S_i con probabilità il quadrato dell'ampiezza dei componenti di ψ in S_i, e proietta lo stato in quella componente, ridimensionando per ottenere lunghezza 1. Equivalentemente, la probabilità che il risultato della misurazione sia un dato valore è la somma dei quadrati dei valori assoluti delle ampiezze di tutti i vettori della base compatibili con quel valore della misurazione.

La misurazione ci fornisce ancora un altro modo di immaginare le particelle in *entanglement*. Delle particelle non sono in correlazione se la misura di una non ha effetto sull'altra. Per esempio, lo stato $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ è in *entanglement* perché la probabilità che il primo bit sia misurato come $|0\rangle$ è $1/2$ se il secondo bit non è stato misurato mentre, se il secondo bit è stato misurato, la probabilità che il primo bit sia misurato come $|0\rangle$ è o 1 o 0, dipendentemente dal fatto che il secondo bit sia stato misurato come $|0\rangle$ o $|1\rangle$ rispettivamente. Quindi il risultato aleatorio di misurare il primo bit è cambiato da una misurazione del secondo bit. D'altra parte, lo stato $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ non è in correlazione: poiché $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, qualsiasi misurazione effettuata sul primo bit restituirà $|0\rangle$ a prescindere che il secondo bit sia stato misurato o meno. Similmente, il secondo bit ha una probabilità del 50% di essere misurato come $|0\rangle$ a prescindere che il primo bit sia stato misurato oppure no. Si noti che l'*entanglement*, nel senso che la misurazione di una particella ha un effetto su misurazioni di un'altra particella, è equivalente alla nostra definizione precedente di stati correlati come stati che non possono essere scritti come prodotti tensoriali di stati individuali.

1.4 Trasformazioni e gate quantistici

Finora si sono considerati sistemi quantistici statici che cambiano solo quando misurati. Le dinamiche di un sistema quantistico, quando non sta venendo misurato, sono governate dall'equazione di Schrödinger; le dinamiche devono portare stati in stati, in una maniera che preservi l'ortogonalità. Per uno spazio vettoriale complesso, le trasformazioni lineari che conservano l'ortogonalità sono trasformazioni unitarie, definite come segue. Qualsiasi trasformazione lineare di uno spazio vettoriale complesso può essere descritto da una matrice. Sia M^* la coniugata trasposta della matrice M. Una matrice M è unitaria (descrive una trasformazione unitaria) se $MM^* = I$. Qualsiasi trasformazione unitaria di uno spazio degli stati quantistico è una trasformazione quantistica legittima, e viceversa. Si può pensare alle trasformazioni unitarie come rotazioni di uno spazio vettoriale complesso.

Una conseguenza importante del fatto che le trasformazioni quantistiche sono unitarie è che sono reversibili: i gate quantistici, di conseguenza, devono essere reversibili. Fortunatamente, come nel caso classico, ci sono gate che, messi insieme, formano un insieme funzionalmente completo e che quindi possono essere usati per costruire ogni altro.

1.4.1 Esempi di gate quantistici

Seguono alcuni esempi di trasformazioni di stato quantico a bit singolo. Grazie alla linearità, le trasformazioni sono completamente descritte dal loro effetto sui vettori della base. La matrice associata è scritta, prendendo $\{|0\rangle, |1\rangle\}$ come base ordinata, in questo modo:

$$\begin{aligned} I :&|0\rangle \to |0\rangle \\ &|1\rangle \to |1\rangle \end{aligned} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{aligned} X :&|0\rangle \to |1\rangle \\ &|1\rangle \to |0\rangle \end{aligned} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{aligned} Y :&|0\rangle \to -|1\rangle \\ &|1\rangle \to |0\rangle \end{aligned} \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\begin{aligned} Z :&|0\rangle \to |0\rangle \\ &|1\rangle \to -|1\rangle \end{aligned} \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

I nomi di queste trasformazioni sono convenzionali. I è la trasformazione identità, X è la negazione, Z è l'operazione di phase shift, e $Y = ZX$ è una combinazione di entrambe. La X era in realtà già stata introdotta nella sezione 1.2. Può essere facilmente mostrato che questi gate sono unitari. Per esempio

$$YY^* = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = I.$$

Il gate NOT-controllato, C_{not}, opera su due qubit come segue: cambia il secondo bit se il primo bit è 1 e lo lascia immutato altrimenti. I vettori $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$ formano una base ortonormale per lo spazio degli stati di un sistema a due qubit, uno spazio vettoriale complesso 4-dimensionale. Per rappresentare trasformazioni di questo spazio in notazione matriciale abbiamo bisogno di scegliere un isomorfismo tra questo spazio e lo spazio delle quadruple ordinate complesse. Non ci sono ragioni, oltre la convenzione, per scegliere un isomorfismo invece di un altro. Quesllo che usiamo associa $|00\rangle$, $|01\rangle$, $|10\rangle$ e $|11\rangle$ alla base standard per le 4-uple $(1,0,0,0)^T$, $(0,1,0,0)^T$, $(0,0,1,0)^T$ e $(0,0,0,1)^T$, in quell'ordine. La trasformazione C_{not} si rappresenta:

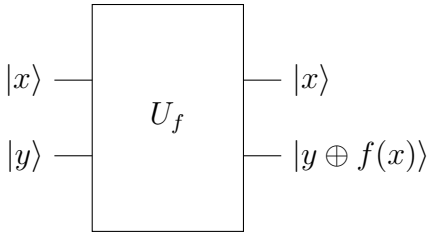
$$\begin{array}{r} C_{not} : |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{array} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

La trasformazione C_{not} è unitaria perché $C_{not}^* = C_{not}$ e $C_{not}C_{not} = I$. Il gate C_{not} non può essere scomposto in un prodotto tensoriale di due trasformazioni a bit singolo.

1.4.2 Gate universali

Malgrado il NOT classico sia reversibile, AND, OR e NAND non lo sono. Quindi non è immediato che le trasformazioni quantistiche possano effettuare tutta la computazione classica.

Sapendo che una funzione classica arbitraria f ha m bit di input e k bit di output, supponiamo l'esistenza di un gate array quantistico U_f che implementa f. U_f è una trasformazione a $m+k$ bit della forma $U_f : |x,y\rangle \to |x, y \oplus f(x)\rangle$ dove $\oplus$ denota l'OR-esclusivo bit per bit[3]. I gate array quantici U_f, definiti in questa maniera, sono unitari per ogni funzione f. Per calcolare $f(x)$ si applica U_f a $|x\rangle$ moltiplicato tensorialmente con k zero, $|x,0\rangle$. Poiché $f(x) \oplus f(x) = 0$ si ha $U_f U_f = I$. Graficamente la trasformazione $U_f : |x,y\rangle \to |x, y \oplus f(x)\rangle$ è rappresentata come



[3] $\oplus$ non rappresenta la somma diretta tra spazi vettoriali.

Si può mostrare che C_{not} insieme a tutti i gate quantistici a 1-bit forma un insieme di gate universali. È sufficiente includere le seguenti trasformazioni a un bit

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix}$$

per ogni $0 \leq \alpha \leq 2\pi$ insieme al C_{not} per ottenere un insieme universale di gate. Questo tipo di trasformazioni non classiche sono necessarie per sfruttare il potere dei computer quantistici.

1.5 Parallelismo quantistico

Cosa accade se si applica U_f a un input che è in una sovrapposizione? La risposta è semplice ma potente: poiché U_f è una trasformazione lineare, viene applicata a tutti i vettori della base nella sovrapposizione simultaneamente e genererà una sovrapposizione dei risultati. In questa maniera , è possibile calcolare $f(x)$ per n valori di x in una singola applicazione di U_f. Questo effetto è chiamato parallelismo quantistico.

Il potere degli algoritmi quantistici viene dallo sfruttamento del parallelismo quantistico e dell'*entanglement*. Quindi molti algoritmi quantistici cominciano calcolando una funzione di interesse in una sovrapposizione di tutti i valori nella maniera seguente. Si cominci con uno stato a n bit $|00\ldots0\rangle$.

Definiamo ora la trasformazione a bit singolo detta di Hadamard:

$$\begin{aligned} H :|0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

La trasformazione H ha molte importanti applicazioni. Quando applicata a $|0\rangle$, H crea uno stato di sovrapposizione $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Applicata a n bit individualmente, H genera una sovrapposizione di tutti i 2^n possibili stati, che possono essere visti come la rappresentazione binaria dei numeri da 0 a $2^n - 1$.

$$\begin{aligned} &(H \otimes H \otimes \ldots \otimes H)|00\ldots0\rangle \\ =&\frac{1}{\sqrt{2^n}}((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle)) \\ =&\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \end{aligned}$$

La trasformazione che applica H a n bit è detta trasformazione di Walsh, o di Walsh-Hadamard, e si indica con la lettera W. Può essere definita come una scomposizione ricorsiva della forma

$$W_1 = H, \quad W_{n+1} = H \otimes W_n.$$

Possiamo perciò applicare W a $|00\ldots0\rangle$ per ottenere una sovrapposizione:

$$\frac{1}{\sqrt{2^n}}(|00\ldots0\rangle + |00\ldots1\rangle + \cdots + |11\ldots1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

che dovrebbe essere vista come una sovrapposizione di tutti gli interi $0 \leq x < 2^n$. Si aggiunga un registro $|0\rangle$ di k bit, allora per linearità:

$$\begin{aligned} U_f(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x,0\rangle) &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f(|x,0\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x,f(x)\rangle \end{aligned}$$

dove $f(x)$ è la funzione interessata. Si noti che poiché n qubits permettono di lavorare simultaneamente con 2^n stati, il parallelismo quantistico elude lo scambio spazio/tempo del parallelismo classico attraverso la sua abilità di fornire una quantità esponenziale di spazio computazionale in un ammontare lineare di spazio fisico.

Calcolare le funzioni su una sovrapposizione in questo modo, però, non dà vantaggi rispetto al parallelismo classico, perché soltanto un risultato viene ottenuto, e peggio ancora non si può nemmeno scegliere quale risultato ottenere. Il cuore di qualsiasi algoritmo quantistico è nella maniera con la quale manipola il parallelismo per fare in modo che i risultati desiderati saranno poi misurati con alta probabilità. Questo tipo di manipolazione non ha un analogo classico, e richiede tecniche di programmazione non-tradizionali. Alcuni metodi attualmente conosciuti sono:

- Amplificare valori interessanti. L'idea generale è di trasformare lo stato in maniera che i valori di interesse abbiano una grande ampiezza e perciò abbiano una maggiore probabilità di venir misurati.

- Trovare proprietà comuni di tutti i valori di $f(x)$. Quest'idea è sfruttata nell'algoritmo di Shor, che usa una trasformata di Fourier quantistica per ottenere il periodo di f.

Capitolo 2

L'algoritmo di Shor

L'idea di sfruttare le qualità della meccanica quantistica per scopi informatici era già nella mente degli scienziati negli anni '80: ci si aspettava che, rimpicciolendo sempre di più la componentistica, si sarebbe arrivati a conservare un bit nello stato di un solo atomo, e che questo avrebbe costretto a prendere contromisure per bilanciare il comportamento quantistico che si ha oltre quella soglia. Si sapeva, ovviamente, che certe possibilità che offre la meccanica quantistica non sono simulabili in ambiente classico, ma non esistendo né computer quantistici, né algoritmi che riuscivano a incanalarne le qualità, la branca di studi rimase per molto tempo relegata a qualcosa di puramente accademico.

Tutto cambiò nel 1994, quando Peter Shor, uno scienziato che lavorava ai *Bell Labs* mostrò al mondo il suo algoritmo capace di fattorizzare numeri velocemente utilizzando le regole della meccanica quantistica. Nell'introduzione si è cercato di mostrare perché questo potesse essere utile; nel precedente capitolo sono state fornite molte nozioni per comprendere il possibile funzionamento di un tale procedimento: in questo, si tenterà di spiegare il meglio possibile come funziona, effettivamente, tale algoritmo.

Come molti metodi che risolvono il problema della fattorizzazione, l'approccio di Shor riduce il tutto al calcolo del periodo di una funzione. Shor usa il parallelismo quantistico nella maniera standard, per ottenere una sovrapposizione di tutti i valori di una funzione in un passaggio solo. Calcola poi la trasformata di Fourier quantistica della funzione, che come la trasformata di Fourier classica, manda tutti i valori della funzione in multipli della sua frequenza (e quindi del reciproco del periodo). Con alta probabilità, misurare lo stato restituisce il periodo, che è a sua volta usato per fattorizzare l'intero M.

La descrizione appena data cattura l'essenza dell'algoritmo quantistico, ma è ovviamente una grande semplificazione. La parte più complicata è che la trasformata di Fourier quantistica è basata sulla trasformata di Fourier veloce e quindi fornisce solo risultati approssimati in molti casi. Quindi estrarre il periodo è più difficile che quanto descritto sopra, ma le tecniche usate sono classiche.

Si darà prima una descrizione della trasformata di Fourier quantistica e poi si descriverà dettagliatamente l'algoritmo di Shor.

2.1 La trasformata di Fourier quantistica

Le trasformate di Fourier in generale sono mappe che scrivono funzioni dipendenti dal tempo nel dominio delle frequenze. Quindi le trasformate di Fourier mandano funzioni di periodo r in funzioni che hanno valori diversi da zero solo in multipli della frequenza $\frac{2\pi}{r}$. La trasformata di Fourier discreta (DFT)[1] opera su N campioni equamente spaziati nell'intervallo $[0, 2\pi[$ per qualche N e restituisce una funzione che ha come dominio gli interi tra 0 e $N-1$. La trasformata di Fourier discreta di una funzione (campionata) di periodo r è una funzione concentrata vicino ai multipli di $\frac{N}{r}$. Se il periodo r divide N interamente, il risultato è una funzione che ha valori diversi da zero solo nei multipli di $\frac{N}{r}$. Altrimenti, il risultato approssimerà questo comportamento, e ci saranno termini diversi da zero negli interi vicini a multipli di $\frac{N}{r}$.

La trasformata di Fourier veloce (FFT)[2] è una versione della DFT dove N è una potenza di 2. La trasformata di Fourier quantistica (QFT)[3] è una variante della trasformata di Fourier discreta che, come FFT, usa potenze di 2. La trasformata di Fourier quantistica opera sull'ampiezza dello stato quantico, mandando

$$\sum_x g(x)|x\rangle \rightarrow \sum_c G(c)|c\rangle$$

dove $G(c)$ è la trasformata di Fourier discreta di $G(x)$, e sia x sia c possono assumere valori tra 0 e $N-1$ in rappresentazione binaria. Se lo stato venisse misurato dopo aver effettuato la trasformata di Fourier, la probabilità di avere come risultato $|c\rangle$ sarebbe $|G(c)|^2$. Si noti che la trasformata di Fourier quantistica non funziona come la trasformazione U_f; non appare alcun output in un registro extra.

Applicando la trasformata di Fourier quantistica a una funzione periodica $g(x)$ con periodo r, ci si aspetterebbe di ottenere $\sum_c G(c)|c\rangle$, dove $G(c)$ è zero eccetto che nei multipli di $\frac{N}{r}$. Quindi, quando lo stato è misurato, il risultato dovrebbe essere un multiplo di $\frac{N}{r}$, si dica $j\frac{N}{r}$. Ma come descritto sopra, la trasformata di Fourier quantistica fornisce solo risultati approssimati per periodi che non sono una potenza di due, ossia non dividono N. Tuttavia tanto più grande è la potenza di due usata come base per la trasformata, tanto migliore sarà l'approssimazione. La trasformata di Fourier quantistica U_{QFT} con base $N = 2^m$ è definita come

$$U_{QFT} : |x\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{\frac{2\pi i c x}{2^m}} |c\rangle.$$

Affinché l'algoritmo di Shor sia un algoritmo polinomiale, la trasformata di Fourier quantistica deve essere calcolabile efficientemente. Shor mostrò che la trasformata di

[1] Discrete Fourier transform.
[2] Fast Fourier transform.
[3] Quantum Fourier transform.

Fourier quantistica con base 2^m può essere costruita usando solo $\frac{m(m+1)}{2}$ gate. La costruzione fa uso di due tipi di gate. Uno è un gate che esegue la familiare trasformazione di Hadamard H. Si denoterà come H_j la trasformazione di Hadamard applicata al j-esimo bit. L'altro tipo di gate esegue trasformazioni a due bit della forma

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{k-j}} \end{pmatrix}$$

dove $\theta_{k-j} = \pi/2^{k-j}$. Questa trasformazione agisce sul k-esimo e j-esimo bit di un registro più grande. La trasformata di Fourier quantistica è data da

$$\prod_{n=0}^{m-1} (H_n \prod_{i=n+1}^{m-2} S_{n,i})$$

cioè

$$H_0 S_{0,1} \dots S_{0,m-1} H_1 \dots H_{m-3} S_{m-3,m-2} S_{m-3,m-1} H_{m-2} S_{m-2,m-1} H_{m-1}$$

seguita da una trasformazione di inversione di bit. Se FFT è seguita da una misurazione, come nell'algoritmo di Shor, l'inversione di bit può essere eseguita classicamente.

2.2 Una descrizione dettagliata dell'algoritmo di Shor

I passaggi dettagliati dell'algoritmo di Shor sono illustrati con un esempio dove viene fattorizzato $M = 21$.

Passo 1. Parallelismo quantistico. Si scelga un intero a arbitrario. Se a non è coprimo a M, si è trovato un fattore di M. Altrimenti si applichi il resto dell'algoritmo.

Sia m tale che[4] $M^2 \leq 2^m < 2M^2$. Si usi il parallelismo quantistico come descritto in 1.5 per calcolare $f(x) = a^x \mod M$ per tutti gli interi da 0 a $2^m - 1$. La funzione è quindi codificata nello stato quantico

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x, f(x)\rangle. \tag{1}$$

Esempio. Si supponga che $a = 11$ sia scelto casualmente. Sicché $M^2 = 441 \leq 2^9 < 882 = 2M^2$ troviamo $m = 9$. Dunque sono richiesti un totale di 14 bit, di cui 9 per x e 5 per $f(x)$, per calcolare la sovrapposizione dell'equazione 1.

[4]Questa scelta è stata fatta per far sì che l'approssimazione usata nel passaggio 3 per funzioni che hanno periodo diverso da una potenza di 2 sia abbastanza buona da permettere al resto dell'algoritmo di funzionare.

Passo 2. Uno stato del quale l'ampiezza è uguale al periodo di f. La trasformata di Fourier quantistica agisce sulla funzione ampiezza associata con lo stato in input. Affinché si possa usare la trasformata di Fourier quantistica per ottenere il periodo di f, viene costruito uno stato tale che la funzione ampiezza abbia lo stesso periodo di f.

Per costruire un tale stato, si misurino gli ultimi $\lceil \log_2 M \rceil$[5] qubit dello stato dell'equazione 1 che codifica $f(x)$. Viene ottenuto un valore casuale u. Il valore u non è interessante di per sé; solo l'effetto che la misurazione ha sul nostro insieme di sovrapposizioni è d'interesse. Questa misura proietta lo spazio degli stati su un sottospazio compatibile con i valori misurati, così che lo stato dopo la misurazione sia

$$C \sum_x g(x)|x, u\rangle,$$

per qualche parametro C dove

$$g(x) = \begin{cases} 1 & \text{se } f(x) = u \\ 0 & \text{altrimenti.} \end{cases}$$

Si noti che gli x che appaiono effettivamente nella somma, quelli con $g(x) \neq 0$, differiscono gli uni gli altri per multipli del periodo, dunque $g(x)$ è la funzione che stiamo cercando. Se potessimo misurare due x successivi nella somma, avremmo il periodo. Sfortunatamente le leggi della fisica quantistica permettono solo una misurazione.

Esempio. Si supponga che una misurazione casuale della sovrapposizione di equazione 1 produca 8. Lo stato dopo la misurazione[6] (Figura 2.1) mostra chiaramente la periodicità di f.

Passo 3. Applicare una trasformata di Fourier quantistica. La parte $|u\rangle$ dello stato non sarà più usata, quindi non verrà più scritta. Si applichi la trasformata di Fourier quantistica allo stato ottenuto nel passo 2.

$$U_{QFT} : \sum_x g(x)|x\rangle \rightarrow \sum_c G(c)|c\rangle$$

L'analisi di Fourier standard dice che quando il periodo r della funzione $g(x)$ definita nel passo 2 è una potenza di due, il risultato della trasformata di Fourier quantistica è

$$\sum_j c_j |j\frac{2^m}{r}\rangle,$$

dove l'ampiezza è 0 eccetto che nei multipli di $2^m/r$. Quando il periodo r non divide 2^m, la trasformata approssima il caso esatto, quindi la maggior parte del modulo è concentrato attorno a interi vicini a multipli di $2^m/r$.

[5] Dove $\lceil \alpha \rceil$ indica la parte intera superiore di α.

[6] solo i 9 bit di x sono mostrati nella figura; i bit di $f(x)$ sono noti dalla misura

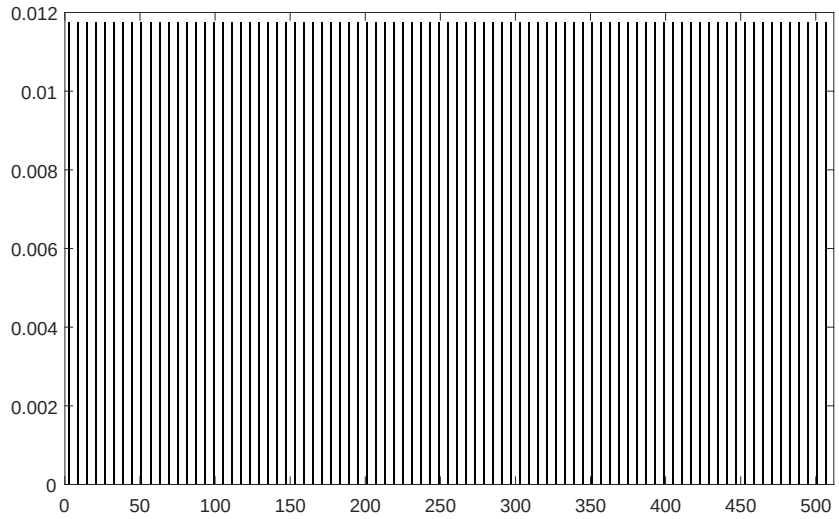


Figura 2.1: Probabilità di misurare x misurando lo stato $C \sum_{x \in X} |x, 8\rangle$ ottenuto nel Passo 2, dove $X = \{x | 11^x \mod 21 = 8\}$

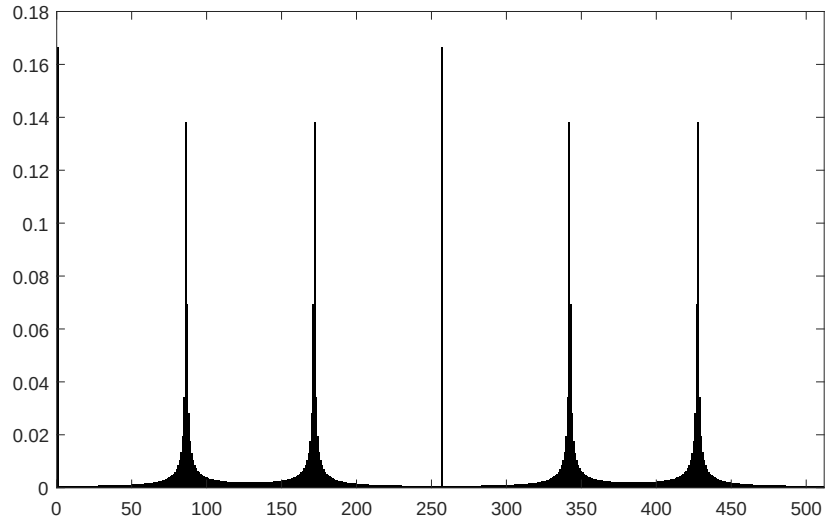


Figura 2.2: Distribuzione di probabilità dello stato quantistico dopo la trasformata di Fourier.

Esempio. L'immagine 2.2 mostra cosa si ottiene applicando la trasformata di Fourier quantistica allo stato ottenuto nel Passo 2. Si noti che l'immagine 2.2 è il grafico della trasformata di Fourier veloce della funzione mostrata nell'immagine 2.1. In questo particolare esempio il periodo di f non divide 2^m.

Passo 4. Estrarre il periodo. Si misuri lo stato nella base standard per l'informatica quantistica, e si chiami v il risultato. Nel caso in cui il periodo coincide con una potenza di 2, in modo che la trasformata di Fourier quantistica fornisce esattamente multipli di $2^m/r$, il periodo è facile da estrarre. In questo caso, $v = j\frac{2^m}{r}$ per qualche j. La maggior parte delle volte j e r saranno coprimi: in quel caso ridurre la frazione $\frac{v}{2^m}(=\frac{j}{r})$ ai minimi termini fornirà una frazione che ha come denominatore q il periodo r. Il fatto che in generale la trasformata di Fourier quantistica dia solo approssimativamente multipli della frequenza dilatata complica l'estrazione del periodo dalla misurazione. Quando il periodo non è una potenza di 2, una buona approssimazione per il periodo può essere ottenuta usando la scrittura in frazione continua di $\frac{v}{2^m}$.

Esempio. Si supponga che la misurazione dello stato restituisca $v = 427$. Poiché v e 2^m sono relativamente primi il periodo r molto probabilmente non dividerà 2^m e sarà necessaria la riscrittura in frazione continua. Lo schema seguente è una traccia dell'algoritmo necessario:

i	a_i	p_i	q_i	ε_i
0	0	0	1	0.8339844
1	1	1	1	0.1990632
2	5	5	6	0.02352941
3	42	211	253	0.5

che termina con $6 = q_2 < M \leq q_3$. Dunque, $q = 6$ è con alta probabilità il periodo di f.

Passo 5. Trovare un fattore di M. Quando la nostra ipotesi di periodo, q, è pari, si usa l'algoritmo Euclideo per controllare efficientemente se uno tra $a^{q/2}+1$ e $a^{q/2}-1$ ha un fattore comune non banale con M.

La ragione per cui $a^{q/2}+1$ o $a^{q/2}-1$ hanno probabilmente un fattore comune non banale con M è la seguente: se q è in effetti il periodo di $f(x) = a^x \mod M$, allora $a^q = 1 \mod M$ sicché $a^q a^x = a^x \mod M$ per tutti gli x. Se q è pari, si può scrivere

$$(a^{q/2}+1)(a^{q/2}-1) = 0 \mod M.$$

Quindi, a patto che né $a^{q/2}+1$ né $a^{q/2}-1$ siano multipli di M, uno tra $a^{q/2}+1$ e $a^{q/2}-1$ ha un fattore comune non banale con M.

Esempio. Poiché 6 è pari uno tra $a^{6/2}+1 = 11^3+1 = 1332$ e $a^{6/2}-1 = 11^3-1 = 1330$ avrà un fattore comune con M. In questo particolare esempio si trovano due fattori $\gcd(21, 1330) = 7$ e $\gcd(21, 1332) = 3$.

Passo 6. Ripetere l'algoritmo, se necessario. Varie cose possono essere andate male, così da fare in modo che il processo non restituisca un fattore di M:

(1) Il valore v non era abbastanza vicino ad un multiplo di $\frac{2^m}{r}$.

(2) Il periodo r e il moltiplicatore j potrebbero aver avuto un fattore in comune, così che il denominatore q era in realtà un fattore del periodo e non il periodo stesso.

(3) Il passo 5 restituisce M come fattore di M.

(4) Il periodo di $f(x) = a^x \mod M$ è dispari

Shor mostra che poche ripetizioni di questo algoritmo restituiscono un fattore di M con alta probabilità.

2.2.1 Un commento sul Passo 2 dell'Algoritmo di Shor.

La misura nel Passo 2 può essere interamente saltata. Più generalmente si può dimostrare che le misurazioni nel mezzo di un algoritmo possono sempre essere evitate. Se la misurazione nel passo 2 viene omessa, lo stato consiste di una sovrapposizione di diverse funzioni periodiche, ognuna delle quali ha lo stesso periodo. Per la linearità degli algoritmi quantistici, applicare la trasformata di Fourier quantistica porta a una sovrapposizione delle trasformate di Fourier di queste funzioni, ognuna delle quali è in correlazione quantistica con le corrispondenti u e per tanto non interferiscono le une le altre. La misurazione fornisce un valore da una di queste trasformate di Fourier. Vedendo come questa tesi può essere formalizzata mette in luce alcune delle sottigliezze di lavorare con sovrapposizioni quantistiche. Si applichi la trasformata di Fourier quantistica moltiplicata tensorialmente con l'identità, $U_{QFT} \otimes I$, a $C \sum_{x=0}^{2^n-1} |x, f(x)\rangle$ per ottenere

$$C' \sum_{x=0}^{2^n-1} \sum_{c=0}^{2^m-1} e^{\frac{2\pi i x c}{2^m}} |c, f(x)\rangle,$$

che è uguale a

$$C' \sum_{u} \sum_{x|f(x)=u} \sum_{c} e^{\frac{2\pi i x c}{2^m}} |c, u\rangle$$

per u nell'insieme delle immagini di $f(x)$. Ciò che si ottiene è una sovrapposizione dei risultati del Passo 3 per tutti i possibili u. Si sta applicando la trasformata di Fourier quantistica a una famiglia di funzioni separate g_u indicizzate da u dove

$$g_u = \begin{cases} 1 & \text{se} f(x) = u \\ 0 & \text{altrimenti,} \end{cases}$$

tutte con lo stesso periodo. Si noti che le ampiezze in stati con diversi u non interferiscono mai (sommarsi o cancellarsi) le une le altre. La trasformata $U_{QFT} \otimes I$ come applicata

sopra può essere scritta

$$U_{QFT} \otimes I : C \sum_{u \in Imm(f)} \sum_{x=0}^{2^n-1} f_u(x)|x, f(x)\rangle \rightarrow C' \sum_{u \in Imm(f)} \sum_{x=0}^{2^n-1} \sum_{c=0}^{2^m-1} G_u(c)|c, u0\rangle,$$

dove$G_u(c)$ è la trasformata di Fourier discreta di $g_u(x)$ e $Imm(f)$ è l'insieme delle immagini di $f(x)$ al variare di x.

Si misuri c e si eseguano i Passi 4 e 5 come prima.

Capitolo 3

Stato dell'arte della crittografia quantistica

A questo punto verrebbe da chiedersi se tutta questa trattazione abbia effettivamente delle conseguenze concrete, o se invece sia solo una descrizione di qualcosa che è teorizzabile, ma infattibile nella pratica.

La risposta è intermedia: si è ancora agli "albori" dell'informatica quantistica, e la costruzione di computer (o in generale di dispositivi) che sfruttino i concetti descritti nei precedenti capitoli rimane un processo molto costoso e non così efficace. Questo capitolo cercherà di descrivere lo stato dell'arte odierno per quanto riguarda i computer quantistici, lo scambio di chiave quantistica, e descriverà alcuni metodi di cifratura cosiddetti "post-quantistici", ossia che, date le conoscenze che si hanno oggi, dovrebbero rimanere sicuri anche sotto attacco di un computer quantistico.

3.1 Computer quantistici

La prima cosa che viene da chiedersi è se al giorno d'oggi esistono dei dispositivi degni di essere chiamati, effettivamente, "computer quantistici". Nei precedenti capitoli ci si è mantenuti sul vago quando si descrivevano processi o qualità di un computer quantistico, per il semplice fatto che esistono molte maniere, implementate o solo proposte, di costruirne uno, ognuna con vantaggi e svantaggi fisici ed economici.

Nel 2008, David DiVincenzo, dell'IBM, descrisse un "computer quantistico pratico" come avente le seguenti caratteristiche:

- scalabile fisicamente per aumentare il numero di qubit;
- qubit che possono essere inizializzati a valori arbitrari;
- gate quantistici che siano più veloci del tempo di decoerenza;

- un set universale di gate;

- qubit che possono venir facilmente letti.

Quello che salta all'occhio è che queste richieste sono simili a quelle che vengono fatte anche al più banale dei computer classici, tranne per quanto riguarda quella sulla decoerenza. I calcolatori quantistici infatti, soffrono molto più di quelli classici le interferenze dell'ambiente esterno, e soltanto isolando bene il sistema e tenendolo a temperature molto basse, si può sperare di avere una quantità tollerabile di errori, per i quali esistono tecniche di correzione.

Oggi, diversi colossi dell'informatica si impegnano attivamente nella costruzione di computer quantistici: Google ha dichiarato pubblicamente di aver testato processori fino a 72 bit; ci si sta avvicinando alla costruzione di calcolatori che non possono essere simulati dai dispositivi classici esistenti oggigiorno. La IBM ha poi sviluppato una piattaforma attraverso cui gli sviluppatori possono fornire codice da far eseguire ai suoi processori da 5 e da 16 qubit, la *IBM quantum experience*.

Un altra strada che si è intrapresa è quella dell'hardware costruito ad-hoc per affrontare uno specifico problema. L'azienda D-Wave ha raggiunto quota 1024 qubit su un processore che è però in grado di eseguire i calcoli necessari per trovare il minimo di una funzione attraverso la cosiddetta "ricottura quantistica"[1]. Non sembra però un "vero" computer quantistico: ad esempio, non dovrebbe riuscire ad eseguire l'algoritmo di Shor.

E proprio qui diventa palese quanto ancora si debba evolvere questo campo di studi e di tecnologie: ad oggi, il più grande numero che si sia riuscito a scomporre usando l'algoritmo di Shor è 21, anche se numeri più grandi (come 143) sono stati scomposti usando altri algoritmi su computer quantistici. Ciononostante, una possibile "supremazia quantistica" sembra sempre più vicina: in pochi anni, i super computer potrebbero essere tutti soppiantati da computer quantistici.

3.2 Crittografia post-quantistica

In uno scenario dove si apre la possibilità di computer capaci di svolgere in breve tempo un attacco contro la maggior parte dei sistemi crittografici, l'idea è di "correre ai ripari", sostituendo gli schemi esistenti che si basano su problemi come quello della fattorizzazione o del logaritmo discreto, con schemi che si basano su problemi differenti.

Gli schemi oggi usati per la crittografia a chiave privata sono in generale considerati resistenti agli attacchi quantistici: sistemi come AES non basano la propria difficoltà su problemi "dimostrabilmente difficili". Essi si basano in genere su una serie di funzioni facili da eseguire in un verso, ma complesse nel verso opposto: a patto che si usino chiavi di lunghezza sufficiente, gli schemi già esistenti oggi si possono considerare resistenti ad

[1] Molto spesso si usa il termine inglese *quantum annealing*.

attacchi quantistici. Il problema di questi sistemi è che hanno bisogno che una chiave sia scambiata, e questo si fa in genere con schemi a chiave pubblica, dei quali il più diffuso è il già menzionato (e non protetto contro gli attacchi quantistici) RSA.

Esistono però soluzioni alternative, ossia schemi a chiave pubblica che non sembrano influenzati da avversari quantistici. Uno di questi è NTRU, che opera sull'anello di polinomi $\mathbb{Z}[X]/(X^N - 1)$, utilizzando cioè un tipo di matematica diversa da quella che l'algoritmo di Shor è in grado di affrontare. Tuttavia, questo sistema è ancora "giovane", e non è per tanto da escludere che si possa trovare un algoritmo quantistico in grado di attaccarlo con successo. L'unica maniera veramente dimostrata di costruire un sistema immune ad attacchi quantistici è quello di usare la distribuzione di chiave quantistica, di cui si è parlato in 1.3.1.

3.3 Scambio quantistico della chiave

L'idea di utilizzare le qualità intrinseche delle particelle quantistiche per scambiare una chiave crittografica era già ben chiara negli anni '80. In effetti già nel 2004 una banca in Austria utilizzava un siffatto sistema, che poteva però funzionare solo per brevi distanze. Negli anni seguenti, però, si è migliorata la distanza di fibra ottica che è possibile percorrere mantenendo una velocità di comunicazione sufficiente, raggiungendo la quota (probabilmente ancora molto migliorabile) di 307km.

Nel 2017, la Cina ha mostrato uno scambio quantistico della chiave attraverso un satellite lungo una distanza di 1203km, aprendo la porta verso sistemi che utilizzano i satelliti come appoggio per scambiare fotoni polarizzati che verranno poi utilizzati per comunicare chiavi in maniera estremamente sicura.

Esistono comunque controindicazioni anche in questo caso: le implementazioni odierne utilizzano laser a bassa potenza per scambiare pochi fotoni alla volta. Questo vuol dire che, a volte, imprevedibilmente, il laser può emettere due fotoni quando se ne aspetterebbe uno solo, permettendo ad Eva di intercettare il secondo senza interagire con lo schema (e quindi senza farsi individuare).

Conclusioni

In definitiva, si può dire che l'inserirsi della meccanica quantistica sempre più profondamente nella teoria della computazione, e nella crittografia nello specifico, porterà al pensionamento di molti dei sistemi che si usano oggi. Ma come ogni innovazione, porterà anche all'introduzione di nuovi sistemi, più robusti di quelli che abbiamo oggi.

L'articolo di Shor nel 1994 ha influenzato senz'altro quest'evoluzione: mostrò cos'erano capaci di fare i computer quantistici, prima ancora che diventassero una realtà plausibile. Ogni innovazione tecnologica viene realizzata in pratica solo dopo che qualche pioniere, qualche *profeta*, ha mostrato come funziona in teoria. Se il mondo del futuro sarà quantistico, è anche grazie all'algoritmo inventato da Peter Shor.

Bibliografia

[1] Rafael Pass, Abhi Shelat, *A course in Cryptography*, prima edizione: 2007; ultima edizione: 2010, disponibile online al sito `https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf`

[2] Eleanor Rieffel, Wolfgang Polak, *An introduction to Quantum Computing for Non-Physicists*, originale: 1998; revisionato nel 2000.

[3] Matthew Hayward, *Quantum Computing and Shor's Algorithm* originale: 1999; revisionato nel 2015.

[4] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, originale: 1994; versione finale: 1996.

[5] Celeste Biever, *First quantum cryptography network unveiled*, 4 giugno 2004, *NewScientist*.

[6] Yuen Yiu, *Is China the Leader in Quantum Communications?*, 19 gennaio 2018, *Inside Science*.

[7] David P. DiVincenzo, *The Physical Implementation of Quantum Computation*, 1 febbraio 2008.

[8] L. M.K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, I. L. Chuang, *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*, 2001.

[9] N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng, J. Du, *Quantum Factorization of 143 on a Dipolar-Coupling NMR system*, 2011.

[10] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, E. M. Chapple, C. Enderud, J. P. Hilton, K. Karimi, E. Ladizinsky, N. Ladizinsky, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, C. J. S. Truncik, S. Uchaikin, J. Wang, B. Wilson, G. Rose, *Quantum annealing with manufactured spins*, 2011, *Nature*.

[11] Larry Hardesty, *3Q: Scott Aaronson on Google's new quantum-computing paper*, 2015, *MIT News Office*.

[12] Susan Curtis, *Google aims for quantum supremacy*, 6 marzo 2018, *Physics World*.

[13] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X. Zhou, J. L. O'brien, *Experimental realisation of Shor's quantum factoring algorithm using qubit recycling*, 2012

[14] Don Coppersmith, Adi Shamir, *Lattice Attacks on NTRU* , 1997

Ringraziamenti

Le persone da ringraziare sono in realtà tante.

Ringrazio i miei insegnanti, dalle elementari fino all'università, per avermi fatto appassionare alla matematica, e a tutto ciò che vi è correlato: in particolare il prof Aliffi, per avermi introdotto alla crittografia e avermi aiutato a completare questo lavoro.

Ringrazio i miei familiari, che mi hanno sostenuto anche nei miei momenti più difficili, e i miei amici, che mi hanno sempre dato la forza andare avanti, divertendomi: in particolare Greta, che più di chiunque altro ha sopportato il mio nervosismo e la mia malinconia.

Ringrazio infine il corso di matematica, perché mi ha permesso di incontrare compagni leali, amichevoli, che hanno creato un bellissimo ambiente di supporto reciproco: in particolare Flavia, perché senza i suoi consigli, i suoi aiuti, e in certi casi i suoi appunti, non sarei dove sono ora.