ISTITUTO LOMBARDO

ACCADEMIA DI SCIENZE E LETTERE

RENDICONTI

Scienze Chimiche e Fisiche, Geologiche, Biologiche e Mediche

B

Vol. 137 (2003) - Fasc. 1 e 2

ESTRATTO

G.M. D'ARIANO, C. MACCHIAVELLO

INTRODUZIONE ALLA TEORIA DELL'INFORMAZIONE QUANTISTICA

Istituto Lombardo Accademia di Scienze e Lettere

MILANO
2004

Fisica *Istituto Lombardo (Rend. Sc.)* B 137, *289-307 (2003)*

INTRODUZIONE ALLA TEORIA DELL'INFORMAZIONE QUANTISTICA

GIACOMO MAURO D'ARIANO e CHIARA MACCHIAVELLO (*)

Nota presentata dal m. e. Attilio Rigamonti
(Adunanza del 26 giugno 2003)

ABSTRACT. — We give a tutorial introduction to the theory of quantum information. We review the concept of entanglement in quantum mechanics and show how it can be exploited to achieve new ways of communication, such as quantum teleportation, and computation.

We finally explain how to achieve secure communication channels by means of quantum systems.

1. Introduzione

Negli ultimi decenni si è assistito a un rapido progresso nella miniaturizzazione delle componenti dei calcolatori elettronici e, più in generale, dei sistemi fisici che trasmettono ed elaborano informazione. Se questo progresso continuerà con lo stesso ritmo, si prevede che in breve tempo i portatori elementari di informazione raggiungeranno le

(*) Università degli Studi di Pavia, Dipartimento di Fisica "A. Volta", Via A. Bassi, 6 - 27100 Pavia.

dimensioni di una singola molecola o di un singolo atomo, e pertanto la loro natura quantistica non potrà più essere trascurata. Ciò non deve essere considerato come una limitazione, ma al contrario come un'opportunità unica che può portare a nuovi modi di computazione e di comunicazione. Sulla base delle motivazioni sopra citate, il nuovo campo dell'informazione quantistica, dove i principi della fisica quantistica si uniscono a quelli della teoria dell'informazione, si è sviluppato enormemente negli ultimi anni [1].

La teoria quantistica dell'informazione si occupa dello studio della trasmissione e dell'elaborazione di informazione nei casi in cui l'informazione stessa viene codificata su sistemi quantistici anziché gli usuali sistemi classici utilizzati ad esempio nei calcolatori ordinari, e viene elaborata in accordo alle leggi della meccanica quantistica. I più recenti progressi in questo campo comprendono la scoperta di nuovi modi di trasmettere informazione, nuovi modi di comunicare in segretezza e la possibilità di risolvere alcuni problemi molto più velocementeche con risorse classiche.

Le proprietà tipicamente quantistiche cha hanno portato a queste scoperte sono il principio di sovrapposizione, ovvero il fatto che i sistemi quantistici elementari funzionano con un nuovo tipo di bit, i *qubit* ("quantum bit") che assumono valore 0 o 1 ed anche ogni possibile sovrapposizione fra i due valori, e la forte correlazione, detta *entanglement*, tra sistemi quantistici. Sulla base di questi concetti verranno illustrati brevemente alcune tematiche fondamentali di informazione quantistica, in particolare il teletrasporto quantistico, e le basi della crittografia e del calcolo quantistico.

2. L'entanglement

Il concetto di entanglement è definito nel modo seguente. Se abbiamo un sistema quantistico composto di due sottosistemi, lo stato $|\psi\rangle_{12}$ che descrive il sistema complessivo nel formalismo di Dirac [2] è entangled se non può essere espresso nella forma fattorizzata

$$|\psi\rangle_{12} = |\phi\rangle_1 \otimes |\chi\rangle_2$$

Un esempio di *stato massimamente entangled* è lo stato di singoletto di due particelle a spin $\frac{1}{2}$ correlate in modo da dare spin totale nullo. Questo stato si scrive come segue:

$$|\Psi_{12}\rangle = \sqrt{\frac{1}{2}}\,(|\uparrow_1\rangle|\downarrow_2\rangle - |\downarrow_1\rangle|\uparrow_2\rangle)\,. \tag{2}$$

La scrittura dello stato non è unica: se si cambia la base ovvero si sceglie una generica direzione di quantizzazione "obliqua" dello spin:

$$|\nearrow\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle\,,$$

$$|\swarrow\rangle = \beta^*|\uparrow\rangle - \alpha^*\beta|\downarrow\rangle\,, \qquad |\alpha|^2 + |\beta|^2 = 1\,, \tag{3}$$

si ottiene

$$|\Psi_{12}\rangle = \sqrt{\frac{1}{2}}\,(|\nearrow_1\rangle|\swarrow_2\rangle - |\swarrow_1\rangle|\nearrow_2\rangle)\,, \tag{4}$$

La conseguenza è che, in accordo a von Neumann [3], se si misura lo spin 1 in una qualunque direzione fissata $\swarrow$ si ottiene lo spin nei versi $\nearrow$ e $\swarrow$ con ugual probabilità 1/2. Ma, si ha anche che se la misura sullo spin 1 dà risultato $\nearrow$, allora si prevede con certezza che una misura nella stessa direzione per lo spin 2 darà verso opposto $\swarrow$. Analogamente, se sullo spin 1 si ottiene $\swarrow$,allora sullo spin 2 si ottiene certamente $\nearrow$. Tutto ciò è ovviamente in accordo alla conservazione del momento angolare totale, ma, cosa meno banale, ciò avviene istantaneamente (superluminalmente), e in assenza di alcun tipo di interazione tra le particelle, anche se le particelle vengono portate a distanza molto grande, nell'ipotesi che esse non interagiscano con altre particelle circostanti. Invece, quando le direzioni di misura per i due spin anziché parallele sono ortogonali, i risultati ottenuti sulle due particelle sono perfettamente scorrelati. Infine, poiché la probabilità di rilevare lo spin in uno dei due versi opposti è comunque $\frac{1}{2}$, indipen-

dentemente dal fatto che sia stata eseguita una misura sull'altro spin, ne consegue che pur essendo l'effetto di correlazione superluminale, esso non può essere utilizzato per trasmissione di informazione a velocità infinita. Infatti, quando si misura lo spin 2 si ottiene comunque un risultato casuale, e non c'è modo di sapere se il risultato sia dovuto ad un cambiamento della direzione di misura sullo spin 1: le correlazioni possono essere verificate solo a posteriori [4].

Questo tipo di correlazione ha stupito Einstein che nel 1935 con Podolsky e Rosen scrisse un articolo [5] che metteva in dubbio l'obiettivita e la completezza della descrizione quantistica. Esistono forse variabili nascoste che possono descrivere questa correlazione? Bell nel 1964 [6] ha dimostrato un teorema che afferma che una qualunque teoria di meccanica classica con ipotetiche variabili nascoste non è in grado di spiegare questa correlazione (a meno di non avere teorie strane *non locali*, ovvero con interazioni che si propagano istantaneamente). È molto difficile verificare sperimentalmente questa correlazione con particelle, in quanto è difficile eliminare le interazioni fra le particelle ed il circondario. Solo molto recentemente l'entanglement è stato verificato sperimentalmente con mesoni K^o neutri a distanza del metro, distanza enormemente più grande della lunghezza d'onda di de Broglie molto piccola [7]. In ottica quantistica, invece, è veramente molto semplice verificare l'entanglement, utilizzando, anziché i due possibili versi dello spin di una particella, la polarizzazione verticale/orizzontale del fotone. Per un approfondimento sul tema dell'entanglement si veda anche il testo divulgativo di Gian Carlo Ghirardi [8].

3. Il teletrasporto

Il concetto di entanglement è l'ingrediente fondamentale del teletrasporto quantistico, del quale si è anche sentito parlare sui quotidiani e sui media relativamente agli esperimenti del gruppo di Francesco De Martini a Roma La Sapienza [9], di Anton Zeilinger a Innsbruk [10], e di Jeff Kimble al Caltech [11, 12]. Innanzitutto, cosa vuol dire *teletrasporto*? La definizione dell'Oxford dictionary dice testualmente: "*Paranormale* e *Fantascienza:* il trasferimento di persone (specialmente di se stesso!) o cose mediante energia psichica. In una descrizione futuristi-

ca: trasporto apparentemente istantaneo di persone o cose attraverso lo spazio mediante mezzi tecnologicamente avanzati".

Si può senz'altro affermare che il termine teletrasporto è uscito dal dominio della fantascienza per entrare in quello della scienza da quando Bennett, Brassard, Crèpau, Yozsa, Peres e Wotters pubblicarono nel 1993 il Physical Review Letters dal titolo: *Teletrasporto di uno stato quantistico ignoto mediante doppio canale classico e EPR* [13]. Il canale EPR è lo stato massimamente entangled che abbiamo visto nella Sezione 2, e viene così chiamato dopo il lavoro di Einstein, Podolsky, e Rosen ivi menzionato. Il problema è il seguente.

In accordo alla Meccanica Classica teletrasportare un oggetto corrispondebbe a "spostare" fisicamente tutte le particelle di cui l'oggetto è composto. Ricostruire l'oggetto con particelle diverse da quelle originali darebbe luogo ad un oggetto identico (cioè con le stesse proprietà fisiche), ma "distinto" dall'originale, in quanto classicamente le particelle sono *distinguibili*, ovvero, anche se identiche (per carica, massa, spin), esse mantengono sempre la loro identità, che in principio ci permette di seguirle individualmente nel loro moto. In Meccanica Quantistica, invece, particelle identiche sono anche *indistinguibili*, ovvero non è possibile seguirle individualmente nel loro moto: a tutti gli effetti, particelle identiche sono la stessa entità fisica. Potremo quindi affermare che un oggetto non è identificabile con le molecole che lo compongono, bensì si riconosce nello stato quantistico delle sue molecole. In altri termini, l'identità di un oggetto risiede nello stato quantistico delle particelle di cui è composto, e non si identifica con l'insieme delle particelle componenti stesse. Il teletrasporto di un oggetto consiste appunto nel trasmettere e ricostruire a distanza, su materia ivi presente, lo stato quantistico delle particelle di cui l'oggetto è composto. Quindi, in sintesi: teletrasporto significa ricostruire lo stato quantico di un oggetto in un luogo distante su materia ivi presente.

Ciò che rende non banale la realizzazione del teletrasporto è l'impossibilità in principio di conoscere lo stato quantistico di un oggetto. Come possiamo trasmettere e ricostruire a distanza lo stato se non possiamo conoscerlo? D'altra parte, abbiamo anche il secondo problema, non meno grave del precedente: se anche lo stato quantico fosse noto – come nel caso che esso fosse stato "preparato" sotto il nostro controllo – l'informazione che descrive lo stato, e che dovremmo quindi trasmettere, sarebbe infinitamente grande. Infatti, lo stato

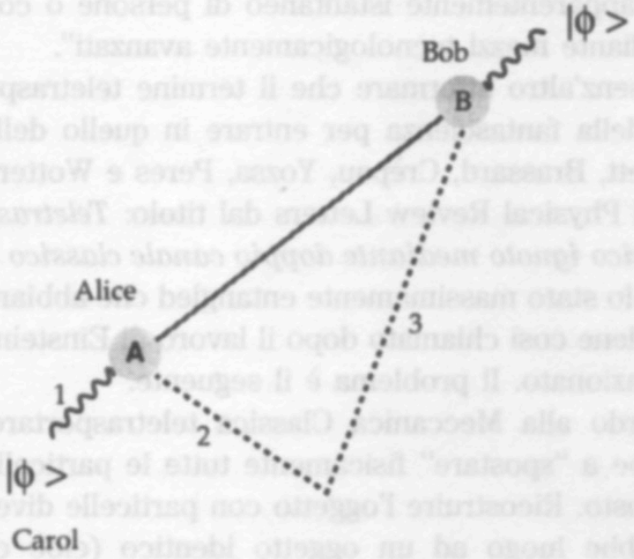

Figura 1. – Schema del teletrasporto quantistico del Rif. [13]. Per la spiegazione si rimanda al testo

quantistico di un solo spin (ovvero di un semplice sistema a due soli livelli energetici) è descritto da un numero complesso (si veda l'equazione (3)). Pertanto, il numero di bit da trasmettere aumenta con la precisione con la quale si approssima il numero complesso, ed occorre un'informazione virtualmente infinita per trasmettere lo stato in modo esatto. Quindi, in sintesi: a) non si può conoscere lo stato quantico; b) se anche lo stato fosse noto occorrerebbe un'informazione infinita per trasmetterlo. Come quindi è possibile "teletrasportare" lo stato quantistico, ovvero trasmetterlo e ricostruirlo a distanza? E qui il risultato eclatante del lavoro [13]: non è necessario conoscere lo stato per teletrasportarlo, anzi, per non distruggerlo, si deve far in modo di conoscerlo in alcun modo. Inoltre, per teletrasportare lo stato di uno spin bastano solo 2 bit di informazione più un canale entangled!

Ed ecco qui la soluzione del problema del teletrasporto. In Fig. 2 la lettera *A* rappresenta la sorgente, mentre la lettera *B* denota il ricevitore: nella letteratura sull'argomento essi sono chiamati rispetti-

vamente "Alice" e "Bob". Alice deve teletrasportare uno stato $|\phi\rangle$ a Bob. Poiché Alice non deve conoscere lo stato $|\phi\rangle$, diremo che è Carol a consegnarglielo. Alice e Bob dispongono di due risorse: un canale classico (telefono, radio), ed un canale entangled costituito da una coppia di particelle in uno stato di singoletto che si dipartono da un luogo intermedio verso Alice e Bob. Alice correla la particella 1 con la particella 2 della coppia eseguendo la misura completa descritta dal set ortonormale di Bell:

$$|\Psi_{12}^{\pm}\rangle = \sqrt{\frac{1}{2}}\,(|\uparrow_1\rangle|\downarrow_2\rangle - |\downarrow_1\rangle|\uparrow_2\rangle)\,,$$

$$|\Phi_{12}^{\pm}\rangle = \sqrt{\frac{1}{2}}\,(|\uparrow_1\rangle|\uparrow_2\rangle - |\downarrow_1\rangle|\downarrow_2\rangle)\,. \tag{7}$$

La misura ha quattro possibili risultati, che denoteremo con $\{\Psi^{\pm}, \Phi^{\pm}\}$. Scriviamo quindi il generico stato ignoto della particella 1 come segue:

$$|\phi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle \qquad |\alpha|^2 + |\beta|^2 = 1\,. \tag{8}$$

Lo stato delle tre particelle prima della misura è:

$$|\Psi_{123}\rangle = |\phi_1\rangle|\Psi_{23}^{-}\rangle = \frac{\alpha}{\sqrt{2}}\,(|\uparrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\uparrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle) + \frac{\beta}{\sqrt{2}}\,(|\downarrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle)$$

che in termini della base di Bell può essere riscritto come segue:

$$|\Psi_{123}\rangle = \frac{1}{2}[|\Psi_{12}^{-}\rangle \underbrace{(-\alpha|\uparrow_3\rangle - \beta|\downarrow_3\rangle)}_{-|\phi_3\rangle} + |\Psi_{12}^{+}\rangle \underbrace{(-\alpha|\uparrow_3\rangle + \beta|\downarrow_3\rangle)}_{-\sigma_z|\phi_3\rangle}$$

$$+ |\Phi_{12}^{-}\rangle \underbrace{(\beta|\uparrow_3\rangle + \alpha|\downarrow_3\rangle)}_{-\sigma_x|\phi_3\rangle} + |\Phi_{12}^{+}\rangle \underbrace{(-\beta|\uparrow_3\rangle + \alpha|\downarrow_3\rangle)}_{-i\sigma_y|\phi_3\rangle}] \tag{7}$$

Come si vede, a seconda del risultato della misura di Alice, Bob riceve uno stato diverso. Ma Alice trasmette a Bob il suo risultato sul canale classico. Se il risultato è Ψ^- Bob non fa nulla: egli ha già lo stato giusto (cambiato di segno: ma in Meccanica Quantistica lo stato è definito a meno di un fattore di fase). Se il risultato è Ψ^+ Bob fa una rotazione dello spin di 180^o gradi intorno all'asse z (descritta dalla matrice di Pauli σ_z). Se invece il risultato è Φ^- Bob fa una rotazione di 180^0 attorno all'asse x (matrice di Pauli σ_x), ed infine se il risultato è Φ^+ Bob fa una analoga rotazione attorno all'asse y (matrice σ_y). Alla fine Bob si trova sempre con la particella 3 nel corretto stato incognito $|\phi\rangle$ che precedentemente apparteneva alla particella 1. Alice ottiene uno dei quattro possibili risultati $\{\Psi^{\pm}, \Phi^{\pm}\}$ con probabilità $\frac{1}{4}$, indipendentemente dallo stato $|\phi\rangle$, del quale, pertanto, non ottiene alcuna informazione dalla misura eseguita. Si noti che poiché i risultati della misura sono quattro, i bit da trasmettere sul canale classico sono due.

Lo schema precedente è ovviamente generalizzabile in vari modi [14], per esempio a più particelle, o a bosoni anziché fermioni. Come accennato in precedenza, il teletrasporto quantistico è stato dimostrato sperimentalmente utilizzando radiazione, ovvero teletrasportando stati della luce [9, 10, 11, 12].

4. Calcolatori quantistici

Vediamo ora come l'entanglement può essere utilizzato per fare un nuovo tipo di calcolatori, i "computer quantistici". Innanzitutto dobbiamo amaramente constatare che la attuale tecnologia elettronica raggiungerà un punto di saturazione previsto nell'arco di 10-20 anni. Nell'arco degli ultimi trent'anni il numero di transistor per microchip è passato da alcune migliaia alla fine degli anni '60 a miliardi o decine di miliardi con legge esponenziale (questa crescita esponenziale è detto volgarmente detta "legge di Moore"). Colin Worwick commentava alcuni anni or sono che se si avesse avuto, per confronto, un analogo progresso nell'auto avremmo automobili che costano 40 dollari, con un bagagliaio 1500m^3, che viaggiano a 2 milioni di km/h e consumano solo un litro di carburante ogni 600000 km! Purtroppo nel progresso dei computer, come già detto, si raggiungerà presto una saturazione. In

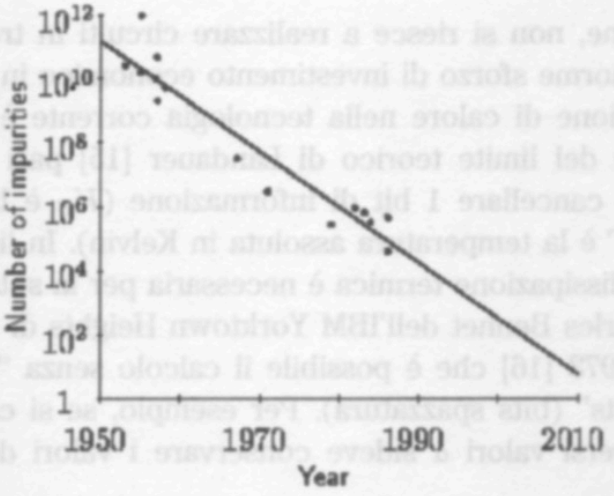

Figura 2. – Numero di impurezze droganti per transistor in circuiti logici versus l'anno di produzione [fig. 5 da R. W. Keyes, IBM J. Res. Develop. **32**, 24 (1988), reprinted with permission of IBM T.J. Watson Research Center]

Fig. 2 è riportato il numero di impurezze droganti per transistor in circuiti logici dagli anni '50 agli anni '90. Si vede che il numero di elettroni per transistor segue una legge esponenziale inversa in funzione del tempo (in realfa nell'ultima decade si è avuta addirittura una accelerazione ulteriore dovuta alla concorrenza!) Se si estrapola la retta si vede che si raggiungerà il limite dell'elettrone singolo per transistor attorno al 2010, ovvero fra pochi anni! Dopodiché o cambia la tecnologia, o inizia un nuovo medioevo di stasi tecnologica. Una memoria commerciale ha ora un dimensione minima di 0.35 μm, e sta iniziando la transizione fra microtecnologia e nanotecnologia. Il prossimo obbiettivo è il cosiddetto *pointone*, ovvero 0.1 μm; si arriverà infine a poche decine di nanometri.

I problemi coinvolti nella miniaturizzazione elettronica spinta sono molteplici. Innanzitutto il *cross-talk:* gli elettroni cominciano a "tunnellare" fra i transistor e i fili di collegamento. Occorre poi gestire correnti molto piccole, e c'è l'enorme problema della dissipazione di-

calore. Ed infine, non si riesce a realizzare circuiti in tre dimensioni, nonostante l'enorme sforzo di investimento economico in questo settore. La dissipazione di calore nella tecnologia corrente è 1 milione di volte maggiore del limite teorico di Landauer [15] pari a $K_B T \log 2$, necessario per cancellare 1 bit di informazione (K_B è la costante di Boltzmann, e T è la temperatura assoluta in Kelvin). In linea di principio, infatti, la dissipazione termica è necessaria per la sola cancellazione di dati. Charles Bennet dell'IBM Yorktown Heights di New York ha mostrato nel 1973 [16] che è possibile il calcolo senza "erase", utilizzando "junk bits" (bits spazzatura). Per esempio, se si calcola la funzione f su diversi valori a sideve conservare i valori di input come segue:

$$f : \quad a \to (a, f(a)) \,. \tag{14}$$

In Meccanica Quantistica trasformazione reversibile è sinonimo di trasformazione unitaria. Utilizzando bit quantistici, detti qubit, con stati $|0\rangle$ e $|1\rangle$ (corrispondenti a spin *down* $|\downarrow\rangle$ e spin *up* $|\uparrow\rangle$) e tutte le possibili sovrapposizioni $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ il computer potrebbe avvantaggiarsi della dimensione esponenziale dello spazio di Hilbert (dimensione $q = 2^k$ per k qubits) per eseguire un *calcolo parallelo quantistico*! Le prime idee sul calcolo quantistico sono dovute a David Deutsch [17], un teorico di Oxford (alcune idee risalgono allo stesso Richard Feynman [18]). Si vede innanzitutto che esiste un gate reversibile (ovvero descritto da una trasformazione unitaria), il *controlled-NOT* (o XOR), che opera su due qubit simultaneamente, mediante il quale con l'aggiunta di operazioni unitarie a qubit singolo si realizza un set universale.

Si può quindi calcolare una funzione in parallelo sullo spazio di Hilbert mediante una trasformata di Hadamard che trasforma lo stato di "reset" (con tutti i bit 0) nella sovrapposizione di tutti i possibili valori. Questa trasformazione è ovviamente unitaria. Per k qubits (dimensione $q = 2^k$ dello spazio di Hilbert) si ha

$$|0\rangle \to \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \,. \tag{15}$$

Si aggiunge quindi un nuovo registro e si calcola la funzione f mediante una opportuna trasformazione unitaria U_f che dipende da f

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle|0\rangle \to \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle\,|f(a)\rangle\,. \tag{16}$$

I due registri sono ora entangled. Il computer ha in memoria tutti i risultati possibili nella sovrapposizione entangled! Si consideri che per soli $k = 140$ qubits il computer calcola e tiene in memoria più risultati delle particelle dell'universo! Purtroppo questi risultati non sono accessibili a piacimento, bensì in modo casuale. Ma un singolo calcolo di interesse che dipende da tutti irisultati precedenti può essere in linea di principio ottenuto mediante una appropriata misura quantistica sulla sovrapposizione! Il computer quantistico può eseguire in tal modo calcoli improponibili con computer di ogni dimensione o potenza. Può, per esempio, fattorizzare numeri. Definiamo *classe di complessita* di un algoritmo di calcolo il numero di *step* dell'algoritmo in funzione del numero di bit dell'input. Nel problema della fattorizzazione del numero N la dimensione dell'input è $\log N$, ovvero il numero di cifre di N. Il miglior algoritmo noto, una variante dell'algoritmo RSA [19], impiega un tempo di esecuzione dell'ordine di

$$O\left(\exp\left[(64/9)^{1/3}\,(\log N)^{1/3}\,(\log\log N)^{2/3}\right]\right), \tag{17}$$

ovvero il tempo di calcolo cresce esponenzialmente con la dimensione dell'input. Facciamo un esempio per rendere l'idea. La fattorizzazione dei grandi numeri sta alla base di uno dei metodi a chiave pubblica usato dai militari per comunicazioni crittografate (questo perché è molto facile costruire il prodotto di due numeri grandi a piacere, ma è difficile estrarre i fattori di un numero). Nel 1994 mediante l'algoritmo suddetto è stato fattorizzato un numero di 129 cifre, e ci sono voluti otto mesi di calcolo parallelo di 1600 workstations. Alla stessa velocità occorrerebbero 800.000 anni per un numero di 250 cifre e 10^{25} anni (molto più dell'età dell'universo!) per un numero di sole 1000 cifre. Ebbene, Peter Shor [20] ha mostrato che con un algoritmo quantistico

è possibile fattorizzare in tempo polinomiale! E basterebbero pochi milioni di steps per fattorizzare un numero di 1000 cifre. Per fattorizzare numeri occorre un numero grande di qubits $k > 2\log_2 N$. Ma per simulare un sistema quantistico di 20 spin basta un computer di soli 20 qubits (più quelli necessari per l'error correction). Ma nessun computer classico potrebbe mai eseguire una tale simulazione, in quanto occorrerebbe diagonalizzare una matrice $10^6 \times 10^6$! Dobbiamo però cautelare facili entusiasmi sull'uso del quantum computer. Infatti, il quantum computer non è semplicemente "più veloce" del computer classico, ma permette di risolvere molto rapidamente solo problemi specifici, che si risolvono con un algoritmo particolare che può avvantaggiarsi del parallelismo quantistico. Per esempio, pur potendo eseguire il calcolo di una funzione $f \to f(a)$ in principio in una sola step (la trasformazione unitaria nell'equazione (10)), non si conosce a tutt'oggi un algoritmo quantistico che permetta di calcolare, per esempio, la somma $\sum_a f(a)$ (come abbiamo già visto, uno solo dei risultati $f(a)$ è accessibile, e solo in modo casuale). Siamo ancora agli inizi, e molta strada deve ancora essere percorsa dai *computer scientists* per individuare e classificare le strutture algoritmiche che possono avvantaggiarsi del computer quantistico. Allo stato attuale dell'arte esiste solo un altro algoritmo che si velocizza con il quantum computer, ed è l'algoritmo di Grover per ricerca su database [21]. Inoltre, di deve notare che il parallelismo quantistico è congegnato in modo da velocizzare problemi che non necessitano di calcolare esplicitamente un numero esponenzialmente grande di soluzioni, e/o soluzioni con range esponenzialmente grande.

5. Crittografia quantistica

Nella crittografia classica l'unico sistema di cui è stata dimostrata matematicamente la sicurezza è il "one time pad" a chiave segreta, cioè un protocollo in cui è necessario che il mittentee il destinatario del messaggio si scambino una chiave segreta costituita da una sequenza di numeri casuali che deve essere utilizzata una sola volta. Il problema fondamentale rimasto ancora aperto nella crittografia classica è comunque quello della sicurezza della distribuzione della chiave: in linea

di principio qualsiasi canale privato tradizionale, per quanto sicuro e protetto, può essere tenuto sotto controllo passivamente, senza cioè che i due interlocutori si accorgano del tentativo di intercettazione in atto. Un qualsiasi tentativo di spionaggio del segnale corrisponde infatti a un processo fisico di misura e in fisica classica si possono misurare tutte le proprietà fisiche di un sistema senza perturbarle. Sono allora possibili interventi passivi su un canale classico, cioè atti di spionaggio che non provocano alterazioni del segnale trasmesso e quindi impediscono ai due interlocutori di stabilire se il segnale è stato in qualche modo intercettato.

In meccanica quantistica invece un atto di misurazione provoca in generale una perturbazione del sistema. Questa particolarità del mondo quantistico ha suggerito di impiegare come canale di trasmissione per la chiave *un canale privato quantistico, progettato in modo tale che un qualsiasi tentativo di intercettazione disturbi necessariamente il segnale con conseguenze osservabili dagli utenti*. Si possono realizzare così canali di trasmissione dell'informazione intrinsecamente sicuri, protetti cioè dalle leggi stesse della meccanica quantistica. L'idea fondamentale della crittografia quantistica è quindi quella di risolvere il problema della distribuzione della chiave attraverso l'utilizzo di canali di trasmissione quantistici e ottenere quindi un sistema crittografico del tipo "one time pad" assolutamente inviolabile. I principali schemi quantistici finora proposti si possono distinguere in:

a) sistemi basati sull'utilizzo di osservabili che non commutano sistema BB84 [22]);
b) sistemi che sfruttano l'entanglement quantistico di coppie di particelle (sistema EK91 [23]).

Diamo qui una breve descrizione del sistema BB84. Lo schema BB84, ideato da Charles Bennett e Gilles Brassard nel 1984, è stato il primo sistema quantistico proposto. Per descrivere il suo funzionamento ricorriamo ancora ad Alice e Bob, rispettivamente mittente e destinatario della chiave. Alice sia dotata di una sorgente di fotoni polarizzati e Bob di un polarimetro che misuri la polarizzazione lungo direzioni perpendicolari nel piano ortogonale alla direzione di propagazione dei fotoni. In particolare, supponiamo che Alice possa inviare fotoni polarizzati secondo quattro possibili direzioni: due direzioni ortogonali individuate da due assi prefissati x e y, e due direzioni orto-

gonali x' e y' ruotate di 45^o rispetto a x e y. Se indichiamo con $|\leftrightarrow\rangle$ e $|\updownarrow\rangle$ la coppia di stati ortogonali e normalizzati di un fotone con polarizzazione diretta lungo x e y rispettivamente, gli stati con polarizzazione diretta lungo x' e y' (ruotata cioè di 45^o e 135^o rispetto all'asse x) sono dati da

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle + |\updownarrow\rangle\right) \tag{12}$$

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}\left(|\leftrightarrow\rangle - |\updownarrow\rangle\right). \tag{19}$$

Supponiamo inoltre che il polarimetro di Bob possa misurare o la polarizzazione lungo i due assi ortogonali x e y (che nel seguito sarà chiamata per convenzione polarizzazione allineata agli assi) o quella lungo i due assi x'e y' ruotati di 45^o rispetto ai precedenti (polarizzazione ruotata).

ALICE	BOB	
$\oplus$	$\oplus$	$\otimes$
0	0	0 1
1	1	0 1

ALICE	BOB	
$\otimes$	$\oplus$	$\otimes$
0	0 1	0
1	0 1	1

Tabella 1. – Corrispondenza dei risultati ottenuti da Alice e Bob nel sistema BB84

Polarizzazione allineata e polarizzazione ruotata corrispondono a due osservabili che non commutano. Per convenzione si assegni il valore 0 ai fotoni che risultano polarizzati lungo x o x' e il valore 1 ai fotoni polarizzati lungo y o y'. Supponiamo che Alice mandi a Bob un fotone polarizzato rettilineamente lungo x o lungo y; se Bob effettua una misura di polarizzazione allineata agli assi x e y, che verrà indicata con il simbolo $\oplus$, si ha come risultato la trasmissione di un bit di informazione in quanto egli è in grado di determinare con esattezza la polarizzazione del fotone spedito da Alice. Se invece Bob misura la

polarizzazione nella base ruotata $\otimes$, il risultato della misura è del tutto casuale: può assumere i valori 0 o 1 con uguale probabilità. In tal caso l'informazione trasportata dal fotone inviato da Alice viene completamente persa. La situazione è rappresentata schematicamente in Tab. 1.

La trasmissione della chiave avviene nel modo seguente: Alice invia a Bob fotoni con polarizzazione lungo x, x', y, y' scelta a caso. Può scegliere ad esempio di inviare la seguente sequenza di fotoni:

$$\updownarrow \nearrow \searrow \updownarrow \nearrow \searrow \leftrightarrow \updownarrow \searrow \leftrightarrow \searrow \nearrow \updownarrow \nearrow \leftrightarrow \cdots .$$

Bob sceglie a caso e indipendentemente da Alice il tipo di misurazionedi polarizzazione da effettuare per ciascun fotone incidente, allineata agli assi x e y o ruotata. Può scegliere ad esempio la seguente successione di misure:

$$\oplus \otimes \oplus \oplus \oplus \oplus \otimes \oplus \oplus \otimes \otimes \otimes \otimes \oplus \cdots ,$$

ottenendo i risultati

$$\updownarrow \nearrow \leftrightarrow \updownarrow \updownarrow \leftrightarrow \leftrightarrow \searrow \updownarrow \leftrightarrow \searrow \searrow \nearrow \nearrow \leftrightarrow \cdots .$$

Dopo che tutti i fotoni sono stati trasmessi e misurati Bob rivela pubblicamente ad Alice il tipo di misurazione effettuato per ciascun fotone, senza però rivelarne il risultato. Alice, confrontando questi dati con la polarizzazione da lei scelta di volta in volta comunica a Bob quali risultati vanno scartati perché corrispondenti a misurazioni di polarizzazione non coincidenti. Nell'esempio mostrato si devono scartare il terzo risultato, il quinto, il sesto, ecc. I rimanenti risultati, che sono rimasti segreti, sono una sequenza di numeri casuali lunga a piacere e quindi costituiscono la chiave:

$$1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ \cdots$$

Consideriamo ora il problema della sicurezza del sistema. Supposto che un utente esterno riesca a intercettare il canale di comunica-

zione, l'unico modo per ottenere informazioni sulla chiave è misurare la polarizzazione dei fotoni in transito verso Bob. È però noto che non è possibile misurare simultaneamente le polarizzazioni $\oplus$ e $\otimes$ di un singolo fotone con infinita precisione e non è quindi possibile ottenere un'informazione completa sullo stato di polarizzazione del fotone.

Una semplice strategia da parte della spia può essere quindi quella di scegliere per ogni fotone uno dei due tipi di misurazione e inviare poi a Bob fotoni polarizzati in accordo con il risultato ottenuto nella misura. La probabilità di effettuare la scelta di misurazione sbagliata è 1/2 e in tal caso i fotoni che giungono a Bob hanno perso memoria della polarizzazione originaria. Se comunque Bob effettua la misura giusta su questi fotoni ha probabilità 1/2 di ottenere il risultato corretto, in accordo con la polarizzazione scelta da Alice. Allora per ciascun fotone un eventuale tentativo di intercettazione del canale ha probabilità $P = 3/4$ di non essere scoperto. Tale probabilità è abbastanza alta, ma per n fotoni diviene

$$P(n) = \left(\frac{3}{4}\right)^n . \tag{14}$$

Non esiste pertanto una buona strategia di spionaggio che non venga rivelata in quanto per n grande $P(n) \to 0$. Si noti che si possono architettare strategie di spionaggio molto più sofisticate di quella appena descritta, che producono una probabilità di non essere scoperti maggiore della (14). Comunque, il fatto che qualsiasi tipo di misura causa una perturbazione sul sistema svela ad Alice e Bob la presenza di un tentativo di spionaggio.

Per verificare se effettivamente la chiave condivisa da Alice e Bob è segreta oppure no si possono utilizzare diversi metodi. Il più immediato consiste nel confronto diretto di un sottoinsieme scelto a caso dei risultati ottenuti. Se i risultati concordano si può con un buon livello di confidenza stabilire che non ci sono stati interventi esterni sul canale; i dati confrontati vengono scartati, mentre gli altri costituiscono la chiave. Se invece nel confronto si osservano delle discrepanze tra i dati (un intervento di spionaggio sistematico, in base a quanto detto prima, provoca degli errori in 1/4 circa dei risultati) il processo di trasmissione della chiave viene ripetuto da capo.

6. Conclusioni e prospettive future

In questo lavoro abbiamo descritto brevemente alcuni aspetti dell'informazione quantistica, in particolare il teletrasporto quantistico, il computer quantistico e la crittografia quantistica. Sono stati fatti molti passi avanti negli ultimi anni nella direzione di poter implementare sperimentalmente questi sistemi. Dal punto di vista teorico, attraverso lo sviluppo di tecniche quantistiche di correzione degli errori [24], è stato risolto il problema del rumore dovuto all'interazione del sistema quantistico con l'ambiente esterno. Sul fronte della crittografia quantistica i progressi tecnici hanno già raggiunto la fase applicativa: è stata dimostrata la possibilità di realizzare comunicazioni crittografiche quantistiche in fibra ottica su distanze di decine di km [25]e già si punta a protocolli commerciali.

Ciò nonostante è difficile fare delle previsioni sul futuro delle nuove tecniche di informazione quantistica. Anche se sono già disponibili prototipi di quantum computers basati su spettrometri NMR, è difficile immaginare la realizzazione in tempi brevi di computer quantistici che lavorino con alcune decine – o addirittura un centinaio – di qubit, in quanto allo stato attuale delle conoscenze si presume che essi debbano funzionare con reticoli ottici, ed il problema dell'isolamento dal circondario (pur considerata la possibile implementazione di tecniche di correzione degli errori) sembra a tutt'oggi quasi insormontabile. Per ora, si parla di realizzare appena due qubit in uno stato entangled! Altrettanto difficile risulta l'implementazione di un teletrasporto quantistico di un sistema esteso o composito. Qui il problema maggiore è rappresentato dalla misurazione quantistica di Bell che deve essere condotta su tutto il sistema congiuntamente. Per esempio, non si conosce attualmente nemmeno una tecnica per teletrasportare un singolo atomo di idrogeno, ed una vera tecnica di teletrasporto dovrebbe funzionare invariabilmente in modo indipendente dal tipo di sistema (ovvero dalla sua composizione chimica). Bisogna comunque sottolineare il grande interesse suscitato dalle tematiche dell'informazione quantistica in diversi campi della fisica sperimentale e dallo sforzo impiegato attualmente dagli sperimentatori per proporre sistemi adatti per implementare un computer quantistico.

RIFERIMENTI BIBLIOGRAFICI

[1] Rassegne recenti del campo sono: A. Steane, Rep. Prog. Phys. **61**, 117 (1998); the issue of *Phys. World*, **11** (1998); M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press (2000); *Quantum computation and quantum information theory*, C. Macchiavello, G.M. Palma and A. Zeilinger eds., World Scientific, Singapore (2001).

[2] P.A.M. Dirac, *Principles of Quantum Mechanics, 4th Ed.*, Oxford University Press, London, 1954.

[3] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton 1955.

[4] Nonostante l'ovvietà dell'impossibilità di comunicare superluminale mediante entanglement, questo metodo (fallace) è stato addirittura oggetto di un brevetto! Si veda: N. Herbert, *Found. Phys.* **12**, 1171 (1982). Sull'impossibilità delle comunicazioni superluminali nonostante la non località si veda anche: G.C. Ghirardi, A. Rimini and T. Weber, Lett. Nuovo Cim. **27**, 263 (1980), e più recentemente D. Bruss, G.M. D'Ariano, C. Macchiavello and M.F. Sacchi, *The principles of quantum mechanics and the impossibility of superluminal communications*, Phys. Rev. A. **62**, 62302 (2000).

[5] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).

[6] S. Bell, *Speakable and unspeakable in quantum mechanics*, Cambridge University Press (Cambridge 1987); si veda anche: J.F. Clauser, M. Horne, A. Shimony and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[7] A. Apostolakis *et al.*, Phys. Lett. B **422**, 339 (1998).

[8] G.C. Ghirardi, *Un'Occhiata alle Carte di Dio*, il Saggiatore, Milano 1997.

[9] D. Boschi, S. Branca, F. De Martini, L. Hardy and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[10] D. Boumeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature **390**, 575, London (1997).

[11] S.L. Braunstein and H.J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).

[12] A. Furasawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble and E.S. Polzik, Science **282**, 706 (1998).

[13] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres and W.K. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).

[14] S.L. Braunstein, G.M. D'Ariano, G.J. Milburn and M.F. Sacchi, Phys. Rev. Lett. **84**, 3486 (2000).

[15] R. Landauer, IBM J. Res. Dev. **5**, 183 (1961).

[16] C. Bennet, IBM J. Res. Dev. **17**, 525 (1973).

[17] D. Deutsch, Proc. R. Soc. Lond. A **400**, 97 (1985).

[18] R.P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[19] R. Rivest, A. Shamir and L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for ComputerScience Technical Report, MIT/LCS/TR-212 (January 1979)

[20] P.W. Shor, p. 124 in *Proceedings pf the 35th Annual Symposium of the Foundations of Computer Science*, ed. S. Goldwasser, IEEE Computer Society Press, Los Alamitos, CA, (1994).

[21] L.K. Grover, p. 212 in *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, (May 1996), preprint **quant-ph/9605043**; Phys. Rev. Lett. **79**, 325 (1997).

[22] C.H. Bennett, G. Brassard, in "Proc. IEEE Int. Conference on Computers, Systems and Signal Processing", IEEE, New York (1984).

[23] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[24] P.W. Shor, Phys. Rev. A **52**, 2493 (1995); A.M. Steane, Proc. R. Soc. Lond. A **452**, 2551 (1996); A. Ekert and C. Macchiavello, Phys. Rev. Lett **77**, 2585 (1996).

[25] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).