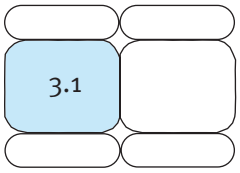
QUANTUM COMPUTING: SOGNO TEORICO O REALTÀ IMMINENTE?

Emanuele Angeleri

Una pregnante osservazione del premio Nobel R. Feynman, risalente a una quarantina di anni fa, ha aperto la strada a interessanti studi e a stupefacenti applicazioni della fisica quantistica nel campo delle macchine per il calcolo automatico. Si è aperto, a seguito di ciò, un nuovo settore informatico conosciuto con il nome di *Quantum Computing*. Nell'articolo qui presentato vengono forniti i primi elementi per comprendere il funzionamento di questi nuovi dispositivi dai quali si attendono, in futuro, innovative realizzazioni sperimentali.



1. INTRODUZIONE

Un'antica e interessante intuizione, nata a quanto pare in India e rimbalzata in Occidente attraverso il filosofo greco Democrito, ha trovato, agli inizi del secolo XX, una ragionevole conferma nelle evidenze sperimentali a cui la scienza moderna sottopone, a scopo di verifica, ogni affermazione circa la realtà fisica. La felice intuizione, secondo quanto argomenta Democrito, ha una sua base razionale: il pane, la carne e i diversi cibi di cui si nutre l'uomo vengono trasformati dal suo organismo in capelli, unghie e sangue. È pertanto assai verisimile che gli oggetti che si osservano sono prodotti da componenti elementari, gli atomi appunto, che aggregandosi diversamente producono le varie apparenze con cui si manifesta ciò che si indica, generalmente, con il termine di "realtà".
Democrito si pone a questo proposito una domanda molto intrigante: è possibile estendere agli oggetti materiali il procedimento di suddivisione all'infinito che si immagina di poter eseguire per gli enti geometrici? Se è possibile pensare di suddividere un segmento in un processo senza termine, fino a pervenire a un oggetto senza dimensioni, infinitamente piccolo, il punto geometrico[1], sarà anche possibile pensare di suddividere un oggetto materiale con un analogo processo infinito? Democrito risponde negativamente a questa domanda. L'ente geometrico astratto, il "segmento", permette la conseguente definizione di un ente astratto senza dimen-

1 L'antinomia che il problema della infinita suddivisibilità geometrica inevitabilmente propone non è sconosciuta a Democrito (se gli infiniti punti di cui si compone un segmento hanno dimensione finita, la loro somma non può che fornire un segmento di lunghezza infinita – ciò che non è vero; se poi hanno dimensione nulla, la loro somma non può che dare un segmento di lunghezza nulla – ciò che ancora non è vero). Per Democrito la suddivisone di enti geometrici, essendo riferibili a entità astratte, malgrado la difficoltà menzionata, è perseguibile all'infinito e può essere legittimamente usata per il calcolo di lunghezze, aree, volumi ecc., ma la stessa cosa non è lecita per gli oggetti materiali.

sioni, il "punto geometrico", ma per un ente fisico il processo di suddivisione avrà un termine concreto quando si raggiungeranno i "granuli" (o semi) di cui ogni oggetto materiale è costituito, o anche i suoi "atomi" (= *indivisibili*), secondo l'apposito nome che venne per essi appositamente coniato.
La scienza moderna, come si è detto, ha verificato questa ipotesi e ha costruito su di essa tutta la *teoria atomica*. Ma l'operazione non è stata indolore. La scoperta e lo studio dell'universo microscopico ha aperto, in campo fisico, un'immensa voragine teorica – il termine, in questo caso, non è affatto esagerato – in quanto le evidenze sperimentali hanno costretto a concludere che i fenomeni microscopici obbediscono a leggi nuove e diverse da quelle della fisica classica, con le quali per lungo tempo l'umanità ha creduto di poter spiegare tutta la realtà fisica. Infatti, da un lato si collocano i fenomeni macroscopici classici per i quali il *principio di causalità in senso forte deterministico* è strettamente applicabile, dall'altro i fenomeni microscopici quantistici per i quali il *principio di causalità* della fisica classica viene a cadere.

1.1. Principi e paradossi della fisica quantistica

Nel riquadro, si è voluto evidenziare una delle più eclatanti evidenze in base alle quali si è prodotta la menzionata frattura. Il punto focale fra le due posizioni è tutto racchiuso in tre sole parole atomi più leggeri.
Laplace, estendendo i brillanti risultati ottenuti dalla fisica classica, sostiene che la causalità deterministica vale anche per gli "atomi più leggeri". **Heisenberg**, sulla base delle osservazioni effettuate nella realtà microscopica e delle difficoltà apparentemente insolubili in termini classici ad esse connesse, sostiene che detto principio debba essere fatto cadere, per essere sostituito dal principio di causalità statistica.
Su questo contrasto si apriva un nuovo meraviglioso capitolo della fisica che ebbe l'effetto di imbarazzare e stupire i contemporanei e di continuare a imbarazzare e stupire anche coloro che sono venuti dopo, noi compresi. Infatti, come conseguenza del **principio di indeterminazione**, scoperto ed enunciato da W. Heisenberg, derivano una serie di circostanze che non possono non lasciare perplessi.

Il punto di vista classico
"Una intelligenza che, per un dato istante conoscesse tutte le forze da cui è animata la natura e la situazione reciproca degli esseri che la compongono, se per di più fosse abbastanza profonda per sottoporre questi dati all'analisi, potrebbe abbracciare nella stessa formula i moti dei più grandi corpi dell'universo e degli atomi più leggeri, nulla sarebbe incerto per essa e l'avvenire come il passato, sarebbe presente a suoi occhi".

Laplace PS: *da Essai philosophique sur les probabilités*

Il punto di vista quantistico
"Nella proposizione s*e conosciamo con precisione il presente, possiamo calcolare il futuro* non è falsa la conseguenza, bensì la premessa. Infatti siccome non possiamo partire da alcuna determinazione simultanea di impulso e posizione, la nullità del principio di causalità classica è inappellabile".

Heisenberg W: *da Das Naturbild der heutigen Physik*

Il principio di indeterminazione è il prodotto delle imprecisioni che risultano nella determinazione simultanea della coordinata di posizione "q" e della corrispondente cooordinata coniugata di impulso "p"(*) è almeno eguale alla costante $h/2\pi$.
In formula:

$$\Delta q \, \Delta p \geq h/2\pi$$

dove "h", costante di Planck, vale 6.63×10^{-34} Joule $\times$ secondi.
Data l'estrema piccolezza della costante di Planck questo effetto diventa significativo solo per oggetti di dimensioni microscopiche.

(*) Si ricorda che l'impulso è dato dal prodotto m $\underline{v}$, essendo m la massa e $\underline{v}$ la velocità dell'oggetto materiale considerato

1.1.1. Il principio di indeterminazione

Il principio di indeterminazione di Heisenberg ha, infatti, delle conseguenze di una portata vastissima, tali da sconvolgere le consolidate certezze della più ovvia esperienza quotidiana.
Per riferirsi a una circostanza banale, all'idea che gli elettroni, costituenti ultimi della materia, siano sferette materiali di dimensioni piccolissime si deve aggiungere la constatazione che, pur trattandosi di sferette, hanno un comportamento, quanto meno, molto capriccioso. Ammesso di poter superare le difficoltà di maneggiare oggetti di dimensioni così piccole, nessuno, tanto per fare un esempio ripreso dall'esperienza quotidiana, potrebbe mai, in base al principio di indeterminazione, pensare di giocare a bocce o a biliardo con simili oggetti. Infatti, quando si gioca, ciascuno riconosce le proprie bocce, semplicemente

seguendole con gli occhi durante il loro moto. O meglio, durante il gioco, per tener sotto controllo la situazione, i giocatori sono costretti in continuazione a eseguire "a occhio" misure di posizione e di velocità. E poiché, nel caso delle microbocce, l'individuazione esatta della posizione esclude un'altrettanto esatta individuazione della velocità (e viceversa), è impossibile che con questo metodo giocatori o arbitro possano garantire con certezza l'appartenenza delle varie "microbocce" in gioco. Qualcuno potrebbe proporre, in analogia a ciò che si può fare con le normali bocce macroscopiche, di colorare i vari elettroni per indicarne l'appartenenza. Ma, purtroppo, anche questa possibilità è esclusa. Esiste, nella fisica quantistica, accanto al principio di indeterminazione un altro principio, noto come **principio di indiscernibilità**, in base al quale le particelle microscopiche – e, quindi, anche gli elettroni con cui si è ipotizzato di giocare - risultano *indiscernibili*: ovvero le particelle elementari sono tutte identiche, tanto da non poter essere distinguibili le une dalle altre né con tecniche di colorazione, né con altri sistemi. Come diceva sorridendo il vecchio professore di chi scrive di fisica teorica, "non è possibile tingere di verde un elettrone!"

C'è già, dunque, molta materia per una riflessione. Porzioni piccolissime di materia, che costituisce un solido e sicuro riferimento nell'essere umano al punto che è impossibile, per quest'ultimo, pensare alla realtà fisica se non in termini materiali[2], perdono ogni connotazione di localizzazione e distinzione provocando in esso un senso di vertigine e smarrimento.

Ma allora, sorge spontanea la domanda, che cosa è veramente ciò che viene indicato con l'espressione "realtà fisica"?

Si potrebbe agevolmente mostrare, ma

Se si parte dalla osservazione incontrovertibile che l'unico modo per distinguere due particelle è l'esame delle loro proprietà fisiche, si è necessariamente portati a concludere che due particelle saranno identiche e indistinguibili se le loro proprietà fisiche sono *identicamente* le medesime, in tal caso, infatti, viene a cadere ogni mezzo fisico per distinguerle. In particolare, se si considera una particella come un pacchetto d'onde – principio di complementarietà - è abbastanza agevole trarre la conclusione, visto che le onde non hanno una individualità propria, che, dopo che due particelle A e B hanno interagito, non sarà più possibile distinguere la particella A dalla particella B.
Pertanto, se si indica che la particella 1 si trova nello stato quantico "*m*" con funzione d'onda $\psi_m(1)$ e che la particella 2 si trova nello stato quantico "*n*" con funzione d'onda $\psi_n(2)$, segue che la probabilità di trovare certe coordinate per l'una particella e certe coordinate per l'altra - considerato che la probabilità è calcolabile col quadrato del modulo della funzione d'onda – sarà data da:

$$P(1,2) = |\psi_m(1)|^2 |\psi_n(2)|^2 = |\psi_m(1)\,\psi_n(2)|^2$$

da cui ne discende che esiste una funzione d'onda complessiva per le due particelle che verrà indicata con $\Psi(1,2) = \psi_m(1)\,\psi_n(2)$. Ora, per l'**indiscernibilità** più sopra menzionata, detta funzione d'onda dovrà essere indipendente da uno scambio di particelle (cosa che, per come è stata indicata la $\Psi(1,2)$, non risulta vera). Ma poiché è noto che, se due funzioni d'onda sono soluzioni dell'equazione di Schrödinger che governa l'evoluzione dei sistemi microscopici, anche le loro combinazioni lineari ne sono ancora soluzione, allora è chiaro che la cercata indipendenza dallo scambio di particelle sarà ottenuta considerando le due seguenti combinazioni lineari:

$$\Psi_s(1,2) = A[\psi_m(1)\,\psi_n(2) + \psi_m(2)\,\psi_\beta(1)$$

$$\Psi_a(1,2) = A[\psi_m(1)\,\psi_n(2) - \psi_m(2)\,\psi_\beta(1)$$

Ove Ψ_s è funzione d'onda simmetrica e Ψ_a funzione d'onda antisimetrica per scambio di particelle.
Le funzioni d'onda simmetriche corrispondono a due o più particelle che possono stare nello stesso stato quantico (bosoni), mentre quelle antisimmetriche corrispondono a particelle in cui due o più particelle non possono stare nello stesso stato quantico (fermioni). Sarà interessante notare che il Principio di Esclusione di Pauli, sul quale si fonda la varietà della materia conosciuta, deriva direttamente dalla constatazione che gli elettroni sono fermioni.

Stato quantico e funzione d'onda di un sistema microscopico

Lo stato quantico in cui si può trovare un sistema microscopico è rappresentabile con un vettore dello spazio hilbertiano – opportuna generalizzazione dello spazio euclideo ordinario da utilizzare per gli oggetti del mondo microscopico – e viene indicato col seguente simbolismo $|B>$, dove $B(x, y, z, t)$ rappresenta la *funzione d'onda* relativa allo stato del sistema descritto dalla coordinate x, y, z nel tempo t.

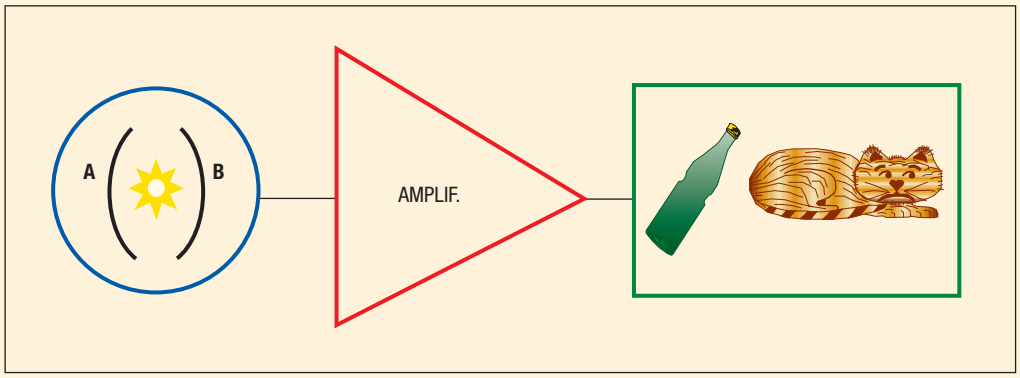
2 Questa affermazione di antichi filosofi in termini moderni deve essere estesa a tutta la realtà fisica che ricade o, direttamente, sotto i nostri sensi o, indirettamente, sotto le possibilità di rivelazione di appropriati ausili strumentali.

questa non sembra a chi scrive la sede adatta, che al principio di indeterminazione corrisponde un'altra singolare circostanza presente nella realtà microscopica, nota come principio di complementarietà. Secondo questo principio, esistono a livello microscopico proprietà complementari tali da escludersi l'una con l'altra, nel senso che la rivelazione dell'una, mediante esperimento, esclude la rivelazione dell'altra. Tali, per fare un esempio, sono l'aspetto corpuscolare e l'aspetto ondulatorio di una particella che, di volta in volta, può essere rivelata nell'una forma (*corpuscolo*) o nell'altra (*onda*), ma mai percepita nella sintesi delle due.

1.1.2. Il principio di sovrapposizione

Ma le sfide e la provocazione della fisica quantistica non si esauriscono qui. Un'altra circostanza, sbalorditiva per l'intuizione sviluppatasi nelle menti umane abituate all'impatto con oggetti macroscopici sottoposti alle leggi della fisica classica, è quanto asserito dal *principio di sovrapposizione*, in base al quale per gli oggetti microscopici è possibile che stati differenti relativi a un determinato ente, possano tranquillamente convivere in uno stato di non-definizione, da intendersi come combinazione lineare dei vari stati in cui esso può venirsi a trovare.
La singolarità di questa possibilità è stata messa in evidenza, in forma particolarmente icastica, dal cosiddetto paradosso del **gatto di Schrödinger**, che non fa altro che riportare gli effetti di questo principio nell'ambito della realtà macroscopica del mondo classico.
Le ragioni di stupore prodotte dalle scoperte della fisica quantistica sono tantissime e spesso, come si è già avuto occasione di osservare, così sconvolgenti da creare un profondo stato di disagio, al punto di portare il grande fisico Heisenberg a osservare che per capire la fisica quantistica bisogna sapersi liberare del pregiudizio classico, di cui ogni essere umano è inevitabilmente prigioniero, in quanto la fisica classica non

Un gatto viene chiuso in una stanza blindata in cui viene collocata una fiala sigillata contenente un gas velenoso. La fialetta è collegata attraverso un opportuno amplificatore con l'interno di un contenitore, dove un atomo in stato di eccitazione si trova situato fra le pareti "A" e "B" di materiale rispettivamente, assorbitore o fotoelettrico.



L'atomo, uscendo dallo stato di eccitazione, emetterà un fotone che andrà a colpire o la parete "A" o la parete "B" del contenitore. Quando il fotone colpisce la parete "A" verrà assorbito senza produrre alcun effetto, quando colpisce la parete "B" viene invece emesso un impulso elettrico che opportunamente magnificato dall'amplificatore riesce con un appropriato congegno a far esplodere la fialetta contenente il gas velenoso provocando la morte del gatto. Ora, in base al principio di sovrapposizione, l'atomo diseccitato si trova in uno stato di sovrapposizione fotone verso destra e fotone verso sinistra, dal quale si potrà uscire soltanto con una misura. Per cui, seguendo la catena degli effetti a cascata e ammettendo di poter descrivere il gatto in termini di vettori dello spazio hilbertiano si dovrà concludere che, finché non viene effettuata la misura, il gatto si troverà in uno stato di sovrapposizione fra vita e morte. Sarebbe, quindi, lo spettatore a far morire il gatto con una semplice osservazione! È la trasposizione del principio di sovrapposizione in ambito macroscopico che porta al paradosso.
Il **gatto di Schrödinger** ha fatto scorrere fiumi di inchiostro sul significato della partecipazione dell'osservatore al processo di misura e sulle implicazioni filosofiche di tipo idealistico che se ne possono dedurre.

è altro che la precisazione in termini matematici e rigorosi dell'esperienza quotidiana del mondo fisico, necessariamente basata su oggetti macroscopici.
Si può tentare di trovare esempi dalla fisica di tutti i giorni con i quali aiutarsi a capire alcune singolarità della fisica del microscopico, ma il gioco può essere pericoloso portando a grossolani errori e incomprensioni. Infatti, la difficoltà a comprendere lo stato di sovrapposizione, viene spesso illustrata con un esempio tratto dal mondo classico. Una moneta, sorteggiata nel gioco di "Testa" o "Croce", mentre ruota in aria, prima di impattare la superficie su cui verrà osservata, può essere assunta come immagine "classica" di uno stato non-definito di sovrapposizione Testa/Croce. Lo stato della moneta, ovviamente, si definisce in maniera stabile soltanto all'impatto - che può essere considerato come l'effettuazione di una misura - sulla superficie del tavolo.
In realtà, l'analogia è vera solo parzialmente. Intanto la moneta, mentre ruota, mantiene sempre ben distinte le due facce. Al limite con una moderna osservazione stroboscopica non sarebbe impensabile vedere a ogni istante una determinata faccia. Nel caso di una particella, viceversa, lo stato di sovrapposizione è proprio uno stato di totale non-definizione, in cui gli stati possibili sono sovrapposti e non-definiti e anche tali da prendere connotazione solo all'atto della misura. Ancora, di fatto lo stato di non definizione della moneta in volo può essere rappresentato con un *vettore di stato* dello spazio ordinario, mentre lo stato di sovrapposizione di una particella microscopica deve essere rappresentato con un vettore di stato dello spazio hilbertiano.
Le due situazioni hanno delle analogie ma sono profondamente diverse. Nel caso della moneta, i due stati sono sempre presenti e prendono forma stabile all'atto dell'impatto, nel caso di una particella microscopica lo stato di sovrapposizione è una "realtà indistinta", una sovrapposizione delle varie possibilità, che prende forma solo con la misura. È, dunque, il processo di misura che permette di configurare una delle varie possibilità altrimenti indistinguibili. Intorno a quest'ultimo concetto è nata una diatriba non ancora del tutto esaurita sul significato profondo dell'operazione di misura in fisica.

1.1.3. Il Paradosso EPR (Einstein-Podolsky-Rosen)

Partendo dalla considerazione che lo *spin* è una grandezza conservativa, si consideri un sistema quantistico costituito da due protoni, fra loro localmente molto vicini e con spin totale nullo. Questa situazione corrisponde ad avere gli spin dei due protoni, misurati lungo una direzione assegnata, orientati in sensi opposti, ovvero, se un protone ha spin $+h/2^{TM}$ lungo una direzione, l'altro avrà necessariamente spin $-h/2^{TM}$ lungo la stessa direzione. Per essere certi di questa situazione non occorre fare alcuna misura, esistono opportuni mezzi per accertarsene. Di fatto, non è neppure conveniente effettuare misure, perché in fisica quantistica le misure perturbano irrimediabilmente il sistema.
Se adesso si immagina che i due protoni si allontanino indefinitamente l'uno dall'altro fino a raggiungere enormi distanze reciproche (anche moltissimi anni luce, se è il caso!) si deve ammettere, per la menzionata conservazione, che la relazione di antiparallelismo degli spin resta conservata. Pertanto, ove si effettui la misura di una componente di spin di una delle due particelle lungo una direzione assegnata, forzandolo in uno stato determinato, necessariamente anche la particella lontana verrà forzata immediatamente in uno stato determinato del suo momento angolare in modo da conservare, lungo la stessa direzione, la relazione di antiparallelismo di partenza. Per indicare questa stretta interdipendenza fra particelle nel mondo anglosassone viene usata l'espressione *entanglement*. Questa azione istantanea a distanza è stata per lungo tempo considerata paradossale, finché J. Bell dimostrò che lo strano effetto, anche se apparentemente paradossale, è effettivamente verificato in natura [9].
Si osservi che il paradosso in esame era per mettere in difficoltà le conclusioni della fisica teorica: di fatto, così veniva argomentato, la possibilità di avere un effetto a distanza in un tempo nullo si configura come una violazione del cosiddetto principio di

località[3]. In realtà, il paradosso citato, non viola il principio di località, in quanto, essendo il risultato della prima misura (quella sul protone vicino) casuale come lo è quello della seconda misura (quella sul protone lontano), non è possibile con l'esperienza descritta, trasmettere informazione fra i due estremi e, quindi, produrre significativi effetti a distanza.
L'esperimento può essere descritto in termini macroscopici in forma più accessibile nel modo seguente. Un signore a Milano e il suo gemello a New York hanno ciascuno in tasca una coppia di palline, una bianca e una nera. Quando il signore di Milano estrae in successione palline bianche e nere con il 50% di probabilità il signore di New York estrarrà necessariamente palline nere e bianche con la stessa percentuale di probabilità. Con un tale procedimento è, ovviamente, impossibile trasmettere informazione fra Milano e New York. Infatti si sa che l'informazione è quella conoscenza passata al destinatario per rimuoverlo da uno stato di incertezza, ma nel caso del gemello di New York l'incertezza non viene diminuita dalla conoscenza della misura del gemello di Milano, dato che si dovrà limitare a ripetere semplicemente un'estrazione casuale[4].
La conferma di questo aspetto "paradossale" ha, tuttavia, una notevole portata e un impatto sconvolgente sul concetto di "realtà" che l'essere umano si è costruito.
In forma molto immaginifica, il fenomeno è stato descritto come un meccanismo secondo il quale due roulette, situate in località con distanze grandi a piacere, forniscono le stesse[5] estrazioni (sincronismo del caso?). Il concetto di separazione, così caro alla fisica classica, viene messo in discussione al punto di far affermare al fisico-filosofo B. d'Espagnat "*Un importante insegnamento della fisica contemporanea* "*fondamentale*" *è che la separazione spaziale degli oggetti è in parte anch'essa* un modo della nostra sensibilità" [3].

2. LA FISICA QUANTISTICA E IL COMPUTER

Si esamina, adesso, come la "nuova fisica" possa introdurre nell'universo del calcolo automatico i suoi strabilianti effetti. Si osserva, intanto, che per lungo tempo non si è data molta importanza alle modalità fisiche secondo le quali un dispositivo di calcolo viene realizzato. Soltanto recentemente, a seguito dell'incessante progresso della tecnologia di realizzazione dei moderni computer, si è cominciato a percepire che la forma fisica secondo cui una macchina di calcolo è realizzata non può non avere un impatto determinante sul suo funzionamento.
Nel corso della seconda guerra mondiale, il semplice passaggio dalla tecnologia elettromeccanica alla tecnologia elettronica consentì agli alleati di infrangere il segreto della mitica macchina criptografica "Enigma" di cui durante la prima parte del conflitto l'esercito tedesco disponeva per mascherare i contenuti delle proprie comunicazioni con decisivo vantaggio strategico. Il cambiamento di tecnologia portò come conseguenza una diminuzione dei tempi elementari di processo di un fattore 1000 (dal millisecondo al micro-

[3] Einstein ha mantenuto fermi due principi ritenendoli inviolabili anche per trasformazioni relativistiche, *il principio di località*, secondo il quale si afferma che ciò che avviene in *A* non può avere alcuna relazione con ciò che avviene in *B* se *A* e *B* sono separati da una distanza $\Delta\ell > c\Delta t$(eventi al di fuori del cono di luce); *il principio di causalità* secondo il quale nessuna trasformazione relativistica può capovolgere la relazione temporale fra causa ed effetto (la causa precede sempre l'effetto).

[4] Per estrema chiarezza si esamina il caso in dettaglio. Se l'estrazione *B* avviene *prima* dell'estrazione in *A*, si tratta inevitabilmente di estrazione casuale; se l'estrazione in *B* avviene simultaneamente a quella in *A* si tratta ancora di estrazione casuale (il "caso" si manifesta in *A* con palla bianca e in *B* con palla nera – e viceversa); se l'estrazione in *B* avviene *posteriormente* a quella in *A*, il risultato in *B* sarà *necessitato* da quello in *A*, ma ancora *casuale*: l'estrazione in *A forza* lo spin del protone facendolo precipitare in uno stato determinato (spin ↑ o spin ↓) *con legge casuale* e l'estrazione in *B mostra* lo spin del protone in uno stato determinato (spin ↑ o spin ↓) *con legge casuale*.

[5] In realtà, sulla base dell'esempio, i valori estratti dalle due roulette sarebbero reciprocamente negati, ma la circostanza non toglie nulla alla conclusione del ragionamento.

secondo!). Fu chiaro che la veste fisica di un computer aveva un effetto così determinante da poter trasformare un problema insolubile in problema solubile.
La questione può essere posta in termini più generali, domandandosi quali sono i limiti di calcolo raggiungibili con una assegnata realizzazione fisica. Esistono dei limiti che per un certo tipo di realizzazione fisica sono invalicabili. La questione è stata brillantemente visualizzata da Vazirani [12]: "*per la fattorizzazione di un numero di duemila cifre non si tratta del caso che non sarebbe possibile far lavorare tutti i computer del mondo per riuscirci* [...] *perché, anche se uno immaginasse che ogni particella dell'universo fosse un computer classico e calcolasse a pieno ritmo per l'intera vita dell'universo, la cosa sarebbe ancora insufficiente a fattorizzare un numero di quelle dimensioni*".
Ma la domanda può essere generalizzata ancora in maniera più drastica, ponendo la questione non in termini di tecnologia impiegata, ma in termini di fisica sottostante alle operazioni elementari di calcolo con cui funziona un computer. Questo imbarazzante versante della domanda è stato affrontato dal fisico Feynman già fin dal 1960 [4], dimostrando che *non c'è possibilità di far funzionare una macchina di Turing*[6] *classica in modo da simulare alcuni processi quantistici senza incorrere in un rallentamento di tipo esponenziale della macchina stessa*.
Poiché il computer si è dimostrato anche un potente ausilio per la simulazione e lo studio di svariate circostanze sperimentali, la conclusione di Feynman non poteva che provocare delusione e sconcerto nella comunità scientifica. Dunque, non si poteva evitare l'amara conclusione che il computer, il meraviglioso strumento che ha cambiato il volto della modernità, ha dei limiti invalicabili nelle sue prestazioni, tali da precluderne l'uso nella simulazione di determinati processi fisici.
Allo stesso tempo, non si poteva eludere neppure l'altra importante questione che si poneva spontaneamente e urgentemente sul tavolo: *è possibile immaginare un computer che funzioni secondo i principi della fisica quantistica*? O anche, *quali trasformazioni possono essere immaginate nel computer e nella grandezza che esso maneggia – l'informazione - ove si decida di riferirsi alla fisica quantistica piuttosto che alla fisica classica*?
A questa seconda possibilità cominciò subito a riflettere lo stesso Feynman [5], tentando di concepire una macchina funzionante sulla base dei principi della fisica quantistica e aprendo in tal modo un nuovo promettente capitolo per l'informatica. Lo scopo e i limiti del presente articolo ci impediscono di entrare in dettaglio sull'argomento che, in una quarantina di anni di ricerche, ha prodotto in ambito teorico notevoli risultati, per i quali si attendono nel prossimo futuro interessanti riscontri sul piano delle applicazioni. Qui basterà dire che tutta la "Teoria della Informazione classica" così come impostata da C. Shannon, è in corso di revisione.
La definizione tradizionale di unità di informazione – il *bit* – che poggia inevitabilmente su assunti di tipo classico, avendo come oggetto di riferimento un dispositivo a funzionamento classico quale un circuito *bistabile*, deve essere rivista ove si faccia riferimento a oggetti a funzionamento quantistico, quali lo spin di un elettrone o la polarizzazione di un fotone. Accanto al bit, basato su fenomeni di tipo classico, si deve collocare il *qu-bit*, la nuova unità di informazione basata su fenomeni quantistici. Il concetto di entropia informativa deve essere opportunamente riveduto, diventa essenziale il concetto di informazione accessibile, ovvero della informazione che effettivamente si riesce a estrarre da un sistema quantistico per effetto di un'operazione di misura, ma, ciò che da un punto di vista pratico è assai più importante, si comincia a valutare la possibilità teorica di concepire sistemi fisici con i quali effettuare operazioni impensabili con le tecniche classiche di computazione. Per fare un esempio, il caso, sopra menzionato, esemplificato da Vazirani per dimostrare l'impossibilità computazionale di problemi a elevata complessità combinatoria in termini classici, diventa solubile se affrontato in termini quantistici, come dimostrato dal celebre lavoro di Shor [10], successivamente confermato con una realizzazione

[6] *La macchina di Turing è il dispositivo teorico immaginato da Turing secondo cui è fondata l'architettura delle moderne macchine di calcolo*.

sperimentale [11], apparentemente risibile – nel contributo si descrive un sistema quantistico mediante il quale si riesce a fattorizzare il numero 15 - ma di grande portata in quanto dimostra la fattibilità, in termini di dispositivi a funzionamento quantistico, di una macchina in grado di risolvere l'arduo problema della fattorizzazione.
Ovvero, dopo questo risultato, le possibilità di risolvere il problema avanzato dal Vazirani diventano più concrete e più vicine.

2.1. Gli effetti quantistici applicati alle macchine di calcolo

Alla base del funzionamento di processi di calcolo molto promettenti stanno alcuni degli effetti quantistici sinteticamente descritti nei precedenti paragrafi. A questo proposito, però, varrà la pena di osservare che l'interesse per il calcolo quantistico non sta nel ripetere procedimenti e calcoli che possono essere eseguiti dai convenzionali computer a funzionamento classico, ma nel fatto che, mediante questa nuova tecnologia, operazioni che risultano impossibili con la tecnica tradizionale possono diventare possibili o, quanto meno, che operazioni eseguibili con scarsa efficienza con il calcolatore classico possono diventare molto più efficienti con la QC (*Quantum Computing*). A. Berthiaume e G. Brassard [1], in un celebre articolo, nel 1992, hanno posto termine alla discussione circa la superiorità del calcolo quantistico su quello classico dimostrando che la QC può battere in efficienza il computer classico sia di tipo deterministico che di tipo probabilistico. Resta, tuttavia, da osservare che i problemi sui quali si fonda la dimostrazione sono piuttosto particolari per cui la conclusione può lasciare qualche perplessità. Fra i problemi non solubili con mezzi deterministici, ma possibili in termini quantistici, si cita il *problema della generazione di numeri veramente casuali e il problema della fattorizzazione di numeri molto grandi*, di altissimo interesse per la criptografia. Ma sono già stati proposti algoritmi quantistici per il *problema della ricerca efficiente in database* (*database search problem*), per il *calcolo dei cicli Hamiltoniani*, per la soluzione del *problema del commesso viaggiatore* e di quello dei *logarimi discreti*. Infine, tutta la *simulazione di fenomeni quantistici*, così importante per l'esplorazione del mondo microscopico, precluso in forma classica, diventa possibile con la QC, come brillantemente presagito dal fisico Feynman.
Qui di seguito verrà esaminato, con maggiore dettaglio, come alcuni dei principi ricordati possano permettere di immaginare stupefacenti applicazioni. Si farà particolare riferimento a due esempi, sui quali la ricerca contemporanea si è particolarmente dedicata, in cui l'uso del computer quantistico consente di risolvere problemi di grande interesse non altrimenti solubili in forma classica.

2.1.1. Il principio di sovrapposizione e il parallelismo quantistico

Un sistema quantistico evolve secondo un'equazione scoperta dal fisico Schrödinger, fino alla effettuazione di una misura, all'atto della quale il sistema collassa in uno dei suoi stati possibili. L'equazione in questione ha la proprietà che la combinazione lineare delle sue soluzioni è ancora una sua soluzione, per cui se il sistema parte da una sovrapposizione di stati farà evolvere nel suo processo di evoluzione tutta la sovrapposizione di stati in blocco.
Si torni per un momento a considerare l'omologo del bit classico, il qu-bit, ossia l'informazione contenuta in un sistema quantistico a due stati, come lo spin di un elettrone.
Dove l'elettrone non sia in uno stato definito, ma in sovrapposizione di stati ↑ (Spin "su") e ↓ (Spin "giù"), qualora si assegni allo stato ↑ (Spin "su") il valore binario "0" e allo stato ↓ (Spin "giù") il valore binario "1", si dovrà concludere che il sistema elettrone si trova in uno stato che rappresenta la sovrapposizione di "0" e "1" – uno stato classicamente inimmaginabile!
Se adesso si procede a costruire un registro costituito da due elettroni, i cui stati stabili di spin saranno quattro (↑↑, ↑↓, ↓↑, ↓↓), corrispondenti ai quattro stati binari (00, 01, 10, 11), ove lo stato del registro non si trovi in uno stato definito, ma in sovrapposizione di stati, si dovrà concludere che il sistema "coppia di elettroni" (= il registro a due elettroni) si troverà in uno stato che rappresenta la sovrapposizione delle coppie di stati

00, 01, 10, 11. E dunque, in un registro a due celle, possono convivere in stato di sovrapposizione tutti e quattro gli stati indicati. Nel registro sono sovrapposti e simultaneamente scritti i simboli 00, 01, 10, 11, estraibili con un'opportuna misura.

Segue una prima importante conclusione: mentre per registrare i quattro valori indicati in forma classica occorrerebbero quattro registri a due celle, in forma quantistica i quattro valori indicati sono contenibili in un solo registro a due celle! E procedendo nella costruzione, un registro a 1 cella può contenere 2^1 valori, un registro a 2 celle può contenere 2^2 valori, un registro a 3 celle può contenere 2^3 valori ... un registro a *n* celle potrà contenere 2^n valori.

La seconda conclusione è la seguente: se il sistema quantistico "registro" viene lasciato evolvere, esso farà evolvere simultaneamente tutti gli stati in sovrapposizione, realizzando una sorta di funzionamento in parallelo per il quale si usa l'espressione parallelismo quantistico[7]. Se l'equazione di evoluzione verrà scelta in modo tale da portare alla soluzione di un determinato problema, tutto ciò che occorrerà fare sarà lasciar evolvere il sistema verso la soluzione desiderata, alla quale esso si porterà, valutando simultaneamente tutti i dati in sovrapposizione fornitigli. Questa tecnica può risultare enormemente vantaggiosa qualora si debba utilizzare il computer per valutare una serie di dati numerosissima.

Si consideri, per esempio, il problema menzionato da Vazirani consistente nella fattorizzazione di un numero grandissimo. Il procedimento teorico, in termini di sovrapposizione quantistica sarà il seguente: si carichi il primo di due registri quantistici eguali con una sovrapposizione di ingressi che rappresentano tutti gli interi compresi fra "o" e $\lceil \sqrt{n} \rceil$ (ossia il primo intero maggiore di $\sqrt{n}$) e il secondo con una sovrapposizione di ingressi che rappresentino tutti gli interi compresi fra $\lceil \sqrt{n} \rceil$ e *n*, essendo *n* il numero di cui si cerca la fattorizzazione. Si lasci evolvere il sistema in modo che esso esegua in *parallelismo quantistico* i prodotti di tutte le coppie dei numeri inseriti nei due registri, allocando i risultati in un terzo registro. Leggendo i risultati su questo terzo registro, quando si riuscisse a trovare il numero *n*, dovrebbe essere possibile risalire alla coppia di numeri cercata che l'ha prodotto.

Tuttavia, la probabilità di trovare il numero corretto sarà in realtà molto esigua, in quanto nel registro le *non-soluzioni* saranno in stato di sovrapposizione con la *soluzione*, rendendo assai ardua l'operazione immaginata.

Per risolvere il problema, occorrerà trovare il modo di far interferire le non-soluzioni in modo da cancellarle: in questo consiste, appunto, la tecnica elaborata da Shor con la quale il problema può essere risolto.

Naturalmente, occorre poter disporre di registri quantistici di appropriate dimensioni, ciò che costituisce un problema tecnologico an-

[7] Non è possibile passare sotto silenzio l'importanza del parallelismo quantistico in grosse questioni scientifiche irrisolte dalle quali emergono contraddizioni insanabili alla luce delle conoscenze attuali. Il parallelismo quantistico è stato, infatti, invocato come possibilità per la soluzione di un rompicapo proposto dalla teoria della evoluzione. Si cita dalla "Rete del fisico" di H.P. Dürr. "*È noto che la teoria della evoluzione di Darwin, che è oggi considerata al di sopra di ogni sospetto, ha qualche difficoltà a spiegare, anche in termini quantitativi, lo sviluppo delle forme di vita, persino le più primitive, dal gioco combinato di pure mutazioni casuali e successive selezioni delle varianti più adatte alla vita. Sebbene sia notoriamente molto difficile valutare in modo affidabile il tempo necessario per un tale meccanismo, qualcosa indica che l'età della nostra terra, calcolata sulla base di considerazioni cosmologiche e geologiche (pari a 4.5 miliardi di anni) sarebbe per questo lungo e faticoso processo troppo breve, di molti ordini di grandezza. Non c'è pertanto da stupirsi se si continuino ad avanzare congetture, secondo le quali non si potrebbe, in ultima analisi, rinunziare ad una componente teleologica nell'evoluzione. Ma i processi quantomeccanici si sviluppano diversamente. Per passare da uno stato ad un altro, non è necessario che i passi intermedi siano reali, essi possono essere semplicemente effettuati in forma virtuale per mezzo del campo quantistico di possibilità le future possibilità di realizzazione vengono in certo qual modo spontaneamente attuate e utilizzate per il processo di sviluppo nel tempo. Con una coerente sovrapposizione di possibilità, uno sviluppo può pertanto procedere in modo più mirato che con una serie di prove incoerenti e casuali di queste stesse possibilità*".

cora irrisolto e di non facile soluzione. Tuttavia, come è stato anticipato la procedura è stata verificata per la scomposizione di un numero molto piccolo ($15 = 5 \times 3$), dimostrando che l'operazione è possibile. L'enorme vantaggio della procedura proposta sta nel parallelismo quantistico che permette di effettuare, per così dire, in un "colpo solo", l'enorme numero di prodotti richiesti per ottenere la fattorizzazione desiderata.
L'uso di due numeri primi molto grandi e del loro prodotto è il fondamento di un moderno processo di criptazione ritenuto molto sicuro per le sopramenzionate ragioni spiegate da Vazirani. La cripto-analisi di un testo criptato con questa tecnologia richiede per l'appunto la fattorizzazione di un numero intero molto grande. È di conseguenza evidente l'enorme interesse che la fattorizzazione di grandi numeri interi possiede per ovvi motivi di sicurezza nazionale e di controllo sociale.

2.1.2. Criptografia assolutamente ermetica

Un altro problema per il quale l'impiego delle proprietà quantistiche sembra schiudere promettenti orizzonti è quello relativo alla soluzione del cosiddetto problema del corriere presente nei sistemi criptografici. Questo problema è[8] relativo al fatto che qualunque trasmissione criptografica protetta include l'inevitabile impiego di un corriere per il trasporto della chiave. E, manifestamente, il corriere è il punto debole di tutto il sistema (esso stesso può "tradire", o, essere sequestrato e costretto a tradire). Non giova pensare al fatto che le due parti possano incontrarsi per lo scambio delle chiavi una volta per tutte, preventivamente a qualsiasi collegamento, perché ovvie ragioni di sicurezza consigliano di cambiare ad ogni collegamento la chiave. Dunque, alle due parti, se vogliono comunicare standosene nella propria sede, non resta altro che affidarsi ad un corriere.

A beneficio del lettore non specialista e per chiarezza di esposizione, verrà ricordato che i sistemi di criptografia hanno notevoli similitudini con una cassaforte, nella quale si possono distinguere relativamente alla sicurezza due aspetti.
a. Quello della sicurezza fisica, rappresentato dalla robustezza del sistema di fronte a effrazioni operate con mezzi fisici (strumenti da scasso di vario genere, lancia termica ecc.). La sicurezza fisica di una cassaforte corrisponde al problema del corriere in un sistema di trasmissione criptografico.
b. Quello della sicurezza logica, rappresentato dalla complessità e non falsificabilità della chiave di apertura. La sicurezza logica di una cassaforte corrisponde al problema di costruire algoritmi matematici sufficientemente complessi tali da non poter essere facilmente violati da chi illegittimamente tenti di infrangere il sistema.
È possibile dimostrare teoricamente che si possono ottenere messaggi criptografati a ermeticità assoluta ove, a ogni sessione, si ricorra a chiavi realizzate con sequenze casuali di dati, in modo da non fornire al criptoanalista della parte avversa "dati storici" su cui poter lavorare. La tecnica di criptazione, qui di seguito illustrata, presenta un procedimento quantistico per realizzare scambio di chiavi tali da produrre assoluta ermeticità.

2.1.2.1. Il canale di Ekert

L'idea, su cui si basa il sistema proposto, è quella che un sistema quantistico può essere descritto come una sovrapposizione di stati stazionari che rimane indeterminata, fino al momento in cui si effettua una misura, la quale ha come effetto di *forzare* il sistema in uno stato definito fra quelli possibili.
Recentemente, A. Ekert [8] sulla base delle considerazioni sopra illustrate, ha proposto un canale criptografico, che sarà indicato come *canale di Ekert*, mediante il quale è possibile trasmettere una chiave criptografica con *ermeticità assoluta*. Il funzionamento è illustrato in figura 1.
Secondo questa proposta, l'utente "*A*" e l'utente "*B*" possono scambiarsi una chiave con l'assoluta certezza della segretezza procedendo nel modo seguente. Una *Sorgente EPR* invia una successione di protoni

[8] Recentemente, sono stati inventati sistemi criptografici a "chiave pubblica", per i quali il problema della chiave può essere eluso. Detti sistemi, basati sulla difficoltà di decomposizione di numeri primi molto grandi, per la quale, come si mostra nel testo, si intravede la possibilità di effrazione con mezzi quantistici, non sono da considerarsi in prospettiva assolutamente ermetici.

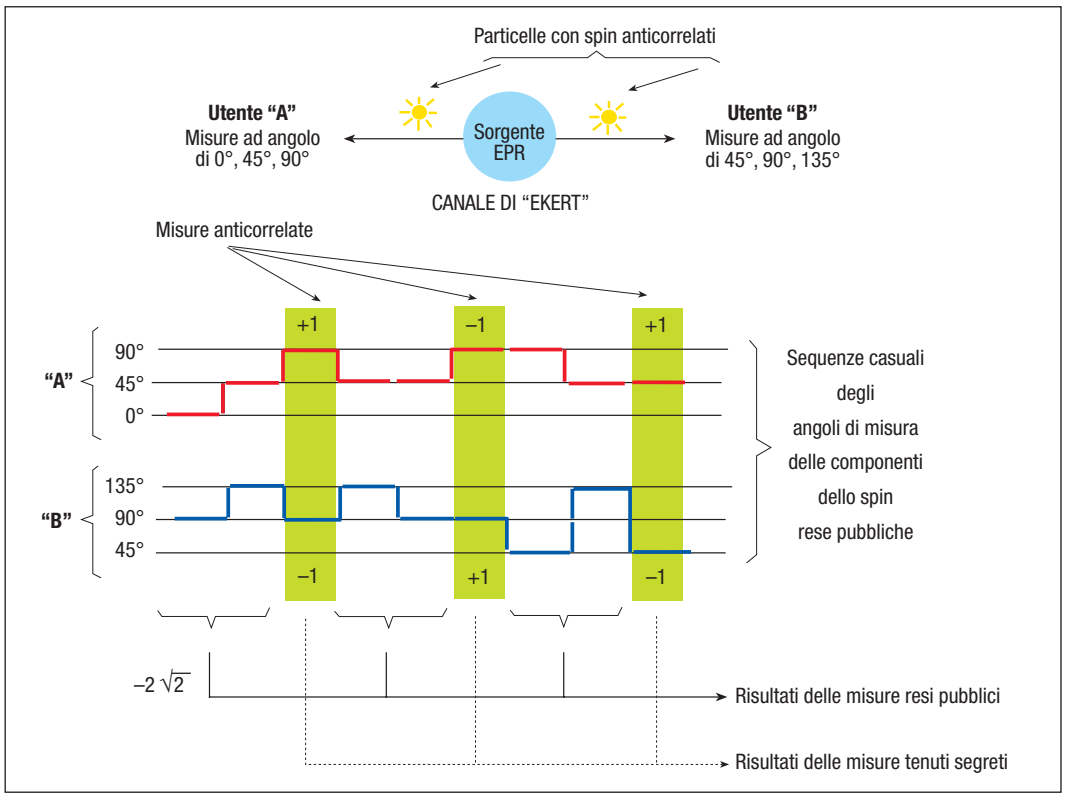


FIGURA 1
Illustrazione schematica del canale di Ekert per trasmissioni assolutamente ermetiche. La sequenza di chiave è data dai risultati delle misure effettuate dalle due parti in contatto lungo le stesse direzioni

prelevandoli da una coppia a momento angolare totale nullo, indirizzandone uno verso l'utente "*A*" e il suo associato verso l'utente "*B*". I due utenti misurano la componente angolare della particella ricevuta secondo angoli perpendicolari all'asse di comunicazione pari a 0°, 45°, 90° (utente "*A*") oppure pari a 45°, 90°, 135° (utente "*B*"). L'angolo di misura viene cambiato per ogni particella ricevuta secondo una sequenza "casuale" (differente per "*A*" e per "*B*") che viene resa di dominio pubblico: in particolare, la pubblicazione delle sequenze degli angoli di misura permette ai due interlocutori in contatto di suddividere le misure che essi effettuano in due classi, quelle compiute da entrambi con angoli concordi e quelle compiute con angoli discordi.

Secondo i risultati della fisica quantistica, se "*A*" e "*B*" misurano il momento angolare delle particelle con lo stesso angolo di orientamento i valori che ottengono sono totalmente anticorrelati (lo stato del protone ricevuto da "*A*" è esattamente l'opposto dello stato del protone ricevuto da "*B*"), se invece "*A*" e "*B*" effettuano le misure con angoli di orientamento differenti il risultato ottenuto – come verificabile sperimentalmente – sarà pari per entrambi a $S = -2\sqrt{2}$. Alla fine del processo di trasmissione, "*A*" e "*B*" rendono pubblici anche i risultati delle misure effettuate con orientamenti discordi, ma tengono rigorosamente segreti i risultati delle misure ottenute per orientamenti concordi. Se durante tutta l'operazione indicata il canale non è stato disturbato (nel senso che non sono state effettuate misure da parte di chicchessia per scopi fraudolenti nell'intento di ricavare informazione, intercettando la particella inviata a uno dei due utenti in contatto, misurandone lo spin secondo un certo orientamento per poi rinviarla al legittimo destinatario) gli utenti "*A*" e "*B*" troveranno il valore $S = -2\sqrt{2}$ per orientamenti discordi, con cui potranno concludere con certezza che non sono stati spiati. D'altro canto, i risultati delle misure per orientamenti concordi, tenuti segreti, costituiranno per entrambe le parti una sequenza, a loro soltanto nota, che potrà essere adoperata come chiave criptografica assolutamente sicura (più precisamente, ciascuna parte avrà la sequenza negata dell'altra parte, ma ciò non costituisce ovviamente difficoltà di sorta).

Con i dati resi pubblici è possibile a un utente illegittimo conoscere gli istanti in cui gli utenti legittimi effettuano misure anticorrelate trasmettendosi la sequenza di chiave, ma detta sequenza non può, da questi essere conosciuta perché tenuta segreta dagli interlocutori autorizzati. Si potrebbe, tuttavia, pensare di compiere un attacco criptoanalitico, senza essere scoperti, effettuando misure, *esattamente negli istanti* in cui "*A*" e "*B*" compiono essi stessi le misure, secondo identici orientamenti. Ma poiché le sequenze degli orientamenti secondo cui si fanno le misure sono casuali, questa possibilità è esclusa.
L'obiezione più ingegnosa che è stata avanzata è quella secondo la quale sarebbe comunque possibile ingannare gli utenti legittimi utilizzando una sorgente *EPR* fasulla in grado di trasmettere tre particelle alla volta, invece che due, procedendo, quindi, a intercettare sistematicamente il terzo fascetto di particelle per immagazzinarlo opportunamente, rinviando la misura degli spin, per non essere scoperti, in un momento successivo alle misure effettuate dai legittimi interlocutori. In tal modo, l'ente intercettatore potrebbe disporre degli stessi dati degli utenti autorizzati mettendosi in grado, sulla base dei dati da questi resi pubblici, di ricostruire la sequenza di chiave di cui essi vengono a disporre. Il problema della conservazione di particelle per memorizzarne lo stato è stato preso in esame nella valutazione della possibilità di costruire una *moneta non falsificabile* [13] e costituisce una difficoltà la cui soluzione pratica non si ritiene attualmente realistica. Di conseguenza, anche la possibilità di ingannare gli interlocutori autorizzati mediante una sorgente *EPR* fasulla non è possibile.

2.2. Problemi di fisica realizzabilità

La realizzabilità fisica di dispositivi per QC è fortemente condizionata da un fenomeno noto come "decoerenza quantistica", ossia l'inevitabile effetto dell'interscambio fra un sistema quantistico e l'ambiente in cui esso è immerso. Per tornare, pur con tutte le cautele del caso, a un parallelismo col mondo classico già menzionato, il fenomeno della decoerenza può essere paragonato all'impatto di una moneta lanciata con la superficie di un tavolo: all'impatto la "sovrapposizione di testa e croce", presente durante il volo conseguente al lancio, scompare immediatamente facendo precipitare la moneta in uno stato definito. Similmente, la sovrapposizione quantistica, per molti versi assai differente dalla sovrapposizione classica di testa e croce nel lancio di una moneta, viene a cadere per effetto della interazione con l'ambiente, in cui il sistema quantistico si trova necessariamente immerso. Lo stupefacente effetto della sovrapposizione degli stati con la conseguente possibilità di ciò che è stato chiamato parallelismo quantistico, viene messo in seria discussione dal fenomeno della decoerenza. Comunque, molti progressi in questa direzione sono stati effettuati ed è da ritenere che in prospettiva il fenomeno delle decoerenza possa essere in qualche modo superato [6].
Qui di seguito, si fornisce qualche informazione sulle tecnologie attualmente allo studio presso i laboratori attivi in questo tipo di ricerche per realizzare dispositivi in grado di funzionare sui principi della fisica quantistica.

2.2.1. Confinamento ionico lineare ("Trapped Ions")

Nel 1995 Cirac e Zoller [2] hanno messo a punto una tecnologia detta di *confinamento ionico lineare* (*trapped ions*). Secondo questa proposta un gruppo di ioni[9] viene sistemato linearmente in un'area di confinamento realizzata mediante opportuno campo elettromagnetico. I due stati stabili dei q-bit, rappresentati dai vari ioni (un q-bit per ione), sono dati dallo stato di riposo dell'ione e dallo stato di eccitazione del medesimo. I singoli ioni (Figura 2) sono allineati come a formare un registro e possono essere singolarmente irradiati mediante impulsi di luce laser. Tali impulsi laser provocano transizioni negli stati ionici eccitandoli convenientemente e, se il caso, posizionando questo particolare registro in uno stato di sovrapposizione.
Gli ioni confinati nel registro hanno tutti la stessa carica ed esercitano l'uno sull'altro

[9] In alcuni esperimenti sono stati usati ioni di Berillio Be^{+}.

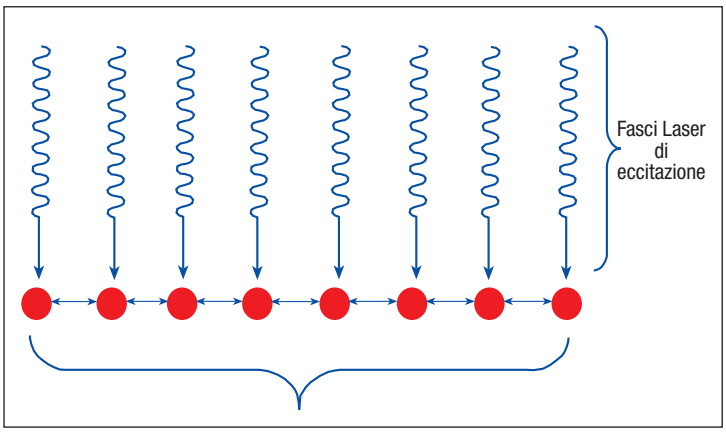


FIGURA 2
Registro a confinamento ionico lineare (trapped ions)

una repulsione mutua di tipo elettrostatico per modo che il movimento di ciascun ione si trasmette a tutti agli altri creando vari possibili movimenti collettivi detti *fononi*. Con singoli raggi laser, come indicato in figura, si può agire sui singoli ioni separatamente in quanto la distanza interionica di separazione fra le particelle è stabilita in modo da essere molto più grande della lunghezza d'onda del laser di eccitazione. A mezzo di opportune manipolazioni è anche possibile realizzare correlazione (*entanglement*) fra le singole coppie di bit. Questo dispositivo costituisce un notevole passo avanti nella tecnologia di realizzazione di computer quantistici: come si vede esso permette di realizzare *bus quantistici*, in via di principio, delle dimensioni volute.
Il tempo di decoerenza per q-bit immagazzinati con confinamento lineare è stato misurato in migliaia di secondi. Il meccanismo di decoerenza più significativo, fra l'altro ancora non perfettamente chiarito, è il riscaldamento dei *modi* dei fononi.
A partire dai risultati sperimentali finora ottenuti è prevedibile che entro i prossimi dieci anni sia possibile realizzare registri a confinamento lineare contenenti qualche decina di ioni. L'ostacolo più significativo che dovrà essere superato è costituito, come già menzionato, dal fenomeno della decoerenza.

2.2.2. Risonanza magnetica nucleare (NMR)

Il metodo della risonanza magnetica nucleare utilizza come supporto per il qu-bit lo spin del nucleo atomico agendo su di esso mediante campi magnetici esterni. È stato possibile con questo sistema realizzare semplici gate logici che agiscono su di un singolo qubit con l'uso dei campi prodotti con radiofrequenze, mediante i quali si può interagire sugli spin con buona precisione. Azioni più complesse dirette ad influenzare mediante un qu-bit molti altri qu-bit hanno trovato difficoltà di implementazione, per la necessità di far sì che gli spin interagiscano fra loro.
I sistemi *NMR* si distinguono per il fatto che il segnale ottenibile da una singola molecola è troppo debole per essere rivelato; è, pertanto, necessario ricorrere a molte molecole per ottenere un segnale utilizzabile. Questa circostanza non costituisce di per sé un problema in quanto per quantità minime di una sostanza chimica si ha a disposizione uno sterminato numero di molecole. La difficoltà nasce dal fatto di riuscire a fare in modo che tutte le molecole nell'effettuare il calcolo partano dallo stesso stato iniziale. Nel 1997, il problema è stato risolto da alcuni ricercatori riuscendo a ottenere uno *stato puro* da una miscela ottenendo in tal modo di far partire il sistema dallo stesso stato. Alcuni ricercatori sono piuttosto scettici sulla possibilità di poter realizzare computer basati sul principio *NMR* funzionanti con molti qu-bit, dato che il rendimento del processo per l'ottenimento dello stato puro diminuisce sensibilmente al crescere del numero delle molecole. Sono segnalati anche problemi relativamente alla possibilità di riuscire a influire sui singoli spin in presenza di numerose molecole.
Si ritiene che sia possibile arrivare in termini temporalmente accettabili alla sperimentazione di computer *NMR* con non più di 6 qubit. Questa dimensione consentirebbe, tuttavia, di risolvere alcuni interessanti problemi e sembra più a portata di mano rispetto a soluzioni ottenute con altre proposte.

2.2.3. Spin nucleare basato sulla tecnologia al silicio

Recentemente, si è avuto notizia [7] della possibilità di realizzare dispositivi per la QC che impieghino la tecnologia dello "stato solido" già collaudata con enorme successo in tutta la moderna tecnologia di produzione elettronica. L'idea è di incorporare gli spin nucleari in un dispositivo elettronico rivelandoli mediante opportune tecniche di controllo. Gli spin elettronici e nucleari sono accop-

piati mediante l'interazione iperfine. Sotto convenienti condizioni è possibile effettuare un trasferimento di polarizzazione fra i due tipi di spin riuscendo a rivelare lo spin nucleare attraverso i suoi effetti sulle proprietà elettroniche del campione. Sono già stati sviluppati dispositivi funzionanti a bassa temperatura su strutture di GaAs/$Al_xGa_{1-x}A_s$ che sono state incorporate in appropriate nanostrutture.
I ricercatori ritengono che la realizzazione di Quantum Computer basati sulla tecnica al silicio sia una eccezionale sfida che vada affrontata data la possibilità di sfruttare l'enorme rendita di posizione conseguibile dalla conoscenza tecnologica accumulata nella fabbricazione di dispositivi elettronici convenzionali allo stato solido. L'intento è quello di raggiungere ancora più piccole dimensioni e maggiore complessità di funzionamento.
La proposta su cui si lavora è quella di utilizzare il silicio Si come *host* e il fosforo ^{31}P come *donor*. A concentrazioni sufficientemente basse e alla temperatura di 1.5 K, è noto che il tempo di rilassamento degli spin elettronici ammonta a migliaia di secondi, mentre il tempo di rilassamento dello spin nucleare del ^{31}P è dell'ordine dei 10^{18} s, presentando quindi ottimi valori per la computazione quantistica. Il sistema proposto è anche in grado di fornire un buon isolamento dei qu-bit da qualsiasi grado di libertà che ne possa provocare la decoerenza. Con la tecnologia proposta diventerebbe possibile realizzare dispositivi per la computazione quantistica codificando l'informazione negli spin nucleari degli atomi "donor" di dispositivi al silicio opportunamente drogati. Le operazioni logiche sui singoli spin verrebbero eseguite applicando campi elettrici esterni e le misure sui valori di spin verrebbero eseguite usando correnti di elettroni polarizzati di spin.

3. SCENARI FUTURI

Cercare di prevedere il futuro è sempre un esercizio rischioso. È, tuttavia, possibile affermare che quaranta anni di studi teorici sull'argomento Quantum Computing forniscono solidi elementi per ritenere che si avranno interessanti ricadute sul piano realizzativo, se non nell'immediato, certamente a breve. L'avvento di computer quantistici "tascabili" non sembra imminente e forse nemmeno interessante. La QC non si pone come tecnologia concorrenziale alle attuali moderne macchine di calcolo in termini di realizzazione (maggiore economia, più ridotte dimensioni ecc.), ma piuttosto in termini di permettere la soluzione di problemi con la tecnica attuale dichiarati non solubili. I primi passi secondo questa modalità di implementazione saranno, pertanto, sicuramente compiuti nella direzione di macchine specializzate nella soluzione di problemi particolarmente ardui, con importanti ricadute sul piano teorico-pratico, non solubili o difficilmente solubili con le tecniche classiche tradizionali.
Si vuole chiudere con un'osservazione, ripresa dal premio Nobel H.P. Dürr, per mostrare come le idee che si sviluppano dalla fisica quantistica possano portare a conclusioni di carattere generale molto interessanti. L'esempio del sorteggio e della decoerenza hanno una evoluzione di direzione opposta a quella che generalmente si incontra nei fenomeni naturali. In questo caso, gli infiniti orientamenti della moneta durante il volo - e della corrispondente sovrapposizione quantistica - all'impatto con il piano del tavolo - con l'ambiente, nel caso quantistico - si riducono a due stati possibili soltanto (dal molteplice al semplice!), procedendo in una direzione di maggior ordine.
"*Orbene*" – osserva il Dürr, a questo proposito, - "*questo processo di ordinamento non avviene soltanto nel procedimento intenzionale che chiamiamo "misura", bensì questa trasformazione del possibile nel fattibile avviene anche senza il nostro intervento. Inoltre, questo continuo processo di coagulazione conferisce significato assoluto al tempo. Lo svolgersi del tempo rispecchia un ininterrotto processo di evoluzione. Perciò l'evoluzione non è in realtà nel tempo, ma piuttosto tempo ed evoluzione sono la stessa cosa, secondo la loro caratteristica natura. Il presente di volta in volta contrassegna il continuo formarsi del reale dal possibile, corrispondendo ad un progressivo processo di ordine*".

Bibliografia

[1] Bethiaume A, Brassard G: *The Quantum Challenge to Complexity Theory*. Proceedings of the 7th. IEEE Conference on Structure in Complexity Theory, 1994, p. 2521-2535.

[2] Cirac JL, Zoller P: Quantum Computation with Cold Trapped Ions. *Physical Review Letters,* Vol. 74, 1995, p. 4091-4094.

[3] d'Espagnat B: *Alla ricerca del Reale*. Boringhieri – Torino, 1983.

[4] Feynman RP: There is Plenty of Room at the Bottom. *Eng. and Science*, Vol. 23, 1960, p. 22-36.

[5] Feynman R: Quantum Mechanical Computers. *Optics News*, Vol. 11, 1985, p. 11-20.

[6] Giulini D, et alii: *Decoherence and the appearance of a classical World in Quantum Theory*. Springer, Berlin 1996.

[7] Kane BE: A Silicon-based nuclear spin quantum computer. *Nature*, Vol. 393, 14 May 1998, p. 133-137.

[8] *Phys. Rev. Lett*. 67, 1991, p. 661-663.

[9] Sakurai JJ: *Meccanica quantistica moderna*, p. 220 e segg. Zanichelli- Bologna 1990.

[10] Shor P: *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*. Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994, p. 124-134.

[11] Vandersypen LKM, et alii: *Experimental realization of Shor's quantum algorithm using nuclear magnetic resonance*. IBM Almaden Research Center, San Josè, CA 95120. Solid styate and photonics Laboratory. Stanford University, Stanford CA 94305-4075. December 2001.

[12] Vazirani U: Conference Sponsored by the Santa Fe Institute, Los Alamos Nat. Lab. and the University of New Mexico, 1994.

[13] Wiesner S: *Sigact news*. Vol. 15, 1983, p. 78-88.

Letture consigliate

Dürr HP: *Das Netz des Physikers*. Gutenberg, Frankfurt 1989.

Feynman RP: *La fisica di Feynman Voume III, Meccanica Quantistica*. Addison Wesely P. Co. London,1970.

Persico E: *Fundamental of Quantum Mechanics*. Prentice Hall, Inc. Englewood Cliffs, N.J.1957.

Sakurai JJ: *Meccanica quantistica moderna*. Zanichelli- Bologna 1990W.

Nolting: *Grundhurs Theoretische Physik: Quantenmechanik*. Wieweg, Wiesbaden 1997.

Williams CP, Clearwater SH: *Explorations in Quantum Computing*. Spreinger-Telos, Berlin, 1997.

Brooks M: *Quantum Computing and Communications*. Springer, London 1999.

Emanuele Angeleri, laureato in Fisica nel 1956 con il massimo dei voti. Esperienza industriale (1956-1986) nel settore nucleare e delle Telecomunicazioni. Docente di Teoria dei Codici (1979-1985) presso la Scuola Superiore di Telecomunicazioni SIP. Professore associato (Università di Milano, 1986) di Teoria della Informazione e della Trasmissione. Autore di numerose pubblicazioni scientifiche e di alcuni libri nel campo della Teoria della Informazione.
eangeleri@tiscalinet.it