IL COMPUTER QUANTICO E IL PRINCIPIO DI INDETERMINAZIONE

Il qbit (quantum bit) rappresenta la più piccola unità di informazione della computazione quantica, una scienza che si occupa della trasmissione dei dati attraverso la luce.
La realizzazione di un computer quantico è legata alla proprietà di polarizzazione di fotoni e, soprattutto, alla capacità che essi hanno di viaggiare in direzioni opposte, comportandosi come se avessero le stesse identità ed occupando virtualmente la medesima posizione contemporaneamente; in poche parole nel mondo dei quanti non esiste né il prima né il dopo, tutto è semplicemente "presente".

La rivista *Nature* riporta la notizia secondo la quale un team di ricercatori di ottica quantistica delle "Sapienza" di Roma, guidati dal prof: Francesco De Martini, docente di Fisica, ha messo a punto la versione quantica della **porta logica NOT.**[1]
Il docente e il suo gruppo hanno utilizzato nella loro ricerca i fotoni e i loro stati di polarizzazione, proprietà legata alla direzione di propagazione di un'onda luminosa.
Un fotone può essere preparato in due stati distinti di polarizzazione che rappresentano lo 0 e l'1, ma le sue proprietà gli possono consentire di rimanere sospeso in uno stato in cui i due valori sono posseduti allo stesso istante.
Ciò può accadere finchè non si effettua una *misurazione*, dopo di che lo stato posseduto dalla particella "collassa", per assumere quindi definitivamente il valore 0 o il valore 1.
Nell'esperimento è stato usato in entrata un fotone preparato in un arbitrario stato quantico polarizzato.
In uscita sono stati prodotti tre fotoni: quello originario, uno ad esso identico e uno che ha rivelato caratteristiche invertite rispetto alle precedenti.
La trasformazione che si è avuta è quella propria della porta logica NOT.
Secondo l'astrofisico giapponese MICHIO KAKN il PC quantico rappresenta "*the ultimate computer*", il computer definitivo, cioè dopo di esso nulla di più potente potrà essere creato.

I quanti si possono definire solo come insieme di rapporti tra il loro stato "reale" e quello "virtuale".
Si diceva prima che i fotoni possono annoverare in sé contemporaneamente i due stati corrispondenti allo 0 e l'1, finchè non viene effettuata una misurazione. E ciò è garantito dal "principio di indeterminazione " di Heisenberg[2], che nasce e si sviluppa all'interno della meccanica quantistica nella prima metà del secolo scorso.
Plank[3], per primo, introdusse il concetto di energia *quantizzata*, secondo il quale l'energia di un'onda elettromagnetica di frequenza *f* (misurata in hertz) varia per multipli interi di un valore minimo $E = hf$.
Nella formula dell'"*energia quantizzata" h* è la costante determinata da Plank che vale $6{,}625 \times 10^{-27}\ erg\,\sec$. A questa quantità minima di energia Plank diede il nome di *quanto di luce*.

---

[1] In un Pc classico le informazioni sono codificate mediante i bit (0,1) di un linguaggio binario ed essi esprimono gli stati *vero* e *falso*.
I circuiti elettronici del calcolatore poi elaborano i dati ed eseguono i calcoli a grande velocità. Tali operazioni sono effettuate dalle **porte logiche.**
La porta NOT è il circuito logico che trasforma lo zero in input in 1 in output e viceversa.
Nel PC quantico la natura delle unità elementari di informazione cambia.
Mentre i bit in un computer classico obbediscono alle leggi delle meccanica newtoniana, i qbit sono particelle che rispondono alle leggi della meccanica quantistica; quindi, oltre ad assumere i valori 0 e 1 , un qbit si può trovare in una sovrapposizione coerente di essi, cioè può rappresentare simultaneamente entrambi gli stati e quindi un PC quantico avrebbe una potenza di calcolo teoricamente infinita
[2] W. Heisenberg (1902 – 1975) Fisico teorico, le sue ricerche hanno contribuito in modo fondamentale all'elaborazione e allo sviluppo della meccanica quantistica, teoria che ha reso possibile un notevole approfondimento nella comprensione della natura. Premio Nobel per la Fisica nel 1932.
[3] M.Plank (1858 – 1947) Fisico teorico, formulò per primo l'ipotesi del "*quanto d'azione*", che rivoluzionò la fisica all'alba del XX secolo. Crebbe in un ambiente colto ed austero; la musica e l'alpinismo furono tra i suoi svaghi principali.

Quindi, in base a questa idea, la luce emessa da una qualsiasi sorgente luminosa si può considerare come costituita da un numero grandissimo di *quanti di luce*.
L'idea di Plank, secondo la quale l'energia di un'onda elettromagnetica sia quantizzata, può essere considerata come un'estensione della concezione atomistica della materia suggerita già da Democrito[4].
Einstein[5] riprese quanto suggerito da Plank e lo espose in un lavoro sull'effetto fotoelettrico[6] del 1905.
I quanti hanno un comportamento simile a corpuscoli che si muovono nel vuoto con velocità della luce *c* e hanno massa nulla[7]. I quanti del campo elettromagnetico furono chiamati *fotoni*.
I *fotoni* annoverano le caratteristiche, da una parte, delle onde elettromagnetiche, dall'altra presentano proprietà simili a quelle di un corpuscolo che si muove nel vuoto con velocità costante *c*.
Punto di partenza della fisica quantistica è il **principio di indeterminazione** enunciato da W. Heisenberg.
Tale principio è diretta conseguenza del fatto che la Fisica prende in considerazione solo le entità che si possono misurare. Nel mondo microscopico questa osservazione porta a considerazioni completamente nuove rispetto a ciò che invece accade nel caso dei fenomeni macroscopici, cioè non più di natura "deterministica".

Spieghiamo ciò con un esempio.
L'osservazione e la misurazione del moto di una palla da biliardo può essere eseguita illuminandola con una sorgente luminosa, senza che il moto stesso venga perturbato.
Ciò non accade se si prende in esame il moto di una particella elementare.
La *quantità di moto*[8] trasportata da un'onda luminosa, che investe la palla, è trascurabile rispetto alla *quantità di moto* della palla stessa, pertanto non ne altera il moto.
Invece, nel caso di una particella elementare, investendola con una radiazione luminosa per poterne determinare la posizione, se ne perturba il moto. Pertanto nel caso di una particella elementare non ha più senso parlare di traiettoria, perché questa non può essere determinata.
Il **principio di indeterminazione** è l'espressione quantitativa di quanto appena detto:
"Se un corpo si muove lungo una retta, non è possibile misurare *contemporaneamente* con precisione grande quanto si vuole, sia la posizione *x* che la *quantità di moto* $\vec{p}$"[9].
In altre parole esso afferma che "non è possibile misurare contemporaneamente e con esattezza le proprietà che definiscono lo stato di una particella elementare"-
Ciò vuol dire che se si determina con precisione assoluta la posizione *x*, si avrà la massima incertezza sulla velocità *v*.
Torniamo alla particella di prima e supponiamo che essa sia piccola al punto tale da non poterne esaminare il moto a occhio nudo. Utilizzando un microscopio sempre più potente si può pensare di individuarne la posizione con sempre maggior precisione.
Ma, così facendo, si deve illuminare la particella con un fascio di luce e, poiché la luce trasporta energia, la particella in esame riceverebbe una piccola spinta che cambierebbe il suo stato di moto.

---

[4]Democrito filosofo greco, vissuto tra il V° e il IV° secolo a. C, massimo esponente della filosofia atomista.
[5] A. Einstein (1879 – 1955), noto come il creatore della relatività, ha contribuito profondamente alla teoria del calore e alla fisica quantistica, per cui è stato giudicato il maggior fisico e filosofo naturale da Newton in poi. Einstein ha partecipato alla lotta dell'umanità contro la guerra e la tirannide. Per i suoi contributi alla fisica teorica ha ricevuto nel 1922 Il Premio Nobel.
[6]Effetto fotoelettrico: emissione di elettroni da parte di una superficie metallica colpite da raggi luminosi (cfr J. Orear - Fisica generale Zanichelli vol.3)
[7] Per comprendere come si possa parlare di corpuscoli di *massa nulla* basta pensare che i quanti del campo elettromagnetico devono muoversi con la velocità delle onde elettromagnetiche. Poiché dalla teoria della relatività segue che la velocità di un corpo con massa di riposo maggiore di zero non può mai raggiungere la velocità delle onde elettromagnetiche, la massa di riposo di un quanto del campo elettromagnetico non può che essere eguale a zero.(cfr. U. Amaldi -Dal pendolo ai quark Zanichelli vol.2)
[8] Per *quantità di moto* si intende il prodotto della massa per la velocità: $\vec{p} = m\vec{v}$
[9] In termini quantitativi il **principio di indeterminazione** assume la seguente forma: $\Delta x \cdot \Delta p = h/2\pi$ con *h* costante di Plank.

Più si illumina la particella, più le si fornisce energia, più si cambia la sua velocità e quindi meno se ne può determinare la velocità di partenza.
Quindi le misure della posizione e della velocità comportano un'indecisione complessiva.
Il meglio che si può fare è determinare le incertezze Δx e Δp delle grandezze *posizione x* e *quantità di moto p*. Allora quanto più piccolo è Δx (cioè quanto più preciso è il valore *x*) tanto più grande è Δp (cioè maggiore è l'imprecisione relativa alla *quantità di moto p*) e viceversa.
Questo limite nella precisione non dipende dagli strumenti, ma dal fatto che, eseguendo la misurazione di *x*, si perturba inevitabilmente il valore di *p*, cioè la velocità del corpuscolo e quindi il suo moto. Δx e Δp dipendono dalla costante di Plank *h* (cfr. nota 9): se essa fosse uguale a zero, allora Δx e Δp potrebbero essere uguali a zero e avrebbe senso parlare di traiettoria del corpuscolo e insieme della sua *quantità di moto.* Ma *h* è diversa da zero, pertanto le indecisioni Δx e Δp non potranno mai essere eguali a zero.
Da un punto di vista concettuale il principio di indeterminazione sostiene che lo scienziato che effettua la misurazione non è mai un semplice spettatore, ma il suo intervento produce effetti non calcolabili, cioè un'indeterminazione non eliminabile.

Il primo ad avere l'idea di usare i fotoni come base per il "*computer quantico*" è stato un giovane fisico, Stephen Wiesner, studente di dottorato a New Jork presso la Columbia University.
Egli, riflettendo sul comportamento dei fotoni e sul principio di indeterminazione, ebbe l'intuizione che la meccanica dei quanti potesse servire a generare banconote a prova di falsario.
Se l'idea di Wiesner risultò troppo "avanzata" e soprattutto troppo dispendiosa per costruire le "banconote quantiche", essa fu ripresa nel 1984 dall'americano Charles Bennett[10] e dal canadese Gilles Brassard[11] per inventare la "*crittografia quantistica*".

Se fosse realizzato il computer quantico, la crittografia ne sarebbe avvantaggiata.
Infatti la caratteristica principale della *crittografia quantistica* risiede nel fatto che è impossibile intercettare un messaggio senza modificarlo e quindi senza lasciare tracce della propria intrusione.
Inoltre, sfruttando le proprietà dei *fotoni,* sarebbe superato il problema dello scambio di chiavi tramite canali insicuri, perché i fotoni approfittano del principio di Heisenberg per mischiare le carte, quando sono costretti a passare attraverso una fenditura. In particolare non si avrà mai la possibilità di sapere esattamente quali fotoni attraverseranno le fenditure chiamate "*filtri di polarizzazione"*.

Facciamo un esempio di come può essere usata la crittografia quantica.

Supponiamo che Alice e Bob siano due personaggi che vogliano spedirsi un messaggio ed immaginiamo che Alice e Bob decidano di usare fotoni polarizzati e canali quantistici (per esempio una fibra ottica) per la loro comunicazione in codice.
Per scrivere il messaggio cifrato e il codice per decifrarlo, Alice sceglie fotoni polarizzati in quattro direzioni diverse: orizzontale (A), verticale (B), a +45° (C), a –45° (D). Alice e Bob possono comunicare inoltre anche attraverso un canale pubblico (il telefono, internet): A questo punto la comunicazione in chiave quantistica avviene in quattro stadi:
Primo stadio – Alice sceglie una sequenza casuale di fotoni polarizzati (ad esempio la sequenza AADCCDBBADCDBA……..) e la registra, prima di inviarla. Bob ha due analizzatori a disposizione: uno (indicato con 1) gli consente di distinguere i fotoni del tipo A e B, cioè quelli polarizzati in direzione orizzontale e verticale, l'altro (indicato con 2) di distinguere i fotoni del tipo C e D, cioè quelli polarizzati in direzioni diagonali opposte. Bob effettua la lettura utilizzando un analizzatore a caso per ogni fotone e avendo cura di registrare la successione degli analizzatori usati (ad esempio 122111212221…….).

[10] Charles Bennett, ricercatore presso i Watson Laboratories della IBM.
[11] Gilles Brassard, fisico presso l'Università di Montreal.

Ogni volta che Bob utilizza l'analizzatore 1 legge correttamente le A e le B di Alice, ma commette un errore del 50% sulle C e sulle D. Viceversa, quando impiega l'analizzatore 2, individua al 100% la giusta sequenza di C e di D, mentre una volta su due sbaglia le A e le B.

Secondo stadio – Dopo aver analizzato una sequenza abbastanza lunga di fotoni, Bob chiama al telefono Alice e le comunica la successione di analizzatori usata (nel nostro caso, 122111212221……), ma non i risultati ottenuti. Alice verifica la sequenza e, sempre al telefono, dice a Bob per quali fotoni la successione risulta compatibile (nel nostro caso la serie è compatibile per i fotoni 1, 3, 7, 9…), tuttavia non gli dice in quale stato di polarizzazione ha inviato i fotoni 1, 3, 7, 9. A questo punto Bob e Alice si concentrano su tali fotoni e trascurano gli altri.

Terzo stadio – Quindi Alice e Bob scelgono un piccolo insieme della sequenza compatibile di fotoni e verificano, sempre attraverso il telefono,se c'è la dovuta corrispondenza tra gli input iniziali inviati da Alice e i risultati ottenuti da Bob. Se tale corrispondenza esiste, Alice e Bob possono trarre la conclusione che nessuno a cercato di leggere il messaggio. Se invece è intervenuto il terzo personaggio della vicenda, lo spione, al quale la letteratura scientifica attribuisce il nome di Eva, ella avrà necessariamente utilizzato la medesima procedura di Bob per leggere la sequenza di fotoni e poi avrà inviato a Bob una nuova successione di fotoni.
Una breve analisi statistica dimostra che, nella fase di lettura, Eva utilizza necessariamente un analizzatore sbagliato nel 50% dei casi e, nella fase di scrittura per Bob, elabora una sequenza sbagliata anch'essa nel 50% dei casi. In altre parole, Bob legge alla fine una successione che, per almeno il 25%, sarà differente da quella che gli aveva inviato Alice. Questo errore è sufficiente a fargli comprendere senza alcun dubbio che qualcuno ha cercato di intercettare il messaggio.

Quarto stadio – Anche senza l'intervento di Eva, la comunicazione tra Alice e Bob sarà macchiata da errori. Tuttavia questi errori possono essere minimizzati a piacere. Cosicché, una volta certi che nessuna Eva ha disturbato la comunicazione, Alice e Bob possono scambiarsi il resto del cifrario e, infine, decrittare il messaggio, con la certezza assoluta non solo che nessuno lo ha letto, ma che hanno realizzato una comunicazione crittografica perfetta.