

# UNIVERSITÀ DEGLI STUDI DI PADOVA

**Dipartimento di Fisica e Astronomia "Galileo Galilei"**

**Corso di Laurea in Fisica**


**Tesi di Laurea**

## Storia del teorema di non-clonazione quantistica


**Relatore**

**Prof. Giulio Peruzzi**

**Laureando**

**Nicolò Giuseppe Magrelli**



**Anno Accademico 2018/2019**

**Sommario**

Il lavoro mira a ricostruire le tappe fondamentali del dibattito intorno alle possibili conseguenze, teoriche e pratiche, delle correlazioni non-locali fra stati quantistici entangled stabilite dal teorema di Bell, che ha portato, all'inizio degli anni '80 del secolo scorso, alla formulazione del teorema di non-clonazione quantistica e alla nascita del nuovo campo di ricerca dell'informazione quantistica. In particolare, viene messo in evidenza il ruolo fondamentale svolto dal teorema di non-clonazione quantistica nel conciliare il carattere non-locale dell'entanglement quantistico con il principio di relatività ristretta, ovvero nell'assicurare l'impossibilità di trasmettere informazioni a velocità superiore a quella della luce nel vuoto.

Nel primo capitolo si introduce il fenomeno dell'entanglement quantistico fra due particelle e si fornisce una dimostrazione del teorema di Bell sul carattere non-locale della meccanica quantistica. Nel secondo si ripercorre invece il dibattito sopracitato esponendo le proposte di sistemi di comunicazione superluminale basati sull'entanglement avanzate, tra fine anni '70 e inizio anni '80, da alcuni giovani fisici di Berkeley e se ne riportano le criticità. Proprio a partire dall'analisi di una di queste proposte, il sistema 'Flash' di Nick Herbert, si giunge, come avvenuto storicamente, alla formulazione del teorema di non-clonazione, cui è dedicato il terzo capitolo. Infine, nel quarto capitolo, vengono esposti il primo protocollo di crittografia quantistica e quello di teletrasporto quantistico, come primi esempi di applicazione del teorema di non-clonazione e dell'entanglement quantistico nell'ambito dell'Informazione.

# Indice

# 1 La non-località della meccanica quantistica

## 1.1 Entanglement quantistico

L'entanglement quantistico è un fenomeno fisico che ha luogo quando due o più particelle vengono generate o interagiscono in modo tale che lo stato quantistico di ciascuna non possa essere descritto indipendentemente dallo stato delle altre.

Ad esempio, nel caso in cui due particelle, ipotizziamo due fermioni, vengano generate in modo tale che il loro spin totale sia nullo, il loro stato di spin lungo un asse generico sarà descritto dalla funzione d'onda:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle\ |\downarrow\rangle - |\downarrow\rangle\ |\uparrow\rangle),$$

appartenente allo spazio di Hilbert composto $H_1 \otimes H_2$, che descrive il sistema complessivo, dove $|\uparrow\rangle$ indica lo stato di spin-up e $|\downarrow\rangle$ lo stato di spin-down.

In particolare, si nota immediatamente che lo stato $|\Psi\rangle$ non è fattorizzabile in stati delle singole particelle 1 e 2 e questo fa sì che, nel momento in cui venga effettuata una misura di spin su una delle due, la proiezione di $|\Psi\rangle$ in uno dei due autostati $|\uparrow\rangle\ |\downarrow\rangle$ e $|\downarrow\rangle\ |\uparrow\rangle$ determini istantaneamente lo stato di spin (lungo lo stesso asse) anche dell'altra particella, a prescindere dalla distanza spaziale che separa le due.

Questo particolare fenomeno aveva spinto Einstein a sostenere, in un celebre articolo del 1935 passato alla storia come argomento EPR (Einstein-Podolsky-Rosen), che la meccanica quantistica non fosse una teoria completa. L'ipotesi fondamentale degli autori dell'articolo consisteva nel principio di località, in base al quale, data la separazione spaziale tra due sistemi, la realtà fisica di uno non poteva dipendere istantaneamente dalle operazioni svolte sull'altro. Nel caso in questione, del tutto analogo a quello in origine considerato da Einstein e i colleghi, la misura dello spin lungo un certo asse, poniamo l'asse x, sulla particella 1, avrebbe proiettato lo stato della seconda in un autostato dello spin lungo x, mentre la misura dello spin lungo l'asse y, sempre sulla prima particella, avrebbe proiettato lo stato della seconda in un autostato dello spin lungo y, differente dal precedente. Inoltre, trattandosi di grandezze fisiche non commutanti, secondo la meccanica quantistica la misura dello spin lungo x sulla particella 1 avrebbe reso completamente indeterminato il valore dello spin lungo y della particella 2, e viceversa nel secondo caso. Di conseguenza, dato che, sebbene non venisse svolta alcuna operazione sulla particella 2, risultava possibile attribuirle due differenti descrizioni fisiche mediante funzioni di stato quantistiche, gli autori concludevano che entrambe le descrizioni in qualche modo tralasciassero qualcosa

e che la descrizione quantistica della realtà fisica mediante le funzioni di stato fosse quindi incompleta. Una teoria completa avrebbe invece fornito una descrizione univoca della realtà fisica e consentito di prevedere sempre con esattezza i risultati delle singole misure, preservandone così l'indipendenza rispetto a qualunque altro evento da queste causalmente sconnesso secondo i princìpi della relatività ristretta.

## 1.2 Il teorema di Bell

Nonostante il successivo tentativo da parte di David Bohm (Meccanica di Bohm-1952) di implementare la teoria quantistica con una variabile addizionale in grado di renderne deterministica, come auspicato da Einstein, la descrizione della realtà fisica, nel 1964 il fisico nordirlandese John Bell dimostrò che qualsiasi teoria fisica, anche a variabili nascoste (i.e. completa) come quella di Bohm, che riproducesse le predizioni della meccanica quantistica, avrebbe dovuto abbandonare il principio di località formulato da EPR.

Nel suo articolo Bell accettava l'ipotesi di località formulata da Einstein, Podolsky e Rosen, e in particolare la richiesta che i risultati di misura su ciascuno dei due sistemi non dovessero essere influenzati dai settaggi dell'apparato di misura lontano, e dimostrava che una qualunque teoria consistente con tale richiesta avrebbe prodotto delle limitazioni sulle correlazioni statistiche fra i risultati di misura riguardanti sistemi entangled come quelli considerati. Tali limitazioni, note come disuguaglianze di Bell, sarebbero però state esplicitamente violate dalla meccanica quantistica e da qualunque sua estensione a variabili nascoste.

Ripercorriamo il ragionamento di Bell in una versione diversa dall'originale ma equivalente.

Consideriamo una coppia di particelle generate nello stato di singoletto di spin $S_{tot} = 0$ e in volo in direzioni opposte.

Supponiamo poi che gli osservatori A e B misurino la componente di spin della propria particella lungo due direzioni arbitrarie individuate rispettivamente dai versori $\mathbf{a}$ e $\mathbf{b}$ . Denotiamo con A il risultato della misura del primo osservatore e con B il risultato della misura del secondo.

Come noto, a meno di una costante $\frac{\hbar}{2}$, i risultati delle misure potranno essere esclusivamente +1 (spin-up) e -1 (spin-down).

Considerando una teoria a variabili nascoste $\lambda$ e supponendo che sia in accordo con il principio di località formulato da EPR, si avrà allora:

$$A(\mathbf{a}, \lambda) = \pm 1, \qquad B(\mathbf{b}, \lambda) = \pm 1,$$

dove la richiesta di località si traduce nell'indipendenza del risultato A per la prima particella dal settaggio b dell'apparato di misura per la seconda particella, e viceversa.

Se $\rho(\lambda)$ è la distribuzione di probabilità del parametro addizionale (o del set di parametri addizionali) $\lambda$, il valore d'aspettazione del prodotto fra i risultati delle due misure sarà dato da:

$$p(\mathbf{a},\mathbf{b}) = \int d\lambda\, \rho(\lambda) A(\mathbf{a},\lambda) B(\mathbf{b},\lambda).$$

Nel caso in cui i due sperimentatori misurino la componente di spin della propria particella lungo lo stesso asse, sappiamo che, poichè $S_{tot} = 0$, i due risultati saranno discordi, ovvero si avrà $A(\mathbf{b},\lambda) = -B(\mathbf{b},\lambda)$. Pertanto, la precedente equazione potrà essere riscritta come:

$$p(\mathbf{a},\mathbf{b}) = -\int d\lambda\, \rho(\lambda) A(\mathbf{a},\lambda) A(\mathbf{b},\lambda).$$

A questo punto si suppone di ripetere più volte l'esperimento cambiando i settaggi dei due apparati di misura. Lo sperimentatore A potrà decidere se misurare la componente di spin lungo $\mathbf{a}$ o lungo $\mathbf{a}'$, mentre lo sperimentatore B potrà decidere se misurare la componente di spin lungo $\mathbf{b}$ o lungo $\mathbf{b}'$.

Combinando i diversi valori di aspettazione per il prodotto fra i risultati delle due misure, potremo allora scrivere:

$$\begin{aligned}
&p(\mathbf{a},\mathbf{b}) - p(\mathbf{a}',\mathbf{b}) + p(\mathbf{a},\mathbf{b}') + p(\mathbf{a}',\mathbf{b}') = \\
&= -\int d\lambda\, \rho(\lambda)[A(\mathbf{a},\lambda)A(\mathbf{b},\lambda) - A(\mathbf{a}',\lambda)A(\mathbf{b},\lambda) + A(\mathbf{a},\lambda)A(\mathbf{b}',\lambda) + A(\mathbf{a}',\lambda)A(\mathbf{b}',\lambda)] = \\
&= -\int d\lambda\, \rho(\lambda)[A(\mathbf{a},\lambda)(A(\mathbf{b},\lambda) + A(\mathbf{b}',\lambda)) - A(\mathbf{a}',\lambda)(A(\mathbf{b}',\lambda) - A(\mathbf{b},\lambda))].
\end{aligned}$$

Notiamo a questo punto che il valore delle espressioni all'interno delle due parentesi tonde potrà essere esclusivamente 0, +2 o -2 e in particolare, se il risultato della prima sarà 0, il risultato della seconda sarà $\pm 2$, o viceversa. Pertanto, dal momento che $\rho(\lambda)$ è una distribuzione di probablità normalizzata, la precedente equazione porgerà:

$$p(\mathbf{a},\mathbf{b}) - p(\mathbf{a}',\mathbf{b}) + p(\mathbf{a},\mathbf{b}') + p(\mathbf{a}',\mathbf{b}') = \pm 2 \int d\lambda\, \rho(\lambda) = \pm 2.$$

Come è facile verificare, considerando i valori medi $\bar{A}(\mathbf{a},\lambda)$, $\bar{A}(\mathbf{a}',\lambda)$, $\bar{B}(\mathbf{b},\lambda)$ e $\bar{B}(\mathbf{b}',\lambda)$ dei vari risultati, tutti in modulo minori di 1, si avrà:

$$|\bar{p}(\mathbf{a},\mathbf{b}) - \bar{p}(\mathbf{a}',\mathbf{b}) + \bar{p}(\mathbf{a},\mathbf{b}') + \bar{p}(\mathbf{a}',\mathbf{b}')| \leq 2 \qquad (Disuguaglianza\, di\, Bell).$$

Consideriamo ora il caso in cui $\mathbf{a}' = \mathbf{b}$ e vi sia un angolo $\vartheta$ sia fra i versori $\mathbf{a}$ e $\mathbf{b}$ che fra i versori $\mathbf{b}$ e $\mathbf{b}'$ in modo tale che l'angolo compreso fra $\mathbf{a}$ e $\mathbf{b}'$ sia pari a $2\vartheta$. In tali condizioni le previsioni della Meccanica Quantistica riguardo ai valori di aspettazione $\bar{p}$ sono i seguenti:

$$\begin{aligned}
\bar{p}(\mathbf{a}, \mathbf{b}) &= -\,\mathbf{a} \cdot \mathbf{b} = -\,cos\,\vartheta \\
\bar{p}(\mathbf{a}', \mathbf{b}) &= -\,\mathbf{a}' \cdot \mathbf{b} = -1 \\
\bar{p}(\mathbf{a}, \mathbf{b}') &= -\,\mathbf{a} \cdot \mathbf{b}' = -\,cos\,2\vartheta \\
\bar{p}(\mathbf{a}', \mathbf{b}') &= -\,\mathbf{a}' \cdot \mathbf{b}' = -\,cos\,\vartheta
\end{aligned}$$

Per valori di $\vartheta$ compresi tra $\frac{\pi}{2}$ e $\pi$ si verifica però che le suddette predizioni quantistiche vìolano la disuguaglianza di Bell poc'anzi ricavata.

Di conseguenza, concludeva Bell nel suo articolo:

> In una teoria in cui vengano aggiunti parametri alla meccanica quantistica per determinare i risultati di misure individuali, senza che cambino le predizioni statistiche, deve esserci un meccanismo attraverso il quale i settaggi di un apparato di misura possano influenzare la lettura di un altro strumento, seppur lontano. Inoltre, il segnale in questione deve propagarsi istantaneamente.

Per qualche anno l'articolo di Bell rimase pressoché ignorato in virtù della scarsa considerazione per le questioni filosofiche e interpretative riguardanti la meccanica quantistica da parte della quasi totalità della comunità scientifica. Fu solo nella seconda metà degli anni '70 che le citazioni dell'articolo cominciarono ad aumentare ed iniziarono a formarsi, intorno al tema, veri e propri gruppi di interesse fra Stati Uniti, Gran Bretagna, Francia e Italia.

In particolare, nel 1975 si formò a Berkeley, in California, un gruppo di discussione informale chiamato 'Fundamental Fysiks Group', cui presero parte molti giovani fisici interessati all'interpretazione della meccanica quantistica e accomunati da una forte passione per la ricerca speculativa.

Fra i membri del nuovo gruppo c'era John Clauser, uno fra i primi ad accorgersi dell'importanza dell'articolo di Bell e primo fisico in assoluto a proporre un esperimento reale in grado di testare i risultati previsti da Bell sulle correlazioni quantistiche. Insieme ad Albert Shymony, professore di fisica e di filosofia della Boston University, e a due suoi studenti, Michael Horne e Richard Holt, Clauser aveva dato una nuova formulazione della disuguaglianza algebrica ricavata da Bell, in modo da renderla più adatta ad un confronto con i dati sperimentali. Così nel 1972, con la collaborazione di Stuart Freedman, un dottorando di Berkeley, aveva messo in pratica presso i

laboratori dell'università il primo 'esperimento di Bell', basato sulla polarizzazione di coppie di fotoni entangled prodotte dalla diseccitazione di atomi di calcio surriscaldati.

Nonostante Clauser sperasse di rovesciare la meccanica quantistica in favore della località, i risultati del suo esperimento confermarono le previsioni quantistiche, costituendo la prima violazione sperimentale della disuguaglianza di Bell.

# 2 Comunicazioni superluminali?

## 2.1 Il Fundamental Fysiks Group

All'interno del Fundamental Fysiks Group si cominciò presto a ragionare sulle possibili implicazioni delle correlazioni a distanza fra particelle entangled teorizzate da Bell e da poco verificate da Clauser. In particolare, era possibile sfruttare tale caratteristica per comunicare a distanza?

In caso affermativo sarebbe stato allora possibile, almeno in linea di principio, inviare messaggi ad una velocità superiore a quella della luce, mettendo in contrasto meccanica quantistica e relatività einsteineana. Inoltre, osservava Nick Herbert, uno dei membri del gruppo, i benefici tecnologici di uno strumento di comunicazione così rapida sembravano tali da rendere interessante un'indagine sul tema non soltanto da un punto di vista puramente filosofico.

Fu così che nel maggio del 1978 un altro membro del gruppo, Jack Sarfatti, ispirandosi alle discussioni sul teorema di Bell, preparò un documento con le caratteristiche tecniche di un "sistema di comunicazione quantistica più veloce della luce".

L'apparecchio di Sarfatti consisteva in una sorgente che emetteva coppie di fotoni entangled verso due rilevatori A e B, collocati ad una reciproca distanza sufficiente a far sì che nessun segnale luminoso potesse viaggiare tra questi prima che ciascuno dei rispettivi osservatori avesse completato le proprie misure sui fotoni entranti. Lo sperimentatore presso il rilevatore A poteva scegliere se lasciare che i fotoni attraversassero una doppia fenditura e producessero la consueta figura d'interferenza su una lastra fotografica, oppure inserire un rilevatore di fenditura sul percorso del fotone per determinare attraverso quale fenditura fosse passato ciascun fotone. Poteva inoltre modulare l'efficienza del suo rivelatore di fenditura: fissandola al 100%, il rilevatore sarebbe stato sempre in grado di determinare attraverso quale fenditura sarebbe passato ciascun fotone e non ci sarebbe quindi stata alcuna figura d'interferenza, mentre fissandola allo 0% la figura di interferenza si sareb-

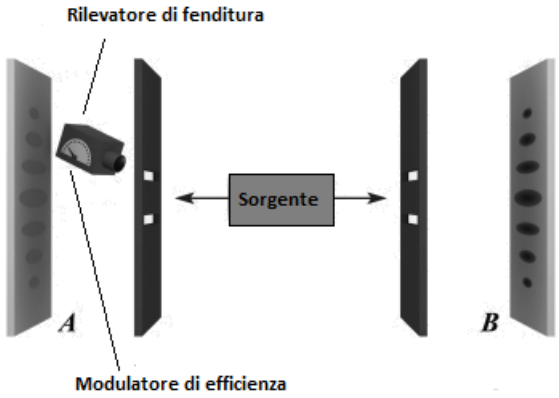


Figura 1: Schema del dispositivo di Jack Sarfatti

be presentata nitidamente. Variando l'efficienza del rilevatore di fenditura, proponeva Sarfatti, lo sperimentatore presso A avrebbe potuto codificare un messaggio per l'altro sperimentatore, posizionato presso il remoto rilevatore B. Infatti, proseguiva Sarfatti, in virtù della correlazione non-locale tra fotoni entangled, il ricevente presso B avrebbe visto la propria figura d'interferenza passare da nitida a sfocata e viceversa nel corso del tempo, man mano che il trasmettitore presso A agiva sull'efficienza del suo rilevatore di fenditura.

Le potenziali applicazioni erano innumerevoli. Innanzitutto, pensava Sarfatti, un apparecchio del genere avrebbe potuto trasmettere la voce umana a grande distanza, senza alcuna possibilità di intercettazione. Se l'efficienza del rilevatore di fenditura presso A fosse stata controllata da qualche trasduttore, per esempio un microfono, allora la figura delle vibrazioni nella voce di chi parla si sarebbe potuta codificare ai diversi livelli di nitidezza della figura d'interferenza della doppia fenditura. Un altoparlante all'altra estremità avrebbe potuto ritradurre in onde sonore i margini delle figure di interferenza ricevuti presso B. Grazie alla rete di contatti del Fundamental Fysiks Group l'idea di Sarfatti iniziò a circolare e a chiarirsi. Poco più tardi, un altro assiduo frequentatore delle riunioni di Berkeley, il fisico Philippe Eberhard, inviò un lungo articolo dal titolo 'Il teorema di Bell e i differenti concetti di località' alla rivista italiana 'Il Nuovo Cimento'.

In esso sottolineava che il teorema di Bell e gli esperimenti di Clauser avevano definitivamente dimostrato che i risultati del rilevatore B dipendevano dal settaggio del rilevatore A – proprio quello che Sarfatti sperava di sfruttare con il suo nuovo apparecchio – però, proseguiva, il fatto che i risultati

dipendessero dal settaggio del rilevatore remoto non significava che si potesse controllare tale relazione di dipendenza per inviare un messaggio intellegibile. Era infatti fondamentale distinguere, secondo Eberhard, il concetto di "località dei processi fisici" da quello di "località relativa agli effetti delle azioni di un osservatore sull'altro". Come dimostrava considerando alcuni esempi, gli effetti delle correlazioni quantistiche proprie di singoli eventi sarebbero sempre state alterate o nascoste alla vista degli osservatori qualora si fosse tenuto conto delle medie tra un elevato numero di simili eventi.

Per quanto riguarda il dispositivo di Sarfatti, questo avrebbe precluso la possibilità di decodificare un eventuale messaggio fra i due sperimentatori, dal momento che qualunque figura d'interferenza, fosse essa netta o sbiadita, sarebbe comunque stata composta da un grande numero di singoli fotoni incidenti sullo schermo.

A questo punto allora Nick Herbert, che, come detto, era stato fin da subito tra i più ferventi sostenitori delle comunicazioni superluminali, si chiese se ci fosse un modo per eludere la dimostrazione di Eberhard, ovvero un qualche sistema in grado di far emergere il segnale superluminale sfruttando singoli eventi quantistici (e non medie statistiche come avveniva nel sistema di Sarfatti). Nella primavera del '79 preparò un documento in cui descriveva un sistema in cui l'informazione veniva codificata attraverso gli stati di polarizzazione di singoli fotoni, come noto legati alla direzione di oscillazione del vettore campo elettrico rispetto a quella di propagazione del fascio luminoso.

In caso di campo elettrico oscillante in una direzione fissa si parla di luce polarizzata linearmente, mentre in caso di campo elettrico ad intensità costante ma con direzione che ruota rispetto all'asse di propagazione si parla di polarizzazione circolare (caso particolare di polarizzazione ellittica, in cui l'intensità del campo può non essere costante). Nel caso, invece, in cui la variazione di direzione del campo elettrico trasportato dall'onda non segua una legge precisa si parla di luce non polarizzata. D'ora in avanti indicheremo con R la polarizzazione circolare destra (rotazione del campo in senso orario, se osservata dalla coda del vettore d'onda), con L la polarizzazione circolare sinistra (senso antiorario), con H la polarizzazione lineare orizzontale (oscillazione del campo lungo l'asse x, una volta fissato il sistema di riferimento) e con V la polarizzazione lineare verticale (lungo l'asse y).

Ispirato ad un esperimento degli anni '30 di Richard Beth, un fisico di Princeton, sulla misura del momento angolare della luce circolarmente polarizzata, il sistema 'Quick' di Herbert si basava sulla differenza tra gli effetti provocati dal passaggio di un fotone polarizzato circolarmente ed un fotone polarizzato linearmente attraverso un congegno chiamato 'half-wave-plate'. Infatti, un fotone polarizzato circolarmente (non importa se R o L ai fini del

progetto), essendo dotato di un quanto di momento angolare, avrebbe, secondo Herbert, fatto ruotare l'half-wave-plate, mentre un fotone polarizzato linearmente no. In questo modo, sfruttando le correlazioni perfette tra coppie di fotoni provenienti da una sorgente comune in uno stato di momento angolare totale pari a zero (come nell'esperimento di Clauser), uno sperimentatore presso A avrebbe potuto determinare istantaneamente, attraverso una misura di polarizzazione circolare o di polarizzazione lineare sul proprio fotone, la rotazione o la quiete di un half-wave-plate situato in un punto dello spazio B, anche remoto, attraverso cui sarebbe transitato il fotone gemello. Infine, un osservatore presso B avrebbe potuto risalire al tipo di misura effettuata in A e leggerne un eventuale messaggio codificato in una successione di misure.

Tuttavia, come mostrò qualche mese più tardi GianCarlo Ghirardi, un fisico italiano che al tempo lavorava al Centro Internazionale di Fisica Teorica di Trieste, il sistema di Herbert avrebbe funzionato in conflitto con un limite quantistico fondamentale, simile al principio di indeterminazione di Heisemberg, il teorema di Wigner-Araki-Yanase.

Secondo quanto stabilito dal teorema, la presenza, in un sistema, di una certa grandezza conservata (come il momento angolare) imporrebbe delle limitazioni al processo di misura, nel caso del 'Quick' rendendo non perfettamente distinguibili gli stati finali dell'half-wave-plate dopo il passaggio del fotone. In altre parole, per funzionare nel modo ideale descritto da Herbert, l'half-wave-plate avrebbe dovuto avere massa infinita: in tal caso, però, il passaggio di un singolo fotone non sarebbe stato sufficiente a farlo ruotare.

Pertanto, se da un lato il fatto di sfruttare singoli eventi quantistici (passaggio di singoli fotoni attraverso l'half-wave-plate) permetteva di eludere l'argomento di Eberhard, dall'altro rendeva impercettibili gli effetti delle correlazioni e di conseguenza impossibile l'identificazione di un eventuale segnale.

## 2.2 Il FLASH

A questo punto allora Herbert cominciò a ragionare sulla possibilità di amplificare le minuscole distinzioni fra i diversi stati quantistici in modo da renderle percettibili agli eventuali osservatori, pur non ricadendo nel caso delle medie statistiche descritto da Eberhard.

Così un anno più tardi presentò una nuova proposta: il 'FLASH' (First Laser-Amplifier Superluminal Hookup).

Il nuovo sistema immaginato da Herbert si basava, come il precedente, sulla distinzione fra i diversi stati di polarizzazione dei fotoni, R, L (polarizzazione circolare), H e V (polarizzazione lineare). In più però si avvaleva del-

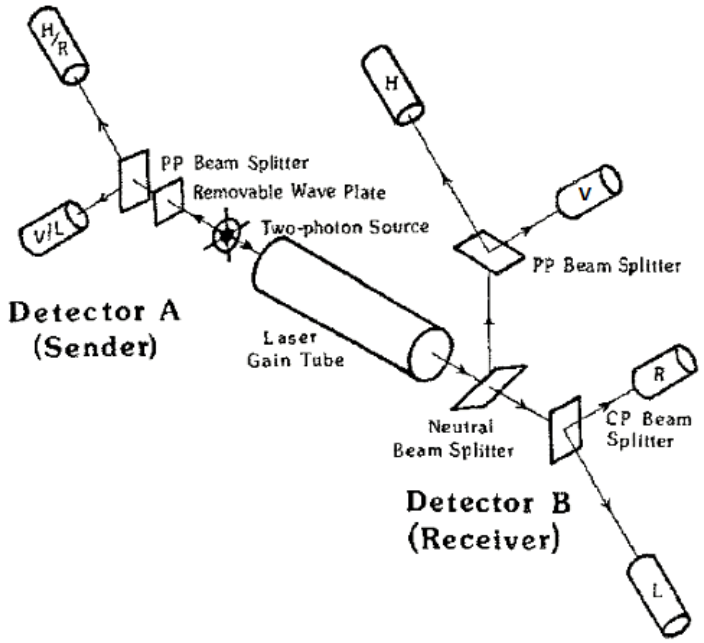


Figura 2: Schema del dispositivo Flash di Nick Herbert

l'effetto di amplificazione di un laser posto fra la sorgente di coppie entangled e uno dei due osservatori, effetto che avrebbe svolto un ruolo determinante nel permettere l'identificazione del segnale superluminale.

Secondo l'idea di Herbert lo sperimentatore A avrebbe effettuato per primo la misura sul proprio fotone, decidendo se misurarne la polarizzazione circolare (trovando R o L) o la polarizzazione lineare (trovando H o V). Di conseguenza, in virtù della correlazione perfetta fra i due fotoni, il fotone in viaggio verso B sarebbe stato forzato nello stato di polarizzazione complementare e quindi dello stesso tipo misurato da A. A questo punto avrebbe inciso sul laser che ne avrebbe restituito, stando ad Herbert, N copie nel medesimo stato di polarizzazione, che avrebbero poi raggiunto lo sperimentatore B, il quale, servendosi di uno specchio semiriflettente, avrebbe diviso in due il fascio in modo da poter infine misurare la polarizzazione circolare per metà dei fotoni e la polarizzazione lineare per l'altra metà.

Supponendo, ad esempio, che A avesse misurato la polarizzazione circolare del suo fotone trovando come risultato L, l'amplificatore avrebbe inviato a B, trascurando il rumore, ovvero i fotoni emessi spontaneamente, un fascio di N fotoni polarizzati R. Effettuando le sue misure, B avrebbe quindi trovato N/2 fotoni R, nessuno nello stato L e mediamente N/4 nello stato H ed

N/4 nello stato V, dal momento che ogni fotone nello stato di polarizzazione circolare destra $|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ avrebbe avuto la stessa probabilità di essere misurato H o V in seguito ad una misura di polarizzazione lineare.

Pertanto, confrontando i quattro conteggi $n_R, n_L, n_H$ ed $n_V$ a sua disposizione, lo sperimentatore B sarebbe potuto risalire al tipo di misura effettuata da A identificando il canale con numero di conteggi nullo, il tutto in un tempo inferiore a quello che avrebbe impiegato un fotone a coprire l'intera distanza AB. In questo modo allora A avrebbe potuto codificare un messaggio binario per B attraverso una serie di misure sui propri fotoni.

Un possibile ostacolo al riconoscimento del segnale, ammetteva Herbert, poteva provenire dal rumore, ovvero dal fenomeno di emissione spontanea di fotoni in uno stato di polarizzazione indefinito da parte del laser. Tuttavia sarebbe stato possibile, secondo Herbert, stimare il rumore analizzando più serie di conteggi ed individuare comunque il segnale come eccesso $|n_H - n_V|$ in caso di misura di polarizzazione lineare da parte di A o come eccesso $|n_R - n_L|$ in caso di misura di polarizzazione circolare.

Herbert propose il suo articolo alla rivista 'Foundations of Physics', una testata relativamente nuova che pubblicava volentieri scritti speculativi su argomenti filosofici, e lo fece diffondere attraverso la rete degli ormai ex membri del Fundamental Fysiks Group.

I pareri dei revisori scelti dalla rivista per lo scritto di Herbert risultarono contrastanti. Ciò nonostante il redattore optò, nel gennaio dell'82, per la pubblicazione di 'Flash'. A convincerlo fu in particolare uno dei revisori, il fisico israeliano Ascher Peres, che raccomandò la pubblicazione dell'articolo di Herbert nonostante fosse convinto che Flash non avrebbe funzionato. Secondo Peres, infatti, l'individuazione dell'errore nel ragionamento di Herbert avrebbe consentito di fare un passo avanti nella comprensione della fisica quantistica. E fu esattamente ciò che avvenne. Qualche mese più tardi, infatti, in seguito all'attenta analisi della proposta di Herbert, gli statunitensi Wootters e Zurek e, separatamente, l'olandese Dieks, pubblicarono le rispettive versioni di quello noto oggi come teorema di non-clonazione quantistica.

# 3 Il teorema di non-clonazione quantistica

Wojciech Zurek e Bill Wootters avevano notato l'articolo di Herbert grazie a John Wheeler, con cui collaboravano presso l'università di Austin, dove entrambi avevano da poco conseguito il dottorato, mostrando spiccato interesse per le questioni di fisica fondamentale. Dieks, giovane fisico di Utrecht, invece, l'aveva ricevuto da un collega appartenente ad un gruppo di discussione libero di Amsterdam, il 'Quantum Club'.

Presto sia Zurek e Wootters che Dieks si convinsero che la questione cruciale risiedesse nella linearità della meccanica quantistica, principio fondamentale che avrebbe impedito all'amplificatore laser del FLASH di funzionare come un perfetto clonatore di stati quantistici.

In particolare, la buona riuscita dell'esperimento di Herbert prevedeva che il laser fosse in grado di clonare arbitrariamente ciascuno dei quattro possibili stati di polarizzazione di un fotone incidente: L, R, H o V.

Tuttavia, supponendo che il laser, inizialmente nello stato $|M_0\rangle$ fosse stato in grado di clonare, ad esempio, i due stati di polarizzazione circolare:

$$|M_0\rangle|L\rangle \longrightarrow |M_L\rangle|nL\rangle$$
$$|M_0\rangle|R\rangle \longrightarrow |M_R\rangle|nR\rangle$$

non sarebbe stato in grado di clonare quelli di polarizzazione lineare. Infatti, dal momento che gli stati di polarizzazione lineare sono legati a quelli di polarizzazione circolare dalle relazioni:

$$|H\rangle = \frac{1}{\sqrt{2}}(|R\rangle + |L\rangle), \qquad |V\rangle = -\frac{i}{\sqrt{2}}(|R\rangle - |L\rangle),$$

in virtù del principio di sovrapposizione si avrà allora:

$$|M_0\rangle|H\rangle \longrightarrow \frac{1}{\sqrt{2}}(|M_L\rangle|nL\rangle + |M_R\rangle|nR\rangle) \neq |M_H\rangle|nH\rangle$$
$$|M_0\rangle|V\rangle \longrightarrow -\frac{i}{\sqrt{2}}(|M_L\rangle|nL\rangle - |M_R\rangle|nR\rangle) \neq |M_V\rangle|nV\rangle.$$

Ovvero, gli stati $|H\rangle$ e $|V\rangle$ di polarizzazione lineare, in quanto particolari combinazioni di stati di polarizzazione circolare, sarebbero evoluti linearmente in combinazioni di copie identiche $|nR\rangle$ ed $|nL\rangle$ dei singoli stati di polarizzazione circolare e non nelle copie di combinazioni:

$$\{\frac{1}{\sqrt{2}}(|R\rangle + |L\rangle)\}^n \equiv |nH\rangle, \qquad \{\frac{1}{\sqrt{2}}(|R\rangle - |L\rangle)\}^n \equiv |nV\rangle.$$

Questo avrebbe impedito al dispositivo di Herbert di distinguere i casi in cui A avrebbe misurato la polarizzazione circolare del proprio fotone da quelli in cui avrebbe misurato quella lineare, rendendo impossibile l'eventuale codificazione di un segnale superluminale. Infatti, se A avesse misurato la polarizzazione lineare trovando H o V, in entrambi i casi l'amplificatore avrebbe inviato a B un fascio di fotoni "polarizzati", con uguale probabilità, o tutti R o tutti L e di conseguenza il canale con zero conteggi (o con un apprezzabile difetto di conteggi, considerando il rumore) sarebbe comunque stato individuato fra uno dei due canali R ed L, esattamente come nel caso in cui A avesse misurato la polarizzazione circolare.

Riassumendo, se l'amplificatore fosse stato in grado di clonare gli stati di polarizzazione circolare dei fotoni, non sarebbe stato in grado di clonare quelli di polarizzazione lineare, e viceversa.

E' importante notare che si sarebbe giunti alla stessa conclusione considerando che l'evoluzione temporale in meccanica quantistica è rappresentata da un operatore unitario, ovvero da un operatore lineare densamente definito in uno spazio di Hilbert che conserva il prodotto scalare fra qualsiasi coppia di stati appartenenti al suo dominio.

Considerando il processo di clonazione questo vuol dire che per ogni coppia di stati clonati con successo $|\psi\rangle$ e $|\phi\rangle$ deve valere:

$$\langle \psi \mid \phi \rangle = \langle \psi \mid \phi \rangle^n$$

Ovvero, se diversi, $|\psi\rangle$ e $|\phi\rangle$ devono essere ortogonali, $\langle \psi \mid \phi \rangle = 0$. Per gli stati di polarizzazione dei fotoni si ha infatti:

$$\langle R|L\rangle = 0, \qquad \langle H|V\rangle = 0,$$

mentre:

$$\langle R|H\rangle \neq 0, \qquad \langle R|V\rangle \neq 0, \qquad \langle L|H\rangle \neq 0, \qquad \langle L|V\rangle \neq 0.$$

Quanto stabilito per l'amplificatore del FLASH vale naturalmente per qualsiasi altra macchina di clonazione quantistica e si può riassumere in questo breve enunciato:

**Teorema di non-clonazione quantistica** *Come conseguenza dell'unitarietà dell'operatore di evoluzione temporale della meccanica quantistica, non è possibile clonare due o più stati quantistici non ortogonali.*

In altre parole, come concludevano Wootters e Zurek nel loro articolo pubblicato da 'Nature' nell'ottobre dell'82:

> Le regole della meccanica quantistica ammettono la clonazione per una coppia o set di stati fra loro ortogonali, ma solo attraverso una macchina di clonazione specificamente costruita per quel set di stati e questa comunque fallirà per qualsiasi altro set di stati. Ciò significa che non è possibile clonare uno stato quantistico arbitrario, dal momento che senza conoscerlo a priori risulta impossibile scegliere la macchina di clonazione adatta.

Data la semplicità della sua dimostrazione, ci si potrebbe chiedere come mai il teorema di non-clonazione quantistica sia stato scoperto solo nel 1982. La risposta va ricercata nel fatto che non fosse consuetudine tra i fisici, fino a quel momento, considerare la meccanica quantistica dal punto di vista dell'informazione e che, come già accennato, dagli anni Quaranta in poi la ricerca sulle questioni di fisica fondamentale fosse stata scarsamente incoraggiata.

D'altro canto, va riportato che un argomento piuttosto simile a quello di Wootters, Zurek e Dieks compare in un controverso articolo del 1970 del fisico statunitense J.L.Park riguardante l'ammissibilità di misurazioni quantistiche 'senza disturbo' sullo stato misurato, articolo rimasto al tempo pressoché ignorato per via del suo esplicito rifiuto dell'interpretazione ortodossa di Bohr e von Neumann.

Allo stesso periodo risale anche uno scritto di Stephen Wiesner, giovane dottorando della Columbia University e amico di Charles Bennett, sull'idea di 'denaro quantistico', in cui l'autore assumeva implicitamente l'impossibilità di clonare stati quantistici non conosciuti a priori per dimostrare la possibilità di produrre banconote impossibili da falsificare, dotate ciascuna di un personale codice costituito da una serie di fotoni in diversi stati di polarizzazione.

# 4 Meccanica quantistica e Informazione: primi sviluppi

## 4.1 Bb84: il primo protocollo di crittografia quantistica

Se nella sua formulazione il teorema di non-clonazione pareva esclusivamente porre un limite alle operazioni ammesse in ambito quantistico, presto invece si rivelò come fondamentale presupposto teorico per lo sviluppo di un campo di ricerca del tutto nuovo: la crittografia quantistica.

Nei primi anni Ottanta Charles Bennett lavorava come fisico esperto di modelli computazionali presso i laboratori di ricerca dell'IBM a Yorktown Heights e aveva da un po' cominciato a concentrarsi sui possibili risvolti della teoria quantistica nell'ambito dell'informazione e della computazione. Era stato compagno di studi di Wiesner alla Brandeis University e i due, rimasti in contatto, avevano di recente riflettuto insieme sulla vecchia idea di Wiesner sul denaro quantistico quando all'inizio del 1983, tramite Wheeler, Bennet conobbe Wootters e Zurek, che gli parlarono del loro recente lavoro sul teorema di non-clonazione. Bennett comprese presto l'importanza di quel risultato e nel giro di un anno elaborò insieme Gilles Brassard, un suo collega di Montrèal, il primo protocollo di crittografia quantistica, noto come Bb84 (Bennett-Brassard 1984).

Il Bb84 è un algoritmo a chiave pubblica, basato cioè sul pubblico scambio di informazioni fra due utenti al fine di condividere una chiave di cifratura comune a partire da altre informazioni tenute invece segrete. A differenza però dei classici sistemi a chiave pubblica, che dovevano la loro sicurezza alla difficoltà pratica di scomporre in fattori primi serie di cifre molto lunghe, il nuovo protocollo di Bennett e Brassard fondava la sua sicurezza proprio sul teorema di non-clonazione, nonchè sulla natura quantistica delle unità di informazione scambiate, originariamente fotoni in stati di polarizzazione non ortogonali.

Supponiamo che un primo utente, Alice, voglia condividere un codice binario con un secondo utente, Bob, utilizzando fotoni polarizzati linearmente (H o V) o circolarmente (R o L):

- Per condividere un bit "0" Alice invierà a Bob, con uguale probabilità, o un fotone polarizzato linearmente H o un fotone polarizzato circolarmente R.

- Per condividere invece un bit "1", Alice invierà a Bob, sempre con uguale probabilità, o un fotone polarizzato linearmente V o un fotone polarizzato circolarmente L.

- Ricevuti i fotoni, Bob potrà decidere se misurarne, di ciascuno e con la stessa probabilità, la polarizzazione lineare o circolare. Di conseguenza, per ciascun fotone avrà probabilità $\frac{1}{2}$ di aver effettuato la misura nella base corretta e probabilità $\frac{1}{2}$ di aver misurato nella base sbagliata. Nel caso Bob abbia misurato nella base corretta, il risultato della misura gli consentirà di risalire al bit di Alice, mentre in caso contrario il risultato della misura gli fornirà un bit casuale.

- A questo punto Bob comunicherà, attraverso un canale pubblico, ad Alice la base utilizzata in ciascuna delle sue misurazioni in modo che entrambi possano scartare i bit corrispondenti ai fotoni misurati in basi diverse.

Nel caso in cui nessuno abbia tentato di intercettare la stringa codificata nei fotoni, i bit rimanenti condivisi da Alice e Bob coincideranno sicuramente e potranno essere utilizzati come chiave di cifratura per un successivo scambio di messaggi sicuro fra i due.

In virtù dell'utilizzo sia di fotoni polarizzati linearmente che di fotoni polarizzati circolarmente, l'eventuale tentativo da parte di una spia di intercettare la stringa di bit produrrebbe invece un disaccordo fra alcuni dei bit selezionati da Alice e Bob (quelli misurati nella stessa base), che potrebbe essere facilmente rivelato attraverso il confronto pubblico (e successivo scarto) di una certa frazione di questi.

Supponendo, infatti, che una spia decidesse di misurare lo stato di polarizzazione dei fotoni in volo da Alice a Bob, avrebbe probabilità $\frac{1}{2}$ di misurare nella base corretta e probabilità $\frac{1}{2}$ di misurare nella base sbagliata. In quest'ultimo caso, altererebbe lo stato di polarizzazione del fotone inducendo, con probabilità $\frac{1}{4}$, un disaccordo fra i bit condivisi da Alice e Bob, che rileverebbero quindi la sua presenza.

Allo stesso modo, se decidesse di copiare i fotoni in volo da Alice e Bob, in virtù del teorema di non-clonazione avrebbe successo mediamente solo in metà dei casi, poiché solo in metà dei casi utilizzerebbe la macchina di clonazione adatta. Inoltre, supponendo che decidesse di tenere per sé il fotone originale e di inviare a Bob la presunta copia prodotta, in metà dei casi invierebbe a Bob un fotone in uno stato di polarizzazione diverso dall'originale, inducendo anche questa volta un disaccordo di $\frac{1}{4}$ fra i bit condivisi da Alice e Bob.

## 4.2 Il teletrasporto quantistico

Come già accennato, la scoperta del teorema di non-clonazione quantistica ed il dibattito ad essa preceduto riguardo le implicazioni del teorema di Bell, favorirono l'incontro fra campi di ricerca fino ad allora separati come la meccanica quantistica e la teoria dell'informazione.

Fra la seconda metà degli anni Ottanta e la prima metà degli anni Novanta, infatti, si fece strada fra fisici e informatici l'idea di utilizzare oggetti fisici come fotoni, atomi o ioni come supporto per delle nuove unità di informazione, i 'qubits'.

A tal proposito, uno dei primi e più importanti risultati nell'ambito dell'informazione quantistica, risalente al 1993, fu l'invenzione del cosiddetto teletrasporto quantistico.

Se, come definitivamente dimostrato, le correlazioni quantistiche fra sistemi entangled non potevano essere utilizzate per trasmettere informazioni a velocità superiore a quella della luce, potevano tuttavia servire per "teletrasportare" uno stato quantistico, ovvero trasferirlo intatto (i.e. con tutta l'informazione in esso originariamente contenuta) da un luogo a un altro, senza la necessità di trasportarlo fisicamente.

Supponiamo, ad esempio, che un primo sperimentatore, Alice, sia in possesso di un sistema in un certo stato quantistico $|\phi\rangle$, ad essa sconosciuto, e che voglia mettere un secondo sperimentatore, Bob, nelle condizioni di riprodurlo esattamente. Se, considerando un caso semplice, quello di Alice consiste in un sistema a due livelli, come per esempio un fotone in un generico stato di polarizzazione lineare, potremo scrivere il suo stato come una generica sovrapposizione dei due stati di base:

$$|\phi_1\rangle = \alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle,$$

con $|\alpha|^2 + |\beta|^2 = 1$.

Supponiamo poi che Alice e Bob condividano una coppia di fotoni entangled descritta, ad esempio, dallo stato:

$$|\Psi_{23}\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle\,|\leftrightarrow\rangle - |\leftrightarrow\rangle\,|\updownarrow\rangle).$$

Sappiamo che, in virtù del postulato di proiezione, in generale una misurazione di Alice sul singolo stato $|\phi_1\rangle$ farebbe perdere l'informazione sullo stato originale forzando $|\phi_1\rangle$ in uno dei due stati di base $|\updownarrow\rangle$ e $|\leftrightarrow\rangle$. Infatti, supponendo che Alice potesse ricavare le informazioni necessarie a riprodurre $|\phi\rangle$, ovvero le ampiezze $\alpha$ e $\beta$, attraverso una misura sulla particella 1, e che

poi le comunicasse a Bob attraverso un canale pubblico, ciò permetterebbe a più persone di riprodurre lo stato $|\phi\rangle$, il che violerebbe il teorema di non-clonazione.

Pertanto Alice effettuerà, anziché una misura sul singolo fotone 1, una misura congiunta, detta 'misura di Bell', sui fotoni 1 e 2, che li proietterà in uno dei seguenti quattro stati entangled:

$$|\Psi_{1_2}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle\,|\leftrightarrow\rangle \pm |\leftrightarrow\rangle\,|\updownarrow\rangle), \qquad |\Phi_{1_2}^{\pm}\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle\,|\leftrightarrow\rangle \pm |\updownarrow\rangle\,|\updownarrow\rangle),$$

che insieme costituiscono una base ortonormale completa per le particelle 1 e 2.

Lo stato completo dei tre fotoni prima della misura di Alice è:

$$|\Psi_{123}\rangle = \frac{\alpha}{\sqrt{2}}(|\updownarrow\rangle\,|\updownarrow\rangle\,|\leftrightarrow\rangle - |\updownarrow\rangle\,|\leftrightarrow\rangle\,|\updownarrow\rangle) + \frac{\beta}{\sqrt{2}}(|\leftrightarrow\rangle\,|\updownarrow\rangle\,|\leftrightarrow\rangle - |\leftrightarrow\rangle\,|\leftrightarrow\rangle\,|\updownarrow\rangle),$$

che può essere riscritto come segue esprimendo ogni prodotto fra gli stati 1 e 2 in termini dei vettori della base di Bell $|\Psi_{1_2}^{\pm}\rangle$ e $|\Phi_{1_2}^{\pm}\rangle$ :

$$\begin{aligned}|\Psi_{123}\rangle = \frac{1}{2}[&|\Psi_{1_2}^{-}\rangle(-\alpha\,|\updownarrow\rangle - \beta\,|\leftrightarrow\rangle) + |\Psi_{1_2}^{+}\rangle(-\alpha\,|\updownarrow\rangle + \beta\,|\leftrightarrow\rangle) \\ &+ |\Phi_{1_2}^{-}\rangle(\alpha\,|\leftrightarrow\rangle + \beta\,|\updownarrow\rangle) + |\Phi_{1_2}^{+}\rangle(\alpha\,|\leftrightarrow\rangle - \beta\,|\updownarrow\rangle)].\end{aligned}$$

Ne segue che, indipendentemente dallo stato $|\phi_1\rangle$ sconosciuto, i quattro possibili risultati della misura di Alice saranno tutti equiprobabili. Inoltre, in virtù dell'entanglement tra i fotoni 2 e 3, dopo la misura di Alice anche il fotone di Bob (il 3) verrà proiettato, a seconda del risultato, in uno dei quattro stati puri della precedente equazione, ovvero:

$$-|\phi_3\rangle \equiv \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \quad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}|\phi_3\rangle, \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}|\phi_3\rangle, \quad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}|\phi_3\rangle.$$

Quindi sarà ora sufficiente che Alice comunichi a Bob, attraverso un canale di comunicazione pubblico, il risultato della propria misura, consistente in due bit di informazione classica, affinchè Bob possa risalire allo stato originario $|\phi\rangle$ del primo fotone applicando un'opportuna trasformazione unitaria al proprio.

Infatti, nel primo caso, lo stato del fotone di Bob corrisponderà a $|\phi\rangle$ al netto di un fattore di fase (-1) irrilevante, mentre negli altri tre casi, per

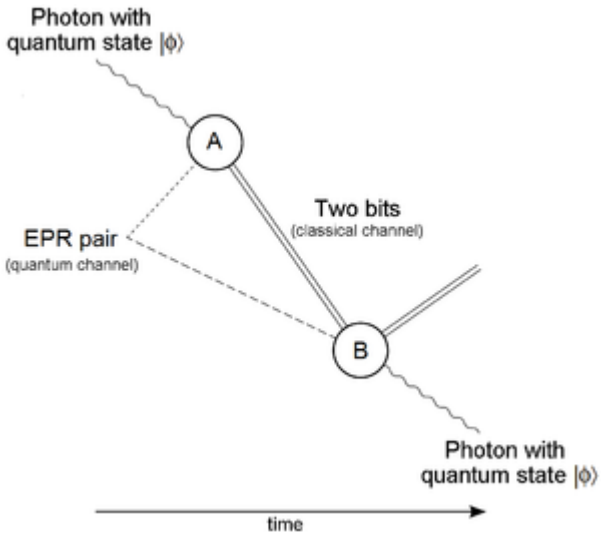


Figura 3: Schema sintetico del protocollo di teletrasporto quantistico

convertire il suo fotone in una replica dello stato originario $|\phi\rangle$, Bob dovrà applicare una delle trasformazioni unitarie sopra riportate, corrispondenti alle rotazioni di 180° rispettivamente attorno agli assi z, x, e y.

Se, come nel caso considerato, $|\phi\rangle$ rappresenta lo stato di polarizzazione del fotone, queste trasformazioni unitarie potranno essere eseguite attraverso delle adeguate combinazioni di 'half-wave plates'.

Solo a questo punto il teletrasporto sarà completato.

Si noti che, in accordo con il teorema di non-clonazione, prima che lo stato $|\phi\rangle$ possa essere riprodotto da Bob è necessario che presso Alice venga definitivamente distrutto: in nessun istante di tempo esisteranno due copie identiche di $|\phi\rangle$. Infatti, quanto rivelato ad Alice dalla misura di Bell sulle particelle 1 e 2 consiste unicamente nei due bit di informazione classica che individuano uno dei quattro stati $|\Psi_{12}^{\pm}\rangle$ e $|\Phi_{12}^{\pm}\rangle$, dunque nulla riguardo i singoli sistemi e, in particolare, riguardo lo stato iniziale $|\phi\rangle$ da teletrasportare.

# Bibliografia


[1] J.S.Bell (1964), *On the Einstein Podolsky Rosen paradox*, Physics 1.

[2] P.Eberhard (1978), *Bell's theorem and the different concepts of locality*, Il Nuovo Cimento 46.

[3] G.Ghirardi, T.Weber (1979), *On some recent suggestion of superluminal communication through the collapse of the wave function*, Lettere al Nuovo Cimento.

[4] N.Herbert (1982), *FLASH - A superluminal communicator based upon a new kind of quantum measurement*, Foundations of Physics 12.

[5] D.Kaiser (2012), *How the hippies saved physics*, Le Navi.

[6] A.Peres (2008), *How the no-cloning theorem got his name*, Department of Physics, Technion - Israel Institute of Tecnology.

[7] B.Wootters, W.Zurek (1982), *A single quantum cannot be cloned*, Nature 299.

[8] C.Bennett, G.Brassard (2014), *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science 560.

[9] C.Bennett *et al.* (1993), *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Physical Review Letters 70.