Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE
Corso di Laurea in Matematica

E91: un protocollo crittografico basato sulla disuguaglianza di Bell

Tesi di Laurea in
Algoritmi della teoria dei numeri e Crittografia

Relatore:
Prof. Davide Aliffi

Presentata da:
Martina Berarducci

Correlatore:
Prof.ssa Elisa Ercolessi

Anno Accademico 2017/2018

Indice

Introduzione

La crittografia quantistica rappresenta una corrente dello studio della crittografia che, come suggerisce il nome, fonda la sua struttura e soprattutto la sua sicurezza su alcuni concetti alla base della meccanica quantistica.

È bene ricordare che lo studio della crittografia si divide in due grandi filoni:

- la crittografia asimmetrica, la quale prevede che ogni attore sia in possesso di una coppia di chiavi, una pubblica che viene distribuita e l'altra privata che invece viene mantenuta segreta, per cui se con una chiave si cifra il messaggio con l'altra si decifra;

- la crittografia simmetrica, che prevede la presenza di una chiave privata in possesso di tutti gli utenti che serve sia per cifrare che per decifrare il messaggio.

Nell'ambito di quest'ultima si inserisce la *crittografia quantistica*, la quale si propone di risolvere il problema dovuto alla necessità dello scambio dell'unica chiave segreta per la comunicazione. Infatti, è opportuno specificare che è più giusto definirla come *Quantum Key Distribution* (QKD). I protocolli di QKD sono esclusivamente utilizzati per generare e distribuire chiavi segrete che poi possono essere utilizzate insieme ad algoritmi di crittografia classica, come il famoso Cifrario di Vernam.

Nel primo capitolo verranno introdotte le nozioni di crittografia classica necessarie alla comprensione del funzionamento del cifrario di Vernam e alla dimostrazione della sua sicurezza perfetta. In questo capitolo buona parte del materiale viene presentato secondo quanto esposto in [1].

Nel secondo capitolo saranno introdotti principi base della meccanica quantistica necessari per la descrizione della versione di Bohm del paradosso EPR e la derivazione della disuguaglianza di Bell proposta dagli studiosi Clauser, Horne, Shimony e Holt, alla base del protocollo di Ekert. Per questa parte si farà riferimento al manuale [5] e agli articoli [6] e [8].

Il terzo capitolo sarà invece interamente dedicato alla descrizione del protocollo E91 e della sua versione successiva. Il lavoro ha interessato lo studio dell'articolo [2] e del manuale divulgativo [9].

Capitolo 1

Crittografia classica

Nella crittografia ci sono tre protagonisti: Alice e Bob che desiderano comunicare segretamente, detti anche mittente e destinatario; Eva, il terzo incomodo, che intende impadronirsi impropriamente del messaggio segreto. In questo capitolo ci occuperemo di introdurre il concetto di *crittografia simmetrica*, anche detta *crittografia a chiave privata*, mettendo in risalto gli aspetti chiave per comprendere la nascita di sistemi crittografici basati sulla meccanica quantistica.

1.1 Crittografia a chiave privata

Prima di iniziare una conversazione segreta è necessario che Alice e Bob si scambino un "codice segreto" che consiste in una chiave, un algoritmo *Enc* per cifrare e uno per decifrare detto *Dec*. Il funzionamento di entrambi gli algoritmi è subordinato all'uso della chiave. Alice utilizza la chiave per cifrare il messaggio e poi lo manda a Bob. Quest'ultimo a sua volta usa la chiave per decifrare il messaggio cifrato e ottenere il messaggio iniziale. Inoltre è necessario aggiungere un altro algoritmo, *Gen*, il quale genera la chiave. Il funzionamento è mostrato in Figura 1.1.

Nell'ottica di questo ragionamento la prima domanda è: quali di queste informazioni devono essere pubbliche e quali private? Nel 1884 Kerchoff diede una risposta con il suo *Principio di Kerchoff* per cui l'unica informazione che deve rimanere segreta è la chiave. Questo ha come conseguenza che non tutti gli algoritmi (*Gen,Enc,Dec*) possono essere deterministici altrimenti Eva sarebbe in grado di calcolare tutto. Infatti *Gen* deve essere casuale.

Definizione 1.1 *Il **sistema crittografico a chiave privata** è una terna di algoritmi (Gen,Enc,Dec) definiti su uno spazio dei messaggi $\mathcal{M}$ e su uno spazio delle chiavi $\mathcal{K}$ tali che valgono i seguenti:*

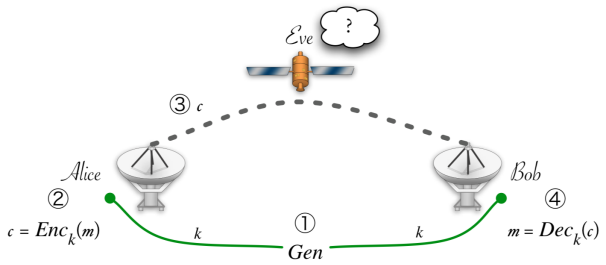
1. *Gen (algoritmo di generazione delle chiavi) è un algoritmo non deterministico che genera la chiave k dove $k \in \mathcal{K}$. Indichiamo con $k \leftarrow Gen$ il processo di generazione di una chiave;*

2. *Enc (algoritmo di cifratura) è un algoritmo potenzialmente probabilistico che, data la chiave $k \in \mathcal{K}$ e un messaggio $m \in \mathcal{M}$, restituisce un testo cifrato c. Indichiamo con $c \leftarrow Enc_k(m)$ il processo di cifratura di m tramite l'algoritmo Enc con chiave k;*

3. *Dec (algoritmo di decifratura) è un algoritmo deterministico che, data la chiave $k \in \mathcal{K}$ e il messaggio cifrato c, restituisce $m \in \mathcal{M}$. Indichiamo con $m \leftarrow Dec_k(c)$ il processo di decifrazione di c tramite l'algoritmo Dec con chiave k;*

4. $\forall\ m \in \mathcal{M}$,
   $Pr[k \leftarrow Gen : Dec_k(Enc_k(m)) = m] = 1$

Figura 1.1: Schema dei passaggi del sistema di crittografia a chiave privata (da [1, Figure 2.1])



I primi sistemi crittografici a chiave privata erano dei *sistemi a sostituzione monoalfabetica*, ovvero utilizzavano un alfabeto per il testo in chiaro e una sua permutazione per il testo cifrato. La permutazione costituiva la chiave del sistema. Chiaramente usando la permutazione inversa del testo cifrato si ricava il messaggio. L'esempio più celebre e anche più antico è il *Cifrario di Cesare*, chiamato così da Giulio Cesare che lo utilizzava per comunicare con i suoi generali. In questo cifrario ogni lettera del messaggio viene sostituita dalla lettera che si trova 3 posizioni dopo nell'alfabeto, e dunque la decifrazione è immediata sostituendo ogni lettera con la lettera dell'alfabeto tre posizioni prima.
Pur non conoscendo la chiave, questo tipo di cifratura monoalfabetica risulta

essere molto semplice da forzare per via della stretta correlazione tra il testo del messaggio originale e il testo cifrato, ad esempio grazie ad un'analisi della frequenza delle lettere nell'alfabeto, e quindi successivamente venne sostituito da quello polialfabetico. I *sistemi a sostituzione polialfabetica* permettono di eliminare il problema della frequenza delle lettere dell'alfabeto, utilizzando tanti "alfabeti" diversi alternati tra loro. Riportiamo l'esempio più semplice di cifrario polialfabetico, descritto da Blaise de Vigenère nel 1586, ritenuto per secoli un sistema inattacabile.

Definizione 1.2 *Sia n numero intero positivo, $m = (m_1, \ldots, m_n)$ e $c = (c_1, \ldots, c_n)$, allora il* ***Cifrario di Vigenère*** *è definito come segue:*

- $\mathcal{M} = \mathcal{K} = (\mathbb{Z}_{26})^n$
- $k \leftarrow (\mathbb{Z}_{26})^n, k = (k_1, \ldots, k_n)$
- $\mathrm{Enc}_k(m_1, \ldots, m_n) = (m_1 + k_1, \ldots, m_n + k_n)$
- $\mathrm{Dec}_k(c_1, \ldots, c_n) = (c_1 - k_1, \ldots, c_n - k_n)$

1.2 Sicurezza di sistemi crittografici

La crittografia moderna, ossia dimostrabile, nacque nel 1949 quando Claude Shannon formalizzò la nozione di crittografia a chiave privata e diede la prima definizione di *sicurezza*.

Definizione 1.3 (Sicurezza di Shannon.) *Uno schema crittografico a chiave privata $(\mathcal{M}, \mathcal{K}, Gen, Enc, Dec)$ si dice* ***sicuro secondo Shannon*** *rispetto alla distribuzione $\mathcal{D}$ sullo spazio dei messaggi $\mathcal{M}$ se $\forall m' \in \mathcal{M}$ e $\forall c$ si ha:*

$$Pr[k \leftarrow Gen; m \leftarrow \mathcal{D} : m = m' \mid Enc_k(m) = c] = Pr[m \leftarrow \mathcal{D} : m = m'],$$

ossia vedere c non influenza la probabilità che il messaggio tramesso sia proprio m'. In altre parole ancora, c non da informazioni su m.

Bisogna notare che m $\leftarrow \mathcal{D}$ significa che m $\in \mathcal{M}$ secondo la distribuzione uniforme $\mathcal{D}$ in $\mathcal{K}$.
Uno schema crittografico ha ***sicurezza di Shannon*** se questa definizione vale $\forall \mathcal{D} \in \mathcal{K}$.

Ora diamo una definizione di sicurezza alternativa la quale richiede che la distribuzione dei testi cifrati per qualsiasi coppia di messaggi sia identica.

Definizione 1.4 (Sicurezza perfetta.) *Una tupla* $(\mathcal{M}, \mathcal{K}, Gen, Enc, Dec)$ *ha* ***sicurezza perfetta*** *se* $\forall m_1, m_2 \in \mathcal{M}$ *e* $\forall c$ *si ha:*

$$Pr[k \leftarrow Gen : Enc_k(m_1) = c] = Pr[k \leftarrow Gen : Enc_k(m_2) = c],$$

ossia c ha la stessa probabilità di provenire da m_1, m_2.

Osservazione 1.5 *Nella Definizione 1.4 non si fa riferimento alla conoscenza a priori dell'avversario, né alla distribuzione dei messaggi.*

Nel seguente teorema mostriamo che le due definizioni di sicurezza date sono in realtà equivalenti.

Teorema 1.6 *Uno schema crittografico a chiave privata ha sicurezza perfetta se e solo se è sicuro secondo Shannon.*

Dimostrazione. Per comodità con $Pr_k[\ldots]$ indicheremo $Pr[k \leftarrow Gen; \ldots]$ e con $Pr_m[\ldots]$ indicheremo $Pr[m \leftarrow \mathcal{D} : \ldots]$ e con $Pr_{k,m}[\ldots]$ invece $Pr[k \leftarrow Gen; m \leftarrow \mathcal{D} : \ldots]$.
($\Longrightarrow$) Supponiamo che lo schema abbia sicurezza perfetta. Consideriamo la distribuzione $\mathcal{D}$ su $\mathcal{M}$, m' $\in \mathcal{M}$ e il messaggio cifrato c. Vogliamo dimostrare che

$$Pr_{\mathrm{k,m}}[m = m' \mid Enc_{\mathrm{k}}(m) = c] = Pr[m = m'] \tag{1.1}$$

Per definizione di probabilità condizionata

$$Pr_{\mathrm{k,m}}[m = m' \mid Enc_{\mathrm{k}}(m) = c] = \frac{Pr_{\mathrm{k,m}}[m = m' \cap Enc_{\mathrm{k}}(m) = c]}{Pr_{\mathrm{k,m}}[Enc_{\mathrm{k}}(m) = c]}$$

che per definizione di sicurezza perfetta può essere riscritto come

$$\frac{Pr_{\mathrm{k,m}}[m = m' \cap Enc_{\mathrm{k}}(m') = c]}{Pr_{\mathrm{k,m}}[Enc_{\mathrm{k}}(m) = c]}$$

e a sua volta si può scrivere come

$$\frac{Pr_{\mathrm{m}}[m = m']Pr_{\mathrm{k}}[Enc_{\mathrm{k}}(m') = c]}{Pr_{\mathrm{k,m}}[Enc_{\mathrm{k}}(m) = c]}.$$

Rimane dunque da dimostrare che

$$Pr_{\mathrm{k,m}}[Enc_{\mathrm{k}}(m) = c] = Pr_{\mathrm{k}}[Enc_{\mathrm{k}}(m') = c].$$

Riscriviamo il termine a destra e applichiamo la definizione di sicurezza perfetta:

$$\sum_{m'' \in M} Pr[m = m'']Pr_{\mathrm{k}}[Enc_{\mathrm{k}}(m'') = c] = \sum_{m'' \in M} Pr[m = m'']Pr_{\mathrm{k}}[Enc_{\mathrm{k}}(m') = c].$$

Sostituendo a (1.1) e semplificando si conclude.
($\Longleftarrow$) Si dimostra in modo analogo. □

1.3 Il cifrario di Vernam e Teorema di Shannon

In questa sezione descriveremo il *cifrario di Vernam*, basato sul cifrario di Vigenère con l'aggiunta che la chiave di cifratura sia lunga quanto il testo e non riutilizzabile. Tale sistema, inventato da Gilbert Vernam nel 1917 e poi brevettato da Joseph Maubourgne nel 1919, è anche chiamato *OTP*, acronimo per One Time Pad (letteralmente "cifrario monouso"), ed è famoso per essere l'unico cifrario a sicurezza perfetta. Tuttavia, il cifrario di Vernam presenta un importante svantaggio: per comunicare in sicurezza occorre aver preventivamente inviato la chiave attraverso un canale che deve essere sicuro. Dunque, il protocollo E91, che verrà analizzato in questo elaborato, ha l'obiettivo di completare quest'ultimo proponendo una soluzione al problema della distribuzione della chiave: utilizzando principi alla base della meccanica quantistica, permette di stabilire una chiave comune senza passare attraverso un canale sicuro e allo stesso tempo evitando che questa possa essere intercettata da Eva.

Definizione 1.7 *L'operazione di* ***XOR*** *in* $\mathbb{Z}_2$ *viene indicata con il simbolo* $\oplus$ *il quale indica la somma modulo 2.*

Definizione 1.8 *Lo* ***schema crittografico One-Time Pad*** *è descritto dalla tupla* $(\mathcal{M}, \mathcal{K}, Gen, Enc, Dec)$*, dove:*

- $\mathcal{M} = \mathcal{K} = \{0,1\}^n$
- $k \leftarrow \{0,1\}^n, k = (k_1, \ldots, k_n)$
- $\mathrm{Enc}_k(m_1, \ldots, m_n) = (m_1 \oplus k_1, \ldots, m_n \oplus k_n)$
- $\mathrm{Dec}_k(c_1, \ldots, c_n) = (c_1 \oplus k_1, \ldots, c_n \oplus k_n)$

Teorema 1.9 *Il cifrario di Vernam ha sicurezza perfetta.*

Dimostrazione. Bisogna fare due osservazioni.

Osservazione 1.10 $\forall c, m \in \{0,1\}^n$ *esiste un solo* k *tale che* $Enc_k(m) = m \oplus k = c$*, ossia* $k = m \oplus c$*. Dunque si ha che:*

$$Pr[k \leftarrow \{0,1\}^n : Enc_k(m) = c] = 2^{-n}$$

Si può quindi concludere che $\forall m_1, m_2 \in \{0,1\}^n$ e $\forall c$,

$$Pr[k \leftarrow \{0,1\}^n : Enc_k(m_1) = c] = Pr[k \leftarrow \{0,1\}^n : Enc_k(m_2) = c]$$

□

Quindi abbiamo dimostrato che il cifrario di Vernam è perfettamente sicuro, e quindi per il Teorema 1.6 è anche sicuro secondo Shannon. Tuttavia presenta alcuni problemi pratici, primo fra tutti il fatto che la chiave deve essere lunga quanto il messaggio. Questo aspetto è sfortunatamente legato alla definizione di sicurezza perfetta, come vedremo nel seguente Teorema.

Teorema 1.11 (Teorema di Shannon.) *Se uno schema crittografico a chiave privata $(\mathcal{M}, \mathcal{K}, Gen, Enc, Dec)$ è sicuro secondo Shannon (o equivalentemente perfettamente sicuro), allora $|\mathcal{K}| \geq |\mathcal{M}|$.*

Dimostrazione. Supponiamo per assurdo che esista uno schema crittografico a chiave privata $(\mathcal{M}, \mathcal{K}, Gen, Enc, Dec)$ tale che $|\mathcal{K}| < |\mathcal{M}|$. Sia $m_1 \in \mathcal{M}, k \in \mathcal{K}$ e $c \leftarrow Enc_k(m_1)$. Definiamo **Dec**(c) l'insieme di tutte le possibili cifrature di c. Questo ha cardinalità almeno $|\mathcal{K}|$ poiché l'algoritmo Dec è deterministico. Ma abbiamo supposto che $(\mathcal{M}, \mathcal{K}, Gen, Enc, Dec)$, quindi esiste almeno un $m_2 \notin$ **Dec**. Allora si ha:

$$Pr[k \leftarrow \mathcal{K} : Enc_k(m_2) = c] = 0. \tag{1.2}$$

Invece per m_1

$$Pr[k \leftarrow \mathcal{K} : Enc_k(m_1) = c] > 0, \tag{1.3}$$

e quindi concludiamo che (1.2) e (1.3) sono diverse, contraddicendo l'ipotesi di sicurezza perfetta. □

La dimostrazione del Teorema di Shannon rappresenta un vero e proprio attacco dell'avversario, ed è possibile verificare che già nel caso in cui la chiave ha un bit in meno del messaggio il vantaggio dell'avversario non è trascurabile.

Il problema della lunghezza della chiave porta automaticamente al problema preso in analisi dalla crittografia quantistica. Come abbiamo già detto, è necessario che Alice e Bob prima di iniziare la comunicazione si scambino la chiave in segreto, ma questa chiave deve avere la stessa lunghezza del messaggio, e questo può risultare molto complicato. Quello che ci permette di fare il protocollo di distribuzione delle chiavi E91 è di produrre chiavi condivise in modo sicuro.

Capitolo 2

Introduzione alla meccanica quantistica

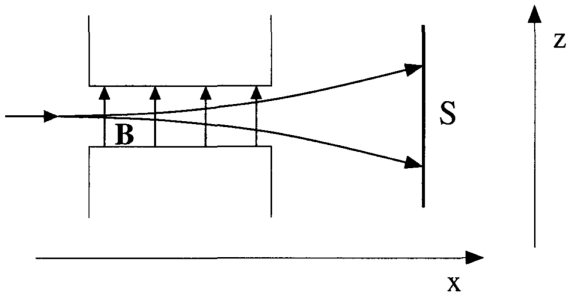
In questo capitolo introdurremo i concetti fondamentali alla base della meccanica quantistica, soffermandoci sugli aspetti chiave per la comprensione del protocollo di Ekert. Innanzitutto si farà una breve analisi di uno degli esperimenti più importanti in tale ambito, che mette in luce alcuni dei tratti distintivi di questa nuova teoria. A seguire, verranno ripresi concetti base dell'algebra lineare in spazi di Hilbert, introducendo il formalismo della meccanica quantistica, e saranno enunciati i postulati alla base di questa teoria. Infine verranno analizzati nel dettaglio la versione di Bohm del paradosso EPR e la disuguaglianza di Bell proposta da Clauser, Horne, Shimony e Holt, esattamente le due esperienze a cui Ekert fa riferimento per lo schema di base e per la sicurezza del suo protocollo.

2.1 L'esperimento di Stern e Gerlach

In questo paragrafo descriveremo l'esperimento condotto nel 1921 dai fisici Otto Stern e Walther Gerlach che portò alla scoperta di una proprietà degli elettroni che non può essere spiegata dalla meccanica classica: lo spin. Inoltre, analizzeremo alcune proprietà che lo spin mostra di possedere se sottoposto a misure sequenziali.

In questo esperimento degli atomi d'argento vengono condotti in una regione in cui c'è un campo magnetico non omogeneo diretto lungo l'asse z. All'uscita della zona di influenza del campo magnetico, è inserito uno schermo, perpendicolarmente alla direzione di propagazione degli atomi, il quale registra l'arrivo delle particelle. Il seguente schema è rappresentato in Figura 2.1.

Figura 2.1: Schema esperimento Stern e Gerlach. **B** indica il campo magnetico, **S** lo schermo. Tratto da [5]

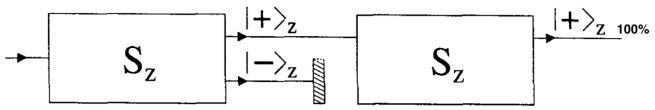


Secondo la meccanica classica, alla fine dell'esperimento dovremmo osservare sullo schermo una banda nella parte centrale, derivante dal fatto che in un atomo d'argento l'insieme delle orbite degli elettroni attorno al nucleo ha una struttura perfettamente simmetrica con momento angolare nullo. Quindi le forze si annullano a vicenda, ossia gli atomi non interagiscono con il campo magnetico. Invece si osserva la formazione di due fasci orizzontali distinti, uno più in basso e un altro più in alto.
Questo fenomeno si spiega ipotizzando che gli elettroni siano in possesso di un altro momento angolare intrinseco chiamato *spin*. Le due bande corrispondono ai due valori che lo spin può assumere, spin su o spin giù, ed il valore del momento angolare di spin, calcolato in modo sperimentale, corrisponde a $+\frac{\hbar}{2}$ e $-\frac{\hbar}{2}$ rispettivamente, dove $h = 2\pi\hbar$ ed è chiamata *costante di Planck*. Quindi, possiamo affermare che un elettrone è una particella *di spin* $\frac{1}{2}$.

Consideriamo un altro esperimento, illustrato in Figura 2.2, che consiste di due apparati di Stern e Gerlach sequenziali, entrambi con campo magnetico disposto lungo l'asse z: il primo divide il fascio iniziale in due componenti, che chiameremo $|+\rangle_z$ (spin su) e $|-\rangle_z$ (spin giù), e permette solo a elettroni con spin su di passare al secondo, inserendo uno schermo che assorbe tutti e soli gli elettroni con spin $-\frac{\hbar}{2}$; dal secondo apparato esce un unico fascio di particelle tutte con spin su lungo l'asse z.

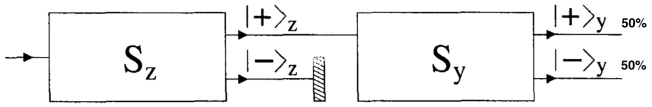
Scegliamo un'altra tipologia di misure consecutive, dove contrariamente al caso precedente si ha che il secondo apparato di Stern e Gerlach è rivolto lungo l'asse y, come in Figura 2.3. Il primo apparato si comporta come prima, ossia blocca gli elettroni con spin giù. Dunque, il fascio composto da particelle con lo spin opposto viene fatto passare attraverso il secondo

Figura 2.2: Ispirato da [5]



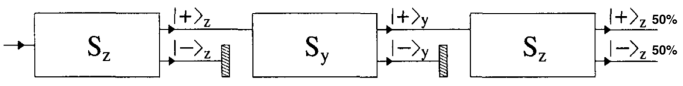
apparato, dal quale si osserva che fuoriescono due fasci di uguale intensità, uno con spin su e l'altro con spin giù lungo la direzione y, che indichiamo rispettivamente con $|+\rangle_y$ e $|-\rangle_y$.

Figura 2.3: Ispirato da [5]



Per capire meglio la situazione, analizziamo un altro esperimento ancora, spiegato in Figura 2.4. In questo caso la successione è la seguente: il primo apparato, con campo magnetico lungo l'asse z, filtra le particelle con spin giù lungo l'asse z; il secondo, con campo magnetico lungo l'asse y, filtra le particelle con spin giù lungo l'asse y; un terzo apparato, con campo disposto lungo l'asse z, compie la misura lungo tale asse. Da quest'ultimo stadio si ottengono entrambe le componenti, $|+\rangle_z$ e $|-\rangle_z$, con la stessa intensità, anche quelle che erano state precedentemente filtrate ($|-\rangle_z$).

Figura 2.4: Ispirato da [5]

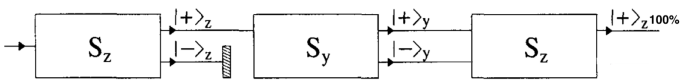


La spiegazione è che il secondo apparato individua lo stato $|+\rangle_y$ e nel farlo distrugge tutte le informazioni sul valore di S_z.
Quest'ultimo esperimento è la prova di una importante proprietà alla base della meccanica quantistica: lo stato finale dipende solo dallo stato in cui le

particelle entrano nell'apparato di Stern e Gerlach e dalla sua azione, ossia l'elettrone non ha memoria di quale fosse il suo stato prima della misura.

Infine consideriamo un quarto esperimento 2.5 che consiste in una piccola modifica del precedente.

Figura 2.5: Ispirato da [5]



Classicamente il risultato ottenuto nell'ultima misurazione dovrebbe essere 50% e 50%, ma il risultato è 100% spin su. Quello che accade è che l'elettrone si ricorda dello stato iniziale, dal momento che nello stadio intermedio lungo l'asse y non si sa quale dei due cammini ha compiuto, ossia non viene effettuata la misura. Tale risultato è la prova che in meccanica quantistica non è possibile seguire le regole classiche, è necessario introdurre concetti probabilistici diversi che approfondiremo nel prossimo capitolo.

2.2 Le basi della meccanica quantistica

2.2.1 Notazione bra-ket di Dirac e richiami di algebra lineare complessa

Prima di enunciare i postulati, diamo una breve introduzione alla notazione utilizzata per descrivere uno stato quantico.

- Sia $\mathcal{H}$ uno spazio vettoriale complesso finito dimensionale. Secondo la *notazione di Dirac*, indichiamo i vettori di $\mathcal{H}$ con il simbolo $|\alpha\rangle$ e li chiamiamo **ket**. Diciamo che $\mathcal{H}$ è uno **spazio di Hilbert** se esiste un'applicazione
$$\langle \ | \ \rangle : \mathcal{H} \times \mathcal{H} \to \mathbb{C},$$
chiamata **prodotto scalare**, tale che :

  1. $\langle\alpha|\beta\rangle = \langle\beta|\alpha\rangle^*$,
  dove $\forall\ c = a+ib$ numero complesso c^* è il suo complesso coniugato, $c^* = a - ib$;
  2. $\langle\alpha|c\beta + d\gamma\rangle = c\langle\alpha|\beta\rangle + d\langle\alpha|\gamma\rangle \quad \forall\ |\alpha\rangle,|\beta\rangle,|\gamma\rangle \in \mathcal{H}$ e $c, d \in \mathbb{C}$;

3. $\langle\alpha|\alpha\rangle \geq 0 \; \forall \; |\alpha\rangle \in \mathcal{H}$ e $\langle\alpha|\alpha\rangle = 0$ se e solo se $|\alpha\rangle = 0$.

Nel seguito considereremo sempre $\mathcal{H}$ come uno spazio di Hilbert finito dimensionale.

Si definisce la **norma** di un vettore $|\alpha\rangle$ come $|||\alpha\rangle|| = \sqrt{\langle\alpha|\alpha\rangle}$. In particolare, si dice **unitario** un vettore che ha norma uguale a 1. Dato un vettore non nullo si può normalizzare dividendo per la norma e ottenendo un vettore di norma unitaria.

Diciamo che un insieme di vettori $|\alpha_1\rangle, \ldots, |\alpha_n\rangle$ è **ortogonale** se, $\forall i \neq j \; \langle\alpha_i|\alpha_j\rangle = 0$; si dice **ortonormale** se i vettori sono anche unitari.

Un insieme di vettori $\{|\alpha_1\rangle, \ldots, |\alpha_n\rangle\}$ linearmente indipendenti nello spazio di Hilbert $\mathcal{H}$ di dimensione n si dice **base** e ogni vettore $|\alpha\rangle$ si può scrivere come combinazione lineare di vettori della base, ossia

$$|\alpha\rangle = \sum_{i=1}^{n} a_i |\alpha_i\rangle,$$

dove gli $a_i \in \mathbb{C}$ sono le componenti del vettore rispetto alla base.

- Definiamo un **operatore lineare** come un'applicazione $A : \mathcal{H} \to \mathcal{H}$ che trasforma ogni vettore in un altro vettore, cioè tale che $A|\alpha\rangle = |\beta\rangle \in \mathcal{H}$, e che sia lineare, ossia $\forall|\alpha\rangle$ e $|\beta\rangle$ e $\forall a, b \in \mathbb{C}$ si ha:

$$A(a|\alpha\rangle + b|\beta\rangle) = aA|\alpha\rangle + bB|\beta\rangle.$$

Dati due operatori lineari è possibile definire il prodotto $D = AB$ dove

$$D|\alpha\rangle = AB|\alpha\rangle.$$

In generale $AB \neq BA$; nel caso in cui sono uguali si dice che i due operatori *commutano*.

Ad un operatore lineare A è possibile dare una *rappresentazione matriciale*. Scriviamo $|\alpha\rangle$ e $|\beta\rangle$ come combinazione lineare dei vettori della base ortonormale $\{|\gamma_1\rangle, \ldots, |\gamma_n\rangle\}$:

$$|\alpha\rangle = \sum_i a_i |\gamma_i\rangle \qquad |\beta\rangle = \sum_i b_i |\gamma_i\rangle,$$

e quindi

$$b_i = \langle\gamma_i|\beta\rangle = \langle\gamma_i|A\alpha\rangle = \sum_j \langle\gamma_i|A\gamma_j\rangle a_j, \quad i = 1, \ldots, n. \tag{2.1}$$

Definiamo $A_{ij} = \langle \gamma_i | A \gamma_j \rangle$, dunque il sistema di equazioni (2.1) si scrive come:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1n} \\ A_{21} & A_{22} & \cdots & A_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ A_{n1} & A_{n2} & \cdots & A_{nn} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$$

Dato un operatore lineare A si chiama **autovettore** un vettore non nullo $|\alpha\rangle$ tale che:

$$A|\alpha\rangle = a|\alpha\rangle,$$

dove $a \in \mathbb{C}$ è chiamato **autovalore**. In particolare, lo spazio generato dagli autovettori associati ad $|\alpha\rangle$ è detto **autospazio** associato all'autovalore a.

Si può definire lo **spazio duale** di $\mathcal{H}$ come l'insieme di tutti i funzionali lineari, cioè :

$$\mathcal{H}^* = \{f : \mathcal{H} \to \mathbb{C}\}$$

Teorema 2.1 (Teorema di Riesz) Siano $\mathcal{H}$ e $\mathcal{H}^*$ rispettivamente uno spazio di Hilbert finito dimensionale e il suo duale. Se $|\alpha\rangle \in \mathcal{H}$ allora si ha che il funzionale definito da $\langle \beta | \alpha \rangle$ è un elemento di $\mathcal{H}^*$ per ogni $|\beta\rangle \in \mathcal{H}$. In altre parole, $\mathcal{H}$ e $\mathcal{H}^*$ sono isomorfi. Dunque, ogni funzionale in $\mathcal{H}^*$ può essere scritto in modo unico in tale forma.

Per la dimostrazione si veda [12].

Per la notazione di Dirac, gli elementi del duale sono chiamati **bra** e si indicano con il simbolo $\langle \alpha |$.

Sia operatore lineare A, allora è possibile dimostrare che esiste ed è unico un operatore $A^\dagger$ in $\mathcal{H}$, chiamato **aggiunto** oppure **Hermitiano coniugato**, che sia tale che $\forall |\alpha\rangle, |\beta\rangle \in \mathcal{H}$

$$\langle \alpha | A \beta \rangle = \langle A^\dagger \alpha | \beta \rangle.$$

Un caso particolare è quello in cui A è un operatore **Hermitiano** o **autoaggiunto**, ossia A è uguale al suo aggiunto

$$A^\dagger = A.$$

In questo caso, il prodotto scalare $\langle \alpha | A \alpha \rangle$ è reale, quindi gli autovalori sono reali.

Un operatore U si dice **unitario** se

$$UU^\dagger = U^\dagger U = I.$$

Allora si ha che l'operatore aggiunto nel caso unitario coincide con l'inverso

$$U^\dagger = U^{-1},$$

ovvero $U^\dagger$ è unitario. Notiamo inoltre che il prodotto di due operatori unitari è unitario e che gli operatori unitari preservano il prodotto interno tra vettori, ossia, dati 4 vettori tali che $|\gamma\rangle = U|\alpha\rangle$ e $|\nu\rangle = U|\beta\rangle$ si ha

$$\langle\gamma|\nu\rangle = \langle\alpha|\beta\rangle.$$

Dato un operatore è possibile cambiare il tipo di rappresentazione, ossia passare da una base ortonormale ($|\gamma_i\rangle$) ad un'altra $|\gamma_i'\rangle$ tramite una trasformazione unitaria S

$$|\gamma_i'\rangle = \sum_j S_{ji}|\gamma_j\rangle,$$

con $i = 1, 2, \ldots, n$.

Definiamo un'altra operazione tra due vettori importante a livello pratico spesso chiamata **prodotto esterno**, la quale definisce un operatore lineare che si indica con

$$|\alpha\rangle\langle\beta|.$$

Questo è definito dalla sua azione lungo un vettore generico $|\gamma\rangle$:

$$(|\alpha\rangle\langle\beta|)|\gamma\rangle = |\alpha\rangle\langle\beta|\gamma\rangle,$$

cioè fornisce sempre un multiplo di un vettore $|\alpha\rangle$, moltiplicato per il prodotto scalare di $|\beta\rangle$ e $|\gamma\rangle$.

Esempio 1 Calcoliamo il prodotto esterno $|0\rangle\langle 1|$:

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

Allora $|0\rangle\langle 1|$ è l'operatore lineare che trasforma $|1\rangle$ in $|0\rangle$ e $|0\rangle$ in $(0,0)^T$.

Equivalentemente si può scrivere $|0\rangle\langle 1|$ in forma matriciale, considerando $|0\rangle = (1,0)^T$, $\langle 0| = (1,0)$, $\langle 1| = (0,1)$ e $|1\rangle = (0,1)^T$:

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

.

Un operatore lineare A si dice **diagonalizzabile** se è possibile dare una rappresentazione diagonale, cioè A si può scrivere come

$$A = \sum_{i=1}^{n} \lambda_i |i\rangle\langle i|, \tag{2.2}$$

dove λ_i sono gli autovalori di A e $|i\rangle$ gli autovettori.

Un operatore lineare A si dice **normale** se commuta con il suo autoaggiunto, ossia

$$AA^\dagger = A^\dagger A.$$

Ricordiamo il seguente teorema per i nostri scopi:

Teorema 2.2 (Teorema di decomposizione spettrale) Un operatore è normale se e solo se è diagonalizzabile con una base ortonormale di autovettori.

Per la dimostrazione si veda [13].

Per definizione, sia gli operatori Hermitiani che quelli unitari sono normali, allora per i Teorema 2.2 sono diagonalizzabili con una base ortonormale di autovettori. Allora ogni vettore nello spazio di Hilbert $\mathcal{H}$ si può scrivere come una sovrapposizione lineare di vettori di questa base ortonormale.

Definiamo il **proiettore** come un operatore lineare tale che $P = P^2$ e che sia autoaggiunto, ossia $P^\dagger = P$. Per via del Teorema 2.2, risulta possibile scrivere un operatore normale come una combinazione lineare dei proiettori sugli autospazi (decomposizione spettrale):

$$A = \sum_i a_i P_i,$$

dove gli a_i sono gli autovalori relativi ad ogni autospazio e vale la relazione $P_i P_j = \delta_{ij} P_j$. Inoltre si ha che $\sum_i P_i = I$

- Si definisce **commutatore** di due operatori A e B

$$[A, B] = AB - BA$$

Teorema 2.3 (Teorema di diagonalizzazione simultanea) Due operatori A e B commutano, ossia sono tali che $[A, B] = 0$, se e solo se esiste una base ortonormale rispetto alla quale sia A che B sono diagonali.

Per la dimostrazione si veda [5].

Quindi, per il Teorema 2.2 si ha che due operatori commutano se e solo se esiste una base di autovettori comune.

Si definisce **anti-commutatore** di due operatori A e B

$$\{A, B\} = AB + BA$$

Diciamo che due operatori anti-commutano se $\{A, B\} = 0$.

- Consideriamo due spazi di Hilbert $\mathcal{H}_1$ e $\mathcal{H}_2$ di dimensione rispettivamente m e n. Chiamiamo $\mathcal{H}$ il **prodotto tensoriale** dei due spazi di Hilbert, $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, se ad ogni coppia di vettori $|\alpha\rangle \in \mathcal{H}_1$ e $|\beta\rangle \in \mathcal{H}_2$ è possibile associare un vettore appartenente ad $\mathcal{H}$ che scriviamo come $|\alpha\rangle \otimes |\beta\rangle$. Per definizione, ogni vettore in $\mathcal{H}$ si scrive come sovrapposizione lineare dei vettori $|\alpha\rangle \otimes |\beta\rangle$.
  Lo spazio vettoriale $\mathcal{H}$ ha dimensione nm. Infatti, se $|i\rangle$ e $|j\rangle$ sono due basi ortonormali per $\mathcal{H}_1$ e $\mathcal{H}_2$ si ha che $|i\rangle \otimes |j\rangle$ è una base ortonormale per $\mathcal{H}$.

  Per semplificare la notazione spesso scriviamo il prodotto tensoriale tra due vettori $|\alpha\rangle \otimes |\beta\rangle$ come $|\alpha\beta\rangle$.

  Siano A e B due operatori lineari in $\mathcal{H}_1$ e $\mathcal{H}_2$, rispettivamente, allora dato un generico vettore $|\psi\rangle \in \mathcal{H}$, che posso scrivere come

$$|\psi\rangle = \sum_{i,j} c_{ij} |i\rangle \otimes |j\rangle,$$

  con $c_{ij} = \langle ij|\psi\rangle$, allora l'azione di $\big(A \otimes B\big)$ su $|\psi\rangle$ è uguale a

$$\big(A \otimes B\big)\big(\sum_{i,j} c_{ij} |i\rangle \otimes |j\rangle\big) = \sum_{i,j} c_{ij} A|i\rangle \otimes B|j\rangle.$$

  Un operatore lineare O in $\mathcal{H}$ si può scrivere come

$$O = \sum_{i,j} \gamma_{ij} A_i \otimes B_j,$$

  dove A_i è in $\mathcal{H}_1$ e b_j in $\mathcal{H}_2$. La rappresentazione matriciale del prodotto tensoriale nella base $|K\rangle \equiv |ij\rangle$ è data da

$$\begin{pmatrix} A_{11}B & A_{12}B & \dots & A_{1m}B \\ A_{21}B & A_{22}B & \dots & A_{2m}B \\ \vdots & \vdots & & \vdots \\ A_{n1}B & A_{n2}B & \dots & A_{nm}B \end{pmatrix}$$

dove $A_{ij}B$ indica la sottomatrice n x n, con A e B la rappresentazione matriciale degli operatori A e B.

Esempio 2 Sia $|\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ e $|\beta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Calcoliamo il prodotto tensoriale. Rispetto alle basi $\{|00\rangle, |01\rangle, |11\rangle, |10\rangle\}$, la rappresentazione matriciale è la seguente:

$$|\alpha\rangle \otimes |\beta\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \cdot |\beta\rangle \\ -1 \cdot |\beta\rangle \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}$$

Esempio 3 Calcoliamo il prodotto tensoriale delle matrici di Pauli (2.5)

$$\sigma_x \otimes \sigma_z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 \cdot \sigma_z & 1 \cdot \sigma_z \\ 1 \cdot \sigma_z & 0 \cdot \sigma_z \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

- Definiamo le **matrici di Pauli** che saranno utilizzate spesso nel seguito:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Queste matrici hanno due importanti proprietà:

1. $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$ (matrice identità)
2. $\sigma_x\sigma_y = i\sigma_z$, $\sigma_y\sigma_z = i\sigma_x$, $\sigma_z\sigma_x = i\sigma_y$

Osservazione 2.4 Le matrici di Pauli σ_x, σ_y e σ_z sono operatori Hermitiani e unitari.

Analizziamo l'esempio di rappresentazione diagonale dato dalla matrice di Pauli

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$$

che è diagonale rispetto agli autovettori $|0\rangle = \binom{1}{0}$ e $|1\rangle = \binom{0}{1}$, corrispondenti agli autovalori +1 e -1, rispettivamente. In questa rappresentazione $\{|0\rangle, |1\rangle\}$, la matrice di Pauli σ_x si scrive come $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$. σ_x

è diagonale rispetto agli autovettori $|+\rangle = \frac{1}{\sqrt{2}}\binom{1}{1}$ e $|-\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1}$, e dunque $\sigma_x = |+\rangle\langle+| - |-\rangle\langle-|$. Si può passare dalla base originale$\{|0\rangle, |1\rangle\}$ alla nuova base $\{|+\rangle, |-\rangle\}$ tramite il cambiamento di base dato dalla trasformazione unitaria

$$S = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Osservazione 2.5 Le matrici di Pauli anti-commutano, ossia $\{\sigma_i, \sigma_j\} = 0$ con $i, j = x, y, z$. Valgono invece le seguenti relazioni per i commutatori:

$$[\sigma_x, \sigma_y] = 2i\sigma_z, \qquad [\sigma_y, \sigma_z] = 2i\sigma_x, \qquad [\sigma_z, \sigma_x] = 2i\sigma_y.$$

Si può notare che $\sigma'_x = \frac{1}{2}\sigma_x, \sigma'_y = \frac{1}{2}\sigma_y, \sigma'_z = \frac{1}{2}\sigma_z$ generano l'algebra di Lie del gruppo $SU(2) = \{A \in \mathbb{C}^{2\times 2} : A^* = A^{-1}, det(A) = 1\}$.

2.2.2 I postulati della meccanica quantistica

Postulato 1 *Lo stato di un sistema fisico S viene descritto da un vettore unitario $|\psi\rangle$, chiamato vettore di stato o funzione d'onda, appartenente allo spazio di Hilbert $\mathcal{H}_S$ associato al sistema.*
L'evoluzione temporale di un vettore di stato è data dalla equazione di Schrödinger

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle, \tag{2.3}$$

dove H è un operatore autoaggiunto, anche conosciuto come Hamiltoniana, e $\hbar = \frac{h}{2\pi}$ con h costante di Planck.

L'equazione di Schrödinger è una equazione differenziale lineare di primo ordine rispetto al tempo; quindi, dato lo stato iniziale $|\psi(t_0)\rangle$, è unicamente determinata la soluzione $|\psi(t)\rangle$ al tempo t.

La linearità dell'equazione di Schrödinger implica che valga il **principio di sovrapposizione**: se $|\psi_1(t)\rangle$ e $|\psi_2(t)\rangle$ sono soluzioni della ((2.3)), allora la sovrapposizione $|\psi(t)\rangle = \alpha|\psi_1(t)\rangle + \beta|\psi_2(t)\rangle$ con $\alpha, \beta \in \mathbb{C}$ è anch'essa una soluzione.

Definiamo ora l'*operatore di evoluzione temporale* U

$$|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle,$$

che risulta essere lineare. Inoltre, se H è indipendente da t, la soluzione della ((2.3)) si può scrivere come

$$|\psi(t)\rangle = exp\big[-\frac{i}{\hbar}H(t-t_0)\big]|\psi(t_0)\rangle,$$

e quindi si trova che $U(t,t_0) = exp\big[-\frac{i}{\hbar}H(t-t_0)\big]$, che risulta essere unitario.

Postulato 2 *Ad ogni osservabile è associato un operatore autoaggiunto A sullo spazio di Hilbert $\mathcal{H}_S$. L'unico possibile risultato della misura di tale osservabile è uno degli autovalori di A. Se a_i è un autovalore si ha*

$$A|i\rangle = a_i|i\rangle,$$

dove $|i\rangle$ è una base ortonormale di autovettori di A. Possiamo riscrivere $|\psi(t)\rangle$ in funzione di questa base, ossia

$$|\psi(t)\rangle = \sum_i c_i(t)|i\rangle,$$

allora la probabilità di misurare un osservabile A al tempo t con risultato a_i è uguale a

$$p_i(t) = p(a = a_i|t) = |\langle i|\psi(t)\rangle|^2 = |c_i(t)|^2.$$

I coefficienti $c_i(t)$ prendono il nome di *ampiezze di probabilità.*

Notiamo che, per semplicità, stiamo supponendo solo il caso in cui gli autovalori di A siano non degeneri, ossia ad ogni autovalore è associato un solo autovettore.

Osservazione 2.6 Il motivo per cui associamo operatori autoaggiunti agli osservabili viene dal fatto che, come abbiamo visto nella sezione 2.2.1, gli autovalori di un operatore autoaggiunto sono reali e i rispettivi autovettori formano una base ortonormale per lo spazio di Hilbert associato al sistema. Dal momento che $|\psi(t)\rangle$ ha norma unitaria, si ha

$$\sum_i p_i(t) = \sum_i |c_i(t)|^2 = 1, \tag{2.4}$$

quindi le probabilità sono normalizzate, ossia la probabilità totale ottenuta dalla misura dell'osservabile A è 1. Questo è il motivo per cui nel Postulato 1 si richiede che il vettore $|\psi(t)\rangle$ sia unitario.

Osservazione 2.7 Nel caso in cui il vettore di stato coincida con l'autovettore dell'operatore A con autovalore a_i ad un certo istante t_0,

$$|\psi(t_0)\rangle = |i\rangle,$$

allora la misura di A al tempo t_0 ha come risultato a_i. Questo è il motivo per cui gli autovettori di un operatore sono anche detti *autostati*.

Osservazione 2.8 Supponiamo che $|\psi_1\rangle$ e $|\psi_2\rangle$ siano due autovettori distinti e normalizzati dell'operatore A, con autovalori rispettivamente a_1 e a_2. Allora per il principio di sovrapposizione si ha:

$$|\psi\rangle = \lambda_1|\psi_1\rangle + \lambda_2|\psi_2\rangle,$$

dove $\lambda_1,\ \lambda_2 \in \mathbb{C}$, è anch'esso uno stato del sistema, supponendo che $|\psi\rangle$ sia unitario, quindi $|\lambda_1|^2 + |\lambda_2|^2 = 1$. Dunque, se un sistema è descritto da un vettore di stato $|\psi\rangle$, e noi misuriamo un osservabile A, abbiamo come risultato a_1 con probabilità $|\lambda_1|^2$ e a_2 con probabilità $|\lambda_2|^2$.

Analizziamo ora cosa accade al sistema quando effettuiamo una misura. Supponiamo di misurare un osservabile A e ottenere come risultato a_n, un autovalore non degenere dell'operatore autoaggiunto A. Se viene immediatamente effettuata un'altra misura su A, otteniamo di nuovo a_n con probabilità 1. La spiegazione di questo è data dal fatto che la funzione d'onda di un sistema, in uno stato $|\psi\rangle$, appena dopo aver effettuato la misura, *collassa* nell'autostato $|n\rangle$ di A associato all'autovalore a_n.

Postulato 3 *Se un sistema è descritto dalla funzione d'onda $|\psi\rangle$, supponendo di compiere una misura su A e ottenere come risultato a_n, allora lo stato del sistema immediatamente dopo la misura è dato da*

$$\frac{P_n|\psi\rangle}{\sqrt{\langle\psi|P_n|\psi\rangle}},$$

dove P_n è la proiezione sul sottospazio corrispondente ad a_n.

Si ha che la probabilità di ottenere a_n misurando A è uguale a

$$p_n = \langle\psi|P_n|\psi\rangle.$$

Il valore medio di A è dato da $\langle A\rangle = \sum_n a_n p_n$, quindi, usando che $A = \sum_n a_n P_n$ (decomposizione spettrale), si ha:

$$\langle A\rangle = \sum_n a_n\langle\psi|P_n|\psi\rangle = \langle\psi|\Big(\sum_n a_n P_n\Big)|\psi\rangle = \langle\psi|A|\psi\rangle \tag{2.5}$$

Inoltre è possibile definire la deviazione standard ΔA associata all'osservazione di A, $\Delta A = \sqrt{\langle (A - \langle A \rangle)^2 \rangle} = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}$. Dunque, facendo molti esperimenti in cui effettuiamo la misura di un osservabile A e consideriamo uno stato $|\psi\rangle$, otteniamo dei risultati con valore medio $\langle A \rangle$ e deviazione standard ΔA.

Analizzando alcuni esperimenti ideali, il fisico Werner Karl Heisenberg trovò che non è possibile assegnare ad una particella, allo stesso momento e in modo preciso, velocità e posizione. Questo fatto portò alla formulazione del seguente principio.

Teorema 2.9 (Principio di indeterminazione di Heisenberg) *Siano A e B due operatori Hermitiani ciascuno associato ad un osservabile e sia $|\psi\rangle$ uno stato quantico. Allora vale la seguente disuguaglianza:*

$$\Delta A \Delta B \geq \frac{|\langle \psi | [A, B] | \psi \rangle|}{2} \tag{2.6}$$

Per la dimostrazione rimandiamo a [5].

In altre parole il principio di Heisenberg afferma che, se due osservabili A e B non commutano, ossia $[A, B] \neq 0$, effettuare una misura su uno di questi necessariamente disturba l'altro. Se misuriamo A con una certa accuratezza ΔA, allora B viene disturbato di un certo valore ΔB, e $\Delta A \Delta B$ verificano la disuguaglianza (2.6). Dunque, nell'effettuare una misura simultanea di A e B bisogna tener conto del fatto che aumentare l'accuratezza di uno implica una diminuzione nell'accuratezza dell'altro, cioè sono inversamente proporzionali.

Consideriamo un esempio di apparato che funziona sia da "preparatore" di un certo stato che da "misuratore": l'esperimento di Stern e Gerlach analizzato in 2.1. Se l'apparato è orientato lungo l'asse z, possiamo ottenere solo uno dei due stati possibili $|0\rangle$ o $|1\rangle$, che coincidono con gli autovettori dell'operatore di Pauli σ_z corrispondenti agli autovalori +1 e -1. Se blocchiamo lo stato $|1\rangle$, otteniamo l'autostato $|0\rangle$ dell'operatore di spin σ_z. Se l'apparato è invece diretto lungo l'asse x, ci sono due possibili risultati, ossia agli autovettori dell'operatore di Pauli σ_x: $|+\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|-\rangle_x = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, che corrispondo agli autovalori +1 e -1.

2.3 La versione di Bohm del paradosso EPR

Lo spazio di Hilbert $\mathcal{H}$ associato ad un *sistema quantico composto* è il prodotto tensoriale degli spazi di Hilbert associati alle singole componenti del

sistema e il prodotto tensoriale delle basi di questi è la base più naturale di $\mathcal{H}$. L'esempio più semplice è quello in cui $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ e i due spazi di Hilbert hanno dimensione 2 con basi $\{|0\rangle_1, |1\rangle_1\}$ e $\{|0\rangle_2, |1\rangle_2\}$. Per cui si ha che una base per $\mathcal{H}$ è $\{|0\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2, |1\rangle_1 \otimes |0\rangle_2, |1\rangle_1 \otimes |1\rangle_2\}$. Quindi, per il *principio di sovrapposizione*, lo stato più generale in uno spazio di Hilbert viene descritto da una sovrapposizione di stati in $\mathcal{H}_1$ e $\mathcal{H}_2$, ossia

$$|\psi\rangle = \sum_{i,j=0}^{1} c_{ij}|i\rangle_1 \otimes |j\rangle_2 \tag{2.7}$$

Definizione 2.10 *Uno stato in $\mathcal{H}$ si definisce **entangled** se non può essere scritto come un semplice prodotto tensoriale, ossia $|\psi\rangle = |\alpha_1\rangle \otimes |\beta_2\rangle$, dove $|\alpha_1\rangle$ e $|\beta_2\rangle$ sono due stati rispettivamente in $\mathcal{H}_1$ e in $\mathcal{H}_2$.*

Esempio 4 Consideriamo uno stato entangled $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ e uno non entangled $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$. Quest'ultimo si può scrivere anche come $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$.

Fu proprio il fenomeno dell'entanglement che portò Einstein, Podolsky e Rosen nel 1935 alla redazione dell'articolo [6] che portava alla luce alcune contraddizioni della descrizione quantistica della realtà. Nell'articolo vengono illustrate le proprietà "non classiche" degli stati entangled che portano a delle contraddizioni, supponendo vere due assunzioni fondamentali:

- **Principio di Realtà**: se possiamo prevedere con certezza il valore di una quantità fisica , allora questo valore ha realtà fisica, indipendentemente dalla nostra osservazione;
- **Principio di Località**: se due sistemi sono causalmente disconnessi, il risultato della misura sull'uno non condiziona l'altra, dove con il termine disconnesso si intende che vale $(\Delta x)^2 > c^2\Delta t^2$ con Δx e Δt variazioni di spazio e tempo e c velocità della luce.

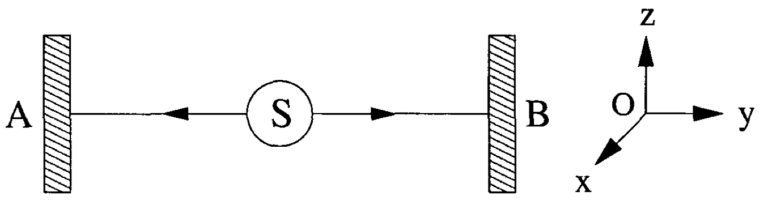
Come afferma il principio di Heisenberg 2.6, se due operatori A e B non commutano, allora non possiamo prevedere con certezza il risultato della misura simultanea di entrambi, ossia A e B non possono avere realtà simultanea.

Analizziamo il paradosso EPR tramite la spiegazione di un esempio ideato da Bohm [6]. Consideriamo una sorgente S che emette coppie di particelle di spin $\frac{1}{2}$ nello stato entangled

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{2.8}$$

chiamato *stato EPR* oppure *stato di Bell*. In particolare, diciamo che il sistema è nello stato di singoletto. Una particella viene mandata ad Alice e una a Bob, come in Figura 2.6, che sono posti ad una distanza tale che le misure eseguite dai due osservatori siano *disconnesse*.

Figura 2.6: Schema dell'esperimento EPR *gedanken*. Tratto da [5]



Supponiamo che Alice misuri lo spin della particella lungo l'asse z e ottenga, ad esempio, $\sigma_z^{(A)} = +1$, allora lo stato EPR collassa nello stato $|01\rangle$. Di conseguenza, se Bob misura lo spin della sua particella, anch'esso lungo l'asse z ottiene $\sigma_z^{(B)} = -1$ con probabilità 1. Quindi, i risultati di Alice e Bob sono perfettamente anticorrelati. Notiamo che la (2.8) si può scrivere anche come

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle),$$

dove $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ e $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ sono gli autostati di σ_x associati ai due autovalori +1 e -1. Infatti

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle) = \frac{1}{\sqrt{2}}\big[\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle - |01\rangle - |10\rangle -$$
$$- |00\rangle - |01\rangle + |10\rangle + |11\rangle)\big] = \frac{1}{\sqrt{2}}\big[\frac{1}{\sqrt{2}}(2|01\rangle - 2|10\rangle)\big]$$

Se Alice misura $\sigma_x^{(A)}$ e ottiene +1, allora lo stato EPR collassa nello stato $|+-\rangle$ e Bob ottiene sicuramente $\sigma_x^{(B)} = -1$. Dunque, lo stato di una particella dipende dal risultato ottenuto nell'altra.

Parlando in termini di EPR, abbiamo che non è possibile assegnare contemporaneamente realtà fisica ai due osservabili poiché questi non commutano, infatti $[\sigma_x^{(B)}, \sigma_z^{(B)}] \neq 0$ (Osservazione 2.5). Dunque, se Alice misura $\sigma_z^{(A)}$ allora associa un elemento di realtà a $\sigma_z^{(B)}$, se misura $\sigma_x^{(A)}$ associa un elemento di realtà fisica a $\sigma_x^{(B)}$. In altre parole, Alice può associare all'altra particella solo la realtà fisica correlata con la propria.

Il punto chiave è che Alice può decidere quale osservabile misurare anche dopo che le particelle vengono separate. Quindi, seguendo il principio di località, la misura fatta da Alice non può modificare lo stato della particella di Bob perché sono *disconnessi*. Questo porta ad una evidente contraddizione, se si considerano validi entrambi i principi di realtà e località.

La conclusione di Einstein fu che la meccanica quantistica è incompleta. Più tardi vennero proposte diverse teorie, tra queste la più nota è quella delle variabili nascoste, le quali dovrebbero rendere completa la teoria quantistica. Solo più tardi si capì che in realtà questo paradosso aveva messo in luce che la non località fosse una caratteristica propria della meccanica quantistica, conseguenza naturale dell'esistenza di stati entangled.

2.4 Il teorema di Bell e la disuguaglianza di CHSH

Le disuguaglianze di Bell vennero introdotte inizialmente da John S. Bell nel 1964 e rappresentano la prova della coerenza della meccanica quantistica. L'esperimento di Bell è stato per la prima volta fatto da Aspect, Grangier e Roger nel 1982 [11] e mostrò la violazione delle disuguaglianze. Come abbiamo visto nel capitolo precedente, Einstein, Poldosky e Rosen reputarono la teoria quantistica incompleta e proposero un esperimento ideale che evidenziava la non località delle teorie quantistiche, principio alla base di tutta la fisica conosciuta fino ad allora.

Il *Teorema di Bell* afferma che una teoria quantistica, per cui vengano assunti i principi di realtà e località, deve rispettare delle relazioni di disuguaglianza fra misure su particelle correlate, che non sono invece soddisfatte dalla meccanica quantistica. In altre parole, Bell dimostrò che nessuna teoria fisica a variabili nascoste locali può riprodurre le predizioni della meccanica quantistica. Ci furono varie dimostrazioni del Teorema di Bell; in questa sezione descriveremo quella più utile nel caso del protocollo di Ekert, ossia quella data da John Clauser, Michael Horne, Abner Shimony, and Richard Holt.
Introduciamo una variabile nascosta λ tale per cui misurando la quantità osservabile $\mathcal{O}$ si ottiene il risultato ben definito $\mathcal{O}(\lambda)$ e richiediamo che la distribuzione di probabilità $\rho(\lambda)$ sia tale che venga ottenuto il valore medio predetto dalla meccanica quantistica, ossia:

$$\langle O \rangle = \int O(\lambda)\rho(\lambda)d\lambda. \tag{2.9}$$

Essendo $\rho(\lambda)$ la distribuzione di probabilità dei valori di λ, allora non è negativa $\forall\lambda$ ed è tale che $\int \rho(\lambda)\, d\lambda = 1$. Siano inoltre $A(\mathbf{a}, \lambda)$ e $B(\mathbf{b}, \lambda)$ i risultati delle misure dello spin $\sigma^{(A)} \cdot \mathbf{a}$ e $\sigma^{(B)} \cdot \mathbf{b}$ misurate da Alice e Bob rispettivamente lungo le direzioni a e b. Assumiamo il *principio di località*, dunque le misure sono indipendenti. Allora il *coefficiente di correlazione delle misure* di Alice lungo $\mathbf{a}$ e Bob lungo $\mathbf{b}$ è il seguente:

$$E(\mathbf{a}, \mathbf{b}) = \int A(\mathbf{a}, \lambda) B(\mathbf{b}, \lambda) \rho(\lambda) d\lambda. \tag{2.10}$$

Per la meccanica quantistica quando $\mathbf{a} = \mathbf{b}$ i risultati sono discordi, pertanto

$$E(\mathbf{a}, \mathbf{a}) = -1. \tag{2.11}$$

Consideriamo il seguente calcolo:

$$\begin{aligned} E(\mathbf{a}, \mathbf{b}) - E(\mathbf{a}, \mathbf{b'}) &= \int \big[A(\mathbf{a}, \lambda) B(\mathbf{b}, \lambda) - A(\mathbf{a}, \lambda) B(\mathbf{b'}, \lambda)\big] \rho(\lambda) d\lambda = \\ &= \int A(\mathbf{a}, \lambda) B(\mathbf{b}, \lambda) \big[1 \pm A(\mathbf{a'}, \lambda) B(\mathbf{b'}, \lambda)\big] \rho(\lambda) d\lambda - \\ &- \int A(\mathbf{a}, \lambda) B(\mathbf{b'}, \lambda) \big[1 \pm A(\mathbf{a'}, \lambda) B(\mathbf{b}, \lambda)\big] \rho(\lambda) d\lambda. \end{aligned}$$

Al variare di $\mathbf{a}$ e $\mathbf{b}$ si hanno dei valori diversi di A e B, ma comunque tali che:

$$|A(\mathbf{a}, \lambda)| = 1 \quad |B(\mathbf{b}, \lambda)| = 1.$$

Allora si ha :

$$\begin{aligned} |E(\mathbf{a}, \mathbf{b}) - E(\mathbf{a}, \mathbf{b'})| \leq &\int \big[1 \pm A(\mathbf{a'}, \lambda) B(\mathbf{b'}, \lambda)\big] \rho(\lambda) d\lambda + \\ &+ \int \big[1 \pm A(\mathbf{a'}, \lambda) B(\mathbf{b}, \lambda)\big] \rho(\lambda) d\lambda. \end{aligned}$$

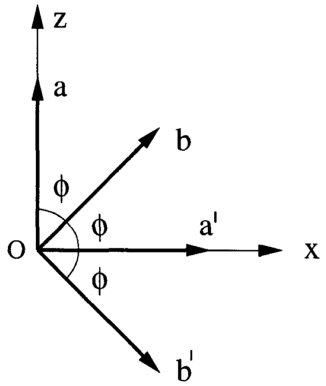
Questo implica che:

$$\begin{aligned} &|E(\mathbf{a}, \mathbf{b}) - E(\mathbf{a}, \mathbf{b'})| \leq \pm\big[E(\mathbf{a'}, \mathbf{b'}) + E(\mathbf{a'}, \mathbf{b})\big] + 2 \int \rho(\lambda)\, d\lambda = \\ &= -|E(\mathbf{a'}, \mathbf{b'}) + E(\mathbf{a'}, \mathbf{b})| + 2 \end{aligned}$$

In conclusione si ottiene una disuguaglianza conosciuta come **disuguaglianza di CHSH**:

$$|S| := |E(\mathbf{a}, \mathbf{b}) - E(\mathbf{a}, \mathbf{b'})| + |E(\mathbf{a'}, \mathbf{b}) + E(\mathbf{a'}, \mathbf{b'})| \leq 2. \tag{2.12}$$

Figura 2.7: Scelta delle direzioni tale che non soddisfi la disuguaglianza CHSH, dove $\phi = \frac{\pi}{4}$. Tratta da [5].



L'aspetto fondamentale è che esistono delle direzioni (**a**,**b**,**a'**,**b'**) tali che, considerando gli stati entangled, la meccanica quantistica non soddisfa la disuguaglianza vista. Consideriamo un esempio che poi risulterà utile nel terzo capitolo per la comprensione del funzionamento del protocollo crittografico, ovvero il caso in cui le direzioni (**a**,**b**,**a'**,**b'**) sono come in Figura 2.7.

Per le considerazioni del Paragrafo 2.3 si ha che :

$$E(\mathbf{a}, \mathbf{b}) = \langle\psi|(\sigma^{(A)} \cdot \mathbf{a})(\sigma^{(B)} \cdot \mathbf{b})|\psi\rangle = -a \cdot b = -cos(\theta_{a,b}), \tag{2.13}$$

dove θ_{ab} è l'angolo compreso tra **a** e **b**.
Dunque si ottiene che:

$$\begin{aligned} &|E(\mathbf{a}, \mathbf{b}) - E(\mathbf{a}, \mathbf{b'})| + |E(\mathbf{a'}, \mathbf{b}) - E(\mathbf{a'}, \mathbf{b'})| = \\ &= |-cos(\frac{\pi}{4}) + cos(\frac{3\pi}{4})| + |-cos(\frac{\pi}{4}) - cos(\frac{\pi}{4})| = 2\sqrt{2} \geq 2, \end{aligned}$$

quindi non soddisfa la disuguaglianza (2.12).

Capitolo 3

Il protocollo di Ekert

La crittografia quantistica nasce dall'idea di Stephen Wiesener, uno studente di dottorato, che negli ultimi anni '60 propose una tecnica per costruire teoricamente delle banconote non falsificabili basate sulla meccanica quantistica. Secondo questo modello, le banconote quantistiche sono identificate da un numero di serie e dagli stati di polarizzazione di alcuni fotoni in essa intrappolati. Il lavoro di Wiesener non fu compreso da nessuno al tempo, tutte le riviste scientifiche a cui sottopose il suo articolo dal titolo *Conjugate Coding* [3] si rifiutarono di pubblicarlo, e quindi finì per abbandonare i suoi studi sul tema. Solo 20 anni dopo Charles Bennet e Gilles Brassard intuirono la genialità di Wiesener e rielaborarono l'idea delle banconote quantistiche, ossia usare dei fotoni per *conservare* l'informazione. A loro si deve infatti il primo protocollo di crittografia quantistica, la cui descrizione venne pubblicata nel 1984 [4], chiamato protocollo BB84, in cui i fotoni vengono utilizzati invece per *trasmettere* informazione.

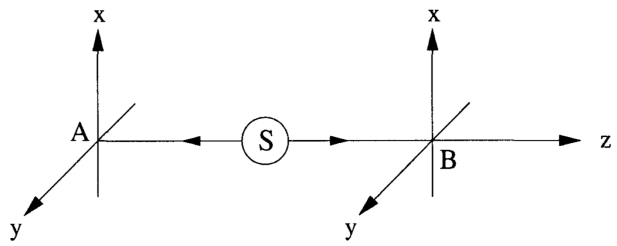
In questo capitolo ci occuperemo di analizzare nel dettaglio il funzionamento del protocollo chiamato E91, dal nome del suo ideatore Artur K. Ekert che nel 1991 lo descrisse in un articolo della rivista *Physical Reviews Letters* [2]. Si tratta di un protocollo di distribuzione quantistica della chiave basato su misure di spin di particelle correlate secondo lo schema EPR e sulla disuguaglianza di Bell, e quindi sulla completezza della meccanica quantistica. Come già anticipato, consente a due soggetti che vogliono comunicare di giungere alla condivisione di una chiave segreta, che poi viene utilizzata per comunicare tramite, ad esempio, il cifrario di Vernam descritto nella sezione 1.3 a pagina 11. Inoltre daremo una descrizione anche di un secondo protocollo basato su EPR, mettendo in luce le differenze e i vantaggi.

3.1 Descrizione del protocollo E91

Il protocollo E91 è basato sulla versione data da Bohm del paradosso EPR descritta in 2.3 e sulla versione della disuguaglianza di Bell proposta da Clauser, Horne, Shimony e Holt analizzata in 2.4 per dimostrare l'impossibilità di Eva di impossessarsi della chiave senza essere scoperta.

Il sistema consiste in una sorgente S che emette coppie di particelle di spin $\frac{\hbar}{2}$ che si muovono lungo l'asse z in direzioni opposte. Alice e Bob sono disposti ad una distanza adeguata in modo da evitare iterazioni tra le particelle e compiono sulle particelle misure di spin con apparati di Stern e Gerlach (2.1) lungo le 4 direzioni possibili date dai vettori unitari a_i e b_j, con $i, j = 1, 2, 3$, rispettivamente, per Alice e Bob, come in Figura 3.1

Figura 3.1: Tratta da [5].



Per semplicità supponiamo che i vettori a_i e b_j giacciano sul piano formato dagli assi x e y, siano perpendicolari all'asse z e formino i seguenti angoli con l'asse x: $\phi_1^a = 0, \phi_2^a = \frac{\pi}{4}, \phi_3^a = \frac{\pi}{2}, \phi_1^b = \frac{\pi}{4}, \phi_2^b = \frac{\pi}{2}, \phi_3^b = \frac{3\pi}{4}$ (come mostrato in Figura 3.2)

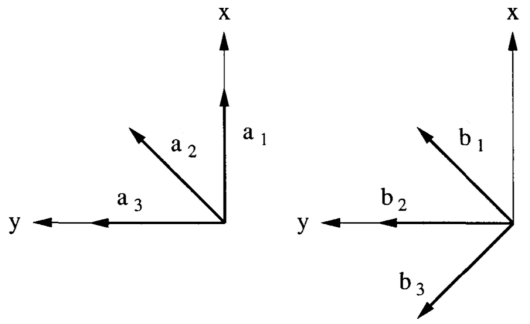
Ogni misurazione può avere due risultati: +1 (spin su) e -1 (spin giù), in $\frac{\hbar}{2}$, e potenzialmente può portare a definire un bit della chiave. Definiamo il *coefficiente di correlazione delle misure* di Alice lungo a_i e Bob lungo b_j come in (2.10), che nel caso specifico è uguale a

$$E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j), \qquad (3.1)$$

dove $P_{\pm\pm}(a_i, b_j)$ indica la probabilità che ± 1 sia ottenuto lungo a_i e lungo b_j. Come abbiamo calcolato in (2.13) si ottiene, si ha:

$$E(a_i, b_j) = -a_i \cdot b_j = -cos(\theta_{a_i, b_j}), \qquad (3.2)$$

Figura 3.2: Ispirato da [5]



dove θ_{a_i,b_j} è l'angolo compreso tra a_i e b_j. La meccanica quantistica, come già visto in 2.11 prevede che i risultati siano discordi per le coppie che hanno lo stesso orientamento (nel nostro caso a_2, b_1 e a_3, b_2), quindi si trova che:

$$E(a_2, b_1) = E(a_3, b_2) = -1 \tag{3.3}$$

È possibile dare un'altra definizione legata alla (3.1), nei casi in cui Alice e Bob scelgano direzioni diverse:

$$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3) \tag{3.4}$$

L'esempio in questione è già stato analizzato nel Paragrafo 2.4, per cui abbiamo visto che la disuguaglianza di Bell corrisponde esattamente a $|S| \leq 2$ (2.12), e invece risulta

$$|S| = 2\sqrt{2} > 2. \tag{3.5}$$

Dunque, la disuguaglianza di Bell non viene soddisfatta.

Una volta date le definizioni preliminari, descriviamo come avviene effettivamente la distribuzione della chiave, distinguendo quattro fasi.

1. Inizialmente Alice e Bob comunicano tramite un canale pubblico per accordarsi sugli aspetti tecnici preliminari: le 4 direzioni (in particolare quelle comuni e quelle non comuni), il numero complessivo di particelle da misurare e la scelta dei bit da associare ai risultati.

2. Nella seconda fase avviene la vera a propria *trasmissione quantistica*. Dunque, ogni volta che gli utenti ricevono una particella, la direzione lungo cui compiere la misura viene decisa da ciascuno in modo casuale. Entrambi annotano il risultato ottenuto e la direzione scelta, alla fine della trasmissione ottengono due tabelle come in 3.1.

Tabella 3.1: Misure di Alice e Bob

1)	a_1	$-\frac{\hbar}{2}$
2)	a_2	$+\frac{\hbar}{2}$
3)	a_1	$+\frac{\hbar}{2}$
4)	a_3	$-\frac{\hbar}{2}$
5)	a_1	$+\frac{\hbar}{2}$
6)	a_3	$-\frac{\hbar}{2}$
7)	a_3	$+\frac{\hbar}{2}$
8)	a_3	$-\frac{\hbar}{2}$
	$\vdots$	

1)	b_1	$+\frac{\hbar}{2}$
2)	b_3	$+\frac{\hbar}{2}$
3)	b_3	$+\frac{\hbar}{2}$
4)	b_2	$+\frac{\hbar}{2}$
5)	b_1	$-\frac{\hbar}{2}$
6)	b_1	$-\frac{\hbar}{2}$
7)	b_2	$-\frac{\hbar}{2}$
8)	b_2	$+\frac{\hbar}{2}$
	$\vdots$	

3. Dopo la trasmissione, Alice e Bob annunciano le *direzioni* scelte per misurare lo spin di ciascuna particella tramite un canale pubblico classico, dividono le misure in due gruppi: quelle per cui hanno scelto direzioni diverse e le altre per cui hanno utilizzato le stesse direzioni. Il primo gruppo vedremo che ci sarà utile successivamente in caso di intromissione di Eva. Nel caso di direzioni coincidenti invece la meccanica quantistica ci assicura una anticorrelazione tra i risultati.

4. Infine Alice e Bob sono in grado di convertire i risultati in una stringa segreta di bit che rappresenta la chiave (come nella Tabella 3.2), seguendo le scelte accordate nel primo passaggio. Questa chiave viene utilizzata per comunicare in modo sicuro tramite il cifrario di Vernam dai due protagonisti.

Tabella 3.2: Chiave di Alice e Bob

4)	$-\frac{\hbar}{2}$	0
7)	$+\frac{\hbar}{2}$	1
8)	$-\frac{\hbar}{2}$	0
	$\vdots$	

4)	$+\frac{\hbar}{2}$	0
7)	$-\frac{\hbar}{2}$	1
8)	$+\frac{\hbar}{2}$	0
	$\vdots$	

3.1.1 Presenza di un intercettatore

In questa parte vediamo come i tentativi di Eva di intromettersi fra Bob e Alice nel processo di distribuzione della chiave vengono vanificati grazie al

teorema di Bell.
Innanzitutto bisogna notare che sarebbe inutile per Eva misurare le particelle in transito lungo l'asse z poiché, a causa del funzionamento del sistema, non ne trarrebbe alcuna informazione, ma potrebbe pensare di sostituirsi ingannevolmente alla sorgente. In questo caso Eva prepara due stati da inviare a Bob e Alice che quindi misureranno lo spin di due particelle che sono *già state misurate*, piuttosto che lo spin di due particelle appena prodotte. Dunque l'intercettatore deve scegliere una direzione e inviare coppie di particelle di spin opposto lungo questa. Il vantaggio sta nel fatto che nei casi in cui Alice e Bob scelgono entrambi la sua stessa direzione, Eva conosce con certezza i loro risultati. In altre parole è in grado di entrare a conoscenza di alcuni bit della chiave, quelli per cui sia Alice che Bob hanno effettuato la misura lungo la stessa direzione scelta da lei.

Procediamo alla spiegazione in termini matematici di quello che accade. Citando Ekert "In questo caso l'intervento di Eva è equivalente a introdurre elementi di *realtà fisica* a le misure delle componenti di spin". Questo è evidente modificando (3.4), e quindi, sommando su tutte le possibili scelte, otteniamo:

$$S = \int \rho(n_a, n_b) dn_a\, dn_b \big[(a_1 \cdot n_a)(b_1 \cdot n_b) - (a_1 \cdot n_a)(a_3 \cdot n_b) + \\ + (a_3 \cdot n_a)(b_1 \cdot n_b) + (a_3 \cdot n_a)(b_3 \cdot n_b)\big], \tag{3.6}$$

dove n_a e n_b sono due vettori sull'asse z, rispettivamente riferiti alle particelle a e b, che rappresentano le informazioni che acquisisce Eva, e $\rho(n_a, n_b)$ corrisponde alla probabilità di intercettare una componente di spin, ossia descrive la strategia di Eva.
Supponiamo che una particella venga intercettata e misurata da Eva, ad esempio a, lungo la direzione n_a, allora $n_a{=}{-}n_b$. Sostituendo in (3.6) il valore di a_1, b_1, a_3, b_3 (per costruzione, $k_i = cos(\phi_i^k)$, con $i = 1, 3$ e $k = a, b$), otteniamo:

$$S = \int \rho(n_a, n_b) dn_a\, dn_b \big[\sqrt{2} n_a \cdot n_b\big]. \tag{3.7}$$

Allora, usando che $\int \rho(n_a, n_b) dn_a\, dn_b = 1$, per il modulo si ha:

$$|S| \leq \int \Big|\rho(n_a, n_b)\big[\sqrt{2} n_a \cdot n_b\big]\Big|\, dn_a\, dn_b \leq \sqrt{2} \int \rho(n_a, n_b) dn_a\, dn_b \leq \sqrt{2}.$$

Dunque risulta che $-\sqrt{2} \leq S \leq \sqrt{2}$, ossia rispetta la disuguaglianza di Bell, contraddicendo (3.5).

Questa contraddizione deriva dal fatto che particelle con valori di spin fissate a priori rispettano la disuguaglianza di Bell, al contrario di quelle invece

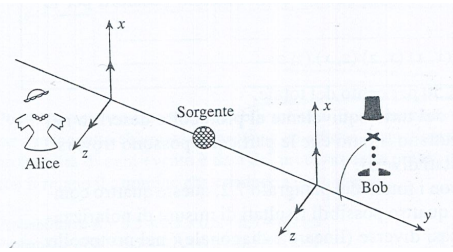
non misurate in precedenza ma direttamente emesse dalla sorgente. Parlando in termini quantistici, il fatto che Eva effettui la misura sulla particella fa sì che lo stato collassi in uno dei due possibili autostati, quindi le misure di Alice e Bob sono certe e non più probabilistiche.

Come già anticipato nel paragrafo precedente, si utilizza ora il secondo gruppo, quello per cui Alice e Bob hanno scelto misure discordi. Dunque si servono ognuno dei risultati dell'altro per capire se le coppie soddisfano la disuguaglianza di Bell. Se dovessero rispettarla allora sarebbe certa la presenza di un intercettatore.

3.2 Un secondo protocollo basato su EPR

Dall'idea di Ekert nel 1992 Charles Bennet e Gilles Brassard, insieme a David Mermin, proposero un secondo protocollo basato sempre sul paradosso EPR, ma più semplice. Infatti prevede che le misure di spin siano effettuate soltanto lungo due direzioni, non quattro. Alice e Bob compiono misure lungo l'asse x e y come in Figura 3.3.

Figura 3.3: Tratto da [9]



Per quanto riguarda il funzionamento è del tutto identico al protocollo E91: trasmissione quantistica, comunicazione pubblica delle direzioni scelte, associazione dei risultati ai bit 0 e 1. Oltre ad essere più semplice questo protocollo risulta anche più *efficiente*. Il concetto di efficienza a livello intuitivo può essere espresso nel seguente modo: "...a parità di numero di particelle misurate da Alice e Bob, esisteranno più casi in cui i risultati delle misure entrano a far parte della chiave" [9].

Infatti, nel caso del protocollo di Ekert la probabilità di trovare delle coppie utili alla creazione della chiave è pari al 22%, mentre nel caso in questione la probabilità è del 50%. Infatti nel primo protocollo esistono 9 combinazioni possibili, ma solo due sono utilizzabili per la formazione della chiave:

$$(a,b),(a,c),(a,d),(c,b),\mathbf{(c,c)},(c,d),(d,b),(d,c),\mathbf{(d,d)}.$$

Invece nel secondo ce ne sono solo 4, ma due utili:

$$\mathbf{(x,x)},\mathbf{(y,y)},(x,y),(y,x).$$

Infine è opportuno notare che questo secondo protocollo risulta essere equivalente al protocollo BB84, ideato dagli stessi Bennet e Brassard, ma presenta un vantaggio legato alla difficoltà pratica di quest'ultimo di conservare particelle polarizzate per tempi lunghi.

Conclusioni

Possiamo concludere che la fisica quantistica sia stata fondamentale per l'ideazione teorica di protocolli di distribuzione della chiave sicuri, *in primis* il protocollo di Ekert analizzato nello specifico. Tuttavia, essendo quello della meccanica quantistica un campo dello studio della crittografia "nuovo", per diversi anni queste idee rimasero ad un livello meramente teorico, senza produrre alcun risultato concreto a livello sperimentale. La ragione è legata principalmente alle tecnologie non adeguate per riprodurre questa tipologia di esperimenti, oltre che agli errori sperimentali, per cui è difficile distinguere questi dagli errori dovuti alla presenza di un intercettatore. Inoltre, bisogna sottolineare un fatto intuitivo: la crittografia quantistica permette di rilevare la presenza di Eva nella fase di condivisione della chiave, ma non propone una soluzione vera al problema dell'intercettatore. In altre parole, non suggerisce una tecnica per prevenire i tentativi di "origliare" di Eva e, nel momento in cui questa viene scoperta, la chiave condivisa diventa inutilizzabile.

Il primo tentativo di realizzazione sperimentale risale al 1990, quando Bennet e Brassard insieme a Smotlin riuscirono a comunicare in segretezza tramite il protocollo BB84. Successivamente ci furono diversi esperimenti basati su questa stessa idea, ma solo nel 2001 venne fondata la prima società, *IdQuantique*, che si occupava di costruire e distribuire prototipi commerciali di distribuzione quantistica della chiave. Seguirono *MagiQ*, *BBN Technologies*, ma anche altre aziende iniziarono ad interessarsi e decisero di investire in questo campo, come ad esempio Toshiba, NEC e Cornig.

Bisogna notare che la maggior parte delle implementazioni pratiche a cui si fa riferimento riguardano la polarizzazione dei fotoni, non la misura dello spin di elettroni come è previsto nel protocollo E91. Infatti, lo spin è una caratteristica delle particelle atomiche che sono difficili da manipolare, al contrario invece dei fotoni la cui manipolazione avviene per mezzo di campi elettromagnetici. Tuttavia, utilizzare misure di spin piuttosto che polarizzazioni dei fotoni presenterebbe sicuramente dei vantaggi a livello di funzionamento del protocollo, poiché nel caso del protocollo di Ekert non è necessario sacrificare parte della chiave per scoprire la presenza dell'intercet-

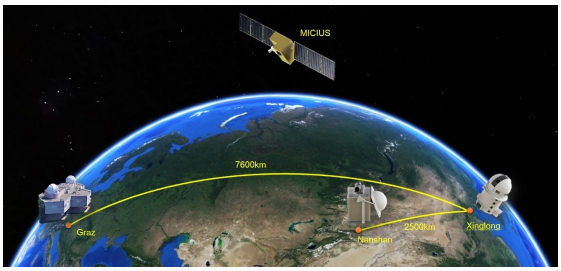
tatore, al contrario del BB84. Dunque, nonostante i limiti pratici, ci sono ancora tentativi di riprodurre esperimenti che utilizzino misure di spin per lo scambio quantistico della chiave in maniera sicura.

Il motivo del grande interesse nei confronti di questo ambito risiede principalmente nel fatto che la crittografia quantistica costituisce un sicuro sostituto alla crittografia a chiave pubblica, minacciata dall'avvento del computer quantistico. Tale interesse è scaturito soprattutto dal possibile passaggio futuro da sistemi di comunicazione classici a sistemi quantistici.

Uno dei problemi su cui sono basati alcuni dei sistemi crittografici attuali più efficienti, tra cui il noto RSA, è la fattorizzazione: dato un numero composto trovare la sua scomposizione in fattori primi. Per decifrare un messaggio cifrato tramite RSA si deve fare un'inversione dell'elevamento a potenza modulo un certo numero composto, che risulta essere molto difficile, soprattutto per via dei tempi tecnici, se non si conoscono i due primi (per maggiori dettagli si consulti [1]). Nel 1994 Peter Shor pubblicò un articolo [10] in cui veniva descritto un algoritmo in grado di fattorizzare in numeri primi in un tempo polinomiale grazie ad un computer quantistico. Questo renderebbe inefficiente ogni sistema crittografico basato sul principio sopra spiegato e quindi i sistemi crittografici conosciuti finora.

Per quanto riguarda la comunicazione quantistica, il più recente passo in avanti è stato compiuto in Cina negli ultimi anni, dove è stato creato il più esteso canale di comunicazione quantistica in fibra ottica. Il percorso, tra Pechino e Shanghai, ammonta a 2000 km, a fronte delle poche centinaia di km raggiunte fino ad allora a causa della perdita di segnale.

Figura 3.4: Illustrazione del collegamento tra Graz,Xinglong e Micius. Tratto da [7]

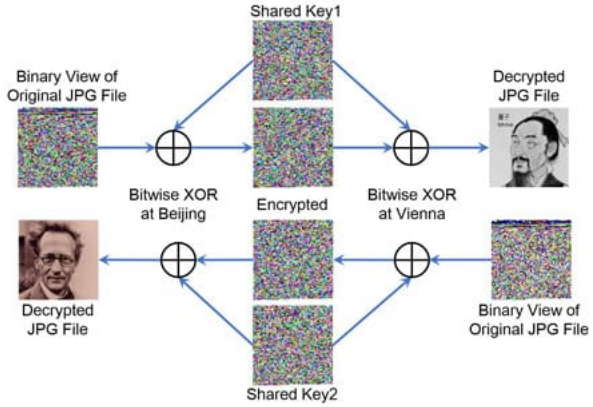


Inoltre, nel 2016 è stato lanciato il primo satellite sperimentale per comunicazioni quantistiche chiamato *Micius*, dal nome di un antico scienziato cinese. Grazie al satellite *Micius* è stato possibile comunicare in crittografia quantistica QKD tra Xinglong in Cina e Graz in Austria, separate da ben

7600 km, come mostrato nella Figura 3.4, dove *Micius* è stato utilizzato da "ponte" [7]. I ricercatori prima inviarono delle semplici immagini (Figura 3.5) e poi riuscirono ad avviare una videoconferenza.

Micius è parte di un progetto internazionale chiamato QUESS, acronimo di *Quantum Experiments at Space Scale*, che ha come obiettivo quello di creare un canale quantistico effettivamente utilizzabile tra Asia e Europa entro il 2020.

Figura 3.5: Rappresentazione dello schema quantistico di scambio della chiave che ha consentito di decifrare le immagini cifrate di Erwin Schroedinger (a sinistra), e del filosofo cinese Micius(a destra). Tratto da [7].



Bibliografia

[1] Pass, R., Shelat, A. (2010). *A Course in Cryptography.* Disponibile online sul sito https://www.cs.cornell.edu/courses/cs4830/2010fa/lecnotes.pdf

[2] Ekert, A. K.(1991). Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, 67, 6, 661-663

[3] Wiesner., S. (1983). Conjugate coding. *SIGACT News*, 15, 1, 78-88

[4] Bennett, C. H. , Brassard, G. (1984).Quantum cryptography: Public key distribution and coin tossing *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175-179

[5] Benenti, G. ,Casati, G. ,Strini, G.(2004) *Principles of Quantum Computation and Information*, Volume 1: Basic Concept. Singapore: World Scientific Publishing Co. Pte. Ltd.

[6] Bohm, D. (1979) *Quantum Theory.* Englewood Cliffs, NJ: Prentice Hall

[7] Liao, S. K. (2018). Satellite-relayed intercontinental quantum network. *Physical Review Letters*, 120, 3

[8] Clauser, J. F. , Horne, M. A. , Shimony, A. , Holt, R. A.(1969). Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*, 23, 880

[9] Filoramo, E. , Giovannini, A. , Pasquero, C. (2006). *Alla scoperta della crittografia quantistica*, Torino:Bollati-Boringhieri

[10] Shor, P. W. (1994). Algorithms for quantum computation: Discrete Logarithms and Factoring. *Proceedings of 35th Annual Symposium on Foundations of Computer Science*

[11] Aspect, A. , Grangier, P. , Roger, G. (1982). Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Physical Review Letters* , 49, 2, 91–4

[12] Rudin, W.(1970). *Real and Complex Analysis*, Mladinska Knjiga: McGraw-Hill

[13] Lang, S. (1992) *Algebra lineare*, Torino:Bollati Boringhieri

Ringraziamenti

Ringrazio innanzitutto il mio relatore, il prof. Davide Aliffi, per la disponibilità e per l'aiuto nella stesura del mio lavoro, e per avermi dato la possibilità di approfondire una materia così affascinante.

Ringrazio inoltre la mia correlatrice, la prof.ssa Elisa Ercolessi, per i suoi preziosi consigli e per avermi aiutata a entrare nel mondo della fisica quantistica.

Ringrazio i miei cari amici e i miei colleghi di corso per avermi incoraggiata e per aver creduto in me.

Un grazie anche a Federico per avermi sostenuta nei momenti più difficili.

Infine ringrazio la mia famiglia che mi ha permesso di sostenere i miei studi al meglio e che mi è stata sempre vicina, anche se lontana da me.