Alma Mater Studiorum · Università di Bologna

Dipartimento di Fisica e Astronomia "Augusto Righi"
Corso di Laurea in Fisica

ENTANGLEMENT E CRITTOGRAFIA QUANTISTICA: FONDAMENTI E ANALISI DEL PROTOCOLLO E91

Relatore:
Prof. Lorenzo Piroli

Presentata da:
Eleonora Paoletti

Anno Accademico 2024/2025

Sommario

In questa tesi viene analizzato il ruolo dell'entanglement quantistico come risorsa fondamentale per la crittografia, con particolare attenzione al protocollo E91. Dopo aver introdotto i concetti di base della meccanica quantistica e delle correlazioni non locali, si mette in evidenza come la violazione delle disuguaglianze di Bell possa trasformarsi in uno strumento concreto per garantire la sicurezza delle comunicazioni. L'attenzione si concentra quindi sulla struttura del protocollo E91, mostrando come i meccanismi di correzione d'errore e di privacy amplification permettano di adattare la teoria a scenari realistici, nei quali rumore e perdite sono inevitabili. Infine, viene discusso l'aspetto sperimentale, dalla generazione e distribuzione delle coppie entangled alle prospettive di implementazione su lunga distanza, delineando il protocollo non solo come una proposta teorica elegante, ma come un punto di partenza verso lo sviluppo di reti quantistiche sicure su scala globale.

Indice

Introduzione

La teoria dell'informazione quantistica nasce dall'incontro tra due idee profonde: da un lato, la nozione classica di informazione e i suoi limiti; dall'altro, le regole della meccanica quantistica che ridefiniscono cosa sia possibile comunicare, misurare e preservare. Mentre nel mondo classico l'informazione può essere copiata e trasmessa senza vincoli profondi; in quello quantistico entrano in gioco caratteristiche radicalmente nuove: gli stati possono trovarsi in sovrapposizione, non sono in generale distinguibili con certezza e — come vedremo — non possono essere copiati perfettamente. Queste differenze, che di primo acchito potrebbero apparire degli ostacoli nel riprodurre i meccanismi della crittografia classica, si rivelano risorse pratiche che aprono la strada a protocolli di comunicazione e crittografia non solo in grado di riprodurre i corrispondenti classici, ma di superarli nettamente in sicurezza e potenzialità.
Al centro di questa rivoluzione sta l'entanglement: una proprietà dei sistemi quantistici composti che crea correlazioni più forti di quelle ammesse da qualsiasi modello classico locale. Più che un fenomeno paradossale, l'entanglement è oggi interpretato come una vera e propria *risorsa*— misurabile, manipolabile e sfruttabile in protocolli di calcolo, comunicazione e, soprattutto, crittografia. Dal punto di vista pratico, coppie massimamente entangled consentono a due parti di ottenere esiti perfettamente correlati pur essendo ciascun esito individuale casuale; dal punto di vista concettuale, la monogamia dell'entanglement e il teorema del no-cloning garantiscono che un avversario non può apprendere tali correlazioni senza lasciare tracce misurabili.
Dunque, questa tesi esplora il ruolo dell'entanglement nella generazione sicura di chiavi crittografiche. Partendo da un inquadramento teorico (concetti di qubit, spazio di Hilbert e sistemi composti) e dalle proprietà peculiari come la sovrapposizione, l'entanglement e le disuguaglianze di Bell nel Capitolo 1, nel secondo si passa ad analizzare i meccanismi (effetti del disturbo di misura, teorema del no-cloning e monogamia dell'entanglement) che rendono possibili protocolli di *Quantum Key Distribution* (QKD), fino a concentrarsi, nel Capitolo 3, su come questi vengano applicati al protocollo E91, analizzato nella sua struttura e nei meccanismi di sicurezza.
L'obiettivo del lavoro è mostrare come concetti apparentemente astratti diventino criteri concreti per progettare, analizzare e valutare sistemi di comunicazione realmente sicuri nel mondo quantistico.

Capitolo 1

Fondamenti di computazione quantistica

1.1 Il qubit e la sovrapposizione

Per comprendere la crittografia quantistica, il primo passo è ridefinire il concetto di informazione elementare. Nel mondo classico, il bit è l'unità fondamentale: una variabile che può assumere esclusivamente uno dei due valori possibili, 0 oppure 1. Nel contesto quantistico, questa nozione viene estesa introducendo il *qubit* (quantum bit) [1], che rappresenta il sistema quantistico più semplice e che, come il bit classico, possiede due stati base distinti, indicati convenzionalmente con $|0\rangle$ e $|1\rangle$.

A differenza dell'equivalente classico, però, un qubit non è limitato ad assumere solo uno di questi due stati. In virtù del **Primo Postulato della meccanica quantistica** [1], ad ogni sistema fisico isolato è associato uno spazio di Hilbert, cioè uno spazio vettoriale complesso dotato di prodotto scalare. Lo stato del sistema è descritto da un vettore unitario appartenente a questo spazio, detto *vettore di stato*. Nel caso di un qubit, lo spazio di Hilbert è bidimensionale e ogni stato puro può essere espresso come combinazione lineare (o *sovrapposizione*) degli stati base:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle,$$

dove $a, b \in \mathbb{C}$ sono detti *ampiezze di probabilità*, e soddisfano la condizione di normalizzazione

$$|a|^2 + |b|^2 = 1.$$

Il modulo al quadrato di ciascun coefficiente rappresenta la probabilità di ottenere il corrispondente stato base in seguito ad una misura nella cosiddetta *base computazionale*.

Il concetto di sovrapposizione è centrale: esso afferma che un qubit può trovarsi simultaneamente "in parte" nello stato $|0\rangle$ e "in parte" nello stato $|1\rangle$, con proporzioni e fasi relative determinate dai coefficienti complessi a e b [2]. Questa proprietà, priva di

analoghi nel mondo classico, è alla base di molti fenomeni unicamente quantistici e sarà un elemento essenziale quando, nei capitoli successivi, introdurremo l'entanglement.

Un modo intuitivo per visualizzare lo stato di un qubit è la *sfera di Bloch* [1]. Grazie al fatto che un fattore di fase globale non è osservabile e quindi può sempre essere eliminato, ogni stato puro di un qubit può essere scritto come:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle,$$

dove $0 \leq \theta \leq \pi$ e $0 \leq \phi < 2\pi$ sono due angoli che identificano univocamente un punto sulla superficie di una sfera unitaria.

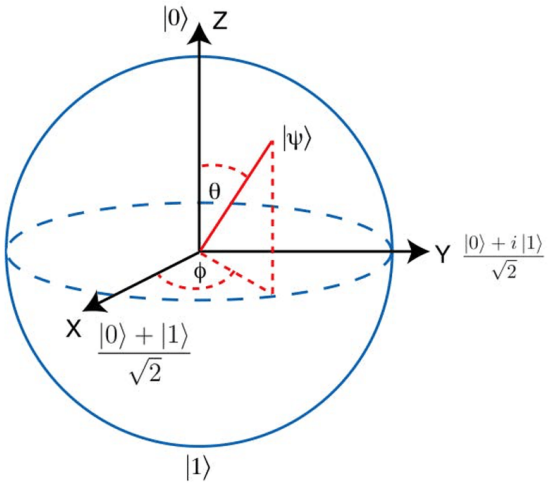


Figura 1.1: Sfera di Bloch [1]

Il polo nord ($\theta = 0$) corrisponde allo stato $|0\rangle$, il polo sud ($\theta = \pi$) allo stato $|1\rangle$, mentre i punti sull'equatore rappresentano sovrapposizioni equiprobabili dei due stati base, con diverse fasi relative.

Per esempio, lo stato:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

rappresenta una sovrapposizione in cui i due esiti sono equiprobabili e in fase tra loro, mentre:

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

ha la stessa distribuzione di probabilità ma una fase relativa di π.
Questi stati giocano un ruolo cruciale nei protocolli di crittografia quantistica [3], poiché

permettono di sfruttare interferenze e correlazioni quantistiche che non hanno controparte classica.

In sintesi, il Primo Postulato stabilisce il contesto matematico (lo spazio di Hilbert e la natura vettoriale dello stato quantistico) e garantisce il *principio di sovrapposizione*. Tale principio è la radice delle differenze tra informazione classica e informazione quantistica, e prepara il terreno per concetti più complessi come l'evoluzione unitaria e l'entanglement, che analizzeremo nelle sezioni successive.

1.2 Sistemi composti ed entanglement

Finora il qubit è stato introdotto come il sistema quantistico più elementare, la cui descrizione matematica è data da uno spazio di Hilbert di dimensione due. Tuttavia, molti fenomeni di interesse per la crittografia quantistica — e, in particolare, per il protocollo E91 — si manifestano unicamente quando si considerano sistemi composti da più sottosistemi.

In ambito classico, la descrizione congiunta di due sistemi è piuttosto intuitiva: se un sistema può trovarsi in n stati e un altro in m stati, la combinazione può trovarsi in una delle $n \times m$ possibili coppie di stati. Nel mondo quantistico, la struttura matematica che consente di descrivere correttamente questa combinazione è il *prodotto tensoriale* degli spazi di Hilbert [1].

Il **Quarto Postulato della meccanica quantistica** afferma infatti che lo spazio di stati di un sistema composto è dato dal prodotto tensoriale degli spazi di stati dei sottosistemi [1]. In formula, se un sistema A ha stato $|\psi_A\rangle$ appartenente allo spazio $\mathcal{H}_A$ e un sistema B ha stato $|\psi_B\rangle$ appartenente a $\mathcal{H}_B$, lo stato complessivo si scrive come:

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle,$$

dove $\otimes$ indica il prodotto tensoriale. Più in generale, per n sistemi indipendenti:

$$|\psi_{1\ldots n}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.$$

Questa costruzione è alla base di tutta la teoria dei sistemi quantistici composti, ed è la cornice matematica che rende possibile definire e studiare l'entanglement.

Per capire perché il prodotto tensoriale sia essenziale, consideriamo due qubit A e B. Se A può trovarsi in una qualunque sovrapposizione di $|0\rangle_A$ e $|1\rangle_A$, e lo stesso vale per B, allora lo spazio congiunto $\mathcal{H}_A \otimes \mathcal{H}_B$ non solo contiene le *combinazioni dirette* degli stati base

$$|0\rangle_A \otimes |0\rangle_B, \quad |0\rangle_A \otimes |1\rangle_B, \quad |1\rangle_A \otimes |0\rangle_B, \quad |1\rangle_A \otimes |1\rangle_B,$$

ma anche tutte le loro combinazioni lineari [2]. Ciò significa che, a differenza del caso classico, è possibile avere stati che non si riducono a un semplice "prodotto" di due stati individuali.

Uno stato del sistema AB si dice *separabile* o *non entangled* se può essere scritto come prodotto tensoriale di uno stato di A e uno stato di B:

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle.$$

Al contrario, si parla di *stato entangled* quando tale fattorizzazione non è possibile.

> If two separated bodies, each by itself known maximally, enter a situation in which they influence each other, and separate again, then there occurs regularly that which I have just called entanglement of our knowledge of the two bodies [4].

Un esempio noto è lo stato di Bell:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

che non può essere espresso come prodotto di due stati singoli [1]. In questo stato, le misure effettuate sul qubit A e sul qubit B mostrano correlazioni che non possono essere spiegate da alcuna teoria classica a variabili nascoste locali, come vedremo discutendo la disuguaglianza di Bell [5].

La differenza tra stati separabili ed entangled è sostanziale: mentre nei primi l'informazione sullo stato complessivo è interamente contenuta nelle descrizioni individuali di A e B, negli stati entangled esiste un contenuto informativo "non locale" che emerge solo considerando il sistema come un tutto unico. Questo fenomeno, che non ha analoghi classici, è alla base di protocolli di comunicazione e sicurezza impossibili nel mondo tradizionale, inclusa la distribuzione di chiavi quantistiche sicure [3].

Un aspetto importante del Quarto Postulato è che esso fornisce anche la struttura matematica per introdurre sistemi ausiliari, detti *ancilla*, utilizzati come supporto in molte operazioni di elaborazione quantistica. In crittografia, ad esempio, un'ancilla può essere impiegata per implementare misure complesse o per simulare l'effetto di un canale rumoroso, sfruttando il fatto che, unendo il sistema principale e l'ancilla in un unico spazio di Hilbert più ampio, si può realizzare qualsiasi operazione quantistica ammissibile tramite evoluzione unitaria e misurazione [1].

1.3 Stati di Bell e correlazioni non locali

Come discusso nella sezione precedente, la descrizione di sistemi composti in meccanica quantistica si fonda sul prodotto tensoriale degli spazi di Hilbert dei singoli sottosistemi. Questa struttura matematica non solo permette di rappresentare stati separabili, ma rende possibile la definizione di stati entangled, in cui le proprietà dei sottosistemi non possono essere descritte indipendentemente. Tra tutti gli stati entangled, un ruolo di

rilievo è ricoperto dagli *Stati di Bell* o *coppie EPR* (Einstein–Podolsky–Rosen), che rappresentano la forma massimamente entangled di un sistema a due qubit [1].

Un sistema bipartito puro è detto massimamente entangled quando la misura su uno dei sottosistemi lascia l'altro in uno stato completamente misto, ovvero descritto da una matrice densità proporzionale all'identità. Questo significa che, se si osserva solo uno dei due qubit e si ignora l'altro, il risultato sarà del tutto casuale: non c'è alcuna informazione sullo stato del qubit rimanente presa singolarmente. Tutti gli stati di Bell condividono questa caratteristica e possono essere trasformati l'uno nell'altro tramite semplici operazioni locali sui singoli qubit. Proprio per questa simmetria e per le loro correlazioni perfette, gli stati di Bell sono considerati una risorsa fondamentale in molti protocolli di comunicazione quantistica sicura [3].

Gli stati di Bell formano una base ortonormale dello spazio di Hilbert a due qubit e sono definiti come:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \qquad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \qquad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

In ciascuno di questi stati, la misura di un qubit determina istantaneamente lo stato dell'altro, indipendentemente dalla distanza che li separa. Ad esempio, nello stato $|\Phi^+\rangle$, la misura nella base computazionale restituisce esiti perfettamente correlati: se il primo qubit è 0, anche il secondo sarà 0; se il primo è 1, il secondo sarà 1. Ciascun risultato è imprevedibile singolarmente, ma le correlazioni tra le misure sono determinate con certezza.

Ciò che rende questi stati particolarmente rilevanti è che queste correlazioni non sono limitate alla base computazionale: se entrambi i qubit vengono misurati in basi diverse (ad esempio ruotate sulla sfera di Bloch), le correlazioni statistiche previste dalla meccanica quantistica persistono, assumendo forme non spiegabili con modelli classici. Questo aspetto fu evidenziato da Einstein, Podolsky e Rosen che, nel 1935, proposero un *gedankenexperiment* — noto come **paradosso EPR** — in cui misero in dubbio la completezza della meccanica quantistica, invocando l'esistenza di variabili nascoste per spiegare tali correlazioni [6].

Il passo decisivo fu compiuto nel 1964 da John Bell, che dimostrò come ogni teoria a variabili nascoste locali debba soddisfare determinate relazioni, conosciute ad oggi come *disuguaglianze di Bell* [5]. Le previsioni della meccanica quantistica per stati entangled, e in particolare per gli stati di Bell, violano tali disuguaglianze, indicando che le correlazioni quantistiche sono intrinsecamente *non locali*. Questo risultato ha trovato conferma sperimentale in una lunga serie di test, culminati negli esperimenti *loophole-free*

degli anni più recenti, che hanno consolidato la natura non classica di queste correlazioni e valso il Premio Nobel per la Fisica 2022 ad Aspect, Clauser e Zeilinger.

Dal punto di vista operativo, gli stati di Bell possono essere generati a partire da stati separabili tramite semplici operazioni quantistiche. Ad esempio, partendo da $|00\rangle$, l'applicazione di una porta di Hadamard al primo qubit seguita da una porta CNOT (con il primo qubit come controllo e il secondo come bersaglio) produce lo stato $|\Phi^+\rangle$. Analoghe sequenze consentono di ottenere gli altri tre stati della base di Bell.

Approfondimento

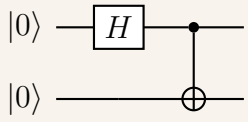


Figura 1.2: Generazione dello stato di Bell $|\Phi^+\rangle$ a partire dallo stato separabile $|00\rangle$.

Porte Hadamard e CNOT. La *porta di Hadamard* H è un'operazione unitaria che agisce su un singolo qubit trasformando gli stati base come:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

In forma matriciale:

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

Essa genera una *sovrapposizione* equiprobabile dei due stati base, condizione necessaria per la creazione di entanglement.
La *porta CNOT* (*Controlled-NOT*) è un'operazione a due qubit in cui il primo agisce da controllo (*control qubit*) e il secondo da bersaglio (*target qubit*). La sua azione è la seguente:

$$\text{CNOT}\,|x, y\rangle = |x,\, y \oplus x\rangle\,,$$

dove $\oplus$ denota la somma modulo 2. In altre parole, il bersaglio viene invertito se e solo se il controllo è nello stato $|1\rangle$. In forma matriciale, nella base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Generazione di $|\Phi^+\rangle$. Applicando H al primo qubit dello stato iniziale $|00\rangle$, si ottiene:

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

Successivamente, la porta CNOT, con il primo qubit come controllo e il secondo come bersaglio, trasforma $|10\rangle$ in $|11\rangle$ e lascia $|00\rangle$ invariato, producendo:

$$\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Pertanto, gli stati di Bell non sono soltanto una verifica per i fondamenti della meccanica quantistica, ma rappresentano una risorsa tecnologica concreta. La loro capacità di generare correlazioni non locali e resistenti a descrizioni classiche è alla base della sicurezza fisica dei protocolli di distribuzione di chiavi quantistiche come l'E91, trasformando un fenomeno apparentemente paradossale in uno strumento pratico per la protezione dell'informazione [3].

1.4 Paradosso EPR e le disuguaglianze di Bell

> *"La meccanica quantistica è degna di ogni rispetto, ma una voce interiore mi dice che non è ancora la soluzione giusta. È una teoria che ci dice molte cose, ma non ci fa penetrare più a fondo il segreto del gran Vecchio. In ogni caso, sono convinto che questi non gioca a dadi col mondo".*
>
> — A. Einstein, 1926. Lettera a Max Born [7].

Negli anni Trenta del Novecento, Albert Einstein, Boris Podolsky e Nathan Rosen sollevarono una critica profonda alla meccanica quantistica, nota come paradosso EPR [6]. Al centro della loro argomentazione vi era il concetto di "elemento di realtà": una proprietà fisica che può essere predetta con certezza senza disturbare il sistema e che dovrebbe essere rappresentata in qualsiasi teoria fisica completa. Oltre al principio di realismo sostenevano quello di **località**, secondo cui l'informazione derivante da una misura su uno dei due sistemi isolati non può produrre un cambiamento reale nell'altro.

Per discutere la completezza della funzione d'onda, EPR considerano due sistemi I e II che interagiscono in un intervallo $[0, T]$ e poi si separano definitivamente. Per $t > T$, lo stato composto $\Psi(x_1, x_2)$ è noto (calcolabile tramite l'equazione di Schrödinger a partire dallo stato iniziale). Tuttavia, lo stato di ciascun sottosistema non è definito in termini di valori certi prima della misura, ma è descritto da una matrice densità ridotta.

Solo l'atto della misura determina, tramite la *riduzione del pacchetto d'onda*, uno stato puro corrispondente all'esito osservato. Se si misura su I un osservabile A con autostati $\{u_n(x_1)\}$, si può scrivere:

$$\Psi(x_1, x_2) = \sum_n \phi_n(x_2)\, u_n(x_1).$$

Un esito a_k proietta il sistema I nello stato $u_k(x_1)$ e, simultaneamente, II nello stato condizionato $\phi_k(x_2)$. Se invece si misura un osservabile B non commutante con A, con autostati $\{v_s(x_1)\}$, si ottiene una diversa decomposizione:

$$\Psi(x_1, x_2) = \sum_s \varphi_s(x_2)\, v_s(x_1).$$

Poiché, per ipotesi, dopo T non c'è più interazione tra I e II, la *realtà fisica* del sistema II non può dipendere dalla scelta di misura compiuta su I; eppure, a seconda se su I si misuri A oppure B, a II vengono assegnate funzioni d'onda *diverse* (rispettivamente ϕ_k o φ_r), associate per di più a osservabili P e Q non commutanti su II. Ne segue che, per via della sola *scelta a distanza* della misura su I, possiamo prevedere con certezza ora P ora Q su II *senza* disturbarlo: per il criterio EPR, *entrambe* le grandezze sono allora elementi di realtà del sistema II. Se la funzione d'onda fosse una descrizione completa, dovrebbe contenere simultaneamente questi valori; ma ciò è impossibile quando gli operatori non commutano. Dunque, conclude EPR, la descrizione fornita dalla funzione d'onda non è completa [6].

Nella formulazione originaria, l'esempio riguarda variabili continue accoppiate: due particelle sono preparate in uno stato per cui la combinazione $x_1 - x_2$ e la somma delle quantità di moto $p_1 + p_2$ sono perfettamente correlate. Con una misura su I si può predire con certezza la coordinata (o il momento) di II; con una misura alternativa, *incompatibile* con la prima, si può predire esattamente il suo momento (o la sua coordinata). Poiché la scelta tra le due misure su I non può alterare la realtà fisica di II, EPR deducono che coordinate e momenti per II debbano possedere valori ben definiti simultaneamente, sebbene gli operatori corrispondenti non commutino: l'inevitabile conclusione è l'*incompletezza* della funzione d'onda [6].

Una riformulazione moderna dello stesso schema logico usa gradi di libertà di spin o qubit. Consideriamo, ad esempio, lo stato di singoletto

$$\left|\psi^-\right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}},$$

che esibisce anticorrelazione perfetta per misure di spin lungo qualunque direzione $\vec{v}$: misurando $\sigma_{\vec{v}}$ su entrambi i qubit, gli esiti sono sempre opposti (± 1). Se Alice e Bob sono lontani, l'esito di Alice permette di *predire con certezza* l'esito di Bob quando misura nella stessa direzione: per il criterio EPR, il valore di $\sigma_{\vec{v}}$ di Bob è un elemento di realtà.

Ma poiché Alice avrebbe potuto scegliere un'altra direzione $\vec{w}$ (non commutante con $\vec{v}$), anche $\sigma_{\vec{w}}$ di Bob sarebbe predicibile con certezza e dunque un elemento di realtà. La coesistenza di *entrambi* gli elementi per osservabili non commutanti contraddice la struttura della teoria standard, riproponendo la tensione fra completezza della funzione d'onda e *realismo locale*.

EPR indicano quindi un bivio concettuale: o si rinuncia alla completezza della funzione d'onda introducendo ulteriori variabili ("nascoste") che ripristinino una descrizione realistica, oppure si accetta che non tutte le grandezze fisiche ammettano valori preesistenti e simultanei quando i relativi operatori non commutano. Storicamente, la risposta sperimentale a questa tensione arriva nel 1964 con John Bell, che mostrò l'incompatibilità del *realismo locale* con le predizioni quantistiche [5]. Infatti, Bell formulò un risultato fondamentale che traduce questa discussione in un test quantitativo: le **disuguaglianze di Bell**. Queste stabiliscono un limite massimo alla correlazione tra risultati di misure su sistemi spazialmente separati, valido per qualsiasi teoria a variabili nascoste locali.

Una delle formulazioni più rilevanti delle disuguaglianze di Bell è l'**ineguaglianza CHSH** (Clauser–Horne–Shimony–Holt) [8]. Essa considera due osservatori spazialmente separati, convenzionalmente detti Alice e Bob, ciascuno in possesso di una particella di un sistema bipartito. Alice può scegliere di misurare una delle due osservabili Q o R, mentre Bob può misurare una delle due osservabili S o T. Ciascuna osservabile è rappresentata da un operatore hermitiano con autovalori ± 1. Ripetendo l'esperimento su un insieme statistico di coppie preparate nello stesso stato, si considerano le correlazioni $E(QS)$, $E(RS)$, $E(RT)$ ed $E(QT)$ e si definisce la combinazione

$$S = E(Q,S) + E(R,S) + E(R,T) - E(Q,T).$$

Nel quadro del realismo locale, vale il vincolo

$$|S| \leq 2,$$

mentre la meccanica quantistica ammette violazioni fino al limite teorico di Cirel'son, $|S| \leq 2\sqrt{2}$ [9], raggiungibile per stati massimamente entangled e scelte ottimali delle direzioni di misura.

> Il limite di Cirel'son quantifica quanto "non locale" può essere la meccanica quantistica, pur rimanendo coerente con le sue regole interne. Nel contesto di un protocollo QKD come l'E91, la verifica sperimentale che S superi 2 (limite classico) ma non superi $2\sqrt{2}$ è una prova sia della presenza di entanglement sia della conformità con la teoria quantistica.

Questa violazione è stata confermata sperimentalmente in numerosi contesti, dai primi esperimenti di Aspect negli anni '80 [10] fino ai moderni test *loophole-free* [11].

La rilevanza delle disuguaglianze di Bell per la crittografia quantistica — e in particolare per il protocollo E91 — risiede nel fatto che la violazione osservata fornisce una certificazione *device-independent* dell'entanglement. Infatti, studiando il protocollo E91, analizzeremo dal punto di vista operativo come, grazie alla verifica delle disuguaglianze CHSH, vengano scoperte eventuali intercettazioni.

Le disuguaglianze di Bell, nate come strumento concettuale per indagare i fondamenti della meccanica quantistica, diventano così, nella seconda rivoluzione quantistica, un elemento operativo cruciale per la sicurezza delle comunicazioni quantistiche basate su entanglement.

Capitolo 2

Sicurezza e informazione quantistica

2.1 Il disturbo della misura

Un aspetto che segna una vera frattura rispetto alla fisica classica è il ruolo della misura nei sistemi quantistici. Nella descrizione classica, almeno idealmente, misurare una grandezza significa semplicemente leggere un valore già esistente, senza modificare lo stato del sistema. In meccanica quantistica, invece, la misura non si limita a rivelare un'informazione: essa *interviene attivamente* sullo stato, alterandolo in modo irreversibile. Non è più, quindi, perfettamente netta neanche la distinzione tra chi è l'oggetto e chi il soggetto della misura, non esiste più l'osservatore della fisica classica "esterno" al sistema:lo stesso osservatore (che può anche semplicemente consistere nell'apparato di misura) cambia l'esito di un esperimento. È per questo motivo che la misura quantistica viene spesso definita *intrinsecamente probabilistica e distruttiva* [12].

Dal punto di vista formale, il cosiddetto **Postulato 3** della meccanica quantistica stabilisce che una misura è descritta da un insieme di operatori $\{M_m\}$, detti *operatori di misura*, che agiscono sullo spazio di Hilbert del sistema e che rispettano la condizione di completezza

$$\sum_m M_m^\dagger M_m = I.$$

Se lo stato iniziale del sistema è $|\psi\rangle$, la probabilità di osservare l'esito m è data da

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle ,$$

mentre lo stato post-misura (condizionato a quell'esito) diventa

$$|\psi_m\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}.$$

Questa regola, apparentemente tecnica, porta con sé una conseguenza di fondamentale importanza: dopo la misura lo stato non è più quello di partenza, ma uno stato nuo-

vo, compatibile con il risultato osservato [1]. Oltre alla formulazione più generale delle misure *POVM* (Positive Operator-Valued Measures) appena riportata, un caso particolarmente importante è quello delle *misure proiettive* (o misure di von Neumann), in cui ciascun esito è associato a un proiettore ortogonale P_m. In questo scenario, il risultato corrisponde a un autovalore di un osservabile hermitiano, e il sistema collassa in uno degli autostati $|m\rangle$. Inoltre, tali misure sono *ripetibili*: se subito dopo la prima esecuzione si misura nuovamente lo stesso osservabile, il risultato sarà lo stesso con probabilità unitaria, proprio perché lo stato è già collassato in un autostato corrispondente [12, 2]. Questo formalismo amplia il quadro tradizionale, permettendo di descrivere situazioni più realistiche, come misure rumorose o incomplete.

Il carattere peculiare della misura quantistica si apprezza pienamente quando si considerano osservabili incompatibili. Per esempio, se un qubit nello stato $\alpha\,|0\rangle + \beta\,|1\rangle$ viene misurato nella base computazionale $\{|0\rangle, |1\rangle\}$, i risultati possibili sono 0 e 1, con probabilità $|\alpha|^2$ e $|\beta|^2$. Se però scegliamo la base di Hadamard $\{|+\rangle, |-\rangle\}$, con $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, le probabilità diventano

$$p(+) = \frac{|\alpha+\beta|^2}{2}, \qquad p(-) = \frac{|\alpha-\beta|^2}{2}.$$

In questo modo emerge chiaramente che la scelta della base di misura cambia radicalmente le statistiche degli esiti. In termini più profondi, ciò significa che non è possibile conoscere simultaneamente con precisione osservabili che non commutano, come formalizzato dal principio di indeterminazione di Heisenberg.

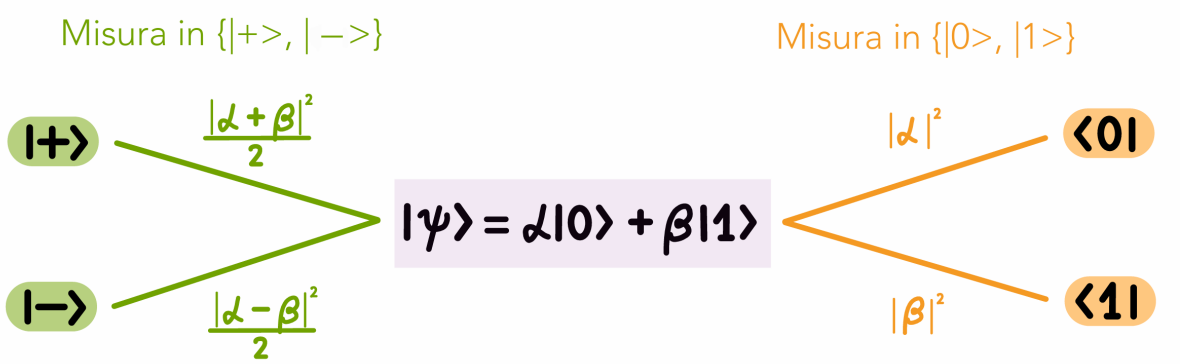


Figura 2.1: Effetto del disturbo della misura: lo stesso stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ produce esiti diversi a seconda della base scelta. A destra la misura nella base computazionale, a sinistra quella nella base di Hadamard

Il messaggio che emerge è che il *disturbo della misura* non è un inconveniente tecnico legato all'imperfezione degli strumenti, ma una caratteristica costitutiva della teoria quantistica. Ogni misura modifica inevitabilmente lo stato del sistema, e questo fatto,

che sfida l'intuizione classica, diventa invece una risorsa preziosa. Nei protocolli di distribuzione di chiavi quantistiche (QKD), infatti, l'eventuale presenza di un eavesdropper che tenti di misurare i qubit si traduce in un disturbo rilevabile, che consente ad Alice e Bob di accorgersi dell'intrusione [11]. In questo senso, quella che potrebbe sembrare una "debolezza" della teoria quantistica si trasforma in un principio di sicurezza fondato sulle leggi stesse della natura.

2.2 Il teorema del *no-cloning*

Introduzione e contesto storico Il teorema del *no-cloning* è una delle affermazioni centrali dell'informazione quantistica: esso stabilisce che non esiste un'operazione quantistica che, partendo da uno stato puramente ignoto, ne produca una copia perfetta in modo universale. Sebbene a primo impatto possa sembrare un limite, vedremo che svolgerà un ruolo cruciale nel protocollo E91, sventando possibili intercettazioni. Questo teorema mette in evidenza una differenza fondamentale rispetto all'informazione classica (dove la copia è banale) e si radica nella struttura lineare dell'evoluzione quantistica, con profonde implicazioni concettuali sulla natura dello stato quantistico. Le prime formulazioni del teorema risalgono all'inizio degli anni ottanta (Wootters–Zurek e Dieks), a seguito di proposte di schemi che suggerivano la possibilità di comunicazione superluminale via entanglement; la riflessione su tali proposte condusse alla formulazione rigorosa dell'impossibilità di clonare stati quantistici arbitrari [13, 14, 15].

Enunciato formale e prova elementare (stati puri) *Non esiste un processo quantistico che, per ogni stato puro arbitrario $|\psi\rangle$, produca due copie perfette $|\psi\rangle \otimes |\psi\rangle$.*

Prova per stati puri (argomento di linearità) Per dimostrare il teorema del no-cloning si può adottare un ragionamento per assurdo. Come discusso nell'Appendice A, il teorema di Kraus garantisce che ogni evoluzione fisicamente ammissibile di un sistema quantistico può essere descritta come una mappa completamente positiva e a traccia preservata. In particolare, tale mappa può sempre essere realizzata introducendo un sistema ausiliario (un'ancella), facendo evolvere congiuntamente sistema e ancella tramite un operatore unitario, e infine tracciando via l'ancella.

Alla luce di ciò, se la clonazione perfetta di uno stato quantistico fosse possibile, essa dovrebbe necessariamente poter essere realizzata mediante un'evoluzione unitaria estesa a un sistema più ampio che comprenda, oltre al qubit da clonare, anche l'ancella che rappresenta la "macchina di clonazione".

Formalmente, postuliamo dunque l'esistenza di un operatore unitario U tale che, per ogni stato puro $|\psi\rangle$, valga la trasformazione ideale

$$U\big(|\psi\rangle \otimes |R\rangle \otimes |M\rangle\big) = |\psi\rangle \otimes |\psi\rangle \otimes |M(\psi)\rangle\,, \tag{2.1}$$

dove $|R\rangle$ è lo stato destinato alla copia e $|M\rangle$ lo stato iniziale della macchina, che può anche evolvere in uno stato dipendente da ψ, indicato con $|M(\psi)\rangle$. Questa assunzione, che sembra ragionevole se pensiamo per analogia alla copiatura classica dell'informazione, è proprio il punto d'inizio della dimostrazione per assurdo: mostrare che una tale unitaria non può esistere se non nei casi banali di stati ortogonali. Consideriamo, infatti, due stati ortonormali di base $|0\rangle$ e $|1\rangle$ per i quali (per ipotesi) il cloner lavora correttamente:

$$U\big(|0\rangle\,|R\rangle\,|M\rangle\big) = |0\rangle\,|0\rangle\,|M(0)\rangle\,, \qquad U\big(|1\rangle\,|R\rangle\,|M\rangle\big) = |1\rangle\,|1\rangle\,|M(1)\rangle\,.$$

Per linearità dell'operazione unitaria e per sovrapposizione, se si applica U alla sovrapposizione $|0\rangle + |1\rangle$ si ottiene

$$U\big((|0\rangle + |1\rangle)\,|R\rangle\,|M\rangle\big) = |0\rangle\,|0\rangle\,|M(0)\rangle + |1\rangle\,|1\rangle\,|M(1)\rangle\,,$$

che non coincide (in generale) con la copia perfetta del sovrapposto, ossia con

$$\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes |M(0+1)\rangle\,.$$

Questa contraddizione evidenzia che non esiste U che cloni perfettamente *tutti* gli stati; si può anche ricavare la condizione più generale sulla preservazione del prodotto scalare che implica che solo stati mutuamente ortogonali (o identici) possono essere clonati perfettamente [13, 14]. Come argomento di dimostrazione, al posto della linearità, si possono applicare esplicitamente le proprietà degli operatori unitari, come mostrato in Appendice B. Quindi, nel mondo quantistico non è possibile riprodurre una fotocopiatrice classica 2.2, Fissiamo le idee con il seguente esempio visivo:

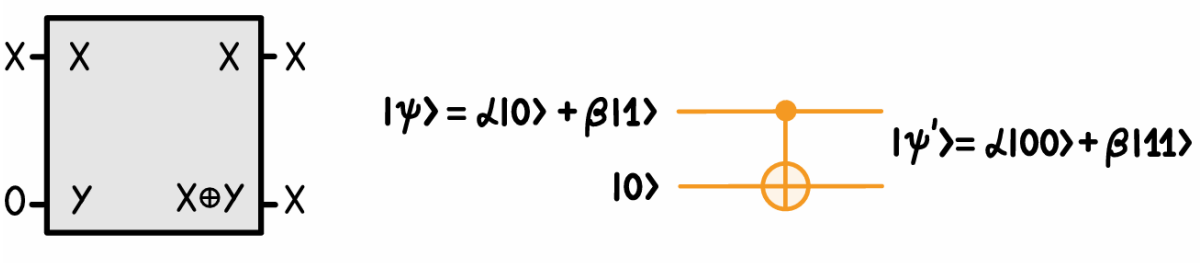


Figura 2.2: fotocopiatrice classica (a sinistra) e circuito con porta CNOT che tenta di riprodurre una fotocopiatrice quantistica

Se la fotocopiatrice quantistica funzionasse perfettamente, dovrei ottenere lo stato dei due qubit clonato:

$$|\psi\rangle_1 \otimes |0\rangle_2 \xrightarrow{\text{CLONA}} |\psi\rangle_1 \otimes |\psi\rangle_2$$

ovvero,

$$(\alpha\,|0\rangle + \beta\,|1\rangle)_1 \otimes |0\rangle_2 \;\longmapsto\; (\alpha\,|0\rangle + \beta\,|1\rangle)_1 \otimes (\alpha\,|0\rangle + \beta\,|1\rangle)_2.$$

Esplicitando i termini, lo stato risultante sarebbe

$$|\psi\rangle\,|\psi\rangle = \alpha^2\,|00\rangle + \alpha\beta\,|01\rangle + \alpha\beta\,|10\rangle + \beta^2\,|11\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle)(\alpha\,|0\rangle + \beta\,|1\rangle).$$

Questo stato non è entangled, infatti può essere scritto come prodotto di stati puri e non coincide con lo stato ottenuto con il circuito costituito dal CNOT.

Dal no-cloning al no-broadcasting: estensione a stati misti Per stati misti la questione è più sottile: clonare uno stato misto non significa necessariamente produrre il prodotto $\rho \otimes \rho$; è sufficiente che le marginali sul sistema A e B del complesso riproducano ρ. Questo problema di *broadcasting* è stato affrontato e risolto da Barnum *et al.* in modo rigoroso: esiste un canale fisico che broadcasta una famiglia $\{\rho_s\}$ se e solo se tutti gli elementi della famiglia commutano fra loro. In altre parole, non esiste broadcasting generale per stati misti non commutanti; il no-broadcasting generalizza così il no-cloning al caso misto. Per una trattazione completa e la dimostrazione basata sulle proprietà della fedeltà fra densità si veda [16].

Clonazione asimmetrica, clonazione dipendente dallo stato e attacchi su QKD Per studiare attacchi realistici su protocolli QKD (ad es. BB84, B92, etc.) si considerano frequentemente cloners asimmetrici o cloners ottimizzati per un sottoinsieme di stati (cloning *phase-covariant*, cloning per due stati, ecc.). In tali scenari la macchina lascia un clone di qualità maggiore e l'altro peggiore; questa asimmetria permette di modellare scambi d'informazione tra l'eavesdropper e il legittimo destinatario. I collegamenti formali tra misurazione ottimale (state estimation), clonazione ottimale e trade-off informazione-disturbo sono stati ampiamente studiati e sono parte integrante dell'analisi di sicurezza di attacchi incoerenti e, con opportune generalizzazioni, di attacchi più complessi nelle analisi moderne [15].

Il teorema del no-cloning è un esempio significativo di come un semplice principio matematico (linearità/unitarietà) abbia conseguenze operative e tecnologiche profonde. Esso impedisce la replicazione universale dell'informazione quantistica, ma apre contemporaneamente la strada a tecniche sofisticate: clonazione approssimata ottimale, clonazione probabilistica, strategie di attacco e difesa in QKD e implementazioni ottiche che sfruttano l'emissione stimolata. Comprendere sia la prova elementare sia le sue generalizzazioni (no-broadcasting, limiti di fidelità, relazioni con la stima dello stato) è essenziale per valutare correttamente il ruolo dell'entanglement e della non-località nella sicurezza dei protocolli come E91.

2.3 L'entanglement come risorsa per la sicurezza

Nelle sezioni precedenti abbiamo discusso l'entanglement come caratteristica fondamentale della meccanica quantistica, responsabile delle violazioni delle disuguaglianze di Bell e dei paradossi concettuali legati al realismo locale. In questa parte cambiamo radicalmente prospettiva: l'entanglement non è soltanto un fenomeno curioso, ma un'autentica *risorsa operativa*, alla base della possibilità stessa di implementare protocolli di comunicazione sicura. L'idea è che le correlazioni quantistiche non-classiche possano essere utilizzate come strumento per garantire la *privacy intrinseca* delle comunicazioni, senza doversi affidare ad assunzioni computazionali o ipotesi sulla potenza di calcolo dell'avversario.

Monogamia e protezione delle correlazioni

Una delle proprietà più importanti dell'entanglement è la cosiddetta *monogamia*. A differenza delle correlazioni classiche, che possono essere distribuite liberamente fra più sistemi, l'entanglement non è arbitrariamente condivisibile. Se due sistemi quantistici A e B sono massimamente entangled, la loro correlazione con qualsiasi terza parte E (eventualmente controllata da un intruso, Eve) è inevitabilmente limitata. Questo principio è stato formalizzato, per il caso dei qubit, dal teorema di Coffman–Kundu–Wootters (2000) [17], che esprime la concorrenza degli stati entangled come una quantità soggetta a precise disuguaglianze di monogamia.

Approfondimento

Teorema (Coffman–Kundu–Wootters). Per uno stato puro di tre qubit $|\psi_{ABC}\rangle$, si definisce la *concorrenza* C_{XY}[1]come misura dell'entanglement bipartito tra due sottosistemi X e Y. Il teorema afferma che:

$$C^2_{A:BC} \;\geq\; C^2_{AB} + C^2_{AC}, \tag{2.2}$$

dove $C_{A:BC}$ è la concorrenza tra A e l'intero sistema BC, mentre C_{AB} e C_{AC} sono le concorrenze bipartite relative.

La quantità

$$\tau_{ABC} = C^2_{A:BC} - C^2_{AB} - C^2_{AC} \tag{2.3}$$

è detta *tangle* a tre parti, e rappresenta la frazione di entanglement di A che non è attribuibile a correlazioni bipartite, ma solo a correlazioni tripartite pure. Il significato fisico è chiaro: se A è fortemente entangled con B, la sua correlazione con C deve essere ridotta. L'entanglement "speso" in una relazione bipartita non può essere redistribuito liberamente su altri legami, a differenza delle correlazioni classiche.

Dal punto di vista della sicurezza, ciò significa che l'informazione condivisa tra due utenti non può essere "copiata" o replicata da un terzo senza degradare la correlazione originale. Se Alice e Bob verificano di possedere un elevato grado di entanglement (misurabile ad esempio tramite concorrenza o violazioni di Bell), questo è già di per sé garanzia che un eventuale eavesdropper non detiene una conoscenza comparabile del loro stato. L'entanglement diventa quindi una sorta di barriera fisica: non è possibile che esista un terzo soggetto pienamente correlato con i legittimi interlocutori senza che questi ultimi se ne accorgano, perché le correlazioni sarebbero inevitabilmente più deboli.

Entanglement e chiave privata

La connessione fra entanglement e generazione di chiavi segrete è al centro di molte dimostrazioni di sicurezza. Una strategia concettuale spesso adottata consiste nell'immaginare che Alice e Bob dispongano di una sorgente ideale di coppie entangled, su cui applicano procedure di *distillazione*: attraverso operazioni locali e comunicazione classica (LOCC), cercano di trasformare stati imperfetti e rumorosi in una quantità minore di stati altamente puri e massimamente entangled (singlet). Se la distillazione riesce, la possibilità di estrarre da quegli stati una chiave sicura è immediata, perché le misure effettuate in basi appropriate producono risultati perfettamente correlati e totalmente ignoti a un intruso. Per formalizzare questa intuizione si introducono due quantità fondamentali.

- L'*entanglement distillabile* $E_D(\rho)$ di uno stato ρ è il tasso massimo (numero di coppie di Bell per copia) con cui, mediante LOCC, è possibile trasformare molte copie di ρ in stati singlet quasi perfetti:

$$E_D(\rho) = \sup\left\{ r : \lim_{n\to\infty} \inf_{\Lambda\in\mathrm{LOCC}} \left\| \Lambda(\rho^{\otimes n}) - \Phi_2^{\otimes \lfloor rn \rfloor} \right\| = 0 \right\},$$

  dove Φ_2 è lo stato di Bell e $\|\cdot\|$ la norma di traccia.

- La *chiave distillabile* $K_D(\rho)$ è invece il tasso massimo di bit segreti che si possono estrarre da ρ, sempre tramite LOCC, ma mirando non a singlet puri bensì a *private*

[1] Si ricorda che la *concorrenza* per uno stato puro di due qubit $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ è definita come

$$C(|\psi\rangle) = 2|ad - bc|.$$

Per stati misti ρ di due qubit, Wootters [18] ha introdotto la formula generale

$$C(\rho) = \max\{0,\, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\},$$

dove le λ_i sono le radici quadrate degli autovalori dell'operatore $\rho\,\tilde{\rho}$, con $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$ e ρ^* la complessa coniugata in base computazionale. Questa è la definizione quantitativa standard che sottende le disuguaglianze di monogamia.

states γ_2, cioè stati che garantiscono direttamente la privacy della chiave:

$$K_D(\rho) = \sup\left\{ r : \lim_{n\to\infty} \inf_{\Lambda\in \mathrm{LOCC}} \left\| \Lambda(\rho^{\otimes n}) - \gamma_2^{\otimes \lfloor rn \rfloor} \right\| = 0 \right\}.$$

[2]

È chiaro che $K_D(\rho) \geq E_D(\rho)$, in quanto ogni singlet perfetto è già un private state, ma non vale la relazione inversa.

Approfondimento

Teorema fondamentale (Horodecki et al., 2005) Esistono stati detti *bound entangled*, ovvero che hanno bisogno di entanglement puro per essere creati, ma dai quali non può essere distillato entanglement puro, per i quali $K_D(\rho) > 0$. In termini operativi, anche in assenza di entanglement distillabile è possibile ottenere una chiave privata sicura.

Questo risultato è sorprendente perché ribalta la visione iniziale secondo cui la sicurezza in crittografia quantistica sarebbe equivalente alla disponibilità di stati massimamente entangled. La scoperta dei *private states* mostra che la risorsa fondamentale non è l'entanglement distillabile in sé, bensì la possibilità di estrarre correlazioni private. Si apre così uno scenario molto più ricco, in cui stati apparentemente "deboli" dal punto di vista dell'entanglement possono comunque fornire sicurezza crittografica.

Dal punto di vista operativo, questa distinzione suggerisce che la verifica sperimentale non deve limitarsi a misurare il grado di distillabilità, ma può essere basata su criteri più generali (entanglement witness, violazioni di Bell, stime di K_D), che riflettono direttamente la capacità di generare chiavi segrete.

Entanglement witness e verifica sperimentale

Affinché le proprietà teoriche dell'entanglement diventino garanzie operative, occorre verificarne la presenza a partire dai dati sperimentali. A questo scopo si introducono i cosiddetti *entanglement witness*, osservabili ermitiane W tali che

$$\mathrm{Tr}(W\rho_{\mathrm{sep}}) \geq 0 \qquad \forall\, \rho_{\mathrm{sep}} \in \mathcal{S}, \tag{2.4}$$

dove $\mathcal{S}$ è l'insieme degli stati separabili. Se per uno stato sperimentale ρ si trova invece

$$\mathrm{Tr}(W\rho) < 0, \tag{2.5}$$

[2]Nelle definizioni abbiamo usato la *norma di traccia* come metrica di distanza. In alternativa si può adottare la *fidelity*, ma in regime asintotico entrambe le scelte portano a definizioni equivalenti dei tassi E_D e K_D [19].

allora ρ è necessariamente entangled. Questa definizione fornisce quindi un criterio operativo: la misura di un witness adeguatamente scelto certifica l'entanglement senza richiedere una tomografia completa dello stato [20].

Un esempio importante è fornito dalle *disuguaglianze di Bell*, che possono essere viste come casi particolari di witness: la violazione di un vincolo del tipo

$$S \equiv \langle \mathcal{B} \rangle \leq S_{\mathrm{LHV}} \tag{2.6}$$

($S_{\mathrm{LHV}} = 2$ nel caso CHSH) implica che lo stato non è descrivibile da variabili nascoste locali, e dunque possiede entanglement. Tuttavia, il formalismo dei witness è più generale e permette di trattare stati rumorosi o sistemi di dimensione superiore.

Dal punto di vista sperimentale, i witness vengono implementati decomponendoli in combinazioni lineari di osservabili locali. Ad esempio,

$$W = \alpha\, \mathbb{I} - \sum_i c_i\, (A_i \otimes B_i), \tag{2.7}$$

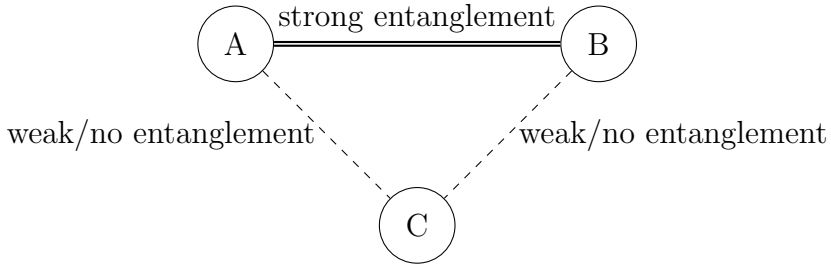
dove A_i e B_i sono osservabili accessibili a Alice e Bob, e i coefficienti c_i dipendono dal witness progettato. La misura sperimentale dei valori attesi $\langle A_i \otimes B_i \rangle$ consente di stimare $\mathrm{Tr}(W\rho)$ e determinare la presenza di entanglement.

Senza una verifica tramite witness o disuguaglianze, le correlazioni osservate potrebbero sempre essere simulate da un modello classico con rumore. La teoria dei witness fornisce quindi lo strumento rigoroso e pratico per trasformare l'entanglement in una risorsa sperimentale affidabile per la sicurezza quantistica.
E'importante sottolineare che un singolo witness non è universale: non può rilevare tutti gli stati entangled. Tuttavia, per ogni stato entangled esiste *almeno un witness* che lo separa dal set degli stati separabili, per il teorema di separazione di Hahn–Banach. Questo chiarisce perché la scelta di un witness adeguato sia fondamentale nelle verifiche sperimentali.

Trade-off informazione–disturbo

Un'altra proprietà essenziale dell'entanglement, direttamente collegata al *no-cloning theorem*, è che l'accesso di un intruso allo stato quantistico comporta inevitabilmente un disturbo osservabile [21]. Se Eve tenta di acquisire informazione sullo stato condiviso, il suo intervento modifica le statistiche sperimentali di Alice e Bob. In termini operativi, si può descrivere l'attacco dell'intruso come un canale quantistico che agisce sui qubit in transito: spesso questo viene modellato come un *quantum cloner approssimato ottimale*, capace di produrre copie con la massima fedeltà possibile, compatibilmente con le leggi della meccanica quantistica [20]. Una trattazione quantitativa di quanto detto verrà introdotta analizzando la sicurezza del protocollo E91.

Implementazioni e scenari reali



Monogamia dell'entanglement:
se A e B sono fortemente correlati, C non può esserlo allo stesso modo

Figura 2.3: Diagramma concettuale sulla monogamia dell'entanglement

Dal punto di vista sperimentale, l'entanglement può essere generato oggi con diverse tecniche consolidate. La più comune è la spontanous parametric down-conversion (SPDC), in cui un cristallo non lineare produce coppie di fotoni entangled in polarizzazione o in altri gradi di libertà [22]. Tecniche più recenti includono sorgenti integrate su chip fotonici, che consentono di ottenere stati entangled in maniera scalabile e con elevata stabilità [23].

Vedremo nell'ultimo capitolo come questi stati possono essere trasmessi attraverso fibre ottiche o canali in spazio libero [24]. In entrambi i casi, la sfida principale è preservare l'entanglement a fronte di perdite e rumore. Da qui l'importanza dei test periodici (witness, violazioni di Bell, stima del QBER) che permettono di valutare la qualità delle correlazioni[20]. In scenari pratici si può optare per due famiglie di protocolli: quelli di tipo *prepare&measure* (come il BB84), e quelli *entanglement-based* (come l'E91), che sfruttano esplicitamente la distribuzione di coppie entangled. Sebbene sotto ipotesi ideali i due approcci siano equivalenti, la formulazione entangled rende esplicito e controllabile il ruolo della non-località come certificatore di sicurezza, e permette l'uso di test di Bell come garanzia sperimentale.

In sintesi, l'entanglement svolge un duplice ruolo: da un lato è la risorsa che rende possibili correlazioni forti e non simulabili classicamente; dall'altro costituisce un criterio operativo che permette di certificare la sicurezza di un protocollo. Proprietà come la monogamia, il legame informazione–disturbo e la possibilità di verificare sperimentalmente l'entanglement tramite witness o test di Bell conferiscono all'entanglement un valore unico: esso non solo garantisce la generazione di correlazioni private, ma fornisce anche gli strumenti per accertarne la qualità. Nei capitoli successivi vedremo come questi concetti generali si incarnano nei protocolli concreti, analizzando l'E91, che costruisce la sua sicurezza direttamente sull'entanglement.

Capitolo 3

Il protocollo E91

Per garantire la riservatezza delle comunicazioni digitali, per lungo tempo ci si è affidati a sistemi crittografici che richiedevano la condivisione anticipata di una chiave segreta tra i due interlocutori. Un esempio emblematico è il cifrario di Vernam, noto anche come one-time pad: un metodo semplice (vedi 3.1), ma teoricamente inviolabile, a patto che la chiave utilizzata sia lunga quanto il messaggio, venga usata una sola volta e rimanga completamente segreta. Tuttavia, risiede proprio su questo punto la criticità di tale approccio: come distribuire la chiave in modo sicuro senza che venga intercettata? In ambito classico è difficile assicurare la completa segretezza della chiave, infatti anche se i bit della chiave vengono controllati assiduamente e distrutti subito dopo la loro distribuzione, qualsiasi copia non autorizzata comprometterebbe l'intera comunicazione.

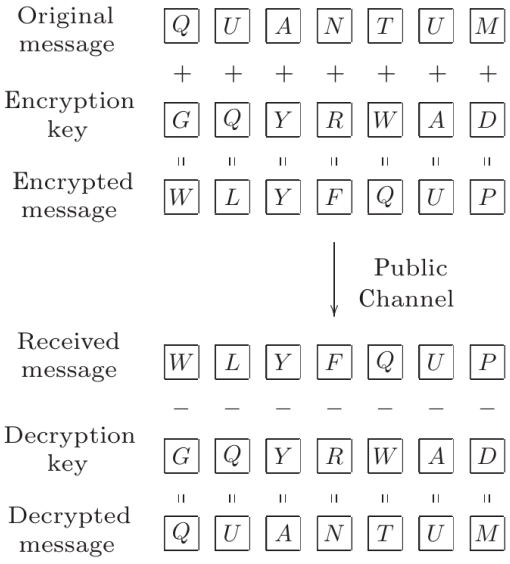


Figura 3.1: Il cifrario di Vernam. Il messaggio da comunicare viene cifrato sommando bit casuali della chiave segreta (in questo esempio, per semplicità, sono state usate lettere). Successivamente, l'interlocutore decifra il messaggio ricevuto sottraendo i medesimi bit della chiave. [Immagine da [1]]

È in questo contesto che si comprende l'importanza rivoluzionaria della distribuzione quantistica delle chiavi (QKD). Una delle differenze fondamentali tra il mondo classico e quello quantistico, infatti, è che i sistemi quantistici composti possono trovarsi in stati che sono al tempo stesso puri e correlati, una caratteristica del tutto assente nella fisica classica, nota come entanglement. Questa proprietà consente ad Alice e Bob di creare correlazioni perfette tra loro, anche a distanza, e rende immediatamente rilevabile qualsiasi tentativo di intercettazione.

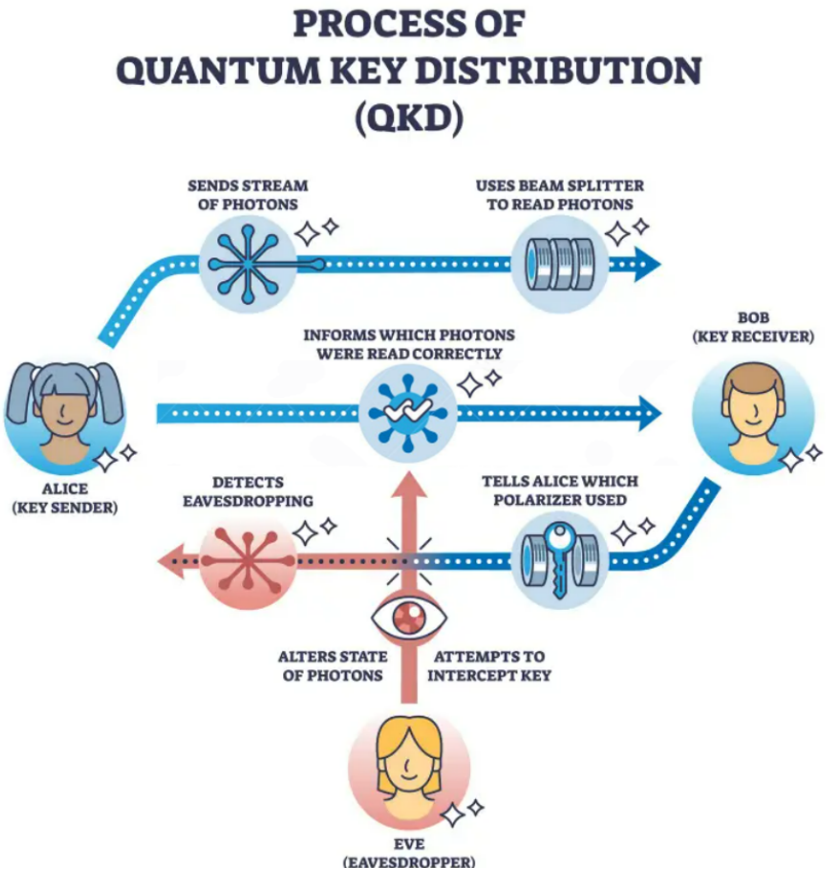


Figura 3.2: Processo di distribuzione della chiave quantistica. [immagine presa da `stock.adobe.com`]

Nel 1991 Artur Ekert afferra questa potenzialità e propone il primo protocollo basato sugli stati entangled: nasce così quello che verrà definito E91 [3]. Il protocollo E91, non solo garantisce la sicurezza grazie alle leggi della meccanica quantistica, ma introduce vantaggi strategici inediti rispetto a protocolli precedenti come il BB84. Ad esempio, le coppie di particelle entangled possono essere misurate in un secondo momento, permettendo ai due interlocutori di posticipare la generazione della chiave segreta, fino al

momento del bisogno. Questo significa che un eventuale intruso, che tentasse di accedere fisicamente ai dispositivi prima dell'uso, altererebbe inevitabilmente lo stato quantistico, venendo così rilevato.

L'idea centrale del protocollo è che due utenti, Alice e Bob, ricevano da una sorgente comune delle coppie di qubit in uno stato entangled, tipicamente un singoletto di spin o una coppia di fotoni entangled in polarizzazione. Se Alice e Bob misurano ciascuno la propria particella lungo direzioni opportune, i risultati sono fortemente correlati e possono essere utilizzati per costruire una chiave segreta condivisa. Ciò che rende questo approccio sicuro non è l'impossibilità di un'intercettazione, ma l'immediata e attedibile rilevazione di questa. Infatti, la presenza di un eventuale intruso (Eve) altererebbe inevitabilmente le correlazioni, riducendo la violazione delle disuguaglianze di Bell.

3.1 Struttura e funzionamento del protocollo

Il funzionamento del protocollo può essere suddiviso in alcune fasi principali:

1. **Distribuzione delle coppie entangled.** Una sorgente quantistica, genera coppie di qubit in uno stato di Bell (tipicamente lo stato singoletto $|\Psi^-\rangle$).

$$\left|\Psi^-\right\rangle = \frac{1}{2\sqrt{2}}(|x\rangle + i\,|y\rangle) \otimes (-\,|x\rangle + i\,|y\rangle) - \frac{1}{2\sqrt{2}}(-\,|x\rangle + i\,|y\rangle) \otimes (|x\rangle + i\,|y\rangle)$$

$$= \frac{i}{\sqrt{2}}(|x\rangle\,|y\rangle - |y\rangle\,|x\rangle) = \frac{i}{\sqrt{2}}(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle) = \frac{1}{\sqrt{2}}(|H\rangle\,|V\rangle - |V\rangle\,|H\rangle)$$

   Le particelle si muovono lungo l'asse z, verso i due utenti del canale, diciamo Alice e Bob.

2. **Scelta casuale delle basi di misura.** Sia Alice che Bob dispongono di diverse possibili direzioni di misura.Alice e Bob. Dopo che le particelle si sono separate, effettuano entrambi, tramite apparati di Stern e Gerlach (vedi AppendiceC), delle misurazioni sulle componenti dello spin lungo una delle tre direzioni, che corrispondono alla base rispetto alla quale calcolare l'osservabile,. Nel protocollo originale, scelgono tra tre possibili basi, formate da vettori unitari a_i e $b_j (i, j = 1, 2, 3)$, rispettivamente, per Alice e Bob. Per semplicità entrambi i vettori giacciono sul piano x-y, perpendicolari alla traiettoria delle particelle, e sono caratterizzati da angoli azimutali:

	ϕ_1	ϕ_2	ϕ_3
a	0	$\frac{1}{4}\pi$	$\frac{1}{2}\pi$
b	$\frac{1}{4}\pi$	$\frac{1}{2}\pi$	$\frac{3}{4}\pi$

   Le scelte sono effettuate in maniera casuale e indipendente per ogni coppia ricevuta. Ogni misurazione puo avere due risultati: $+1$ (spin *up*) e -1 (spin *down*), in

unità di $\frac{1}{2}\hbar$, e potrebbe contribuire con un bit alla formazione della chiave. Questo garantisce che un eventuale intruso non possa adattare la propria strategia di intercettazione senza introdurre disturbo.

3. **Raccolta e confronto delle basi.** Dopo molte ripetizioni, Alice e Bob comunicano attraverso un canale pubblico quali basi di misura hanno utilizzato, senza però rivelare i risultati ottenuti. Scartano immediatamente le misure in cui non sono entrambi a rilevare la particella. Quindi, solo le misure effettuate in basi compatibili vengono conservate per formare la chiave, mentre le altre servono per verificare la violazione delle disuguaglianze di Bell.

4. **Test di Bell e sicurezza.** I due interlocutori divulgano i risultati delle misure non utilizzate per la chiave e li impiegano per calcolare il parametro di correlazione, che entra nella disuguaglianza CHSH. Se la violazione osservata è sufficientemente marcata, si può concludere che le correlazioni condivise non possono essere spiegate da modelli a variabili nascoste locali, e dunque che un eventuale eavesdropper non ha potuto ottenere informazione significativa senza essere rilevato.

5. **Generazione della chiave.** I rimanenti dati, provenienti dalle misure effettuate nelle stesse basi, sono fortemente (anti)correlati e possono essere convertiti in una stringa di bit condivisa. A questo punto Alice e Bob possono applicare procedure di *error correction* e *privacy amplification* per ottenere una chiave finale segreta e sicura.

3.2 Creazione e distribuzione di coppie entangled

La realizzazione sperimentale delle coppie entangled è stata resa possibile soprattutto grazie al fenomeno della *spontaneous parametric down-conversion* (SPDC) [25]. Un esperimento di riferimento è quello di Kwiat e collaboratori [22], che ha introdotto una sorgente brillante e stabile di coppie entangled, ancora oggi ampiamente utilizzata in QKD.

Spontaneous Parametric Down Conversion (SPDC)

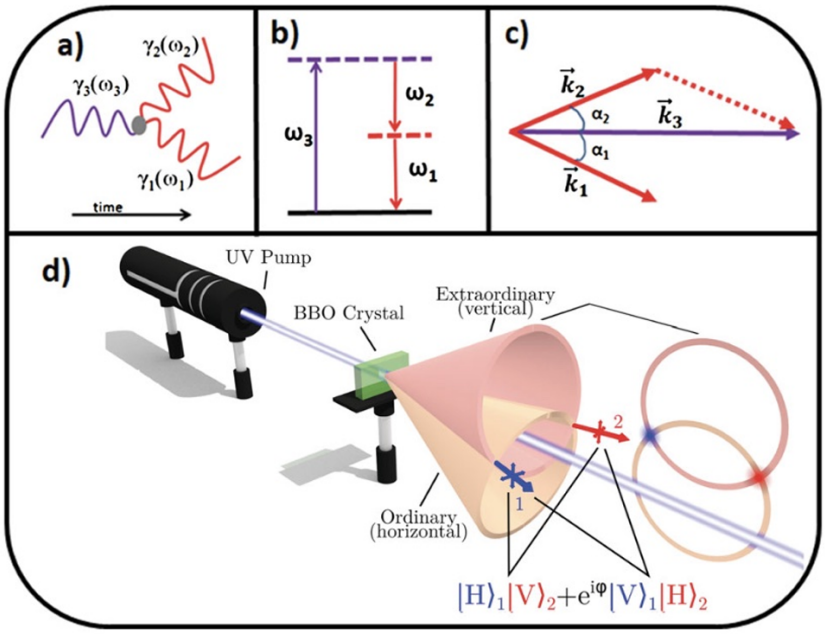


Figura 3.3: (a) Diagramma di Feynman del processo SPDC, in cui un fotone con energia $\hbar\omega_3$ si scinde in due fotoni gemelli con energie $\hbar\omega_2$ e $\hbar\omega_1$; (b) rappresentazione della conservazione dell'energia nel processo SPDC; (c) rappresentazione della conservazione della quantità di moto; (d) schema dello SPDC in cui un laser di pompa ultravioletta genera fotoni rossi emessi dal cristallo lungo due coni caratteristici. [Immagine da [25]].

La sorgente più utilizzata negli esperimenti di crittografia quantistica, incluso il protocollo E91, è la *Spontaneous Parametric Down-Conversion* (SPDC), processo non lineare di secondo ordine che avviene all'interno di cristalli birifrangenti. In termini semplici, un fotone di pompa ad alta frequenza (ω_p) interagisce con il mezzo non lineare e può decadere spontaneamente in due fotoni a frequenza minore (ω_s, ω_i), detti rispettivamente

signal e *idler*, nel rispetto delle leggi di conservazione:

$$\omega_p = \omega_s + \omega_i, \qquad \vec{k}_p = \vec{k}_s + \vec{k}_i,$$

dove la seconda equazione rappresenta la condizione di *phase matching*. Senza quest'ultima, le ampiezze quantistiche delle diverse traiettorie interferirebbero distruttivamente e l'efficienza del processo sarebbe trascurabile.

Descrizione quantistica

Il contributo non lineare della polarizzazione indotta nel cristallo è proporzionale al tensore di suscettività quadratica $\chi^{(2)}$. L'Hamiltoniana di interazione può essere scritta, in approssimazione, come:

$$\hat{H}_{\mathrm{SPDC}} \propto \chi^{(2)}\, \hat{a}_p\, \hat{a}_s^\dagger\, \hat{a}_i^\dagger + \mathrm{h.c.},$$

dove $\hat{a}_p$ è l'operatore di annichilazione del campo di pompa, e $\hat{a}_s^\dagger, \hat{a}_i^\dagger$ sono gli operatori di creazione dei due fotoni generati. Dal punto di vista quantistico, quindi, un singolo fotone della pompa viene "distrutto" e compare una coppia di fotoni correlati. Nella SPDC la probabilità di generazione è bassa (circa 10^{-11}–10^{-12} per fotone incidente), ma sufficiente in presenza di laser di pompa intensi.

Phase matching e birifrangenza

La condizione di conservazione dell'impulso, o phase matching, non è banalmente soddisfatta a causa della dispersione cromatica: indici di rifrazione diversi per frequenze diverse portano a $\Delta k = k_p - k_s - k_i \neq 0$. Per correggere questa discrepanza si utilizzano cristalli birifrangenti, come il beta-bario-borato (BBO), in cui l'indice di rifrazione dipende dalla polarizzazione. Nel caso degenere ($\omega_s = \omega_i = \omega_p/2$), le direzioni di emissione formano due coni che si intersecano: nei punti di intersezione le polarizzazioni sono indeterminate e si ottengono stati entangled del tipo

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle_s|V\rangle_i + e^{i\phi}|V\rangle_s|H\rangle_i\Big),$$

dove la fase relativa ϕ può essere controllata variando l'orientazione del cristallo o introducendo elementi ottici di ritardo.

Approfondimento

Sorgenti brillanti di entanglement: l'esperimento di Kwiat (1995)

Un punto di svolta fondamentale nella generazione di fotoni entangled è rappresentato dal lavoro di Kwiat e collaboratori [22], che introdusse per la prima volta una sorgente pratica e ad alta intensità di coppie entangled basata su SPDC in cristalli non lineari. Lo schema utilizzava un cristallo di beta–borato di bario (BBO) in configurazione di tipo II non collineare: in questo modo le due modalità di polarizzazione ordinaria ed extraordinaria venivano emesse lungo coni di radiazione che si intersecano.

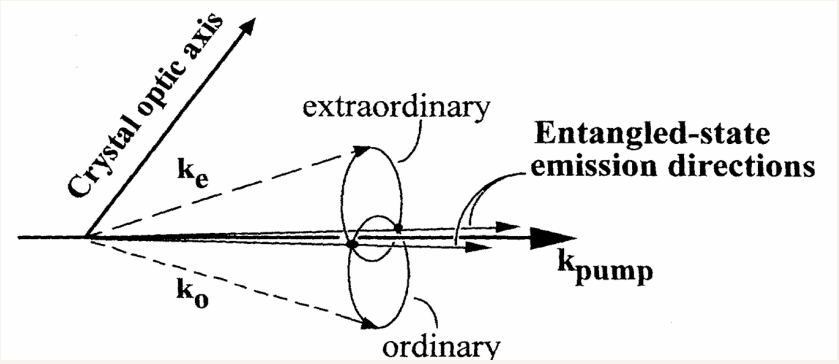


Figura 3.4: Schema dei due celebri coni di emissione SPDC generati dal cristallo con polarizzazioni ortogonali. La selezione spaziale permette di isolare soltanto i fotoni provenienti dalla regione di intersezione dei due coni. [Immagine da [22]].

Nei punti di intersezione i due fotoni risultano indistinguibili e lo stato complessivo è una sovrapposizione coerente delle possibilità di emissione. Il risultato è uno stato entangled di polarizzazione del tipo

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle_1|V\rangle_2 + e^{i\alpha}\,|V\rangle_1|H\rangle_2\Big),$$

dove α è una fase relativa regolabile con elementi ottici birifrangenti.
Mediante opportune tecniche di compensazione della birifrangenza (cristalli aggiuntivi e piastre a mezz'onda), Kwiat et al. dimostrarono la possibilità di preparare non solo questo stato, ma tutti e quattro gli stati massimamente entangled di Bell:

$$|\Phi^{\pm}\rangle = \tfrac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle), \qquad |\Psi^{\pm}\rangle = \tfrac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle).$$

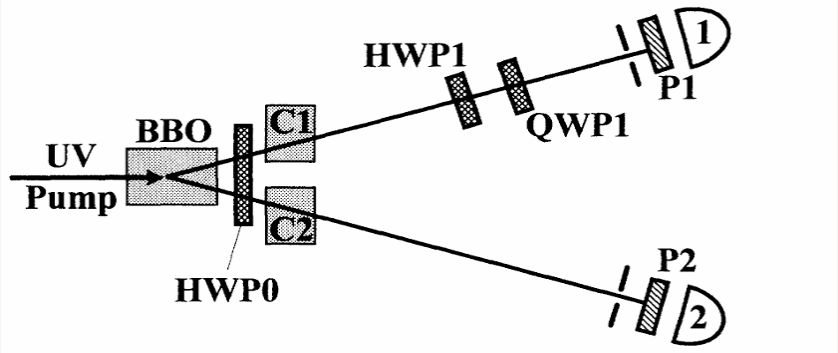


Figura 3.5: Schema di un metodo per produrre e selezionare stati entangled di polarizzazione da un cristallo di down-conversion. I cristalli birifrangenti addizionali C1 e C2, insieme alla piastra a mezza lunghezza d'onda HWPO, servono a compensare gli effetti di walk-off dovuti alla birifrangenza del cristallo di produzione. Regolando opportunamente la piastra a mezza lunghezza d'onda HWP1 e la piastra a un quarto d'onda QWP1, è possibile generare tutti e quattro gli stati ortogonali di Bell (EPR). I polarizzatori P1 e P2 sono realizzati con due beam splitter polarizzanti sovrapposti, preceduti da una piastra a mezza lunghezza d'onda rotabile. [Immagine da [22]]

La sorgente risultante si distingueva per brillantezza e stabilità: la visibilità sperimentale delle frange di interferenza superava il 97%, consentendo una violazione delle disuguaglianze di Bell di oltre cento deviazioni standard in tempi dell'ordine di pochi minuti. Queste caratteristiche resero la sorgente di Kwiat immediatamente un riferimento per esperimenti di non-località e applicazioni di crittografia quantistica. Ancora oggi, varianti di quello schema costituiscono la piattaforma sperimentale più diffusa per la distribuzione di chiavi segrete nel protocollo E91 e nei suoi successivi sviluppi.

Nuove tecniche di generazione

Oltre alla SPDC in cristalli non lineari, che rimane il metodo più diffuso, negli ultimi anni sono state esplorate anche sorgenti alternative:

- **Sistemi a stato solido**: punti quantici e difetti NV nel diamante possono emettere coppie di fotoni entangled con buona efficienza e integrazione in dispositivi su chip.
- **Ioni e atomi intrappolati**: consentono di generare entanglement tra stati interni della materia o tra spin elettronici e fotoni.

- **Circuiti fotonici integrati**: permettono di produrre e manipolare stati entangled in dispositivi compatti e scalabili, aprendo prospettive per reti quantistiche su larga scala [23].

Distribuzione su canali reali

Una volta generato, l'entanglement deve essere trasmesso a distanza tra i due utenti. Esistono due scenari principali:

- **Fibre ottiche terrestri**: rappresentano la tecnologia più consolidata, ma le perdite aumentano esponenzialmente con la distanza. Infatti, le fibre monomodali a 1550 costituiscono l'infrastruttura standard per QKD su rete terrestre, con attenuazione tipica $\alpha \simeq 0.2$ dB/km. La trasmittanza su una tratta di lunghezza L è
$$\eta(L) = 10^{-\alpha L/10},$$
che implica perdite del 99% già dopo 100 [26]. Nei protocolli discreti, il tasso di chiave segreta è limitato dal cosiddetto *PLOB bound* $-\log_2(1-\eta)$ (dove μ è l'intensità media del segnale), che evidenzia il decadimento esponenziale della capacità di canale in assenza di nodi intermedi [27].

  Per estendere la distanza oltre poche centinaia di chilometri si seguono due strategie principali:

  – Ottimizzazione dell'hardware: l'impiego di fibre ultra-low-loss e rivelatori a singolo fotone basati su nanofili superconduttori (SNSPD), con elevata efficienza e bassissimo rumore, ha permesso di estendere le dimostrazioni di distribuzione di chiavi fino a centinaia di chilometri.

  – Protocolli a scaling migliorato: oltre agli schemi Measurement-Device-Independent (MDI-QKD) [28], un avanzamento decisivo è rappresentato dalla Twin-Field QKD (TF-QKD), caratterizzata da un tasso segreto che scala come $\propto \sqrt{\eta}$, in contrasto con il limite lineare fissato dal bound di Pirandola–Laurenza–Ottaviani–Banchi (PLOB) [27]. Le prime dimostrazioni hanno riportato distribuzione sicura di chiavi su fibre terrestri oltre i 400, confermando sperimentalmente questo vantaggio [29, 30].

  Quando occorrono distanze ancora maggiori, si ricorre a nodi *trusted* o allo sviluppo di veri e propri *quantum repeaters*, che combinano entanglement swapping e memorie quantistiche, e che costituiscono oggi un'area di ricerca attiva.

- **Spazio libero e satelliti**: le perdite atmosferiche sono significative, ma non crescono esponenzialmente come nelle fibre. L'esperimento Micius, guidato da Yin e collaboratori [24], ha dimostrato la distribuzione di entanglement su oltre 1200

km tra stazioni a terra, stabilendo un record mondiale e aprendo la via a reti quantistiche globali.

Approfondimento

QKD da satellite: l'esperimento *Micius*

L'impiego di collegamenti ottici spaziali rappresenta una strategia efficace per superare il decadimento esponenziale dovuto all'assorbimento nelle fibre. Oltre i ~ 100, infatti, la capacità segreta di un canale ottico in fibra è drasticamente ridotta e non è possibile amplificare stati quantistici come si fa nelle trasmissioni classiche. L'atmosfera terrestre costituisce un mezzo di propagazione molto meno assorbente rispetto a centinaia di chilometri di fibra, rendendo realistico l'utilizzo di piattaforme satellitari per distribuzione di chiavi quantistiche. Infatti, sopra i ~ 10 di altezza ottica equivalente l'assorbimento è quasi nullo, così una tratta satellite–terra attraversa solo uno strato sottile e concentrato di turbolenza vicino al suolo.

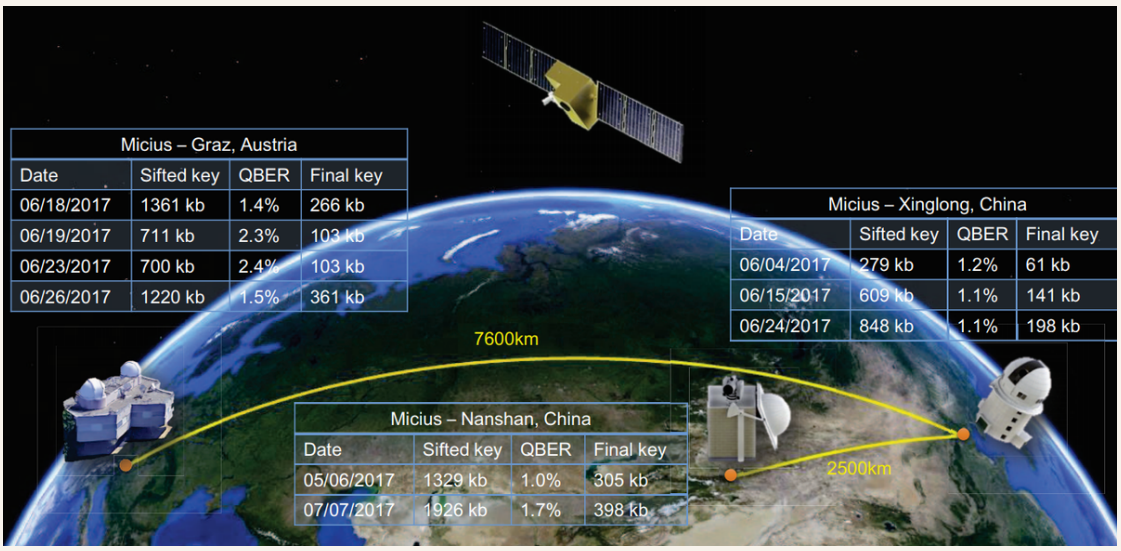


Figura 3.6: Trasmissione intercontinentale di chiave tra Graz in Austria e Xinglong in Cina. Sono illustrate le tre stazioni terrestri (Graz, Nanshan e Xinglong) e tutti i percorsi utilizzati per la generazione della chiave [immagine presa da [24]].

Nel 2017 il satellite cinese *Micius*, posto in orbita bassa (~ 500), ha realizzato la prima distribuzione di chiavi su scala intercontinentale.
Il terminale ottico di bordo genera impulsi attenuati a frequenza dell'ordine di 100, implementando il protocollo BB84 con tecnica *decoy state* per la stima delle componenti a singolo fotone. L'ottica trasmittente produce un fascio con divergenza di

circa 10 μrad, che a 1200 di distanza forma uno spot di una decina di metri; il puntamento è stabilizzato tramite laser ausiliari con accuratezza sub–μrad, garantendo l'allineamento anche durante l'orbita.
Per ridurre il rumore di fondo, i rivelatori a terra accettano soltanto coincidenze entro una finestra di ~ 2. Le perdite complessive del canale, dovute a diffrazione, turbolenza e inefficienza di raccolta, portano a un rate netto di chiave dell'ordine di 10 durante i circa cinque minuti di visibilità del satellite per ogni passaggio. Il dato significativo è che, pur partendo da una sorgente a cento milioni di impulsi al secondo, dopo filtraggio temporale e correzione d'errore si ottiene una chiave utilizzabile per cifratura a prova d'intercettazione.
L'esperimento è stato esteso alla distribuzione di chiavi verso due stazioni geograficamente distanti: Xinglong (Cina) e Graz (Austria). Il satellite trasmette due chiavi indipendenti, M_{X} (Micius Xinglong) e M_{G}(Micius-Graz), attraverso due passaggi consecutivi. Per sincronizzare le stazioni senza canale ottico diretto, a bordo viene calcolato l'XOR bit a bit

$$\mathrm{PUB} = M_{\mathrm{G}} \oplus M_{\mathrm{X}},$$

che viene trasmesso su canale classico. Ciascuna stazione ricostruisce la chiave dell'altra combinando la propria stringa con il messaggio pubblico:

$$M_{\mathrm{X}} = M_{\mathrm{G}} \oplus \mathrm{PUB}, \qquad M_{\mathrm{G}} = M_{\mathrm{X}} \oplus \mathrm{PUB}.$$

In questo modo le due sedi ottengono una chiave identica pur non avendo mai avuto un collegamento diretto, mentre l'XOR non rivela informazione utile a un eventuale eavesdropper oltre a quella già protetta dal protocollo BB84.

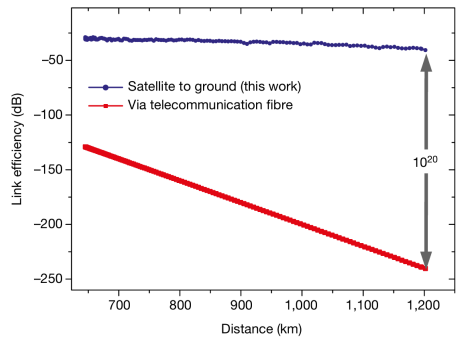


Figura 3.7: **Efficienze dei collegamenti QKD**. Le efficienze dei collegamenti sono mostrate per la trasmissione diretta attraverso fibre ottiche per telecomunicazioni (in rosso) e per l'approccio satellite-terra (in blu). Le efficienze per quest'ultimo sono state calcolate dividendo l'intensità dei fotoni che arrivano davanti ai rivelatori della stazione a terra per quella in uscita dal trasmettitore del satellite. A una distanza di 1.200 km, l'approccio satellite-terra (durante il tempo di copertura del satellite) risulta più efficiente della trasmissione diretta di 20 ordini di grandezza. [immagine presa da [24]].

Questo esperimento ha segnato il passaggio da dimostrazioni in laboratorio a una reale infrastruttura *space-to-ground*, dimostrando che la riduzione dell'assorbimento atmosferico e l'accuratezza di puntamento possono rendere praticabile la QKD

su scala continentale e porre le basi per future costellazioni satellitari dedicate alla crittografia quantistica globale.

3.3 Sicurezza tramite Test di Bell

Nel protocollo E91 la segretezza della chiave non dipende da limiti tecnologici contingenti, ma dal principio fisico da noi già analizzato: le correlazioni generate da stati entangled non possono essere spiegate da teorie locali a variabili nascoste. Come mostrato da Ekert [3], la violazione di una disuguaglianza di tipo CHSH [8] diventa così, non soltanto un test fondamentale della teoria, ma anche un vero e proprio strumento operativo per escludere la presenza di un eavesdropper.

Poiché i canali quantistici sono inevitabilmente affetti da perdite e rumore, la qualità delle coppie di qubit distribuite deve essere controllata di continuo. A tale scopo, Alice e Bob estraggono un campione delle misure e verificano la non-località attraverso un test di Bell o, in alternativa, mediante opportuni entanglement witness. Il parametro di correlazione e il tasso di errore quantistico (QBER) ottenuti permettono di valutare se le statistiche osservate restano incompatibili con un modello locale. Una violazione sufficiente implica che le informazioni disponibili a un potenziale intercettatore siano trascurabili; al contrario, un degrado della violazione segnala rumore eccessivo o possibili tentativi di intrusione.

La procedura di sicurezza prevede quindi due passaggi essenziali: la verifica della non-località tramite un test di Bell, con la relativa stima del *Quantum Bit Error Rate* (QBER) rispetto alle soglie teoriche e la distillazione della chiave tramite correzione d'errore e privacy amplification.

Verifica di Bell

Con due fotoni nello stato di Bell singoletto

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\Big),$$

Alice e Bob misurano la trasmissione attraverso polarizzatori con angoli $\alpha/2$ e $\beta/2$.

Approfondimento

Proiettori: i polarizzatori Un polarizzatore è un elemento ottico che seleziona la componente del campo elettrico lungo una direzione prestabilita (l'asse del polarizzatore) e attenua le componenti ortogonali. Dal punto di vista quantistico esso realizza un proiettore sullo spazio di Hilbert del qubit in polarizzazione. Indi-

chiamo con $|H\rangle$ e $|V\rangle$ una coppia di base ortogonale (orizzontale e verticale): uno stato, descritto nella sfera di Bloch da un angolo α, forma con l'asse delle x un angolo $\frac{\alpha}{2}$ e può essere scritto come

$$|\alpha\rangle = \cos\frac{\alpha}{2}|H\rangle + \sin\frac{\alpha}{2}|V\rangle.$$

Proiettare lo Stato α nella sfera di Bloch equivale a prendere un polarizzatore e orientarne l'asse con un angolo $\frac{\alpha}{2}$ rispetto all'asse x. Il proiettore corrispondente è

$$\hat{P}_\alpha = |\alpha\rangle\langle\alpha|,$$

e la probabilità che un fotone nello stato con vettore di polarizzazione $\vec{\epsilon}$ venga trasmesso è data dalla regola di Born:

$$P_T(\alpha;\varepsilon) = \langle\varepsilon|\hat{P}_\alpha|\varepsilon\rangle = |\langle\alpha|\varepsilon\rangle|^2.$$

Si noti che lo stato vettoriale è definito a fase globale: $|\alpha+\pi\rangle = -|\alpha\rangle$, perciò il proiettore $\hat{P}_\alpha$ è periodico di π.

La regola di Born fornisce la probabilità congiunta di trasmissione:

$$P_{TT} = |\langle\alpha,\beta|\Psi^-\rangle|^2 = \frac{1}{2}|\cos\frac{\alpha}{2}\sin\frac{\beta}{2} - \sin\frac{\alpha}{2}\cos\frac{\beta}{2}|^2 = \frac{1}{2}\sin^2\left(\frac{\alpha}{2}-\frac{\beta}{2}\right).$$

Analogamente:

$$P_{RT} = |\langle\alpha+\pi,\beta|\Psi^-\rangle|^2 = \frac{1}{2}\cos^2\left(\frac{\alpha}{2}-\frac{\beta}{2}\right),$$
$$P_{TR} = |\langle\alpha,\beta+\pi|\Psi^-\rangle|^2 = \frac{1}{2}\cos^2\left(\frac{\alpha}{2}-\frac{\beta}{2}\right),$$
$$P_{RR} = |\langle\alpha+\pi,\beta+\pi|\Psi^-\rangle|^2 = \frac{1}{2}\sin^2\left(\frac{\alpha}{2}-\frac{\beta}{2}\right).$$

Il COEFFICIENTE DI CORRELAZIONE, dato dal valor medio del prodotto degli esiti ($+1$ per trasmissione, -1 per riflessione), è

$$\begin{aligned} E(\alpha,\beta) &= (+1)(P_{TT}+P_{RR}) + (-1)(P_{RT}+P_{TR}) \\ &= \sin^2\left(\frac{\alpha}{2}-\frac{\beta}{2}\right) - \cos^2\left(\frac{\alpha}{2}-\frac{\beta}{2}\right) \\ &= -\cos(\alpha-\beta), \end{aligned}$$

Per gli altri stati di Bell (ad es. $|\Psi^+\rangle$) il segno cambia, ma la dipendenza angolare resta $\cos(\alpha-\beta)$. Questa relazione segna un'anti-correlazione perfetta per tutti gli stati

selezionati in cui gli angoli scelti sono uguali; infatti con $\alpha = \beta$, $E(\alpha, \beta) = -1$, quindi se Alice misura (+1) = T, Bob misura (1) = R e viceversa.

Costruzione del parametro CHSH. Per quattro scelte di angoli, Alice e Bob calcolano

$$S = E(\alpha_1, \beta_1) - E(\alpha_1, \beta_3) + E(\alpha_3, \beta_1) + E(\alpha_3, \beta_3).$$

Con gli angoli proposti da Ekert ($\alpha_1 = 0, \alpha_3 = +\pi/2, \beta_1 = +\pi/4, \beta_3 = +3\pi/4$, la meccanica quantistica predice

$$S = -\cos\left(-\frac{\pi}{4}\right) + \cos\left(-\frac{3\pi}{4}\right) - \cos\left(\frac{\pi}{4}\right) - \cos\left(-\frac{\pi}{4}\right) = -2\sqrt{2},$$

violando la disuguaglianza $|S| \leq 2$ vista nei capitoli precedenti [8]. Una violazione significativa dell'ineguaglianza di Bell indica la presenza di correlazioni quantistiche non simulabili classicamente e quindi la resistenza ad attacchi locali di un eventuale intruso. Al contrario, se la disuguaglianza di Bell viene rispettata è un indizio che siano avvenute delle intercettazioni, poiché mostra che i due fotoni non sono più entangled quindi Eve deve aver agito su uno dei due (analizzeremo i dettagli nei prossimi paragrafi).

Esperimento di Naik (2000)

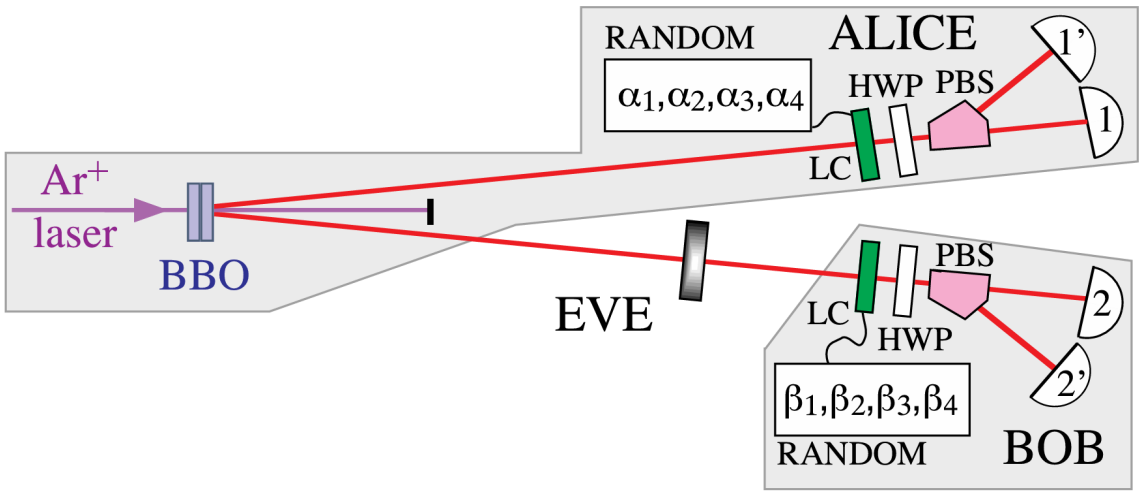


Figura 3.8: Schema dell'esperimento che realizza la distribuzione di chiavi Ekert91. Una luce a 351.1 nm da un laser a ioni di Argon viene usata per pompare due cristalli ottici non lineari (BBO) orientati perpendicolarmente. I fotoni entangled risultanti vengono inviati a Alice e Bob, che li analizzano ciascuno in una delle quattro basi scelte casualmente. L'intercettatore, se presente, è stato incorporato utilizzando un polarizzatore o una lastra birigrangente che genera decoerenza (entrambi orientabili, e in alcuni casi con piastre d'onda aggiuntive per consentire analisi in basi di polarizzazioni ellittiche arbitrarie[Fig. 2a,c]). [immagine presa da [31]]

Nel 2000 Naik condusse un esperimento basato sul protocollo E91[31], apportando piccole variazioni, prime fra tutte l'utilizzo di fotoni polarizzati al posto di elettroni e il diverso stato di partenza. Le coppie di fotoni sono emesse in parametric down-conversion da laser "pompa" a 351 nm, nello stato di Bell

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B\Big) = \frac{1}{\sqrt{2}}\Big(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\Big),$$

Anche l'analisi avviene con proiettori su una base diversa dalla proposta di Ekert. Alice usa i seguenti proiettori:

$$\{\Pi_\alpha = |\alpha\rangle\langle\alpha|\,,\ I - \Pi_\alpha\}\,, \qquad |\alpha\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\alpha}|1\rangle\big),$$

scegliendo per l'angolo α i valori

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = \left(\tfrac{\pi}{4}, \tfrac{\pi}{2}, \tfrac{3\pi}{4}, \pi\right).$$

Si noti che nei primi tre casi la base non corrisponde a due polarizzazioni lineari perpendicolari, bensì a polarizzazioni ellittiche.

Approfondimento

Polarizzazioni (lineare, circolare, ellittica) Nel sistema di riferimento standard per la polarizzazione dei fotoni si scelgono come base gli stati di polarizzazione orizzontale e verticale, indicati rispettivamente con $|H\rangle$ e $|V\rangle$. Uno stato di polarizzazione generale si scrive come

$$|\psi(\theta,\varphi)\rangle = \cos\left(\frac{\theta}{2}\right)|H\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|V\rangle\,,$$

dove $\theta \in [0,\pi]$ e $\varphi \in [0,2\pi)$ sono le coordinate polari e azimutali sulla sfera di Poincaré (analoga alla sfera di Bloch per il qubit di polarizzazione).

Casi particolari:

- *Polarizzazione orizzontale:* $|H\rangle \equiv |\psi(0,\varphi)\rangle$ ($\theta = 0$).
- *Polarizzazione verticale:* $|V\rangle \equiv |\psi(\pi,\varphi)\rangle$ ($\theta = \pi$).
- *Polarizzazione circolare destra/sinistra:*

$$|R\rangle = \frac{|H\rangle + i\,|V\rangle}{\sqrt{2}} = \left|\psi\left(\tfrac{\pi}{2},\tfrac{\pi}{2}\right)\right\rangle, \qquad |L\rangle = \frac{|H\rangle - i\,|V\rangle}{\sqrt{2}} = \left|\psi\left(\tfrac{\pi}{2},-\tfrac{\pi}{2}\right)\right\rangle.$$

Polarizzazione ellittica. La polarizzazione ellittica corrisponde al caso generale $\theta \neq 0,\pi$ e φ arbitrario: il vettore campo descrive un'ellisse il cui orientamento e eccentricità sono fissati da θ,φ. La *polarizzazione lineare* è il caso particolare in cui l'ellisse si riduce ad una retta ($\varphi = 0$ o $\varphi = \pi$ sull'equatore), mentre la *polarizzazione circolare* è il caso dell'ellisse con eccentricità nulla ($\theta = \pi/2$, $|\sin\varphi| = 1$).

Riferimenti pratici per la manipolazione ottica:

- *Half-wave plate (HWP)*: ruota la polarizzazione lineare di un angolo 2α se il suo *asse veloce* è inclinato di α rispetto all'orizzontale. È lo strumento standard per ruotare basi lineari (es. da 0° a 45°).
- *Quarter-wave plate (QWP)*: trasforma linearità in circolarità e viceversa quando orientata opportunamente (ad esempio a 45° trasforma $|\pm 45°\rangle$ in $|R\rangle, |L\rangle$). In pratica i modulatori LCD (liquid-crystal devices) forniscono uno sfasamento variabile che svolge un ruolo analogo alle lastre a ritardo.
- Per ottenere proiezioni su basi ellittiche si combinano HWP ed elementi che introducono uno sfasamento variabile (QWP o LCD): la sequenza e l'orientamento determinano (θ,φ).

Bob usa proiettori analoghi a quelli di Alice, parametrizzati dall'angolo β, scegliendo

i valori

$$\vec{\beta} = \vec{\alpha} - \frac{\pi}{4},$$

di cui solo il primo corrisponde a polarizzazioni lineari.

Con queste basi, le probabilità congiunte sono:

$$P_{TT} = \left|\left\langle \alpha, \beta | \Phi^+ \right| \rangle\right|^2 = \left| \frac{1}{2\sqrt{2}} \left[1 + e^{-i(\alpha+\beta)}\right] \right|^2 = \tfrac{1}{4}\left[1 + \cos(\alpha+\beta)\right] = P_{RR},$$

$$P_{TR} = |\langle \alpha, \beta + \pi | \Phi^+ \rangle|^2 = \tfrac{1}{4}\left[1 + \cos(\alpha+\pi+\beta)\right] = \tfrac{1}{4}\left[1 - \cos(\alpha+\beta)\right] = P_{RT}.$$

Mentre, per generare la chiave, utilizzano il sottinsieme $\alpha + \beta = \pi$, per il quale si hanno risultati perfettamente anti-correllati ($P_{TR} + P_{RT} = 1$), 2/3 delle altre misurazioni vengono impiegate per verificare le disuguaglianze CHSH su due distinti osservabili:

$$S = -E(\alpha_1, \beta_1) + E(\alpha_1, \beta_3) + E(\alpha_3, \beta_1) + E(\alpha_3, \beta_3)$$

$$S' = -E(\alpha_2, \beta_2) + E(\alpha_2, \beta_4) - E(\alpha_4, \beta_2) + E(\alpha_4, \beta_4)$$

[1] Analizzeremo di seguito come i loro valori siano sensibili alle diverse possibili intercettazioni. ’ possibile distinguere due famiglie principali di strategie di attacco:

- **Intercept–resend (misura proiettiva forte).** Eve misura, tramite un operatore di proiezione, la polarizzazione del fotone destinato a Bob in una base scelta da lei (ad esempio una delle basi usate da Alice/Bob o una terza base), registra il risultato e invia a Bob un nuovo fotone preparato nello stato corrispondente al risultato ottenuto. Questo processo distrugge l’entanglement originario e sostituisce il canale quantistico con un canale effettivamente locale, con correlazioni che dipendono dalla base scelta da Eve (vedere 3.10). Consideriamo il caso semplice e pedagogico in cui Alice e Bob misurano in due basi complementari: Eve sceglie a caso (probabilità 1/2) una di queste due basi per la sua misura. Per ogni fotone intercettato:

  - se Eve sceglie la *stessa* base di Alice/Bob non introduce errori (il fotone reinviato è coerente con le misure che verrebbero ottenute senza Eve);
  - se Eve sceglie la *base sbagliata* (la base mutuamente non commutativa), il fotone reinviato è congruo con la misura di Eve ma ha probabilità 1/2 di differire dal risultato che avrebbe ottenuto Bob in assenza di Eve.

[1] I coefficienti di correlazione sono stati calcolati come

$$E(\alpha, \beta) = \frac{R_{12}(\alpha,\beta) + R_{1'2'}(\alpha,\beta) - R_{12'}(\alpha,\beta) - R_{1'2}(\alpha,\beta)}{R_{12}(\alpha,\beta) + R_{1'2'}(\alpha,\beta) + R_{12'}(\alpha,\beta) + R_{1'2}(\alpha,\beta)},$$

dove R_{ij} sono i RATE DI COINCIDENZA nelle quattro configurazioni possibili.

Da ciò segue la stima standard del QBER per intercettazione totale ($f = 1$):

$$Q_{Eve} = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} = 25\%.$$

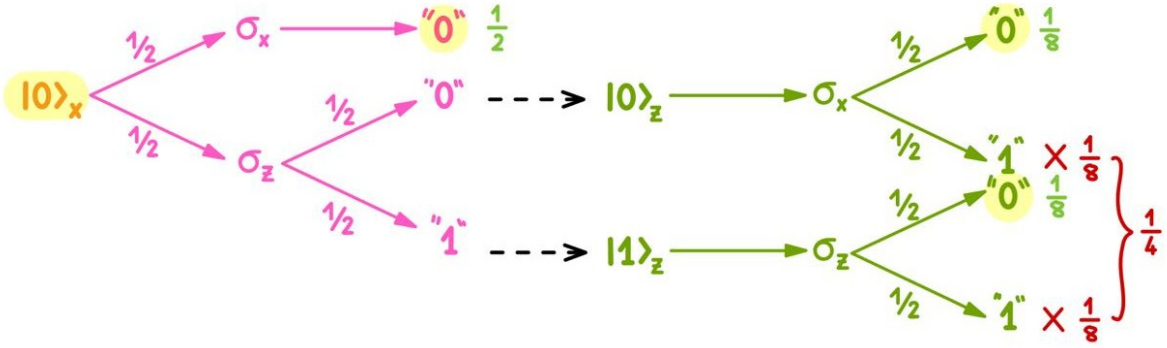


Figura 3.9: Esempio di un caso di intercettazione in cui il fotone mandato da Alice è nello stato $|0\rangle_x$, dove x indica la base scelta da Alice . In fucsia sono rappresentate le possibili scelte di Eve, mentre in verde quelle di Bob. Si può constatare come solo in un caso su quattro Eve introduca un errore. Le linee nere tratteggiate indicano che Eve rimanda a Bob un determinato stato a seconda del risultato ottenuto. Nel caso in cui Eve misura il fotone nella stessa base di Alice non è riprodotta l'intera catena in quanto Eve manda a Bob lo stesso stato di Alice, non introducendo errori.

Questa è la soglia minima (per l'attacco *intercept–resend* su tutte le coppie) che Alice e Bob possono aspettarsi: un QBER così elevato rende l'attacco immediatamente evidente. Per una frazione f di coppie intercettate, viene ridotto il QBER, e allo stesso tempo aumenta il parametro S. Eve riduce così la probabilità di essere rivelata, ma anche l'informazione guadagnata sulla chiave, che, se si considera una frazione di fotoni misurati minore del 58.6%, è inferiore a quella di Bob, permettendo in ogni caso la generazione della chiave grazie a tecniche di privacy amplification.

- **Misure "QND" (*quantum non-demolition*).** Queste misure hanno come effetto l'entanglement tra il fotone misurato e l'apparato di lettura, inducendo una fase casuale tra i componenti di polarizzazione. Ciò può essere simulato introducendo elementi birefringenti che separano componenti spettrali oltre la lunghezza di coerenza: l'effetto statisticamente osservabile è analogo ad una misura che impone una fase casuale tra gli autostati, degradando le interferenze di polarizzazione. Naik et al. hanno simulato questo scenario inserendo nel percorso di uno dei due fotoni entangled un elemento birifrangente che induce un ritardo temporale tra le

componenti ordinaria e straordinaria superiore alla lunghezza di coerenza (circa $140\mu m$). Dal punto di vista teorico, tale operazione può essere rappresentata da un operatore di proiezione del tipo:

$$|\chi\rangle\langle\chi| + e^{i\xi}|\chi^{\perp}\rangle\langle\chi^{\perp}|,$$

dove $\langle\xi\rangle$ è una fase casuale.

Nel contesto della distribuzione quantistica delle chiavi, la posizione geometrica delle basi di misura gioca un ruolo centrale nella sicurezza del protocollo. Due casi estremi sono instruttivi:

1. **Eve misura nel *medesimo piano* di Alice/Bob (base ottimale).** In questo caso la probabilità d'errore per ogni fotone intercettato è $\approx 25\%$ e il valore misurato di $|S|$ si riduce a $\approx \sqrt{2}$ quando $f = 1$.

2. **Eve misura in un piano ortogonale.** Nel caso in cui Eve non abbia accesso all'orientamento del piano delle basi, e decida di effettuare misurazioni casuali in un piano ortogonale, le sue probabilità di successo diminuiscono sensibilmente. In media, l'errore introdotto per bit cresce al 32.5%, mentre il valore medio di $|S|$ scende a $1/\sqrt{2} \approx 0{,}707$, peggiorando la posizione di Eve e aumentando la probabilità che venga rivelata.

È immediato, quindi, pensare di adottare insiemi di basi appartenenti a piani tra loro ortogonali sulla sfera di Poincaré, al fine di amplificare l'effetto perturbativo indotto da un eavesdropper. In particolare, l'uso di due o tre piani mutuamente ortogonali consente di superare significativamente il limite standard di probabilità di errore del 25%, migliorando la sensibilità del protocollo a intrusioni indesiderate. La dipendenza angolare è mostrata sperimentalmente nei grafici 3.10 (tre pannelli corrispondenti a tre famiglie di basi di attacco), in cui sono tracciati i valori misurati di $|S|$ e del QBER in funzione dell'angolo della base di Eve; i punti sperimentali (misure forti con polarizzatore e misure QND simulate con lastre BBO) seguono le curve teoriche attese.

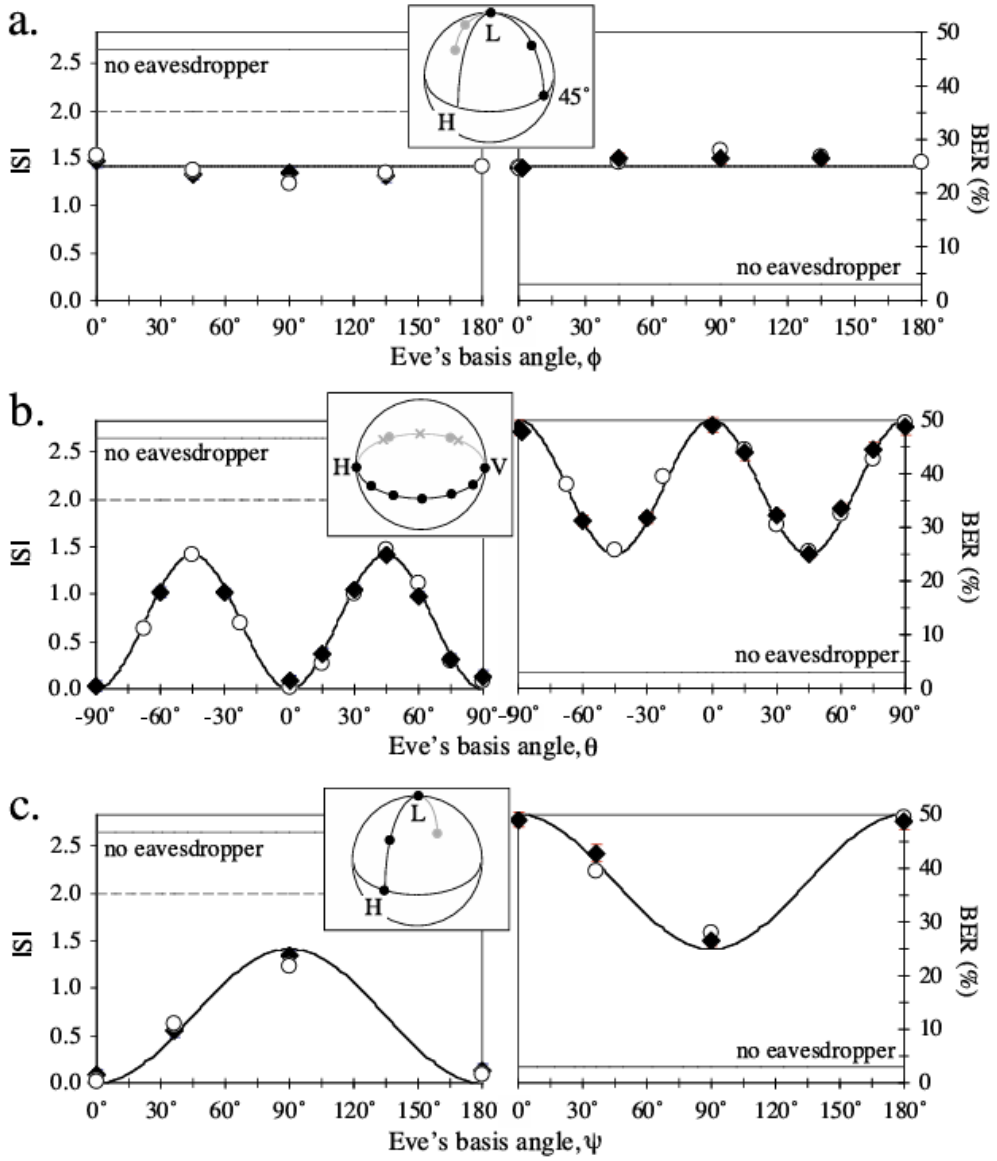


Figura 3.10: Dati e teoria che mostrano l'effetto di un intercettatore su S e BER per varie basi d'attacco (poiché S' è molto simile a S, non è mostrato per chiarezza). I rombi rappresentano misure forti, effettuate con un polarizzatore; i cerchi rappresentano attacchi QND simulati con un cristallo BBO spesso 3mm; le barre d'errore sono comprese nei punti. Le basi d'attacco sono: a. $|H\rangle + e^{i\phi}|V\rangle$; b. $\cos\theta|H\rangle + \sin\theta|V\rangle$; e c. $|45°\rangle + e^{i\psi}|-45°\rangle$; i punti di misura effettivi in queste basi sono illustrati nelle sfere di Poincaré negli inserti. I valori medi misurati in assenza di un intercettatore sono indicati dalle linee grigie continue, mentre le linee tratteggiate rappresentano il valore massimo classico di $|S|$. [immagine presa da [31]]

Grazie ai dati raccolti durante l'esperimento è possibile quantificare quanto trattato:

- **Parametri sperimentali di base.** Tipicamente la sorgente fornisce ~ 40 coppie utili/s; di queste solo 1/4 contribuisce alla chiave grezza (altre sono usate per il test di Bell), così che il tasso netto di bit grezzi è $\sim 10.1\ \mathrm{s}^{-1}$. In quattro run di ~ 10 min ciascuno si raccolgono $n = 24\,252$ bit grezzi.

- **Valori sperimentali misurati senza attacco.**

  $$S = 2.6650.019, S = 2.6440.019,$$

  violano entrambe la CHSH di 34σ, confermando l'entanglement. La discrepanza tra l'errore teorico puro (circa 10^{-2}) e quello riportato è dovuta a contributi sistematici (doppie coppie SPDC, sbilanciamento nei rivelatori[2]). Mentre un errore di

  $$Q = 3.06\% \pm 0.11\%.$$

  [3] è molto inferiore alla soglia di errore in caso di attacco (25%), rientrando nei valori compatibili con il rumore ottico.

- **Stima della conoscenza potenziale di Eve.** Attribuendo conservativamente l'intero QBER a Eve, considerando una strategia intercept-resend e un 0.7% dato da doppie coppie SPDC Naik calcola una stima superiore dell'informazione di Eve pari al 10.3% della chiave (circa 2,500 bit). Per ridurre l'informazione di Eve si applicano le procedure di error detection e privacy amplification contraendo la chiave progressivamente a 17,452 e a 12,215 bit, con informazione residua trascurabile ($\ll$ 1 bit).

Correzione d'errore e Privacy Amplification

Superato il test di Bell e stimato un QBER accettabile, la chiave grezza non è ancora perfetta. Alice e Bob eseguono:

[2] Un rivelatore di singoli fotoni converte l'arrivo di un fotone in un segnale elettrico misurabile; a livello microscopico ciò avviene con processi fotoelettrici seguiti da uno stadio di amplificazione. Un parametro che caratterizza il rivelatore, molto imporatante dal punto di vista sperimentale, è l'**Efficienza quantistica** η , ovvero la probabilità che un fotone incidente produca un evento di rivelazione.

[3] Il QBER è definito come

$$Q = \frac{n_e}{n}, \qquad \sigma_Q = \sqrt{\frac{Q(1-Q)}{n}}.$$

dove n_e è il numero di bit discrodanti tra Alice e Bob e n la lunghezza totale della chiave crittografica. (Un QBER pari a 0.5 indica stringhe completamente non correllate.)

Correzione d'errore: protocolli di information reconciliation che aumentano la correlazione tra le stringhe di Alice e Bob, fino a giungere a una stessa chiave;

Privacy amplification: compressione della chiave corretta mediante funzioni hash universali, al fine di diminuirne la correlazione con Eve.[1]

Information reconciliation. Questa fase consiste in un protocollo di correzione degli errori eseguito attraverso il canale pubblico, il cui scopo è far sì che Alice e Bob arrivino a condividere una stessa stringa W, minimizzando la quantità di informazione addizionale resa accessibile a Eve. Operativamente, Alice calcola un messaggio u di parità su sottoinsiemi dei suoi bit X e lo trasmette a Bob, che lo utilizza per correggere la propria stringa Y. Questo inevitabilmente rivela a Eve una variabile $U = u$, riducendo l'entropia di collisione di W condizionata alle informazioni di Eve.

Privacy amplification. Come appena visto il processo di information reconciliation aumenta le informazioni di Eve . La privacy amplification riduce questa informazione tramite *funzioni hash universali*[4] , che comprimono W in una chiave segreta S. L'idea fondamentale è formalizzata dal seguente risultato:

[[1], Thm. 12.16] Sia X una variabile casuale su un alfabeto $\mathcal{X}$ con distribuzione di probabilità $p(x)$ ed entropia di collisione $H_c(X)$ [5]. Sia G la variabile casuale corrispondente alla scelta casuale (con distribuzione uniforme) di un membro della classe universale di funzioni hash da $\mathcal{X}$ a $\{0,1\}^m$. Allora

$$H(G(X)|G) \;\geq\; H_c(G(X)|G) \;\geq\; m - 2^{\,m-H_c(X)}.$$

Questo garantisce che, se $H_c(W|Z = z)$ (l'entropia di collisione di W data l'informazione di Eve Z) è sufficientemente grande ($> d$), allora Alice e Bob possono scegliere una funzione hash universale $g \in \mathcal{G}$ e calcolare $S = g(W)$, ottenendo una chiave che massimizza l'incertezza di Eve ($H_c(SG, Z = z) \geq m - 2^{md}$, con m abbastanza piccolo $H_c(SG, Z = z) \approx m$).

[4] la classe di funzioni hash universali $\mathcal{G}$, che mappano l'insieme dei bit stringa di n-bit A nell'insieme dei bit stringa di m-bit B, tale che per qualsiasi $a_1, a_2 \in A$ distinti, quando g è scelto uniformemente a caso da $\mathcal{G}$, allora la probabilità che $g(a_1) = g(a_2)$ è al massimo $\frac{1}{|B|}$.

[5] l'Entropia di collisione è definita come

$$H_c(X) = -\sum_x p(x)^2 \log p(x)^2$$

dove $p(x)$ è la distribuzione di probabilità della variabile casuale X

L'intera procedura — violazione di Bell, QBER sotto soglia, correzione e privacy amplification — costituisce una garanzia intrinseca di segretezza fondata su principi fisici. Qualsiasi perturbazione introdotta da un intruso riduce $|S|$ e aumenta Q; superata una soglia critica, la sessione viene scartata, preservando la sicurezza del sistema.

Conclusioni

Questo lavoro ha evidenziato il ruolo dell'entanglement come risorsa essenziale per la crittografia quantistica, con particolare attenzione al protocollo E91. È stato mostrato come principi, nati in ambito teorico, possano tradursi in strumenti operativi: l'E91, in particolare, collega sicurezza e non-località, rendendo i test di Bell una garanzia concreta contro possibili intercettazioni. Al tempo stesso, l'analisi dei limiti pratici ha sottolineato la necessità di procedure come *correzione d'errore* e *privacy amplification*, mentre i progressi sperimentali — dalla generazione di coppie entangled alla loro distribuzione tramite fibre e collegamenti satellitari — delineano il percorso verso reti quantistiche globali. In questo quadro, il protocollo E91 si configura più come punto di partenza che come punto di arrivo, aprendo la strada a soluzioni più avanzate come la *measurement-device-independent* e la *twin-field QKD*.

Ciò che emerge, in ultima analisi, è che la sicurezza offerta dall'entanglement non è un dettaglio tecnico, ma il segno di un cambiamento concreto e potenzialmente rivoluzionario: la possibilità di sviluppare un'infrastruttura di comunicazione realmente nuova, che non si affida più alla garanzia dei costruttori, bensì a proprietà fondanti di una teoria fisica, quella della meccanica quantistica, ed è questo che la rende una modalità di comunicazione su cui si può riporre affidamento, indipendentemente da fattori contingenti. La sicurezza fondata su principi fisici — e non soltanto su algoritmi o su hardware, inevitabilmente più vulnerabili — offre la possibilità di proteggere dati personali, infrastrutture critiche e comunicazioni sensibili. Questo aspetto incide profondamente sulla società, in un'epoca in cui i sistemi digitali assumono un ruolo sempre più centrale, ma al tempo stesso la fiducia nei loro confronti vacilla e cresce la consapevolezza dell'importanza di tutelare i propri dati in rete.

L'avanzare di reti quantistiche e di nuovi standard post-quantistici rappresenta quindi, non solo una risposta operativa, ma anche un passo verso una società più solida e consapevole. Molte sfide restano aperte — dai repeater alle memorie quantistiche — ma i progressi conseguiti rendono plausibile immaginare che la distribuzione sicura di chiavi crittografiche su scala globale diventi presto realtà. In

questa prospettiva, il percorso avviato con il protocollo E91 continua a indicare una delle strade più promettenti lungo cui la fisica quantistica manifesta il proprio potenziale applicativo, senza rinunciare al suo rigore concettuale.

Appendice A

Il Teorema di Kraus

Un risultato fondamentale della teoria dell'informazione quantistica è il **teorema di Kraus** [32], che caratterizza in maniera generale tutte le trasformazioni fisicamente realizzabili su uno stato quantistico. Tali trasformazioni, dette *operazioni quantistiche*, descrivono l'evoluzione più generale di un sistema quando si tiene conto sia della dinamica unitaria sia dell'interazione con l'ambiente.

Teorema (Kraus) Siano $\mathcal{H}$ e $\mathcal{G}$ due spazi di Hilbert di dimensione finita n e m rispettivamente, e sia Φ una mappa lineare che descrive un'operazione quantistica tra $\mathcal{H}$ e $\mathcal{G}$. Allora esiste un insieme finito di operatori

$$\{B_i : \mathcal{H} \to \mathcal{G}\}_{1 \leq i \leq nm}$$

detti *operatori di Kraus*, tali che per ogni stato quantistico ρ valga

$$\Phi(\rho) = \sum_i B_i \, \rho \, B_i^\dagger .$$

Viceversa, ogni mappa della forma sopra definita è un'operazione quantistica, a condizione che gli operatori di Kraus soddisfino la relazione di completezza

$$\sum_i B_i^\dagger B_i \leq I,$$

dove I è l'operatore identità.

Quando vale l'uguaglianza $\sum_i B_i^\dagger B_i = I$, la trasformazione Φ è detta *completamente positiva e a traccia preservata* (CPTP), e rappresenta il modello più generale di evoluzione fisicamente ammissibile di un sistema isolato più ambiente.

Il teorema di Kraus mostra che ogni trasformazione quantistica può essere vista come una combinazione statistica di evoluzioni "elementari" B_i, le quali agiscono sugli stati e codificano in modo implicito l'interazione con un ambiente non osservato.

Appendice B

Argomento di unitarietà del teorema del No-Cloning

Consideriamo due stati puri separabili arbitrari $|\psi_1\rangle$ e $|\psi_2\rangle$ che si desidera clonare su un secondo sistema preparato in uno stato iniziale fisso $|\phi\rangle$, utilizzando un'operazione unitaria ipotetica $\hat{U}$.

Supponiamo che tale operatore unitaria $\hat{U}$ realizzi la clonazione dei due stati nel modo seguente:

$$\hat{U}(|\psi_1\rangle \otimes |\phi\rangle) = |\psi_1\rangle \otimes |\psi_1\rangle \tag{B.1}$$

$$\hat{U}(|\psi_2\rangle \otimes |\phi\rangle) = |\psi_2\rangle \otimes |\psi_2\rangle \tag{B.2}$$

Considerando il prodotto scalare delle sovrascritte equazioni, si ha:

$$\langle\psi_1| \langle\phi| \hat{U}^\dagger \hat{U} |\psi_2\rangle |\phi\rangle = \langle\psi_1 \otimes \psi_1|\psi_2 \otimes \psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2 \tag{B.3}$$

Ma applicando l'unitarietà della trasformazione, si ottiene anche:

$$\langle\psi_1| \langle\phi| \hat{U}^\dagger \hat{U} |\psi_2\rangle |\phi\rangle = \langle\psi_1| \langle\phi| |\psi_2\rangle |\phi\rangle \tag{B.4}$$

$$= (\langle\psi_1|\psi_2\rangle)(\langle\phi|\phi\rangle) = \langle\psi_1|\psi_2\rangle \tag{B.5}$$

Segue quindi:

$$\langle\psi_1|\psi_2\rangle = (\langle\psi_1|\psi_2\rangle)^2 \tag{B.6}$$

Le uniche soluzioni di questa equazione sono:

- $\langle\psi_1|\psi_2\rangle = 0$ (stati ortogonali)
- $\langle\psi_1|\psi_2\rangle = 1$ (stati identici)

Ciò implica che la trasformazione unitaria $\hat{U}$ può clonare perfettamente solo stati che siano mutualmente ortogonali o identici. Tuttavia, in generale, due stati quantistici qualsiasi non sono ortogonali né identici. Pertanto, non esiste un'operazione unitaria che cloni in modo perfetto uno stato arbitrario sconosciuto.

Appendice C

L'apparato di Stern e Gerlach

L'apparato di Stern–Gerlach (prende il nome da Walther Gerlach and Otto Stern che lo idearono nel 1922 [33]) rappresenta il primo esempio sperimentale di misura quantistica a due esiti [1]. La sua importanza, nel contesto dell'informazione quantistica e dei protocolli di crittografia, è legata al fatto che realizza fisicamente una misura proiettiva sullo spin di una particella. L'idea di base dello schema di Stern–Gerlach è sfruttare l'interazione tra il momento magnetico $\hat{\boldsymbol{\mu}}$ del sistema e un campo magnetico non omogeneo $\mathbf{B}(\mathbf{r})$. Per una particella con spin $\hat{\mathbf{S}}$ si ha l'operatore momento magnetico

$$\hat{\boldsymbol{\mu}} \;=\; -g\,\mu_B\,\frac{\hat{\mathbf{S}}}{\hbar}, \tag{C.1}$$

dove g è il fattore di Landé e $\mu_B = e\hbar/(2m_e)$ il magnetone di Bohr. Se il campo ha una componente non nulla con gradiente lungo l'asse z, la forza risultante sulla particella è (in prima approssimazione)

$$\hat{F}_z \;=\; \nabla\big(\hat{\boldsymbol{\mu}}\cdot\mathbf{B}\big)\cdot\hat{\mathbf{z}} \simeq \hat{\mu}_z\,\frac{\partial B_z}{\partial z}. \tag{C.2}$$

Per uno spin 1/2 (che caratterizza gli elettroni), gli autovalori di $\hat{S}_z$ sono $m_s\hbar$ con $m_s = \pm\frac{1}{2}$, quindi gli autovalori di $\hat{\mu}_z$ sono $-g\mu_B m_s$ (valori con segno opposto rispetto a m_s). La forza diretta lungo z separa spazialmente le componenti di spin associate ai due autovalori, portando a due traiettorie distinte, corrispondenti agli stati base $|0\rangle \equiv |+z\rangle$ e $|1\rangle \equiv |-z\rangle$. Lo stato iniziale

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

evolve quindi in una sovrapposizione di due pacchetti spazialmente separati. L'osservazione della traiettoria equivale a proiettare il qubit su uno dei due autostati $|0\rangle$ e $|1\rangle$, con probabilità rispettivamente $|a|^2$ e $|b|^2$.

Orientando opportunamente i magneti si può scegliere l'asse di misura. Ad esempio, una misura lungo x corrisponde a proiettare sugli stati

$$|+x\rangle \equiv |+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-x\rangle \equiv |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

mentre una misura lungo y coinvolge stati con fasi relative. In generale, misurare lo spin lungo un asse unitario $\mathbf{n} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ equivale a proiettare sugli autostati $|\pm_{\mathbf{n}}\rangle$, ottenuti ruotando la base z:

$$|+_{\mathbf{n}}\rangle = \cos\frac{\theta}{2}\,|+_z\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|-_z\rangle\,, \tag{C.3}$$

e analogamente per $|-_{\mathbf{n}}\rangle$. In termini di sfera di Bloch, l'apparato SG implementa quindi misure proiettive su basi diverse, selezionate dall'orientazione del campo magnetico.

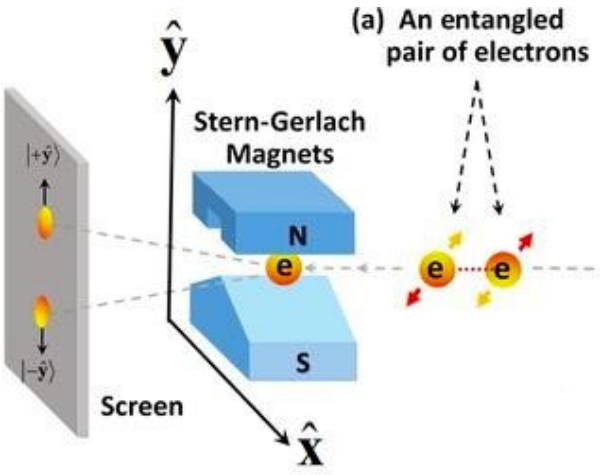


Figura C.1: Alice misura lo spin della sua particella di spin-1/2 con un apparato sperimentale di Stern-Gerlach. Dopo questa misurazione, gli assi dei due spin sono paralleli agli assi dei magneti di Stern-Gelarch. [Immagine presa da [34]]

Nel protocollo E91, l'apparato di Stern-Gerlach è il modello naturale per descrivere le misure di spin eseguite lungo gli assi scelti casualmente tra un insieme prefissato. Infatti, ruotando i magneti, e quindi l'orientazione del campo del dispositivo, si seleziona la base di misura del corrispondente angolo, e i due esiti discreti forniscono i bit grezzi della chiave.

Bibliografia

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition edition, 2010.

[2] John Preskill. Lecture notes on quantum computation. `http://theory.caltech.edu/~preskill/ph229/`, 1998. California Institute of Technology.

[3] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[4] Erwin Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(4):555–563, 1935.

[5] John S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195–200, 1964.

[6] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.

[7] A. Einstein and M. Born. *Scienza e vita. Lettere 1916–1955*. Einaudi, Torino, 1973.

[8] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[9] B. S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.

[10] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:1804–1807, 1982.

[11] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[12] Asher Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic Publishers, 1995.

[13] William K. Wootters and Wojciech H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[14] Dennis Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271–272, 1982.

[15] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín. Quantum cloning. *Rev. Mod. Phys.*, 77:1225–1256, 2005.

[16] Howard Barnum, Carlton M. Caves, Christopher A. Fuchs, Richard Jozsa, and Benjamin Schumacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76:2818–2821, 1996.

[17] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *arXiv preprint quant-ph/9907047*, 1999. Version 2, 24 Jul 1999. Published in Phys. Rev. A **61**, 052306 (2000).

[18] William K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80(10):2245–2248, 1998.

[19] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, 2009.

[20] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009.

[21] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, 2009.

[22] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75(24):4337–4341, 1995.

[23] Francesco Flamini, Nicolò Spagnolo, and Fabio Sciarrino. Photonic quantum information processing: a review. *Reports on Progress in Physics*, 82(1):016001, 2019.

[24] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zhou, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Qiang Zhang, Yu-Ao Chen, Nai-Le Liu, Xiang-Bin Wang, Zhen-Cai Zhu, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground quantum key distribution. *Nature*, 549:43–47, 2017.

[25] Christophe Couteau. Spontaneous parametric down-conversion. *Contemporary Physics*, 59(3):291–304, 2018.

[26] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, 2002.

[27] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nat. Commun.*, 8:15043, 2017.

[28] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, 2012.

[29] Ji-Gang Chen, Cheng Zhang, Cong Liu, and et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.*, 124:070501, 2020.

[30] Yang Liu, Zong-Wen Yu, Weijun Zhang, and et al. Experimental twin-field quantum key distribution over 428 km. *Phys. Rev. Lett.*, 126:250502, 2021.

[31] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat. Entangled state quantum cryptography: Eavesdropping on the ekert protocol. *Physical Review Letters*, 84:4733–4736, 2000. Received 18 October 1999; Published 15 May 2000.

[32] K. Kraus. *States, Effects, and Operations*. Springer-Verlag, Berlin, 1983.

[33] Martin Bauer. The stern-gerlach experiment, translation of: "der experimentelle nachweis der richtungsquantelung im magnetfeld". *arXiv preprint arXiv:2301.11343*, 2023.

[34] Jonathan Nemirovsky, Eliahu Cohen, and Ido Kaminer. Spin-spacetime censorship. *Annalen der Physik*, 534(1):2100348, 2022.