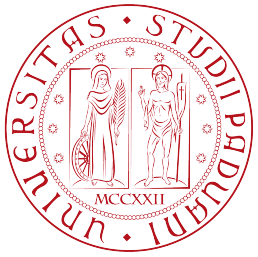


UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Fisica e Astronomia "Galileo Galilei"

Dipartimento di Ingegneria dell'Informazione

Corso di Laurea in Fisica

Tesi di Laurea

Realizzazione di un ricevitore per Distribuzione Quantistica di Chiave

Relatore

Prof. Giuseppe Vallone

Correlatore

Dr. Alberto Santamato

Laureando

Riccardo Cusinato

Anno Accademico 2017/2018

Indice

Capitolo 1

Comunicazione Quantistica

Il seguente lavoro di tesi è da inquadrarsi nel più ampio ambito della *comunicazione quantistica (CQ)*, in particolare della distribuzione di chiavi. È dunque doveroso, oltre che utile, iniziare il lavoro cercando si esporre cosa sia e su cosa si fondi quest'ambito.

1.1 Introduzione

Così come l'elettrodinamica, scoperta e formalizzata nel corso del 19° secolo, ha poi portato nel 20° secolo a straordinarie applicazioni (si pensi agli acceleratori o più semplicemente a segnali radio, televisivi ecc.), si sta ora assistendo ad un rapido sviluppo di quella che potrebbe essere una tra le prime applicazioni "pratiche" della meccanica quantistica, branca della fisica formalizzata negli anni '20 dello scorso secolo; pratiche qui è da intendersi nel senso di commerciali, esempi delle quali al giorno d'oggi sono solo laser e semiconduttori.
L'applicazione di cui si sta parlando e che costituisce il fulcro del lavoro di tesi è la *Quantum Key Distribution (QKD)* (distribuzione quantistica di chiave). Per capire meglio in cosa consista quest'ultima è utile prima capire cosa sia la crittografia.
La crittografia di per sè è una scienza antichissima, le cui origini si possono far risalire a più di duemila anni fa, che studia i metodi e gli stratagemmi da adottare affinché ci sia una trasmissione sicura di informazioni; con sicura si intende che colui che riceve il messaggio, il destinatario (o i destinatari), sia solo colui al quale il mittente voleva arrivasse il suddetto messaggio. Per far ciò, oltre al messaggio è necessario possedere più informazione, ovvero una chiave consistente in una stringa di numeri casuali, in modo da produrre un crittogramma. In linea teorica, affinché quest'ultimo possa essere conside-

rato sicuro, è necessario che solo coloro che possiedono la chiave possano essere in grado di leggere il messaggio. In linea pratica, invece, è sufficiente che il crittogramma sia inaccessibile a terze parti per un tempo maggiore del tempo in cui l'informazione contenuta nel messaggio possa essere considerata preziosa. È facile capire che il problema principale per una comunicazione sicura non è la trasmissione del messaggio cifrato in sé, ma la distribuzione di una chiave; in questo modo il problema di una comunicazione segreta si trasferisce meramente al problema della generazione di una chiave sicura e segreta.

È esattamente per risolvere questo problema che entra in gioco la meccanica quantistica. Essa, con le sue due caratteristiche principali: l'esistenza di elementi indivisibili, i quanti, e l'entanglement, garantisce in certi casi sicurezza e casualità che altrimenti non si potrebbero avere; alla costruzione e allo sviluppo della QKD hanno contribuito anche gli altri due pilastri della fisica del 20° secolo: la relatività e la teoria dell'informazione, la prima tramite il paradosso EPR (collegato alla sicurezza della CQ) e la seconda per le ovvie connessioni che presenta con la descrizione dell'informazione contenuta nel messaggio. La QKD (e con essa la seguente tesi), dunque, si prefigge lo scopo di comunicare segnali correlati attraverso particelle quantistiche tramite un canale classico con lo scopo di produrre chiavi completamente sicure (cioè teoricamente inviolabili) attraverso l'uso dei principi della meccanica quantistica.

Si può dire allora che la peculiarità della QKD consiste nel fatto che costituisce uno dei pochi ambiti nella fisica in cui i postulati della meccanica quantistica vengono usati "attivamente": essa attinge tutta la sua potenza dal fatto che un atto di misura interferisce col sistema misurato; al contrario, in generale, i postulati sono semplicemente trattati come delle regole a cui ogni sistema fisico deve obbedire "passivamente".

I primi a proporre questa possibilità furono S. Wiesner (1983) e, indipendentemente, C.H. Bennett e G. Brassard (1984) e la loro idea fu molto semplice: uno degli assiomi della meccanica quantistica afferma che una misurazione su un sistema modifica il sistema stesso (a meno che la misurazione non sia compatibile col sistema, cioè lo stato sia autostato dell'operatore); dunque, se in una conversazione tra Alice (nome convenzionale dato al mittente) e Bob (nome convenzionale dato al destinatario) fatta attraverso sistemi quantistici (ad esempio fotoni), i due scoprono che le sequenze inviata e ricevuta sono diverse, significa che c'è stata un'interferenza ed una terza persona si è intromessa nel canale (convenzionalmente Eve); la potenza della QKD sta qui, in una comunicazione classica sarebbe stato impossibile sapere se Eve stesse spiando il canale

o no.

Prima di procedere e approfondire quest'ultimo punto è utile trattare in tutta generalità gli enti usati nella QKD per trasmettere informazioni, precedentemente chiamati semplicemente "sistemi quantistici".

1.2 Il Qubit

Un qubit (quantum bit) è l'unità elementare d'informazione nella comunicazione quantistica, ma è anche l'elemento base dei computer quantistici: quest'ultimi, infatti, possono essere trattati come una collezione di n qubit, aventi una funzione d'onda collettiva che segue l'evoluzione temporale dettata dall'equazione di Schrödinger (precisamente, ciò succede se gli effetti di interazione con l'ambiente esterno sono trascurabili). Nell'ambito dei computer quantistici, ciò che rende speciali i qubit rispetto ai classici bit 0 e 1 sono gli effetti quantistici di sovrapposizione delle funzioni d'onda e di entanglement, che rendono un computer quantistico molto più potente di uno classico.

Il qubit è un sistema quantistico a due livelli, ovvero descritto da una funzione d'onda che risiede in uno spazio di Hilbert complesso bidimensionale, che può essere manipolato e misurato in maniera controllata. In questo spazio di Hilbert, si sceglie una base ortonormale di stati, detta *base computazionale*, convenzionalmente [1]

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

ed ogni stato del qubit potrà essere scritto come combinazione lineare dei vettori della base

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{, con } |\alpha|^2 + |\beta|^2 = 1$$

Alternativamente, è possibile usare una notazione che sarà utile in seguito, introducendo due angoli θ e ϕ, così da poter scrivere il generico stato come

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle = \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix} \qquad (0 \le \theta \le \pi\ ,\ 0 \le \phi \le 2\pi) \qquad (1.1)$$

Dunque il generico qubit risiede in uno spazio vettoriale, parametrizzato dalle variabili continue α e β (o θ e ϕ) e, a differenza dei classici bit che possono essere solo di due tipi, ammette un continuo di stati diversi. Tuttavia, per determinare il singolo stato è necessario un numero infinito di misure, volte a determinare con precisione "infinita" i due parametri che caratterizzano lo stato: per questo non è possibile pensare di usare un singolo qubit per immagazzinare una quantità infinita d'informazione. Infine, un sistema bidimensionale può essere usato in pratica come un qubit se soddisfa le seguenti caratteristiche:

1. può essere preparato in uno stato noto (es. $|0\rangle$);
2. ogni stato può essere trasformato in qualsiasi altro tramite una trasformazione unitaria;
3. lo stato può essere misurato nella base computazionale.

Esistono vari sistemi usati in pratica come qubit: lo spin nucleare di una molecola, un atomo in una cavità, lo stato di polarizzazione di un fotone ecc.

1.2.1 La sfera di Bloch

La sfera di Bloch è un'utile rappresentazione grafica che fornisce una visione geometrica si un qubit e delle operazioni ad esso applicabili. Essendo infatti lo stato vincolato ad avere modulo unitario, può essere pensato come un punto su una sfera di raggio unitario, chiamata appunto *sfera di Bloch*; questa sfera è immersa in uno spazio tridimensionale e, ricordando le trasformazioni tra coordinate polari e cartesiane $x = \sin\theta\cos\phi$, $y = \sin\theta\sin\phi$ e $z = \cos\theta$, lo stato (1.1) potrà essere scritto nelle nuove coordinate come [1]

$$|\psi\rangle = \begin{pmatrix} \sqrt{\frac{1+z}{2}} \\ \frac{x+iy}{\sqrt{2(1+z)}} \end{pmatrix} \tag{1.2}$$

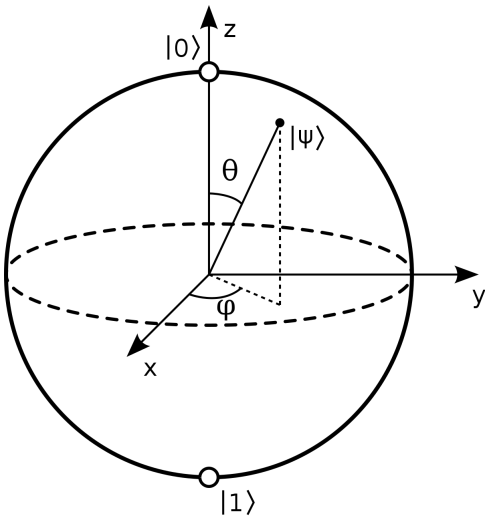


Figura 1.1: Sfera di Bloch di un qubit.

La Figura 1.1 mostra che ogni punto della sfera può essere collegato all'origine tramite un vettore di Bloch, che, naturalmente, dovrà avere modulo unitario $x^2 + y^2 + z^2 = 1$. Inoltre, gli stati della base computazionale sono posizionati ai poli opposti della sfera, come ci si aspetta da (1.1).

1.2.2 I fotoni

Nell'ambito della comunicazione quantistica i qubit di gran lunga più utilizzati sono i fotoni ed il motivo è facilmente intuibile: sono i sistemi più facili da trasmettere su grandi distanze (ovvero dove la QKD ha senso di esistere) e possono essere trasmessi quasi senza introdurre decoerenza, dato che esistono sistemi ottimizzati per trasportare la luce senza che questa interagisca fortemente col mezzo (l'esempio che viene subito alla mente sono le fibre ottiche). Dunque, come esempio rilevante e che sarà di interesse in seguito, si può usare come qubit la polarizzazione di un fotone; per quanto riguarda ciò che verrà trattato in seguito, è sufficiente considerare due diverse basi formate da vettori ortonormali tra loro: quella orizzontale($|H\rangle$)/verticale($|V\rangle$) (+) e quella diagonale($|D\rangle$)/antidiagonale($|A\rangle$) (×), ovvero ruotata di 45° rispetto agli assi.

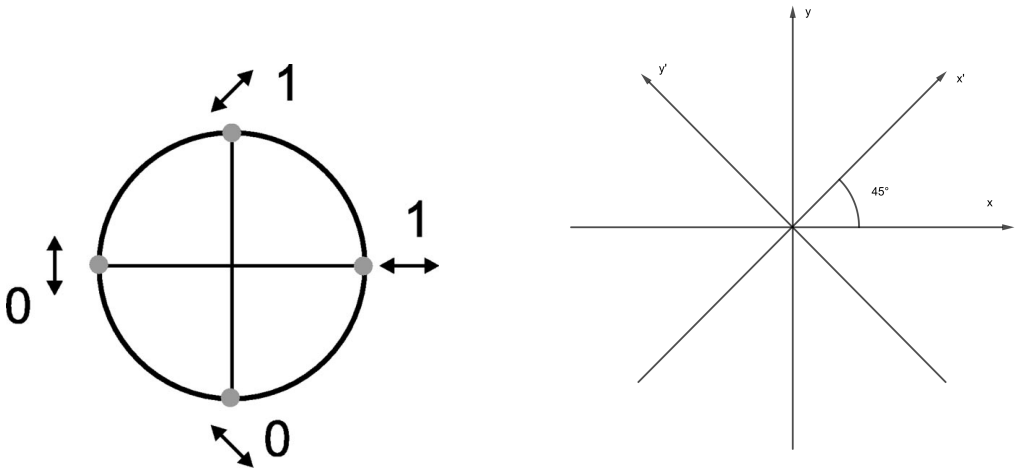


Figura 1.2: Proiezione della sfera di Bloch per quattro stati di polarizzazione (sinistra) e rappresentazione "classica" delle diverse polarizzazioni (destra).

Dall'immagine a sinistra nella Figura 1.2 si vede come questi quattro stati possano essere mappati sulla sfera di Bloch e ad essi possano essere associati dei ket per la base computazionale. In quella a destra, invece, si ha una visualizzazione classica dei quattro stati: gli assi x,y corrispondono ad oscillazioni del campo rispettivamente orizzontale e verticale, dunque saranno associati ad $|H\rangle$ e $|V\rangle$; similmente gli assi ruotati x',y' sono associati $|D\rangle$ e $|A\rangle$.
Infine va fatto notare che i vettori della base diagonale si possono scrivere come combinazioni di quelli della base verticale (e viceversa), infatti vale:

$$|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \qquad |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{1.3}$$

Quest'osservazione risulterà molto importante in seguito, essendo alla base di uno dei protocolli più importanti della QKD.

1.2.3 Lamine

I quattro stati notevoli sull'equatore della sfera di Bloch possono essere ottenuti da stati di partenza $|H\rangle$ o $|V\rangle$ mediante trasformazioni unitarie. Queste trasformazioni unitarie sono implementate nell'apparato per mezzo delle lamine *a quarto d'onda (QWP)* e *a mezz'onda (HWP)*. È utile esaminare più nel dettaglio in cosa consistono queste lamine. Fisicamente, entrambe le lamine sono costituite da un cristallo di quarzo che sfrutta il fenomeno della birifrangenza per creare differenze di cammino ottico tra due polarizzazioni ortogonali rispettivamente di $\lambda/4$ e $\lambda/2$: dunque le prime trasformano una polarizzazione lineare in una circolare, mentre le seconde in un'altra lineare, ma ruotata

rispetto alla prima. Come detto, le due lamine non sono altro che trasformazioni unitarie che agiscono sullo stato in ingresso e possono essere espresse come matrici 2×2; è abbastanza semplice trovare queste matrici se si pensa che la matrice dello sfasamento per uno stato in ingresso con polarizzazione parallela all'asse veloce della lamina può essere scritta nella seguente forma diagonale [2]:

$$S(\Gamma) = e^{i\frac{2\pi}{\lambda}dn_{fast}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{\lambda}d\delta n} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Gamma} \end{pmatrix}$$

in cui d è lo spessore della lamina e n_{fast} l'indice di rifrazione dell'asse veloce, ovvero quello in cui l'indice di rifrazione è più piccolo e dunque la luce si propaga più velocemente. In particolare la HWP corrisponde ad uno sfasamento $\Gamma = \pi$, mentre la QWP a $\Gamma = \pi/2$, ottenendo rispettivamente le matrici

$$S(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad S(\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{1.4}$$

Detto ciò, con una polarizzazione casuale, che forma un angolo θ con l'asse della lamina, sarà necessario applicare una rotazione allo stato, far agire le matrici di sfasamento e poi riapplicare una rotazione di angolo opposto, ovvero l'azione delle lamine può essere ricavata a partire dall'azione combinata di tre operatori unitari

$$HWP \quad \leftrightarrow \quad R(-\theta)S(\pi)R(\theta) \qquad QWP \quad \leftrightarrow \quad R(-\theta)S(\pi/2)R(\theta)$$

usando una generica matrice di rotazione

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

La formula completa si ricava svolgendo il prodotto e le matrici finali rappresentanti l'azione delle lamine ad un angolo generico sono [3]

$$QWP \quad \leftrightarrow \quad e^{-i\pi/4} \begin{pmatrix} \cos^2\theta + i\sin^2\theta & (1-i)\sin\theta\cos\theta \\ (1-i)\sin\theta\cos\theta & \sin^2\theta + i\cos^2\theta \end{pmatrix} \tag{1.5}$$

$$HWP \quad \leftrightarrow \quad e^{-i\pi/2} \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \tag{1.6}$$

In cui θ è l'angolo che forma l'asse veloce rispetto all'asse x (quello orizzontale). Si può mostrare che una combinazione di tre lamine, rispettivamente QWP, HWP, QWP può trasformare un dato stato in ingresso in qualsiasi altro stato, infatti si trova che [2]

$$\hat{U}_{QHQ}(\alpha,\beta,\gamma) = S_\alpha^Q S_\beta^H S_\gamma^Q = \hat{R}_y(2\gamma)\hat{R}_x(2\gamma - 4\beta + 2\alpha)\hat{R}_y(-2\alpha) \tag{1.7}$$

Questo risultato, naturalmente, sarebbe triviale se vi fossero tre diversi assi di rotazione: la cosa più importante, però, di questa formula è il fatto che compaiono solo due assi di rotazione (x,y), fatto che permette di usare solamente due tipi d lamine anziché tre per trasformare uno stato in un altro a piacere.

Per fare un esempio dell'applicazione del risultato, è bene introdurre due nuovi stati, ovvero le polarizzazioni circolari; questi sono a loro volta delle combinazioni lineari delle polarizzazioni verticale e orizzontale, infatti si ha (anche se non c'è una convenzione generale sul segno)

$$|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i\,|V\rangle) \qquad |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i\,|V\rangle) \tag{1.8}$$

Si consideri ora uno stato con polarizzazione orizzontale $|H\rangle$. Esiste un angolo particolare θ^*, per cui una HWP trasformerà $|H\rangle$ in $|D\rangle$, mentre una QWP lo trasforma in $|L\rangle$. I due angoli sono rispettivamente $\pi/8$ e $\pi/4$ e le matrici corrispondenti a questi angoli sono

$$HWP(\theta^*) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad QWP(\theta^*) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

Nella seguente tabella si riassumono tutte le trasformazioni che possono operare queste due matrici sugli stati notevoli

	$HWP(\theta^*)$	$QWP(\theta^*)$
$\|H\rangle$	$\|D\rangle$	$\|L\rangle$
$\|V\rangle$	$\|A\rangle$	$\|R\rangle$
$\|D\rangle$	$\|H\rangle$	$\|D\rangle$
$\|A\rangle$	$\|V\rangle$	$\|A\rangle$
$\|L\rangle$	$\|R\rangle$	$\|V\rangle$
$\|R\rangle$	$\|L\rangle$	$\|H\rangle$

Trasformazioni operate dalle lamine

Si vede come tutti gli stati notevoli vengano mappati in altri stati notevoli; di conse-

guenza tutti gli altri stati verranno a loro volta mappati in stati diversi.

1.3 Vantaggi e problemi

Come conclusione di questo capitolo, si vogliono illustrare i motivi per cui si sta lavorando sulla QKD e i problemi da superare, fisici e tecnologici. Dei primi si è già parlato in precedenza: le chiavi generate da protocolli quantistici assicurano, in linea teorica, una sicurezza assoluta, basata sui principi della meccanica quantistica; in aggiunta, se (quando) i computer quantistici dovessero diventare realtà, esisterebbe già un algoritmo (Shor) che renderebbe l'attuale sistema di crittografia obsoleto.
La QKD non è ovviamente esente da problemi: da una parte quelli pratici, principalmente riuscire ad assicurare la trasmissione di dati lungo notevoli distanze, senza introdurre effetti di disturbo sul segnale; dall'altra quelli economici, ovvero riuscire a creare infrastrutture tali da rendere possibile la QKD a costi inferiori o paragonabili a quelli destinati ai sistemi di crittografia classica; inoltre le applicazioni per cui serve sicurezza assoluta sono limitate, spesso bastano protocolli "abbastanza" sicuri, dove l'abbastanza va quantificato caso per caso.
Molto verosimilmente la QKD non rimpiazzerà completamente gli algoritmi classici, ma coesisterà assieme a questi ultimi per migliorarli.

Capitolo 2

I protocolli della QKD

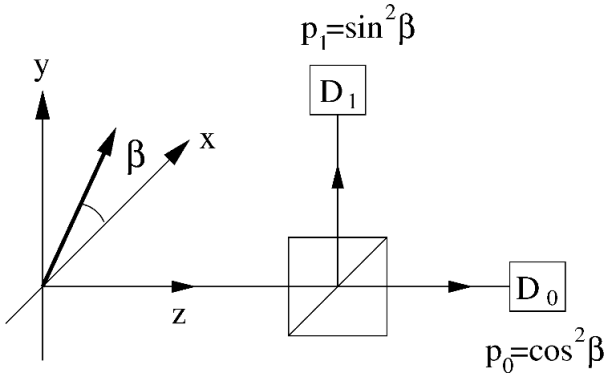
Prima di studiarli più o meno nel dettaglio, è opportuno presentare un risultato di fondamentale importanza per la QKD.

2.1 Teorema di no-cloning quantistico

Prima di presentarlo come teorema vero e proprio, è utile illustrarlo brevemente con un esempio.
Si supponga di avere uno stato generico, polarizzato linearmente lungo una direzione che forma un angolo β (sconosciuto) con l'asse x; allora lo stato si potrà scrivere come combinazione lineare di vettori della base (+), ovvero

$$|\psi\rangle = \cos\beta\,|H\rangle + \sin\beta\,|V\rangle \tag{2.1}$$

Si dispone poi di un apparato di misura, un *polarization beam splitter(PBS)*, ovvero un cristallo avente un materiale dielettrico posizionato lungo la diagonale in grado di lasciar passare la polarizzazione orizzontale e riflettere quella verticale, che separa le due componenti ed un fotone che entra emergerà polarizzato orizzontalmente o verticalmente, rispettivamente con probabilità $p_0 = |\langle H|\psi\rangle|^2 = \cos^2\beta$ e $p_1 = |\langle V|\psi\rangle|^2 = \sin^2\beta$, come illustrato nella figura seguente



Dai postulati della meccanica quantistica, si sa che una misura di una osservabile può dare come risultato un autostato dell'operatore associato all'osservabile con una certa probabilità. Nel caso specifico, il fotone emergerà in uno stato $|H\rangle$ con probabilità p_0 e in uno stato $|V\rangle$ con probabilità p_1: una misura della polarizzazione fornisce dunque un solo bit d'informazione, ovvero lo stato in cui emerge il fotone. Al contrario, se esistesse una macchina capace di clonare lo stato e creare un numero arbitrariamente grande di copie, sarebbe possibile determinare l'angolo β con altissima precisione e ciò vorrebbe dire riuscire a estrarre un quantitativo d'informazione arbitrariamente grande (i bit necessari a rappresentare β); dato che la macchina è da considerarsi parte dell'apparato di misura, ciò contraddirebbe il postulato. È importante sottolineare che lo stato iniziale $|\psi\rangle$, debba essere uno stato generico, altrimenti nulla proibisce di misurare lo stato e a quel punto crearne delle copie. Viene presentato ora il risultato appena ottenuto, formalizzandolo sotto forma di teorema generale, presentato per la prima volta da Zurek e Wootters (1982). [1]

Teorema 1 (Teorema no-cloning)**.** *È impossibile costruire una macchina che operi una trasformazione unitaria capace di clonare uno stato generico ψ di un qubit.*

Come ultima osservazione su questo teorema, si vuole menzionare il fatto che, se quest'ultimo non fosse vero, sarebbe violato il postulato della relatività speciale secondo cui nessuna informazione può viaggiare più velocemente della luce, a riprova dell'intima connessione presente tra meccanica quantistica e relatività speciale già menzionata nel capitolo 1.

2.2 BB84

Il protocollo BB84 fu tra i primi ad essere ideati ed è tutt'oggi uno tra i più importanti, oltre ad essere quello su cui si basa l'esperimento che verrà presentato e descritto in seguito. Questo protocollo fu sviluppato per la prima volta da C.H. Bennett e G. Brassard nel 1984 (da cui il nome del protocollo, formato dalle iniziali e dall'anno) e prevede l'uso di di due alfabeti diversi e di quattro diversi stati, ciascuno appartenente ad un certo alfabeto, nel senso che formerà uno stato di base per quell'alfabeto.
In concreto, si useranno i due alfabeti già presentati σ_+ e $\sigma_\times$, a cui sono associati a due a due rispettivamente $|H\rangle$, $|V\rangle$, $|D\rangle$ e $|A\rangle$; è bene qui ricordare la relazione (1.3), che lega i diversi stati, la quale si traduce nel fatto che, scelti due stati appartenenti a due diversi alfabeti, vale sempre $|\langle H|D\rangle|^2 = \frac{1}{2}$, ovvero, in analogia all'algebra delle particelle di spin 1/2, le due osservabili σ_+ e $\sigma_\times$ non commutano.
L'uso di quattro stati non tutti ortogonali tra loro è necessario al fine di sfruttare il principio di indeterminazione di Heisenberg, la base su cui poggia il protocollo: l'idea, infatti, è che, usando due osservabili che non commutano -com'è il caso di σ_+ e $\sigma_\times$- un processo di misura proietterà lo stato in un certo autospazio e inevitabilmente ciò disturberà il sistema; così per Alice e Bob è possibile sapere se Eve abbia ascoltato la conversazione, cosa che sarebbe classicamente impossibile da capire.
In pratica, la descrizione del protocollo è la seguente: [1]

1. Alice genera una sequenza casuale di 0 e 1. Qui è molto importante che la sequenza sia realmente casuale.

2. Alice sceglie, in accordo con Bob, quali stati associare a ciascun bit. Ad esempio una scelta convenzionale è quella di associare $|V\rangle$ e $|D\rangle$ a 0 e gli altri due a 1. Anche qui, Alice sceglie casualmente quale tra i due stati associare a ciascun bit, ovvero che alfabeto usare.

3. Quando Bob riceve i qubit, deve a sua volta scegliere casualmente che alfabeto usare. In media, il 50 % delle volte sceglierà lo stesso di Alice e i due condivideranno lo stesso bit (se non vi è stato un intervento da parte di Eve e trascurando le possibili cause di rumore che possano alterare lo stato del qubit); negli altri casi, quando i due alfabeti sono diversi, i due otterranno lo stesso bit solo la metà delle volte, in forza della probabilità già calcolata. Da qui in poi Alice e Bob scambiano informazioni solo tramite un canale classico.

4. Alice e Bob comunicano attraverso questo canale quali alfabeti hanno usato ad ogni qubit (senza però rivelare il risultato della misura) e scartano tutti i bit in cui hanno usato alfabeti diversi. Alla fine di questo passaggio i due condividono quella che è chiamata *raw key*, che sarà formata da circa metà bit rispetto a quelli iniziali.

5. I due a questo punto comparano una parte dei bit, in modo da stimare il tasso d'errore R: se quest'ultimo è troppo alto i due concludono che ci possa essere stata un'intrusione di Eve nel canale (non è sicuro al 100 %, potrebbero anche essere solo effetti di rumore) e ricominciano il protocollo da capo.

Arrivati a questo punto, dunque, Alice e Bob condividono la raw key, che conterrà un certo numero di errori; è prudente assumere che quest'ultimi siano causati dall'intromissione di Eve nel canale, con conseguente aumento dell'informazione che Eve ha sulla chiave. È utile illustrare come questo possa succedere con un esempio.
Senza entrare troppo nel dettaglio dei tipi di strategie che Eve potrebbe adottare, ve n'è una classe detta *attacchi individuali*, in cui Eve intercetta e misura individualmente ogni bit inviato da Alice; tra queste, in particolare, Eve potrebbe fare quello che viene chiamato *intercept and resend* in cui ella misura i qubit inviati da Alice in uno dei due alfabeti -scelto casualmente- e li rispedisce a Bob; grazie al teorema no-cloning, infatti, Eve non può copiare lo stato per capire quale alfabeto usare ed è costretta a sceglierlo in modo casuale. Chiaramente Eve sceglierà lo stesso alfabeto di Alice metà delle volte ed in quei casi il suo intervento non perturberà lo stato del qubit, dunque avrà un'informazione sulla chiave I=0.5; al contrario, quando sceglie l'alfabeto "sbagliato", comunque in metà dei casi Bob otterrà lo stesso risultato di Alice, quindi Eve introduce errori nella chiave solo quando Bob misura nella stessa base di Alice, ma ottiene un risultato diverso a causa di Eve, dunque il tasso d'errore sarà R=0.25. Eve potrebbe anche decidere di adottare questa strategia solo su una frazione p dei qubit e naturalmente si avrà R=p/4 e I=p/2=2R; si trova poi che se p$\gtrsim$68%, cioè se R$\gtrsim$17% Eve ha più informazione di Bob sulla stringa di bit e ovviamente è necessario ricominciare il protocollo. [4]
Al fine di correggere gli errori ed aumentare la sicurezza della chiave, si utilizzano due protocolli classici, chiamati informtion riconciliation e privacy amplification. Il primo è un algoritmo classico di correzione di errori su un canale pubblico e funziona nel modo seguente: Alice sceglie in modo casuale delle parti di chiave di lunghezza l (in modo che Rl$\ll$1, cioè sia poco probabile avere più di un errore in ciascun insieme) e per ognuno di questi sottoinsiemi i due procedono a controllare la parità, ovvero la somma dei bit

modulo 2; se questa risulta uguale, i due tengono i bit della sequenza scartando l'ultimo, altrimenti scartano la sequenza; così facendo si assicurano che Eve non ottenga alcuna informazione aggiuntiva da questa procedura. Il secondo, invece, si utilizza per ridurre l'informazione che Eve ha sulla chiave finale: anche in questo caso si scelgono dei sottoinsiemi e se ne calcola la parità, ma stavolta quest'ultima viene utilizzata come bit vero e proprio nella chiave finale; si capisce che, in questo modo, Eve dovrebbe conoscere ogni bit del sottoinsieme per risalire al bit finale, altrimenti l'informazione che possedeva diminuisce.
È bene infine ricordare che Alice e Bob inizialmente devono comunque condividere una chiave, seppur corta, in modo da poter autenticare il canale; in questo senso la QKD può essere vista come un protocollo per espandere la chiave inizialmente posseduta dalle due parti.

2.3 Altri protocolli

Nel corso degli anni sono state sviluppate decine di protocolli, ognuno con le proprie caratteristiche peculiari, più o meno utili a seconda del particolare esperimento. Di seguito si illustrano brevemente due di essi.

2.3.1 Sei stati

È una variante del BB84 che usa tre alfabeti anziché due; ad esempio, se come qubit si usa la polarizzazione del fotone, i due stati aggiuntivi possono essere la polarizzazione circolare destra ($|R\rangle$) e sinistra ($|L\rangle$).

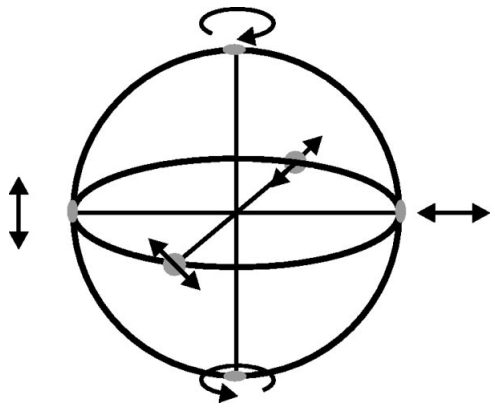


Figura 2.1: Posizione sulla sfera di Bloch dei sei stati usati nel protocollo.

Dunque il protocollo costituisce a tutti gli effetti un'estensione del BB84. Il vantaggio derivante dall'usare tre alfabeti anziché due è che l'intervento di Eve può essere notato più facilmente, ovvero se Eve misura ogni qubit introduce un tasso d'errore del 33% anziché 25%, in quanto ha solo 1/3 delle possibilità di usare la stessa base di Alice. Lo svantaggio, naturalmente, è che la preparazione dell'esperimento richiede una maggiore attenzione. [5]

2.3.2 E91

Più interessante è il seguente protocollo, inventato da Ekert nel 1991. L'approccio è completamente diverso dal BB84, in quanto utilizza coppie di qubit entangled, dette coppie EPR, e sfrutta violazioni delle disuguaglianze di Bell per capire se vi sono state intromissioni nel canale da parte di Eve.

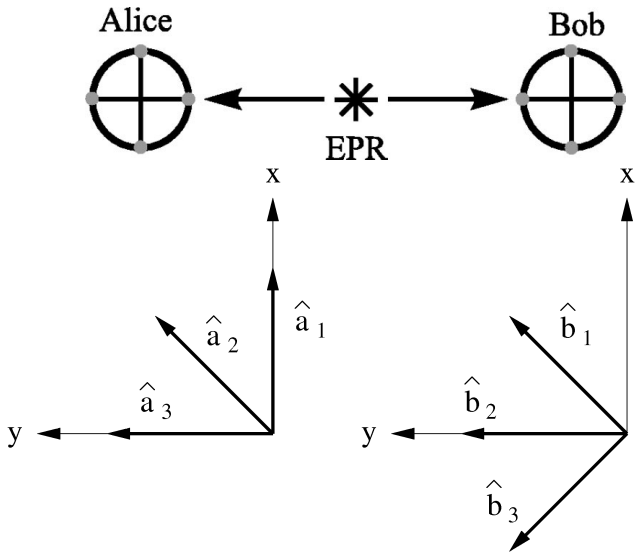


Figura 2.2: Schema del protocollo E91 (sopra) e posizionamento degli assi di misura (sotto)

La sorgente S emette coppie di qubit (ad es. particelle di spin 1/2) entangled, aventi una funzione d'onda del tipo

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

poi un qubit arriva ad Alice e l'altro a Bob. A questo punto i due potrebbero confrontare la scelta delle basi e scartare i bit in cui le hanno scelte diversamente e il protocollo sarebbe equivalente al BB84, perché nei casi in cui i due hanno scelto la stessa base, i loro bit sono perfettamente correlati.

Il protocollo E91, invece, prevede che Alice possa misurare la polarizzazione lungo tre assi $(\hat{a_1}, \hat{a_2}, \hat{a_3})$ e analogamente Bob lungo $(\hat{b_1}, \hat{b_2}, \hat{b_3})$, come mostrato in Fig. 2.2; si calcolano poi le probabilità $p_{\pm\pm}(\hat{a_i}, \hat{b_j})$ che Alice ottenga ± 1 misurando la polarizzazione lungo l'asse $\hat{a_i}$ e contemporaneamente Bob ottenga ± 1 misurando la polarizzazione lungo l'asse $\hat{b_j}$ e si definiscono i coefficienti di correlazione (altro non sono che il valore d'aspettazione delle correlazioni tra le due misure effettuate lungo due determinati assi scelti rispettivamente da Alice e Bob)

$$E(\hat{a_i}, \hat{b_j}) = p_{++}(\hat{a_i}, \hat{b_j}) + p_{--}(\hat{a_i}, \hat{b_j}) - p_{+-}(\hat{a_i}, \hat{b_j}) - p_{-+}(\hat{a_i}, \hat{b_j})$$

e da qui si ottiene la funzione di correlazione

$$C \equiv E(\hat{a_1}, \hat{b_1}) - E(\hat{a_1}, \hat{b_3}) + E(\hat{a_1}, \hat{b_3}) + E(\hat{a_3}, \hat{b_3}) = -2\sqrt{2} \tag{2.2}$$

Il risultato è ottenuto utilizzando i postulati della meccanica quantistica, i quali predicono un risultato $|C| \leq 2\sqrt{2}$, mentre considerando validi realismo e località si otterrebbe la disuguaglianza CHSH $|C| \leq 2$ [1], dunque violazioni della disuguaglianza sono predette dalla meccanica quantistica.

A questo punto Alice e Bob annunciano sul canale pubblico gli assi scelti per ogni misura e, se questi risultano diversi, anche i risultati, in modo da verificare l'uguaglianza (2.2). Se $|C| \neq 2\sqrt{2}$, significa che Eve stava ascoltando la conversazione e potrebbe aver acquisito delle informazioni (oppure il canale era molto rumoroso). Altrimenti, i due tengono i bit nei quali hanno scelto gli stessi assi, sapendo che i risultati che hanno ottenuto sono perfettamente correlati e questa costituirà la loro raw key; si procede poi analogamente al BB84. Chiaramente, in un esperimento reale sarà impossibile raggiungere il valore $C = 2\sqrt{2}$, ma si fisserà preventivamente un certo valore di controllo (che sarà espresso in percentuale rispetto al valore ideale $2\sqrt{2}$): se C risulta maggiore di questo valore si prosegue, altrimenti si abbandona il protocollo.

Infine, va menzionato che questo protocollo è utile per l'immagazzinamento della chiave: una volta creata la chiave, questa va tenuta al sicuro finché non risulta necessario utilizzarla; in questo lasso di tempo, però, Eve potrebbe entrarne in possesso. Al contrario, utilizzando coppie EPR, queste potrebbero essere create e tenute da parte fino al momento in cui si inizia la conversazione, dove verrebbero poi misurate al fine di creare la chiave.

Capitolo 3

Apparato Sperimentale

Di seguito vengono presentati via via i vari componenti utilizzati per costruire l'apparato sperimentale e i risultati numerici ottenuti dall'esperimento nel suo insieme; è bene sempre ricordare che l'apparato è pensato per l'implementazione del protocollo BB84. A tal proposito, nell'immagine seguente è illustrato un apparato pensato per l'implementazione di tale protocollo nella sua interezza.

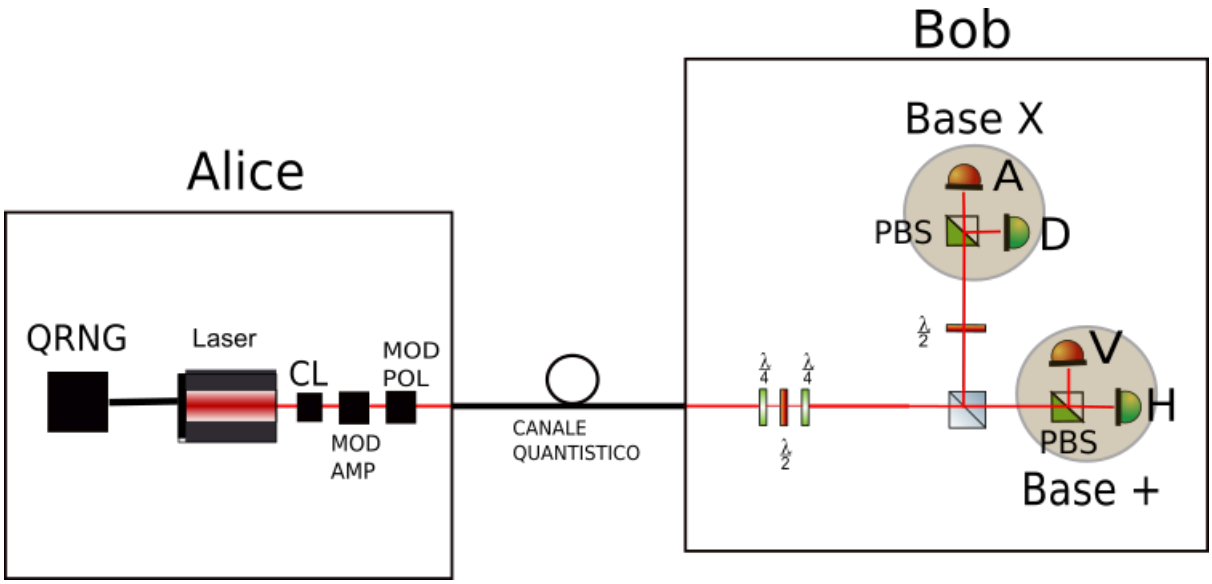


Figura 3.1: Schema completo di un apparato sperimentale per l'implementazione del BB84. Nella parte di Alice sono presenti: laser, controllo laser, QRNG(generatore numeri casuali), modulatore di ampiezza(per creare fasci in approssimazione a singolo fotone) e modulatore di polarizzazione (per creare i quattro stati H,V,D e A da usare ne protocollo). Il canale quantistico solitamente può essere fibra oppure free space. Dalla parte di Bob vi sono tre lamine, un BS (beam splitter) che separa in due canali diversi i due alfabeti utilizzati nel protocollo, PBS (polarization beam splitter) e dei fotodiodi per registrare la potenza del segnale in output.

Alice è il *sender*, ovvero il mittente, ma il seguente lavoro di tesi si concentra sull'apparato di ricezione, rappresentato da Bob; i vari componenti caratterizzanti l'apparato verranno presentati e descritti in seguito. Innanzitutto bisognerà assicurarsi che ogni elemento non distrugga o modifichi il qubit codificato nella polarizzazione dei fotoni; successivamente bisognerà caratterizzare le lamine per essere in grado di ricevere tutti e quattro (o sei, considerando anche le polarizzazioni circolari) gli stati di polarizzazione necessari nell'implementazione del protocollo e bisognerà allineare le basi di Alice con quelle dell'apparato di ricezione, in modo da assicurarsi di usare gli stessi stati di riferimento. In particolare, un problema nell'apparato di ricezione consiste nel fatto che il canale quantistico cambia lo stato di polarizzazione del qubit inviato da Alice; questo cambiamento può essere causato da imperfezioni nella fibra, fluttuazioni meccaniche o termiche ecc. Si vedrà che una combinazione di tre lamine come in figura può cambiare uno stato in qualsiasi altro a piacere: per segnali molto veloci questo non potrà essere fatto manualmente, ma c'è bisogno di uno strumento automatico che verrà descritto e caratterizzato successivamente.

3.1 Caratterizzazione degli stati

Negli esperimenti di QKD con protocollo BB84 solitamente vengono usati deboli impulsi laser, per approssimare meglio possibile la situazione di fotone singolo; qui debole significa che la probabilità che dal laser esca più di un fotone è molto bassa. Infatti, lo stato della luce all'uscita del laser può essere descritta da uno stato del tipo: [4]

$$|\alpha\rangle = e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{3.1}$$

in cui $\mu = |\alpha|^2$ è l'intensità del fascio (ovvero il numero medio di fotoni emessi) e $|n\rangle$ è lo stato caratterizzato da n fotoni (sono gli stessi autostati dell'oscillatore armonico); dunque, dire che gli impulsi laser sono deboli equivale a dire che μ sarà un numero $\lesssim 1$. Si fa ciò per evitare che Eve possa mettere in atto un attacco al canale detto *PNS (photon number splitting)* in cui, negli impulsi in cui è presente più di un fotone, Eve intercetta quelli "in più", ma ne fa comunque arrivare almeno uno a Bob; in questo modo ella possiede lo stesso stato che ha Bob e può estrarre informazioni da esso.
Lo scopo della presente tesi, però, è quello di caratterizzare il sistema ricevitore, dunque non si è mai reso necessario l'uso di sorgenti deboli, ma si è sempre utilizzato un laser

che erogava una potenza di alcuni milliWatt, regolabile a seconda delle necessità, in quanto risulta molto più pratico sperimentalmente lavorare con sorgenti di questo tipo. Per tutta la durata dell'esperimento, inoltre, si sono sempre utilizzate fibre ottiche in silice per guidare la luce, tranne in un caso che verrà descritto a breve. Nelle fibre la luce è guidata dal profilo dell'indice di rifrazione $n(x, y)$(assumendo l'asse z quello di propagazione della luce): in particolare l'equazione che descrive il cammino ottico della luce è uguale all'equazione di Schrödinger con $V(x, y) = -n(x, y)$, dunque un picco nell'indice di rifrazione equivale ad una buca di potenziale per la luce; questa zona viene chiamata *core*. Inoltre nelle moderne fibre le perdite sono state ridotte fino a 0.2 dB/km alla lunghezza d'onda di 1550 nm (anche se per questo lavoro le perdite lungo le fibre non sono importanti). In particolare, se ne sono usate di due tipi:

Single Mode Fiber (SMF) Possiedono un core relativamente piccolo, le cui dimensioni dipendono dalla lunghezza d'onda per cui è stata costruita la fibra, così da permettere il passaggio della luce a 1550 nm in un unico modo (armonica). Diametri più grandi, infatti, permetterebbero il passaggio della luce con diverse armoniche, ma queste si accoppiano facilmente e agiscono sul qubit come del rumore esterno; fibre di questo tipo sono dette multimodo ma non risultano appropriate per la costruzione di canali quantistici, sono invece utili ad esempio se si vuole misurare la potenza totale quando si accoppia da free space a fibra (si perdono, però, tutte le altre informazioni) . Le fibre singolo modo, invece, hanno un profilo di intensità nel piano (x, y) approssimativamente gaussiano (di fatto dunque con dipendenza radiale).

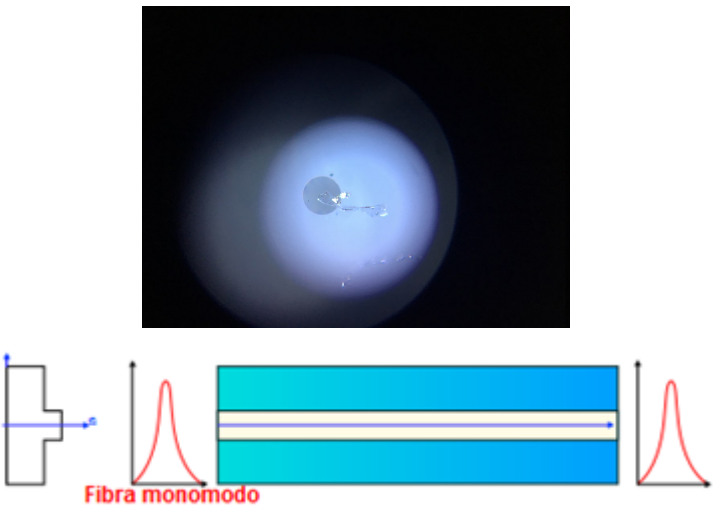


Figura 3.2: Interno di una fibra SMF, il core si trova all'interno del cerchio nero (sopra) e profilo di n(r) in una SMF (sotto).

Polarization Mantaining Fiber (PMF) Tutti i materiali possono presentare birifrangenza, l'effetto per cui due polarizzazioni ortogonali tra loro si propagano a velocità diverse a causa di asimmetrie nella fibra, che si riflettono in asimmetrie nell'indice di rifrazione. Questo tipo di fibre è costruito appositamente per presentare una forte birifrangenza e disaccoppiare i due autostati della polarizzazione [5]; l'asimmetria è introdotta nella fibra attraverso due placche metalliche poste ai lati del core , le quali aumentano l'indice di rifrazione lungo quella direzione, definendo così un asse lento ed un altro veloce, come mostrato nella figura di seguito. Lo svantaggio di queste fibre è che possono introdurre depolarizzazione; è chiaro, però, che il loro utilizzo risulta imprescindibile, in quanto indispensabili per misurare le diverse potenze associate ai vari stati di polarizzazione: esse infatti costituiscono la parte fondamentale di un PBS in fibra (il principio di funzionamento è lo stesso dei cristalli), mostrato nella figura sottostante.

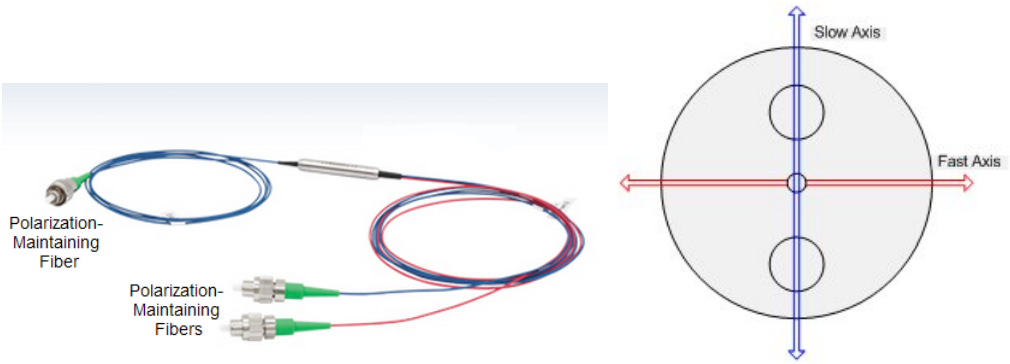


Figura 3.3: PBS in fibra, che utilizza due fibre PMF in output per guidare le due diverse polarizzazioni su canali diversi(a sinistra) e sezione, con in evidenza le placche metalliche lungo l'asse lento(a destra)

3.1.1 Depolarizzazione

Il primo passo della caratterizzazione dell'apparato ricevitore consiste proprio nel verificare che i vari elementi non introducano depolarizzazione. Prima di proseguire con la presentazione dei vari risultati, è utile approfondire meglio quest'ultimo concetto.
La *depolarizzazione* è un fenomeno che si verifica quando si perde il grado di libertà sulla polarizzazione: lo stato non è semplicemente polarizzato casualmente (cosa che, come verrà mostrato, è facilmente risolvibile), ma perde del tutto la polarizzazione e non ne possiede più una definita. Chiaramente, questo effetto è assolutamente da evitare se si usano come qubit proprio le polarizzazioni dei fotoni, in quando perdere la polarizzazione significa perdere informazione. Classicamente, uno stato non polarizzato

è descritto da un insieme di varie polarizzazioni ognuna avente un certo peso: in uno stato completamente depolarizzato ogni polarizzazione è presente con uguale probabilità. Quantisticamente è necessario parlare di stati misti col formalismo delle matrici di densità. Per quanto riguarda le depolarizzazioni nel presente apparato strumentale, la matrice di densità può essere espressa in termini di $|H\rangle$ e $|V\rangle$ nel modo seguente

$$\rho = \omega_H |H\rangle \langle H| + \omega_V |V\rangle \langle V| \qquad , \qquad \omega_H + \omega_V = 1 \tag{3.2}$$

in cui ω_H e ω_V sono i pesi probabilistici dei due stati. Una caratteristica che si evince da questa formula è che uno stato misto non sta sulla sfera di Bloch, cioè non è descritto da un versore unitario (in generale sarà più piccolo, dunque interno alla sfera).

Stati H e V

Al fine di verificare che i vari componenti non introducano depolarizzazione, è necessario verificare, mediante l'uso di un *manual polarization controller (MPC)*, che sia sempre possibile, partendo dallo stato generico (2.1) raggiungere lo stato puro (0,1), in cui tutta la potenza viene raccolta da un determinato tipo di polarizzazione, ad esempio cioè che lo stato finale sia $|H\rangle$ (o $|V\rangle$ equivalentemente); infatti, guardando la formula (3.2) si nota che se, ad esempio, $\omega_V \neq 0$ non sarà mai possibile ottenere uno stato $|H\rangle$ puro, qualsiasi operazione unitaria si faccia agire sullo stato di partenza.
Nella figura sottostante (a sinistra) è mostrato un esempio di MPC, consistente di tre lamine, rispettivamente a quarto d'onda *(QWP)* e a mezz'onda *(HWP)* e di nuovo a quarto d'onda, che consentono di trasformare qualsiasi stato di partenza del tipo (1.1) in un altro stato qualsiasi a scelta, e il risultato (1.7) assicura che per fare ciò bastino due tipi di lamine combinate in questo modo; muovendo le tre lamine, infatti, è possibile cambiare lo stato in entrata fino a raggiungere quello desiderato.
È chiaro che, sperimentalmente, sarà impossibile raggiungere una potenza esattamente nulla su un certo ramo: quello che si è fatto è stato cercare di minimizzare la potenza su un ramo, massimizzando in corrispondenza la potenza sull'altro, fino ad ottenere un rapporto tra le due potenze sufficientemente basso; nel caso della QKD tale rapporto è sufficiente sia almeno 1 a 50.
Un semplice apparato per creare stati ortogonali $|H\rangle$ e $|V\rangle$ è mostrato nella figura seguente (a destra), consistente nella sorgente, l'MPC per variare la potenza sui due

rami H e V e, infine, un PBS in fibra per separare le due polarizzazioni.

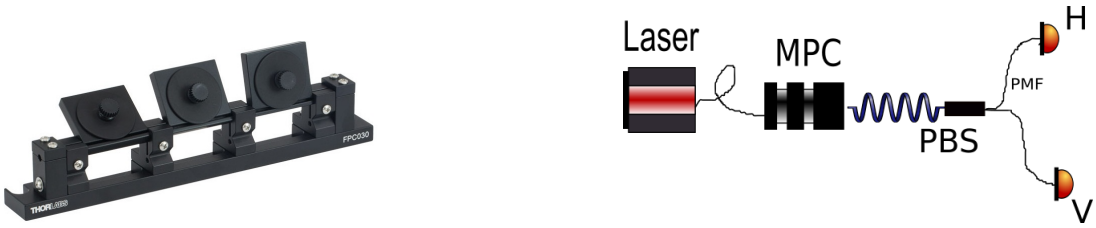


Figura 3.4: Esempio di MPC (a sinistra) e raffigurazione di un semplice apparato per la misura di due stati ortogonali di polarizzazione (a destra).

Le potenze in uscita vengono sempre misurate attraverso dei fotodiodi connessi con dei powermeter, strumenti in grado di leggere la potenza in ingresso e dotati di un display digitale che mostra tale potenza letta. Il risultato ricavato da questo semplice apparato è il seguente:

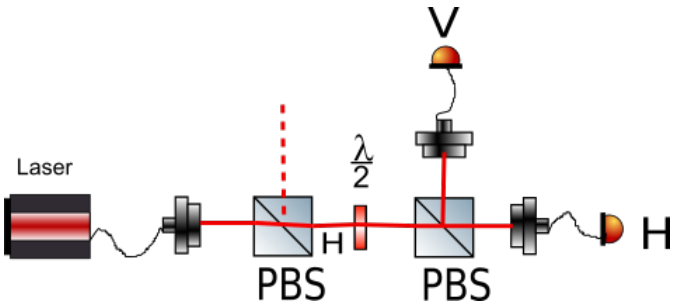
P_H	P_V	rapporto
$2.577\ mW$	$310 \pm 200\ nW$	$\sim$ 1 a 8000

Risultati per le polarizzazioni H e V

Il valore dell'errore di P_V è stato ricavato notando che il minimo cambiamento nella potenza possibile usando il MPC era appunto di $200\ nW$; per P_H questo risulta talmente piccolo che è irrilevante. Al di là di ciò, quello che conta è che il rapporto tra le due potenze si mantiene molto più alto del necessario, dunque si può concludere che le fibre PMF utilizzate nell'apparato non introducono depolarizzazione.

Stati D,A,R e L

L'apparato usato per la caratterizzazione degli altri stati è rappresentato di seguito:



Per prima cosa è stato necessario allineare e collimare i fasci laser uscenti ed entranti nei detector per evitare dispersione della luce; questo è stato possibile attraverso

l'uso di adattatori tra fibra e free space montati su cavalletti mobili: muovendo appropriatamente cavalletti e adattatori (tramite delle piccole viti che permettevano lievi spostamenti in tutte e tre le direzioni) è stato possibile guidare appropriatamente la luce negli adattatori che la raccoglievano e la inviavano ai detector. Tramite l'uso di un PBS è stato possibile fare in modo di avere in entrata della lamina lo stato $|H\rangle$. A questo punto per caratterizzare le lamine è necessario trovare l'angolo per cui lo stato $|H\rangle$ viene trasformato in $|R\rangle$ (QWP) o $|A\rangle$ (HWP); in questo modo, successivamente, si saprà che, impostando la lamina sull'angolo corretto, se da un lato entra $|H\rangle$, dall'altro uscirà $|R\rangle$ o $|A\rangle$ e, viceversa, avendo $|R\rangle$ o $|A\rangle$ in entrata uscirà $|H\rangle$, stato che può essere rilevato dai detector tramite l'uso delle PMF; quest'ultimo caso è quello rilevante nell'implementazione del BB84. In realtà gli angoli per cui ciò accade sono quattro: ruotando la lamina si nota, infatti, che si raggiungono quattro massimi e quattro minimi della potenza. La caratterizzazione delle due lamine è praticamente analoga, ma presenta una differenza.

Per quanto riguarda la HWP, trattandosi di lamine che trasformano una polarizzazione lineare in un'altra lineare, ma ruotata, si sono cercati tutti i massimi e tutti i minimi segnandosi l'angolo associato a tutti e otto; ci si è poi posizionati all'incirca nell'angolo a metà tra quelli corrispondenti a due estremi consecutivi cercando di fare in modo che la potenza letta sul ramo V fosse uguale a quella letta sul ramo H: infatti, ricordando la (1.3), questo succede quando lo stato in uscita dalla lamina è $|A\rangle$ (o equivalentemente $|D\rangle$). Si è ottenuto il seguente risultato

	P_{max}/θ_{max}	P_{min}/θ_{min}	θ	P_H	P_V
1°	4.446 mW / 37°	12.9 μW / 82°	60°	2.217 mW	2.262 mW
2°	4.400 mW / 126°	6.85 μW / 173°	150°	2.209 mW	2.200 mW
3°	4.460 mW / 219°	13.5 μW / 262°	241°	2.215 mW	2.250 mW
4°	4.545 mW / 309°	14.6 μW / 352°	332°	2.210 mW	2.230 mW

Risultati per la caratterizzazione della HWP

A questo punto, si può cercare di capire se questi risultati sperimentali ben si accordino con le previsioni teoriche; infatti, la potenza in uscita è data, in funzione dell'angolo, dal prodotto $|\langle H|\, HWP\, |H\rangle|^2$. Ricordando la matrice della lamina a mezz'onda (1.6), si trova $P(\theta) = \cos^2 2\theta$, che andrà poi ovviamente riscalata per la potenza totale del circuito. Il grafico risultante è il seguente

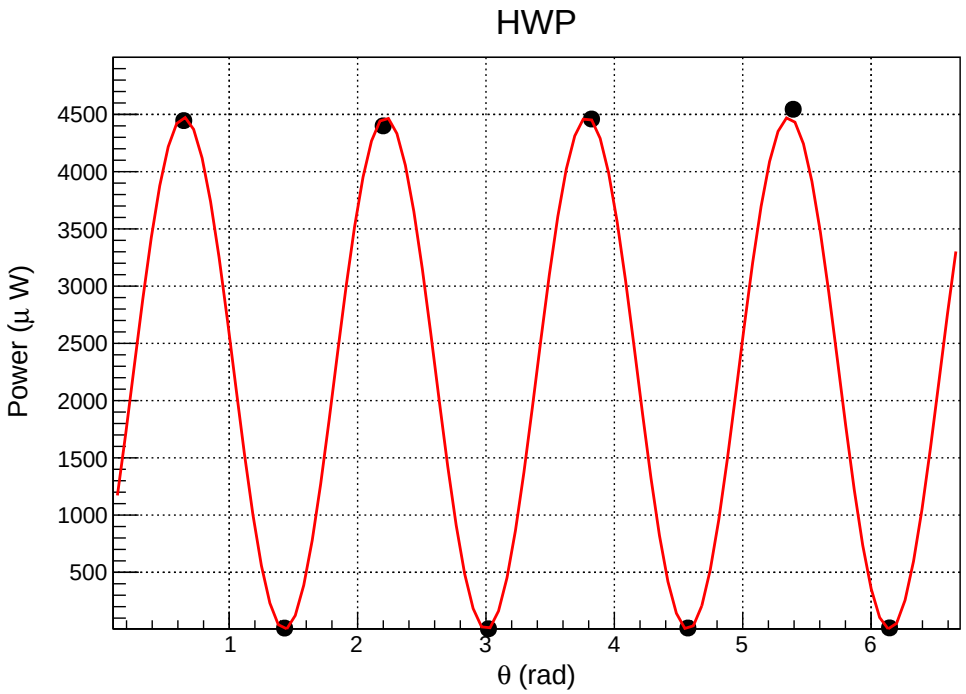


Figura 3.5: Confronto tra potenza teorica e punti sperimentali per la HWP

Dunque i punti sperimentali sono in buon accordo con l'andamento teorico della potenza. La lamina, inoltre, non introduce depolarizzazione, in quanto P_{max}/P_{min} è sempre maggiore di 1 a 500, dunque ancora molto alto.

Dai vari angoli θ ottenuti si può fare una media (tenendo conto di sottrarre multipli crescenti di 90° per ogni angolo successivo); così facendo si ottiene che il valore per l'angolo della lamina è $\theta_{HWP} = 61°$ (sempre a meno di multipli interi di 90°).

Per quanto riguarda le QWP, invece, esse in generale trasformano una polarizzazione lineare in una ellittica. Se, però, la polarizzazione è allineata con l'asse della lamina, questa agirà come l'identità sullo stato in ingresso, lasciando dunque lo stato invariato; al contrario, se la polarizzazione in ingresso è ruotata di 45° rispetto all'asse, la polarizzazione in uscita sarà circolare, la quale è data dalla combinazione lineare di due polarizzazioni lineari sfasate di $\pi/2$ l'una rispetto all'altra; per tutti gli altri angoli la polarizzazione sarà, appunto, ellittica. Dunque, nel caso della QWP la potenza in uscita non può estinguersi, ma il "minimo" corrisponderà proprio al caso della polarizzazione circolare; anche qui sono riassunti in tabella i vari angoli trovati

	P_{max}/θ_{max}	P_{min}/θ_{min}	θ	P_H	P_V
1°	4.460 mW / 38°	2.240 mW / 81°	82°	2.255 mW	2.170 mW
2°	4.450 mW / 125°	2.180 mW / 170°	170°	2.190 mW	2.230 mW
3°	4.400 mW / 216°	2.220 mW / 260°	262°	2.223 mW	2.180 mW
4°	4.377 mW / 308°	2.220 mW / 351°	351°	2.235 mW	2.220 mW

Risultati per la caratterizzazione della QWP

Anche qui, ricordando la rappresentazione matriciale (1.5) è possibile risalire alla potenza teorica $P(\theta) = \cos^4\theta + \sin^4\theta$ e rappresentarla graficamente

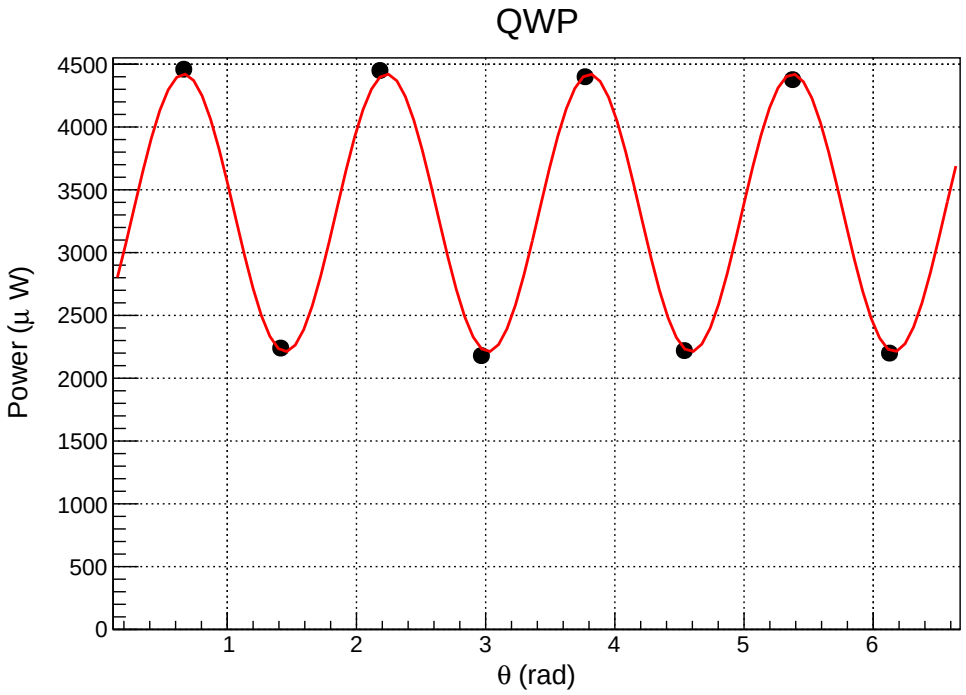


Figura 3.6: Confronto tra potenze teorica e punti sperimentali per la QWP

Qui si vede chiaramente come la potenza non vada mai a zero; inoltre i punti si dispongono abbastanza bene lungo la curva.

Anche qui, come per l'altra lamina, si può fare una media ottenendo $\theta_{QWP} = 81°$ (a meno di multipli interi di 90°).

3.2 Automatic Polarization Controller

Appurato che sia possibile ricevere sia gli stati $|H\rangle$ e $|V\rangle$, che quelli diagonali $|A\rangle$ e $|D\rangle$ da Alice senza introdurre depolarizzazione nell'apparato, è possibile passare al componente principale del sistema, ovvero l'*Automatic Polarization Controller (APC).*

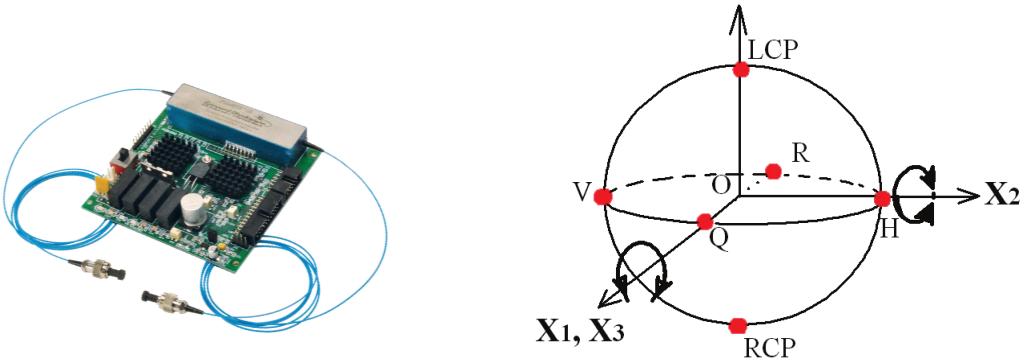


Figura 3.7: Immagine del dispositivo APC (sinistra) e corrispondenti assi di rotazione sulla sfera di Bloch(destra).

In generale, nella trasmissione del qubit lungo il canale da Alice a Bob, lo stato subirà delle modificazioni; queste sono da imputarsi principalmente a cambiamenti locali dell'indice di rifrazione, dovuti a modificazioni meccaniche della fibra (torsioni o pressioni sul filo) e a fluttuazioni termiche, i quali causano diversi fenomeni di birifrangenza che, appunto, ruotano e modificano lo stato di polarizzazione del qubit. Essendo queste modificazioni casuali e talvolta molto rapide, è necessario uno strumento che controlli costantemente che un certo parametro del sistema soddisfi certe condizioni e corregga eventuali errori non appena queste condizioni non sono più soddisfatte, agendo, dunque, come strumento a feedback.

Nel seguente esperimento, questo ruolo è ricoperto proprio dall'APC. Il cuore di quest'ultimo è formato da quattro placche di materiale piezoelettrico allineate una dopo l'altra capaci di modificare la loro struttura meccanica (e dunque il loro indice di rifrazione) se sottoposte ad una differenza di potenziale: controllando il potenziale applicato ad ogni placca, è dunque possibile controllare e modificare lo stato di polarizzazione della luce in input, ottenendo lo stato desiderato in output. L'immagine di destra della Fig. 3.6 mostra come l'applicazione di un certo potenziale ad ogni placca, corrisponda ad una rotazione dello stato sulla sfera di Bloch (oraria se il voltaggio aumenta, antioraria altrimenti) intorno a due diversi assi tra loro ortogonali (i pedici degli assi corrispondono ad una certa placca); la prima e la terza fanno ruotare attorno all'asse

D-A, mentre la seconda attorno a H-V (la quarta, in realtà, non è associata a nessun asse di rotazione, perciò vengono usate solo le prime tre): in questo modo, da ogni stato in input è possibile raggiungere qualsiasi altro stato desiderato in output (agisce per l'appunto allo stesso modo di un MPC).

Anche in questo caso, si è verificato che, inserendo l'apparato in un sistema come quello in Fig. 3.3, questo non introducesse depolarizzazione. Ciò che si è ottenuto è riassunto in tabella

P_H	P_V	rapporto
2.363 mW	420 ± 200 nW	$\sim$ 1 a 5600

Risultati per l'introduzione dell'APC nel sistema

Anche in questo caso il rapporto si mantiene ben al di sopra del minimo necessario, dunque non si presenta alcun problema di depolarizzazione nell'uso dell'APC.

Appurato ciò, si è potuto procedere a testare e caratterizzare l'APC usandolo attivamente nel circuito. Questa operazione risulta possibile tramite l'utilizzo di una scheda Arduino, in grado di collegare l'APC al computer; da quest'ultimo è possibile lanciare i programmi, scritti in codice Arduino, in grado di far lavorare nella maniera desiderata gli APC. Ogni placca può assumere un valore di voltaggio compreso tra 0 ed un valore massimo di ~ 140 V; questo voltaggio nei codici è espresso da un valore compreso tra 0 e 2048, che poi viene passato dall'Arduino all'APC tramite dodici collegamenti (infatti $2^{12} = 4096$, ma il range 0-4096 corrisponde a una rotazione di 4π, dunque di fatto una rotazione arriva fino a 2048), ognuno dei quali corrisponde ad una potenza del due: il valore è dunque trasferito tramite sistema binario tra i due dispositivi. Prima di esporre il principio base di funzionamento comune a tutti i codici, è bene presentare più in dettaglio il meccanismo di feedback su cui si basa il funzionamento dell'APC.

La quantità che viene costantemente monitorata ed eventualmente corretta dal dispositivo è la *fidelity* di un certo stato. Dati due stati ρ e σ, anche misti, la fidelity è definita nel modo seguente [6]

$$F(\rho, \sigma) = \left[\mathrm{Tr} \sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right]^2 \tag{3.3}$$

e ciò che misura è quanto due stati siano "vicini" l'un l'altro, ovvero misura la probabilità che, in un test con lo scopo di distinguere i due stati, uno stato venga scambiato per l'altro o viceversa, visto che la fidelity ha la proprietà di essere simmetrica; si capisce allora anche che $0 \leq F(\rho, \sigma) \leq 1$. La definizione diventa più comprensibile e più utile nel presente contesto se gli stati considerati sono stati puri, nel qual caso essa si riduce

al modulo quadro del prodotto tra gli stati:

$$F(\rho, \sigma) = |\langle \psi_\sigma | \psi_\rho \rangle|^2 \qquad \text{(per stati puri)} \tag{3.4}$$

Nel caso concreto si misura la fidelity tra lo stato nel sistema $|\psi\rangle$ e uno di quelli di riferimento inviati da Alice, ad esempio $|H\rangle$ (per gli altri tre stati di riferimento il discorso è analogo) e si vuole fare in modo che, tramite l'uso dell'APC, questa raggiunga e mantenga un valore maggiore del 99%, ovvero $0.99 \leq F(\psi, H) \leq 1.00$; tradotto in parole, ciò significa che lo stato $|\psi\rangle$ nel sistema verrà identificato effettivamente come stato $|H\rangle$ almeno il 99% delle volte, introducendo al più un errore dell'1% (noto) nelle misurazioni di Bob. La fidelity, infatti, è strettamente legata ad un parametro molto importante nella QKD, ovvero il *Quantum Bit Error Rate (QBER)* dalla formula $QBER = 1 - F$; il QBER misura il rapporto tra i bit sbagliati posseduti da Bob (dovuti a Eve o rumore esterno) e il numero totale di bit inviato da Alice.
I codici, dunque, dovranno far lavorare l'APC al fine di portare uno stato generico ad uno stato ψ, il cui valore della fidelity rispetto allo stato $|H\rangle$ sia soggetto a determinati vincoli (ad es. sia maggiore o uguale a 0.99). È chiaro che lo stato ψ non sarà unico: per chiarezza, prendendo la Fig. 1.1 e considerando $|0\rangle \equiv |H\rangle$, ψ potrà essere un qualunque stato risiedente sulla calotta sferica che ha come base la circonferenza generata dall'intersezione tra la sfera di Bloch e il piano z=0.99. Tramite l'APC è possibile raggiungere questo stato finale solo attraverso rotazioni intorno a due assi tra loro ortogonali sulla sfera di Bloch, come mostrato in Fig. 3.7, dunque data una certa placca ci si potrà muovere solo su una certa circonferenza contenente il punto iniziale. L'idea di base, che sta al cuore del funzionamento dei programmi, è una sorta di *random walk*:

i. Viene inizialmente misurata la F e si compie un passo in una certa direzione (nel senso di spostamento angolare) tanto più grande quanto più piccola è quest'ultima; lo spostamento sulla sfera di Bloch è ottenuto tramite la modificazione del voltaggio su una placca: più questo è grande, più sarà grande il passo.

ii. Se il valore della F aumenta, si compie un nuovo passo, sempre di grandezza inversamente proporzionale alla F, nella stessa direzione, altrimenti si compie un passo di ugual grandezza ma in direzione inversa.

iii. Si procede allo stesso modo finché si raggiunge un punto in cui procedendo in entrambe le direzioni la F diminuisce. Significa che, tra tutti i punti sulla circonferenza generata dall'intersezione della sfera di Bloch con il piano passante per il

punto iniziale e perpendicolare all'asse di rotazione, si è giunti su quello più vicino al polo dove giace lo stato di riferimento.

iv. Si passa alle placche successive e, per ciascuna di esse, si ripetono i punti (i)-(iii), eventualmente ricominciando dalla prima. La procedura termina non appena la F raggiunge un valore ≥ 0.99.

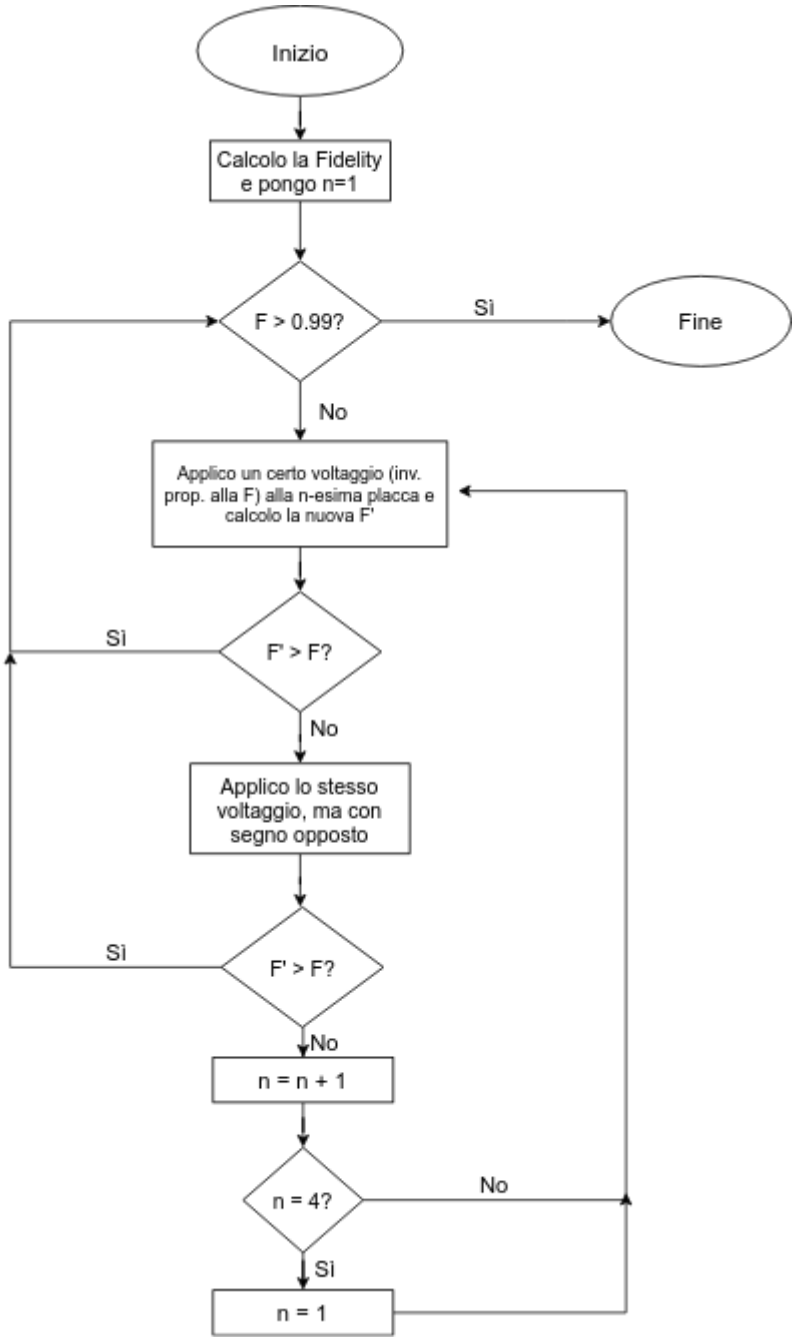


Figura 3.8: Schema a blocchi del principio di funzionamento del random walk implementato nei codici.

Avendo 12 bit di precisione, il minimo passo possibile corrisponde a $\Delta V = \frac{140V}{2^{12}} \approx 34.18$ mV, dunque la mappatura della sfera, per quanto gli stati possano essere densi, risulta

comunque discreta e non consta di un continuo di punti;

$$\frac{\Delta V}{2} = 17.09mV \tag{3.5}$$

corrisponde anche all'errore massimo sul voltaggio applicato alla placca, che si traduce direttamente all'errore sullo stato finale raggiunto. Queste due condizioni insieme concorrono all'impossibilità di raggiungere esattamente lo stato di riferimento. Una difficoltà che si è incontrata nella scrittura del codice è stata l'ottimizzazione del passo in funzione della F misurata: la scelta è stata fatta in modo empirico sulla base di diverse combinazioni provate; una scelta più oggettiva è sicuramente possibile, ma ciò sarebbe andato al di là del presente lavoro. Un'altra difficoltà, di tipo più tecnico, è stata riscontrata nel trasferimento dei dati dal powermeter alla scheda Arduino: questa procedura è avvenuta tramite collegamenti analogici che trasferiscono i dati sotto forma di voltaggio da 0 ad un massimo di 2 V; ogni powermeter, però, ha un range casuale diverso, che può differire da quello di riferimento di $\pm 0.3V$; è stato perciò necessario, durante la presa dati, fissare inizialmente tutti i range e tenerne conto nella scrittura del codice; inoltre potrebbe presentarsi il problema che, seppur non sia stata raggiunta la fidelity desiderata, a causa di questo spostamento nello zero del voltaggio, il programma legga un voltaggio superiore/inferiore a quello effettivo e arresti la procedura prima del dovuto. Infine, va precisato che il codice è stato scritto in modo da cercare di minimizzare la fidelity dello stato ortogonale a quello di riferimento e il motivo è facilmente intuibile: il minimo nella potenza è di certo zero, mentre la potenza massima, seppur in linea teorica sia costante, è sperimentalmente più difficile da misurare, dato che può subire oscillazioni dovute al laser stesso, o agli strumenti di misura, fluttuazioni termiche ecc.

L'apparato usato per la presa dati effettiva è rappresentato di seguito

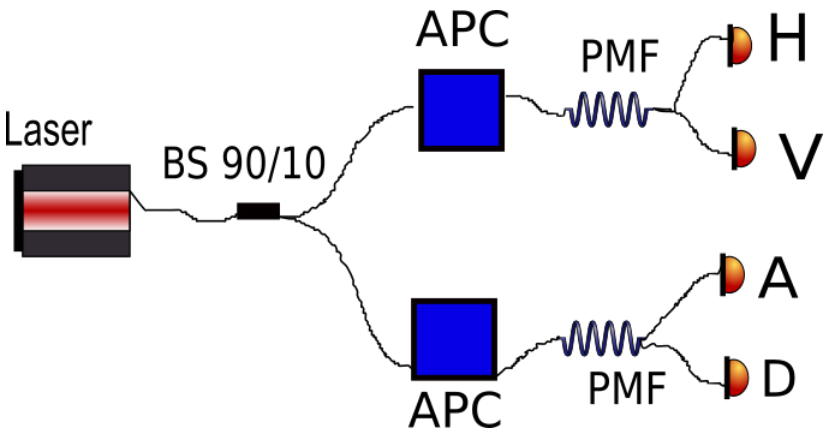


Figura 3.9: Schema per la presa dati usando due APC in parallelo

È stato usato un *beam splitter (BS)* per dividere la potenza in due canali diversi, in questo caso il 90% in uno e il restante 10% nell'altro, senza modificare lo stato di polarizzazione. Anche se nella Fig. 3.9 sono segnati i quattro stati di polarizzazione H,V,D e A, di fatto i due canali sono speculari; l'utilità nel fare ciò è duplice: si è verificato che entrambi gli APC potessero lavorare con basi diverse indipendentemente, ma allo stesso tempo che potessero lavorare in parallelo, non nel senso che lavorassero contemporaneamente, ma che potessero coesistere due APC nello stesso sistema (di fatto lavorava un APC e, successivamente, l'altro, alternandosi), prendendo contemporaneamente dati su due canali diversi, aventi potenze un ordine di grandezza diverso (fatto dovuto all'utilizzo di un BS 90/10). Nella parte finale del circuito si utilizzano ancora dei PBS implementati direttamente in fibra.

3.2.1 Background

Inizialmente è stato necessario misurare il segnale di fondo presente nell'apparato di misura in Fig. 3.9, ovviamente usando gli APC come semplici componenti passivi la cui unica funzione era quella di trasmettere il segnale. I quattro powermeter hanno registrato quattro segnali diversi, il più alto dei quali è riportato nel grafico seguente

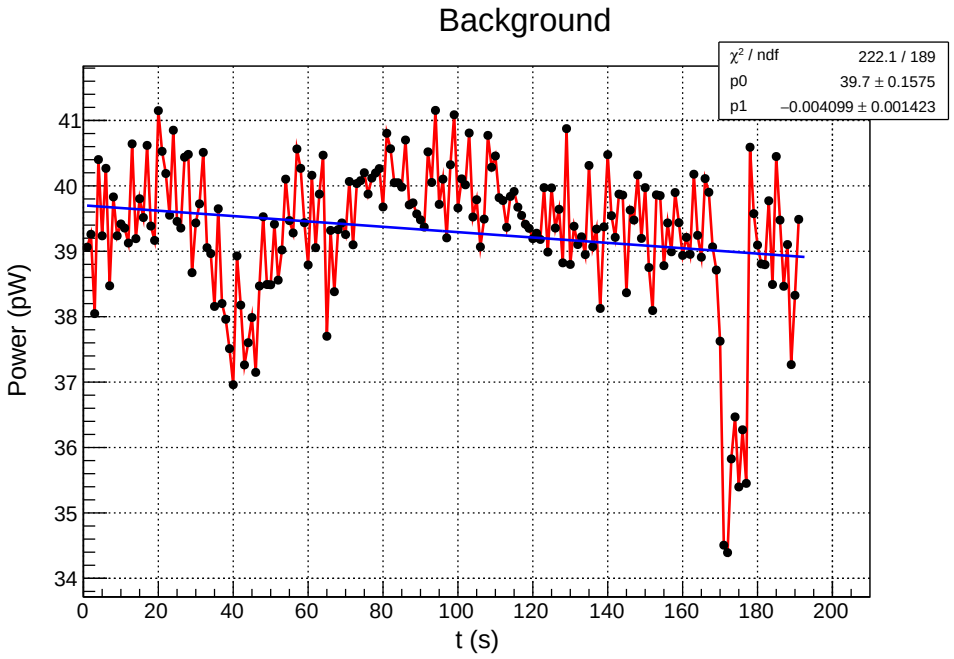
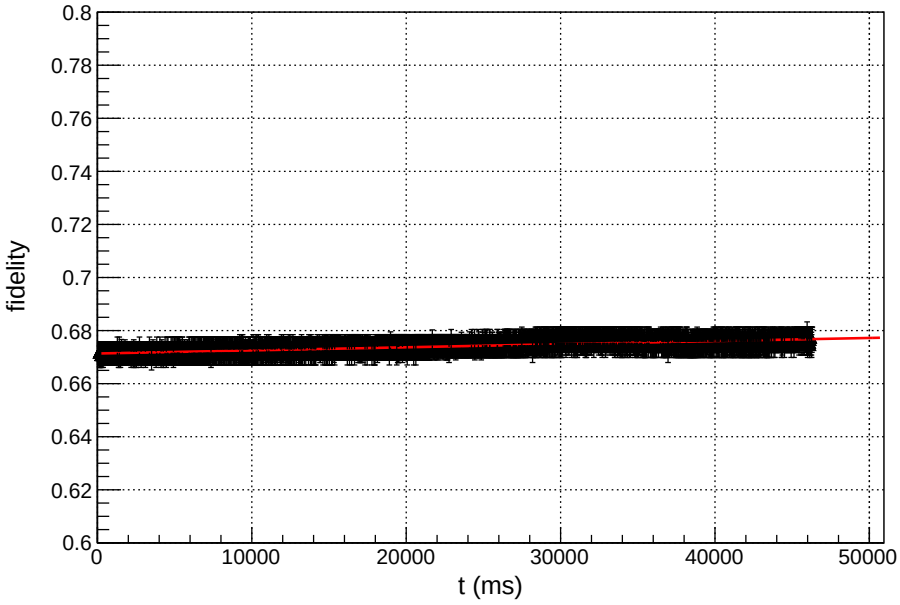


Figura 3.10: Misura del segnale di background e fit con una retta

A parte l'anomalia verso la fine del grafico, i dati sono disposti abbastanza casualmente attorno ad un valore di $\sim$ 39.5 pW; li si è interpolati, ottenendo una retta del tipo $Power(pW) = -0.004t(s) + 39.7$, dunque non completamente orizzontale - probabilmente dovuto al sopracitato picco- ma comunque abbastanza piatta. Inoltre il valore di qualche decina di pW è completamente trascurabile rispetto alle potenze in gioco; in ogni caso, per non correre rischi si è usato questo detector nel canale con più potenza, dove la minima potenza da raggiungere per la fidelity desiderata è $\sim 4.3\ \mu W$, dunque più di 100 volte superiore al valore di background.

3.2.2 Fluttuazioni

Sono stati presi dati sulle fluttuazioni della potenza in assenza degli APC, in modo da capire quanto cambi la potenza associata alle varie polarizzazioni se queste non sono controllate. Il grafico ottenuto della fidelity in funzione del tempo è il seguente



È doveroso fare subito alcune osservazioni in merito a questo grafico (che varranno poi anche per i successivi):

- la fidelity è qui intesa rispetto allo stato di riferimento $|V\rangle$, dunque, in formule, è semplicemente $F = \frac{P_V}{P_V+P_H}$;
- gli errori sulla fidelity sono stati ricavati a partire dall'errore sul voltaggio (3.5) e successivamente tramite propagazione; inizialmente si è trasformato l'errore massimo (3.5) in un errore casuale, considerandolo derivato da una distribuzione uniforme e poi trasformando l'errore sul voltaggio nell'errore sulla potenza

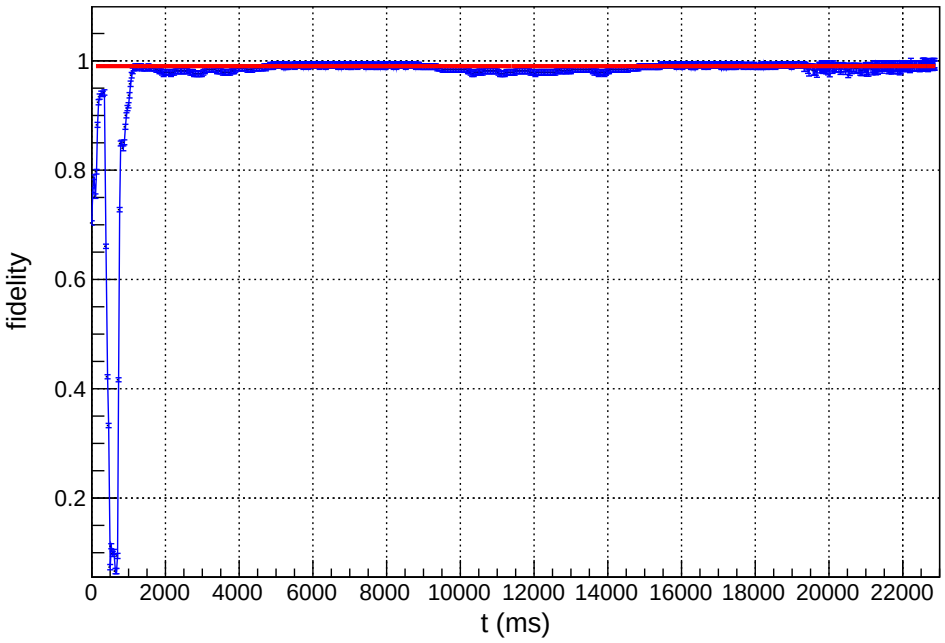
$$\sigma_V = \frac{\Delta V}{2\sqrt{3}} \approx 9.87 \text{ mV} \qquad \Longrightarrow \qquad \sigma_P = \sigma_V \frac{f.s.}{2} \tag{3.6}$$

  in cui f.s. denota il fondo scala usato nel powermeter, come già detto, tenuto fisso durante tutta la presa dati. L'errore sulla fidelity sarà poi

$$\sigma_F = \frac{F^2}{P_V}\sqrt{\sigma^2_{P_H} + \left(\frac{P_H}{P_V}\right)^2 \sigma^2_{P_V}} \tag{3.7}$$

In rosso è mostrata la retta del tipo $F = m * t(ms) + q$, risultante dal fit lineare dei dati; i parametri trovati sono $m = (117 \pm 6) \times 10^{-9}\ (ms)^{-1}$ e $q = 0.6714 \pm 0.0002$. Si nota dunque che, sebbene i valori della fidelity non presentino grandi fluttuazioni, cosa verificabile dalla precisione dei parametri (soprattutto q), vi sia un drift generale verso valori di F più grandi, visto che m assume un valore positivo non nullo.

Successivamente, si è verificato che l'APC funzionasse correttamente, lasciandolo lavorare per un tempo abbastanza lungo da poter controllare sia la funzione di correzione, sia quella di monitoraggio della fidelity. La situazione è la seguente



Anche qui in rosso è mostrata la retta che rappresenta il fit dei valori della fidelity dopo che si è raggiunta la fidelity desiderata (cioè dopo ~ 4.8 s). Si trova $m = (8 \pm 28) \times 10^{-9}$ $(ms)^{-1}$ e $q = 0.9902 \pm 0.0004$. Sebbene l'errore sull'intercetta in questo caso sia leggermente più grande (anche se si tratta di valori comunque molto precisi, dunque la differenza è praticamente trascurabile), la cosa importante è che il valore di m abbia compatibilità ottima col valore 0, dunque la retta possa a buon titolo essere considerata orizzontale. Ciò mostra come l'APC effettivamente tenga sotto controllo il valore di F, evitando tutti i drift dovuti alle cause già citate.

Nel grafico seguente, invece, si mettono più in luce eventuali fluttuazioni che possono occorrere finché l'APC è in funzione:

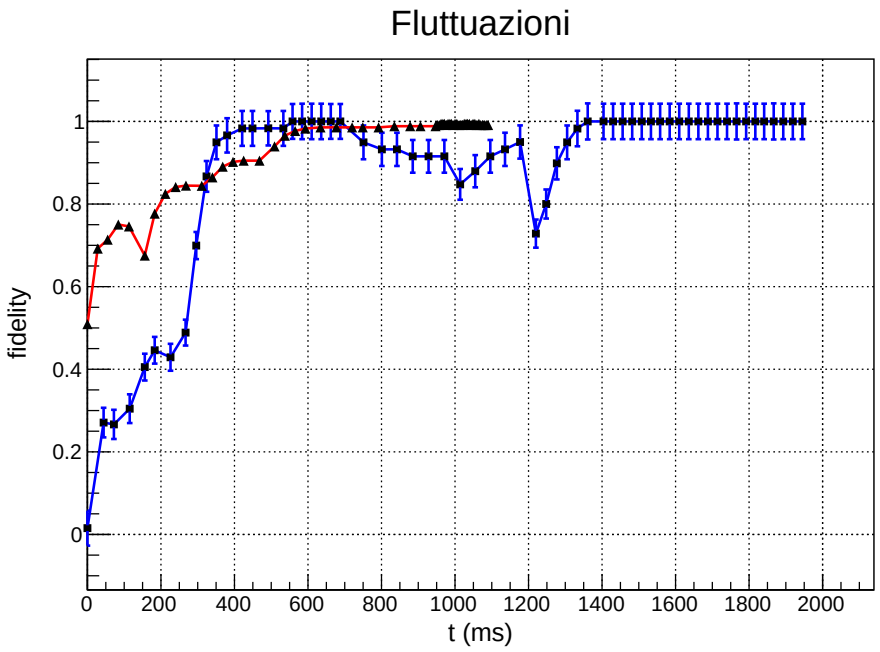


Figura 3.11: Grafico che mostra il lavoro di feedback operato dai due APC

Anche qui è necessario fare un paio di osservazioni:

- le due linee di colori diversi sono da riferirsi a due diversi APC, implementati contemporaneamente nel circuito, come in Fig. 3.9. L'APC blu inizialmente ha fidelity 0, infatti è stato fatto partire dallo stato $|H\rangle$ e poi portato alla fidelity desiderata; l'APC rosso, invece è partito da una fidelity di 0.5, dunque dallo stato $|D\rangle$ (o, equivalentemente, $|A\rangle$). Questa distinzione è stata realizzata per mostrare che da due stati iniziali diversi è, ovviamente, comunque possibile raggiungere lo stato desiderato;
- si nota come l'APC blu ci stia meno a raggiungere la fidelity rispetto a quello rosso (~ 0.6 s contro ~ 0.9 s); però nel ramo dell'APC blu, dopo un certo tempo intervengono degli effetti di disturbo, che possono essere termici o meccanici, che portano la fidelity ad un valore inferiore rispetto a quello desiderato: si vede allora come l'APC rientri in funzione e dopo un certo tempo riporti nuovamente il sistema nello stato appropriato.

3.2.3 Analisi dei tempi

A questo punto si è voluta studiare la velocità d'esecuzione degli APC. Inizialmente si è scritto un codice che permetteva di raggiungere una certa fidelity iniziale (sempre la stessa), per poi raggiungere la fidelity desiderata, il tutto ripetuto un certo numero di

volte. Sono stati raccolti dati per due fidelity iniziali caratteristiche: 0 e 0.5, che poi venivano portate a 1, ottenendo i seguenti risultati per i due tempi di lavoro

$$\begin{aligned} \text{F iniziale } 0 &\longrightarrow \bar{t} = 1255 \pm 75 \text{ ms} \qquad \sigma_t = 1125 \text{ ms} \\ \text{F iniziale } 0.5 &\longrightarrow \bar{t} = 437 \pm 26 \text{ ms} \qquad \sigma_t = 396 \text{ ms} \end{aligned} \tag{3.8}$$

In entrambi i casi i campioni presentano una dispersione molto grande (in rapporto alla media): questo effetto è da imputarsi al fatto che in tutti i casi la fidelity partiva dallo stesso valore, ma non l'APC; le placche stesse, infatti, inizialmente saranno sottoposte di volta in volta a voltaggi differenti, rendendo di fatto lo stato iniziale del sistema diverso di volta in volta. Nondimeno, i risultati sono comunque significativi perché forniscono un'indicazione sull'ordine di grandezza dei tempi in gioco (comunque inferiore ai due secondi, dunque molto piccoli) e fanno notare come il tempo medio impiegato per portare la fidelity da 0 a 1 sia più del doppio di quello impiegato partendo da 0.5. Appurato ciò, è stato implementato un altro codice che faceva in modo che, una volta che un APC avesse terminato un ciclo (ovvero una volta che la F avesse il giusto valore), questo smettesse di lavorare e ripartisse con un altro ciclo partendo però da una fidelity diversa; così facendo si può in un certo senso mappare la sfera di Bloch, cioè studiare il comportamento degli APC al variare del punto di partenza. Sono stati raccolti dati corrispondenti a 300 cicli per ogni APC. Alcuni esempi di questi cicli sono mostrati nella seguente figura

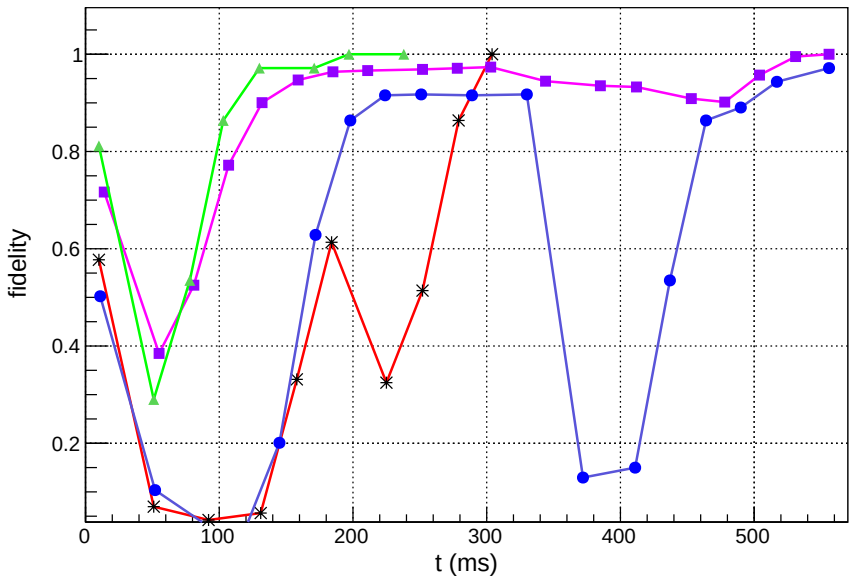


Figura 3.12: Grafico che mostra diversi cicli di lavoro operati dai due APC

Dal grafico emerge chiaramente la natura di "random walk" dell'algoritmo: certi cicli son più corti di altri e, in generale, i tempi sono molto diversi ma, in ogni caso, il percorso fatto prima di raggiungere la fidelity giusta è diverso da caso a caso. Si nota però anche un problema: in base a come è stato scritto il programma, la fidelity, una volta diminuita, non dovrebbe più diminuire ulteriormente; dal grafico, invece, si vede chiaramente che in alcuni cicli (ad esempio quello in rosso od in blu) essa diminuisce anche tre o quattro volte di seguito; ciò sta a significare che vi è un problema intrinseco nel codice stesso, oppure vi sono problemi dalla trasmissione dei dati dai powermeter all'Arduino o, ancora, gli APC non si comportano come inizialmente pensato.
Dopodiché, si è costruito un istogramma per vedere l'andamento generale dei tempi di lavoro per uno dei due APC e si è visto chiaramente come la dispersione dei dati sia enorme. Chiaramente in alcuni casi qualcosa non ha funzionato come dovuto e questi casi non sono utili per l'analisi dati. Si è dovuto trovare un modo oggettivo per scartare un determinato range di dati. Un criterio utilizzabile è allora quello di scartare tutti i dati che presentino dei bin nell'istogramma non più alti di un'unità, ovvero, si scartano tutti i cicli per cui il tempo di lavoro sia maggiore o uguale a 1350 ms. Anche se può sembrare una manipolazione troppo drastica non lo è, infatti i rimanenti dati costituiscono più del 77% di quelli originali, dunque il campione è ancora piuttosto corposo. È anche possibile, a questo punto, costruire un grafico che abbia in ascissa la fidelity del punto di partenza ed in ordinata il tempo di lavoro del ciclo, in modo da evidenziare eventuali correlazioni: sebbene si noti che i punti con fidelity iniziale maggiore di ~ 0.6 presentino tempi di lavoro anche inferiori ai 200 ms ed in generale minori di quelli con fidelity iniziale minore, non vi sono particolari correlazioni e i processi risultano in buona approssimazione casuali. Considerando questo caso è dunque possibile associare ai vari tempi una distribuzione normale, ricavando da essa una media ed una deviazione standard indicative del tempo di lavoro tipico del dispositivo. Si ottiene:

$$\bar{t} = 620 \pm 20 \text{ ms} \qquad \sigma_t = 360 \text{ ms} \tag{3.9}$$

L'errore sulla media è stato ricavato dalla formula usuale $\sigma_{\bar{t}} = \sigma_t/\sqrt{N}$, dove N è il numero di dati. La distribuzione anche qui presenta una varianza molto alta, ma il risultato (3.9) fornisce una buona stima dell'ordine di grandezza dei tempi in gioco.
L'analisi condotta finora è stata fatta su uno dei due APC, precisamente quello sul ramo con potenza più bassa (il 10 % del totale). L'analisi procede analogamente anche per

l'APC che lavora con potenze più alte, trovando

$$\bar{t} = 1500 \pm 80 \text{ ms} \qquad \sigma_t = 1300 \text{ ms} \tag{3.10}$$

In questo caso il tempo medio di lavoro risulta molto più alto che in precedenza e il campione risulta anche molto più disperso. Ciò può essere indice del fatto che, lavorando con potenze vicine al valore del fondo scala, il codice implementato perde efficacia, probabilmente a causa del sopracitato sfasamento casuale nel voltaggio. Si può allora concludere che la situazione migliore si ha per potenze lontane dal fondo scala, ma non eccessivamente, in quanto per potenze troppo piccole si perderebbe la precisione necessaria a misurarle. In questo senso $\sim 10\%$ del valore del fondo scala può essere considerato un valore ottimale.

3.3 WDM

Il *wavelenght division multiplexer (WDM)* è un apparecchio che permette la multiplazione (ovvero la combinazione di diversi segnali in ingresso sullo stesso collegamento fisico) e la demultiplazione (chiaramente, la separazione di tali segnali combinati) di segnali ottici trasmessi lungo una fibra a lunghezze d'onda (o, equivalentemente, frequenze) diverse. Può essere in un certo senso pensato come l'equivalente in fibra ottica di un prisma. Il filtraggio dei segnali avviene tramite l'utilizzo di interferometri di Fabry-Pérot, dispositivi costituiti da due specchi altamente riflettenti posti paralleli tra loro, che permettono il passaggio solo di una piccola frazione di frequenze attorno ad una frequenza di risonanza (il profilo è quello tipico di una Lorentzina). Questa tecnologia è utile nelle telecomunicazioni, ad esempio nella trasmissione di segnali telefonici, che in questo modo possono essere trasmessi contemporaneamente su una sola linea, invece di dover costruire una apposita fibra per ogni canale. Nel presente lavoro è utile nella prospettiva di una implementazione free-space, in cui l'atmosfera costituisce una gran fonte di rumore per il segnale e si vogliono dunque eliminare tutte le tracce spurie costituite da segnali a frequenza diversa da quella scelta per la trasmissione.
Il WDM usato in laboratorio aveva un ingresso e due uscite: l'ingresso accetta segnali costituiti da più lunghezze d'onda diverse, una delle uscite emette segnali a lunghezza d'onda di 1550 nm con una tolleranza di ± 10 GHz che, tradotta in lunghezza d'onda, costituisce l'intervallo 1549.92-1550.08 nm, l'altra uscita invece emette tutti i rimanenti segnali a diverse lunghezza d'onda; ovviamente tra i due si è interessati al primo output,

che sperimentalmente è facilmente individuabile, in quanto in esso si riversa la maggior parte della potenza.

Il problema principale di questi dispositivi è che sono molto inclini alla depolarizzazione, per cui è stato fondamentale verificare sin dal primo utilizzo che il dispositivo non introducesse tale effetto; per fare ciò si è inserito il dispositivo in un sistema semplice come quello in Fig. 3.4, tra il laser e l'MPC, ottenendo

P_H	P_V	rapporto
2.395 mW	330 ± 200 nW	$\sim$ 1 a 7300

Risultati per l'introduzione del WDM nel sistema

Fortunatamente, dunque, il WDM non introduce nel sistema alcun tipo di depolarizzazione.

Dopodiché, si procede analogamente a prima analizzando i tempi di lavoro, anche qui senza evidenziare particolari correlazioni; la distribuzione dei dati, però, presenta ancora una dispersione molto alta ed è dunque necessaria una selezione degli stessi. Si sono tenuti i cicli con t<2000 ms, in quanto oltre questo valore la distribuzione presenta solo dati sporadici; un altro motivo per scegliere questo intervallo consiste nel fatto che i rimanenti dati costituiscono $\sim 91\%$ del campione iniziale, quindi, se considerassimo la distribuzione gaussiana, questi corrisponderebbero a circa 2σ. I risultati sono i seguenti

$$\bar{t} = 550 \pm 30 \text{ ms} \qquad \sigma_t = 440 \text{ ms} \tag{3.11}$$

Risultati molto simili al caso in cui il WDM non era presente nel circuito, anzi addirittura il tempo medio risulta inferiore, probabilmente perché ai detector arriva un segnale più pulito (meno rumoroso) proprio a causa del filtraggio operato dal WDM.

Per il ramo a potenza più alta si ottiene invece

$$\bar{t} = 1440 \pm 60 \text{ ms} \qquad \sigma_t = 960 \text{ ms} \tag{3.12}$$

Risultati anche in questo caso inferiori al caso senza WDM, ma come prima molto superiori al caso con potenza più bassa; le stesse considerazioni fatte prima a proposito di questa discrepanza valgono anche qui.

3.4 Conclusioni

Nel corso del seguente lavoro di tesi è stata trattata, in maniera abbastanza generale, la parte della Comunicazione Quantistica riguardante la distribuzione di chiavi, ovvero la QKD, in luce di applicazioni nella crittografia; è stato studiato in modo particolare il protocollo BB84, base teorica su cui si è basata poi tutta la parte sperimentale. Durante quest'ultima, inizialmente si è presa confidenza con le fibre, imparando sia come maneggiarle, sia il loro principio di funzionamento; andando avanti si è presa confidenza con una serie di strumenti ottici, utilizzati poi nell'apparato sperimentale: BS, PBS (sia in fibra che in free space), lamine, APC e WDM. Una volta studiati questi componenti costituenti il ricevitore in fibra, si è verificato che i più importanti -fibre PMF, lamine, WDM e APC- non introducessero depolarizzazione nel circuito; ciò risulta vero perché nel circuito è sempre possibile creare stati molto vicini a $|H\rangle$ e a $|V\rangle$, che costituiscono gli stati base ortonormali nel protocollo BB84. A tal proposito, utilizzando lamine e PBS, si è costruito anche un apparato in grado di ricevere stati con polarizzazione diagonale e circolare. Successivamente, si è verificato che gli APC mantenessero la polarizzazione stabile e si sono raccolti dati per capire quanto tempo impiegassero gli APC a correggere lo stato; si è trovato che questi strumenti sono abbastanza veloci, impiegandoci in media $\lesssim 1.5$ s e trovando che essi lavorano meglio quando la potenza totale presente nel circuito (o nel ramo del circuito se si usa un BS) è $\sim 10\%$ del valore del fondo scala del detector; inoltre gli APC lavorano più velocemente se nel circuito è presente un WDM, capace di filtrare il segnale in uscita dal laser attenuando il rumore presente nell'apparato. Sebbene i codici implementati funzionino ed i risultati siano comunque soddisfacenti, è stato però notato che qualcosa non ha funzionato come ci si aspettava nel processo che porta da un certo stato presente nel circuito a quello di riferimento. Il problema, come già detto, potrebbe risiedere in varie cause; se risolto potrebbe portare a tempi di lavoro degli APC ancora minori, dunque ad una più alta efficienza del sistema ricevente.

Bibliografia

[1] Benenti G., Casati G., Strini G., *Principles of Quantum Computation and Information Volume I: Basic Concepts*, Singapore, World Scientific, 2004.

[2] Vedovato F., Quantum Optics Experiments in Space, PhD Thesis, University of Padova (2018).

[3] https://en.wikipedia.org/wiki/Jones_calculus

[4] Scarani V., Bechmann-Pasquinucci H., Cerf J. N., Dusek M., Lütkenhaus N., Peev M., 2009, Rewiews of Modern Physics 81, 290909.

[5] Gisin N., Ribordy G., Tittel W., Zbinden H., 2002, Rewiews of Modern Physics 74, 080302.

[6] https://en.wikipedia.org/wiki/Fidelity_of_quantum_states