Università degli Studi di Padova

Dipartimento di Fisica "G. Galilei"
Corso di laurea in Fisica

Dipartimento di Ingegneria dell'Informazione.

Realizzazione di un canale per QKD basato sul protocollo PBC00

Laureando:
Andrea Grimaldi

Relatore:
Paolo Villoresi

Correlatore
Giuseppe Vallone

Anno Accademico 2014-2015

A Claudia
che continua a sopportarmi.

Sommario

L'obbiettivo di questa tesi è la realizzazione di un sistema ottico per la condivisione di chiavi tramite il Protocollo **PBC00**. In questa tesi presenterò la caratterizzazione di una sorgente di fotoni Entangled basata sullo schema di Kim, Fiorentino e Wong e la progettazione dello schema ottico degli apparati di misura.

Indice

1

Introduzione

La Crittografia studia la progettazione di sistemi di comunicazione sicura che permettano di proteggere le informazioni sensibili da intercettazioni indesiderate. La sua nascita ha motivi principalmente militari in quanto nascondere o meno le informazioni strategiche al nemico è sempre andato di pari passo con il vincere o meno le battaglie, basti pensare al Cifrario di Cesare in cui si scambiavano le lettere delle parole o al metodo degli spartani in cui si arrotolava il messaggio intorno ad un bastone in modo da far comparire il messaggio.

Il primo approccio matematico al problema viene dato in epoca contemporanea da Vernam che nel 1926 pubblica un articolo in cui illustra l'algoritmo *One Time Pad*. Questo algoritmo utilizza una chiave crittografica, cioé un lista segreta di simboli, per codificare il messaggio, lunga quanto il messaggio stesso e non riutilizzabile. Questo metodo diviene famoso quando, un po' di anni dopo, Shannon non solo ne dimostra la sicurezza incondizionata ma verifica anche che l'algoritmo è ottimizzato, nel senso che utilizza la chiave più piccola possibile. [9]

Se da una parte il problema dell'algoritmo di criptazione viene così risolto dall'altra se ne crea uno molto più grande: come condividere delle chiavi così lunghe in modo completatamene segreto. Negli anni sono stato pubblicati vari protocolli che però non possono garantire una sicurezza incondizionata, a causa dell'impossibilità di individuare un infiltrato in un canale che sfrutta solo protocolli classici per condividere informazioni.

La Meccanica Quantistica invece fornisce gli strumenti necessari per garantire la riservatezza della chiave utilizzando il postulato di misura e il principio di indeterminazione di Heisenberg che permettono di individuare eventuali infiltrati.

2

Protocolli QKD

L'obbiettivo dei protocolli di *Key Distibution* è permettere a due parti, indicate per tradizione come Alice e Bob, di condividere una sequenza casuale di caratteri, chiamata *chiave*, senza che un possibile infiltrato nella comunicazione, chiamato Eva, riesca ad ottenere informazione a riguardo. Questa condivisione avviene tramite un sistema fisico e l'informazione viene codificata negli stati che possono descriverlo.

La totalità delle comunicazioni attuali sfruttano sistemi non quantistici per condividere informazioni e l'estrarre informazioni da un mezzo di questo tipo può non essere individuabile, negando la possibilità di avere protocolli di **KD** classici che siano incondizionatamente sicuri. Ad esempio nella radiocomunicazione il sistema fisico utilizzato sono le onde elettromagnetiche in cui le informazioni vengono codificate tramite la modulazione del segnale. In questo caso è impossibile individuare se qualcuno è in ascolto sulla frequenza che si sta utilizzando.

Nella meccanica quantistica si ha che l'interazione del sistema con un osservatore non può mai essere trascurata: il postulato della misura indica come l'atto di misura sia un processo irreversibile e probabilistico, di cui si può prevedere solo la probabilità di ottenere un determinato risultato. Inoltre il teorema di non-clonazione garantisce che un generico stato non possa essere clonato. In una comunicazione quantistica si ha quindi che da una parte non si può interagire con il canale senza rendere possibile la propria individuazione, dall'altra non si può clonare il segnale per agire indisturbati su una copia di esso. Su questi due fatti si basa la *Quantum Key Distribution* che permette di sviluppare dei protocolli incondizionatamente sicuri.

2.1 Canali

Ogni schema di **QKD** si basa sull'utilizzo di due canali:

- Un canale quantistico in cui viene condivisa la chiave, tramite qubit;
- Uno classico autenticato, in cui Alice e Bob si scambiano informazioni relative al protocollo.

Le informazioni condivise sul primo canale possono essere intercettate e modificate nel rispetto dei postulati della meccanica quantistica, mentre nel secondo canale avviene una comunicazione pubblica, in cui si ha garanzia dell'integrità dei messaggi e certezza del mittente. Entrambi i canali sono necessari: tramite il canale quantistico si possono condividere informazioni in maniera sicura però serve il canale classico per estrarle.

2.2 Alice e Bob

Generalmente ogni protocollo distingue due parti, Alice e Bob, con due ruoli ben distinti e caratterizzati.

Il ruolo di Alice è di creazione e codifica della chiave: il suo compito è creare una sequenza casuale di simboli e, rispettando delle regole prestabilite, preparare degli stati da inviare a Bob. Ogni protocollo deve infatti definire l'alfabeto, cioè una relazione biunivoca tra l'insieme dei simboli $\{s_i\}_{i=1,\cdots,n}$ che compongono la chiave S_n e un insieme di stati $\{|\psi_i\rangle\}_{i=1,\cdots,n}$, in modo tale che

$$|\Psi(S_n)\rangle := \bigotimes_{j=1}^{n} |\psi_j\rangle$$

rappresenti l'intera chiave.

Gli stati utilizzati possono appartenere ad uno spazio di Hilbert $\mathscr{H}$ di dimensione finita o infinita. In entrambi i casi è necessario che siano non ortogonali tra loro, così da rendere più difficile per Eva estrarre informazioni dal sistema senza perturbarlo.

Definito l'alfabeto, Alice ha due modi per codificare la chiave:

Prepare & Measure (P&M) in cui Alice prepara lo stato $|\Psi(s_i)\rangle$ corrispondente al carattere s_i della chiave e lo invia a Bob il quale lo misura;

Entanglement Based (EB) in cui Alice prepara un insieme di stati entangled del tipo:

$$|\phi\rangle = \frac{1}{\sqrt{d_n}} \sum_{S_n} |S_n\rangle_A \otimes |\Psi(S_n)\rangle_B,$$

dove d_n è il numero di possibili stringhe S_n, e i $|S_n\rangle$ sono una base ortonormale dello spazio. Successivamente invia il sottosistema "B" a Bob e misurando il sottostato nelle sue basi $|S_n\rangle_A$ prepara nel sottosistema di Bob lo stato $|\Psi(S_n)\rangle$. Dal punto di vista di Bob il protocollo è uguale al precedente.

Questa distinzione è puramente pratica, poiché, dal punto di vista teorico, dimostrare la sicurezza incondizionata per un protocollo basato sul primo metodo di codifica è equivalente a dimostrarla per lo stesso protocollo basato sul secondo.

Nel caso trattato in questa tesi si è utilizzato il metodo **EB**, poiché sperimentalmente più facile da realizzare e da mantenere stabile.

Il compito di Bob è decodificare il segnale di Alice utilizzando un appropriato sistema di **POVM**[1] legato agli alfabeti usati da Alice.

2.3 Chiave

Dopo che Alice ha inviato la chiave di lunghezza N, Bob decide insieme a lei una primo filtraggio degli eventi individuando quelli inconcludenti, cioè quelli per cui è stato impossibile discriminare lo stato ricevuto. Questa fase viene detta di *sifting*.

A questo punto Alice e Bob hanno due versioni della stessa stringa, chiamata *Raw Key*, composte da $n \leqslant N$ caratteri che non sono ancora né private né totalmente correlate. Da queste si procedere ad una post-analisi che permette di estrarre una *Secure Key* di lunghezza $l \leqslant n$.

In questi termini un parametro utile per confrontare vari protocolli è il *rate*, cioè il numero di simboli per unità di tempo prodotti.

[1] Positive Operator Valued Measurement

2.3.1 Raw Key rate

Una prima quantità indicativa dell'efficienza del protocollo è il *rate* della Raw Key R, che può essere espresso come:

$$R = \nu_S \cdot P_{sif} \tag{2.1}$$

Il primo termine ν_S indica il *rate* di fotoni emessi dalla sorgente che arrivano a Bob e dipende esclusivamente dall'apparato. In particolare, nel caso studiato in questa tesi, in cui viene utilizzata una sorgente laser in emissione continua, si ha che:

$$\nu_S^{cw} = \min\left(\eta_A t_A \mu, \quad \frac{1}{\tau_d^A}, \quad \frac{1}{t \cdot \eta_B t_B \tau_d^B}, \quad \frac{1}{\Delta t}\right) \tag{2.2}$$

dove η_i e τ_d^i sono rispettivamente l'efficienza e il tempo morto del rivelatore i-esimo; t_A, t_B e t sono la trasmissività dall'apparato di Alice e Bob e del canale quantistico che li collega, Δt è la finestra delle coincidenze e infine μ è il rate della sorgente. Il secondo termine, cioé la probabilità che Bob accetti un evento come buono, deriva principalmente dal termine di *sifting* tipico del protocollo e per questo verrà trattato in maniera più approfondita nel Capitolo 3.

2.3.2 Secure Key rate

Il secondo parametro interessante è il rate della Secure Key, cioé la velocità con cui si produce il risultato finale del protocollo. Si è preferito studiare il caso limite di chiave infinita, definendo la *Secret Fraction* come:

$$s = \lim_{N\to\infty} \frac{l}{N}. \tag{2.3}$$

Si può dimostrare che tale parametro sia pari all'informazione totale della Secure Key, ed è quindi stimabile in via teorica.

Ottenuta una Raw Key è necessaria, come già spiegato, una post-elaborazione classica del segnale al fine di migliorare da una parte la coerenza della stringa e dall'altra aumentarne la segretezza. Durante la prima fase, Alice e Bob utilizzano parte delle Raw Key al fine di correggere eventuali errori ottenendo una frazione della chiave originale perfettamente correlata, che ha come limite superiore l'informazione mutua tra Alice e Bob:

$$s_{ec} = I(A:B) = H(A) + H(B) - H(AB) = H(A) - H(A|B) \tag{2.4}$$

Nella seconda fase si ha la Privacy Amplification, in cui si aumenta la segretezza della chiave, distruggendo le informazioni che Eva ha a riguardo della chiave. In questo modo la frazione di chiave rimanente viene ridotta ancora ottenendo la Secure Fraction:

$$s = I(A:B) - \min_{Eva}\{I_{EA}, I_{EB}\} \tag{2.5}$$

dove I_{EA} è l'informazione che Eva ha a riguardo della chiave di Alice. In questo modo si ottiene il rate della Secure Key $K \leqslant R$ dato da:

$$K = R \cdot \left(I(A:B) - \left(\min_{Eva}\{I_{EA}, I_{EB}\}\right)\right). \tag{2.6}$$

2.3.3 Stima del rate della Secure Key

Al fine di stimare numericamente il rate della Secure Key si studiano i termini di Correzione degli Errori e di Amplificazione della Privacy, partendo direttamente dalla Raw Key. In generale inviare un singolo stato per evento può essere difficile: nel caso trattato in questa tesi ad esempio si usano fotoni prodotti con una statistica poissoniana

e si ha una probabilità non nulla di avere eventi a 0 fotoni o a 2. Per stimare i parametri è quindi necessario precedere per via statistica.

Per concretezza, consideriamo un ciclo di distribuzione fotonica di chiave, con un rate totale R scomposto nei rate R_j dati dagli eventi a j-fotoni e il numero di errori R_j^w sul singolo tipo di evento. In questo modo si identificano i seguenti parametri:

- $Y_j = \frac{R_j}{R}$ che indica quanto sono stati importanti gli eventi a j-fotoni nella distribuzione totale;
- $\epsilon_j = \frac{R_j^w}{R_j}$ che indica il rapporto tra gli errori e gli eventi a j-fotoni associati.

Questi due valori possono essere anche riletti rispettivamente come la probabilità di avere un evento a j-fotoni e l'errore percentuale su di esso. In questa ottica si può definire un importante parametro, il **QBER**:

$$Q = \sum_{j=1}^{\infty} Y_j \epsilon_j \tag{2.7}$$

che è equivalente alla media dell'Error Rate totale. Questo valore è facilmente stimabile facendo un confronto tra le due versioni della Raw Key, sacrificando una parte di essa.

Considerando l'eq. 2.6, nei casi studiati si ha che $H(A) = H(B) = 1$ e che $H(A|B) = H(B|A) = h(Q)$, dove h è l'entropia binaria e si ha quindi che il Secure Key rate è dato da:

$$K = R \cdot (1 - h(Q) - I_E)\,. \tag{2.8}$$

dove $I_E = \min_{Eva}\{I_{EA}, I_{EB}\}$

È importante distinguere due tipi di errori: gli errori di bit e gli errori di fase. Il primo tipo di errore è dato dal semplice scambio tra due simboli ed è quello che viene stimato dal **QBER**. Il secondo tipo è dato invece da una variazione di fase dello stato inviato da Alice ed è più difficile stimarlo con una misura diretta.

Questa distinzione degli errori è utile poiché, come dimostrato da Gottesman et al.[4], la massima informazione che Eva può ottenere nel protocollo è data da $h\left(e_{phase}\right)$ ed in molti casi si riesce a stimarne un limite superiore.[4]

Da questa analisi si ottiene che il rate massimo per la Secure Key è dato da:

$$K = R \cdot \left(1 - h(e_{bit}) - h(e_{phase})\right)\,. \tag{2.9}$$

Da questa equazione possiamo notare come i protocolli **QKD** non sono assolutamente sicuri: nel caso in cui gli errori rivelati nella realizzazione del protocollo sono tali per cui il rate K è negativo si ha che la chiave condivisa non è sicura e quindi bisogna abbandonare il protocollo e ricominciare dall'inizio.

3

PBC00: a metà tra il BB84 e il B92.

Il protocollo che si cerca di realizzare dal punto di vista sperimentale è il **PBC00**. Questo protocollo vuole porsi come via di mezzo tra due protocolli noti, il **BB84** e il **B92**, cercando di unire i vantaggi ed attenuare le problematiche.

3.1 BB84

Il primo protocollo di **QKD** creato fu il BB84 di Bennett e Brassard. In questo protocollo vengono usati due alfabeti composti da due differenti basi ortogonali di un sistema bidimensionale: $\{|0\rangle, |1\rangle\}$ e $\{|+\rangle, |-\rangle\}$ dove $|\pm\rangle = |0\rangle \pm |1\rangle$. Lo schema è il seguente:

Creazione della Chiave Alice prepara due stringhe binarie lunghe n composte da due sequenze casuali di 0 e 1 indicate con $S^{(a)}$ e $D^{(a)}$;

Codifica Successivamente prepara gli stati utilizzando il primo alfabeto se $D_i^{(a)}$ è 0, e l'altro se è uguale a 1 codificando di conseguenza il bit $S_i^{(a)} = 0$ con lo stato $|0\rangle$ o $|+\rangle$ e il bit $S_i^{(a)} = 1$ con lo stato $|1\rangle$ o $|-\rangle$;

Lettura Bob prepara una stringa binaria lunga n composta da una sequenza casuale di 0 e 1 indicata con $D^{(b)}$. Se il valore dell' i-esimo elemento è 0 misura utilizzando il primo alfabeto, se è 1 il secondo.

Sifting Alice e Bob comunicano pubblicamente le stringhe D e scartano gli eventi in cui le stringhe non coincidono;

Post elaborazione Alice sceglie in maniera casuale metà della sua chiave e la confronta con Bob tramite il canale pubblico. Se le due chiavi differiscono troppo si abbandona il protocollo;

EC & PA Se si procede con il protocollo Alice e Bob eseguono gli algoritmi di correzione degli errori e Privacy Amplification;

3.2 B92

Il protocollo B92, pubblicato da Bennett in un suo articolo del 1992, è a singolo alfabeto binario, in cui vengono utilizzati due stati non ortogonali per condividere la chiave.[2]

Chiameremo i due stati $|u_0\rangle$ e $|u_1\rangle$ e i proiettori con cui verranno misurati gli stati $P_0 = |\bar{u}_1\rangle\langle\bar{u}_1|$ [1] e $P_1 = |\bar{u}_0\rangle\langle\bar{u}_0|$, questi ultimi accoppiati con i loro rispettivi complementari $\bar{P}_i$ tali che $\bar{P}_i = 1 - P_i$.

[1] Dove $|\bar{u}\rangle$ è l'ortogonale di $|u\rangle$.

Definito l'alfabeto usato si procede con la distribuzione della chiave, dove per concretezza useremo $|0\rangle$ come stato $|u_0\rangle$ e $|+\rangle$ come $|u_1\rangle$, il protocollo seguirà il seguente schema:

Creazione della Chiave Alice prepara una stringa binaria lunga n composta da una sequenza casuale di 0 e 1 indicata con $S^{(a)}$;

Codifica Successivamente prepara uno stato $|0\rangle$ se l'i-esimo valore della stringa è 0 e $|+\rangle$ se invece è 1;

Lettura Bob prepara una stringa binaria lunga n composta da una sequenza casuale di 0 e 1 indicata con $S^{(b)}$. Se il valore dell' i-esimo elemento è 0 usa il proiettore P_0 nell'altro caso usa P_1. Si segna tutti gli eventi concludenti, cioè in cui ha individuato lo stato inviato da Alice;

Sifting Bob comunica pubblicamente gli stati inconcludenti e insieme ad Alice li scarta;

Post elaborazione Alice sceglie in maniera casuale metà della sua chiave e la confronta con Bob tramite il canale pubblico. Se le due chiavi differiscono troppo si abbandona il protocollo;

EC & PA Se si procede con il protocollo Alice e Bob eseguono gli algoritmi di correzione degli errori e amplificazione della Privacy;

3.3 PBC00

Come già anticipato nell'introduzione il protocollo **PBC00** viene proposto dai suoi autori Phoenix, Barnett e Chefles con l'idea di trovare una via di mezzo tra il protocollo **B92** e il **BB84**. Entrambi i protocolli infatti hanno vantaggi specifici non indifferenti: il **B92** ha un costo sperimentale ridotto in quanto utilizza solo due stati per la distribuzione della chiave e richiede quindi una apparecchiatura relativamente semplice, mentre **BB84** è stato ottimizzato nel tempo raggiungendo ottimi risultati sia dal punto di vista dell'efficienza che da quello della sicurezza. In entrambi i casi però si hanno degli svantaggi: il primo ha dei problemi nella sicurezza legati al rumore del canale, il secondo invece, utilizzando 4 stati, ha un costo operativo molto alto.

Con il **PBC00** si utilizzano 3 stati, uno in meno del **BB84**, si riesce a garantire una sicurezza incondizionata indipendentemente dalle condizioni del canale, a differenza del **B92**. Se si considera l'implementazione data dal protocollo **R04**[2] si ottiene anche che il protocollo è non-sacrificale, nel senso che non serve comunicare pubblicamente parte della chiave per stimare l'error rate.

3.3.1 Descrizione

Il PBC00 si basa sull'utilizzo di tre stati distinti non ortogonali appartenenti ad uno spazio di Hilbert di dimensione 2. Chiameremo i tre stati $|A\rangle$, $|B\rangle$, $|C\rangle$ e indicheremo con $\hat{P}_k$ il proiettore sullo stato $|k\rangle$ e $\hat{P}_{\bar{k}}$ il suo complementare tale che $\hat{P}_k + \hat{P}_{\bar{k}} = 1$. Si richiede inoltre che siano dati da una rotazione di $\frac{2}{3}\pi$ nello spazio di Hilbert dei qubit in modo che presi due stati $|k_1\rangle$ e $|k_2\rangle$ si ha che $\langle k_1|k_2\rangle = \frac{1}{2}$.

Creazione della Chiave Alice prepara una stringa ternaria r^a in maniera completamente casuale e una stringa binaria b della stessa lunghezza;

Codifica Alice codifica la stringa b utilizzando la seguente tabella:

[2] Vedi articolo [8].

Bit	Stati Quantistici		
Classico	Alfabeto 1	Alfabeto 2	Alfabeto 3
0	$\|A\rangle$	$\|B\rangle$	$\|C\rangle$
1	$\|B\rangle$	$\|C\rangle$	$\|A\rangle$

ed invia i segnali a Bob;

Lettura Bob prepara una stringa ternaria r^b in maniera casule, e in rapporto ad essa misura gli stati che Alice gli ha inviato:

- se $r_i^b = 1$ misurerà $|\bar{A}\rangle$
- se $r_i^b = 2$ misurerà $|\bar{B}\rangle$
- se $r_i^b = 3$ misurerà $|\bar{C}\rangle$

Se utilizza il proiettore complementare a quello dello stato inviato non legge nulla e scarta l'evento

Sifting Quando Bob finisce di leggere tutti gli stati lo comunica ad Alice indicando quali eventi ha letto. Alice dichiara quindi pubblicamente il dizionario utilizzato. Se Bob ha utilizzato il proiettore giusto si ha un evento concludente, in caso contrario Bob comunica ad Alice di scartare l'evento. Ad esempio: Alice invia $|A\rangle$, Bob misura $|\bar{B}\rangle$ e Alice comunica che quel bit utilizzava l'Alfabeto 3. In questo caso Bob non sa dire se il bit era 0 o 1. Se invece Alice avesse utilizzato l'alfabeto 1 allora Bob saprebbe che lo stato inviato non era $|B\rangle$ e quindi decodificherebbe 0.

Post Elaborazione Alice sceglie a caso una parte delle chiave, la comunica a Bob e insieme stimano i vari parametri.

EC & PA Alice e Bob procedono nella correzione degli errori e della Amplificazione della Privacy.

3.3.2 Rate della Secure Key

Il Rate della Secure Key è stato stimato da Boileau et al. come:

$$K = \frac{1}{2 - e_{bit}} \left(1 - h\left(e_{bit}\right) - h\left(\frac{5}{4} e_{bit}\right)\right) \tag{3.1}$$

dove il e_{bit} è la stima del errore di bit mentre $\frac{5}{4} e_{bit}$ è la stima del massimo errore di fase.[3]

4

Realizzazione della condivisione di una chiave tramite PBC00

4.1 Strumenti di comunicazione

Fino ad adesso si è discusso di **QKD** in maniera strettamente teorica. Un altro aspetto molto importante è la realizzazione effettiva del protocollo in cui gli stati sono legati ad un mezzo.

Il canale fisico più utilizzato è la luce. Da una parte è banalmente il mezzo più veloce con cui condividere informazioni, dall'altra lo stato dell'arte nelle scienze ottiche fornisce un ampio strumentario teorico e pratico.

La scelta del grado di libertà in cui codificare lo stato può essere molteplice come la frequenza, la fase o la polarizzazione. Nel caso trattato si è scelta quest'ultima.

4.1.1 Polarizzazione

Al fine di poter codificare la chiave nello stato dei fotoni bisogna scegliere quale grado di libertà utilizzare. Per protocolli di questo tipo la scelta naturale è la polarizzazione poiché, anche qui, lo stato della tecnologia esistente fornisce ottimi strumenti per controllare questa proprietà della luce.

La polarizzazione di un fotone è la direzione rispetto a cui il campo elettrico oscilla, si distinguono due tipi di polarizzazione: quella ellittica e quella lineare. Esistono vari modi per rappresentare la polarizzazione ma tutti discendono dal fatto che si può rappresentare l'onda in formalismo esponenziale:

$$\mathbf{E} = \mathrm{Re}\left((a_x \hat{x} + a_y \hat{y})\, e^{i\omega t} \right) \tag{4.1}$$

dove a_x e a_y sono in generale due numeri complessi. Se questi due valori sono reali puri si ha che le due componenti, quella parallela all'asse $\hat{x}$ e quella parallela all'asse $\hat{y}$, sono una più grande dell'altra e questo comporta solo che la polarizzazione totale è inclinata. Se invece si ha una componente immaginaria questa può essere scritta come $a_x = |a_x| \cdot \exp(i\varphi_x)$ e se si ha che $\varphi_x \neq \varphi_y$, dove φ_y è l'argomento di y, le due componenti dell'onda risultano sfasate e si ha la polarizzazione ellittica. Lavorando quindi in uno spazio $\mathbb{C}^2$ si possono rappresentare tutte le polarizzazioni utilizzando un formalismo vettoriale noto, in cui ad esempio, considerando come basi $|H\rangle$ e $|V\rangle$, un'onda polarizzata circolarmente viene rappresentata da $|\circlearrowleft\rangle = \frac{1}{\sqrt{2}} (|H\rangle + i\,|V\rangle)$.

4.2 Sorgente di Fotoni entangled

Come già preannunciato lo scopo dell'esperimento trattato in questa tesi è realizzare il protocollo PBC00 basandolo sullo schema **EB**. Per ottenere fotoni entangled si è usato lo schema descritto da Kim, Fiorentino e Wong [5].

Nel caso studiato il laser di pompa di frequenza $404.50(26)\,\mathrm{nm}$[1] è stato accoppiato in una fibra *PMSM*[2], che mantiene la polarizzazione lineare dei fotoni generati.

In uscita dalla fibra è stata posto in ordine: un *PBS*[3] utilizzato come filtro in polarizzazione lineare, una lamina *HWP*[4] per controllarne la direzione e una lamina *QWP*[5] per controllare la fase tra le componenti $|V\rangle$ e $|H\rangle$ dello stato. Il tutto è stato regolato in modo da avere la massima trasmissibilità e poter minimizzare la fase dello stato prodotto dall'interferometro.

Successivamente il fascio incontra uno specchio dicroico che trasmette la banda infrarossa e riflette quella ultravioletta e dopo averlo attraversato entra in un interferometro Sagnac, rappresentato in Fig. 4.1. Il singolo fotone $|+\rangle$ incontrando il BPS proietta le sue due componenti dello stato $|H\rangle$ e $|V\rangle$, nel senso di rotazione in cui percorre l'interferometro $|S_{\circlearrowleft}\rangle$ e $|S_{\circlearrowright}\rangle$.

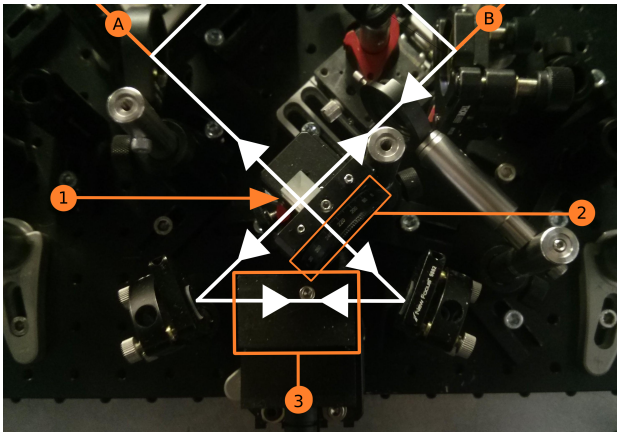


Figura 4.1: Schema dell'interferometro Sagnac.
A e B sono le uscite sugli apparati di Alice e Bob;
1. è il *PBS*;
2. è la lamina *HWP*;
3. è il cristallo **PPKTP** con la cella di Peltier.

Esattamente a metà del percorso è stato posto un cristallo non lineare che, tramite il fenomeno del *SPDC*, produce una coppia di fotoni negli stati $|H\rangle$ $|V\rangle$.
Subito prima dell'uscita del percorso orario è posta una lamina *HWP* che scambia la polarizzazione trasformando lo stato $|H\rangle$ in $|V\rangle$ e $|V\rangle$ in $|H\rangle$. Si avrà quindi che

$$\begin{aligned} |S_{\circlearrowleft}\rangle &\rightarrow |VH_{\circlearrowleft}\rangle \\ |S_{\circlearrowleft}\rangle &\rightarrow |HV_{\circlearrowleft}\rangle \end{aligned} \tag{4.2}$$

dove i due percorsi creano due stati identici in polarizzazione ma distinguibili spazialmente poiché in un senso si incontra prima il cristallo **PPKTP** e poi la lamina *HWP* raggiungendo il *PBS* su due facce differenti. In questo modo si ottiene lo stato complessivo:

$$|HV\rangle + |VH\rangle \tag{4.3}$$

in cui un fotone raggiungerà l'apparato di Alice e uno quello di Bob.

Questo semplice schema teorico necessita di alcune implementazioni sperimentali per essere realizzato. Di seguito verranno illustrati i vari componenti del sistema ottico necessari a migliorare la purezza dello stato prodotto. Quest'ultima verrà descritta dalla Tomografia trattata nella sezione 4.2.4.

[1] Vedi Appendice B.1
[2] Polarization Maintaining Single Mode
[3] *Polarization Beam Splitter*: un cristallo che riflette la componente $|V\rangle$ della funzione d'onda del fotone e trasmette quella $|H\rangle$
[4] *Half Wave Plane*: una lamina dicroica che aggiunge una fase Reale tra le componenti $|H\rangle$ e $|V\rangle$ del fotone permettendo di *girare* l'asse di polarizzazione
[5] *Quarter Wave Plane*: una lamina dicroica che aggiunge una fase Complessa tra le componenti $|H\rangle$ e $|V\rangle$

4.2.1 Cristallo

Come sorgente per i fotoni entangled si è usato un cristallo non lineare **PPKTP** con periodo di 10 µm e lungo 30.00 mm. Questo tipo di cristalli sfruttando il processo di **SPDC** in Quasi-phase-matching producono coppie di fotoni che rispettano le seguenti condizioni:

Consevarvazione dell'energia $\omega_1 + \omega_2 = \omega_{in}$

Phase-Matching $\mathbf{k}_1 + \mathbf{k}_0 + \frac{2\pi}{\Lambda} = \mathbf{k}_{in}$

dove ω_{in} e $\mathbf{k}_{in}$ si riferiscono ai fotoni in entrata e Λ è il periodo del cristallo. Il cristallo è costruito in modo da lavorare in maniera ottimale con una pompa a lunghezza d'onda di 405 nm, cioè quella del laser usato.

La frequenza dei due fotoni prodotti è data dalla temperatura del cristallo la quale viene mantenuta stabile a 20 °C tramite un cella Peltier. Lo spettro è stato studiato in maniera più approfondita nella sezione 4.2.3.2.

4.2.2 Preparazione di uno stato Entangled

Al fine di avere una mistura di stati il più possibile pura si è cercato di eliminare le varie cause di decoerenza.

Il principale problema è la purezza dei fotoni prodotti dal laser. Analizzando lo spettro in uscita si sono notate alcune instabilità della sorgente, analizzate in maniera specifica nella Appendice B.1. Al fine di eliminare questi problemi si è introdotto un specchio con una banda di riflessione ristretta intorno alla frequenza interessata[6] prima dell'immissione in fibra del fascio di pompa e si è scelto di mantenere il diodo ad una temperatura di 20 °C.

4.2.3 Analisi della Sorgente

Lo studio della sorgente è divisa in due parti: nella prima si è fatta una prima caratterizzazione dei fotoni prodotti mentre nella seconda si è analizzato lo stato prodotto. Al fine di avere una buona misura degli stati si sono considerati i seguenti parametri:

Delay è la distanza temporale tra due eventi correlati a una coincidenza. La distribuzione teorica è gaussiana e in rapporto alla sua larghezza si può definire la finestra di coincidenza.

Visibilità è definita come

$$V_{ij} = \frac{P_{ij} + P_{ji} - P_{ii} - P_{jj}}{P_{ij} + P_{ji} + P_{ii} + P_{jj}} \tag{4.4}$$

Dove dove P_{ij} è il numero di coincidenze con misurati con le basi (i, j) sui due canali. Questo valore calcolato nelle basi HV e $+-$ permette di avere un stima sulla qualità dello stato prodotto, stimando l'effetto del rumore sul segnale[7].

Per verificare la qualità delle coppie di fotoni prodotte si sono eseguite due tipi di analisi:

- Un'analisi spettrale per individuare un eventuale distinguibilità spettrale degli stati $|H\rangle$ e $|V\rangle$ e per verificare il corretto utilizzo dei singoli apparati ottici;
- Una Tomografia dello stato prodotto per verificarne la composizione.

[6] Vedi Appendice B.2
[7] Vedi Appendice A.1.

4.2.3.1 Analisi del Segnale

Delay Dall'analisi sullo ritardo temporale tra gli eventi di una coincidenza non si è rilevato nessun problema. Come si vede dal grafico in Fig. 4.2 gli eventi che compongono una coincidenza sono centrati sullo zero e non è stato necessario aggiungere un delay tra i due canali. Inoltre dato che la distribuzione ha una *FWHM* di 405 ps si è ristretta la finestra di coincidenza a 243 ps.

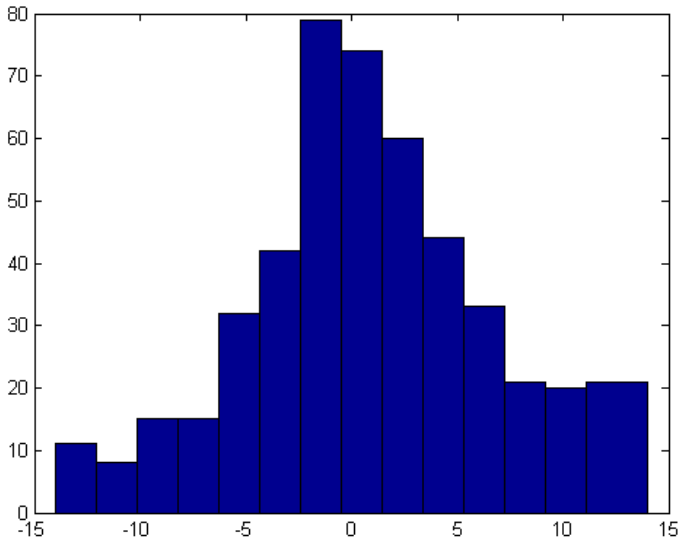


Figura 4.2: Distribuzione dello delay temporale tra i singolo eventi che compongono una coincidenza. Un bin è largo 81 ps.

Visibilità Al fine di stimare la visibilità si sono considerate le misure su due basi in polarizzazione: $\{|H\rangle, |V\rangle\}$ e $\{|+\rangle, |-\rangle\}$, ottenendo i seguenti valori:

$$\begin{aligned} V_{HV} &= 99.7\% \\ V_{+-} &= 98.4\% \end{aligned} \tag{4.5}$$

4.2.3.2 Analisi spettrale

Per studiare lo spettro dei fotoni emessi si è usato reticolo in trasmissione con passo $a = 3.3\,\mu m$ che lega agli angoli di riflessione θ_i e di trasmissione θ_r del fascio con la sua lunghezza d'onda λ secondo l'equazione:

$$\sin\theta_i + \sin\theta_t = m\frac{\lambda}{a} \tag{4.6}$$

dove m è l'ordine della riflessione.

Nel caso trattato in questa tesi si è usato il reticolo come monocromatore ad angolo sottesso costante cioè si è fatto variare l'angolo di incidenza del fascio sul reticolo mentendo ferma la sorgente[8] che il rivelatore considerando solo il primo ordine di riflessione. In questo modo la relazione con l'angolo tra la normale del reticolo α e la lunghezza d'onda del fascio incidente diviene:

$$\frac{\lambda}{a} = \sin\frac{\varphi}{2}\cos\left(\alpha - \frac{\varphi}{2}\right) \tag{4.7}$$

[8]Come sorgente qui si intende una uscita di una fibra ottica mono-modale che aveva in entrata le sorgenti effettive.

dove φ è la posizione angolare del rivelatore rispetto al fascio. Per piccole deviazioni dell'angolo si può considerare la relazione come lineare e i vari parametri si possono ottenere tramite una taratura dell'apparato in vicinanza della lunghezza d'onda che ci interessa, circa 808 nm.

A tal fine si è utilizzato il laser Mira-HP della Coherent in cui variando la cavità ottica si è potuto far variare la lunghezza d'onda della radiazione emessa tra $798.6(1)$ nm e $808.5(1)$ nm. Come si vede dal grafico in Fig. 4.3, la relazione tra la lunghezza d'onda e l'angolo di incidenza è in buona approssimazione lineare e tramite i parametri ottenuti da un fit lineare si è potuto stimare la frequenza dei fotoni emessi dalla sorgente Sagnac nel canale di Alice e Bob a diverse temperature del cristallo rappresentate in Figura 4.4. La condizione di lavoro ottimale è quando i fotoni prodotti hanno la stessa lunghezza d'onda. Considerando che il laser di pompa è a $404.50(25)$ nm si dovrebbe impostare una temperatura tale da avere un'emissione a $809.0(18)$ nm. Tale lunghezza d'onda è ottenibile ad una temperatura leggermente superiore ai 20 °C. Per impostare esattamente tale frequenza è necessario però uno spettrometro più preciso di quelli disponibili. Si è quindi preferito impostare una temperatura di 20 °C, ottenendo una frequenza in uscita per il canale Alice di $807.2(18)$ nm.

4.2.4 Tomografia

Per ottenere una Tomografia della matrice densità dello stato prodotto dalla sorgente si utilizza una tecnica di Maximum Likelihood.

Stimata la matrice, rappresentata in Fig 4.5 divisa nelle sue componenti Reale e Immaginaria, si sono calcolati i seguenti parametri:

Fidelity Ψ^+	0.034 ± 0.001
Fidelity Ψ^-	0.952 ± 0.001
Purezza	$0.911 \pm .001$
Tangle	$0.849'\mathrm{pm}0.001$

dove la Fidelity è data dall'overlap tra lo stato indicato e quello misurato cioè $\mathrm{Tr}\,(A_{\pm}\rho)$ dove A è la matrice densità dello stato $\Psi^{\pm}$, la Purezza è data da $\mathrm{Tr}\left(\rho^2\right)$ e indica quanto la stato misto si avvicina ad uno stato puro mentre il *Tangle* indica quanto siano entangled i due fotoni che si calcola tramite:

$$\mathrm{Tangle} = (\Lambda_1 - \Lambda_2 - \Lambda_3 - \Lambda_4)^2 \tag{4.8}$$

dove Λ_i^2 sono gli autovalori della matrice ρ

Lo stato ottenuto dalla sorgente Sagnac non è ottimale: con una sorgente simile Smith ha ottenuto una Fidelity sullo stato interessato di 0.9726 ± 0.0005 e un *Tangle* di $0.9097^{+0.0017}_{-0.0016}$ [10]. Questo però non è un problema per l'obbiettivo della tesi.

4.3 Realizzazione del Protocollo PBC00

La realizzazione effettiva del protocollo **PBC00** non si distanzia di molto da quella descritta nella Sezione 3.3 come si può vedere nel seguente schema:

Creazione della Chiave In questo caso Alice prepara solo una stringa binaria b in cui è codificata la chiave.

Codifica Alice associa ad ogni uno dei tre rivelatori uno stato preparato nel sistema di Bob[9]. Misurando i fotoni entangled che riceve dalla sorgente saprà quale stato riceverà Bob.

[9] Vedi Appendice C.1.

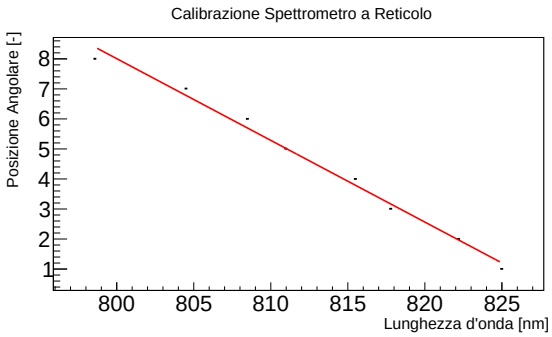


Figura 4.3: Relazione tra l'angolo di inclinazione del reticolo e la lunghezza d'onda del laser incidente.
$m = -0.2721 \pm 0.0004$
$c = 225.7 \pm 0.3$
$correl. = -0.99$
$\chi^2_{rid.} = 676$

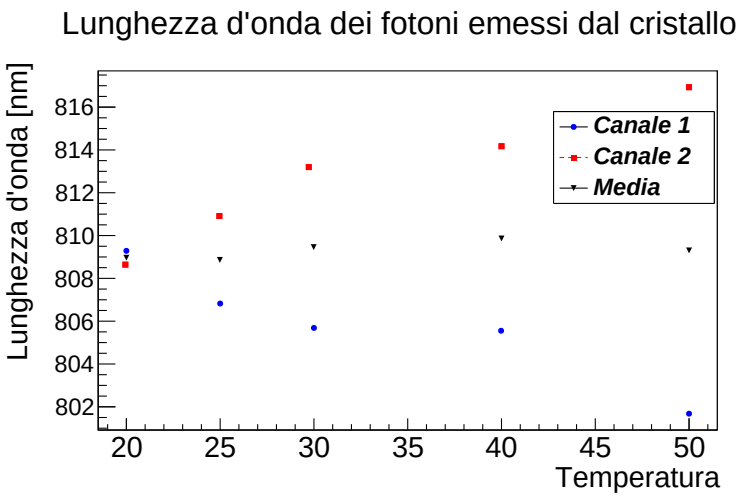
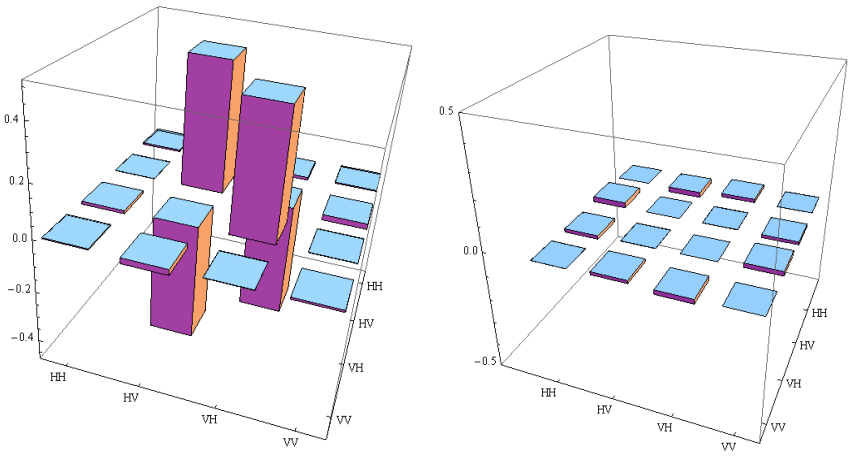


Figura 4.4: Variazione della lunghezza d'onda dei fotoni emessi dal cristallo nel canale di Alice, dopo aver modificato l'inclinazione del cristallo.



(a) Parte Reale. **(b)** Parte Immaginaria.

Figura 4.5: Rappresentazione della matrice densità dello stato prodotto dalla sorgente di fotoni entangled.

Lettura Bob associa ad ogni uno dei tre rivelatori una misura sugli stati ortogonali a quelli "inviati" da Alice. In questo caso è impossibile per Bob misurare nello stato ortogonale a quello inviato da Alice.

Sifting Quando Bob finisce di leggere tutti gli stati lo comunica ad Alice. Alice considerando gli stati che ha misurato comunica gli alfabeti che li codificano nei bit che voleva inviare secondo la tabella:

Bit	Stati Quantistici		
Classico	Alfabeto 1	Alfabeto 2	Alfabeto 3
0	$\|A\rangle$	$\|B\rangle$	$\|C\rangle$
1	$\|B\rangle$	$\|C\rangle$	$\|A\rangle$

Per esempio se ha misura $|A\rangle$ e voleva inviare il bit 0 dirà che ha usato l'"Alfabeto 1", se invece voleva inviare il bit 1 dirà comunicherà l'"Alfabeto 3".

Post Elaborazione Alice sceglie a caso una parte delle chiave, la comunica a Bob e insieme stimano i vari parametri.

EC & PA Alice e Bob procedono nella correzione degli errori e della Amplificazione della Privacy.

In questo schema gli stati necessari per realizzare il protocollo PBC00 sono i seguenti:

$$\begin{aligned} |A\rangle &= |H\rangle \\ |B\rangle &= \frac{|H\rangle + \sqrt{3}\,|V\rangle}{2} \\ |C\rangle &= \frac{|H\rangle - \sqrt{3}\,|V\rangle}{2} \end{aligned} \tag{4.9}$$

e si nota facilmente che non sono ortogonali tra loro e che il braket tra due stati diversi è pari a $\frac{1}{2}$.

4.3.0.1 Schema del sistema ottico

Alice e Bob hanno due sistemi ottici uguali per eseguire le misure necessarie al protocollo: il singolo fotone che arriva dalla sorgente Sagnac incontra prima un *PPBS*, che funziona come un *PBS* con la differenza che in polarizzazione *s* ha una Riflettività del 66.7±7%. Il fascio riflesso viene accoppiato in un rivelatore *SPCM*, quello trasmesso arriva su una lamina *HWP* impostata in modo da ruotare la polarizzazione di $\frac{\pi}{4}$. Infine il fascio incontra un *PBS* le cui due uscite sono associate ad altri due rivelatori.

4.3.1 Evoluzione di uno singoletto Entengled attraverso i rivelatori

Per lo studio dell'evoluzione dei fotoni si è assunto che i fotoni arrivino prima nell'apparato di Alice.

Considerando l'evoluzione definita dai vari componenti si ottiene il seguente stato:

$$\begin{aligned} -\frac{1}{\sqrt{3}}\,|a_1\rangle \quad & \frac{1}{\sqrt{2}}\,(|c_2\rangle - |b_2\rangle) \\ -\frac{1}{\sqrt{3}}\,|b_1\rangle \quad & \frac{1}{\sqrt{2}}\,(|a_2\rangle + |c_2\rangle) \\ -\frac{1}{\sqrt{3}}\,|c_1\rangle \quad & \frac{1}{\sqrt{2}}\,(|a_2\rangle + |b_2\rangle) \end{aligned} \tag{4.10}$$

dove $|a_i\rangle$, $|b_i\rangle$ e $|c_i\rangle$ sono i fotoni che raggiungono il rivelatori associati agli stati $|A\rangle$, $|B\rangle$ e $|C\rangle$ degli apparati di Alice (1) e Bob (2). Si nota ad esempio che se Alice misura $|A\rangle$, Bob lo può rilevare con eguale probabilità misurando $|\bar{B}\rangle$ o $|\bar{C}\rangle$ avendo un click sui rispettivi rivelatori.

4.3.2 Verifica della distribuzione di una Chiave

A causa di un problema tecnico con l'apparato non si è riusciti a fare una misura completa del protocollo. In particolare è risultato impossibile implementare lo schema ottico presentato nella Sezione 4.3.0.1 e si è dovuto fare le misure utilizzando un unico canale per i sistemi di Alice e Bob utilizzando la seguente variante: il **PPBS** viene utilizzato come filtro e al posto del **PBS** si è posto un polarizzatore.

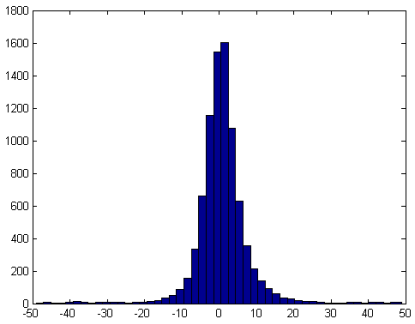
In questo modo si ignora di fatto il Canale A_i studiando la fattibilità del protocollo considerando solo gli altri due stati. In pratica quello che si è fatta una misura di visibilità sugli stati $|B\rangle$ e$|C\rangle$ calcolando:

$$V_{BC} = \frac{P_{B\bar{C}} + P_{C\bar{B}} - P_{B\bar{B}} - P_{C\bar{C}}}{P_{B\bar{C}} + P_{C\bar{B}} + P_{B\bar{B}} + P_{C\bar{C}}} \tag{4.11}$$

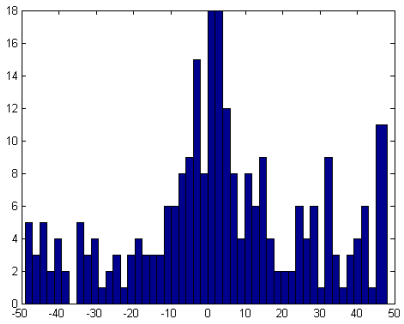
dove $P_{K\bar{J}}$ sono le coincidenze misurate nel caso Alice invia $|K\rangle$ e Bob misuri $|\bar{J}\rangle$ ottenendo:

$$V_{BC} = 0.92 \tag{4.12}$$

che ci indica come il set-up dell'apparato funzioni in queste basi. Si è poi studiato l'andamento della visibilità in funzione della dimensione della finestra: Ci si aspetta infatti che all'aumentare della finestra aumentino le coincidenze accidentali e di conseguenza la visibilità cali. Dal grafico in Figura 4.7 si nota però che per finestre di coincidenza minori di 30 bin, cioé di 2.430 ns, la visibilità non varia in maniera evidente. Se si guarda inoltre l'istogramma in Figura 4.6b rappresentante il delay tra eventi di fondo, si nota un picco centrato intorno al bin 0 con un ampiezza pari a quella del segnale reale. Questo ci fa vedere come lo stato prodotto dalla sorgente non sia ottimale: bisogna infatti migliorare ancora la Fidelity sullo stato Ψ^- per eliminare questo fondo sistematico dato dalla presenza di coppie Ψ^+.



(a) Istogramma la distribuzione dei delay tra le coincidenze in evento di segnale.



(b) Istogramma la distribuzione dei delay tra le coincidenze in evento di fondo.

Figura 4.6: Istogrammi riguardanti i delay nei segnali sugli stati $|B\rangle$ e $|C\rangle$ del **PBC00**.

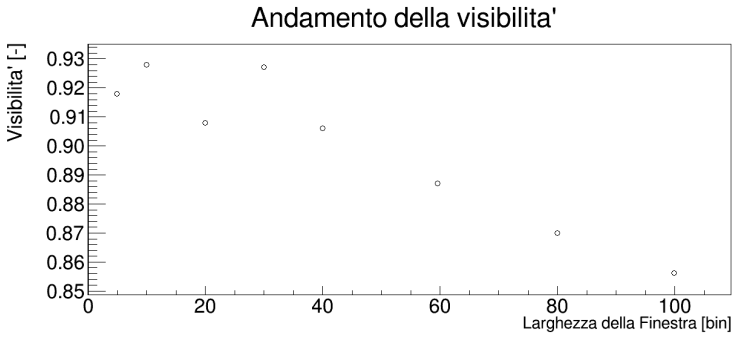


Figura 4.7: Visibilità in funzione della larghezza della finestra. Un bin è largo 81 ps.

5

Conclusioni

Data la mistura di stati prodotta dalla sorgete Sagnac discussa nella Sezione 4.2.3 e le misure preliminari sul protocollo **PBC00** discusse nella Sezione 4.3.2 si può vedere come il protocollo sia realizzabile nello schema presentato in questa tesi. In conclusione si può **PBC00** delle buone aspettative: la realizzazione dei proiettori $|B\rangle$ e $|C\rangle$ è stata molto facile e l'aggiungere quello relativo allo stato $|A\rangle$ è una cosa relativamente semplice. Questo ci permette di ipotizzare la realizzazione di un set-up molto più compatto di quello utilizzato creando ad esempio un circuito integrato.

Bisogna però sottolineare ancora che tali misure non sono complete e per avere una verifica definitiva della fattibilità del protocollo serve completare le misure su tutti gli stati richiesti. Inoltre la sorgente va ancora ottimizzata migliorando da una parte facendo una caratterizzazione completa del cristallo al fine di utilizzarlo nelle migliori condizioni dall'altra bisogna migliorare la Fidelity sullo stato Ψ^- poiché come visto nello studio sul delay nelle coincidenze $(|B\rangle, |C\rangle)$ la presenza della stato Ψ^+ presenta un segnale sistematico nel fondo che può causare un aumento degli errori nella distribuzione di chiave. Una volta costruito il set-up per il **PBC00** potrebbe essere interessante verificare sperimentalmente se l'evoluzione dello stato Entangled è esattamente quella descritta nell'Appendice C.1 facendo una tomografia dei fotoni nel sottosistema di Bob ad una data misura di Alice.

A

Parametri per l'analisi del segnale

A.1 Visibilità

La visibilità è un parametro sperimentale che serve per stimare facilmente quanto è visibile lo stato ed è stimato tramite:

$$V_{ij} = \frac{P_{ij} + P_{ji} - P_{ii} - P_{jj}}{P_{ij} + P_{ji} + P_{ii} + P_{jj}} \tag{A.1}$$

dove P_ij sono le coincidenze misurate nelle basi (i, j) nei rispettivi canali.

Se si considera la misura di uno stato di Entangled puro

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle) \tag{A.2}$$

in assenza di qualsiasi rumore si ha ovviamente che la Visibilità misurata in HV e in $+-$ è pari a 1. Il caso più interessante è invece quello reale in cui, lo stato misurato non è puro a causa della presenza di rumore nel canale. Questo tipo di effetti possono essere divisi in due tipi: rumore bianco, e rumore colorato, dati da:

$$\begin{aligned} \rho_{withe} &= \frac{1}{4} (|HH\rangle \langle HH| + |VV\rangle \langle VV| + |HV\rangle \langle HV| + |VH\rangle \langle VH|) \\ \rho_{colored} &= \frac{1}{2} (|HV\rangle \langle HV| + |VH\rangle \langle VH|) \end{aligned} \tag{A.3}$$

Come si può vedere il rumore colorato deriva da termini già presenti nello stato Ψ^-, mentre il rumore bianco è una mistura di stati completamente scorrelati tra loro.

Considerando il rumore lo stato misurato è rappresentato dalla seguente mistura:

$$\rho_{tot} = p\, |\Psi^-\rangle \langle \Psi^-| + (1 - p)\, \rho_{noise} \tag{A.4}$$

dove p è il contributo relativo dello stato che ci interessa rispetto al rumore del segnale che è una combinazione di rumore bianco e colorato.

Per verificare la presenza delle due componenti del rumore serve fare misure di visibilià su due basi opportune: il rumore bianco si riesce a individuare usando la base HV mentre per quello colorato serve la base $+-$. In questo modo si ottiene una misura semplice che permette dare una stima dello stato Entangled prodotto.

A.2 Maximum Likelhood

Per stimare la matrice densità dello stato prodotto dalla sorgente si è utilizzato il Metodo della Maximum Likelhood, in cui definita una parametrizzazione della matrice densità

si stimano i parametri che più l'avvicinano a quella associata alla misure fatte. Di seguito presenterò una breve introduzione al metodo, per una discussione più approfondita si rimanda al seguente articolo [6].

A.2.1 Paramatrizzazione

La matrice densità per definizione deve avere le seguenti proprietà:

- Deve essere Hermitiana: $\rho^\dagger = \rho$
- Deve essere positiva: $\langle\psi|\,\rho\,|\psi\rangle \geqslant 0 \quad \forall\,|\psi\rangle$
- Deve essere normalizzata: $\mathrm{Tr}\{\rho\} = 1$

Le prime due proprietà si possono ottenere definendo ρ come prodotto di una matrice per il suo autoaggiunto, la terza normalizzando il prodotto:

$$\rho = \frac{\tau\tau^\dagger}{\mathrm{Tr}\left\{\tau\tau^\dagger\right\}} \tag{A.5}$$

inoltre la matrice τ deve a sua volta rispettare due richieste: essere triangolare e con traccia reale:

$$\tau = \begin{pmatrix} t_1 & t_2 + t_3 & t_4 + t_5 & t_6 + t_7 \\ 0 & t_8 & t_9 + t_{10} & t_{11} + t_{12} \\ 0 & 0 & t_{13} & t_{14} + t_{15} \\ 0 & 0 & 0 & t_{16} \end{pmatrix} \tag{A.6}$$

A.2.2 Funzione di Verosimiglianza

Come stima di verosimiglianza tra la matrice densità e lo stato misurato si considera il χ^2 cioè:

$$\chi^2\,(\mathbf{t}) == \bar{N} \sum_i \frac{(\mathbf{W}_i - \mathbf{w}_i(\mathbf{t}))^2}{\mathbf{w}_i(\mathbf{t})} \tag{A.7}$$

dove $\mathbf{w}_i(\mathbf{t}) = \mathrm{Tr}\{\rho(\mathbf{t})W_i\}$ con $\rho(\mathbf{t})$ una matrice densità parametrizzata dal vettore $\mathbf{t}$ e $\mathbf{W}_i = \frac{N_i}{\bar{N}}$ con N_i il numero di conteggi misurati sul proiettore su $\bar{N}$ conteggi totali. Minimizzando il χ^2 sui parametri $\mathbf{t}$ si ottiene la matrice ρ cercata.

B

Analisi delle Componenti principali

Di seguito verranno elencati i componenti principali dell'apparato

B.1 Laser

Come sorgente di Pompa per il Sagnac si è utilizzato il laser **LM-405-PLR-40-2** prodotto dalla Ondax.

Durante la calibrazione della sorgente di fotoni entangled si sono presentati alcuni problemi dovuti a questa componente e si è quindi deciso di studiarne lo spettro di emissione. Guardando lo spettro a varie temperature si è notato che alla temperatura del diodo di 40 °C si verifica la coesistenza di due modi in lunghezza d'onda distinti. Questo ha portato alla scelta di tenere il laser ad una temperatura controllata di 20 °C dove il picco di emissione è unico a 404.50(26) nm, Fig B.1a.

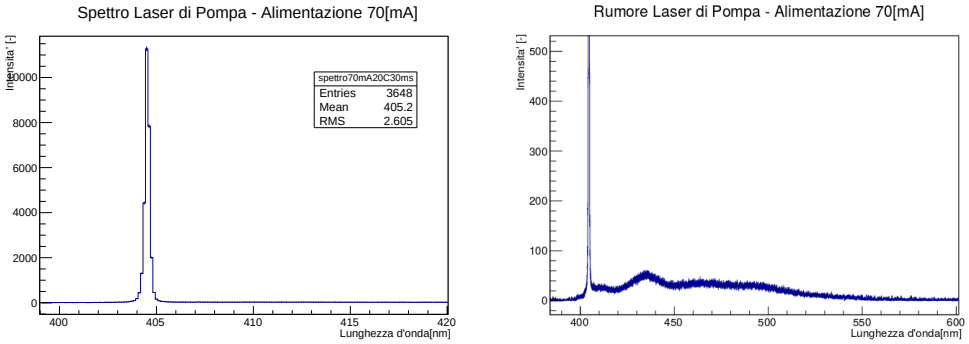
Al variare dell'intensità di alimentazione, si è notata invece una coda a destra del picco evidenziata nella Fig. B.1. Come si nota è poco intenso ma interessa una parte molto ampia dello spettro, il rapporto tra l'intensità del picco e quella della coda è 0.93, cioé metà dei fotoni che arrivano al sistema ottico sono ad una lunghezza d'onda diversa da quella nominale.

B.2 Filtro

Come già detto, per ovviare ai problemi descritti sopra si è posto un filtro prima della fibra. Per essere precisi, al fine di ridurre al più possibile le componenti a bassa frequenza si è sostituito uno specchio di accoppiamento inserendo un **BB1-E01** della ThorLabs che ha una banda di riflessione rappresentata in Fig. B.2 che include quella di emissione principale del laser usato e permette di rimuovere il rumore sopra i 450 nm. Questo ha permesso di ridurre della metà l'intensità della coda.

B.3 Partial Polarization Beam Splitter

I PPBS utilizzati sono stati costruiti per questo esperimento. Le informazioni sulla trasmissività sono in Fig. B.3



(a) Spettro del Laser alla temperatura di lavoro, 20 °C.**(b)** Dettagli dello spettro del Laser, in cui si presenta la coda.

Figura B.1: Spettro del Laser **LM-405-PLR-40-2** utilizzato come pompa per la produzione dei fotoni entangled.

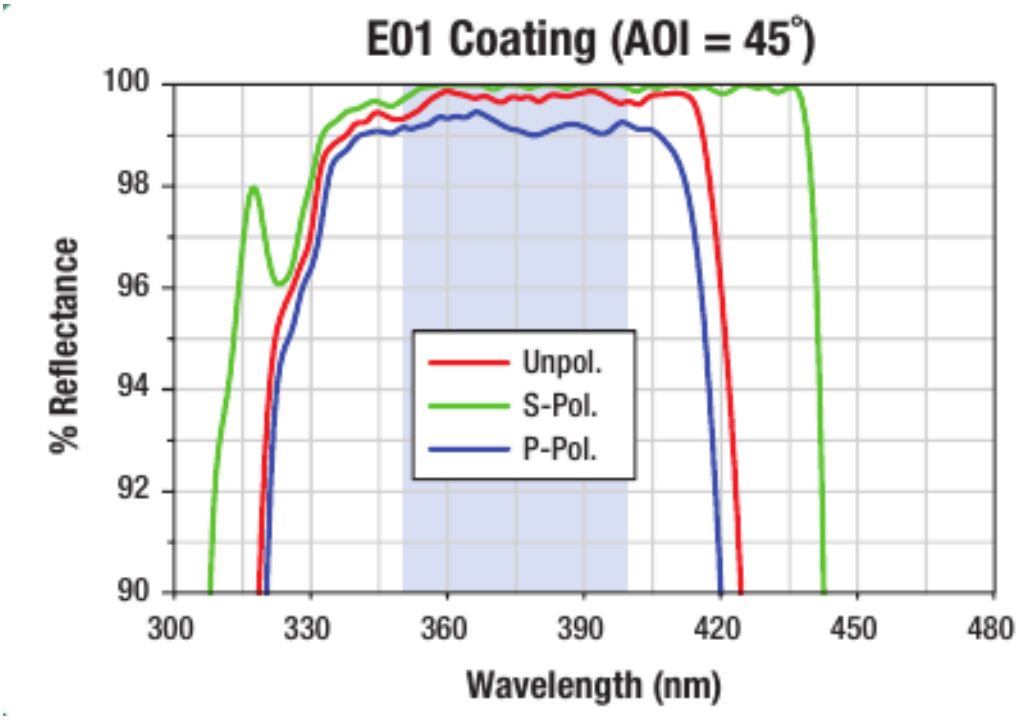


Figura B.2: Banda riflettente di uno specchio **BB1-E01** per fasci che incidono a 45°.

B.4 Single Photon Counter Module

Per misurare il numero di fotoni si sono usati dei rivelatori allo stato solido chiamati *Single Photon Count Module*, prodotti dall'Excelitas Technoligies. Il modello usato è il **SPCM AQRH-14** le cui caratteristiche principali sono:

Parametri	Minimo	Tipico	Massimo	Unità di misura
Dead Time		20	40	ns
Dark Count			100(2)	counts / second

mentre l'efficienza e il rapporto tra fotoni in arrivo e i conteggi misurati sono rappresentati nei due grafici in Fig. B.4 dove sono state evidenziate le zone in cui si è lavorato.

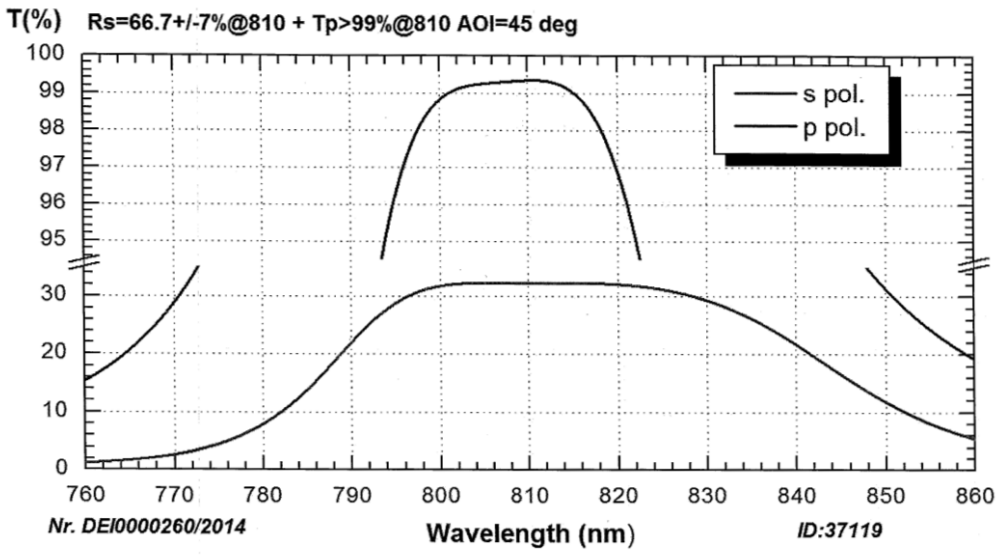
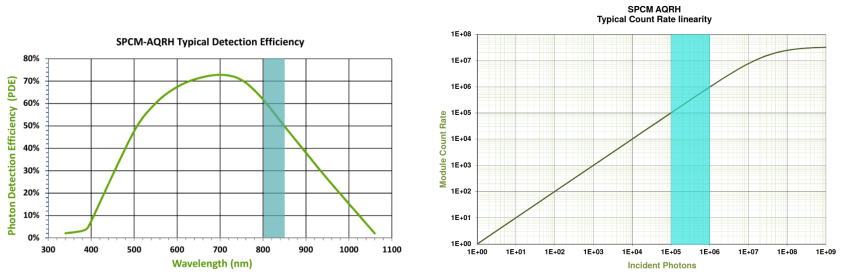


Figura B.3: Plot Sheet dei due PPBS utilizzati in questa tesi.



(a) Efficienza in funzione della lunghezza d'onda dei fotoni rilevati.

(b) Rapporto tra il numero di fotoni incidenti sul rivelatore e il numero di conteggi misurato.

Figura B.4: Risposta dei rilevatori SPMC in funzione della sorgente.

C

Evoluzione dei stati Entangled nel PBC00

Come già spiegato nella tesi al fine di realizzare il protocollo **PBC00** si è utilizzata una sorgente di singoletti Entangled $|HV\rangle - |VH\rangle$ in modo che un fotone raggiunga l'apparato di Alice e uno quello di Bob. Assumendo che il fotone di Alice sia misurato per prima mostriamo qual'è l'evoluzione temporale degli stati. A tal fine indicheremo $|k_i^l\rangle$ un fotone k con polarizzazione l che appartiene al sottosistema di Alice per $i = 1$ o di Bob per $i = 2$, mentre assoceremo ad ogni elemento ottico dello schema un operatore unitario che ne descrivi l'effetto sul fotone:

$$\begin{aligned} U_{PPBS}^{(i)} &= \frac{\sqrt{2}}{\sqrt{3}} |r_i^V\rangle \langle V_i| + \frac{1}{\sqrt{3}} |t_i^V\rangle \langle V_i| + |t_i^H\rangle \langle H_i| \\ U_{PBS}^{(i)} &= |r_i^V\rangle \langle V_i| + |t^H\rangle \langle H_i| \\ U_{HWP}^{(i)} &= |t_i^+\rangle \langle H_i| + |t^-\rangle \langle V_i| \end{aligned} \tag{C.1}$$

dove $|t^l\rangle$ e $|r^l\rangle$ sono rispettivamente il fotone trasmesso e quello riflesso.

C.1 Evoluzione nel sistema di Alice

Per semplificare i conti si è calcolata l'evoluzione temporale degli stati $|V\rangle$ e $|H\rangle$ presi singolarmente e successivamente si è considerato tutto il sistema. Indichiamo con $\hat{\alpha}_0^l$ in entrata nell'apparato e $|n_i\rangle$ lo stato che entrerà nel rivelatore N:

PPBS

$$\begin{aligned} U_{PPBS} |\alpha_i^H\rangle &= \\ &\quad kett_i^H \\ U_{PPBS} |\alpha_i^V\rangle &= \frac{\sqrt{2}}{\sqrt{3}} |a_i^V\rangle + \frac{1}{\sqrt{3}} |t_i^V\rangle \end{aligned} \tag{C.2}$$

HWP

$$\begin{aligned} U_{PBS} |t_i^H\rangle &= \frac{1}{\sqrt{2}} \left(|d_i^H\rangle + |d_i^V\rangle \right) \\ U_{PBS} |t_i^V\rangle &= \frac{1}{\sqrt{2}} \left(|d_i^H\rangle - |d_i^V\rangle \right) \end{aligned} \tag{C.3}$$

PBS Semplicemente manda $|d_i^V\rangle$ nel rivelatore B e $|d_i^H\rangle$ in C.

In fine si ottiene che l'evoluzione dello stato è data da:

$$\begin{aligned} &\frac{1}{\sqrt{3}}|a_1\rangle \quad |H_2\rangle + \\ &\frac{1}{\sqrt{3}}|b_1\rangle \quad \frac{|H_2\rangle + \sqrt{3}|V_2\rangle}{2} + \\ &\frac{1}{\sqrt{3}}|c_1\rangle \quad \frac{|H_2\rangle - \sqrt{3}|V_2\rangle}{2} \end{aligned} \tag{C.4}$$

Che mostra come la misura sullo stato di Alice prepara nel sistema di Bob uno dei tre stati del **PBC00**.

C.2 Evoluzione nel sistema di Bob

Partendo dallo stato in eq. C.4 si ottiene l'equazione mostra in 4.10 che riscriviamo per completezza:

$$\begin{aligned} &-\frac{1}{\sqrt{3}}|a_1\rangle \quad \frac{1}{\sqrt{2}}(|c_2\rangle - |b_2\rangle) \\ &-\frac{1}{\sqrt{3}}|b_1\rangle \quad \frac{1}{\sqrt{2}}(|a_2\rangle + |c_2\rangle) \\ &-\frac{1}{\sqrt{3}}|c_1\rangle \quad \frac{1}{\sqrt{2}}(|a_2\rangle + |b_2\rangle) \end{aligned} \tag{C.5}$$

Bibliografia

[1] CH Bennett e G Brassard. «Quantum cryptography: Public key distribution and coin tossing». In: *Proceedings of IEEE International ...* 1 (1984), pp. 175–179. URL: http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf.

[2] Charles H. Bennett. «Quantum cryptography using any two nonorthogonal states». In: *Physical Review Letters* 68.21 (1992), pp. 3121–3124. DOI: http://dx.doi.org/10.1103/PhysRevLett.68.3121. URL: http://scholar.google.com/scholar?hl=en\&btnG=Search\&q=intitle:No+Title\#0http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.68.3121.

[3] J.-C. Boileau et al. «Unconditional Security of a Three State Quantum Key Distribution Protocol». In: *Physical Review Letters* 94.4 (gen. 2005), p. 040503. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.94.040503. URL: http://link.aps.org/doi/10.1103/PhysRevLett.94.040503.

[4] Daniel Gottesman et al. «Security of quantum key distribution with imperfect devices». In: *Quantum Information and Computation* 4.5 (2002), p. 36. arXiv: 0212066 [quant-ph]. URL: http://arxiv.org/abs/quant-ph/0212066.

[5] Taehyun Kim, Marco Fiorentino e Franco N. C. Wong. «Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer». In: *Physical Review A* 73.1 (gen. 2006), p. 012316. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.73.012316. URL: http://link.aps.org/doi/10.1103/PhysRevA.73.012316.

[6] NK Langford. «Encoding, manipulating and measuring quantum information in optics». Tesi di dott. University of Queensland, 2007, pp. 1–295. URL: http://espace.library.uq.edu.au/view/UQ:136626.

[7] Simon J. D. Phoenix, Stephen M. Barnett e Anthony Chefles. «Three-state quantum cryptography». In: *Journal of Modern Optics* 47.2-3 (feb. 2000), pp. 507–516. ISSN: 0950-0340. DOI: 10.1080/09500340008244056. URL: http://www.tandfonline.com/doi/abs/10.1080/09500340008244056.

[8] Joseph Renes. «Spherical-code key-distribution protocols for qubits». In: *Physical Review A* 70.5 (nov. 2004), p. 052314. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.70.052314. URL: http://link.aps.org/doi/10.1103/PhysRevA.70.052314.

[9] C. E. Shannon. «Communication Theory of Secrecy Systems». In: *Bell System Technical Journal* 28.4 (ott. 1949), pp. 656–715. ISSN: 00058580. DOI: 10.1002/j.1538-7305.1949.tb00928.x. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6769090.

[10] Devin Hugh Smith. «An Ultrafast Source of Polarization Entangled Photon Pairs based on a Sagnac Interferometer». Tesi di dott. 2009.

[11] G. S. Vernam. «Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications». In: *Transactions of the American Institute of Electrical Engineers* XLV (gen. 1926), pp. 295–301. ISSN: 0096-3860. DOI: 10.1109/T-AIEE.1926.5061224. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5061224.