UNIVERSITÁ DEGLI STUDI DI PADOVA

Dipartimento di Ingegneria dell'Informazione

Tesi di Laurea Magistrale

L'ENTANGLEMENT COME RISORSA NELLA SPERIMENTAZIONE DELL'INFORMAZIONE QUANTISTICA

Laureando: **Marco Tomasin**

Relatore: Ch.mo Prof. **Paolo Villoresi**

Correlatore: Dott. **Giuseppe Vallone**

Corso di Laurea Magistrale in Ingegneria delle Telecomunicazioni

Padova, 23 Ottobre 2012

Anno Accademico 2011-2012

alla mia famiglia e a Chiara

Abstract

Questo lavoro di tesi descrive l'implementazione di un setup ottico utilizzato per testare dei protocolli di comunicazione quantistica derivati dal B92. Per l'implementazione si è utilizzato uno stato non massimamente entangled, generato attraverso il processo ottico non lineare SPDC (Spontaneus Parametric Down Conversion).
I risultati ottenuti hanno mostrato come sia possibile implemetare un protocollo derivato dal b92 utilizzando uno stato non massimamente entangled. Tali risultati hanno mostrato un guadagno di chiave sicura (cioè la probabilità che un qubit diventi un bit della chiave finale) maggiore di zero.
Sono state poste, inoltre, le basi per la creazione di una sorgente di fotoni hyper-entangled.

Indice

Introduzione

La digitalizzazione delle informazioni è un processo in costante crescita, che richiede, come conseguenza, un aumento di metodi efficaci per proteggere tali dati da eventuali spie. Per soddisfare quest'esigenza, si è fatto ricorso alla crittografia, la quale, grazie a robusti algoritmi matematici, ha reso la comunicazione impenetrabile da terze parti.
Poichè questi algoritmi basano la loro forza sulla difficoltà computazionale di fattorizzare numeri elevati, non possono essere considerati del tutto sicuri. Infatti, lo sviluppo del computer quantistico sembra prospettare uno scenario in cui le chiavi crittografiche possono essere facilmente decodificate grazie alla sua capacità di fattorizzazione dei numeri. In futuro dunque, sarà necessario utilizzare un sistema di crittografia sicuro, a prescindere dalla sempre maggior capacità di calcolo computazionale disponibile. Per questo, già dagli anni ottanta (vedi par. 2.2), è stato avanzato un metodo crittografico, che basa la sua sicurezza sui fondamenti della meccanica quantistica.
Si è in tal modo dato il via alla crittografia quantistica, più propriamente detta Quantum Key Distribution (QKD), dato che le procedure di codifica coinvolgono lo scambio sicuro delle chiavi. La QKD permette di creare chiavi intrinsecamente sicure, codificando le informazioni (quantum bit) negli stati quantistici, come per esempio lo stato di polarizzazione del fotone.
Grazie al *No-cloning Theorem* [Zur82], il ricevitore è in grado di accorgersi se la chiave è stata copiata da un attaccante esterno. Da ciò si può capire che la QKD permette di codificare i dati in tutta sicurezza, grazie a proprietà derivanti dalla natura quantistica della chiave e non dalla complessità di un algoritmo matematico.
Il lavoro svolto in questa tesi si inserisce in questo ambito ed è stato incentrato nello sviluppo di un setup, per testare un protocollo di comunicazione quantistica alla cui base vi è l'entanglement. Per realizzare tale stato, si è fatto ricorso al processo di *spontaneous parametric downconversion* (SPDC vedi par. 3.3), che consente di generare fotoni entagled in polarizzazione. Tali fotoni vengono impiegati per implementare e testare il protocollo B92-ent, B92-gen e un protocollo QKD per massimizzare il guadagno di chiave

sicura (vedi par. 2.2.3). Il fulcro di ogni test consiste nel misurare le coppie di fotoni entangled in base agli stati necessari per implementare i precedenti protocolli. Alla fine di questa tesi verranno mostrati i risultati ottenuti sperimentalmente.
Il passo seguente è stato creare una sorgente di fotoni hyper-entangled partendo dal setup precedente. Tale setup sarà sicuramente utile per aumentare la complessità della chiave e il lavoro fin qui condotto sarà una solida base per proseguire in tale ricerca.
Nei capitoli seguenti verranno trattati questi argomenti:

- Capitolo 1: Basi della meccanica quantistica
- Capitolo 2: Crittografia classica e crittografia quantistica
- Capitolo 3: Concetti di ottica non lineare
- Capitolo 4: Analisi degli strumenti e dei componenti utilizzati
- Capitolo 5: Sviluppo setup dell'esperimento
- Capitolo 6: Risultati delle misure
- Capitolo 7: Sorgente hyper-entangled
- Capitolo 8: Conclusioni

Capitolo 1

Metodi e strumenti della Meccanica Quantistica

Introduciamo in questo capitolo gli aspetti teorici della meccanica quantistica, i quali costituiscono le basi necessarie per comprendere il contenuto di questa tesi. La meccanica quantistica è una teoria che fornisce un modello del mondo fisico, introducendo, rispetto la meccanica classica, dei concetti che entrano in contrasto con l'intuizione comune. Ad esempio, il modello fornito dalla meccanica quantistica presenta situazioni indeterminate, aleatorie, mentre nella meccanica classica tutto è determinato (avendo conoscenza dell'intero sistema). Un'altra differenza si ha nella misura, infatti nella meccanica quantistica la misura di una quantità fisica disturba il sistema, alterandolo (come spiegato in seguito nel principio di indeterminazione di Heisenberg), aspetto non presente nella meccanica classica. Nei successivi paragrafi verrano mostrati ulteriori aspetti della meccanica quantistica. Introduciamo brevemente in questo capitolo la notazione e le definizioni usate in questa tesi.

1.1 Notazione e definizioni base

Spazi di Hilbert e vettori

Uno Spazio di Hilbert H è uno spazio vettoriale complesso sul quale è definito un prodotto interno. Gli elementi di questo spazio, vengono indicati come $|\phi\rangle$, $|\chi\rangle \ldots$, chiamati *ket*, e corrispondono a vettori colonna. Il trasposto e coniugato di questi vettori vengono indicati come $\langle\phi|$, $\langle\chi| \ldots$, chiamati *bra*. Il prodotto interno tra due vettori di H viene indicato con $\langle\phi|\theta\rangle$.

Osservabili

Le osservabili sono operatori lineari hermitiani associati a quantità fisiche misurabili. Il valore di questa quantità fisica non è definito con certezza, ma assume con una certa probabilità un certo valore. Come vedremo in seguito, una misura su un sistema quantistico non è altro che una proiezione dello stato, che collassa su un autostato dell'osservabile. Sia A la nostra osservabile, abbiamo

$$A|\alpha_m\rangle = a_m|\alpha_m\rangle$$

Gli autovettori $|\alpha_m\rangle$ costituiscono il proiettore $|\alpha_m\rangle\langle\alpha_m|$, mentre gli autovalori a_m sono i possibili risultati della misura dell'osservabile. Poichè ogni stato è dato da una sovrapposizione di stati, possiamo scrivere

$$|\theta\rangle = \sum_m c_m|\alpha_m\rangle$$

con $c_m = \langle\alpha_m|\theta\rangle$. La probabilità di ottenere la misura α_m dallo stato $|\theta\rangle$ è

$$P_m = |\langle\alpha_m|\theta\rangle|^2$$

mentre il valore medio di una misura sull'osservabile A vale

$$\langle A\rangle = \langle\theta|A|\theta\rangle$$

Matrice densità

La matrice densità ρ è un operatore sullo spazio di Hilbert H utilizzato per descrivere statisticamente lo stato di un sitema quantistico su H.
Se un sistema si trova in uno stato puro $|\varphi\rangle$, la matrice densità sarà

$$\rho = |\varphi\rangle\langle\varphi|$$

Nel caso in cui il sistema si trovi in una miscela di stati, ovvero quando si trovi nello stato $|\varphi_j\rangle$ con una certa probabilità p_j si ha

$$\rho = \sum p_j|\varphi_j\rangle\langle\varphi_j|$$

Postulati della meccanica quantistica

La meccanica quantistica basa i suoi principi nei seguenti postulati:

Postulato 1 Ad ogni sistema fisico isolato viene associato uno spazio di Hilbert H di dimensioni opportune sul corpo dei numeri complessi C,

chiamato spazio degli stati. In ogni istante della sua evoluzione il sistema è completamente specificato da uno stato $|\psi\rangle$, dato da un vettore unitario di H.

Postulato 2 L'evoluzione di un sistema quantistico isolato è descritto da un operatore unitario $\mathbf{U}$. Se $|\psi(t_0)\rangle$ è lo stato del sistema al tempo t_0, lo stato del sistema al tempo t è

$$|\psi(t)\rangle = \boldsymbol{U}|\psi(t_0)\rangle \qquad t > t_0 \tag{1.1}$$

dove $\boldsymbol{U} = \boldsymbol{U}(t_0, t)$ dipende soltanto da t_0 e t.

Postulato 3 Una misura su un sistema quantistico, inquadrato in uno spazio di Hilbert H, è ottenuta mediante un sistema di proiettori $\{\boldsymbol{\Pi_i},\ i \in M\}$. L'alfabeto M fornisce i possibili risultati della misura. Se immediatamente prima della misura il sistema si trova nello stato $|\psi\rangle$, la probabilità che la misura dia il risultato $m = i \in M$ è data da

$$P\left[m = i|\psi\right] = \langle\psi|\boldsymbol{\Pi}_i|\psi\rangle, \qquad i \in M \tag{1.2}$$

Se il risultato è $m = i$, dopo la misura il sistema si porta nello stato

$$|\psi_{post}\rangle = \frac{\boldsymbol{\Pi_i}|\psi\rangle}{\sqrt{\langle\psi|\boldsymbol{\Pi}_i|\psi\rangle}} \tag{1.3}$$

Postulato 4 Un sistema composto da due sottosistemi H_1 e H_2 va inquadrato in uno spazio di Hilbert H dato dal prodotto tensoriale dei due sottosistemi componenti

$$H = H_1 \otimes H_2$$

e quindi se $|\psi_1\rangle$ è uno stato di H_1 e $|\psi_2\rangle$ è uno stato di H_2 lo stato su cui si viene a trovare il sistema composito H è

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

Teorema di non clonazione

Una conseguenza importante del Postulato 2 che si verifica nella combinazione di sistemi quantistici prevede che alcune evoluzioni di questi sistemi siano impossibili, come ad esempio la copia, o clonazione, di uno stato quantistico. Consideriamo un sistema quantistico H che si trovi in uno stato $|\psi\rangle$, e si voglia copiare questo stato ad un altro sistema H_c, che si trova in un certo stato iniziale $|0\rangle$. Combinando insieme i due sistemi, si vuole passare dallo stato iniziale $|\psi\rangle \otimes |0\rangle$ allo stato $|\psi\rangle \otimes |\psi\rangle$, dove anche il sistema H_c si è posto nello stato $|\psi\rangle$. Deve perciò esistere un operatore tale per cui

$$\boldsymbol{U}(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

per ogni stato $|\psi\rangle$. Deve valere perciò

$$\boldsymbol{U}(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

con $|\psi\rangle \neq |\phi\rangle$. Quindi se esistesse un simile operatore, per la linearità del prodotto tensoriale rispetto al primo elemento, si avrebbe:

$$\boldsymbol{U}(\alpha|\psi\rangle + \beta|\phi\rangle) \otimes |0\rangle = \alpha|\psi\rangle \otimes |\psi\rangle + \beta|\phi\rangle \otimes |\phi\rangle \neq (\alpha|\psi\rangle + \beta|\phi\rangle) \otimes (\alpha|\psi\rangle + \beta|\phi\rangle)$$

Questo risultato è noto come **teorema di non clonazione**, il quale afferma che l'informazione quantistica non può essere copiata.

Il qu-bit

Vediamo ora il più elementare sistema quantistico, il *qu-bit*. Consideriamo due persone (per noi saranno Alice e Bob) che vogliono scambiarsi un messaggio. Per far ciò, utilizzano dei fotoni polarizzati, cioè, viene associato il valore 1 quando il fotone ha polarizzazione orizzontale, mentre viene associato il valore 0 quando ha polarizzazione verticale. In questo modo, quando Alice invia un fotone con polarizzazione verticale, Bob decifra uno 0, mentre se il fotone aveva polarizzazione orizzontale Bob decifra un 1. In questo caso siamo di fronte ad un classico bit. Nella meccanica quantistica un qu-bit, ovvero quantum bit, è un oggetto molto più ricco di un classico bit poichè, oltre agli stati 0 e 1, può assumere tutti i valori compresi tra loro. Il ruolo del qu-bit per le comunicazioni quantistiche è lo stesso ruolo che il bit ricopre per le comunicazioni classiche, cioè è la più piccola quantità utilizzabile per trasmettere un'informazione. Per descrivere matematicamente un qu-bit utilizziamo uno spazio di Hilbert H a due dimensioni, che ci permette di descrivere con un vettore un qualsiasi stato di polarizzazione. Come base di questo spazio scegliamo i vettori $|x\rangle$ per la polarizzazione orizzontale e $|y\rangle$ per la polarizzazione verticale. Il qu-bit assumerà la forma

$$|\Phi\rangle = \lambda|0\rangle + \mu|1\rangle$$

con i vettori della base ortonormali e con norma unitaria

$$\langle 0|0\rangle = \langle 1|1\rangle, \qquad \langle 0|1\rangle = 0$$

e λ e μ soddisfano la condizione di normalizzazione

$$|\lambda|^2 + |\mu|^2 = 1 \quad \rightarrow \quad ||\Phi||^2 = 1$$

Sperimentalmente, i metodi più utilizzati per generare qu-bit sono: la polarizzazione dei fotoni, lo spin degli elettroni, lo spin dei nuclei degli atomi

Teorema di indeterminazione di Heisenberg

Il principio di Heisenberg afferma l'impossibilità di effettuare una misura con precisione arbitraria su una coppia di grandezze fisiche, come la posizione e la quantità di moto di una particella. Tale incertezza è dovuta al fatto che in meccanica quantistica le particelle ha anche natura ondulatoria, non più solo puntiforme. Tralasciamo la dimostrazione di questo teorema [Bel06, par 4.1.3] e consideriamo il risultato nel caso in cui le quantità misurate siano la posizione e la quantità di moto, si ha

$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

dove Δx e Δp sono gli errori sulla posizione e sulla quantità di moto. Da questo risultato si nota che le due grandezze prese insieme non possono essere precise a piacere, ma la maggior precisione di una comporta un maggior errore per l'altra.

1.2 Entanglement

L'entanglement è un fenomeno quantistico molto importante, che si trova alla base della crittografia quantistica e di altre tecnologie, come i computer quantistici e il teletrasporto quantistico. Questo fenomeno, previsto dalla meccanica quantistica, consiste in un sistema di due particelle, nel quale il valore di una certa propietà misurabile assunto da una delle due particelle nel momento della misura, influenza immediatamente, senza alcun vincolo, il valore dell'altra, fornendo un preciso risultato correlato con la prima misura. Fu proprio su questa proprietà che nel 1935 Einstein, Podolsky, Rosen formularono il paradosso EPR [Ein35] in cui si voleva mostrare l'inconsistenza della meccanica quantistica. I tre scienziati partirono dall'ipotesi che la meccanica quantistica obbedisse ad alcuni principi: il principio di realtà (la possibilità di predire una misura con certezza), di completezza e di località. Affermarono che, presi due osservabili A e B non commutabili riferiti a due quantità fisiche, la misura su A porta alla certezza del risultato di B, senza che la misura di A influenzi la misura su B. La condizione di località non era in discussione, poichè se la misura su una particella poteva avere ripercussioni immediate sulla misura dell'altra, a qualsiasi distanza si trovino, la relatività verrebbe contradetta. Come può quindi, la meccanica quantistica essere completa? La mancanza di informazioni secondo loro si doveva risolvere aggiungendo alcune 'variabili nascoste' le quali dovevano contenere le informazioni mancanti. Successivamente il paradosso venne risolto con il teorema di Bell e con l'esperimento di Aspect sulla correlazione quantistica

[J.B64], [AA82], [AA81] . Bell con il suo teorema affermava che per una teoria quantistica nella quale sono presenti variabili nascoste e che assuma i principi di realtà e località, devono valere relazioni di disuguaglianza fra misure su particelle correlate che invece vengono violate dalla meccanica quantistica. Nel prossimo paragrafo vedremo la dimostrazione di ciò.

Caratterizzazione dell'entanglement

Consideriamo uno stato formato da due qubit, il primo appartenente allo spazio H_A con base $\{|0_A\rangle, |1_A\rangle\}$, il secondo allo spazio H_B con base $\{|0_B\rangle, |1_B\rangle\}$. Possiamo scrivere ad esempio $|00\rangle = |0_A \otimes 0_B\rangle$, con $\otimes$ prodotto tensoriale, o brevemente $|00\rangle = |0_A 0_B\rangle$. I possibili valori che possono assumere i qubit sono

$$|00\rangle = |0_A 0_B\rangle, \;\; |01\rangle = |0_A 1_B\rangle, \;\; |10\rangle = |1_A 0_B\rangle, \;\; |11\rangle = |1_A 1_B\rangle$$

Consideriamo ora un generico stato di H_A in forma normalizzata

$$|\varphi_A\rangle = \lambda_A |0_A\rangle + \mu_A |1_A\rangle, \quad |\lambda_A|^2 + |\mu_A|^2 = 1$$

e un generico stato di H_B sempre in forma normalizzata

$$|\varphi_B\rangle = \lambda_B |0_B\rangle + \mu_B |1_B\rangle, \quad |\lambda_B|^2 + |\mu_B|^2 = 1$$

Lo stato che si ottiene dai due precedenti è

$$\begin{aligned} |\varphi_A\rangle|\varphi_B\rangle &= \lambda_A\lambda_B|0_A 0_B\rangle + \lambda_A\mu_B|0_A 1_B\rangle + \mu_A\lambda_B|1_A 0_B\rangle + \mu_A\mu_B|1_A 1_B\rangle \\ &= \lambda_A\lambda_B|00\rangle + \lambda_A\mu_B|01\rangle + \mu_A\lambda_B|10\rangle + \mu_A\mu_B|11\rangle \end{aligned} \tag{1.4}$$

Si nota che gli stati $|\varphi_A\rangle|\varphi_B\rangle$ rappresentano solo un piccolo insieme degli stati dello spazio $H_A \otimes H_B$. Un generico stato di questo spazio ha la forma seguente

$$\begin{aligned} |\psi\rangle &= \alpha_{00}|0_A 0_B\rangle + \alpha_{01}|0_A 1_B\rangle + \alpha_{10}|1_A 0_B\rangle + \alpha_{11}|1_A 1_B\rangle \\ &= \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \end{aligned} \tag{1.5}$$

Affinchè lo stato $|\psi\rangle$ sia della forma $|\varphi_A\varphi_B\rangle$ dev'essere $\alpha_{00}\alpha_{11} = \alpha_{10}\alpha_{10}$. Consideriamo ora uno stato

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{1.6}$$

Lo stato $|\phi\rangle$ appartiene allo spazio $H_A \otimes H_B$ ma non è nella forma $|\varphi_A\varphi_B\rangle$, poichè

$$\alpha_{00} = \alpha_{11} = 0, \qquad \alpha_{01} = \alpha_{10} = \frac{1}{\sqrt{2}} \rightarrow \alpha_{00}\alpha_{11} \neq \alpha_{10}\alpha_{10}$$

Uno stato come 1.6 che non può essere scritto nella forma $|\varphi_A\varphi_B\rangle$ è chiamato stato *entangled*. Uno stato entangled è uno stato che non è possibile separare, ovvero non è possibile definire una coppia di stati $|\varphi_A\rangle$ $|\varphi_B\rangle$ tali per cui la loro composizione $|\varphi_A\varphi_B\rangle = |\phi\rangle$.

1.2.1 Stati non massimamente entangled

Uno stato non massimamente entangled è uno stato entangled definito come

$$|\psi\rangle = \frac{1}{\sqrt{1+|\epsilon|^2}}(|00\rangle + e^{i\phi}\epsilon|11\rangle)$$

con ϵ grado dell'entanglement. Se $\epsilon = 1$ lo stato si riconduce ad uno stato massimamente entangled. Nel paragrafo 3.6 vedremo un metodo per generare questa tipologia di stati.

1.2.2 Stati hyperentangled

L'entanglement di due particelle in più gradi di libertà viene chiamato hyperentanglement. Questa tecnica permette di sfruttare meglio i vantaggi offerti dalla meccanica quantistica. In questo modo si ha a disposizione uno spazio di Hilbert di maggiori dimensioni permettendo di creare nuovi test più efficaci per provare la non località della meccanica quantistica [Oh02]. Altri test sono stati eseguiti per la rivelazione completa dei quattro stati di Bell (3.36,3.37) [PK98] [YS11] e per migliorare la sicurezza nella QKD [Cha12]. Vediamo ora come si definisce uno stato hyperentangled [GV11]. Consideriamo due particelle A e B a n gradi di libertà, indicati con $\{a_j\}$ e $\{b_j\}$, con $j = 1, ..., n$. Ad ogni grado di libertà è associato uno spazio di Hilbert bidimensionale, con base $\{|0\rangle_{a_j}, |1\rangle_{a_j}$ per A, $\{|0\rangle_{b_j}, |1\rangle_{b_j}$ per B. Ogni particella, quindi, può essere vista come n qubits. Uno stato $|\Psi\rangle$ si definisce entangled-separabile se soddisfa la seguente condizione

$$\exists j \text{ tale che} \qquad |\Psi\rangle = |\Psi_1\rangle_{a_j I}|\Psi_2\rangle_{b_j J} \tag{1.7}$$

con $\{I,\ J\}$ partizione dell'insieme $T_j = \{a_1, b_1, ...a_n, b_n\}\backslash\{a_j, b_j\}$, $I \cup J = T_j$, $I \cap J = \emptyset$.
Uno stato si definisce *hyperentangled* in n gradi di libertà se è entangled-separabile in ogni suo grado di libertà e se non può essere scritto come uno stato misto che soddisfi 1.7.

1.2.3 Disuguaglianza di Bell

Mostriamo ora come nessuna teoria delle variabili nascoste può riprodurre tutte le previsioni della meccanica quantistica. Consideriamo uno stato entangled in polarizzazione (vedi paragrafo 3.5), definito da

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|V_1 H\rangle_2 - |H_1 V\rangle_2 \tag{1.8}$$

Utilizzando due lamine a $\lambda/2$ (4.3.4), una su ciascuna direzione dei fotoni, è possibile ruotare la polarizzazione del primo fotone lungo θ e la sua ortogonale θ', e del secondo lungo ϕ e la sua ortogonale ϕ':

$$\begin{aligned}
|\theta\rangle &= \cos(\theta)|H\rangle_1 + \sin(\theta)|V\rangle_1 \\
|\theta'\rangle &= -\sin(\theta)|H\rangle_1 + \cos(\theta)|V\rangle_1 \\
|\phi\rangle &= \cos(\phi)|H\rangle_2 + \sin(\phi)|V\rangle_2 \\
|\phi'\rangle &= -\sin(\phi)|H\rangle_2 + \cos(\phi)|V\rangle_2
\end{aligned}$$

Possiamo ora riscrivere 1.8 come [CG05]

$$\begin{aligned}
|\psi\rangle =& \frac{1}{\sqrt{2}}\{(\cos(\theta)\sin(\phi) - \sin(\theta)\cos(\phi))|\theta\rangle|\phi\rangle \\
&+ (\cos(\theta)\cos(\phi) + \sin(\theta)\sin(\phi))|\theta\rangle|\phi'\rangle \\
&- (\sin(\theta)\sin(\phi) + \cos(\theta)\cos(\phi))|\theta'\rangle|\phi\rangle \\
&- (\sin(\theta)\cos(\phi) - \cos(\theta)\sin(\phi))|\theta'\rangle|\phi'\rangle\} \\
=& \frac{1}{\sqrt{2}}\{\sin(\phi-\theta)|\theta\rangle|\phi\rangle + \cos(\phi-\theta)|\theta\rangle|\phi'\rangle \\
&- \cos(\phi-\theta)|\theta'\rangle|\phi\rangle - \sin(\theta-\phi)|\theta'\rangle|\phi'\rangle\}
\end{aligned} \tag{1.9}$$

Consideriamo due funzioni, la prima chiamata A che vale 1 se Alice misura il primo fotone con polarizzazione parallela a $|\theta\rangle$, mentre vale -1 se la sua polarizzazione è parallela a $|\theta'\rangle$. La seconda funzione B di conseguenza, vale 1 se Bob misura il secondo fotone con polarizzazione parallela a $|\phi\rangle$, mentre vale -1 se è parallela a $|\phi'\rangle$. Il prodotto AB vale quindi 1 per le coppie $|\theta\rangle|\phi\rangle$ e $|\theta'\rangle|\phi'\rangle$ mentre -1 per le coppie $|\theta'\rangle|\phi\rangle$ e $|\theta\rangle|\phi'\rangle$.

Assumendo il principio di località, introduciamo le variabili nascoste. Le misure effettuate da Alice e Bob risulteranno legate al valore della variabile aleatoria λ (variabile nascosta) appartenente allo spazio di probabilità Λ con distribuzione $\rho(\lambda)$. Questa variabile definisce perciò la correlazione tra le due misure effettuate, cioè le funzioni A e B sono dipendenti sia dalla rispettiva

posizione della lamina (ovvero la proiezione sugli angoli $\theta,\ \theta^{'}$ o $\phi,\ \phi^{'}$) sia dal valore assunto da λ. Poichè abbiamo assunto per vero il principio di località, la misura che effettuiamo su di un fotone, non influenza la misura dell'altro. La funzione di correlazione è data da

$$C_{VN}(\theta,\phi) = \int A(\theta,\lambda)B(\theta,\lambda)\rho(\lambda)d\lambda \tag{1.10}$$

dove il pedice VN sta per variabili nascoste.

Se ora consideriamo una semplice funzione S, dove $X_1,\ X_1^{'},\ X_2,\ X_2^{'} = \pm 1$

$$\begin{aligned} S &= X_1X_2 + X_1X_2^{'} + X_1^{'}X_2 - X_1^{'}X_2^{'} \\ &= X_1(X_2 + X_2^{'}) + X_1^{'}(X_2 - X_2{'}) = \pm 2 \end{aligned} \tag{1.11}$$

Poniamo ora $X_1 = A(\theta,\lambda),\ X_1^{'} = A(\theta^{'},\lambda),\ X_2 = B(\phi,\lambda),\ X_2^{'} = B(\phi^{'},\lambda)$, moltiplichiamo per $\rho(\lambda)$ e integriamo su λ, otteniamo

$$-2 \leq C_{VN}(\theta,\phi) + C_{VN}(\theta,\phi^{'}) + C_{VN}(\theta^{'},\phi) - C_{VN}(\theta^{'},\phi^{'}) \leq 2 \tag{1.12}$$

Questa disuguaglianza è nota come disuguaglianza di Clauser, Horne, Shimony e Holt ([Hol69]), e viene utilizzata al posto di quella inizialmente introdotta da Bell. Vediamo ora cosa succede per la meccanica quantistica.

Calcoliamo l'aspettazione del prodotto AB nel caso in cui i due fotoni appartengano allo stato 1.8:

$$E[AB] = P(|\theta\rangle|\phi\rangle) + P(|\theta^{'}\rangle|\phi^{'}\rangle) - P(|\theta^{'}\rangle|\phi\rangle) - P(|\theta\rangle|\phi^{'}\rangle) \tag{1.13}$$

Le probabilità in 1.13 si ricavano da 1.9

$$P(|\theta\rangle|\phi\rangle) = |\langle\psi|\theta\rangle|\phi\rangle|^2 = \frac{1}{2}\sin^2(\phi-\theta)$$

$$P(|\theta^{'}\rangle|\phi^{'}\rangle) = |\langle\psi|\theta^{'}\rangle|\phi^{'}\rangle|^2 = \frac{1}{2}\sin^2(\theta-\phi)$$

$$P(|\theta^{'}\rangle|\phi\rangle) = |\langle\psi|\theta^{'}\rangle|\phi\rangle|^2 = \frac{1}{2}\cos^2(\theta-\phi)$$

$$P(|\theta\rangle|\phi^{'}\rangle) = |\langle\psi|\theta\rangle|\phi^{'}\rangle|^2 = \frac{1}{2}\cos^2(\theta-\phi)$$

ottenendo

$$\begin{aligned} E[AB] &= \sin^2(\theta-\phi) - \cos^2(\theta-\phi) \\ &= 1 - 2cos^2(\theta-\phi) \\ &= -\cos(2(\theta-\phi)) \end{aligned} \tag{1.14}$$

Notiamo che $E[AB] = E[A(\theta)B(\phi)] = C(\theta, \phi)$

Andiamo ora a calcolare l'equazione 1.12 scegliendo come angoli $\theta = 0,\ \theta' = \pi/4,\ \phi = \pi/8,\ \phi' = -\pi/8$

$$S = C(\theta, \phi) + C(\theta, \phi') + C(\theta', \phi) - C(\theta', \phi') = 2\sqrt{2} \tag{1.15}$$

Come si osserva il risultato di 1.15 è chiaramente fuori dai limiti di 1.12 ottenuta nel caso di teoria delle variabili nascoste. Questa violazione indica che la meccanica quantistica non può essere una teoria delle variabili nascoste. La conferma sperimentale di ciò si ha soprattutto grazie ad Aspect [AA82; AA81], il quale attraverso alcuni esperimenti ha verificato la disuguaglianza di Bell, mostrando come la meccanica quantistica contrasti in modo eclatante con la realtà quotidiana.

1.2.4 Interferenza con stati entangled

È interessante notare cosa succede quando si misura su uno stato entangled piuttosto che uno stato generato ad-hoc, costituito da una sorgente classica che generi coppie $|HV\rangle$ e $|VH\rangle$ con uguale probabilità. Per capire meglio questa differenza, consideriamo lo stato entangled

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) \tag{1.16}$$

Effettuando delle misure sulla base $\{H, V\}$ si ottiene, per lo stato $|HV\rangle$ (lo stesso si ottiene con lo stato $|VH\rangle$)

$$P_{HV} = \langle HV|\rho|HV\rangle = \langle HV|\Phi\rangle\langle\Phi|HV\rangle = |\langle HV|\Phi\rangle|^2 = \frac{1}{2}\left|\frac{1}{2} + \frac{1}{2}\right|^2 = \frac{1}{2}$$

mentre per $|HH\rangle$ (o $|VV\rangle$) si ha

$$P_{HH} = \langle HH|\rho|HH\rangle = \langle HH|\Phi\rangle\langle\Phi|HH\rangle = |\langle HH|\Phi\rangle|^2 = \frac{1}{2}|0|^2 = 0$$

Consideriamo ora il caso della sorgente classica. Per una tale sorgente si ha

$$\rho' = \frac{1}{2}(|HV\rangle\langle HV| + |VH\rangle\langle VH|)$$

Ripetendo le stesse misure fatte in precedenza, ma con il nuovo sistema, otteniamo

$$P'_{HV} = \langle HV|\rho'|HV\rangle = \frac{1}{2}$$

e

$$P'_{HH} = \langle HH|\rho'|HH\rangle = 0$$

In questo caso non si nota alcuna differenza fra i due. Vediamo ora, invece, cosa succede quando effettuiamo la misura su un'altra base ortogonale, ovvero sulla base $\{+,-\}$. Lo stato $|+\rangle$ è definito come

$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$$

, mentre lo stato $|-\rangle$ è definito come

$$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$$

Calcoliamo la probabilità di ottenere lo stato $|+-\rangle$ (lo stesso vale per $|-+\rangle$)

$$P_{+-} = \langle +- |\rho| +-\rangle = \langle +- |\Phi\rangle\langle\Phi| +-\rangle = |\langle +- |\Phi\rangle|^2 = \frac{1}{2}\left|\frac{1}{2} + \frac{1}{2}\right|^2 = \frac{1}{2}$$

Nella misura di $|++\rangle$ (lo stesso vale per $|--\rangle$) si ha invece

$$P_{++} = \langle ++ |\rho| ++\rangle = \langle ++ |\Phi\rangle\langle\Phi| ++\rangle = |\langle ++ |\Phi\rangle|^2 = \frac{1}{2}\left|\frac{1}{2} - \frac{1}{2}\right|^2 = 0$$

Spostandoci dallo stato $|+-\rangle$ allo stato $|++\rangle$ la probabilità passa da un valore di massimo ad un valore di minimo, ovvero gli stati della base $\{+,-\}$ interferiscono. Nel secondo caso invece presi uno qualsiasi degli stati $|++\rangle$ $|+-\rangle$ $|-+\rangle$ o $|--\rangle$ la probabilità di ottenere uno degli stati precedenti è

$$\begin{aligned} P'_{++} =& \langle ++ |\rho'| ++\rangle = \frac{1}{2}(\langle ++ |HV\rangle\langle HV| ++\rangle + \langle ++ |VH\rangle\langle VH| ++\rangle) \\ =& \frac{1}{2}\left(\frac{1}{2} + \frac{1}{2}\right) = \frac{1}{4} \end{aligned}$$

dove $++$ può essere sostituito con $+-$, $--$, $-+$. In questo caso se ci spostiamo dallo stato $|++\rangle$ ad uno qualsiasi degli stati $|+-\rangle$ $|-+\rangle$ e $|--\rangle$, non otteniamo interferenza. Questo risultato è molto importante, perchè ci permette di capire se stiamo effettivamente osservando uno stato entangled.

1.2.5 Visibilità

Per stimare la qualità dell'interferenza si può utilizzare la seguente formula:

$$V = \frac{I_{MAX} - I_{min}}{I_{MAX} + I_{min}}$$

dove I_{MAX} è l'intensità nella posizione di massimo e I_{min} nel minimo. Nel nostro caso la formula viene riscritta in questo modo

$$V = \frac{N_{MAX} - N_{min}}{N_{MAX} + N_{min}} \tag{1.17}$$

dove N_{MAX} sono il numero delle coppie rivelate (coincidenze) nella posizione di massimo e N_{min} nel minimo. Se $V = 1$ l'interferenza è massima, in quanto c'è una perfetta distinzione tra N_{MAX} e N_{min}, mentre se $V = 0$ N_{MAX} e N_{min} sono uguali, ovvero non c'è interferenza.

1.2.6 Fidelity

La *fidelity* $F(\rho, \sigma)$ di due stati quantistici è la misura di quanto essi siano simili tra di loro.
Se $|\phi\rangle$ e $|\varphi\rangle$ sono stati puri, si ha semplicemente

$$F(|\phi\rangle\langle\phi|, |\varphi\rangle\langle\varphi|) = |\langle\phi|\varphi\rangle|^2$$

Nel caso di stati misti, invece si ha che la fidelity è data da

$$F(\rho, \sigma) = Tr\left(\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}\right)^2$$

dove ρ e σ sono le matrici densità dei due stati. La fidelity può essere utilizzata per misurare quanto lo stato generato sperimentalmente assomigli a quello che si vorrebbe ottenere.

1.2.7 Tangle

Il tangle è una misura del grado di entanglement di un sistema. Se questa misura è pari a 0 siamo nel caso di stati separabili, mentre se vale 1 gli stati sono massimamente entangled.
La definizione di questa misura è apparsa nell'articolo di Coffman, Kundu e Wootters [Woo00]. Definiamo la matrice densità spin-flipped come:

$$\widetilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$$

dove ρ^* è la matrice densità complessa coniugata dello stato da misurare, e

$$\sigma_y = \begin{matrix} 0 & -i \\ i & 0 \end{matrix}.$$

Sia ora $R = \rho\widetilde{\rho}$ e siano λ_1, λ_2, λ_3, λ_4 la radice quadrata degli autovalori di R, in ordine decrescente. Il tangle si calcola come

$$T = \max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\}$$

Capitolo 2

Crittografia classica e crittografia quantistica

2.1 Cenni storici sulla crittografia

Il desiderio di comunicare segretamente è molto antico, già in molte società antiche, come in Mesopotamia, Egitto, Cina erano presenti metodi di cifratura, ma i particolari che hanno portato alla nascita di questi modi di scrittura segreta sono sconosciuti. Gli esempi di comunicazioni cifrate più antiche provengono da alcuni geroglifici egiziani (attorno al 2500 a.C.). Successivamente, in mesopotamia sono state ritrovate incisioni cifrate, probabilmente con lo scopo di proteggere informazioni di carattere commerciale. Nell'antichità i pionieri della crittografia in Europa erano gli Spartani, nemici per definizione dei Greci. Attorno al 400 a.C. i comandanti dell'esercito di Sparta per comunicare tra di loro utilizzavano un dispositivo, conosciuto come *scitala*. Questo era un bastone affusolato attorno al quale veniva avvolto un nastro di pergamena o di pelle. Le parole del messaggio venivano poi scritte lungo il bastone, inserendo una lettera per ogni rivoluzione. Per leggere il messaggio era necessario riavvolgere il nastro attorno ad un altro bastone con la stessa forma. Successivamente, nell'antica Roma, Giulio Cesare utilizzo, come metodo di cifratura, la sostituzione delle lettere. Ogni lettera del messaggio veniva rimpiazzata dalla lettera che la seguiva di un numero fisso di posizioni. Durante il medioevo passi importanti furono compiuti da parte degli arabi, soprattutto da Al-Kindi, il quale inventò un metodo chiamato analisi delle frequenze per violare i cifrari a sostituzione (come quello di Cesare): tutti i cifrari, ad eccezione del cifrario polialfabetico di Leon Battista Alberti, erano vulnerabili a questa tecnica di crittanalisi. Fino a qualche decina di anni fa, i metodi di crittografia complessi erano prevalentemente

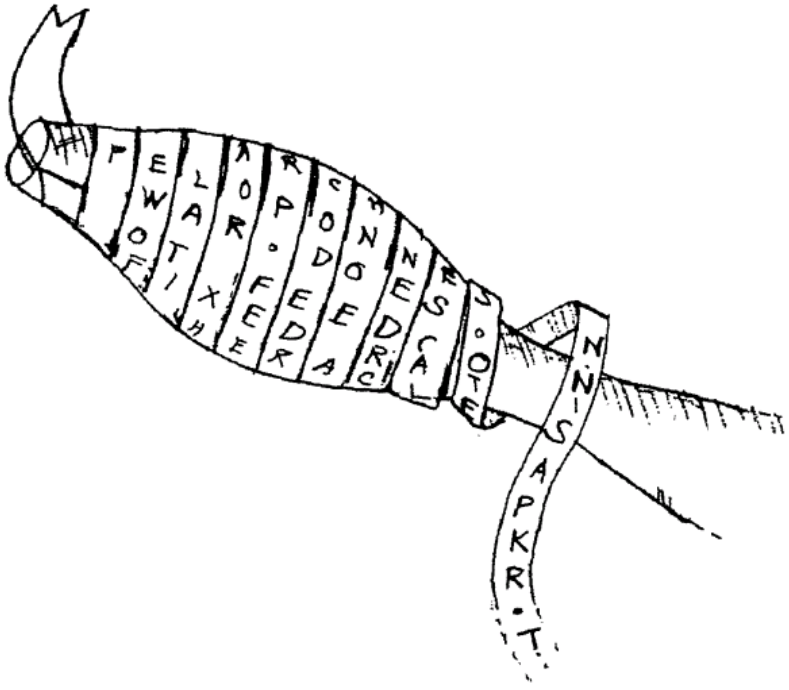


Figura 2.1: Scitala spartana

sviluppati ed utilizzati da parte delle forze militari, poichè solo loro potevano disporre delle risorse per costruire sofisticati sistemi elettro-meccanici, come ad esempio ENIGMA, strumento utilizzato nella Seconda Guerra Mondiale dai tedeschi violato dal polacco Rejewski nel 1932. Venne creato anche il primo computer programmabile, il Colossus, per aiutare gli alleati nella crittanalisi dei messaggi nemici. I due metodi base della crittografia utilizzati ancora oggi sono quelli presenti nella scitala e nel cifrario di Cesare, ovvero la trasposizione e la sostituzione. Nella trasposizione il messaggio da trasmettere viene riscritto facendo una permutazione delle lettere. Nella sostituzione invece, le lettere del messaggio vengono sostituite da altre lettere, numeri o simboli. Prima delle moderne tecniche di cifratura, la sicurezza di un cifrario dipendeva dalla sicurezza di tutto il processo, mentre oggi si utilizzano cifrari i cui algoritmi sono ben conosciuti a tutti, senza compromettere la sicurezza della comunicazione. In questi cifrari, ciò che deve rimanere segreto per mantenere l'integrità del messaggio cifrato, è la chiave, un parametro utilizzato dall'algoritmo di cifratura. Questa viene fornita insieme al messaggio, all'algoritmo di cifratura, e in seguito, con il messaggio cifrato, all'algoritmo di decifratura:

$$\hat{E}_k(M) = C \;\rightarrow\; \hat{D}_k(C) = M$$

dove M è il messaggio da cifrare, C è il messaggio cifrato, E e D sono le operazioni di cifraggio e decifraggio. Come detto in precedenza, la sicurezza in questo tipo di crittografia, dipende totalmente dalla sicurezza della chiave che deve essere il più possibile lunga e casuale. Prendiamo come esempio l'algoritmo introdotto da Vernam, il one-time pad. Ad ogni lettera o simbolo dell'alfabeto lungo N viene associato un numero, da 0 a $N-1$. Per ottenere il messaggio cifrato, si prende il numero associato ad ogni lettera o simbolo del messaggio e si fa la somma modulo N con un numero che viene scelto a caso tra 0 e $N-1$. Possiamo scrivere il procedimento così:

$$P \oplus_N k = C \ \rightarrow \ C \ominus_N k = M$$

In seguito Claude Shannon dimostrò che se la chiave è lunga come il messaggio ed inoltre è veramente una chiave casuale e non più riutilizzata, allora il one-time pad è perfettamente sicuro. Rimane tuttavia un problema molto importante, cioè come condividere la chiave in modo sicuro tra l'emettitore e ricevente. Per la trasmissione del messaggio criptato non ci sono particolari requisiti di sicurezza riguardo al canale, mentre, quando i due utenti devono scambiare la chiave, allora questo scambio di informazioni deve avvenire attraverso un canale molto sicuro. Quindi, perchè utilizzare un canale sicuro per trasmettere una chiave lunga come il messaggio quando si potrebbe utilizzare lo stesso canale sicuro per trasmettere il messaggio? Una soluzione a questo problema è la crittografia a chiave pubblica. Questo sistema non prevede lo scambio di una chiave ma si basa sull'utilizzo di due chiavi, una pubblica, conosciuta a molti e utilizzata per criptare il messaggio, e una privata, conosciuta solo da una persona utilizzata per decifrare il messaggio. In questo modo viene superato l'ostacolo della distribuzione della chiave, ma la sicurezza si basa sulla difficoltà di recuperare la chiave privata da quella pubblica, a causa di difficili operazioni matematiche quali la fattorizzazione di grandi numeri interi. Questo vuol dire che con l'avvenire di tecnologie più avanzate e con migliori procedure matematiche la soluzione di questi problemi non sarà più difficile come oggi. Una seconda soluzione è la crittografia quantistica. A differenza della crittografia classica, la crittografia quantistica fornisce una perfetta sicurezza in quanto questa è basata su leggi fisiche invece che sulla difficoltà computazionale di risolvere fattorizzazioni complesse.

2.2 Crittografia quantistica

Il problema dello scambio della chiave nella crittografia classica può essere risolto utilizzando le proprietà della meccanica quantistica, offrendo un'al-

Stato	Bit	Polarizzazione fotoni
$\|0\rangle$	0	Orizzontale H
$\|1\rangle$	1	Verticale V
$\|+\rangle$	0	+ 45°
$\|-\rangle$	1	- 45°

Tabella 2.1: Codifica stato-bit BB84

ternativa all'utilizzo della distribuzione della chiave privata. In meccanica quantistica lo scambio di una chiave condivisa avviene sempre in modo sicuro, infatti, se un utente esterno si inserisce nel canale per ottenere informazioni sulla chiave Alice e Bob riescono ad accorgersene, poichè la comunicazione tra di loro verrebbe disturbata. Vediamo ora alcuni protocolli che ci permetteranno di comprendere meglio la crittografia quantistica

2.2.1 Protocollo BB84

In questo protocollo Alice e Bob necessitano di due canali, uno quantistico, dove Alice invierà i qu-bit preparati negli stati $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, i quali possono essere rappresentati da fotoni con polarizzazioni orizzontali ($|0\rangle$), verticali ($|1\rangle$), a 45° ($|+\rangle$) o a $-45°$ ($|-\rangle$), e un canale classico. Ad ogni stato delle basi $\{|0\rangle, |1\rangle\}$ e $\{|+\rangle, |-\rangle\}$ può essere associato il valore di un bit, 1 o 0, come mostrato in tabella 2.1

Il primo passo del protocollo consiste nella scelta da parte di Alice dei bit casuali da trasmettere e della base, sempre scelta casualmente, da utilizzare per la trasmissione dei qubit. Ad esempio per trasmettere il bit 0 può scegliere se utilizzare la base HV e quindi trasmettere un fotone con polarizzazione orizzontale, oppure la base $+-$, trasmettendo un fotone con polarizzazione a 45°. In ricezione Bob effettua una misura sul fotone ricevuto, scegliendo a caso una base e ottenendo come risultato della misura un bit. Terminato l'invio di qubit Bob invia ad Alice, attraverso il canale classico, le basi utilizzate per la codifica, mentre Alice invia le basi utilizzate per codificare i bit. A questo punto vengono scartati tutti i bit ricevuti per i quali sono state scelte basi diverse da parte di Alice e Bob. Infatti, se Alice invia uno 0 codificato con lo stato $|0\rangle$, Bob può effettuare una sola misura sul qubit scegliendo la base HV o $+-$ (principio di indeterminazione per misure incompatibili par.1.1). Se viene scelta la base sbagliata, Bob ha una probabilità del 50% di ottenere un 1 o uno 0, cioè la misura fornisce un risultato casuale. In questo modo anche un attaccante in grado di intercettare la comunicazione, scegliendo la base

Bit casuali Alice	0	1	1	0	0	0	0	1	1	0	1
Base casuale Alice	×	×	+	×	+	×	×	+	×	+	+
Pol. dei fotoni Alice	↗	↘	↑	↗	→	↗	↗	↑	↘	→	↑
Base casuale misura Bob	×	+	×	+	+	×	+	×	×	+	×
Pol. fotoni misura Bob	↗	→	↘	↑	→	↗	→	↘	↘	→	↘
Bit Bob	0	0	1	1	0	0	0	1	1	0	1

Tabella 2.2: Esempio protocollo BB84

sbagliata otterrebbe un risultato casuale. Inoltre, sempre per il principio di indeterminazione, se l'attaccante intercettasse i qubit, modificherebbe il risultato della misura effettuata da Bob, anche nel caso in cui venisse scelta la base corretta. Inoltre, l'attaccante non potrebbe neppure duplicare il qubit, poichè è vietato dal teorema di non clonazione(par.1.1). Dopo lo scarto dei bit ottenuti con basi diverse sia Alice che Bob possiederanno la stessa chiave segreta. Se le due chiavi non sono uguali, significa che c'è stato l'intervento di una spia, quindi la chiave non è sicura.

2.2.2 Protocollo di Ekert

Questo protocollo, introdotto nel 1991 da Artur Ekert [Eke91], si basa sull'entanglement quantistico (vedi paragrafo 1.2). Lo scambio delle informazioni avviene attraverso la trasmissione di fotoni *entangled* da parte di una sorgente che si trova nel mezzo tra Alice (mittente) e Bob (destinatario). Lo stato preparato dalla sorgente è uno stato entangled del tipo $|\psi\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$, cioè se il primo fotone è misurato con polarizzazione H, il secondo avrà polarizzazione V e viceversa. Come abbiamo visto nel paragrafo 1.2.4, questo è valido anche nel caso in cui venga scelta per la misura la base $\{+, -\}$, ovvero sulle polarizzazioni a 45° e -45°, per la quale si ha $|\psi\rangle = \frac{1}{\sqrt{2}}(|+,-\rangle + |-,+\rangle)$. Facciamo ora un piccolo esempio. Se la misura sulla coppia generata viene effettuata da Alice utilizzando un polarizzatore verticale e da Bob utilizzando un polarizzatore orizzontale, vedranno entrambi sempre lo stesso risultato, cioè o entrambi vedono passare il fotone (la coppia misurata era H, V) o entrambi non vedono passare niente (in questo caso la coppia misurata era

V, H). Questo succede anche nel caso in cui il polarizzatore di Alice sia ruotato a 45° e quello di Bob a -45°.Diversamente, quando i due polarizzatori sono scelti entrambi con la stessa polarizzazione, i risultati saranno opposti, o solo Alice vede passare il fotone, o solo Bob vede passare il fotone. Alice

Alice		Bob	
H	↗	V	↘
1			0
	0	1	
1		1	
0			1
	0		0
	1		1
	0	1	
1			0
0		0	
1			1
	0		0
0			0
1		1	
	1		1
1		1	
0		0	
0			0

(a) Misure effettuate da Alice e Bob. Sono evidenziate in grigio le misure in cui sono state utilizzate polarizzazioni non ortogonali

Alice		Bob	
H	↗	V	↘
1		1	
	0		0
	1		1
0		0	
	0		0
1		1	
	1		1
1		1	
0		0	

(b) Risultati delle misure dopo aver eliminato le misure diverse

Tabella 2.3: Protocollo Ekert

e Bob inizialmente si accordano su quali basi effettuare le misure (nel nostro caso scegliamo per Alice H e $+$, per Bob V e $-$). Tali basi verranno scelte casualmente nel momento della lettura, ed entrambi dovranno tenere traccia di quale stato hanno utilizzato per la misura. Inoltre si considera di aver ricevuto 0 quando la misura viene eseguita sulla base $\{H, V\}$, 1 quando viene eseguita sulla base $\{+, -\}$. Dopo aver effettuato un numero sufficiente di misure, Alice e Bob comunicano pubblicamente le basi utilizzate, che possono ora essere note anche ad un eventuale attaccante. Si procede con l'elimina-

zione dei casi in cui le misure sono state eseguite con basi diverse. Come si fa a capire se un attaccante sia riuscito ad intromettersi e a recuperare informazioni? Per risolvere questo punto, Alice e Bob devono condividere pubblicamente alcuni risultati (appartenenti alla tabella 2.3b), per verificare se sono coincidenti. Naturalmente i risultati scambiati pubblicamente non sono più utilizzabili.
Se la spia interviene effettuando una misura perturba la correlazione tra le misure effettuate da Alice e Bob. Infatti, l'esito delle misure di Alice e Bob sono casuali, con probabilità 0.5 per ciascun caso, però, nel caso in cui Alice scelga di effettuare una misura H o $+$ e Bob rispettivamente V o $-$ si ha, con probabilità pari a 1, lo stesso risultato. L'effetto della spia non è altro che quello di abbassare quest'ultima probabilità. Per questo, scambiando alcuni risultati si può vedere se la correlazione perfetta è venuta meno, permettendo di capire se è avvenuto un attacco.

2.2.3 Protocollo B92

Questo protocollo è una variante del BB84. La principale differenza è l'utilizzo di due soli stati di polarizzazione non ortogonali. Vediamo brevemente

Bit	Alice	Bob
0	$\|H\rangle$	$\|-\rangle$
1	$\|+\rangle$	$\|V\rangle$

Tabella 2.4: Codifica bit-stato B92

le varie fasi di questo protocollo. Per prima cosa Alice sceglie la sequenza casuale di bit da trasmettere, poi codifica i bit secondo la tabella 2.4 e trasmette i fotoni polarizzati. Quando Bob riceve un fotone, effettua casualmente una delle due misure (polarizzazione V o $-45°$) e salva il risultato nel caso in cui abbia rivelato un fotone (se Alice invia un fotone con polarizzazione H e Bob effettua una misura su V non vedrà alcun segnale, se invece usa la base $-45°$ allora Bob rivela uno 0 con probabilità 0.5). Al termine Bob comunica pubblicamente ad Alice le posizioni in cui ha rivelato un fotone. In questo modo Alice scarta tutti bit non ricevuti da Bob, ottenendo la stessa sequenza di bit di Bob. Questo protocollo tuttavia, è vulnerabile ad un attacco di tipo USD, che permette ad un attaccante di recuperare informazioni sfruttando i punti deboli della realizzazione pratica del sistema. In questa tesi verrà testato un protocollo derivato dal B92, resistente ad un attacco tipo USD, dove l'attaccante è in grado di distinguere senza errori una frazione degli stati inviati da Alice e, per questa frazione di stati, prepara il corrispondente

stato da inviare a Bob in modo da farglielo ricevere senza errori. Se non rivela nulla, non invia nulla. Entriamo nel dettaglio di questo protocollo che chiamiamo *us-B92*[GM11].

Protocollo us-B92

I qubit codificati da Alice assumono la forma

$$|\varphi_j\rangle = \beta|H\rangle - (-1)^j\alpha|V\rangle \tag{2.1}$$

e il loro ortogonale

$$|\overline{\varphi}_j\rangle = \alpha|H\rangle + (-1)^j\beta|V\rangle \tag{2.2}$$

dove $J = \{0, 1\}$ sono i bit, e

$$\beta = cos(\theta/2), \qquad \alpha = sin(\theta/2) \tag{2.3}$$

con $0 < \theta < \pi/2$. La base $\pm$ è legata alla base $\{H, V\}$ dalla relazione

$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{2.4}$$

Come nel protocollo B92, Alice sceglie casualmente i bit j da inviare, questa volta però codificati negli stati $|\varphi_j\rangle$ (che sono sempre non ortogonali tra loro). A sua volta Bob misura gli stati per decodificarli, usando gli stati della base $\boldsymbol{B}_k = \{|\varphi_k\rangle, |\overline{\varphi}_k\rangle\}$, con $k = \{0, 1\}$. Se Bob rivela lo stato $|\overline{\varphi}_k\rangle$ (cioè fa una misura con esito positivo su quello stato) allora decodifica il bit come $j = k \oplus 1$, marcandolo come *conclusivo*. Se invece rivela lo stato $|\varphi_k\rangle$, Bob non può avere la certezza dello stato preparato da Alice, e segna la misura come *non conclusiva*. Ad esempio, se Bob rivela lo stato $|\varphi_0\rangle$ non può sapere se Alice aveva preparato lo stato $|\varphi_0\rangle$ o $|\varphi_1\rangle$ poichè $|\langle\varphi_0|\varphi_0\rangle|^2 \neq 0$ $|\langle\varphi_0|\varphi_1\rangle|^2 \neq 0$, cioè hanno entrambe una probabilità diversa da 0 di essere individuati, impedendo a Bob di determinare deterministicamente lo stato. Per prevenire attacchi di tipo USD, Alice trasmette a Bob con probabilità $1-p$ gli stati visti precedentemente, mentre con probabilità $p << 1$ altri due stati. Questi ultimi stati non portano informazione e sono $|s_1\rangle = |0_x\rangle$ con probabilità $(p \cdot \beta^2)$ e $|s_2\rangle = |1_x\rangle$ con probabilità $(p \cdot \alpha^2)$, con α e β definiti in 2.3. In questo modo un attaccante esterno non è in grado di distinguere la matrice di densità relativa agli stati che portano informazione da quella degli stati che non portano informazione. Infatti si ha

$$\rho_A = (|\varphi_0\rangle\langle\varphi_0| + |\varphi_1\rangle\langle\varphi_1|)/2 = \beta^2|0_x\rangle\langle 0_x| + \alpha^2|1_x\rangle\langle 1_x| = (|s_1\rangle\langle s_1| + |s_2\rangle\langle s_2|)$$

Protocollo ent-B92

Questo protocollo può essere realizzato utilizzando uno stato non massimamente entangled distribuito tra Alice e Bob. Chiamiamo questo nuovo protocollo ent-B92. Infatti Alice eseguendo una misura sullo stato

$$|\Phi\rangle_{ab} = \frac{1}{\sqrt{2}}(|+\rangle_a|\varphi_0\rangle_b + |-\rangle_a|\varphi_1\rangle_b) = \beta|H\rangle_a|H\rangle_b - \alpha|V\rangle_a|V\rangle_b \tag{2.5}$$

con la base $\pm$, proietta lo stato di Bob in $|\varphi_0\rangle$ e $|\varphi_1\rangle$ con uguale probabilità. Invece, se utilizza la base $\{H, V\}$, proietterà lo stato di Bob su $|H\rangle$ con probabilià β^2, e su $|V\rangle$ con probabilità α^2. In questo modo, se Alice deve inviare uno stato non informativo, le basta eseguire una misura con la base $\{H, V\}$, in questo modo Bob riceverà uno stato non informativo (con le giuste probabilità). Se invece vuole inviare uno stato informativo, le basta eseguire una misura con la base $\pm$. Questa realizzazione si riduce al protocollo usB92 se i bit ottenuti quando Alice misura nella base $\pm$ si considerano come bit della chiave segreta, mentre i bit ottenuti con la base $\{H, V\}$ come bit di controllo contro attacchi USD.

Utilizzando lo stato 2.5 è possibile eseguire delle misure per testare la proprietà di realismo locale. Nel caso in cui Alice e Bob utilizzino un solo canale per la misura, si deve utilizzare la disuguaglianza introdotta da Clauser e Horne, che deriva da 1.12:

$$\begin{aligned} S_{CH} = {} & P(a_1, b_1) + P(a_0, b_1) + P(a_1, b_0) \\ & - P(a_0, b_0) - P(a_1) - P(b_1) \leq 0 \end{aligned} \tag{2.6}$$

dove $P(a_i, b_j)$ è la probabilità congiunta che Alice (Bob) riveli lo stato $|a_i\rangle$ ($|b_j\rangle$), mentre $P(a_i)$ ($P(b_j)$) la probabilità che Alice (Bob) riveli lo stato $|a_i\rangle$ ($|b_j\rangle$). La probabilità $P(a_i)$ si può riscrivere come $P(a_i) = P(a_i, b_j) + P(a_i, \overline{b}_j)$, ottenendo la seguente disuguaglianza, dovuta ad Hardy:

$$S_H = P(a_1, b_1) - P(\overline{a}_0, b_1) - P(a_1, \overline{b})_0 - P(a_0, b_0) \leq 0 \tag{2.7}$$

Mostriamo ora che, scegliendo alcuni stati, si ottengono valori di S_H che violano la disuguaglianza, ovvero maggiori di 0. Per Alice si sono scelti gli stati

$$|a_0\rangle = |+\rangle \qquad |a_1\rangle = |V\rangle, \tag{2.8}$$

mentre per Bob

$$|b_0\rangle = |\overline{\varphi}_0\rangle \qquad |b_1\rangle = |\overline{\varphi}_1\rangle \tag{2.9}$$

Calcoliamo ora il valore di S_H

$$\begin{aligned}
P(a_1, b_1) &= |\langle V|\langle\overline{\varphi}_1|\Phi\rangle|^2 = sin^2(\theta/2)|\langle\overline{\varphi}_1|V\rangle|^2 \\
&= sin^2(\theta/2)cos^2(\theta/2) \\
P(a_1, \overline{b}_0) &= |\langle V|\langle\varphi_0|\Phi\rangle|^2 = sin^2(\theta/2)|\langle\varphi_0|V\rangle|^2 \\
&= sin^4(\theta/2) \\
P(\overline{a}_0, b_1) &= |\langle -|\overline{\varphi}_1|\Phi\rangle|^2 \\
&= \frac{1}{2}(cos(\theta/2)sin(\theta/2) - sin(\theta/2)cos(\theta/2))^2 = 0 \\
P(a_0, b_0) &= |\langle +|\overline{\varphi}_0|\Phi\rangle|^2 \\
&= \frac{1}{2}(cos(\theta/2)sin(\theta/2) - sin(\theta/2)cos(\theta/2))^2 = 0
\end{aligned} \tag{2.10}$$

$$\begin{aligned}
S_H &= sin^2(\theta/2)cos^2(\theta/2) - sin^4(\theta/2) = \\
&= sin^2(\theta/2)(cos^2(\theta/2) - sin^2(\theta/2)) = \\
&= \left(\frac{1 - cos(\theta)}{2}\right)(2cos^2(\theta/2) - 1) = \frac{1}{2}\left[1 - cos(\theta)\right]cos(\theta)
\end{aligned} \tag{2.11}$$

La massima violazione si ha per $\theta_M = \pi/3$, per il quale corrisponde un valore di $S_{H_M} = 0.125$. Bisogna osservare che questo non è il valore massimo che può assumere S_H utilizzando uno stato non massimamente entangled.

Protocollo B92-gen

Consideriamo il caso in cui Alice esegua la misura sullo stato 2.5 con gli stessi stati 2.8 e Bob con i nuovi stati $|b'_0\rangle = |\overline{\varphi'}_0\rangle$ e $|b'_1\rangle = |\overline{\varphi'}_1\rangle$ definiti come in 2.2 ma con un nuovo angolo θ' tale che $tan(\theta') = sin(\theta)$ (chiamiamo questo protocollo B92-gen), si ha:

$$\begin{aligned}
P(a'_1, b'_1) &= |\langle V|\langle\overline{\varphi'}_1|\Phi\rangle|^2 = sin^2(\theta/2)|\langle\overline{\varphi'}_1|V\rangle|^2 \\
&= sin^2(\theta/2)cos^2(\theta'/2) \\
P(a'_1, \overline{b'}_0) &= |\langle V|\langle\varphi'_0|\Phi\rangle|^2 = sin^2(\theta/2)|\langle\varphi'_0|V\rangle|^2 \\
&= sin^2(\theta/2)sin^2(\theta'/2) \\
P(\overline{a'}_0, b'_1) &= |\langle -|\overline{\varphi'}_1|\Phi\rangle|^2 \\
&= \frac{1}{2}(cos(\theta/2)sin(\theta'/2) - sin(\theta/2)cos(\theta'/2))^2 \\
P(a'_0, b'_0) &= |\langle +|\overline{\varphi'}_0|\Phi\rangle|^2 \\
&= \frac{1}{2}(cos(\theta/2)sin(\theta'/2) - sin(\theta/2)cos(\theta'/2))^2
\end{aligned} \tag{2.12}$$

ottenendo

$$\begin{aligned} S_H^{gen} =& sin^2(\theta/2)cos^2(\theta'/2) - sin^2(\theta/2)sin^2(\theta'/2) \\ & - (cos(\theta/2)sin(\theta'/2) - sin(\theta/2)cos(\theta'/2))^2 \\ =& - sin^2(\theta/2)sin^2(\theta'/2) - cos^2(\theta/2)sin^2(\theta'/2) \\ & + 2cos(\theta/2)sin(\theta'/2)sin(\theta/2)cos(\theta'/2) \\ =& - sin^2(\theta/2)sin^2(\theta'/2) - cos^2(\theta/2)sin^2(\theta'/2) + \frac{1}{2}sin(\theta)sin(\theta') \\ =& - sin^2(\theta/2)\frac{1-cos(\theta')}{2} - cos^2(\theta/2)\frac{1-cos(\theta')}{2} + \frac{1}{2}sin(\theta)sin(\theta') \\ =& \frac{1}{2}\left(-sin^2(\theta/2) - cos^2(\theta/2)\right) + \frac{1}{2}cos(\theta') + \frac{1}{2}sin(\theta)sin(\theta') \end{aligned} \tag{2.13}$$

Poichè $tan(\theta') = sin(\theta)$ e utilizzando le relazioni fondamentali della trigonometria si ha

$$\begin{aligned} S_H^{gen} =& \frac{1}{2}\left[-1 + \frac{1}{\sqrt{1+sin^2(\theta)}} + \frac{sin^2(\theta)}{\sqrt{1+sin^2(\theta)}}\right] = \\ =& \frac{1}{2}\left[\frac{1+sin^2(\theta) - \sqrt{1+sin^2(\theta)}}{\sqrt{1+sin^2(\theta)}}\right] = \frac{1}{2}(\sqrt{1+sin^2(\theta)} - 1) \end{aligned} \tag{2.14}$$

L'equazione 2.14 definisce In figura 2.2 viene mostrato il confronto dei due casi S_H e S_H^{gen}

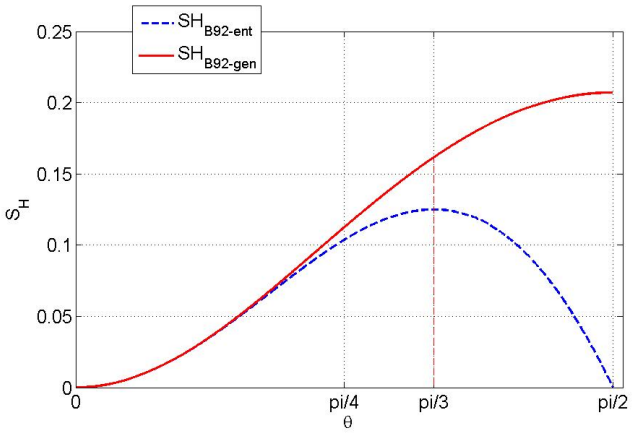


Figura 2.2: Confronto S_H e S_H^{gen}

In questo esperimento, ci interessa un altro dato, il guadagno del protocollo, ovvero la probabilità che un qubit diventi un bit della chiave finale. Il

guadagno è dato da ([LM11]):

$$G_{CHSH} \geq -log_2\left(\frac{1}{2}+\frac{1}{2}\sqrt{2-\frac{S_{CHSH}^2}{4}}\right)-H(a|b) \tag{2.15}$$

nel caso in cui per testare il protocollo si sia utilizzata la disuguaglianza di Bell introdotta da CHSH ([Hol69]). La relazione tra S_{CHSH} e S_H è data da ([GM11]) $S_{CHSH} = 4S_H + 2$. Il termine $H(a|b)$ è dovuto all'entropia degli errori $h(QBER)$, con $QBER = \frac{N_{err}}{N_{con}}$, con N_{err} il numero degli errori trovati nella fase di correzione degli errori e N_{con} il numero degli eventi conclusivi. La quantità N_{err} è legata alla probabilità di effettuare una misura sugli stati $|-|\overline{\varphi}_1\rangle$ e $|+|\overline{\varphi}_0\rangle$, poichè una misura con esito positivo su questi stati corrisponde ad un errore. Nel nostro caso otteniamo che

$$G_H = 1 - log_2\left(1+\sqrt{1-4S_H-4S_H^2}\right)-h\left(QBER\right) \tag{2.16}$$

In generale si ha che il $QBER$ è dato da

$$QBER = \frac{P(a_0b_0)+P(\overline{a}_0b_1)}{P(a_0b_0)+P(\overline{a}_0b_1)+P(\overline{a}_0b_0)+P(a_0b_1)} = \frac{cos(\theta-\theta')-1}{2(cos(\theta)cos(\theta')-1)} \tag{2.17}$$

Nel protocollo ent-B92 il termine $h(QBER)$ è nullo, poichè, abbiamo visto che le probabilià $P(a_0b_0)$ e $P(\overline{a}_0b_1)$ sono nulle.
In questa tesi verificheremo sperimentalmente tali risultati, sia nel caso del protocollo us-B92 (stati 2.1 e 2.2) sia nel caso B92-gen (usando gli stati 2.1 e 2.2 con $\theta = \theta'$)

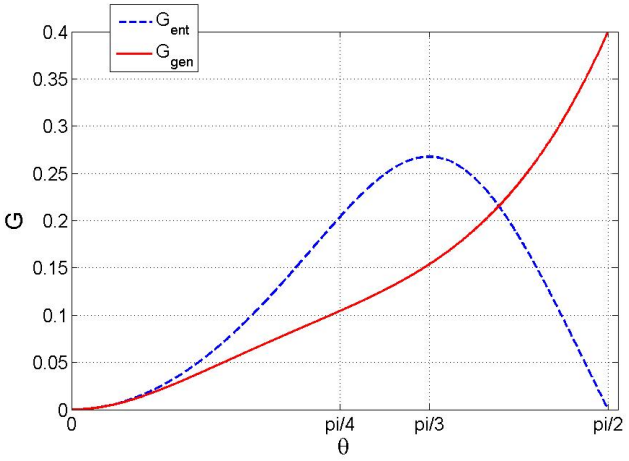


Figura 2.3: Confronto per G nei due protocolli

Capitolo 3

Ottica non lineare

In questo capitolo vengono mostrati, partendo dall'equazioni di Maxwell, gli effetti dovuti all'interazione di un campo elettrico di notevole intensità con un mezzo non lineare. Successivamente verrà data una versione quantistica di questi effetti, mostrando come l'interazione di un campo elettrico possa portare alla generazione di una coppia di fotoni entangled.

Gli effetti non lineari, inoltre, sono alla base della realizzazione del setup del nostro esperimento, oltre che ad essere applicati in componenti da noi utilizzati.

3.1 Equazioni di Maxwell in un mezzo non lineare

Vediamo come si modificano le equazioni di Maxwell propagando la radiazione in un mezzo non lineare con $\mu = \mu_0$ invece che nel vuoto

$$\nabla \times \mathbf{E} = -\frac{\delta \mathbf{B}}{\delta t}$$

$$\nabla \times \mathbf{H} = -\frac{\delta \mathbf{D}}{\delta t}$$

$$\mathbf{B} = \mu \mathbf{H}$$

$$\mathbf{D} = \epsilon_0 \mathbf{E} + \mathbf{P}$$

In un mezzo dielettrico lineare la relazione tra il vettore di polarizzazione $\mathbf{P}$ ed il campo elettrico $\mathbf{E}$ è lineare, $\mathbf{P} = \epsilon_0 \chi \mathbf{E}$. Invece se ci troviamo in un mezzo non lineare, questa relazione è non lineare. In genere la dipendenza tra $\mathbf{E}$ ed $\mathbf{P}$ è lineare quando $\mathbf{E}$ assume valori piccoli, ma, quando il campo

elettrico assume valori elevati $\cong 10^5 - 10^8 V/m$, la relazione diventa non lineare. Questa relazione si può espandere in serie di Taylor diventando

$$\mathbf{P} = \epsilon_0 \chi \mathbf{E} + 2d\mathbf{E}^2 + 4\chi^{(3)}\mathbf{E}^3 + \dots$$

dove d e $\chi^{(3)}$ sono coefficienti che rappresentano rispettivamente gli effetti del secondo e del terzo ordine. Vediamo ora come la radiazione incidente sul mezzo non lineare viene assorbita e rilasciata.

In un mezzo non lineare, la propagazione della luce avviene secondo la relazione [Sal07, p.161]

$$\nabla^2 \mathbf{E} - \frac{1}{c_0^2}\frac{\partial^2 \mathbf{E}}{\partial t^2} = \mu_0 \frac{\partial^2 \mathbf{P}}{\partial t^2}$$

dove l'ultimo termine, espandendo $\mathbf{P}$ in serie di Taylor, si può riscrivere come

$$\mu_0 \frac{\partial^2 \mathbf{P}}{\partial t^2} = \mu_0 \epsilon_0 \chi \frac{\partial^2 \mathbf{E}}{\partial t^2} + 2\mu_0 d \frac{\partial^2 \mathbf{E}^2}{\partial t^2} + 4\mu_0 \chi^{(3)} \frac{\partial^2 \mathbf{E}^3}{\partial t^2}$$

che unita alla precedente da

$$\nabla^2 \mathbf{E} - \frac{\mu_0 \epsilon_0 \chi}{c_0^2}\frac{\partial^2 \mathbf{E}}{\partial t^2} = 2\mu_0 d \frac{\partial^2 \mathbf{E}^2}{\partial t^2} + 4\mu_0 \chi^{(3)} \frac{\partial^2 \mathbf{E}^3}{\partial t^2}$$

ricordando che $\mu_0 \epsilon_0 = c_0$ e che $n^2 = 1 + \chi$

$$\nabla^2 \mathbf{E} - \frac{1}{c^2}\frac{\partial^2 \mathbf{E}}{\partial t^2} = -S$$

dove è stata effettuata la sostituzione

$$S = -2\mu_0 d \frac{\partial^2 \mathbf{E}^2}{\partial t^2} + 4\mu_0 \chi^{(3)} \frac{\partial^2 \mathbf{E}^3}{\partial t^2} \tag{3.1}$$

L'equazione 3.1 si può pensare come un'equazione d'onda dove il termine S compie il ruolo di sorgente che irradia in un mezzo non lineare con indice di rifrazione n. Questa equazione è non lineare in $\mathbf{E}$ a causa di S.

La sorgente di radiazione S in 3.1 dipende da $\mathbf{E}$, quindi $\mathbf{E}$ irradia se stesso. Per rendere più evidente questo fatto scriviamo $S = S(\mathbf{E})$.

Come mostrato in figura 3.1, un campo $\mathbf{E}_0$ incidente in un mezzo non lineare crea una sorgente di radiazioni $S(\mathbf{E}_0)$ che irradia un campo $\mathbf{E}_1$. A questo nuovo campo, $\mathbf{E}_1$, corrisponde una sorgente $S(\mathbf{E}_1)$ che a sua volta irradia un campo $\mathbf{E}_2$. Questa soluzione iterativa, al primo passo, viene chiamata la prima approssimazione di Born, ed è efficace per linearità piccole. In questa approssimazione, la propagazione della luce attraverso il mezzo si

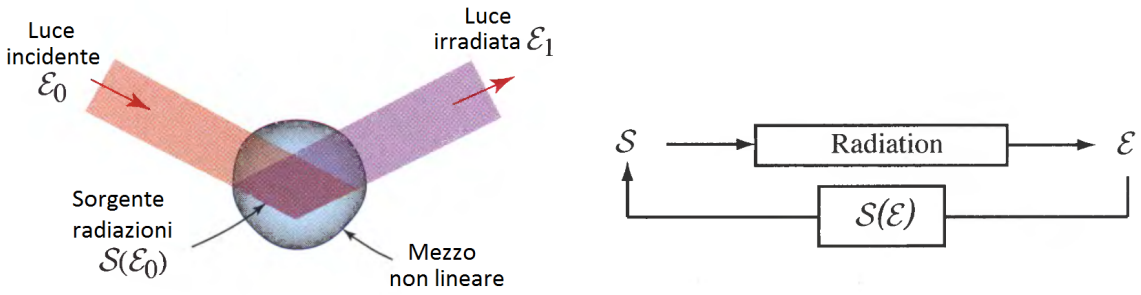


Figura 3.1: Sorgente non lineare

può considerare come un processo di scattering, dove il campo incidente è disperso dal mezzo. Poichè $S(\mathbf{E}_0)$ è una funzione non lineare, il campo emesso $\mathbf{E}_1$ presenterà delle nuove frequenze non presenti in $\mathbf{E}_0$.

Le proprietà di nostro interesse sono quelle dovute al secondo ordine, poichè sono responsabili degli effetti su cui si basa il nostro esperimento, cioè **SGH***(second armonic generation)* e **SPDC***(spontaneous parametric downconversion)*.

Esaminiamo ora le caratteristiche di un mezzo non lineare in cui le non linearità di ordine superiore al secondo sono trascurabili. Chiamiamo $\mathbf{P}_{NL}$ il contributo delle non linearità, quindi $\mathbf{P} = \epsilon_0\chi\mathbf{E} + 2d\mathbf{E}^2 + 4\chi^{(3)}\mathbf{E}^3 + \ldots = \epsilon_0\chi\mathbf{E} + \mathbf{P}_{NL}$. Nel nostro caso, le non linearità superiori al secondo ordine vengono trascurate, abbiamo che

$$\mathbf{P}_{NL} = 2d\mathbf{E}^2 \tag{3.2}$$

3.2 Second-Harmonic Generation SGH

La generazione di seconda armonica (*Second-Harmonic Generation SGH*) è un processo ottico non lineare del secondo ordine, dove i fotoni, interagendo con il mezzo non lineare, sono combinati a formare un nuovo fotone, avente il doppio dell'energia, quindi il doppio delle frequenza e metà della lunghezza d'onda dei fotoni iniziali.

Consideriamo un campo elettrico con pulsazione ω e inviluppo complesso $A(\omega)$

$$E(t) = Re\{Aexp(j\omega t)\} = \frac{1}{2}\left[A\ exp(j\omega t) + A^*\ exp(-j\omega t)\right] \tag{3.3}$$

Sostituendo 3.3 in 3.2 otteniamo

$$P_{NL}(t) = P_{NL}(0) + ReP_{NL}(2\omega)\ exp(j2\omega t) \tag{3.4}$$

dove

$$P_{NL}(0) = d\ A\ A^* \tag{3.5}$$

$$P_{NL}(2\omega) = d\ A^2 \tag{3.6}$$

La sorgente $S(t) = -\mu_0 \frac{\partial^2 P_{NL}}{\partial t^2}$ riferita a 3.4 ha una componente a 2ω con inviluppo complesso pari a $S(2\omega) = 4\,\mu_0 \omega^2 d\ A^2$, che irradia un campo con lunghezza d'onda dimezzata $(\lambda_0/2)$. Questo significa che il campo irradiato ha una componente alla seconda armonica del campo incidente. L'intensiatà del campo irradiato alla seconda armonica ha un'intesità $I(2\omega)$ proporzionale a $|S(2\omega)|^2$, che a sua volta è proporzionale all'intensità dell'onda incidente$I(\omega)$. L'intensità $I(2\omega)$ inoltre è proporzionale al quadrato della lunghezza L della regione d'interazione, poichè le emissioni si sommano coerentemente. L'efficienza della generazione di seconda armonica $\eta_{SHG} = I(2\omega)/I(\omega)$ con $I(2\omega) = C^2 L^2 I(\omega)$ e $I(\omega) = P/A_{ST}$, dove C è una costante proporzionale a d^2 e ω^2, P è la potenza incidente e A_{ST} l'area della sezione trasversale, risulta

$$\eta_{SHG} = C^2 \frac{L^2}{A_{ST}} P \tag{3.7}$$

Dall'equazione 3.7 si osserva che per aumentare l'efficienza è necessario incrementare la potenza incidente, e ciò si può fare utilizzando laser impulsati, che confinano molta energia in impulsi di breve durata, ottenendo potenze di picco molto elevate. Sempre osservando l'equazione 3.7 si nota che è possibile aumentare l'efficienza anche massimizzando il rapporto L^2/A_{ST}, focalizzando il fascio in un area A_{ST} molto piccola e utilizzando un'area di interazione il più lungo possibile.
Nel nostro setup ottico per il processo SHG è stato utilizzato un cristallo *Bismuth Borate* BiBO.

3.3 Spontaneus Parametric Downconversion SPDC

Questo processo non lineare è molto importante in ottica quantistica, poichè è utilizzato per la generazione delle coppie di fotoni entangled. Si può pensare che il processo SPDC operi al contrario del SHG, in quanto un fotone viene diviso in una coppia di fotoni, in accordo con la legge della conservazione dell'energia. La coppia di fotoni generata avrà momento ed energia pari al momento ed energia del fotone che l'ha generata, quindi ogni fotone della coppia avrà energia più bassa del fotone che l'ha generata.

Il processo SPDC è dovuto al Three Wave Mixing, che prevede la miscelazione di 3 lunghezze d'onda. Consideriamo un campo elettrico con due armoniche alle pulsazioni ω_1 e ω_2 con inviluppo complesso $A(\omega)$

$$E(t) = Re\{A(\omega_1)exp(j\omega_1 t) + A(\omega_2)\ exp(-j\omega_2 t)\} \tag{3.8}$$

Ora andiamo a calcolare la componente non lineare P_{NL}

$$\begin{aligned} P_{NL}(t) &= 2\ d\ E(t)E^*(t) \\ &= \underbrace{d\ \left[|A(\omega_1)|^2 + |A(\omega_2)|^2\right]}_{P_{NL}(0)} \\ &+ Re\{\underbrace{dA(\omega_1)A(\omega_1)}_{P_{NL}(2\omega_1)}\ exp(j2\omega_1 t)\} \\ &+ Re\{\underbrace{dA(\omega_2)A(\omega_2)}_{P_{NL}(2\omega_2)}\ exp(j2\omega_2 t)\} \\ &+ Re\{\underbrace{2dA(\omega_1)A(\omega_2)}_{P_{NL}(\omega_+)}\ exp(j(\omega_1+\omega_2)t)\} \\ &+ Re\{\underbrace{2dA(\omega_1)A^*(\omega_2)}_{P_{NL}(\omega_-)}\ exp(j(\omega_1-\omega_2)t)\} \end{aligned} \tag{3.9}$$

Si nota la presenza di 5 componenti a pulsazione diversa 0, $2\omega_1$, $2\omega_2$, $\omega_+ = \omega_1 + \omega_2$, $\omega_- = \omega_1 - \omega_2$. Da ciò si vede che un mezzo non lineare può essere utilizzato per miscelare 2 onde a frequenza diversa, generandone una terza con frequenza pari alla somma(*frequency up-conversion*) o alla differenza(*frequency down-conversion*) delle due.

Consideriamo le onde 1 e 2 come onde piane con vettore d'onda $\mathbf{k}_1$ e $\mathbf{k}_2$. I rispettivi campi sono $E(\omega_1) = A_1\, exp(-j\boldsymbol{k_1}\cdot\mathbf{r})$ e $E(\omega_2) = A_2\, exp(-j\boldsymbol{k_2}\cdot\mathbf{r})$, ottenendo, secondo l'equazione 3.9, $P_{NL}(\omega_+ = \omega_3) = 2dA_1A_2\ exp(-j\boldsymbol{k}_3\cdot\boldsymbol{r})$ con

$$\omega_1 + \omega_2 = \omega_3 \tag{3.10}$$

$$\boldsymbol{k}_1 + \boldsymbol{k}_2 = \boldsymbol{k_3} \tag{3.11}$$

Queste due equazioni ci dicono che il mezzo opera come sorgente alla pulsazione ω_3 con vettore d'onda $\boldsymbol{k_3}$.

L'equazione 3.10 è la condizione di Frequency-Matching, mentre l'equazione 3.11 è la condizione di Phase-Matching.

Il Three-wave mixing può assumere diverse forme, a seconda dell'input che viene fornito al cristallo. Il caso di nostro interesse, SPDC, si ha quando la pompa del cristallo è l'onda 3, chiamata pompa, e la conversione alle pulsazioni più basse ω_2 e ω_3, le cui onde sono chiamate di signal e idler, è

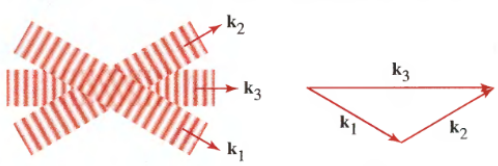


Figura 3.2: Condizione di phase-matching

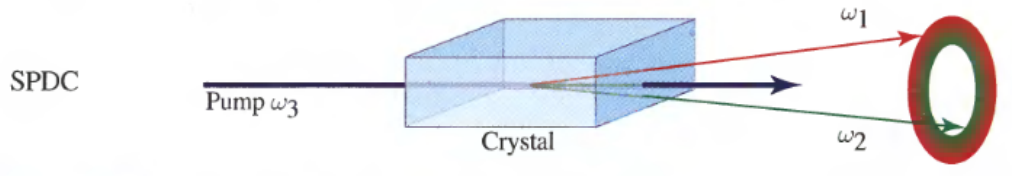


Figura 3.3: SPDC

spontanea. Dalle equazioni 3.10 e 3.11 si ricavano diverse soluzioni, ognuna delle quali forma una coppia di onde con una specifica frequenza e direzione. La conversione è molto poco efficiente, nell'ordine di una coppia ogni 10^{12} fotoni incidenti[AL08]
Nel nostro setup ottico per il processo SPDC è stato utilizzato un cristallo β-*Barium Borate* BBO.

Ci sono 2 tipi di SPDC, a seconda del cristallo in cui viene l'interazione. Nel Tipo I le onde di signal e idler hanno la stessa polarizzazione ortogonale alla pompa, mentre nel Tipo II hanno polarizzazioni ortogonali. Le condizioni di phase matching impongono che nel cristallo di Tipo I la coppia di fotoni emessa stia su parti opposte di coni concentrici nella direzione della pompa. Nel Tipo II invece, i fotoni vengono emessi su due coni, uno per l'onda ordinaria e l'altro per l'onda extraordinaria.

Questo processo si può vedere anche come un'interazione a tre fotoni, nel quale due fotoni vengono distrutti e ne viene creato uno a frequenza maggiore. Nel caso di SPDC si ha che un fotone viene distrutto e vengono creati due fotoni a frequenza minore(fig. 3.4).

Gli stati entangled vengono generati utilizzando questo effetto. Per capire questo processo da un punto di vista quantistico dobbiamo prima parlare della quantizzazione del campo elettrico.

3.4 Quantizzazione del campo

Consideriamo un campo in spazio aperto senza sorgenti di radiazioni e senza cariche. Le equazioni del campo elettromagnetico si possono riscrivere

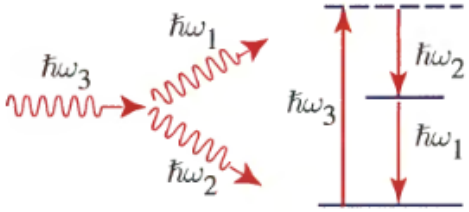


Figura 3.4: Creazione di due fotoni a partire da un fotone a frequenza maggiore

utilizzando il potenziale vettore $\mathbf{A}(\mathbf{r}, t)$ che soddisfa l'equazione delle onde

$$\nabla^2(A) - \frac{1}{c^2}\frac{\partial^2(A)}{\partial t^2} = 0 \tag{3.12}$$

e, utilizzando la Coulomb gauge condition

$$\nabla \cdot \boldsymbol{A}(\boldsymbol{r}, t) = 0 \tag{3.13}$$

si ha

$$\boldsymbol{E}(\boldsymbol{r}, t) = -\frac{\partial \boldsymbol{A}(\boldsymbol{r}, t)}{\partial t} \tag{3.14a}$$

$$\boldsymbol{B}(\boldsymbol{r}, t) = \nabla \times \boldsymbol{A}(\boldsymbol{r}, t) \tag{3.14b}$$

Il potenziale vettore lo possiamo scrivere come superposizione di onde piane

$$\boldsymbol{A}(\boldsymbol{r}, t) = \sum_{\boldsymbol{k},s} \boldsymbol{e}_{\boldsymbol{k}s} \left[A_{\boldsymbol{k}s}(t)e^{i\boldsymbol{k}\cdot\boldsymbol{r}} + A^*_{\boldsymbol{k}s}(t)e^{-i\boldsymbol{k}\cdot\boldsymbol{r}}\right] \tag{3.15}$$

La sommatoria precedente è fatta sui vari modi del campo (per quanto riguarda $\boldsymbol{k}$) e sulle due polarizzazioni del campo (per quanto riguarda s).

Dalle equazioni 3.13, 3.12 e 3.15 si ottiene per l'inviluppo complesso $A_{\boldsymbol{k}s}(t)$

$$\frac{d^2 A_{\boldsymbol{k}s}}{dt^2} + \omega_k^2 A_{\boldsymbol{k}s}(t) = 0 \tag{3.16}$$

con $\omega_k = ck$ che ammette come soluzione $A_{\boldsymbol{k}s}(t) = A_{\boldsymbol{k}s}e^{-i\omega_k t}$. Dalle equazioni in 3.14a otteniamo

$$\boldsymbol{E}(\boldsymbol{r}, t) = i\sum_{\boldsymbol{k},s} \omega_k \boldsymbol{e}_{\boldsymbol{k}s} \left[A_{\boldsymbol{k}s}(t)e^{i(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t)} - A^*_{\boldsymbol{k}s}(t)e^{-i(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t)}\right] \tag{3.17a}$$

$$\boldsymbol{B}(\boldsymbol{r},t) = \frac{i}{c}\sum_{\boldsymbol{k},s}\omega_k(\boldsymbol{\kappa}\times\boldsymbol{e}_{\boldsymbol{k}s})\boldsymbol{e}_{\boldsymbol{k}s}\left[A_{\boldsymbol{k}s}(t)e^{i(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t)} - A^*_{\boldsymbol{k}s}(t)e^{-i(\boldsymbol{k}\cdot\boldsymbol{r}-\omega_k t)}\right] \tag{3.17b}$$

L'energia del campo è data dall'hamiltoniano

$$H = \frac{1}{2}\int_V \left(\epsilon_0\boldsymbol{E}\cdot\boldsymbol{E} + \frac{1}{\mu_0}\boldsymbol{B}\cdot\boldsymbol{B}\right)dV \tag{3.18}$$

Tralasciando i vari passaggi [CG05, p.37] arriviamo a

$$H = 2\epsilon_0 V\sum_{\boldsymbol{k},s}\omega_k^2 A_{\boldsymbol{k}s}(t)A^*_{\boldsymbol{k}s}(t) \tag{3.19}$$

Per quantizzare il campo, dobbiamo introdurre le variabili canoniche $p_{\boldsymbol{k}s}$ e $q_{\boldsymbol{k}s}$. Possiamo scrivere

$$A_{\boldsymbol{k}s} = \frac{1}{2\omega_k\sqrt{(\epsilon_0 V)}}\left[\omega_k q_{\boldsymbol{k}s} + ip_{\boldsymbol{k}s}\right] \tag{3.20a}$$

$$A^*_{\boldsymbol{k}s} = \frac{1}{2\omega_k\sqrt{(\epsilon_0 V)}}\left[\omega_k q_{\boldsymbol{k}s} - ip_{\boldsymbol{k}s}\right] \tag{3.20b}$$

L'hamiltoniano di 3.19 diventa

$$H = \frac{1}{2}\sum_{\boldsymbol{k},s}(p^2_{\boldsymbol{k}s} + \omega_k^2 q^2_{\boldsymbol{k}s}) \tag{3.21}$$

Ogni termine della sommatoria rappresenta l'energia di un oscillatore armonico di massa unitaria. Imponiamo alle variabili canoniche di soddisfare la relazione di commutazione

$$[\hat{q}_{\boldsymbol{k}s}, \hat{q}_{\boldsymbol{k}'s'}] = 0 = [\hat{p}_{\boldsymbol{k}s}, \hat{p}_{\boldsymbol{k}'s'}] \tag{3.22a}$$

$$[\hat{q}_{\boldsymbol{k}s}, \hat{p}_{\boldsymbol{k}'s'}] = i\hbar\delta_{\boldsymbol{k}\boldsymbol{k}'\boldsymbol{s}\boldsymbol{s}'} \tag{3.22b}$$

Definiamo ora gli operatori di creazione e di distruzione

$$\hat{a}_{\boldsymbol{k}s} = \frac{1}{\sqrt{2\hbar\omega_k}}\left[\omega_k q_{\boldsymbol{k}s} + ip_{\boldsymbol{k}s}\right] \tag{3.23a}$$

$$\hat{a}^\dagger_{\boldsymbol{k}s} = \frac{1}{\sqrt{2\hbar\omega_k}}\left[\omega_k q_{\boldsymbol{k}s} - ip_{\boldsymbol{k}s}\right] \tag{3.23b}$$

che soddisfano

$$[\hat{a}_{\boldsymbol{k}s}, \hat{a}_{\boldsymbol{k}'s'}] = 0 = \left[\hat{a}^\dagger_{\boldsymbol{k}s}, \hat{a}^\dagger_{\boldsymbol{k}'s'}\right] \tag{3.24a}$$

$$\left[\hat{a}_{\boldsymbol{k}s}, \hat{a}^{\dagger}_{\boldsymbol{k}'s'}\right] = \delta_{\boldsymbol{k}\boldsymbol{k}'ss'} \tag{3.24b}$$

Considerando l'operatore Hamiltoniano, troviamo che l'energia del campo risulta:

$$\begin{aligned} \hat{H} &= \sum_{\boldsymbol{k}s} \hbar\omega_k \left(\hat{a}^{\dagger}_{\boldsymbol{k}s}\hat{a}_{\boldsymbol{k}s} + \frac{1}{2}\right) \\ &= \sum_{\boldsymbol{k}s} \hbar\omega_k \left(\hat{n}_{\boldsymbol{k}s} + \frac{1}{2}\right) \end{aligned} \tag{3.25}$$

dove

$$\hat{n}_{\boldsymbol{k}s} = \hat{a}^{\dagger}_{\boldsymbol{k}s}\hat{a}_{\boldsymbol{k}s}$$

è l'operatore numero del modo $\boldsymbol{k}s$. Ogni modo, indipendente da ogni altro, ha un insieme di autovalori $|n_{\boldsymbol{k}s}\rangle$. Semplifichiamo la scrittura, grazie all'indipendenza dei modi, e poniamo $\hat{a}_{\boldsymbol{k_j}s_j} \equiv \hat{a}_j, \hat{a}^{\dagger}_{\boldsymbol{k_j}s_j} \equiv \hat{a}^{\dagger}_j$ e $\hat{n}_{\boldsymbol{k_j}s_j} = \hat{n}_j$

L'Hamiltoniano risulta

$$\hat{H} = \sum_j \hbar\omega_j \left(\hat{n}_j + \frac{1}{2}\right) \tag{3.26}$$

in un sistema di più fotoni, lo stato numero risulta il prodotto degli stati numero di tutti i modi

$$|n_1\rangle|n_2\rangle|n_3\rangle \ldots = |n_1, n_2, n_3 \ldots\rangle = |\{n_j\}\rangle$$

che è un autostato di $\hat{H}$

$$\hat{H}|\{n_j\}\rangle = E|\{n_j\}\rangle$$

con autovalore E

$$E = \sum_j \hbar\omega_j \left(n_j + \frac{1}{2}\right)$$

Gli stato numero sono ortogonali secondo

$$\langle n_1, n_2, n_3 \ldots | n'_1, n'_2, n'_3 \ldots\rangle = \delta_{n_1 n'_1}\delta_{n_2 n_1 2'}\delta_{n_3 n'_3}$$

Vediamo ora l'azione degli operatori di creazione e di distruzione

$$\hat{a}^{\dagger}_j|n_1, n_2 \ldots n_j \ldots\rangle = \sqrt{n_j + 1}|n_1, n_2 \ldots n_j + 1, \ldots\rangle$$

mentre per l'operatore distruzione si ha

$$\hat{a}_j|n_1, n_2 \dots n_j \dots\rangle = \sqrt{n_j}|n_1, n_2 \dots n_j - 1, \dots\rangle$$

Definito lo stato vuoto

$$|\{0\}\rangle = |0_1, 0_2, \dots, 0_j \dots\rangle$$

l'operatore di distruzione, per questo stato,

$$\hat{a}_j|\{0\} = 0$$

per ogni j. Dallo stato vuoto si possono ricavare tutti gli altri stati numero in questo modo

$$|\{n_j\}\rangle = \prod_j \frac{(\hat{a}_j^\dagger)^{n_j}}{\sqrt{n_j}\,!}|\{0\}\rangle$$

Ora possiamo riscrivere le amplitudini $\boldsymbol{A}_{\boldsymbol{k}s}$ come operatori, cioè

$$\hat{A}_{\boldsymbol{k}s} = \left(\frac{\hbar}{2\omega_k \epsilon_0 V}\right)^{\frac{1}{2}} \hat{a}_{\boldsymbol{k}s}$$

ottenendo il potenziale vettore

$$\hat{A}(\boldsymbol{r}, t) = \sum_{\boldsymbol{k},s} \left(\frac{\hbar}{2\omega_k \epsilon_0 V}\right)^{\frac{1}{2}} \boldsymbol{e}_{\boldsymbol{k}s} \left[\hat{a}_{\boldsymbol{k}s} e^{i(\boldsymbol{k}\cdot\boldsymbol{r} - \omega_k t)} + \hat{a}_{\boldsymbol{k}s}^\dagger e^{-i(\boldsymbol{k}\cdot\boldsymbol{r} - \omega_k t)}\right] \tag{3.27}$$

per il campo elettrico si ottiene

$$\hat{E}(\boldsymbol{r}, t) = i \sum_{\boldsymbol{k},s} \left(\frac{\hbar\omega_k}{2\epsilon_0 V}\right)^{\frac{1}{2}} \boldsymbol{e}_{\boldsymbol{k}s} \left[\hat{a}_{\boldsymbol{k}s} e^{i(\boldsymbol{k}\cdot\boldsymbol{r} - \omega_k t)} - \hat{a}_{\boldsymbol{k}s}^\dagger e^{-i(\boldsymbol{k}\cdot\boldsymbol{r} - \omega_k t)}\right] \tag{3.28}$$

mentre per il campo magnetico

$$\hat{B}(\boldsymbol{r}, t) = \frac{i}{c} \sum_{\boldsymbol{k},s} (\boldsymbol{\kappa} \times \boldsymbol{e}_{\boldsymbol{k}s}) \left(\frac{\hbar\omega_k}{2\epsilon_0 V}\right)^{\frac{1}{2}} \boldsymbol{e}_{\boldsymbol{k}s} \left[\hat{a}_{\boldsymbol{k}s} e^{i(\boldsymbol{k}\cdot\boldsymbol{r} - \omega_k t)} - \hat{a}_{\boldsymbol{k}s}^\dagger e^{-i(\boldsymbol{k}\cdot\boldsymbol{r} - \omega_k t)}\right] \tag{3.29}$$

con $\boldsymbol{\kappa} = \boldsymbol{k}/|\boldsymbol{k}|$

3.5 SPDC dal punto di vista quantistico

Dopo aver introdotto la quantizzazione del campo, vediamo ora come viene caratterizzato il processo SDPC da un punto di vista quantistico.
Un mezzo non lineare pompato da un campo con frequenza ω_p, come spiegato nel paragrafo 3.3, genera in uscita una coppia di fotoni alla frequenza $\omega = \omega_p/2$. L'Hamiltoniano di questo processo è dato da[CG05, p.165]:

$$\hat{H} = \hbar\omega\hat{a}^\dagger\hat{a} + \hbar\omega_p\hat{b}^\dagger\hat{b} + i\hbar\chi^{(2)}(\hat{a}^2\hat{b}^\dagger - \hat{a}^{\dagger\,2}\hat{b})$$

dove b è il modo della pompa e a è il modo del segnale.
Consideriamo ora solo il termine dovuto alla non linearità

$$\hat{H}_1 \sim \chi^{(2)}\hat{a}_p\hat{a}_s^\dagger\hat{a}_i^\dagger + c.c.$$

con $\hat{a}_p$ operatore di distruzione della pompa, $\hat{a}_s^\dagger$ e $\hat{a}_i^\dagger$ operatori di creazione per l'onda di signal e idler. Questo significa che, con gli stati di signal e idler inizialmente nello stato vuoto, un singolo fotone della pompa è convertito in 2 fotoni, uno per il signal e l'altro per l'idler:

$$|1\rangle_p|0\rangle_s|0\rangle_i \to \hat{a}_p\hat{a}_s^\dagger\hat{a}_i^\dagger|1\rangle_p|0\rangle_s|0\rangle_i = |0\rangle_p|1\rangle_s|1\rangle_i$$

I fotoni di signal e idler sono generati simultaneamente, come dimostrato da Burnham e Weinberg(phys. Rev. lett. 25(1970), 84). Questo aspetto è molto importante poichè ci permette di creare una coppia di fotoni indistinguibili utilizzabili per generare uno stato entangled. Come è stato spiegato nel paragrafo 3.3, le frequenze di pompa, idler e signal devono soddisfare il principio di conservazione dell'energia ottenendo $\hbar\omega_P = \hbar\omega_s + \omega_i$. Ci sono due tipi di SPDC. Nel tipo I, l'onda di signal e di idler hanno la stessa polarizzazione, che risulta ortogonale a quella della pompa. L'Hamiltoniano per questo processo è

$$\hat{H}_1 = \hbar\eta\hat{a}_s^\dagger\hat{a}_i^\dagger + c.c.$$

con $\eta = \chi^{(2)}\mathcal{E}_p$ e $\mathcal{E}_p$ ampiezza del campo classico. La condizione di phase matching 3.11 impone che i fotoni di signal e idler escano dal cristallo su parti opposte di coni concentrici nella direzione del laser di pompa.

Nel tipo II, i fotoni di idler e signal hanno polarizzazioni ortogonali. A causa della birifrangenza, i fotoni generati appartengono a due coni diversi, uno per l'onda ordinaria e l'altro per l'onda extraordinaria. I fotoni con polarizzazione verticale vengono indicati con $|V\rangle$ mentre quelli con polarizzazione orizzontale con $|H\rangle$. L'intersezione dei coni costituisce una sorgente di fotoni entangled e nulla si può dire a quale dei due coni appartengano i fotoni.

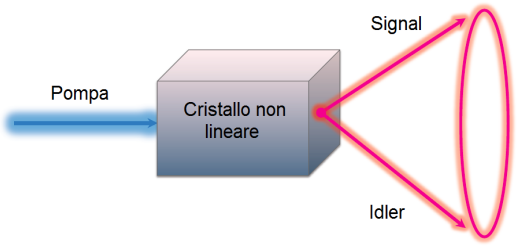


Figura 3.5: SPDC type I

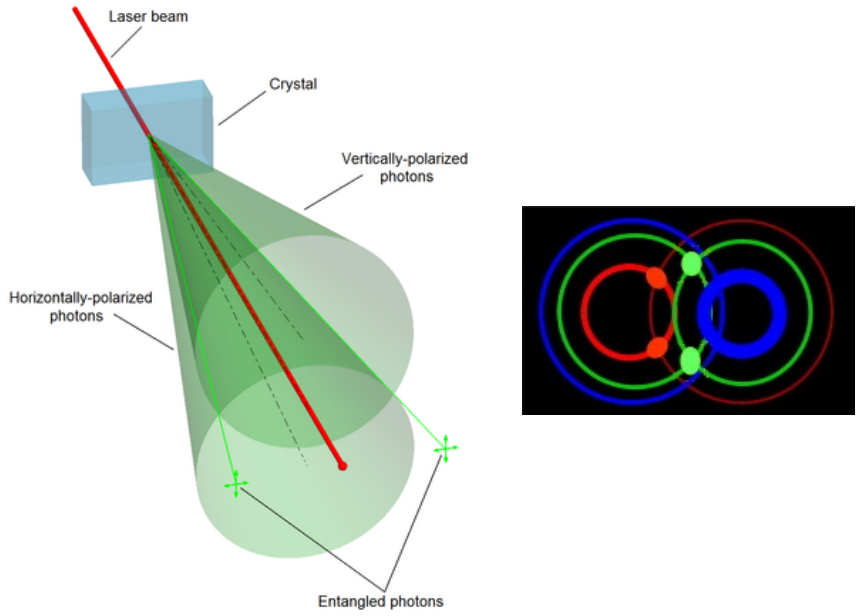


Figura 3.6: SPDC Type II. La figura di destra mostra una rappresentazione di diversi coni generati da SPDC Type-II. Le intersezioni generano coppie di fotoni entangled

L'Hamiltoniano in questo caso è:

$$\hat{H}_1 = \hbar\eta \left(\hat{a}^\dagger_{Vs} \hat{a}^\dagger_{Hi} + \hat{a}^\dagger_{Hs} \hat{a}^\dagger_{Vi} \right) + c.c.$$

dove gli operatori $\hat{a}^\dagger_{Vs}$, $\hat{a}^\dagger_{Hs}$, $\hat{a}^\dagger_{Hi}$, $\hat{a}^\dagger_{Vi}$ sono gli operatori di creazione per i fotoni con polarizzazione verticale ed orizzontale dell'onda di signal e idler. Partendo ora dallo stato di vuoto $|\Psi_0\rangle = |\{0\}\rangle$ si ottiene l'evoluzione dello stato

$$|\Psi(t)\rangle = exp(-it\hat{H}_1/\hbar)|\Psi_0\rangle \tag{3.30}$$

da cui si ottiene, espandendo l'esponenziale fino al secondo ordine e ricordando che $\hat{H}_1$ non dipende dal tempo,

$$|\Psi(t)\rangle \approx \left[1 - it\hat{H}_1/\hbar + \frac{1}{2}(-it\hat{H}_1/\hbar)^2\right]|\Psi_0\rangle \tag{3.31}$$

Consideriamo ora il caso di SPDC Type-1. Abbiamo che $|\Psi_0\rangle = |0\rangle_s|0\rangle_i$ il quale ci permette di riscrivere l'evoluzione dello stato di eq. 3.31 in questo modo

$$|\Psi(t)\rangle = (1 - \mu^2/2)|0\rangle_s|0\rangle_i - i\mu|1\rangle_s|1\rangle_i \tag{3.32}$$

dove $\mu = \eta t$, e il termine di secondo grado contenente $|2\rangle_s|2\rangle_i$ è stato tralasciato. Per quanto riguarda il caso di SPDC Type-II con stato iniziale

$$|\psi_0\rangle = |0\rangle_{Vs}|0\rangle_{Hs}|0\rangle_{Vi}|0\rangle_{Hi}$$

abbiamo:

$$\begin{aligned}|\psi(t)\rangle =&(1 - \mu^2/2)|0\rangle_{Vs}|0\rangle_{Hs}|0\rangle_{Vi}|0\rangle_{Hi} - i\mu\frac{1}{\sqrt{2}}(|1\rangle_{Vs}|0\rangle_{Hs}|0\rangle_{Vi}|1\rangle_{Hi} \\ &+ |0\rangle_{Vs}|1\rangle_{Hs}|1\rangle_{Vi}|0\rangle_{Hi})\end{aligned} \tag{3.33}$$

Definiamo gli stati

$$\begin{aligned}|0\rangle &:= |0\rangle_V|0\rangle_H, \\ |V\rangle &:= |1\rangle_V|0\rangle_H, \\ |H\rangle &:= |0\rangle_V|1\rangle_H,\end{aligned}$$

così da avere

$$|\psi(t)\rangle = (1 - \mu^2/2)|0\rangle_s|0\rangle_i - i\mu(|V\rangle_s|H\rangle_i + |H\rangle_s|V\rangle_i) \tag{3.34}$$

normalizzando il secondo termine di questa equazione si ottiene lo stato

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|V\rangle_s|H\rangle_i + |H\rangle_s|V\rangle_i) \tag{3.35}$$

In generale gli stati ottenibili utilizzando due cristalli Type I disposti in modo ortogonale tra di loro e con la pompa incidente a 45° sono

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|H\rangle_i + e^{j\phi}|V\rangle_s|V\rangle_i) = \frac{1}{\sqrt{2}}(|HH\rangle + e^{j\phi}|VV\rangle) \tag{3.36}$$

mentre per un cristallo Type II si ha

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|V\rangle_s|H\rangle_i + e^{j\phi}|H\rangle_s|V\rangle_i) = \frac{1}{\sqrt{2}}(|VH\rangle + e^{j\phi}|HV\rangle) \tag{3.37}$$

Per $\phi = 0$ e $\phi = \pi$ gli stati precedenti prendono il nome di stati di Bell.

3.6 Generazione di uno stato non massimamente entangled via SPDC

Consideriamo uno stato entangled generato via SPDC da una coppia adiacente di cristalli Type-I, i cui assi sono disposti ortogonalmente, l'asse del primo cristallo è posizionato verticalmente, il secondo orizzontalmente. In questo modo se la pompa incide sui cristalli con polarizzazione verticale, solo il primo cristallo produrrà fluorescenza parametrica, mentre se ha polarizzazione orizzontale, sarà solo il secondo a produrre radiazione parametrica. Se invece la polarizzazione di pompa è di 45° la generazione avverrà in entrambi i cristalli in modo uguale generando lo stato massimamente entangled $|\psi\rangle = 1/\sqrt{2}(|HH\rangle + e^{i\phi}|VV\rangle)$. Se si ruota la polarizzazione della pompa si ottengono stati non massimamente entangled [Kwi99] nella forma

$$|\psi\rangle = \frac{1}{\sqrt{1+|\epsilon|^2}}(|HH\rangle + e^{i\phi}\epsilon|VV\rangle) = \beta|HH\rangle + e^{i\phi}\alpha|VV\rangle$$

con $\epsilon = tan\,\vartheta$, $\alpha = \epsilon/\sqrt{1+|\epsilon|^2} = sin\,\vartheta$ e $\beta = 1/\sqrt{1+|\epsilon|^2} = cos\,\vartheta$.

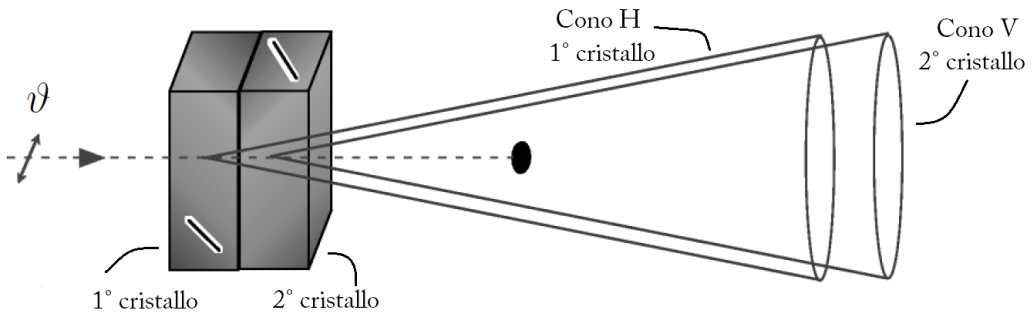


Figura 3.7: Generazione stato non max-entangled con cristallo type-I. ϑ indica la polarizzazione della pompa.

Uno stato non massimamente entangled, quindi, non è altro che uno stato entangled 'sbilanciato', cioè c'è maggior probabilità di ottenere $|HH\rangle$ rispetto a $|VV\rangle$ se $0 < \theta < \pi/4$, o viceversa se $\pi/4 < \theta < \pi$

Capitolo 4

Strumenti

4.1 Il laser MIRA HP

Il laser scelto per la generazione delle coppie entangled è il MIRA HP-F, un laser mode-locking che utilizza come mezzo di guadagno un cristallo di zaffiro dopato al titanio. Il MIRA viene pompato da un ulteriore laser, il VERDI. Le caratteristiche principali sono:

- regolazione della λ tra 700 nm e 980 nm
- generazione di impulsi ultracorti fino a 150 fs
- potenza di uscita elevata (3,3W in media)
- frequenza di ripetizione degli impulsi elevata $76MHz$

4.1.1 Pricipio di funzionamento MIRA

Nella cavità di un laser possono oscillare diversi modi longitudinali, le cui frequenze sono equamente separate di $\nu_F = c/2d$. Questi modi oscillano indipendentemente, ma attraverso un mezzo esterno si possono accoppiare bloccando la loro fase. Approssimando ogni modo come un'onda piana uniforme che si propaga nella direzione z con velocità $c = c_0/n$, il campo risultante è dato dalla somma:

$$U(z,t) = \sum_q A_q exp\left[j2\pi\nu_q\left(t - \frac{z}{c}\right)\right] \tag{4.1}$$

dove

$$\nu_q = \nu_0 + q\nu_F \tag{4.2}$$

è la frequenza del modo q-esimo. Dalle equazioni precedenti si ricava

$$U(z,t) = A\left(t - \frac{z}{c}\right) exp\left[j2\pi\nu_0\left(t - \frac{z}{c}\right)\right] \tag{4.3}$$

dove l'inviluppo complesso della funzione è

$$A(t) = \sum_q A_q exp\left(\frac{jq2\pi t}{T_F}\right) \tag{4.4}$$

con

$$T_F = \frac{1}{\nu_F} = \frac{2d}{c} \tag{4.5}$$

L'inviluppo $A(t)$ risulta essere una funzione periodica di periodo T_F, mentre $A(t - z/c)$ funzione periodica in z con periodo $cT_F = 2d$.

Consideriamo ora M modi, con $M = 2S+1$, tutti con lo stesso coefficiente $A_q = A$. Si ha

$$A(t) = A\sum_{q=-S}^{S} exp\left(\frac{jq2\pi t}{T_F}\right) \tag{4.6}$$

Dopo alcuni passaggi algebrici si ottiene

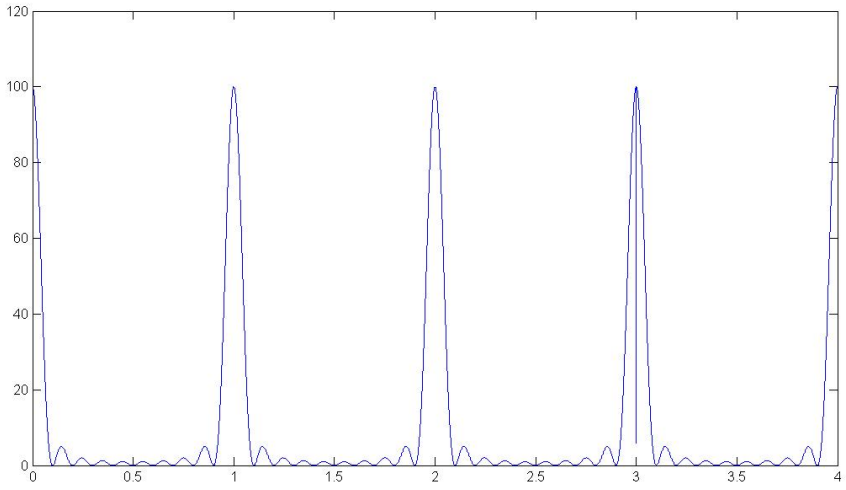
$$A(t) = A\frac{sin(M\pi t/T_F)}{sin(\pi t/T_F)} \tag{4.7}$$

da cui si ottiene l'intensità $I(t,z) = |A(t - z/c)/T_F|^2$

$$I(t,z) = |A|^2\frac{sin^2(M\pi(t - z/c)/T_F)}{sin^2(\pi(t - z/c)/T_F)} \tag{4.8}$$

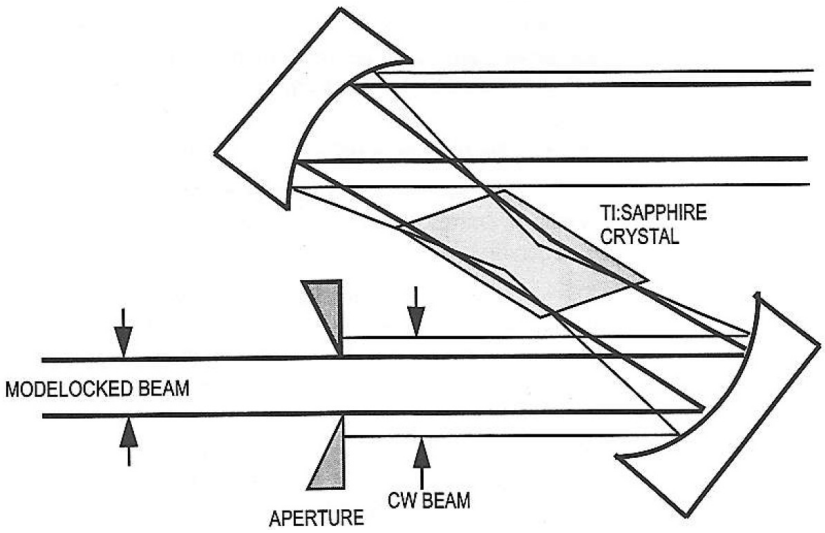
La forma dell'impulso dipende soprattutto dal numero di modi M, che a sua volta è proporzionale a $\Delta\nu$, inverso del tempo di decadimento degli stati di lasing del cristallo. Se $M \cong \Delta\nu/\nu_F$, la durata dell'impulso risulta pari a $\tau = T_F/M \approx 1/\Delta\nu$. Inoltre, il picco dell'impulso risulta proporzionale a M. Il cristallo del MIRA ha la particolarità di avere una $\Delta\nu$ molto elevata, 100 THz, che permette la generazione di impulsi ultracorti, nel nostro caso a $150ns$.

Per bloccare la fase dei diversi modi si può inserire all'interno della cavità uno switch che blocca la luce fino a che l'impulso non sia quasi generato, momento in cui lo switch permetterà il passaggio della luce per tutta la durata dell'impulso. In generale ogni modo ha la propria fase casuale, ma, se per caso, la fase dei modi assume lo stesso valore, allora la somma dei modi



produrrà l'impulso. Una volta innestato l'oscillazione continua, mantenendo la fase dei modi bloccata.

Questo può essere effettuato in due modi, il primo con uno switch attivo, il secondo con uno passivo. Nel MIRA viene utilizzato uno switch passivo, chiamato *saturable absorber*. Un saturable absorber è un materiale che diminuisce l'assorbimento della luce che lo attraversa all'aumentare dell'intensità di questa. Gli impulsi con un'elevata intensità riescono a passarlo, mentre quelli più deboli vengono assorbiti. Perciò, solo quando i modi hanno una fase simile tra di loro in modo da formare un impulso abbastanza intenso riescono ad attraversarlo, inescando l'oscillazione. All'interno della cavità del MIRA, tuttavia, vi sono due elementi che, agendo insieme, formano un saturable absorber. La cavità del MIRA è stata disegnata affinchè al suo interno il diametro del fascio laser potesse cambiare di poco al variare dell'intensità. Il diametro in modalià continua, in prossimità dell'uscita della cavità, risulta più largo rispetto agli impulsi ad alta intensità. Questo è dovuto all'effetto Kerr, effetto non lineare del terzo ordine, che comporta una variazione dell'indice di rifrazione del mezzo, proporzionale al quadrato del campo elettrico che lo attraversa. Come conseguenza, se un fascio incide su un materiale non lineare, l'indice di rifrazione ricalca la distribuzione dell'intensità del fascio. Ad esempio, se il fascio ha la massima intensità al centro, il massimo cambiamento dell'indice di rifrazione sarà al centro. Il mezzo non lineare opera quindi come un mezzo a gradiente d'indice, causando la curvatura del fronte d'onda dell'onda che lo attraversa. Si comporta perciò, come una lente la cui focale dipende dalla potenza dell'onda che lo attraversa.



Come si nota dalla figura, solo il fascio impulsato viene focalizzato, in questo modo, grazie ad una slitta posizionata nel punto appropriato, il fascio laser continuo viene bloccato, mentre quello impulsato viene lasciato passare. Le perdite introdotte dalla slitta sono sufficienti a far estinguere la componente continua del fascio.

4.2 Il laser VERDI

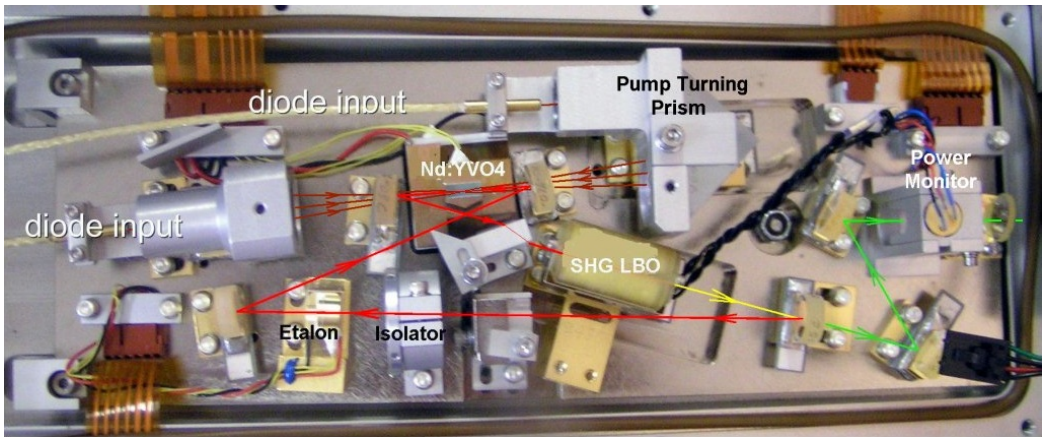
Il mezzo attivo del MIRA deve essere pompato da una sorgente esterna. Nel nostro caso è stato utilizzato il laser VERDI.

4.2.1 Principio di funzionamento VERDI

Il VERDI è un laser a singola frequenza con cavità ad anello. Questo tipo di cavità permette alla luce di viaggiare in senso orario oppure antiorario, evitando così la formazione di interferenze che potrebbero portare ad effetti non deisiderati(spatial hole burning [Pho]).

Il mezzo attivo utilizzato è un cristallo $Nd : YVO_4$ (neodymium-doped yttrium orthovanadate). Offre una larga banda di assorbimento, centrata ad una frequenza d'onda utile per il pompaggio con diodi laser. Inoltre, risulta poco sensibile alle variazioni della lunghezza d'onda con cui viene pompato, facendone un mezzo attivo facilmente pompabile da diodi laser.

Il cristallo di vanadate ha una forte birifrangenza, che permette di polarizzare il fascio senza l'ausilio di ulteriori dispositivi.



La lunghezza d'onda tipica del vanadate è di $1064nm$, che si trova nella regione del vicino infrarosso. La cavità è disegnata appositamente per far circolare luce a tale lunghezza d'onda, e i livelli di potenza che si raggiungono superano i $100W$. La luce visibile in uscita dal VERDI, che ha una lunghezza d'onda di $532nm$, è dovuta alla conversione di una parte di questa potenza a $1064nm$ ad opera di un cristallo birifrangente(SGH, second harmonic generator).

Il cristallo utilizzato per SHG è un cristallo di lithium triborate LBO. L'efficienza della conversione, quindi di quanta potenza esce dal laser alla lunghezza d'onda di $532nm$, dipende da tre parametri:

- orientamento del cristallo
- polarizzazione della luce incidente
- temperatura del cristallo

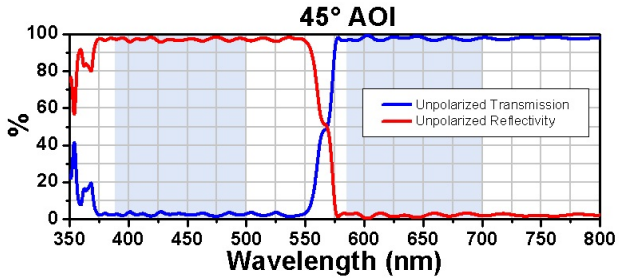
Il cristallo è posto in un contenitore progettato appositamente per mantenere la temperatura dell'LBO attorno i 150°C. Il posizionamento del cristallo e la scelta dell'appropriata polarizzazione vengono fissati al momento dell'assemblaggio, quindi per ottenere la condizione di phase matching si varia la temperatura, che assumerà valori vicino ai 150°C. I due raggi, l'infrarosso e il verde, si propagano collinearmente, e vengono separati all'uscita dell'LBO attraverso uno specchio dicroico, il cui coating è trasparente a $532nm$, mentre riflette la radiazione a $1064nm$.

4.3 Componenti ottici

Diamo ora una piccola descrizione dei componenti utilizzati nel nostro esperimento.

4.3.1 Specchi

Gli specchi utilizzati nel nostro esperimento si distinguono in due gruppi. Gli specchi usati prima del cristallo SPDC sono del tipo dicroico, ovvero riflettono una certa λ e ne lasciano passare un'altra. Infatti la radiazione in uscita al cristallo SHG è composta di due componenti: la componente di pompa del cristallo SHG a $\lambda = 810nm$ e quella generata dal cristallo a $\lambda = 405nm$. Queste due componenti vanno separate, poichè la radiazione a $\lambda = 810nm$ proveniente dal MIRA, introduce rumore, in quanto, avendo la stessa lunghezza d'onda della radiazione parametrica (quella generata dal cristallo SPDC, che costituisce il solo segnale da individuare), verrebbe misurata come segnale utile, alterando la misura. Gli specchi vengono usati per riflettere il viola ($\lambda = 405nm$), al fine di guidarlo verso il cristallo SPDC, mentre il rosso ($\lambda = 810nm$) viene trasmesso e bloccato subito dietro lo specchio. Gli specchi dicroici scelti sono il modello *DMLP567* della Thorlabs. In tabella 4.1b e nel grafico 4.1a sono riportate le specifiche per la banda di trasmissione/riflessione.



(a) Grafico Trasmissione/Riflessione DMLP567

Specifiche per la Banda	
Banda passaalto (50%)	567 nm
Banda riflessione($R_{avg} > 90\%$)	380 - 550 nm
Banda Trasmissione($T_{avg} > 90\%$)	584 - 700 nm

(b) Specifiche DMLP567

Gli specchi utilizzati dopo il cristallo SPDC per guidare la radiazione a $\lambda = 810nm$, sono del tipo dielettrico (modello *BB1-E03* catalogo Thorlabs),

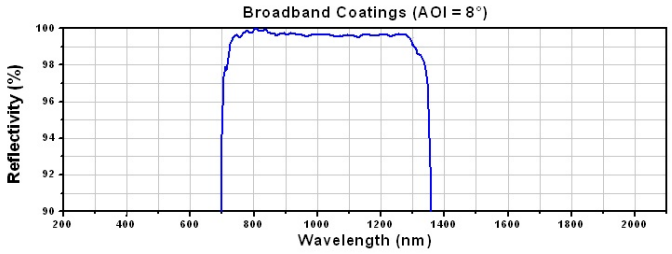


Figura 4.1: Grafico riflettività BB1-E03

con una buona riflettività ($R_{avg} > 99\%$) nella regione dell'infrarosso. In figura 4.1 viene riportato il grafico della riflettività per un angolo di incidenza (AOI) di 8° Ogni specchio è montato su un supporto tip-tilt, che permette di inclinare la direzione del fascio in orizzontale e verticale.

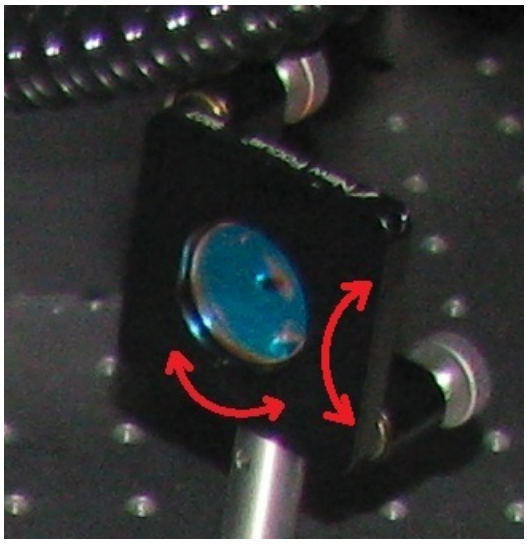


Figura 4.2: Specchio su montaggio tip-tilt

4.3.2 Lenti

Per le lenti vale lo stesso discorso fatto precedentemente per gli specchi, ovvero a seconda della radiazione da guidare si sono utilizzate lenti in silicio con coating differente, per prevenire il riflesso della superficie. Le lenti utilizzate sono del tipo piano-convesse.

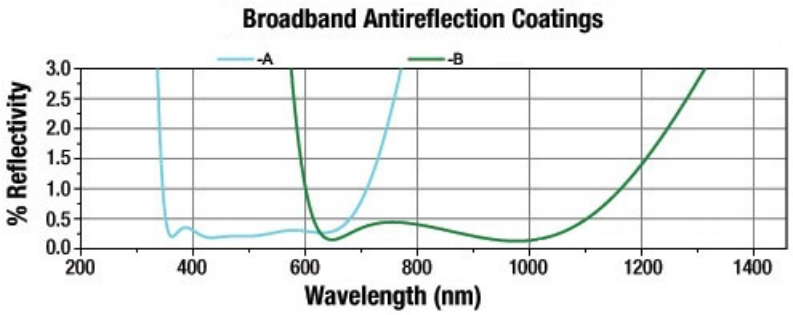


Figura 4.3: Riflettività radiazione incidente. Il coating A è usato per $\lambda = 405nm$, il coating B per $\lambda = 810nm$

4.3.3 Filtri

I filtri sono stati utilizzati per eliminare le componenti di radiazione non desiderata. Poichè gli specchi dicroici non eliminavano del tutto la componente del viola, si è utilizzato un filtro passabanda, centrato a $405nm$ con banda $10nm$ (modello *FB405-10* catalogo Thorlabs)

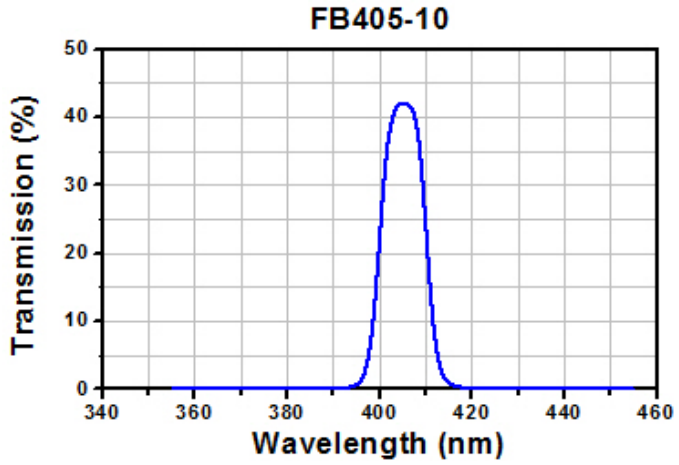


Figura 4.4: Filtro passabanda $\lambda = 405nm$

Per prevenire l'entrata di radiazione viola negli accoppiatori si sono utilizzati filtri per bloccare il viola.

4.3.4 Lamine ritardanti

Le lamine $\lambda/2$ e $\lambda/4$, dette anche ritardanti, sono delle lamine che ritardano una componente del campo incidente rispetto l'altra. Ad esempio, se pensia-

mo al campo incidente suddiviso nelle componenti (E_x, E_y), la trasformazione che comporta la lamina, con asse parallelo all'asse x, è $(E_x, e^{-j\theta}E_y)$ dove θ è lo sfasamento, o ritardo, introdotto dalla lamina. L'asse y risulta quindi 'più lento' dell'asse x. Se $\theta = \pi/2$ si ha una lamina a $\lambda/4$, la quale converte una radiazione con polarizzazione lineare in radiazione con polarizzazione circolare sinistrorsa, e una radiazione con polarizzazione circolare destrorsa in radiazione con polarizzazione lineare. Se invece $\theta = \pi$, si ha una lamina a $\lambda/2$, la quale converte una radiazione con polarizzazione lineare in lineare ma con una rotazione di 2ϕ, dove ϕ è l'angolo tra l'asse ottico della lamina e il vettore di polarizzazione del fascio che l'attraversa. Se invece la radiazione ha polarizzazione circolare destrorsa, viene convertita in circolare sinistrorsa.

4.3.5 Beamsplitter

Il beamsplitter è un dispositivo ottico che divide la radiazione incidente in due componenti, una riflessa e l'altra trasmessa. Entrambe le componenti hanno un'intensità pari alla metà di quella in ingresso al beamsplitter. Nel nostro esperimento sono stati utilizzati beamsplitter polarizzanti (PBS), ovvero le componenti venivano divise a seconda della polarizzazione, ad esempio la radiazione con polarizzazione orizzontale veniva trasmessa mentre quella con polarizzazione verticale veniva riflessa (in questo caso le intensità delle componenti di uscita dipendono dalla polarizzazione del fascio in ingresso).

L'accoppiata lamina $\lambda/2$-PBS costituisce il nostro proiettore. La rotazione della lamina permette di modificare la polarizzazione del fotone, mentre il PBS lo lascia passare con una certa probabilità dipendente dalla polarizzazione imposta dalla lamina.
Supponiamo che il PBS lasci passare i fotoni con polarizzazione orizzontale. Se il fotone arriva con polarizzazione V e la lamina ha l'asse parallelo a V (non modifica la sua polarizzazione) il fotone viene sempre scartato dal PBS, mentre se la lamina rimane nella posizione precedente e il fotone ha polarizzazione H, passa sempre, poichè dopo la lamina si ritrova con polarizzazione H (ruotata di 180°). Se invece la lamina ha l'asse ruotato di $22,5°$ (la polarizzazione viene ruotata di 45°), il fotone con polarizzazione H o V si ritrova, dopo la lamina, con polarizzazione 45° o $-45°$, e riuscirà a passare il PBS con probabilià pari a 0.5.

4.3.6 Fibre ottiche

La rilevazione delle coppie di fotoni generate dal cristallo SPDC viene eseguito da parte di due rivelatori particolari, chiamati SPAD, che devono essere

accoppiati in fibra. Grazie all'utilizzo delle fibre ottiche ed al supporto a 3 assi mobili, è possibile avere una notevole precisione nell'allineamento del setup ottico. Sono stati utilizzati due tipologie di fibre: multimodo e singolo modo. Le prime, avendo la dimensione del core maggiore, permettono di accoppiare il segnale molto facilmente, tuttavia oltre al segnale utile, viene accoppiata anche una elevata componente di rumore. Per questo si sono utilizzate prima le fibre multimodo per un accoppiamento 'grossolano', ed in seguito, per un accoppiamento più 'fine' si sono utilizzate le fibre singolo modo.

4.4 Elettronica di controllo

4.4.1 SPAD

Lo SPAD, *Single Photon Avalanche Diode*, è un fotorilevatore a stato solido basato su una giunzione p-n a polarizzazione inversa in grado di generare una corrente in uscita in risposta alla rivelazione di segnali a bassissima intensità (come la rivelazione di un fotone) grazie al fenomeno della ionizzazione da impatto che permette un'elevata amplificazione interna. A differenza dei classici APD *Avalanche PhotoDiode* gli SPAD operano con una tensione di polarizzazione inversa superiore alla tensione di breakdown. Ad ogni evento rivelato, lo SPAD fornisce in uscita un impulso TTL.

4.4.2 FPGA

Per il conteggio delle coincidenze veniva utilizzata una scheda FPGA. Lo scopo di questa scheda era di determinare la coincidenza di due eventi (nel nostro caso l'arrivo della coppia di fotoni) all'interno di una finestra temporale(*coincidence window* τ_c), fissata a $5ns$. Questa finestra temporale deve essere molto stretta, poichè se due eventi non correlati (fotoni di buoi, dark counts) accadono all'interno di essa vengono classificati come coincidenti, aumentando il numero delle coincidenze reali, cioè quelle date dalle coppie di fotoni entangled. Questo deve essere evitato poichè porterebbe a risultati errati. Nel nostro caso, con una finestra di $5ns$ non si notavano eventi di questo tipo. Tuttavia nel conteggio delle coincidenze totali c'è una quantità di coincidenze accidentali da tener conto. Le coincidenze accidentali si hanno quando due coppie di fotoni entangled vengono generate dallo stesso impulso. Queste coppie non vengono considerate poichè non si è in grado di distinguerle. Infatti l'impulso generato nel Mira ha una durata che va da qualche centinaio di femtosecondi a qualche picosecondo, in base alla configurazione adottata. Se un impulso genera due coppie, significa che queste sono separate

temporalmente al massimo di qualche picosecondo, valore troppo basso per poterle distinguere. Il conteggio delle coppie accindentali è dato da

$$R_{acc} = \frac{N_1 N_2}{\nu T}$$

con N_1 e N_2 conteggi dei singoli eventi, ν frequenza di ripetizioni dell'impulso laser e T finestra di osservazione (vedi in seguito). Il valore R_{acc} veniva sottratto al totale delle coincidenze. La scheda FPGA si interfacciava al computer tramite USB. Attraverso un programma Matlab si poteva

- iniziare/fermare il conteggio degli eventi
- settare una finestra di osservazione degli eventi(da non confondere con la coincidence window), la cui durata doveva essere multipla di $0.5s$
- leggere il totale degli eventi avvenuti all'interno della finestra di osservazione degli eventi per ciascun rivelatore
- leggere il totale delle coincidenze avvenute all'interno della finestra di osservazione degli eventi
- avere una stima delle coincidenze reali ($R = R_{tot} - R_{acc}$)

Capitolo 5

Setup dell'esperimento

Vediamo ora le varie fasi che si sono susseguite nel montaggio del setup ottico.

5.1 Generazione seconda armonica

Il laser Mira è stato impostato per generare impulsi con $\lambda = 808nm$ della durata di $150fs$, con una potenza media di $P = 2,9W$.
Per generare la seconda armonica, il cristallo SHG è stato posizionato in uscita dal Mira su un supporto tip-tilt che permetteva anche la rotazione del cristallo. L'efficienza della generazione della radiazione a $\lambda = 404nm$ dipende dalla direzione dell'asse ottico del cristallo, per questo era necessario operare sulla rotazione e sul tilt dell'asse ottico. Inoltre, sempre per aumentare l'efficienza (vedi eq. 3.7), il fascio laser di pompa è stato focalizzato nel cristallo utilizzando una lente con focale $f = 150mm$. In seguito il fascio è stato collimato con una lente a focale $f = 150mm$, ed è stato guidato, utilizzando specchi dicroici per eliminare la radiazione di pompa, al cristallo SPDC. Questo cristallo è stato montato su un supporto tip-tilt con rotazione sopra una *breadboard* per una eventuale futura applicazione esterna al laboratorio. Il fascio viola è stato fatto passare per due iridi (I_5 e I_6 fig. 5.3), uno posto prima del cristallo SPDC e uno dopo il cristallo, ad una distanza di circa $40cm$. In questo modo se il fascio subisce una deviazione è possibile riallineare il sistema facendo passare il fascio per i due iridi. Il fascio uscente dal Mira ha polarizzazione orizzontale, mentre la radiazione viola ha polarizzazione verticale (dovuta al phase matching).

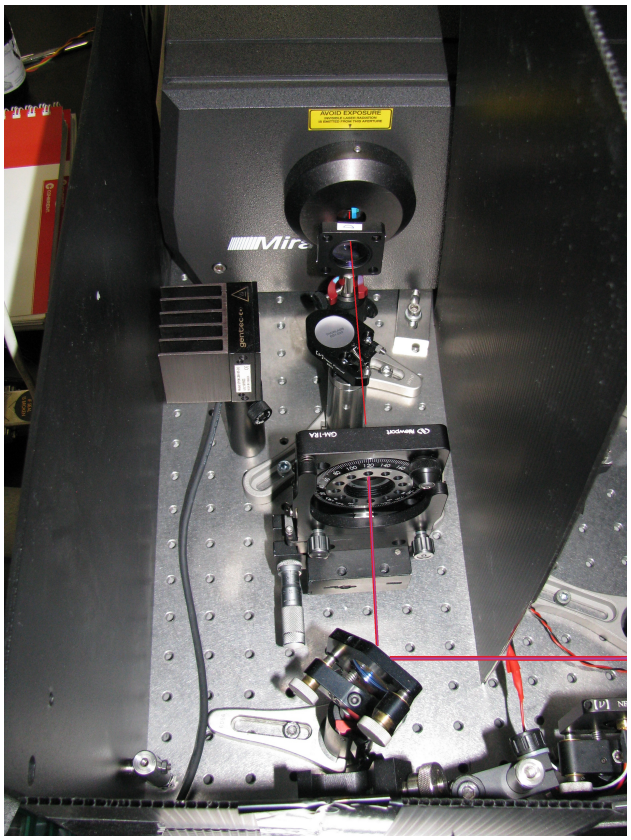


Figura 5.1: Cristallo di seconda armonica. Viene mostrato il percorso della pompa del cristallo SHG e della radiazione di seconda armonica

5.2 Generazione cerchi parametrici

Per la generazione SPDC è stato utilizzato inizialmente un cristallo BBO type-II. Per poter osservare i cerchi parametrici è stato necessario eliminare la pompa a $\lambda = 404nm$. Per far ciò è stato messo uno specchio dicroico per riflettere la radiazione a $404nm$ e trasmettere la radiazione generata dalla SPDC a $808nm$ e in seguito un beam stopper per bloccare la rimanente.

Per visualizzare i cerchi parametrici è stato utilizzato un intensificatore d'immagine, un dispositivo che permette di amplificare di migliaia di volte la luce in ingresso, seguito da una camera a basso rumore, il modello è l'*Allied G-145B/C*. Inoltre per eliminare la componente di radiazione a $\lambda = 404nm$ che passa oltre il beam stopper, sono stati utilizzati filtri passa alto con lunghezza d'onda di cut-on a $750nm$. Nello stesso modo in cui si è tenuto riferimento della direzione del fascio viola, sono stati posizionati due iridi per ciascuna

intersezione dei cerchi parametrici. In questo modo è possibile creare un sistema di simulazione con due laser, a $\lambda = 635nm$, posti prima del cristallo SPDC. Infatti la radiazione SPDC è molto debole, non visibile ad occhio nudo. Utilizzando i due laser invece, è possibile vedere la direzione delle intersezioni, rendendo l'allineamento più agevole. In figura 5.2 è mostrata

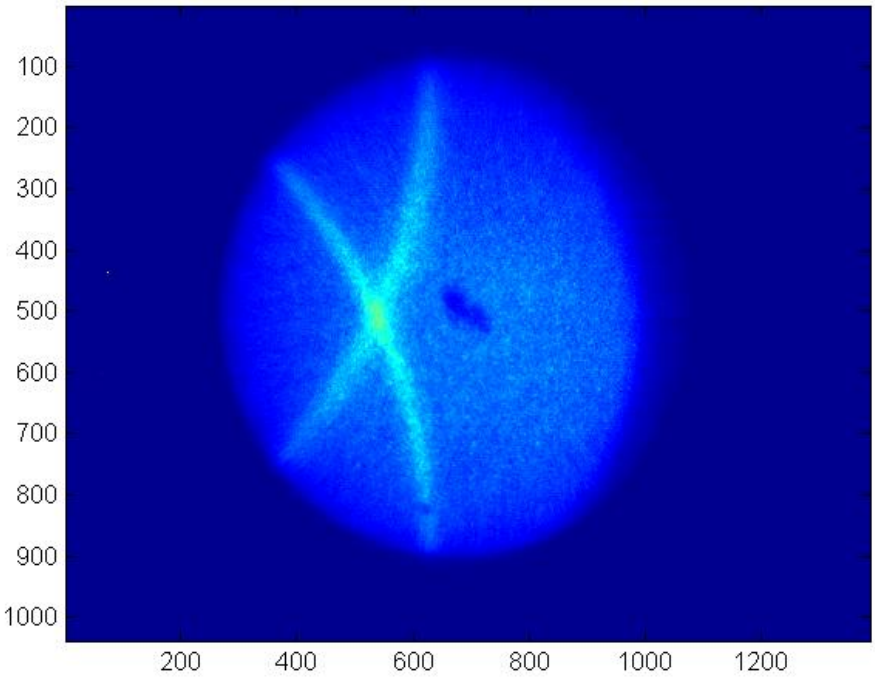


Figura 5.2: Intersezione cerchi parametrici

l'intersezione destra dei cerchi parametrici. Gli iridi venivano centrati sempre utilizzando l'intensificatore e la camera.

Rimozione della pompa dalla radiazione SHG

Per eliminare la componente di rosso del fascio del Mira, che si propaga insieme alla radiazione di seconda armonica, si è utilizzato un filtro (inizialmente si era adottata una soluzione alternativa, utilizzando un singolo prisma, ma questa soluzione è stata abbandonata poichè l'impulso subiva una dispersione temporale e spaziale). Il fascio che incide su questo filtro (F_1 vedi fig.5.3) non deve essere troppo focalizzato, altrimenti c'è il rischio di danneggiare il filtro stesso. Per evitare ciò, si è lasciato divergere il fascio finchè il diametro non

fosse di circa $4mm$, si è inserita una lente L_2 con $f = 750mm$ di collimazione ed il filtro. In seguito è stata inserita una lente L_3 con $f = 750mm$ per rifocalizzare il fascio ed una lente L_4 con $f = 150mm$ per collimarlo (vedi app. A). Con questa configurazione la potenza del fascio a $\lambda = 404nm$ prima del cristallo SPDC oscillava tra i $20mW$ e i $35mW$. Il fascio inoltre doveva essere ben focalizzato nel cristallo, infatti un recente lavoro svolto presso i nostri laboratori ha evidenziato quanto questa procedura sia delicata. Mancando la posizione di fuoco di pochi mm, la collezione della fluorescienza parametrica perde più del 20% di efficienza [Vil12].

5.3 Setup ottico

Il setup finale dell'esperimento è mostrato in figura 5.3. Dopo aver posizionato gli iridi che individuano la direzione delle intersezioni dei cerchi parametrici sono stati posizionati gli specchi dielettrici, i filtri F_2 e i collimatori. Il percorso che segue la radiazione parametrica (mostrato in fig. 5.3) è stato scelto per motivi di spazio. Tale percorso inoltre doveva essere uguale per entrambe le direzioni, poichè se i percorsi fossero differiti in lunghezza, i fotoni della coppia sarebbero arrivati con tempi diversi, impedendo la coincidenza. Una volta posizionati i collimatori, si è fatto un primo allineamento del sistema. Per far ciò, si è collegato un laser in fibra ai collimatori (vedi fig. 5.4). La fibra utilizzata per collegare il laser al collimatore era una fibra multimodo, utilizzata in seguito per collegare il collimatore allo SPAD. In questo modo è stato simulato il percorso della radiazione parametrica al contrario, dai collimatori al cristallo SPDC. Il sistema di simulazione a due laser (par. 5.2) era utile per un primo allineamento degli specchi, ma non permetteva di allineare correttamente i collimatori. Per allineare il braccio superiore si sono utilizzati gli assi del collimatore e i tip-tilt degli specchi S_{dich4} e S_{dich4}, in modo che il fascio in uscita dal collimatore passasse per i due iridi I_4 e I_5. Lo stesso veniva ripetuto per l'altro braccio. In questo modo ottenevamo un buon allineamento di partenza. La procedura descritta precedentemente si è rivelata buona anche nel caso in cui si deve ritrovare un discreto allineamento in seguito alla perdita totale di una o entrambe le direzioni.

Il passo successivo è stato collegare gli SPAD ai collimatori con le fibre multimodo, le quali devono avere la stessa lunghezza (per lo stesso motivo visto precedentemente). Gli SPAD a loro volta erano collegati alla scheda FPGA con cavi coassiali. In questo caso, però i cavi erano di lunghezze diverse per motivi di progettazione del programma di controllo della scheda FPGA. A questo punto si ottimizza l'allineamento. Innanzitutto si doveva controllare la direzione del fascio di pompa del cristallo SPDC, se non passa-

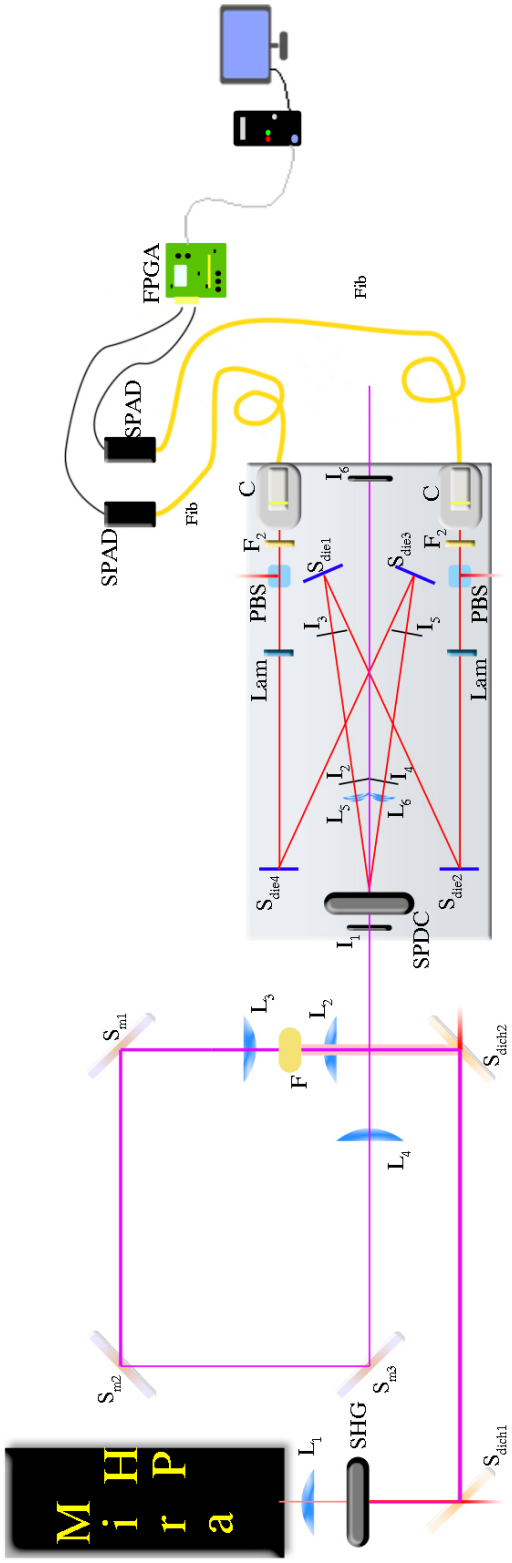


Figura 5.3: Setup ottico. Elenco componenti: L_1 lente con $f = 150mm$, L_2 lente con $f = 750mm$, L_3 lente con $f = 750mm$, L_4 lente con $f = 150mm$, L_5 lente con $f = 100mm$, L_6 lente con $f = 100mm$, SHG cristallo seconda armonica, S_{dich} specchio dicroico, S_m specchio metallico, S_{die} specchio dielettrico, I iride, F_1 filtro per $405nm$, F_2 filtro per $810nm$, Lam lamina $\lambda/2$, PBS beamspletter polarizzante, C collimatore, Fib fibra ottica

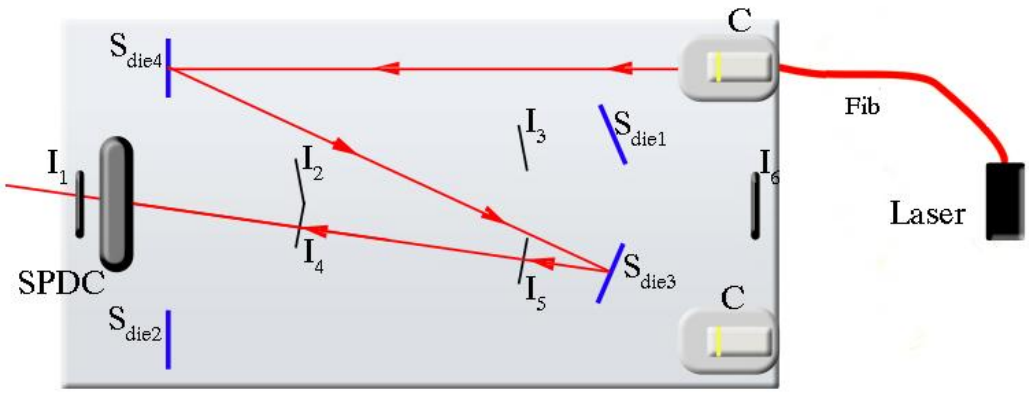


Figura 5.4: Allineamento braccio

va per i due iridi I_1 e I_6 si allineava il fascio sugli iridi utilizzando gli specchi metallici (S_{m1}, S_{m2}, S_{m3}). In seguito si controllavano i conteggi dei singoli SPAD, e le coincidenze. Se l'allineamento fatto precedentemente era buono, attraverso la scheda di acquisizione FPGA si iniziano ad individuare delle coincidenze tra i due canali. Per sapere se queste coincidenze sono generate dai fotoni entangled o da rumore di fondo si ruota il cristallo SPDC. Ruotando il cristallo si cambia il phase matching fino al punto di non avere più generazione parametrica. Se dopo aver ruotato il cristallo di 90° le coincidenze sono sparite, allora le coincidenze che si ottenevano prima sono dovute a fotoni entangled generati via SPDC.
Se il numero di coincidenze è basso si procede con una serie di operazioni:

1. si massimizzano i singoli conteggi di un braccio operando sugli specchi e sul collimatore di quel braccio, cercando di non perdere mai del tutto le coincidenze

2. si massimizzano le coincidenze agendo sugli specchi e sul collimatore dell'altro braccio, cercando contemporaneamente di aumentare i singoli conteggi

3. si ripetono i punti 1 e 2

4. Se non si notano miglioramenti si prova a massimizzare il rate delle coincidenze con piccoli spostamenti degli specchi in entrambi i bracci.

Successivamente sono state inserite le lamine $\lambda/2$, i PBS e sono state aggiunte le lenti L_5 e L_6 con focale $f = 100mm$ a distanza f dal cristallo SPDC. In questo modo si riusciva a collimare meglio la radiazione parametrica, aumentando l'efficienza del sistema. Con questa configurazione sono state

fatte misure a $\approx 200Kc/s$ (c/s conteggi al secondo) per canale e $\approx 20Kc/s$ coincidenze, mentre prima si arrivava a $\approx 110Kc/s$ per canale (singles) e $\approx 10Kc/s$ coincidenze con una potenza di pompa di $\approx 30mW$. L'efficienza, riferita a quanti singles concorrono nella rivelazione di una coppia, è del $\eta_M = \frac{N_s}{N_c} \cong 10\%$.
Dopo l'inserimento della lamina e PBS le coincidenze vengono ripartite sui due stati $|HV\rangle$ e $|VH\rangle$. Per ottenere lo stato $|HV\rangle$ si ruota una lamina a 0° e l'altra a 45° mentre per lo stato $|VH\rangle$ si ruota una lamina a 45° e l'altra a 0° (vedi app.B).

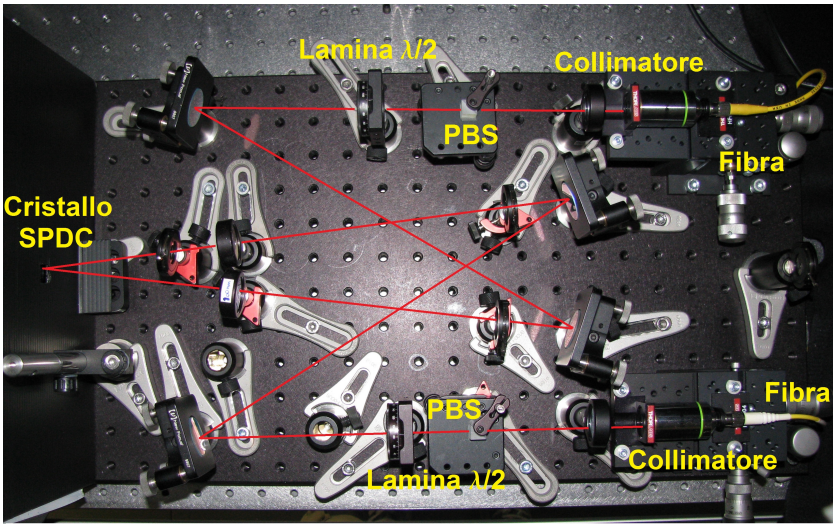


Figura 5.5: Particolare del setup ottico relativo alla rivelazione delle intersezioni

Se spostandosi da uno stato all'altro il numero di coincidenze non è uguale (o comunque molto simile) significa che non si stanno prendendo correttamente le direzioni delle coincidenze. Per correggere il rate delle coincidenze ho utilizzato questa procedura

1. si ruota il cristallo (non oltre 1°-2°) in una posizione di compromesso, ovvero si cerca la posizione che permette di alzare un po' le coincidenze dello stato che ne aveva di meno (con le fibre multimodo questo metodo era poco efficace).

2. mettendosi nello stato con meno coincidenze si osservano i singoli. Se un canale è più basso dell'altro si cerca di portarlo ad un livello più alto (agendo sugli specchi e collimatore del braccio in questione) e con

l'altro canale si cerca di ottimizzare le coincidenze. Se invece i singoli sono uguali, si ripetono i punti 1 e 2 della procedura precedente

3. si passa sull'altro stato, se le coincidenze sono più basse dell'altro si ripete il punto 2 tenendo questo stato

4. infine, se passando da uno stato all'altro il rate delle coincidenze è molto simile, si ottimizza il rate delle coincidenze con piccoli movimenti degli specchi e dei collimatori per entrambi li stati, mantenendo le coincidenze il più possibile uguali

Finito questo allineamento, sono stati riallineati gli iridi I_2, I_3, I_4 e I_5 in modo da selezionare la direzione ottenuta. Le fibre multimodo permettono un rapido allineamento, poichè avendo un core di dimensioni maggiori permettono la propagazione di più modi, guidando fasci che entrano con direzioni che si discostano dall'asse ottico principale. Successivamente sono state montate le fibre singolo modo. Poichè il sistema è ottimizzato per le fibre multimodo, si deve agire con piccoli spostamenti prima sui collimatori e poi sugli specchi per ottenere nuovamente un buon allineamento. Con le fibre singolo modo si può osservare l'interferenza (vedi par. 1.2.4) della coppia entangled sulla base $\{+,-\}$. Con le fibre multimodo ciò succedeva in parte, ovvero si aveva una visibilità (1.17) $V = 93\%$ nella base $\{H,V\}$, mentre per la base $\{+,-\}$ non si è mai ottenuto un valore migliore di $V = 50\%$.
Con le fibre singolo modo invece si è ottenuta per la base $\{H,V\}$ una visibilità fino al $V = 98\%$ mentre per la base $\{+,-\}$ una $V = 96\%$. Tuttavia non è detto che se la visibilità sulla base $\{H,V\}$ è buona, allora lo sia anche sulla base $\{+,-\}$. Spesso si riusciva ad ottenere una buona visibilità su $\{H,V\}$ mentre su $\{+,-\}$ scendeva anche a 0. Questo è dovuto al fatto che non si prendevano correttamente le intersezioni dei cerchi parametrici. Per evitare ciò, un metodo che ha portato ad avere buona visibilità in entrambe le basi consisteva nell'allineare il setup ottico facendo riferimento alla base $\{+,-\}$, ovvero massimizzando gli stati $|+-\rangle$ e $|-+\rangle$. In questo modo, quando poi si passava sulla base $\{H,V\}$ si aveva già una buona visibilità. In questa configurazione si otteneva un rate di singles di $N_s \approx 8Kc/s$, mentre per le coincidenze si arrivava a $N_c \approx 500c/s$, con una efficienza $\eta_S = \frac{N_s}{N_c} \cong 6\%$, con una potenza di pompa di $\approx 30mW$. In seguito a varie ottimizzazioni del sistema si è arrivati ad avere nel caso migliore $N_s \approx 10Kc/s$ e $N_c \approx 1000c/s$ con una efficienza $\eta_S \cong 10\%$. I metodi descritti per allineare il setup sono solo una linea guida, poichè di volta in volta bisognava valutare la direzione verso cui spostare gli specchi per non allontanarsi troppo dalla direzione delle intersezioni perdendo di conseguenza il segnale.

Infine è stata aggiunta una lamina $\lambda/2$ dopo la lente L_4 ed è stato sostituito il cristallo SPDC type-II con il doppio cristallo type-I per poter generare lo stato non massimamente entangled (vedi par. 3.6). Inoltre è stato cambiato il modo di funzionamento del Mira, in modo da ottenere impulsi della durata di $7ps$. Quando la radiazione si propaga all'interno del cristallo SPDC type-I (si ricorda che in questo caso i cristalli sono 2 consecutivi con assi ottici perpendicolari) gli impulsi in uscita hanno velocità diverse a seconda della polarizzazione in ingresso. Infatti incidendo con polarizzazione a 45° si può pensare di scomporre il fascio in due fasci, uno con polarizzazione H e l'altro con polarizzazione V. Questi due fasci, all'interno dei cristalli viaggeranno a velocità diverse a causa della differenza degli indici di rifrazione (ordinario e extraordinario). La differenza temporale che si ha tra i due impulsi in uscita (riferiti alle coppie HH e VV) è stata calcolata supponendo che le coppie fossero generate a metà del cristallo (ogni cristallo era lungo $1mm$) e vale $d \approx 200fs$. Come si vede in figura, nel caso si utilizzi il laser in modalità femto, con impulsi lunghi circa $150fs$, in uscita al cristallo gli impulsi derivanti dalle polarizzazioni H e V non si sovrappongono. Utilizzando il laser in modalità pico invece si riesce ad avere una migliore sovrapposizione.

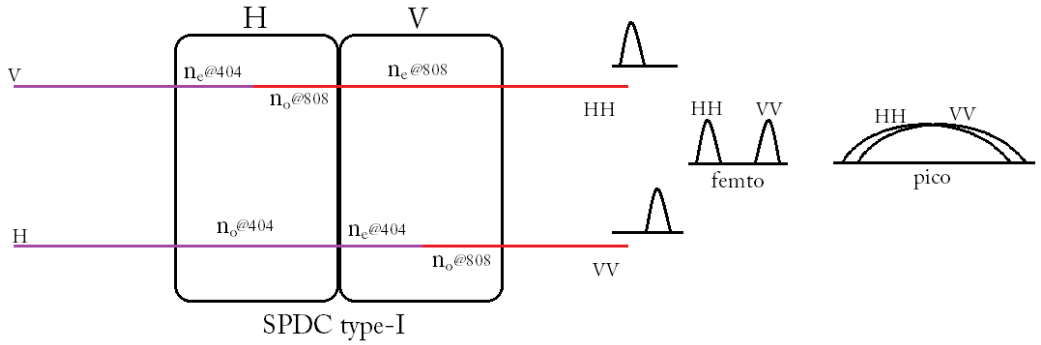


Figura 5.6: Impulsi in uscita al cristallo SPDC a seconda della modalità di funzionamento scelta (femto/pico)

Capitolo 6

Risultati misure

In questo capitolo vengono mostrate le fasi di preparazione delle misure per i protocolli ent-B92 e B92-gen. In seguito vengono mostrati i risultati ottenuti nei due casi diversi. Inoltre si è cercato, prima attraverso una simulazione con Matlab e poi con una prova sperimentale, di trovare quali stati massimizzassero il guadagno G per uno stato entangled definito in 2.5 con $\theta = \pi/3$.

6.1 Caratterizzazione della sorgente

L'instabilità della potenza della radiazione di seconda armonica e della lunghezza d'onda del laser Mira impedivano il successo della misura. Vediamo di seguito come queste instabilità influenzassero le misure.

Variazioni della lunghezza d'onda nel Mira

Lo stato entangled generato (eq.3.36) poteva avere un contributo di fase non nullo, e questo portava ad avere per gli stati misurati, un rate di coincidenze sbagliato. Vediamo cosa succede nel caso delle misure sugli stati $|-\overline{\varphi}_1\rangle$ e $|+\overline{\varphi}_0\rangle$. Consideriamo uno stato entangled con fase ϕ non nulla

$$|\Psi\rangle = \cos(\theta/2)|HH\rangle + e^{j\phi}\sin(\theta/2)|VV\rangle \tag{6.1}$$

Fissato θ abbiamo che la misura sullo stato $|-\overline{\varphi}_1\rangle$ ha una probabilità (lo stesso vale per $|+\overline{\varphi}_0\rangle$)

$$\begin{aligned} P_{-\overline{\varphi}_1} =& |\langle -\overline{\varphi}_1|\Psi\rangle|^2 \\ =& \frac{1}{2}\left|\cos(\theta/2)\sin(\theta/2) - e^{j\phi}\cos(\theta/2)\sin(\theta/2)\right|^2 \\ =& C|1-e^{j\phi}|^2 = 4C\sin^2(\phi/2) \end{aligned} \tag{6.2}$$

L'equazione 6.2 mostra che, nel caso in cui si ha $\phi \neq 2k\pi$, la probabilità $P_{-\overline{\varphi}_1}$ risulta maggiore di 0. Queste probabilità sono presenti nel calcolo di S_H con un segno "-" e, per valori $P_{-\overline{\varphi}_1} > 0$ e $P_{+\overline{\varphi}_0} > 0$, si ha un valore minore di S_H. Inoltre, dalla relazione di G con S_H 2.16 si osserva che una diminuzione di S_H corrisponde ad un guadagno più basso. In figura 6.1 viene mostrato

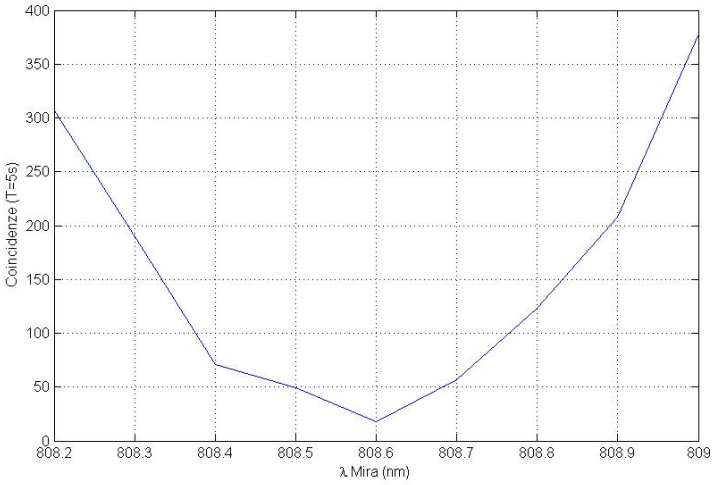
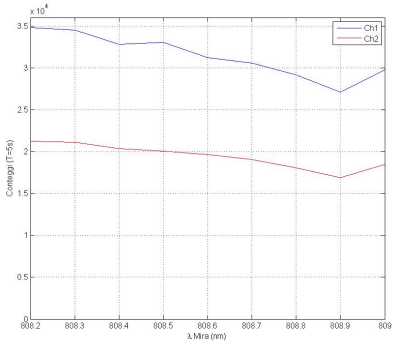
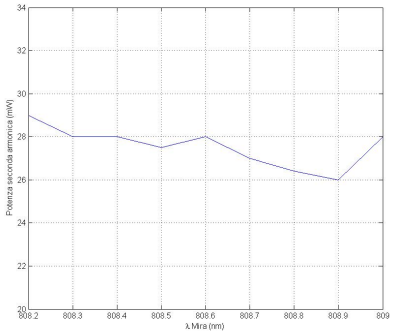


Figura 6.1: Variazione coincidenze al variare di λ per lo stato $|-\overline{\varphi}_1\rangle$

come variano le coincidenze riferite allo stato $|-\overline{\varphi}_1\rangle$ al variare di λ.
Come si è visto sopra, fissato θ, la probabilità di misurare lo stato $|-\overline{\varphi}_1\rangle$ è proporzionale ad $\sin^2(\phi/2)$, e il grafico 6.1 mostra proprio questo andamento. Variazioni dell'ordine dei decimi di nm sulla λ corrispondono ad aumenti superiori al 100% sul numero di coincidenze. Si potrebbe pensare che questo sia dovuto a variazioni della potenza di seconda armonica (più potenza, più coppie entangled), ma come si nota dalle figure 6.2a e 6.2b la potenza ed i singoli rimangono abbastanza costati. Si nota ad esempio che per $\lambda = 808,9nm$ la potenza ed i singoli si abbassano più che negli altri punti, mentre le coincidenze continuano a seguire il profilo di $\sin^2(\phi/2)$.
Le variazioni della λ corrispondono a piccole variazioni del fascio all'interno del cristallo SPDC, le quali comportano a variazioni della fase in 6.1 [JBA05]. Durante il funzionamento del laser si sono notate variazioni improvvise (nell'ordine di $0.1/0.2nm$ per la durata di qualche secondo) della λ attorno al valore medio.



(a) Variazione singoli al variare della λ per lo stato $|-\overline{\varphi}_1\rangle$



(b) Variazione della potenza al variare della λ

Variazioni della potenza di pompa

Un altro problema riscontrato riguarda la variazione della potenza della radiazione di seconda armonica. Queste variazioni possono essere dovute all'instabilità della potenza e della λ della radiazione in uscita dal Mira, in quanto viene a modificarsi il phase matching sul cristallo SHG. In figura 6.2 viene

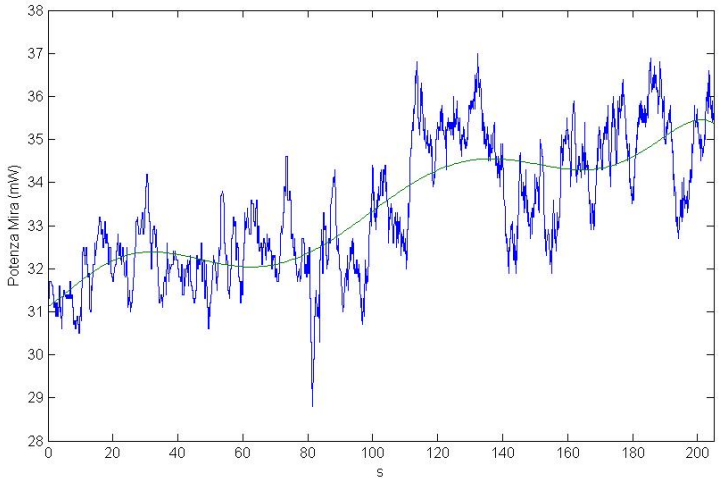


Figura 6.2: Misura della potenza di seconda armonica. Funzionamento non stabile

mostrato che nell'arco di circa 3 minuti la potenza di seconda armonica aumenta di $5mW$. A questa variazione di potenza è corrisposto un incremento dei conteggi dei singoli di circa $1000c/s$ per canale, e per le coincidenze, nello stato $|HH\rangle$ ci circa $60c/s$.

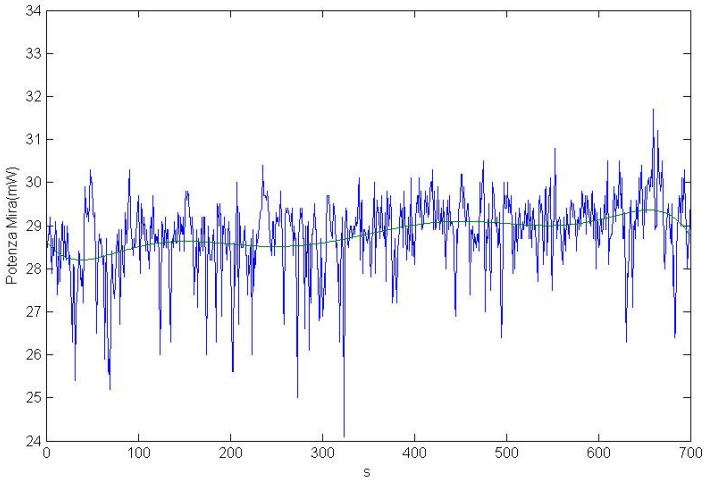


Figura 6.3: Misura della potenza di seconda armonica. In questo caso si nota che il funzionamento del laser è molto più stabile, in quanto la potenza media è rimasta sempre attorno ad un valore di $28,5mW$

L'acquisizione del set base di misure (6.5) richiedeva non meno di 5 minuti, perciò se la potenza di seconda armonica in questo tempo variava sensibilmente (oltre il mW) si ottenevano risultati errati, portando S_H e G a valori troppo elevati o troppo bassi.

6.2 Preparazione della misura

Vediamo ora le operazioni che venivano eseguite prima di effettuare una misura.

Prima di effettuare la misura, veniva controllato che il setup ottico fosse ben allineato e che la lamina $\lambda/2$ utilizzata per generare lo stato non massimamente entangled fosse a $22,5°$ (per avere polarizzazione a 45° sul cristallo SPDC). Si doveva avere una buona visibilità nelle basi $\{H, V\}$ e $\{+, -\}$ (soprattutto in quest'ultima, per la quale ho scelto come limite inferiore una $V = 95\%$) e le coincidenze su HH, VV, $+-$ e $-+$ dovevano essere molto simili fra loro (abbiamo visto che la probabilità di misurare uno dei precedenti stati partendo da uno stato entangled è la stessa, par. 1.2.4). Se non era così si cercava ad portarle tutte allo stesso rate operando con piccoli spostamenti sugli elementi del setup ottico, altrimenti si procedeva ad allinearlo come mostrato nel capitolo 5. In seguito si controllava che la lunghezza d'onda del

Mira fosse stabile a $808nm$ e che la potenza della radiazione di pompa del cristallo SPDC non fosse inferiore ai $20mW$.

6.3 Misure protocollo ent-B92

L'obiettivo è di mostrare la possibilità di ottenere un guadagno di chiave sicura $G > 0$ in modo da verificare la sicurezza del protocollo ent-B92. Per far ciò dobbiamo stimare la S_H usando un set di 4 misure, più il totale delle coincidenze generate. Gli stati da misurare sono

$$|V\overline{\varphi}_1\rangle \quad |V\varphi_0\rangle \quad |-\overline{\varphi}_1\rangle \quad |+\overline{\varphi}_0\rangle$$

mentre il totale delle coincidenze si ottiene effettuando la somma delle coincidenze misurate sugli stati definiti da una base ortogonale (abbiamo scelto la base $\{H, V\}$)

$$|HH\rangle \quad |VV\rangle \quad |HV\rangle \quad |VH\rangle$$

La stima di S_H veniva perciò valutata in questo modo:

$$S_H = \frac{N(V\overline{\varphi}_1) - N(V\varphi_0) - N(-\overline{\varphi}_1) - N(+\overline{\varphi}_0)}{N(HH) + N(VV) + N(HV) + N(VH)} \tag{6.3}$$

dove $N(JI)$ indica il rate di coincidenze nella misura degli stati J e I. Ricordiamo che la probabilità di ottenere lo stato $|J\ I\rangle$ si ottiene dividendo il numero delle coincidenze ottenute in quello stato per il totale delle coincidenze, cioè $P_{JI} = |\langle JI|\Phi\rangle|^2 = N(JI)/(N(HH) + N(VV) + N(HV) + N(VH))$.

Selezione stato non max-entangled

L'equazione 2.11 mostra la dipendenza di S_H da θ, il quale definisce il rapporto tra gli stati di 2.5. L'angolo della lamina $\lambda/2$ utilizzata per generare lo stato non massimamente entangled veniva scelto in base al punto di S_H che si voleva misurare. Scelto θ la lamina veniva ruotata in posizione $\theta/4$ (la lamina $\lambda/2$ ha periodo $p = \pi$ e si veda 2.3). A questo punto si faceva una prima misura sulla base $\{H, V\}$, e si stimava il valore di θ

$$\theta = \frac{\arctan(\sqrt{\frac{N(HH)}{N(VV)}}) \cdot 180}{\pi \cdot 2} \tag{6.4}$$

con $N(HH)$ e $N(VV)$ numero delle coincidenze per gli stati $|HH\rangle$ e $|VV\rangle$ su una finestra temporale di a $3s$. Se il valore di θ differiva da quello voluto si provvedeva a ruotare la lamina $\lambda/2$ fino ad ottenere un valore di θ apprezzabile. Per la selezione degli stati $|\varphi_0\rangle$, $|\varphi_1\rangle$ e dei loro ortogonali si ruotavano le

lamine $\lambda/2$ davanti ai collimatori di $\theta/4$ in avanti rispetto alla posizione dello $0°$ per $|\varphi_1\rangle$ e di $\theta/4$ indietro rispetto allo $0°$ per $|\varphi_0\rangle$. Gli stati ortogonali si ottengono ruotando le lamine di $45°$ rispetto le posizioni precedenti.

Ottimizzazione fase stato entangled

Una condizione importante per avere una buona stima di S_H era che gli stati $|+\overline{\varphi}_0\rangle$ e $|-\overline{\varphi}_1\rangle$ avessero un rate di coincidenze molto basso, cioè $N(+\overline{\varphi}_0) \approx 0$ e $N(-\overline{\varphi}_1) \approx 0$ (vedi par.2.10). Poichè questa condizione dipende dalla fase dello stato entangled, si tiltava di poco il cristallo SPDC lungo la direzione dell'asse ottico finchè non si otteneva una buona condizione per le coincidenze, $N(+\overline{\varphi}_0) \approx N(-\overline{\varphi}_1) \approx 3 - 5c/s$.

Finestra di osservazione

In seguito si fissava la finestra di osservazione ad un valore $T \geq 20s$, poichè per valori elevati di T la statistica del processo risulta più accurata. Tuttavia non si poteva scegliere un valore troppo elevato, poichè molte volte il Mira, durante l'intervallo delle misure, non riusciva a rimanere stabile in potenza ed in λ portando a delle misure non corrette (vedi 6.1). Veniva perciò scelto un T per il quale si riusciava ad ottenere un valore totale di coincidenze nella base $\{H, V\}$ di circa $7Kc$.

Misure

A questo punto iniziavano le misurazioni degli stati necessari a stimare S_H e G. L'ordine in cui sono stati misurati gli stati è il seguente:

$$\begin{aligned} HH \to VV \to HV \to VH \to -\overline{\varphi}_1 \to -\overline{\varphi}_0 \to \\ \to +\overline{\varphi}_0 \to +\overline{\varphi}_1 \to V\overline{\varphi}_1 \to V\varphi_0 \to HH \to VV \end{aligned} \tag{6.5}$$

in questo modo si ruotava una sola lamina alla volta. Le misure su HH e VV sono state ripetute alla fine per capire se il numero delle coincidenze totali era diminuito o aumentato a causa dell'instabilità del Mira (vedi 6.1). Nel caso in cui vi fosse una notevole differenza, l'intero set di misure veniva scartato, altrimenti si continuava a prendere le misure sugli altri stati. Le misure venivano scartate anche se la λ del Mira oscillava per più di qualche nm, in quanto si ottenevano valori di $N(+\overline{\varphi}_0)$ e $N(-\overline{\varphi}_1)$ elevati. Questi due valori infatti si utilizzano nel calcolo del $QBER$

$$QBER = \frac{N_{err}}{N_{conc}} = \frac{N(-\overline{\varphi}_1) + N(+\overline{\varphi}_0)}{N(-\varphi_1) + N(+\varphi_0) + N(-\overline{\varphi}_1) + N(+\overline{\varphi}_0)},$$

essendo $N(-\overline{\varphi}_1) + N(+\overline{\varphi}_0)$ la somma degli errori commessi.
In tabella 6.4 sono state riportate le misure per cui si è ottenuto un $QBER < 5\%$, mentre in figura 6.7 sono riportati i valori di S_H e di G.
Nel calcolo di G si è tenuto conto di un $QBER$ medio del 2.5%, ottenuto mediando i $QBER$ di ogni singola misura. Si nota che, nelle misure con $QBER$ basso, si riescono ad ottenere buoni risultati per G. Per $\theta = \pi/3$ si è riusciti ad ottenere un $QBER = 1.4\%$ a cui corrisponde un valore di $G_{\pi/3} = 0.1425$. Questo valore tuttavia è ancora lontano da quello teorico di $G_{teo} = 0.2675$ a causa di un $QBER$ non nullo.

Per tutti i valori in cui $G > 0$ è possibile trasmettere in modo sicuro. Si osserva, dalla figura 6.6, che i punti per i quali si ha un $QBER \approx 2.5\%$ approssimano molto bene la curva teorica di G nella quale è stato tenuto conto un contributo di $QBER$ di circa il 2.5%. Nel grafico è mostrata anche la curva nel caso in cui il $QBER$ sia del 5%. Al di sopra di questo valore è molto difficile ottenere un $G > 0$ per qualsiasi θ.

6.4 Misure protocollo B92-gen

La preparazione del setup per le misure con gli stati $|\varphi_0'\rangle$, $|\varphi_0'\rangle$ ed i relativi stati ortogonali è simile alla precedente. Per l'ottimizzazione del phase matching una volta scelto θ ho utilizzato la procedura precedente.
Poichè in questo protocollo gli stati $|+\overline{\varphi}_0'\rangle$ e $|-\overline{\varphi}_1'\rangle$ hanno una probabilità $P > 0$ di essere misurati, ottimizzavo la posizione del cristallo minimizzando il rate delle coincidenze per gli stati $|+\overline{\varphi}_0\rangle$ e $|-\overline{\varphi}_1\rangle$.
L'angolo θ' dipende dall'angolo θ (si veda 6.4), dalla relazione

$$\theta' = \arctan(\sin\theta).$$

Come prima, per la selezione degli stati $|\varphi_0'\rangle$, $|\varphi_1'\rangle$ e dei loro ortogonali si ruotavano le lamine $\lambda/2$ di un angolo $\theta'/4$ in avanti rispetto alla posizione dello 0° per $|\varphi_1'\rangle$ e di $\theta/4$ indietro rispetto allo 0° per $|\varphi_0'\rangle$. Gli stati ortogonali si ottengono ruotando le lamine di 45° rispetto le posizioni precedenti. La scelta di questi stati permette di avere la massima violazione di S_H. I valori teorici che si ottengono dall'equazione 2.14 vanno considerati come un bound superiore

Dal grafico 6.7 si può osservare che i dati sperimentali riferiti a S_H sono in linea con i dati teorici. Inoltre, com'era atteso, i valori di S_H a parità di θ per il protocollo B92-gen risultano maggiori di quelli ottenuti con il protocollo B92-ent.

HH	VV	HV	VH	θ	$V\overline{\varphi}_1$	$V\varphi_0$	$+\overline{\varphi}_1$	$+\overline{\varphi}_0$	$-\overline{\varphi}_1$	$-\overline{\varphi}_0$	S_H	G	$QBER$
5757	3281	23	63	74,10	2266	1047	3600	257	153	4337	0,0842	-0,1281	0,0491
4878	2255	10	3	68,42	1736	456	2905	58	68	3177	0,1020	0,0563	0,0203
3841	1353	29	13	61,37	1043	344	2122	31	48	1871	0,1184	0,1085	0,0194
8669	2916	12	28	60,22	2236	691	4231	58	68	4363	0,1200	0,1425	0,0144
4450	1318	82	16	57,11	1107	282	1832	34	44	2072	0,1256	0,1306	0,0196
7327	1555	13	15	49,46	1373	265	2328	54	69	2826	0,1105	0,0635	0,0233
4466	654	46	24	41,88	596	66	1265	25	32	1057	0,0911	0,0082	0,0240
7425	811	20	12	36,57	748	73	1656	31	38	1324	0,0736	-0,0255	0,0226
11362	549	29	17	24,79	547	47	957	37	22	934	0,0343	-0,1416	0,0303

Tabella. 6.4: Misure per il protocollo ent-B92

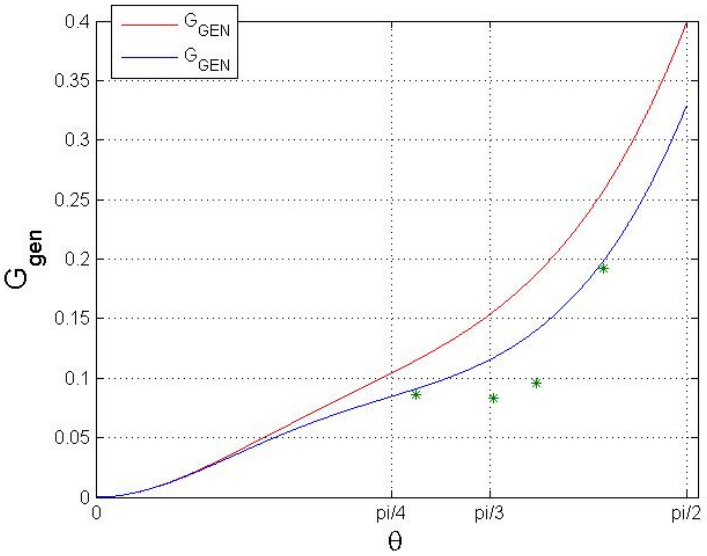


Figura 6.5: Stima G_{GEN}

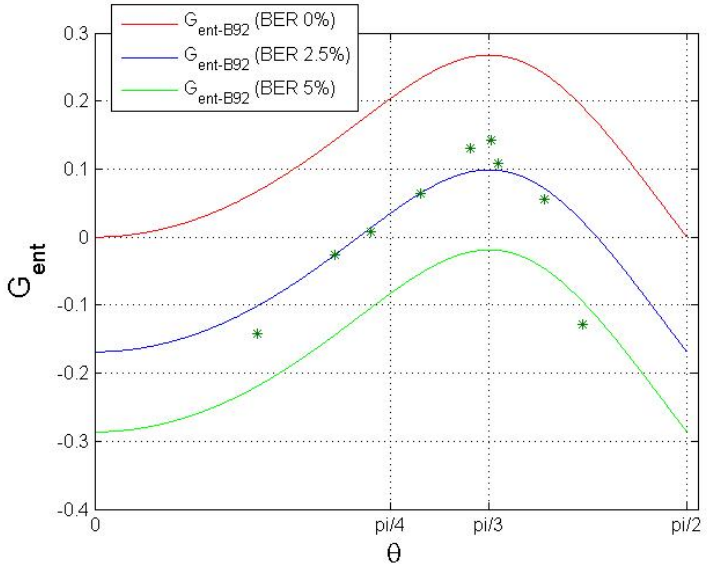


Figura 6.6: Stima G con $QBER = 2.5\%$ e $QBER = 5\%$

Nelle misure per il protocollo B92-gen a causa dell'elevato $QBER$ dovuto alla natura del protocollo, non si riescono ad ottenere buoni valori di G tranne che per valori di θ elevati. Infatti, il valore di S_H per questi valori di θ è molto alto e compensa l'elevato $QBER$.

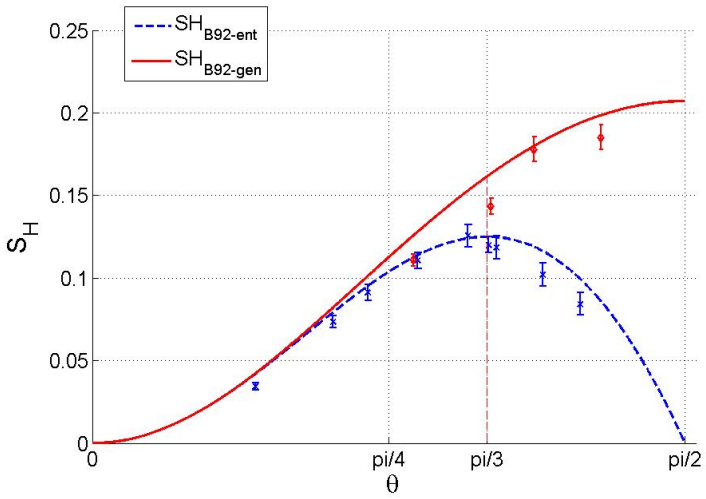


Figura 6.7: Confronto della stima S_H per i protocolli B92-ent e B92-gen

Protocollo per max-G

Poichè il protocollo B92-ent ha un guadagno maggiore rispetto al b92-gen quando $\theta = pi/3$ si sono cercati altri stati che massimizzassero il guadagno G. Attraverso una simulazione Matlab si è trovato che per $\theta = \pi/3$ gli stati che massimizzano G sono definiti per un $\theta_M \approx 52°$. Sono state eseguite delle misure anche per questi stati ottenendo i risultati riportati in tabella 6.10. Il valore teorico di S_H per questa scelta di stati per $\theta = \pi/3$ corrisponde a $S_{HG} = 0.1490$, mentre $G = 0.2970$.
Si nota che il valore di S_H ottenuto sperimentalmente per questo protocollo è superiore a quello ottenuto per il B92-gen, ma comunque minore al bound imposto dalla teoria. Nel primo caso abbiamo ottenuto un valore di $S_{HGs}^{\pi/3} = 0.1468 < S_H^{bound} = 0.1614$ mentre per il B92-gen si ha $S_{Hgen}^{\pi/3} = 0.1433$. Le cause di ciò possono essere un allineamento non perfetto delle lamine durante la misura per il B92-gen, oppure una condizione di phase-matching non ottimale.
Per il protocollo descritto in questo paragrafo si è ottenuto un valore di $G = 0.1737$ per $\theta = \pi/3$.

	B92-ent	B92-gen	B92-maxG
S_H	0.1200	0.1433	0.1468
G	0.1425	0.828	0.1737

Tabella 6.1: Confronto tra i tre protocolli nel caso $\theta = \pi/3$

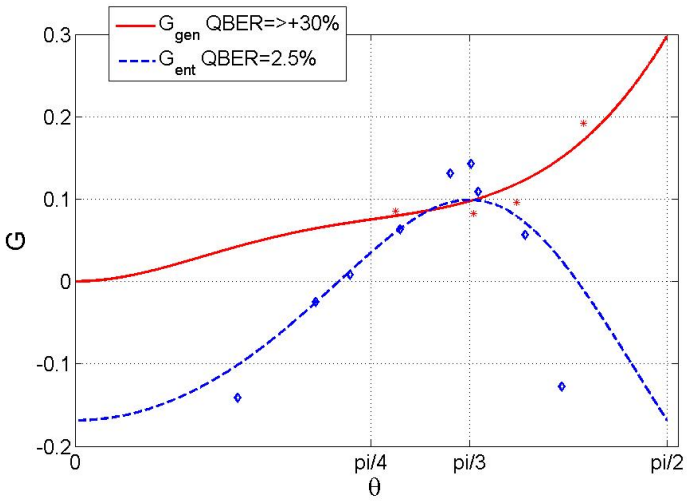


Figura 6.8: Confronto G_{ent} e G_{gen}. Nel caso del protocollo B92-ent il QBER è stato stimato al 2.5%, mentre nel caso del protocollo B92-gen è stato stimato incrementando del 30% quello teorico.

HH	VV	HV	VH	θ	$V\overline{\varphi}'_1$	$V\varphi'_0$	$+\overline{\varphi}'_1$	$+\overline{\varphi}'_0$	$-\overline{\varphi}'_1$	$-\overline{\varphi}'_0$	S_H	G	$QBER$
5608	3585			77,28	3041	759	3747	304	275	3639	0,1852	0,1923	0,0727
4957	2185	22	46	67,16	1940	217	2221	211	229	2571	0,1779	0,0961	0,0841
9093	3106	56	11	60,60	2646	455	3885	170	167	3820	0,1433	0,0828	0,0419
12448	2557	38	100	48,76	2381	327	4150	109	67	4729	0,1109	0,0858	0,0194

Tabella. 6.9: Misure per il protocollo B92-gen

HH	VV	HV	VH	θ	$V\overline{\varphi}_{M1}$	$V\varphi_{M0}$	$+\varphi_{M1}$	$+\overline{\varphi}_{M0}$	$-\overline{\varphi}_{M1}$	$-\varphi_{M1}$	S_H	G	$QBER$
8910	3173	5	24	61,65	2579	483	3917	81	138	4275	0,1468	0,1737	0,0260

Tabella. 6.10: Misure per il protocollo B92-max

Capitolo 7

Sviluppi futuri

Successivamente all'esperimento presentato nei capitoli precedenti, si è iniziato a preparare il setup ottico per un esperimento che ha come obiettivo la generazione di stati hyper-entangled.
Attualmente si è deciso di mantenere parte del setup ottico utilizzato per l'esperimento precedente, sostituendo alcuni componenti per aumentare l'efficienza dell'intero sistema. La realizzazione del sistema scelta, infatti, comporta delle perdite notevoli.

Lo stato hyper-entangled che si vuole generare è uno stato hyper-entangled in 2 stati di libertà, nella polarizzazione e nel tempo:

$$\frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle) \otimes \frac{1}{\sqrt{2}}(|SS\rangle + |LL\rangle) \tag{7.1}$$

Per generare un stato entangled nel tempo si può utilizzare lo schema introdotto da Franson[Fra89] mostrato in 7.1 Nel nostro esperimento abbiamo

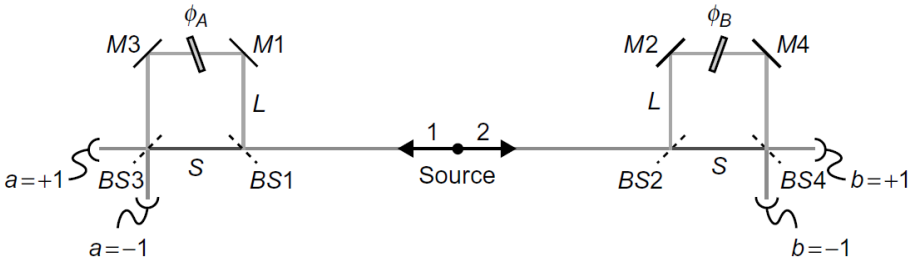


Figura 7.1: Schema per la generazione di uno stato entangled nel tempo introdotto da Franson

scelto un'implementazione diversa mostrata in figura 7.2. In questa imple-

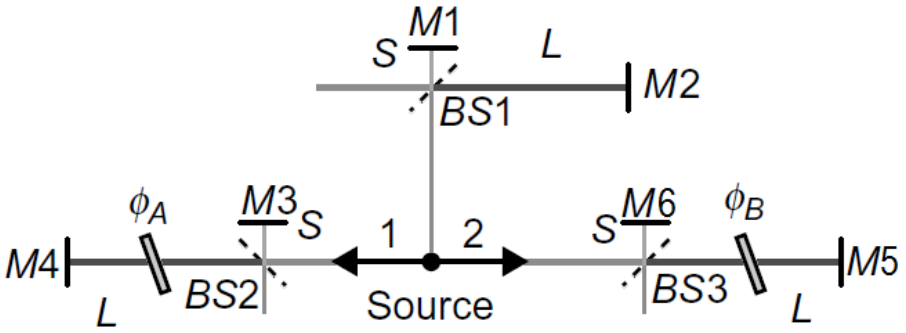


Figura 7.2: Schema utilizzato per la generazione dello stato entangled nel tempo

mentazione sono stati utilizzati degli interferometri di Michelson, che sono più semplici nella taratura ma comportano in uscita una perdita del 50% della potenza in ingresso.

Vediamo ora come si genera lo stato entangled. Immaginiamo di seguire il percorso di un fotone che entra nel sistema di figura 7.2.
Per prima cosa, il fotone entra nell'interferometro al tempo t, dove con una probabilità del 50%, può scegliere il percorso lungo oppure quello breve. Una volta uscito dal primo interferometro viene convertito tramite un processo SPDC in due fotoni, i quali si muovono in direzioni opposte (1 e 2). Questi due fotoni a loro volta entrano nell'interferometro che incontrano nel loro cammino scegliendo sempre con una probabilità del 50% il percorso breve o quello lungo. Infine escono per essere rivelati. In totale si possono avere le seguenti possibiltà*:

1. il fotone iniziale sceglie il percorso breve S(lungo L). In seguito il fotone 1 sceglie il percorso breve S e il fotone 2 quello lungo L. Il fotone 1 viene rivelato al tempo $t+S/c+S/c$ $(t+L/c+S/c)$ diverso dal tempo $t+S/c+L/c$ $(t+L/c+L/c)$ in cui viene rivelato il fotone 2. Non si ha coincidenza.

2. il fotone iniziale sceglie il percorso breve S(lungo L). In seguito il fotone 1 sceglie il percorso lungo L e il fotone 2 quello breve S. Il fotone 1 viene rivelato al tempo $t+S/c+L/c$ $(t+L/c+L/c)$ diverso dal tempo $t+S/c+S/c$ $(t+L/c+S/c)$ in cui viene rivelato il fotone 2. Non si ha coincidenza.

*Nel calcolo dei tempi non è stato tenuto conto del percorso dei fotoni in spazio aperto, in quanto è una costante uguale in tutti i casi

3. il fotone iniziale sceglie il percorso breve S(lungo L). In seguito il fotone 1 sceglie il percorso breve S e il fotone 2 quello breve S. Entrambi i fotoni vengono rivelati nello stesso istante $t_1 = t + S/c + S/c$ ($t_2 = t + L/c + S/c$). In questo caso si ha la coincidenza.

4. il fotone iniziale sceglie il percorso breve S(lungo L). In seguito il fotone 1 sceglie il percorso lungo L e il fotone 2 quello lungo L. Entrambi i fotoni vengono rivelati nello stesso istante $t_2 = t + S/c + L/c$ ($t_3 = t + L/c + L/c$). In questo caso si ha la coincidenza.

Notiamo che nel caso in cui si abbia coincidenza, si possono avere tre tempi di arrivo diversi $t_1 = t+S/c+S/c$, $t_2 = t+S/c+L/c$ e $t_3 = t+L/c+L/c$. Nel primo e nel terzo caso sarebbe possibile quindi sapere se i fotoni hanno seguito il percorso breve o quello lungo. Nel secondo caso invece non è possibile distinguere il percorso scelto dai fotoni, in quanto al tempo di rivelazione t_2, a seconda del percorso scelto dal fotone iniziale nel primo interferometro, corrispondono entrambe le possibilità.
Per generare lo stato $|\Psi_t\rangle = \frac{1}{\sqrt{2}}(|SS\rangle + |LL\rangle)$ è quindi necessario sincronizzare il sistema in modo da effettuare la misura al tempo t_2, scegliendo come t il tempo in cui viene emesso l'impulso dal laser.

7.1 Calibrazione interferometri

La differenza dei due percorsi è di $1m$, ovvero si ha una differenza, in tempi di arrivo, di circa $3ns$. La differenza dei percorsi S e L nei tre interferometri deve essere la stessa, poichè se non fosse così, i tempi di arrivo per i due fotoni sarebbero sempre diversi.
Il primo interferometro, una volta montato, è stato preso come riferimento per tarare gli altri due. I beam splitter e gli specchi del percorso S sono stati montati utilizzando i fori del banco ottico. Gli specchi del percorso L invece sono stati montati su delle slitte motorizzate, che permettevano spostamenti dell'ordine di $0.1\mu m$. In questo modo agendo solo sulla posizione dello specchio su L, si poteva regolare la differenza dei due percorsi in modo molto preciso.
L'uscita del primo interferometro è stata portata in entrata al secondo(terzo) interferometro. Se i percorsi S e L del primo interferometro sono uguali a quelli del secondo(terzo), in uscita di quest'ultimo si nota un pattern di interferenza costituito da frange verticali. Nel caso in cui i percorsi siano di lunghezze diverse invece, non si notano frange, ovvero non si ha interferenza.
In figura 7.3 riportiamo il pattern d'interferenza ottenuto in seguito alla

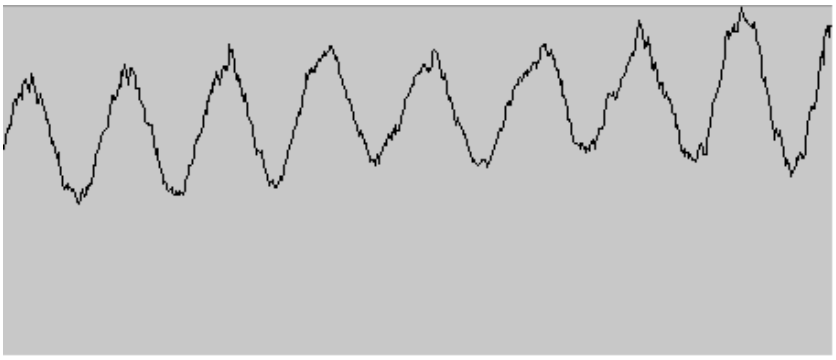


Figura 7.3: Pattern di interferenza. Gli interferometri sono tarati in modo da avere la stessa differenza sui percorsi L e S

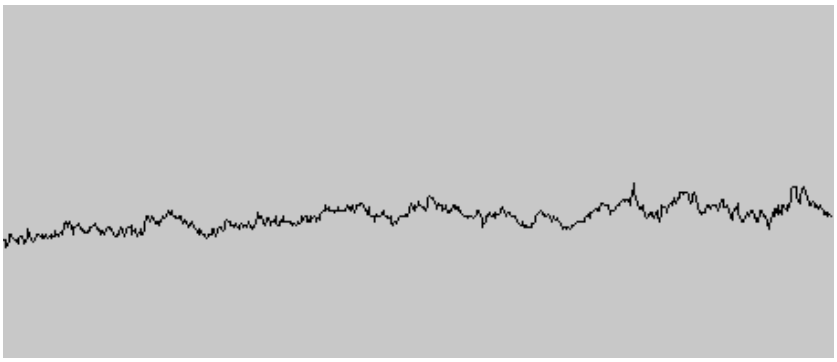


Figura 7.4: Questo pattern si ha quando non c'è interferenza

taratura dell'interferometro, mentre in figura 7.4 il pattern che si ottiene spostando lo specchio di appena $1\mu m$.

7.2 Tomografia dello stato quantistico

Quando si effettua un'esperimento, è molto importante sapere se lo stato generato dal nostro setup è effettivamente quello desiderato. Tuttavia il principio di indeterminazione di Heisenberg ci dice che non è possibile misurare contemporaneamente e con precisione arbitraria due proprietà di un sistema quantistico. Inoltre, collegato al precedente principio, il teorema di non clonazione ci dice che non è possibile usare un sistema quantistico per generare copie dello stesso stato. Perciò, per conoscere lo stato del nostro sistema è necessario utilizzare una tecnica basata sulla ricostruzione statistica, poichè non è possibile avere tutte le informazioni da una sola misura e non è possibile creare copie dello stesso stato.

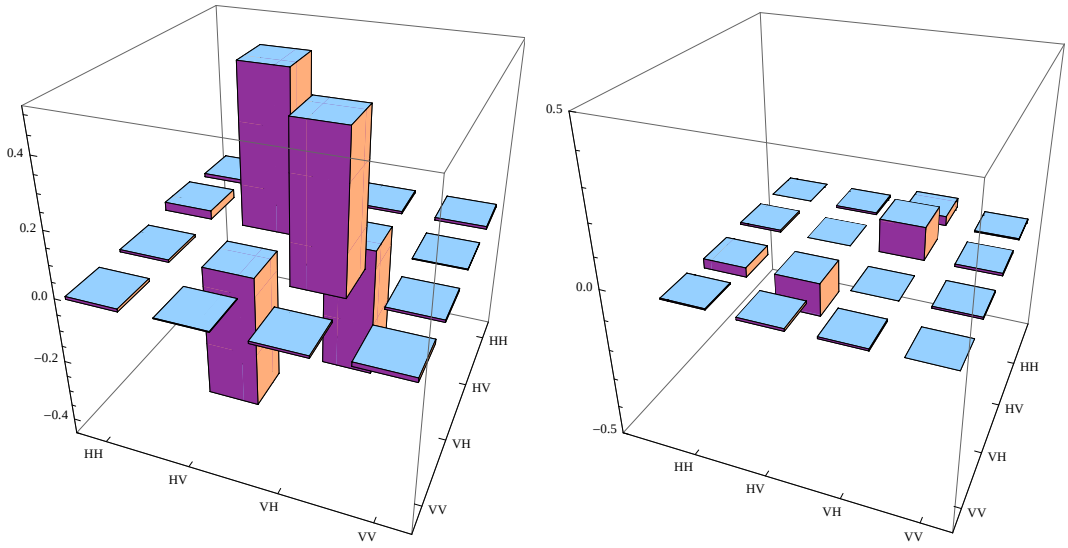
Questa tecnica prende il nome di tomografia dello stato quantistico, e, attraverso una serie di misurazioni sullo stato che si ha intenzione di caratterizzare, permette di ricavare la matrice di densità ρ del sistema.

Come mostrato da James [Whi01], la tomografia di uno stato di n-qubit può essere composta da 4^n misure. Nel nostro caso avendo uno stato di 2-qubit, il totale delle misure da effettuare è di 16, rappresentate dagli operatori $\mu_i \otimes \mu_j$ con $i, j = 0, 1, 2, 3$ dove $\mu_1 = |H\rangle\langle H|$, $\mu_2 = |V\rangle\langle V|$, $\mu_3 = |D\rangle\langle D|$, $\mu_4 = |R\rangle\langle R|$ con $|H\rangle$, $|V\rangle$, $|D\rangle = 1/\sqrt{2}(|H\rangle - |V\rangle)$ e $|R\rangle = 1/\sqrt{2}(|H\rangle - i|V\rangle)$ i kets rappresentanti i qubits nelle varie polarizzazioni.

Per ricavare la matrice di densità ρ, si può costruire una matrice triangolare τ

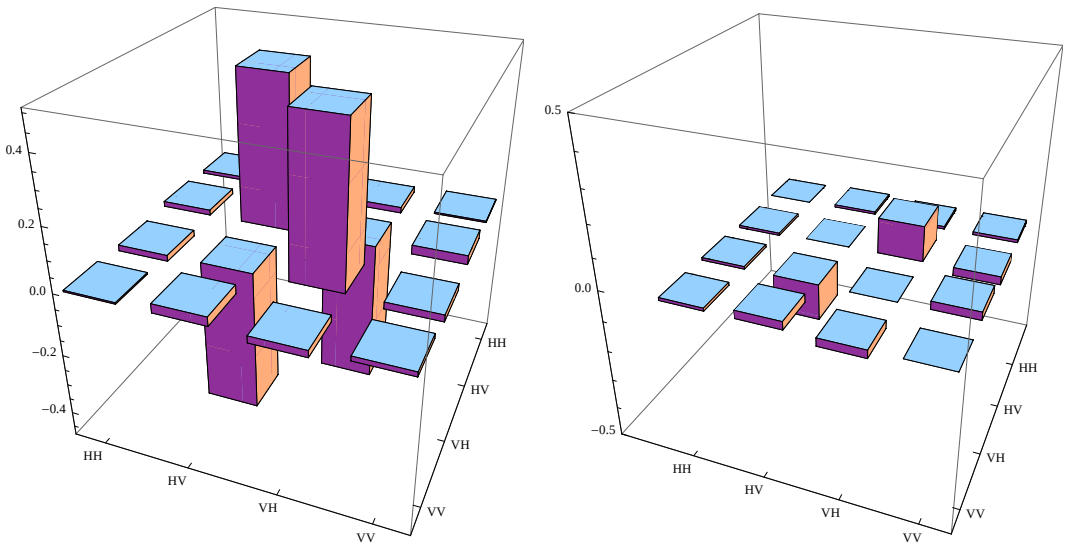
$$\tau = \begin{bmatrix} t_1 & t_2 + it_3 & t_4 + it_5 & t_6 + it_7 \\ 0 & t_8 & t_9 + it_{10} & t_{11} + it_{12} \\ 0 & 0 & t_{13} & t_{14} + it_{15} \\ 0 & 0 & 0 & t_{16} \end{bmatrix} \tag{7.2}$$

con diagonale reale, dalla quale si ricava $\rho = \tau\tau^\dagger$, dove i parametri $t_1, ..., t_{16}$ sono ricavati dalle misure descritte precedentemente.



(a) (b)

Figura 7.5: Tomografia per il canale L. La visibilità in questo esperimento era del 96%. I risultati ottenuti sono tangle=0.77, fidelity=0.92, purity=0.87. Nel grafico a destra è mostrata la componente reale mentre in quello a sinistra la componente immaginaria



(a) (b)

Figura 7.6: Tomografia per il canale S. La visibilità in questo esperimento era ancora del 96%.I risultati ottenuti sono tangle=0.87, fidelity=0.95, purity=0.93. Nel grafico a destra è mostrata la componente reale mentre in quello a sinistra la componente immaginaria

Capitolo 8

Conclusioni

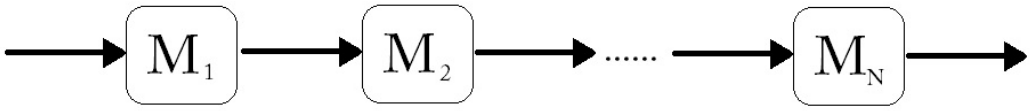
In questa tesi viene mostrato lo sviluppo di un sistema che sfrutta, attraverso l'utilizzo di un laser impulsato e di cristalli non lineari, un processo SPDC per la generazione di coppie di fotoni entangled in polarizzazione. Questi fotoni entangled vengono utilizzati in seguito per produrre quantum bit per comunicazioni quantistiche in spazio libero. Gli stati non massimamente entangled creati con questa sorgente hanno permesso di testare con successo il protocollo ent-B92. Tale protocollo implementa il protocollo B92, ma con un ulteriore vantaggio. Infatti, l'impiego di stati non massimamene entangled per scambiare la chiave permette di rivelare attacchi di tipo USD. Per questo, l'utilizzo di stati non massimamente entangled nei protocolli QKD costituisce un vantaggio ed i risultati ottenuti sono un punto di partenza per future applicazioni.
I test eseguiti hanno mostrato la violazione della disuguaglianza di Bell, e la possibilità di ottenere un guadagno di chiave sicura maggiore di 0. Inoltre, il protocollo ent-B92 è stato confrontato con il protocollo gen-B92, il quale ammette violazione massima per la disuguaglianza di Bell a scapito di un $QBER$ maggiore di 0. In seguito, attraverso una simulazione con Matlab è stato definito un protocollo con massimo guadagno G per $\theta = 60°$, verificato poi sperimentalmente. In tutti e tre i casi si sono ottenuti risultati in linea con le previsioni teoriche.
In seguito, modificando il setup utilizzato per l'esperimento precedente, è stata preparata una sorgente per fotoni hyper-entangled, nei gradi del tempo e della polarizzazione. Tale metodo innovativo costituisce un ulteriore sviluppo per costruire stati entangled in più gradi di libertà.
Attualmente sono stati calibrati gli interferometri, e si è effettuata una tomografia dello stato entangled generato via SPDC. La tomografia ha mostrato risultati soddisfacenti, tuttavia mostra uno stato entangled con fase non nulla. Per eliminare questa componente di fase è necessario un'ulteriore ottimizza-

zione del sistema. In futuro questa sorgente di fotoni hyper-entangled potrà essere utilizzata per esperimenti volti a mostrare come l'utilizzo di tali stati possa aumentare le prestazioni dei protocolli di comunicazione quantistica.

Appendice A

Simulazione della propagazione del fascio: la regola ABCD

Un fascio laser è gaussiano quando il profilo dell'intensità su un piano perpendicolare alla direzione di propagazione ha una distribuzione gaussiana. Tralasciamo il formalismo e consideriamo il parametro $q(z)$, detto raggio di curvatura complesso, definito come $\frac{1}{q(z)} = \frac{1}{R(z)} - i\frac{\lambda}{\pi W z^2}$, dove $R(z)$ è la curvatura del fronte d'onda e $W(z)$ è il raggio dello spot del fascio (waist). Una definizione alternativa è $q(z) = z + iz_0$, con z_0 lunghezza di Rayleigh (distanza dove il waist diventa $\sqrt{2}W_0$, con W_0 wait minimo). Per vedere come



il fascio viene alterato da un sistema ottico, si può ricorrere all'ottica matriciale. In questo modo ogni elemento ottico viene descritto da una matrice M, e l'intero sistema ottico dal prodotto delle matrici degli elementi che lo compongono, $M = M_N \dots M_2 M_1$, dove M_n è nella forma

$$M_n = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

Il parametro q_o in uscita ad un sistema descritto da $M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ si ottiene dal parametro q_i in ingresso attraverso la relazione:

$$q_2 = \frac{Aq_1 + B}{Cq_1 + D}$$

dal quale poi si ricava la dimensione W_o. Nel nostro caso usiamo solo lenti e spazi liberi (gli specchi hanno una matrice indentità, quindi non modificano il fascio), descritti delle matrici:

$$L = \begin{bmatrix} 1 & 0 \\ -\frac{1}{f} & 1 \end{bmatrix}$$

$$D = \begin{bmatrix} 1 & d \\ 0 & 1 \end{bmatrix}$$

dove f è il fuoco della lente, e d è la distanza in spazio aperto.

Vediamo ora come abbiamo simulato il percorso del laser che incide sul filtro F_1. L'obiettivo era di ottenere un fascio largo almeno $4 \cdot 10^{-3}m$. Le simulazioni sono state eseguite utilizzando le lenti disponibili in laboratorio. Di seguito viene descritta la soluzione adottata. Il fascio proveniente dal Mira, prima di incidere nel filtro F_1 (vedi fig. 5.3), passa attraverso una lente L_1 con $f = 0.15m$, si propaga per uno spazio di $0.9m$ (viene focalizzato a $d_1 = 0.15m$ dalla lente L_1, e poi si lascia espandere per altri $d_2 = 0.75m$, focale della lente successiva) e viene collimato attraverso una lente L_2 con $f = 0.75m$. Il sistema ottico fino questo punto è descritto dalla matrice $M = L_2 D_2 D_1 L_1 = \begin{bmatrix} -5 & 0.9 \\ 0 & -0.2 \end{bmatrix}$ ottenendo un $W = 4 \cdot 10^{-3}m$ sul filtro F_1. In seguito si è aggiunta una lente L_3 con $f = 0.75m$ per rifocalizzare il fascio, e una lente L_4 con $f = 0.15m$ per ricollimarlo. Tuttavia abbiamo bisogno di un waist più piccolo nel cristallo SPDC, e contemporaneamente uno z_0 elevato, altrimenti la radiazione dei cerchi parametrici propagandosi fino ai collimatori, divergerebbe troppo. Per simulare il comportamento del fascio, si può operare sulle matrici di propagazione in spazio libero, variandone di poco la distanza finchè non si ottiene un risultato soddisfacente. Abbiamo scelto di tenere una distanza di spazio libero tra le lenti L_3 e L_4 di circa $d_3 = 0.88m$, ottenendo un $W \approx 0.6 \cdot 10^{-3}m$ e uno $z_0 \approx 0.3m$. Il sistema ottico, fino alla lente L_4, è descritto dalla matrice

$$M_{tot} = L_4 D_3 L_3 L_2 D_2 D_1 L_1 = \begin{bmatrix} 0.87 & 0. - 0.33 \\ 0.89 & 0.81 \end{bmatrix}$$

Appendice B

Calibrazione lamine

Al fine di posizionare correttamente le lamine quando si effettua una misura, è necessario conoscerne esattamente la posizione dell'asse ottico. Le indicazioni fornite dal produttore della lamina, infatti, possono essere errate, ed inoltre, quando vengono montate nei supporti che permettono la rotazione è necessario avere un punto di riferimento.
Per la calibrazione abbiamo inserito una sola lamina alla volta prima dei PBS (vedi 5.3). Poi abbiamo iniziato a ruotare la lamina ogni 4° misurando il numero di coincidenze ottenute per ogni posizione. Infine, attraverso un programma Matlab, abbiamo cercato una funzione proporzionale ad un cos^2 che approssimasse al meglio i dati ottenuti.* Nelle figure B.1 e B.2 riportiamo i grafici con i risultati ottenuti. Cercando il minimo delle due funzioni ottenute si ottiene che per la prima lamina si ha quando il rotatore è posizionato a 41° (posizione V) mentre per la seconda si ha $-2°$ (posizione H).

*Si ricorda che l'intensità di un fascio che passa attraverso una lamina $\lambda/2$ ed un polarizzatore è proporzionale ad un cos^2.

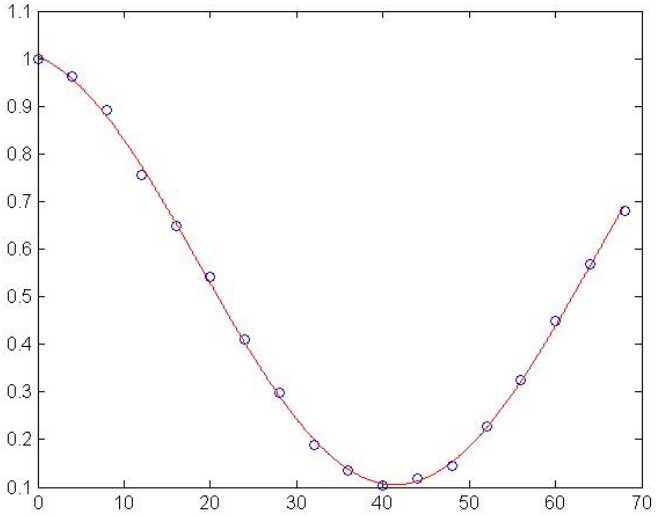


Figura B.1: Calibrazione prima lamina $\lambda/2$. Il rate delle coincidenze è stato normalizzato a 1. Poichè sono state utilizzate fibre multimodo, si nota che la funzione non raggiunge lo zero a causa del rumore di fondo (luce ambientale, luce laser)

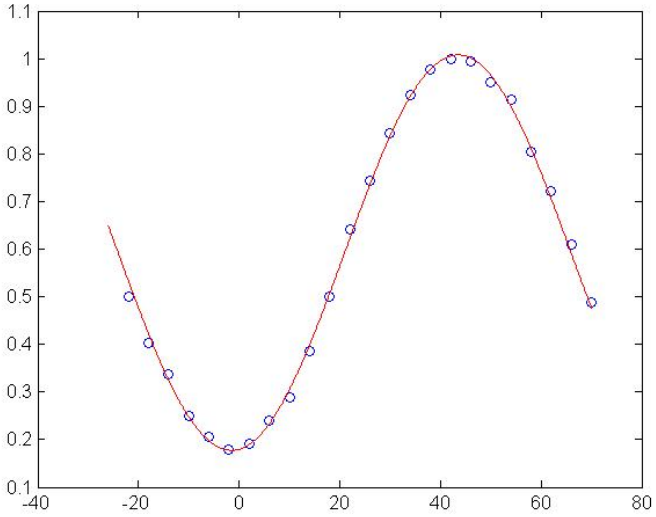


Figura B.2: Calibrazione seconda lamina $\lambda/2$. Anche qui la funzione non raggiunge lo zero a causa del rumore di fondo

Bibliografia

[AA81] G. Roger A. Aspect P. Grangier. «Experimental Test of Realistic Local Theories via Bell's Theorem». In: *Phys. Rev. Lett. 47, 460-463* (1981).

[AA82] G. Roger A. Aspect P. Grangier. «Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities». In: *Phys. Rev. Lett. 49, 91-94* (1982).

[AL08] C. Kurtsiefer A. Ling A. Lamas-Linares. «Absolute emission rates of Spontaneous Parametric Down Conversion into single transverse Gaussian modes». In: *Phys. Rev. A 77,043834* (2008).

[Bel06] M. Le Bellac. *Quantum Physics*. Cambridge University Press, 2006.

[CG05] P. Knight C. Gerry. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[Cha12] D. Gauthier H. Guilbert Y. Zhu M. Shi K. McCusker B. Christensen P. Kwiat T. Brougham S. M. Barnett V. Chandar. «Quantum Key Distribution Using Hyperentanglement». In: *Optical Society of America QT4A.2* (2012).

[Ein35] Rosen Einstein Podolsky. «*Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*» In: *Phys. Rev. 47 (10): 777-780* (1935).

[Eke91] A.K. Ekert. «Quantum Cryptography Based on Bell's Theorem». In: *Phys. Rev. Lett. 67, 661-663* (1991).

[Fra89] J.D. Franson. «Bell inequality for position and time». In: *Phys. Rev. Lett. 62, 2205* (1989).

[GM11] M. Lucamarini G. Vallone I. Gianani G. Di Giuseppe e P. Mataloni. «Device-independent entanglement-based Bennett 1992 protocol». In: *arXiv:1111.1997* (2011).

[GV11] P. Mataloni G. Vallone. «Generation and Applications of n-Qubit Hyperentangled Photon States». In: *Advances In Atomic Molecular and Optical Physics 60* (2011).

[Hol69] Clauser Horne Shimony Holt. «Proposed experiment to test local hidden-variable theories». In: *Phys. Rev. Lett. 23, 880* (1969).

[J.B64] J.Bell. «On the Einstein Podolsky Rosen paradox». In: *Physics 1(3): 195-200* (1964).

[JBA05] P. G. Kwiat J. B. Altepeter E. R. Jeffrey. «Phase-compensated ultra-bright source of entangled photons». In: *Opt. Express 13, 8951-8959* (2005).

[Kwi99] A.G. White D.F. James P.H Eberhard P.G. Kwiat. «Nonmaximally Entangled States: Production, Characterization and Utilization». In: *Phys. Rev. Lett. 83, 16* (1999).

[LM11] A. Acin Ll. Masanes S. Pironio. «Secure device-independent quantum key distribution with causally independent measurement devices». In: *Nat. Commun. 2,238* (2011).

[Oh02] D. Kaszlikowski L. C. Kwek J. Chen M. Zukowski C. H. Oh. «Clauser-Horne inequality for three-state systems». In: *Phys. Rev. A 65, 032118* (2002).

[PK98] H: Weinfurter P.G. Kwiat. «Embedded Bell-state analysis». In: *Phys. Rev. A 58, 2623* (1998).

[Pho] *Spatial hole burning.* URL: http://www.rp-photonics.com/ring_lasers.html.

[Sal07] Teich Saleh. *Fundamentals of photonics, 2ed.* Wiley, 2007.

[Vil12] M. Minozzi S. Bonora A. V. Sergienko G. Vallone P. Villoresi. «Biphoton propagation control with optimized wavefront by means of Adaptive Optics». In: *arXiv:1210.2306* (2012).

[Whi01] D.F.V. James P.G. Kwiat W.J. Munro A.G. White. «Measurement of qubits». In: *Phys. Rev. A 64, 052312* (2001).

[Woo00] V. Coffman J. Kundu W.K. Wootters. «Distributed entanglement». In: *Phys. Rev. A 64, 052306* (2000).

[YS11] G. Long Y. Sheng F. Deng. «Complete hyperentangled Bell-state analysis for quantum communication». In: *arXiv:1103.0230v1* (2011).

[Zur82] W.K. Wootters W.H Zurek. «A single quantum cannot be cloned». In: *Nature V. 299, 802* (1982).

Ringrazizmenti

Desidero ringraziare il Prof. Paolo Villoresi che per la seconda volta mi ha dato l'opportunità di lavorare con il suo gruppo, partecipando alla ricerca nell'ambito delle comunicazioni quantistiche.

Un ringraziamento anche al Dott. Giuseppe Vallone, che, nonostante tutte le volte si sia scontrato con la mia testardaggine, si è reso sempre disponibile nel fornire chiarimenti, soluzioni ed aiuti.

Ringrazio anche tutti i colleghi del Luxor, Francesca, Stefano, Alberto G., Davide B., Davide M., Alberto D.A., Simone, Nicola per il sostegno, le chiacchierate alla macchinetta del caffè e le discussioni musicali.

Un particolare ringraziamento a Mattia che durante tutto il lavoro è sempre stato disponibile a dare una mano nei momenti di difficoltà (soprattutto quando avevo perso le intersezioni dei cerchi!), a fornire spiegazioni su quanto non capivo, per la costante compagnia e per l'aiuto nella correzione della tesi.