UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Fisica e Astronomia "Galileo Galilei"

Corso di Laurea Triennale in Fisica

Tesi di Laurea

Analisi delle prestazioni della Quantum Key Distribution con dispositivi non-ideali

Relatore

Prof. Giuseppe Vallone

Correlatore

Dr. Costantino Agnesi

Laureando

Marika Sartore

Anno Accademico 2019/2020

Indice

Capitolo 1

Introduzione alla QKD

La crittografia classica permette a due parti separate, convenzionalmente chiamate Alice e Bob, di scambiarsi messaggi in maniera privata e sicura: le informazioni inviate vengono cifrate attraverso un algoritmo e possono essere decodificate dal destinatario, solo mediante una chiave apposita.
La crittografia può essere principalmente di due tipi, a chiave simmetrica o a chiave asimmetrica. La prima prevede che vi sia un'unica chiave, condivisa da Alice e Bob, per crittare e decrittare il messaggio; nella seconda, invece, sono previste due chiavi diverse, una resa pubblica da Alice e visibile a tutti che serve per crittografare, e una privata, nota soltanto a lei, per decifrare il messaggio.
Il principale problema di questi tipi di crittografia è che si basano sulla matematica e sulla fisica classica e sui limiti computazionali attualmente presenti [1], di conseguenza, con l'avvento della meccanica quantistica, hanno iniziato a svilupparsi algoritmi basati sulla fisica quantistica che si sono rivelati essere più potenti di quelli classici ad oggi conosciuti, minando la sicurezza delle comunicazioni tradizionali.
Si prenda ad esempio il sistema di crittografia a chiave pubblica più usato, l'RSA [2], inventato nel 1978 si basa sulla difficoltà di fattorizzare numeri interi molto grandi: dal punto di vista teorico matematico è un problema possibile da risolvere ma, computazionalmente parlando, richiederebbe costi e tempi talmente elevati da renderlo praticamente infallibile agli algoritmi di decrittazione classici ad oggi noti. Tuttavia, con lo sviluppo di algoritmi quantistici, nel 1994 Peter Shor ideò l'algoritmo a lui omonimo [3], in grado di risolvere, su un computer quantistico, il problema della fattorizzazione di numeri interi in un tempo polinomiale. Ecco, dunque, che non è più sicuro basare la sicurezza delle comunicazioni sulla sola inefficienza degli algoritmi di decrittazione ad oggi noti, sapendo che con lo sviluppo, attuale e futuro, dell'informazione quantistica la segretezza ne verrebbe meno.

1.1 Basi dell'Informazione Quantistica

Nell'informatica classica, l'unità di misura elementare dell'informazione è il bit, un costrutto matematico che può assumere soltanto due valori tra loro mutuamente esclusivi: 0 e 1. Il suo corrispettivo quantistico, il quantum bit (abbreviato qubit), è un sistema microscopico, solitamente un fotone, che sottostà alle leggi della meccanica quantistica. I suoi due valori booleani 0 e 1 sono rappresentati da una coppia di stati fisici distinguibili tra loro, come ad esempio due stati di polarizzazione del fotone tra loro ortogonali. Dal momento che gli stati quantistici sono rappresentati da raggi vettori in spazi di Hilbert, si può applicare il principio di sovrapposizione e, dunque, lo stato del qubit può essere visto come una sovrapposizione lineare di $|0\rangle$ e $|1\rangle$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.1}$$

con $|\alpha|^2 + |\beta|^2 = 1$. Quindi, a differenza del caso classico in cui il bit può assumere quei due soli valori, il qubit può rappresentare un numero infinito di combinazioni lineari e questo si vede molto chiaramente riscrivendo l'equazione 1.1 in funzione dei due angoli θ e ϕ:

$$|\psi\rangle = cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}sin\frac{\theta}{2}\,|1\rangle \tag{1.2}$$

In questo modo è possibile una rappresentazione geometrica degli stati tramite la sfera di Bloch, una sfera tridimensionale di raggio unitario, i cui punti della superficie sono in corrispondenza biunivoca con gli stati del qubit.

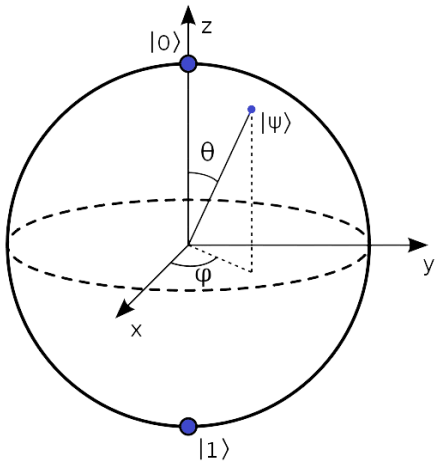

Figura 1.1: Rappresentazione stato qubit mediante sfera di Bloch.

Tuttavia, per il postulato di proiezione di Von Neumann, quando si compie una misurazione di uno stato quantistico, la sua funzione d'onda $|\psi\rangle$ collassa in uno degli autostati e, nel caso del qubit, l'esito di una misura dello stato $|\psi\rangle$ sarà $|0\rangle$ con probabilità $|\alpha|^2$ e $|1\rangle$ con probabilità $|\beta|^2$. Dunque, dopo essere stato misurato, un qubit porta la stessa quantità di informazione di un bit, ma con il grande vantaggio che il suo comportamento segue teoremi e postulati della fisica quantistica che non hanno analogo classico e, di conseguenza, introducono regole davvero favorevoli, soprattutto nell'ambito della comunicazione quantistica.

1.2 QKD tra ideale e reale

Il settore della crittografia quantistica che per questo motivo più si è sviluppato, al punto da avere già anche implementazioni reali, è la Quantum Key Distribution (QKD), la distribuzione quantistica di chiave.
Essa ha inizio nel 1984 quando viene presentato da Bennett e Brassard il primo protocollo per la distribuzione di chiave basato sulla fisica quantistica, il BB84 [4], che ancora oggi viene ampiamente utilizzato.
Alle origini della sicurezza della QKD [5] ci sono alcuni principi fondanti della fisica quantistica, primo fra tutti il postulato secondo cui compiere una misura su un sistema, ne modifica in maniera irreversibile lo stato: si pensi, dunque, all'azione di un ascoltatore non autorizzato, detto Eve, che non appena prova ad estrarre informazioni dallo stato quantistico, apporta ad esso delle modifiche che permettono alle parti autorizzate, Alice e Bob, di accorgersene e di scartare tale chiave.
Un altro risultato interessante è sicuramente il no-cloning theorem, il quale stabilisce che uno stato quantistico sconosciuto non può essere clonato: ecco che quando Alice distribuisce una chiave attraverso un segnale quantistico, non c'è modo per Eve di crearne una copia e di riuscire a risalire ad essa.
Infine, i risultati della misura non esistono prima che essa venga fatta e una volta conclusasi una comunicazione quantistica, non esiste alcuna trascrizione di essa che Eve nel futuro possa recuperare.
Grazie a queste proprietà, per molti protocolli di QKD, tra cui il BB84, la sicurezza è stata provata essere incondizionata, questo significa che la loro sicurezza può essere dimostrata senza imporre alcuna restrizione sulle risorse computazionali o sulle tecniche di manipolazione che sono disponibili ad un ascoltatore Eve: questo rappresenta un enorme passo avanti rispetto alla crittografia classica.

Tuttavia, se nella teoria si dimostra che la quantum key distribution garantisce comunicazioni sicure tra Alice e Bob, bisogna sottolineare che nella gran parte delle dimostrazioni di sicurezza vengono fatte ipotesi irreali e non vengono prese in considerazione le imperfezioni dei dispositivi utilizzati. Di conseguenza nelle implementazioni pratiche non si riesce a garantire effettivamente questo livello di

sicurezza e si manifestano attacchi hacker che sfruttano proprio la non-idealità della sorgente e dei detector [6]. Come sottolinea l'articolo [7], la necessità è quella di colmare questo grande gap tra la teoria e la pratica e, in tale direzione, si stanno sviluppando protocolli che riescono a garantire la sicurezza pur tenendo conto di tali imperfezioni.

1.3 Una sorgente reale: il POGNAC

Per rendere possibile l'utilizzo della QKD nelle infrastrutture delle telecomunicazioni attualmente disponibili, è necessario che i sistemi che vengono sviluppati siano semplici, abbiano un prezzo accessibile e siano stabili. Tuttavia, le implementazioni della QKD fino ad ora ideate prevedono hardware addizionali che si occupino della sincronizzazione temporale e controllino la polarizzazione delle basi.
In questo contesto, il gruppo di ricerca QuantumFuture del Dipartimento di Ingegneria dell'Informazione dell'Università di Padova ha recentemente presentato [8] un semplice sistema per la QKD in cui la comunicazione quantistica, la sincronizzazione temporale e la compensazione della polarizzazione sono realizzate tutte all'interno dello stesso setup. La sorgente di stati da loro ideata, il POGNAC [9], si è dimostrata essere molto stabile e raggiungere, mediamente, un $QBER_{opt} = 0.05\%$ (Quantum Bit Error Rate) che corrisponde ad un extinction ratio tra le basi di 33 dB: un risultato mai ottenuto in precedenza. Inoltre, è compatibile con la QKD in free-space, nelle fibre ottiche e addirittura via satellite.

Nello specifico, il POGNAC è un modulatore di polarizzazione basato su un modulatore di fase in $LiNbO_3$ all'interno di un interferometro di Sagnac.

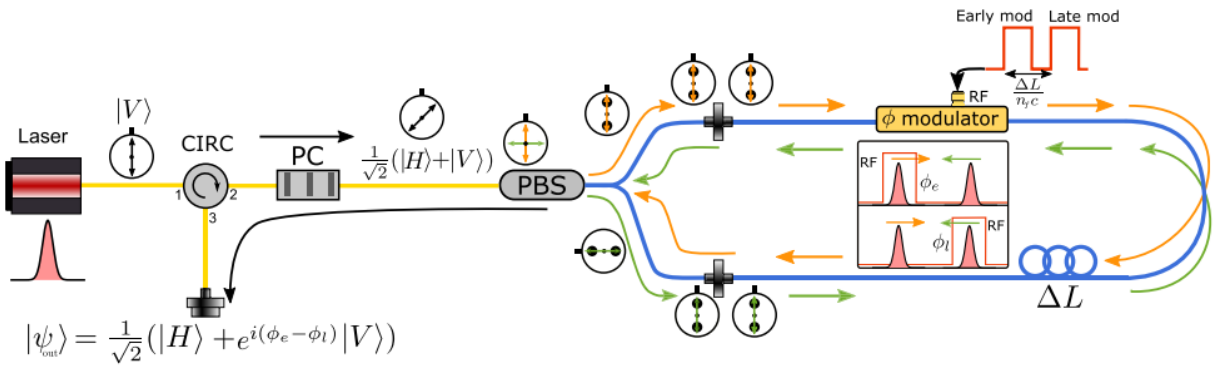

Figura 1.2: Setup del POGNAC presentato in [9].

Il setup presentato nella figura 1.2 mostra che l'impulso laser polarizzato linearmente entra nella porta 1 del circolatore ottico (CIRC) e ne esce dalla 2, incontra poi un polarization controller (PC) che trasforma lo stato di polarizzazione in $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i\phi_0}|V\rangle)$. Dunque il fascio incide in un polarization beam splitter (PBS), il quale scompone le due componenti ortogonali e le fa entrare in un interferometro di Sagnac: la componente $|V\rangle$ viaggia in senso orario, incontra prima un modulatore di fase che introduce una fase ϕ_l, poi la linea di ritardo in fibra PM e infine rientra nel PBS con polarizzazione orizzontale. Contemporaneamente la componente $|H\rangle$ viaggia in senso antiorario e, perciò, incontra prima la linea di ritardo e poi il modulatore di fase, rientrando nel PBS con polarizzazione verticale. Entrambe le componenti viaggiano all'interno dell'interferometro di Sagnac con polarizzazione allineata all'asse lento della fibra PM, così non si ha dispersione dei modi di polarizzazione e si propaga un singolo modo. In questo modo è garantito anche l'arrivo delle due componenti nello stesso istante al PBS, così da venir ricombinate e generare uno stato di polarizzazione pari a:

$$\left|\psi_{out}^{\phi_e,\phi_l}\right\rangle = \frac{1}{\sqrt{2}}(|H\rangle + e^{i(\phi_e-\phi_l-\phi_0)}|V\rangle) \tag{1.3}$$

La luce modulata, infine, esce dalla terza porta del circolatore.
Scelto per semplicità $\phi_0 = 0$, modificando il voltaggio applicato alle componenti oraria e antioraria si possono ottenere i tre diversi stati di polarizzazione necessari per eseguire il protocollo BB84

semplificato a tre stati:

$$\left|\psi_{out}^{0,0}\right\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \tag{1.4}$$

$$\left|\psi_{out}^{\frac{\pi}{2},0}\right\rangle = |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i\,|V\rangle) \tag{1.5}$$

$$\left|\psi_{out}^{0,\frac{\pi}{2}}\right\rangle = |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i\,|V\rangle) \tag{1.6}$$

Di questi, la base che viene utilizzata per generare la chiave è $Z = \{|0\rangle, |1\rangle\}$ con $|0\rangle := |L\rangle$, $|1\rangle := |R\rangle$, mentre la base di controllo è $X = \{|+\rangle, |-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$.

Il POGNAC, pur avendo prestazioni eccellenti, è un dispositivo sperimentale e non sarà mai in grado di generare in maniera perfetta gli stati teorici riportati in precedenza e, in tal senso, non è una 'sorgente ideale'.
Il lavoro che è stato fatto e che verrà presentato nei prossimi capitoli è, dunque, quello di costruire un polarimetro che permetta di analizzare gli stati di polarizzazione generati dal POGNAC (capitolo 3), in modo da quantificarne lo scostamento dal caso ideale (capitoli 4 e 5). Prima di passare a questa parte, nel prossimo capitolo verrà introdotto il formalismo necessario alla trattazione dell'argomento.

Capitolo 2

Formalismo usato nella polarizzazione

2.1 La polarizzazione

La polarizzazione è la proprietà delle onde elettromagnetiche che descrive la direzione dell'oscillazione del vettore campo elettrico durante la propagazione dell'onda nello spazio-tempo.
Solitamente, dunque, si rappresenta lo stato di polarizzazione di un'onda luminosa tramite l'evoluzione del suo vettore campo elettrico $\vec{\boldsymbol{E}}$: se la variazione della direzione di questo vettore in funzione della coordinata spaziale di propagazione e del tempo può essere espressa da una legge precisa, si dice che l'onda è polarizzata, altrimenti, se tale dipendenza è casuale, si dice che l'onda non è polarizzata.
Considerando un'onda piana monocromatica che viaggia lungo la direzione z, alla velocità della luce c e con frequenza ω, il suo vettore campo elettrico è descritto da:

$$\vec{\boldsymbol{E}}(z,t) = E_x\hat{\boldsymbol{x}} + E_y\hat{\boldsymbol{y}} \tag{2.1}$$

con

$$E_x = E_{0x}cos[\omega(t - \frac{z}{c}) + \phi_x] \tag{2.2}$$

$$E_y = E_{0y}cos[\omega(t - \frac{z}{c}) + \phi_y] \tag{2.3}$$

$$\tag{2.4}$$

E queste rappresentano l'equazione parametrica di un'ellisse:

$$\frac{E_x^2}{E_{0x}^2} + \frac{E_y^2}{E_{0y}^2} - 2\frac{E_xE_y}{E_{0x}E_{0y}}cos\phi = sin^2\phi \tag{2.5}$$

con $\phi = \phi_y - \phi_x$. Quindi, per un valore di z fissato, il vettore del campo elettrico ruota periodicamente compiendo un'ellisse sul piano xy. In particolare, la forma dell'ellisse può degenerare in una circonferenza o in un segmento e questo dà luogo, rispettivamente, alle polarizzazioni circolari e lineari.
Si parla di polarizzazione circolare quando $\phi = \pm\pi/2$ e $E_{0x} = E_{0y} = E_0$: con $\phi = \pi/2$ il vettore del campo elettrico, nella propagazione dell'onda, compie una circonferenza in senso orario (polarizzazione circolare destronsa), mentre con $\phi = -\pi/2$ la percorre in senso antiorario (polarizzazione circolare sinistronsa). La polarizzazione lineare, invece, si ottiene quando una delle due componenti $E_{0i} = 0$ $(i = x, y)$, e in questo caso il vettore del campo elettrico mantiene la propria direzione lungo la componente che non si annulla, oppure quando la differenza di fase $\phi = 0, \pi$.

2.2 Formalismo di Jones

Attraverso il formalismo introdotto da Jones è possibile rappresentare lo stato di polarizzazione dell'onda mostrato nel paragrafo precedente, in termini del vettore complesso di Jones, le cui componenti sono:

$$\mathbf{J} = \begin{pmatrix} E_x \\ E_y \end{pmatrix} = \begin{pmatrix} E_{0x}e^{i\phi_x} \\ E_{0y}e^{i\phi_y} \end{pmatrix} \tag{2.6}$$

Nella seguente tabella vengono riportati i principali stati di polarizzazione scritti sottoforma di vettori di Jones:

polarizzazione	vettore di Jones	polarizzazione	vettore di Jones
lineare orizzontale	$\|H\rangle = \begin{pmatrix}1\\0\end{pmatrix}$	lineare verticale	$\|V\rangle = \begin{pmatrix}0\\1\end{pmatrix}$
lineare a 45°	$\|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	lineare a $-45°$	$\|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
circolare sinistronsa	$\|L\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$	circolare destronsa	$\|R\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$

Tabella 2.1: Vettori di Jones per i principali stati di polarizzazione.

Questo formalismo risulta essere molto conveniente nella descrizione dei sistemi ottici lineari, in quanto permette di rappresentare elementi come polarizzatori, lamine ritardatrici e rotatori di polarizzazione, in termini di matrici 2x2. Così facendo, si può riassumere il comportamento del sistema in esame tramite la relazione:

$$\boldsymbol{J_{out} = T J_{in}} \tag{2.7}$$

ove $\boldsymbol{T}$ rappresenta la matrice di Jones del sistema ottico attraversato e, per proprietà matriciale, è data dal prodotto delle n matrici degli n dispositivi attraversati. Dunque, nota la polarizzazione dell'onda incidente, si può stabilire quale sarà il vettore di Jones, e quindi lo stato, in uscita.

Nello specifico, si riporta lo studio attraverso il formalismo di Jones di un sistema composto da sole lamine ritardatrici, in modo da mostrarne il comportamento che tornerà utile nel capitolo 3.

2.2.1 Lamine QWP e HWP

Le lamine ritardatrici con fast axis lungo la direzione x trasformano le componenti del campo dell'onda incidente su di esse, ritardandone la componente y con l'aggiunta di una fase Γ, e lasciandone invariata la componente x (da qui il nome fast axis per la direzione x e slow axis per y). Questa proprietà permette di ruotare la polarizzazione del fotone incidente, in modo da ottenere altri stati di polarizzazione, ovvero, in termini di matrice di Jones:

$$\boldsymbol{T} = \begin{bmatrix}1 & 0\\ 0 & e^{-i\Gamma}\end{bmatrix} \tag{2.8}$$

dove per la lamina a quarto d'onda (Quarter Wave Plate) $\Gamma = \pi/2$, mentre per quella a mezz'onda (Half Wave Plate) $\Gamma = \pi$. In particolare, la lamina QWP trasforma un'onda con polarizzazione circolare, in polarizzazione lineare e viceversa, mentre la lamina HWP converte la polarizzazione circolare sinistronsa in destronsa e la diagonale nella antidiagonale, e viceversa [10].

Quando si ruota la lamina di un angolo ϕ, bisogna tener presente che si sta applicando la matrice delle rotazioni:

$$\boldsymbol{R}(\phi) = \begin{bmatrix}\cos(\phi) & \sin(\phi)\\ -\sin(\phi) & \cos(\phi)\end{bmatrix} \tag{2.9}$$

con $\phi = \theta + \gamma$, ove θ è l'angolo che si sta ruotando del goniometro della lamina, e γ un angolo di offset dovuto al fatto che lo zero del goniometro non coincide con il fast axis della lamina.
Perciò, la matrice effettiva è data da $\boldsymbol{T'} = \boldsymbol{R}(-\phi)\boldsymbol{T}\boldsymbol{R}(\phi)$, ovvero:

$$\boldsymbol{T'_{QWP}} = e^{-i\frac{\pi}{4}}\begin{bmatrix}\cos^2(\phi) + i\sin^2(\phi) & (1-i)\sin(\phi)\cos(\phi)\\ (1-i)\sin(\phi)\cos(\phi) & \sin^2(\phi) + i\cos^2(\phi)\end{bmatrix} \tag{2.10}$$

$$\boldsymbol{T'_{HWP}} = e^{-i\frac{\pi}{2}}\begin{bmatrix}\cos(2\phi) & \sin(2\phi)\\ \sin(2\phi) & -\cos(2\phi)\end{bmatrix} \tag{2.11}$$

Per studiare il comportamento delle lamine, per prima cosa è necessario creare una sorgente di stati noti: a tal scopo si è utilizzato un laser a 1550nm (MMC-GASFP) collegato in fibra SM ad un polarization controller e ad un collimatore, seguito da un polarizzatore di Glan-Taylor. Il fascio polarizzato viene poi fatto incidere in un PBS, in modo da uscirne scomposto nelle due componenti di polarizzazione ortogonali. Alle due uscite del PBS sono posti due Power Meter per registrare l'intensità in uscita.

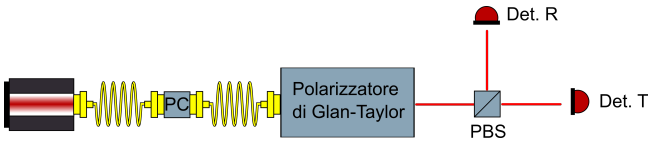

Figura 2.1: Setup iniziale.

Ruotando il polarizzatore si è cercato l'angolo a cui esso produce uno stato a polarizzazione orizzontale $|H\rangle = \binom{1}{0}$, ovvero l'angolo a cui si registra il massimo nella potenza rilevata all'uscita del ramo trasmesso del PBS e, di conseguenza, un minimo nel ramo riflesso. Il valore trovato è di $308° \pm 1°$ e si è dunque bloccato il polarizzatore a quest'angolo.
A questo punto sono state inserite una per volta le lamine ritardatrici a quarto d'onda e a mezz'onda tra polarizzatore e il PBS, come raffigurato in figura 2.2.

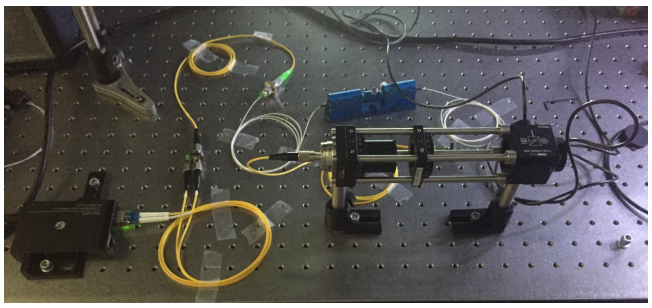

Figura 2.2: Setup per analizzare comportamento lamine.

Ruotando il goniometro delle lamine sono stati raccolti i valori delle potenze registrate dai due detector. Per calcolare l'andamento di tali potenze in funzione dell'angolo, si usano le matrici di Jones: applicando le matrici 2.10 e 2.11 allo stato in ingresso $|H\rangle = \binom{1}{0}$, si ottiene lo stato del fotone dopo aver passato la lamina e questo è anche lo stato che entra nel PBS e viene trasmesso o riflesso.
I fotoni che incidono nel PBS hanno, quindi, probabilità di venir trasmessi pari a $|\langle H|\boldsymbol{T'}|H\rangle|^2$, mentre di venir riflessi $|\langle V|\boldsymbol{T'}|H\rangle|^2$.
In funzione dell'angolo ϕ si ottengono:

lamina	$t(\phi)$	$r(\phi)$
QWP	$\frac{\cos^2(2\phi)+1}{2}$	$\frac{\sin^2(2\phi)}{2}$
HWP	$\cos^2(2\phi)$	$\sin^2(2\phi)$

Tabella 2.2: Andamento probabilità di trasmissione e riflessione per lamine QWP e HWP.

Tali probabilità sono dette coefficienti di trasmissione e riflessione e, per definizione, la loro somma è pari ad 1.
Le potenze raccolte sono quindi state normalizzate al massimo di potenza rilevato, in modo da poterne comparare l'andamento attraverso un fit, con quello delle probabilità in tabella 2.2.
Di seguito vengono riportati i grafici con i dati raccolti, $t(\phi)$ e $r(\phi)$, e la tabella con gli angoli γ di offset ricavati dai fit di entrambe le lamine e i rispettivi errori σ_γ.

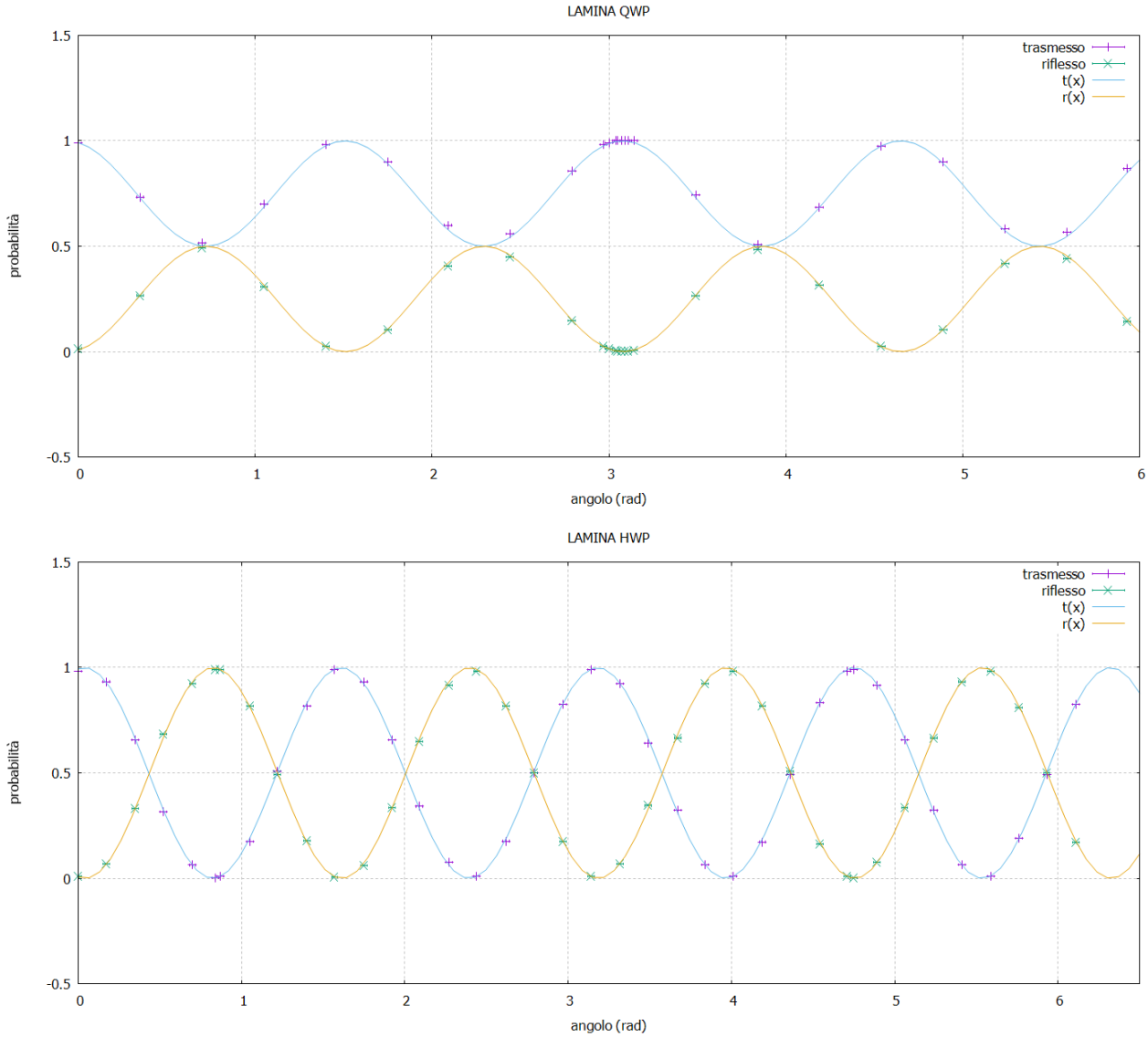

Figura 2.3: Andamento delle probabilità di trasmissione e riflessione per le lamine QWP e HWP.

lamina	$\gamma(rad)$	$\sigma_\gamma(rad)$
QWP	1.633	0.002
HWP	1.529	0.001

Tabella 2.3: γ ricavati dal fit.

2.3 Parametri di Stokes e sfera di Ponicaré

Il formalismo di Jones, tuttavia, è applicabile solamente in presenza di onde completamente polarizzate, ovvero onde il cui grado di polarizzazione $P = \frac{I_{pol}}{I_{tot}}$, rapporto tra intensità della componente polarizzata e intensità totale dell'onda, sia pari ad 1.
Per trattare, invece, anche onde parzialmente polarizzate, con $0 \leq P \leq 1$, è necessario passare alla rappresentazione di Stokes, la quale prevede l'utilizzo di quattro parametri dipendenti dalle componenti

del campo elettrico dell'onda tramite:

$$S_0 = |E_x|^2 + |E_y|^2 \tag{2.12}$$

$$S_1 = |E_x|^2 - |E_y|^2 \tag{2.13}$$

$$S_2 = 2Re(E_x^* E_y) = |E_{45}|^2 - |E_{135}|^2 \tag{2.14}$$

$$S_3 = 2Im(E_x^* E_y) = |E_R|^2 - |E_L|^2 \tag{2.15}$$

Dunque, S_0 è collegato all'intensità totale dell'onda, mentre S_1, S_2, S_3 rispettivamente alle intensità delle componenti di polarizzazione lineare verticale e orizzontale, lineare diagonale e antidiagonale e circolare sinistronsa e destronsa.
Il grado di polarizzazione dell'onda può essere dunque riscritto in termini di parametri di Stokes:

$$P = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0} \quad \text{con} \quad 0 \leq P \leq 1 \tag{2.16}$$

Solitamente questi 4 parametri vengono usati come componenti di un vettore quadridimensionale, il vettore di Stokes:

$$\boldsymbol{S} = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} \tag{2.17}$$

Nella tabella seguente vengono riportati i vettori di Stokes per i principali stati di polarizzazione:

polarizzazione	vettore di Stokes	polarizzazione	vettore di Stokes
$\|H\rangle$	$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$	$\|V\rangle$	$\begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix}$
$\|+\rangle$	$\begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$	$\|-\rangle$	$\begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$
$\|L\rangle$	$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$	$\|R\rangle$	$\begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$

Tabella 2.4: Vettori di Stokes per i principali stati di polarizzazione.

Una rappresentazione geometrica di questi vettori e, di conseguenza, degli stati di polarizzazione, è data dalla sfera di Poincaré: ogni stato di polarizzazione dell'onda luminosa è in corrispondenza biunivoca con un punto $S(S_1, S_2, S_3)$ sulla sfera di raggio S_0.
La figura 2.4 evidenzia come gli stati di polarizzazione lineare giacciano sul piano equatoriale, le due polarizzazioni circolari siano ai due poli della sfera, mentre tutti gli altri punti intermedi sono stati a polarizzazione ellittica.
Visto il comportamento delle lamine ritardatrici nel paragrafo 2.2.1, esse permettono di spostarsi sulla superficie della sfera di Poincaré: le HWP spostano gli stati sul piano equatoriale, mentre le QWP passano dai poli all'equatore compiendo una sorta di otto sulla superficie sferica.

I punti che giacciono sulla superficie della sfera di raggio unitario ($S_0 = 1$) rappresentano stati completamente polarizzati, mentre quelli all'interno hanno polarizzazione parziale, fino ad arrivare all'origine che corrisponde ad uno stato non polarizzato.
Con il formalismo di Jones, dunque, è possibile rappresentare soltanto stati che appartengono alla superficie della sfera unitaria (quelli completamente polarizzati), mentre grazie ai vettori di Stokes e alla sfera di Poncaré è possibile descrivere l'intera sfera e avere una trattazione più completa.

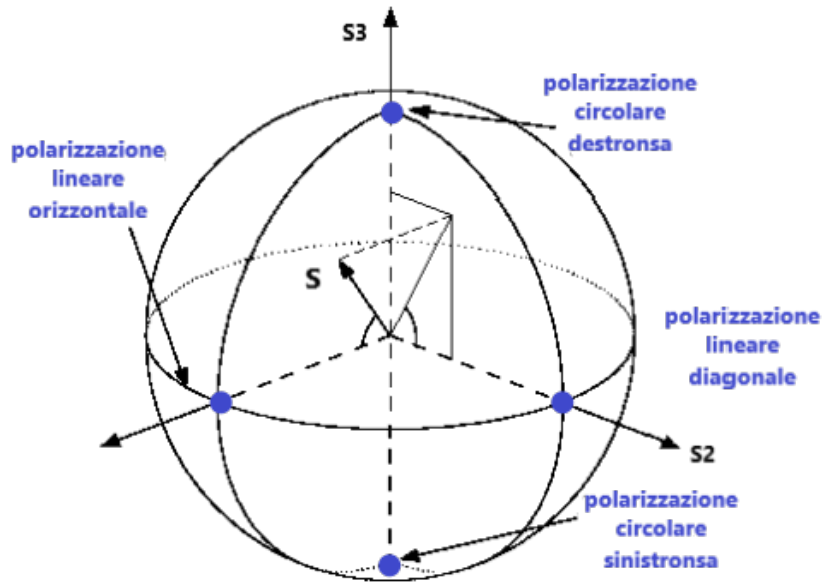

Figura 2.4: Rappresentazione di alcuni stati di polarizzazione sulla sfera di Poincaré.

2.4 Formalismo di Mueller

Per unire la comodità del calcolo matriciale di Jones all'immediatezza della rappresentazione tramite vettori di Stokes e sfera di Poincaré conviene introdurre la trattazione di Mueller, con la quale è possibile utilizzare il formalismo matriciale con stati anche a polarizzazione non completa. In questo caso per descrivere i vari componenti ottici si usano matrici 4x4 e ogni matrice di Jones può essere trasformata in una matrice di Mueller tramite la relazione:

$$\boldsymbol{M_J = A(J \otimes J^*)A^{-1}} \tag{2.18}$$

con

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & i & -i & 0 \end{bmatrix} \tag{2.19}$$

Mentre il viceversa non sempre è possibile, per i motivi menzionati sopra.
La relazione che lega gli stati in ingresso a quelli in uscita è:

$$\boldsymbol{S_{out} = M S_{in}} \tag{2.20}$$

Con **S** vettori di Stokes e **M** matrice di Mueller del campione o del componente ottico in considerazione.

Capitolo 3

Polarimetro di Stokes

Ricordando che lo scopo del lavoro presentato in questa tesi è andare a verificare la bontà degli stati creati dalla sorgente non-ideale POGNAC, lo strumento che è stato utilizzato per far ciò è il polarimetro di Stokes a sei canali. Si tratta di un analizzatore di stati di polarizzazione a sei uscite, che permette di misurare tutte e quattro le componenti dei vettori di Stokes degli stati che riceve in ingresso.

3.1 Setup

Il setup del polarimetro che è stato creato è il seguente:

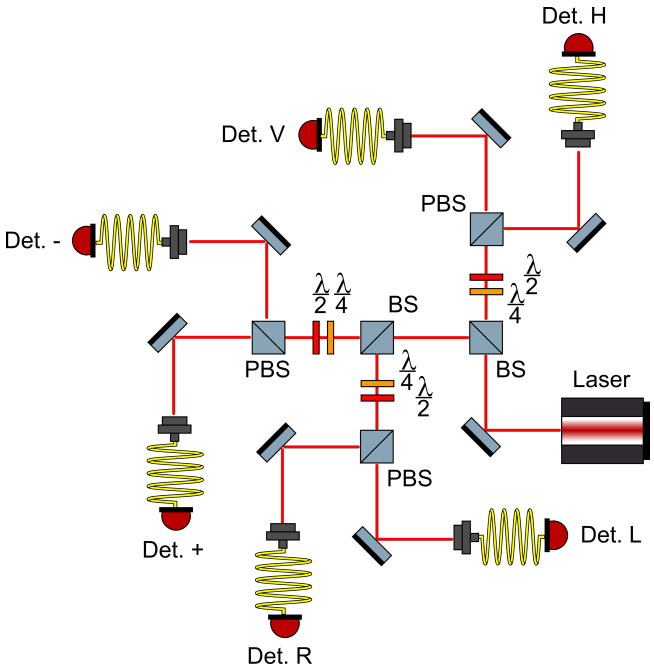

Figura 3.1: Schema ottico del polarimetro.

Come sorgente in ingresso si è utilizzato un laser (MMC-GASFP) a 1550 nm e 1.01 mW di potenza, il quale entra nel polarimetro attraverso una fibra SM e un collimatore. Per generare stati 'ideali' è stato utilizzato un polarizzatore di Glan-Taylor e una lamina a quarto d'onda, in modo da valutare le risposte del polarimetro e poterlo calibrare di conseguenza. Lo specchio che segue ha la funzione di agevolare la procedura di allineamento del fascio tra entrata ed uscita.
Da questo punto inizia propriamente il setup del polarimetro: il fascio incontra due beam splitter a 50:50 che lo separano nei tre rami, ovvero nelle tre basi di misura $(|H\rangle, |V\rangle)(|+\rangle, |-\rangle)(|L\rangle, |R\rangle)$. Ognuno dei tre rami prevede poi due lamine, una a $\frac{\lambda}{4}$ e l'altra a $\frac{\lambda}{2}$, in modo da garantire che ogni

coppia di uscite misuri i due stati ortogonali stabiliti. Infine, è presente un PBS che divide la luce in due fasci aventi polarizzazione ortogonale e che porta alle sei uscite del polarimetro, precedute da uno specchio ciascuna. Ad ogni uscita il fascio laser entra in un collimatore collegato in fibra al detector.

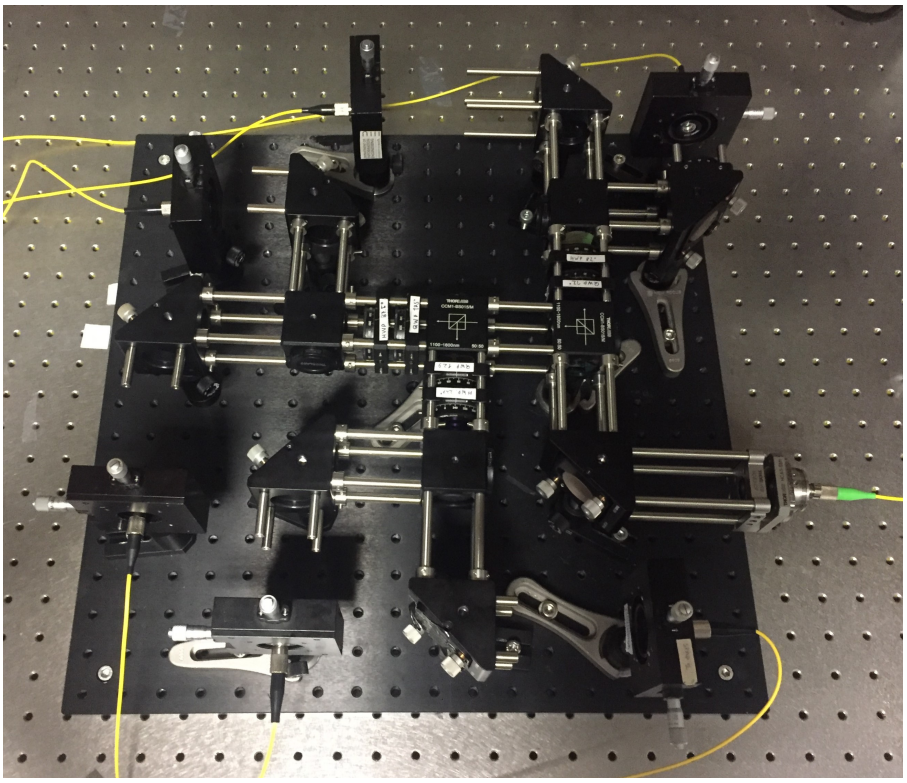

Figura 3.2: Setup del polarimetro.

Per prima cosa è stato necessario accoppiare in fibra le uscite del polarimetro, ovvero verificare che il laser una volta compiuto tutto il percorso ottico, fosse allineato ai collimatori posti alle sei uscite del polarimetro. Per far questo sono state regolate le viti presenti nel supporto del collimatore in entrata, in tutti gli specchi e nei supporti dei collimatori finali, controllando che il Power Meter posto ad ogni uscita rilevasse la massima intensità possibile. Si è ottenuto un accoppiamento del 30% tra intensità rilevata nel collimatore grazie alla fibra e quella all'uscita degli specchi.
Il passo successivo è stato regolare le tre coppie di lamine, in modo che ognuno dei tre rami misurasse in una base e che, quindi, alle sei uscite totali venissero effettivamente misurati i sei stati: $|H\rangle, |V\rangle, |+\rangle, |-\rangle, |L\rangle, |R\rangle$. Per fare questo, sono stati generati uno alla volta i sei diversi stati di polarizzazione attraverso le configurazioni del polarizzatore di Glan-Taylor e della lamina QWP riportate nella seguente tabella:

stato mandato	$\theta_{polarizzatore}(gradi)$	$\theta_{QWP}(gradi)$
$\|H\rangle$	230	assente
$\|V\rangle$	320	assente
$\|+\rangle$	275	assente
$\|-\rangle$	5	assente
$\|L\rangle$	275	222
$\|R\rangle$	5	222

Tabella 3.1: Angoli di polarizzatore e lamina per ottenere i sei stati.

e, assegnata ad ogni ramo una base di misura, sono state ruotate le coppie di lamine QWP e HWP in modo che i Power Meter posti alle uscite registrassero il massimo dell'intensità all'invio dello stato che avrebbe dovuto misurare quella uscita. Di conseguenza, l'altra uscita di quel ramo avrebbe registrato un minimo nell'intensità e si sarebbe così distinto quale dei due stati ortogonali fosse stato mandato.

3.2 Calibrazione

Una volta ottimato il setup, si è passati alla calibrazione del polarimetro, ovvero a caratterizzarne il comportamento attraverso una matrice **W**, detta appunto matrice di calibrazione del polarimetro. La relazione che lega gli stati mandati in ingresso alle intensità rilevate all'uscita del polarimetro è:

$$\mathbf{S} = \mathbf{W}\ \mathbf{I} \tag{3.1}$$

con **S** matrice 4xn, le cui colonne sono formate dai vettori di Stokes degli stati inviati e **I** matrice 6xn, le cui colonne sono formate dalle intensità misurate dai 6 detector. n è il numero di stati inviati. Dunque, per ricavare **W**, sono stati generati gli $n = 6$ stati definiti nella tabella 3.1 e, per ognuno di questi, sono state raccolte le 6 intensità viste dai Power Meter Det. H, V, +, -, L, R in figura 3.1. Tali intensità vengono riportate nella seguente tabella:

detector	$\|H\rangle$ (μW)	$\|V\rangle$ (μW)	$\|+\rangle$ (μW)	$\|-\rangle$ (μW)	$\|L\rangle$ (μW)	$\|R\rangle$ (μW)
$Det.H$	120.40	4.40	63.30	62.70	59.50	66.10
$Det.V$	0.06	126.70	62.10	64.30	61.30	59.80
$Det.+$	19.60	30.00	51.20	0.87	27.10	22.50
$Det.-$	27.10	20.20	0.50	46.10	20.50	25.60
$Det.L$	25.20	24.90	23.80	26.60	47.60	0.26
$Det.R$	26.30	23.00	25.20	24.50	0.11	48.50

Tabella 3.2: Intensità viste dai sei detector mandando i sei stati ideali.

Dunque, la matrice **I** riporta come colonne, le colonne della tabella 3.2, normalizzate alla potenza totale del laser in ingresso, pari a 1.01 mW.
Facendo invece riferimento alla tabella 2.4 in cui sono definiti i vettori di Stokes per i diversi stati di polarizzazione, la matrice **S** degli stati inviati risulta essere:

$$\mathbf{S} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \tag{3.2}$$

La matrice di calibrazione **W** è stata, dunque, ricavata seguendo il metodo descritto nell'articolo [11], che prevede l'utilizzo della pseudo-inversa di Moore-Penrose:

$$\boldsymbol{W} = \boldsymbol{S}\boldsymbol{I}^{+} \tag{3.3}$$

$$\mathbf{W} = \begin{bmatrix} 20.456 & 17.889 & 1.454 & 2.272 \\ 1.499 & -13.350 & -16.912 & -19.495 \\ 21.426 & 18.052 & -31.967 & -80.315 \\ 5.799 & 4.004 & 8.509 & 8.602 \end{bmatrix} \tag{3.4}$$

Capitolo 4

Caratterizzazione del POGNAC

Ora che è noto il comportamento del polarimetro in funzione degli stati che riceve in ingresso, sostituendo il generatore di stati 'ideali' usato fino ad ora, ovvero il laser che incide sul polarizzatore di Glan-Taylor e sulla lamina QWP, con una sorgente 'reale' quale il POGNAC, è possibile valutare quanto si discostino dal caso ideale gli stati generati da quest'ultima.
Il setup complessivo prevede: un FPGA a controllo del laser, dei modulatori di fase e intensità, collegata ad un laser (Q fotonics QDFBLD-1550) il quale genera impulsi con un repetition rate di 50MHz, un modulatore di intensità, il quale crea i decoy states per riuscire ad ottenere una sorgente a singolo fotone e il POGNAC. Quest'ultimo è a sua volta collegato all'entrata del polarimetro e, infine, alle sei uscite in fibra sono presenti altrettanti polarization controller e detector SNSPD.
Il POGNAC utilizzato in questo esperimento riporta delle modifiche rispetto a quello descritto nella sezione 1.3: sono stati introdotti degli automatic polarization controller, in modo da compiere rotazioni molto più precise e regolabili attraverso il software Kinesis e il circolatore è stato sostituito con un beam splitter.
Gli SNSPD, invece, sono detector a singolo fotone tra i migliori attualmente disponibili, grazie al loro basso dark counts e all'alta efficienza raggiunta:

detector	canale	efficienza%
$Det.H$	1	87
$Det.V$	6	74
$Det.+$	8	81
$Det.-$	7	81
$Det.L$	4	52
$Det.R$	2	28

Tabella 4.1: Efficienze dei detector.

4.1 Raccolta e analisi dati

La fase di raccolta dati consiste nella generazione e nell'invio da parte del POGNAC dei tre stati $|+\rangle, |H\rangle, |V\rangle$ e delle sequenze $|H\rangle|+\rangle$, $|H\rangle|V\rangle$, $|V\rangle|+\rangle$; per ognuno di questi invii sono stati registrati i conteggi visti dai sei detector, per un tempo di acquisizione di circa 5 minuti l'uno. Tuttavia, avendo le prese dati dei tempi di acquisizione effettivi diversi tra loro, si sono presi in considerazione solo i primi 9.85 s, pari alla presa dati risultata essere più breve a causa di un problema nel software di acquisizione.
Il software di acquisizione, il QuTAG, registra l'orario e il canale in cui arriva un fotone: questi conteggi sono stati quindi suddivisi in base al canale e, dal momento che il segnale è periodico di 20 ns, è stato calcolato il modulo 20000 (o 40000 quando si hanno sequenze di due stati) dell'orario registrato.

Tali conteggi, per ogni stato mandato e per ciascun canale, sono stati graficati in istogrammi che hanno mostrato un picco Gaussiano nel caso di stato singolo e due picchi nel caso delle sequenze di due stati. Un esempio è riportato nei grafici seguenti:

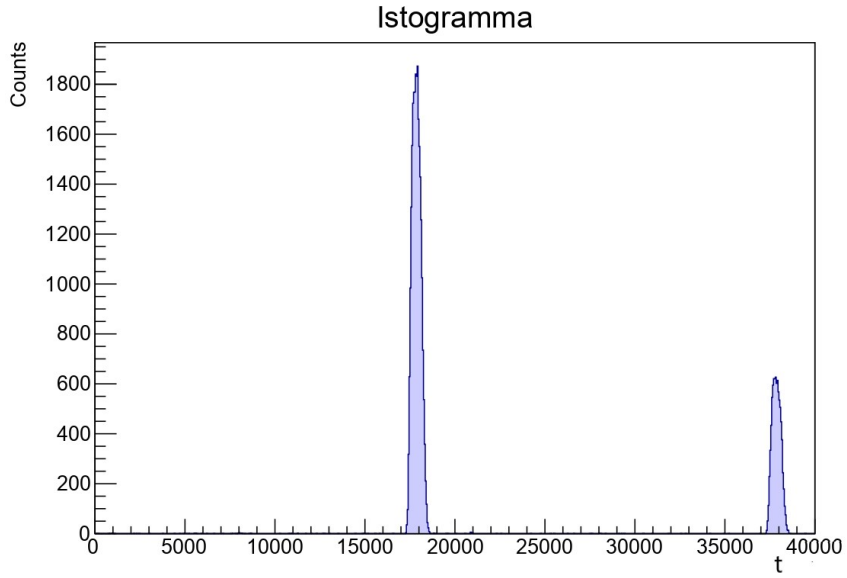

Figura 4.1: Conteggi visti dal quinto detector quando si manda la sequenza HD.

Gli istogrammi sono stati fittati con una Gaussiana e, attraverso il parametro $sigma$, si è calcolata la larghezza a mezza altezza del picco: $fwhm = sigma\sqrt{8ln(2)}$. Dunque si sono considerati e sommati solo i conteggi interni all'intervallo $[mean - fwhm; mean + fwhm]$, con $mean$ media del fit Gaussiano.

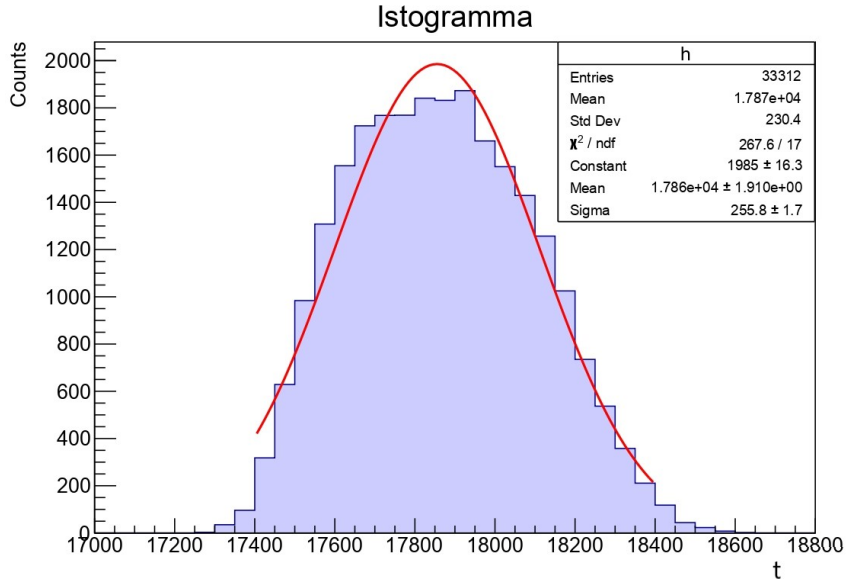

Figura 4.2: Ingrandimento sul primo picco.

I conteggi sono quindi stati normalizzati all'efficienza del rispettivo canale (riportata nella tabella 4.1) e, dal momento che la loro distribuzione è di tipo Poissoniano, l'errore σ ad essi associato è dato dalla radice del numero di conteggi, normalizzato anch'esso all'efficienza del relativo detector.
Tali dati sono riportati in tabella 4.2 per gli stati mandati singolarmente, nelle tabelle 4.3, 4.4 per gli stati mandati in sequenza.

detector	$\|+\rangle$		$\|H\rangle$		$\|V\rangle$	
	conteggi	σ	conteggi	σ	conteggi	σ
Det.H	1502874	1314	1516011	1320	434610	707
Det.V	862999	1080	774731	1023	2504230	1840
Det.+	488552	777	123526	391	1045102	1136
Det.−	470683	762	706449	934	67619	289
Det.L	84773	404	649171	1117	293796	752
Det.R	147711	726	53589	437	108146	621

Tabella 4.2: Conteggi e relativi errori degli stati mandati singolarmente.

detector	$\|H\rangle$		$\|+\rangle$	
	conteggi	σ	conteggi	σ
Det.H	811317	966	706383	901
Det.V	379927	717	375484	712
Det.+	59119	270	209527	509
Det.−	364654	671	254814	561
Det.L	310765	773	43527	289
Det.R	77057	525	25329	301

detector	$\|H\rangle$		$\|V\rangle$	
	conteggi	σ	conteggi	σ
Det.H	936464	1037	350940	635
Det.V	517155	836	1694595	1513
Det.+	84185	322	726072	947
Det.−	430072	729	55772	262
Det.L	477133	958	153942	544
Det.R	81411	539	26939	310

Tabella 4.3: Conteggi e relativi errori degli stati mandati in sequenza, $|H\rangle\,|+\rangle$ a sinistra e $|H\rangle\,|V\rangle$ a destra.

É stata fatta un'ulteriore rinormalizzazione dei conteggi presentati nelle tabelle 4.2, 4.3 e 4.4, al numero totale di fotoni inviati, ovvero al prodotto tra il numero di impulsi mandati e il numero medio di fotoni per impulso. Il primo dei due termini si ricava dalla moltiplicazione del tempo di acquisizione per il repetition rate di 50 MHz, il secondo, invece, è il rapporto tra la somma dei conteggi in ogni canale (normalizzati alle rispettive efficienze) e il numero di impulsi mandati per la perdita di fotoni dovuta all'accoppiamento in fibra, pari al 30%. Inoltre, per tener conto delle perdite in ciascun ramo del polarimetro, nel compiere questi calcoli si è imposto che la distribuzione nelle tre basi fosse la stessa osservata in fase di calibrazione, ovvero il 56.1% nella base H/V, il 21.8% in +/- e il restante 22.1% in L/R.
Con questo procedimento si riesce ad costruire un vettore 6-dimensionale per ogni stato inviato, ove ciascuna componente rappresenta l'intensità rinormalizzata rilevata da ciascun detector. Dunque, ricavati questi vettori è possibile procedere al calcolo dei rispettivi vettori di Stokes.

4.2 Calcolo vettori Stokes

Attraverso la matrice di calibrazione del polarimetro **W** 3.4 e all'equazione 3.1, inserendo al posto della matrice **I** descritta nella sezione 3.2, i vettori delle intensità ottenuti nel paragrafo precedente, si sono potuti calcolare i vettori di Stokes $\boldsymbol{S}$ degli stati mandati dal POGNAC.
Tuttavia, per avere una miglior stima di tali vettori e per poter quantificare l'errore sperimentale, sono state fatte 100 simulazioni dei conteggi visti dai sei detector, presi ciascuno dalle distribuzioni Poissoniane aventi come media i conteggi ricavati dall'istogramma e presentati nelle tabelle 4.2, 4.3 e 4.4. A ciascun esito della simulazione ed è stata poi applicata la stessa analisi dei dati sperimentali descritta in precedenza. Infine, è stata fatta una media dei vettori di Stokes simulati e ne è stata calcolata la deviazione standard $\boldsymbol{\sigma}$. Tali risultati vengono riportati in tabella 4.5, dove le prime tre righe rappresentano gli stati mandati singolarmente, mentre le altre tre coppie di righe corrispondono alle sequenze di stati.

detector	$\|V\rangle$		$\|+\rangle$	
	conteggi	σ	conteggi	σ
$Det.H$	216989	499	732076	917
$Det.V$	1045409	1189	424982	758
$Det.+$	443278	740	207953	507
$Det.-$	34927	208	254243	560
$Det.L$	134010	508	35229	260
$Det.R$	83096	545	52761	434

Tabella 4.4: Conteggi e relativi errori degli stati $|V\rangle\,|+\rangle$ mandati in sequenza.

stato mandato	$\boldsymbol{S}$				$\boldsymbol{\sigma}$			
$\|+\rangle$	$[1.0000$	0.2531	-0.784	$0.606]$	$[0.0001$	0.0007	0.001	$0.002]$
$\|H\rangle$	$[1.0000$	0.2111	0.044	$-0.246]$	$[0.0002$	0.0006	0.001	$0.003]$
$\|V\rangle$	$[1.0000$	-0.6745	0.8872	$0.445]$	$[0.0002$	0.0005	0.0007	$0.003]$
$\|H\rangle$	$[1.0000$	0.2111	0.044	$-0.246]$	$[0.0002$	0.0007	0.001	$0.004]$
$\|+\rangle$	$[1.0000$	0.2531	-0.784	$0.606]$	$[0.0002$	0.0009	0.001	$0.002]$
$\|H\rangle$	$[1.0000$	0.2411	-0.114	$0.288]$	$[0.0003$	0.0009	0.002	$0.006]$
$\|V\rangle$	$[1.0000$	-0.6103	0.8346	$0.717]$	$[0.0002$	0.0006	0.0008	$0.004]$
$\|V\rangle$	$[1.0000$	-0.6102	0.8346	$0.717]$	$[0.0002$	0.0006	0.0009	$0.004]$
$\|+\rangle$	$[1.0000$	0.2001	-0.096	$-0.174]$	$[0.0002$	0.0009	0.002	$0.005]$

Tabella 4.5: Vettori di Stokes degli stati del POGNAC ricavati dalla simulazione e rispettiva deviazione standard.

Capitolo 5

Conclusioni

I vettori riportati in tabella 4.5, ottenuti dai dati sperimentali e dalla simulazione, non possono essere confrontati direttamente con i vettori ideali riportati invece in tabella 2.4, in quanto il collegamento tra POGNAC e polarimetro è effettuato tramite svariati metri di fibra a singolo modo, la quale introduce modifiche randomiche allo stato che il POGNAC invia. Dunque, lo stato che rivela il polarimetro non è più quello che nominalmente il POGNAC dovrebbe aver inviato. Tuttavia, ciò che è importante ai fini della QKD è che $\boldsymbol{S_H}$ e $\boldsymbol{S_V}$ siano antiparalleli perchè ai poli opposti della sfera di Poincaré, mentre che $\boldsymbol{S_+}$ sia ortogonale ad essi. Di conseguenza, ci si aspetta che $\langle H|V\rangle = 0$, $\langle H|+\rangle = \frac{1}{\sqrt{2}}$ e $\langle V|+\rangle = \frac{1}{\sqrt{2}}$.
Per verificare queste relazioni si è, perciò, calcolato il prodotto interno tra gli stati che i vettori di Stokes rappresentano e i risultati sono i seguenti:

$\langle H\|+\rangle$	$\langle H\|V\rangle$	$\langle V\|+\rangle$
0.659 ± 0.001	0.6274 ± 0.0009	0.449 ± 0.001

Tabella 5.1: Prodotti interni tra gli stati inviati singolarmente dal POGNAC.

$\langle H\|+\rangle$	$\langle H\|V\rangle$	$\langle V\|+\rangle$
0.659 ± 0.001	0.694 ± 0.002	0.580 ± 0.002

Tabella 5.2: Prodotti interni tra gli stati inviati in sequenza dal POGNAC.

Come dimostrano i risultati ottenuti, mentre $\langle H|+\rangle$ sembra avvicinarsi al valore atteso, per i prodotti $\langle H|V\rangle$ e $\langle V|+\rangle$ non c'è corrispondenza, indice del fatto che durante la fase di calibrazione del polarimetro o di presa dati sono subentrati degli errori. Se gli stati che generasse il POGNAC avessero realmente questi prodotti scalari, il key rate ne risentirebbe e diminuirebbe [7].

I risultati non sono, dunque, ottimali e purtroppo non è stato possibile ripetere le misurazioni a causa dei tempi e degli accessi limitati ai laboratori come conseguenza della situazione attuale. Tuttavia, se fosse stato possibile, un miglioramento da apportare alla misura sarebbe sicuramente quello di ottimizzare i conteggi visti dagli SNSPD attraverso il polarization controller, minimizzando quelli rilevati dal detector designato a misurare lo stato ortogonale a quello mandato, e non cercando di massimizzare quelli visti dal detector predisposto alla misurazione di tale stato. In questo modo si riuscirebbero a migliorare i rapporti tra gli stati della stessa base e, nello specifico, il rapporto tra H e V che, come dimostrato, non è risultato essere quello atteso.

Bibliografia

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. *Quantum cryptography.* Rev. Mod. Phys. 74, 145 (2002).

[2] R. L. Rivest, A. Shamir, and L. Adleman. *A method for obtaining digital signatures and public-key cryptosystems.* Commun. ACM 21, 120 (1978).

[3] P. W. Shor. *Polynomial-time algorithms fir prime factorization and discrete logarithms on a quantum computer.* SIAM J. Comput. 26, 1484 (1997).

[4] C. H. Bennett, and G. Brassard. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing.* Bangalore, India, December 1984, pp. 175–179.

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. *The security of pratical quantum key distribution.* Rev. Mod. Phys. 81, 1301 (2009).

[6] F. Xu, X. Ma, Q. Zhang, H. Lo, and J. Pan. *Secure quantum key distribution with realistic devices.* Rev. Mod. Phys. 92, 025002 (2020).

[7] M. Pereira, M. Curty, and K. Tamaki. *Quantum key distribution with flawed and leaky sources.* npj Quantum Inf. 5, 62 (2019).

[8] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi. *Simple quantum key distribution with qubit-based synchronization and self-compensating polarization encoder.* Optica 7, 284 (2020).

[9] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone. *All-fiber self-compensating polarization encoder for quantum key distribution.* Opt. Lett. 44, 2398-5401 (2019).

[10] B. E. A. Saleh, and M. C. Teich. *Foundamentals of photonics.* Wiley Series in Pure and Applied Optics, B. E. A. Saleh, Series Editor, second edition (2007).

[11] B. Boulbry, J. C. Ramella-Roman, and T. A. Germer. *Improved method for calibrating a Stokes polarimeter.* Appl. Opt. 46, 8533-8541 (2007).