Università degli Studi di Padova

Centro di Ateneo di Studi e Attività Spaziali "Giuseppe Colombo" (CISAS)

Corso di Dottorato di Ricerca in
Scienze Tecnologie e Misure Spaziali

Curriculum: Scienze e Tecnologie per Applicazioni Spaziali e Aeronautiche (STASA)

# Space Quantum Communication

*Coordinatore:*
Ch.mo Prof. Giampiero Naletto

*Supervisore:*
Ch.mo Prof. Giampiero Naletto

*Co-supervisore:*
Ch.mo Prof. Paolo Villoresi

*Dottorando:*
Matteo Schiavon

XXIX CICLO

# Ringraziamenti

Innanzitutto vorrei ringraziare il Prof. Giampiero Naletto, per avermi fatto da supervisore in questa tesi di dottorato e per il lavoro da lui svolto per il corso di dottorato in Scienze, Tecnologie e Misure Spaziali. Ringrazio poi i Prof. Paolo Villoresi e Giuseppe Vallone, per avermi accettato nel loro gruppo di ricerca e per le molte cose che, grazie a loro, ho imparato.

Quindi, vorrei ringraziare tutte le persone con cui ho avuto modo di lavorare in questi tre anni al Luxor e quelle con cui ho avuto il piacere di condividere le pause pranzo. Non me ne vogliate se non vi ringrazio uno ad uno, ma ognuno di voi meriterebbe un paragrafo a parte, facendo lievitare le dimensioni di questa tesi (nonché facendomi mancare la scadenza del 31 Gennaio).

Ringrazio quindi i miei amici: i pochi compagni delle medie con i quali, nonostante i quasi tre lustri, sono ancora in contatto; il gruppo delle superiori (comprese le aggiunte più recenti), i quali hanno alleviato la noia di innumerevoli sabati e domeniche; i colleghi dell'università, ormai sparpagliati in giro per l'Europa. Anche voi meritereste una menzione uno per uno, ma anche in questo caso lo spazio-tempo è un limite.

Ringrazio poi gli Amatori Atletico 2000 per l'ignoranza, fonte di ristoro dopo le troppe ore di scienza.

Ringrazio la mia famiglia, mia madre Valeria, mio padre Luigi, mio fratello Luca, i miei zii Fausto e Milena, Dalì, gli zii e i cugini da parte di padre (molti di più), per esserci sempre stati quando ne avevo bisogno (e non solo).

Infine, ringrazio coloro che, per mia dimenticanza, non sono menzionati in questa lista. Non ne abbiano a male.

# Introduction

At the end of the nineteenth century, physical theory had reached a high level of maturity, being able to explain almost all natural phenomena. This explanation was supported by a highly developed experimental practice, a fundamental tool for the confirmation of the theoretical models. Nevertheless, some aspects, such as light propagation without ether, the interaction between light and matter and black-body radiation, still lacked a theoretical explanation. The quest for such explanation is the basis of the scientific revolution that took place in the first 30 years of twentieth century. The first paradigm shift is the new approach to space and time led by the theories of special and general relativity. The second one is due to quantum physics, which profoundly modifies even the concept of physical reality. Despite its experimental verification to a level of precision unknown to all other physical theories, a philosophical interpretation of quantum theory is still lacking.

Indeed, many aspects of the theory are in strong contrast with the logic at the basis of our study of nature. It predicts that light behaves both like a wave and a particle, and extends the same duality to the matter, giving rise to interference phenomena between particles, such as electrons, atoms or even molecules. Moreover, one of its key features, the *indeterminacy principle*, states that it is impossible to know both the position and the velocity of a particle with arbitrary precision, making the mere definition of particle a critical issue. Probably, one of the most shocking aspects of the theory is the existence of *entangled states*, i.e., multi-particle states that cannot be described as a sum of the states of the particles composing them. This effect makes it difficult to give a proper interpretation of the concepts of reality and locality, which are at the basis of all other physical theories.

More recently, some people have started to look at this weirdness from another point of view, looking for some methods to exploit it for the solution of practical problems. The beginning of the eighties, indeed, saw the first proposals for the use of quantum systems in practical problems of information theory, a field in full expansion with the spread of computers and communication systems. The exploitation of entangled systems was looked as a way of enhancing some computation tasks, giving rise to the first proposals of *quantum computing* algorithms, while the indeterminacy principle was the basis of the new *quantum communication* protocols, such as *quantum cryptography.*

This last field, in particular, has reached the highest level of maturity among all the other applications of quantum theory, especially for what concerns the problem of the secure exchange of cryptographic keys (*quantum key distribution*). Quantum key distribution (QKD) is already a commercial reality, even though still restricted to high level costumers like banks or governments. Its force lies in the fact that it allows two parties to exchange a secure cryptographic key by exploiting the indeterminacy principle. Since an eavesdropper cannot gain information about the quantum state without perturbing it, it is possible to bound the information leaked by looking at the transmission error in the channel. If this information is low enough, it is possible to use information theory techniques to distill a secret key between the two parties. What makes this protocols so appealing is the fact that their security is not based on some assumptions on the computational power of the attacker, like in the key exchange protocols used on the internet, but they can be proved secure even if the adversary has complete control on the communication channel. This is called *unconditional security.*

A major problem of quantum cryptography is the fact that it is based on the transmission of quantum states, i.e., single- or few-photon states. Moreover, the indeterminacy principle makes it impossible to copy and, consequently, “amplify” quantum states, limiting the use of quantum cryptography to channels with attenuation low enough to allow a significant fraction of the transmitted photons to reach the detector. In fiber-based channels, this distance is limited to a few hundred kilometers. This is the reason for the interest in free-space quantum communication, especially in the ground-satellite channel. In this channel, indeed, most the propagation happens in vacuum. This allows the transmission of single-photon states over distances longer that one thousand kilometers.

This thesis work studies this aspect of quantum communication, i.e., the implementation in the laboratory of quantum communication protocols that could, in the future, be applied to free-space and satellite-based optical communication. This comes side by side with the improvement of the receiving station for quantum communications at the Matera Laser Ranging Observatory (MLRO), managed by the Italian Space Agency (ASI). This thesis, therefore, describes both the study, in the laboratory, of techniques and protocols for free-space quantum communication and the experimental activity in the ground-satellite channel.

Chapter 1 gives a short introduction to quantum information, starting from an axiomatic description of quantum mechanics, followed by the exposition of some useful models for the study of quantum protocols. This is followed by a brief description of the ways of encoding and processing information using the electromagnetic field, the most suitable mean to transfer information over long distances.

Chapter 2 is focused on the development of a source of polarization-entangled photons. Among the different ways of information encoding, indeed, polarization plays a crucial role for what concerns the transmission over the free-space channel. This degree of freedom, indeed, preserves itself over propagation through long distances, proving a suitable choice for the ground-satellite link. The source is based on a non-linear crystal in a polarization-based Sagnac interferometer, giving the high pair generation rate required in high loss channels. It is built in an optical breadboard and has fiber-based inputs and outputs, in order to be easily transportable for experiments out of the laboratory. In this Chapter, after a brief physical introduction, this source is described, both in its design and in its experimental characterization.

Chapter 3 describes the laboratory-based part of the thesis. It is divided in two large Sections, the first on the study of some aspects of Quantum Key Distribution (QKD), the second one reporting the results of a recent experiment investigating some recently discovered aspects of non-locality. Section 3.1 starts with the theoretical study of the performance of a new kind of single-photon source, based on a chain of non-linear crystals in an asymmetric configuration, when inserted in a real QKD environment. Then, it describes the proof-of-principle of a three-state QKD protocol, which presents an interesting compromise between noise tolerance and a low-resource receiver, both important for free-space or satellite-based applications. Section 3.2, on the other hand, describes the experimental study of a particular aspect of quantum non-locality, allowing two independent observers to share non-locality with a third one at the same time. This study is important both for its impact in basic research on quantum theory and for the study of the relationship between acquired information and disturbance on a measured system.

Chapter 4 starts the description of the exploitation of the space channel. This Chapter deals with the experimental work aimed at the improvement of the performance of the quantum communication station at the MLRO, activity performed in collaboration with the INFN within the project Moonlight-2. This improvement consists of a new design of the experimental setup, based on higher efficiency hardware. Besides the hardware improvement, a new software for data analysis has been developed. The software has been structured modularly, in order to allow an easy processing of the data coming from the new hardware and an easier development of newer analysis tasks for complex experiments. Another aspect of this work is the improvement of orbit estimation, a necessary step in the exploitation of the higher precision of the new hardware. A fundamental step to this goal is the use of the instrumental corrections applied by the laser ranging system.

Finally, Chapter 5 describes a recent experiment performed using the quantum communication station at the MLRO, demonstrating single-photon interference over the space channel. This experiment is fundamental to prove that time-bin encoding is a viable choice for quantum transmission in this channel.

# Introduzione

Alla fine del Diciannovesimo secolo, la teoria fisica era arrivata a un livello tale da essere in grado di spiegare praticamente tutti i fenomeni del mondo naturale e la pratica sperimentale si era evoluta al punto da essere diventata una parte fondamentale dello studio della natura. Nonostante ciò, erano ancora presenti alcuni aspetti che la teoria non era in grado di spiegare, in particolare riguardanti l'elettromagnetismo e le sue interazioni con la materia. Fenomeni come la propagazione della luce in assenza di etere, l'interazione tra atomi e campo elettromagnetico e la radiazione di corpo nero continuavano a sfuggire a ogni spiegazione, nonostante fossero stati verificati sperimentalmente con una precisione tale da non poter essere confutati. Sono stati proprio questi fenomeni, tutto sommato marginali se confrontati con la vastità della natura, che hanno portato, nei primi trent'anni del Ventesimo secolo, a una vera rivoluzione nel modo di vedere il mondo. La prima rivoluzione fu portata dalla teoria della relatività, che costrinse a rivedere il significato di concetti di base come lo spazio e il tempo. La seconda, e forse più profonda, rivoluzione fu quella portata dalla fisica quantistica, la quale mise in dubbio il concetto stesso di realtà e che, dopo quasi cent'anni e un livello di verifica sperimentale sconosciuto a qualsiasi altra teoria fisica, ancora sfugge a qualsiasi tentativo di interpretazione in uno scenario logico coerente.

Questa teoria, infatti, presenta molti aspetti in aperto contrasto con la logica sulla quale la conoscenza del mondo era (ed è tuttora) costruita. Essa prevede, infatti, non solo che la luce si comporti sia come onda che come particella, ma che questa dualità sia presente anche nella materia, oppure che la posizione e la velocità di una particella non siano di principio conoscibili con assoluta precisione, ma che una maggiore conoscenza di una sia causa di una maggiore incertezza nell'altra (*principio di indeterminazione*). Spingendosi oltre, essa prevede l'esistenza di sistemi di due particelle in uno stato tale da non poter essere descrivibile a partire dalla descrizione delle singole particelle (*entanglement*), un fenomeno che porta a mettere in discussione un concetto di base come la realtà di una teoria fisica.

Più recentemente si è intuito come queste stranezze, se sfruttate, potessero dare origine a nuove opportunità. Agli inizi degli anni '80, infatti, si cominciarono a proporre le prime possibili applicazioni di sistemi quantistici alla crescente teoria dell'informazione, sia nel campo del processamento e dell'elaborazione dell'informazione, con la *computazione quantistica*, sia nel campo della trasmissione dell'informazione, con i vari protocolli di *comunicazione quantistica*, tra i quali un'importanza particolare detengono quelli di *crittografia quantistica.*

Il campo della crittografia quantistica, in particolare, è quello che al momento attuale è giunto al maggior livello di maturità, soprattutto per quel che riguarda lo scambio di chiavi crittografiche. Le prime applicazioni commerciali, anche se ancora per una clientela di fascia molto alta, sono già una realtà, e forte è la competizione per renderle accessibili anche al di fuori di università e istituzioni governative. Essa permette a due parti di scambiare una chiave crittografica in modo sicuro sfruttando il principio di indeterminazione, grazie al quale, monitorando l'errore di trasmissione nel canale, è possibile dare una stima della massima informazione che un eventuale intercettatore può aver acquisito. Nel caso questa informazione sia sufficientemente bassa, si possono utilizzare tecniche di teoria dell'informazione per arrivare ad avere una chiave segreta condivisa tra le due parti. La cosa importante di questi protocolli è che la loro sicurezza non è basata sull'assunzione di un limitato potere computazionale da parte dell'attaccante, come i protocolli attualmente in uso per lo scambio di chiavi attraverso internet, ma dà all'avversario potere illimitato sul canale di comunicazione. Questo tipo di sicurezza è definito *sicurezza incondizionata*.

Uno dei problemi della crittografia quantistica è che essa si basa sulla trasmissione di stati quantistici, cioè principalmente stati a singolo o a numero ridotto di fotoni. Inoltre, il principio di indeterminazione, se da una parte protegge lo stato quantistico da ogni tentativo di carpirne l'informazione, dall'altra ne impedisce la copia e, conseguentemente, l'amplificazione. Questo limita l'utilizzo della crittografia quantistica a distanze sulle quali l'attenuazione dovuta al canale sia tale da permettere a una frazione significativa dei fotoni trasmessi di arrivare a destinazione. Per quanto riguarda le fibre ottiche, questa distanza è limitata a qualche centinaio di chilometri. Questo è il motivo dell'interesse per le comunicazioni quantistiche in spazio libero e, in particolare, via satellite. Per esse, infatti, la trasmissione avviene per la maggior parte nel vuoto, permettendo di effettuare trasmissione a singolo fotone su distanze dell'ordine delle migliaia di chilometri.

Il lavoro di questa tesi si inserisce proprio in questo aspetto delle comunicazioni quantistiche, cioè lo studio a terra di protocolli e aspetti dell'informazione quantistica che potrebbero, in un futuro prossimo, portare ad applicazioni nel canale in spazio libero e, eventualmente, nel canale satellitare. A questo si affianca il lavoro di miglioramento e utilizzo della stazione per comunicazione quantistica satellitare presso il Matera Laser Ranging Observatory (MLRO), gestito dall'Agenzia Spaziale Italiana (ASI) e centro all'avanguardia in questo nascente settore. Questa tesi, quindi, descrive sia lo studio, in laboratorio, di tecniche e protocolli per la comunicazione quantistica in spazio libero che il lavoro sperimentale svolto nel canale terra-spazio.

Nel capitolo 1 viene fornita una breve introduzione alla meccanica quantistica prima e all'informazione quantistica in seguito, con riferimento ad alcuni modelli utili per lo studio dei protocolli quantistici, e una breve descrizione dei possibili modi per codificare e processare l'informazione usando il campo elettromagnetico, al momento attuale il mezzo più adatto per la trasmissione dell'informazione su lunghe distanze.

Il capitolo 2 riguarda invece lo sviluppo di una sorgente di fotoni entangled in polarizzazione. Tra i modi di codificare l'informazione, infatti, la polarizzazione gode di un'importanza particolare, soprattutto per quanto riguarda le trasmissioni in spazio libero. Essa si può propagare inalterata per lunghe distanze ed ha già dimostrato di essere adatta in principio anche per le comunicazioni terra-satellite. Il tipo di sorgente scelto, basato su un cristallo non lineare inserito in un interferometro di Sagnac, ha la caratteristica importante di avere un alto tasso di generazione di coppie entangled, fondamentale per il suo utilizzo in situazioni ad alto livello di perdite come le comunicazioni su lunga distanza. La sorgente è costruita su una breadboard ottica ed ha fibre ottiche sia in ingresso che in uscita, in modo da poter essere facilmente trasportata. In questo capitolo, dopo una breve introduzione sulla fisica sottostante il suo funzionamento, questa sorgente verrà descritta, sia per quanto riguarda le scelte fatte nel suo progetto che i risultati della sua caratterizzazione.

Nel capitolo 3 viene data una descrizione del lavoro svolto in laboratorio. Esso è diviso in due sezioni, dal peso di un capitolo ciascuna, riguardanti una lo studio, sia teorico che sperimentale, di alcuni aspetti della crittografia quantistica, l'altra un esperimento volto a provare sperimentalmente alcuni recenti risultati sulla non località, altro aspetto fondamentale nell'implementazione di protocolli quantistici. Nel dettaglio, la sezione 3.1 affronta prima lo studio teorico delle prestazioni di un nuovo tipo di sorgente, basata su una catena di cristalli non lineari in configurazione asimmetrica, quando inserita in in contesto reale di crittografia quantistica, e in seguito presenta la proof of principle di un protocollo di crittografia quantistica a tre stati, il quale presenta un compromesso interessante tra risorse del ricevitore e tolleranza al rumore, entrambi aspetti importanti per l'implementazione in applicazioni in spazio libero o su satellite. Nella sezione 3.2, invece, viene studiato sperimentalmente un aspetto della non località quantistica legato alla possibilità che due osservatori indipendenti possano condividere simultaneamente tale non località con un terzo osservatore. Questo studio, oltre che essere importante dal punto di vista della ricerca di base, è fondamentale anche per sondare nuovi aspetti della relazione tra informazione acquisita e disturbo sul sistema misurato.

Col capitolo 4 comincia la parte rigurdante lo sfruttamento del canale spaziale. Questo capitolo in particolare si concentra sul lavoro fatto per il miglioramento delle performance della stazione di comunicazione quantistica presso MLRO, dovuta soprattutto alla collaborazione con l'INFN nell'ambito del progetto Moonlight-2. Questo miglioramento consiste in un nuovo design dell'apparato sperimentale, con l'utilizzo di strumenti più performanti. Oltre al nuovo schema hardware, questo processo ha portato alla riscrittura del software per l'analisi dei dati presi nei vari esperimenti terra-satellite. Il software è stato riscritto in maniera modulare, in modo da poter integrare facilmente i dati presi con la nuova strumentazione e da permettere l'analisi di esperimenti sempre più complessi. Un altro aspetto del lavoro di upgrade riguarda il miglioramento della stima delle orbite, necessario in modo da poter sfruttare la più alta precisione della nuova strumentazione. Fondamentale per questo aspetto è l'utilizzo nella stima non solo dei segnali provenienti dal sistema di laser ranging, ma anche delle correzioni strumentali applicate in tale sistema.

Infine il capitolo 5 è incentrato su un recente esperimento effettuato usando la stazione di comunicazione quantistica presso MLRO e dimostrante l'interferenza a singolo fotone sul canale spaziale, fondamentale per l'utilizzo della codifica in time bin su tale canale.

# Contents

# Chapter 1

# Elements of Experimental Quantum Information

Information theory is the science that studies the transmission, processing, utilization, and extraction of information. Since its birth, dating back to the 1948 article "A Mathematical Theory of Communication" by Claude E. Shannon [1], it is the theoretical framework upon which a large part of our technology is built. Information is strongly related to the physical system used to store it, as stated by Rolf Landauer in his famous sentence *"Information is physical"* [2].

In classical information theory, the information is carried by systems obeying the laws of classical physics. The state of a general system is described by a point in its phase space, while its evolution is described by the Hamiltonian of the system. There are two main ways of storing the information in a classical system: using an analog degree of freedom, such as the amplitude or the phase of an electromagnetic wave, or a digital one, by assigning different values to different, finite regions of the phase space. Nowadays, digital systems are dominant in general-purpose information transmission and processing, with analog ones playing a minor role.

The key element of a digital system is the *bit* (*bi*nary digi*t*), which can assume the values 0 or 1. Each value is represented by a different region of the phase space and the separation between the two regions is such that a noise-induced bit switch is very unlikely.

At the beginning of the 20th century, however, classical physics has shown to be inadequate to describe systems at a very small scale. For such systems, there is a fundamental limitation in the knowledge of the different measurable properties of the system, embodied by the *uncertainty principle*. Therefore, it is no longer possible to assign to a system a single point in the phase space, making classical physics inadequate to describe it. This led to the development of a new model for the description of physical systems: *quantum mechanics*. For this reason, the information stored in systems that cannot be described by classical physics can no longer be described using classical information theory, but requires the development of a new framework, *quantum information theory*.

This chapter will provide a short introduction of quantum mechanics from an axiomatic point of view, then it will deal with quantum information and its realization using optical systems.

## 1.1 The postulates of quantum mechanics

The fundamental difference between classical and quantum mechanics lies in the impossibility of knowing with arbitrary precision all the measurable properties of a physical system. Therefore, it is no longer possible to define a state by assigning a definite value to its measurable properties (e.g. position and momentum). This requires the construction of a new theoretical framework for the description of physical systems. Among the different formulations of quantum mechanics, the axiomatic one introduced by Dirac and Von Neumann is the most widely used in quantum information. It is based on a series of postulates, listed here below [3, 4].

**Postulate 1.** ***States.*** *A state is the complete description of a physical system. The state of an isolated physical system can be described by a normalized vector $|\psi\rangle$, unique up to a phase factor, in a projective complex Hilbert space $\mathscr{H}$.*

**Postulate 2.** ***Composition.*** *If the state of a system A is in $\mathscr{H}_A$ and the state of a system B is in $\mathscr{H}_B$, the state of the composite system AB is in the tensor product $\mathscr{H}_A \otimes \mathscr{H}_B$. Given a system A in state $|\psi\rangle_A$ and a system B in $|\phi\rangle_B$, then the state of the composite system is $|\psi\rangle_A \otimes |\phi\rangle_B$.*

**Postulate 3.** ***Dynamics.*** *The dynamics describes the evolution of a system over time. For any possible evolution of a closed physical system with state in $\mathscr{H}$ and for any fixed time interval $[t_0, t_1]$, there exists a unitary $U(t_0, t_1)$ describing it. A system in state $|\psi(t_0)\rangle$ evolves into $|\psi(t_1)\rangle = U\,|\psi(t_0)\rangle$. The unitary $U(t_0, t_1)$ is unique up to a phase factor and its form is determined by the Schrödinger equation*

$$\frac{d}{dt}\,|\psi(t)\rangle = -\frac{i}{\hbar}H(t)\,|\psi(t)\rangle\,,$$

*where $H$ is the Hamiltonian of the system.*

**Postulate 4.** ***Observables.*** *An observable is a property of a physical system that can in principle be measured. All observables are represented by self-adjoint linear operators acting on $\mathscr{H}$. The possible values that an observables $O$ can assume are the eigenvalues $x$ of the correspondent operator. Since $O$ is self-adjoint, it takes the form $O = \sum_x x\Pi_x$, where $\Pi_x$ is the projector onto the subspace with eigenvalue $x$.*

**Postulate 5.** ***Measurements.*** *Measurement is the process of acquiring information about a measurable property of a system. If the state just prior to the measurement is $|\psi\rangle$, then the probability of observing outcome $x$ is*

$$\mathbb{P}_X(x) = Tr\left[\Pi_x\,|\psi\rangle\,\langle\psi|\right].$$

*If the outcome of the measurement is $x$, the state $|\phi_x\rangle$ of the system just after the measurement is*

$$|\phi_x\rangle = \sqrt{\frac{1}{\mathbb{P}_X(x)}}\Pi_x\,|\psi\rangle\,.$$

## 1.2 The Qubit

The basic unit of classical information theory is the *bit*, an object that can assume two values, 0 or 1. Similarly, quantum information theory has adopted as basic unit its quantum counterpart, called *qubit* (quantum bit). It is a two-level system described within the framework of quantum mechanics. Because of Postulate 1, such a system corresponds to a two-dimensional Hilbert space $\mathscr{H} \approx \mathbb{C}^2$, with basis vectors $|0\rangle$ and $|1\rangle$. The general qubit state $|\psi\rangle$, therefore, is written as

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

where $\alpha$ and $\beta$ are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$. Postulate 1 states also that quantum states are defined up to a global phase factor (the vectors $|\psi\rangle$ and $e^{i\gamma}|\psi\rangle$ describe the same physical state). Therefore, it is possible to take as representative of the physical state the vector with $\alpha \in \mathbb{R}$. This, together with the requirement of normalization, allows us to write the state of a single qubit as

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

with $\theta$ and $\phi$ real numbers. These numbers define a point on the unit three-dimensional sphere, the *Bloch sphere*, shown in Figure 1.1. In this representation, the qubit $|\psi\rangle$ is associated with the point $(\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$. The $Z$ axis corresponds to the *computational basis* $\{|0\rangle, |1\rangle\}$, while the two other axes are associated with the *diagonal basis* $X \equiv \left\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$ and the *circular basis* $Y \equiv \left\{|r\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}, |l\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\right\}$ [5]. Another useful qubit representation is the matrix one, that associates the vectors of the computational basis with

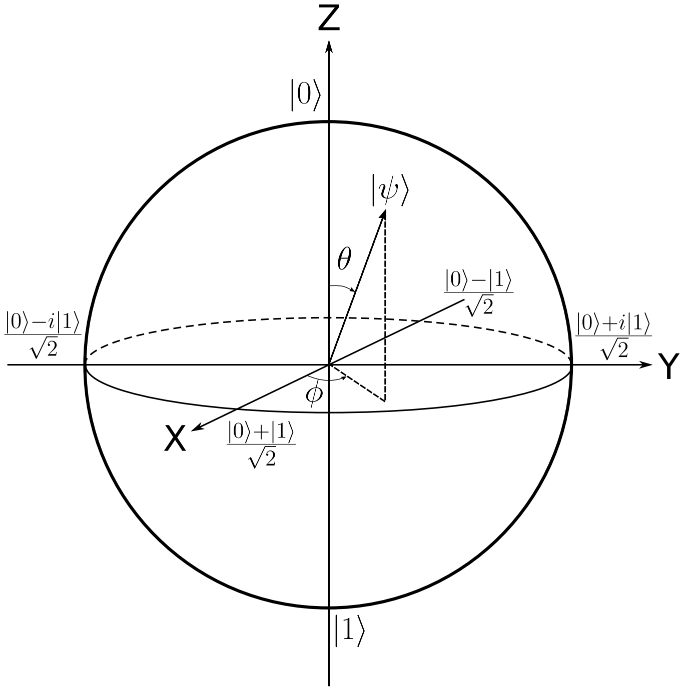
Z
$|0\rangle$
$|\psi\rangle$
$\theta$
$\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
$\frac{|0\rangle-i|1\rangle}{\sqrt{2}}$
$\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$
Y
$\phi$
X
$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
$|1\rangle$

Figure 1.1: Bloch sphere representation of a single qubit.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{1.3}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.4}$$

### 1.2.1 Multiple qubit systems

The difference between classical and quantum information is more marked when dealing with compound systems. Classically, the composition of $n$ systems is described by an $n$-bit string of 0s and 1s (e.g. the composition of 8 bits is described by an 8-bit string called *byte*). In the quantum case, on the other hand, things are slightly more complicated. Postulate 2 says that the state of the compound of two systems lies in the tensor product of Hilbert spaces describing the single systems. Therefore, if the $i$-th qubit lies in $\mathscr{H}_i \approx \mathbb{C}^2$, the state describing the composition of $n$ qubits is described by a vector in

$$\mathscr{H} = \mathscr{H}_1 \otimes \cdots \otimes \mathscr{H}_n \approx \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} \approx \mathbb{C}^{2^n}. \tag{1.5}$$

The state of a 2-qubit system is described by a vector in the space $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2 \approx \mathbb{C}^4$, whose computational basis is $\{|0\rangle \otimes |0\rangle \equiv |00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. The nature of the space $\mathscr{H}$ gives rise to the phenomenon of *entanglement*, since there exist states $|\psi\rangle \in \mathscr{H}$ which cannot be described as the tensor product of a state $|\phi\rangle \in \mathscr{H}_1$ and $|\chi\rangle \in \mathscr{H}_2$. An example is given by the so-called *Bell states*,

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{1.6}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \tag{1.7}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \tag{1.8}$$

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \tag{1.9}$$

which form an alternative basis for the 2-qubit space $\mathscr{H}$ [6, 7]. Like single-qubit systems, multiple-qubit systems can be represented using $2^n$-component complex vectors.

## 1.3 The density matrix formalism

The formalism described in Section 1.1 is useful to describe systems that are in a state that is known exactly, called *pure state*. It can happen, however, that a system is in a statistical ensemble of pure states. In this case, the system is said to be in a *mixed state*. The new formalism, while mathematically equivalent to the former, can be naturally applied to both pure and mixed states [7]

Consider a system that is in one of a number of states $|\psi_i\rangle$, with respective probability $p_i$. The state of the system is represented by the *density operator*

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|. \tag{1.10}$$

A pure state $|\phi\rangle$ is described by $\rho = |\phi\rangle\langle\phi|$. Density operators are characterized by $\rho \geq 0$ and $Tr[\rho] = 1$.

Differently than in the classical case, however, it is not possible to uniquely define the states composing the mixture. For example, the equal mixture of $|0\rangle$ and $|1\rangle$, described by the density operator

$$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{I_2}{2}, \tag{1.11}$$

is not distinguishable from the equal mixture of $|+\rangle$ and $|-\rangle$

$$\rho = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{I_2}{2}. \tag{1.12}$$

The postulates of Section 1.1 can be restated in terms of density operators [4, 7].

**Postulate 1.** *The state of an isolated physical system is described by a density operator, i.e., a positive operator $\rho$ with trace one, acting on a complex Hilbert space $\mathscr{H}$.*

**Postulate 2.** *If a system $A$ is in the state $\rho_A$ and system $B$ is in $\rho_B$, the state of the composite system is $\rho_A \otimes \rho_B$.*

**Postulate 3.** *The evolution of a closed physical system in the interval $[t_0, t_1]$ is described by an unitary operator $U(t_0, t_1)$. A system in the initial state $\rho(t_0)$ evolves into $\rho(t_1) = U(t_0, t_1)\rho(t_0)U(t_0, t_1)^\dagger$. The Schrödinger equation for density operators is*

$$\frac{d}{dt}\rho(t) = -\frac{i}{\hbar}[H, \rho(t)], \tag{1.13}$$

*with $H$ the Hamiltonian of the system.*

**Postulate 5.** *If the state before the measurement is $\rho$, then the probability of observing outcome $x$ is*

$$\mathbb{P}_X(x) = Tr[\Pi_x \rho]. \tag{1.14}$$

*If the outcome of the measurement is $x$, the state $\rho_x$ of the system just after the measurement is*

$$\rho_x = \frac{1}{\mathbb{P}_X(x)} \Pi_x \rho \Pi_x. \tag{1.15}$$

### 1.3.1 Subsystems and purification

The density operator formalism is useful to study the behaviour of the subsystem $A$ of a larger system $AB$. If the system $AB$ is described by the density operator $\rho_{AB}$, its subsystem $A$ can be described using the *reduced density operator* $\rho_A$ defined as

$$\rho_A \equiv Tr_B[\rho_{AB}], \tag{1.16}$$

where $Tr_B$ is the partial trace over system $B$.

Generally, the reduced density operator of an entangled system $AB$ is a mixed state. Moreover, if the system $AB$ is in one of the four Bell states of Equation (1.9), the reduced density matrix of each subsystem is $\rho_A = \frac{I_2}{2}$, thus ruling out the possibility of using entangled states for faster than light communication [3].

On the other hand, given a density operator $\rho_A$ on a system $\mathscr{H}_A$, it is always possible to find a system $\mathscr{H}_E$ such that $\rho_A = Tr_A[\rho_{AE}]$ and the joint system is in a pure state $|\phi\rangle_{AE} \in \mathscr{H}_A \otimes \mathscr{H}_E$. This procedure is called *purification* [3].

### 1.3.2 Generalized measurements

The projective measurement described by Postulate 5 is not the most general kind of measurement that can be performed on a quantum system [8]. In general, it is possible to make the system $\mathscr{H}_A$ interact with another system $\mathscr{H}_B$, the *ancilla*, which is then measured with a projective measurement. The overall system is described by $\mathscr{H}_A \otimes \mathscr{H}_B$, and the interaction is represented by the unitary operator $U$. Before the measurement takes place, the ancilla and the system are independent, so their state can be described by $\rho_A \otimes \rho_B$, and the ancilla can be considered to be in a pure state $\rho_B = |\phi_B\rangle \langle\phi_B|$ (this is always possible by taking a large enough ancilla system because of purification). We can obtain information about the system by measuring the observable $X$ on the ancilla. From Postulate 5, the probability of obtaining $x$ from the measurement is

$$\mathbb{P}_X(x) = Tr_{AB}\left[U\rho_A \otimes \rho_B U^\dagger \left(I \otimes \Pi_x\right)\right]. \tag{1.17}$$

By taking the partial trace over system $B$, it is possible to rewrite (1.17) from the point of view of system $A$, obtaining

$$\mathbb{P}_X(x) = Tr_A\left[\rho_A \Lambda_x\right], \tag{1.18}$$

where $\rho_A$ is the reduced density operator of system $A$ and $\{\Lambda_x\}$ is a set of operators on $\mathscr{H}_A$ such that

- $\Lambda_x$ is self-adjoint,
- $\Lambda_x$ is non-negative,
- $\sum_x \Lambda_x = I$.

A generalized measurement described by such set of operators is called *positive-operator valued measurement* (POVM). It can also be demonstrated that any group of operators meeting these requirements corresponds to a generalized measurement (Neumark/Naimark Theorem [3, 8]). It can therefore be expressed using the formalism of Postulates 4 and 5 with a large enough ancilla system.

## 1.4 The circuit model

The mathematical framework at the basis of digital information processing is Boolean algebra, which can be used to describe all possible functions from $n$-bit into $m$-bit systems. This computational framework can be represented using the *circuit model* [7], which is based on *gates*, that implement logical functions $f : \{0,1\}^n \to \{0,1\}^m$, and *wires*, that connect different gates and provide the circuit with its inputs and outputs. A general gate can be substituted by a network of simpler ones. It has been demonstrated, indeed, that all logical functions can be implemented by using just a finite set of 1-to-1 and 2-to-1 logical gates [7].

A similar information processing model can be introduced also in the quantum case. Similarly to the classical case, the basic computational quantum unit is called *quantum gate*. Postulate 3 restricts quantum gates to unitary operations from $n$-qubit into $n$-qubit systems. Quantum gates are linked together using *wires*, representing an ideal system that transmits a quantum state from one side to the other.

The possibility of entanglement between different qubits, however, makes it impossible to assign a precise value to the state in each wire, requiring a collective description of the state at the different steps of the circuit. While the most general description of quantum circuits should require the use of the density matrix formalism and a more comprehensive model of quantum dynamics to take into account open system evolution (using complete positive trace-preserving linear transformations [5]), it is still possible to apply purification to reduce them to a system of pure-state qubits and unitary quantum gates [9]. In this way, it is possible to study quantum circuits using the formalism introduced in Section 1.1.

### 1.4.1 Quantum wires

The wire is the simplest component of a quantum circuit (this does not mean that it is simple to implement physically, though). It is a system that transfers a qubit from one end to the other one and is used to connect gates or to provide input and output to the circuit. Quantum wires can be used also for the transfer of qutrit states (i.e. states lying in a three-dimensional Hilbert space). As a convention used through this thesis, qubit wires will be single, while qutrit wires will be doubled, as shown in Figure 1.2.

Figure 1.2: Qubit (left) and qutrit (right) wire.

### 1.4.2 Quantum gates

Quantum gates are unitary operations acting on quantum state-vectors [5]. In general, they act on $n$-qubit systems and can be represented, in matrix form, as a $2^n \times 2^n$ matrix. Among all possible quantum gates, however, just a small set of one- and two-qubit gates is necessary to approximate with arbitrary accuracy any possible unitary operation. This set is said to be *universal for quantum computation* [7].

#### Single-qubit gates

Single-qubit gates are represented by $2 \times 2$ unitary matrices in the computational basis. The circuit representation of single-qubit gates is shown in Figure 1.3, with the type of gate is identified by the letter inside the square ($A$ stands for *arbitrary gate*).

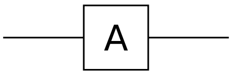

Figure 1.3: An arbitrary single-qubit gate.

An important set of single-qubit gates is represented by *Pauli gates*, whose matrix representation in the computational basis is

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{1.19}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{1.20}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.21}$$

Pauli matrices are strongly related to the Bloch sphere representation by the fact that the point in the sphere associated to a state $|\psi\rangle$ is the one whose coordinates are the expectation values of the Pauli operators $(\langle\psi|\,\sigma_x\,|\psi\rangle\,, \langle\psi|\,\sigma_y\,|\psi\rangle\,, \langle\psi|\,\sigma_z\,|\psi\rangle)$ [5]. In particular, the axes $\{X, Y, Z\}$ of the Bloch sphere correspond to the eigenvectors of the Pauli gates $\{\sigma_x, \sigma_y, \sigma_z\}$.

Another useful gate is the *Hadamard gate*, described by the matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{1.22}$$

that transforms the computational basis $\{|0\rangle\,, |1\rangle\}$ into the diagonal one $\{|+\rangle\,, |-\rangle\}$ and vice-versa.

The *rotation gates*, that rotate the qubit about one axis of the Bloch sphere by an angle $\theta$, are described by

$$R_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{1.23}$$

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{1.24}$$

$$R_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}. \tag{1.25}$$

The rotation about the $z$ axis shifts the qubit phase of an angle $\theta$ and can be used to construct the *phase gate*

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{1.26}$$

and the *"$\frac{\pi}{8}$" gate*

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}. \tag{1.27}$$

### Two-qubit gates

The most important class of two-qubit gates is the one of *controlled operations*, shown in Figure 1.4.

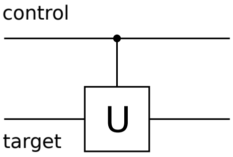

Figure 1.4: Controlled-U operation. The unitary $U$ is applied to the target qubit only if the control qubit is in $|1\rangle$.

They have two inputs, the *target* and the *control* bit, and perform the unitary operation $U$ on the target qubit only if the control is in state $|1\rangle$. An important controlled gate is the *CNOT gate*, with matrix

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{1.28}$$

in the two-qubit computational basis. The set formed by single-qubit gates and the CNOT gate is universal for quantum computation [7].

Another important controlled gate, that will be used later in this thesis, is the *controlled-phase-shift gate*, that implements a rotation of the target qubit around the $z$ axis of the Bloch sphere conditioned on the value of the control qubit. This operation is described by the matrix

$$CP(\epsilon) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\epsilon} & 0 \\ 0 & 0 & 0 & e^{-i\epsilon} \end{pmatrix}. \tag{1.29}$$

### 1.4.3 Measurement

In general, the only way to get information about a physical system is through measurements. While the most general description of a measurement on a system is given by a POVM, the Neumark/Naimark Theorem allows us to see it as a projective measurement on an ancilla subsystem. Moreover, projective measurements on an arbitrary basis are equivalent to a unitary transformation followed by a projective measurement on the computational basis.

In the circuit model, a measurement in the computational basis is represented as in Figure 1.5.

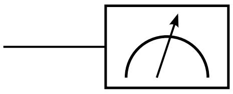

Figure 1.5: Projective measurement in the computational basis.

## 1.5 Photonic implementation of Quantum Information

As stated in previous Sections, quantum information requires information carriers to follow the rules of quantum mechanics. However, there are many different systems fulfilling this requirement, with their peculiar characteristics and their own physical laws.

The transmission of information requires information carriers that can propagate through long distances without being altered by the environment they propagate within. The most suitable physical system for such task is the electromagnetic field, both in the classical and in the quantum case. Indeed, electromagnetic waves can travel for long distances both in vacuum and in transparent media, such as the air or the glass. Moreover, its low interaction with matter makes it very resistant to the noise introduced by its coupling with the environment.

Electrodynamics is the branch of physics that studies the interaction of charges and currents. These interactions are mediated by the electromagnetic field, whose behaviour is described by Maxwell's equations (1865). These equations predict, in absence of both charges and currents, that the electromagnetic field propagates as a wave at the speed of light $c \simeq 3 \cdot 10^8\,\text{m/s}$. This fact, in apparent contradiction with Galilean relativity, led to the development, by Einstein, of special and general relativity, in the first decade of the 20th century. These theories are all built upon the classical mechanics framework.

Electrodynamics played a crucial role also in the development of quantum mechanics, which started as an attempt to justify a discrepancy between the theory and the experiment in the study of black body radiation. The first adaptation of existing physical theories to the new framework was based on the transformation of classical observables into operators, a procedure called *first quantization.* While this process was adequate for the description of non-relativistic systems with a fixed number of particles, it proved inadequate to describe relativistic systems, where the particle description must be substituted with a field description.

A new procedure for the quantization of field theories, called *second quantization*, was then developed, and this is the basis for the construction of quantum electrodynamics.

The study of quantum electrodynamics, even in its description of the free electromagnetic field, is far beyond the scope of this thesis. This Section will just give a very short introduction to the matter, limited to some results of interest for the photonic implementation of quantum information protocols. The quantization of the electromagnetic field is the subject of many books [6, 10–13]. In order to keep this Section as short as possible, it will mainly based on the book by Kok and Lovett [6]. A similar formalism, however, can also be found in the *Effective Quantum Optics* book by Leonhardt [11].

### 1.5.1 Quantum theory of the electromagnetic field

**Classical theory**

The electromagnetic field is the combination of the electric field $\mathbf{E}(\mathbf{r},t)$ and the magnetic field $\mathbf{B}(\mathbf{r},t)$, whose generation and propagation is governed by Maxwell's equations. An alternative description of classical electrodynamics uses, instead of the field, the scalar potential $\Phi(\mathbf{r},t)$ and the vector potential $\mathbf{A}(\mathbf{r},t)$, linked to the electromagnetic field by the equations

$$\mathbf{E}(\mathbf{r},t) = -\nabla\Phi(\mathbf{r},t) + \frac{\partial\mathbf{A}(\mathbf{r},t)}{\partial t}, \tag{1.30}$$

$$\mathbf{B}(\mathbf{r},t) = \nabla\times\mathbf{A}(\mathbf{r},t). \tag{1.31}$$

Since the observables are the fields and not the potentials, different potentials giving the same electric fields must be treated as equivalent. This freedom, called *gauge freedom*, allows to fix some constraints for the potentials. In the theory of radiation, it is convenient to adopt the so-called Coulomb gauge, defined by

$$\nabla\cdot\mathbf{A} = 0, \text{ and } \Phi = 0. \tag{1.32}$$

With this choice, the equation governing the free electromagnetic field (i.e. the regime with no free charges and currents) is

$$\nabla^2\mathbf{A} - \varepsilon_0\mu_0\frac{\partial^2\mathbf{A}}{\partial t^2} = 0. \tag{1.33}$$

The classical solution to this equation can be written as

$$\mathbf{A}(\mathbf{r},t) = \sum_\lambda\int\frac{d\mathbf{k}}{\sqrt{\varepsilon_0}}\frac{A_\lambda(\mathbf{k})\epsilon_\lambda(\mathbf{k})e^{i\mathbf{k}\cdot\mathbf{r}-i\omega_\mathbf{k}t}}{\sqrt{(2\pi)^3 2\omega_\mathbf{k}}} + c.c. \tag{1.34}$$

$$= \sum_\lambda\int\frac{d\mathbf{k}}{\sqrt{\varepsilon_0}}A_\lambda(\mathbf{k})\epsilon_\lambda(\mathbf{k})u(\mathbf{k};\mathbf{r},t) + c.c. \tag{1.35}$$

where $A_\lambda(\mathbf{k})$ denotes the amplitude of the mode with wave vector $\mathbf{k}$ and polarization $\lambda$, $\epsilon_\lambda$ gives the direction of the polarization and *c.c.* denotes the complex conjugate. The dispersion relation for the free field is given by

$$|\mathbf{k}|^2 - \varepsilon_0\mu_0\omega_\mathbf{k}^2 \equiv k^2 - \frac{\omega_\mathbf{k}^2}{c^2} = 0, \tag{1.36}$$

where $c = \frac{1}{\sqrt{\varepsilon_0\mu_0}}$ is the speed of light in vacuum. In this form, the vector potential is written in the plane wave basis, described by mode functions

$$u(\mathbf{k};\mathbf{r},t) = \frac{A_\lambda(\mathbf{k})\epsilon_\lambda(\mathbf{k})e^{i\mathbf{k}\cdot\mathbf{r}-i\omega_\mathbf{k}t}}{\sqrt{(2\pi)^3 2\omega_\mathbf{k}}}. \tag{1.37}$$

The energy density of the free field is given by the Hamiltonian density

$$\mathcal{H}(\mathbf{r},t) = \frac{\varepsilon_0}{2}|\mathbf{E}(\mathbf{r},t)|^2 + \frac{1}{2\mu_0}|\mathbf{B}(\mathbf{r},t)|^2 = \sum_\lambda\int d\mathbf{k}\omega_\mathbf{k}|A_\lambda(\mathbf{k})|^2. \tag{1.38}$$

### Quantization of the free electromagnetic field

Quantization is a technique used to transform a classical theory into a theory compatible with the quantum mechanics framework. Classical field theories, like electrodynamics, are quantized within the *second quantization* framework, that consists of transforming the fields into quantum operators obeying a commutation relation compatible with the Heisenberg uncertainty principle. By applying this procedure to the electromagnetic field in Equation (1.35), the field is transformed into the field operator

$$\hat{\mathbf{A}}(\mathbf{r},t) = \sum_{\lambda} \int d\mathbf{k} \sqrt{\frac{\hbar}{\varepsilon_0}} \left[ \hat{a}_{\lambda}(\mathbf{k}) \epsilon_{\lambda}(\mathbf{k}) u(\mathbf{k};\mathbf{r},t) + \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) \epsilon^{*}_{\lambda}(\mathbf{k}) u^{*}(\mathbf{k};\mathbf{r},t) \right], \tag{1.39}$$

where the amplitude $A_{\lambda}(\mathbf{k})$ has been promoted to the field operator $\hat{a}_{\lambda}(\mathbf{k})$, obeying the commutation relation

$$\left[ \hat{a}_{\lambda}(\mathbf{k}), \hat{a}^{\dagger}_{\lambda'}(\mathbf{k}') \right] = \delta_{\lambda\lambda'} \delta^{3}(\mathbf{k}-\mathbf{k}'), \tag{1.40}$$

and

$$\left[ \hat{a}_{\lambda}(\mathbf{k}), \hat{a}_{\lambda'}(\mathbf{k}') \right] = \left[ \hat{a}^{\dagger}_{\lambda}(\mathbf{k}), \hat{a}^{\dagger}_{\lambda'}(\mathbf{k}') \right] = 0. \tag{1.41}$$

Consequently, the Hamiltonian density of Equation (1.38) is transformed into the operator

$$\hat{\mathscr{H}}(\mathbf{r},t) = \sum_{\lambda} \int d\mathbf{k} \frac{\hbar\omega_{\mathbf{k}}}{2} \left[ \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) \hat{a}_{\lambda}(\mathbf{k}) + \hat{a}_{\lambda}(\mathbf{k}) \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) \right] \tag{1.42}$$

$$= \sum_{\lambda} \int d\mathbf{k} \hbar\omega_{\mathbf{k}} \left[ \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) \hat{a}_{\lambda}(\mathbf{k}) + \frac{1}{2} \right] = \sum_{\lambda} \int d\mathbf{k} \hbar\omega_{\mathbf{k}} \left[ \hat{n}_{\lambda}(\mathbf{k}) + \frac{1}{2} \right], \tag{1.43}$$

where the first equality is obtained by inserting the commutation relation (1.40), and the second one is expressed using the number operator for the mode with wave vector $\mathbf{k}$ and polarization $\lambda$ defined as

$$\hat{n}_{\lambda}(\mathbf{k}) = \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) \hat{a}_{\lambda}(\mathbf{k}). \tag{1.44}$$

The number operator is the quantum mechanical analogous of the mode intensity $|A_{\lambda}(\mathbf{k})|^2$. The main difference lies in the fact that, in quantum electrodynamics, the intensity of a mode of the electromagnetic field is quantized. The quanta of intensity of a mode of the field are called *photons* of that mode. A general state of the electromagnetic field can be expressed by counting the photons present in each mode of the electromagnetic field, using the so-called *Fock representation.*

Another crucial difference between classical and quantum electrodynamics is given by the $\frac{1}{2}$ term in Equation (1.43). This term, summed over all mode vectors and polarizations, gives an infinite term to the Hamiltonian density operator, usually called the *vacuum energy.* For most applications, where the crucial aspect is the energy difference between two states, the vacuum energy cancels out and can therefore be neglected.

The field operators $\hat{a}_{\lambda}(\mathbf{k})$ and $\hat{a}^{\dagger}_{\lambda}(\mathbf{k})$ are called *creation* and *annihilation* operators, respectively. Indeed, by applying them to an eigenstate of the number operator $|n_{\mathbf{k}\lambda}\rangle$ of eigenvalue $n_{\mathbf{k}\lambda}$, we obtain

$$\hat{n}_{\lambda}(\mathbf{k}) \hat{a}_{\lambda}(\mathbf{k}) |n_{\mathbf{k}\lambda}\rangle = \hat{a}_{\lambda}(\mathbf{k}) \left( \hat{n}_{\lambda}(\mathbf{k}) - 1 \right) |n_{\mathbf{k}\lambda}\rangle = (n_{\mathbf{k}\lambda} - 1) \hat{a}_{\lambda}(\mathbf{k}) |n_{\mathbf{k}\lambda}\rangle, \text{ and} \tag{1.45}$$

$$\hat{n}_{\lambda}(\mathbf{k}) \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) |n_{\mathbf{k}\lambda}\rangle = \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) \left( \hat{n}_{\lambda}(\mathbf{k}) + 1 \right) |n_{\mathbf{k}\lambda}\rangle = (n_{\mathbf{k}\lambda} + 1) \hat{a}^{\dagger}_{\lambda}(\mathbf{k}) |n_{\mathbf{k}\lambda}\rangle. \tag{1.46}$$

These operators, therefore, can be used to create a photon in mode $(\mathbf{k}, \lambda)$ or to destroy it.

### Physical mode functions

Despite being useful for the quantization of the free electromagnetic field, plane waves are unphysical solutions. To obtain physical states, it is necessary to construct an appropriate superposition of plane waves

$$f(\mathbf{r},t) = \int d\mathbf{k} \left[\alpha^*(\mathbf{k})u(\mathbf{k};\mathbf{r},t) + \beta^*(\mathbf{k})u^*(\mathbf{k};\mathbf{r},t)\right], \tag{1.47}$$

which, if its polarization is $\lambda$, is associated with mode operator

$$\hat{b}_{f\lambda} = \sqrt{\frac{\varepsilon_0}{\hbar}} \left(\epsilon_\lambda f, \hat{\mathbf{A}}\right) = \int d\mathbf{k} \left[\alpha(\mathbf{k})\hat{a}_\lambda(\mathbf{k}) + \beta(\mathbf{k})\hat{a}^\dagger_\lambda(\mathbf{k})\right], \tag{1.48}$$

where $(\cdot,\cdot)$ is the time-independent scalar product

$$(\phi,\psi) \equiv i \int d\mathbf{r} \left[\phi^* \left(\partial_t \psi\right) - \left(\partial_t \phi^*\right) \psi\right]. \tag{1.49}$$

Usually, $f$ is chosen to belong to an orthonormal set of normal modes $\{f_j\}_{j\in\mathbb{N}}$. In this case, mode operators can be demonstrated to obey the commutation relations

$$\left[\hat{b}_{j\lambda}, \hat{b}^\dagger_{k\lambda'}\right] = \delta_{\lambda\lambda'}\delta_{jk}, \text{ and } \left[\hat{b}_{j\lambda}, \hat{b}_{k\lambda'}\right] = \left[\hat{b}^\dagger_{j\lambda}, \hat{b}^\dagger_{k\lambda'}\right] = 0. \tag{1.50}$$

These mode operators create or destroy a photon with spatial mode $f_j$ and polarization mode $\epsilon_\lambda$.

### Evolution of field operators

Postulate 3 describes the dynamics of a closed system, so it can be applied also to the evolution of the free electromagnetic field. The main objects encountered in the quantum theory of the free electromagnetic fields, however, are field operators. It is therefore more convenient to see the states as fixed and the let the operators evolve, the so-called *Heisenberg picture*. The dynamics equation for quantum operators, called Heisenberg equation of motion, is

$$\frac{d\hat{A}(t)}{dt} = \frac{i}{\hbar}\left[\hat{H}(t), \hat{A}(t)\right] + \frac{\partial \hat{A}}{\partial t}, \tag{1.51}$$

where $\hat{H}$ is the Hamiltonian operator, defined as

$$\hat{H}(t) = \int d^3\mathbf{r}\mathcal{H}(\mathbf{r},t). \tag{1.52}$$

For the field operators, Equation (1.51) becomes

$$\frac{d\hat{a}_{j\lambda}(t)}{dt} = \frac{i}{\hbar}\left[\hat{H}(t), \hat{a}_{j\lambda}(t)\right], \tag{1.53}$$

$$\frac{d\hat{a}^\dagger_{j\lambda}(t)}{dt} = \frac{i}{\hbar}\left[\hat{H}(t), \hat{a}^\dagger_{j\lambda}(t)\right]. \tag{1.54}$$

If mode functions are sharply peaked around the central wave vector $\mathbf{k}_j$, and the time evolution is governed by the free-field Hamiltonian $\hat{\mathcal{H}}_{j\lambda} = \hbar\omega_\mathbf{k}\hat{a}^\dagger_{j\lambda}\hat{a}_{j\lambda}$, the solutions to these equations is given by

$$\hat{a}_{j\lambda}(t) = \hat{a}_{j\lambda}e^{-i\omega_j t}, \tag{1.55}$$

$$\hat{a}^{\dagger}_{j\lambda}(t) = \hat{a}^{\dagger}_{j\lambda} e^{i\omega_j t}. \tag{1.56}$$

Since most optical setups are stationary, it is convenient to remove the explicit time dependency on the field operators and only consider the phase $\phi$ introduced in a certain part of the setup.

The evolution induced by a general optical element depends on its Hamiltonian. If the Hamiltonian operator has the form

$$\hat{\mathcal{H}} = \sum_{jk,\lambda\lambda'} A_{jk,\lambda\lambda'} \hat{a}^{\dagger}_{j\lambda} \hat{a}_{k\lambda'}, \tag{1.57}$$

the evolution preserves the number of photons and it is said to be *linear* [14]. Linear evolution mixes input and output modes, and can be described in matrix form as

$$\vec{b} = S\vec{a}, \tag{1.58}$$

where $\vec{a} = \left(\hat{a}_{j_1\lambda_1}, \hat{a}_{j_2\lambda_2}, \dots\right)$ and $\vec{b} = \left(\hat{b}_{k_1\lambda_1}, \hat{b}_{k_2\lambda_2}, \dots\right)$ are the vectors containing the modes entering and exiting the optical element and $S$ is a unitary matrix describing the evolution, called the *scattering matrix* [15].

### 1.5.2 Photons as information carriers

There exist many different ways to encode the information into the degrees of freedom of the electromagnetic field. They are grouped into two different classes, called *continuous variables* and *discrete variables.*

Continuous variables encode the information in the quadratures of a single mode $(j, \lambda)$ of the electromagnetic field (quadratures are, roughly speaking, the real and the imaginary part of the field operator). While continuous variables play an important role in quantum information [16], they are out of the scope of this thesis.

The other way to encode quantum information is using discrete variables. In this case, the information is encoded into the degrees of freedom of a single photon. The most common encoding scheme implements a qubit using a single photon in two orthogonal modes of the electromagnetic field, a technique called *dual-rail encoding.* The orthogonal modes can be two orthogonal polarizations, two non-overlapping transverse modes or two non-overlapping temporal modes, giving, respectively, *polarization*, *path* or *time-bin* encoding. In this Section, these encoding schemes will be rapidly reviewed.

There exists another important scheme, that uses orthogonal transverse modes of the field and is called *orbital angular momentum* (*OAM*) encoding. Since it will not be used in this thesis, this encoding scheme will not be treated in this Section.

#### Polarization encoding

Polarization is related to the vector behavior of the electric field $\mathbf{E}$ (and, by extension, of the vector potential $\mathbf{A}$, since the time derivative in Equation (1.30) does not change the vector behaviour of the field). The vector character of the field is captured by vector $\epsilon_\lambda$. The Coulomb gauge condition $\nabla \cdot \mathbf{A} = 0$ restricts the polarization vector to the plane

$$\epsilon_\lambda(\mathbf{k}) \cdot \mathbf{k} = 0. \tag{1.59}$$

Therefore, polarization is restricted to the bi-dimensional plane perpendicular to the wave vector $\mathbf{k}$.

Polarization encoding represents a qubit in the two-dimensional complex Hilbert space of a single-mode field[1]. The computational basis is often chosen to be $\{\epsilon_H, \epsilon_V\}$, where the spatial mode index has been omitted for simplicity. The correspondence between field modes and field operators makes it possible to write the computational basis states as

$$|0\rangle := \hat{a}_H^\dagger |0,0\rangle_{HV} = |1,0\rangle_{HV} = |H\rangle , \tag{1.60}$$

$$|1\rangle := \hat{a}_V^\dagger |0,0\rangle_{HV} = |0,1\rangle_{HV} = |V\rangle , \tag{1.61}$$

where $|n_H, n_V\rangle_{HV}$ is the Fock state representation of the polarization of a single-mode field.

Single-qubit gates are easy to implement in the polarization encoding by using wave-plates. Wave-plates are optical devices made of a birefringent material, characterized by a different refractive index for two orthogonal axes. The material used in most wave-plates is quartz, which is a positive uniaxial crystal ($n_e > n_o$) [17]. The axis characterized by the lower refraction index is called *fast axis* ($n_{slow} > n_{fast}$ because $v = c/n$), therefore quartz wave-plates have $n_{fast} = n_o$ and $n_{slow} = n_e$. In the basis $\{|F\rangle, |S\rangle\}$ of the fast and slow axes, the scattering matrix is

$$\Lambda(\Gamma) = \begin{pmatrix} e^{i\frac{2\pi}{\lambda}n_{fast}d} & 0 \\ 0 & e^{i\frac{2\pi}{\lambda}n_{slow}d} \end{pmatrix} = e^{i\frac{2\pi}{\lambda}n_{fast}} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{\lambda}(n_{slow}-n_{fast})d} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Gamma} \end{pmatrix} , \tag{1.62}$$

with $\Gamma = \frac{2\pi}{\lambda}\delta nd$ the relative phase introduced by the plate. The two common types of wave-plates are the *half wave-plate*, characterized by $\delta nd = \frac{\lambda}{2} + m\lambda$ and $\Gamma = \pi + 2\pi m$, and the *quarter wave-plate*, with $\delta nd = \frac{\lambda}{4} + m\lambda$ and $\Gamma = \frac{\pi}{2} + 2\pi m$. The value of $m$ gives the order of the plate (*zero-order* plates have $m = 0$). The resulting scattering matrices are

$$\Lambda_{HWP} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \Lambda_{QWP} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} . \tag{1.63}$$

In general, wave-plates are mounted on rotator stages, so that the slow and fast axis form an angle $\epsilon$ with the computational basis axis, as shown in Figure 1.6.

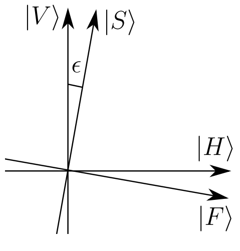

Figure 1.6: Relationship between the $\{|F\rangle, |S\rangle\}$ and the computational basis $\{|H\rangle, |V\rangle\}$. The laser beam is coming out of the page.

Since the rotation is described by

$$\begin{pmatrix} \hat{a}_F \\ \hat{a}_S \end{pmatrix} = \begin{pmatrix} \cos\epsilon & -\sin\epsilon \\ \sin\epsilon & \cos\epsilon \end{pmatrix} \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix} = R_y(2\epsilon) \begin{pmatrix} \hat{a}_H \\ \hat{a}_V \end{pmatrix} , \tag{1.64}$$

[1] The most frequently spatial mode used for polarization encoding is the $TEM_{00}$ mode, which can be well approximated to a plane wave in the condition of not too strong focusing.

the resulting rotated wave-plate scattering matrix is

$$\Lambda(\Gamma,\epsilon) = R_y^{-1}(2\epsilon)\Lambda(\Gamma)R_y(2\epsilon) = \begin{pmatrix} \cos^2\epsilon + e^{i\Gamma}\sin^2\epsilon & \cos\epsilon\sin\epsilon\left(1-e^{i\Gamma}\right) \\ \cos\epsilon\sin\epsilon\left(1-e^{i\Gamma}\right) & e^{i\Gamma}\cos^2\epsilon + \sin^2\epsilon \end{pmatrix}. \tag{1.65}$$

The general form of the rotated half-wave plate and quarter-wave plate is given by

$$\Lambda_{HWP}(\epsilon) = \begin{pmatrix} \cos^2\epsilon - \sin^2\epsilon & 2\cos\epsilon\sin\epsilon \\ 2\cos\epsilon\sin\epsilon & \sin^2\epsilon - \cos^2\epsilon \end{pmatrix} = \begin{pmatrix} \cos 2\epsilon & \sin 2\epsilon \\ \sin 2\epsilon & -\cos 2\epsilon \end{pmatrix}, \text{ and} \tag{1.66}$$

$$\Lambda_{QWP}(\epsilon) = \begin{pmatrix} \cos^2\epsilon + i\sin^2\epsilon & \cos\epsilon\sin\epsilon\,(1-i) \\ \cos\epsilon\sin\epsilon\,(1-i) & \sin^2\epsilon + i\cos^2\epsilon \end{pmatrix}. \tag{1.67}$$

Half- and quarter-wave plates can also be used to implement a generic $R_z$ rotation. This can be obtained by rotating the wave-plate along its vertical axis of an angle $\theta$, as shown in Figure 1.7. The scattering matrix of this system is

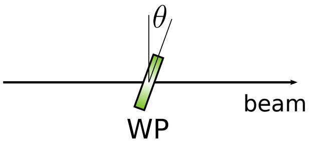

Figure 1.7: Wave plate used as phase shifter.

$$\Lambda_{HWP}(\theta) \simeq \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{\cos\theta}} \end{pmatrix} \tag{1.68}$$

for the half-wave plate and

$$\Lambda_{QWP}(\theta) \simeq \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2\cos\theta}} \end{pmatrix} \tag{1.69}$$

for the quarter-wave plate.

### Path encoding

In path encoding, the computational basis is composed by two non-overlapping spatial modes. The modes are usually described by the same mode function (usually $TEM_{00}$), with approximate wave-vectors $\mathbf{k}_1$ and $\mathbf{k}_2$, characterized by the same wavelength but different direction. The field operators for such modes are $\hat{a}_{\mathbf{k}_1\lambda}$ and $\hat{a}_{\mathbf{k}_2\lambda}$, where $\lambda$ is the polarization mode. In order to preserve coherence, it is important that the two field operators have the same polarization mode, otherwise the trace over the polarization space will produce a mixture of the two modes[2]. The computational basis states of path encoding are

$$|0\rangle := \hat{a}^\dagger_{\mathbf{k}_1}|0,0\rangle_{\mathbf{k}_1\mathbf{k}_2} = |1,0\rangle_{\mathbf{k}_1\mathbf{k}_2}, \text{ and } |1\rangle := \hat{a}^\dagger_{\mathbf{k}_2}|0,0\rangle_{\mathbf{k}_1\mathbf{k}_2} = |0,1\rangle_{\mathbf{k}_1\mathbf{k}_2}, \tag{1.70}$$

where $|n_{\mathbf{k}_1}, n_{\mathbf{k}_2}\rangle_{\mathbf{k}_1\mathbf{k}_2}$ is the Fock state representation of the two spatial modes, with the polarization degree of freedom neglected for simplicity.

[2] Since most optical elements produce a coherent superposition of $\hat{a}_{\mathbf{k}_1\lambda}$ and $\hat{a}_{\mathbf{k}_1\lambda'}$, it is sufficient to filter polarization before detection.

Single-qubit operations in path encoding use beam-splitters and phase retarders. Beam-splitters are partially reflecting devices, used to mix two spatial modes creating interference effects. It is usually used with two incoming and two outgoing modes, as shown in Figure 1.8.

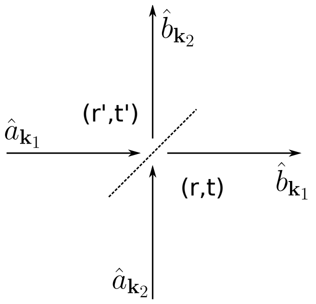

Figure 1.8: Quantum mechanical description of the beam-splitter. For simplicity, input modes are marked with $\hat{a}$ and output modes with $\hat{b}$.

The mode transformation introduced by the beam-splitter is

$$\begin{pmatrix} \hat{b}_{\mathbf{k}_1} \\ \hat{b}_{\mathbf{k}_2} \end{pmatrix} = \begin{pmatrix} t' & r \\ r' & t \end{pmatrix} \begin{pmatrix} \hat{a}_{\mathbf{k}_1} \\ \hat{a}_{\mathbf{k}_2} \end{pmatrix}, \tag{1.71}$$

where input modes are marked with field operators $\hat{a}_j$ and output modes with $\hat{b}_j$, with $j$ the approximate wave vector of the two spatial modes. Since the scattering matrix must be unitary, $(r,t)$ and $(r',t')$ must satisfy $|r'| = |r|$, $|t'| = |t|$, $|r|^2 + |t|^2 = 1$, $r^*t' + r't^* = 0$, and $r^*t' + r't'^* = 0$ [18]. The 50:50 beam-splitter has $r = r' = \frac{i}{\sqrt{2}}$ and $t = t' = \frac{1}{\sqrt{2}}$, therefore it is described by the scattering matrix

$$U_{BS} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{1.72}$$

The phase retarder simply consists of a different propagation length of one spatial mode with respect to the other one. The path difference between the two modes, however, must be shorter than the coherence length of the two modes, to keep the temporal overlap between the single-photon wave-packets in the two modes. It is described by the scattering matrix

$$U_{phase}(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}. \tag{1.73}$$

### Time-bin encoding

Until now, we have neglected the temporal modes of the electromagnetic field. Single-wavelength photons are completely unlocalized, and their coherence length in infinite. This approximation is equivalent to the plane wave approximation for spatial modes, but does not describe the behaviour of real photons, which are more or less localized[3]. It is possible to define the continuous frequency creation and annihilation operators of mode $i$ by $\hat{a}_i(\omega)$ and $\hat{a}_i^\dagger(\omega)$, where $i$ is an index for both the spatial and the polarization mode [15].

[3] The meaning of photon localization is a debated problem. Here, the term "localized photon" is used to indicate the excitation of a temporally localized mode of the electromagnetic field, equivalent to the one described by a laser pulse.

The dependence on $\mathbf{k}$ of the pulsation $\omega$ has been omitted, because we are dealing with modes with the same spatial pattern, differing only in their frequency. The commutation relation between these operators is

$$\left[\hat{a}_i(\omega), \hat{a}_j^\dagger(\omega')\right] = \delta_{ij}\delta(\omega - \omega'). \tag{1.74}$$

These operators are the temporal equivalent of plane wave operators for spatial modes. The creation operator of a photon in a pulse about time $t_0$ is given by the *photon wave-packet creation operator*

$$\hat{a}_{i,t_0}^\dagger = \int d\omega \xi(\omega; t_0)\hat{a}_i^\dagger(\omega), \tag{1.75}$$

where the function $\xi(\omega; t_0)$ is the pulse shape. In the case of two Gaussian pulses, with shape

$$\xi(\omega; t_i) = \frac{1}{(2\pi\Delta^2)^{1/4}} \exp\left[i\left(\omega - \omega_0\right)t_i - \frac{(\omega - \omega_0)^2}{4\Delta^2}\right] \tag{1.76}$$

of central frequency $\omega_0$ and bandwidth $\Delta$, centered on $t_0$ and $t_1$, the commutation relation of the respective wave-packet operators is

$$\left[a_{i,t_0}, a_{j,t_1}^\dagger\right] = \delta_{ij} \exp\left(-\frac{\Delta^2(t_1 - t_0)^2}{2}\right). \tag{1.77}$$

It the time separation between the two wave-packet is much larger than their temporal width, that is

$$t_1 - t_0 \gg \frac{1}{\Delta}, \tag{1.78}$$

the two pulses can be considered as independent and can be used as orthonormal modes for the encoding of quantum information.

The computational basis for time-bin encoded photons is

$$|0\rangle := \hat{a}_{t_0}^\dagger \left|0, 0\right\rangle_{t_0,t_1} = \left|1, 0\right\rangle_{t_0,t_1}, \text{ and } |1\rangle := \hat{a}_{t_1}^\dagger \left|0, 0\right\rangle_{t_0,t_1} = \left|0, 1\right\rangle_{t_0,t_1}, \tag{1.79}$$

where $\left|n_{t_0}, n_{t_1}\right\rangle_{t_0,t_1}$ is the Fock state representation of the two time-bin modes, with the both the spatial and the polarization degree of freedom neglected.

Single-qubit gates of time-bin photons cannot be implemented using passive linear optical devices, but require active devices or interferometric setups. Despite that, the resistance of time-bin modes to long distance propagation over optical fiber, together with the existence of fast optical modulating devices, has made time-bin encoding the preferred choice for many quantum information protocols, among which Quantum Key Distribution. The first commercial implementations of QKD use this kind of encoding.

### Filters

In the previous Sections, we treated only the degree of freedom used for encoding, neglecting all the other ones. Generally, this is not true, since that degree of freedom may be entangled with the others. In that case, the coherence in the encoding degree of freedom is, at least partially, destroyed, producing a mixed state. The usual solution to this problem is by filtering all the other degrees of freedom.

The filtering process is analogous to a projective measurement, with two possible outcomes, “fail” or “success”. In the “fail” case, the photon is discarded, while in the “success” case it goes on through the experimental setup. If the system used to encode a qubit is prepared in state $\rho$, and it is filtered $N$ times, with filtering operators $\left\{\Pi_F^{(i)}, \Pi_{NF}^{(i)}\right\}_{i\in 1..N}$, where $\Pi_F^{(i)}$ is the projector onto the filtered subspace and $\Pi_{NF}^{(i)} = I - \Pi_F^{(i)}$, the probability of getting a filtered qubit is

$$p_F = Tr\left[\Pi_F^{(1)} \cdots \Pi_F^{(N)} \rho\right], \tag{1.80}$$

with the filtered state given by

$$\rho_F = \frac{1}{p_F} \Pi_F^{(1)} \cdots \Pi_F^{(N)} \rho \Pi_F^{(1)} \cdots \Pi_F^{(N)}. \tag{1.81}$$

Filtering has a serious impact on the experimental preparation of a photonic experiment. Indeed, if a photonic setup produces single photons with a rate of $R$ photons per second, the rate of filtered qubits is just $p_F R$. On the other hand, not filtering a photonic state can lead to qubits in a non-pure state, preventing the execution of the desired quantum information protocol. The trade-off between rate and pure qubit implementation is therefore crucial for photonic quantum information.

### Measurement

In the generalized measurement scheme described in Section 1.3.2, the system is entangled with an ancilla system that is subsequently measured projectively. This scheme respects what generally happens in photonic experiments. Indeed, photonic measurements are usually performed with detectors which produce a detection event if a photon strikes its sensitive area.

The two kinds of detectors used throughout this thesis are *avalanche photo-diodes* (APD) and *photo-multipliers* (PMT). Their working mechanism is similar: when a photon hits the sensitive area, it produces an electron, whose effect is to produce an electron avalanche that is measurable by standard electronics. The technology behind these two kinds of detector, however, is different. In photo-multipliers, the sensitive area consists of a photocathode, which, when hit by an incoming photon, produces an electron into a vacuum tube, where it is accelerated by an electric field onto a cascade of metallic plates, called dynodes, where the number of electrons is multiplied, in order to produce, at the end of the cascade, a detectable electric signal. Avalanche photo-diodes, on the other hand, are solid state devices operated with a reverse voltage above their breakdown voltage, so that a photon hitting the device and producing an electron by photoelectric effect produces an electron avalanche that is detectable by the downstream electronics.

Both kinds of device are characterized by a detection efficiency $\eta$, given by the probability of the photoelectric effect, and a dark count probability $D(k)$, measuring the probability that, in a certain time interval, $k$ detection events are triggered by a thermally produced electron. The resulting detector POVM is

$$\hat{E}^{(noclick)} = D(0) \sum_{m=0}^{\infty} (1-\eta)^m |m\rangle \langle m|, \tag{1.82}$$

$$\hat{E}^{(click)} = I - \hat{E}^{(noclick)} = \sum_{m=0}^{\infty} \left[1 - D(0)(1-\eta)^m\right] |m\rangle \langle m|, \tag{1.83}$$

where $|m\rangle$ is the Fock state with $m$ photons in the spatial mode hitting the sensitive area[4]. This simplified model neglects the time resolution of the detection event and assumes a

[4] We are considering transverse spatial modes smaller than the sensitive area of the detector and a uniform detection efficiency over the whole sensitive area.

flat spectral response of the detector at the wavelengths of the incoming photons.

Incorporated into the circuit model of Section 1.4, these detectors perform projective measurements over qubits encoded in the path degree of freedom. In order to use them for the measurement of qubits in other degrees of freedom it is therefore necessary to entangle them with path qubits, that are subsequently measured. Polarization encoding can be easily entangled with path encoding by using a *polarizing beam-splitter* (PBS), shown in Figure 1.9. The mode transformation induced by the PBS is

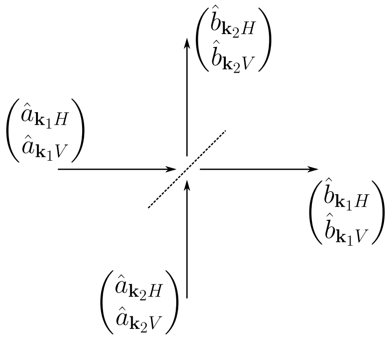
$\begin{pmatrix}\hat{b}_{\mathbf{k}_2H}\\ \hat{b}_{\mathbf{k}_2V}\end{pmatrix}$
$\begin{pmatrix}\hat{a}_{\mathbf{k}_1H}\\ \hat{a}_{\mathbf{k}_1V}\end{pmatrix}$
$\begin{pmatrix}\hat{b}_{\mathbf{k}_1H}\\ \hat{b}_{\mathbf{k}_1V}\end{pmatrix}$
$\begin{pmatrix}\hat{a}_{\mathbf{k}_2H}\\ \hat{a}_{\mathbf{k}_2V}\end{pmatrix}$

Figure 1.9: Polarizing beam-splitter.

$$\begin{pmatrix}\hat{b}_{\mathbf{k}_1H}\\ \hat{b}_{\mathbf{k}_1V}\\ \hat{b}_{\mathbf{k}_2H}\\ \hat{b}_{\mathbf{k}_2V}\end{pmatrix} = \begin{pmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix}\begin{pmatrix}\hat{a}_{\mathbf{k}_1H}\\ \hat{a}_{\mathbf{k}_1V}\\ \hat{a}_{\mathbf{k}_2H}\\ \hat{a}_{\mathbf{k}_2V}\end{pmatrix}. \tag{1.84}$$

A polarization measurement in the computational basis is equivalent to using a PBS followed by two detectors in the spatial modes corresponding to $\hat{b}_{\mathbf{k}_1}$ and $\hat{b}_{\mathbf{k}_2}$.

# Chapter 2

# A source of polarization-entangled photons

One of the most important features of the new quantum mechanical framework is the existence of multi-particle states that cannot be described from the separate description of the state of each particle composing it, the phenomenon of *entanglement*. Particles that are entangled in some of their degrees of freedom possess correlations that cannot be explicated within the classical framework, a feature that makes entanglement one of the main obstacles in finding a convincing interpretation of quantum theory.

Entanglement can exist between different degrees of freedom of a single particle, or in the same degree of freedom of multiple particles. The latter is the most interesting situation for quantum communication, since it allows non-classical correlations to travel along very long distances. One of the crucial requirements for the generation of photonic entangled states is a system that generates pairs of correlated photons. The other crucial ingredient in the generation of an entangled pair is the coherent superposition of different generation processes, so that it is impossible to determine in principle from which one the pair has originated.

The most widely employed process in the generation of photonic entanglement is spontaneous parametric down-conversion (SPDC) in a non-linear crystal. While the generation of polarization correlated pairs using spontaneous parametric down-conversion is relatively simple, the superposition of different processes is not a trivial task. The first polarization-entangled sources employed SPDC to create pairs of photons with orthogonal polarizations, and created entanglement by sending the two photons to the two input ports of a beam-splitter. In this way, it is possible to generate entangled pairs by post-selecting the cases in which the two photons leave the BS via different ports. The major problem of this source architecture is that it is probabilistic, i.e., it generates an entangled state only half of times. A breakthrough in polarization-entanglement was the implementation of a new scheme producing a true entangled state [19]. This scheme exploits one characteristic feature of phase-matched type-II SPDC, in which the photons of the pair (of orthogonal polarizations) are produced in two different cones. By taking the photon pairs produced at the intersection of the two cones, it is not possible to distinguish even in principle which process each photon comes from, thus generating a real entangled state[1].

Recently, a wider interest has grown around sources based on quasi-phase matched SPDC. This technique allows the creation of co-propagating photons in a linear crystal.

[1] Actually, it is still possible to distinguish the two processes because the birefringence of the non-linear crystal delays one polarization with respect to the other. This information, however, can be canceled by inserting an opposite delay just after the crystal, thus making the two processes indistinguishable again.

Despite its lower efficiency with respect to phase matching, the co-propagation heavily simplifies the collection of the down-converted photons, thus allowing the use of longer crystals, for an overall enhancement in the pair production rate.

One possible way of superposing different quasi-phase matched SPDC processes consists in using two different non-linear crystals in a crossed configuration, i.e., the second crystal is rotated by 90° around the propagation axis with respect to the first one [20]. This scheme generates entanglement by superposing the pairs generated by the two crystals. This requires the erasure of the which-crystal information, by finely tuning the temperature of the crystals, canceling the dispersive de-phasing effect with another non-linear crystal, and spectrally filtering the output photons. Moreover, the wavelength of the output photons is limited by the need of separating them, using a wavelength division multiplexer (WDM) or a dichroic mirror.

An alternative way of superposing different quasi-phase matched SPDC processes is by using a single non-linear crystal in a polarization-based Sagnac interferometer [21]. In this scheme, the superposition happens between photon pairs produced in the clockwise and anticlockwise path. Despite the tighter optical alignment required, this scheme has some advantages over the linear one. Indeed, the use of a single non-linear crystal simplifies the erasure of the which crystal information, preventing the use of spectral filtering and dispersive de-phasing compensation. Moreover, the polarization-based way of separating the produced photons gives higher tunability to the wavelength of the output photons, while keeping the high pair production rate and the narrow bandwidth of the linear scheme [21, 22].

This Section will deal with the development of a polarization-entangled source based on a Sagnac interferometer. The employed scheme is the well-tested one developed by Kim *et al.* [21]. After a first introduction on spontaneous parametric down-conversion and on the filtering procedures necessary for high quality entanglement generation using this scheme, this Section will describe the experimental design of this source and its calibration.

## 2.1 Spontaneous parametric down-conversion

The formalism described in Section 1.5.1, despite its usefulness in the study of the free electromagnetic field, is not very useful when studying its interaction with matter. This interaction happens at the atomic level, therefore it could be theoretically possible to describe the passage of an electromagnetic wave through some medium by explicitly treating atomic charges and currents within the theory. However, the high number of atoms in a general system makes this approach highly impractical, making it preferable to find a model that approximates this interaction. The model used in electromagnetism splits currents and charges into "free" ones, that can move freely through the medium (like the electrons in a conductor), and "bound" ones, which are forced to oscillate around their atom [23, 24]. Bound charges and currents are described by electric and magnetic multi-poles [25]. Within this theory, Maxwell's equations become

$$\nabla \cdot \mathbf{D}(\mathbf{r},t) = \rho(\mathbf{r},t) \tag{2.1}$$

$$\nabla \times \mathbf{H}(\mathbf{r},t) - \frac{\partial \mathbf{D}(\mathbf{r},t)}{\partial t} = \mathbf{J}(\mathbf{r},t) \tag{2.2}$$

$$\nabla \times \mathbf{E}(\mathbf{r},t) + \frac{\partial \mathbf{B}(\mathbf{r},t)}{\partial t} = 0 \tag{2.3}$$

$$\nabla \cdot \mathbf{B}(\mathbf{r},t) = 0, \tag{2.4}$$

where $\mathbf{D} = \varepsilon_0 \mathbf{E} + \mathbf{P}$ is the *displacement field* and $\mathbf{H} = \frac{1}{\mu_0}\mathbf{B} - \mathbf{M}$ is the *magnetizing field*. These fields capture the effects of the field on bound charges and currents, which are described by the *polarization vector* $\mathbf{P}$ and the *magnetization vector* $\mathbf{M}$, while the behavior of free charges and currents is still described by the source terms $\rho$ and $\mathbf{J}$. Most materials used in optics are uncharged non-conducting materials, therefore both free charges and currents are zero. Moreover, they are also non-magnetic materials, therefore the magnetization vector $\mathbf{M} \simeq 0$ and the interaction of the material with the field is completely captured by the polarization vector $\mathbf{P}$.

In the general case, the polarization vector can be expressed as a power series

$$\begin{aligned} P_i &= \varepsilon_0 \left( \sum_j \chi^{(1)}_{ij} E_j + \sum_{jk} \chi^{(2)}_{ijk} E_j E_k + \sum_{jkl} \chi^{(3)}_{ijkl} E_j E_k E_l + \cdots \right) \\ &= P^{(1)}_i + P^{(2)}_i + P^{(3)}_i + \cdots = P^{(1)}_i + P^{(NL)}_i , \end{aligned} \tag{2.5}$$

where the term $P^{(1)}_i$ gives the phenomenon of refraction, while the higher order terms $P^{(NL)}_i$ act like a source of the electromagnetic field at different frequencies [23, 24, 26].

Using the *Poynting theorem* [25], it is possible to write the field energy density (i.e., the Hamiltonian density) in the medium as

$$\mathcal{H}(\mathbf{r}, t) = \frac{1}{2} \left( \mathbf{E} \cdot \mathbf{D} + \mathbf{B} \cdot \mathbf{H} \right). \tag{2.6}$$

By writing $\mathbf{H} = \frac{1}{\mu_0}\mathbf{B}$ and $\mathbf{D} = \varepsilon_0 \mathbf{E} + \mathbf{P}$, Equation (2.6) becomes

$$\begin{aligned} \mathcal{H} &= \frac{1}{2}\varepsilon_0 |\mathbf{E}|^2 + \frac{1}{2\mu_0}|\mathbf{B}|^2 + \frac{\varepsilon_0}{2} \sum_{ij} \chi^{(1)}_{ij} E_i E_j + \frac{\varepsilon_0}{2} \sum_{ijk} \chi^{(2)}_{ijk} E_i E_j E_k + \ldots \\ &= \mathcal{H}_0 + \mathcal{H}_I , \end{aligned} \tag{2.7}$$

where $\mathcal{H}_0$ is the Hamiltonian density (1.38) of the free electromagnetic field and $\mathcal{H}_I$ is the Hamiltonian density describing the interaction of the field with matter.

Once the classical Hamiltonian density has been written as a function of the classical fields, it is possible to write the quantum Hamiltonian density operator in the second quantization framework by transforming the electric and magnetic fields into field operators[2]. The Hamiltonian density operator is therefore written as $\hat{\mathcal{H}} = \hat{\mathcal{H}}_0 + \hat{\mathcal{H}}_I$, the sum of a free field Hamiltonian density $\hat{\mathcal{H}}_0$ and an interaction Hamiltonian $\hat{\mathcal{H}}_I$. This allows to work in the *interaction picture*, in which the field operators $\hat{\mathbf{E}}$ and $\hat{\mathbf{B}}$ satisfy the Heisenberg-like equation of motion (1.51), but involving only the free Hamiltonian $\hat{H}_0$ instead of the complete Hamiltonian $\hat{H}$ [13]. In particular, field operators keep all the properties of free field operators described in Section 1.5.1. They can still be described by their quantum mechanical amplitude operator $\hat{a}_\lambda(\mathbf{k})$, that satisfy the same commutation relations (1.40) and (1.41) and are the result of the same mode expansion as the free electric and magnetic field[3].

The interaction Hamiltonian density $\hat{\mathcal{H}}_I$ can therefore be written as

$$\begin{aligned} \hat{\mathcal{H}}_I \; \alpha \; & \sum_{ij} \chi^{(1)} \left( \hat{E}^{(+)}_i + \hat{E}^{(-)}_i \right) \left( \hat{E}^{(+)}_j + \hat{E}^{(-)}_j \right) \\ & + \sum_{ijk} \chi^{(2)}_{ijk} \left( \hat{E}^{(+)}_i + \hat{E}^{(-)}_i \right) \left( \hat{E}^{(+)}_j + \hat{E}^{(-)}_j \right) \left( \hat{E}^{(+)}_k + \hat{E}^{(-)}_k \right) + \ldots , \end{aligned} \tag{2.8}$$

[2] This procedure is equivalent to the transformation of the electromagnetic potentials into operators.

[3] They are related to vector potential mode expansion of Equation (1.39) by using Equations (1.30) and (1.31).

where $E^{(+)}$ is the positive frequency mode (proportional to the annihilation operator) and $E^{(-)}$ is the negative frequency one (proportional to the creation operator).

In the interaction picture, the evolution of the state is governed by operator

$$\hat{U} = \mathcal{T} \exp\left[-\frac{i}{\hbar}\int_{-\infty}^{\infty} \hat{H}_I(t)\right], \tag{2.9}$$

where $\mathcal{T}$ it the time-ordered product [27], and the integration limits $-\infty$ and $+\infty$ are justified by the fact that the state is observed long after the non-linear interaction in the medium [26]. The interaction Hamiltonian is given by the spatial integration of the Hamiltonian density as in Equation (1.52). The above integral can be evaluated using the rotating-wave approximation, which allows to neglect rapidly oscillating terms in the Hamiltonian $\hat{H}_I$ [26].

The $\chi^{(1)}$ term of the Hamiltonian density (2.8) gives rise to refractive effects (such as, for example, birefringence). The only surviving terms are those of the form $E^{(+)}E^{(-)}$ (and its complex conjugate), leaving a photon-number preserving Hamiltonian of the form (1.57). These effects can be treated by aligning the system of reference to the *principal axes* of the material, in which the $\chi^{(1)}$ tensor assumes a diagonal form (i.e., $\chi^{(1)}_{ij} \neq 0$ iff $i = j$) [17].

The $\chi^{(2)}$ term gives rise to a wide range of non-linear effects [23]. Spontaneous parametric down-conversion is the effect described by the interaction term of the form

$$\hat{H}_{SPDC} = \int d^3\mathbf{r} \sum_{i_p j_s k_i} \chi^{(2)}_{i_p j_s k_i} \hat{E}^{(+)}_{i_p} \hat{E}^{(-)}_{j_s} \hat{E}^{(-)}_{k_i} + c.c., \tag{2.10}$$

where the term $\hat{E}^{(+)}_{i_p}$ corresponds to the annihilation of a *pump* photon of mode $i_p$ and the terms $\hat{E}^{(-)}_{j_s}$ and $\hat{E}^{(-)}_{k_i}$ to the creation of two photons in modes $j_s$ and $k_i$, called, respectively, *signal* and *idler* photons. By properly adjusting the pump field, it is possible to make the SPDC term the only one giving a considerable effect. In order to have this, however, it is necessary that the fields respect the so-called *phase-matching* conditions

$$\omega_{i_p} = \omega_{j_s} + \omega_{k_i} \tag{2.11}$$

$$\mathbf{k}_{i_p} = \mathbf{k}_{j_s} + \mathbf{k}_{k_i}, \tag{2.12}$$

where the first condition is required to avoid SPDC to be negligible due to the rotating-wave approximation, and the second condition is the correspondent in the spatial domain.

The optimization of the SPDC process requires to study the form of the Hamiltonian (2.10) for different pump, signal and idler modes. The large number of variables required to describe these fields makes it preferable to perform some approximations about their form, in order to simplify the problem. The analysis of the SPDC process has been carried in a very lot of papers, each one considering a different approximation [28–32]. The most suitable analysis for our setup is the one by Bennink [28], that considers the interaction of a gaussian pump field with a non-linear crystal, leading to the production of two collinear photons in gaussian modes. In addition to this, the approximation made in Section 1.5.1 of single-frequency spatial modes must be dropped, in order to take into account the whole spectral properties of the SPDC phenomenon. Since in collinear propagation the phase-matching condition (2.12) is not obtainable, it is necessary adopt other strategies to give a considerable production of down-converted pairs, called *quasi phase-matching*. Quasi phase-matching consists in modulating the $\chi^{(2)}$ coefficient of the crystal, alternating its sign with spatial period $\Lambda$. In this way, it is possible to have a significant improvement of the down-conversion efficiency [17].

In Bennink's study [28], the field $E^{(+)}$ is expanded as a superposition of different frequency gaussian modes

$$\hat{\mathbf{E}}^{(+)}(\mathbf{r}, t) = \int_0^\infty d\omega \sqrt{\frac{\hbar\omega}{2\varepsilon_0}} \mathbf{E}_\omega(\mathbf{r}) e^{-i\omega t} \hat{a}_\omega(t) + \textit{non gaussian terms}, \tag{2.13}$$

and similarly $\hat{\mathbf{E}}^{(-)}$. Furthermore, he assumes that the second-order interaction is weak, so that it is possible to perform a first-order expansion of the evolution operator of Equation (2.9). The state after the SPDC process is therefore

$$|\psi_{SPDC}\rangle = \hat{U} \, |\text{initial}\rangle \simeq |\text{initial}\rangle - \frac{i}{\hbar} \int_{-\infty}^{\infty} \hat{H}_{SPDC}(t) \, |\text{initial}\rangle \,, \tag{2.14}$$

where $|\text{initial}\rangle$ is the state of the field prior to the interaction and $\hat{H}_{SPDC}(t)$ is the Hamiltoninan (2.10).

Since the crystal is pumped with a laser, he assumes the pump to be described as a classical coherent state, with spectral amplitude $s(\omega_p)$ and mean number of photons $N_p$. With these approximations, and assuming that the pump state is filtered out, Equation (2.14) can be written as

$$|\psi_{SPDC}\rangle = -i \int_0^\infty d\omega_s d\omega_i \psi(\omega_s, \omega_i) \hat{a}^\dagger_{\omega_s} \hat{a}^\dagger_{\omega_i} \, |\Omega\rangle \,, \tag{2.15}$$

where $|\Omega\rangle$ is the vacuum state and

$$\psi(\omega_s, \omega_i) = \sqrt{\frac{2\pi^2 \hbar N_p}{\varepsilon_0 \lambda_p \lambda_s \lambda_i}} s(\omega_p) \mathcal{O}(\omega_s, \omega_i), \tag{2.16}$$

where $\lambda_i = 2\pi c/\omega_j$ is the free-space wavelength of field $j$, and the photons respect the phase-matching condition (2.11). The term

$$\mathcal{O}(\omega_s, \omega_i) = \int_{medium} d^3\mathbf{r} \chi^{(2)}(\mathbf{r}) : \mathbf{E}_{\omega_p}(\mathbf{r}) \mathbf{E}^*_{\omega_s}(\mathbf{r}) \mathbf{E}^*_{\omega_i}(\mathbf{r}) \tag{2.17}$$

gives the efficiency of the quasi-phase-matched down-conversion process, which depends both on the efficiency of quasi-phase matching and on the overlap of the different spatial modes (the : notation in the integral is used to indicate the tensor product of the non-linear coefficient $\chi^{(2)}$ with the polarization terms $\epsilon_{\omega_p}$ of mode $\mathbf{E}_{\omega_p}$).

## 2.2 Experimental design of the source

The source is based on a polarization-based Sagnac interferometer. The scheme of the source is shown in Figure 2.1, while its experimental realization on the optical bench is in Figure 2.2.

The source is pumped with a CW laser diode (LD) at $\lambda_P = 404.5\,\text{nm}$. The beam emitted by the diode is collected onto a polarization-maintaining single-mode fiber (PM-SMF), used to clean its spatial mode. The PM-SMF is sent onto the optical breadboard, where the laser beam is collimated by an aspheric lens of focal length 11 mm into a beam of $\sim$ 1.5 mm diameter. The polarization state of the beam is transformed into $\epsilon_+ =$

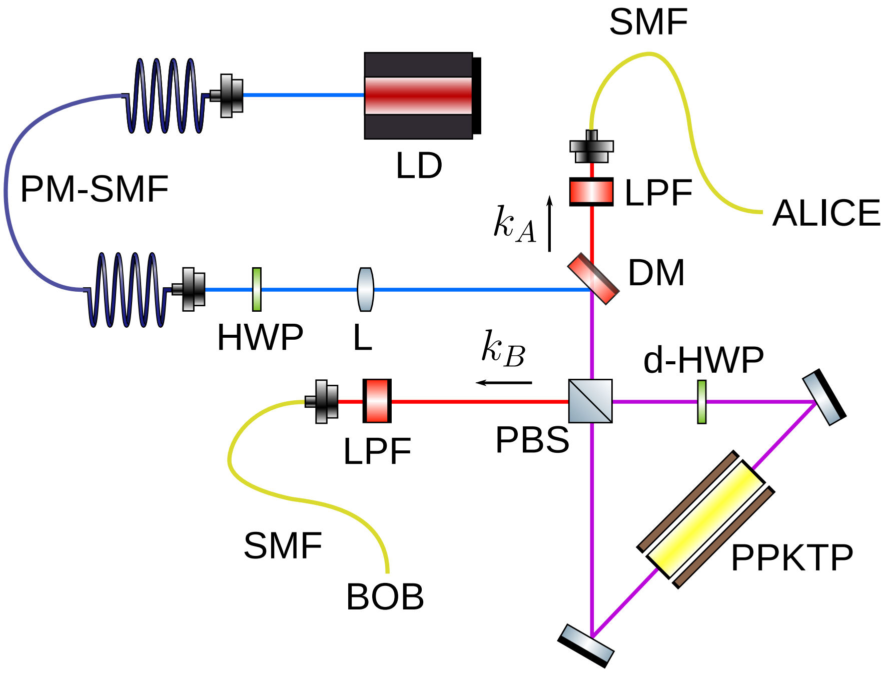

Figure 2.1: Experimental scheme of the source of polarization-entangled photons based on a polarization Sagnac interferometer. The pump laser (LD) is injected into a polarization-maintaining single-mode fiber (PM-SMF) for mode filtering. The output of the fiber is sent onto a half-wave plate (HWP), that rotates the polarization state of the pump laser to $|+\rangle$. The state is then focused into a periodically-poled potassium titanyl phosphate (PPKTP) crystal placed at the center of a Sagnac interferometer. A polarizing-beam splitter (PBS) at the entrance of the interferometer splits the pump onto a superposition of clockwise ($V$) and counterclockwise ($H$) path. The clockwise pump beam crosses a dual-wavelength half-wave plate (d-HWP), that rotates its state from $V$ to $H$. Both paths produce $|H\rangle_S |V\rangle_I$ couples, where the superscript indicates the signal and the idler photon. In the anticlockwise path, the d-HWP changes the couple to $|V\rangle_S |H\rangle_I$. At the PBS the photons are combined so that the resulting state is $|H\rangle_S |V\rangle_I + e^{i\theta} |V\rangle_S |H\rangle_I$, where $\theta$ is a phase term given by the different optical length of the two paths. The pump is removed using a long-pass filter (LPF) before injection into a single-mode fiber (SMF). This image uses elements from the ComponentLibrary by Alexander Franzen [33], licensed under CC BY-NC 3.0 [34].

$(\epsilon_H + \epsilon_V)/\sqrt{2}$ by a half-wave plate (HWP) and then focused by a doublet with equivalent focal length 333 mm into the center of the Sagnac interferometer.

At the entrance of the interferometer, a polarizing-beam splitter (PBS) creates a superposition of clockwise $\mathbf{k}_C$ and counterclockwise $\mathbf{k}_{CC}$ path, by sending $H$ polarization in the first path and $V$ polarization in the second one. The state is then transformed, by the dual-wavelength half-wave plate (d-HWP) into $(E_H(\mathbf{k}_C) + E_H(\mathbf{k}_{CC}))/\sqrt{2}$. This state travels through a periodically-poled $KTiOPO_4$ (PPKTP) crystal[4], that outputs the state

$$\hat{a}^\dagger_{\mathbf{k}_C,H}\hat{b}^\dagger_{\mathbf{k}_C,V} + \hat{a}^\dagger_{\mathbf{k}_{CC},H}\hat{b}^\dagger_{\mathbf{k}_{CC},V}, \tag{2.18}$$

where $\hat{a}^\dagger$ and $\hat{b}^\dagger$ are the mode functions of, respectively, the signal and the idler photon

[4] The crystal is a 30 mm PPKTP by Raicol, with a $\chi^{(2)}$ grating of period $\Lambda = 10\,\mu$m.

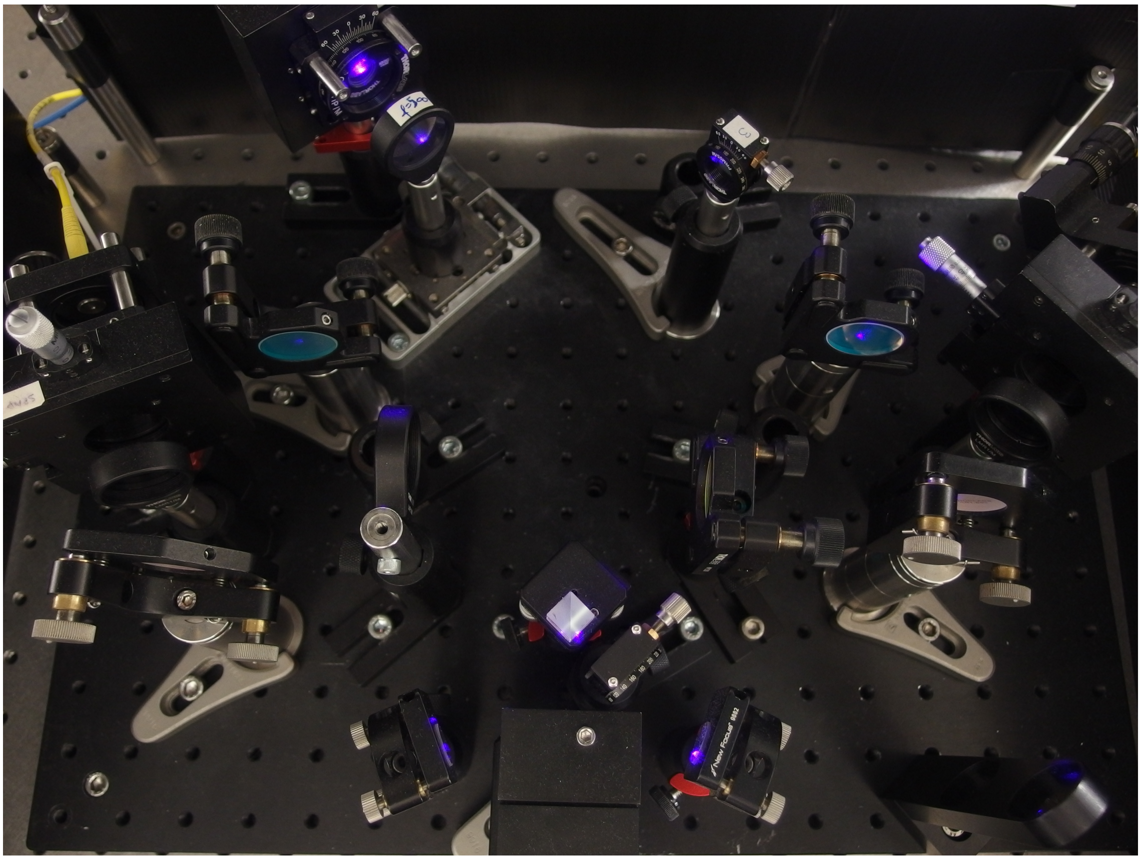

Figure 2.2: Implementation of the scheme described in Figure 2.1 on the optical bench. The source is mounted on a breadboard in order to be transportable for free-space experiments out of the laboratory. The use of an optical breadboard, on the other hand, poses some additional constraints on the possible distance between optical elements, thus requiring more care in the choice of the optimal focal parameters.

(they can have different wavelength and are, in general, not temporally superposed due to the temporal walk-off introduced by crystal birefringence). The pair in the counterclockwise path, then, crosses the d-HWP, being transformed into $\hat{a}^\dagger_{\mathbf{k}_{CC},V}\hat{b}^\dagger_{\mathbf{k}_{CC},H}$.

Just before the polarizing beam-splitter (PBS), the state is

$$\hat{a}^\dagger_{\mathbf{k}_C,H}\hat{b}^\dagger_{\mathbf{k}_C,V} + e^{i\theta}\hat{a}^\dagger_{\mathbf{k}_{CC},V}\hat{b}^\dagger_{\mathbf{k}_{CC},H}, \tag{2.19}$$

where the phase term $e^{i\theta}$ takes into account the different path length of the two arms of the interferometer. The PBS transforms the state into

$$|\text{out}\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger_{\mathbf{k}_A,H}\hat{b}^\dagger_{\mathbf{k}_B,V} + e^{i\theta}\hat{a}^\dagger_{\mathbf{k}_A,V}\hat{b}^\dagger_{\mathbf{k}_B,H}\right)|\Omega\rangle\,, \tag{2.20}$$

where $|\Omega\rangle$ is the vacuum state. The output polarization state is therefore

$$|\psi\rangle = \frac{|H\rangle_A|V\rangle_B + e^{i\theta}|V\rangle_A|H\rangle_B}{\sqrt{2}}. \tag{2.21}$$

In order to produce the maximally entangled state $|\Psi^-\rangle$, therefore, it is necessary to adjust the value of the phase $\theta$ in the state (2.21). In addition to this, it is also necessary to compensate the birefringence effect of optical fibers. Indeed, let $U_A$ be the effect of Alice's fiber and $U_B$ the effect of Bob's one, the state at the output of the fibers is

$$\left|\psi_{fiber}\right\rangle = (U_A \otimes U_B)\, \frac{\left|H\right\rangle_A \left|V\right\rangle_B + e^{i\theta} \left|V\right\rangle_A \left|H\right\rangle_B}{\sqrt{2}}. \tag{2.22}$$

To produce the singlet state $\left|\Psi^-\right\rangle$, it is sufficient to implement a general unitary transformation in one of the two output photons. Indeed, the singlet state has the property that $(U \otimes U)\left|\Psi^-\right\rangle = \left|\Psi^-\right\rangle$. The transformation that must be implemented on the output state is therefore $I_2 \otimes U$, with

$$U = U_A \begin{pmatrix} 1 & 0 \\ 0 & -e^{i\theta} \end{pmatrix} U_B^{-1}. \tag{2.23}$$

Indeed, the applications of this transformation gives

$$\begin{aligned}(I_2 \otimes U)\,(U_A \otimes U_B)\left|\psi\right\rangle &= \frac{U_A \left|H\right\rangle_A (-e^{i\theta}) U_A \left|V\right\rangle_B + e^{i\theta} U_A \left|V\right\rangle_A U_A \left|H\right\rangle_B}{\sqrt{2}} \\ &= (U_A \otimes U_A)\left|\Psi^-\right\rangle = \left|\Psi^-\right\rangle.\end{aligned} \tag{2.24}$$

## 2.3 Performance and calibration

This Section describes the results of the measurements performed on the source in order to characterize it. The first part will describe the pump laser, while the following Sections will deal with the spectral properties of the down-converted photons and the properties of the output state.

### 2.3.1 The pump laser

The source is pumped with an Ondax's LM Series Compact Laser Module, with a nominal wavelength of 405 nm and a linewidth $\Delta\omega < 160\,\mathrm{MHz}$ [35]. The nominal output mode is

Figure 2.3: The Ondax's LM Series Compact Laser Module used as a pump laser for the Sagnac interferometer. From [35].

an elliptic beam with size 0.8 × 0.4 mm, with divergence smaller than 10 mrad.

During the experiments, the laser is operated at 20 °C, with a diode current $I_{pump}$ ranging from 30 mA to 70 mA.

### Spatial mode

The spatial mode output by a laser can be studied by looking at the beam shape at different distances from the laser. A CMOS camera is used to take images of the intensity profile at different positions along the direction of propagation $z$. Each image is then fitted with the function

$$I(x,y;z)\;\alpha\; e^{-\frac{2(x-x_0)^2}{W_x^2(z)}-\frac{2(y-y_0)^2}{W_y^2(z)}}, \tag{2.25}$$

where the relevant fit parameters are the transverse dimensions of the beam [17, 36]. Since the beam is elliptic, the fit is performed with two independent parameters $W_x(z)$ and $W_y(z)$ for the width along the two transversal axes. The values of the beam width are then fitted using the function

$$W_i(z) = W_{0i}\sqrt{1+\left(M_i^2\frac{(z-z_{0i})\lambda}{\pi W_{0i}^2}\right)}, \tag{2.26}$$

where $\lambda$ is the wavelength of the laser beam and the fit parameters are $W_{0i}$, the beam waist, $z_{0i}$, the position of the waist along the direction of propagation, and $M_i^2$, the "beam-quality" parameter [36]. The result of the fit is shown in Figure 2.4.

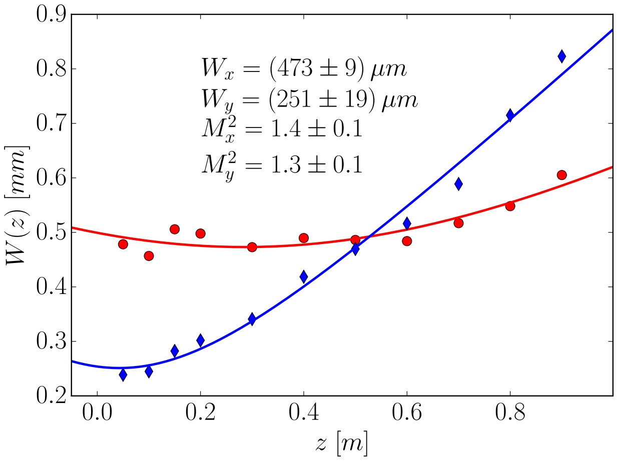

Figure 2.4: Beam width as a function of the propagation distance $z$.

From the values of $M_x^2$ and $M_y^2$, it is evident that the beam is not in TEM$_{00}$ mode as stated by the datasheet[5] [35]. This can also be seen by directly looking at the intensity profile, as shown in Figure 2.5.

This situation makes it advisable to perform some form of mode filtering before injecting the laser into the Sagnac interferometer. Indeed, using the laser in free space with such bad output mode makes it very difficult to have an optimal collection of the down-converted photons into optical fibers. Mode filtering is performed by using a polarization maintaining single-mode optical fiber (PM-SMF)[6].

[5] Such a "beam-quality" parameter, however, is not unusual for a laser diode.

[6] The fiber used is a Thorlabs P1-405BPM-FC.

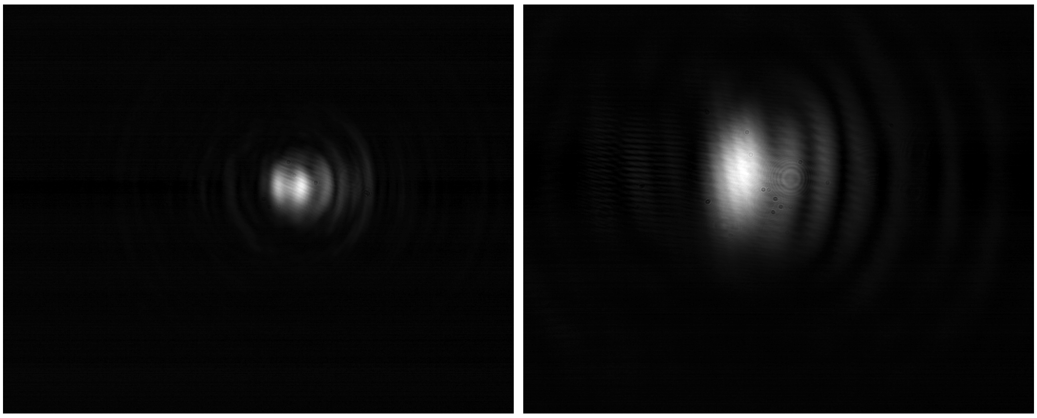

Figure 2.5: Intensity profile of the beam in the near (left) and in the far field (right). The fringes both in the near and in the far field are due to the presence of higher order modes.

### Output power

The output power of the laser as a function of the diode current $I$ is shown in Figure 2.6, both before and after the optical fiber. From the interpolated light-current curve, it is possible to calculate the laser-oscillation threshold current $I_t = (25.6 \pm 0.1)\,\mathrm{mA}$ [17]. During all the experimental work, the laser will be used in the range $[30, 70]$ $mA$.

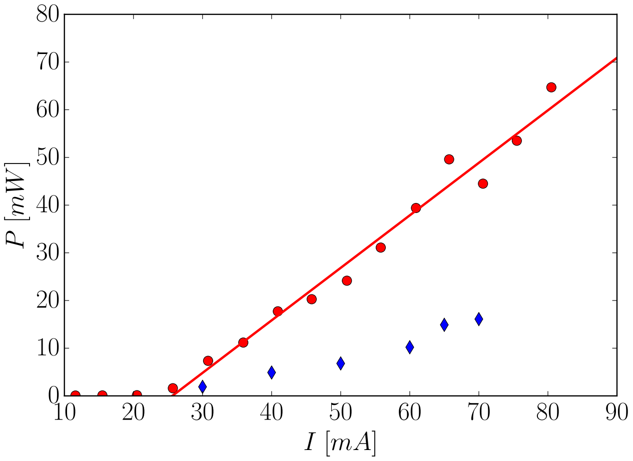

Figure 2.6: Power of the laser as a function of the diode current $I$ before (red circles) and after (blue diamonds) the injection into the mode filtering fiber. The red line is the interpolated light-current curve.

The mean efficiency of the fiber coupling system is $\eta = 0.32 \pm 0.05$. While it is not the maximum coupling efficiency obtainable with single mode fibers, it is enough for all the applications of the source exposed in this thesis. In any case, the single-mode fiber decouples the laser from the source, allowing to add a more sophisticated optical system between the laser and the fiber without altering the entangled source.

### Spectral properties

The wavelength of the pump laser can be estimated indirectly from the measurement of the wavelength of down-converted photons. Indeed, the phase-matching condition (2.11) gives

$$\frac{1}{\lambda_p} = \frac{1}{\lambda_s} + \frac{1}{\lambda_i}, \tag{2.27}$$

where $\lambda_p$ is the wavelength of the pump laser and $\lambda_s$ ($\lambda_i$) is the wavelength of the signal (idler).

The measurement of the wavelength of the down-converted photons is described in Section 2.3.3. From those data, the wavelength of the pump laser can be estimated to be $\lambda_p = (404.6 \pm 0.2)\,\text{nm}$.

The measurement of the bandwidth of the pump laser, on the other hand, has been directly carried by inserting it into a Michelson interferometer and looking at the interference pattern for different path differences, as shown in Figure 2.7. This system can be employed to measure the coherence time of the pump laser. Indeed, given the electric field at the output of the pump laser $E(t) = E_0 e^{-i\omega_0 t} e^{i\phi(t)}$, with $\omega_0$ the angular frequency of the laser, the field after the beam-splitter is given by $E_1(t) + E_2(t)$, where $E_i(t) = (E_0/\sqrt{2}) e^{-i\omega_0 t} e^{i\phi(t)}$ is the electric field propagating in spatial mode $i$. When they recombine at the beam-splitter, the two fields have traveled through two different paths with length difference $\delta d = 2(d_2 - d_1)$, therefore the total electric field is

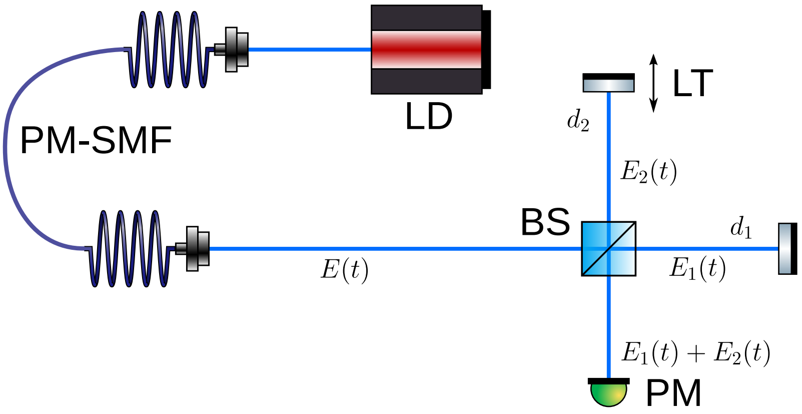

Figure 2.7: Michelson interferometer used in the measurement of the bandwidth. The laser (LD) is inserted into a polarization-maintaining single-mode fiber (PM-SMF), whose output is directed against a beam-splitter (BS), which sends the beam to the two arms of the interferometer, of length $d_1$ and $d_2$. The length of one arm of the interferometer can be precisely changed by a motorized linear translator (LT). The power at the output of the interferometer is measured using a power meter (PM). This image uses elements from the ComponentLibrary by Alexander Franzen [33], licensed under CC BY-NC 3.0 [34].

$$\begin{aligned} E_{det}(t) &= \frac{1}{2}\left[E(t) + E(t+\tau)\right] \\ &= (E_0/2) e^{-i\omega_0 t} e^{i\phi(t)} \left[1 + e^{-i\omega_0 \tau} e^{i\left(\phi(t+\tau) - \phi(t)\right)}\right], \end{aligned} \tag{2.28}$$

where $\tau = 2\delta d/c$, with $c$ the speed of light in the vacuum. The intensity at the detector is therefore

$$\begin{aligned}
I(\tau) &= \left\langle E^*_{det}(t) E_{det}(t) \right\rangle_T \\
&= \frac{1}{2}\left[ \left\langle \left|E(t)\right|^2 \right\rangle_T + \left\langle \left|E(t+\tau)\right|^2 \right\rangle_T + \left\langle E^*(t)E(t+\tau) + E^*(t+\tau)E(t) \right\rangle_T \right] \\
&= \frac{1}{2}\left\langle \left|E(t)\right|^2 \right\rangle_T + \frac{1}{2}\left\langle \left|E(t+\tau)\right|^2 \right\rangle_T + \left\langle \Re\left[E^*(t)E(t+\tau)\right] \right\rangle_T \\
&= \frac{1}{2T}\int_T dt \left|E(t)\right|^2 + \frac{1}{2T}\int_T dt \left|E(t+\tau)\right|^2 \\
&+ \frac{1}{T}\int_T dt \Re\left\{ \left|E_0\right|^2 e^{-i\omega_0\tau} e^{i\left[\phi(t+\tau)-\phi(t)\right]} \right\} \\
&= I_0 + I_0 \left\langle \left| e^{i\left[\phi(t+\tau)-\phi(t)\right]} \right| \right\rangle_T \cos\omega_0\tau \\
&= I_0\left[1 + g_1(\tau)\cos\omega_0\tau\right] \\
&= I_0\left[1 + \mathcal{V}(\tau)\cos\omega_0\tau\right] ,
\end{aligned} \tag{2.29}$$

where $\mathcal{V}(\tau) = g_1(\tau) = \left\langle \left| e^{i\left[\phi(t+\tau)-\phi(t)\right]} \right| \right\rangle$ is the visibility [37], and $I_0$ is the input intensity.

In order to measure the coherence time $\tau_c$ of the laser, it is necessary to measure the intensity of the laser for different values of the path difference $\delta d$. For this measurement, only the envelope of the function $I(\tau)$ is required, therefore it is not necessary to sample the complete $\cos(\omega_0\tau)$ oscillation and it is possible to choose larger $\delta d$ steps. The resulting interference pattern is shown in Figure 2.8.

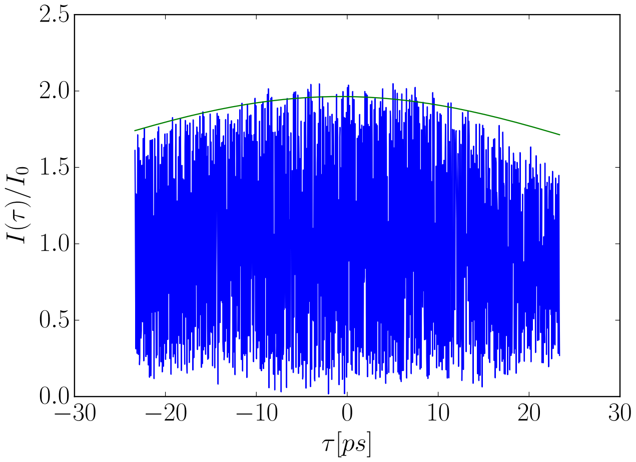

Figure 2.8: Measurement of the function $I(\tau)$ for the pump laser. The chosen sampling is such that the $\cos(\omega_0\tau)$ part of the function is not observable, giving only a direct measurement of the envelope of $I(\tau)$.

By fitting the envelope of $I(\tau)$ with the function [38]

$$f(\tau) = 1 + e^{-\frac{\tau^2}{2\tau_c^2}} , \tag{2.30}$$

it is possible to measure the coherence time of the laser as $\tau_c = (55 \pm 1)$ ps, corresponding to a FWHM bandwidth $\Delta\omega = (76 \pm 1)$ GHz, which is several orders of magnitude higher than the value reported in the datasheet [35]. This is probably due to the effect of the polarization-maintaining fiber. Indeed, a measurement of the value of $I(\tau)$ for the laser without fiber injection, for $\tau \sim 1\,\text{ns}$, has given a visibility $\mathcal{V}(\tau) \sim 1$, without showing the rapid decay of visibility seen in Figure 2.8. Since the coherence time after the fiber was enough for its operation as a pump for the Sagnac source, this effect has not been further investigated.

These measurements highlighted also another problem of the pump laser. Indeed, by changing the intensity of the current driving the laser diode, it was possible to see the appearance in the $I(\tau)$ curve of beating effects due to the presence of multiple modes resonating into the laser cavity, as shown in Figure 2.9. For the QKD experiment is Section 3.1.4 this is not a problem, because the presence of multiple wavelength down-converted photons does not leak any information to an attacker measuring one of the photons in the pair. The experiment of Section 3.2, however, is very sensible to the wavelength of the down-converted photons, since different wavelengths give rise to different optical paths. For this reason, in the apparatus shown in Figure 3.26, a 3 nm filter is used before Charlie's measurement.

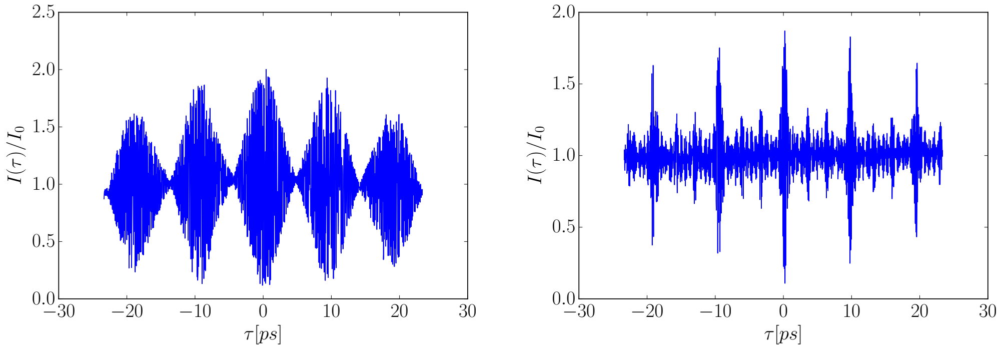

Figure 2.9: Beating effect in the interference pattern due to the presence of multiple resonating modes in the laser cavity.

### 2.3.2 Focusing parameters

The analysis of Bennink [28] is aimed at finding the values of the focal parameters that maximize the efficiency of the SPDC process according to different points of view. In order to simplify the calculations, he makes some approximations based on some assumptions on the experimental parameters involved in the process:

1. the length of the non-linear crystal is $\gtrsim 1\,\text{mm}$ and its refractive index is $\gtrsim 1.5$,
2. SPDC is quasi-phase-matched with a first-order grating of period $\Lambda \gtrsim 5\,\mu\text{m}$,
3. down-converted photons have $\lambda_s \lesssim 1.6\,\mu\text{m}$, while the pump has $\lambda_p \lesssim 0.8\,\mu\text{m}$.

The crystal used for the experimental setup described in Section 2.2 meets all the assumptions made by Bennink for his analysis, since (1) its length is 30 mm and has refractive index $1.7 - 1.8$, (2) the SPDC is quasi-phase-matched with $\chi^{(2)}$ grating period $\Lambda = 10\,\mu\text{m}$, and (3) the pump has $\lambda_p = 404.5\,\text{nm}$, with down-conversion photons of $\lambda_s = \lambda_i = 809\,\text{nm}$.

In his analysis, Bennink studies the optimization of the source with respect to the *focal parameter*

$$\xi_j \equiv \frac{L}{k_j w_j^2}, \tag{2.31}$$

where $L$ is the length of the crystal, $k_j = 2\pi n_j/\lambda_j$, with $n_j$ the refractive index [39, 40] and $\lambda_j$ the wavelength of photon $j \in \{p, s, i\}$, and $w_j$ is the beam waist for photon $j$.

After the PM-SMF, the pump is collimated by a CFC-11X-A into a beam of waist $W_{coll} = (0.70 \pm 0.03)\,\text{mm}$, which is then focused using a doublet of lenses of focal $f_1 \sim 500\,\text{mm}$ and $f_2 \sim 1000\,\text{mm}$, equivalent to a single lens of focal $f \sim 333\,\text{mm}$. The placement of the doublet is such that the waist of the pump falls precisely at the middle of the crystal. The pump beam has been directly measured with the procedure described in Section 2.3.1, giving the beam profile shown in Figure 2.10. By comparing the beam profile of the focused pump beam in Figure 2.10 with the one of Figure 2.4, it is evident the effect of mode filtering. Indeed, the $M^2$ parameter of the pump beam $(1.03 \pm 0.03)$ and the fact that $W_{Py} \simeq W_{Px} = (53 \pm 4)\,\mu\text{m}$ indicate that the beam is, with good approximation, in the TEM$_{00}$ mode. The focal parameter of the pump beam is $\xi_p \sim 0.4$.

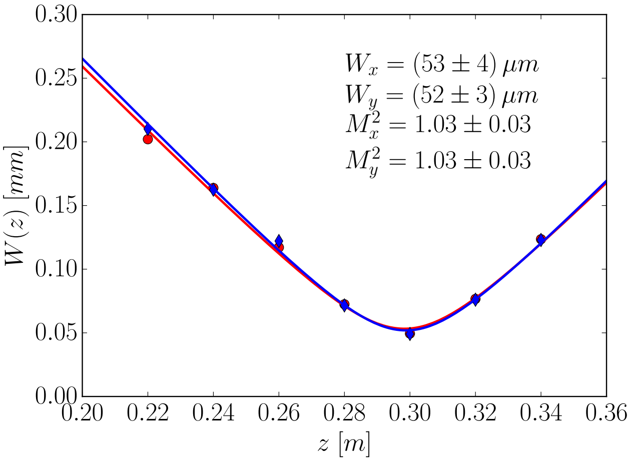

Figure 2.10: Beam profile after the lens used to focus the beam into the PPKTP crystal.

Also signal and idler are focused in the middle of the non-linear crystal. The value of their waist has not been directly measured, but it has been estimated from the values of the focusing optics obtained from the respective datasheets, using the formulas for Gaussian beam propagation [17]. The fiber used for the signal and the idler is a Thorlabs P1-780A-FC2, that is focused at the middle of the crystal using a C280-TME-B aspheric lens of focal length $f_{asph} = 18.4\,\text{mm}$. The theoretical beam waist at the crystal, which is situated at a distance $z \sim 245\,\text{mm}$ from the lens, is $W_s = W_i \sim 31\,\mu\text{m}$, corresponding to focal parameters $\xi_s = 2.3$ and $\xi_i = 2.2$ (the two focal parameters are different because of the birefringence of the crystal, which makes $n_s \neq n_i$).

The pump parameters chosen are a compromise due to the spatial constraints of the implementation. The mean heralding efficiency, calculated as $\eta = C_{12}/\sqrt{C_1 C_2}$, where $C_{12}$ are the coincidences between the two channels and $C_1$ and $C_2$ are the singles on the two channels, is $\eta \sim 0.15$. Taking into account the $\eta_d = 0.6$ detection efficiency, the estimated collection efficiency is $\eta_{coll} = \eta/\eta_d \sim 0.25$. This value corresponds to 6.0 dB of losses, much lower than the value reported in Section 3.1.4. This is due to the fact that the three-state experiment has been performed before the optimization of the source, which gives the results described in this Section.

The brightness of the source can be evaluated by measuring the number of coincidences for $mW$ of pump power. The detected normalized number of coincidences is $C_{12}/P_{pump} \sim$ 18.7 kHz/mW. If the detection efficiency is taken into account, the rate of coincidences is $N_c/P_{pump} = C_{12}/(\eta_d^2 P_{pump}) = 52.0$ kHz/mW, corresponding to a spectral brightness of 289 kHz/mW/nm, in line with what found in previous implementations of the source [22].

### 2.3.3 Down-converted photons

#### Wavelength

In a non-linear crystal, quasi-phase-matched collinear SPDC is realized when

$$k_p - k_s - k_i = \frac{2\pi n_p(\lambda_p, T)}{\lambda_p} - \frac{2\pi n_s(\lambda_s, T)}{\lambda_s} - \frac{2\pi n_i(\lambda_i, T)}{\lambda_i} \simeq \frac{2\pi}{\Lambda(T)}, \tag{2.32}$$

where $k_j$ is the modulus of the wave vector (the wave vector is, in first approximation, parallel for all photons), $n_j(\lambda_j, T)$ is the refractive index, dependent on the temperature, the wavelength and the direction of polarization, and $\Lambda(T)$ is the grating period. Equation (2.32) must be valid under the condition (2.11), therefore, since $\lambda_p$ is fixed by the pump laser, the only way to control the wavelengths $\lambda_s$ and $\lambda_i$ is through the temperature of the crystal.

The behavior of the wavelength of the down-converted photons as a function of the temperature is shown in Figure 2.11. The wavelength of the down-converted photons has been measured using the setup of Figure 2.12.

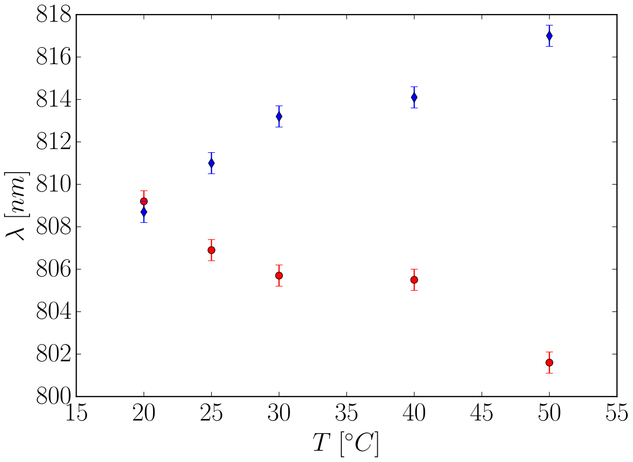

Figure 2.11: Wavelength dependence of the signal (red circle) and the idler (blue diamond) photon as a function of the temperature of the PPKTP crystal.

The measurement procedure exploits the relationship linking the first interference maximum with the incoming wavelength

$$\lambda = a\left(\sin\theta_i \sin\theta_t\right) = 2a\sin\left(\frac{\theta_i + \theta_t}{\sqrt{2}}\right)\cos\left(\frac{\theta_i - \theta_t}{\sqrt{2}}\right), \tag{2.33}$$

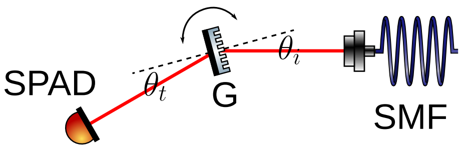

Figure 2.12: Setup used for the measurement of down-converted photon wavelength. The down-converted photon, coming from a single-mode fiber (SMF), is directed against a transmission grating (G) with period $a = 3.3\,\mu$m, mounted on a precision rotation mount. The photon is then collected by a single-photon avalanche photo-diode (SPAD), in a fixed position. By measuring the rotation angle of the grating at which a maximum number of photons is detected, it is possible to infer the wavelength of the photon. This image uses elements from the ComponentLibrary by Alexander Franzen [33], licensed under CC BY-NC 3.0 [34].

where $\theta_i$ is the incidence angle and $\theta_t$ is the transmission angle. Since the position of both the source and the detector is fixed, $\theta_i + \theta_t = \phi$ is constant. Therefore, it is possible to measure the wavelength $\lambda$ of the photon by measuring the angle $\theta_i$ of the grating with respect to the incoming beam (the measurement setup is calibrated by using the tunable wavelength output of the Coherent Mira-HP laser and a power-meter instead of the SPAD). The high losses of the whole measurement system make the signal at the detector quite low, determining the high error in the down-converted photon wavelength shown in Figure 2.11.

The temperature of degenerate phase-matching, where both the signal and the idler photons have the same wavelength, is around $T = 20\,°\text{C}$. All the experiments described in Chapter 3 are performed with $T = 20\,°\text{C}$.

### Bandwidth

The bandwidth of the down-converted photons can be measured using the same procedure described in Section 2.3.1, using a single photon detector instead of the power-meter. The resulting bandwidth of the down-converted photons is $\Delta\lambda = (0.20 \pm 0.02)\,\text{nm}$, corresponding to a coherence time $\tau_c = (7.4 \pm 0.8)\,\text{ps}$. These results are in line with what predicted in Bennink's study [28], according to which, in the case of not too tight focusing, the bandwidth is

$$\Delta\lambda = \frac{\lambda^2}{c\left|n'_s - n'_i\right|}\frac{1}{L}, \tag{2.34}$$

where $\lambda = \lambda_s = \lambda_i$ is the photon wavelength, $L$ is the length of the non-linear crystal and $n'_s$ and $n'_i$ are the group indices of the signal and idler photon, defined as $n'_j \equiv c\partial k_j/\partial\omega$. By inserting the parameters of the used non-linear crystal into (2.34), the predicted value of the bandwidth is $\Delta\lambda \simeq 0.19\,\text{nm}$, compatible with the measured value.

Also in the interference pattern of down-converted photons it is possible to notice the beats due to the presence of multiple wavelengths in the pump, as shown in Figure 2.13.

## 2.3.4 Entangled state properties

### Multi-photon pairs

In Section 2.1, the unitary evolution giving the SPDC process has been approximated to its first order term. This is justified in the study of the efficiency of the process, since single-pair production is far the dominant process, but cannot be just neglected in the

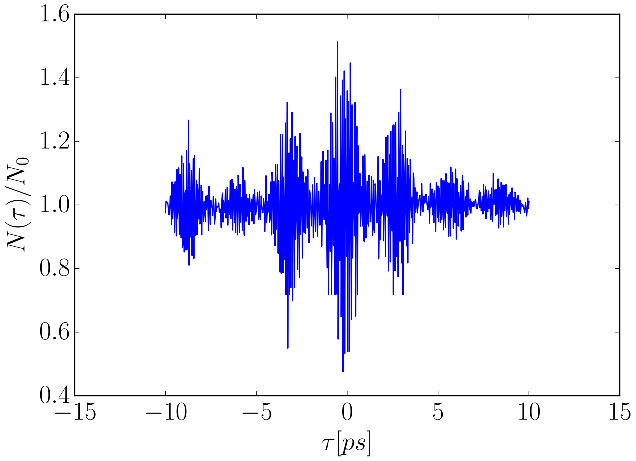

Figure 2.13: Amplitude modulation of the interference pattern due to the presence of multiple pump wavelengths.

quantification of the information leaked to an eventual eavesdropper in a Quantum Key Distribution application, like the one described in Section 3.1.4. The evolution of the state due to the interaction with the crystal, generally described by the unitary operator (2.9), becomes, in the case SPDC is the only second order process giving a considerable contribution,

$$\hat{U} = \exp\left(\xi^* \hat{a}_{\omega_s}\hat{a}_{\omega_i} - \xi\hat{a}^\dagger_{\omega_s}\hat{a}^\dagger_{\omega_i}\right), \tag{2.35}$$

where $\xi$ is a term depending on the parameters of the SPDC interaction [18]. If the pump is filtered out, the Fock state after the interaction has the form

$$|\xi\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}(-1)^n e^{in\theta}(\tanh r)^n \left|n,n\right\rangle_{\omega_s,\omega_i}, \tag{2.36}$$

where $r$ and $\theta$ are the real and imaginary part of the complex parameter $\xi = re^{i\theta}$. The probability of having the production of an $n$-pair state is, therefore,

$$\mathbb{P}(n) = (\cosh r)^2(\tanh r)^{2n}. \tag{2.37}$$

The evaluation of the impact of multi-photon pulses can be made experimentally by inserting Bob's output channel into a Hanbury Brown-Twiss interferometer [41], consisting on a beam-splitter with the two outputs connected to single-photon avalanche photodiodes. Alice's output is directly connected to a single photon detector.

By assuming that the probability $\mathbb{P}(n > 2)$ is negligible (which happens in the case of SPDC, since $r \ll 1$), it is possible to estimate the probability of two-photon emission by comparing the rate of coincidences between the three detectors with the rate of coincidences between Alice's detector and one of the Bob's detectors. This value has been measured to be $\mathbb{P}(n = 2) \sim 3 \cdot 10^{-3}$ in the conditions of Section 3.1.4.

### Output state

There are several ways to measure the output state of the source. The best one is reconstructing the full density matrix of the output state through a series of measurements on the ensemble $\rho_{out}^{\otimes N}$, where $\rho_{out}$ is the density matrix output by the source. This process, called *quantum tomography*, estimates $\rho_{out}$ as the density matrix $\hat{\rho}_{out}$ whose measurement results are closer to the ones obtained experimentally, using the method of maximum likelihood estimation [42]. For two-qubit states, this method requires 16 measurements [42].

The process of quantum tomography, however, requires the use of both half- and quarter-wave plates in order to be performed. A simpler way to validate the produced state is by measuring the visibility of the state in two non-orthogonal basis, such as the $\left\{|H\rangle, |V\rangle\right\}$ and the $\left\{|+\rangle, |-\rangle\right\}$ basis [43, 44]. The visibility of a state of density matrix $\rho$ in a given basis $\left\{|\theta\rangle, |\theta^{\perp}\rangle\right\}$ is defined as

$$V = \left|\frac{\mathbb{P}(+-) + \mathbb{P}(-+) - \mathbb{P}(++) - \mathbb{P}(--)}{\mathbb{P}(+-) + \mathbb{P}(-+) + \mathbb{P}(++) + \mathbb{P}(--)}\right|, \tag{2.38}$$

where

$$\mathbb{P}(ab) = \mathrm{Tr}\left[\rho \, |\theta^a\theta^b\rangle \langle\theta^a\theta^b|\right], \tag{2.39}$$

with $|\theta^+\rangle = |\theta\rangle$ and $|\theta^-\rangle = |\theta^{\perp}\rangle$.

A more precise way to measure the visibility is by fixing the measurement basis on one photon (to some axis $\vec{\theta}$ of the Bloch sphere) and scan the other photon over a great circle of the Bloch sphere passing through $\vec{\theta}$. By doing that procedure for two axes belonging to two mutually unbiased bases (such as the $X$ and the $Z$ axis), it is possible to validate the entanglement of the produced state.

The quality of the output state of the Sagnac source has been validated by measuring the visibility on the two mutually unbiased bases $Z$ and $X$, by fixing the basis of one photon and scanning the other one in the $X$-$Z$ plane of the Bloch sphere, giving the results shown in Figure 2.14. By fitting the experimental data, a visibility of $V_Z = 1.00 \pm 0.01$ and $V_X = 0.985 \pm 0.006$ is obtained.

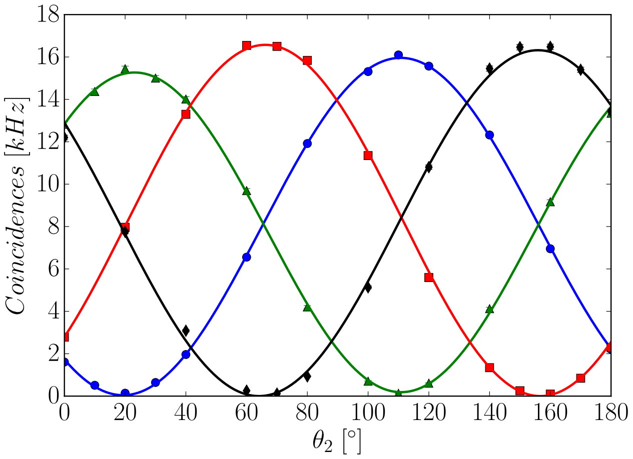

Figure 2.14: Visibility scan changing the value of a polariser at Bob's side, with Alice's polariser at 0° (black diamond), 45° (blue circle), 90° (red square) and 135° (green triangle).

The quality of the state can also be inferred by the analysis of the data from Chapter 3 experiments. Both experiments, indeed, are quite stringent in the quality of the state necessary for their success. So, they can be viewed also as an indirect test of the quality of this entangled source.

# Chapter 3

# Ground experiments

The experimental implementation of quantum information protocols has undergone a great advancement in recent years. The most successful quantum information protocol, Quantum Key Distribution, is already at the commercial stage, with increasing effort into making it more suitable for integration with the existing communication infrastructure, through the development of integrated devices or the study of new protocols. A great input into quantum technologies might be given also by the recent loophole-free violation of Bell's inequality [45–47], that rules out any residual hope to describe reality using a local hidden variable (LHV) model.

Despite these great results, quantum technology is still in its infancy, and the deployment of quantum experiments in a space environment presents a lot of difficulties to overcome. The launch of a small quantum transmitter in the Japanese SOCRATES satellite and the recent launch of the Chinese Micius satellite, completely dedicated to quantum technologies, might demonstrate, in case of success, that the most consolidated quantum protocols are already ready for space implementation. This, however, does not reduce the necessity to test new protocols, or new aspects of older ones, in a ground environment.

This Chapter will show the results, both theoretical and experimental, of the study of some of the key aspects in quantum technology and quantum information in general: Quantum Key Distribution and the study of non-locality through Bell's inequalities.

## 3.1 Quantum Key Distribution

Quantum Key Distribution is the first and probably most successful application of quantum mechanics to the problem of information transmission. Its origin dates back to the early 80s, when Bennett and Brassard proposed a protocol that exploits the indeterminacy principle of quantum systems to allow the sharing of secret bits between two different parties through a public channel. This idea gave great impulse to the field of quantum information, since it demonstrated that the rules of quantum mechanics could give a great advantage over classical mechanics in the treatment of some problems of information theory.

In this Section, the basics of quantum key distribution will be reviewed, from the exigence at the basis of its development to the general security model used to describe it. Then, the novel results of this thesis to the field will be exposed.

### 3.1.1 Cryptography and the key exchange problem

Cryptography, from the Greek *kryptós*, "hidden, secret" and *graphein*, "writing" is the science that studies the techniques of secure communication in the presence of malicious adversaries. This technique is almost as old as civilization.

The oldest text showing a deliberate transformation of the writing is a hieroglyphic inscription on a Egyptian tomb dating back to about 1900 BC [48]. In this case, the aim of the scribe was probably not to hide some information to the reader, but to impart dignity and authority to the inscription. The second ingredient of cryptography, secrecy, comes into play is some later inscriptions[1]. The first examples of using cryptography to protect information is found in some tablets from Mesopotamia [48], showing how this technique goes almost in parallel with writing.

Also in ancient Greece cryptography played an important role, especially in military communication. Among the Spartans, messages were encrypted by writing them into a strip of parchment wrapped around a rod called *skytale*. Once unwrapped, the message could be read only by using a rod with the same diameter as the one used to write it. This is an example of transposition cipher, where the encrypted message (*ciphertext*) is just a permutation of the letters of the original message (*plaintext*). A slightly more sophisticated technique, the so called Caesar's cipher, was used in the Roman era. It was a substitution cipher, where each letter of the plaintext was replaced with a letter some fixed number of position down the alphabet.

Both the skytale and the shift in the Caesar's cipher can be viewed as a first example of *cryptographic keys*, something that is known to the parties that want to communicate and unknown to potential adversaries. Since this "key" must be equal for both communicating parties, these ciphers are examples of *symmetric-key algorithms*.

The birth of cryptanalysis, with the 9th century *Manuscript on Deciphering Cryptographic Messages* by Al-Kindi, changed the situation, with the beginning of a cat-and-mouse game between cryptographers, trying to invent more sophisticated codes, and cryptanalists, trying to break them. Caesar's cipher proved weak against the so called "frequency analysis", consisting in studying the frequency of each letter in the ciphertext and comparing it with the one of the language in which the message was written. Cryptographers answered by proposing more complex substitution schemes, such as the Vigenère cipher (XVI century), which consists of a series of Caesar's ciphers whose shift is given by the key[2]. Despite being considered unbreakable for a large amount of time, this cipher was finally broken during the XIX century.

A modification of this cipher, proposed by Vernam at the beginning of the XX century, became the basis of the *one-time-pad*. In the one-time-pad, the message, seen as a string of bits, is encrypted by performing a XOR operation with a random key. Therefore, if $m = \{m_i\}_{i=1..N}$ is the message and $k = \{k_j\}_{j=1..N}$ the key, the ciphertext is given by

$$c_i = m_i \oplus k_i. \tag{3.1}$$

The ciphertext is then decrypted by XOR-ing it with the same key used for encrypting it, since

$$c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i \oplus (k_i \oplus k_i) = m_i \oplus 0 = m_i. \tag{3.2}$$

In his famous paper, considered the birth of modern information theory, Claude Shannon demonstrated that, if the key is random, secret and at least as long as the message, the one-

[1] Even in this case, however, secrecy was not aimed at the exchange of information between different persons, but rather at giving a sense of arcane and mystery to the inscription.

[2] Assuming CIAO is the key, the first letter of the message is shifted by 3 positions, the second one by 9 positions, and so on up to the 5th letter, where the scheme is repeated.

time-pad is information theoretically secure[3] [1]. Once used, the key must be discarded, since reusing it would indeed give information about the messages. Indeed, given two messages $m_1$, $m_2$ and a common key $k$, the ciphertexts are $c_1 = m_1 \oplus k$ and $c_2 = m_2 \oplus k$. Their XOR is therefore

$$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2, \tag{3.3}$$

which is equal to the XOR of the original messages. The invention of the one-time-pad has shown that the problem of secure communication can be solved, but at the expenses of the secret communication of a key at least as long as the message. The secure communication problem is just shifted from the message to the key.

While in some top secret applications it could be feasible to exchange manually long keys between the parties wishing to communicate, this practice is unfeasible for a widespread usage. For this reason, even after the invention of one-time-pad, cryptography relied on different, less secure, ciphers which required a smaller amount of secret information, easier to manage. This is the reason why XX century cryptography was still based on substitution techniques, even if with ciphers more and more difficult to break.

The great breakthrough in the field has been the development of the so-called *asymmetric-key ciphers*. These ciphers use two different keys, a public key is used to encrypt the messages and a private key is used to decrypt them. A message encrypted with the public key can be decrypted only by someone possessing the private key. These ciphers are based on some mathematical problems, such as prime number factorization or the discrete logarithm, which give functions that are simple to calculate but computationally difficult to invert. Their security is given by the fact that getting the private key from the public one is equivalent to invert these problems.

Asymmetric-key ciphers are at the basis of modern cryptography. The infrastructure upon which all present day secure communication is built is given by a combination of asymmetric ciphers, using to exchange cryptographic keys, and symmetric ones, used to encrypt the communications.

With the development of quantum information, however, this infrastructure is endangered. Indeed, the study of quantum information processing has led to the development of some algorithms, such as the Shor's algorithm [49], which can efficiently invert the problems upon which current asymmetric ciphers are based.

Two different, discording, countermeasures to this threat are currently under investigation. The first one is the development of new, asymmetric-key ciphers based on problems that are hard to invert even for a quantum computer. It has the advantage of being easily integrable with the current network infrastructure, since it would just need the update of the software algorithms used for key exchange, but their security still relies on some assumptions about the computational hardness of some inversion problems. The second approach consists in a total change of the key exchange infrastructure, distributing the key at the physical layer, as happens, for example, in Quantum Key Distribution. This approach has the advantage of a higher security definition, holding also with adversary with infinite computational power, but at the expenses of the requirement of a completely new infrastructure, allowing the exchange of quantum states.

### 3.1.2 General model for Quantum Key Distribution

Among the many models for physical layer key exchange, the most suitable for the study of Quantum Key Distribution is the one built upon the framework of abstract cryptography,

[3] It means that knowing the ciphertext does not gives any information on the message.

proposed by Maurer and Renner in 2011 [50]. This introduction to Quantum Key Distribution will not enter into the details of the model, but will limit to a short presentation of how it can be modeled within this framework (for more details, see [51]).

Quantum Key Distribution is a system that allows two parties, generally called Alice and Bob, to share a secure, random string of bits through an insecure quantum channel and an authenticated classical channel. A *quantum channel* is a *resource* that receives as input a quantum state $\rho$ and outputs another quantum state $\rho'$. The quantum channel is insecure in the sense that it is in full control of the adversary, generally called Eve, that can do whatever she wants with the state in the channel, a situation schematized in Figure 3.1, where Alice's *interface* is represented on the left, Bob's one on the right and Eve's one at the bottom.

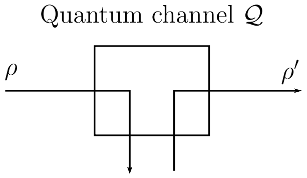

Figure 3.1: Schematic representation of a quantum channel $\mathcal{Q}$. The channel is insecure because the state $\rho$ coming from Alice (on the left) is given to Eve (at the bottom) and then the state $\rho'$ coming from Eve is routed to Bob (on the right).

The other resource necessary for Quantum Key Distribution is an *authenticated channel*, represented as in Figure 3.2. The authenticated channel is a classical channel through

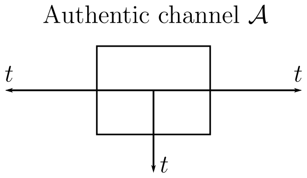

Figure 3.2: Schematic representation of the authenticated channel (or authentic channel).

which the information goes unaltered from Alice to Bob. An eavesdropper (Eve) can see all the information flowing, but she cannot disguise her messages as Alice's or Bob's ones. The presence of the authenticated channel is fundamental to prevent man-in-the-middle (MitM) attacks, where Eve puts herself in the middle of the transmission line, exchanging two different keys with Alice and Bob (pretending to be the legitimate interlocutor) and thus completely breaking the security of future transmissions. Using these two resources, it is possible to construct the Quantum Key Distribution *protocol* $(\pi_A^{qkd}, \pi_B^{qkd})$[4]. There exist three main families of protocols: *discrete-variable* (DV), *continuous-variable* (CV) and *distributed-phase-reference* (DPR) protocols [52]. The first two families encode the information in discrete and continuous variables respectively, as described in Section 1.5.2, while the third family uses discrete variables to encode key bits and exploits the coherence of subsequent pulses to monitor channel disturbance and detect the presence of Eve [53]. Since CV and DPR protocols are out of the scope of this thesis, they will not be mentioned anymore.

[4] To be precise, Quantum Key Distribution requires also a third resource, a Random Number Generator (RNG). Security proofs, however, tend to assume that such device exists and that it provides no information to Eve.

The general DV QKD protocol can be schematized as in Figure 3.3, where the interaction of Eve with the authenticated channel has been removed to preserve the clarity of the scheme.

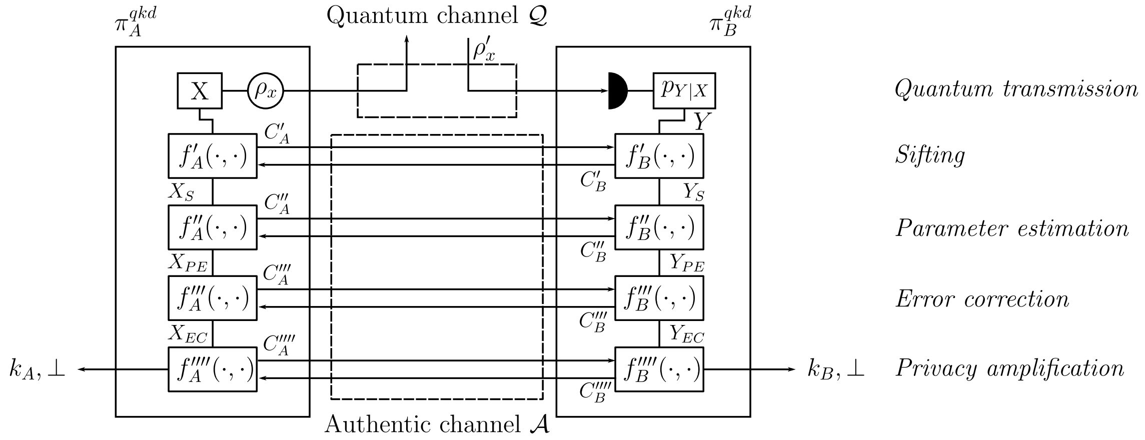

Figure 3.3: Scheme of a general Quantum Key Distribution protocol. $X$ is a random variable provided by a RNG at Alice's side.

It consists of a series of steps:

1. **Quantum transmission**
   During this phase, Alice and Bob exchange quantum states through the quantum channel. In *prepare-and-measurement* (PaM) schemes, the state is explicitly prepared at Alice's side according to some random variable $X$ (which is issued by a RNG). In *entanglement-based* (EB) schemes, on the other hand, the quantum state flowing through the channel is an entangled state, produced somewhere between Alice and Bob and arriving to both of them. If the entangled source is at Alice's side, EB schemes are totally equivalent to PaM ones, since a measurement at Alice's side corresponds to a preparation at Bob's side[5]. In this case, however, the variable $X$ is partially determined by the results of the measurement at Alice's side. In both schemes, Bob's measurement gives a random variable $Y$, dependent on the quantum state sent through the channel and thus partially correlated to Alice's random variable $X$.

2. **Sifting**
   During the sifting phase, Alice and Bob discard all the events where their random variables $X$ and $Y$ are not correlated. This phase is highly dependent on the actual QKD protocol.

3. **Parameter estimation**
   During this phase, Alice and Bob estimate the parameters of the channel, in particular the quantum bit error rate (QBER), that will be used in the estimation of the information leaked to Eve during the quantum transmission phase. If that information is too high (which is equivalent to have the QBER higher than a certain threshold, dependent on the protocol), it is impossible to distill a secret key, therefore the protocol aborts returning $\perp$ to both Alice and Bob.

[5] If the source is not safe in Alice's laboratory, Eve must be assumed to have full control of the source and the two schemes are no longer equivalent. It has been proven, however, under some particular condition, the equivalence still holds [52].

Parameter estimation is usually performed by exchanging a random subset of all the exchanged symbols and calculating the bit error rate on that subset, but some protocols allow a direct estimation of the QBER from the results of the sifting phase.

4. **Error correction**
A fundamental requirement of each key exchange protocol is *correctness*, meaning that the probability that the protocol returns two different keys to Alice and Bob is negligible. A protocol is said to be $\varepsilon_{corr}$-*correct* if

$$\mathbb{P}\left[k_A \neq k_B\right] \leq \varepsilon_{corr}. \tag{3.4}$$

Error estimation consists of an interactive protocol that, taking as input the random variables $X_{PE}$ and $Y_{PE}$, output by the parameter estimation phase, returns two random variables $X_{EC} = f_A'''(X_{PE}, C_B''')$ and $Y_{EC} = f'''(Y_{PE}, C_A''')$ such that

$$\mathbb{P}\left[X_{PE} \neq Y_{PE}\right] \leq \varepsilon_{corr}, \tag{3.5}$$

where $C_A'''$ and $C_B'''$ is the classical information exchanged through the authentic channel during the protocol.

5. **Privacy amplification**
At the end of the error correction phase, Alice and Bob share two random variables that are equal with probability higher than $1 - \varepsilon_{corr}$. However, the other fundamental requirement of a key exchange protocol, *secrecy*, is still lacking. Indeed, Eve still possesses all the information coming from her tampering with the transmitted quantum states, together with the information acquired by sniffing the authenticated channel during the preceding steps of the protocol. In order to meet the secrecy requirement, it is necessary to remove Eve's information from $X_{EC}$ and $Y_{EC}$, ending up with two shorter keys $k_A$ and $k_B$, which are secret to Eve. The security of the resulting key is usually evaluated by using a security parameter $\varepsilon_{sec}$, whose meaning will be briefly reviewed in next Section.

### Composable definition of security

What makes Quantum Key Distribution appalling is the fact that it claims to offer *unconditional security*, i.e., it is secure against adversaries with unbounded computational power. Its security is a direct consequence of the postulates of Quantum Mechanics, that state that the information acquired from a quantum state is proportional to the disturbance on the observed state (*information-disturbance trade-off* [54]) and that quantum states cannot be cloned [55].

These considerations, however, are not enough to prove the security of Quantum Key Distribution as a cryptographic protocol. This requires the establishment of a security definition and the proof that the protocol meets it. This security definition must be such that the protocol can be composed with any other cryptographic protocol without losing its security, a property called *composability*.

In the framework of Abstract Cryptography, the notion of security is given by the indistinguishability between the real QKD protocol and an ideal system that simulates it. Since a complete treatment of the matter if far beyond the scope of this thesis, this Section will just give some hints on the subject, referring to the literature [50, 51] for a more complete exposition.

In this theoretical model, a real protocol can be viewed as a box (*resource*) with some interfaces to the external world (for key exchange schemes, the interfaces correspond to Alice, Bob and Eve). The task that the protocol is required to perform is called *functionality.* The ideal system the real protocol is compared with is a box with its same interfaces, implementing the ideal functionality. The notion of security is captured by the *distinguisher*, who is given access to all interfaces of a black box with either the real protocol or the ideal system inside. If the distinguisher cannot, except with probability $\varepsilon$, distinguish the real protocol from the ideal one, the protocol is said to be $\varepsilon$-secure. This security criterion respects the composability requirement, meaning that, by composing an $\varepsilon$-secure with an $\varepsilon'$-secure protocol, the resulting one is $(\varepsilon + \varepsilon')$-secure [50].

In the key exchange problem, the functionality is the distribution of a secret key between Alice and Bob, and an ideal system implementing it is just a box that outputs the same random string to both Alice's and Bob's interfaces and some other, uncorrelated information to Eve's interface. Therefore, a general key exchange protocol is required to be $\varepsilon_{corr}$*-correct* $(\mathbb{P}(k_A \neq k_B) \leq \varepsilon_{corr})$ and $\varepsilon_{sec}$*-secure*, where this last condition is dependent on the chosen security definition. If these two conditions hold, it can be proven that the protocol is $\varepsilon$-secure, with $\varepsilon = \varepsilon_{corr} + \varepsilon_{sec}$.

In the classical key exchange problem, the notion of security is captured by the mutual information between the key and a random variable $Z$ representing all the information that Eve has acquired during the execution of the protocol. As shown in Figure 3.4 [53, 56], by starting from the joint probability distribution $\mathbb{P}_{XYZ}$ between Alice, Bob and Eve, it is possible, using post-processing, to extract an $\varepsilon$-secure key [57]. It is evident that

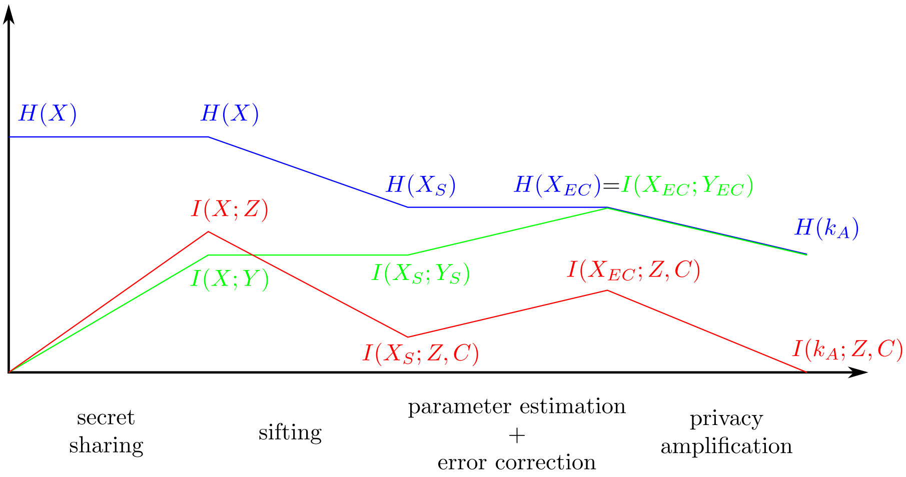

Figure 3.4: Information measures in the classical key exchange problem. $H(\cdot)$ is the entropy and $I(\cdot,\cdot)$ is the mutual information.

the general QKD protocol described in Section 3.1.2 is a realization of the key exchange protocol shown in Figure 3.4. However, it has the crucial difference that the secret sharing phase ends up with a joint quantum state $\rho_{ABE}$ (which is, in general, entangled), instead of the classical joint probability distribution $\mathbb{P}_{XYZ}$. If Eve were forced to measure the state $\rho_x$ during the quantum transmission phase, the two schemes would be completely equivalent, since she would end up with a random variable $Z$ given by the result of her measurements. But, since unconditional security requires to assume that Eve has unlimited resources, it is necessary to take into account also the hypothesis that she has a quantum memory in which she can keep her quantum state $\rho_x$ until needed. In that case, therefore, the mutual information must be replaced with the maximum mutual information that Eve can obtain by applying her best measurement strategy, the *accessible information*

$$I_{acc}(k_A;E) = \max_{\mathcal{M}} I(k_A;\mathcal{M}(E)), \tag{3.6}$$

where the maximum is taken over all possible Eve's measurement strategies $\mathcal{M}(E)$. By taking $I_{acc}(k_A;E) \leq \varepsilon$, a secrecy definition similar to the one used in classical key exchange is recovered. However, this is not enough to obtain $\varepsilon_{sec}$ secrecy of the protocol. Indeed, differently from classical mutual information, the accessible information is *lockable* [58], meaning that, given a key $k_a = k_{A1}k_{A2}$ with $I_{acc}(k_A;E) \leq \varepsilon$, and a joint quantum state $\rho_{k_{A1}K_{A2}E}$, it is possible that

$$I_{acc}(k_A;Ek_{A1}) > H(k_{A1}) + 1. \tag{3.7}$$

By knowing part of the key (as happens in the *known-plaintext attack*), Eve can break the security of the rest of the key.

Therefore, a new security definition is necessary for Quantum Key Distribution. Current security definitions are based on the *trace distance* between the quantum state output by the real protocol $\rho_{ABE}$ with the one that must be shared by the ideal system implementing the key exchange functionality $\tau_{AB} \otimes \rho_E$, where $\tau_{AB} = \sum_{k\in\mathcal{K}} 1/|\mathcal{K}|\, |k,k\rangle \langle k,k|$ is the completely mixed state over the space of all possible keys $\mathcal{K}$ [58, 59]. With this criterion, a protocol is said to be $\varepsilon_{sec}$-secret if

$$\|\rho_{ABE} - \tau_{AB} \otimes \rho_E\|_1 \leq \varepsilon_{sec}, \tag{3.8}$$

where $\|\cdot\|_1$ is the trace norm [59]. Since the trace distance don't increase when appending an additional quantum system, or when applying an arbitrary quantum operation, it provides a composable security definition [60].

### Assumptions of the security model

As specified in Section 3.1.2, the appeal of Quantum Key Distribution lies in its providing an unconditionally secure way of exchanging a key between two parties, Alice and Bob. The claim of unconditional security, however, must not be confused with a claim of "absolute security", which is something that does not exist [52]. The meaning of the security provided by Quantum Key Distribution is well explicated in a short paper by Scarani an Kurtsiefer [61], where they compare it with a key exchange mechanism implemented by giving a CD filled with a random key to a trusted courier Charlie, who brings it from Alice to Bob. The security of this system requires that

(i) the key that Alice's computer writes to the CD is truly random,

(ii) Alice's and Bob's computer are not leaking information in any way,

(iii) Charlie is honest at the moment of receiving the key from Alice,

(iv) during his travel from Alice to Bob, Charlie does not leak information, neither intentionally nor inadvertently.

Condition (i) is a prerequisite of any key exchange protocol, both classical and quantum. Moreover, Quantum Key Distribution does not guarantee conditions (ii) and (iii) more than any other classical key distribution protocol, since (ii) the information used in Alice's and Bob's devices is classical, and (iii) it does not guarantee the absence of side-channel information in the quantum system used for carrying it. What it does guarantee is that, once the information travels as a qubit from Alice to Bob, it cannot leak to an attacker in any possible way. Clearly, since the security of QKD is based on a precise behavioural model of the information carriers, its security requires that this model, namely Quantum Mechanics, is valid.

Given all these assumptions, the general Quantum Key Distribution protocol of Section 3.1.2 uses an insecure quantum channel and an authenticated classical channel to build up an $\varepsilon$-secure key exchange system. In particular, the most critical assumption is the adherence of the physical systems used in the quantum transmission part to the qubit preparation and detection model.

The qubit preparation requires a system that creates one single photon in a desired optical mode. However, the emission of more than one photon is a security issue, because Eve could just non-destructively measure the number of photons in each pulse and, if there are more than one photon, forward a single photon to Bob, keeping all the other ones in a quantum memory. In that case, she would just have to wait for the sifting phase, taking advantage of the sifting information to choose her measurements. This attack, called photon number splitting (PNS) attack [62], is a major problem in practical realizations of QKD protocols, since all systems used for qubit preparation have a non-negligible probability of emitting multi-photon pulses. Possible countermeasures to this problem are given by taking into account this flaw in the security proof, by using the “tagging” technique [63], or finding new protocols that are not affected by this issue, like those exploiting decoy states [64–66]. Section 3.1.3 will be devoted to the study of this problem when an asymmetric heralded source [67] is used in a practical QKD implementation. This problem, of crucial importance in prepare-and-measurement schemes, is less critical for entanglement-based ones, like the one described in Section 3.1.4, since the incidence of multi-photon events in entangled pairs is much lower than in the other kind of sources. Other problems in qubit preparations can be given by some phase-dependence between the systems carrying successive qubits [52, 61], or by the presence of side-channel information, such as, for example, the eventual dependence of other degrees of freedom of the electromagnetic field on the transmitted qubit.

The other critical problem is given by the detection system. The first issue is the requirement that the detection system “squashes” all the complexity of the electromagnetic field into a qubit, something that has been demonstrated for many implementations of QKD [68–70]. The other issue, which has been already exploited for the experimental demonstration of hacking attacks on real quantum devices, is given by some properties of Silicon avalanche photodiodes (APDs) under high illumination conditions [71–74], or by their vulnerability against other side-channel attacks due to back-flash [75] or to different timings of the photo-detection event [76, 77]. While fundamental for the implementation of a real QKD system, detection issues will not be further investigated through this thesis.

### 3.1.3 Heralded single-photon sources

As stated in Section 3.1.2, one of the major problems of practical Quantum Key Distribution is due to the fact that security requires the transmission of a single quantum state from Alice to Bob, since multi-photon events can leak all the information to Eve through the PNS attack. Most practical prepare-and-measurement Quantum Key Distribution implementations use as single photon source an attenuated, pulsed laser, which will be also called weak coherent source (WCS). The output of a single mode laser, generally, is described by a coherent state of the field,

$$|\sqrt{\mu}e^{i\theta}\rangle \equiv |\alpha\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, \tag{3.9}$$

where $|n\rangle$ is the n-photon Fock state, and $\mu = |\alpha|^2$ is the mean photon number per pulse [52]. Since in discrete variable protocols a phase reference is not accessible, the state is described by a mixture

$$\rho_\mu = \int_0^{2\pi}\frac{d\theta}{2\pi}\,|\alpha\rangle\,\langle\alpha| = \sum_{n=0}^{\infty}\mathbb{P}(n|\mu)\,|n\rangle\,\langle n|\,, \tag{3.10}$$

so the output state is completely determined by the photon statistics $\mathbb{P}(n|\mu)$, which for the attenuated laser is

$$\mathbb{P}(n|\mu) = e^{-\mu}\frac{\mu^n}{n!}. \tag{3.11}$$

The probability of single-photon pulse is $\mathbb{P}(1|\mu) = \mu e^{-\mu} \simeq \mu$, while the probability of multi-photon pulses is $\mathbb{P}(n > 1|\mu) = 1 - \mathbb{P}(0|\mu) - \mathbb{P}(1|\mu) = 1 - e^{-\mu} - \mu e^{-\mu} \simeq \mu^2/2$. Therefore, it is necessary to find a trade-off between the maximization of single-photon pulses and the minimization of multi-photon pulses.

These limitations have pushed the research onto sources that better approximate a single-photon source. One possible implementation of such sources is based on localized quantum structures, such as color centers [78], quantum dots [79, 80], atoms [81], or ions [82] in a cavity. These sources, however, require expensive equipment for their operation and have limitations both in wavelength and bandwidth selection [83]. Another family of single photon sources exploits the phenomenon of Spontaneous Parametric Down Conversion (SPDC), already described in Section 2.1. Since photons are always produced in pairs signal-idler, it is possible to use the idler photon to "herald" the presence of the signal photon, giving the so-called heralded source (HS). However, if the duration of the pulse is much greater than the reciprocal of the phase-matching bandwidth, the statistics of the pairs is still poissonian [83], and this source does not present advantages over the WCS. Despite that, these sources allow the use of some strategies to enhance their single-photon character that are not possible with pulsed lasers. One such strategy consists of using a single HS with a photon number resolving detector on the idler channel in order to select the pulses where only one photon is detected [84]. An alternative strategy uses parallel HS units and post-selection. Each HS unit is pumped with a low power laser, in order to reduce the incidence of multi-photon pulses, while the presence of multiple HS units is exploited to keep the rate of single-photon pulses at an acceptable level.

The first proposal making use of parallel HS units and post-selection comes from an article by Migdall *et al.* [85], where the HS units are all linked to an $m$-to-1 optical switch triggered by a detector on the idler photon of each HS unit. Migdall *et al.* analyzed this scheme, which from now on will be referred as MHPS (multiple heralded-sources with post-selection), by taking into account also the finite efficiency of the heralding detectors but, as pointed out by Shapiro and Wong [83], they did not address the problem of the low efficiency of $m$-to-1 optical switches, a serious limitation of such scheme.

This issue is considered by Shapiro and Wong, who propose a new scheme that substitutes the single optical switch with a series of $m - 1$ binary photon switches in a symmetric tree structure [83] (SMHPS), shown in Figure 3.5. A recent reanalysis of the performances of this source has shown that, in the case of imperfect devices, this scheme suffers a scalability issue, with a decrease in one photon probability when increasing the

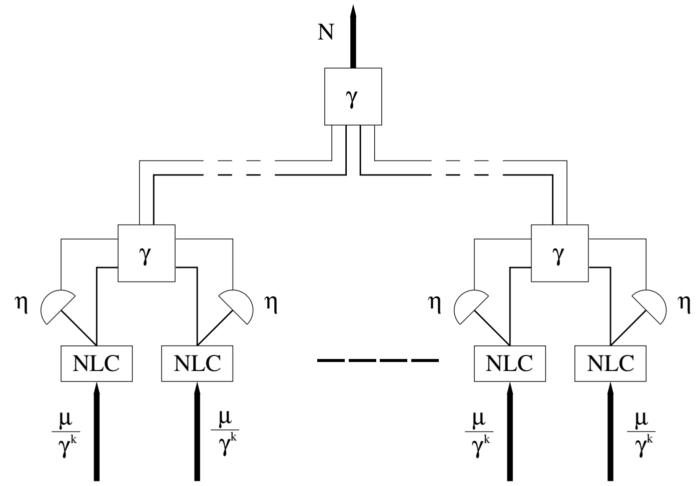

Figure 3.5: Schematics of the SMHPS [83]. Each non-linear crystal (NLC) is fed with pulses such that the mean number of generated pairs per pulse is $\mu/\gamma^k$, with $k = \log_2 m$ and $\gamma$ the transmittance of 2-to-1 optical switches. The idler of each NLC is fed into a detector with quantum efficiency $\eta$.

number of crystals [67]. To overcome this problem, a new, asymmetric scheme (AMHPS) is proposed [67]. In this scheme, the HS units are linked together in the chained network showed in Figure 3.6.

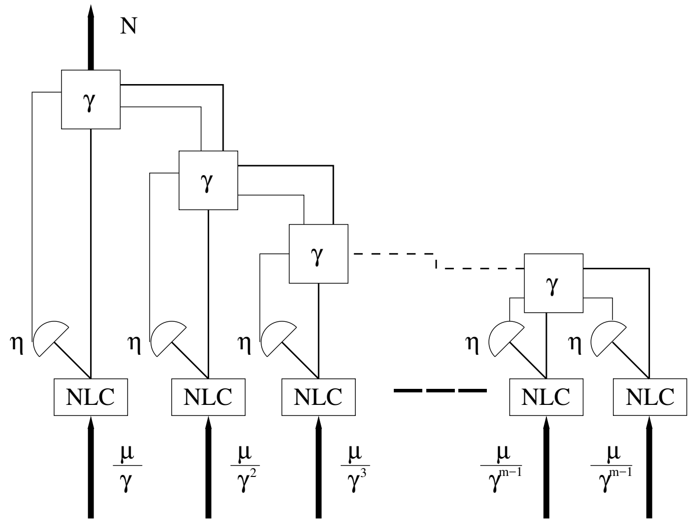

Figure 3.6: Schematics of the AMHPS [67]. Each non-linear crystal (NLC) is pumped with a different intensity in order to compensate the different number of traversed 2-to-1 optical switches, each characterized by its trasmittance $\gamma$. The idler of each NLC is fed into a detector with quantum efficiency $\eta$.

In this Section, the performance of the different schemes is studied in a practical Quantum Key Distribution protocol, taking into account channel losses and imperfect detectors [86]. The analysis will use the Bennett-Brassard 1984 (BB84) protocol [87] in a generic discrete variable scheme, and will cover also the case of active [66] and passive decoy [88, 89].

### The quantum transmission model

*The protocol* - In the quantum transmission phase of the BB84 protocol, the information is encoded into two mutually unbiased bases, like the computational $Z = \{|0\rangle, |1\rangle\}$ and the diagonal $X = \{|+\rangle, |-\rangle\}$ basis. For each basis, the first symbol encode the 0 and the second one the 1. Alice uses her Quantum Random Number Generator (QRNG) to generate two strings of bits, one used to decide the bit of information to send, the other one the basis in which to encode it. The two bases must not necessarily be chosen with the same probability, but Alice and Bob could publicly decide to use one basis more often that the other one, a scheme called *efficient BB84* [90]. Bob measures the incoming qubits choosing at random the measurement basis $X$ or $Z$, and registers the corresponding outcome of the measurement.

*The source* - Similarly to what happens in (3.10), also heralded sources are completely characterized by their output statistics.
The MHPS consists of an array of $m$ HS units, simultaneously pumped with a laser pulse with intensity such that the mean number of generated pairs per pulse is $\mu$ [85]. In the ideal case of perfect detector and optical switch, a post-selection mechanism that selects one of the channels whose detector has fired gives the output statistics

$$\mathbb{P}^M(n|\mu; m) = \frac{\mu^n}{n!} e^{-\mu} \frac{1 - e^{-m\mu}}{1 - e^{-\mu}} (1 - \delta_n) + \delta_n e^{-m\mu}, \tag{3.12}$$

where $\delta_n$ is the Kronecker $\delta$ ($\delta_0 = 1$ and $\delta_{n>0} = 0$) [67].
In the SMHPS, the general $m$-to-1 switch is replaced by a tree of 2-to-1 optical switches of transmittance $\gamma$. The tree scheme requires the number of HS units $m$ to be a power of 2. The idler detector has quantum efficiency $\eta$ and negligible dark count probability. Since the photons produced by each HS unit pass $k = \log_2 m$ switches before reaching the output, the crystals are pumped with an intensity such that the mean number of generated pairs per pulse is $\mu/\gamma^k$ The post-selection mechanism in each optical switch gives priority to the left HS unit and, in case no HS unit triggers, always outputs the left one [67]. The photon statistics at the output is

$$\begin{aligned}\mathbb{P}^S(n|\mu; m, \eta, \gamma) = {} & \frac{(1-\eta)\mu e^{-(1-\eta)\mu}}{n!} e^{-\eta\mu\frac{2^k}{\gamma^k}} \\ & + \frac{\mu^n e^{-\mu}}{n!} \frac{1 - (1-\eta)^n e^{-\eta(\frac{1}{\gamma^k}-1)\mu}}{1 - e^{-\eta\frac{\mu}{\gamma^k}}} (1 - e^{-\eta\mu\frac{2^k}{\gamma^k}}). \end{aligned} \tag{3.13}$$

In the AMHPS, the $m$ HS units, are arranged in a chained scheme, with the route to output crossing a different number of optical switches for each NLC. Therefore, each HS unit must be pumped with an intensity such that the mean number of generated pairs per pulse is $\mu/\gamma^{k_i}$, with

$$k_i = \begin{cases} i & i \leq m-1 \\ m-1 & i = m, \end{cases} \tag{3.14}$$

and a series of delay lines must be introduced in order to compensate the longer transmission time of the rightmost HS units. Like in the SMHPS, the post-selection mechanism gives priority to the left HS and, if none triggers, outputs the left one. Also in this case, the idler detector has quantum efficiency $\eta$ and negligible dark counts. The statistics at the output is

$$\begin{aligned}\mathbb{P}^{A}(n|\mu;m,\eta,\gamma) = {} & \frac{[(1-\eta)\mu]e^{-(1-\eta)\mu}}{n!}e^{-\eta\mu\frac{(2-\gamma)\gamma^{1-m}-1}{1-\gamma}} \\ & + \frac{\mu^{n}e^{-\mu}}{n!}\sum_{i=1}^{m} e^{-\eta\mu\frac{\gamma^{1-i}-1}{1-\gamma}}[1-(1-\eta)^{n}e^{\eta\mu}e^{-\frac{\eta\mu}{\gamma^{k_i}}}]. \qquad (3.15)\end{aligned}$$

For $\gamma \to 1$, the scheme used in the switching network is no longer significant, therefore the output statistics of the SMHPS and the AMHPS coincide. If the heralding efficiency $\eta \to 1$ as well, the two architectures become equivalent to the ideal MHPS.

*Decoy states* - The decoy state technique is a modification of the quantum transmission phase introduced to counteract the PNS attack [65]. It consists of randomly varying the source statistics, so that Eve can no longer adapt her attack to Alice's state. Indeed, after the transmission, Alice communicates Bob the statistics she used for every pulse, allowing them to estimate the channel parameters conditioned on that knowledge. There exist two different decoy state technique, active and passive decoy.

- *Active decoy* - In this technique, Alice chooses the output statistics by using a random number generator and (typically) a variable attenuator after the source. In principle, she can choose an arbitrary number of decoy states, however, it has been shown that just using the vacuum and a weak decoy state gives tight bounds on the relevant parameters [66].

- *Passive decoy* - In the passive decoy technique, the source statistics is not under Alice's direct control, but is conditioned on some random event at Alice's side. A typical example consists of an attenuated coherent state passing through a 50 : 50 beam-splitter (BS) with a single-photon detector at the reflected output: the photon statistics at the transmitting output of the BS changes when Alice detects or not a photon. In the heralded sources, the two statistics are $\mathbb{P}^{(c)}(n)$ and $\mathbb{P}^{(nc)}(n)$, which are conditioned on at least one detector or no detector clicking, respectively. Since the post-selection mechanism outputs the first HS in the case of no detector firing, the statistics $\mathbb{P}^{(nc)}(n)$ is not trivial.

*The channel* - The model used for the quantum channel is a depolarizing lossy channel (DLC), characterized by transmittance $t = 10^{-L/10}$, with $L$ the loss level in decibel, and a depolarization effect with visibility $V$, that incorporates also alignment and stability issues.

*The receiver* - The receiver consists of an optical apparatus, with transmittance $t_B$, and two single-photon threshold detectors, described within the detection model of Section 1.5.2 and characterized by detection efficiency $\eta_B$ and dark count probability $p_d$.

### Classical post-processing

*The sifting* - In the sifting phase, Alice and Bob publicly announce the measurement basis chosen for each qubit, discarding all those events for which the bases do not coincide. They remain with a fraction $p_{sift}$ of the original events, which is $p_{sift} = 0.5$ for the standard BB84 protocol, where both bases are chosen with the same probability, and can be increased up to $p_{sift} \sim 1$ for the efficient BB84. Since this fraction is only dependent on the common measurement strategy and not on the kind of source, $p_{sift}$ is not included in the secure key fraction evaluation.

*Parameter estimation* - In a real QKD protocol, parameter estimation is the phase in which Alice and Bob exchange a randomly chosen subset of the shared symbols in order to evaluate the *quantum bit-error rate* (QBER) $E$, defined as the error probability in Bob's detection events, from which the information leaked to Eve can be estimated. The performance of a protocol, however, depends also on another parameter, the *gain* $Q$, which is defined as the probability that a pulse gives a click in Bob's measurement apparatus. In QKD experiments, this parameters can be estimated by comparing the pulse rate of the source with the rate of detected events. In the theoretical study of this Section, however, these parameters must be estimated from the quantum transmission model.
The gain is defined as

$$Q = \sum_{n=0}^{\infty} Y_n \mathbb{P}(n), \tag{3.16}$$

where $\mathbb{P}(n)$ is the probability of having $n$ photons in a pulse and $Y_n$ is the yield of an $n$-photon signal, i.e. the conditional probability of a detection event at Bob's side given that Alice sends $n$ photons. Assuming independence between signal and background, the yield of an $n$-photon pulse for a DLC can be predicted to be

$$\widetilde{Y}_n = \widetilde{Y}_0 + \eta_n - \widetilde{Y}_0 \eta_n \simeq \widetilde{Y}_0 + \eta_n, \tag{3.17}$$

where $Y_0$ is the probability of a dark count event, which is $\widetilde{Y}_0 \simeq 2p_d$ in the case of two independent detectors and small dark count probability, and

$$\eta_n = 1 - (1 - \eta_D t_B t)^n \tag{3.18}$$

is the probability that a detector clicks when an $n$-photon signal is sent, under the assumption that the effects of the channels on each photon of a pulse are independent. The parameters indicated with a tilde are those predicted by the quantum transmission model used. The negative term, coming from the fact that real detection events and dark counts are not mutually exclusive, can be neglected, since $Y_0 \ll 1$.
The QBER is defined as

$$E = \frac{1}{Q} \sum_{n=0}^{\infty} e_n Y_n \mathbb{P}(n), \tag{3.19}$$

where $e_n$ is the $n$-photon error rate, i.e., the probability of an error when Alice sends an $n$-photon state. For a DLC the $n$-photon error rate can be predicted to be

$$\widetilde{e}_n = \frac{\widetilde{e}_0 \widetilde{Y}_0 + \widetilde{e}_d \eta_n}{\widetilde{Y}_n}, \tag{3.20}$$

where $\widetilde{e}_0 = \frac{1}{2}$ is the error probability of a dark count event, which is assumed to be random, and $\widetilde{e}_d = \frac{1-V}{2}$ is the probability that a photon hits the wrong detector.

*Error correction* - Error correction consists in a protocol that is run by Alice and Bob in order to correct the errors between the respective sifted keys $X_{PE}$ and $Y_{PE}$, giving in the end an equal key with probability larger that $1 - \varepsilon_{corr}$. This protocol, however, requires Alice and Bob to exchange some information about their key, information that must be removed in the subsequent privacy amplification step. The error correction phase leaks a fraction of bits that can be estimated as $f_{EC} h(E)$, where $f_{EC}$ is the efficiency of the error correction protocol used and $h(x)$ is the binary Shannon entropy [52, 63].

*Privacy amplification* - In the privacy amplification phase, Alice and Bob remove all the information leaked to Eve during the preceding steps of the protocol. This quantity determines the secret key rate $R$, defined as the fraction of sifted pulses that produce a secret key [52]. Since it is highly dependent on the source statistics, it is used to determine the performance of the different configurations. It also depends on whether decoy states are used or not.

- **BB84 without decoy states -** In the standard BB84 (without decoy state), the only way to deal with multi-photon pulses in by using the "tagging" technique [63]. In the asymptotic limit of infinite key, the achievable key rate is

  $$R = Q\left\{(1-\Delta)\left[1-h\left(\frac{E}{1-\Delta}\right)\right] - f_{EC}h\left(E\right)\right\}, \tag{3.21}$$

  where $\Delta$ is the fraction of "tagged" photons (i.e., the multi-photon rate), defined as

  $$\Delta = \frac{1-\mathbb{P}(0)-\mathbb{P}(1)}{Q}, \tag{3.22}$$

  $f_{EC}$ is the error correction efficiency and $h(x)$ is the binary Shannon entropy [52, 63]. For true single photon sources $\Delta = 0$ and the secret key rate is written as $R = Q[1-h(E)-f_{EC}h(E)]$: the correction term $1-\Delta$ in (3.21), indeed, takes into account the possible PNS attack on the tagged pulses.

- **BB84 with active decoy -** In the case of active decoy, it is possible to make the simplifying assumption that the parameters are determined exactly [52]. In that case, the secret key rate, in the asymptotic limit of infinite key, is

  $$R = \mathbb{P}(0)Y_0 + \mathbb{P}(1)Y_1[1-h(e_1)] - Qf_{EC}h(E), \tag{3.23}$$

  where $\mathbb{P}(0)$ and $\mathbb{P}(1)$ are given by the source statistics in the signal state and the parameters $e_1$, $Y_0$ and $Y_1$ are the channel parameters estimated using decoy states [66, 91].

- **BB84 with passive decoy -** In the passive decoy state, the relative incidence of the two statistics is not under Alice's control. Therefore, it is not possible to choose one statistics as predominant, and it is convenient to extract the key separately from the two different statistics $\mathbb{P}^{(c)}(n)$ and $\mathbb{P}^{(nc)}(n)$. In this case, the key rate is

  $$R = \mathbb{P}^{(c)}R^c + \mathbb{P}^{(nc)}R^{nc}, \tag{3.24}$$

  where $R^c$ and $R^{nc}$ are the key rate for, respectively, the case of at least one detector and no detector clicking. The key rate is, in the limit of infinite key,

  $$R^\xi = \mathbb{P}^{(\xi)}(0)Y_0^L + \mathbb{P}^{(\xi)}(1)Y_1^L[1-h(e_1^U)] - Q^\xi f_{EC}h(E^\xi), \tag{3.25}$$

  where $\xi \in \{c, nc\}$, $Q^\xi$ and $E^\xi$ are the parameters estimated from the pulses in the corresponding statistics and $Y_0^L$, $Y_1^L$, $e_1^U$ are the lower (L) and upper (U) bounds for the parameters estimated from $\{Q^c, E^c, Q^{nc}, E^{nc}\}$ and the known source statistics. The explicit formulas for parameter estimation, derived from [89], are given in Appendix B in Eqs. (B.10), (B.13) and (B.19).

### Simulation results

The performance of the SMHPS and the AMHPS is evaluated for different values of the number $m$ of HS units by numerically optimizing the $\mu$ parameter of the source in order to maximize the secret key rate.

The simulation assumes the source to be inserted into a fiber-based QKD system [52]. The source is assumed to have an idler detector with $\eta = 0.7$ and negligible dark counts, and optical switches with transmittance $\gamma = 0.5$ [67]. The channel is characterized by a visibility $V = 0.99$ and losses ranging from 0 to 55 dB, which corresponds to a distance of 275 km if we consider the typical fibre attenuation of $\alpha = 0.2\,\text{dB/km}$. Bob's apparatus has optical transmittance $t_B = 1$ and detectors with quantum efficiency $\eta_B = 0.25$ and dark count probability $p_d = 2 \cdot 10^{-7}$, corresponding to the state-of-the-art of infrared semiconductor single photon detectors [92]. The efficiency of the error correction code is $f_{EC} = 1.05$ [93].

All the simulated key rates are compared with those obtained using a weak coherent source (WCS), both with and without active decoy. When dealing with the passive scheme, the comparison is extended to the WCS with one decoy [66], where also the inefficiencies in parameter estimation are taken into account. All schemes are also compared with an ideal single-photon source, giving an upper bound for the rate attainable in a given configuration.

- **BB84 without decoy state -** The maximum key rate that this source architecture can obtain is the one given by the ideal MHPS, shown in Figure 3.7. The rate increases with the number of HS units and approaches the single-photon case for $m = 128$, in the low loss regime. Indeed, for $m \to \infty$, $\Delta = O(\mu)$ and $Q \simeq 1$, approximating the single-photon case for $\mu \ll 1$. When the losses increase, however, the contribution of multi-photon pulses increases and the source shows the same behaviour as the WCS. This had been already observed by Waks *et al.* [94], with the difference that, for low $m$, not only is the fraction of multi-photon pulses higher, determining the lower maximum tolerable loss level, but also the incidence of pulses with zero photons is stronger, determining the lower key rate at $L = 0\,\text{dB}$. This limitation is proper of the multiple-crystal architecture itself.

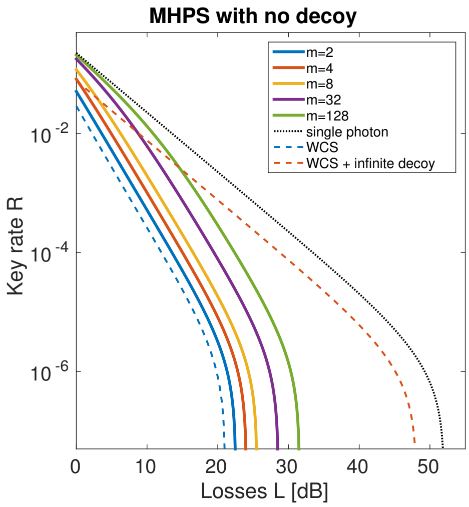

Figure 3.7: Key rate for the MHPS architecture as a function of channel losses.

The secret key rate of the SMHPS and of the AMHPS with finite efficiency detectors and switches is shown in Figure 3.8. In both architectures, the low switch transmittance requires a mean number of generated pairs per pulse higher that the MHPS, therefore increasing also the incidence of multi-photon, "tagged" pulses. In the SMHPS, the number of crossed switches scales as $k = \log_2 m$, therefore, while for few HS units the key rate increases wit $m$, for a higher number of HS units the source shows a WCS-like behaviour for low losses, with a slightly higher maximum tolerable loss level. In the limit $m \to \infty$, however, any advantage over the WCS is lost.

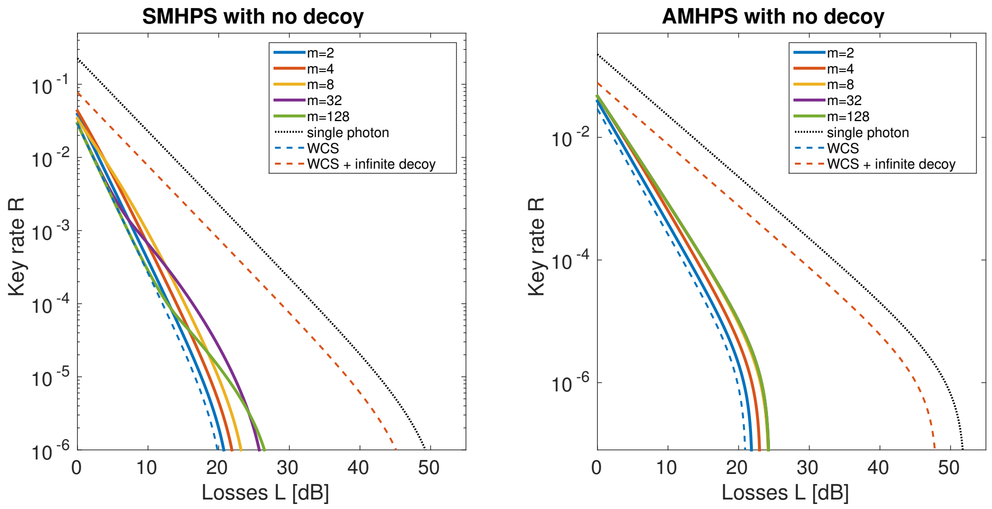

Figure 3.8: Key rate of the SMHPS (left) and the AMHPS (right), with $\eta = 0.7$ and $\gamma = 0.5$ for BB84 without decoy state. For the AMHPS (right), the curves for $m = 8$, $m = 32$ and $m = 128$ are superposed.

The AMHPS, on the other hand, has a more stable behaviour, since its key never decreases for increasing $m$, but reaches an optimum value (already at $m = 8$) and then remains unchanged. This is due to the fact that, when a certain number of HS units has been reached, the further addition of HS units has not effect, because the probability that the rightmost HS units are triggered to output is negligible and the output is given only by the leftmost HS units.

The different behaviour of the two architectures is more marked when studying the dependence of the key rate on the source parameters, i.e., detection efficiency $\eta$ and switch transmittance $\gamma$. The SMHPS (Figure 3.9) and the AMHPS (Figure 3.10) are studied fixing $\eta = 0.7$ and changing $\gamma$ on the left and with fixed $\gamma = 0.5$ and changing $\eta$ on the right.

The behaviour of the SMHPS is highly dependent on switch transmittance. Indeed, for low $\gamma$, the benefits deriving from multiple HS units do not compensate the higher absorption rate, giving a WCS-like behaviour for $\gamma < 0.5$. This result had already been observed in the study of the output statistics of this architecture [67], where, in the asymptotic limit $m \to \infty$, the SMHPS was shown to perform better than the WCS for $\gamma \geq 0.5$, with the curve $\gamma = 0.5$ corresponding to the transition from a WCS-like to a MHPS-like regime. The effect of the detection efficiency $\eta$, on the other hand, is evident in the high loss regime, where the influence of the lower number of multi-photon pulses is more important. In the low loss regime, indeed, the dominant

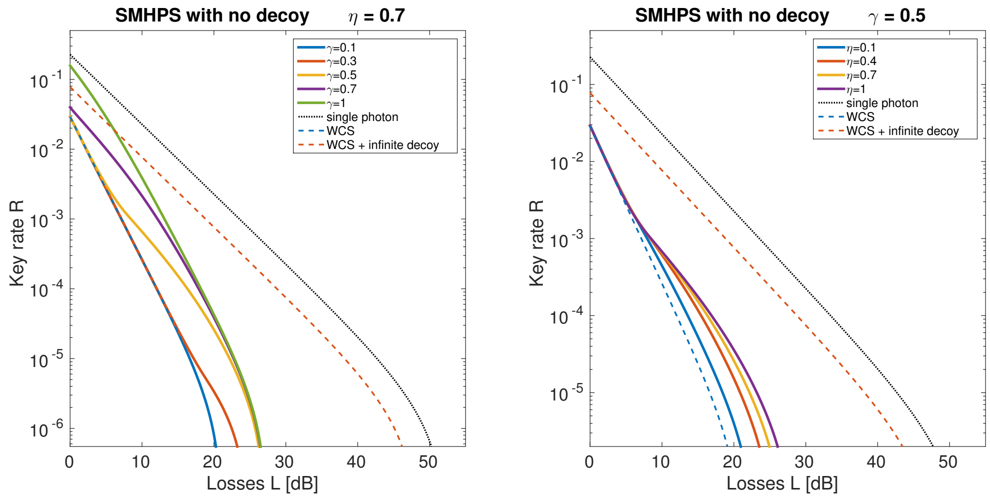

Figure 3.9: Key rate (without decoy state) for the SMHPS for $m = 32$ and (left) $\eta = 0.7$ and different values of $\gamma$, (right) $\gamma = 0.5$ and different values of $\eta$.

effect is the photon absorption in the optical switching, with the detection efficiency playing a secondary role. The effect of increased detection efficiency, indeed, is a better choice of the HS unit to route to output, which allows the HS units to be pumped with lower intensity, decreasing the incidence of multi-photon pulses.

The AMHPS, on the contrary, keeps the same key rate trend for all tested combinations $(\eta, \gamma)$. This is due to the fact that, since the photons emitted by the leftmost HS units pass a low number of switches before being routed to output, the effect of photon absorption never dominates over multi-photon pulses.

- **BB84 with active decoy -** The secret key rate for the active decoy BB84 is calculated using Equation (3.23), with $e_1$, $Y_0$ and $Y_1$ calculated by using the channel parameters of Equations (3.20) and (3.17), in order to simulate the arbitrary precision parameter estimation that can be reached using active decoy. The results of simulations are shown in Figure 3.11. The normalized mean number of generated pairs that maximizes the key rate is almost constant for both sources in the range $\sim 0.6 - 0.9$, with a steep fall in the regime where dark counts become important. The effect of optical absorption is evident in the decreasing of SMHPS rates for increased number of HS units. The AMHPS, on the other hand, reaches its maximum performance already with four HS units.

- **BB84 with passive decoy -** In the proposed passive decoy scheme, parameter estimation is no longer optimal and it has an effect on the final key rate. Therefore, simulations must use the real bounds for the parameters $e_1$, $Y_0$ and $Y_1$ calculated in Appendix B, and have also to consider the relative incidence of the two statistics. The results of simulations, visualized in Figure 3.12, show the expected lower key rate with respect to the active decoy scheme. Indeed, the worse bound on the parameters gives a super-estimation of the information leaked to Eve, thus requiring the source to be pumped with lower intensity, with a normalized mean number of generating pairs $\mu$ oscillating between 0.2 and 0.3. The SMHPS has a key rate comparable with the one given by the one-decoy WCS, because of the detrimental effect on the source caused by optical switch attenuation. On the other hand, the key rate of the

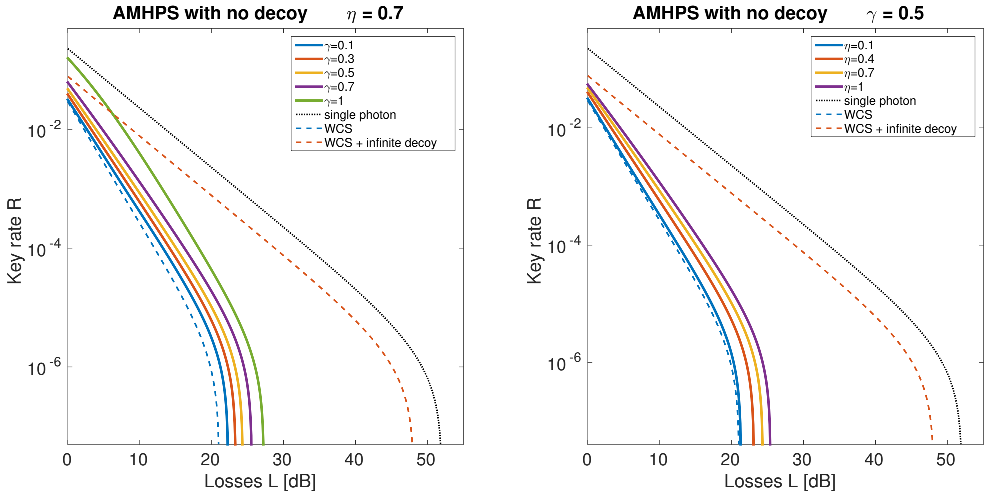

Figure 3.10: Key rate (without decoy state) for the AMHPS for $m = 32$ and (left) $\eta = 0.7$ and different values of $\gamma$, (right) $\gamma = 0.5$ and different values of $\eta$.

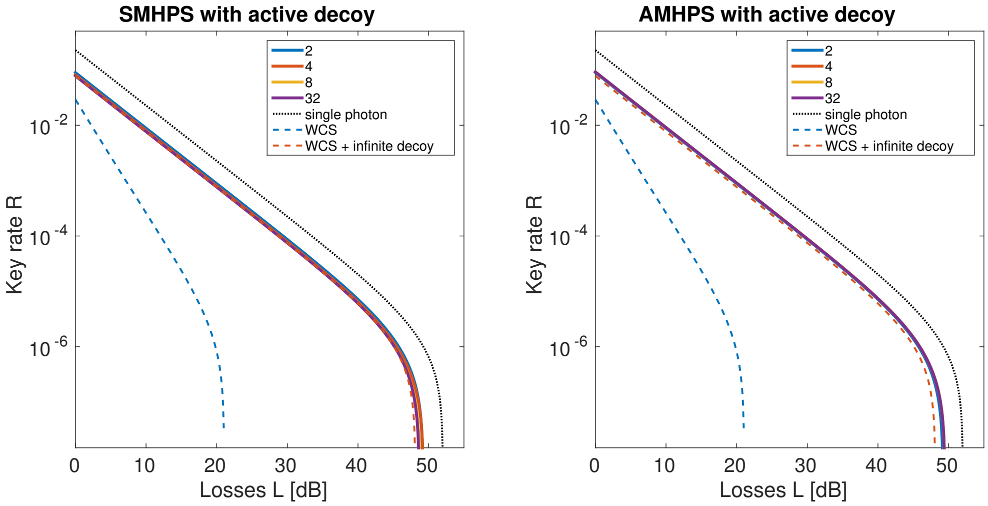

Figure 3.11: Key rate of active decoy state QKD for the SMHPS (left) and the AMHPS (right), with $\eta = 0.7$ and $\gamma = 0.5$. For the SMHPS (left), the curves are very close, with $m = 32$ the lowest curve. In the AMHPS case (right), the lowest curve has $m = 2$, while all the others are superposed.

AMHPS is always higher that the corresponding one-decoy WCS, arriving close to the maximum tolerable loss level of the active decoy WCS. Also in this case, this architecture reaches its maximum performance for $m = 4$.

- **Comparison between active and passive decoy -** The advantage of the AMHPS over the SMHPS with both active and passive decoy is evident from Figure 3.13, where the two architectures are compared. The AMHPS performs better than the SMHPS in both schemes, and this improvement is such that the AMHPS in the passive scheme almost equals both the SMHPS and the WCS in the active scheme, despite the worse parameter estimation.

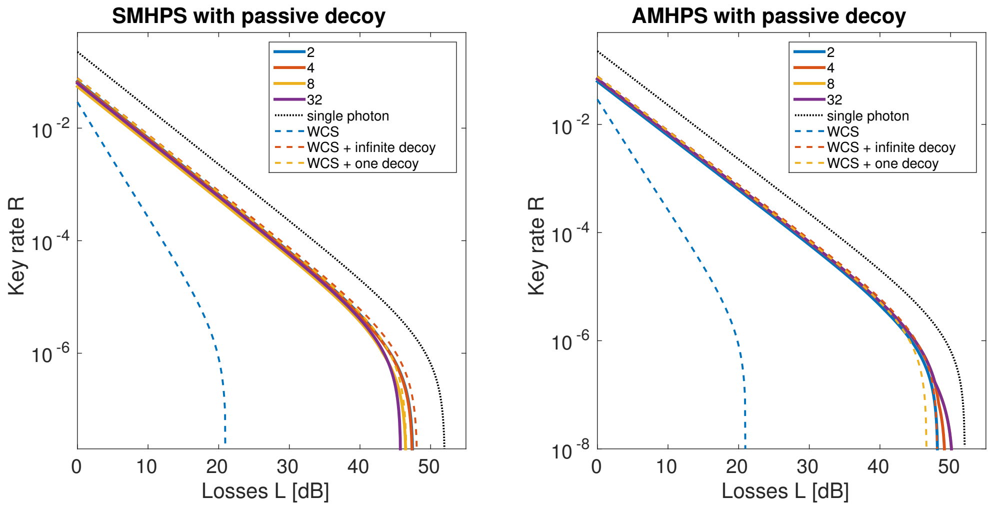

Figure 3.12: Key rate for passive decoy state QKD for the SMHPS (left) and the AMHPS (right), with $\eta = 0.7$ and $\gamma = 0.5$.

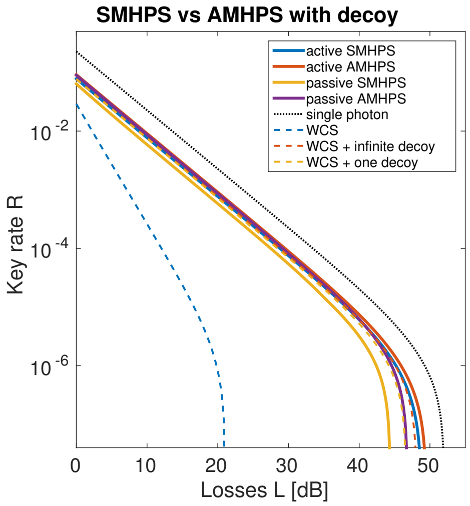

Figure 3.13: Key rate for the SMHPS and the AMHPS for both active and passive decoy with $m = 8$, $\eta = 0.7$ and $\gamma = 0.5$.

### 3.1.4 Symmetric three-state protocol

The QKD protocol described in Section 3.1.3, the BB84, employs four states belonging to two mutually unbiased bases, like for example $X$ and $Z$. However, it has been demonstrated that, for the construction of a QKD protocol, two non-orthogonal states are sufficient. This protocol, introduced by Bennett in 1992 (B92) [95], uses two non-orthogonal states, say $|\psi_0\rangle$ and $|\psi_1\rangle$, associated with bit values 0 and 1. In the quantum transmission phase, Alice sends Bob a series of states according to the value of the random variable $X$. Bob then measures the states in the POVM $\mathcal{M}_{B92} = \{\alpha\,|\psi_0^\perp\rangle\,\langle\psi_0^\perp|\,,\alpha\,|\psi_1^\perp\rangle\,\langle\psi_1^\perp|\,,I_2 - \alpha\,|\psi_0^\perp\rangle\,\langle\psi_0^\perp| - \alpha\,|\psi_1^\perp\rangle\,\langle\psi_1^\perp|\}$, where $\alpha = \frac{1}{1+|\langle\psi_1|\psi_2\rangle|}$, and associates to his measurement, respectively, the values 1, 0, or "inconclusive". Indeed, if Bob measures $|\psi_0^\perp\rangle\,\langle\psi_0^\perp|$, he knows that Alice cannot have sent the bit 0, therefore he associates that event with bit 1, and the same happens if he measures $|\psi_1^\perp\rangle\,\langle\psi_1^\perp|$. If he gets the "inconclusive" result, he cannot discriminate the bit Alice send, therefore that event will be discarded in the sifting phase. While this protocol has been demonstrated to be unconditionally secure in the loss-free scenario [96], it presents some problems in the case of a lossy channel. Indeed, Eve could extract information by performing an unambiguous state discrimination (USD) attack [97]. This attack consists in performing a measurement in the same POVM $\mathcal{M}_{B92}$ as Bob and, in the case inconclusive result, discard the qubit. Thus, she can get all the information on the states that arrive to Bob, with the only detectable effect of an increase in the loss level of the channel. This protocol, therefore, require a low enough level of channel losses in order to be proved unconditionally secure. It has been proved, however, that the addition of a third state is sufficient to make the B92 protocol unconditionally secure independently from the noise of the quantum channel [98, 99].

The optimal three-state QKD protocol, introduced in 2000 by Phoenix-Barnett-Chefles (PBC00) [100], uses states that form an equilateral triangle over one plane of the Bloch sphere (such as the X-Z plane). This symmetry can be exploited to obtain rates and a noise tolerance comparable to the BB84, despite the less number of states employed. An improvement of this protocol, proposed by Renes in 2004 (R04) [101], uses the fraction of inconclusive events to estimate the error rate, thus allowing to use all sifted bits for key extraction. This protocol has been demonstrated unconditionally secure in the asymptotic case for a bit error rate (QBER) up to 9.81% [102], and its security has recently been demonstrated also in the case of finite key [103]. Their finite key security proof, however, assumes a direct parameter estimation, thus neglecting one of the more interesting features of this protocol.

This thesis reports the first experimental implementation of equiangular three state QKD, using an entanglement-based version of the protocol with passive optic devices for the implementation of the POVM [104]. The performance of the protocol is studied by evaluating the secret key rate both in the asymptotic limit and in the finite key scenario. This Section will first describe all the steps of the symmetric three-state protocol in the general finite-key scenario, giving the asymptotic key rate as the limit of the secure finite-key for $N \to \infty$. Then, it will describe the experimental setup used for the implementation of the protocol, and, eventually, it will show the results of the measurements.

#### The protocol

*Quantum transmission* - In the quantum transmission phase, the R04 protocol uses three states, $\{|\psi_1\rangle\,,|\psi_2\rangle\,,|\psi_3\rangle\}$, placed on an equilateral triangle on the X-Z plane of the Bloch sphere, as shown in Figure 3.14. The states are grouped into three different sets, $S_1 = \{|\psi_1\rangle\,,|\psi_2\rangle\}$, $S_2 = \{|\psi_2\rangle\,,|\psi_3\rangle\}$, and $S_3 = \{|\psi_3\rangle\,,|\psi_1\rangle\}$. In each set, the first state is

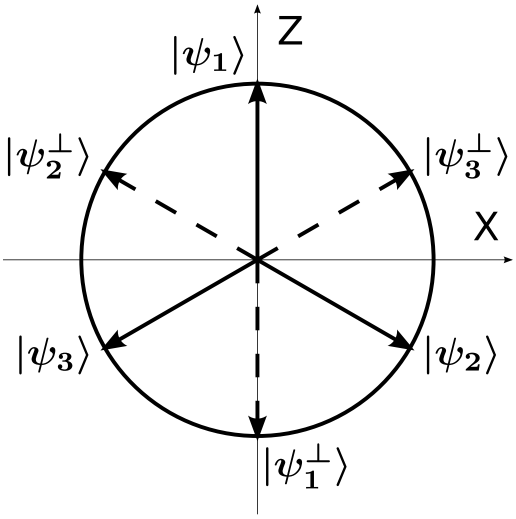

Figure 3.14: States used in the R04 protocol. The states lie in the X-Z plane of the Bloch sphere. They are grouped into the sets $S_1 = \{|\psi_1\rangle, |\psi_2\rangle\}$, $S_2 = \{|\psi_2\rangle, |\psi_3\rangle\}$, and $S_3 = \{|\psi_3\rangle, |\psi_1\rangle\}$, where the first element of each set corresponds to bit 0 and the second to bit 1.

associated with bit 0 and the second with bit 1. Differently from other QKD protocols, in the R04 the state brings no information about its associated bit before the information about the used set is disclosed.

In the entanglement-based version of the R04 protocol, the two photons of the polarization-entangled state

$$|\Psi^-\rangle = \frac{|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B}{\sqrt{2}} \tag{3.26}$$

are sent to Alice's and Bob's measurement setup. If the source is safe at Alice's side, all security proofs implemented for the prepare-and-measurement scheme can be used also for the entanglement-based version, otherwise some more assumptions are required [52]. In this case, the source is assumed to be part of Alice's setup. Alice measures her photon $A$ using the POVM $\{\Pi_i \equiv \frac{2}{3}|\psi_i^\perp\rangle\langle\psi_i^\perp|\}$, with $|\psi_1^\perp\rangle = |V\rangle$, $|\psi_2^\perp\rangle = \frac{\sqrt{3}}{2}|H\rangle - \frac{1}{2}|V\rangle$, $|\psi_3^\perp\rangle = \frac{\sqrt{3}}{2}|H\rangle + \frac{1}{2}|V\rangle$, and $|\psi_i^\perp\rangle$ the orthogonal of $|\psi_i\rangle$. When Alice obtains a detection in the state $|\psi_i^\perp\rangle$ (with probability $\frac{1}{3}$ for each outcome $i$), she is sending to Bob the state $|\psi_i\rangle$ where $|\psi_1\rangle = |H\rangle$, $|\psi_2\rangle = \frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|V\rangle$, and $|\psi_3\rangle = \frac{1}{2}|H\rangle - \frac{\sqrt{3}}{2}|V\rangle$. This operation corresponds to the random preparation, with equal probability, of one of the three states $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$. Bob performs his measurements in the same POVM as Alice $\{\Pi_i\}$.

Differently from the BB84 or the B92, after the quantum transmission phase no bit of key has been shared by Alice and Bob yet. Indeed, each exchanged state can still mean both 0 or 1, according to the chosen set. Both the strings $X$ and $Y$ are generated in the sifting phase, the first one as a result of a random process at Alice's side, and the second one from the set information sent from Alice to Bob.

*Sifting* - At the beginning of the sifting phase, Alice and Bob compare the instants of their events, keeping only those where both have a detection within a fixed coincidence window. Then, Alice generates her $N$-bit raw key $X$ by using a random process (e.g., a QRNG), associating a bit to each state sent to Bob. In such a way, she can unambiguously determine the set $S_i$ used for each event. Indeed, if, for example, the $n$-th state sent by

| | $S_1$ | $S_2$ | $S_3$ |
|---|---|---|---|
| $\Pi_1 \equiv B1$ | 1 | Inc | 0 |
| $\Pi_2 \equiv B2$ | 0 | 1 | Inc |
| $\Pi_3 \equiv B3$ | Inc | 0 | 1 |

Table 3.1: Sifting procedure of the R04 protocol. The rows represents the different results of Bob's measurement, while the columns represent the different sets upon which the states are grouped. Inconclusive results are marked as "Inc".

Alice is $|\psi_2\rangle$ and the $n$-th random bit is 1, Alice knows that the $n$-th set is $S_1$. Alice sends the string of set indices $i$ to Bob, who can thus, from the results of his measurements, determine his random variable $Y$, using a sifting procedure analogous to the one of B92. The sifting procedure is summarized in Table 3.1, where each row represents a different result of Bob's measurement and each column is a different set. The inconclusive results are those events in which Bob is not able to discriminate the bit sent by Alice (analogously to what happens in the B92). Bob tells Alice the position of the inconclusive events and they both discard them, remaining with the $N_{conc}$-bit strings $X_S$ and $Y_S$.

*Parameter estimation* - As already pointed out, one of the interesting features of the R04 protocol is the possibility of estimating the QBER from the fraction of inconclusive events, something that has not been considered in previous finite-key analysis of the symmetric three-state protocol [103]. In order to use this result in the security evaluation of the protocol, however, it is necessary to found an upper bound on this estimation with probability at least $1 - \varepsilon_{PE}$, where $\varepsilon_{PE}$ is the probability of failure of the parameter estimation, i.e., the probability that the real QBER is higher than the estimated one.

The estimation makes use of an $N$-dimension random vector $R$, with $N$ the number of symbols exchanged between Alice and Bob, which takes the value $R_i = +1$ if the $i$-th event is a "good" conclusive result (i.e., a conclusive result which is not a bit error), $R_i = 0$ if the $i$-th event is a bit error, and $R_i = -1$ if the $i$-th event is inconclusive. From our definition of $R_i$, it is obvious that $R_i \in [-1, 1]$. Then, the variable $\bar{R}$ is defined as

$$\bar{R} = \frac{1}{N} \sum_{i=1}^{N} R_i = \frac{1}{N} \left( N_{good} - N_{inc} \right), \tag{3.27}$$

where $N_{good}$ is the number of "good" conclusive events and $N_{inc}$ is the number of inconclusive events. The expected value of this random variable is $\mathbb{E}(\bar{R}) = 0$. This can be easily seen by rewriting the sifting procedure of Table 3.1 as a function of the detection results of Alice and Bob $(Ai, Bj)$ and of the $i$-th bit value $X_i$, giving the procedure described in Table 3.2.

Events of the form $(Ai, Bi)$ are errors independently from the value of the bit $X_i$. All the other events, of the form $(Ai, Bj)$, with $i \neq j$, are either an inconclusive or a "good" conclusive event depending on Alice's bit $X_i$. Since the choice of $X_i$ is a random event with probability $\mathbb{P}(X_i = 0) = \mathbb{P}(X_i = 1) = \frac{1}{2}$, the probability that a "non-error" event is "good" conclusive or inconclusive is $\frac{1}{2}$ and the expected value is $\mathbb{E}(N_{good}) = \mathbb{E}(N_{inc}) = \frac{N - N_{error}}{2}$. It is possible, therefore, to apply the Hoeffding inequality [105] to the random vector $R$

$$\mathbb{P}\left( \left| \bar{R} - \mathbb{E}\left[ \bar{R} \right] \right| \geq \xi \right) \leq 2e^{-\frac{2N^2\xi^2}{4N}} = 2e^{-\frac{N\xi^2}{2}}, \tag{3.28}$$

with $\xi > 0$.

| | $X_i = 0$ | | | $X_i = 1$ | | |
|---|---|---|---|---|---|---|
| | $A1$ | $A2$ | $A3$ | $A1$ | $A2$ | $A3$ |
| $B1$ | 1 | Inc | 0 | 0 | 1 | Inc |
| $B2$ | 0 | 1 | Inc | Inc | 0 | 1 |
| $B3$ | Inc | 0 | 1 | 1 | Inc | 0 |

Table 3.2: Sifting procedure for the $i$-th bit, according to the random choice of the bit $X_i$ (on the left $X_i = 0$, on the right $X_i = 1$). The cell ($Ai$,$Bj$) stands for output $\Pi_i$ at Alice's side and $\Pi_j$ at Bob's side. Inconclusive events are marked as "Inc". The events in the diagonal ($Ai$,$Bi$) give an error independently from the bit choice. The other combinations ($Ai$,$Bj$), with $i \neq j$, are either a "good" conclusive or an inconclusive event, according to Alice's bit $X_i$.

In order to use Equation (3.28) to bound the QBER, it is necessary to rewrite $N_{good}/N$ as a function of the QBER $Q = (N_{error})/(N_{good}+N_{error})$ and of the fraction of inconclusive events $I = N_{inc}/N$. This can be obtained starting from the relation

$$\frac{N_{good} + N_{inc} + N_{error}}{N} = 1, \tag{3.29}$$

from which it is easy to extract

$$\frac{N_{good} + N_{error}}{N} = 1 - I. \tag{3.30}$$

By using it, it is possible to express the QBER as

$$Q = \frac{N_{error}}{N_{good} + N_{error}} = \frac{N_{error}}{(1-I)N}, \tag{3.31}$$

which, inverted, gives

$$\frac{N_{error}}{N} = (1-I)Q. \tag{3.32}$$

By inserting (3.32) into (3.29), it is possible to write the fraction of "good" conclusive events as

$$\frac{N_{good}}{N} = 1 - I - \frac{N_{error}}{N} = (1-I) - Q(1-I) = (1-Q)(1-I). \tag{3.33}$$

With these equations, the Hoeffding bound (3.28) can be rewritten as

$$\mathbb{P}\left(\left|(1-I)(1-Q) - I\right| \geq \xi\right) \leq 2e^{-\frac{N\xi^2}{2}}. \tag{3.34}$$

This equation is equivalent to stating that the inequality

$$\left|(1-Q)(1-I) - I\right| \leq \xi(\varepsilon_{PE}, N) := \sqrt{\frac{2}{N}\log\frac{2}{\varepsilon_{PE}}} \tag{3.35}$$

is valid with probability at least $1 - \varepsilon_{PE}$, where $\varepsilon_{PE}$ is the probability that parameter estimation fails. Indeed, with probability $1 - \varepsilon_{PE}$, the QBER $Q$ is less than

$$\widetilde{Q} := \frac{1 - 2I + \xi(\varepsilon_{PE}, N)}{1 - I}. \tag{3.36}$$

*Error correction* - The error correction (EC) phase takes the two sifted keys $X_{PE}$ and $Y_{PE}$, output by the parameter estimation function, and outputs an $\varepsilon_{EC}$-correct key, i.e., a couple of keys $X_{EC}$ and $Y_{EC}$ such that $\mathbb{P}(X_{EC} \neq Y_{EC}) \leq \varepsilon_{corr}$. To perform this task, they need to communicate some classical information, summarized in the variables $C_A'''$ and $C_B'''$, through the authenticated channel. Since Eve is assumed to have full access to the information in the authentic channel (even though she cannot tamper with it), it is necessary to remove such information in the privacy amplification step. This information, also called $\text{leak}_{EC}$, is highly dependent on the effective error correction protocol used. However, it is possible to estimate it as

$$\text{leak}_{EC} = f_{EC} H(X_{PE}|Y_{PE}) + \log_2 \frac{2}{\varepsilon_{EC}} = N_{conc} f_{EC} h(Q) + \log_2 \frac{2}{\varepsilon_{EC}}, \tag{3.37}$$

where the first term represents the quantity of bits required for error correction, which is dependent on the bit error rate $Q$ through the binary entropy $h(Q) = -Q\log_2 Q - (1 - Q)\log_2(1-Q)$ and on the efficiency of the error correction algorithm $f_{EC} \geq 1$, while the second term counts the quantity of bits that must be leaked to assure that the condition $\mathbb{P}(X_{EC} \neq Y_{EC}) \leq \varepsilon_{EC}$ is valid, by using two-universal hash functions[6] [52, 59, 103]. The efficiency of the error correction algorithm $f_{EC}$ lies in the range $\simeq 1.05 - 1.2$ for currently used algorithms [93].

*Privacy amplification* - The privacy amplification step takes as input the two $\varepsilon_{corr}$-correct strings $X_{EC}$ and $Y_{EC}$ and outputs two $\varepsilon_{sec}$-secret keys $k_A = f''''(X_{EC}, C''''(B))$ and $k_B = f''''(Y_{EC}, C''''(A))$. If a key is $\varepsilon_{corr}$-correct and $\varepsilon_{sec}$-secret, it is said to be $\varepsilon$-secure, with $\varepsilon = \varepsilon_{corr} + \varepsilon_{sec}$. As already shown in Section 3.1.2, a composable security criterion can be based on limiting the trace distance between the state output by the protocol and the tensor product of the maximally mixed state with Eve's subsystem, as show in Equation (3.8). It has been demonstrated that this security criterion holds if privacy amplification uses a class of two-universal hash functions which map the $N_{conc}$-bit strings $X_{EC}$ and $Y_{EC}$ onto an $l$-bit string, with the length of the final key $l$ bounded by

$$l \leq H_{min}^{\bar{\varepsilon}}(X_{EC}|EC) - 2\log_2 \frac{1}{\varepsilon_{PA}}, \tag{3.38}$$

where $H_{min}^{\bar{\varepsilon}}$ is the *smooth min-entropy* of Alice's key $X$ conditioned on the information got by Eve in the quantum transmission phase $E$ and the classical communication $C$[7] [52]. The information leakage in the error correction phase, $\text{leak}_{EC}$, causes a decrease in the smooth min-entropy [52, 108], according to

$$H_{min}^{\bar{\varepsilon}}(X_{EC}|EC) \geq H_{min}^{\bar{\varepsilon}}(X_{PE}|E) - \text{leak}_{EC}. \tag{3.39}$$

In order to find the secure key rate, it is still necessary to find a bound on the smooth min-entropy $H^{\bar{\varepsilon}}(X_{PE}|E)$. It has been shown that this bound is easy to calculate in the case of *collective attacks*, where the only limitation to Eve's power is the fact that she must attack each qubit separately using the same strategy [108]. In this case, the state $\rho_{ABE}$

[6] The class of two-universal hash functions $\mathcal{H}$, each elements of which maps the input $N$-bit string into a $k$-bit string, has the property that, for a randomly chosen $h \in \mathcal{H}$, $\mathbb{P}_{h\in\mathcal{H}}\big(h(x) = h(y)\big) \leq 2^{-k}$, $\forall x \neq y$ [106].

[7] The min-entropy of a random variable $X$, conditioned on $Z$, is the logarithmic form of the maximum probability of guessing the value of random variable $X$, knowing random variable $Z$, i.e., $2^{-H_{min}(X|Z)} = \max_{x\in X z\in Z} \mathbb{P}(X = x|Z = z)$ [107]. The smooth min-entropy $H_{min}^{\bar{\varepsilon}}(X|Z)$ is the min-entropy over all random variables $R$, whose distribution is $\bar{\varepsilon}$-close to $X$, i.e., $\delta(X, R) = \frac{1}{2}\sum_v \big|\mathbb{P}(X = v) - \mathbb{P}(R = v)\big| \leq \bar{\varepsilon}$ [107].

shared by Alice-Bob and Eve during the quantum transmission phase can be written as $(\sigma_{\bar{A}\bar{B}\bar{E}})^{\otimes N}$, where the barred quantities indicate single qubit states, which are identical because of the assumption of collective attacks. In this case, the smooth min-entropy can be lower bounded by

$$H^{\bar{\varepsilon}}_{min}(X_{PE}|E) \geq N_{conc}\left(\min_{\sigma_{\bar{A}\bar{B}\bar{E}}\in\Gamma_{\varepsilon_{PE}}} H(\bar{X}|\bar{E}) - \delta(\bar{\varepsilon})\right), \tag{3.40}$$

where $\Gamma_{\varepsilon_{PE}}$ is the set of all states compatible with parameter estimation and $\delta(\bar{\varepsilon}) = 7\sqrt{\frac{1}{N_{conc}}\log_2\frac{2}{\bar{\varepsilon}}}$ [52]. The value of $\min_{\sigma_{\bar{A}\bar{B}\bar{E}}\in\Gamma_{\varepsilon_{PE}}} H(\bar{X}|\bar{E})$ can be calculated from the asymptotic security proof in [102], and is

$$\min_{\sigma_{\bar{A}\bar{B}\bar{E}}\in\Gamma_{\varepsilon_{PE}}} H(\bar{X}|\bar{E}) = \left(1 - h\left(\frac{5}{4}\widetilde{Q}\right)\right), \tag{3.41}$$

where $h(\cdot)$ is the binary entropy and $\widetilde{Q}$ is the bound on the QBER calculated in the parameter estimation step [103, 108].

Putting all pieces together, the $\varepsilon_{col}$-secure key fraction $r_{col}$ is

$$\begin{aligned} r_{col} =& \frac{N_{conc}}{N}\left[1 - h\left(\frac{5}{4}\widetilde{Q}\right)\right] - 7\sqrt{\frac{N_{conc}}{N^2}\log_2\frac{2}{\bar{\epsilon}}} \\ & - \frac{1}{N}\log_2\frac{2}{\epsilon_{EC}} - 2\frac{1}{N}\log_2\frac{1}{\epsilon_{PA}} - \frac{N_{conc}}{N}f_{EC}h(Q), \end{aligned} \tag{3.42}$$

where $r_{col} = l/N$ is the fraction of the total exchanged bits that are $\varepsilon_{col}$-secure against collective attacks. The security parameter is $\varepsilon_{col} = \bar{\varepsilon} + \varepsilon_{PE} + \varepsilon_{EC} + \varepsilon_{PA}$.

The secure key rate against *general attacks*, i.e., attacks in which Eve has no restrictions in her possible interactions with the transmitted quantum state, can be calculated from $r_{col}$ by using the *post-selection technique* [109]. It states that, under the assumption of invariance under permutation of the inputs[8], the protocol obtained by shortening the secure key rate to

$$r_{gen} = r_{col} - \frac{6\log_2(N+1)}{N} \tag{3.43}$$

is secure against general attacks, with security parameter $\varepsilon_{gen} = (N+1)^3\varepsilon_{col}$.

In the asymptotic limit of infinite key, the fraction of secure conclusive bits becomes

$$r = \lim_{N\to\infty} r_{gen} = \lim_{N\to\infty} r_{col} = \frac{N_{conc}}{N}\left[1 - h\left(\frac{5}{4}Q\right) - f_{EC}h\left(Q\right)\right], \tag{3.44}$$

where $Q = \lim_{N\to\infty}\widetilde{Q} = \frac{1-2I}{1-I}$, and the security parameter $\varepsilon_{gen} \to 0$ [102] (in the hypothesis that the security parameter $\varepsilon_{col}$ is exponentially decreasing with key length [109]).

### Experimental setup

**The source -** The Sagnac interferometer described in Chapter 2 is used as the source of polarization-entangled photons in the singlet state $|\Psi^-\rangle = (|H\rangle|V\rangle - |V\rangle|H\rangle)/\sqrt{2}$, as shown in Figure 3.15. The source is pumped with a power of 3.5 mW, giving a mean

[8] This requirement can be forced by adding a symmetrization step where both Alice and Bob permute their inputs according to a permutation $\pi$ that, after the quantum transmission phase, is communicated through the authentic channel [109].

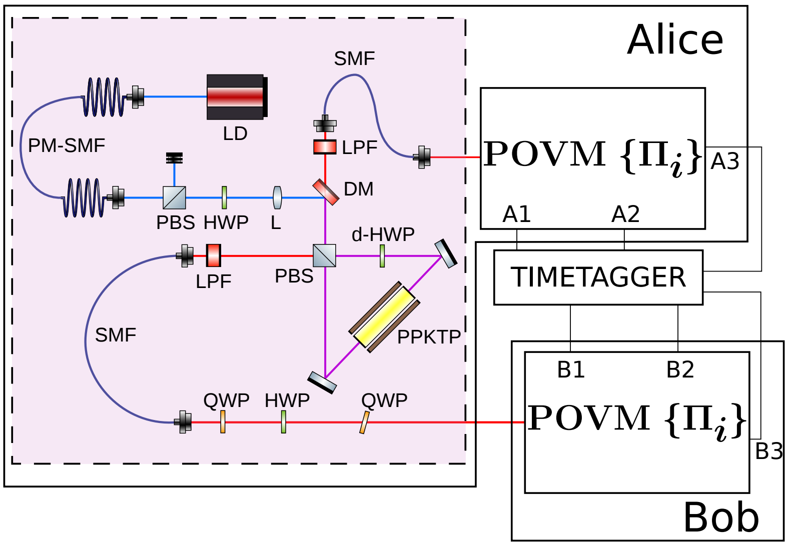

Figure 3.15: Experimental setup used for the experiment [104]. The source is the Sagnac-based entangled source described in Section 2. Fiber birefringence is compensated by using two quarter-wave plates (QWP) and a half-wave plate (HWP). This image uses elements from the ComponentLibrary by Alexander Franzen [33], licensed under CC BY-NC 3.0 [34].

coincidence rate of 29 kHz at the detector, corresponding to a 5% heralding ratio.

**The measurement apparatus -** The measurement apparatus proposed in the original work implemented the measurement POVM using an interferometric setup [100]. The major drawbacks of this scheme are the fact that it requires careful alignment [110, 111] and it is not assured to have the long term stability required for Quantum Key Distribution (a stability of about half an hour is reported [111]). In order to meet the requirements of QKD, a passive linear optics implementation of the POVM has been adopted [112].

The optical scheme used for the measurement is shown in Figure 3.16, and Figure 3.17 shows its realization on the optical bench. Since the POVM $\{\Pi_i\}$ implements a

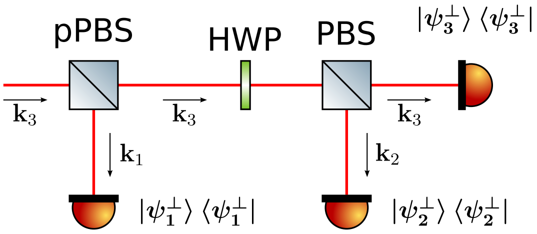
pPBS
HWP
PBS
$|\psi_3^\perp\rangle\langle\psi_3^\perp|$
$\mathbf{k}_3$
$\mathbf{k}_3$
$\mathbf{k}_3$
$\mathbf{k}_1$
$\mathbf{k}_2$
$|\psi_1^\perp\rangle\langle\psi_1^\perp|$
$|\psi_2^\perp\rangle\langle\psi_2^\perp|$

Figure 3.16: Passive linear optics implementation of the POVM $\{\Pi_i\}$ [104]. The setup employs a partially polarizing beam-splitter (pPBS), a half-wave plate (HWP) at 22.5° and a polarizing beam-splitter (PBS). This image uses elements from the ComponentLibrary by Alexander Franzen [33], licensed under CC BY-NC 3.0 [34].

three-output measurement on the 2-dim Hilbert space of photon polarization, it is simpler to think it as a measurement on a path qutrit, defined as

$$\hat{a}^\dagger_{\mathbf{k}_1}\left|0,0,0\right\rangle_{\mathbf{k}_1,\mathbf{k}_2,\mathbf{k}_3} = \left|1,0,0\right\rangle_{\mathbf{k}_1,\mathbf{k}_2,\mathbf{k}_3} = \left|1\right\rangle, \tag{3.45}$$

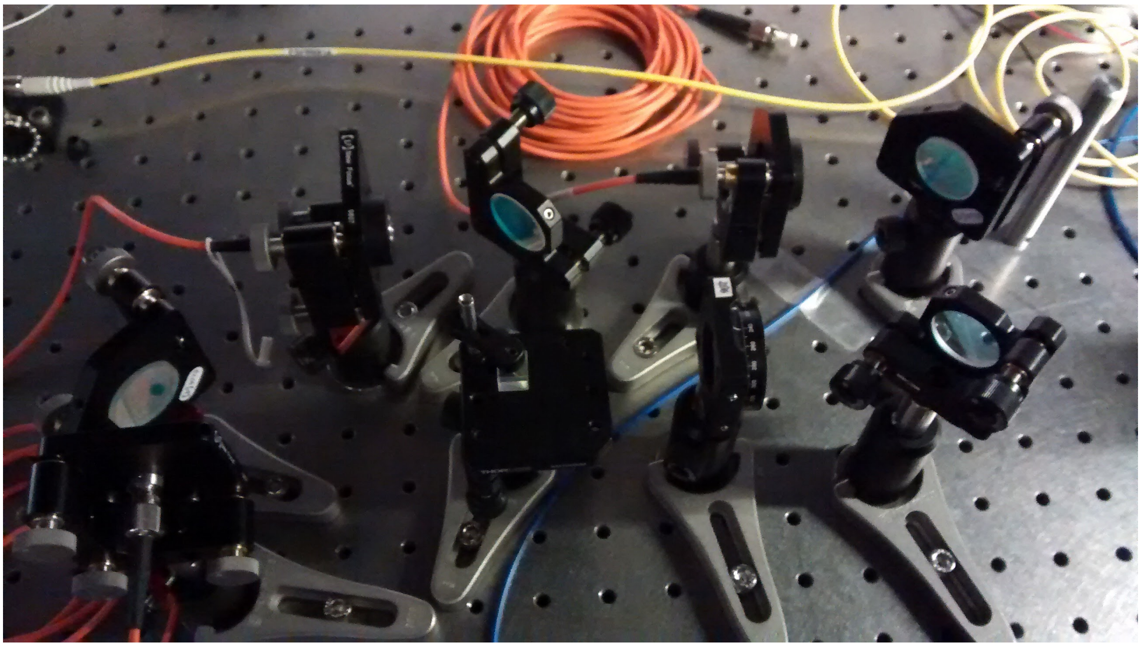

Figure 3.17: Optical bench implementation of the measurement POVM $\{\Pi_i\}$.

$$\hat{a}^\dagger_{\mathbf{k}_2} \left|0,0,0\right\rangle_{\mathbf{k}_1,\mathbf{k}_2,\mathbf{k}_3} = \left|0,1,0\right\rangle_{\mathbf{k}_1,\mathbf{k}_2,\mathbf{k}_3} = \left|2\right\rangle, \tag{3.46}$$

$$\hat{a}^\dagger_{\mathbf{k}_3} \left|0,0,0\right\rangle_{\mathbf{k}_1,\mathbf{k}_2,\mathbf{k}_3} = \left|0,0,1\right\rangle_{\mathbf{k}_1,\mathbf{k}_2,\mathbf{k}_3} = \left|3\right\rangle. \tag{3.47}$$

The circuit implementation of optical setup is show in Figure 3.18, where the black box at the end of the polarization qubit means that the measurement is insensitive from the polarization degree of freedom, as happens experimentally with single-photon avalanche photo-diodes (SPADs).

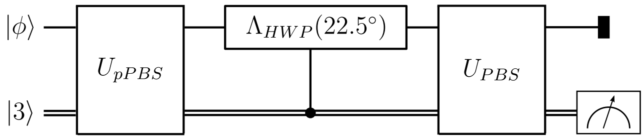

Figure 3.18: Circuit implementation of the POVM $\{\Pi_i\}$. The double line in the ancilla state indicates that it is a qutrit.

The partially polarization beam-splitter is an optical system that completely transmits the horizontal polarization and has a reflectivity of 66.7% for the vertical polarization, therefore inducing the transformation

$$U_{pPBS} \left|H\right\rangle \left|3\right\rangle = \left|H\right\rangle \left|3\right\rangle, \tag{3.48}$$

$$U_{pPBS} \left|V\right\rangle \left|3\right\rangle = \sqrt{\frac{1}{3}} \left|V\right\rangle \left|3\right\rangle + \sqrt{\frac{2}{3}} \left|V\right\rangle \left|1\right\rangle. \tag{3.49}$$

The other optical elements are a controlled half-wave plate (HWP) at 22.5°, of matrix

$$\begin{aligned} & I_2 \otimes \big(\left|1\right\rangle\left\langle 1\right| + \left|2\right\rangle\left\langle 2\right|\big) + \Lambda_{HWP}(\pi/4) \otimes \left|3\right\rangle\left\langle 3\right| \\ = \; & I_2 \otimes \big(\left|1\right\rangle\left\langle 1\right| + \left|2\right\rangle\left\langle 2\right|\big) + \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \left|3\right\rangle\left\langle 3\right| \end{aligned} \tag{3.50}$$

and the PBS, inducing the transformation

$$U_{PBS}\left|H\right\rangle\left|3\right\rangle = \left|H\right\rangle\left|3\right\rangle, \tag{3.51}$$

$$U_{PBS}\left|V\right\rangle\left|3\right\rangle = \left|V\right\rangle\left|2\right\rangle. \tag{3.52}$$

Given an arbitrary polarization input state $\left|\phi\right\rangle = \alpha\left|H\right\rangle + \beta\left|V\right\rangle$, corresponding to the composite state $\left|\phi\right\rangle \otimes \left|3\right\rangle$ in the system $\mathcal{H}_{pol} \otimes \mathcal{H}_{path}$, the transformation induced by the partially polarizing beam-splitter gives

$$U_{pPBS}\left|\phi\right\rangle\left|3\right\rangle = \alpha\left|H\right\rangle\left|3\right\rangle + \sqrt{\frac{1}{3}}\beta\left|V\right\rangle\left|3\right\rangle + \sqrt{\frac{2}{3}}\beta\left|V\right\rangle\left|1\right\rangle. \tag{3.53}$$

Then, the state crosses the controlled HWP, becoming

$$\alpha\frac{\left|H\right\rangle - \left|V\right\rangle}{\sqrt{2}}\left|3\right\rangle - \beta\frac{\left|H\right\rangle + \left|V\right\rangle}{\sqrt{2}}\left|3\right\rangle + \sqrt{\frac{2}{3}}\left|V\right\rangle\left|1\right\rangle, \tag{3.54}$$

and then the PBS, at which output the state is

$$\left|\phi_{out}\right\rangle = \frac{1}{\sqrt{2}}\left(\alpha + \frac{1}{\sqrt{3}}\beta\right)\left|H\right\rangle\left|3\right\rangle + \frac{1}{\sqrt{2}}\left(\alpha - \frac{1}{\sqrt{3}}\beta\right)\left|V\right\rangle\left|2\right\rangle + \sqrt{\frac{2}{3}}\beta\left|V\right\rangle\left|1\right\rangle. \tag{3.55}$$

The measurement on the computational basis of the ancilla qutrit gives, for the different outputs, the probabilities

$$\mathbb{P}(1) = \mathrm{Tr}\left[\left(I_2 \otimes \left|1\right\rangle\left\langle 1\right|\right)\left|\phi_{out}\right\rangle\left\langle\phi_{out}\right|\right] = \frac{2}{3}|\beta|^2, \tag{3.56}$$

$$\mathbb{P}(2) = \mathrm{Tr}\left[\left(I_2 \otimes \left|2\right\rangle\left\langle 2\right|\right)\left|\phi_{out}\right\rangle\left\langle\phi_{out}\right|\right] = \frac{1}{2}\left|\alpha - \frac{1}{\sqrt{3}}\beta\right|^2, \tag{3.57}$$

$$\mathbb{P}(3) = \mathrm{Tr}\left[\left(I_2 \otimes \left|3\right\rangle\left\langle 3\right|\right)\left|\phi_{out}\right\rangle\left\langle\phi_{out}\right|\right] = \frac{1}{2}\left|\alpha + \frac{1}{\sqrt{3}}\beta\right|^2, \tag{3.58}$$

which is equal to $\mathbb{P}(i) = \langle\phi|\Pi_i|\phi\rangle$, with $\Pi_i = \frac{2}{3}\left|\psi_i^{\perp}\right\rangle\left\langle\psi_i^{\perp}\right|$. Therefore, the circuit in Figure 3.18 implements the POVM $\{\Pi_i\}$.

The photons are detected using silicon single-photon avalanche photo-diodes (SPADs), with dead time 21 ns and electronic jitter of ~ 800 ps FWHM. Detection events are tagged with a resolution of 81 ps.

### Results

**Data acquisition -** A two hour continuous run of the apparatus has led to the exchange of about $10^9$ raw bits within a coincidence window $\Delta t = 1.5$ ns. The coincidences $(Ai, Bj)$ between Alice's $i$ detector and Bob's $j$ detector are shown in Table 3.3 and, graphically, in Figure 3.19. The random variable $X$ is generated after the collection of all events using a Quantum Random Number Generator [113].

**Multi-pair events -** The secure key rate evaluation described in Section 3.1.4 is based on the assumption that all sent states are qubits. However, this assumption is invalid in the case of multi-pair events. Indeed, if multiple pairs are emitted within the coherence time of the down-converted photons, they are correlated in the polarization degree of freedom, therefore it could be possible for Eve, in principle, to perform some kind of photon number splitting (PNS) attack in order to get some information about the polarization

|  | $A1$ | $A2$ | $A3$ |
|---|---|---|---|
| $B1$ | 0.6 | 35.8 | 33.6 |
| $B2$ | 35.1 | 0.6 | 32.8 |
| $B3$ | 33.4 | 33.2 | 0.4 |

Table 3.3: Total number of coincidences at the different detectors (million events). The cell (Ai,Bj) corresponds to a coincidence of Alice's detector $i$ and Bob's detector $j$.

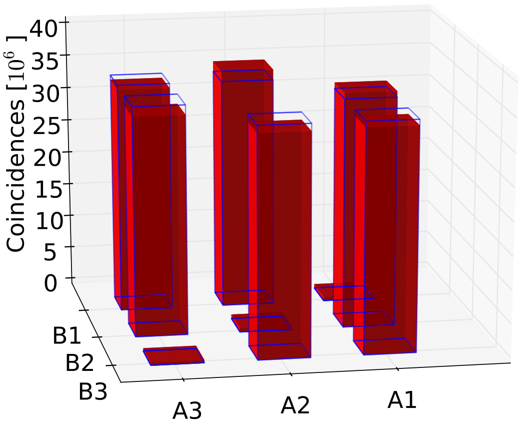

Figure 3.19: Total number of coincidences at the different detectors. Full (red) bars correspond to detected events and (blue) contours represent the expected number of detection events.

state without disturbing the system. As show in Chapter 2, the fraction of multi-pair over one-pair events is $\sim 3 \cdot 10^{-3}$ and the coherence time of the down-converted photons is $\tau_c \simeq 8\,\text{ps}$. Among all the multi-pair events within a coincidence window $\Delta t = 1.5\,\text{ns}$, only those produced within the coherence time of the down-converted photons are partially correlated [61]. Since the pair production is a spontaneous effect, it is fair to assume that pair production is uniform during the coincidence window. Therefore, the fraction of multi-pair events coming from two coherent processes is $\zeta \simeq \tau_c/\Delta t = 5 \cdot 10^{-3}$. Consequently, the fraction of correlated multi-pair events over the total number of transmitted states is $\sim 1.5 \cdot 10^{-5}$, and the information leaked to Eve through this channel is negligible.

**Post-processing block size -** In a real Quantum Key Distribution implementation, the transmission is divided into blocks of a given length and the key is processed separately for each block. Therefore, it is important to study the dependence of the $\varepsilon$-secure key rate on the dimension of the post-processing block. For the R04 protocol, this dependence is shown in Figure 3.20, where $N$ is the number of exchanged symbols. The key fraction is calculated for both collective and general attacks from Equations (3.42) and (3.43). For collective attacks, the security parameter is $\varepsilon_{col} = 4 \cdot 10^{-10}$, with $\bar{\varepsilon} = \varepsilon_{EC} = \varepsilon_{PE} = \varepsilon_{PA} = 10^{-10}$. The same security parameter has been chosen for $\varepsilon_{gen}$, therefore in that case the term $r_{col}$ is calculated with $\bar{\varepsilon} = \varepsilon_{EC} = \varepsilon_{PE} = \varepsilon_{PA} = \frac{10^{-10}}{(N+1)^3}$. The plot shows that at least $10^4$ - $10^5$ signals are required to generate a secure key, while already $N = 10^6$ (slightly more than half a minute at 29 kHz) gives a reasonable key fraction. The difference between collective and general attacks tends to disappear for $N \to \infty$, where both approach the asymptotic

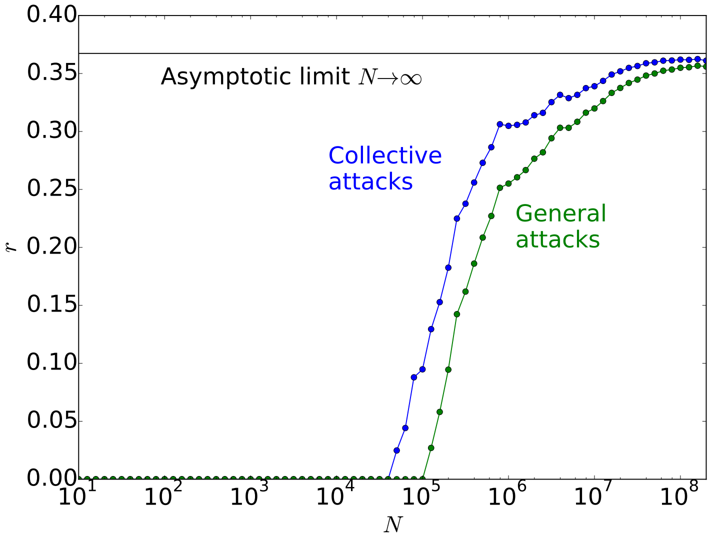

Figure 3.20: Finite key rate as a function of the post-processing block size. The y-axis represent the fraction of exchanged symbols giving a secure key. Each point is calculated using the first $N$ exchanged symbols. The security parameter for both collective and general attacks is fixed to $4 \cdot 10^{-10}$.

key fraction.

**Secret key rate -** The stability of the system during the two hour acquisition has been studied by calculating the QBER and evaluating the key rate both in the asymptotic and in the finite-key scenario against general attacks, obtaining the results shown in Figure 3.21. The system shows a slight decrease in the sifted key rate due to a misalignment in the coupling of the entangled source. The losses, estimated from the ratio of coincidences over single counts, correspond to 13 dB, 1.5 dB due to the POVM, $\sim$ 2.2 dB from the detectors [114] and the remaining 9.3 dB from the fiber coupling of down-converted photons in the Sagnac source (this value should be compared with the one of Chapter 2).

The QBER is estimated as $Q = \frac{1-2I}{1-I}$, where $I$ is the fraction of inconclusive events. It is stable at a level below 2% during the whole acquisition, thus confirming the stability of both the source and the implementation of the POVM. The higher contribution to the QBER is given by the source, whose visibility, measured just before the experiment, was between 97% and 98% in two mutually unbiased bases. However, a small contribution to the QBER is also due to the small imbalances between the channels of the POVM, which vary between 0.95 and 1.05. These imbalances are in line with previous implementations of the POVM [112].

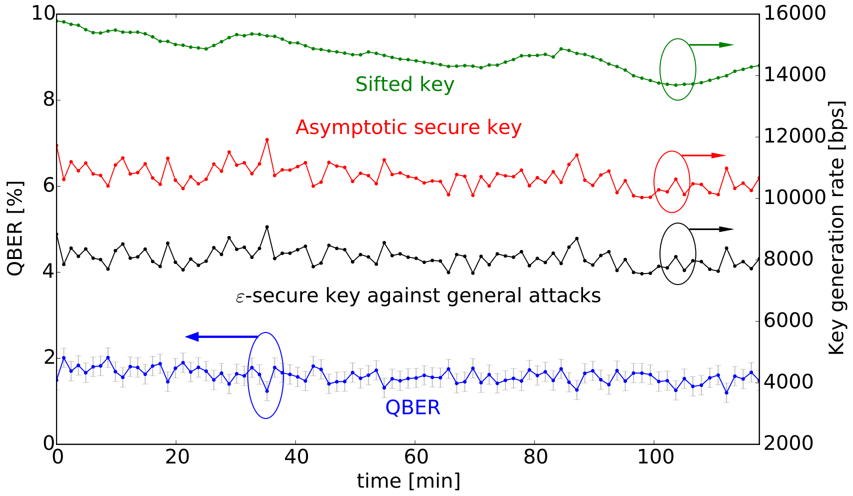

Figure 3.21: Results obtained during 2 hours of continue acquisition. The time has been divided into 90 blocks of about 80 s each, with a mean number of $1.1 \cdot 10^6$ sifted bits per block. The QBER is estimated from inconclusive events and is shown with Poissonian error bars. The asymptotic key rate is estimated using Equation (3.44), while the finite key rate is evaluated using Equations (3.43) and (3.42), with $\varepsilon_{gen} = 10^{-10}$.

## 3.2 Double violation of the CHSH inequality

The measurement process on a quantum system is very different from the classical one. The difference, as stated by Postulate 5, lies in the fact that the result of the measurement is intrinsically probabilistic and the act of measurement irredeemably destroys the measured state, making it collapse into the eigenspace corresponding to the measured value. This feature is present also in the generalized measurement framework described in Section 1.3.2, where the measurement on the ancilla subsystem collapses it into one of its eigenvectors, disturbing also the system under measurement. In general, it can be demonstrated that the quantity of information about a system that it is possible to get through a measurement is proportional to the disturbance on that measurement, something known as *information/disturbance trade-off* [54].

In this Section, this trade-off will be studied in its relationship with another peculiar aspect of quantum mechanics: non-locality. After a short review of Bell's inequalities, a fundamental tool to rule out the possibility of describing a quantum model using a local hidden variable (LHV) model, and of the information-disturbance trade-off, we will show how it is possible to make two independent users, measuring the same subsystem of an entangled state, appear non-locally correlated with a third user, measuring the other subsystem [115].

### 3.2.1 Bell's inequalities

Probably one of the most strange phenomena emerging from quantum mechanics is entanglement. Indeed, the fact that the state of a compound system cannot be described by separately describing its subsystems is something completely out of classical logic. In particular, by applying Postulate 5 to one of the Bell states of Equation (1.9), a measurement of the first subsystem makes the second one immediately collapse in a precise state, dependent on the result of the measurement, no matter how distant the two subsystems are.

This aspect was pointed out already in 1935 by Einstein, Podolsky and Rosen in their famous article *"Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?"* [116], where they arrive to the conclusion that quantum mechanics is not complete. Starting from a classical notion of *reality*, they state that

> *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to thus physical quantity.*

Then, they define *complete* a theory where

> [. . . ] *every element of the physical reality must have a counterpart in the physical theory.*

They analyze a single-particle system, that according to quantum mechanics is completely described by the wave function[9], and show that its position and momentum cannot have both physical reality, since, being non-commuting observables, the precise knowledge of one precludes such a knowledge of the other. The analysis of a single-particle system makes them conclude that

> [. . . ] either (1) *the quantum mechanical description of reality given by the wave function is not complete* or (2) *when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality.*

Subsequently, they study the situation of a two-particle system, whose wave function has been entangled by interaction and placed at a distance not allowing communication among them. According to quantum mechanics, a position measurement on the first one makes the second one collapse in a position eigenstate (so, according to their definition, position is an element of reality for the second particle). But, at the same time, a momentum measurement on the first particle puts the second one in a momentum eigenstate, therefore also momentum must be an element of reality. Since the wave function of the second particle cannot be modified by the measurement on the first one, they conclude that quantum mechanics must not be complete.

According to this view, quantum mechanics is just a theory emerging from a deeper, fundamental theory, just like thermodynamics emerges from classical mechanics. The probabilistic aspect of the measurement would then be just due to the lack of knowledge of the variables of this fundamental theory, which are therefore called *hidden variables.* A fundamental restriction into the possible fundamental theories was given by John Bell in his 1964 paper [117]. In his work, he found an inequality that all such theories based on *local hidden variables* (LHV) must satisfy. This inequality is one of a wider class of Bell-like inequalities that all LHV theories must satisfy. The following exposition of Bell-like inequalities will be mainly taken from a recent review from Brunner *et al.* [118].

The main feature of LHV theories is that they are described by a series of variables whose behaviour is *local*, meaning that they are not influenced by what happens in regions of space-time not causally connected with them. Within such theories, the correlation between the two systems must depend on a hidden variable $\lambda$ that, being local, must

[9] The wave function is a representation of the state of a system.

be established in the region of interaction between the two systems[10]. The two systems are then sent into two space-like separated regions of space-time and measured there by two observers, Alice and Bob, who choose the measurement among a set of measurements, labeled by an index $\{1, \cdots, m\}$. By indicating $x$ and $y$ the indices chosen by Alice and Bob and $a, b \in \{1, \cdots, \Delta\}$ the result of their measurements, the joint distribution, conditioned on the hidden variable $\lambda$, is

$$\mathbb{P}(ab|xy, \lambda) = \mathbb{P}(a|x, \lambda)\mathbb{P}(b|y, \lambda), \tag{3.59}$$

where the factorization is due to the independence of both $a$ and $x$ from what happens at Bob's side (and vice-versa). By assuming that the measurements are freely chosen, so that $x$ and $y$ are independent from $\lambda$, the distribution of the hidden variable can be written as $q(\lambda|xy) = q(\lambda)$. The joint probability distribution is therefore given by the ensemble average on $\lambda$,

$$\mathbb{P}(ab|xy) = \int d\lambda q(\lambda)\mathbb{P}(a|x, \lambda)\mathbb{P}(b|y, \lambda). \tag{3.60}$$

For the experiments with entangled qubits, the most relevant Bell-like inequalities use two measurement choices per observer $x, y \in \{0, 1\}$, with each measurement giving two possible results $a, b \in \{-1, 1\}$. Given a choice of the measurement setup $(x, y)$, the mean value of the product of the measurement results is

$$\langle a_x b_y \rangle = \sum_{a,b} ab\mathbb{P}(ab|xy), \tag{3.61}$$

which, for LHV theories, becomes

$$\begin{aligned} \langle a_x b_y \rangle &= \sum_{a,b} ab \int d\lambda q(\lambda)\mathbb{P}(a|x, \lambda)\mathbb{P}(b|y, \lambda) && (3.62)\\ &= \int d\lambda q(\lambda) \left(\sum_a a\mathbb{P}(a|x, \lambda)\right) \left(\sum_b b\mathbb{P}(b|y, \lambda)\right) && (3.63)\\ &= \int d\lambda q(\lambda) \langle a_x \rangle_\lambda \langle b_y \rangle_\lambda . && (3.64) \end{aligned}$$

The most famous of these inequalities, the Clauser-Horne-Shimony-Holt (CHSH) inequality, is based on a linear combination of these mean values and is given by

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \leq 2, \tag{3.65}$$

where the inequality comes from inserting (3.64) into (3.65) and noticing that, since $a, b \in \{-1, 1\}$, then $\langle a_x \rangle_\lambda , \langle b_y \rangle_\lambda \in [-1, 1]$. Therefore, Bell-like inequalities pose a constraint on the correlations that are possible for LHV theories, included such possible extensions of quantum mechanics.

For quantum mechanics, there exist systems that violate the inequality (3.65). Indeed, taking a two-qubit entangled system in the singlet state $|\Psi^-\rangle = (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)/\sqrt{2}$, it can be shown that, by measuring systems $A$ and $B$ in the bases described by the Bloch sphere vectors $\vec{x}$ and $\vec{y}$, the value of the mean value (3.61) is given by $\langle a_x b_y \rangle = -\vec{x} \cdot \vec{y}$ (see Appendix A). By choosing the measurement bases corresponding to the Bloch sphere

[10] The hidden variable $\lambda$ is not restricted to a real variable, but can generally be a vector.

axes $X$ and $Z$ for Alice and $(-X+Z)\sqrt{2}$ and $-(X+Z)\sqrt{2}$ for Bob, we have $\langle a_0 b_0\rangle = \langle a_0 b_1\rangle = \langle a_1 b_0\rangle = 1/\sqrt{2}$ and $\langle a_1 b_1\rangle = -1/\sqrt{2}$, from which

$$S = 2\sqrt{2}, \tag{3.66}$$

that violates the LHV bound. Therefore, by proving that $S > 2$, it is possible to rule out the possibility of a LHV theory as completion of quantum mechanics[11]. The first experimental violation of a Bell-like inequality dates back to the 1972 [120], but the non-ideality of the experimental setup still allowed an interpretation using LHV theories (such imperfections are called *loopholes*). The technological advancement, however, allowed the implementation of loophole-free experiments [45–47], that finally close all possibilities of extension of quantum mechanics with a LHV theory.

### 3.2.2 Generalized measurement and information/disturbance trade-off

In the general measurement scheme, described in Section 1.3.2 and shown in Figure 3.22, the qubit to be measured, the *signal* qubit $\rho_S$, interacts with a *probe* qubit through a unitary operator $U$. By changing the unitary $U$, it is possible to tune the information/disturbance trade-off. The minimal information gain happens when the unitary is factorisable into $U = U_S \otimes U_P$. In this case, since there is no interaction between the system and the probe, the state after the unitary is still separable and the measurement on the probe qubit reveals no information about it. The opposite case happens when the unitary $U$ is such that the joint state is a maximally entangled state. In this case, a measurement on the probe state is equivalent to a strong measurement on the system (like the one described in Postulate 5), and the state describing post-interaction system $\rho'_S$ is a classical mixture (the density matrix $\rho'_S$ is diagonal). In all other cases, when the joint state is neither separable nor maximally entangled, the measurement gives less information than the strong measurement, but the post-measurement state is no longer a classical mixture, and has still some coherence left. Therefore, by tuning the interaction between the system and the probe, it is possible to obtain the wished trade-off between information gain and system disturbance.

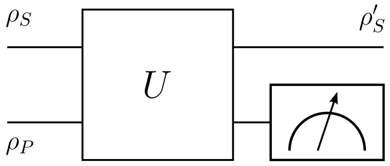

Figure 3.22: Schematic representation of a generalized measurement, that exploits a *probe* qubit to gain information about a *signal* qubit.

### 3.2.3 Multiple violation of the CHSH inequality

Other than proving the impossibility of extending quantum theory using LHV completions, Bell-like inequalities like the CHSH can be also used to study the presence of non-local (i.e., non classical) correlations between systems. In the simple case of two observers, reviewed in Section 3.2.1, the violation of one of these inequalities is an index of the fact that the two systems are sharing a non-local joint probability distribution.

[11] This, however, does not rule out theories based on non-local hidden variables, like the De Broglie-Bohm theory [119].

The situation complicates when more than two parties are involved. Anyhow, it has been demonstrated that, in the case of three non-signaling parties Alice, Bob and Charlie, it is impossible that more than two of them are non-locally correlated, a phenomenon called *monogamy* [118, 121].

A recent work by Silva, *et al.* [122], however, looks at the matter from another point of view. It drops the hypothesis of non-signaling between the parties and investigates whether non-locality can be shared by more than two independent observers. In order to answer the question, they study a tripartite system like the one shown in Figure 3.23, where a pair of photons is shared between Alice and a couple of observers, Bob and Charlie (Bob2 and Bob1, respectively, in the original work). In this scenario, Charlie is placed on the route between the source and Bob and performs a general measurement by making the system $\rho_S$ flying to Bob interact with its own ancilla system and routing the resulting $\rho'_S$ to Bob, which performs a strong measurement. In some sense, the role of Charlie is analogous to the one of Eve in Quantum Key Distribution. The result of the work is the theoretical demonstration that it is indeed possible to share the non-locality between Alice and the two independent observers Bob and Charlie, by precisely tuning the interaction of $\rho_s$ with Charlie's ancilla system. They also study different types of generalized measurement settings, showing that not only it is important to tune the interaction between the system and Charlie's ancilla, but it is also necessary to choose the right type of interaction in order to see both Bob and Charlie share a non-local joint probability distribution with Alice. Except for that, both Charlie and Bob perform a standard CHSH measurement with unbiased basis choices, therefore this result does not require previous agreement between Charlie and Bob.

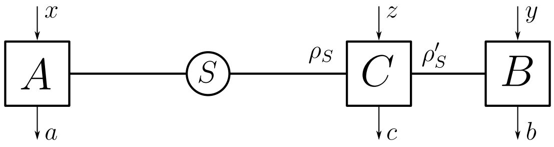

Figure 3.23: General scheme of the tripartite system Alice-Charlie-Bob under exam.

This double non-locality is not a violation of the monogamy of non-locality because, despite being independent, Bob and Charlie are not non-signaling, since the state received by Bob is dependent on the measurement choice by Charlie and, therefore, Charlie can be seen as implicitly signaling this information to Bob.

The same article shows that such a result is possible only in presence of a single Charlie between Alice and Bob. In order to have non-locality with a chain of Charlies between Alice and Bob, it is necessary to perform a biased choice of the measurements of both Bob and the Charlies, thus requiring a previous agreement between the parties before conducting the experiment. This result, only conjectured in Silva's article, has subsequently been analytically proven [123].

### 3.2.4 The circuit model of the experiment

This Section will deal with the circuit model of the generalized measurement chosen to show experimentally the double violation of the CHSH inequality, used as a mean to demonstrate the non-locality between Alice and Bob and Alice and Charlie [115]. The chosen setup exploits a control-phase-shift gate, where the target qubit is Charlie's ancilla system and the control qubit is the qubit flying from Alice to Bob, as shown in the circuit representation of the measurement of Figure 3.24. This scheme implements a generalized

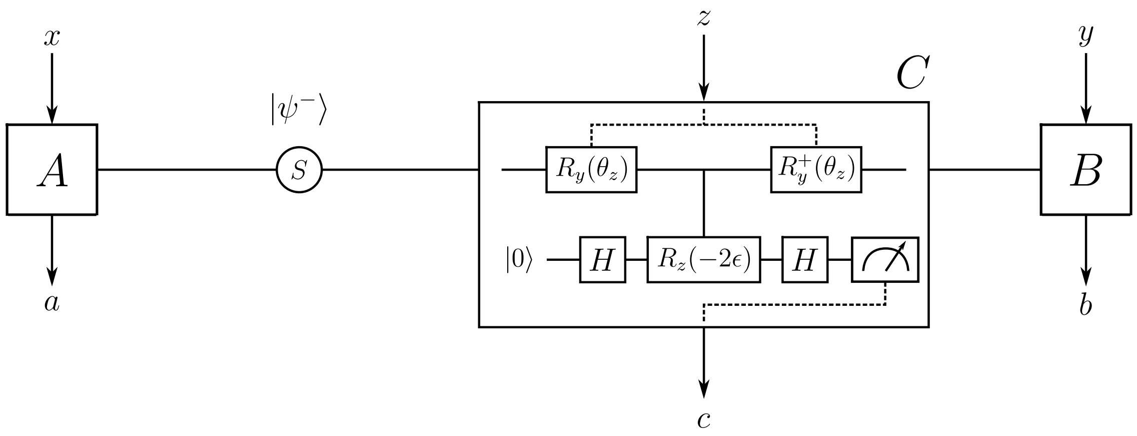

Figure 3.24: Circuit model of the measurement used to demonstrate the double violation of the CHSH inequality.

measurement of the qubit flying to Bob in the computational basis, therefore it is necessary to implement a rotation $R_y(\theta_z)$ before the interaction (and the inverse rotation $R_y^\dagger(\theta_z)$ after it).

The effect of the general measurement setup on the singlet state $|\Psi^-\rangle$ can be understood by simply studying the joint effect of Charlie's and Bob's measurements on the state remaining after Alice's measurement.

### Alice's measurement

If Alice measures her photon in the basis $\left\{|u_x\rangle, |u_x^\perp\rangle\right\}$, where $x \in \{0,1\}$, she projects the other photon onto $|u_x^\perp\rangle$ if she gets $a = +1$ and $|u_x\rangle$ if she gets $a = -1$. Therefore, the state of the photon sent to Bob is $|\psi_{|xa}\rangle = |u_x^{-a}\rangle$, defined as

$$|u_x^{-a}\rangle = \begin{cases} |u_x^\perp\rangle & \text{if } a = 1 \\ |u_x\rangle & \text{if } a = -1 \end{cases}. \tag{3.67}$$

### Charlie's measurement

First of all, Charlie ($C$) chooses a measurement basis $\{|w_z\rangle, |w_z^\perp\rangle\}$, with $z \in \{0,1\}$ his basis choice. The state $|\psi_{|xa}\rangle = |u_x^{-a}\rangle$ entering his setup can be written in this basis as

$$|\psi_{|xa}\rangle = |w_z\rangle \langle w_z|u_x^{-a}\rangle + |w_z^\perp\rangle \langle w_z^\perp|u_x^{-a}\rangle = \alpha\, |w_z\rangle + \beta\, |w_z^\perp\rangle\,, \tag{3.68}$$

with $\alpha$ and $\beta$ given by

$$\alpha = \langle w_z|u_x^{-a}\rangle\,, \text{ and} \tag{3.69}$$

$$\beta = \langle w_z^\perp|u_x^{-a}\rangle\,. \tag{3.70}$$

At the entrance of Charlie's measurement setup, the state is in the product state $|\psi_{|xa}\rangle \otimes |0\rangle$, which becomes $|\psi_{|xa}\rangle \otimes |+\rangle$ after the ancilla undergoes the Hadamard gate $H$. The measurement chosen by Charlie is implemented by rotating the state with $R_y(\theta_z)$, with $\theta_z$ such that

$$R_y(\theta_z)\, |w_z\rangle = |0\rangle\,, \tag{3.71}$$

$$R_y(\theta_z)\,|w_z^{\perp}\rangle = |1\rangle\,. \tag{3.72}$$

The state is thus transformed into $(R_y(\theta_z)\otimes I_2)\,|\psi_{|xa}\rangle \otimes |+\rangle = \big(\alpha\,|0\rangle + \beta\,|1\rangle\big)\otimes|+\rangle$.

The two qubits are entangled by the controlled-phase-shift gate $CP(\epsilon)$, whose action is

$$\begin{aligned} CP(\epsilon)\left[\big(\alpha\,|0\rangle + \beta\,|1\rangle\big)\otimes|+\rangle\right] &= \alpha\,|0\rangle\,|+\rangle + \beta\,|1\rangle\,\frac{e^{i\epsilon}\,|0\rangle + e^{-i\epsilon}\,|1\rangle}{\sqrt{2}} \\ &= \alpha\,|0\rangle\,|+\rangle + \beta\,|1\rangle\,\big(\cos\epsilon\,|+\rangle + i\sin\epsilon\,|-\rangle\big)\,. \end{aligned} \tag{3.73}$$

Before exiting Charlie's measurement setup, the state is rotated back by applying $R_y^{\dagger}(\theta_z)$, giving

$$\begin{aligned} |\psi_{|xza}\rangle &= \left(R_y^{\dagger}(\theta_z)\otimes I_2\right)\alpha\,|0\rangle\,|+\rangle + \beta\,|1\rangle\,\big(\cos\epsilon\,|+\rangle + i\sin\epsilon\,|-\rangle\big) \\ &= \alpha\,|w_z\rangle\otimes|+\rangle + \beta\,|w_z^{\perp}\rangle\otimes\big(\cos\epsilon\,|+\rangle + i\sin\epsilon\,|-\rangle\big) \\ &= \langle w_z|u_x^{-a}\rangle\,|w_z\rangle\otimes|+\rangle + \langle w_z^{\perp}|u_x^{-a}\rangle\,|w_z^{\perp}\rangle\otimes\big(\cos\epsilon\,|+\rangle + i\sin\epsilon\,|-\rangle\big)\,, \end{aligned} \tag{3.74}$$

whose corresponding density matrix is $\rho_{|xza} = |\psi_{|xza}\rangle\,\langle\psi_{|xza}|$.

Charlie extracts the information from the state by measuring its ancilla in the basis $\{|+\rangle\,, |-\rangle\}$, using the POVM $\{I_2\otimes|+\rangle\,\langle+|\,, I_2\otimes|-\rangle\,\langle-|\}$, that returns $c\in\{+1,-1\}$, with $c=+1$ corresponding to $|+\rangle$ and $c=-1$ to $|-\rangle$.

From these measurements, he can calculate the probability distribution of the outcomes of his measurements, conditioned on Alice's results, as

$$\mathbb{P}(+|xz+) = \mathrm{Tr}\left[\big(I_2\otimes|+\rangle\,\langle+|\big)\,|\psi_{|xza}\rangle\,\langle\psi_{|xza}|\right] \tag{3.75}$$

$$= \left|\langle w_z|u_x^{\perp}\rangle\right|^2 + \cos^2\epsilon\left|\langle w_z^{\perp}|u_x^{\perp}\rangle\right|^2 = \frac{1}{2}\,(1-\vec{u}_x\cdot\vec{w}_z) + \frac{1}{2}\cos^2\epsilon\,(1+\vec{u}_x\cdot\vec{w}_z)\,, \tag{3.76}$$

$$\mathbb{P}(+|xz-) = \left|\langle w_z|u_x\rangle\right|^2 + \cos^2\epsilon\left|\langle w_z^{\perp}|u_x\rangle\right|^2 = \frac{1}{2}\,(1+\vec{u}_x\cdot\vec{w}_z) + \frac{1}{2}\cos^2\epsilon\,(1-\vec{u}_x\cdot\vec{w}_z)\,, \tag{3.77}$$

$$\mathbb{P}(-|xz+) = \left|\langle w_z^{\perp}|u_x^{\perp}\rangle\right|^2\sin^2\epsilon = \frac{1}{2}\sin^2\epsilon\,(1+\vec{u}_x\cdot\vec{w}_z)\,, \tag{3.78}$$

$$\mathbb{P}(-|xz-) = \left|\langle w_z^{\perp}|u_x\rangle\right|^2\sin^2\epsilon = \frac{1}{2}\sin^2\epsilon\,(1-\vec{u}_x\cdot\vec{w}_z)\,, \tag{3.79}$$

that can be summarized in the formula

$$\mathbb{P}(c|xza) = \frac{1}{2}\left[1 + c - c\sin^2\epsilon\,(1 + a\vec{u}_x\cdot\vec{w}_z)\right]\,, \tag{3.80}$$

where the vector $\vec{u}$ is the Bloch sphere representation of the state $|u\rangle$ and the calculations are based on the results exposed in Appendix A. The joint probability distribution of Alice and Charlie is given by

$$\begin{aligned} \mathbb{P}(ac|xz) = \mathbb{P}(c|xza)\mathbb{P}(a|x) &= \frac{1}{4}\left[1 + c - c\sin^2\epsilon\,(1 + a\vec{u}_x\cdot\vec{w}_z)\right] \\ &= \frac{1}{4} + \frac{c}{4}\left(1 - \sin^2\epsilon\right) - \frac{ac}{4}\sin^2\epsilon\,(\vec{u}_x\cdot\vec{w}_z)\,, \end{aligned} \tag{3.81}$$

where we used the fact that Alice and Charlie are non-signaling, so the result of Alice's measurement does not depend on Charlie's measurement ($\mathbb{P}(a|xz) = \mathbb{P}(a|x)$), and the fact that $\mathbb{P}(a|x) = \frac{1}{2}$ for every Alice's choice $x$.

The net effect of Charlie's measurement setup is to entangle his ancilla qubit with the one flying towards Bob. The state sent to Bob, therefore, is no longer a pure qubit, but is described by the reduced density matrix of the joint system

$$\begin{aligned}\rho_{|xza} &= \mathrm{Tr}_C \left( |\psi_{|xza}\rangle \langle \psi_{|xza}| \right) \\ &= \left| \langle w_z | u_x^{-a} \rangle \right|^2 |w_z\rangle \langle w_z| + \cos\epsilon \left( \langle w_z | u_x^{-a} \rangle \langle u_x^{-a} | w_z^{\perp} \rangle |w_z\rangle \langle w_z^{\perp}| \right. \\ &+ \left. \langle w_z^{\perp} | u_x^{-a} \rangle \langle u_x^{-a} | w_z \rangle |w_z^{\perp}\rangle \langle w_z| \right) + \left| \langle w_z^{\perp} | u_x^{-a} \rangle \right|^2 |w_z^{\perp}\rangle \langle w_z^{\perp}| \,.\end{aligned} \tag{3.82}$$

### Bob's measurement

Bob performs a projective measurement in the basis $\{|v_y\rangle, |v_y^{\perp}\rangle\}$, with $y \in \{0,1\}$, on the state $\rho_{|xza}$ arriving from Charlie's measurement apparatus. Since this state is explicitly dependent on Charlie's measurement basis, and Bob is acting independently from him, it is necessary to average over all the possible Charlie's bases. The resulting joint probability distribution is therefore

$$\mathbb{P}(ab|xy) = \sum_{z=0,1} \mathbb{P}(abz|xy) = \sum_{z=0,1} \mathbb{P}(b|xyza)\mathbb{P}(a|x)\mathbb{P}(z), \tag{3.83}$$

where $\mathbb{P}(a|x) = \frac{1}{2}$, and $\mathbb{P}(z) = \frac{1}{2}$ because we are assuming that all users apply an unbiased measurement strategy. Using the explicit values for the probabilities and calculating the conditioned probability

$$\begin{aligned}\mathbb{P}(b|xyza) &= \mathrm{Tr}\left[ |v_y^b\rangle \langle v_y^b| \, \rho_{|xza} \right] \\ &= \langle v_y^b | w_z \rangle \langle w_z | u_x^{-a} \rangle \langle u_x^{-a} | w_z \rangle \langle w_z | v_y^b \rangle + \cos\epsilon \left[ \langle v_y^b | w_z \rangle \langle w_z | u_x^{-a} \rangle \langle u_x^{-a} | w_z^{\perp} \rangle \langle w_z^{\perp} | v_y^b \rangle \right. \\ &+ \left. \langle v_y^b | w_z^{\perp} \rangle \langle w_z^{\perp} | u_x^{-a} \rangle \langle u_x^{-a} | w_z \rangle \langle w_z | v_y^b \rangle \right] + \langle v_y^b | w_z^{\perp} \rangle \langle w_z^{\perp} | u_x^{-a} \rangle \langle u_x^{-a} | w_z^{\perp} \rangle \langle w_z^{\perp} | v_y^b \rangle \\ &= \langle u_x^{-a}| \left[ |w_z\rangle \langle w_z| \left| \langle w_z | v_y^b \rangle \right|^2 + |w_z^{\perp}\rangle \langle w_z^{\perp}| \left| \langle w_z^{\perp} | v_y^b \rangle \right|^2 \right] |u_x^{-a}\rangle \left(1 - \cos\epsilon\right) \\ &+ \cos\epsilon \left( \left| \langle u_x^{-a} | v_y^b \rangle \right|^2 \right) \\ &= \langle u_x^{-a}| \left[ \frac{1}{2} I + \frac{1}{2} b \vec{w}_z \cdot \vec{v}_y \left( |w_z\rangle \langle w_z| - |w_z^{\perp}\rangle \langle w_z^{\perp}| \right) \right] |u_x^{-a}\rangle \left(1 - \cos\epsilon\right) \\ &+ \frac{1}{2} \cos\epsilon \left(1 - ab \vec{v}_y \cdot \vec{u}_x\right) \\ &= \frac{1}{2}\left(1 - \cos\epsilon\right) + \frac{1}{2} b \vec{w}_z \cdot \vec{v}_y \left[ \left| \langle u_x^{-a} | w_z \rangle \right|^2 - \left| \langle u_x^{-a} | w_z^{\perp} \rangle \right|^2 \right] \left(1 - \cos\epsilon\right) \\ &+ \frac{1}{2} \cos\epsilon \left(1 - ab \vec{v}_y \cdot \vec{u}_x\right) \\ &= \frac{1}{2}\left(1 - \cos\epsilon\right) + \frac{1}{2} b \vec{w}_z \cdot \vec{v}_y \left[ \frac{1}{2} - \frac{1}{2} a \vec{u}_x \cdot \vec{w}_z - \frac{1}{2} - \frac{1}{2} a \vec{u}_x \cdot \vec{w}_z \right] \left(1 - \cos\epsilon\right) \\ &+ \frac{1}{2} \cos\epsilon \left(1 - ab \vec{v}_y \cdot \vec{u}_x\right) \\ &= \frac{1}{2} \left[ 1 - \cos\epsilon - \left(1 - \cos\epsilon\right) ab \left(\vec{w}_z \cdot \vec{v}_y\right) \left(\vec{u}_x \cdot \vec{w}_z\right) + \cos\epsilon - \cos\epsilon \cdot ab \vec{v}_y \cdot \vec{u}_x \right] \\ &= \frac{1}{2} \left[ 1 - ab \left(\vec{w}_z \cdot \vec{v}_y\right) \left(\vec{u}_x \cdot \vec{w}_z\right) + \cos\epsilon \cdot ab \left(\vec{v}_y \cdot \vec{w}_z\right) \left(\vec{u}_x \cdot \vec{w}_z\right) - \cos\epsilon \cdot ab \vec{v}_y \cdot \vec{u}_x \right]\end{aligned} \tag{3.84}$$

$$= \frac{1}{2}\left[1 - ab\cos\epsilon\left(\vec{u}_x \cdot \vec{v}_y\right) - ab\left(1-\cos\epsilon\right)\left(\vec{u}_x \cdot \vec{w}_z\right)\left(\vec{w}_z \cdot \vec{v}_y\right)\right],$$

it is possible to calculate the joint probability distribution as

$$\begin{aligned}\mathbb{P}(ab|xy) &= \sum_z \frac{1}{8}\left[1 - ab\cos\epsilon\left(\vec{u}_x \cdot \vec{v}_y\right) - ab\left(1-\cos\epsilon\right)\left(\vec{u}_x \cdot \vec{w}_z\right)\left(\vec{w}_z \cdot \vec{v}_y\right)\right] \\ &= \frac{1}{4} - \frac{1}{8}ab\left[\cos\epsilon\left(\vec{u}_x \cdot \vec{v}_y\right) + \left(1-\cos\epsilon\right)\left(\vec{u}_x \cdot \vec{w}_z\right)\left(\vec{w}_z \cdot \vec{v}_y\right)\right].\end{aligned} \tag{3.85}$$

### Basis choice and CHSH parameter

From the joint probabilities $\mathbb{P}(ac|xz)$ and $\mathbb{P}(ab|xy)$, the couples Alice-Charlie and Alice-Bob can compute, independently, the respective CHSH parameters $S_{AC} = \langle a_0c_0\rangle + \langle a_0c_1\rangle + \langle a_1c_0\rangle - \langle a_1c_1\rangle$ and $S_{AB} = \langle a_0b_0\rangle + \langle a_1b_0\rangle + \langle a_0b_1\rangle - \langle a_1b_1\rangle$, with

$$\langle a_xc_z\rangle = \sum_{a,c=\pm1} ac\mathbb{P}(ac|xz) \text{ and } \langle a_xb_y\rangle = \sum_{a,b=\pm1} ab\mathbb{P}(ab|xy). \tag{3.86}$$

It can be shown that, given a probability of the form $P(ab|xy) = \Gamma_{0|xy} + a\Gamma_{1|xy} + b\Gamma_{2|xy} + ab\Gamma_{3|xy}$, the value of the expectation value is $\langle a_xb_y\rangle = 4\Gamma_{3|xy}$. Since both joint probabilities (3.81) and (3.85) are written in this form, the expectation values can be written as

$$\langle a_xc_z\rangle = -\sin^2\epsilon\left(\vec{u}_x \cdot \vec{w}_z\right), \text{ and} \tag{3.87}$$

$$\langle a_xb_y\rangle = -\sum_z \frac{1}{2}\left[\cos\epsilon\left(\vec{u}_x \cdot \vec{v}_y\right) + \left(1-\cos\epsilon\right)\left(\vec{u}_x \cdot \vec{w}_z\right)\left(\vec{w}_z \cdot \vec{v}_y\right)\right]. \tag{3.88}$$

The corresponding values of the CHSH parameter are

$$S_{AC} = \Theta_0 \sin^2\epsilon \tag{3.89}$$

$$S_{AB} = \Theta_1\cos\epsilon + \Theta_2(1-\cos\epsilon) = \Theta_2 + (\Theta_1 - \Theta_2)\cos\epsilon, \tag{3.90}$$

with

$$\Theta_0 = -\left(\vec{u}_0 \cdot \vec{w}_0 + \vec{u}_1 \cdot \vec{w}_0 + \vec{u}_0 \cdot \vec{w}_1 - \vec{u}_1 \cdot \vec{w}_1\right), \tag{3.91}$$

$$\Theta_1 = -\left(\vec{u}_0 \cdot \vec{v}_0 + \vec{u}_1 \cdot \vec{v}_0 + \vec{u}_0 \cdot \vec{v}_1 - \vec{u}_1 \cdot \vec{v}_1\right), \tag{3.92}$$

$$\begin{aligned}\Theta_2 = -\sum_z \frac{1}{2}&\left[(\vec{u}_0 \cdot \vec{w}_z)(\vec{v}_0 \cdot \vec{w}_z) + (\vec{u}_1 \cdot \vec{w}_z)(\vec{v}_0 \cdot \vec{w}_z) + (\vec{u}_0 \cdot \vec{w}_z)(\vec{v}_1 \cdot \vec{w}_z)\right. \\ &\left. - (\vec{u}_1 \cdot \vec{w}_z)(\vec{v}_1 \cdot \vec{w}_z)\right].\end{aligned} \tag{3.93}$$

In order to find out the measurement bases that maximize the violation of both CHSH inequalities $S_{AC} \leq 2$ and $S_{AB} \leq 2$, it is convenient to rewrite the Equations (3.89) and (3.90) by using the parameter $x = \sin^2\epsilon$, that parametrizes the strength of Charlie's measurement, obtaining

$$S_{AC}(x) = \Theta_0 x, \tag{3.94}$$

$$S_{AB}(x) = \Theta_2 + (\Theta_1 - \Theta_2)\sqrt{1-x}. \tag{3.95}$$

Since $x \in [0,1]$, the violation of Eq. (3.94) is possible only if $\Theta_0 > 0$, in which case $S_{AC}(x)$ is strictly increasing. It is also possible to restrict to the case $\Theta_1 > \Theta_2$, otherwise

Eq. (3.95) cannot be violated. Indeed, in the case $\Theta_1 \leq \Theta_2$, $S_{AB}(x)$ is monotonically increasing, but since for $x = 1$ Alice and Bob are no more nonlocal, due to the strong measurement performed by Charlie, we have $S_{AB}(1) \leq 2$, therefore $S_{AB}(x) \leq S_{AB}(1) \leq 2$. The constraints $\Theta_0 > 0$ and $\Theta_1 > \Theta_2$ implies that $S_{AC}(x)$ is increasing and $S_{AB}(x)$ is decreasing, therefore there is a unique intersection $S_{AC}(\tilde{x}) = S_{AB}(\tilde{x})$, which corresponds to the point with the most significant double violation. In order to find the bases giving the maximum simultaneous double violation, it is sufficient to maximize $S_{AC}(\tilde{x})$, for $\tilde{x} = \{x \in [0,1] \,|S_{AC}(x) = S_{AB}(x)\}$, set described by the equation

$$\tilde{x} = \beta - \frac{1}{2}(\alpha - \beta)^2 + \frac{1}{2}\sqrt{(2\beta - (\alpha-\beta)^2)^2 - 4(\beta^2 - (\alpha - \beta)^2)}, \tag{3.96}$$

where $\alpha = \Theta_1/\Theta_0$ and $\beta = \Theta_2/\Theta_0$. This is an optimization problem over the 10 free real parameters that define $\Theta_i$ in the Bloch sphere: two parameter per each of the vectors $\vec{u}_1, \vec{w}_0, \vec{w}_1, \vec{v}_0, \vec{v}_1$. The vector $\vec{u}_0$ can be omitted because of the spherical symmetry of the optimization problem. Since the problem is computationally very intensive, it is necessary to simplify it before the numerical optimization. The first simplification is choosing for $\Theta_0$ highest possible value $\Theta_0 = 2\sqrt{2}$, equivalent to choosing

$$u_0 = -\frac{Z+X}{\sqrt{2}}, \qquad w_0 = Z,$$
$$u_1 = \frac{-Z+X}{\sqrt{2}}, \qquad w_1 = X.$$

It is then possible to numerical optimize over the remaining 4 parameters $\vec{v}_0$ and $\vec{v}_1$, obtaining

$$u_0 = -\frac{Z+X}{\sqrt{2}}, \qquad w_0 = v_0 = Z,$$
$$u_1 = \frac{-Z+X}{\sqrt{2}}, \qquad w_1 = v_1 = X,$$

which correspond to the Bloch vectors

$$\begin{aligned} \vec{u}_0 &= (0,0,1)\,, & \vec{u}_0^{\perp} &= (0,0,-1)\,, \\ \vec{u}_1 &= (1,0,0)\,, & \vec{u}_1^{\perp} &= (-1,0,0)\,, \\ \vec{w}_0 = \vec{v}_0 &= \left(-\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right), & \vec{w}_0^{\perp} = \vec{v}_0^{\perp} &= \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right), \\ \vec{w}_1 = \vec{v}_1 &= \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right), & \vec{w}_1^{\perp} = \vec{v}_1^{\perp} &= \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right). \end{aligned}$$

The vectors $\vec{u}_x$, $\vec{w}_z$ and $\vec{v}_y$ lie on the same two-dimensional space, therefore $\sum_z \frac{1}{2}(\vec{u}_x \cdot \vec{w}_z)(\vec{v}_y \cdot \vec{w}_z) = \frac{1}{2}\vec{u}_x \cdot \vec{v}_z$. Consequently, $\Theta_2 = \frac{1}{2}\Theta_1$ and the inequalities become

$$S_{AC} = \Theta_0 \sin^2 \epsilon, \tag{3.97}$$

$$S_{AB} = \frac{1}{2}\Theta_1(1 + \cos\epsilon). \tag{3.98}$$

By explicitly calculating the scalar products, $\vec{u}_0 \cdot \vec{w}_0 = \vec{u}_1 \cdot \vec{w}_0 = \vec{u}_0 \cdot \vec{w}_1 = -\frac{1}{\sqrt{2}}$ and $\vec{u}_1 \cdot \vec{w}_1 = \frac{1}{\sqrt{2}}$, it is possible to find $\Theta_0 = \Theta_1 = 2\sqrt{2}$, giving

$$S_{AC} = 2\sqrt{2}\sin^2\epsilon, \tag{3.99}$$

$$S_{AB} = \sqrt{2}(1 + \cos\epsilon). \tag{3.100}$$

The maximum violation is found at $\tilde{x} = \sin^2\epsilon = 3/4$, with $S_{AC} = S_{AB} = \frac{3}{2}\sqrt{2} \sim 2.12$.

### Comparison with optimal measurement

To compare the results of our model with the theoretical model described in the article by Silva, *et al.* [122], it is necessary to study the correspondence between the two models. The model of the measurement described by Silva uses a continuous pointer $|\phi(q)\rangle$, which is interacted with a system in initial state $|\psi\rangle = \alpha |H\rangle + \beta |V\rangle$ to give the output state $\alpha |H\rangle |\phi(q-1)\rangle + \beta |V\rangle |\phi(q+1)\rangle$. The measurement is then performed on the orthogonal basis $|H(q)\rangle$ and $|H(-q)\rangle$, where $H(q)$ is the Heaviside step function (the measurement associates $+1$ to positive pointer states and $-1$ to negative ones). The measurement is then described in function of its "quality factor"

$$F = \int_{-\infty}^{+\infty} \phi(q+1)\phi(q-1)dq = \langle \phi(q+1)|\phi(q-1)\rangle , \tag{3.101}$$

and its "precision"

$$\begin{aligned} G &= \int_{-1}^{+1} \phi^2(q)dq \\ &= 1 - \int_{-\infty}^{0} \left|\phi(q-1)\right|^2 dq - \int_{0}^{+\infty} \left|\phi(q+1)\right|^2 dq \\ &= 1 - \int_{-\infty}^{+\infty} \left|H^*(-q)\phi(q-1)\right|^2 dq - \int_{-\infty}^{+\infty} \left|H^*(q)\phi(q+1)\right|^2 dq \\ &= 1 - \left|\langle H(-q)|\phi(q-1)\rangle\right|^2 - \left|\langle H(q)|\phi(q+1)\rangle\right|^2 . \end{aligned} \tag{3.102}$$

In our model, the state $|\psi\rangle = \alpha |H\rangle + \beta |V\rangle$ interacts with the measurement system giving the output state $\alpha |H\rangle |\phi_+\rangle + \beta |V\rangle |\phi_-\rangle$, where $|\phi_+\rangle = |+\rangle$ and $|\phi_-\rangle = (\cos\epsilon |+\rangle + i \sin\epsilon |-\rangle)$. The chosen measurement basis is $\{|+\rangle, |-\rangle\}$, therefore the "quality factor" of our measurement is

$$F = \langle \phi_+|\phi_-\rangle = \cos\epsilon, \tag{3.103}$$

and the "precision" is

$$\begin{aligned} G &= 1 - \left|\langle -|\phi_+\rangle\right|^2 - \left|\langle +|\phi_-\rangle\right|^2 \\ &= 1 - \left|\langle -|+\rangle\right|^2 - \left|\langle +| \left(\cos\epsilon |+\rangle + i \sin\epsilon |-\rangle\right)\right|^2 \\ &= 1 - \cos^2\epsilon = \sin^2\epsilon. \end{aligned} \tag{3.104}$$

The values of the CHSH parameter can therefore be expressed as

$$S_{AC} = 2\sqrt{2}G, \tag{3.105}$$

$$S_{AB} = \sqrt{2}(1+F). \tag{3.106}$$

It is therefore possible to compare our measurement with those proposed in [122] by looking at the two values of the CHSH parameter as a function of the measurement precision $G$, as shown in Figure 3.25. The generalized measurement described in this section implements a sub-optimal pointer type, since $F^2 + G^2 = 1 - G(1-G) \leq 1$ [122] (this expression is 1 only in the case of strong measurement by either Bob or Charlie). In this scheme, it is still possible to vary the pointer type by changing the measurement basis. Indeed, if

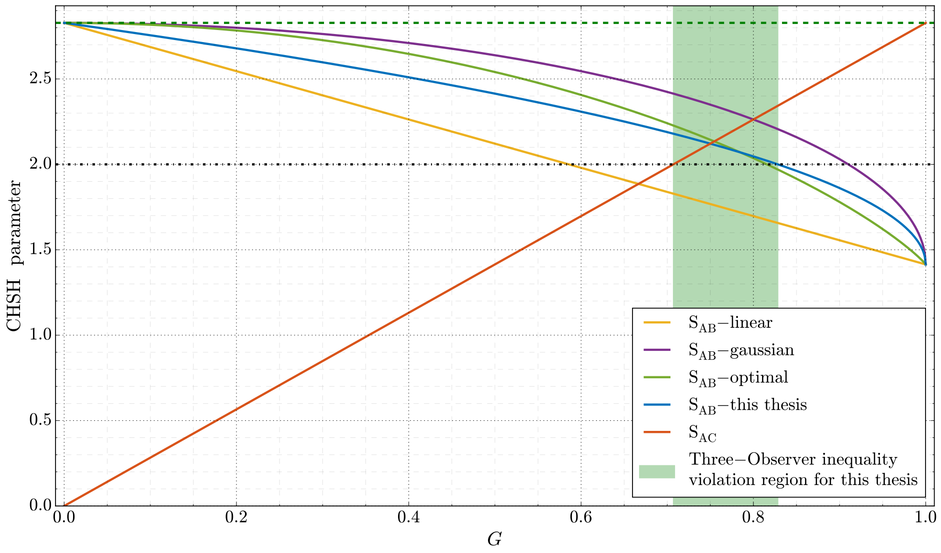

Figure 3.25: Variation of the $S_{AC}$ (red) and $S_{AB}$ for different types of pointer types. Linear (yellow), gaussian (green) and optimal (purple) pointers are taken from [122]. These pointers are compared with the generalized measurement model described in this Section (blue). The dash-dotted and the dashed lines indicate, respectively, classical and Tsirelson's bounds.

Charlie's ancilla is measured in the basis $\{|\phi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/2, |\phi^{\perp}\rangle = (|0\rangle - e^{i\phi}|1\rangle)/2\}$, the "quality factor" is unchanged, but the value of the "precision" becomes

$$\begin{aligned} G(\epsilon, \phi) &= 1 - \left|\langle\phi_+|\phi^{\perp}\rangle\right| + \left|\langle\phi_-|\phi\rangle\right| \\ &= 1 - \sin^2\frac{\phi}{2} - \cos^2\left(\epsilon + \frac{\phi}{2}\right) \\ &= \frac{1}{2}\left[\cos\phi - \cos\left(2\epsilon + \phi\right)\right] \\ &= \sin\epsilon \sin\left(\phi + \epsilon\right). \end{aligned} \tag{3.107}$$

Therefore, it is possible to change the optimality of the pointer by changing Charlie's ancilla measurement basis. For each epsilon, the optimal pointer is given by $G(\epsilon) = \sqrt{1 - F(\epsilon)^2} = \sin\epsilon$, that can be realized by choosing $\phi = \pi/2 + \epsilon$.

By choosing the sub-optimal pointer described in this section, we mean to demonstrate that the optimality of the pointer is not a prerequisite for the success of the experiment [115].

### 3.2.5 Experimental implementation of the optical circuit

The optical circuit described in Section 3.2.4 is implemented using the setup described in Figure 3.26.

#### Alice's and Bob's measurements

Alice and Bob perform a strong polarization measurement on the X-Z plane of the Bloch sphere. As described in Section 1.5.2, a polarization measurement in the computational

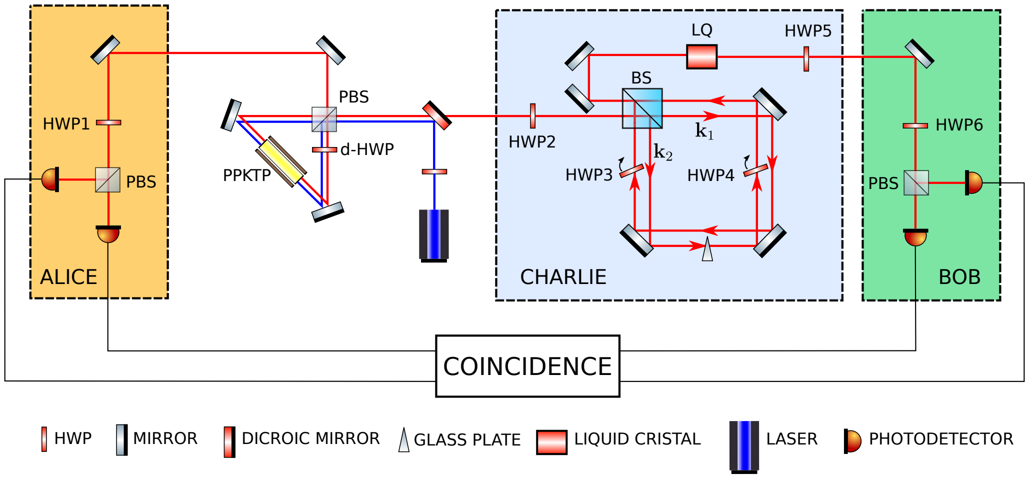

Figure 3.26: Scheme of the experimental setup [115]. The polarization-entangled photons are produced by the Sagnac source described in Chapter 2 and sent to Alice and Bob through optical fibers. Alice and Bob implement a scheme, consisting of a HWP (HWP1 and HWP6) and a PBS, to measure the polarization on two linear bases. The transmitted and reflected photons from the PBS are detected by single-photon avalanche photo-diodes (APDs). Charlie's apparatus performs the general measurement. HWP2 and HWP5 are used to implement the transformations $R$ and $R^\dagger$, respectively. HWP3 and HWP4 are placed in a Sagnac interferometer with clockwise and anticlockwise paths spatially separated. In particular, HWP3 (HWP4) is placed in the clockwise (anticlockwise) path, and is used as a phase retarder between horizontal and vertical polarization. The phase difference between the two paths is adjusted by tilting a thin glass plate. Finally, a liquid crystal (LQ) is used as a phase retarder between horizontal and vertical polarization. This image uses elements from the ComponentLibrary by Alexander Franzen [33], licensed under CC BY-NC 3.0 [34].

basis $\{|H\rangle, |V\rangle\}$ is performed by using a polarizing beam-splitter (PBS), with two single-photon avalanche photo-diodes (APDs) at its exit ports. In order to measure an arbitrary polarization basis $\left\{|a\rangle = \cos\frac{\alpha}{2}|H\rangle + \sin\frac{\alpha}{2}|V\rangle, |a^\perp\rangle = -\sin\frac{\alpha}{2}|H\rangle + \cos\frac{\alpha}{2}|V\rangle\right\}$ on the X-Z plane of the Bloch sphere, it is necessary to perform a rotation around the $y$-axis $R_y(\theta)$, such that

$$R_y(\theta_a)\,|a\rangle = |H\rangle\,, \text{ and } R_y(\theta_a)\,|a^\perp\rangle = |V\rangle\,, \tag{3.108}$$

where the angle $\theta_a = -\alpha = 2\arccos\left(\langle H|a\rangle\right)$. The rotation can be implemented by rotating a HWP of an angle $\theta_a/4$, since $\Lambda_{HWP}(\theta_a/4) = R_y(\theta_a)\sigma_z$. The presence of the $\sigma_z$ after the rotation matrix has no effect because it is followed by a polarization measurement in the computational basis, which is insensitive to the relative phase between $|H\rangle$ and $|V\rangle$.

### Charlie's measurement

Charlie performs his generalized measurement by using a path-encoded ancilla. In path encoding, described in Section 1.5.2, the computational basis corresponds to two non-overlapping spatial modes of the electromagnetic field, such as two gaussian beams with different approximate wave-vector $\mathbf{k}_1$ and $\mathbf{k}_2$. In our experimental scheme, the two modes

$\mathbf{k}_1$ and $\mathbf{k}_2$ correspond, respectively, to the propagation in the clock-wise and anti-clockwise direction of the Sagnac interferometer. The two computational basis vectors are therefore

$$|0\rangle := \hat{a}^\dagger_{\mathbf{k}_1} |0,0\rangle_{\mathbf{k}_1\mathbf{k}_2} = |1,0\rangle_{\mathbf{k}_1\mathbf{k}_2}\,, \text{ and } |1\rangle := \hat{a}^\dagger_{\mathbf{k}_2} |0,0\rangle_{\mathbf{k}_1\mathbf{k}_2} = |0,1\rangle_{\mathbf{k}_1\mathbf{k}_2}\,. \qquad (3.109)$$

The implementation of the theoretical circuit of Figure 3.24 with optical components requires each gate to be replaced with an equivalent circuit using a combination of the unitary operations described in Section 1.5.2, adapt to the encoding used for each qubit. The equivalence of two optical circuits means that, given a generic input state $|\psi\rangle$, they produce the same output (i.e., the two circuits must have, up to a global phase factor, the same matrix representation). Charlie's measurement apparatus uses three gates, one $Y$-axis rotation of the polarization qubit (and its inverse), two Hadamard gates of the path qubit and a controlled-phase-shift gate, which implements a $Z$-axis rotation of the path qubit controlled by the polarization qubit.

- *$Y$-axis rotation* - The $Y$-axis rotation of the polarization qubit $R_y(\theta_z)$ can be implemented by employing a HWP $\Lambda_{HWP}\left(\frac{\theta_z}{4}+\frac{\pi}{4}\right)$ followed by a $\sigma_x$ operation which, being equivalent to a swap between the two basis vectors $|H\rangle$ and $|V\rangle$, does not require to be implemented by using optical elements, but can be corrected in the data analysis phase.

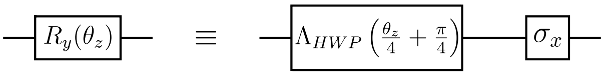
$R_y(\theta_z)$
$\equiv$
$\Lambda_{HWP}\left(\frac{\theta_z}{4}+\frac{\pi}{4}\right)$
$\sigma_x$

Figure 3.27: Optical implementation of the $Y$-axis rotation on a polarization qubit.

- *Hadamard gate* - The Hadamard gate on a path encoded qubit is implemented, as shown in Figure 3.28, by sandwiching a beam-splitter with two $R_z(-\pi/2)$ gates. The two $R_z(-\pi/2)$ gates are necessary in order to compensate the phase-shift between the reflected and the transmitted beam of an optical beam-splitter. However, they do not need to be experimentally implemented because the ones before the first and after the second $U_{BS}$ are irrelevant (indeed, the ancilla is prepared and measured on eigenstates of the computational basis) and the one between the two beam-splitters can all be absorbed in the $U_{phase}(\phi)$ gate used in the implementation of the controlled-phase-shift gate.

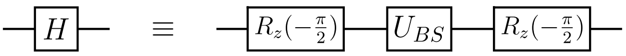

Figure 3.28: Optical implementation of the Hadamard gate on a path-encoded qubit.

- *Controlled-phase-shift gate* - The controlled phase gate is implemented by using an entangling gate $U(\epsilon_1,\epsilon_2)$ of the form

$$U(\epsilon_1,\epsilon_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\epsilon_1} & 0 \\ 0 & 0 & 0 & e^{i\epsilon_2}, \end{pmatrix} \qquad (3.110)$$

and two $Z$-axis rotations $R_z(\xi)$ and $R_z(\phi)$, on the first and the second qubit respectively (which can be put together into the single unitary $R_z(\xi)\otimes R_z(\phi)$), as shown in Figure 3.29.

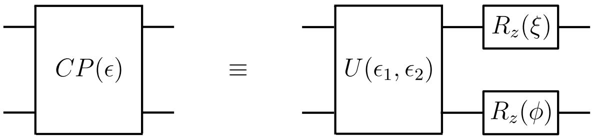

Figure 3.29: Optical implementation of the controlled-phase gate with polarization-encoded control qubit and path-encoded target qubit.

The rotation $R_z(\xi)$ on the first qubit is necessary because, if the input state $|\psi\rangle|+\rangle = \big(\alpha|H\rangle + \beta|V\rangle\big)|+\rangle$ is put into $U(\epsilon_1, \epsilon_2)$, the resulting output state is

$$\alpha|H\rangle|+\rangle + e^{i\frac{\epsilon_1+\epsilon_2}{2}}\beta|V\rangle\left(\cos\left(\frac{\epsilon_1-\epsilon_2}{2}\right)|+\rangle + i\sin\left(\frac{\epsilon_1-\epsilon_2}{2}\right)|-\rangle\right), \tag{3.111}$$

differing from the wanted state (3.74) because of the phase factor $e^{i\frac{\epsilon_1+\epsilon_2}{2}}$. The gate $R_z(\phi)$ on the second qubit is the circuit representation of the total phase difference between the clockwise and the anticlockwise paths, which must be adjusted to the right value in order to obtain the equivalence between the two ports.

In matrix representation, the product of the entangling gate $U(\epsilon_1, \epsilon_2)$ with the two $Z$-axis rotations is

$$(R_z(\xi)\otimes R_z(\phi))U(\epsilon_1,\epsilon_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{i\phi} & 0 & 0 \\ 0 & 0 & e^{i(\xi+\epsilon_1)} & 0 \\ 0 & 0 & 0 & e^{i(\epsilon_2+\xi+\phi)} \end{pmatrix}. \tag{3.112}$$

In order to have this expression describe the controlled-phase gate $CP(\epsilon)$ defined in Equation (1.29), it is necessary that

$$\begin{cases} \phi = 0 \\ \xi + \epsilon_1 = \epsilon \\ \epsilon_2 + \xi + \phi = -\epsilon \end{cases}, \tag{3.113}$$

which gives the necessary conditions for equivalence

$$\begin{cases} \phi = 0 \\ \epsilon = \frac{\epsilon_1-\epsilon_2}{2} \\ \xi = -\frac{\epsilon_1+\epsilon_2}{2} \end{cases}. \tag{3.114}$$

The experimental implementation of Charlie's measurement, shown in Figure 3.26, is equivalent to the circuit shown in Figure 3.30, provided that measurement results are swapped (as underlined by $-c$ at the output of the circuit) and that the phase effect introduced by the two beam-splitters is corrected by the $R_z(\phi)$ gate.

The measurement on the computational basis of the path qubit is experimentally performed by looking at a single output and changing the value of the phase $\phi$ from 0 to $\pi$. If at $\phi = 0$ the state $|+\rangle$ is transformed by the Hadamard gate into $|0\rangle$, at $\phi = \pi$ it is the state $|-\rangle$ which goes into $|0\rangle$ after the Hadamard gate. Indeed, the rotation $R_z(\phi)$ transform the state $|0\rangle + e^{-i\phi}|1\rangle$ into the state $|+\rangle$, which is then transformed into $|0\rangle$ by the Hadamard gate. The POVM $\big\{|0\rangle\langle 0| HR_z(-\phi), |0\rangle\langle 0| HR_z(-\phi+\pi)\big\}$ on the path-encoded qubit is therefore equivalent to a projective measurement on the $\Big\{|\phi\rangle = |0\rangle + e^{i\phi}|1\rangle, |\phi^{\perp}\rangle = |0\rangle - e^{i\phi}|1\rangle\Big\}$ basis.

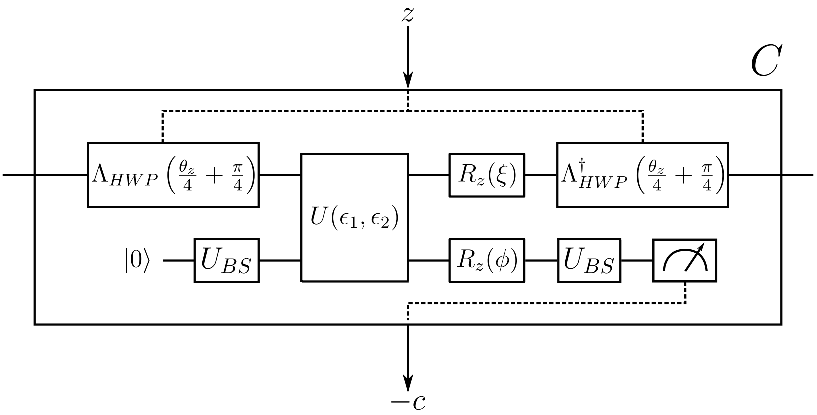
$z$
$C$
$\Lambda_{HWP}\left(\frac{\theta_z}{4}+\frac{\pi}{4}\right)$
$U(\epsilon_1,\epsilon_2)$
$R_z(\xi)$
$\Lambda^\dagger_{HWP}\left(\frac{\theta_z}{4}+\frac{\pi}{4}\right)$
$|0\rangle$
$U_{BS}$
$R_z(\phi)$
$U_{BS}$
$-c$

Figure 3.30: Circuit representation of the experimental Charlie's measurement setup implemented in Figure 3.26.

### 3.2.6 Experimental results

#### The apparatus

The experimental scheme described in Section 3.2.5 is implemented on the optical bench by exploiting the polarization-entangled photons generated by the source described in Chapter 2. The source is pumped with a CW laser at 404.5 nm, and uses a 30 mm PPKTP crystal inside a Sagnac interferometer to produce pairs of photons at 809 nm. The photons are collected to single mode optical fibers and sent one to Alice and the other one to the couple Charlie-Bob.

The photo of Alice's setup is shown in Figure 3.31. Alice's measurement setup is preceded by a three-coil, "bat ears" polarization controller and a half-wave plate (HWP), with horizontal fast axis, which is rotated around its vertical axis. These elements are necessary to implement the arbitrary unitary necessary to produce a singlet state $|\Psi^-\rangle$, as described in Section 2. Alice's basis choice is implemented by using a half-wave plate (HWP) mounted on a mechanized rotation mount, controlled by a personal computer. The measurement in the computational basis $\{|H\rangle, |V\rangle\}$ is performed by a polarizing beam-splitter, whose outputs are collected by multi-mode optical fibers and directed into single-photon avalanche photo-diodes (SPADs). A linear polariser is used to filter out residual $H$ polarization present in the reflected beam.

Bob's measurement apparatus, shown in Figure 3.32, is very similar to Alice's one. The only difference with respect to Alice's setup is the collection, which in this case uses single-mode fibers. This is due to the presence of Charlie's measurement, which requires mode filtering in order to obtain the required interference visibility between the clockwise and the anticlockwise arm of the interferometer.

Charlie's measurement apparatus, shown in Figure 3.33, implements the path encoding by using a Sagnac interferometer, with the computational basis correspondent to clockwise and anticlockwise propagation. Before entering Charlie's setup, the photon is filtered using a 3 nm filter, with central wave-length 808 nm, in order to remove different wave-length photons produced by the source (see Chapter 2), whose presence is detrimental because of the different phase transformations introduced by the different optical elements. Then, the photon is rotated by a half-wave plate on a motorized rotation mount, which is used to select the measurement basis, as described in Section 3.2.5, and encounters a beam-splitter (BS), which creates a superposition of clockwise and anticlockwise arm.

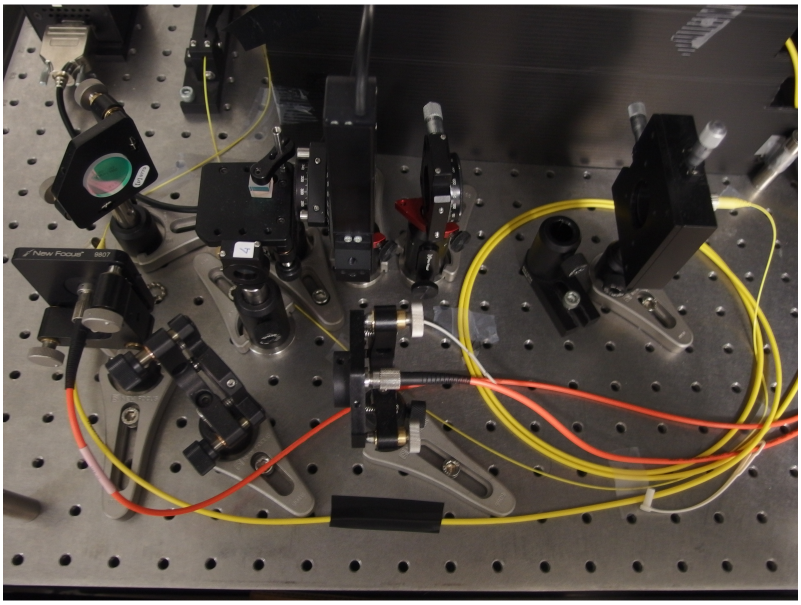

Figure 3.31: Setup used for Alice's measurement. Before Alice's measurement, the photon crosses a three-coil polarization controller (commonly called "bat ears") and a half-wave plate (HWP), rotated about the vertical axis, in order to adjust the phase of the source and the transformation introduced by fiber birefringence. Alice's measurement setup consists of a half-wave plate (HWP1), used to select the measurement basis, and a polarizing beam-splitter (PBS), whose outputs are collected by multi-mode fibers. A polariser is placed on the reflected arm of the PBS in order to filter the residual horizontal polarization reflected.

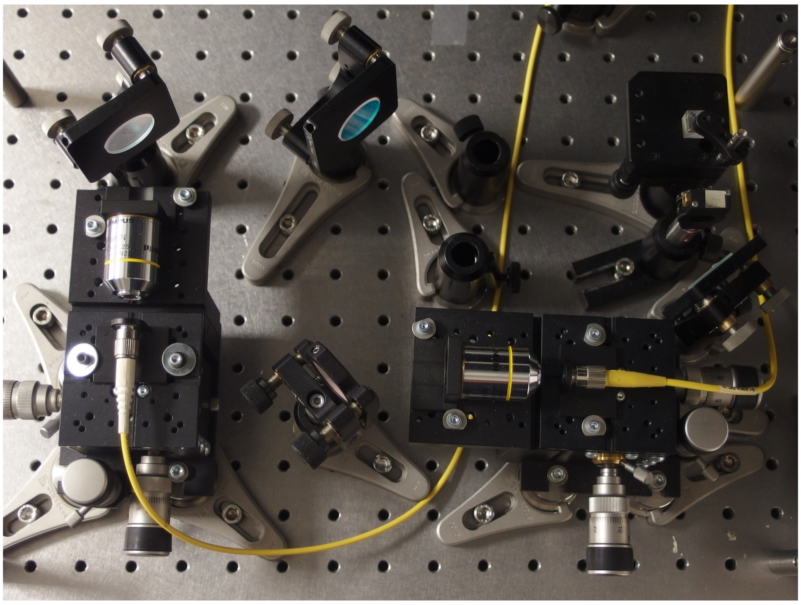

Figure 3.32: Setup used for Bob's measurement. The basis is chosen by a half-wave plate (HWP6) on a mechanized rotation mount, which can be seen in the left side of Figure 3.33. Then, a polarizing beam-splitter (PBS) performs the measurement in the $\{|H\rangle, |V\rangle\}$ basis. The reflected arm of the PBS is filtered by using a linear polariser.

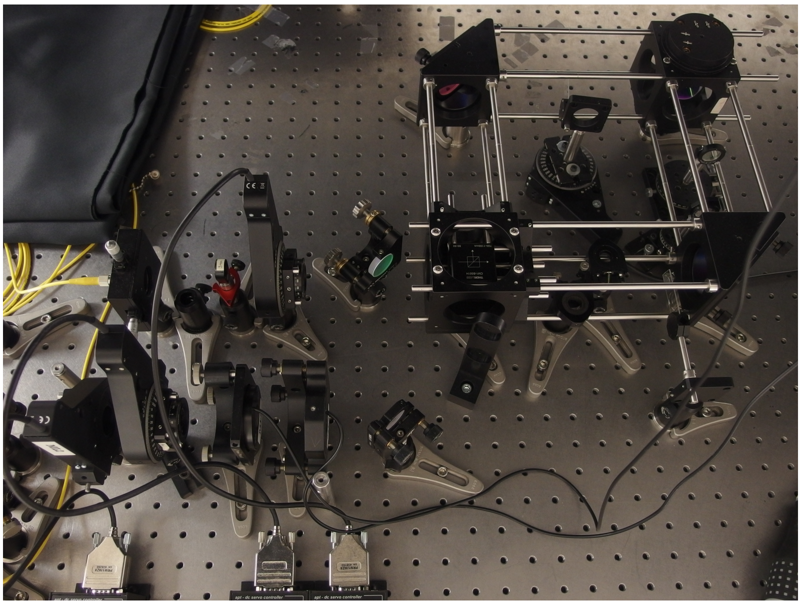

Figure 3.33: Charlie's measurement setup. The fiber coming from the source crosses a half-wave plate (HWP2) and a 3 nm filter before being inserted into the Sagnac interferometer, through a beam-splitter (see Chapter 2). The clockwise and anticlockwise arms of the interferometer are separated by $\sim 1$ cm in order to allow the placement of different optical elements on the two arms. Both arms are equipped with a half-wave plate (HWP3 and HWP4), whose rotation around the vertical axis controls the phase between $H$ and $V$ polarization, and a glass, used to control the global phase of each arm. At the output of the interferometer, the photon crosses a couple of liquid crystals (LQ) and a half-wave plate (HWP5), which implements the inverse of the transformation applied by HWP2, before reaching Bob's basis selection half-wave plate (HWP6), at the bottom-left side of the Figure.

The two arms are separated by $\sim 1$ cm in order to make it possible to place different optical elements on them. Because of the short coherence length of the photons produced by the source, it is necessary to place the same optical elements on both arms of the interferometer in order to see interference at the exit beam-splitter. Each arm has a half-wave plate, with the fast and slow axes correspondent to the $H$-$V$ basis, which is rotated around its vertical axis in order to give a phase between the $H$ and the $V$ polarization. The cumulative effect of these plates, the mirrors and the beam-splitter gives a relative phase $\epsilon_1$ ($\epsilon_2$) between the two polarizations. Both arms are also equipped with an equal-thick glass plate, which is perpendicular to the beam in the anticlockwise arm and mounted on a mechanized rotator stage, which tilts it around the vertical axis, in the clockwise are. By tilting this glass plate, it is possible to control the relative phase $\phi$ of the two arms of the interferometer.

At the output of the interferometer, two liquid-crystals are placed in order to implement the $R_z(\xi)$ transformation required for the implementation of the controlled-phase-shift gate. Then, a half-wave plate implements the inverse of the basis selection transformation before the photon arrives at Bob's measurement setup.

The photons are detected by using four single-photon avalanche photo-diodes (SPADs), characterized by $\sim$ 60% quantum efficiency[12], 21 ns dead time and $\sim$ 800 ps FHWM

[12] The low detection efficiency of semiconductor single-photon detectors makes the experiment subject

electronic jitter [114]. Two detectors are placed at Alice's side and two at Bob's side. Detection events are tagged using a 81 ps resolution time-tagger. Both the acquisition of the time-tags and the control of the experiment is implemented using a personal computer, equipped with a Linux operating system and a custom software implemented in Python.

### Strength of the measurement

The strength of Charlie's measurement is given by parameter $\epsilon = \frac{\epsilon_1 - \epsilon_2}{2}$, which can be controlled by turning the two half-wave plates HWP3 and HWP4 in the clockwise and anticlockwise arm of the interferometer. However, since both $\epsilon_1$ and $\epsilon_2$ depend also on the phase introduced by the other optical elements, the exact value of $\epsilon$ must be measured. This measurement can be performed by noticing that, given a state $|\psi\rangle = \alpha |H\rangle + \beta |V\rangle$ at the input of the interferometer, the state at its $|0\rangle$ output is

$$\begin{aligned} |\psi_{out}\rangle &= (I_2 \otimes |0\rangle \langle 0| U_{BS} R_z(\phi)) U(\epsilon_1, \epsilon_2)(|\psi\rangle \otimes U_{BS} |0\rangle) \\ &= \alpha \sin\left(\frac{\phi}{2}\right) |H\rangle + \beta e^{i\frac{\epsilon_1+\epsilon_0}{2}} \sin\left(\frac{\phi}{2} - \epsilon\right) |V\rangle , \end{aligned} \tag{3.115}$$

where $\phi$ is the phase difference between the clockwise and the anticlockwise arm, which is controlled by the glass plate. For small tilting angle $\theta$ of the thin glass plate, it is possible to neglect the effects of refraction and consider, as a model for $\phi$,

$$\phi(\theta) = \frac{\chi}{\cos(\theta - \theta_0)} + \phi_0, \tag{3.116}$$

$$\chi = \frac{2\pi}{\lambda} d\delta n, \tag{3.117}$$

with $\theta - \theta_0$ the incidence angle of the beam to the plate, $\lambda$ the wavelength, $d$ the thickness of the plate, $\delta n = n_{glass} - n_{air}$ and $\phi_0$ a phase offset. If Bob measures in the $Z$ basis, he obtains

$$\mathbb{P}(H|\phi(\theta)) = \left|\langle H|\psi_{out}\rangle\right|^2 = |\alpha|^2 \sin^2\left(\frac{\phi(\theta)}{2}\right), \tag{3.118}$$

$$\mathbb{P}(V|\phi(\theta)) = \left|\langle V|\psi_{out}\rangle\right|^2 = |\beta|^2 \sin^2\left(\frac{\phi(\theta)}{2} - \epsilon\right). \tag{3.119}$$

By measuring these probabilities for several values of $\theta$, it is possible to interpolate these probabilities, using the model for the phase $\phi(\theta)$, with the functions

$$\mathbb{P}(H|\theta) = I_H \cos^2\left(\frac{\chi}{\cos(\theta - \theta_0)} + \phi_H\right), \tag{3.120}$$

$$\mathbb{P}(V|\theta) = I_V \cos^2\left(\frac{\chi}{\cos(\theta - \theta_0)} + \phi_V\right), \tag{3.121}$$

from which $\epsilon = \phi_H - \phi_V$ can be estimated.

The results of this measurement, together with the interpolating curve, is shown in Figure 3.34.

In order to prove the stability of the measurement strength $\epsilon$, and to evaluate its experimental error, this measurement (for a different value of $\epsilon$) has been performed for a period longer that thirteen hours, obtaining the results shown in Figure 3.35. The measurement shows that $\epsilon$ is stable over a very long period of time. Moreover, it allows to give a direct estimation of the error in the measurement of $\epsilon$.

to the detection loophole. Since this experiment is thought as a first demonstration of the feasibility of the double violation, however, this effect has not been considered, making the "fair sampling" assumption [118].

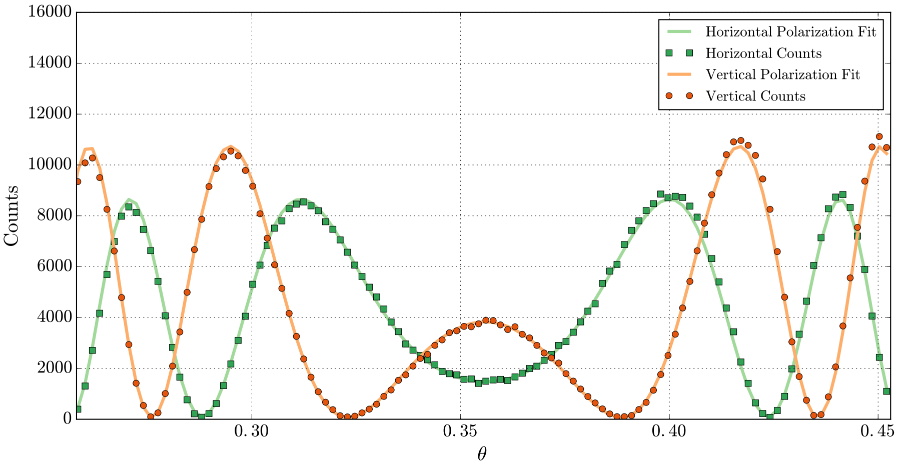

Figure 3.34: Direct measurement of $\mathbb{P}(H|\theta)$ and $\mathbb{P}(V|\theta)$, with the method described above. The fitting functions $\mathbb{P}(H|\theta) = 8600 \cdot \sin^2(\frac{1185.5}{\cos(\theta - 0.356)} + 2.45) + 98$ and $\mathbb{P}(V|\theta) = 11000 \cdot \sin^2(\frac{1185.5}{\cos(\theta - 0.356)} + 1.40) + 68$, with $\theta$ the rotation angle of the glass plate in radians, show the good agreement of the phase model with the experimental data. The phase difference measured in this way is $\epsilon = 1.049 \pm 0.004$ [115].

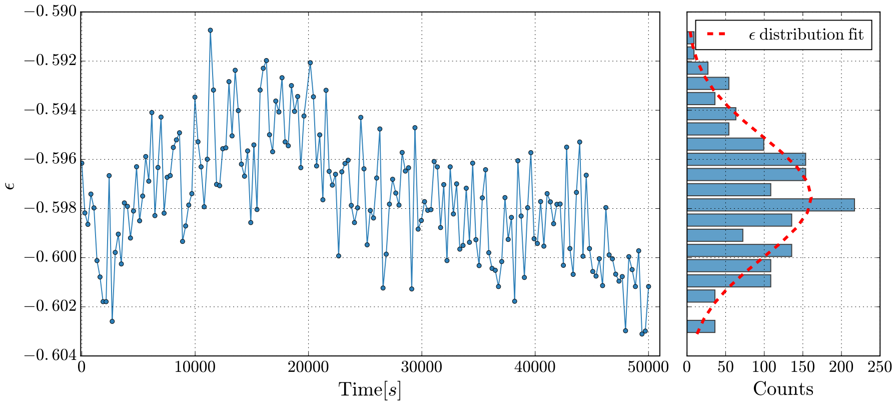

Figure 3.35: Measurement of the $\epsilon$ for a period of thirteen hours [115]. (**Left**) Each point in the graph represents a different estimation of $\epsilon$. (**Right**) Distribution of the measured $\epsilon$. The gaussian curve that fits the data has a mean value $\mu = -0.5975$ and a standard deviation $\sigma = 0.0025$. The standard deviation of the distribution is used as the error on a single measurement of $\epsilon$.

## Results

The results of a series of measurements performed with this experimental setup, for various values of $\epsilon$ in the range $[0, \pi/2]$, is shown in Figure 3.36. The results show a good agreement with the theoretical model. For $\epsilon = 0$, there is no interaction between the polarization and the path degree of freedom, therefore Charlie is not performing any measurement. In this case, as expected, $S_{AC}$ is compatible with 0, while $S_{AB}$ is close to the Tsirelson's bound. By increasing $\epsilon$, the quantity of information got by Charlie increases, as shown by the increase in his correlation $S_{AC}$ with Alice, while the state is more disturbed, determining a lowering in the correlation $S_{AB}$ between Bob and Alice.

Most measurements have been taken in the region around $\epsilon = \pi/3$, where both $S_{AB}$

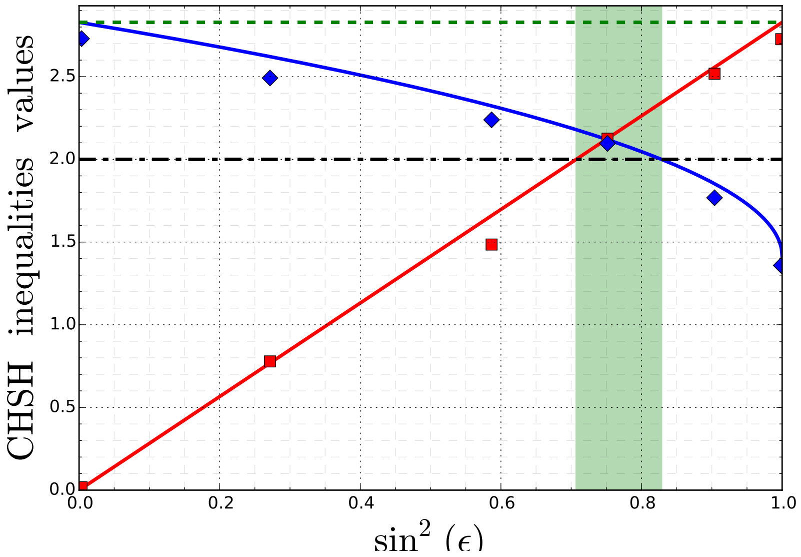

Figure 3.36: Measurement of $S_{AC}$ (red squares) and $S_{AB}$ (blue diamonds) for several values of $\epsilon$. The red and green solid lines show the theoretical values of $S_{AC}$ and $S_{AB}$ from Equations. (3.99) and (3.100), while the dash-dotted and dashed lines indicate classical and Tsirelson's bounds respectively. The green region highlights the values of $\epsilon$ in which double violation is expected. Possonian errors are within the dimensions of the points. From Schiavon *et al.* [115].

and $S_{AC}$ are expected to violate the classical bound. To give a larger statistical evidence of the effect of double violation, several measurements were performed for two different $\epsilon$ values in that region. Figure 3.37 **(Left)** reports the results of 8 consecutive measurements

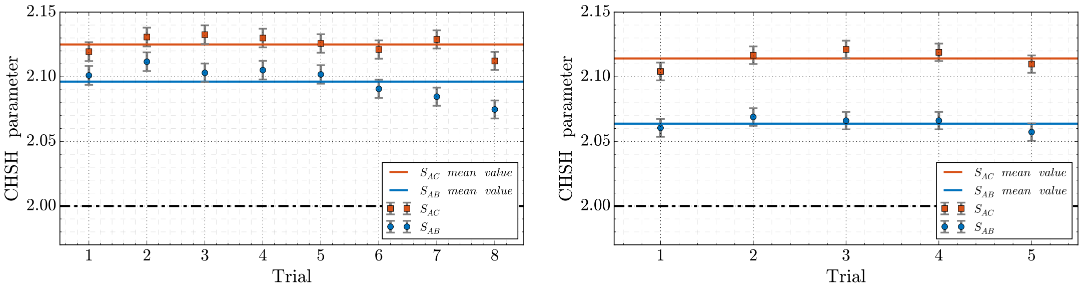

Figure 3.37: Measurements of $S_{AC}$ (red squares) and $S_{AB}$ (blue diamonds) in two consecutive series of trials. Red and blue solid lines indicate the mean value of $S_{AC}$ and $S_{AB}$ respectively. **(Left)** Eight consecutive trials are performed through an hour, with $\epsilon = 1.049 \pm 0.002$. Considering the Poissonian error, the measurements show a violation of 10 standard deviations, fluctuating around mean values of $S_{AC} = 2.125 \pm 0.003$ and $S_{AB} = 2.096 \pm 0.003$. **(Right)** Another series of five consecutive trials performed within an hour, with $\epsilon = 1.053 \pm 0.002$. All the measurements show a violation of 10 standard deviation, fluctuating around mean values of $S_{AC} = 2.114 \pm 0.003$ and $S_{AB} = 2.064 \pm 0.003$. From Schiavon *et al.* [115].

with $\epsilon = 1.049 \pm 0.003$. In all trials, both $S_{AC}$ and $S_{AB}$ are above the classical bound, fluctuating around the mean values $S_{AC} = 2.125 \pm 0.003$ and $S_{AB} = 2.096 \pm 0.003$. Data are acquired at a mean coincidence rate of 700 counts per second, with an exposure time of 30 s for each measurement, therefore each trial takes about eight minutes to be measured. Therefore, these results show that the double violation is stable for a period longer than an hour, proving the reproducibility of the double violation and the stability of the setup.

A second series of trials, with $\epsilon = 1.053 \pm 0.003$ is shown in Figure 3.37 **(Right)**. Similarly to the previous case, both $S_{AC}$ and $S_{AB}$ are above the classical bound for the entire period of the acquisition, with $S_{AC} = 2.114 \pm 0.003$ and $S_{AB} = 2.064 \pm 0.003$.

# Chapter 4

# A receiving station for space quantum communication

The peculiar feature of quantum communication is the necessity of transferring quantum states between large distances. As already shown in Section 1.5.2, single photons are the ideal information carriers for quantum communication, since their low interaction with matter allows them to preserve the coherence of their state over long distances. Besides the information carriers, also the channel used for state transmission is of primary importance, since the peculiar characteristics of quantum states is the fact that they cannot be copied, thus ruling out the possibility of amplifying the state to reach longer distance, as happens in classical communication. This means that the losses of the channel used for quantum communication must be low enough to allow a considerable part of the transmitted photons to reach the receiver.

There exist mainly two ways of transferring optical information through long distances: optical fibers and free-space[1]. The advantage of optical fibers is given by their wide use in existing telecommunication networks, thus offering the possibility to integrate quantum communication with the other communication systems. Their major drawback, however, is given by the relatively high level of losses, limiting the coverable distance to few hundred kilometers (the current distance record in optical fibers is 404 km [125]).

This limitation is the main reason for the interest in free-space quantum communication. The immediate application of free-space quantum communication is the construction of line-of-sight optical channels, with both the transmitter and the receiver on the ground and all the propagation through the atmosphere. While this scheme could be of interest because of the presence in the atmosphere of transmission windows where the mean loss level is very low, ground-to-ground links are limited by Earth curvature, which poses a stringent limit on the coverable distance. However, free-space quantum communication offers also the possibility of creating a link between a ground station and a satellite on orbit. There are various reasons why this is particularly interesting. The ground-to-satellite link, indeed, is characterized by quite short propagation in the atmosphere ($\sim 10\,\mathrm{km}$) and a much longer propagation in vacuum, where it is not affected by turbulence. Moreover, a single satellite can cover a large area on the ground, thus making it possible to implement quantum communication between distances that are beyond the capabilities of ground-to-ground links (both in free-space and with optical fibers).

[1] Free-space quantum communication usually refers to the transmission of quantum states through the atmosphere, or in space. Recently, however, also underwater quantum communication has started being investigated [124].

The goal of satellite quantum communication was already present in the pioneering free-space studies, realized in the late 90s from Richard Hughes's group in Los Alamos [126]. Their 0.5 km free-space optical link provided the first evidence that satellite Quantum Key Distribution was indeed feasible. This opened the way to several other experimental studies, all aimed at the demonstration of the feasibility of satellite-ground quantum communication, over increasing distances. The first experimental demonstration of the feasibility of entanglement transfer with a satellite dates back to 2005, using a 13 km free-space ground-to-ground optical link [127]. A great improvement in this field was due to the implementation of a 144 km free-space optical link between two telescopes situated in two different islands of the Canaries. Through this link, several experiments have been performed, exploring many aspects of free-space quantum communication [128–131]. The same period saw also the beginning of the research for an effective implementation of ground-satellite experiments. The lack of a satellite sending or receiving quantum states made it necessary to think of some way of simulating a quantum source on space. One possibility is the exploitation of the signal retro-reflected by geodesic satellites used in Laser Ranging (LR). These satellites are provided with corner-cube retro-reflectors which, if illuminated by a laser pulse, reflect it back to the transmitting station. By adjusting the power of the transmitting laser, it is possible to simulate an attenuated laser source on the satellite with the wanted mean photon number per pulse. Moreover, this technique allows to exploit the existing LR infrastructure for synchronization and tracking, thus greatly simplifying the experimental work needed for the setup of the station. With this technique, the first single photon exchange with a satellite has been demonstrated [132], followed by the first demonstration of the feasibility of polarization encoding [133] and the first satellite-based single-photon interference [134].

The last few years have seen, if possible, a further increase in the field of satellite quantum communication. Besides the experiments with moving trucks [135], airplanes [136], and balloons [137], in the last few years the first satellites at least partially dedicated to quantum technologies have been launched to space [138–140].

This Chapter will be dedicated to the new experimental scheme of the quantum receiver at the Matera Laser Ranging Observatory (MLRO), with the goal of increasing the signal-to-noise ratio of the receiving system by using high efficiency, low jitter detectors together with a high resolution time-tagger in order to both increase the signal and decrease the background noise through a tighter temporal filtering. It will start with a short description of the SLR network and of the existing experimental setup at the MLRO, used for the already cited experiments [132–134]. Than, it will describe the new experimental scheme for the receiving station, from the new data acquisition system to the new data analysis pipeline. The end of the chapter will give some hints on the ongoing research activity aiming to exploit satellite orbit predictions, provided daily by the International Laser Ranging Service (ILRS), in order to improve the accuracy of the analysis of the satellite orbit to the level required for an optimal exploitation of the new hardware.

## 4.1 Satellite Laser Ranging

Satellite Laser Ranging (SLR) is a distance measurement technique that employs short laser pulses directed towards a satellite and reflected back to the observatory by retro-reflectors (corner-cubes) mounted on the satellite itself. This technique provides very high precision, up to the level of few mm for a single measurement [141]. The high precision measurement of satellite orbits is of primary importance for many goals, both scientific and technological. Its data are of fundamental importance for the elaboration of the International Terrestrial Reference Frame (ITRF), the international standard for the measurements on or near the Earth's surface, such as the position returned by a GNSS system like the GPS [142]. In addition to that, it allows the study of orbital perturbations, of primary importance for the studies of Earth's dynamics or for high accuracy test of fundamental physical theories, like general relativity [143].

Nowadays, there exist more than 40 active SLR stations, coordinated by the International Laser Ranging Service (ILRS), that is in charge of collecting, managing and distributing the data of each SLR station. The stations are distributed all over the Earth, with higher concentration in Europe and in the far East, as shown in Figure 4.1. A SLR station is usually provided with

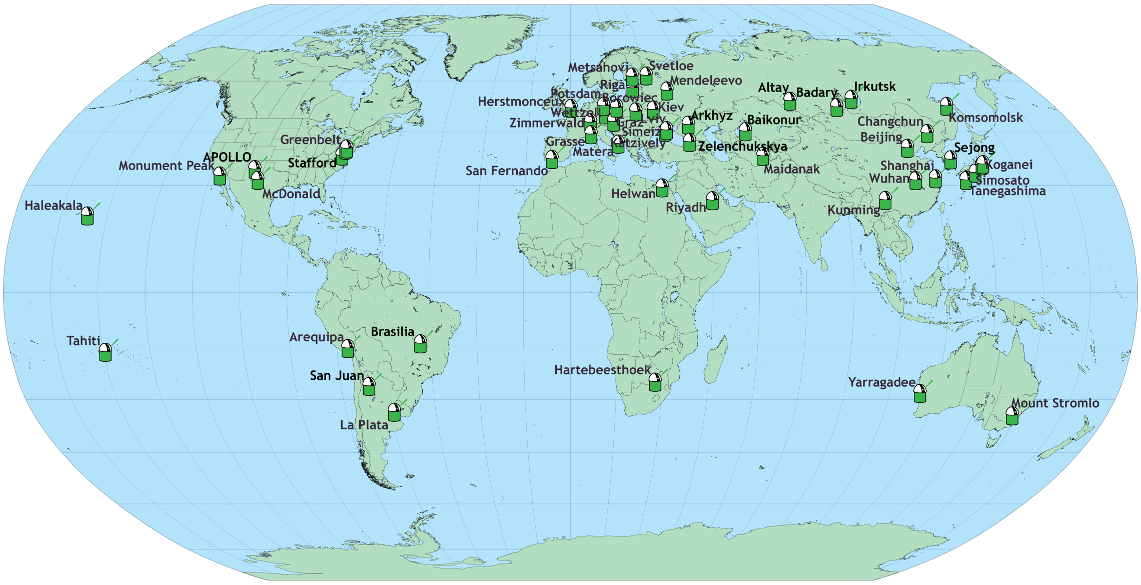

Figure 4.1: Map of the currently operating SLR stations. The map clearly shows the non-uniform coverage of SLR stations, that are mostly situated in the North hemisphere, especially in Europe and Asia. From the ILRS website [141].

- a high speed telescope, able to point and track even the fastest, low Earth orbit (LEO) satellites,
- a high energy pulsed laser,
- a detector able to receive the signal retro-reflected by the satellite, usually a photomultiplier (PMT) or an avalanche photo-diode (APD),
- a data acquisition pipeline, able to tag with high precision both the outgoing and the ingoing pulse, and
- a very stable frequency reference.

The satellites used in laser ranging are provided with retro-reflectors, usually made with corner-cubes, having the property of reflecting back the incident beam regardless of the angle of incidence. They are placed both in low Earth orbit (LEO) and in middle Earth orbit (MEO), with various orbit inclinations and eccentricities, as shown in Figure 4.2. The orbit of the satellites is predicted on a daily basis from the data collected by the

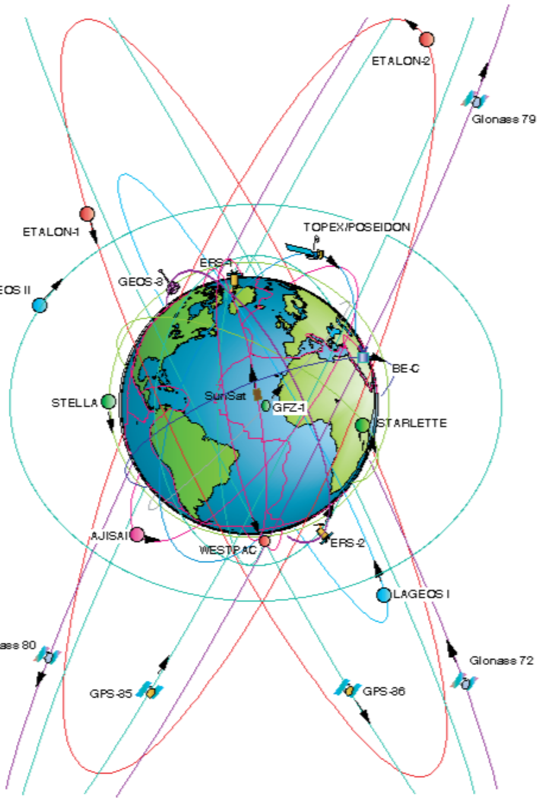

Figure 4.2: Orbit distribution of the satellites used for SLR. From the official ILRS website [141].

different SLR stations. Predictions are then redistributed to SLR station, where they are used as input to the satellite tracking system.

## 4.2 The ground station for quantum communication

### 4.2.1 Existing setup

The ground station for quantum communication at the Matera Lasera Ranging Observatory (MLRO) is constructed sharing the transmission/reception optics with the laser ranging station, using the laser ranging system for satellite tracking and synchronization. The general scheme of the ground station at MLRO is shown in Figure 4.3.

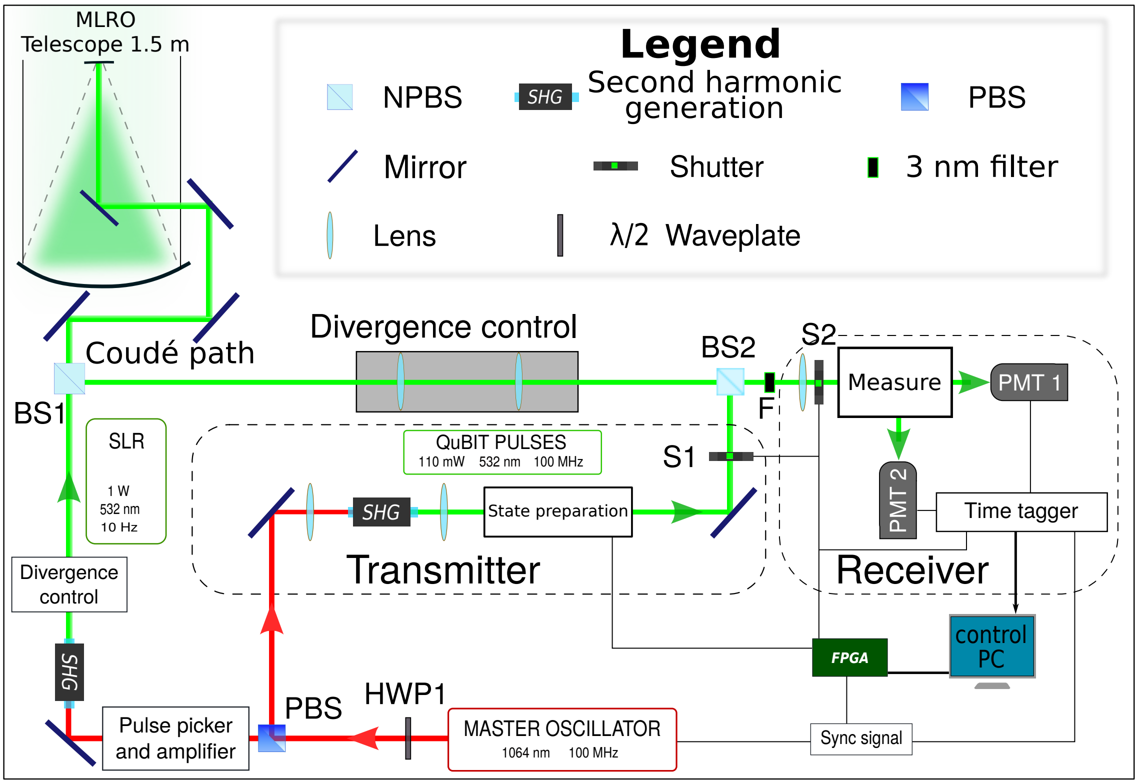

Figure 4.3: General setup of the ground station for quantum communication at the Matera Laser Ranging Observatory. The laser ranging and the quantum subsystem operate in parallel, in order to use the laser ranging system for tracking and synchronization.

Both the laser ranging and the quantum subsystem use a mode-locking laser oscillator mastered by the atomic clock at the MLRO [133]. The laser produces linearly polarized pulses of 100 ps duration at the wavelength of 1064 nm, with a 100 MHz repetition rate and about 400 mW of average power. The laser is split between the two subsystems by a half-wave plate (HWP1) followed by a PBS, in order to adjust the fraction of power giving to both subsystems. The laser ranging system employs a pulse picker to select one pulse every $10^7$, which goes through a regenerative amplifier, a two single-pass amplifiers and a Second Harmonic Generation (SHG) stage to obtain a 100 mJ pulse with 10 Hz repetition rate at a wavelength of 532 nm. Qubit pulses are generated by sending the part of the master oscillator entering the quantum subsystem into a SHG generator unit, whose output is a 532 nm pulsed laser at a 100 MHz repetition rate with a power of 110 mW (each pulse has an energy of 1.1 nJ). The encoding of the pulses in the chosen degree of freedom is performed by the “state preparation” optical setup, which is controlled by a PC and an FPGA. The divergence of satellite Laser Ranging (SLR) and qubit pulses is adjusted independently before the pulses are combined by a NPBS into the Coudé path of the telescope.

The telescope used for laser ranging at the MLRO, described in [56], is a Cassegrain reflector with a parabolic primary mirror $M_1$ of 1.5 m diameter and focal length $f_1 = 2250$ mm, and hyperbolic secondary mirror of 148.5 mm focal length and 10 cm diameter [144]. The whole system has an effective area of 1.7662 $\mathrm{m}^2$ and a focal length $f_{eq} = 225$ m. The other mirrors, $M_3$ to $M_7$, compose the Coudé path shown in Figure 4.4, a system of planar mirrors with the property that the direction of the beam after the last mirror is independent from the pointing direction of the telescope. After $M_7$, the beam enters BS1, with the setup shown in Figure 4.3.

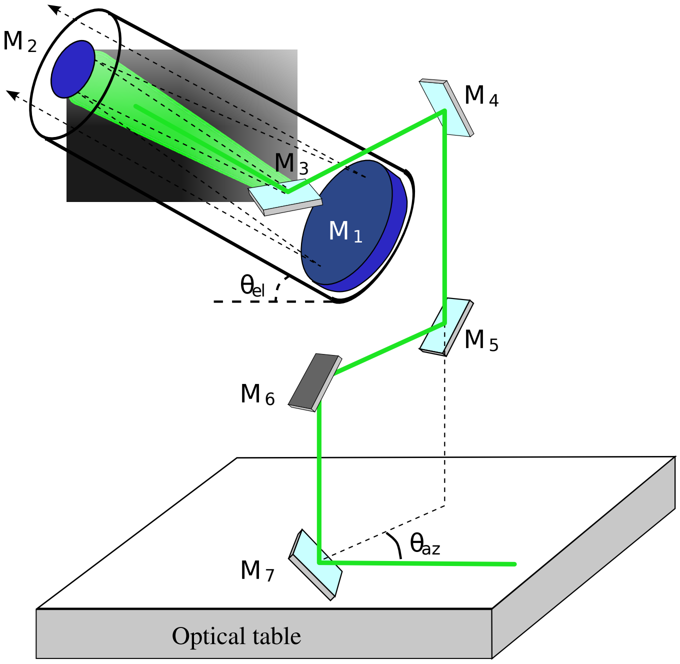

Figure 4.4: The Coudé path of the telescope used for laser ranging at the MLRO. Mirrors $M_4$ to $M_6$ rotate jointly with the telescope as the azimuth angle $\theta_{az}$ is changed. From Vallone *et al.* [133].

At the output of the telescope, the two beams are directed against the observed satellite, which reflects them back with its retro-reflectors. The attenuation in the uplink channel reduces the mean number of photons per pulse to $\mu_{sat}$, which can be adjusted to the value required by the experiment by changing the energy of the pulse sent from the ground station[2]. Indeed, each "qubit" pulse, of energy $E_p = 1.1\,\mathrm{nJ}$[3], can viewed as a coherent state

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n (\hat{a}^\dagger)^n}{n!} |\Omega\rangle\,, \tag{4.1}$$

where $|\Omega\rangle$ is the vacuum state, $|\alpha|^2 = E_P/\hbar\omega = 3 \cdot 10^9$ is the mean number of photons per pulse and $\hat{a}^\dagger$ is the operator of the mode entering the "state preparation" optical network. The state preparation network transforms the field operator $\hat{a}^\dagger$ into $S_{E,11}\hat{b}_1^\dagger + S_{E,12}\hat{b}_2^\dagger$, where $\hat{b}_1^\dagger$ and $\hat{b}_2^\dagger$ are two orthogonal mode operators (they correspond to the two basis

[2] The quantum key distribution feasibility experiments use $\mu_{sat} \leq 2$ [133, 145], while the interference experiment described in Section 5.1 has a higher $\mu_{sat}$ [134].

[3] This value is referred to the QKD experiment of Vallone *et al.* [133], that uses $\mu_{sat} \simeq 1$.

vectors of the encoding degree of freedom), and $S_E$ is the encoding scattering matrix (see Section 1.5.1).

The state reflected by the satellite is again a coherent state, with mean number of photons per pulse $\mu_{sat} = |\alpha_{sat}|^2$. The operator $\hat{a}^\dagger$ of equation 4.1, after reflection, has been transformed into $(S_E S_u S_{sat})_{11}\hat{b}_1^\dagger + (S_E S_u S_{sat})_{12}\hat{b}_2^\dagger$, where $S_u$ and $S_{sat}$ represent the single-photon transformations introduced by the uplink and the satellite, respectively[4]. With this method, therefore, it is possible to simulate an attenuated laser source, with mean number of photons per pulse $\mu_{sat}$ and transmitted quantum state

$$(S_E S_u S_{sat})_{11}\hat{b}_1^\dagger |\Omega\rangle + (S_E S_u S_{sat})_{12}\hat{b}_2^\dagger |\Omega\rangle\,, \tag{4.2}$$

situated on the satellite.

After down-propagation through the atmosphere, the state entering the telescope is a coherent state with mean number of photons per pulse $|\alpha_{rx}|^2 = \mu_{rx} \ll 1$, which can be written as

$$\begin{aligned}|\alpha_{rx}\rangle &= e^{-\frac{|\alpha_{rx}|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha_{rx}^n \left[(S_E S_u S_{sat} S_d)_{11}\hat{b}_1^\dagger + (S_E S_u S_{sat} S_d)_{12}\hat{b}_2^\dagger\right]^n}{n!} |\Omega\rangle \\ &\simeq e^{-\frac{|\alpha_{rx}|^2}{2}} |\Omega\rangle + e^{-\frac{|\alpha_{rx}|^2}{2}} \alpha_{rx} \left[(S_E S_u S_{sat} S_d)_{11}\hat{b}_1^\dagger + (S_E S_u S_{sat} S_d)_{12}\hat{b}_2^\dagger\right] |\Omega\rangle + O(\alpha_{rx}^2),\end{aligned} \tag{4.3}$$

where $S_d$ is the scattering matrix of downlink propagation.

The state is measured in the “Receiver” part of the setup of Figure 4.3, with the measurement optical network implemented in the “Measure” block. In front of the receiver, a 3 nm filter (F) centered at 532 nm is placed for spectral filtering, and a shutter (S2) protects the receiving apparatus from backscattered light during the transmission cycle. The state is detected using two single photon photomultiplier tubes (PMT) (Hamamatsu H7360-2), characterized by detection efficiency $\eta_{PMT} = 0.1$, FWHM electronic jitter $\Delta t_{PMT} = 1.22$ ns and dark count rate $DC_{PMT} = 50$ Hz. The sensitive area of the detector has a diameter of 22 mm.

The necessity of sharing the same path for laser ranging, qubit outgoing and ingoing pulse is the reason of the presence of the two beam-splitters BS1 and BS2 in the optical path of the quantum subsystem. This, despite being necessary for the correct operation of the ground station, adds 75% of losses both in transmission and in reception.

### 4.2.2 New experimental scheme

Last year, the quantum subsystem of the MLRO has started a process of upgrade aimed to increase the performance of the receiving station. The long term goal of the upgrade is to make the system adapt for quantum communication with middle Earth orbit (MEO) or geostationary Earth orbit (GEO) satellites, and to make it suitable for high accuracy lunar laser ranging (LLR) measurements within the Moonlight-2 project.

Differently from satellite laser ranging, lunar laser ranging applies the LR technique in the measurement of the distance between the ground station and the surface of the Moon. This is obtained by exploiting the corner-cube arrays disposed on the Moon by the US Apollo 11, 14 and 15 and the Soviet Luna 17 and Luna 21 missions [141], whose location on the Moon surface is shown in Figure 4.5. These arrays are characterized by a large area

[4] This is true in the hypothesis that channel losses are independent on the encoding degree of freedom.

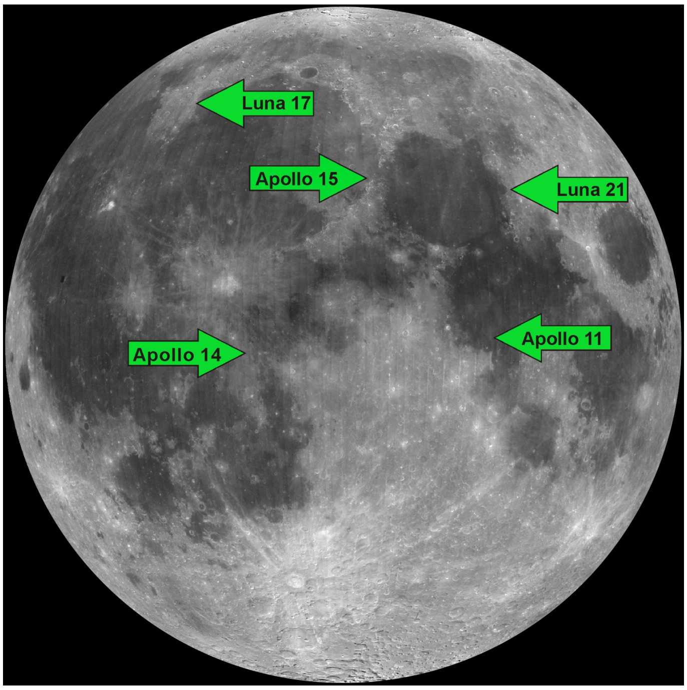

Figure 4.5: Location of corner-cube retro-reflector arrays on the lunar surface. From the ILRS website [141].

($\sim 1\,\mathrm{m}^2$) of small corner-cube retro-reflectors. The optical depth of the array, due to its inclination with respect to the incoming pulse[5], spreads the temporal mode of the incoming pulse, limiting the accuracy of the measurement to the $mm$ level even with the best instrumentation. A further improvement of the accuracy requires the use of a new scheme for the retro-reflectors, whose development is the scientific goal of the Moonlight-2 project.

The Padova group is in charge of improving the quantum receiver part of MLRO in order to make it suitable for high accuracy LLR measurements. To this goal, the new experimental scheme shown in Figure 4.6 has been implemented. The main difference with the old scheme shown in Figure 4.3 consists of an improvement in the hardware used for photon detection and tagging. Indeed, PMT detectors will be substituted with semiconductor single-photon avalanche photo-diodes by Micro Photon Devices (MPD-PDM), characterized by peak detection efficiency $\eta_{PDM} = 0.48$, FWHM timing accuracy $\Delta t_{PDM} = 50\,\mathrm{ps}$ and dark count rate $DC_{PDM} \simeq 350\,\mathrm{Hz}$ [146]. They have a $200\,\mu\mathrm{m}$ diameter sensitive area, thus requiring tight focusing to collect the whole beam coming from the telescope.

The output of these new detectors will be tagged using a quTAG time-tagger, characterized by a 1 ps resolution and a tagging accuracy of less than 25 ps FWHM [147]. The possibility of locking the internal clock to an external periodic signal allows to tag the events with the stability of the MLRO atomic clock. Moreover, the splitting of the master oscillator between the laser ranging and the quantum subsystem will exploit a Pockels cell, switching the polarization according to the destination of the laser pulse (in particular, it will select one pulse over $10^7$ to send to the laser ranging subsystem). This allows to operate both the quantum and the laser ranging subsystems in parallel without the need of increasing the output power of the master oscillator to compensate the fraction of power

[5] The inclination changes periodically due to lunar librations.

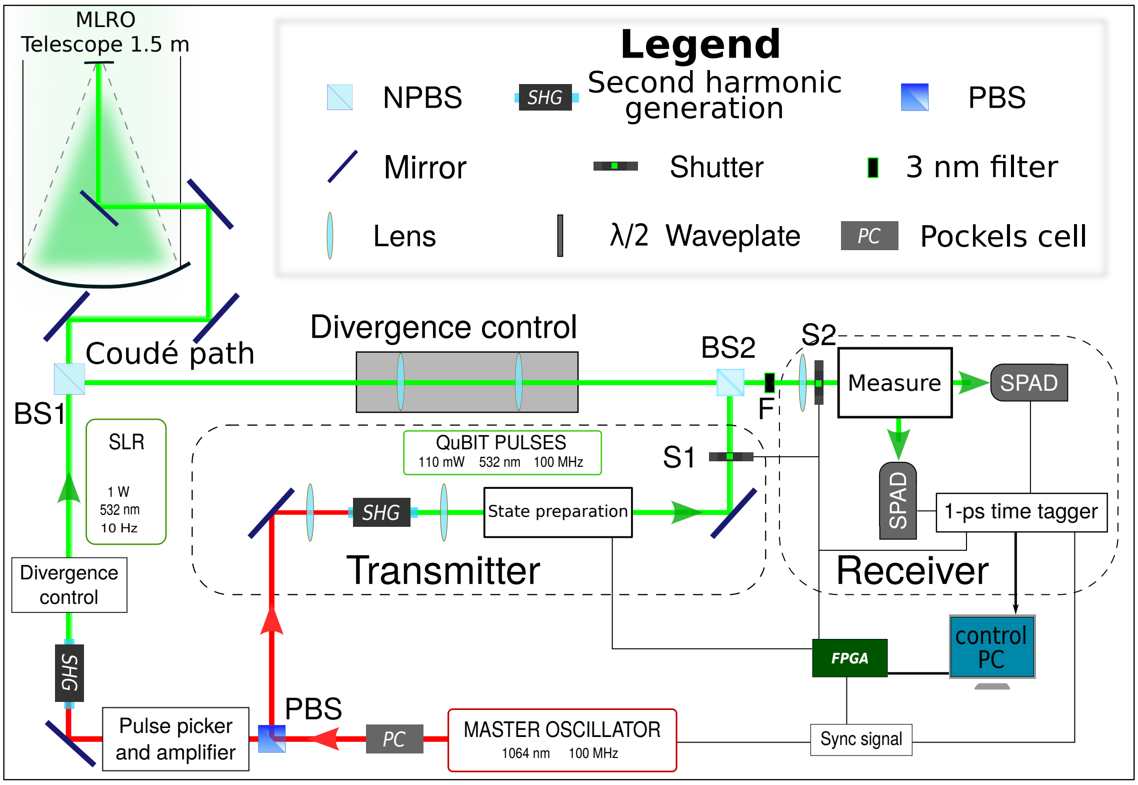

Figure 4.6: New experimental scheme for the MLRO.

sent to the quantum subsystem.

This new experimental setup is currently at the first stages of its development. Extraordinary maintenance of the MLRO telescope, together with delays in the delivering of the new hardware, have slowed down the implementation of the new quantum receiver scheme. A preliminary characterization of the new MPD-PDM detectors, before the delivering of the new time-tagger, already shows the improved timing accuracy of the new detectors with respect to the PMT used in the old setup. Figure 4.7 shows the results of this characterization. By fitting the histograms with a Gaussian curve of standard deviation $\sigma_G$ on the right and an exponential decay of parameter $\tau$ on the left, it is possible to give a first estimate of the timing accuracy of the detectors. The measurements, done at the MLRO using the Beacon-C and the Ajisai satellites, have $\sigma_G \simeq 120\,\text{ps}$ and $\tau \simeq 260\,\text{ps}$

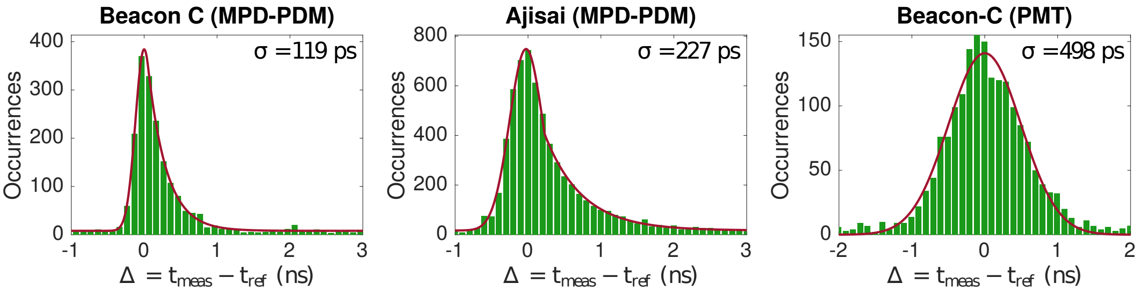

Figure 4.7: Detection time histograms obtained with the silicon SPAD (MPD-PDM) compared to the one obtained by PMT [148].

for the first one and $\sigma_G \simeq 227\,\mathrm{ps}$ and $\tau \simeq 510\,\mathrm{ps}$ for the second one. For comparison, a measurement of the timing accuracy of the PMT detectors has been performed, giving $\sigma_G \simeq 498\,\mathrm{ps}$ [148]. The measurements give an insight of the improved timing performance of the MPD-PDM detectors with respect of the old PMT one, high enough to observe also the pulse spread due to the optical depth of the satellite.

## 4.3 Data collection and analysis

Since the maintenance work at MLRO prevented the testing of the new implementation of the optical setup, the upgrade process focused on the development of the new software for data analysis. This new software divides the analysis task into independent sub-tasks, each involving a single step of the procedure. This Section will start by describing how data collection works, as a prerequisite for the description of the new architecture of the data analysis software. Then it will present some preliminary results on the orbit estimation task, fundamental for the improving of the detection timing accuracy.

### 4.3.1 Data collection

Data collection requires a strict synchronization between the laser ranging and the quantum subsystem, in order to avoid detector damaging due to back-scattered light in the transmission phases. The laser ranging PMT is active during a very narrow detection gate, which is dependent on the predictions of satellite orbits and can be manually adjusted by the operator in order to correct the residual differences with the real orbit. The detectors of the quantum subsystem, on the other hand, are protected by the shutter S2 before the quantum receiver.

The synchronization is obtained by feeding some of the signals coming from MLRO (Sync signals) into the FPGA controlling the quantum subsystem. Using these signals, the FPGA controls the opening and closing of both the transmitting and receiving shutter and, possibly, the quantum state preparation. The sync signals used for synchronization are the *start* signal, emitted when the LR laser is shot, the *gate* signal, when the return signal is expected, and the *stop* signal, corresponding to the effective detection of the return pulse by the laser ranging PMT.

The timing of transmission (TX) and reception (RX) of the qubit signals is dependent on the type of satellite that is being observed. Satellite are divided into four categories: low Earth orbit (LEO), with round trip time (RTT) lower than 25 ms, lower medium Earth orbit (l-MEO), with RTT between 25 and 50 ms, middle MEO (m-MEO), with RTT between 50 and 100 ms, and high MEO (h-MEO), with RTT > 100 ms. The timing diagram for the three categories is shown in Figure 4.8. For LEO satellites, where the beam returning from laser ranging is intense, it is necessary to have the reception shutter S2 closed at the arriving of the LR pulse. In this case, the quantum subsystem starts after the later possible arrival of the LR pulse, and, of the remaining 75 ms, about half is covered by transmission and half by reception. For MEO satellites, it is no longer necessary that the reception is closed at the arrival of the LR pulse, since its energy is not high enough to damage the single photon detector. Therefore, the entire 100 ms can be used for quantum transmission. For low and middle MEO, the predicted arrival of the LR pulse falls during the reception, making it possible to observe the LR pulse at the single photon level, something that might be useful in further exploitation of the setup for higher satellites. In the high MEO case, the transmission and the reception cover 100 ms each. This timing system, however, creates some problems with the LR system, since

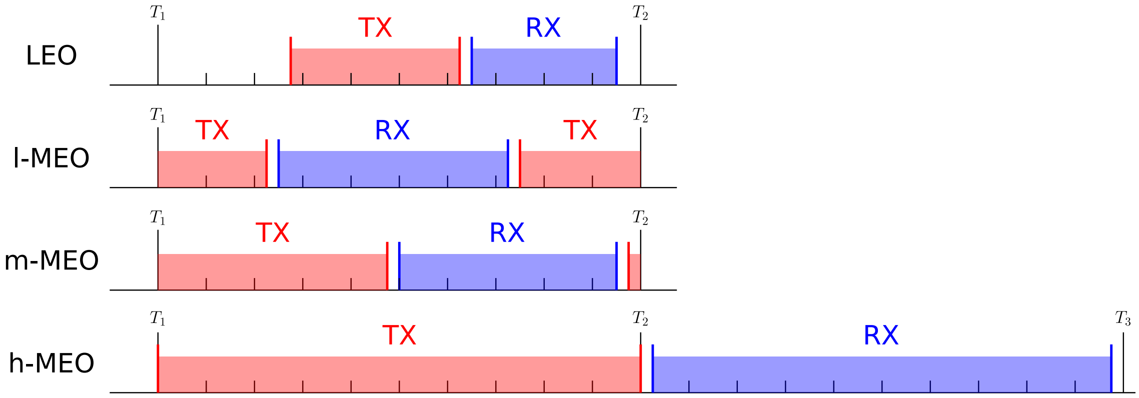

Figure 4.8: Timing diagram of the Matera quantum subsystem, for different kind of satellites. The blue region correspond to the transmission (TX), when the shutter S1 is open, while the red region to the reception (RX), when S2 is open. The instants $T_j$ correspond to the LR outgoing pulse (corresponding to the *start* signal). The intervals between TX and RX are due to the time the shutter takes to fully open (2 ms) and to fully close (2.5 ms) [56].

there is a 50% probability that the quantum system is transmitting during the gating of the LR detector, giving a signal due to back-scattered light. Up to now, this has not been a problem, since h-MEO satellites are almost unreachable with the existing setup. The enhanced performances of the new experimental scheme, however, make these satellites a viable target also for quantum transmission, requiring a slight change in the timing of quantum transmission.

All the relevant signals of the quantum system, the *start*, the *stop*, the *gate*, the *TX*, and the *RX* signal, are tagged into the time-tagger device, together with a reference 10 MHz signal coming from the atomic clock. In the old setup, also the signal coming from the two PMT is tagged into the same time-tagger device. The new setup, on the other hand, must put the output of the single-photon detectors into the new time-tagger, in order to take advantage of the enhanced resolution and accuracy. Since the new time-tagger has 4 regular channels plus a start channel, it is not possible to use it to tag all the signals, but it is still necessary to use the old time-tagging device, matching the tags of the two time-taggers in the data analysis phase.

### 4.3.2 Data analysis

Data analysis is performed using a dedicated program written in MATLAB. The program is divided into two parts, according to the two main tasks of the data analysis. One part of the program covers the load and preprocessing of the raw time-tags collected by the time-tagging devices, while the other one takes the data processed in the first part and analyzes them. In order to keep the code readable and easily modifiable, it has been written using an object-oriented approach, with the classes further grouped into modules. This Section gives a global description of the data analysis software, divided into the two main parts of the analysis.

### Preprocessing raw tags

The first step of data analysis is in charge with loading the data collected from the different time-taggers, process them and put them in a form easily analyzable in the following part. The behavior of this step is shown in the block diagram of Figure 4.9.

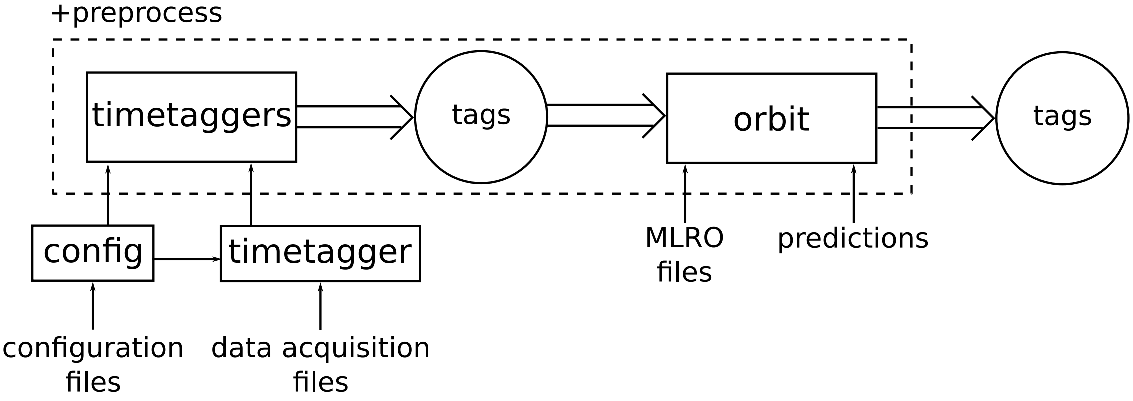

Figure 4.9: Block diagram of the first step of data analysis. The raw data and the configuration, read through the classes `timetagger` and `config` respectively, are provided as an input to the `timetaggers` class of the `+preprocess` module. The class outputs the `tags` structure, containing all the tags from the different time-taggers into a single time-scale. The `tags` structure is then used as input for the `orbit` class, that analyzes the orbit, using the auxiliary input of MLRO files and predictions (loaded by two dedicated classes in the `+preprocess` module).

The classes of the preprocessing pipeline are placed in the `+preprocess` module.

- The class `timetaggers` is in charge with taking the time-tags from the different time-taggers and place them into the `tags` structure. Data loading is performed using the abstract class `timetagger` of the `+timetagger` module, whose subclasses implement the loading method for the different time-taggers. The hardware configuration, such as the number of time-taggers involved and the signals connected to each channel, is loaded into a configuration structure by the `config` class of the `+config` module. Once data are loaded, the `timetaggers` class puts all time-tags into the same timescale using an arbitrary, non-periodic reference signal shared by the different time-taggers and corrects the residual time drifts due to clock instabilities.
- The class `orbit` performs the fit of the satellite orbit, in order to recover eventual *stop* signals not detected by the LR setup. This task is performed through the help of two auxiliary classes of the `+preprocess` package, `mts` and `cpf_pred`. The first one takes as input the file containing all the data acquired by the MLRO during the passage of the satellite, while the second one computes the predictions of the satellite orbit provided by the ILRS. The analysis of the satellite orbit will be treated in Section 4.3.3.

At the end of the preprocessing step, the `tags` structure contains raw time-tags in a single time scale, hardware configuration parameters and fitted orbit.

### Qubit analysis

The second step of data analysis takes the data contained in the `tags` structure and uses them to construct a new `qubit` structure, that contains the time-tags coming from the single photon detectors (corresponding to received qubits), and all the information about that detection event. Indeed, detection events have a different meaning according to their position in the period within two LR pulses. The distribution of the detection events between two $RX$ signals is shown in Figure 4.10.

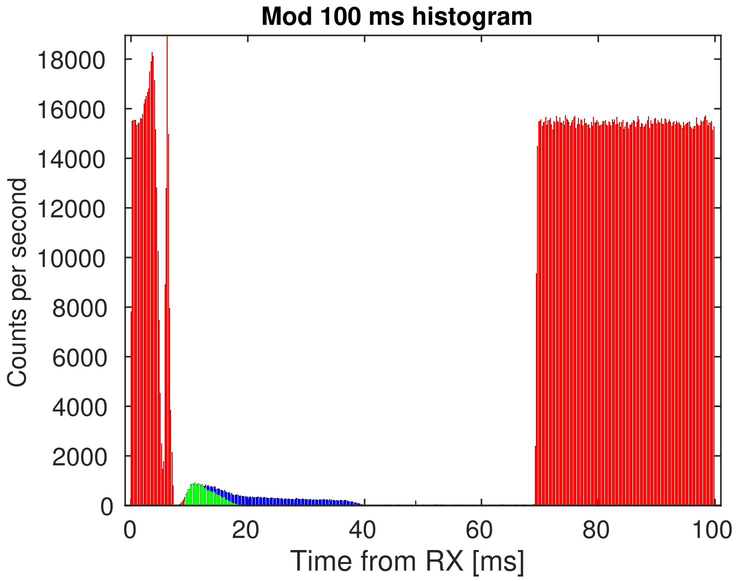

Figure 4.10: Distribution of the detection events between two $RX$ signals for a Beacon-C passage. Red data correspond to detection events happening when the transmission shutter S1 is, at leas partially, opened. Green and blue events correspond to detection events when the receiving shutter S2 is open. Blue events happen later than the time of closure of the transmission plus one round-trip time, therefore they are noise events. Detection events corresponding to qubits reflected by the satellite must lie in the green region.

As described in Section 4.3.1, during the operation of the quantum subsystem there exist three different phases: the transmission (TX) phase, the reception (RX) phase and the LR phase (when both S1 and S2 are closed). During the LR phase (which is present only for LEO satellites, as evident form Figure 4.8), both the transmission and the reception shutters are closed. Qubit events coming from the satellite can happen only in a short region of the RX phase, within one round-trip time from the closure of the transmission shutter S1. All the other events in the reception phase are due to noise coming from the sky, since the telescope is still pointing the satellite, but there is no signal coming from the satellite.

The class `main_analysis` of the module `+analysis` takes the tags coming from the detectors and splits them into the regions shown in Figure 4.10, according to the time difference between each detection event and the preceding $RX$ signal. Then the class takes the data in the region where satellite returns are expected and splits them into "qubit slots", which, summed together, give the histogram show in Figure 4.11.

The analysis implemented in the class `main_analysis` performs the tasks common to all the experiments using the setup described in this Chapter. Some experiments, however, may require some additional analysis, as happens for the interference experiment described in Section 5.1. In this case, the analysis is performed by a subclass of `main_analysis` that implements the functions specific to the experiment.

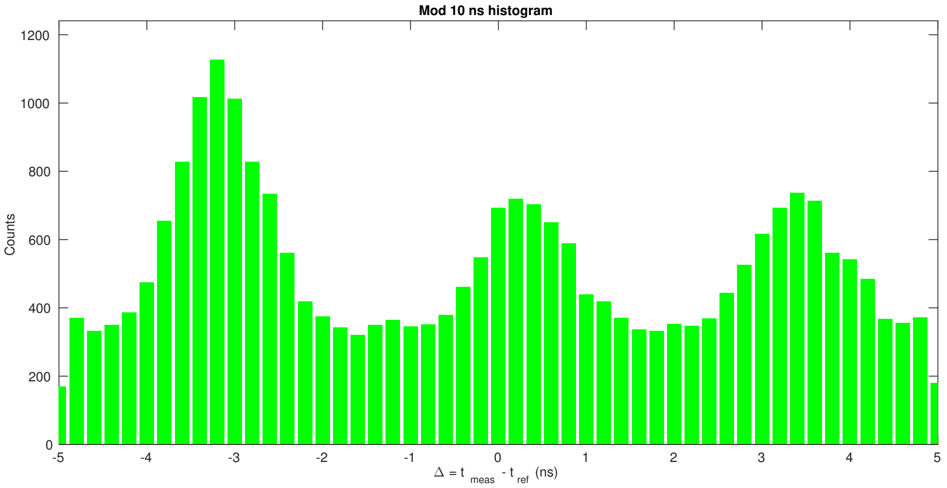

Figure 4.11: Comparison of the measured time of detection $t_{meas}$ with the expected time of arrival $t_{ref}$ for a Beacon-C passage. The three peaks are due to the presence of the interferometric setup described in Section 5.1.

### 4.3.3 Orbit reconstruction

One of the crucial tasks for the exploitation of the improved hardware is the high accuracy prediction of the satellite orbit. Orbit reconstruction is based on the signals coming from the LR subsystems, i.e., the *start* and *stop* signal, corresponding to the transmission and reception of the LR pulse. By taking the difference between stop and starts, it is possible to measure the round-trip time $t_{rtt}$ as a function of the time during a satellite passage, giving a curve like the one shown in Figure 4.12, for a passage of the satellite Ajisai. The

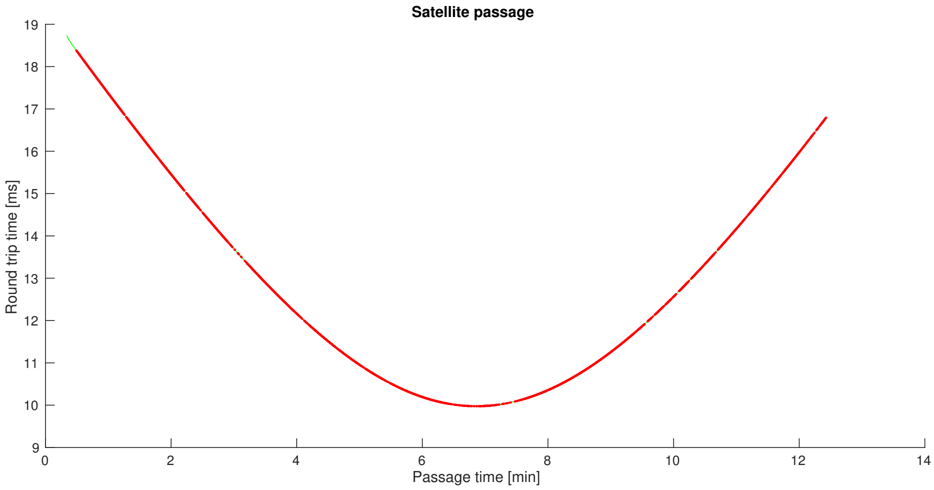

Figure 4.12: Round-trip time curve for a passage of Ajisai satellite (11.07.2015, h 21.11 CEST). Red points represent the measured values of the round-trip time, while the green curve (hidden by the red points on almost all the orbit) represents the segmented fit of the orbit.

measured points correspond to those events in which the MLRO has detected the return pulse (producing a valid *stop* signal). The main reason for the need of an orbital fit is to recover *stop* signals that are not recorded by MLRO (for example, due to a too faint return pulse), in order to have the time reference necessary for the qubit analysis also in those intervals.

The fit is performed by dividing the orbit into segments of 10 s each, and fitting separately each segment with a 4th degree polynomial. The histogram of the residuals of the segmented fit for the Ajisai passage already shown is represented in Figure 4.13. The standard deviation of the residuals is 0.22 ns, much lower than the jitter of the single-photon PMT detectors used in the existing setup. However, the hardware improvement characterizing the new experimental scheme would render the fit procedure the highest source of temporal inaccuracy in the detected events.

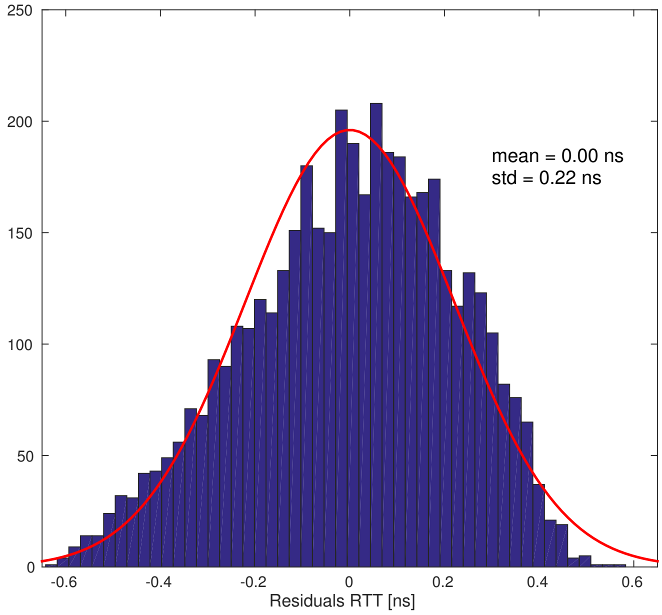

Figure 4.13: Histogram of the residuals of the segmented fit on the stops of a passage of the Ajisai satellite (11.07.2015, h 21.11 CEST). The standard deviation of the residuals is 0.22 ns.

In order to improve the precision of the orbital fit, some techniques are currently being tested. This section reports the first, preliminary results of this investigation, which, however, requires the analysis of the high temporal accuracy data provided by the new experimental scheme in order to be validated.

The first technique used for the improvement of the orbital fit is the exploitation of all the data collected by MLRO during the satellite passage. Indeed, besides the *start* and the *stop* signal, the LR subsystem saves a lot of other data coming from the devices composing it. The most important data for these analysis are those related to the detection and the analysis of the reflected LR pulse, which gives the direct measurement of the round-trip time. The most important datum is the correction to the *stop* signal due to the constant-fraction discriminator (CFD) used in the tagging of the reflected pulse. The study of the response of the CFD as a function of the energy of the reflected pulse, made using a fixed-distance ground target, allowed the laser-ranging team at MLRO to find the relationship between the correction and the received energy. In addition to providing the input to the CFD correction, the received energy is itself a measurement of the timing accuracy of the received LR pulse. Indeed, in low energy pulses the effect of the optical depth of the satellite retro-reflector array starts to give a significant contribute, while in high energy pulses the rising edge of the signal coming from the PMT corresponds almost always to the nearest retro-reflector [149]. This effect can be observed by dividing the incoming pulses into different regions according to the received energy, as shown in Figure 4.14. The standard deviation of the red, green and yellow points is lower than the one observed in Figure 4.13, indicating that, obviously, the accuracy of the orbital fit is highly improved by implementing CFD correction. Indeed, gray points, for which this correction is not possible, have a standard deviation comparable with the one of the data in Figure 4.13. Moreover, the higher precision in the fit of the points with higher received energy suggests that the precision of the orbital fit can be improved by selecting only the points above a certain threshold.

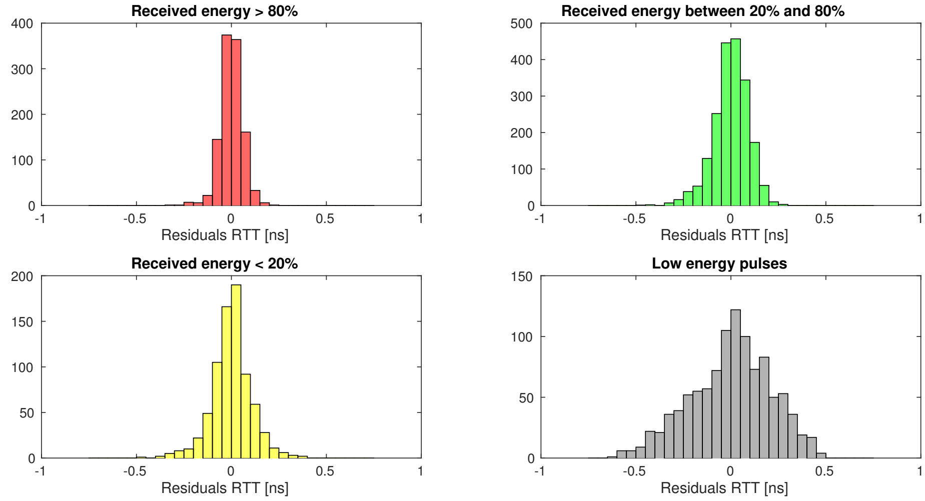

Figure 4.14: Histogram of the residuals of the segmented fit for data where the received energy (top left, red) is at least 80% of the saturation level, (top right, green) is between 20% and 80% of the saturation level, (bottom left, yellow) is below 20% of the saturation level, and (bottom right, gray) the received energy is too low for the energy measurement. In the first three cases, the time-of-flight datum has been corrected for the CFD delay. The standard deviation of the distribution is (red) $\sigma = 58\,\text{ps}$, (green) $\sigma = 92\,\text{ps}$, (yellow) $\sigma = 103\,\text{ps}$, and (gray) $\sigma = 212\,\text{ps}$.

Another technique that is currently being evaluated for the fit of the orbital data uses the predictions of the satellite orbit calculated by the ILRS. Indeed, as already explained in Section 4.1, the ILRS collects the observations coming from all the SLR stations and emits, on a daily basis, the orbit predictions for each LR satellite. These predictions are released in a standard format, the Consolidated Prediction Format (CPF) [150], in which the position of the satellite as a function of time is given using the International Terrestrial Reference Frame (ITRF)[6]. These positions can be converted into the azimuth-elevation-

[6] This reference system, also known as geocentric earth-fixed coordinate system, is centered at the center of the Earth and rotates together with it. In this coordinate system, the coordinates of a point on the Earth, such as a LR station, do not change with time.

range reference system for a given position on the Earth by using a sample program distributed in the ILRS website [141, 150].

The fit technique that is currently being evaluated is a global, polynomial fit of the difference between the predicted and the measured round-trip time. The advantage of the use of a global fit lies in the fact that it allows to recover the position of the *stop* signal even in those cases where the LR subsystem could not detect it. However, despite the high accuracy of LR data and the sophisticated models used to perform the predictions, however, the predicted RTT still present significant differences with the measured one. In order to give an accurate fit of the experimental data, it is necessary to use a very precise *time bias* [151] when calculating the predictions, different from satellite to satellite. The results of the analysis of the Ajisai passage using a 6th degree global fit of the difference between the predicted and the measured RTT in shown in Figure 4.15. As evident from the Figure, the results of this procedure are comparable with the ones obtained with the segmented fit. On the other hand, in order to obtain a good result it is necessary to quite finely tune the value of the time bias, otherwise the fitting procedure is not able to obtain significant results.

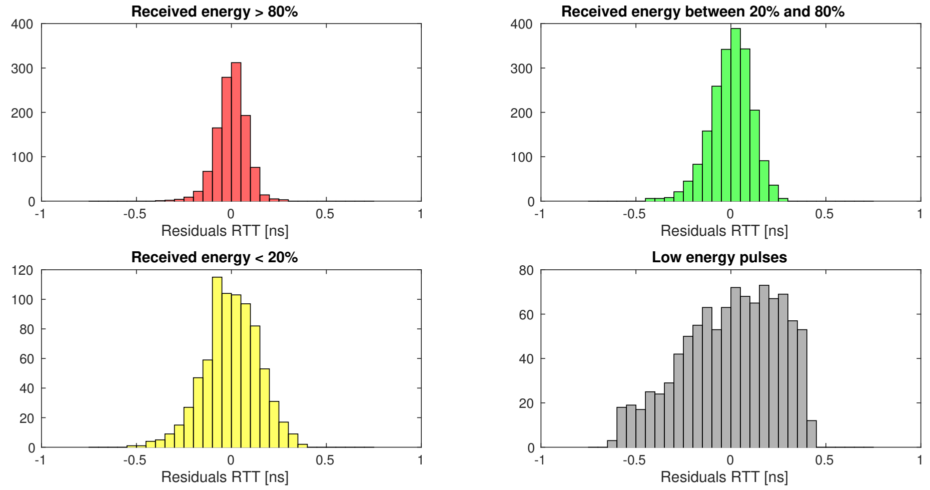

Figure 4.15: Histogram of the residuals for the global fit of the difference between predicted and measured RTT. The predicted RTT has been calculated using a time bias $t_{bias} = -29.5\,\mathrm{ms}$. Data are divided according to their received energy. In particular, the received energy (top left, red) is at least 80% of the saturation level, (top right, green) is between 20% and 80% of the saturation level, (bottom left, yellow) is below 20% of the saturation level, and (bottom right, gray) the received energy is too low for the energy measurement. In the first three cases, the time-of-flight datum has been corrected for the CFD delay. The standard deviation of the distribution is (red) $\sigma = 78\,\mathrm{ps}$, (green) $\sigma = 108\,\mathrm{ps}$, (yellow) $\sigma = 143\,\mathrm{ps}$, and (gray) $\sigma = 253\,\mathrm{ps}$.

Up to now, it is still uncertain which fit procedure is the best one for the new experimental setup. While the ongoing study described in this section is important to compare the different fitting techniques and to develop the software necessary for the task, the final choice must rely on the data of the new experimental scheme, and must therefore wait for its operativeness.

# Chapter 5

# Space experiments

The experimental setup described in the previous Chapter has been exploited since 2003 for a series of pioneering experiments on the study of the satellite-ground channel for quantum communication. These experiments have demonstrated the basis requirements for satellite quantum communication, i.e., the possibility to build a quantum channel between the Earth and a satellite [132, 145], its possible exploitation as a channel for polarization-encoded qubits [133] and, finally, its behavior with respect to time-bin encoded qubits [134]. These results have important consequences both from a scientific and a technical point of view. From the scientific side, they provide a validation for quantum channel models, giving the basis for its possible exploitation for quantum experiments between Earth and satellites. From the technical side, on the other hand, they have stimulated the development of the necessary expertise for the usage of this channel, as testified by the increasing rate of results obtained in this field.

This Chapter is devoted to the description of the last experiment involving the satellite-ground channel, aimed to study its behavior on time-bin encoded qubits. Since the experiment has been implemented using the setup described in Section 4.2.1, with the data collection and analysis procedures described in Section 4.3, the description of the experimental setup will concentrate on the state preparation and measurement prodedures.

## 5.1 Single-photon quantum interference

### 5.1.1 Experimental setup

In time-bin encoding, the information is encoded in the temporal modes of the electromagnetic field. The two basis vectors of the computational basis are $\hat{a}^\dagger_{i,t_0}\left|\Omega\right\rangle = \left|t_0\right\rangle := \left|0\right\rangle$ and $\hat{a}^\dagger_{i,t_1}\left|\Omega\right\rangle = \left|t_1\right\rangle := \left|1\right\rangle$, where the two modes must be orthogonal, i.e.,

$$\langle t_0|t_1\rangle = e^{-\frac{(t_1-t_0)^2}{2\tau_c^2}} \simeq 0, \tag{5.1}$$

requiring that $|t_1 - t_0| \gg \tau_c$. Experimentally, the generation of time-bin encoded qubits employs an unbalanced interferometer, such as a Mach-Zehnder interferometer (MZI), with the difference between the time of flight of the two arms much larger than the coherence time of the laser.

The "state preparation" part of Figure 4.3 consists in an unbalanced MZI, with $l \simeq 1\,\mathrm{m}$, corresponding to a time-of-flight difference $\Delta t = |t_1 - t_0| \simeq 3.4\,\mathrm{ns}$. The coherence time of the qubit laser, measured with the method described in 2.3.1, is $\tau_c = 23.3\,\mathrm{ps}$ (the envelope of the intensity is shown in Figure 5.1). Since the condition $\Delta t \gg \tau_c$ is respected, this

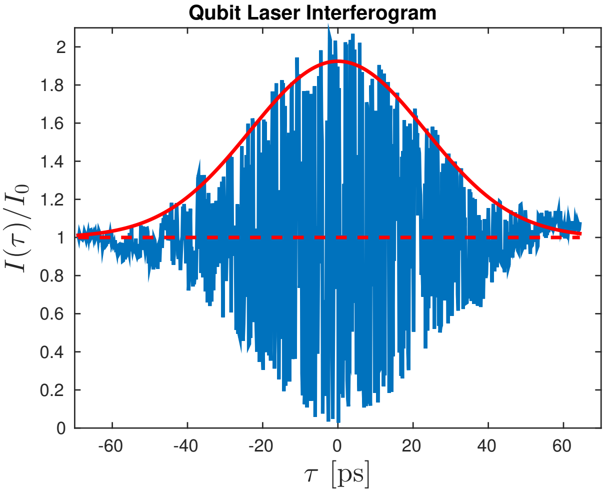

Figure 5.1: Measure of the envelope of $I(\tau)$ for the laser used as a source for the quantum subsystem.

optical network is suitable for the preparation of time-bin encoded qubits. In this configuration, the system is prepared in the time-bin encoded state $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$.

The "measure" part of the quantum subsystem employs the same unbalanced MZI used for state preparation. This configuration, equivalent to the one used in Plug-and-Play Quantum Key Distribution [152, 153], allows to avoid an active stabilization of the preparation and measurement interferometers. The plug-and-play state preparation and measurement setup used for this experiment is shown in Figure 5.2, where the interferometer is placed in the common route of the output and input beams, and the transmitter and the receiver are placed at the two different output ports of BS2.

A fundamental requirement for both state preparation and measurement is that the spatial mode of the electromagnetic field is the same for both entrances of the beam-splitter, otherwise the field operators of the two time-bins are $\hat{a}_{i,t_0}$ and $\hat{a}_{j,t_1}$ with $i \neq j$, which can no longer be used to generate a time-bin encoded qubit[1]. This is obtained by using two $4f$-systems at the long arm of the MZI, realizing an optical relay that compensates the different propagation length in the two arms of the interferometer. Each $4f$-system is composed by two lenses with $f = 125\,\text{mm}$, positioned as in Figure 5.3A. A single $4f$-system generates a mirror transformation of the wavefront from one side to the other. By placing a second $4f$-system in the other arm of the interferometer it is thus possible to compensate the mirror transformation, generating a system whose wavefront is almost identical after propagation through different distances, as evident from Figure 5.3B.

When the time-bin state coming from the satellite enters back the MZI, detection events show a three peak profile like the one shown in Figure 4.11. The first peak corresponds to a photon taking the short arm of the interferometer both in preparation and in measurement, while the third one is due to the combination of two long arm propagations. The central peak, on the other hand, is the superposition of the short-long and long-short path, which interfere at the output beam-splitter BS2. By post-selecting the data on the central peak, the configuration of Figure 5.2 corresponds to a measurement in the basis $\{|+\rangle, |-\rangle\}$ of the

[1] In this case, the time-bin and the spatial modes are entangled, causing decoherence when the time-bin mode is measured.

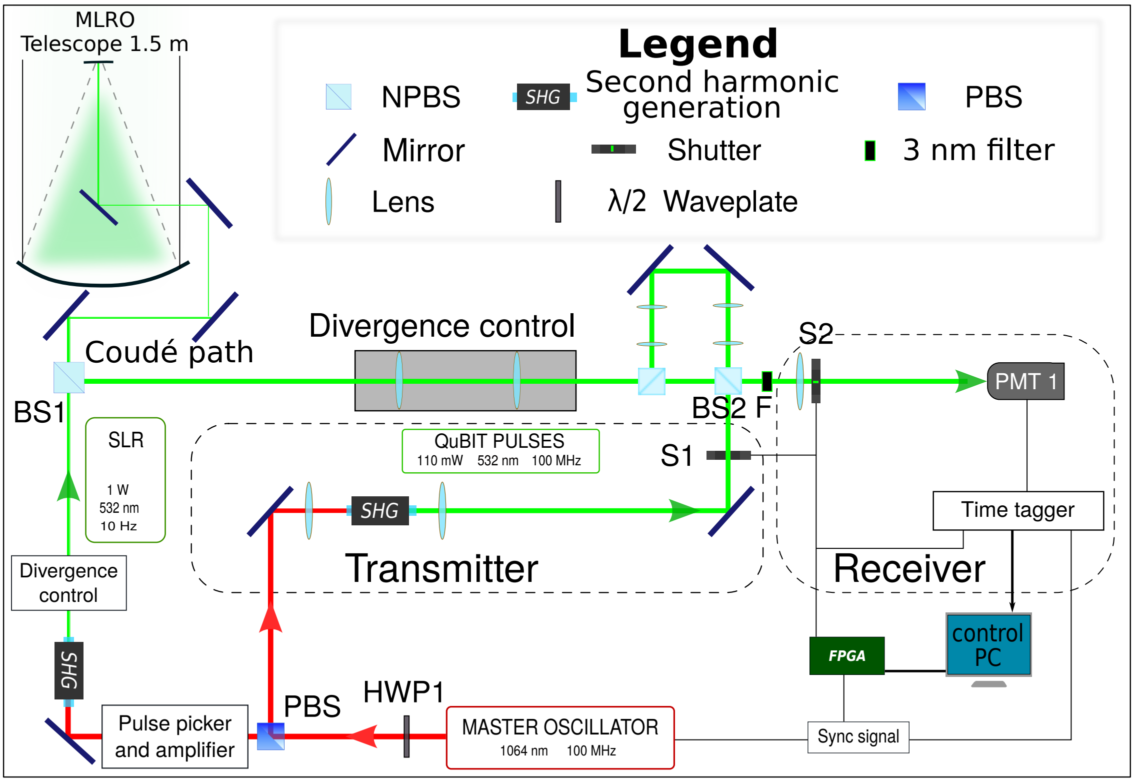

Figure 5.2: Setup used for the single photon interference experiment, aimed to the study of the quantum channel in the time-bin degree of freedom. State preparation and measurement use the same unbalanced MZI.

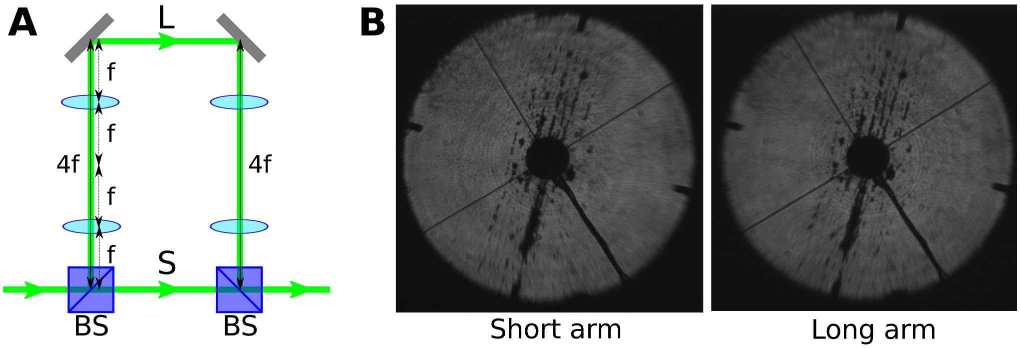

Figure 5.3: (**A**) The unbalanced MZI interferometer used for state preparation and measurement. (**B**) Images of the primary mirror with only the short or long arm opened. From Vallone *et al.* [134].

time-bin qubit, realized as a projection on the state $|+\rangle\langle+|$ (it is the opposite with respect to state preparation because the opposite port of the beam-splitter BS2 is employed in the measurement).

### 5.1.2 Field-operator transformation in the two-way channel

In order to study the transformation introduced by the quantum channel in the time-bin degree of freedom, it is convenient to adapt the notation used in Section 1.5.2 for the time-bin encoding to the case of flying qubits. Since a wavepacket propagating in forward (backward) direction is described by a mode function of the form $f(r/c-t)$ $(f(r/c+t))$, it is convenient to describe the field operator of a forward (backward) propagating wave as $\hat{a}^\dagger_{\tau-}$ $(\hat{a}^\dagger_{\tau+})$, with $\tau_\pm = r/c \pm t$.

With this notation, the field operator of the mode exiting from the qubit laser is $\hat{a}^\dagger_{i,\tau_-}$, which can be expressed as

$$\hat{a}^\dagger_{i,\tau_-} = \int dt \psi(\omega_0;\tau_-)\hat{a}^\dagger_i, \tag{5.2}$$

where $\hat{a}^\dagger_i$ is the field operator corresponding to spatial mode $i$ and

$$\psi(\omega_0;\tau_-) = \frac{1}{\sqrt[4]{\pi\tau_c}} e^{-\frac{\tau_-^2}{2\tau_c^2}} e^{i\omega_0\tau_-}. \tag{5.3}$$

After the state preparation step, the field operator is transformed into

$$\frac{1}{\sqrt{2}}\left(\hat{a}_{i,\tau_-} - \hat{a}_{i,(\tau_- - \Delta t)}\right), \tag{5.4}$$

where $\Delta t$ is the time-of-flight difference between the two arms of the interferometer.

In order to study the effect of the reflection of the satellite on the field operator, it is convenient to change the reference system to one whose origin is at the location of the satellite. By assuming that the satellite is moving with constant velocity with respect to the interferometer and that at time $t=0$ it is located at $r = r_{sat}$, the Lorentz transformation relating the laboratory system $(r,t)$ to the satellite system $(r',t')$ is

$$\begin{cases} r' = \gamma(r - r_{sat} - \beta ct) \\ t' = \gamma\left(t - \beta\dfrac{r - r_{sat}}{c}\right) \end{cases}, \qquad \begin{cases} r = r_{sat} + \gamma(r' + \beta ct') \\ t = \gamma\left(t' + \beta\dfrac{r'}{c}\right) \end{cases}, \tag{5.5}$$

where $\beta = v_r/c$, with $v_r$ the radial velocity of the satellite, and $\gamma = \left(1-\beta^2\right)^{-\frac{1}{2}}$ is the Lorentz factor. In the reference frame of the satellite, therefore, the parameters $\tau_\pm$ are transformed into

$$\tau_\pm = \gamma(1\pm\beta)\tau'_\pm + \frac{r_{sat}}{c} = \sqrt{\frac{1\pm\beta}{1\mp\beta}}\tau'_\pm + \frac{r_{sat}}{c}. \tag{5.6}$$

In this reference frame, the mirror reflection can be simply described as $\tau'_- \to -\tau'_+$. By using the inverse of Equation (5.6), i.e., $\tau'_+ = \frac{1}{\gamma(1+\beta)}\left(\tau_+ - \frac{r_{sat}}{c}\right)$, it is possible to go back to the laboratory reference. The total transformation is

$$\begin{aligned} \tau_- &\xrightarrow{\text{boost to satellite ref. frame}} \gamma(1-\beta)\tau'_- + \frac{r_{sat}}{c} \xrightarrow{\text{reflection}} -\gamma(1-\beta)\tau'_+ + \frac{r_{sat}}{c} \\ &\xrightarrow{\text{boost back to laboratory ref. frame}} -f_\beta(\tau_+ - t_{rtt}), \end{aligned} \tag{5.7}$$

where

$$t_{rtt} = \frac{2}{1-\beta}\frac{r_{sat}}{c} \tag{5.8}$$

is the round-trip time and

$$f_\beta = \gamma^2(1-\beta)^2 = \frac{1-\beta}{1+\beta}. \tag{5.9}$$

The field operator entering back the telescope is

$$\frac{\gamma(1-\beta)}{\sqrt{2}}\left[\hat{a}^\dagger_{i,(-f_\beta(\tau_+ - t_{rtt}))} - \hat{a}^\dagger_{i,(-f_\beta(\tau_+ - t_{rtt})-\Delta t)}\right], \tag{5.10}$$

where the new basis vectors of the time-bin encoding are

$$\begin{aligned} |0\rangle_{sat} &\equiv \hat{a}^{\dagger}_{i,(-f_\beta(\tau_+ - t_{rtt}))} |\Omega\rangle , \\ |1\rangle_{sat} &\equiv \hat{a}^{\dagger}_{i,(-f_\beta(\tau_+ - t_{rtt} - \Delta t))} |\Omega\rangle \end{aligned} \tag{5.11}$$

By looking at the definition of the time-bin field operators in (5.3), it can be noticed that the central frequency of the new basis vector is transformed from $\omega_0$ to $f_\beta \omega_0$, with the new coherence time given by

$$\tau_c' = \frac{\tau_c}{f_\beta} = \frac{1+\beta}{1-\beta}\tau_c. \tag{5.12}$$

By comparing the state entering the interferometer (5.10) with the definition of the time-bin basis vectors (5.11), the state prepared by the satellite can be written as

$$|0\rangle_{sat} - e^{i\phi(t)} |1\rangle_{sat} , \tag{5.13}$$

where

$$\phi(t) = e^{i\omega_0 \Delta t(1-f_{\beta(t)})} = \frac{2\beta(t)}{1+\beta(t)} \frac{2\pi c}{\lambda} \Delta t, \tag{5.14}$$

is the kinematic phase, which is dependent on the instantaneous radial velocity of the satellite $\beta(t)$.

After passing again through the MZI, the field operator at the detection port of the MZI is given by

$$\frac{i\gamma(1-\beta)}{2}\Big[\hat{a}^{\dagger}_{i,(-f_\beta\tilde{\tau}_+)} + \hat{a}^{\dagger}_{i,(-f_\beta(\tilde{\tau}_+ + \Delta t))} - \hat{a}^{\dagger}_{i,(-\Delta t - f_\beta\tilde{\tau}_+)} - \hat{a}^{\dagger}_{i,(-\Delta t - f_\beta(\tilde{\tau}_+ + \Delta t))}\Big], \tag{5.15}$$

where $\tilde{\tau}_+ = \tau_+ - t_{rtt}$. This state gives at the detector the three pulses typical of time-bin measurements. The probability of having the photon in the central pulse is

$$\begin{aligned} \mathbb{P}_c(t) &= \frac{\gamma^2(1-\beta(t))^2}{4} \int dt' |\psi(-f_\beta(t'+\Delta t)) - \psi(-\Delta t - f_\beta t')|^2 \\ &= \frac{1}{2}\left\{1 - \sqrt{\frac{1}{\pi\tau_c^2}} \int dt' \Re \left[ e^{-\frac{(t'+f_\beta\Delta t)^2}{2\tau_c^2}} e^{-\frac{(t'+\Delta t)^2}{2\tau_c^2}} e^{i\omega_0(1-f_\beta)\Delta t} \right] \right\} \\ &= \frac{1}{2}\left[1 - \mathcal{V}(t)\cos\varphi(t)\right] , \end{aligned} \tag{5.16}$$

with $\phi(t)$ the kinematic phase of Equation (5.14) and

$$\mathcal{V}(t) = \sqrt{\frac{1}{\pi\tau_c^2}} \int dt' \, e^{-\frac{(t'+f_\beta\Delta t))^2}{2\tau_c^2}} e^{-\frac{(t'+\Delta t)^2}{2\tau_c^2}} = \exp\{-\left[\frac{\Delta t}{\tau_c}\frac{\beta(t)}{1+\beta(t)}\right]^2\} \tag{5.17}$$

is the theoretical visibility, which is due to the fact that the state is prepared by the satellite in the basis $\left\{|0\rangle_{sat}, |1\rangle_{sat}\right\}$ and measured in the basis $\left\{|0\rangle, |1\rangle\right\}$. In practice, however, the theoretical visibility is approximately 1, since the $\beta$ factor is upper bounded by $3 \cdot 10^{-5}$ for all the observed satellites, while the ratio $\Delta t/\tau_c$ is of the order of $10^2$.

### 5.1.3 Results

The experimental study of the space channel in the time-bin encoding is based on the accuracy of the measurement of the time-bin encoded state coming from the satellite. This accuracy can be validated by observing the interference pattern $\mathbb{P}_c = \frac{1}{2}\left[1 - \cos\phi\right]$ on the central peak for different input states $|\psi\rangle = |0\rangle - e^{i\phi}|1\rangle$. From this point of view, the presence of the kinematic phase can be exploited to make the measurement over the whole range of $\phi$ without having to change the state preparation setup. On the other hand, this requires a way to estimate the kinematic phase in order to know the input state for each point of the passage of a satellite. During the orbit of a satellite, the kinematic phase varies very rapidly, as shown in Figure 5.4, inducing a very rapid variation of the interference pattern. This makes the task of estimation of the kinematic phase crucial for the experiment, since averaging different of its values makes interference diminish or even disappear at all.

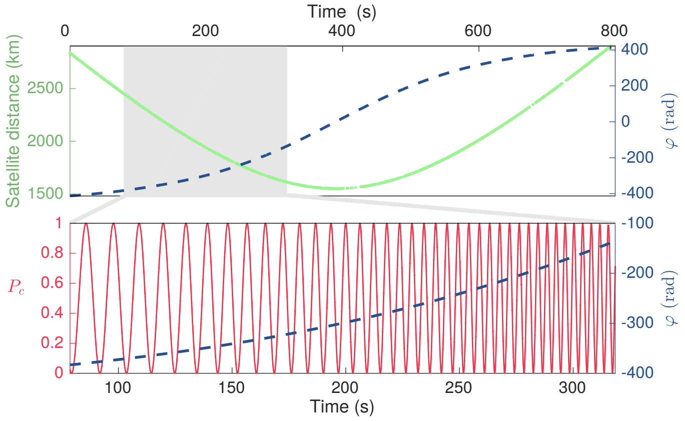

Figure 5.4: Kinematic phase and interference pattern. In the top panel, the measured satellite distance and the predicted kinematic phase $\phi(t)$ as a function of time are shown for a passage of the Ajisai satellite. In the bottom panel, the kinematic phase $\phi(t)$ and the theoretical probability $\mathbb{P}_c(t)$ of the shaded area are shown. From Vallone *et al.* [134].

The kinematic phase can be estimated by using Equation (5.14), once the radial velocity of the satellite $\beta(t)$ is known. This parameter, however, can be easily measured using the data coming from MLRO. Indeed, as shown in Figure 5.5, the temporal separation $\Delta T'$ of two LR pulses at the receiver after satellite retro-reflection, due to the Doppler effect, is related to the temporal separation $\Delta T = 100\,\mathrm{ms}$ of two successive LR pulses by the relation

$$\Delta T' = \Delta T \frac{1 + \beta(t)}{1 - \beta(t)}, \tag{5.18}$$

which allows to estimate the radial velocity $\beta(t)$ as

$$\beta(t) = \frac{\Delta T' - \Delta T}{\Delta T' + \Delta T}. \tag{5.19}$$

Using this method to estimate the kinematic phase, it is possible to make the 10 ns histograms corresponding to constructive and destructive interference shown in Figure 5.6, for a passage of the Beacon-C satellite. The constructive interference is the sum of all detections corresponding to $\phi \pmod{2\pi} \in \left[4\pi/5, 6\pi/5\right]$, while destructive interference corresponds to $\phi \pmod{2\pi} \in \left[-\pi/5, \pi/5\right]$. It is evident from Figure 5.6 the importance

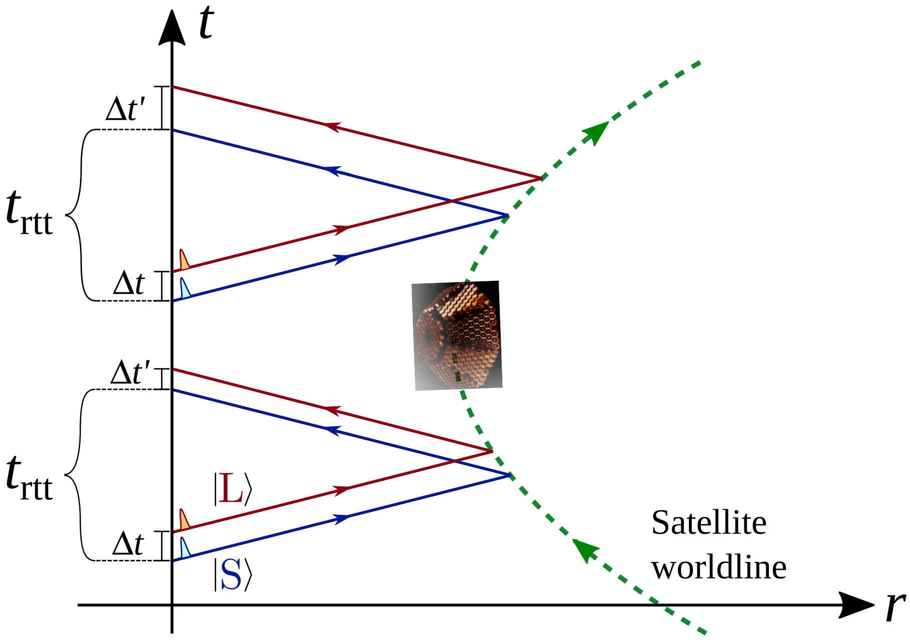

Figure 5.5: **Space-time diagram of light propagation.** As explained in Section 5.1.2, pulses separated on ground by a delay $\Delta t$ are received with a delay $\Delta t' = \Delta t / f_\beta$ due to the motion of the satellite. The round-trip time (rtt) is $t_{rtt}$.

of phase selection in order to see the interference effect, that is marked when the right intervals are selected but is completely washed out if no selection on the kinematic phase is performed. By using these data, it is possible to estimate the probability $\mathbb{P}_c^{(exp)}$ as the ratio of the detections in the central peak $N_c$ to twice the sum $N_\ell$ of the detections in the lateral peaks, namely

$$\mathbb{P}_c^{(exp)} = \frac{N_c}{2N_\ell}. \tag{5.20}$$

The measured values are $\mathbb{P}_c^{(exp)} = 0.87 \pm 0.10$ for constructive interference and $\mathbb{P}_c^{(exp)} = 0.20 \pm 0.03$ for destructive interference. These values deviate with statistical evidence from the value 0.5 expected in the case of no interference.

From the data collected, it is also possible to recover the entire interference curve, by calculating the value of the experimental probability $\mathbb{P}_c^{(ext)}$ for different values of the kinematic phase $\phi$. To this goal, the data from three different satellites have been split into ten regions of different kinematic phase $\phi$, and their interference curve has been plotted in Figure 5.7. By fitting the data with $\mathbb{P}_c^{(exp)} = \frac{1}{2}\left[1 - \mathcal{V}_{exp} \cos\phi\right]$, it is possible to measure the experimental visibility $\mathcal{V}_{exp} = (67 \pm 11)\%$ for Beacon-C, $\mathcal{V}_{exp} = (53 \pm 13)\%$ for Stella and $\mathcal{V}_{exp} = (38 \pm 4)\%$ for Ajisai. The data are collected for $r_{sat} \in [1600, 2500]$ $km$ for Ajisai (12.07.2015, h 3.42 CEST), $r_{sat} \in [1100, 1500]$ $km$ for Stella (12.07.2015, h 3.08 CEST), and for $r_{sat} \in [1200, 1500]$ $km$ for Beacon-C (11.07.2015, h 1.33 CEST).

The observation of the interference patterns clearly demonstrates that the coherence between the two temporal modes is preserved along propagation through the space channel. The different values of experimental visibility is probably due to some residual vibrations of the unbalanced MZI between the up-going and the down-going pulses. The incidence of these vibrations is higher for the Ajisai satellite, which is the further one, thus confirming this hypothesis. Despite that, however, this experiment shows that the quantum channel

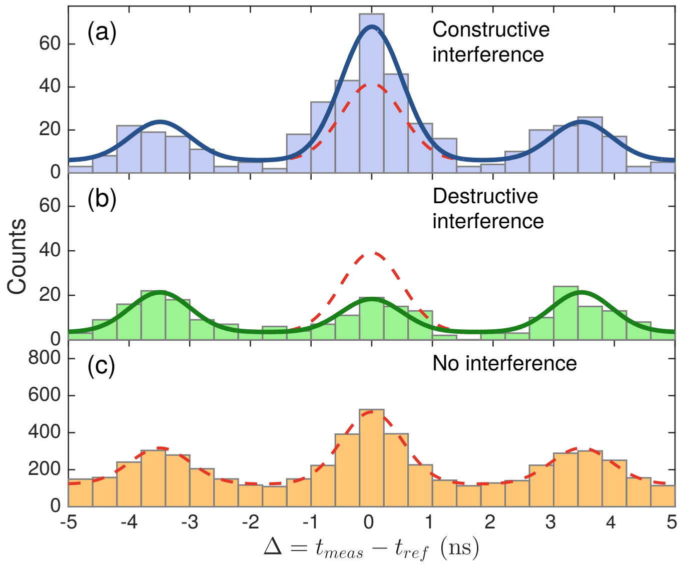

Figure 5.6: Constructive and destructive interference (Beacon-C satellite, 11.07.2015 h 1.33 CEST). $(a)$: histogram of the single photon detections as a function of time $\Delta = t_{meas} - t_{ref}$ realized by selecting only the intervals characterized by $\phi \pmod{2\pi} \in [4\pi/5, 6\pi/5]$ that lead to constructive interference. Solid line shows the tri-Gaussian fit. The Gaussian interpolation gives $N_\ell = 112 \pm 11$ counts for the sum of lateral peaks and $N_c = 196 \pm 14$ for the central one. $(b)$: histogram of the single photon detections realized by selecting only the intervals characterized by $\phi \pmod{2\pi} \in [-\pi/5, \pi/5]$. Here $N_\ell = 112 \pm 11$ and $N_c = 46 \pm 7$. $(c)$: histogram of the single photon detections without any selection on the phase. As expected, interference is completed washed out and the measured counts are $N_c = 1245 \pm 35$ and $N_\ell = 1306 \pm 36$, fully compatible with $P_c = 1/2$. In all panels, dotted red lines represent the expected counts in case of no interference. From Vallone *et al.* [134].

preserves the time-bin encoding, and gives some useful insight into the effects that have to be taken into account in order to implement quantum communication protocols in the satellite-ground channel using this encoding.

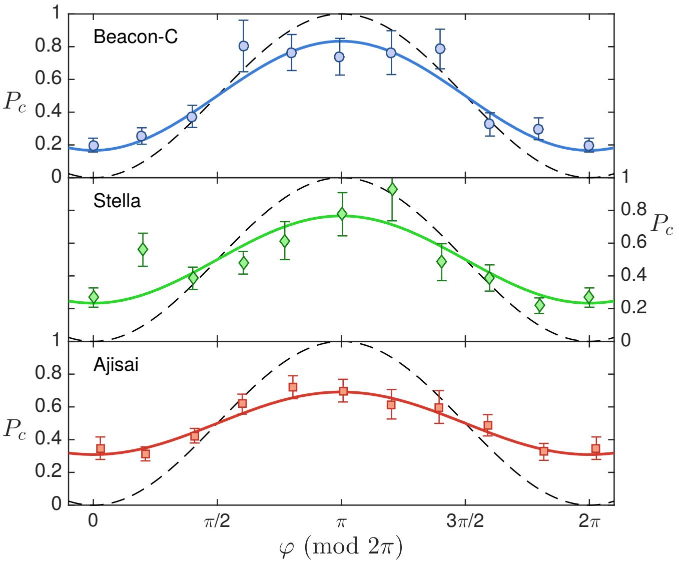

Figure 5.7: Experimental interference pattern. Experimental probabilities $\mathbb{P}_c^{(exp)}$ as a function of the kinematic phase for three different satellites. The curves have been fitted with the formula $\mathbb{P}_c^{(exp)} = \frac{1}{2}\left[1 - \mathcal{V}_{exp}\cos\phi\right]$, obtaining the experimental visibility $\mathcal{V}_{exp} = (67 \pm 11)\%$ for Beacon-C, $\mathcal{V}_{exp} = (53 \pm 13)\%$ for Stella and $\mathcal{V}_{exp} = (38 \pm 4)\%$ for Ajisai. The dashed lines correspond to the theoretical value of $\mathbb{P}_c^{(exp)}$ estimated from (5.16). The points are obtained by splitting the phase into the ten intervals $\mathcal{I}_j \equiv \left[(j - 1/10)\pi, (j + 1/10)\pi\right]$ and summing, for each interval, only the data with $\phi$ (mod $2\pi$) $\in \mathcal{I}_j$. The value of $\mathbb{P}_c^{(exp)}(\phi)$ is obtained by using (5.20). From Vallone *et al.* [134].

# Chapter 6

# Conclusions

This thesis has given an insight on the status of current research in the field of space quantum communication. It has taken into account both the development of techniques and protocols in a laboratory environment and their development for the satellite-ground channel.

The laboratory development and characterization of a high brilliance source of polarization-entangled photons is the starting point for a lot of experiments in the free-space channel, with the expectation of transferring them into the space channel. The narrow bandwidth of the produced photons, moreover, makes it a well suitable choice for those applications where strong filtering is required, as happens when dealing with high noise channel such as daylight free-space operation. The source has already proved to be valid for the implementation of two important experiments in the laboratory, related to Quantum Key Distribution and Bell non-locality, two key aspects of quantum technologies. The Quantum Key Distribution experiment has proved experimentally for the first time a symmetric three-state Quantum Key Distribution protocol, which is well suited for the use in noisy environments where the resources available to the communicating parties are limited, opening the way for its possible technological exploitation. The other laboratory experiment, on the other hand, has proven an important aspect of non-locality in the case of two observers measuring the same photon of a maximally entangled two-photon state.

Regarding the actual development of quantum communication in a space environment, this work describes the new experimental scheme of the ground station for quantum communication at the Matera Laser Ranging Observatory. By combining higher detector sensitivity with stronger background rejection due to improved timing accuracy, this scheme is suitable for the extension of quantum communication towards longer distances, from medium Earth orbit to geostationary Earth orbit satellites, a fundamental step in the development of a world-wide quantum network. This technological advancement has come side-by-side with the experimental study of the satellite-ground channel for the time-bin encoding, a result that, together with the respective study for polarization encoding, opens the space to the implementation of a wide range of quantum communication protocols.

# Appendix A

# Projective measurements in the Bloch sphere

Given an arbitrary qubit $|w\rangle$, the projector onto its eigenspace $|w\rangle\langle w|$ is given by

$$|w\rangle\langle w| = \frac{1}{2}\left[I_2 + \vec{w}\cdot\vec{\sigma}\right], \tag{A.1}$$

where $\vec{w}$ is the representation of $|w\rangle$ in the Bloch sphere and the scalar product $\vec{w}\cdot\vec{\sigma}$ is the two-dimensional matrix $w_x\sigma_x + w_y\sigma_y + w_z\sigma_z$, with $\sigma_i$ the corresponding Pauli matrix. It can be demonstrated that, similarly, the density matrix of a single-qubit state $\rho$ can be written as

$$\rho = \frac{1}{2}\left[I_2 + \vec{r}\cdot\vec{\sigma}\right], \tag{A.2}$$

where $\vec{r}$ is a vector with $|\vec{r}| \leq 1$, with the states on the sphere ($|\vec{r}| = 1$) describing pure states and those inside the sphere ($|\vec{r}| < 1$) mixed states.
When measuring in the $\left\{|w\rangle, |w^{\perp}\rangle\right\}$ basis, with $|w\rangle$ corresponding to outcome 1 and $|w^{\perp}\rangle$ to outcome $-1$, the probability of obtaining 1 is given by

$$\begin{aligned}
\mathbb{P}_1 &= Tr\left[|w\rangle\langle w|\rho\right] &\text{(A.3)}\\
&= \frac{1}{4}Tr\left[\left(I_2 + \vec{w}\cdot\vec{\sigma}\right)\left(I_2 + \vec{r}\cdot\vec{\sigma}\right)\right] &\text{(A.4)}\\
&= \frac{1}{4}Tr\left[I_2 + (w_i + r_i)\sigma_i + w_i r_j \sigma_i\sigma_j\right] &\text{(A.5)}\\
&= \frac{1}{4}\left\{Tr[I_2] + (w_i + r_i)Tr[\sigma_i] + w_i r_j Tr\left[\sigma_i\sigma_j\right]\right\} &\text{(A.6)}\\
&= \frac{1}{4}\left\{2 + 2w_i r_i\right\} &\text{(A.7)}\\
&= \frac{1}{2}\left(1 + \vec{w}\cdot\vec{r}\right), &\text{(A.8)}
\end{aligned}$$

where the Einstein convention of index summation has been adopted and the properties of sigma matrices

$$\begin{aligned}
Tr\left[\sigma_i\right] &= 0, &\text{(A.9)}\\
\sigma_i\sigma_j &= i\varepsilon_{ijk}\sigma_k + \delta_{ij}I_2, &\text{(A.10)}
\end{aligned}$$

have been employed [27].

## A.1 Measurement on the singlet state

The above formalism can be adapted to the single state $|\Psi^-\rangle = \frac{|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B}{\sqrt{2}}$ by noticing that if the measurement on the $A$ photon gives a polarization state $|w\rangle$, the $B$ photon is projected onto $|w^\perp\rangle$. If Alice measures in the $\left\{|x\rangle\,, |x^\perp\rangle\right\}$ basis and Bob in the $\left\{|y\rangle\,, |y^\perp\rangle\right\}$ basis, with the first vector corresponding to outcome $+1$ and the second one to outcome $-1$, the joint probability distribution is

$$\begin{aligned}\mathbb{P}(ab|xy) &= \mathbb{P}(b|axy)\mathbb{P}(a|xy) && \text{(A.11)}\\ &= \frac{1}{2}\left(1 - ab\vec{x}\cdot\vec{y}\right)\cdot\mathbb{P}(a|xy) && \text{(A.12)}\\ &= \frac{1}{4}\left(1 - ab\vec{x}\cdot\vec{y}\right), && \text{(A.13)}\end{aligned}$$

where $\mathbb{P}(a|xy) = \frac{1}{2}$ comes from the properties of the $|\Psi^-\rangle$ state. The explicit expression of these probabilities is

$$\begin{aligned}\mathbb{P}(-1,-1|xy) = \mathbb{P}(1,1|xy) &= \frac{1}{4}\left(1 - \vec{x}\cdot\vec{y}\right), && \text{(A.14)}\\ \mathbb{P}(-1,1|xy) = \mathbb{P}(1,-1|xy) &= \frac{1}{4}\left(1 + \vec{x}\cdot\vec{y}\right), && \text{(A.15)}\end{aligned}$$

from which the expectation value

$$\left\langle a_x b_y\right\rangle = \sum_{a,b} ab\mathbb{P}(ab|xy) = -\vec{x}\cdot\vec{y} \tag{A.16}$$

is easily calculated.

# Appendix B

# Parameter estimation in passive decoy state QKD

The parameters $Y_0$, $Y_1$ and $e_1$, necessary in post-processing, are not directly measured during the key exchange session, but must be estimated from the experimental data $Q$ and $E$. If Alice registers, for each pulse, whether at least one or no detector has clicked, a different gain and QBER for each case can be measured and these can be used for parameter estimation. The probability that no detector clicks in a pulse is

$$\mathbb{P}^{(nc)}(\mu; m, \eta, \gamma) = e^{-\mu\eta\frac{2^k}{\gamma^k}} \tag{B.1}$$

for the SMHPS and

$$\mathbb{P}^{(nc)}(\mu; m, \eta, \gamma) = e^{-\mu\eta\frac{(2-\gamma)\gamma^{1-m}-1}{1-\gamma}} \tag{B.2}$$

for the AMHPS, where $k = \log_2 m$. The statistics in the case of no click is the same for both sources (in both cases the first HS unit is routed to the output) and is

$$\mathbb{P}^{(nc)}(n) = \frac{[\mu(1-\eta)]^n}{n!} e^{-\mu(1-\eta)}, \tag{B.3}$$

while the statistics for the case of at least a detector click is

$$\mathbb{P}^{(c)}(n) = \frac{\mu^n e^{-\mu}}{n!} \left[ 1 - (1-\eta)^n e^{-\eta\mu\left(\frac{1}{\gamma^k}-1\right)} \right] \frac{1}{1 - e^{\frac{-\mu\eta}{\gamma^k}}} \tag{B.4}$$

for the SMHPS and

$$\mathbb{P}^{(c)}(n) = \frac{\mu^n e^{-\mu}}{n!} \sum_{i=1}^{m} \left[ 1 - (1-\eta)^n e^{-\mu\eta\left(\frac{1}{\gamma^{k_i}}-1\right)} \right] \frac{e^{-\mu\eta\frac{\gamma^{1-i}-1}{1-\gamma}}}{1 - e^{-\mu\eta\frac{(2-\gamma)\gamma^{1-m}-1}{1-\gamma}}} \tag{B.5}$$

for the AMHPS [67].

After the key exchange session, Alice tells Bob for which pulses at least one detector has clicked, so that they can estimate the gain and the QBER separately for the two cases. From these values, referenced to as $\{Q^c, E^c, Q^{nc}, E^{nc}\}$, and the known source statistics $\mathbb{P}^{(c)}(n)$ and $\mathbb{P}^{(nc)}(n)$, they can estimate the parameters of the channel using the method described in [89].

The first parameter to be estimated is $Y_0$. Its upper bound $Y_0^U$ can be calculated starting from the relations

$$Q^c E^c = \sum_{n=0}^{\infty} \mathbb{P}^{(c)}(n) Y_n e_n \geq \mathbb{P}^{(c)}(0) Y_0 e_0 \tag{B.6}$$

$$Q^{nc} E^{nc} = \sum_{n=0}^{\infty} \mathbb{P}^{(nc)}(n) Y_n e_n \geq \mathbb{P}^{(nc)}(0) Y_0 e_0. \tag{B.7}$$

Since both inequalities must hold, the parameter $Y_0$ is upper bounded by

$$Y_0 \leq Y_0^U = \min \left\{ \frac{Q^c E^c}{P_0^{(c)} e_0}, \frac{Q^{nc} E^{nc}}{P_0^{(nc)} e_0} \right\}. \tag{B.8}$$

Its lower bound $Y_0^L$ can be calculated from

$$\begin{aligned} \mathbb{P}^{(c)}(1) Q^{nc} - \mathbb{P}^{(nc)}(1) Q^c &= \sum_{n=0}^{\infty} (\mathbb{P}^{(c)}(1) \mathbb{P}^{(nc)}(n) - \mathbb{P}^{(nc)}(1) \mathbb{P}^{(c)}(n)) Y_n \\ &\leq (\mathbb{P}^{(c)}(1) \mathbb{P}^{(nc)}(0) - \mathbb{P}^{(nc)}(1) \mathbb{P}^{(c)}(0)) Y_0, \end{aligned} \tag{B.9}$$

that gives

$$Y_0 \geq Y_0^L = \max \left\{ \frac{\mathbb{P}^{(c)}(1) Q^{nc} - \mathbb{P}^{(nc)}(1) Q^c}{\mathbb{P}^{(c)}(1) \mathbb{P}^{(nc)}(0) - \mathbb{P}^{(nc)}(1) \mathbb{P}^{(c)}(0)}, 0 \right\}, \tag{B.10}$$

since, for both the SMHPS and the AMHPS

$$\mathbb{P}^{(c)}(1) \mathbb{P}^{(nc)}(n) - \mathbb{P}^{(nc)}(1) \mathbb{P}^{(c)}(n) = A_{n,1} [(1-\eta)^n - (1-\eta)] \left\{ \begin{array}{ll} \leq 0 & \text{for } n \geq 2 \\ \geq 0 & \text{for } n = 0, \end{array} \right. \tag{B.11}$$

with $A_{n,1}$ a positive constant.

The lower bound on the single photon yield $Y_0$ is calculated starting from

$$\begin{aligned} \mathbb{P}^{(c)}(2) Q^{nc} - \mathbb{P}^{(nc)}(2) Q^c &= \sum_{n=0}^{\infty} (\mathbb{P}^{(c)}(2) \mathbb{P}^{(nc)}(n) - \mathbb{P}^{(nc)}(2) \mathbb{P}^{(c)}(n)) Y_n \\ &\leq \sum_{n=0}^{1} (\mathbb{P}^{(c)}(2) \mathbb{P}^{(nc)}(n) - \mathbb{P}^{(nc)}(2) \mathbb{P}^{(c)}(n)) Y_n, \end{aligned} \tag{B.12}$$

which leads to

$$\begin{aligned} & Y_1 \geq Y_1^L = \\ & \max \left\{ \frac{\mathbb{P}^{(c)}(2) Q^{nc} - \mathbb{P}^{(nc)}(2) Q^c - (\mathbb{P}^{(c)}(2) \mathbb{P}^{(nc)}(0) - \mathbb{P}^{(nc)}(2) \mathbb{P}^{(c)}(0)) Y_0^U}{\mathbb{P}^{(c)}(2) \mathbb{P}^{(nc)}(1) - \mathbb{P}^{(nc)}(2) \mathbb{P}^{(c)}(1)}, 0 \right\}, \end{aligned} \tag{B.13}$$

since

$$\mathbb{P}^{(c)}(2) \mathbb{P}^{(nc)}(n) - \mathbb{P}^{(nc)}(2) \mathbb{P}^{(c)}(n) = A_{n,2} [(1-\eta)^n - (1-\eta)^2] \left\{ \begin{array}{ll} \leq 0 & \text{for } n \geq 2 \\ \geq 0 & \text{for } n \leq 1 \end{array} \right. \tag{B.14}$$

with $A_{n,2}$ positive.

Similarly, the upper bound on $e_1$ is calculated from

$$\begin{aligned}\mathbb{P}^{(nc)}(0)Q^cE^c - \mathbb{P}^{(c)}(0)Q^{nc}E^{nc} = \\ &\sum_{n=0}^{\infty}(\mathbb{P}^{(nc)}(0)\mathbb{P}^{(c)}(n) - \mathbb{P}^{(c)}(0)\mathbb{P}^{(nc)}(n))e_nY_n \\ &\geq (\mathbb{P}^{(nc)}(0)\mathbb{P}^{(c)}(1) - \mathbb{P}^{(c)}(0)\mathbb{P}^{(nc)}(1))e_1Y_1, \quad \text{(B.15)}\end{aligned}$$

since

$$\mathbb{P}^{(nc)}(0)\mathbb{P}^{(c)}(n) - \mathbb{P}^{(c)}(0)\mathbb{P}^{(nc)}(n) = A_{n,0}[1-(1-\eta)^n] \geq 0 \tag{B.16}$$

for all $n$, and

$$Q^cE^c = \sum_{n=0}^{\infty}\mathbb{P}^{(c)}(n)Y_ne_n \geq \mathbb{P}^{(c)}(0)Y_0e_0 + \mathbb{P}^{(c)}(1)Y_1e_1, \tag{B.17}$$

$$Q^{nc}E^{nc} = \sum_{n=0}^{\infty}\mathbb{P}^{(nc)}(n)Y_ne_n \geq \mathbb{P}^{(nc)}(0)Y_0e_0 + \mathbb{P}^{(nc)}(1)Y_1e_1, \tag{B.18}$$

thus obtaining

$$\begin{aligned}e_1 \leq e_1^U = \min\Bigg\{ &\frac{\mathbb{P}^{(nc)}(0)Q^cE^c - \mathbb{P}^{(c)}(0)Q^{nc}E^{nc}}{(\mathbb{P}^{(nc)}(0)\mathbb{P}^{(c)}(1) - \mathbb{P}^{(c)}(0)\mathbb{P}^{(nc)}(1))Y_1^L}, \\ &\frac{Q^cE^c - \mathbb{P}^{(c)}(0)Y_0^Le_0}{\mathbb{P}^{(c)}(1)Y_1^L}, \frac{Q^{nc}E^{nc} - \mathbb{P}^{(nc)}(0)Y_0^Le_0}{\mathbb{P}^{(nc)}(1)Y_1^L}\Bigg\}. \quad \text{(B.19)}\end{aligned}$$

# Bibliography

[1]C. E. Shannon, "A mathematical theory of communication", Bell Syst. Tech. J. **27**, 379–423 (1948).

[2]R. Landauer, "Information is physical", Phys. Today **44**, 23–29 (1976).

[3]J. Preskill, "Lecture Notes for Physics 219 : Quantum Computation", (2004).

[4]J. M. Renes, *Quantum information theory*, Lecture notes, 2015.

[5]G. Jaeger, *Quantum information: An overview* (Springer-Verlag, New York, 2006).

[6]P. Kok and B. W. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, 2010).

[7]M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).

[8]M. G. A. Paris, *Lecture 02: Generalized measurements and the Naimark Theorem*, 2009.

[9]J. Watrous, "An introduction to quantum information and quantum circuits", ACM SIGACT News **42**, 52–67 (2011).

[10]R. Loudon, *The Quantum Theory of Light* (Oxford University Press, Oxford, 2000).

[11]U. Leonhardt, *Essential Quantum Optics* (Cambridge University Press, Cambridge, 2010).

[12]L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, 1995).

[13]F Mandl and G Shaw, *Quantum Field Theory* (Wiley, 2010).

[14]P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits", Rev. Mod. Phys. **79**, 135–174 (2007).

[15]J. Skaar, J. C. Garca Escartn, and H. Landro, "Quantum mechanical description of linear optics", Am. J. Phys. **72**, 1385 (2004).

[16]S. L. Braunstein and P. van Loock, "Quantum information with continuous variables", Rev. Mod. Phys. **77**, 513–577 (2005).

[17]B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics , 2nd Edition* (Wiley, 2007).

[18]C. C. Gerry, P. L. Knight, and M. Beck, "Introductory Quantum Optics.", Am. J. Phys. **73**, 1197 (2005).

[19]P. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. Sergienko, and Y. Shih, "New High-Intensity Source of Polarization-Entangled Photon Pairs", Phys. Rev. Lett. **75**, 4337–4341 (1995).

[20] F. Steinlechner, P. Trojek, M. Jofre, H. Weier, D. Perez, T. Jennewein, R. Ursin, J. Rarity, M. W. Mitchell, J. P. Torres, H. Weinfurter, and V. Pruneri, “A high-brightness source of polarization-entangled photons optimized for applications in free space”, Opt. Express **20**, 9640 (2012).

[21] T. Kim, M. Fiorentino, and F. N. C. Wong, “Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer”, Phys. Rev. A **73**, 012316 (2006).

[22] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, “A wavelength-tunable fiber-coupled source of narrowband entangled photons”, Opt. Express **15**, 15377 (2007).

[23] R. W. Boyd, *Nonlinear Optics* (Academic Press, 2008).

[24] Y. R. Shen, *Principles of Nonlinear Optics* (Wiley-Interscience, 2002).

[25] J. D. Jackson, *Classical Electrodynamics Third Edition* (John Wiley Sons, INC., 1999).

[26] A Christ, “Theory of ultrafast waveguided parametric down-conversion: from fundamentals to applications”, PhD thesis (University of Paderborn, 2013).

[27] M. E. Peskin and D. V. Schroeder, *An Introduction To Quantum Field Theory* (Addison-Wesley Pub. Co, 1995).

[28] R. S. Bennink, “Optimal collinear Gaussian beams for spontaneous parametric down-conversion”, Phys. Rev. A **81**, 053805 (2010).

[29] P. Kolenderski, W. Wasilewski, and K. Banaszek, “Modeling and optimization of photon pair sources based on spontaneous parametric down-conversion”, Phys. Rev. A **80**, 013811 (2009).

[30] A. Ling, A. Lamas-Linares, and C. Kurtsiefer, “Absolute emission rates of spontaneous parametric down-conversion into single transverse Gaussian modes”, Phys. Rev. A **77**, 043834 (2008).

[31] D. Ljunggren and M. Tengner, “Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers”, Phys. Rev. A **72**, 062301 (2005).

[32] M. Mitchell, “Parametric down-conversion from a wave-equation approach: Geometry and absolute brightness”, Phys. Rev. A **79**, 043835 (2009).

[33] A. Franzen, *ComponentLibrary*, (2006) `http://www.gwoptics.org/ComponentLibrary/`.

[34] C. Commons, *Attribution-NonCommercial 3.0 Unported*, `https://creativecommons.org/licenses/by-nc/3.0/legalcode`.

[35] Ondax, *LM Series Compact Single Frequency Laser Modules Specifications*, (2014) `http://ondax.com/wp-content/uploads/2014/09/SureLock_LM_Series_830_150-Sept-2014.pdf`.

[36] A. E. Siegman, “How to (Maybe) Measure Laser Beam Quality”, in Dpss (diode pumped solid state) lasers appl. issues, Vol. 17, October 1997 (1998), MQ1.

[37] M. Fox, “Quantum Optics: An Introduction”, Quantum Opt. **67**, 441 (2006).

[38] D. R. Blandford and K. S. Thorne, *Applications of Classical Physics* (CalTech, 2013).

[39] F. Just, “A highly non-degenerate PDC source for QKD with passive decoy selection”, MA thesis (University Erlangen-Nurnberg, 2009), p. 72.

[40] S. Emanueli and A. Arie, “Temperature-dependent dispersion equations for KTiOPO4 and KTiOAsO4.”, Appl. Opt. **42**, 6661–6665 (2003).

[41] R. H. Brown and R. Q. Twiss, “Correlation between Photons in two Coherent Beams of Light”, Nature **177**, 27–29 (1956).

[42] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, “Measurement of qubits”, Phys. Rev. A **64**, 052312 (2001).

[43] J. Volz, C. Kurtsiefer, and H. Weinfurter, “Compact all-solid-state source of polarization-entangled photon pairs”, Appl. Phys. Lett. **79**, 869–871 (2001).

[44] P. H. Shun, “Towards a High Quality Polarization-Entangled Multi-Photon Source”, MA thesis (National University of Singapore, 2009), p. 96.

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

[46] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons”, Phys. Rev. Lett. **115**, 250401 (2015).

[47] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, “Strong Loophole-Free Test of Local Realism”, Phys. Rev. Lett. **115**, 250402 (2015).

[48] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Vol. 1 (Scribner, 1996), p. 1200.

[49] P. Shor, “Algorithms for quantum computation: discrete logarithms and factoring”, in Proc. 35th annu. symp. found. comput. sci. (1994), pp. 124–134.

[50] U. Maurer and R. Renner, “Abstract Cryptography”, Second Symp. Innov. Comput. Sci. ICS 2011, 1–21 (2011).

[51] C. Portmann and R. Renner, “Cryptographic security of quantum key distribution”, arXiv:1409.3525 (2014).

[52] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution”, Rev. Mod. Phys. **81**, 1301–1350 (2009).

[53] M. Canale, “Classical processing algorithms for Quantum Information Security”, PhD thesis (University of Padova, 2014), p. 142.

[54] C. Sparaciari and M. G. A. Paris, “Probing qubit by qubit: Properties of the POVM and the information/disturbance tradeoff”, Int. J. Quantum Inf. **12**, 1461012 (2014).

[55] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned”, Nature **299**, 802–803 (1982).

[56] D. Bacco, “Quantum Communications Between Earth and Space”, PhD thesis (University of Padova, 2015), p. 161.

[57]U. M. Maurer, “Protocols for Secret Key Agreement by Public Discussion Based on Common Information”, in *Adv. cryptol. crypto' 92*, Vol. 740, 3 (Springer Berlin Heidelberg, Berlin, Heidelberg, 1993), pp. 461–470.

[58]R. König, R. Renner, A. Bariska, and U. Maurer, “Small Accessible Quantum Information Does Not Imply Security”, Phys. Rev. Lett. **98**, 140502 (2007).

[59]R. Renner, “Security of Quantum Key Distribution”, Int. J. Quantum Inf. **06**, 1–127 (2008).

[60]R. Renner and R. Koenig, “Universally composable privacy amplification against quantum adversaries”, in Theory cryptogr. 20 (2004), pp. 407–425.

[61]V. Scarani and C. Kurtsiefer, “The black paper of quantum cryptography: Real implementation problems”, Theor. Comput. Sci. **560**, 27–32 (2014).

[62]G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, “Limitations on practical quantum cryptography”, Phys. Rev. Lett. **85**, 1330–1333 (2000).

[63]D. Gottesman, Hoi-Kwong Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices”, in Int. symp. oninformation theory, 2004. isit 2004. proceedings. (2004), pp. 135–135.

[64]W.-Y. Hwang, “Quantum Key Distribution with High Loss: Toward Global Secure Communication”, Phys. Rev. Lett. **91**, 057901 (2003).

[65]H.-k. Lo, X. Ma, and K. Chen, “Decoy State Quantum Key Distribution”, Phys. Rev. Lett. **94**, 230504 (2005).

[66]X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution”, Phys. Rev. A **72**, 012326 (2005).

[67]L. Mazzarella, F. Ticozzi, A. V. Sergienko, G. Vallone, and P. Villoresi, “Asymmetric architecture for heralded single-photon sources”, Phys. Rev. A **88**, 023848 (2013).

[68]N. J. Beaudry, T. Moroder, and N. Lütkenhaus, “Squashing Models for Optical Measurements in Quantum Communication”, Phys. Rev. Lett. **101**, 093601 (2008).

[69]C.-H. F. Fung, H. F. Chau, and H.-K. Lo, “Universal squash model for optical communications using linear optics and threshold detectors”, Phys. Rev. A **84**, 020303 (2011).

[70]O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, “Squashing model for detectors and applications to quantum-key-distribution protocols”, Phys. Rev. A **89**, 012325 (2014).

[71]L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination”, Nat. Photonics **4**, 686–689 (2010).

[72]I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system.”, Nat. Commun. **2**, 349 (2011).

[73]I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, “Experimentally faking the violation of Bell's inequalities”, Phys. Rev. Lett. **107**, 170404 (2011).

[74]A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, “Laser damage helps the eavesdropper in quantum cryptography”, Phys. Rev. Lett. **112**, 070503 (2014).

[75]C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?", J. Mod. Opt. **48**, 2039–2047 (2001).

[76]A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel", Opt. Express **15**, 9388 (2007).

[77]Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems", Phys. Rev. A **78**, 042333 (2008).

[78]I Aharonovich, S Castelletto, D. a. Simpson, C.-H. Su, a. D. Greentree, and S Prawer, "Diamond-based single-photon emitters", Reports Prog. Phys. **74**, 076501 (2011).

[79]M. Pelton, C. Santori, J. Vucković, B. Zhang, G. S. Solomon, J. Plant, and Y. Yamamoto, "Efficient Source of Single Photons: A Single Quantum Dot in a Micropost Microcavity", Phys. Rev. Lett. **89**, 233602 (2002).

[80]A. Jamil, J. Skiba-Szymanska, S. Kalliakos, A. Schwagmann, M. B. Ward, Y. Brody, D. J. P. Ellis, I. Farrer, J. P. Griffiths, G. a. C. Jones, D. a. Ritchie, and A. J. Shields, "On-chip generation and guiding of quantum light from a site-controlled quantum dot", Appl. Phys. Lett. **104** (2014).

[81]J McKeever, a Boca, a. D. Boozer, R Miller, J. R. Buck, a Kuzmich, and H. J. Kimble, "Deterministic generation of single photons from one atom trapped in a cavity.", Science **303**, 1992–1994 (2004).

[82]M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, "Continuous generation of single photons with controlled waveform in an ion-trap cavity system", Nature **431**, 1075–1078 (2004).

[83]J. H. Shapiro and F. N. Wong, "On-demand single-photon generation using a modular array of parametric downconverters with electro-optic polarization controls.", Opt. Lett. **32**, 2698–2700 (2007).

[84]M. Lasota, R. Demkowicz-Dobrzański, and K. Banaszek, "Quantum Key Distribution with realistic Heralded Single-photon Sources", Int. J. Quantum Inf. **11**, 1350034 (2013).

[85]A. L. Migdall, D. Branning, S. Castelletto, and M. Ware, "Tailoring Single and Multiphoton Probabilities of a Single Photon On-Demand Source", Phys. Rev. A **66**, 053805 (2002).

[86]M. Schiavon, G. Vallone, F. Ticozzi, and P. Villoresi, "Heralded single-photon sources for quantum-key-distribution applications", Phys. Rev. A **93**, 012331 (2016).

[87]C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in Proc. int. conf. comput. syst. signal process. (1984), pp. 175–179.

[88]Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, "Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion", Phys. Rev. Lett. **99**, 180503 (2007).

[89]M. Curty, T. Moroder, X. Ma, and N. Lütkenhaus, "Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution", Opt. Lett. **34**, 3238 (2009).

[90]M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight Finite-Key Analysis for Quantum Cryptography", Nat. Commun. **3**, 11 (2011).

[91]H.-K. Lo, "Getting Something Out of Nothing", Quantum Inf. Comput. **5**, 413–418 (2005).

[92] IdQuantique, *Infrared single-photon counter*, (2015) `http://www.idquantique.com/wordpress/wp-content/uploads/id230-specs.pdf`.

[93] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the Information Reconciliation Protocol Cascade", Quantum Inf. Comput. **15**, 453–477 (2015).

[94] E. Waks, C. Santori, and Y. Yamamoto, "Security aspects of quantum key distribution with sub-Poisson light", Phys. Rev. A **66**, 042315 (2002).

[95] C. Bennett, "Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett. **68**, 3121–3124 (1992).

[96] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States", Phys. Rev. Lett. **90**, 167904 (2003).

[97] K. Tamaki and N. Lütkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel", Phys. Rev. A **69**, 032316 (2004).

[98] C. H. F. Fung and H. K. Lo, "Security proof of a three-state quantum-key-distribution protocol without rotational symmetry", Phys. Rev. A **74**, 042342 (2006).

[99] M. Lucamarini, G. Di Giuseppe, and K. Tamaki, "Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states", Phys. Rev. A **80**, 032327 (2009).

[100] S. J. D. Phoenix, S. M. Barnett, and A. Chefles, "Three-state quantum cryptography", J. Mod. Opt. **47**, 507–516 (2000).

[101] J. M. Renes, "Spherical-code key-distribution protocols for qubits", Phys. Rev. A **70**, 052314 (2004).

[102] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. Renes, "Unconditional Security of a Three State Quantum Key Distribution Protocol", Phys. Rev. Lett. **94**, 040503 (2005).

[103] M. Mafu, K. Garapo, and F. Petruccione, "Finite-key-size security of the Phoenix-Barnett-Chefles 2000 quantum-key-distribution protocol", Phys. Rev. A **90**, 032308 (2014).

[104] M. Schiavon, G. Vallone, and P. Villoresi, "Experimental realization of equiangular three-state quantum key distribution", Sci. Rep. **6**, 30089 (2016).

[105] W. Hoeffding, "Probability Inequalities for Sums of Bounded Random Variables", J. Am. Stat. Assoc. **58**, 13–30 (1963).

[106] J. Carter and M. N. Wegman, "Universal classes of hash functions", J. Comput. Syst. Sci. **18**, 143–154 (1979).

[107] R. Renner and S. Wolf, "Simple and Tight Bounds for Information Reconciliation and Privacy Amplification", in *Lect. notes comput. sci. (including subser. lect. notes artif. intell. lect. notes bioinformatics)*, Vol. 3788 LNCS (2005), pp. 199–216.

[108] V. Scarani and R. Renner, "Security bounds for quantum cryptography with finite resources", Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) **5106 LNCS**, 83–95 (2008).

[109] M. Christandl, R. König, and R. Renner, "Postselection Technique for Quantum Channels with Applications to Quantum Cryptography", Phys. Rev. Lett. **102**, 020504 (2009).

[110] R. B. M. Clarke, A. Chefles, S. M. Barnett, and E. Riis, "Experimental demonstration of optimal unambiguous state discrimination", Phys. Rev. A **63**, 040305 (2001).

[111] R. Clarke, V. Kendon, A. Chefles, S. Barnett, E. Riis, and M. Sasaki, "Experimental realization of optimal detection strategies for overcomplete states", Phys. Rev. A **64**, 012303 (2001).

[112] D. J. Saunders, M. S. Palsson, G. J. Pryde, A. J. Scott, S. M. Barnett, and H. M. Wiseman, "The simplest demonstrations of quantum nonlocality", New J. Phys. **14**, 113020 (2012).

[113] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, "Quantum randomness certified by the uncertainty principle", Phys. Rev. A **90**, 052327 (2014).

[114] Excelitas, *SPCM-AQRH Single Photon Counting Module*, (2016) `http://www.excelitas.com/Downloads/DTS_SPCM-AQRH.pdf`.

[115] M. Schiavon, L. Calderaro, M. Pittaluga, G. Vallone, and P. Villoresi, "Three-observer Bell inequality violation on a two-qubit entangled state", arXiv:1611.02430 (2016).

[116] A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?", Phys. Rev. **47**, 777–780 (1935).

[117] J. S. Bell, "On the Einstein Podolsky Rosen paradox", Physics (College. Park. Md). **1**, 195–200 (1964).

[118] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, "Bell nonlocality", Rev. Mod. Phys. **86**, 419–478 (2014).

[119] D. Bohm, "A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I", Phys. Rev. **85**, 166–179 (1952).

[120] S. J. Freedman and J. F. Clauser, "Experimental Test of Local Hidden-Variables Theories", Phys. Rev. Lett. **28**, 938 (1972).

[121] B. Toner, "Monogamy of nonlocal quantum correlations", Proc. R. Soc. A Math. Phys. Eng. Sci. **465**, 59–69 (2009).

[122] R. Silva, N. Gisin, Y. Guryanova, and S. Popescu, "Multiple Observers Can Share the Nonlocality of Half of an Entangled Pair by Using Optimal Weak Measurements", Phys. Rev. Lett. **114**, 250401 (2015).

[123] S. Mal, A. Majumdar, and D. Home, "Sharing of Nonlocality of a Single Member of an Entangled Pair of Qubits Is Not Possible by More than Two Unbiased Observers on the Other Wing", Mathematics **4**, 48 (2016).

[124] P. Shi, S.-C. Zhao, Y.-J. Gu, and W.-D. Li, "Channel analysis for single photon underwater free space quantum key distribution", J. Opt. Soc. Am. A **32**, 349 (2015).

[125] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber", Phys. Rev. Lett. **117**, 190501 (2016).

[126] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, "Quantum cryptography for secure free-space communications", in Proc. spie 3615, free-space laser communication technologies xi, edited by G. S. Mecherle (1999), pp. 98–103.

[127]C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication", Phys. Rev. Lett. **94**, 150501 (2005).

[128]H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger, "High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber.", Optics express **15**, 7853–7862 (2007).

[129]A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel", Nat. Phys. **5**, 389–392 (2009).

[130]X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward.", Nature **489**, 269–273 (2012).

[131]G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, and P. Villoresi, "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels", Phys. Rev. A **91**, 042320 (2015).

[132]P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, "Experimental verification of the feasibility of a quantum channel between space and Earth", New J. Phys. **10**, 033038 (2008).

[133]G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental Satellite Quantum Communications", Phys. Rev. Lett. **115**, 040502 (2015).

[134]G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, and P. Villoresi, "Interference at the Single Photon Level Along Satellite-Ground Channels", Phys. Rev. Lett. **116**, 253601 (2016).

[135]J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein, "Free-space quantum key distribution to a moving receiver", Opt. Express **23**, 33437 (2015).

[136]S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication", Nat. Photonics **7**, 382–386 (2013).

[137]J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan, "Direct and full-scale experimental verifications towards groundsatellite quantum key distribution", Nat. Photonics **7**, 387–393 (2013).

[138]A. Carrasco-Casado, H. Kunimori, H. Takenaka, T. Kubo-Oka, M. Akioka, T. Fuse, Y. Koyama, D. Kolev, Y. Munemasa, and M. Toyoshima, "LEO-to-ground polarization measurements aiming for space QKD using Small Optical TrAnsponder (SOTA)", Opt. Express **24**, 12254 (2016).

[139]J.-w. Pan, "Quantum Science Satellite", Chin. J. Sp. Sci. **34**, 547–549 (2014).

[140]Z. Tang, R. Chandrasekara, Y. C. Tan, C. Cheng, L. Sha, G. C. Hiang, D. K. L. Oi, and A. Ling, "Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite", Phys. Rev. Appl. **5**, 054022 (2016).

[141]ILRS, *International Laser Ranging Service*, (2016) `http://ilrs.gsfc.nasa.gov/index.html`.

[142]W. Gurtner, R. Noomen, and M. R. Pearlman, "The international laser ranging service: Current status and future developments", Adv. Sp. Res. **36**, 327–332 (2005).

[143]I. Ciufolini, A. Paolozzi, E. C. Pavlis, R. Koenig, J. Ries, V. Gurzadyan, R. Matzner, R. Penrose, G. Sindoni, C. Paris, H. Khachatryan, and S. Mirzoyan, "A test of general relativity using the LARES and LAGEOS satellites and a GRACE Earth gravity model: Measurement of Earth's dragging of inertial frames", Eur. Phys. J. C **76**, 120 (2016).

[144]T. Varghese, W. Decker, H. Crooks, G. Bianco, and T. Spaziale, "Matera Laser Ranging Observatory (MLRO): an overview", 1994.

[145]D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental single-photon exchange along a space link of 7000 km", Phys. Rev. A **93**, 010301 (2016).

[146]A. Giudice, M. Ghioni, R. Biasi, F. Zappa, S. Cova, P. Maccagnani, and A. Gulinatti, "High-rate photon counting and picosecond timing with silicon-SPAD based compact detector modules", J. Mod. Opt. **54**, 225–237 (2007).

[147]Qutools, "quTAG", (2016).

[148]G. Vallone, D. Dequal, M Tomasin, M Schiavon, F Vedovato, D. Bacco, S. Gaiarin, G. Bianco, V. Luceri, and P. Villoresi, "Satellite quantum communication towards GEO distances", in Proc. spie 9900, quantum optics (2016), 99000J.

[149]G. Bianco, M. Chersich, R. Devoti, V. Luceri, and M. Selden, "Measurement of LAGEOS-2 rotation by satellite laser ranging observations", Geophys. Res. Lett. **28**, 2113–2116 (2001).

[150]R. L. Ricklefs, *Consolidated Laser Ranging Prediction Format*, (2006) `http://ilrs.gsfc.nasa.gov/docs/2006/cpf_1.01.pdf`.

[151]V Glotov, N Abylchatova, V Mitrikas, and M Zinkovsky, "MCC analysis procedure of the SLR data quality and stations performance", in 14th int. work. laser ranging (Russian Mission Control Center, Central Research Institute of Machine Building, Russian Space Agency, 2004).

[152]A Muller, T Herzog, B Huttner, W Tittel, H Zbinden, and N Gisin, "Plug and play" systems for quantum cryptography", Appl. Phys. Lett. **70**, 793–795 (1997).

[153]G Ribordy and N Gisin, "Automated 'plug & play' quantum key distribution", Electronics Letters **34**, 2116–2117 (1998).