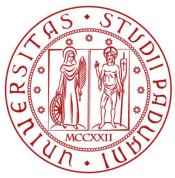


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Sede Amministrativa: Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione (DEI)

SCUOLA DI DOTTORATO DI RICERCA IN: Ingegneria dell'Informazione
INDIRIZZO: Scienza e Tecnologia dell'Informazione (I.C.T.)
CICLO XXVI

ADVANCED TECHNIQUES FOR QUANTUM COMMUNICATIONS IN FREE-SPACE CHANNELS

Direttore della Scuola: Ch.mo Prof. Matteo Bertocco
Coordinatore d'indirizzo: Ch.mo Prof. Carlo Ferrari
Supervisore: Ch.mo Prof. Paolo Villoresi

Dottorando: Alberto Dall'Arche

To my wife

Contents

Abstract

This thesis is focused on the development of advanced techniques for quantum communications in free-space channels.

At present there are several demonstrations of quantum communication protocols at long distances, many of these exploit optical fiber as transmission channel. The optical fiber is very advantageous in that it is scarcely influenced by external conditions and allows to connect remote localities that are not in direct line of sight. On the other hand, it presents strong limitations in transmission distance because of dispersion and attenuation.

It is therefore necessary to explore new transmission channels in order to allow a global spread of quantum communication. The free-space channels are good candidates, both the vertical ones (between earth and space) and the horizontal ones. The study of these is of fundamental importance for the extension of quantum communication over a global scale.

Since the eighties to present day have been defined several quantum communication protocols such as Bennet-Brassard 84 [1] (BB84) , Bennet 92 [2] (B92), Ekert 91 [3], Decoy State [4], Dense Coding [5], etc.. These protocols present different characteristic such as reliability, security and key rate. These three parameters are very important for the characterization of a communication protocol and are directly related to each other. The development of new quantum communication (QC) protocols that maximize these parameters is very important for future progress of quantum communications.

This thesis is divided into three parts. In the first part we consider the characteristics and the behaviour of a free-space horizontal quantum channel. We study the impact of atmospheric turbulence in the case of single beam propagation and

twin-beam propagation. We then measure the losses of the channel and analyze the effect of turbulence on photon statistics. Finally, we propose a method that exploits the turbulence to improve the signal to noise ratio (SNR) of the channel.

In the second part we take into consideration the security and efficiency of Quantum Key Distribution (QKD) protocols . We propose the experimental demonstration of the B92 protocol with non-maximally entangled states . Using this kind of states allow us to improve the security and the key rate of this protocol.

Finally, in the last part, we presented a possible way to improve the quantum channel capacity exploiting hyperentangled photon pairs. We designed and experimentally tested a system that can be used to transmit hyperentangled states at long distances.

Sommario

Questa tesi è incentrata sullo sviluppo di tecniche avanzate per le comunicazioni quantistiche in canali nello spazio libero.

Al stato attuale esistono diverse dimostrazioni di protocolli di comunicazione quantistica a lunga distanza, molte di queste sfruttano le fibre ottiche come canale di trasmissione. Le fibre ottiche sono molto vantaggiose in quanto sono scarsamente influenzate da condizioni esterne e permettono di collegare località remote che non sono in linea visiva diretta. Per contro, presentano forte limitazioni nella distanza di trasmissione in quanto hanno problemi di dispersione e di attenuazione.

Per permettere una diffusione globale delle comunicazioni quantistiche è necessario esplorare nuovi canali di trasmissione. Lo spazio libero è un buon candidato, sia per quanto riguarda i canali verticali tra la terra e lo spazio, sia per quanto riguarda i collegamenti orizzontali. Lo studio di questi è quindi di fondamentale importanza per l'estensione delle comunicazioni quantistiche su larga scala.

Dagli anni ottanta a oggi sono stati definiti molti protocolli di comunicazione quantistica come Bennet-Brassard 84 [1] (BB84) , Bennet 92 [2] (B92), Ekert 91 [3], Decoy State [4], Dense Coding [5], ecc. Questi protocolli si distinguono tra loro per affidabilità, sicurezza e capacità di trasmissione. Questi tre parametri sono molto importanti nella caratterizzazione di un protocollo di comunicazione e hanno la particolarità di essere direttamente legati uno all'altro. Lo sviluppo di nuovi protocolli che massimizzino questi parametri è molto importante per l'avanzamento e lo sviluppo futuro delle comunicazioni quantistiche.

Questa tesi è divisa in tre parti. Nella prima parte sono state considerate le caratteristiche e il comportamento di un canale quantistico orizzontale nello spazio libero. In primo luogo è stato studiato l'impatto della turbolenza atmosferica nel

caso di propagazione di singoli fasci ottici e di fasci ottici paralleli. Successivamente sono state misurate le perdite del canale ed è stato analizzato l'effetto della turbolenza sulla statistica dei fotoni. Infine è stato proposto un metodo che sfrutta la turbolenza per migliorare il rapporto segnale-rumore del canale.

Nella seconda parte sono state prese in considerazione la sicurezza e l'efficienza dei protocolli di Quantum Key Distribution (QKD). È stata proposta la dimostrazione sperimentale del protocollo B92 con stati non-massimamente entangled. L'utilizzo di questa tipologia di stati ha permesso di migliorare la sicurezza e l'efficienza di questo protocollo.

Infine, nell'ultima parte si è proposto un possibile metodo per migliorare la capacità di canale sfruttando coppie di fotoni hyperentangled. A riguardo, è stato progettato e collaudato un sistema per la trasmissione di stati hyperentangled a lunga distanza.

Acknowledgment

I want to firs acknowledge Prof. Paolo Villoresi who supervised me during this three years of work. He gave me the opportunity and the means to deal with new experiences and challenging problems. I also thank Dr. Giuseppe Vallone for his precious and helpful advises and Dr. Francesco Ticozzi for the useful discussion. A special thank to my wife for her dedication and her support during this years, particularly in difficult moments. Thanks also to my friends and colleagues, with whom I exchanged ideas and shared troubles and successes: Davide Bacco, Enrico Ballarin, Paolo Baracca, Stefano Buratin, Matteo Canale, Ivan Capraro, Nicola Dalla Pozza, Daniele Dequal, Enrico Favero, Simone Gaiarin, Francesca Gerlin, Alberto Gurizzan, Davide Giacomo Marangon, Luca Mazzarella, Alberto Michielan, Mattia Minozzi, Andrea Tomaello, Marco Tomasin, Sergio Vendemmiati and all the people of IFN-CNR Luxor laboratories of Padua. Finally, I want to thank my parents and my family whose have always supported my decisions and encouraged me to go ahead during all these years.

Innanzitutto vorrei ringraziare il Prof. Paolo Villoresi che mi ha guidato in questi tre anni di lavoro. Mi ha dato l'opportunitá e gli strumenti per affrontare esperienze nuove e problemi stimolanti. Il mio ringraziamento va anche al Dr. Giuseppe (Pino) Vallone per i suoi preziosi e utili consigli e al Dr. Francesco Ticozzi per le utili discussioni. Un ringraziamento speciale va a mia moglie, che mi è stata accanto e mi ha sostenuto in questi anni, soprattutto nei momenti difficili. Un grazie anche ai miei amici e colleghi, con i quali ho scambiato idee e ho condiviso difficoltá e successi: Davide Bacco, Enrico Ballarin, Paolo Baracca, Stefano Buratin, Matteo Canale, Ivan Capraro, Nicola Dalla Pozza, Daniele Dequal, En-

rico Favero, Simone Gaiarin, Francesca Gerlin, Alberto Gurizzan, Davide Giacomo Marangon, Luca Mazzarella, Alberto Michielan, Mattia Minozzi, Andrea Tomaello, Marco Tomasin, Sergio Vendemmiati e tutte le persone dei laboratori IFN-CNR Luxor di Padova. Infine vorrei ringraziare i miei genitori e la mia famiglia che hanno appoggiato sempre le mie scelte e mi hanno spronato ad andare avanti in tutti questi anni.

List of Acronyms

1SDI-QKD	one-side device independent-Quantum Key Distribution
B92	Bennet 92 [2]
BB84	Bennet-Brassard 84 [1]
BBO	Beta Barium Borate
CH	Clause-Horne
CHSH	Clauser Horne Shimony Holt
CMOS	complementary metal oxide semiconductor
CW	continuous wave
DEI	Department of Information Engineering
DI-QKD	device independent-Quantum Key Distribution
DM	dichroic mirror
DOF	degree of freedom
ent-B92	entangled-based Bennet 92 QKD protocol
EPR	Einstein Podolsky Rosen
ESA	European Space Agency
FPGA	field programmable gate array
FWHM	full width half maximum
H-V	Hufnagel-Valley
HE	hyperentangled
IAC	Instituto de Astrofísica de Canarias

ING	Isaac Newton Telescope
IR	infrared
JKT	Jacobus Kapteyn Telescope
NMES	non-maximally entangled state
OGS	Optical Ground Station
PC	Personal Computer
QBER	quantum bit error rate
QC	quantum communication
QKD	Quantum Key Distribution
SHG	second harmonic generation
SI	scintillation index
SNR	signal to noise ratio
SPAD	single photon avalanche diode
SPDC	spontaneous parametric down conversion
TNG	Telescopio Nazionale Galileo
us-B92	unconditionally secure - B92 protocol

Notations

General	
ln	natural logarithm
$\log_2$	binary logarithm
$\log_{10}$	common logarithm
$\mathbb{1}$	identity matrix
$\langle X \rangle$	mean value of random variable X
ρ^*	complex conjugate of ρ
$\mathrm{Tr}(\rho)$	trace of the operator ρ
$\overline{a}$	angle orthogonal to a

Entropies	
$h_2(Q)$	binary entropy function
$H(\mathbf{A})$	Shannon entropy of the probability distribution $\mathbf{A}$
$H(\mathbf{A}\|\mathbf{B})$	conditional entropy
$H_{min}(\mathbf{A}\|E)$	smooth min-entropy of $\mathbf{A}$ relative to E
$H_{max}(\mathbf{A}\|E)$	smooth max-entropy of $\mathbf{A}$ relative to E

Entanglement measurement

$F(\rho, \sigma)$	fidelity between ρ and σ
$P(\rho)$	purity of ρ
$T(\rho)$	tangle of ρ
$S_L(\rho)$	linear entropy of ρ

Vectors

$\|\phi\rangle\langle\phi\|$	projector onto the vector $\|\phi\rangle$
$\otimes$	tensor product
$\|\phi\rangle\|\psi\rangle$	tensor product between vector $\|\phi\rangle$ and $\|\psi\rangle$
$\|\overline{a}\rangle$	vector orthogonal to $\|a\rangle$

List of Figures

List of Tables

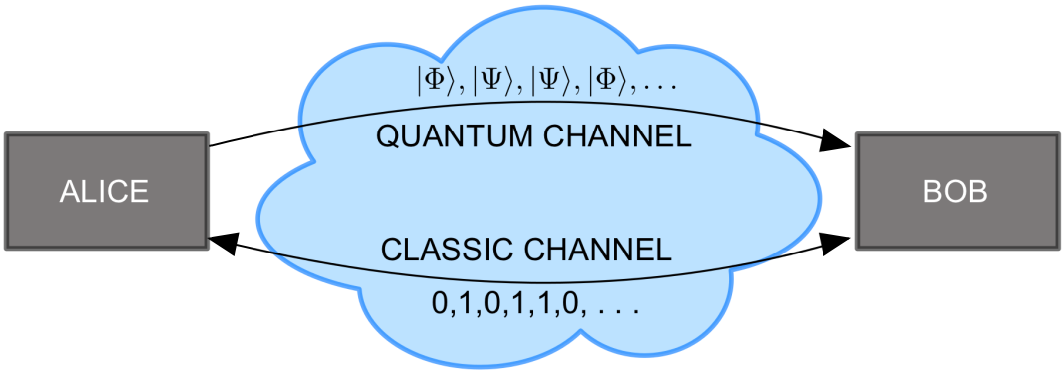
CHAPTER 1

Introduction

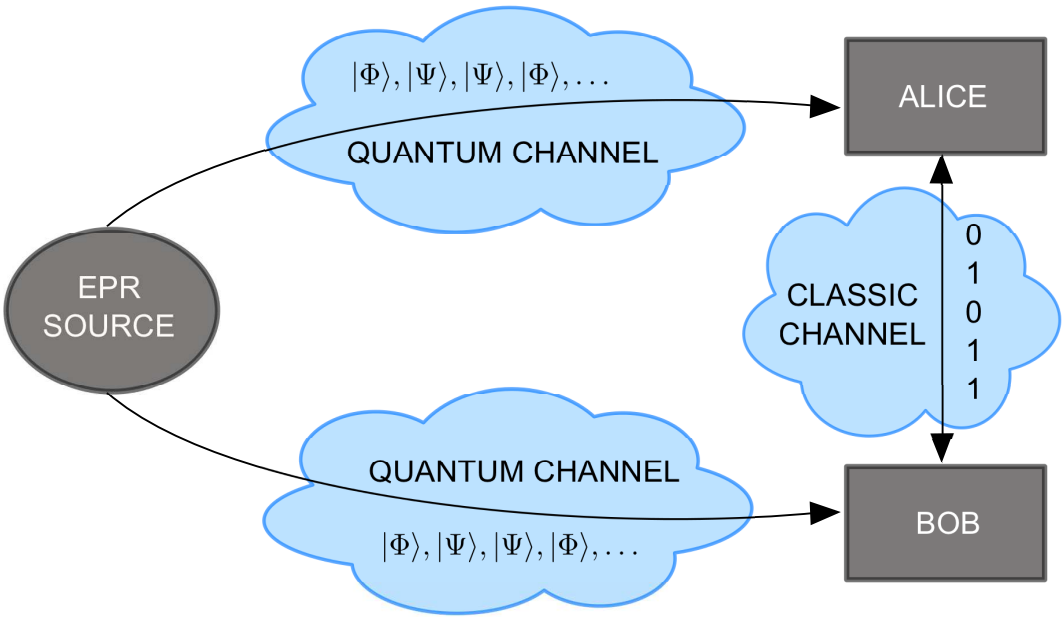
Quantum Key Distribution (QKD) represents an unconditional secure way to share a secret key between two authenticated users, usually called Alice and Bob. It is fundamentally based on the principle that is impossible to observe a quantum system without changing its state. The first QKD scheme was the one proposed by Bennet and Brassard in 1984, commonly known as Bennet-Brassard 84 [1] (BB84). Since then, several QKD schemes were presented and many efforts have been devoted to improve both the theories and the experimental implementation of these systems.

As represented in figure 1.1 typical QKD schemes involves two or three remote parties which communicate by means of quantum and classical channels. In this thesis we take in consideration some parts of a quantum communication (QC) system, we analyze them and propose some improving solutions.

We start our study from the quantum channel, especially we analyse free-space quantum channels considering their characteristics and their interactions with the transmitted photons. One of the main problems of this kind of channels is atmospheric turbulence. A turbulent channel acts as an increment of the losses on the transmitted photons due to beam wandering of the beam centroid or to scintillation, increasing the role of the noise [6–10]. The understanding of the propagation effects induced by turbulence at the receiver as well as the temporal statistics of the incoming photons is crucial to assess the quality of the communication and eventually the feasibility of the free-space ground-ground and space-ground links [11–13].



(a) Scheme for two-party QKD protocol



(b) Scheme for three-party QKD protocol

Figure 1.1: Schematic representation of two different QKD systems.

The second issue we address is the security of the QC systems, in particular we propose and demonstrate a device independent-Quantum Key Distribution (DI-QKD) protocol based on non-maximally entangled states(NMESs). In common QKD protocols the security of the shared key is typically proven under the assumption of trusted apparatuses. In the last years, great effort have been devoted to the so called DI-QKD, aiming at the demonstration of the security when the measuring devices are completely untrusted and their working mechanism is not known to the users. The key ingredient for DI-QKD is the exploitation of entangled states

shared between two parties: by violating a Bell's inequality, it is possible to prove the secrecy of the obtained bits. The DI-QKD offers the advantage that security is independent on the practical details of the implementation: Alice and Bob could even purchase their devices directly from Eve, because the violation of a Bell's inequality would certify the secrecy of the transmission in any case. On the other side, the violation of a Bell test without any additional assumption requires a very high overall (from the light source to the detectors) detection efficiency. It is well known that NMESs offer an advantage for the violation of the Clauser Horne Shimony Holt (CHSH) inequality in terms of required detection efficiency, with respect to maximally entangled state [14, 15]. Recently, detection loophole-free violations of the CHSH inequality by non-maximally entangled photons were indeed reported [16,17]. NMESs were proven to be also useful for several bipartite Bell inequalities [18] and for quantum steering [19].

Finally we focus on the transmission rate and the channel capacity of the QC systems. About that, we developed and tested a system for the generation and measurement of hyperentangled states. Most of the proposed QKD protocols are still not able to compete with actual classical communication. Hyperentanglement, that is entanglement in more than one degree of freedom (DOF), represent a great resource for QC and QKD because offer many advantages on security and channel capacity enhancement. Dense coding, proposed in 1992 in [20], were experimentally demonstrated using entangled photon pairs and simple linear optics [21–23]. This kind of realizations unfortunately does not permit to fully exploit the channel capacity, indeed the best reached rate was 1.585 bits. Hyperentanglement represents a resource for dense coding, in fact enables a complete Bell state discrimination, as proposed by [24].

This Ph.D. thesis is organized as follows:

Chapter 2 - In this chapter we propose the study of the propagation in free-space of a single or twin beam in a scale of several tens to a few hundred kilometers optical links. The experimental models were realized in different localities of Italian Alps as well as between Tenerife and La Palma Islands of the Canary archipelago. We first analyse the single beam propagation taking in consideration the turbulence effects and in particular the beam wander. We

then take in consideration the twin-beam propagation in order to study the correlation of the beam centroids.

Chapter 3 - In this chapter we consider the photon statistic and the link attenuation in a 143 km free-space optical link. We propose a transmitting setup with an active pointing system for a fine alignment. For the determination of the turbulence intensity we analyse the weather condition. We then present the analysis of temporal statistic of the received photons and the measurement of the link losses. We finally develop a technique for signal to noise ratio (SNR) improvement.

Chapter 4 - In this chapter we present the entangled-based Bennet 92 QKD protocol (ent-B92) protocol, a version of the Bennet 92 [2] (B92) protocol realized with NMES, proposed recently in [25]. Particular attention is given to the analysis of security and the estimation of secure key rate. We then propose the generalizations of ent-B92 protocol and analyse its secret key rate when detection inefficiencies are taken into account.

Chapter 5 - In this chapter we propose the implementation of the ent-B92 protocol. We design and realize the experimental setup considering in particular the compactness and the reliability of the system. We report the measurement of Bell's inequality, secure key rate and detection threshold compared with theoretical models. We present also a noise model that takes into account all the non-idealities of the system.

Chapter 6 - In this chapter we propose the design and the experimental implementation of a system for the generation of photon pairs entangled in both polarization and energy-time. We consider the stability of the measurement system and propose some solutions for its improvement. Finally we present some measurement of the hyperentangled photon states.

Chapter 7 - In this chapter we present the conclusions of the thesis with a summary of the principal findings.

CHAPTER 2

Atmospheric turbulence investigation in free-space optical links

Quantum communication (QC) aims to share quantum states between terminals doing quantum operations. The essential requirement of a QC protocol is the preservation of the information carried by the states, which is attacked by the interaction with the environment as well as by the attenuation due to the propagation [26–29]. The partner may be as close as two logic gates in the proposed design of a quantum computer as far away as a terminal in orbit and a telescope on ground, in the proposed schemes of planetary QKD scenarios [6, 13, 30–34]. In the perspective of the extension of QC in free-space to long distances, the analysis of the phenomena that occur to a visible or near-infrared beam in the propagation in atmosphere and their understanding is of crucial importance for devising the most convenient optical terminal. The investigation on the ground-ground case is used also to envisage the space QC, along with a vast area of research in satellite Classical Communications [35].

More in details, optical propagation in atmosphere in the case of links length of over 100 km is affected by several transformations of the beam parameters, resulting in an increase of the link losses. Moreover, the long range optical communication at the single photon limit exploiting quantum protocols, on the other side, differs from the classical protocols in that the signal to be transmitted cannot be intensified,

being a train of very weak pulses with an average about one photon per pulse.

The understanding of the effects induced by the propagation in both the irradiance at the receiver as well as in the temporal statistics is crucial to assess the quality of the communication and eventually the feasibility of the link. Moreover, for the very long links, fading and losses are induced by the decoupling of the beam with the receiver due to large wandering of the beam spot, as it was also investigated for the space channel [36].

In this chapter we first propose a brief introduction on atmospheric turbulence and on effects induced by turbulence. Therefore we present the main characteristics of the investigated links. We then address the study of the phenomena induced in very long propagation by using of laser beams to investigate the links. In the experiments, we performed the observation of the whole beam combined to the measure of the local irradiance at the receiver side. In addition, with the aim to stabilize the centroid position at the receiver, we studied the propagation of two beams forming a small mutual angle in the framework of the isoplanatic angle spread for low and high orders of the beam spatial modes.

The results contained in this chapter and in the next one (chapter 3) are published in [J1, P1–P5] and in the Ph.D. thesis of Tomaello [37] who took part at most of the experiments.

2.1 Atmospheric turbulence

An optical beam that propagates in the atmosphere can experience attenuation losses and random degradation of the beam quality itself. The first effect is induced by absorption and scattering due to molecolar constituents and particulates present in the atmosphere. The second effect is related to turbulent motion in the atmosphere, which is caused by small variations in temperature ($< 1^\circ$ C) that give rise to random changes in wind velocity (eddies). The air mixing due to the temperature gradient induces small change in atmospheric density and, hence, in the refractive index. The random variation of refractive index can be cumulative, and this can cause significant inhomogeneities in the index profile of the atmosphere. Therefore, a beam propagating in the atmosphere can experience deviation of direction which

lead to beam wander, intensity fluctuation (scintillation) and beam spreading.

The small changes in the refractive index can be thought as a set of small lenses in the atmosphere, which focus and redirect the beam. We can assume that each of these small lenses has the size of the turbulence eddy that generated it. This model is a useful approximation of turbulence effects, although is not completely accurate.

Since the complexity of atmosphere does not allow a deterministic description of its phenomena, all the theories related to turbulence are based on statistical analysis.

A detailed description of atmospheric turbulence phenomena can be found in [35, 38].

2.1.1 Refractive index structure parameter

The refractive index structure parameter C_n^2 is the most significant parameter that determines the turbulence strength. This parameter depends on season, geographical location, weather, altitude and time of day. There exist a lot of model that describe the profile of C_n^2, the more used is the Hufnagel-Valley [40] that is given by:

$$C_n^2 = \left\{ \left[\left(2.2 \times 10^{-53}\right) h^{10} \left(\frac{W}{27}\right)^2 \right] \mathrm{e}^{-h/1000} + 10^{-16}\, \mathrm{e}^{-h/1500} \right\} \mathrm{e}^{r(h,t)} \quad \left[\mathrm{m}^{-2/3}\right] \tag{2.1}$$

where h is the height above the sea level in meters, W is the wind correlation factor which is defined as:

$$W = \left[\left(\frac{1}{15 \text{ km}} \right) \int_{5 \text{ km}}^{20 \text{ km}} v^2(h) \mathrm{d}h \right]^{1/2} \tag{2.2}$$

and $r(h,t)$ is a zero-mean homogeneous Gaussian random variable. The term $v(h)$ is the wind speed at height h, as developed by Bufton [38] is equal to:

$$v(z) = 5 + 30 \cdot \mathrm{e}^{-\left(\frac{z-9.4}{4.8}\right)^2} \tag{2.3}$$

where z is in [km] and the wind speed v is in [m/s]. In figure 2.1 the wind speed profile as a function of the altitude is reported.

2.2 Turbulence effects

The effects of turbulence can be divided by spatial frequency as beam spreading (high frequency) and beam wandering (low frequency). The first effect is produced

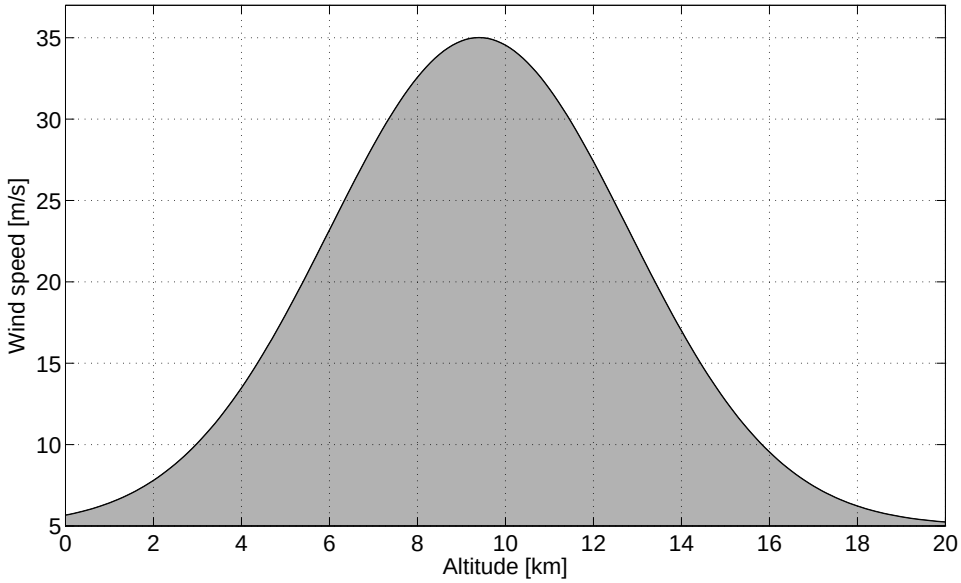


Figure 2.1: Wind speed profile as a function of altitude.

by eddies smaller than the beam size whereas the second one is given by eddies that are larger than the beam size. Another turbulence induced effect is intensity variation that is induced by eddies with sizes on the order of $\sqrt{\lambda L}$, where L is the propagation distance and λ is the wavelength.

2.2.1 Fried coherence length

An useful quantity that describe the atmospheric turbulence is the Fried coherence length. It is defined as the maximum allowable diameter of a receiver collector before atmospheric distortion seriously limits the transmitting performance [38]. Particularly, for a plane wave propagating from altitude $h_0 + L$ to h_0 (downlink) the Fried parameter can be expressed as [35]:

$$r_0 = \left[0.423 \cdot k^2 \sec(\zeta) \int_{h_0}^{h_0+L} C_n^2(h) \mathrm{d}z\right]^{-3/5} \tag{2.4}$$

where L is the path length, ζ is the zenith angle and C_n^2 can vary with altitude h. For an horizontal path, i.e. when the parameter C_n^2 is constant, the Fried coherence length r_0 is equal to [38]:

$$r_0 = 1.68 \cdot \left(k^2 C_n^2 L\right)^{-3/5} \tag{2.5}$$

whereas for spherical waves is given by [38]:

$$r_0 = 3 \cdot \left(k^2 C_n^2 L\right)^{-3/5} \tag{2.6}$$

2.2.2 Scintillation index

The scintillation index (SI) describes the intensity fluctuation of the signal irradiance. It can be expressed as the normalized variance of the intensity fluctuation [35]

$$\sigma_I^2 = \frac{\langle (I - \langle I \rangle)^2 \rangle}{\langle I \rangle^2} = \frac{\langle I^2 \rangle}{\langle I \rangle^2} - 1 \tag{2.7}$$

where I is the signal intensity. Using the results of Rytov method [39] we can describe the SI as the variance of the field log-amplitude σ_χ^2:

$$\sigma_I^2 = A \left[\mathrm{e}^{4\sigma_\chi^2} - 1 \right] \quad [\mathrm{W/cm^2}] \tag{2.8}$$

where A is the aperture average factor, that for weak turbulence and small value of the eddies size can be predicted by:

$$A = \left[1 + 1.07 \left(\frac{kD^2}{4L} \right)^{7/6} \right]^{-1} \tag{2.9}$$

where L is the link distance and D is the aperture diameter of the system. For a plane wave the field log-amplitude is defined as:

$$\sigma_\chi^2 = 0.307 k^{7/6} L^{11/6} C_n^2 \tag{2.10}$$

whereas for a spherical wave is equal to:

$$\sigma_\chi^2 = 0.124 k^{7/6} L^{11/6} C_n^2 \tag{2.11}$$

2.2.3 Beam wander

One of the effect of the air turbulence is beam wander. Considering the temporal velocity of this effect one can also divide it in: beam *jitter* when the wander is fast and *drift* when the wander is slow.

The variance of the waveform tilt angle can be expressed as a function of the Fried coherence length as [38]:

$$\alpha^2 = 0.364 \left(\frac{D}{r_0} \right)^{5/3} \left(\frac{\lambda}{D} \right)^2 \tag{2.12}$$

where as already mentioned above D is the aperture diameter of the system.

2.3 Experimental links

Here is explained the characteristic of the three principal channels that were used in the experiments.

2.3.1 Short range links

The fist link that was studied is an urban link of 2.2 km between the Department of Information Engineering (DEI) building roof to the Specola tower of Department of Physics and Astronomy, across downtown Padua, as shown in Fig. 2.2(a).

We then increased the distance with a 13 km free-space link between two places in the Italian Alps above Santa Croce lake at 1400 m of altitude as shown in Fig. 2.2(b).

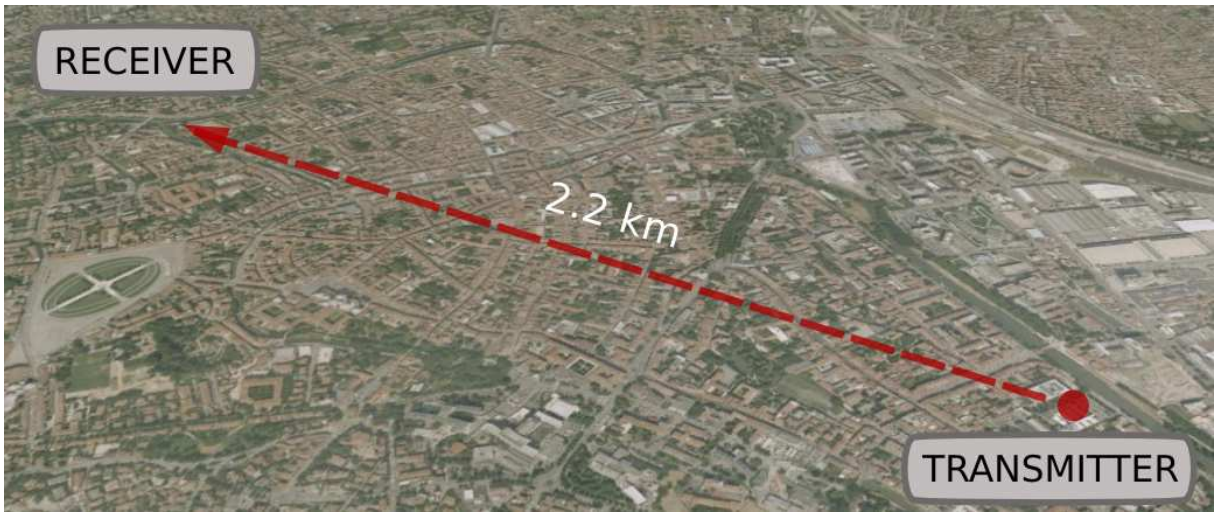
2.3.2 143 km Canary Islands link

The longest free-space optical link that was studied is between Tenerife and La Palma Islands of the Canary archipelagos, as shown in Fig 2.2(c). The channel was probed in both the direction, i.e. from the roof of the JKT at La Palma to the OGS at Tenerife and vice versa. The length of the link is 143 km at a mean altitude of 2300 m over Atlantic Ocean. The experiments reported in this chapter were taken during three different campaign in which different properties of the channel were investigated:

1. *May 2010* - single beam propagation from OGS to JKT, especially the wandering and broadening of the beam spot due to atmospheric turbulence.

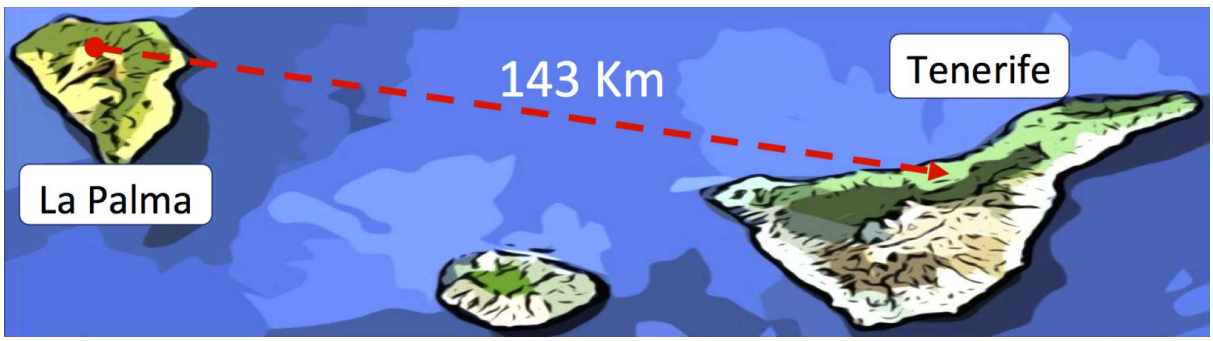
2. *September 2010* - twin beam-propagation from OGS to JKT

3. *May 2011* - symmetry of the optical channel.



(a) Downtown Padua link of 2.2 km from Department of Information Engineering building roof to the Specola tower of Department of Physics and Astronomy

(b) Alpine link of 13 km above Santa Croce lake



(c) Bidirectional path from the JKT of ING in La Palma and the OGS of ESA in Tenerife

Figure 2.2: Experimental links

2.4 Single beam propagation

The optical link between distant terminals may be modeled by combining the diffraction, attenuation and turbulence effects. This latter has been intensively investigated for decades and is suitably parametrized according to the geographical and meteorologic conditions [7, 8, 10, 35, 41]. However, for what concerns the spatial distribution of the spot and its coupling with a receiver in the case of very long path, of tens or hundreds of kilometers, the knowledge of actual atmospheric parameters along the whole distance is hardly feasible in practice. Therefore, the spatial effects induced by the turbulence, that in principle have to be expected significantly larger than the diffractive ones, call for direct testings. With this purpose, we set up the conditions to analyze the parameters of the beam by extending the acquisition of the gathered signal in the time domain to the capture of images at different integration time of the whole beam, in order to point out the effect of the spatial scintillation and the coupling to the receiving telescope. The initial tests were realized across downtown Padova, to test the equipment, and then over mountain links and finally in the Canary archipelagos.

The use of a refractor telescope is convenient in order to avoid the severe cut of the central portion of the gaussian beam by the central obstruction in the case of the reflecting telescopes. For this reason, transmitting refractors have been used in all the trials.

We used different types of optics to investigate the propagation. In the design of these instruments, the spherical aberration was always corrected. Due to the on axis use of the instrument, no further Seidel aberrations are acting, beside defocus. The use of an apochromatic lens was tested in order to simplify the transmission of two beams with different wavelength. When not possible, the chromatic aberration was canceled by separating the optical origin of the beams using a beamsplitter. We have used three different instruments:

1. a commercial 120mm-f/7.5 refractor, SkyWatcher Black Diamond Telescope, that use an apochromatic design and have a 120 mm optical aperture;

2. the secondary telescope of OGS, thank to the kind permission of ESA, that is

a 200mm-f/15 doublet telescope from Zeiss;

3. a 230mm-f/10 aplanatic telescope realized with a custom aspheric singlet from Costruzioni Ottiche Zen, Venezia, Italy.

In the case of both urban and mountain links up to 13 km, we have observed that an Airy-pattern may be obtained in clear nighttime conditions. In particular, the urban link of 2.2 km across downtown Padua, was investigated with refractor telescopes of different diameter. In the case of telescope n.1 above, the direct observation of the spot has shown an Airy pattern of about 30 mm between the two first zeros and with a beam wandering extension of about the spot radius. The Airy pattern was due to beam clipping. Similar results were obtained in the Alpine link where in this case the observed Airy pattern was of about 170 mm. These conditions are well described in the case of weak turbulence [8,10,41]. We investigated the case of longer lengths, finding that the beam is subjected to significant transformation that ends up to an irregular spot distribution. In the case of the Canary link above described and shown in Fig. 2.2(c), we initially studied the propagation from OGS to JKT using the telescope n. 2. The JKT location is fortunate because it is in direct sight of Tenerife top and the Observatory building results nearly normal to the link, so that it may be used as a screen for the spot detection. The telescope was used to transmit toward La Palma one or two beams, at the wavelength of 532 nm, from single mode continuous wave (CW) laser source, realized from an *OptoEngineMGL-III-532-100 DPSS* laser. An optical front-end was designed to realize a Gaussian beam of about 65 mm of waist and with a wavefront of adjustable curvature. The detection in La Palma was done with a refractive optic of 230 mm diameter equipped with both a power meter and a photodiode. In addition, the whole spot was imaged on the JKT wall with different exposure times. The weather conditions may change radically the results of the propagation, due to a series of causes. Some of these may block the propagation, as in the case of rising of clouds, which due to the local atmospheric conditions are usually lower than the link altitude, (2300 m), or the presence of *calima* that is sand from central Africa, brought by high-altitude winds and that invades the link altitude with enough density to diffuse completely the beam. The presence of strong wind or high level of humidity are often cause of

widening of the spot but that remain still clearly visible. However, with fair weather condition, a remarkable small spot was observed. Fig. 2.3 shows one image of the

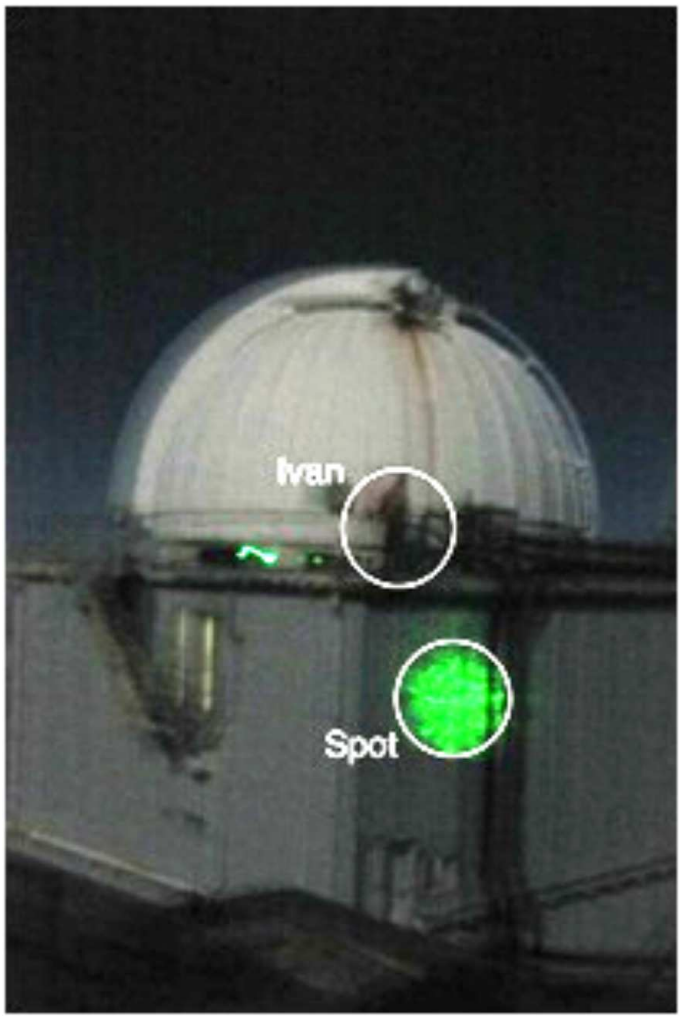


Figure 2.3: Spot size at JKT, La Palma. The two circles are of the same diameter. The top encircles a man whose height is about 1.85 m.

beam spot onto the JKT dome with optimal weather condition, taken in the night of 27 May 2010 with 500 ms exposure time, in which the diameter of the spot compares with a circle with the size of one person of height 1.85 m. From this observation, we may assess the diameter of the integrated spot to about 2 m. This particular condition was observed for and extended period of several hours in that night. For observations with clear sky but with stronger wind, the observed spot diameter was typically equal to 3 ± 0.5 m, with an increase of about 50 % in worst case. In the best case, the full angle subtended by this spot is of 14 μrad. The diffraction limited

full angle of a collimated beam may be calculated from the estimated beam waist at the transmitter as follows:

$$2\theta = \frac{2}{\pi}\frac{\lambda}{w_o} = 5.6\ \mu\text{rad} \tag{2.13}$$

with $w_0 = 60$ mm. The comparison of these two values shows that the observed spot in optimal conditions is less than a factor three of the diffraction limit, in the hypothesis that the beam is collimated at the telescope. The dimension of the spot at a distance of $x = 143$ km may be described in terms of the mean-square long-term beam radius $\langle \rho_L^2 \rangle$ by the combined effect of the propagation in vacuum and the turbulence effect, expressed in Eq. 37 of the 1975 paper of Fante [8]:

$$\langle \rho_L^2 \rangle \simeq \frac{4x^2}{k^2 D^2} + \frac{D^2}{4}\left(1 - \frac{x}{F}\right)^2 + \frac{4x^2}{k^2 \rho_0^2} \tag{2.14}$$

in which D is the beam diameter at the transmitter, that is defined in the case of a gaussian beam of radius w as $D = \sqrt{2w}$, that have an initial curvature of radius $-F$ and k as the wavevector, and ρ_0 is the turbulence coherent radius. This latter is a function of the local value of the structure constant of the refractive index C_n^2 along the path length. It is computed using different approximations depending on the type of beam. Again, using the previous reference [8], ρ_0 is expressed by the following equation:

$$\rho_0 = \left[1.46 k^2 x \int_0^1 (1-\chi)^{\frac{5}{3}} C_n^2(\chi x)\, \mathrm{d}\chi\right]^{-\frac{3}{5}} \tag{2.15}$$

where it is evident that the link is in general asymmetric if the value of C_n^2 is not uniform. We have proven that in the case of realistic values, the inequality $x \ll (k^2 C_n^2 l_0^{\frac{5}{3}})^{-1}$ is verified, where l is the inner scale size of the turbulent eddies [8]. We may note that the expression for the ρ_L as a function of ρ_0 and the definition of ρ_0 itself are defined differently in Dios et al. [6] as they are discussed in the case of collimated beam only. However, an adequate up scaling by a factor $\sqrt{8}$ provides a similar overall description.

In the optimal condition for the propagation, the value of ρ_0 which results from inverting Eq. (2.14) is of 28 mm. From this estimation, we may note that the propagation corresponds to the fourth case described by Fante, as $k\rho_0^2 \ll x$ and it

effectively corresponds to a beam that at the receiver plane breaks up in multiple spots [8].

The dependence of ρ_L on the radius of curvature F of the beam at the transmitter in eq. (2.14) has been verified in the experiment by varying the source position of telescope n. 2 from the front focal length. By observing the back-scattering of the beam with an auxiliary telescope 100 mm diameter $-f/10$ mounted beside the n. 2, it was possible to assess the correct focal position. The feedback from the observer at the receiver-end allowed us to optimize the focal position in order to minimize ρ_L. This condition was observed in the experiment upon the focus at the path end, and corresponds to the minimum of the term $\frac{D^2}{4}\left(1-\frac{x}{F}\right)^2$.

The asymmetry of the link was tested by using telescope n.3 located on the top of JKT in La Palma pointing the OGS building in Tenerife. In this new instrument, we designed the beam shaping in order to exploit the 230 mm diameter of the primary singlet lens using the maximum on-axis irradiance criteria in the Prof. Siegman book (Ch. 18), obtained with the waist-to-aperture-radius rate of 0.89 [42]. The weather condition during the campaign of May 2011 was unfavorable for several nights. However, we had the possibility to observe the spot and, in the most clear night of May 23th 2011 (which had still not optimal weather conditions), we had recorded a spot of about 3.5 ± 0.5 m.

2.4.1 Beam-wander analysis

Since one of the most predominant effect of turbulence is beam-wandering we developed a feedback system to stabilize the beam centroid at the receiver. The system was tested in the campaign of September 2010 in order to measure the spot position and correct it. The experimental setup is pictured in Fig. 2.4. A probe beam is sent from OGS telescope n. 2 to JKT where there is a CCD camera positioned at about 15 meter far from the telescope building and pointing the dome. The camera acquire the whole spot and send the data to a PC that elaborates the images and extract the coordinates of the beam centroid. At the OGS side the measured coordinates are used to move the position of the secondary lens of telescope n.2 in order to compensate the spot drift measured at JKT. Lens positioning at OGS is realized with an XY stage controlled by stepper motors with micrometric accuracy.

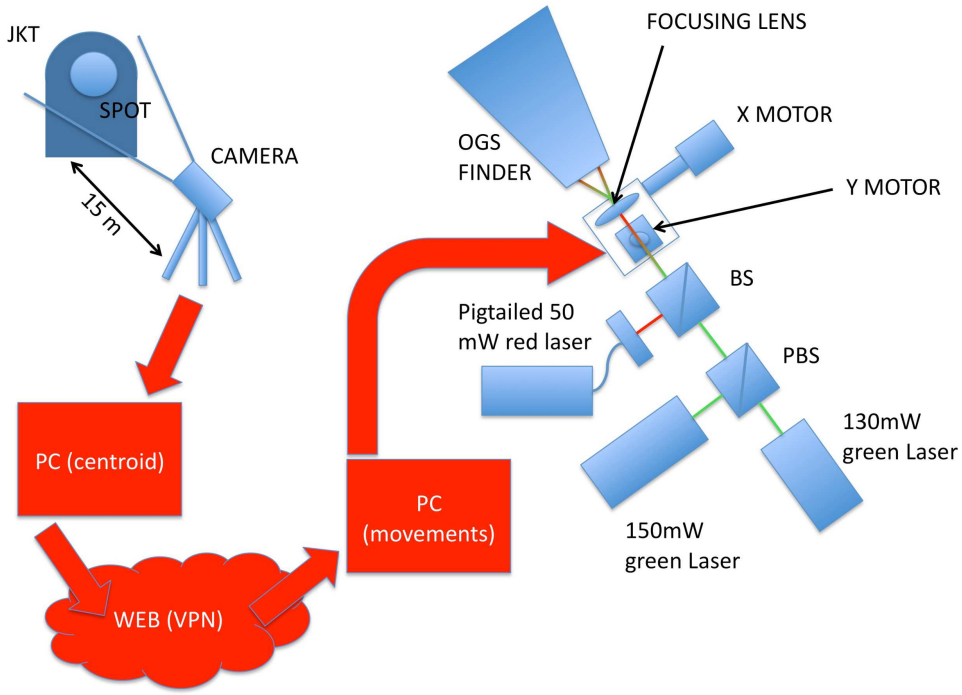


Figure 2.4: Beam-wander correction system

Due to the camera acquisition time the correction frequency is about 2-4 seconds depending on the intensity of the received beam.

In Fig. 2.6 are plotted the spot centroid displacement with respect to a determinate position without (Fig. 2.6(a)) and with (Fig. 2.6(b)) the correction system. We can notice that displacement of the centroid is relevant without the control system, indeed the expectation value and the standard deviation of the displacement are both about 2.6 m. Furthermore, acquisition time is shorter than the controlled one because few minutes after the alignment the beam exited from field of view of the CCD camera. Otherwise, in Fig. 2.6(b) we can see that when the correction system was active the displacement of the beam was on average much smaller (mean displacement = 0.92 m) as well as the standard deviation (STD = 0.55 m). The reliability of the correction system can be observed in the measurements of the received power, in Fig. 2.7 the collected power in both case with and without active correction are shown.

We analyzed also the spatial beam displacement in order to find some evidence between this one and the wind direction. In Fig. 2.8 the centroid displacement

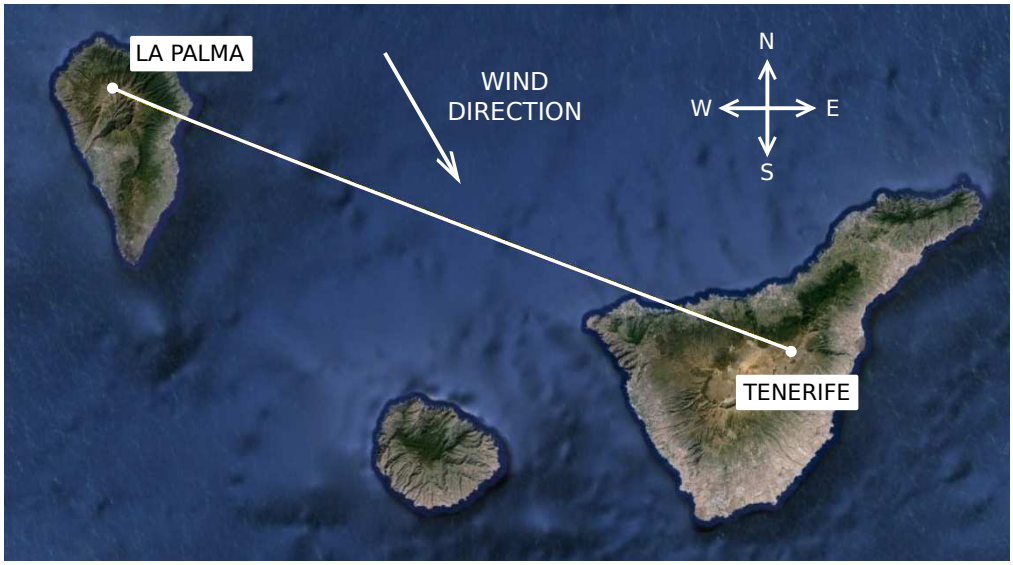
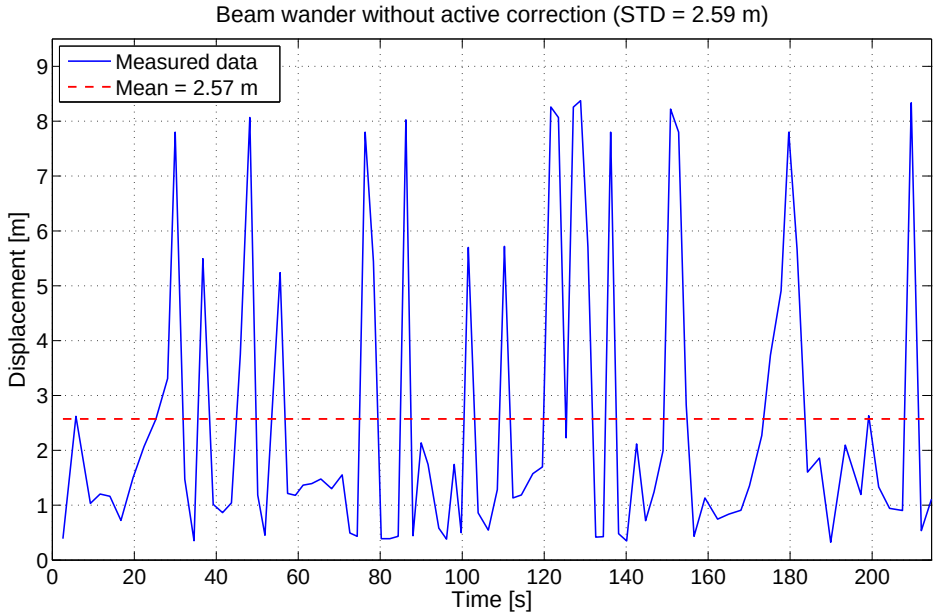
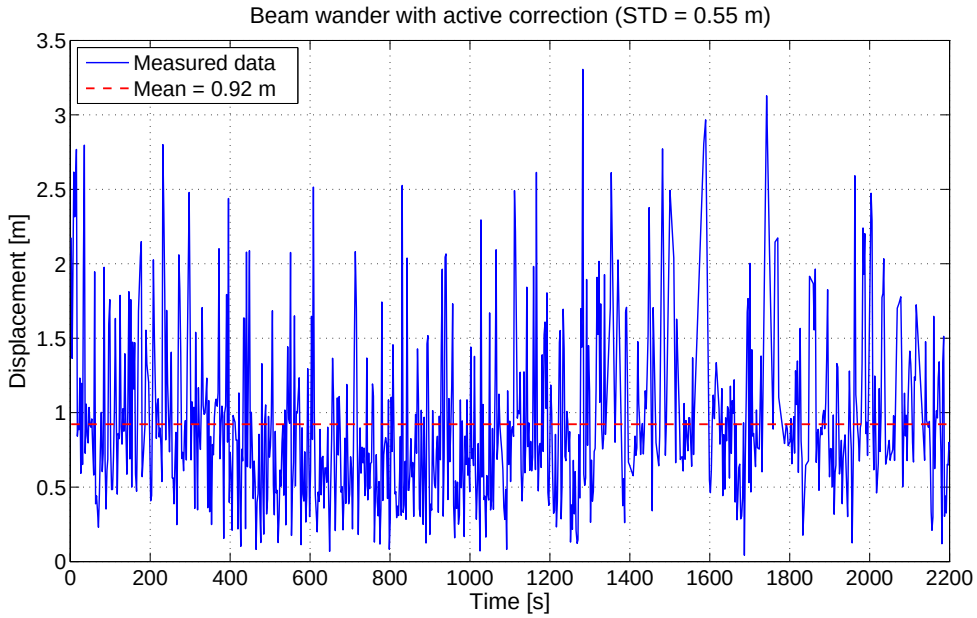


Figure 2.5: Wind direction during data acquisitions

and its spatial frequency in the surface perpendicular to the beam direction are plotted, corresponding to acquired data of September 28, 2010. It seems that beam displacement has a predominant direction as if there was something that pushed the beam from bottom right to top left. As reported in Fig. 2.5 the measured wind direction that night was about 300°, which corresponds to an angle of 40° with the beam direction. The vertical displacement can also be caused by the constant updrafts whose were present during the night due to the thermal gradient between the land-sea and air. According with this considerations we can then say that there is a correlation between wind direction and beam displacement.

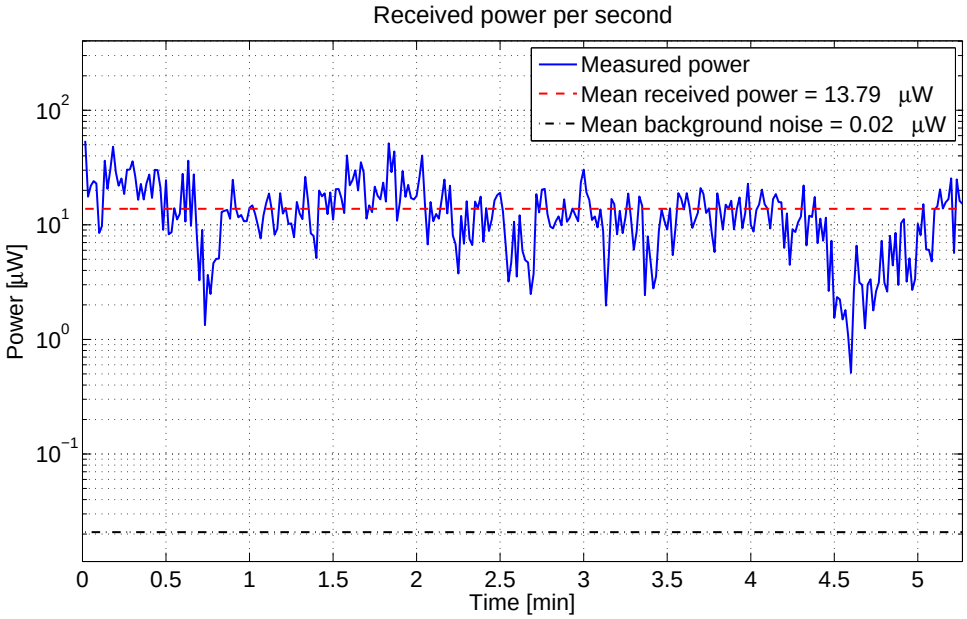


(a) Spot centroid displacement with respect to a determinate position without correction system

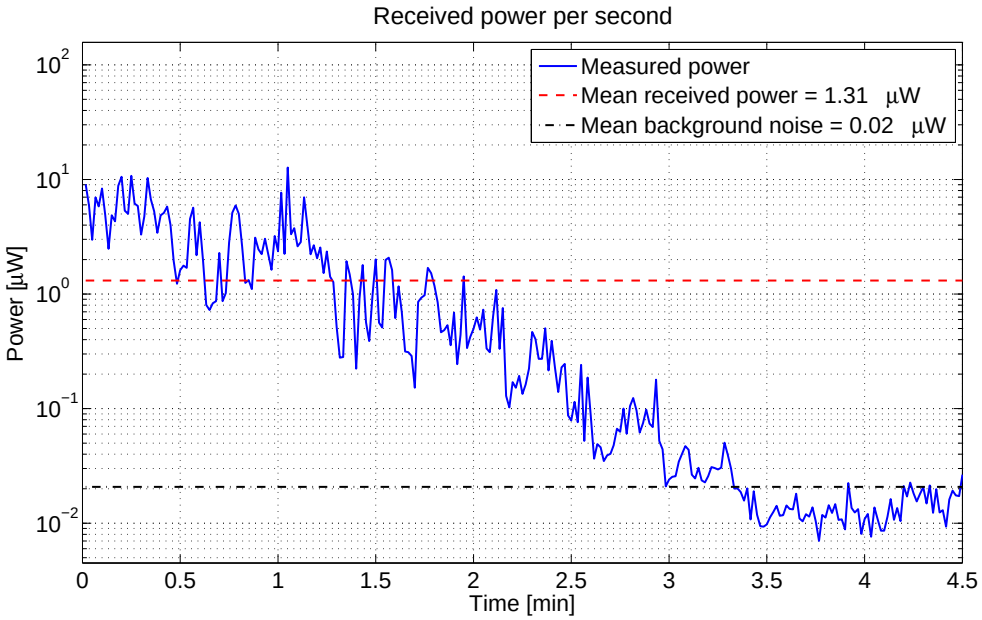


(b) Spot centroid displacement with respect to a determinate position with correction system

Figure 2.6: Beam-wander measurements

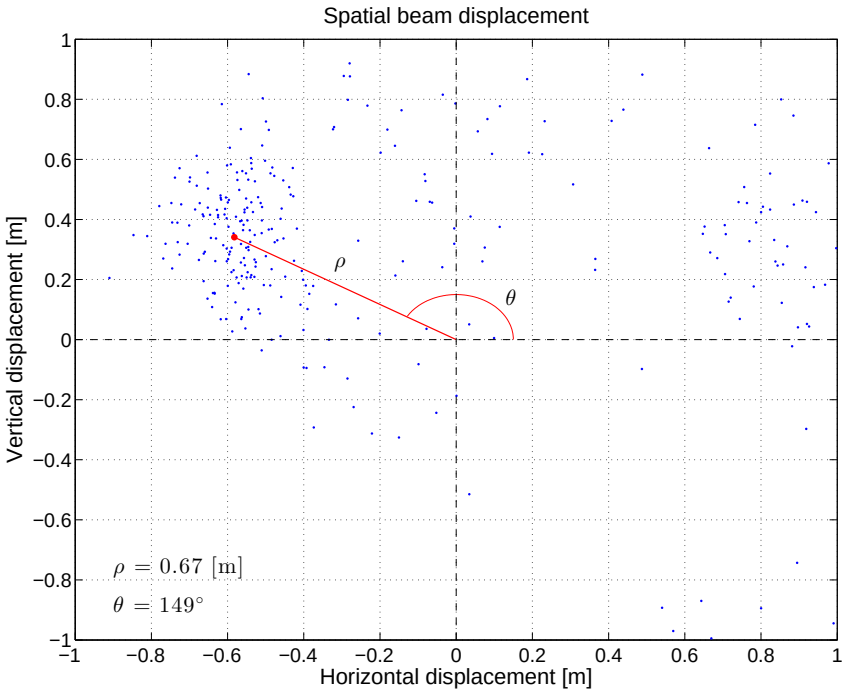


(a) Collected power with active stabilization

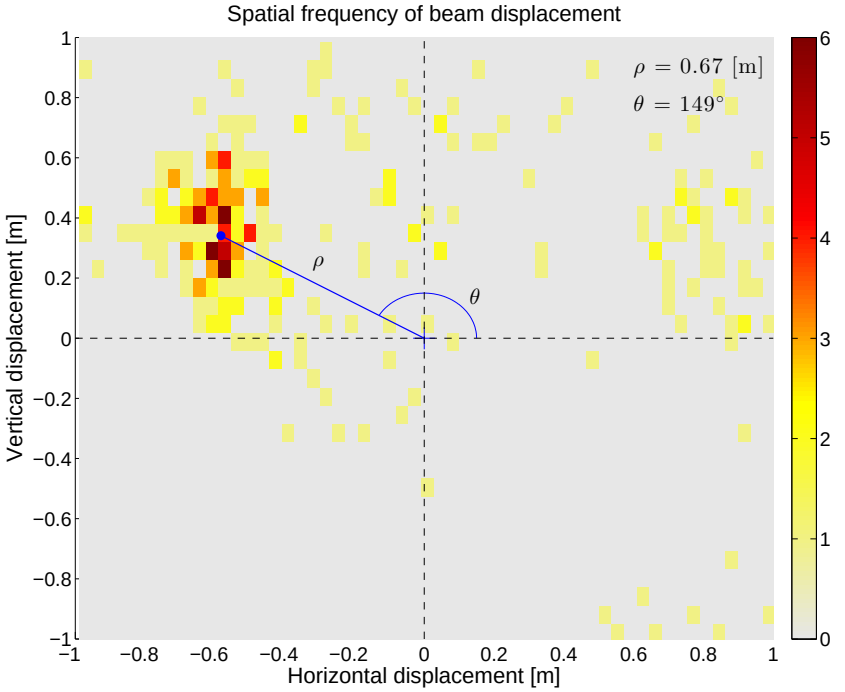


(b) Collected power without active stabilization

Figure 2.7: Power measurements



(a) Spatial position of the beam centroid



(b) Spatial position frequency of the beam centroid: red areas correspond to high frequencies, light-grey areas correspod to low frequencies

Figure 2.8: Analysis of the spatial beam displacement

2.5 Twin-beam propagation: isoplanatic angles for different modes

We analyzed the propagation of two beams along the same path to study the correlation of the beam centroids. We considered this scheme in order to use one beam for the quantum channel - i.e. for the single-photon exchange - and the other as beacon for the beam pointing, in the same direction of propagation. In this way, if the two beams are correlated in their centroids, the instantaneous beam wandering introduced by the turbulence may be compensated by using an error signal from the acquisition of the second beam. In Fig. 2.9 on the left, the image of the JKT building with the two green beams is shown, while on the right the dispersion of the two beam centroids is reported for an extended measurement. The average separation is of 7.7 ± 0.5 meters, corresponding to a subtended angle of $\theta = 53$ μrad. From the analysis of the centroids we have seen that the beams movements are correlated with a standard deviation of 37.9 pixels, equivalent to 0.75 m. We may conclude that at this separation θ, the two beams are correlated at least in a common mode that involve the wander of both beams. This results is not valid for the higher order spatial fluctuations as the centroid is the first order momentum of the distribution. Indeed, the separation angle can be compared with the set of reference values introduced in adaptive optical corrections of phase front, as the isoplanatic angle θ_0 and the independence angle $\theta_{\phi ind}$. The former is the largest angle between two paths for which the turbulence-induced wavefront variations in the two paths are relatively similar, for the vertical propagation is equal to:

$$\theta_0 = \left[2.05 k^2 \left(\sec \zeta \right)^{8/3} \int_0^\infty \mathrm{d}h C_n^2 h^{5/3} \right]^{-3/5} \tag{2.16}$$

where k is the wavenumber, ζ is the zenith angle and h is the height in meter at the sea level. On the other hand, the $\theta_{\phi ind}$ parameter quantify the angle over which the phase effects between the propagation paths of two point sources are nearly uncorrelated [43–47].

The angle θ_0 decrease as the order of the spatial mode of interest increase [48], and its values for vertical observations spans from 7 to 17 μrad [45, 46] even if values of tilt as large as 100 μrad are reported by the Telescopio Nazionale Galileo

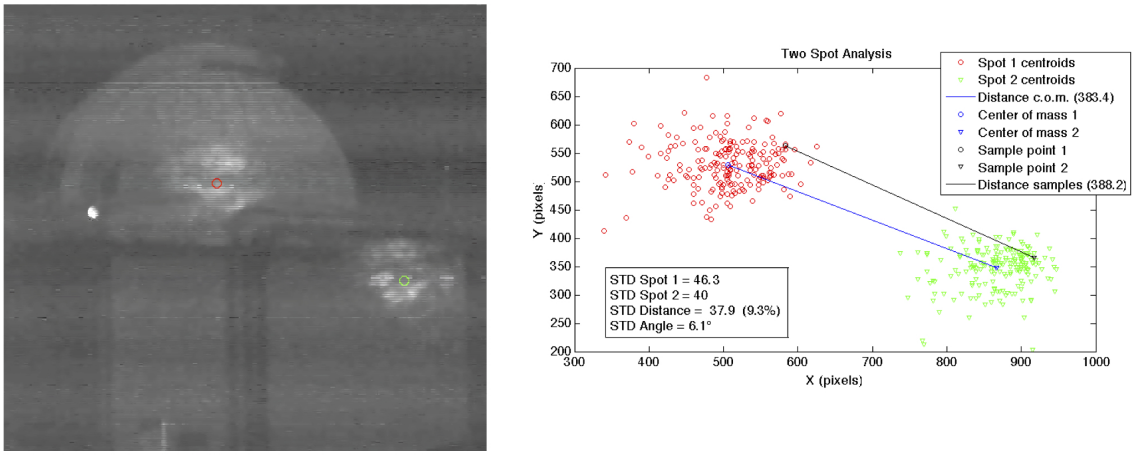


Figure 2.9: Spot of the two green lasers sent from Tenerife in the dome of OGS during the night of Sept. 29th and temporal analysis. 50 pixels = 1 meter.

(TNG) Observatory. Direct calculation of these two values were obtained using the condition of the experiment as follows: wavelength $\lambda = 532$ nm, link length L = 143 km, $C_n^2 = 2 \times 10^{-17}$ m$^{-\frac{2}{3}}$, transmitting aperture D = 200 mm, wind speed V = 10 m/s, outer scale $L_0 = 70$ m and inner scale $l_i = 7.5$ mm, where for the turbulence parameters we extracted the values from the various meteo stations of Instituto de Astrofísica de Canarias (IAC). The results are:

$$\theta_0 = 0.18 \ \mu\text{rad} \qquad \theta_{\phi ind} = 3.1 \ \text{mrad} \tag{2.17}$$

This results show a strong correlation in the spot movement, which is in agreement with the following interpretation: the separation angle is greater than the isoplanatic angle. This can be deduced from the different scintillation patterns and the centroid relative motion. However the separation is significantly lower than the independence angle, thus attesting the feasibility of the above described type of control.

In chapter 3 we will present a different and more efficient control for the beam stabilization that was tested in the same link.

2.6 Conclusion

The observation of the propagation of a single or a pair of beams along very long paths of over 100 km have shown that the beam is subjected to splitting into multiple

spots but its long-term diameter may be confined into a spot which is only a factor 3 to 5 the diffraction limit. This results have been obtained by using a suitable large aperture aplanatic refractive transmitter. In this way a significant reduction of the link losses for quantum communication channels in this extreme conditions are possible by the implementation of such scheme. This setup was used in both the OGS-to-JKT propagation and the reverse. This latter case have shown a larger spot than the former, although in the poorer weather conditions. The correlations of the two spots in the twin-beam propagation have demonstrated the possibility of the centroid control of the quantum channel by the use of an auxiliary co-propagating beam. These results have been propaedeutical to experiments upon the impact of turbulence on temporal statistics explained in chapter 3.

CHAPTER 3

Impact of turbulence on temporal statistics

In chapter 2 we have seen that a beam propagating in the atmosphere is subjected to beam-wandering, broadening and scintillation due to turbulence. However, for the study of the free-space propagation of quantum correlations is necessary to have a complete framework of all the turbulence-induced effects. In this chapter we first introduce the optical setup used to investigate the free-space channel and consider the weather conditions during the experiments. We then analyse the temporal statistic of the received photons and we present the link budget of the channel considering different measurement conditions. From the analysis of the data we finally propose the exploitation of turbulence to improve the signal to noise ratio of the channel.

3.1 Experiment description

The experiments were taken in the Canary archipelagos link described in 2.3.2 during the campaign of September 2011. We placed the transmitter in La Palma island at JKT observatory whereas the receiver was in Tenerife island at OGS observatory. We designed a feedback system for the beam stabilization in order to improve the SNR of the transmission. It consists in a complementary metal oxide semiconductor (CMOS) camera placed at JKT which acquire a beacon signal sent from OGS. Using the centroid position calculated from the camera data it is possible to correct the direction of the laser beam sent from JKT. In next section we will describe in detail

the optical setup of the experiment.

3.1.1 Optical setup

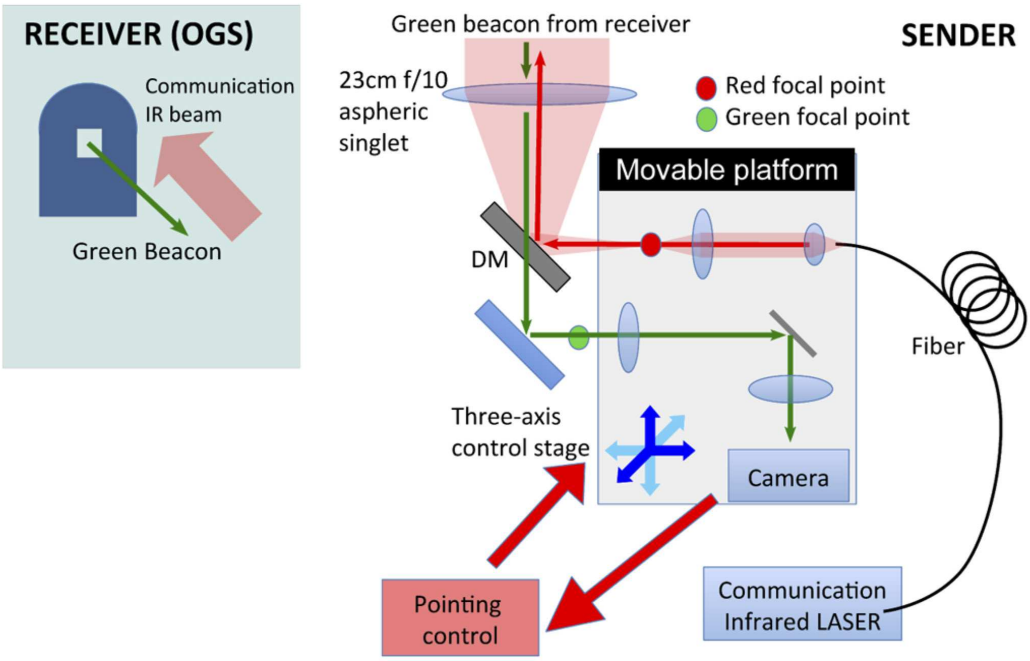


Figure 3.1: Schematic of the optical setup. DM: dichroic mirror

The optical setup of the transmitter is shown in Fig. 3.1. It consists of a suitably designed telescope whose key component is a singlet aspheric lens of 23 cm diameter and 220 cm focal length at 810 nm. The lens diameter was chosen to be significantly greater than the estimated Fried parameter r_0 [49] in order to obtain at the OGS a beam whose spot is comparable to the telescope primary mirror and consequently enhance the power transfer between the two sites. The fact that the lens is not achromatic was solved inserting a dichroic mirror (DM) to separate the path of the two wavelengths used in the experiment.

Our light source is an infrared (IR) diode at 808 nm coupled into a single mode fiber with an output power of about 6 mW and suitable attenuators. In order to facilitate the raw pointing, a mechanical XY stage has been added (we define the Z direction as the optical axis of the system). This stage moves all the 2.5 m long telescope in the XY plane. All the structure is assembled by three aluminum flanges;

one holds the lens and one the focal plane, and the other is attached to the XY back stage. The lens is fixed to an articulated mount to prevent bending of the structure.

The IR source has been aligned by means of the DM that reflect the 808 nm radiation. The platform carrying the focusing lens, the collimating lens, and the fiber port for the IR can be moved by a micrometric XYZ system based on stepper motors. In this way, the beam can be slightly steered by moving the focal spot at the singlet focus. The instantaneous deviation from the initial pointing direction is acquired by using a 532 nm beacon beam sent from the receiver by using a small portable low power laser module directly pointed towards La Palma without any optics. The beacon laser is acquired with a CMOS camera placed on the movable platform after the DM transmission. The centroid of the beacon spot on the camera determines the correction on the outcoming IR laser by means of an error signal with respect to the reference position. The position of the spot at the camera is sampled about once a second and averaged for a number of frames; these data feed a control software that calculates the movement for the fine XY stage in order to compensate slow drifts in the beam direction.

We collected data at the OGS in Tenerife in order to measure the received power and the scintillation and analyze the temporal structure of the signal. We placed in the OGS Coudé focus a photodiode and a power meter. When the beam was suitably attenuated at the transmitter with a neutral density filter we also collected data at the receiver with a single photon avalanche diode (SPAD) (Excelitas SPCM-AQRH model).

3.2 Weather conditions

Weather conditions play an important role in determining the turbulence intensity. We analyse the seeing, the Fried coherence parameter r_0 and the structural constant of the refraction index C_n^2 for different weather conditions. In table 3.1 we report the average meteorological data of the two sites during the observing nights compared with the turbulence parameters.

The determination of r_0 is obtained starting from the vertical seeing. First we estimate the value $r(V)$ i.e. the Fried coherence length for the vertical propagation,

Night	WS (T)	WD (T)	RH (T)	WS (R)	WD (R)	RH (R)	Seeing (R)	r_0 (R)	C_n^2(R)	C
17-18	14,31	328	4	23,55	271	1	0,9	3,4	0,19	G
18-19	15,17	186	6,5	31,6	221	6	1,165	2,6	0,3	G
19-20	5,9	129,5	4,5	12,4	151	3	1,75	$1,7^\star$	0,59	P
20-21	15,4	241,5	18,5	18,6	98,5	8	0,695	4,4	0,12	M
23-24	7,57	193,5	21	24,95	229,5	26	0,775	3,9	0,15	M

Table 3.1: Weather Data on both sites (T=Teide OGS, R=Roque JKT) for all the observing nights. Wind Speed (WS) is in [km/h], Wind Direction (WD) in degrees, Relative Humidity (RH) in percent, the seeing in [arcsec] whereas r_0 in [cm]. The value of C_n^2 is to be intended as explained in section 3.2 multiplied by 10^{-14} for 1 km along the path and by 10^{-16} for the others 143 km. C is the validity index for seeing based on the number of seeing data: Poor, Medium, Good. Value with * has been recalculated with video data (as explained in 3.2)

which is given by [50]:

$$r(V) = 2.013 \times 10^5 \cdot \lambda/\text{seeing} \tag{3.1}$$

then we estimate two C_n^2 using the Hufnagel-Valley (H-V) model [51], the first for the first 100 m (L_{v1}) and the second for the rest of the vertical propagation (L_{v2}). This is done by resolving the system given by this equations:

$$C_{n_{(2)}}^2 = \frac{\left(r_0^{(V)}\right)^{-5/3}}{0.423k^2\left(L_{v2} + C_{n_{(1)}}^2 L_{v1}\right)} \tag{3.2}$$

and the equation derived from the mean ratio of C_n^2 close to ground and far above the ground in the H-V model:

$$C_{n_{(1)}}^2 = 100 C_{n_{(2)}}^2 \tag{3.3}$$

At this point the value of r_0 for the horizontal propagation is easily obtained with the standard formula using the two distances $L_{h1} = 1$ km e $L_{h2} = 143$ km. In this way it is better taken into consideration the fact that for some km the beam travel close enough to the ground especially in Tenerife, therefore we have:

$$r_0 = 0.423k^2\left(L_{h1} \cdot C_{n_{(1)}}^2 + L_{h2} \cdot C_{n_{(2)}}^2\right)^{-3/5} \tag{3.4}$$

This approach is good when the weather conditions are acceptable in the sense that the approximation of the C_n^2 can be considered valid even for horizontal propagation using the formulas above. Moreover in the table 3.1 a *validity index* in three levels is reported indicating whether the r_0 approximation is good or poor. This index takes into consideration the amount of seeing data available for the calculation. In a particular case, the 3rd night, only one value of seeing was obtained not at ING weather station (close to JKT) but at the TNG site. In that night it was recorded also a number of videos which allow to estimate directly the value of C_n^2 and r_0 from a measure of the spot size at the CCD and considering the optical setup. These values are: $C_n^2 = 3 \times 10^{-17}$ and $r_0 = 3.76$ cm.

3.3 Temporal statistic analysis

Let us first describe the single photon detection acquisition. We performed several measurements by setting the counting interval T to 0.1, 1, and 10 ms. Because of turbulence effects, the mean photon number q in a counting interval at the receiver should follow a lognormal probability distribution [30]:

$$P(q) = \frac{1}{q\sqrt{2\pi\sigma^2}} \mathrm{e}^{-\left[\ln(q/\langle q\rangle)+(1/2)\sigma^2\right]/(2\sigma^2)} \tag{3.5}$$

where $\langle q\rangle$ is the average, $\sigma^2 = \ln(1 + \mathrm{SI})$, and $\mathrm{SI} = \frac{\Delta q^2}{\langle q\rangle^2}$ is the scintillation index (SI). If the counting interval T is large compared with the coherence time of the source and T is short compared with the turbulence time scale, the probability of detecting n photon in each interval follows the Mandel distribution:

$$p_n = \int \mathrm{d}q \frac{q^n \mathrm{e}^{-q}}{n!} P(q) \tag{3.6}$$

Note that the mean number of detected photons is $\langle n\rangle = \sum_n n p_n = \langle q\rangle$. In Fig. 3.2 (top) the analysis of the temporal distribution of an acquisition with 1 ms counting interval is reported. It is possible to observe that, when the average number of detected photons $\langle n\rangle$ is large (typically larger than 50) and the SI bigger than 1, the lognormal and Mandel distribution are quite similar. Given the experimental scintillation as 2.23 ± 0.01 and the mean value of detected photons as 234, we show the counting occurrences together with the corresponding lognormal distribution in

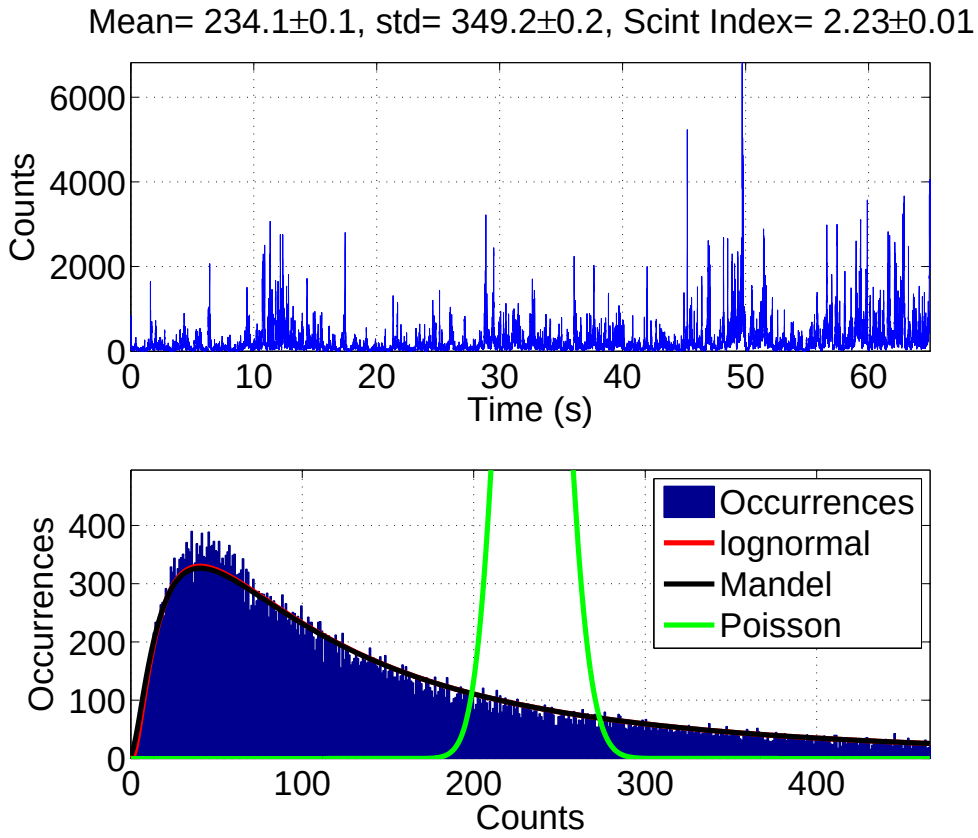


Figure 3.2: SPAD temporal distribution of count occurrences and corresponding lognormal and Mandel curves. We can compare the data with the corresponding Poissonian distribution with the same mean value 234 ± 0.1 that would be obtained without turbulence.

Fig. 3.2 (bottom). For comparison, it has been also inserted the corresponding Mandel distribution with the $\langle q \rangle = 234.1 \pm 0.1$ and $\sigma = 349.2 \pm 0.2$ parameters obtained from the raw data. We evaluated the similarity between the experimental data and the lognormal or the Mandel curve, defined as:

$$S = \left[\left(\sum \sqrt{p_i q_j} \right)^2 \right] / \left(\sum p_i \sum q_j \right) \tag{3.7}$$

where p_i and q_i are, respectively, the theoretical and experimental occurrences. The similarity of the lognormal curve with the data is 0.9959, while the Mandel curve has a similarity of 0.9967 showing clear evidence of the statistic transformation. The green curve represents the corresponding Poisson distribution with the same observed mean value, to compare what would have been obtained if the statistic

of the arrival photon were purely Poissonian. In Table 3.2, the data obtained for several different SPAD acquisitions are reported.

As mentioned, we also measured the intensity of received light with a fast photodiode by using an intense laser source. In Fig. 3.3 the temporal distribution of the photodiode voltage of a data set covering 20 s is plotted. The intensities are recorded with 50 kHz frequency. Also in this case the intensity occurrences follow a lognormal distribution (3.5) as shown from the lognormal curve with a similarity of 0.9896. In this case, the SI evaluated from the experimental data is SI $= \frac{\Delta I^2}{\langle I \rangle^2} = 1.19 \pm 0.01$.

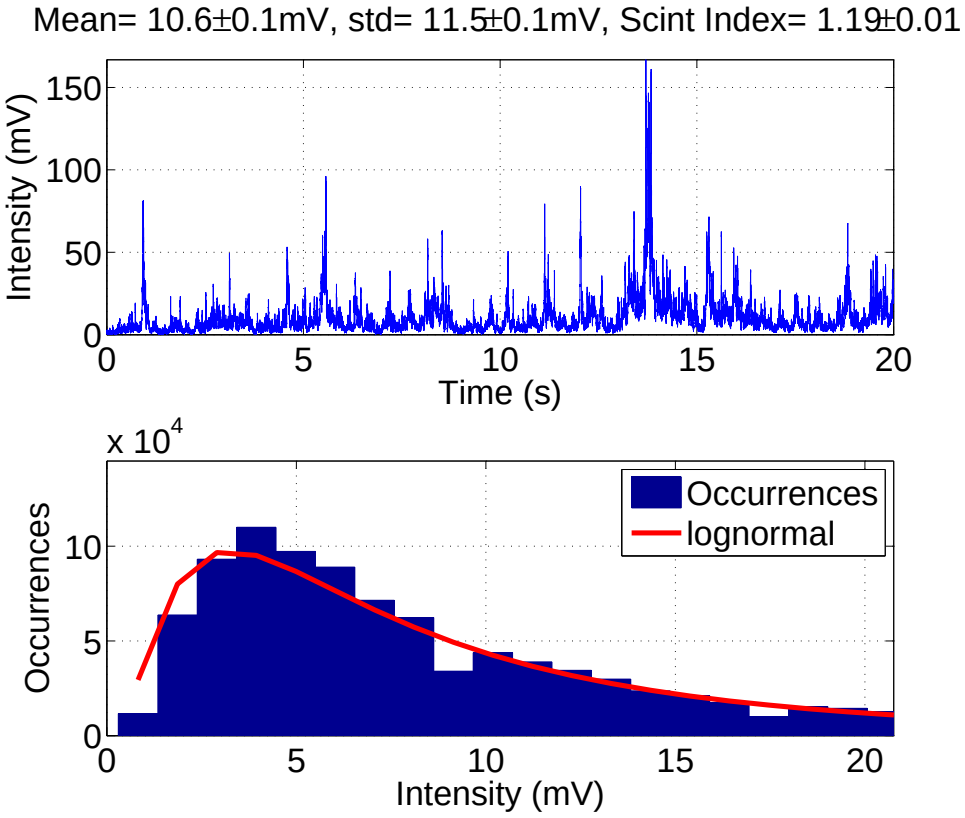


Figure 3.3: Photodiode temporal distribution intensity occurrences and corresponding lognormal curve.

3.4 Link budget

As already mentioned, one of the most important effects induced by turbulence is the attenuation. With the setup described in section 3.1.1 we measured the link losses

	Mean	Std	Time(s)	Window(ms)	SI	Bound(Hz)
backgr.	0.4732	0.7256	10	1	2.3515	475
Hi	5291	9135	650	10	2.9805	22
Hi	678.7	820.8	65	1	1.4626	43
Hi	510.4	751.9	65	1	2.1704	45
Hi	781.5	951.9	65	1	1.4834	42
Hi	180.2	312.0	65	1	2.997	39
Hi	234.1	349.2	65	1	2.2251	51
Hi	43.18	48.76	6.5	0.1	1.2748	81
Hi	21.17	26.34	6.5	0.1	1.5485	88
Hi	75.37	132.10	6.5	0.1	3.072	35
Hi	59.97	105.01	6.5	0.1	3.0659	37
Low	37.86	48.42	200	10	1.6355	35
Low	20.83	24.18	200	10	1.3479	35
Low	2.862	3.795	65	1	1.7578	384
Low	5.267	7.519	65	1	2.0383	258

Table 3.2: Data obtained for different single photon acquisition compared to the background (first line). For each acquisition is reported the total duration of the acquisition (Time), the temporal windows defining the counting interval (Window), the mean number of counts in the counting interval (Mean) and its the standard deviation (Std). It is also reported the SI and the frequency bound defined in such a way that all the frequencies below the bound contribute to 95% of the SI (Bound). With High (Low) it is indicated acquisition with high (low) mean photon number detected during 1 s. We can notice that for the last two data sets the bound is higher due to the low signal compared to the background (having flat frequency spectrum).

and we also demonstrated the capability of the system to maintain low attenuation and high stability along the night. The attenuation was calculated from the fiber and not from the singlet lens: telescope losses are thus included in the measured attenuation. The experiments were taken during the nights between 21 and 24 September 2011.

We measured an average attenuation that vary between 30 dB to 35 dB and during the best run we obtained an average attenuation of about 30 dB with peaks of 27 dB averaged over 2 minutes, as we can see in Fig. 3.4.

We also tried to correlate the losses with the weather conditions: as expected the lower the wind and the relative humidity, the lower the losses. In Fig. 3.5, 3.6, 3.7 and 3.8 we reported the attenuation for different night compared to wind speed and relative humidity at the transmitter (JKT) and at the receiver (OGS).

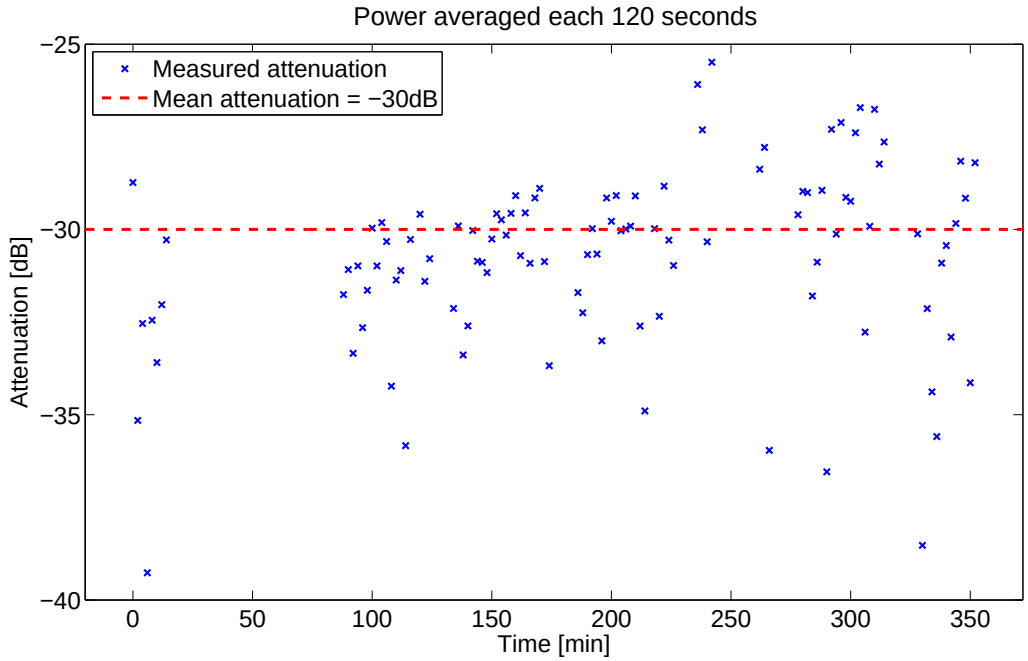
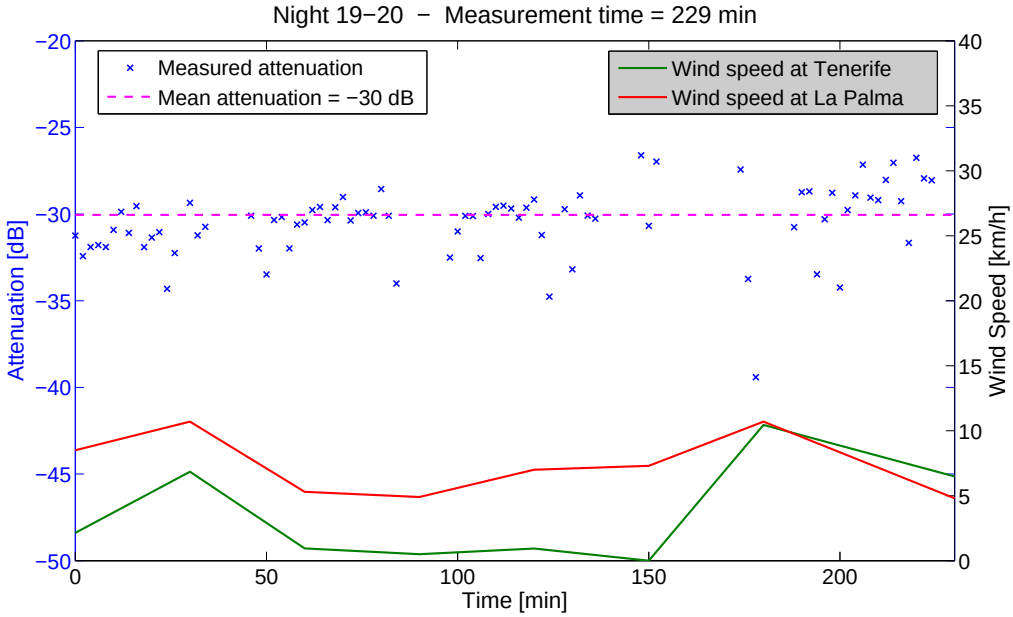
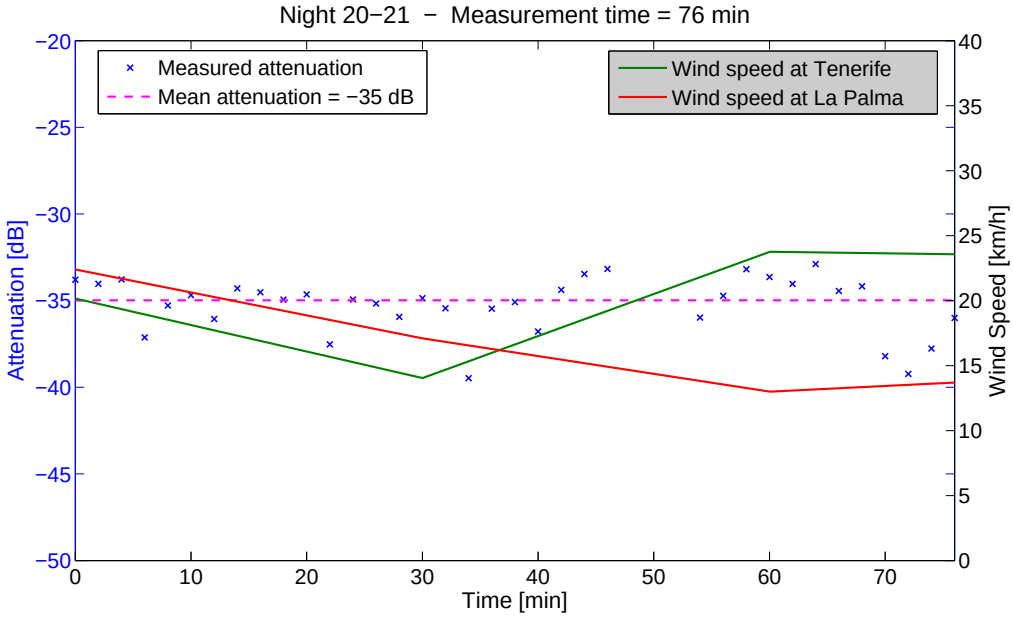


Figure 3.4: Measured attenuation averaged over 2 minutes. Red line states for the total average attenuation.



(a) Wind Speed vs Attenuation - Night 19-20



(b) Wind Speed vs Attenuation - Night 20-21

Figure 3.5: Measured attenuation compared with wind speed at the transmitter and the receiver.

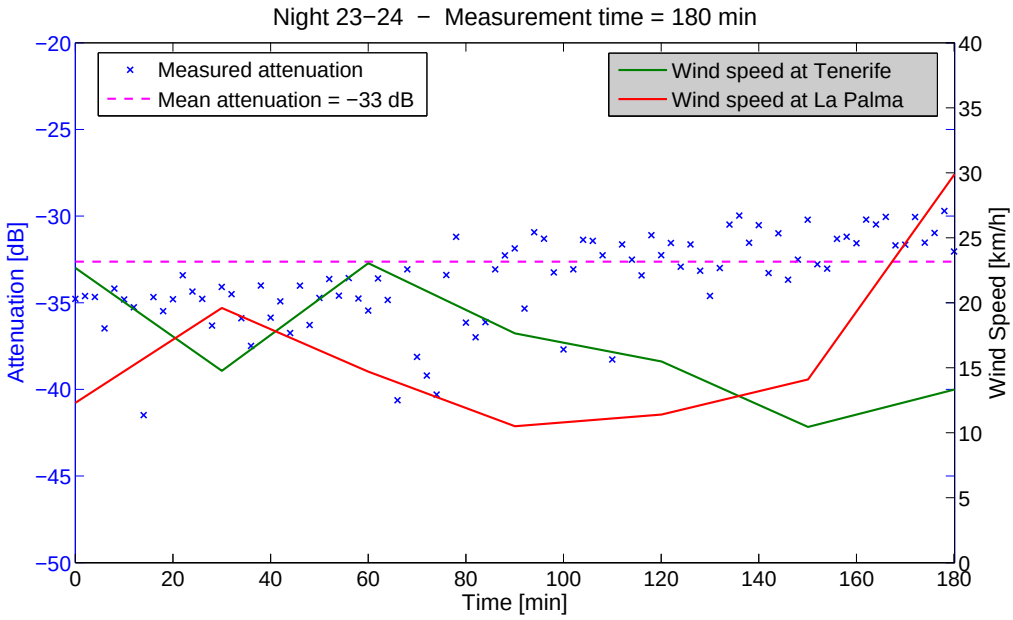


Figure 3.6: Measured attenuation compared with wind speed at the transmitter and the receiver - Night 23-24

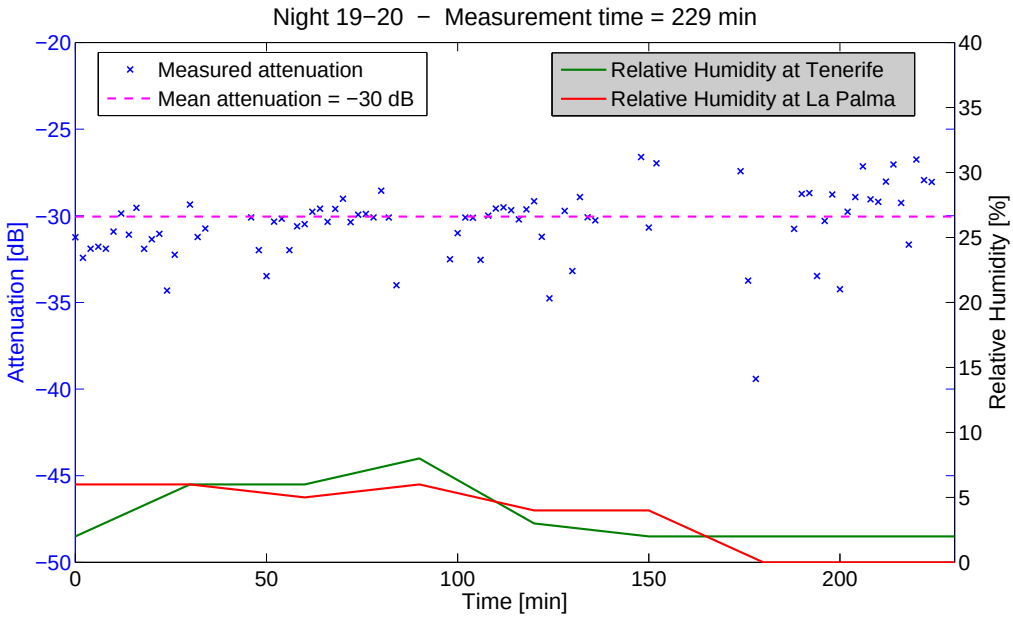
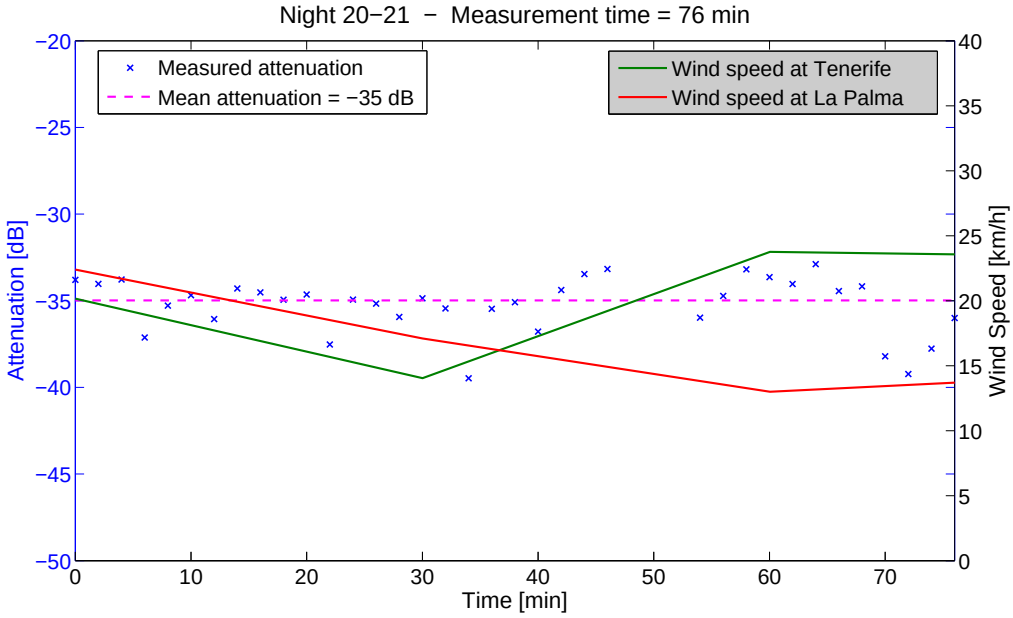
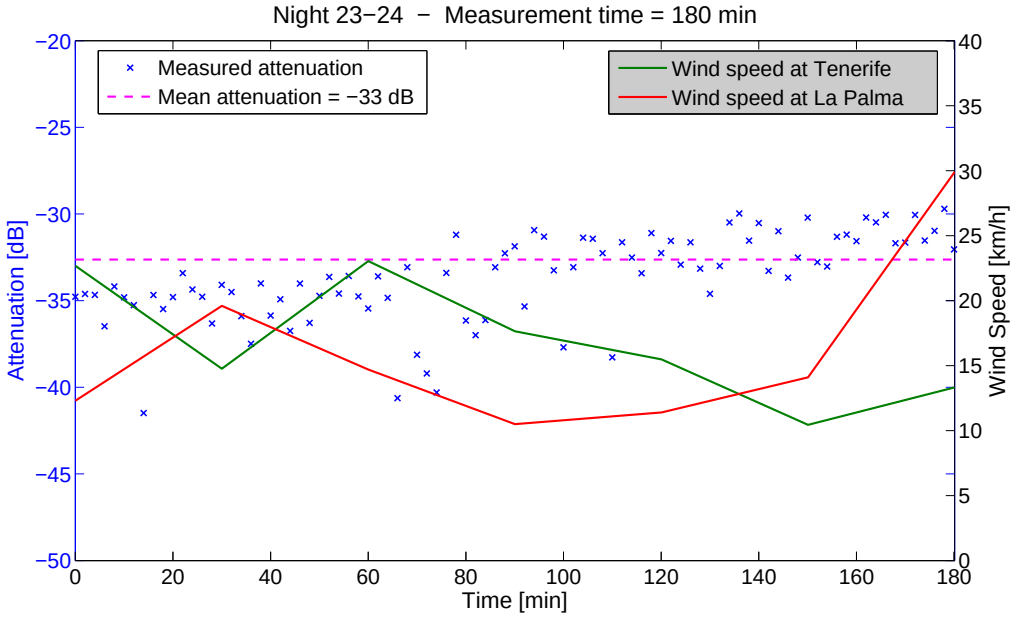


Figure 3.7: Measured attenuation compared with relative humidity at the transmitter and the receiver - Night 19-20



(a) Relative Humidity vs Attenuation - Night 20-21



(b) Relative Humidity vs Attenuation - Night 23-24

Figure 3.8: Measured attenuation compared with relative humidity at the transmitter and the receiver

3.5 Improving the Signal to Noise Ratio

For both quantum and classical communication, it is of paramount importance to achieve a high SNR. If a qubit state $|\Phi\rangle$ encoded in the photon polarization must be sent between two remote locations, it is possible to determine the effect of (white) noise on the polarization fidelity, which is defined as:

$$F = \langle\Phi|\rho|\Phi\rangle \tag{3.8}$$

where $|\Phi\rangle$ is the polarization state of the sent photon and ρ is the polarization density matrix of the received photon. Let us measure the SNR in dB, namely,

$$\mathrm{SNR} = 10\log_{10}\frac{N_s}{N_n} \tag{3.9}$$

where N_n is the average amount of noise (coming from dark detections or background radiation) and N_s is the average number of detected photons. It is easy to show that the fidelity depends on the SNR as

$$F = 1 - \frac{1}{2(10^{SNR/10})} \tag{3.10}$$

In fact, since the background photons are completely depolarized, the received quantum state can be written as

$$\rho = \frac{N_s - N_n}{N_s}|\Phi\rangle\langle\Phi| + \frac{N_n}{N_s}\frac{\mathbb{1}}{2} \tag{3.11}$$

In order to improve the SNR for the transmission of single photons in a long distance free-space link as the present one, which uses a 1 m optical receiver, out of this findings we can envisage the exploitation of the following procedure. With a given frequency (slower than the single photon transmission rate), the free-space channel is probed by means of a classical signal that gives the information of the instantaneous transmission of the channel. Only if the transmission is above a given threshold the single photon signal is acquired. It is crucial for the protocol to be efficient to correctly identify the "probing" frequency and the threshold to be used. This technique can also be used in the classical case, for instance, in on-off keying.

We report in Fig. 3.9 the frequency spectrum and the cumulative power spectrum of the data plotted in Fig. 3.2. The normalized plot of the power spectrum is

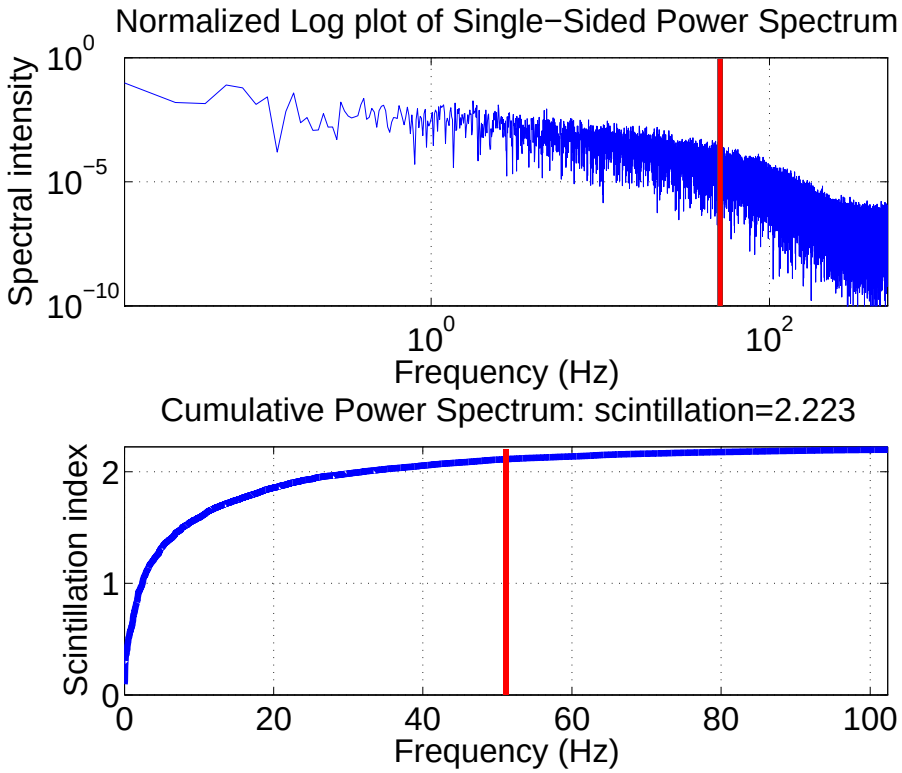


Figure 3.9: SPAD power spectrum and cumulative power spectrum. Frequency bound (red vertical line): The frequencies below 51 Hz contribute to 95% of the SI.

obtained by normalizing the intensities by the average $I' = I/\langle I \rangle$. The power spectrum is related to the SI as follows. We can write the set of (normalized) acquisitions as I'_k with $k = 0, \ldots, N-1$ and $N = 20\ s/20\ \mu s = 10^6$ the number of intensity acquisitions over 20 s. The Fourier components are given by

$$\tilde{I} = \sum_k I'_k \omega^{nk} \tag{3.12}$$

with $\omega = \mathrm{e}^{-(2\pi i/N)}$. By Parseval's theorem it is easy to show that the SI can be rewritten as:

$$\mathrm{SI} = \frac{2}{N^2} \sum_{n=1}^{N/2} |\tilde{I}_n|^2 \tag{3.13}$$

namely, it is the cumulative power spectrum without the zero frequency ($\tilde{I}_0$) component. We can notice that the frequencies contributing to the scintillation (up to 95%) are within (almost) 50 Hz. For frequencies above around 500 Hz, the spectrum becomes flat, indicating that at this frequency the random noise is dominant. The

typical fluctuations of the transmission channel due to turbulence are within 100 Hz (see Table 3.2). The frequency analysis of the temporal scintillation indicates that the probing frequency does not need to be higher than 1 KHz.

In order to obtain further evidence, we analysed the features of the counts above a given threshold of the signal reported in Fig. 3.2. By considering a threshold of 1, 2, 4, and 6 dB above the average, we considered the duration (in milliseconds) of events with overthreshold counting. The results are shown in Fig. 3.10. The probability of obtaining an event above a given threshold q_0 can be predicted from the lognormal distribution[1]:

$$p(q > q_0) = \frac{1}{2} - \frac{1}{2}\mathrm{erf}\left[\frac{\ln \frac{q_0}{\langle q \rangle} + \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right] \tag{3.14}$$

where $\mathrm{erf}(x)$ is the Gaussian error function $\mathrm{erf}(x) = (2/\sqrt{\pi}) \int_0^x \mathrm{e}^{-t^2}\, \mathrm{d}t$. Acquiring the single photon channel only if the probed transmission is above a given threshold implies an increase of the average photon counts in each time slot. It is possible to show that, by considering only the events in which the transmission satisfy $T > T_0$, the new mean value $\langle n \rangle_{thres}$ is

$$\frac{\langle n \rangle_{thres}}{\langle n \rangle} = \frac{1 - \mathrm{erf}\left[\frac{\ln \frac{T_0}{\langle T \rangle} - \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right]}{1 - \mathrm{erf}\left[\frac{\ln \frac{T_0}{\langle T \rangle} + \frac{1}{2}\sigma^2}{\sqrt{2\sigma^2}}\right]} > 1 \tag{3.15}$$

Clearly, this threshold selection increases the SNR but at the same time decreases the overall counts in a given time. In Fig. 3.11, we show the increase (in decibels) of the SNR and the percentage of the overall counts that will be detected. In cases of strong turbulence and high noise, this technique could help the qubit transmission by "exploiting turbulence", namely, considering only the particular moments in which the turbulence increases the channel transmission.

[1]Here the Mandel distribution was replaced with the lognormal distribution

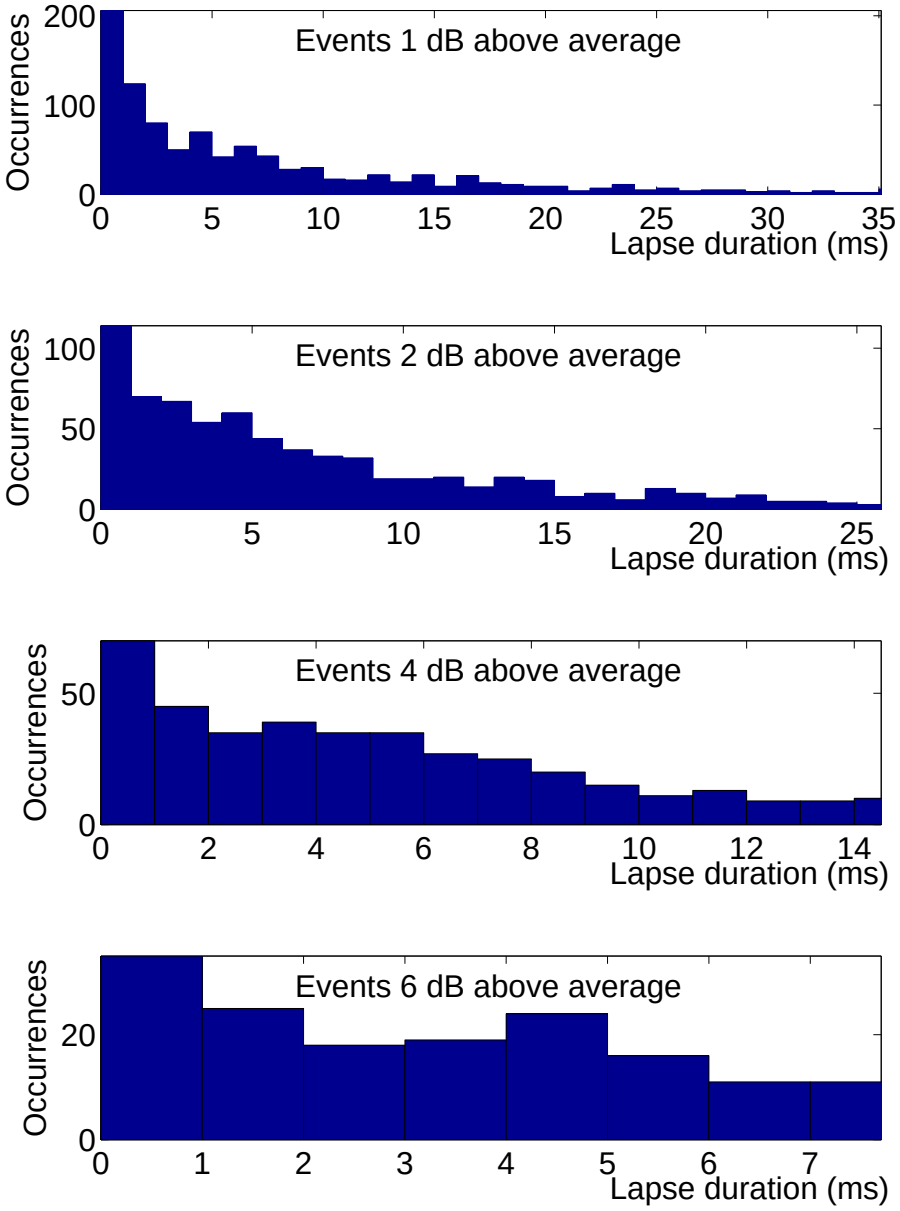


Figure 3.10: Duration (in milliseconds) of events with overthreshold counting. In the different plots we considered a threshold of 1, 2, 4, and 6 dB above the average.

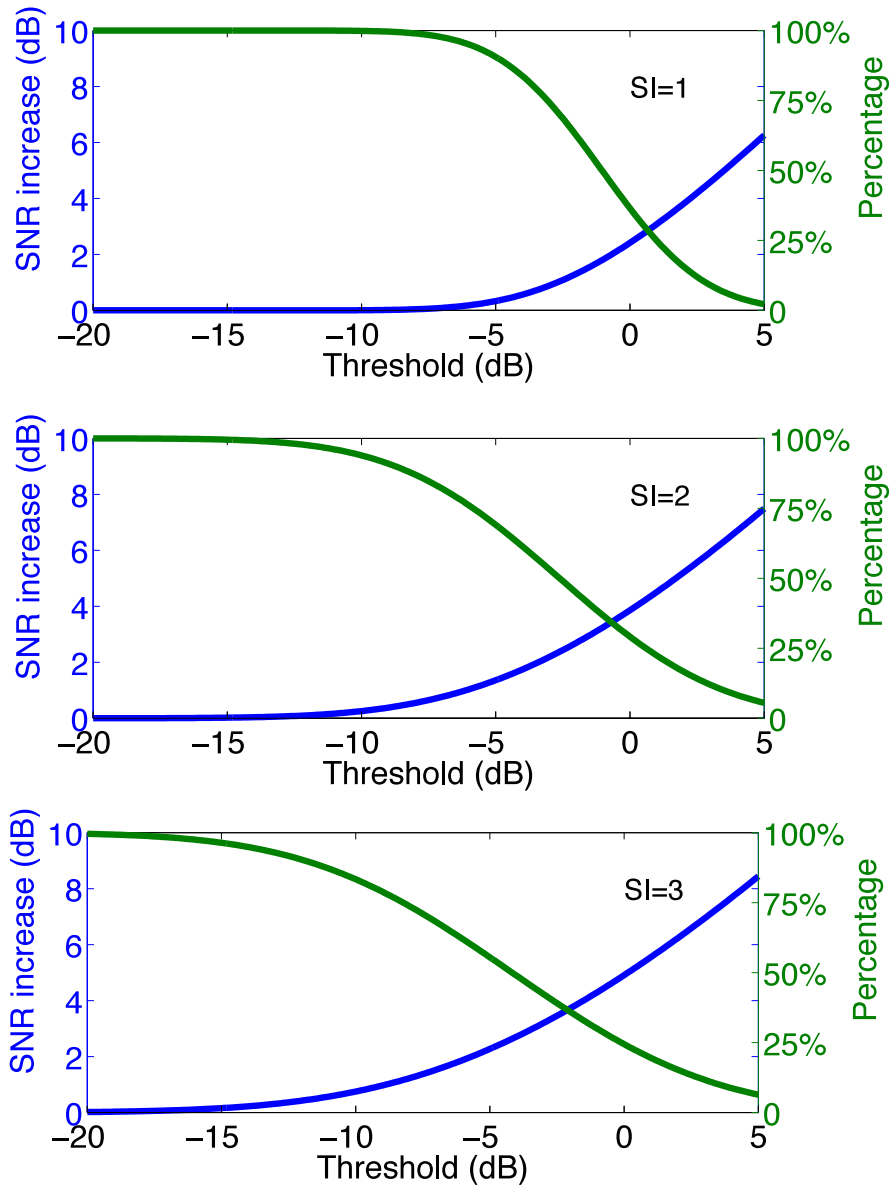


Figure 3.11: SNR and the percentage of the overall counts that will be detected in the function of the threshold selection.

3.6 Conclusions

In this chapter we studied the effect of atmospheric turbulence on the statistic of arrival of single photons over a free-space 143 km optical link, demonstrating the transformation from Poissonian to lognormal distribution. We also carried out the analysis of the temporal losses in order to improve the SNR of the channel. The evidence of consecutive sub-intervals of low losses allow us to envisage the exploitation of turbulence as a SNR improvement technique.

CHAPTER 4

Device-independent Quantum Key Distribution

Quantum Key Distribution (QKD) is a method that allows two distant parties, Alice and Bob, to share secure keys. It makes use of a quantum channel (typically optical) and an authenticated classical channel. Since the first QKD protocol proposed by Bennet and Brassard (Bennet-Brassard 84 [1] (BB84)), many security proofs were carried out [52–55], including also finite-size key demonstrations [56, 57].

Great importance in this last years has been devoted to the so-called device independent-Quantum Key Distribution (DI-QKD) protocols [58]. Unlike typical QKD protocols, in a device-independent scenario the security assumptions are not related to the internal working of the used quantum devices but are based on the violation of a Bell's inequality.

A fundamental part of the QKD protocols is data processing that permits to distill a secure key from the transmitted raw key. In this chapter we first consider the main structure of this processing as explained in [59], hence we present a brief description of DI-QKD protocols. Therefore, we analyse in detail a QKD protocol and its implementation in a one-side device independent-Quantum Key Distribution (1SDI-QKD) scenario [60]. We then present a version of the Bennet 92 [2] (B92) protocol implemented with non-maximally entangled states(NMESs) [25]. This kind of implementation offers some advantages regarding efficiency and key rate with respect to DI-QKD protocols realized with maximally entangled states. Starting from this protocol we propose its generalizations and analyse its secret key rate

when detection inefficiencies are taken into account. This theoretic results are also published in [J2].

4.1 Data processing of a QKD protocol

Typical QKD protocols involve two phases: the physical phase in which a key is shared between the two distant parties by means of quantum signals (typically photons) and the data processing phase that enables to obtain secure keys. By definition a secure key has to be **identical** between Alice and Bob (respectively the transmitter and the receiver) and **private**, i.e. unknown to a possible eavesdropper (Eve). Data processing can typically be divided in three steps:

- **sifting process:** in which Alice and Bob select the data received correctly, it always needs two-way communication;
- **error correction:** thanks to which the keys shared became identical;
- **privacy amplification:** after which the key is private, namely the information owned by a third party is equal to zero.

The main goal of a QKD protocol is to maximize the rate of the secure key, in fact every step of the data processing reduces the size of the raw key making the final key much smaller than the initial one. There exist many security proofs for QKD protocols, usually these are referred to the infinite key limit case. For a generic QKD protocol the length of secure key rate can be lower bounded by:

$$R_{\text{inf}} \geq H(\mathbf{A}) - fH(\mathbf{A}|\mathbf{B}) - I_{pa} \tag{4.1}$$

where $H(\mathbf{A})$ is the Shannon entropy of Alice's data after the sifting. $H(\mathbf{A}|\mathbf{B})$ is the error correction term, that is the minimum number of bits that Alice has to send to Bob in order for him to be able to correct his data to match Alice's data. The f term is the efficiency of error correction protocol that usually is greater than 1. The last term I_{pa} is related to the privacy amplification process, and takes into account the information gained by Eve. The form of I_{pa} depends on many factors, in particular the security definition and the security proof technique. This latter is

the reason why the secret key rate is lower bounded, in fact any valid security proof guarantees that at least this amount of secret key can be extracted from the raw key.

4.2 Device independent protocols

The aim of DI-QKD protocols is to generate secret keys between two parties without making any assumption about the implementation of their devices. These protocols are divided into 1SDI-QKD when only one of the two devices is trusted and fully DI-QKD when both devices are untrusted. Since in DI-QKD protocols one or both the quantum apparatuses are non trusted, they can be seen as black boxes with some classical inputs and some classical outputs. In figure 4.1 it is possible to see different QKD protocol scenarios.

In usual QKD protocols two parties named Alice and Bob receive entangled particles from a common source which is not trusted by the parties. By making random measurements on the particles and by comparing some results, Alice and Bob can estimate if the source is controlled by an eavesdropper or not. In a DI-QKD scenario Alice and Bob would not trust only the source but also their devices.

The DI-QKD protocols represent a relaxation of the security assumptions of usual QKD protocols. The minimal set of required security assumption for DI-QKD protocols are:

- the physical location of Alice and Bob are secure
- they own a quantum random generator
- they have trusted classical device for key processing
- they share an authenticated public channel
- Quantum Mechanics is a valid and complete theory

The security of the DI-QKD is proven by means of the Bell's inequality, in fact the violation of this inequality guarantees the secrecy of the communication. Non-locality is not only a necessary condition for the security of these protocols but is

the physical principle which all device-independent security proofs are based on. For the 1SDI-QKD case the security requirements are less stringent since it is sufficient the violation of a steering inequality.

A very detailed review on DI-QKD protocols can be found in [58].

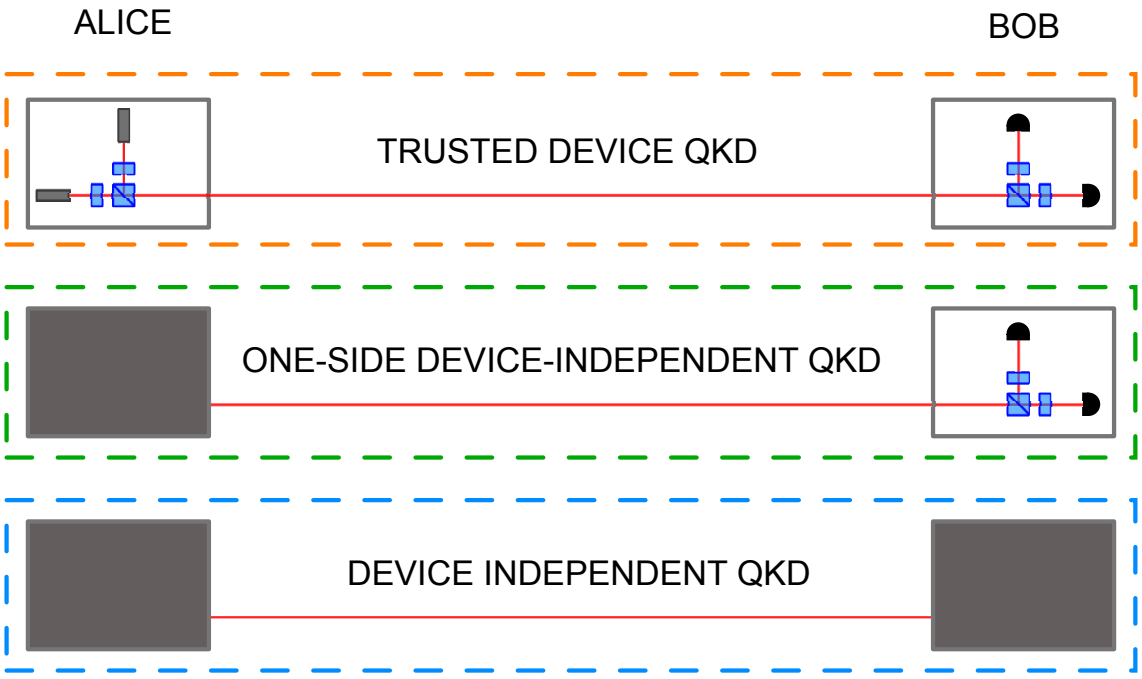


Figure 4.1: Schematic representation of different QKD scenarios.

4.2.1 Bell's inequalities

In 1935, in their famous article [62], Einstein, Podolsky and Rosen formulated the so-called *Einstein Podolsky Rosen (EPR) paradox* in which they stated that Quantum Mechanics is not a complete theory and therefore there exists some kind of "hidden variables" which were not taken into account. In 1964 John Bell expressed a mathematical model to demonstrate the implicit assumption of the EPR paradox [63], meaning that physic world should be characterized by realism and locality. Bell introduced an inequality based on physical measurements made by observers on pairs of particles which have interacted and then separated. This inequality is true for any local realistic theory; on the other side is violated by Quantum Mechanics predictions. In 1969 Clauser, Horne, Shimony and Holt proposed a generalization

of original Bell's inequality with four correlation measurements [64]. The Clauser Horne Shimony Holt (CHSH) inequality is defined as:

$$S(a, a', b, b') = E(a, b) - E(a', b) + E(a, b') + E(a', b') \tag{4.2}$$

where E is the correlation between the measurements of the pair of particles and a, a', b, b' are referred to arbitrary angles of measurement. It can be shown that for any realistic local theory the CHSH inequality holds:

$$|S(a, a', b, b')| \leq 2 \tag{4.3}$$

whereas quantum mechanics expected to violate it. Therefore the CHSH inequality and more in general any Bell-like inequality represents a Quantum Mechanics test against classical hidden-variable theories. There exists many experimental violation of the Bell's inequalities and recently detection loophole-free violations of the CHSH inequality by non-maximally entangled photons were indeed performed [16, 17].

4.3 One-side device independent BBM92 protocol

We consider a modified version of the B92 protocol with entangled photons proposed by [60], in which both parties, Alice and Bob, receive some entangled pairs from an external source. Alice can choose between two measurement basis, A_0 and A_1, therefore she has two possible outputs for each pair, however she does not trust her device so she considers it as a black box. On the other side Bob trusts his measurement device to make two projective measurements B_0 and B_1 typically corresponding to the Pauli operators σ_x and σ_z. After Alice and Bob made their measurement they use the conclusive results from A_0 and B_0 to extract the raw key while the measurement in A_1 and B_1 basis will be used to perform the security test.

Alice and Bob have to deal with the losses and the inefficiencies of the detectors because of whom they not always detect the photons generated by the source. Alice can not simply discard no-detection events because she has an untrusted device and the eavesdropper Eve could control her detectors and influence the measurement results. Bob instead can consider only the detection event since he trust his device

can not be controlled by Eve. If N is the length of the raw keys $\mathbf{A}_0$ and $\mathbf{B}_0$, after the post selection process Alice and Bob will have two strings of bits $\mathbf{A}_0^{\mathbf{ps}}$ and $\mathbf{B}_0^{\mathbf{ps}}$ with length $n \leq N$.

4.3.1 Security proof and key rate

As proposed recently by Tomamichel, Renes, Lim, Gisin and Renner in [56, 61, 65] the length of the final secret key can be bounded by:

$$\ell \geq H_{min}(\mathbf{B}_0^{\mathbf{ps}}|E) - H(\mathbf{B}_0^{\mathbf{ps}}|\mathbf{A}_0^{\mathbf{ps}}) \tag{4.4}$$

where $H_{min}(\mathbf{B}_0^{\mathbf{ps}}|E)$ is the *smooth min-entropy* [66] of $\mathbf{B}_0^{\mathbf{ps}}$ conditioned to Eve's information. The error correction term is equal to:

$$H(\mathbf{B}_0^{\mathbf{ps}}|\mathbf{A}_0^{\mathbf{ps}}) = nh_2(Q_0^{\mathrm{ps}}) \tag{4.5}$$

where h_2 is the binary entropy function: $h_2(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$ and Q_0^{ps} is the bit error rate between $\mathbf{A}_0^{\mathbf{ps}}$ and $\mathbf{B}_0^{\mathbf{ps}}$. As demonstrated in [60], by using the chain rule and the data-processing inequality for smooth min-entropies [65, 67], it is possible to bound Eve's information on the sifted bits by using her information on Bob's raw key $\mathbf{B}_0$:

$$H_{min}(\mathbf{B}_0^{\mathbf{ps}}|E) \geq H_{min}(\mathbf{B}_0|E) + N - n \tag{4.6}$$

When performing the security test Alice and Bob measure in the A_1 and B_1 basis obtaining two strings of bits $\mathbf{A}_1$ and $\mathbf{B}_1$. From the generalized uncertainty relation in [68] we have:

$$H_{min}(\mathbf{B}_0|E) \geq qN - H_{max}(\mathbf{B}_1|\mathbf{A}_1) \tag{4.7}$$

where q is the orthogonality of the measurement basis B_1, for orthogonal measurements $q = 1$. The term $H_{max}(\mathbf{B}_1|\mathbf{A}_1)$ is the *smooth max-entropy* [66] of $\mathbf{B}_1$ conditioned on $\mathbf{A}_1$ and according to [56] satisfy the following:

$$H_{max}(\mathbf{B}_1|\mathbf{A}_1) \lesssim Nh_2(Q_1) \tag{4.8}$$

where Q_1 is the bit error rate between $\mathbf{A}_1$ and $\mathbf{B}_1$. Substituting (4.6), (4.7) and (4.8) in equation (4.4) we have:

$$\ell \gtrsim n\left[1 - h_2(Q_0^{\mathrm{ps}})\right] - N\left[h_2(Q_1) + 1 - q\right] \tag{4.9}$$

We denote $\eta_A = n/N$ as the fraction of photons detected by Alice respect to Bob detections. Therefore, the final secret key rate $r = l/N$, which is the the number of secret bits obtained per photon detected by Bob, is equal to:

$$r \geqslant \eta_A \left[1 - h_2(Q_0^{\text{ps}})\right] - h_2(Q_1) - (1 - q) \tag{4.10}$$

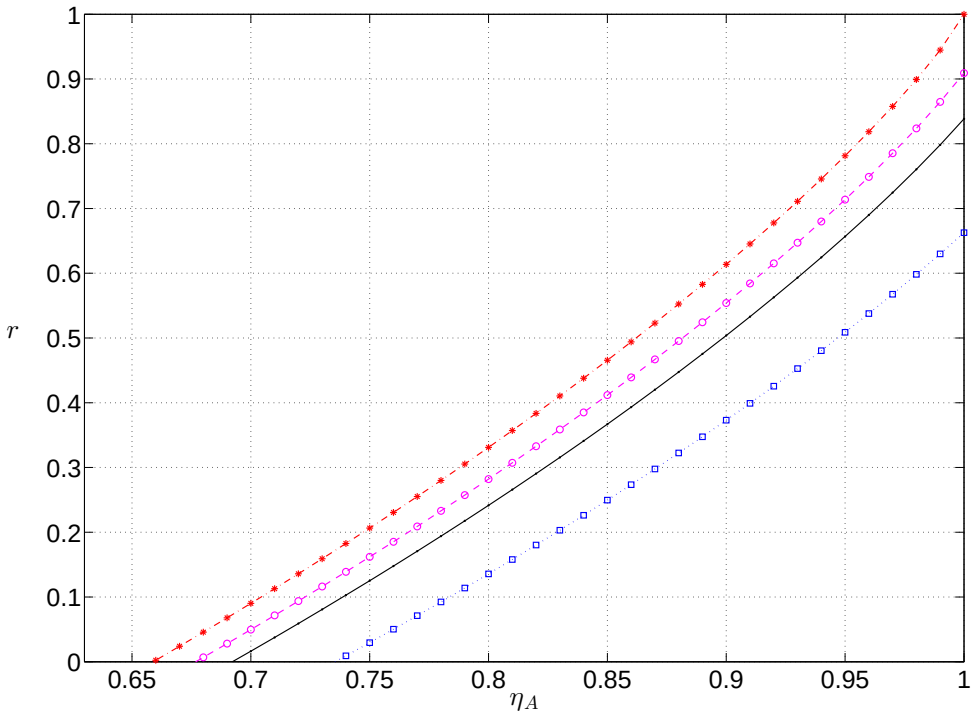


Figure 4.2: Secure key rate (4.10) as a function of Alice's detection efficiency, for visibilities $V = 1, 0.99, 0.98, 0.95$ (from top to bottom) and $q = 1$

4.3.2 Feasibility analysis

It will be considered now a typical experimental setup where Alice and Bob receive maximally-entangled photons from a source through a depolarizing channel with visibility V. As in BBM92 protocol (see 4.3) the measurement basis are $A_0 = B_0 = \sigma_z$ and $A_1 = B_1 = \sigma_x$ and quantum bit error rates(QBERs) are equal to:

$$Q_1^{\text{ps}} = (1 - V)/2, \qquad Q_2 = (1 - \eta_A V)/2 \tag{4.11}$$

In figure (4.2) is reported the values of the bound (4.10) as a function of η_A, and for different values of V. With perfect visibility $V = 1$ it is possible to have positive secret key rates for $\eta_A > 65.9\%$. This bound is lower than those required for fully device independent QKD, this is related to the fact that it is much easier to close the detection loophole with a steering equipment than in a Bell test.

It is interesting to note that for the one side device independent case the losses between the source and Bob's apparatus do not affect the security of the protocol (since Bob is trusted). Thus, in principle it is possible to reach long distances if Alice is close to the source of entangled photons.

4.4 ent-B92 QKD protocol

Entangled-based Bennet 92 QKD protocol (ent-B92) is a protocol proposed in [25] which is based on the implementation of the standard B92 protocol with NMESs. The configuration of the protocol is very similar to the one proposed in the section above 4.3, but the use of NMESs instead of maximally entangled ones gives some advantages that will be described below.

Let's now consider Alice and Bob sharing the following NMES:

$$|\Phi\rangle_{AB} = \cos\frac{\theta}{2}|H\rangle_A|H\rangle_B + \sin\frac{\theta}{2}|V\rangle_A|V\rangle_B \tag{4.12}$$

where $|H\rangle$ and $|V\rangle$ are the horizontal and vertical polarization states and $0 < \theta \leq \pi/2$. The parameter θ is monotonically related to the amount of entanglement. The protocol works as follow: Alice measures with low probability $p \ll 1$ its photon along the $A_1 = \{|a_1\rangle, |\overline{a}_1\rangle\}$ basis, with $|a_1\rangle = |V\rangle$ and $|\overline{a}_1\rangle = |H\rangle$. With high probability $1-p$ she measures along the $A_0 = \{|a_0\rangle, |\overline{a}_0\rangle\}$ basis, where $|a_0\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle$ and $|\overline{a}_0\rangle$ is its orthogonal state; Bob randomly and with probability 1/2 measures the incoming states in the B_0 or B_1 basis where $B_k = \left\{|b_k\rangle, |\overline{b}_k\rangle\right\}$ and

$$\begin{aligned} |b_k\rangle &= \sin\tfrac{\varphi}{2}|H\rangle - (-1)^k\cos\tfrac{\varphi}{2}|V\rangle \\ |\overline{b}_k\rangle &= \cos\tfrac{\varphi}{2}|H\rangle + (-1)^k\sin\tfrac{\varphi}{2}|V\rangle \end{aligned} \tag{4.13}$$

In figure 4.3 it is presented the scheme for ent-B92 protocol. The results from Alice's A_0 basis measurements are used as bits of the raw key together with Bob's results,

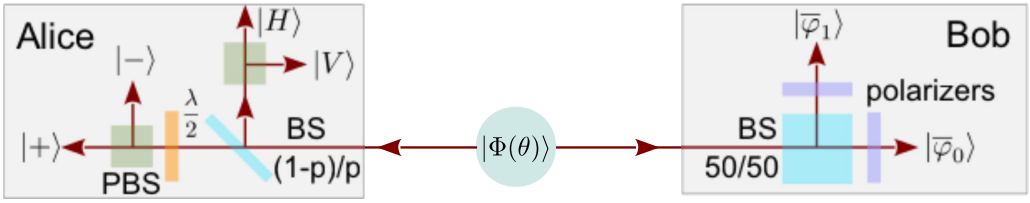


Figure 4.3: Scheme of the ent-B92 protocol

while those from the A_1 basis will be used to perform a test against the eavesdropper attack, as in the unconditionally secure - B92 protocol (us-B92) [69]. On Alice's side, the states $|a_0\rangle$ and $|\overline{a}_0\rangle$ correspond to bits 0 and 1 respectively. Upon obtaining the state $|b_k\rangle$ Bob decodes Alice's bit as $j = k \oplus 1$ (the symbol $\oplus$ means "addition modulo 2") and labels the result as *conclusive*; on the contrary, upon obtaining the state $|\overline{b}_k\rangle$, Bob labels the result as *inconclusive*. The probability of a conclusive event is given by

$$P_{conc} = \frac{1}{2}\left(1 - \cos\theta\cos\varphi\right) \tag{4.14}$$

that is independent on Alice's measurements. The sifted key is obtained by selecting the conclusive results corresponding to Alice's A_0 measurements. The so-called ent-B92 protocol described in [25] corresponds to the choice $\varphi = \theta$. The theoretical QBER, defined as the ratio of the number of errors over the number of conclusive outcome, can be calculated as

$$Q_{th} = \frac{n_{err}}{n_{conc}} = \frac{1 - \cos(\theta - \varphi)}{2 - 2\cos\theta\cos\varphi} \tag{4.15}$$

and the choice $\varphi = \theta$, used in the ent-B92 protocol, gives null QBER.

4.4.1 Security proofs of ent-B92 QKD protocol

For the derivation of the secure key rate it is considered a general case in which both Alice and Bob can have inefficiencies. Let's consider a transmission with $\mathcal{N}$ pairs where Alice choose the A_0 basis and Bob chooses with probability 1/2 the basis B_0 or B_1. The ± 1 outputs of Alice's measurement correspond to bit 1 and 0 of the sifted key. On Bob's side, only $+1$ outputs, the so called conclusive outcomes, are taken into account to build the key: thus, on Bob side, non-detection event will be associated to -1 output (corresponding to non-conclusive outcomes). Then, all the

Alice's bits corresponding to non-conclusive Bob's outcome, can be simply discarded as it is usually done in the sifting phase of the BB84 protocol.

If the efficiencies are given by η_A and η_B, Bob receives $\mathcal{N}P_c\eta_B$ conclusive counts and Alice obtains $\mathcal{N}\eta_A$ detections where P_c is the probability of obtaining a Bob conclusive outcome in case of perfect detection efficiency, defined in (4.14). Alice and Bob will perform a post-selection on the conclusive events, by selecting the bits in which Alice obtained a physical detection: then the number of bits of the final sifted key is given by $\mathcal{N}P_c\eta_A\eta_B$. Let's call $\mathbf{A^{ps}}$ and $\mathbf{B^{ps}}$ the Alice and Bob strings of bits after the post selection, while $\mathbf{B}^c$ is the original Bob's string of conclusive outcomes. The equation of the length of the secure key rate can be derived from (4.4):

$$\ell \geq H_{min}(\mathbf{B^{ps}}|E) - H(\mathbf{B^{ps}}|\mathbf{A^{ps}}) \tag{4.16}$$

The term related to error correction is now equal to:

$$H(\mathbf{B^{ps}}|\mathbf{A^{ps}}) = \mathcal{N}P_c\eta_A\eta_B h_2(Q^{ps}) \tag{4.17}$$

The relation between smooth min-entropies defined in (4.6) can be now rewritten as:

$$H_{min}(\mathbf{B^{ps}}|E) \geq H_{min}(\mathbf{B}^c|E) - \mathcal{N}P_c\eta_B(1-\eta_A) \tag{4.18}$$

where $\mathcal{N}P_c\eta_B(1-\eta_A)$ is the difference between the $\mathbf{B}^c$ and $\mathbf{B^{ps}}$ string length. As shown in [68], the min-entropy can be related to the maximal probability of guessing the key bits, namely

$$H_{min}(\mathbf{B}^c|E) = -\mathcal{N}P_c\eta_B \log_2 P_{guess}(\mathbf{B}^c|E) \tag{4.19}$$

By using the results of [70], the probability of guessing the bits can be related to the Bell's inequality by

$$P_{guess}(\mathbf{B}^c|E) \leq \frac{1}{2}\left[1 + \sqrt{1 - 4S_{\mathrm{CH}} - 4S_{\mathrm{CH}}^2}\right] = \frac{f(S_{\mathrm{CH}})}{2} \tag{4.20}$$

where S_{CH} is the Clause-Horne (CH) parameter:

$$S_{\mathrm{CH}} = P(a_1b_1) + P(a_0b_1) + P(a_1b_0) - P(a_0b_0) - P(a_1) - P(b_1) \tag{4.21}$$

In the previous expression $P(a_i, b_j)$ is the joint probability that Alice measures the state $|a_i\rangle$ and Bob detects the state $|b_i\rangle$, while $P(a_1)$ and $P(b_1)$ are the probabilities

that Alice and Bob respectively measure $|a_1\rangle$ and $|b_1\rangle$, regardless of what is measured by the other user. The final secure key length can be thus written as

$$\ell \geq \mathcal{N} P_c \eta_B \left[\eta_A (1 - h_2(Q^{\rm ps})) - \log_2 f(S_{\rm CH})\right] \tag{4.22}$$

and the final rate $r = \ell/\mathcal{N}$ is given by

$$r = \eta_B P_c \left[\eta_A (1 - h_2(Q^{\rm ps})) - \log_2 f(S_{\rm CH})\right] \tag{4.23}$$

as usual the $h_2(Q^{\rm ps})$ corresponds to the bits used for error correction, while the $\log_2$ contribution is related to Eve's knowledge on the key and the required compression in the privacy amplification stage. In case of standard QKD (corresponding to $\eta_A = \eta_B = 1$), the achievable rate with the ent-B92 protocol (corresponding to $\varphi = \theta$), is shown in Fig. 4.4 with the maximum rate obtained for $\theta \simeq 65.28°$. By using the angle that maximizes the violation of the Bell inequality ($\varphi = \arctan(\sin\theta)$) it is possible to improve the rate when $\theta \gtrsim 71.62°$ (see Fig. 4.4). More generally, it is possible to numerically optimize the value of the parameter $\varphi = \varphi^\star(\theta)$ as a function of θ to maximize the achievable rate, as shown with dashed line in Fig. 4.4. Note that, whenever $\varphi \neq \theta$, the theoretical QBER is not vanishing: however, the non-vanishing QBER can be compensated by a larger violation of the CH inequality, allowing more secrecy in the privacy amplification stage. The rate in (4.23) can be compared to the one obtained with the post-selection technique in section (4.3) using the usual DI-QKD protocol of [70] implemented with maximally entangled states:

$$r' = \left[\eta_A \eta_B (1 - h_2(Q^{\rm ps})) - \log_2 f(S_{\rm CH})\right] \tag{4.24}$$

The difference between r and r' arises from the fact the in the BBM92 protocol the key is obtained by using the results of Bob in a single basis, while in the generalized ent-B92 protocol the key is obtained by keeping the Bob's conclusive results in the basis B_0 and B_1. It is also useful to compare the equation (4.23) with the one proposed in [25], where the key rate of the ent-B92 protocol was given as

$$\tilde{r} = \eta_A \eta_B P_c \left[1 - h_2(Q) - \log_2 f(S_{\rm CH})\right] \tag{4.25}$$

where now the QBER Q must be evaluated over all conclusive events. When Alice and Bob do not get a detection they must decide which value should outcome:

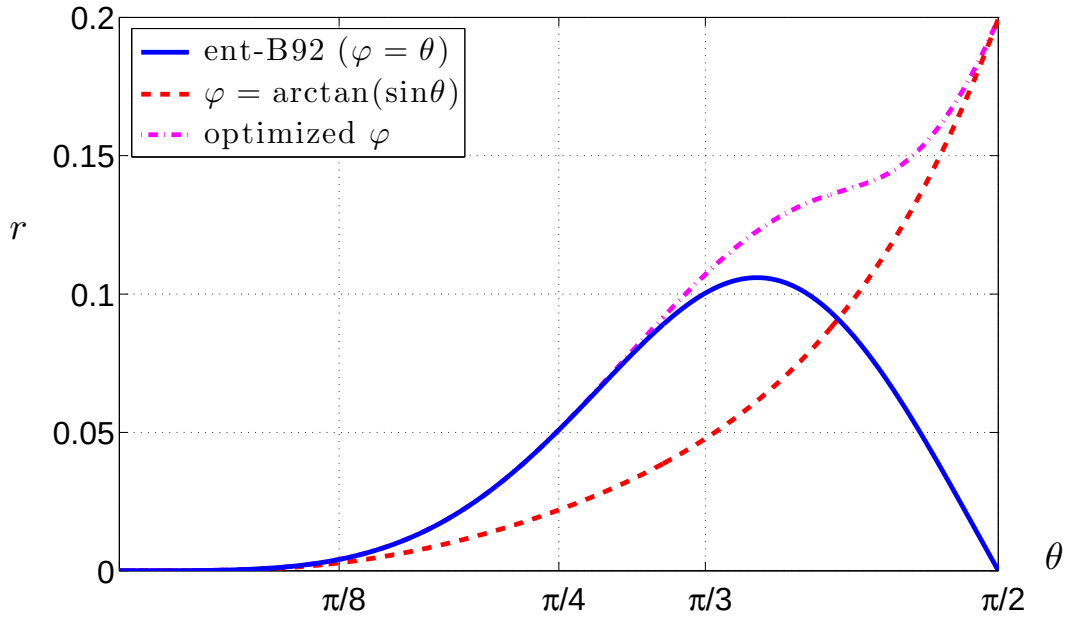


Figure 4.4: Theoretical secure key rate r for the generalized ent-B92 protocol, in case of perfect detection efficiencies ($\eta_A = \eta_B = 1$)

discarding the data is in fact equivalent to the fair sampling assumption in Bell's inequalities. If Bob assign to non-detection events the $|\overline{b}_k\rangle$ outcomes, the non-detection events do not contribute to the key, since only $|b_k\rangle$ outcomes will be contained in the key. When Alice measure the A_1 basis, on the other side, whatever value she decides to output, the bit will enter into the key. If Alice assigns to non-detection events the $|a_1\rangle$ or $|\overline{a}_1\rangle$ outcomes with probability 1/2, the QBER of the sifted key will be

$$Q = \eta_A Q^{\mathrm{ps}} + \frac{1-\eta_A}{2} \tag{4.26}$$

It is easy to show that the rate $\tilde{r}$ (4.25) is lower than the rate r (4.23) achievable with the post-selection technique in the fully DI-QKD scenario, while $\tilde{r} = r$ in the one-side device independent-Quantum Key Distribution (1SDI-QKD) scenario with Alice's trusted device.

4.4.2 Clause-Horne inequality

The theoretical value of the CH parameter S_{CH} (4.21) for the NMES (4.12) and for the measurement defined in (4.13) is given by

$$S_{\mathrm{CH}}(\theta, \varphi) = \frac{1}{2}\left(\cos\varphi + \sin\theta \sin\varphi - 1\right) \tag{4.27}$$

The choice of ent-B92 protocol $\varphi = \theta$ gives the following expression for the CH inequality:

$$S_{\mathrm{CH}}(\theta) = \frac{1}{2}\cos\theta\left(1 - \cos\theta\right) \tag{4.28}$$

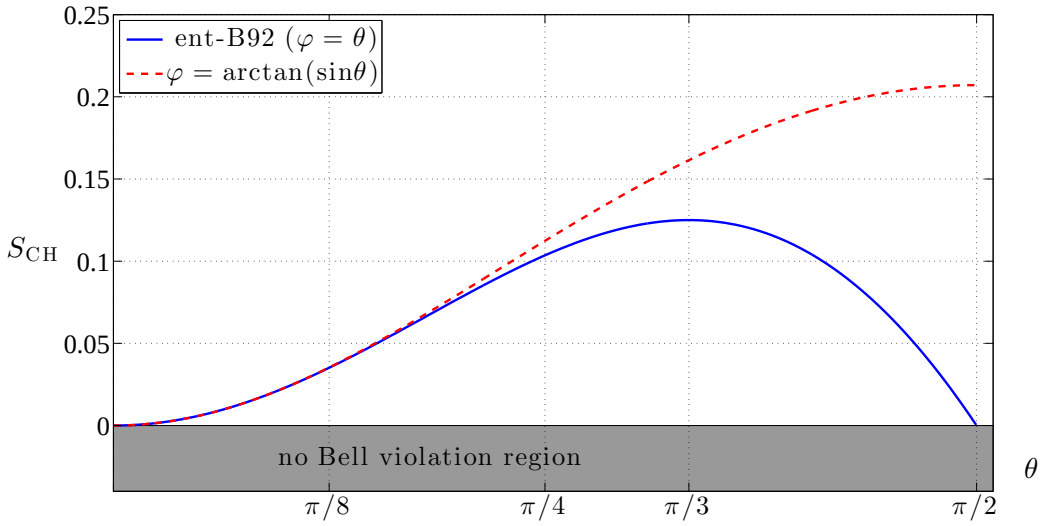


Figure 4.5: Plot of S_{CH} as a function of θ; red dashed line for ent-B92 protocol, blue solid line for $\varphi = \arctan(\sin\theta)$ protocol.

Figure (4.5) shows the value of S_{CH} as a function of the angle θ; in red dashed line is plotted the value obtainable with the expression above. As we can see the CH parameter is positive in the interval $0 < \theta < \pi/2$, i.e. it violates the Bell's inequality for the same interval of θ in which the ent-B92 protocol is defined. The maximum of the function is approximately at $\pi/3$, corresponding to $S_{\mathrm{CH}} = 1/8$, and it reaches the zero for $(\theta = 0)$ and $(\theta = \pi/2)$, respectively when the state (4.12) is separable and when is maximally entangled. However the choice of ent-B92 protocol does not

give the maximum achievable violation, the best choice is for $\varphi = \arctan(\sin\theta)$ that gives

$$S_{\mathrm{CH}}^{max}(\theta) = \frac{1}{2}\left(\sqrt{\sin^2\theta + 1} - 1\right) \tag{4.29}$$

In figure 4.5 S_{CH}^{max} is represented in solid blue line, the maximum is now at $\theta = \pi/2$ and it reaches the zero value when the state is separable $\theta = 0$, as we expected. The violation of the CH inequality $S_{\mathrm{CH}} \leq 0$ can be then used as a test against the local-realism of quantum physics: it can be trivially checked that, when the inequality is not violated, the secure rate (4.23) is zero. Further, if the key rate (4.23) is negative, no secure key can be distilled.

4.4.3 Detection efficiency

The main problem of the fully DI-QKD is related to the so-called detection loophole, namely the fact that the photon detection is inefficient and, if the detectors are not trusted, an eavesdropper can exploit this inefficiency to gain information on the key. In case of detection inefficiencies η_A and η_B we can predict the values of each probability of the CH parameter 4.21. In the generalized ent-B92 protocol, non-detection events are associated to the states $|\overline{a}_1\rangle$, $|\overline{b}_0\rangle$ and $|\overline{b}_1\rangle$ with the observables A_1, B_0 and B_1. Then the probabilities P can be predicted as:

$$\begin{aligned} P(a_1, b_1) &= \eta_A\eta_B p(a_1b_1), \quad P(a_1) \;\; = \eta_A p(a_1) = \eta_A\left[p(a_1b_0) + p(a_1\overline{b}_0)\right] \\ P(a_1, b_0) &= \eta_A\eta_B p(a_1b_0), \quad P(b_1) \;\; = \eta_B p(b_1) = \eta_B\left[p(a_0b_1) + p(\overline{a}_0b_1)\right] \end{aligned} \tag{4.30}$$

where $p(a_ib_j)$ are the probabilities normalized on the post-selected events in which Alice and Bob have a coincidence. On the other side, when measuring the A_0 observable, it is necessary to remember that the state $|\overline{a}_0\rangle$ is randomly chosen, with probability 1/2, in case of non-detection. Then

$$\begin{aligned} P(a_0, b_0) &= \eta_A\eta_B p(a_0b_0) + (1-\eta_A)\eta_B\frac{1}{2}p(b_0) \\ &= \eta_A\eta_B p(a_0b_0) + (1-\eta_A)\eta_B\frac{1}{2}\left[P(a_0b_0) + p(\overline{a}_0b_0)\right] \\ P(a_0, b_1) &= \eta_A\eta_B p(a_0b_1) + (1-\eta_A)\eta_B\frac{1}{2}p(b_1) \\ &= \eta_A\eta_B p(a_0b_1) + (1-\eta_A)\eta_B\frac{1}{2}\left[P(a_0b_1) + p(\overline{a}_0b_1)\right] \end{aligned} \tag{4.31}$$

By inserting equation (4.30) and (4.31) into (4.21) we obtain the predicted Bell parameter

$$S_{\mathrm{CH}} = \eta_A\eta_B\left[p(a_1b_1) + \frac{1}{2}p(a_0b_1) + p(a_1b_0) - \frac{1}{2}p(a_0b_0) + \frac{1}{2}p(\overline{a}_0b_0) - \frac{1}{2}p(\overline{a}_0b_1)\right] - \cdots$$
$$- \eta_A\left[p(a_1b_0) + p(a_1\overline{b}_0)\right] - \frac{\eta_B}{2}\left[p(a_0b_1) + p(\overline{a}_0b_1) + p(a_0b_0) + p(\overline{a}_0b_0)\right] \tag{4.32}$$

It is worth noting that considering a trusted measurement device is equivalent to consider perfect efficiencies, namely $\eta_A = 1$ and/or $\eta_B = 1$. In fact, if the device is trusted, we can safely consider only the detected events. In this way, we can have three possible scenarios: fully DI-QKD when the actual efficiencies are considered, 1SDI-QKD in which only one of the two devices (Alice or Bob) is trusted, and standard QKD with both trusted devices.

It is clear that, when Alice and Bob have trusted devices (corresponding to the fair sampling assumption of non-locality tests), the ent-B92 protocol cannot offer advantages with respect to the entangled version of the BB84 protocol [3, 70]. In fact, in this case, the secure key rate of ent-B92 is always lower than the BB84, given by $r_{\mathrm{BB84}} = 1 - 2h_2(Q)$. The advantages come when one (or both) device is not trusted: in this case, the lower threshold detection required by the ent-B92 protocol to violate the CH inequality, gives considerable improvement on the secure key rate with respect to protocols based on maximally entangled states. From the equation (4.32) we can derive the threshold detection efficiencies required to violate the Bell's inequality. For the 1SDI-QKD case ($\eta_A = \eta_B = \eta^{th}$) we have:

$$\eta^{th} = \frac{p(a_1b_0) + p(a_1\overline{b}_0) + \frac{1}{2}p(\overline{a}_0b_1) + \frac{1}{2}p(a_0b_1) + \frac{1}{2}p(\overline{a}_0b_0) + \frac{1}{2}p(a_0b_0)}{p(a_1b_1) + \frac{1}{2}p(a_0b_1) + p(a_1b_0) - \frac{1}{2}p(a_0b_0) + \frac{1}{2}p(\overline{a}_0b_0) - \frac{1}{2}p(\overline{a}_0b_1)} \tag{4.33}$$

If $\eta_A = 1$ (corresponding to Alice trusted device), the Bob's threshold detection efficiency η_B, can be be predicted to be:

$$\eta_B^{th} = \frac{P(a_1b_0) + P(a_1\overline{b}_0)}{P(a_1b_0) + P(a_1b_1) - P(a_0b_0) - P(\overline{a}_0b_1)} \tag{4.34}$$

The two expression above can be expressed also as a function of the angles θ and φ using the states (4.13):

$$\eta^{th} = \frac{2 - \cos\theta(1 + \cos\varphi)}{1 + \cos\varphi - \cos\theta - \cos(\theta + \varphi)} \tag{4.35}$$

$$\eta_B^{th} = \frac{1 - \cos\theta}{\cos\varphi - \cos\theta + \sin\theta\sin\varphi} \tag{4.36}$$

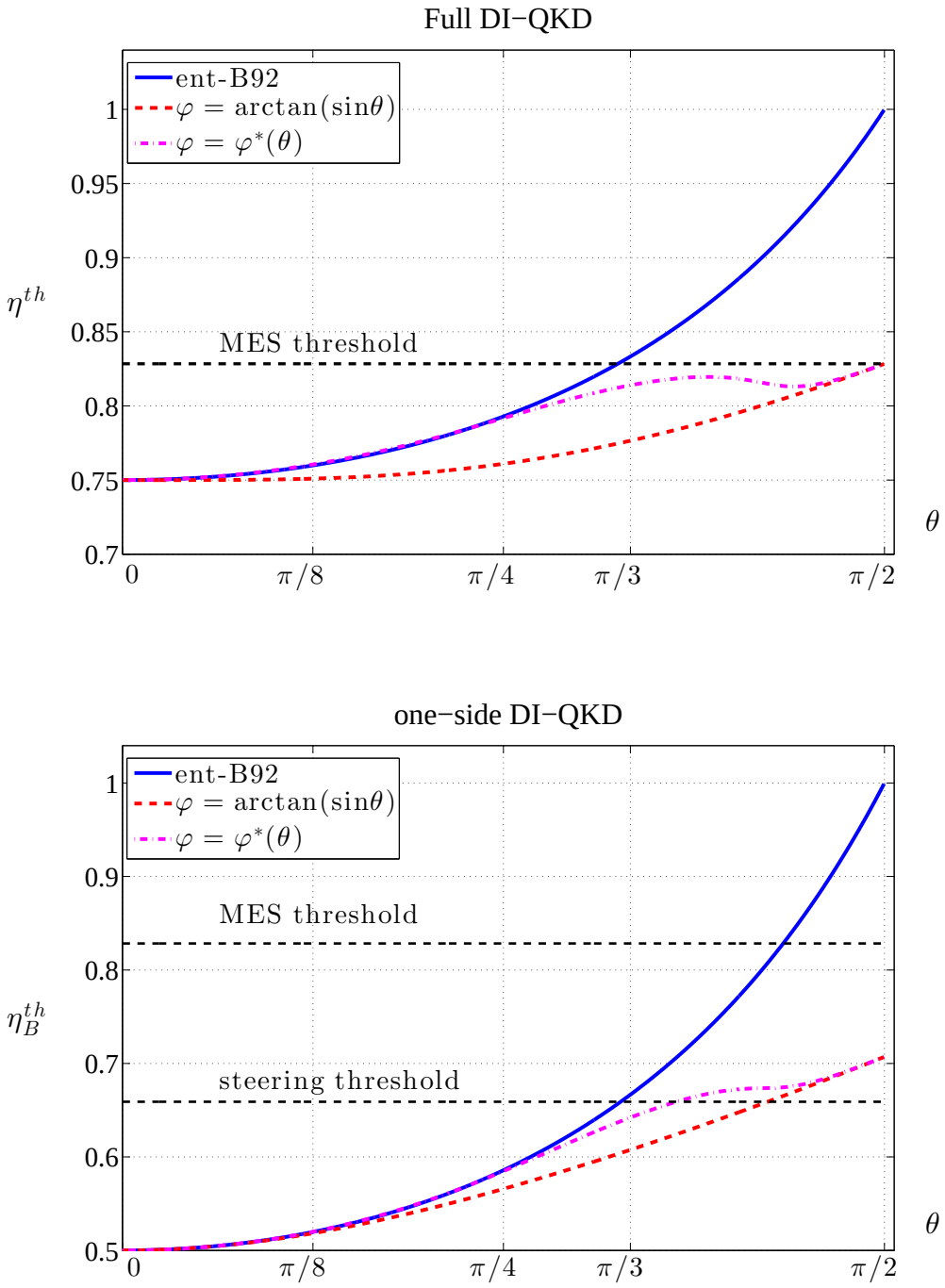


Figure 4.6: Threshold detection efficiency as a function of the angle θ for the $\eta_A = \eta_B = \eta$ case (top) and the $\eta_A = 1$ case (bottom) for the different choice of the angle φ.

In figure 4.6 are shown the theoretical curve for η^{th} and η_B^{th} for both the choice $\varphi = \theta$ (ent-B92 protocol) and $\varphi = \arctan(\sin\theta)$.

4.4.4 Feasibility analysis

Considering a real scenario, we can estimate the value of the Bell parameter in case of arbitrary efficiencies η_A and η_B and thus predict the secure key rate achievable. Let's first consider fully DI-QKD with Alice and Bob having the same efficiency $\eta_A = \eta_B = \eta^{th}$. For each value of η^{th} it is possible to optimize the value of θ (or both θ and φ) that maximize the key rate for the ent-B92 protocol: in figure 4.7 it is illustrated the achievable key rate as a function of the detection efficiency for this case. We note that positive secure key rate can be obtained up to 90.57% efficiency, improving the results of 90.9% and 91.1% obtained respectively in [59] and [60]. Great improvement with respect to previous results are obtained by considering 1SDI-QKD in which Alice device is trusted, corresponding to $\eta_A = 1$ in the secure key rate (4.23) and in the predicted Bell parameter (4.32). In this case the rate r correspond to the fraction of secure bits over the Alice's detected bits. In figure 4.7 it is shown the achievable key rate as a function of the detection efficiency in the 1SDI-QKD case. For the ent-B92 protocol, the secure key rate (without experimental imperfection) becomes

$$r = \eta_B P_c \left[1 - \log_2 f(S_{\mathrm{CH}})\right] \tag{4.37}$$

which is positive whenever the Bell inequality $S_{\mathrm{CH}} \leq 0$ is violated. We note that with this protocol it is possible to obtain positive secure key rate up to 50% detection efficiency, improving the result obtained in previous section (4.3) in which an efficiency greater than 65.9% is required for key generation. This result closes the gap between one-side Bell inequality (also known as steering inequality [60, 71, 72]) and key generation, since the violation of the Bell's inequality corresponds to a positive secure key rate. It still remains the gap for fully DI-QKD, where there is a difference between the threshold of $\eta > 82.8\%$ for a violation of the CHSH inequality [15] and the efficiency required for the security of fully DI-QKD, namely $\eta > 90.57\%$.

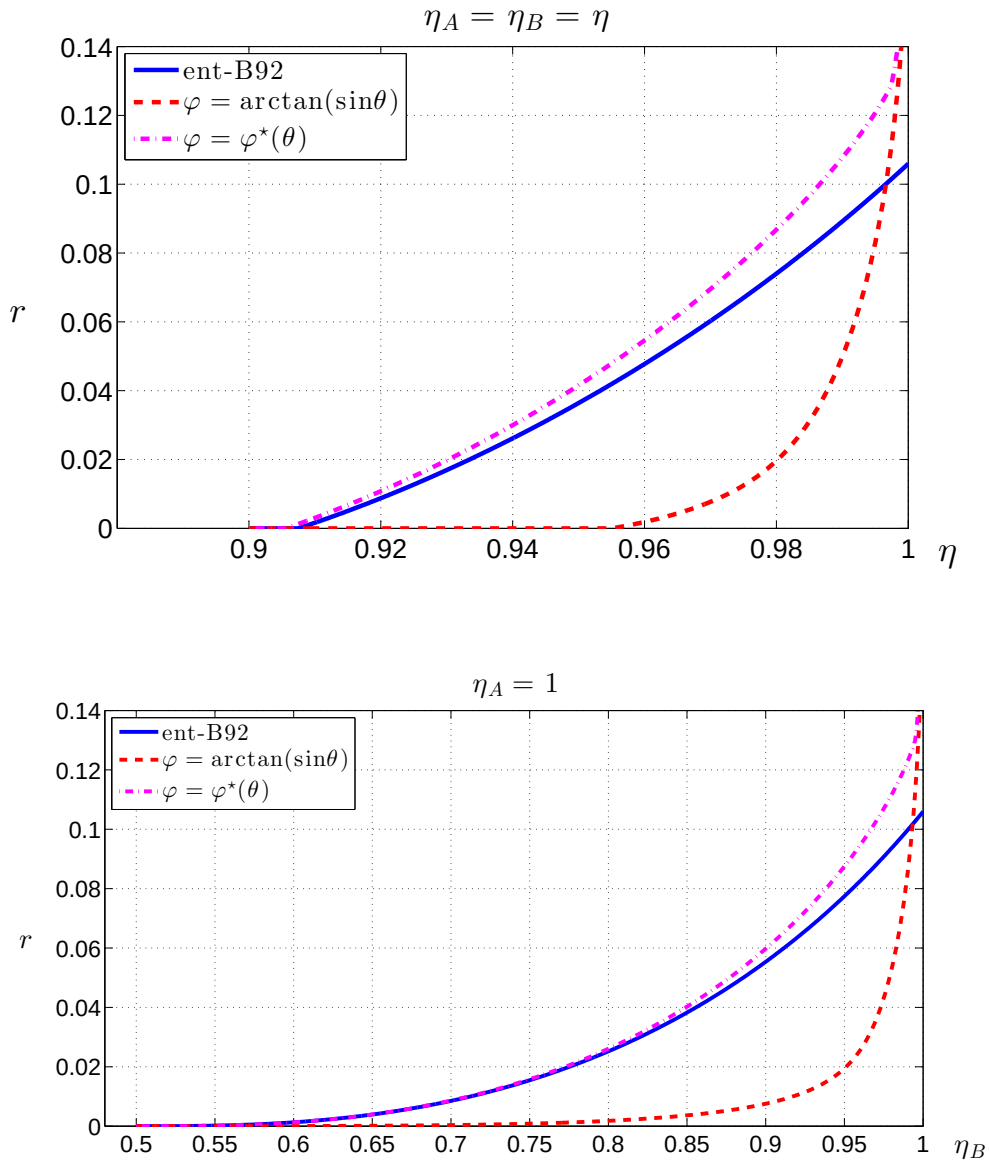


Figure 4.7: Achievable key rate as a function of the threshold detection efficiency for (top) the fully DI-QKD case ($\eta_A = \eta_B = \eta$) and for (bottom) the 1SDI-QKD ($\eta_A = 1$). For 1SDI-QKD the rate is the amount of secure bits over the detected Alice bits.

4.5 Conclusions

In this chapter was presented two QKD protocols in the 1SDI-QKD and fully DI-QKD implementation scenarios. For ent-B92 protocol has been derived an efficient key rate in case of detection inefficiencies. While the improvement for the fully DI-QKD case is small (it was lowered the threshold efficiency from 90.9% to 90.57%), great improvement was obtained in the 1SDI-QKD case: it was in fact possible to achieve positive secure key rate up to 50% efficiency, in comparison with the state of the art result of 65.9% [60].

CHAPTER 5

Feasibility of B92 protocol with non-maximally entangled states

In this chapter we consider the experimental realization of the ent-B92 protocol proposed in chapter 4. First the design and the realization of the experimental setup is described, then we illustrate the noise model used to take into account the non-idealities of the system. Finally, we present the measurement results compared with theoretic curves proposed in section 4.4. The results presented in this chapter are published in [J2] and in the master thesis of Tomasin [73].

5.1 Experimental setup

The experimental setup for the ent-B92 protocol feasibility demonstration (see Fig. 5.1) was designed and developed in order to generate and measure the NMES:

$$|\Phi\rangle_{AB} = \cos\frac{\theta}{2}|H\rangle_A|H\rangle_B + \sin\frac{\theta}{2}|V\rangle_A|V\rangle_B \tag{5.1}$$

A typical scheme for the generation of NMES in polarization is the one proposed by Kwiat in [74], which is given by two identical spontaneous parametric down conversion (SPDC) crystals with orthogonal axis. The used source consists of two overlapped Type-I non-linear Beta Barium Borate (BBO) crystals, with 1 mm length which are pumped by a laser with 810 nm of wavelength, 10 ps of pulse width, 76 MHz of repetition rate and about 100 mW of mean power. To generate different

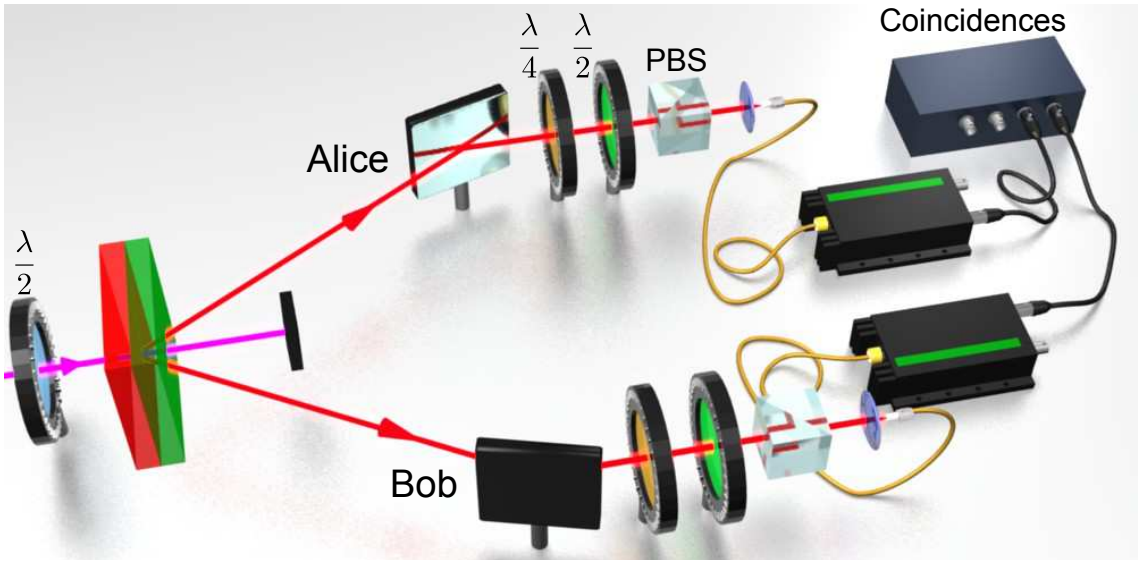


Figure 5.1: Experimental setup used for generation and measurement of the NMESs.

NMES, i.e. to vary the angle θ of the generated NMES (5.1), we positioned before the crystal an half waveplate retarder mounted on a rotating stage. The pump light is focused on the crystal with a lens of focal $f = 200$ mm in order to have an appropriate Rayleigh distance. As represented in figure 5.2, the experimental setup after the crystal is composed by two lenses ($f = 100$ mm) and some tip-tilt mirrors in order to select the intersection of the two parametric circles. The measurement stages are given by a half and a quarter waveplates followed by a polarizing beam-splitter for each measurement channel. The outcoming photons are then collected by two single mode fibers through 20× focusing objective. In front of fibers we placed also two band-pass filters with 810 nm of center wavelength and 7 nm of full width half maximum (FWHM) bandwidth in order to select only the entangled photons. The fibers are attached to two single photon avalanche diodes(SPADs) with 40 % of photon detection efficiency, 50 photon/s of dark counts and 40 ns of dead time.

The entire setup, except for the pump source, was designed to be compact in order to be mounted over a 300 × 600 mm breadboard. Due to the long coherence time of the pump laser compared with the crystals length, it was not necessary to compensate the temporal walk-off in the BBO crystals.

The signals coming from the SPADs were collected by dedicated electronics which enables to detect the coincidence events. We used a time-tagger with 81 ps of

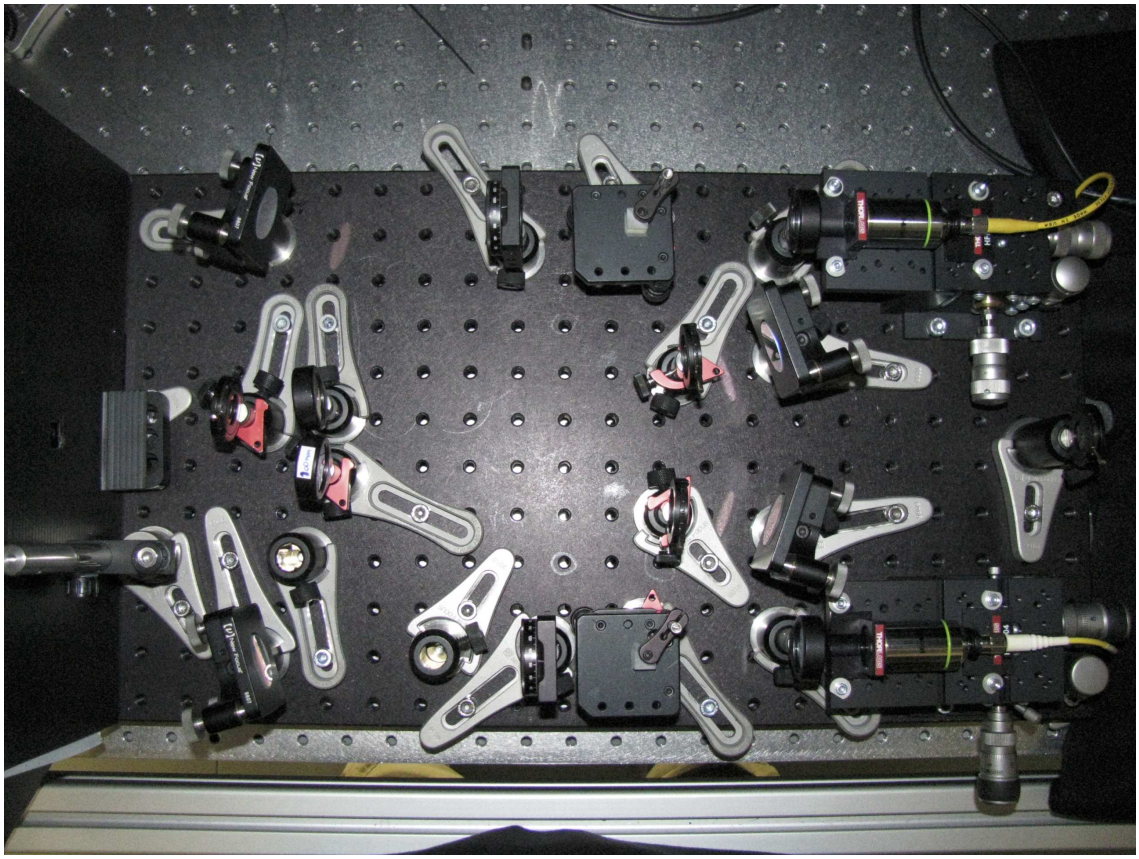


Figure 5.2: Experimental setup after the SPDC crystal

temporal resolution which is far below the temporal resolution of the SPADs. The coincidence time window, that is the maximum delay between the two revealed photons to be considered a coincidence, was set to $\Delta T = 2.4$ ns.

The detection efficiency of the entire system was calculated taking into account the coupling efficiency of the fibers and the photon detection efficiency of the SPADs, the overall measured efficiency is about 10 %.

5.2 Noise estimation

In order to take into account imperfections in the setup we elaborated a noise model. Principal sources of noise are background photons and decoherence of the generated state. Background noise is produced by all detected photon pairs that are not entangled, the best model for this is white noise since is totally depolarized. In the generation of the NMES (5.1) it is difficult to produce the contributions $|HH\rangle$

and $|VV\rangle$ perfectly distinguishable. This, indeed, introduces a decoherence in the generated state that can be modeled with colored noise. Considering these noise contributions we can express the experimental generated state as:

$$\rho_{exp} = (1 - \epsilon_c - \epsilon_w)|\Phi(\theta)\rangle\langle\Phi(\theta)| + \epsilon_c\rho_c + \epsilon_w\frac{\mathbb{1}}{4} \tag{5.2}$$

In the previous equation $\rho_c = \cos^2\frac{\theta}{2}|HH\rangle\langle HH| + \sin^2\frac{\theta}{2}|VV\rangle\langle VV|$ and ϵ_c (ϵ_w) represent the amount of colored (white) noise. The effect of the noise contribution can be easily seen also making explicit the density matrix:

$$\rho_{exp} = \begin{bmatrix} \frac{1}{4}(2 - \epsilon_w + 2(1-\epsilon_w)\cos\theta) & 0 & 0 & \frac{1}{2}(1-\epsilon_w-\epsilon_c)\sin\theta \\ 0 & \frac{1}{4}\epsilon_w & 0 & 0 \\ 0 & 0 & \frac{1}{4}\epsilon_w & 0 \\ \frac{1}{2}(1-\epsilon_w-\epsilon_c)\sin\theta & 0 & 0 & \frac{1}{4}(2 - \epsilon_w - 2(1-\epsilon_w)\cos\theta) \end{bmatrix} \tag{5.3}$$

As we can see, white noise affects the elements in the diagonal while colored one introduces some off-diagonal components.

With this noise definition it is possible to recalculate all the theoretic curve of section 4.4 in presence of noise. The Bell's parameter S_{CH} becomes:

$$S_{\mathrm{CH}} = \frac{1}{2}\left((1-\epsilon_w)\cos\varphi + (1-\epsilon_w-\epsilon_c)\sin\theta\sin\varphi - 1\right) \tag{5.4}$$

and the QBER is equal to:

$$Q_{BER} = \frac{1}{2}\left(1 - \frac{(1-\epsilon_w-\epsilon_c)\sin\theta\sin\varphi}{1-(1-\epsilon_w)\cos\theta\cos\varphi}\right) \tag{5.5}$$

It is easy to see that in presence of noise also the choice $\varphi = \theta$ gives a non-zero quantum bit error rate, as expected. The probability of a conclusive event is given by:

$$P_{conc} = \frac{1}{2}\left(1 - (1-\epsilon_w)\cos\varphi\cos\theta\right) \tag{5.6}$$

It is interesting noting that the colored noise term ϵ_c is not present in this equation, since distinguishability between $|HH\rangle$ and $|VV\rangle$ contributions in (5.1) does not affect the measurement in the basis used to produce the raw key but affects only the ones used for the violation of the Bell's inequality. The threshold detection efficiencies in presence of noise can be rewritten as:

$$\eta^{th} = \frac{2 - (1-\epsilon_w)\cos\theta(1+\cos\varphi)}{1 + (1-\epsilon_w)\left(\cos\varphi - \cos\theta - \cos(\theta+\varphi)\right) - \epsilon_c\sin\theta\sin\varphi} \tag{5.7}$$

$$\eta_B^{th} = \frac{1-(1-\epsilon_w)\cos\theta}{(1-\epsilon_w)(\cos\varphi-\cos\theta)+(1-\epsilon_w-\epsilon_c)\sin\theta\sin\varphi} \tag{5.8}$$

since the parameter ϵ_c is multiplied with a sine function in both the equations we can predict that the colored noise is more effective for low values of the angles θ and φ.

5.3 Experimental results for ent-B82

All the parameters of ent-B92 protocol can be directly derived from the measurement probabilities. These are given by the ratio between the number of events when Alice measures the state $|a_k\rangle$ and Bob measures the state $|b_k\rangle$ upon the sum of the counts when Alice and Bob measure in the basis $A_1 = \{|H\rangle, |V\rangle\}$:

$$P(a_k, b_k) = \frac{N(a_k, b_k)}{N(H,H)+N(V,V)+N(H,V)+N(V,H)} \tag{5.9}$$

5.3.1 Measurements

The measurements taken for both the ent-B92 protocol ($\theta = \varphi$) and the $\varphi = \arctan(\sin\theta)$ protocol are listed in tables 5.1 and 5.2. For every measurement we reported the number of coincidence collected for different time windows. We took in consideration also the accidental coincidences that can be given by the generation of double pairs in the SPDC process, the estimated rate is equal to:

$$R_{acc} = \frac{N_A N_B}{\nu \Delta T} \tag{5.10}$$

where N_1 and N_2 are the counts of single events for Alice and Bob respectively, ν is the repetition rate of the laser pump and ΔT is the temporal observation interval. We evaluated also the SPDC efficiency, i.e. the ratio between the single count events and the coincidence counts:

$$\eta_S = \frac{N_s}{N_c} \tag{5.11}$$

the measured efficiency is about $\eta_S \simeq 10\%$. To assess the quality of the generated NMES we also measured the average visibilities for the basis $L = \{|H\rangle, |V\rangle\}$ and

$D = \{|+\rangle, |b_k\rangle\}$ (with $\varphi = \theta$):

$$V_L = \frac{N(H,H) + N(V,V) - N(H,V) - N(V,H)}{N(H,H) + N(V,V) + N(H,V) + N(V,H)} \gtrsim 99\%$$
$$V_D = \frac{N(+,b_1) + N(-,b_0) - N(+,b_0) - N(-,b_1)}{N(+,b_1) + N(-,b_0) + N(+,b_0) + N(-,b_1)} \gtrsim 96\%$$

Those values confirm a good interference in the generated entangled state.

The angles θ reported in tables 5.1 and 5.2 were not calculated from the rotation of the half-waveplate placed in front of the SPDC crystal, but directly from the measurements as:

$$\theta = \frac{90}{\pi} \arctan\left(\sqrt{\frac{N(H,H)}{N(V,V)}}\right) \tag{5.12}$$

θ [deg]	$N(H,H)$	$N(V,V)$	$N(H,V)$	$N(V,H)$	$N(V,\overline{b}_0)$	$N(V,b_1)$	$N(V,b_0)$	$N(+,b_0)$	$N(+,b_1)$	$N(-,b_1)$	$N(-,b_0)$
12°	25969	272	45	27	59	274	246	35	699	27	370
16°	17278	357	25	17	53	362	341	24	805	35	511
25°	11362	549	29	17	47	516	547	37	957	22	934
29°	2977	196	10	7	29	228	232	13	412	12	357
35°	2279	220	7	4	40	245	184	9	410	12	405
41°	2465	336	6	8	65	309	297	10	584	14	490
45°	6771	1182	11	10	179	1020	1004	39	1986	35	1895
52°	4331	1045	17	8	260	940	761	27	1581	41	1652
57°	4450	1318	82	16	282	1097	1107	34	1832	44	2072
65°	5068	2030	20	12	609	1521	1225	35	2871	40	2558
70°	1700	833	3	4	317	625	605	23	1095	14	1090
74°	4089	2341	15	41	1012	1730	1308	37	3048	52	2640
82°	2772	2060	27	17	957	1388	1045	28	2519	37	2078
83°	1355	1061	2	7	486	622	562	18	1222	21	1227
90°	1483	1460	5	17	709	743	753	22	1386	23	1463

Table 5.1: Measurements for ent-B92 protocol with $\varphi = \theta$

θ [deg]	$N(H,H)$	$N(V,V)$	$N(H,V)$	$N(V,H)$	$N(V,\overline{b}_0)$	$N(V,b_1)$	$N(V,b_0)$	$N(+,b_0)$	$N(+,b_1)$	$N(-,b_1)$	$N(-,b_0)$
11°	12013	119	33	6	36	113	89	14	304	8	166
15°	11858	208	28	9	57	206	187	12	496	13	319
25°	11804	568	22	15	102	584	515	39	1178	19	849
29°	4785	318	12	3	49	344	281	16	550	12	497
35°	9620	938	66	16	126	1006	859	30	1403	30	1285
40°	5612	744	9	36	101	757	598	28	1115	48	1023
48°	4577	910	13	7	142	846	734	49	1256	47	1110
52°	4166	990	11	11	155	961	877	68	1255	72	1255
58°	6187	1868	19	62	369	1788	1450	142	2219	92	2022
64°	3946	1567	11	15	263	1433	1373	111	1686	153	1802
69°	3502	1662	15	9	291	1568	1372	137	1675	179	1699
72°	3644	1928	12	38	402	1800	1569	177	1925	209	1926
82°	1304	975	4	10	180	911	880	140	950	149	967
83°	2859	2233	9	34	463	1989	1856	344	2262	184	1820
89°	3108	2965	10	39	624	2612	2239	399	2436	363	2579

Table 5.2: Measurements for ent-B92 protocol with $\varphi = \arctan(\sin\theta)$

5.3.2 Measurements plots

In this subsection we present the plots of the measured parameters regarding the ent-B92 protocol. For each experimental parameter we report also the errors calculated by means of standard propagation of the Poissonian photon-counting statistic. A detailed description of the calculation of all the standard deviations can be found in appendix A.

In figure 5.3 we report the experimental values for the CH inequality S_{CH} as a function of the amount of entanglement parameter θ. We can see that the presence of noise does not affect significantly the experimental curve. Otherwise in the secure key rate the noise plays an important role in fact as we can see in figure 5.4, for some values of θ, it lowers the experimental curve below the minimum achievable secret key rate. In figure 5.6 it is possible to observe the effect of noise on the threshold

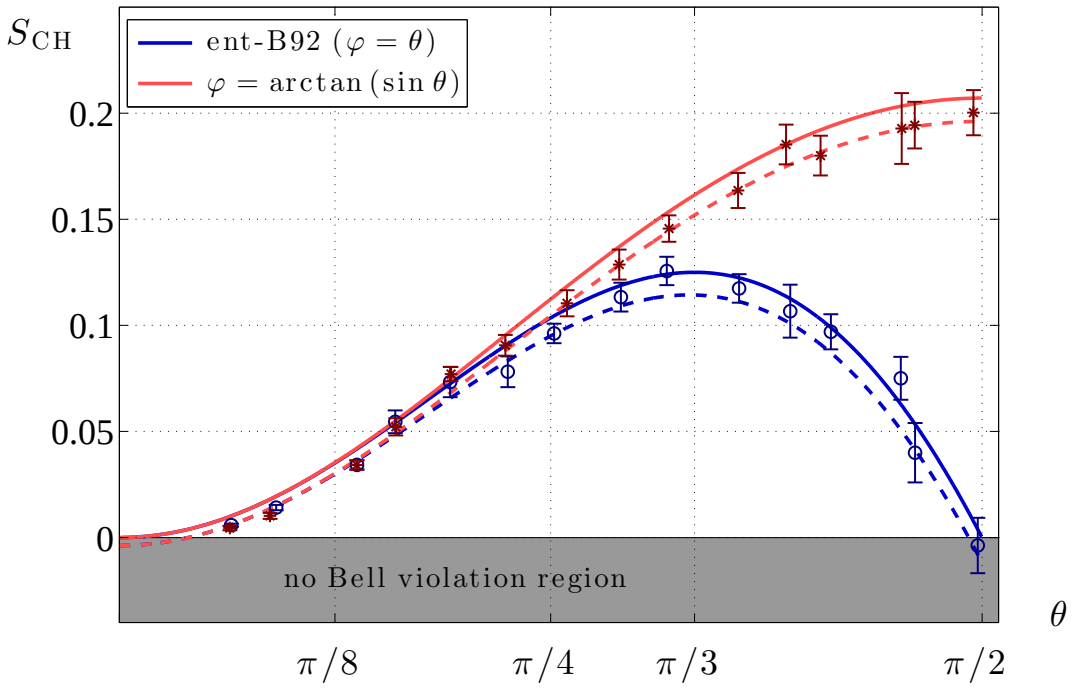


Figure 5.3: Experimental values of the parameter S_{CH} and corresponding errors for the ent-B92 (blue circles) and the $\varphi = \arctan(\sin\theta)$ (red stars) protocol. Continuous lines refer to theoretical predictions, corresponding to perfect state generation. Dashed lines refer to noise model of equation (5.2) with $\epsilon_w = 0.007$ and $\epsilon_c = 0.015$.

detection efficiencies required to violate the CH inequality, it is interesting noting that noise has a huge impact on the measurements as the NMES get closer to the separable state. The same can be observed in the plot of the QBER as a function of θ in figure 5.5 in which it is possible noting that also the choice $\varphi = \theta$ has non-zero QBER in presence of noise. In figure 5.7 the maximum achievable secure key rate as a function of the threshold detection efficiency is proposed, in this case noise acts as an increment of the minimum required threshold detection efficiency. The only term in which the noise is negligible is the probability of a conclusive event, as we can see in figure 5.8.

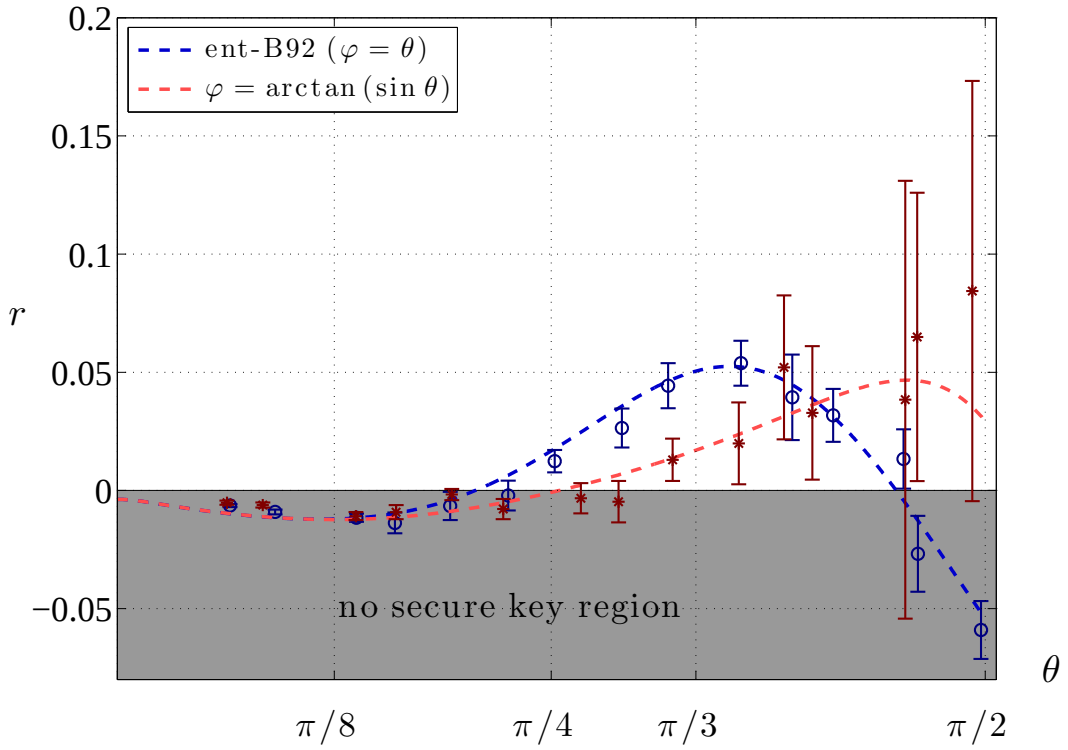


Figure 5.4: Experimental key rates as a function of angle θ with trusted measurement devices for the ent-B92 (blue circles) and the $\varphi = \arctan(\sin\theta)$ (red stars) protocol. Dashed lines refer to noise model of equation (5.2) with $\epsilon_w = 0.007$ and $\epsilon_c = 0.015$.

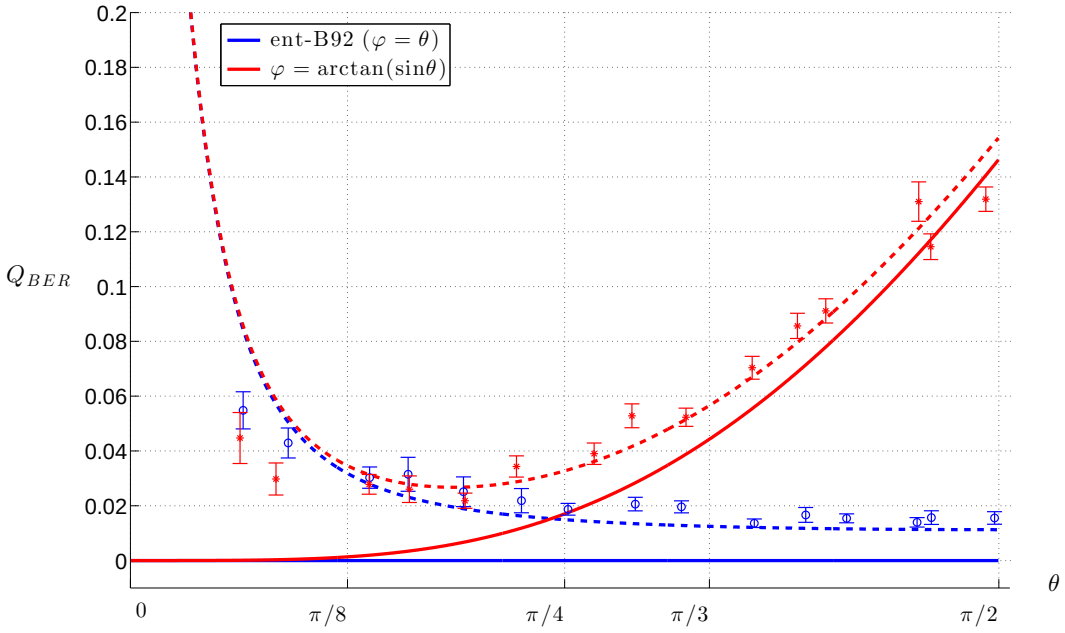


Figure 5.5: Quantum Bit Error Rate as a function of the angle θ for the ent-B92 (blue circles) and the $\varphi = \arctan(\sin\theta)$ (red stars) protocol. Continuous lines refer to theoretical predictions, corresponding to perfect state generation. Dashed lines refer to noise model of equation (5.2) with $\epsilon_w = 0.007$ and $\epsilon_c = 0.015$.

5.4 Conclusions

In this chapter we proposed the experimental feasibility of the protocol ent-B92 exposed in chapter 4. We illustrated the setup and the experimental results, in particular we analyzed in detail the incidence of noise in the measurements. The results show a good agreement between the theory and the experiment.

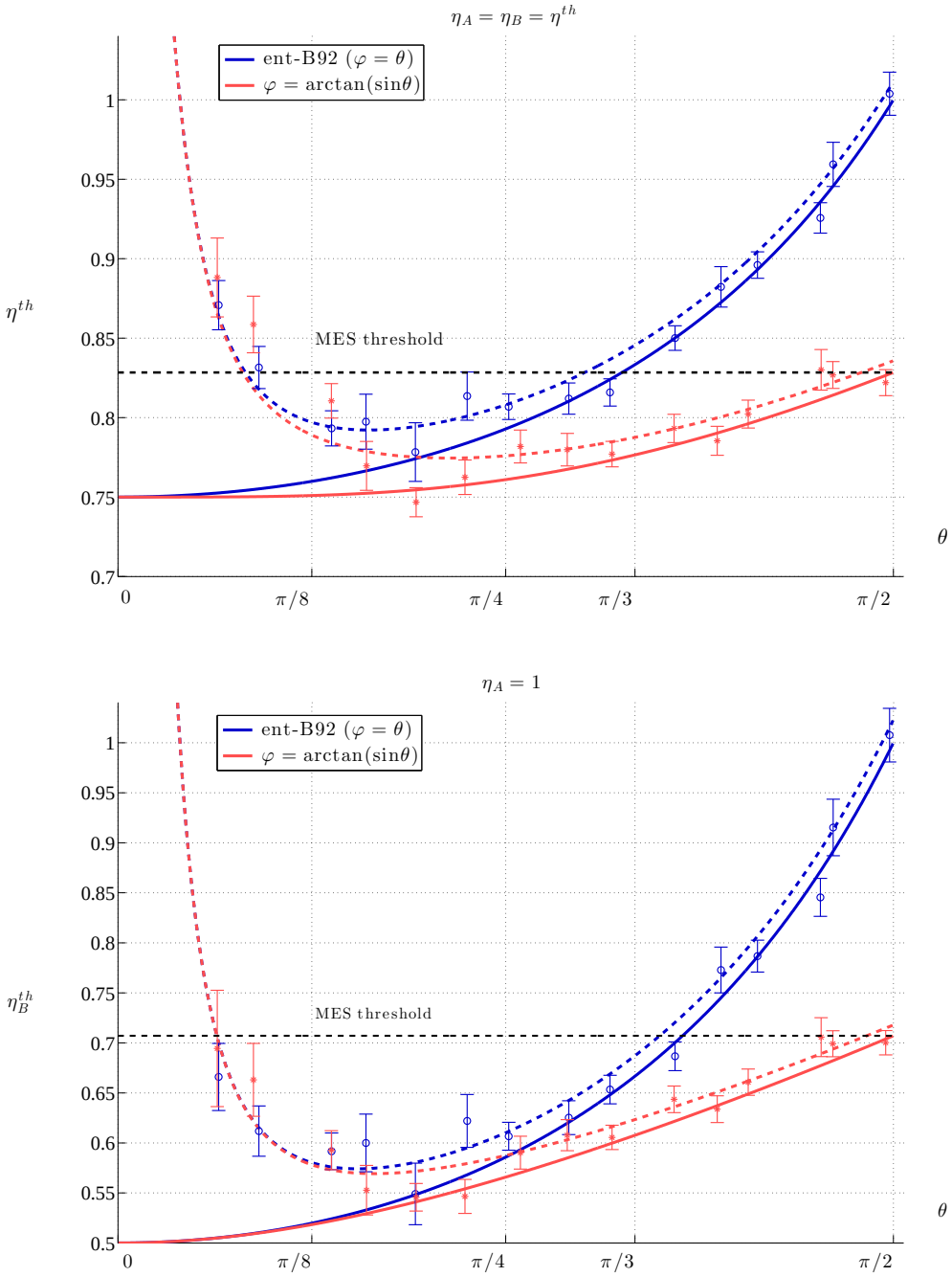


Figure 5.6: Threshold detection efficiency as a function of the angle θ for the $\eta_A = \eta_B = \eta^{th}$ case (top) and the $\eta_A = 1$ case (bottom) for the ent-B92 (blue circles) and the $\varphi = \arctan(\sin\theta)$ (red stars) protocol. Continuous lines refer to theoretical predictions, corresponding to perfect state generation. Dashed lines refer to noise model of equation (5.2) with $\epsilon_w = 0.007$ and $\epsilon_c = 0.015$.

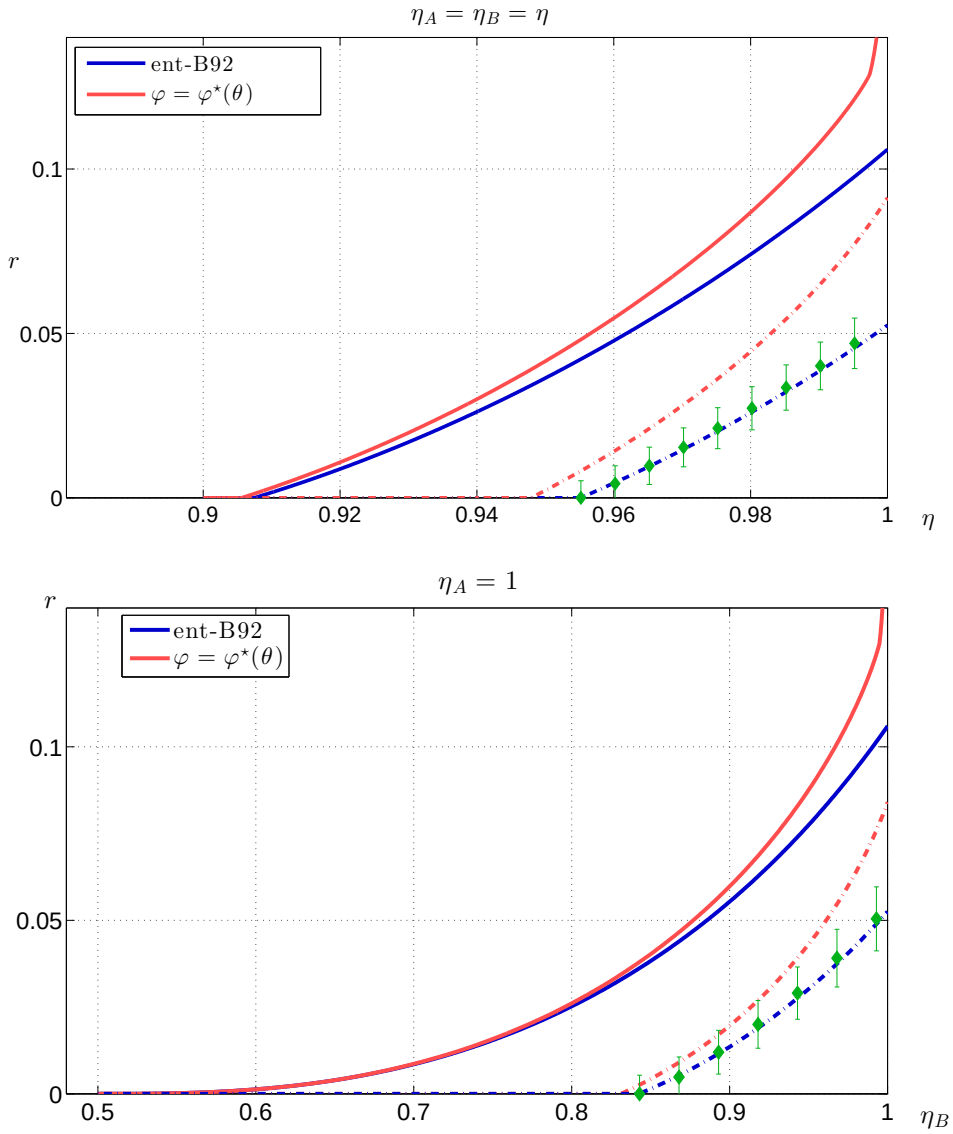


Figure 5.7: Secure key rate as a function of the threshold detection efficiency for the fully DI-QKD case (top) and the 1SDI-QKD case (bottom) for the ent-B92 (green dots) protocol. Continuous lines refer to theoretical predictions, corresponding to perfect state generation. Dashed lines refer to noise model of equation (5.2) with $\epsilon_w = 0.007$ and $\epsilon_c = 0.015$.

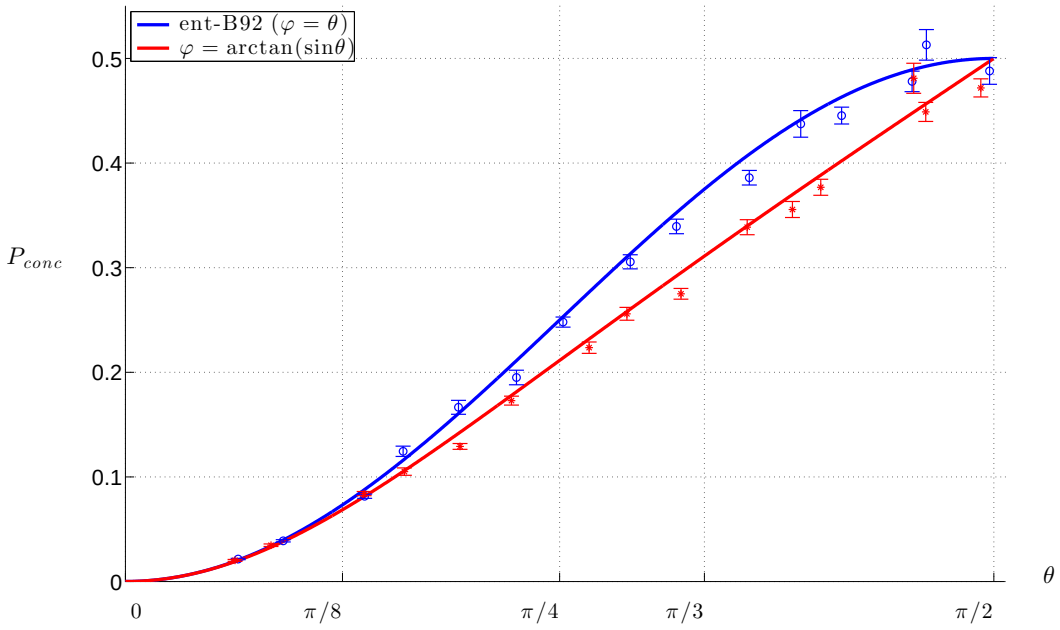


Figure 5.8: Probability of a conclusive event as a function of the angle θ for the ent-B92 (blue circles) and the $\varphi = \arctan(\sin\theta)$ (red stars) protocol. Continuous lines refer to theoretical predictions, corresponding to perfect state generation, noise model curves are not presented because differences with theoretical ones are negligible.

CHAPTER 6

Hyperentanglement as a resource for QKD

Entanglement represents a great resource for Quantum Mechanics and plays an important role in experimental tests of quantum information theories. Quantum state of photons are easily generated by means of spontaneous parametric down conversion (SPDC), as already seen in chapter 5. SPDC typically generates no more than one photon pair time by time, and this corresponds to deal with a 2×2 Hilbert space. However, information tasks and fundamental tests of Quantum Mechanics involve large number of qubits. Thus, it is necessary to add more than one qubit to the quantum states in order to fully exploit the advantages offered by quantum mechanics. For example, the greater the number of qubits, the stronger the violation of Bell's inequalities.

In order to increase the number of qubits it is possible to enhance the number of entangled particles or, as treated in this chapter, to encode more than one qubit in each particle. This latter can be obtained exploiting different degrees of freedom (DOFs) of the photon, as proposed by [75–80]. This kind of entanglement in more than one DOFs is called hyperentanglement.

Hyperentanglement gives the possibility to perform many quantum non-locality tests, such as the demonstration of Mermin's growing-with-size quantum non-locality effect [81]. It also allows to generalize the Greenberger-Horne-Zeilinger (GHZ) theorem [82] with only two entangled particles. As seen in chapter 4 and 5, one of the main limitation of the non-locality tests performed with photons is represented by

the so-called "detection loophole". Recently was demonstrated that by using hyperentangled states with two DOFs the threshold detection efficiency can be lowered to 61.8 % [83]. Massar in [84] also shown that lower bounds decrease exponentially with the dimension of the Hilbert space by increasing the dimension of the entangled state.

Bell state analysis, i.e. the discrimination between the four orthogonal Bell states, is a fundamental resource in several quantum information processing and applications, such as dense coding [20, 21], teleportation [85–87], entanglement swapping [85, 88–90], cryptography [91, 92]. However, the complete deterministic discrimination between the four states is not possible using linear optical elements and classical communications. Enlarging the size of the Hilbert space and using hyperentangled (HE) states allow us to achieve a complete Bell state analysis [93–96].

In this chapter we first make an overview on HE states generation, focusing on hyperentangled states in polarization and energy-time DOFs. We then present the design and the implementation of an experimental system for the generation and measurement of photon pairs entangled in both polarization and energy-time. To access the quality of the generated states we propose the results of the separate tomography of both the DOFs. Detailed informations on hyperentanglement can be also found in [97].

6.1 Hyperentangled states generation

As early mentioned, the entanglement of two particles in different DOFs corresponds to so-called HE state. We now propose a more formal definition of HE state. Let us consider two photons A and B and n independent DOFs $\{a_j\}$ and $\{b_j\}$, with $j = 1, \ldots n$. Each DOF spans a 2-dimensional Hilbert space with basis $\{|0\rangle_{a_j}, |1\rangle_{a_j}\}$ ($\{|0\rangle_{b_j}, |1\rangle_{b_j}\}$) for particle A (B). Therefore, each particle carries exactly n qubits. A state $|\varphi\rangle$ is *separable in the HE sense* if it satisfies the following condition:

$$\exists \text{ a } j \text{ such that } |\varphi\rangle = |\varphi_1\rangle_{a_j\mathcal{I}}|\varphi_2\rangle_{b_j\mathcal{J}} \tag{6.1}$$

where $\{\mathcal{I}, \mathcal{J}\}$ represents a generic bi-partition of the set $\mathcal{T}_j \equiv \{a_1, b_1, \ldots, a_n, b_n\} \setminus \{a_j, b_j\}$, so that $\mathcal{I} \cup \mathcal{J} = \mathcal{T}_j$ and $\mathcal{I} \cap \mathcal{J} = \varnothing$.

Definition: A (mixed) state is **hyperentangled** in n degrees of freedom if it is separately entangled in each of them and cannot be written as a mixture of states satisfying equation (6.1) [97].

Hyperentanglement can be experimentally checked by means of measurement of an *(hyper-)entanglement witness*. A witness W is an hermitian operator whose expectation value is non-negative for any separable state, whereas it is negative for entangled states. For HE states this consists in verifying the presence of entanglement for each DOF and measuring an hyperentanglement witness which is positive for the states that can be written as a mixture of states satisfying equation (6.1).

A very useful technique to generate entangled photons is the SPDC process. Typically an intense pump laser beam (p) shines a non-linear birefringent crystal from which are probabilistically generated pairs of photons, referred as idler (i) and signal (s). For the maximization of the emission probability is necessary to satisfy the following condition:

$$\text{phase-matching: } \vec{k}_p = \vec{k}_i + \vec{k}_s, \qquad \text{energy matching: } \omega_p = \omega_i + \omega_s \tag{6.2}$$

The SPDC two-photon state can be expressed as [97]:

$$|\Psi\rangle = \mathcal{N} \int \mathrm{d}^2\mathbf{k}_s \mathrm{d}^2\mathbf{k}_i \mathrm{d}\omega_s \mathrm{d}\omega_i A_p(\mathbf{k}_s + \mathbf{k}_i, \omega_s + \omega_i) \mathrm{sinc}\left(\frac{\Delta k_z L}{2}\right) |\mathbf{k}_s, \omega_s\rangle |\mathbf{k}_i, \omega_i\rangle \tag{6.3}$$

where $\mathbf{k}_i$ and $\mathbf{k}_s$ are the transverse momentum coordinates, $|\mathbf{k}, \omega\rangle = a^\dagger(\mathbf{k}, \omega)|0\rangle$, $A_p(\mathbf{k}, \omega)$ is the pump profile in the momentum-frequency space, $\mathcal{N}$ is a normalization constant, and L is the crystal length. Δk_z represents the longitudinal phase mismatch $\Delta k_z(\mathbf{k}_s, \mathbf{k}_i, \omega_s, \omega_i) = k_{pz}(\mathbf{k}_s + \mathbf{k}_i, \omega_s + \omega_i) - k_{sz}(\mathbf{k}_s, \omega_s) - k_{iz}(\mathbf{k}_i, \omega_i)$ and the longitudinal component of momentum is given by $k_z(\mathbf{k}, \omega) = \sqrt{\left[\frac{n(\omega)\omega}{c}\right]^2 - \mathbf{k}^2}$. The phase-matching condition is satisfied when $\Delta k_z = 0$. Usually, there exist two kinds of phase-matching condition, depending on the polarization of ordinary (o) and extraordinary (e) axes of the SPDC crystal:

$$\text{Type-I: } e \to o + o, \qquad \text{Type-II: } e \to e + o \tag{6.4}$$

In the first case the phase-matching condition is satisfied for all the wavevectors $\vec{k}_i$ and $\vec{k}_s$ lying on the external surface of a single emission cone. For Type-II

phase-matching, the two degenerate photons are emitted over two different, mutually crossing, emission cones.

In our experiment the photon pairs are entangled in the polarization and the energy-time DOFs. The generation of polarization entangled photon pairs was already mentioned in chapter 5. In next section we will briefly introduce the process of generation of entangled photon pairs in energy-time.

6.1.1 Entanglement in energy-time

Let us define $|\omega\rangle = a^\dagger_\omega|0\rangle$ and consider only two definite spatial modes and a Gaussian pump profile $A_p(\mathbf{k},\omega) = C_0\,\mathrm{e}^{-\frac{w_0^2}{4}\mathbf{k}_p^2}\,\mathrm{e}^{\frac{\tau_p^2}{4}(\omega-\omega_p)^2}$, with τ_p and w_0 respectively representing the coherence time and the beam waist of the pump laser beam. Considering a perfect phase-matching and constant refractive indices $n_0(\omega) \sim n_o(\omega_0)$, one can express the SPDC two-photon state as:

$$|\Psi\rangle = \sqrt{\frac{\tau_p T}{\pi}} \int \mathrm{d}\omega_s \mathrm{d}\omega_i\, \mathrm{e}^{-\frac{T^2}{4}(\omega_s-\omega_i)}\, \mathrm{e}^{\frac{\tau_p^2}{4}(\omega_s+\omega_i-\omega_p)^2}\, |\omega_s\rangle|\omega_i\rangle \tag{6.5}$$

The time constant is equal to $T = \frac{n_0(\omega_0)\overline{w}\theta}{c}$, where $\overline{w}$ is the beam waist of the pump and the selected photons, and θ is the emission angle. Let us define the following quantity $|t\rangle = \frac{1}{\sqrt{2\pi}} \int \mathrm{d}\omega\, \mathrm{e}^{-i\omega t}\, |\omega\rangle$. The SPDC state 6.5 can be expressed as:

$$|\Psi\rangle = \sqrt{\frac{1}{\pi T \tau_p}} \int \mathrm{d}t_1 \mathrm{d}t_2\, \mathrm{e}^{-\frac{(t_1-t_2)^2}{4T^2}}\, \mathrm{e}^{\frac{(t_1+t_2)^2}{4\tau_p^2}}\, \mathrm{e}^{i\omega_0(t_1+t_2)}\, |t_1\rangle|t_2\rangle \tag{6.6}$$

When the condition $T \neq \tau_p$ is satisfied the SPDC state is entangled in energy-time. In figure 6.1 is represented the scheme proposed by Franson [98] which allows to measure energy-time entanglement. For each generated photon, it consists of two unbalanced Mach-Zehnder interferometer with a long (L) and a short (S) arm. If $c\tau_p \gg L - S$, when both the photon of the pair are detected in coincidence interference is observed since it is not possible to ascertain if they followed both the long or the short path.

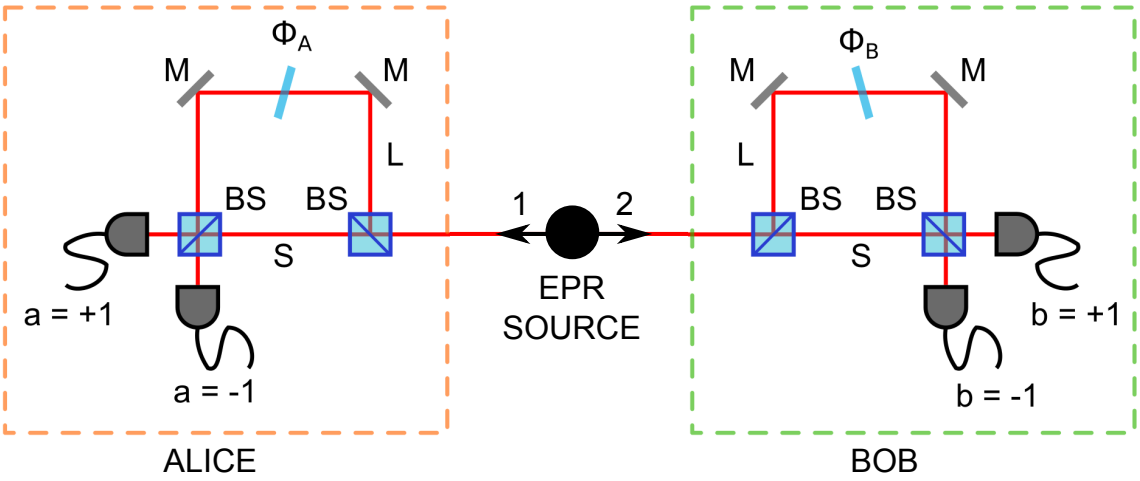


Figure 6.1: Experimental scheme for the measurement of energy-time entanglement. M: mirror, BS: beamsplitter, L: long arm, S: short arm.

Considering the scheme in figure 6.1 and the equation (6.6) we can write the four Bell states for the energy-time DOF as:

$$|\Phi^{\pm}\rangle = \tfrac{1}{\sqrt{2}}\left(|L\rangle_A|L\rangle_B \pm |S\rangle_A|S\rangle_B\right) \tag{6.7}$$

$$|\Psi^{\pm}\rangle = \tfrac{1}{\sqrt{2}}\left(|L\rangle_A|S\rangle_B \pm |S\rangle_A|L\rangle_B\right) \tag{6.8}$$

where $|L\rangle$ ($|S\rangle$) corresponds to the long (short) arm of the interferometer.

6.1.2 Hyperentanglement in polarization and energy-time

Combining the scheme described above and the one presented in chapter 5 it is possible to generate photon states that are entangled in both polarization and energy-time. This kind of HE state can be written as:

$$|\Psi_{PT}\rangle = \frac{1}{\sqrt{2}}\underbrace{\left(|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B\right)}_{\text{POLARIZATION}} \otimes \frac{1}{\sqrt{2}}\underbrace{\left(|L\rangle_A|L\rangle_B - |S\rangle_A|S\rangle_B\right)}_{\text{ENERGY-TIME}} \tag{6.9}$$

where the polarization DOF is the Bell state $|\Psi^+\rangle$ whereas the energy-time DOF is the Bell state $|\Phi^-\rangle$. With this state it is possible to encode four qubits into two photons.

6.2 Design of experimental QKD system with hyperentangled states

The aim of the experiment is to build a system for the propagation of HE states at long distances. We focus on the design of a measurement apparatus that is portable and stabilized also in an environment outside the laboratory. Therefore, we place one of the two measurement apparatus upon a breadboard. The outputs of the source and the inputs of the receivers are connectorized with fiber optics in order to make easy the connection between them. This does not affect the use of free-space links in the future as the fibers can always be used to connect the apparatuses to telescopes. In next section we will describe in detail all the experimental setup.

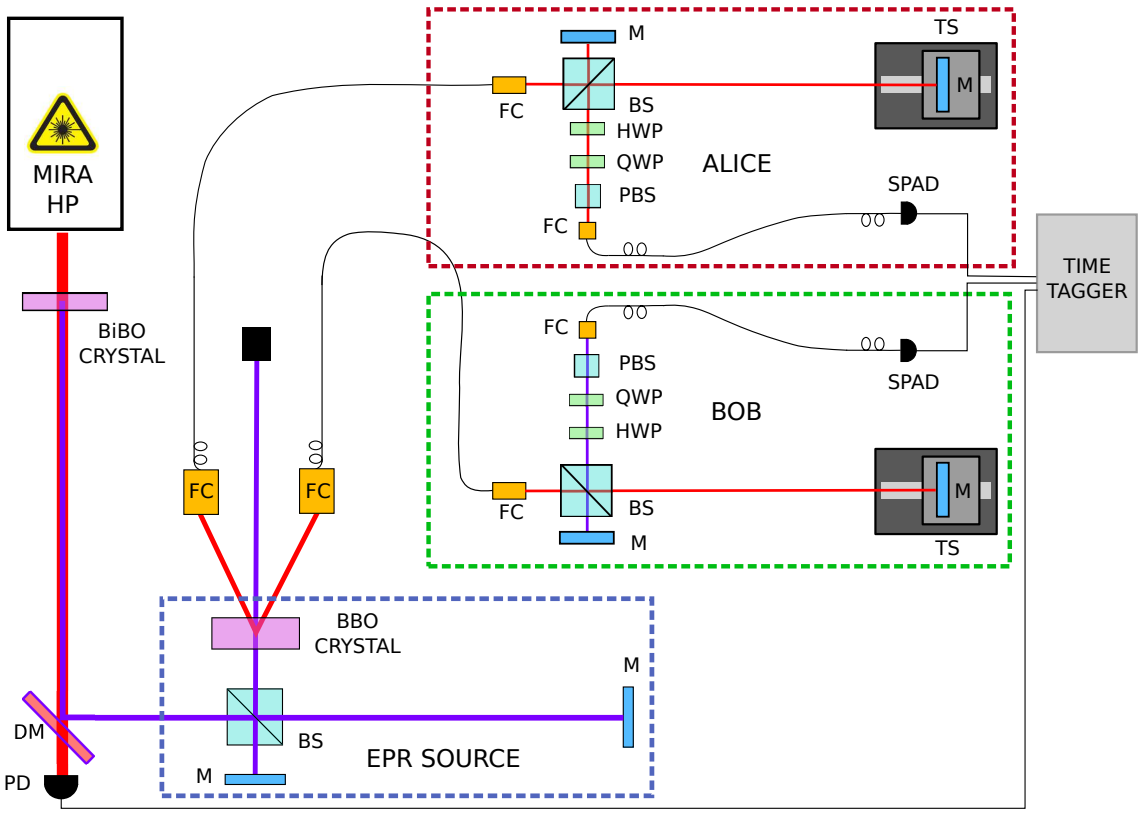


Figure 6.2: Scheme of the experimental setup for the generation and measurement of HE states. DM: dichroic mirror, M: mirror, FC: fiber coupler, TS: translation stage, PD: photodiode, BS: beamsplitter, HWP: half waveplate, QWP: quarter waveplate, PBS: polarizing beamsplitter.

6.2.1 Experimental setup

The scheme of the experimental setup is shown in figure 6.2, the light source is a titanium sapphire laser with 810 nm of wavelength, 150 fs of pulse width and 76 MHz of repetition rate. The laser is focused with a f= 50 mm lens inside a BiBo (Bismuth Borate, BiB_3O_6) crystal for the second harmonic generation (SHG) at 405 nm, after the crystal is placed a second lens with the same focal length of the previous one. The fundamental wavelength is then filtered with a dichroic mirror, the rejected 810 nm pump is sent to a photodiode which is used as a trigger source.

The pulsed light then enters inside an unbalanced Michelson interferometer which divides the incoming pulses into two identical pulses of one-quarter the original intensity and separates them of 1.5 ns each other.

After the interferometer we placed a f = 200 mm lens that focus the light into a type-II BBO SPDC crystal which generates the entangled photon pairs that are then injected into two single mode optical fibers through a couple of 20 × focusing objectives. In front of the fibers we positioned also two band-pass filters with 810 nm of center wavelength and 7 nm of FWHM bandwidth in order to select only the entangled photon pairs.

The measurement setup consists in two identical Michelson interferometer which have arms with same path difference as the source interferometer. The mirrors of the longest paths are placed upon two positioning stages with nanometric accuracy which can be remotely controlled in order to adjust the path differences. After the interferometers we put some linear optical elements for polarization tomography of the entangled state.

The photons are then injected into two single mode optical fibers which are connected to two SPADs with 40 % of photon detection efficiency, 50 photon/s of dark counts and 40 ns of dead time.

A dedicated time tagger collects then the signals from the SPADs and the trigger photodiode. Since the frequency of the photodiode signal is equal to the laser repetition rate (f = 76 MHz) and the time tagger maximum event rate is 3 MEvents/s, we used a field programmable gate array (FPGA) board to decimate the photodiode signal by a factor of 100.

At the end, all the data from the time-tagger are collected by a Personal Computer (PC) for the elaboration. For individuation of the interference in energy-time entanglement it is necessary to select only the coincidences that are collected in a determinate time window.

6.3 Interferometers stabilization

One of the main problem we had to face was the interferometers stabilization, in fact this is a crucial point for the generation and detection of energy-time entanglement. The path difference between the interferometers arms must be equal for all the three interferometers of the experiments, moreover, also the relative phase between them must be stable for all the duration of the measurements. We tested the stability measuring the coincidence during a long time period, the results are reported in figure 6.3. As we can see the phase of the interferometers is not stable because it varies rapidly.

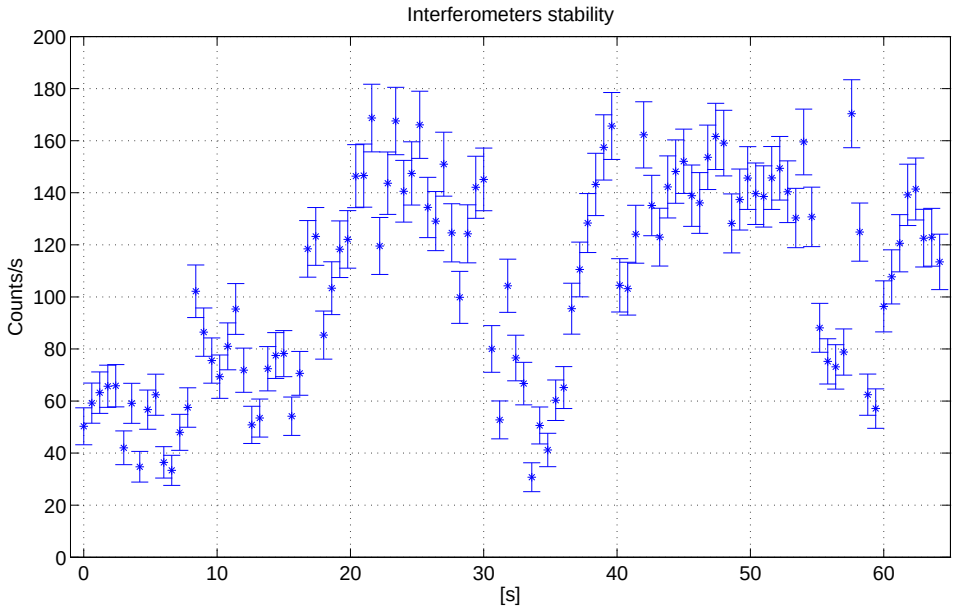


Figure 6.3: Interferometers phase stability before the stabilization during a time period of 60 seconds

To prevent this instability the following solutions were adopted:

- closing the interferometers inside boxes to keep stable the temperature and prevent air flows;
- using feedback stabilized translation stages with nanometric accuracy;
- shortening of the interferometer arms of about one half the previous distance.

The idea of using an active feedback system for the stabilization was discarded because it would have inevitably increased the background noise.

In figure 6.4 we can see that after the stabilization process the relative phase is pretty stable, therefore during the measurements period (about 10 s) it can be considered constant.

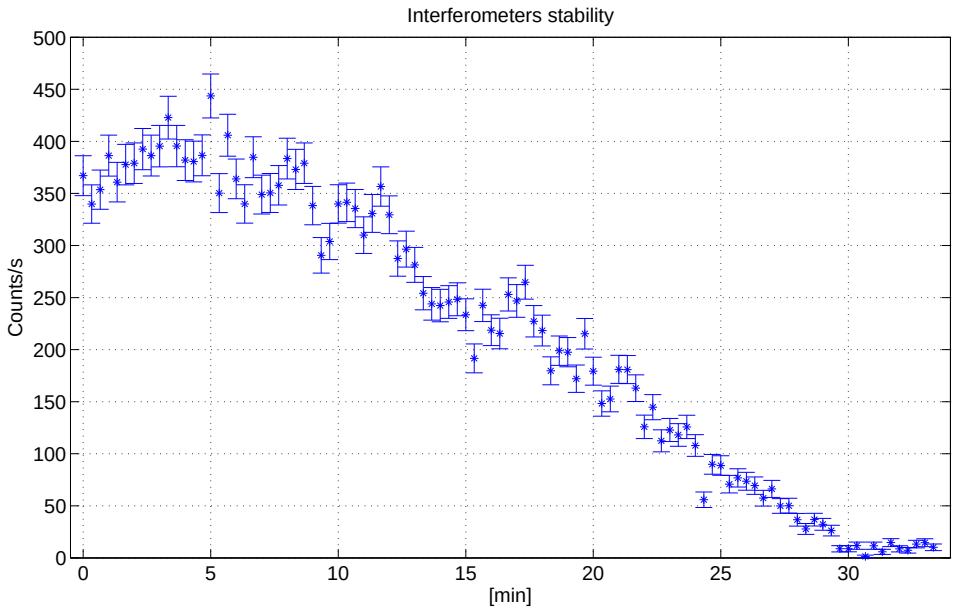


Figure 6.4: Interferometers phase stability after the stabilization during a time period of 33 minutes

6.4 Measurements and analysis of experimental data

We assess the quality of the generated state and the reliability of the measurement system taking the separate tomography of the hyperentangled state. We first took the tomography of the state in the energy-time DOF in two different polarization measurement basis. We then measured the polarization state in the energy-time basis $\{|L\rangle_A, |L\rangle_B\}$ and in the basis $\{|S\rangle_A, |S\rangle_B\}$. The coincidence measurements are taken within a time window of 20 seconds, whereas for the coincidence window we set a period of 2.43 ns. For the density matrix reconstruction we used the maximum-likelihood method described in [99]. For every tomography measurement we calculated also the principal entanglement parameters which are described in appendix B.

6.4.1 Energy-time tomography

In tables 6.1 we present the measurement in the energy-time DOF with the polarization measurement basis $\{|H\rangle_A, |V\rangle_B\}$ and $\{|V\rangle_A, |H\rangle_B\}$ respectively. The expected Bell state from the tomography is Φ^-, which gives the following density matrix:

$$\sigma_{ET} = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} \tag{6.10}$$

The reconstructed density matrix when the polarization measurement basis is set to $\{|H\rangle_A, |V\rangle_B\}$ is:

$$\rho_{HV} = \begin{bmatrix} 0.477 & 0.015+0.015i & 0.016-0.013i & -0.488+0.013i \\ 0.015+0.015i & 0.006 & -0.002+0.002i & -0.013+0.014i \\ 0.016+0.013i & -0.002+0.002i & 0.009 & -0.0-0.01i \\ -0.488-0.013i & -0.013-0.014i & -0.01-0.01i & 0.508 \end{bmatrix} \tag{6.11}$$

and the entanglement parameters are equal to:

Fidelity: $F(\rho_{HV}, \sigma_{ET}) = 0.98$

Tangle: $T(\rho_{HV}) = 0.94$

Purity: $P(\rho_{HV}) = 0.96$

Linear entropy: $S_L(\rho_{HV}) = 0.05$

While for the polarization measurement basis set to $\{|V\rangle_A, |H\rangle_B\}$ the reconstructed density matrix is given by:

$$\rho_{VH} = \begin{bmatrix} 0.494 & -0.018 - 0.013i & -0.017 - 0.001i & -0.46 + 0.013i \\ -0.018 + 0.013i & 0.006 & 0.01 - 0.006i & 0.007 + 0.003i \\ -0.017 + 0.001i & 0.001 + 0.006i & 0.007 & -0.002 + 0.01i \\ -0.46 - 0.013i & 0.007 - 0.003i & -0.002 + 0.01i & 0.493 \end{bmatrix} \tag{6.12}$$

and the entanglement parameters are equal to:

Fidelity: $F(\rho_{VH}, \sigma_{ET}) = 0.95$

Tangle: $T(\rho_{VH}) = 0.86$

Purity: $P(\rho_{VH}) = 0.91$

Linear entropy: $S_L(\rho_{VH}) = 0.11$

The graphical representations of the density matrix for both the tomographies are reproduced in figures 6.5 and 6.6.

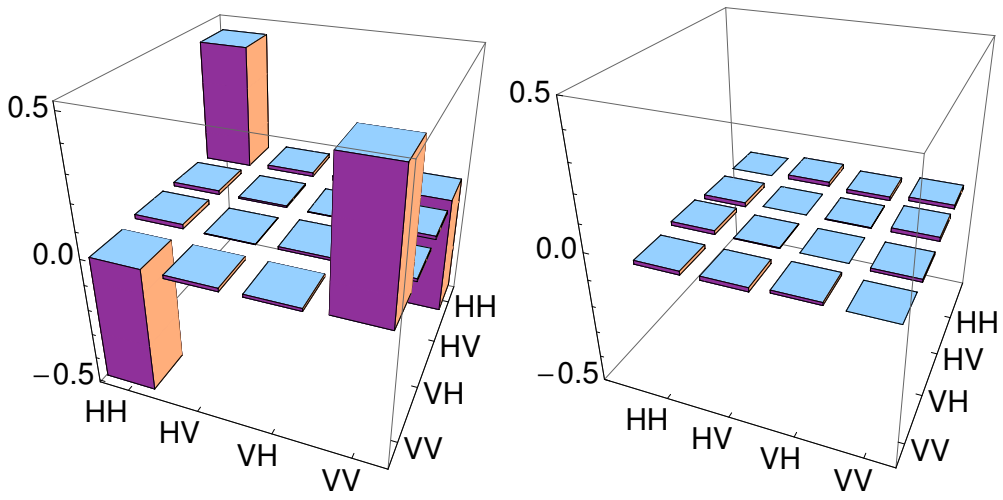


Figure 6.5: The density matrix (real part on the left and imaginary part on the right) of the measured polarization state with $\{|H\rangle_A, |V\rangle_B\}$ polarization basis.

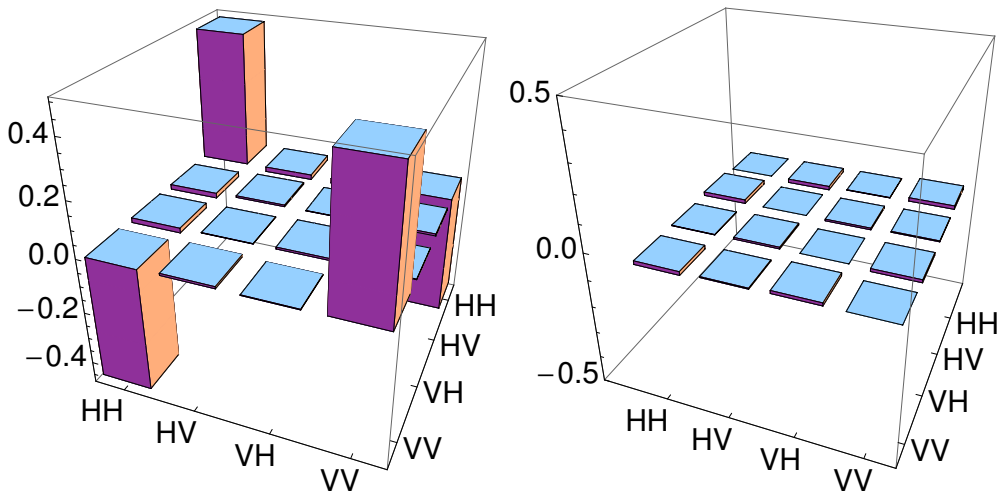


Figure 6.6: The density matrix (real part on the left and imaginary part on the right) of the measured polarization state with $\{|V\rangle_A, |H\rangle_B\}$ polarization basis.

(a) With $\{|H\rangle, |V\rangle\}$ polarization basis

Alice	Bob	Coincidences
$\|L\rangle$	$\|L\rangle$	942
$\|L\rangle$	$\|S\rangle$	5
$\|L\rangle$	$\|D\rangle$	1005
$\|L\rangle$	$\|P\rangle$	7
$\|S\rangle$	$\|L\rangle$	515
$\|S\rangle$	$\|S\rangle$	486
$\|S\rangle$	$\|D\rangle$	495
$\|S\rangle$	$\|P\rangle$	526
$\|D\rangle$	$\|L\rangle$	483
$\|D\rangle$	$\|S\rangle$	10
$\|D\rangle$	$\|D\rangle$	491
$\|D\rangle$	$\|P\rangle$	519
$\|P\rangle$	$\|L\rangle$	505
$\|P\rangle$	$\|S\rangle$	500
$\|P\rangle$	$\|D\rangle$	512
$\|P\rangle$	$\|P\rangle$	16

(b) With $\{|V\rangle, |H\rangle\}$ polarization basis

Alice	Bob	Coincidences
$\|L\rangle$	$\|L\rangle$	686
$\|L\rangle$	$\|S\rangle$	5
$\|L\rangle$	$\|D\rangle$	685
$\|L\rangle$	$\|P\rangle$	3
$\|S\rangle$	$\|L\rangle$	343
$\|S\rangle$	$\|S\rangle$	340
$\|S\rangle$	$\|D\rangle$	355
$\|S\rangle$	$\|P\rangle$	311
$\|D\rangle$	$\|L\rangle$	339
$\|D\rangle$	$\|S\rangle$	5
$\|D\rangle$	$\|D\rangle$	326
$\|D\rangle$	$\|P\rangle$	320
$\|P\rangle$	$\|L\rangle$	331
$\|P\rangle$	$\|S\rangle$	327
$\|P\rangle$	$\|D\rangle$	327
$\|P\rangle$	$\|P\rangle$	4

Table 6.1: Coincidence for energy-time DOF measurement. The states $|D\rangle$ and $|P\rangle$ are equal to: $|D\rangle = 1/\sqrt{2}(|L\rangle + |S\rangle)$ and $|P\rangle = 1/\sqrt{2}(|L\rangle + i|S\rangle$

6.4.2 Polarization tomography

In tables 6.2 we listed the measurement in the energy-time DOF with the polarization basis $\{|L\rangle_A, |L\rangle_B\}$ and $\{|S\rangle_A, |S\rangle_B\}$ respectively. The expected Bell state from the tomography is Ψ^+, which gives the following density matrix:

$$\sigma_P = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{6.13}$$

The reconstructed density matrix when the energy-time measurement basis is set to $\{|L\rangle_A, |L\rangle_B\}$ is:

$$\rho_{LL} = \begin{bmatrix} 0.019 & -0.01 - 0.02i & 0.01 + 0.018i & 0.002i \\ -0.01 + 0.02i & 0.485 & 0.433 - 0.038i & -0.001 - 0.01i \\ 0.01 - 0.018i & 0.433 + 0.038i & 0.481 & -0.002 - 0.005i \\ -0.002i & -0.001 + 0.01i & -0.002 + 0.005 & 0.014 \end{bmatrix} \tag{6.14}$$

and the entanglement parameters are equal to:

Fidelity:	$F(\rho_{LL}, \sigma_P) = 0.92$
Tangle:	$T(\rho_{LL}) = 0.73$
Purity:	$P(\rho_{LL}) = 0.85$
Linear entropy:	$S_L(\rho_{LL}) = 0.2$

While for the energy-time measurement basis set to $\{|S\rangle_A, |S\rangle_B\}$ the reconstructed density matrix is given by:

$$\rho_{SS} = \begin{bmatrix} 0.004 & 0.002 + 0.007i & 0.009 + 0.015i & -0.009 + 0.001i \\ 0.002 - 0.007i & 0.446 & 0.462 + 0.067i & -0.006 - 0.049i \\ 0.009 - 0.015i & 0.462 - 0.067i & 0.520 & -0.03 - 0.028i \\ -0.009 - 0.001i & -0.006 + 0.049i & -0.03 + 0.028i & 0.029 \end{bmatrix} \tag{6.15}$$

and the entanglement parameters are equal to:

Fidelity:	$F(\rho_{SS}, \sigma_P) = 0.95$
Tangle:	$T(\rho_{SS}) = 0.86$
Purity:	$P(\rho_{SS}) = 0.92$
Linear entropy:	$S_L(\rho_{SS}) = 0.11$

The graphical representations of the density matrix for both the tomographies are reproduced in figures 6.7 and 6.8.

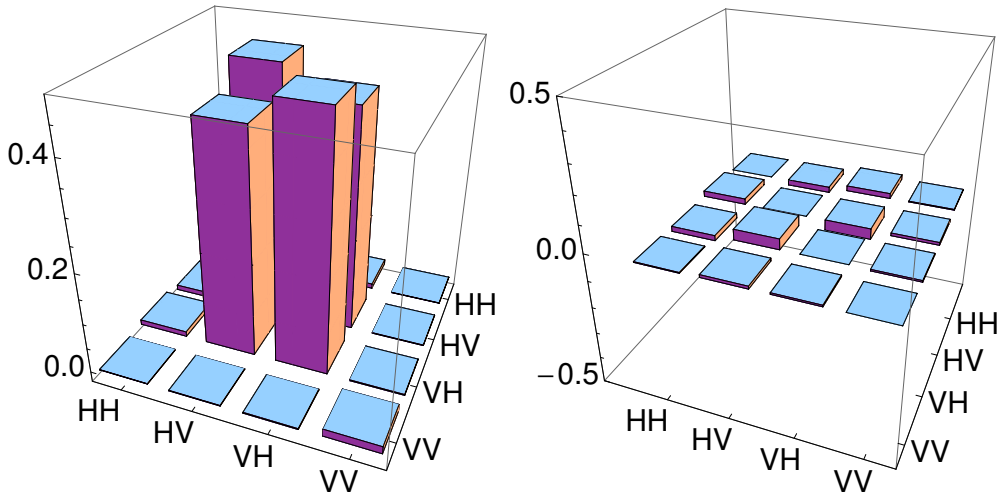


Figure 6.7: The density matrix (real part on the left and imaginary part on the right) of the measured polarization state with $\{|L\rangle_A, |L\rangle_B\}$ energy-time basis.

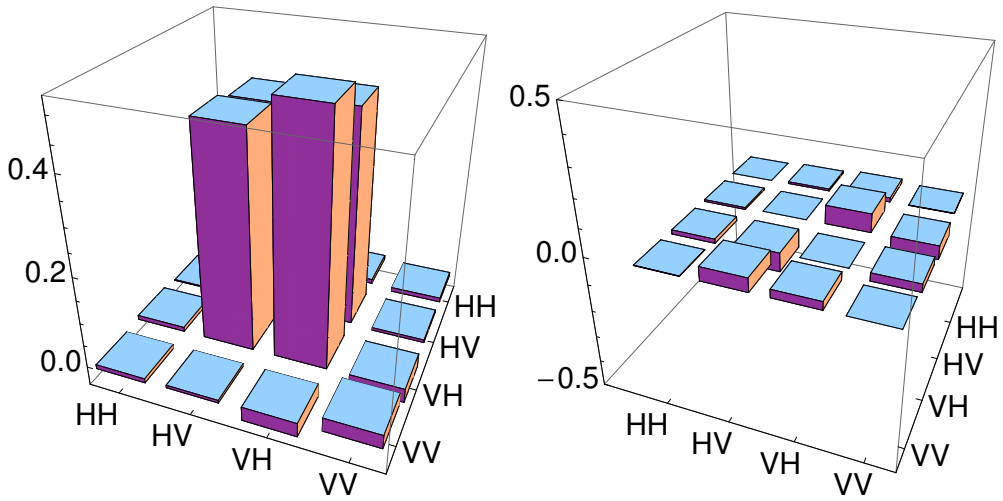


Figure 6.8: The density matrix (real part on the left and imaginary part on the right) of the measured polarization state with $\{|S\rangle_A, |S\rangle_B\}$ energy-time basis.

(a) With $\{|L\rangle, |L\rangle\}$ energy-time basis

Alice	Bob	Coincidences
$\|H\rangle$	$\|H\rangle$	13
$\|H\rangle$	$\|V\rangle$	369
$\|H\rangle$	$\|+\rangle$	12
$\|H\rangle$	$\|R\rangle$	361
$\|V\rangle$	$\|H\rangle$	157
$\|V\rangle$	$\|V\rangle$	197
$\|V\rangle$	$\|+\rangle$	183
$\|V\rangle$	$\|R\rangle$	197
$\|+\rangle$	$\|H\rangle$	175
$\|+\rangle$	$\|V\rangle$	361
$\|+\rangle$	$\|+\rangle$	185
$\|+\rangle$	$\|R\rangle$	165
$\|R\rangle$	$\|H\rangle$	172
$\|R\rangle$	$\|V\rangle$	178
$\|R\rangle$	$\|+\rangle$	150
$\|R\rangle$	$\|R\rangle$	12

(b) With $\{|S\rangle, |S\rangle\}$ energy-time basis

Alice	Bob	Coincidences
$\|H\rangle$	$\|H\rangle$	12
$\|H\rangle$	$\|V\rangle$	437
$\|H\rangle$	$\|+\rangle$	23
$\|H\rangle$	$\|R\rangle$	515
$\|V\rangle$	$\|H\rangle$	226
$\|V\rangle$	$\|V\rangle$	296
$\|V\rangle$	$\|+\rangle$	233
$\|V\rangle$	$\|R\rangle$	264
$\|+\rangle$	$\|H\rangle$	269
$\|+\rangle$	$\|V\rangle$	477
$\|+\rangle$	$\|+\rangle$	192
$\|+\rangle$	$\|R\rangle$	209
$\|R\rangle$	$\|H\rangle$	221
$\|R\rangle$	$\|V\rangle$	239
$\|R\rangle$	$\|+\rangle$	192
$\|R\rangle$	$\|R\rangle$	10

Table 6.2: Coincidence for polarization DOF measurement. The states $|+\rangle$ and $|R\rangle$ are equal to: $|+\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle)$ and $|R\rangle = 1/\sqrt{2}(|H\rangle + i|V\rangle$

6.5 Conclusions and future steps

In this chapter we proposed the design and the experimental realization of a system for the generation and measurement of photon states which are entangled in both polarization and energy-time. We realized the apparatus considering the portability of the system and a possible use for long-range transmission. We focused in the temporal stability of the interferometers which is a crucial point for the energy-time measurements. We finally presented the separate tomographic measurement of both the DOF to verify the validity and the reliability of the system.

As future steps we envisage the complete tomography of the HE state and the demonstration of hyperentanglement distribution at long distances.

CHAPTER 7

Conclusions

This thesis studies the impact of atmospheric turbulence in free-space quantum communication channels and investigates new QKD protocols in order to improve the security and the channel capacity in quantum communications.

We started our study in Chapter 2 with the analysis of atmospheric turbulence by means of propagation at long distances of single beam and twin beam. We showed that also for very long paths propagation the beam diameter is confined to a spot that is only a factor 3 to 5 the diffraction limit. The study of the correlation of two spot in twin beam propagation demonstrated the possibility of the centroid control of the quantum channel by the use of an auxiliary co-propagating beam.

In Chapter 3 we studied the effect of the atmospheric turbulence on the statistic of arrival of single photons over a free-space 143 km optical link. We demonstrated the transformation of the single photon statistic from Poissonian to lognormal distribution. The analysis of the losses along the same link gave us the possibility to develop a technique to exploit the turbulence to improve the signal to noise ratio (SNR) of the channel.

In Chapter 4 we presented the ent-B92 QKD protocol in the 1SDI-QKD and fully DI-QKD scenarios. We derived an efficient key rate in case of detection efficiencies with a great improvement in the 1SDI-QKD case in comparison with the state of the art.

In Chapter 5 we implemented the ent-B92 QKD protocol presented in Chapter

4 using non-maximally entangled states. It was designed and developed an experimental setup for the demonstration of the experimental feasibility of the protocol. Our results showed a good agreement between the theory and the experiments.

Finally, in chapter 6 we developed a system for the generation and the measurement of photon states entangled in both polarization and energy-time DOFs. We designed and realized an experimental apparatus taking particular attention to the temporal stability of the system. We took the separate tomography of each DOF to verify the validity and the reliability of the system. As future steps we envisage the complete tomography of the hyperentangled state and the demonstration of hyperentanglement distribution at long distances.

The study of the QKD had a remarkable development in last thirty years both theoretically and experimentally. Recently, the QKD has also started to grow in the global market, as evidenced by some spin-off companies [100–102]. In the future, the European roadmap [103] envisage further developments in this field to a global quantum network extent.

APPENDIX A

Errors calculation

In this appendix chapter we report the error calculation of the experimental measurements presented in chapter 5. The uncertainty on the measurement is an important parameter to take into account to establish the goodness of experimental results. To calculate the errors in the measurement, the photon source was modeled with a Poissonian statistics, therefore standard deviations were calculated taking the square root of the measured photon counts. Here we report the error estimation for all the analysis parameter of the protocol.

Let's define the parameter $\mathcal{N}$ that will be useful in the error calculation:

$$\mathcal{N} = N(H,H) + N(V,V) + N(H,V) + N(V,H) \tag{A.1}$$

The measurement probability (5.9) can be rewritten as:

$$P(a_k, b_k) = \frac{N(a_k, b_k)}{\mathcal{N}} \tag{A.2}$$

Then the variance for the measurement probability is given by:

$$\sigma^2_{P(a_k,b_k)} = \frac{P(a_k, b_k)}{\mathcal{N}} \left(1 + P(a_k, b_k)\right) \tag{A.3}$$

and the variance of the parameter $\mathcal{N}$ is equal to the parameter itself $\sigma^2_{\mathcal{N}} = \mathcal{N}$.

Let's define three other useful quantities with their respective variance:

$$A = N(a_1 b_1) - N(a_1 \overline{b}_0), \qquad \sigma^2_A = N(a_1 b_1) + N(a_1 \overline{b}_0) \tag{A.4a}$$

$$B = N(\overline{a}_0 b_1) + N(a_0 b_0), \qquad \sigma^2_B = B \tag{A.4b}$$

$$C = N(a_0 b_1) + N(\overline{a}_0 b_0), \qquad \sigma^2_C = C \tag{A.4c}$$

With this definition it is possible to write the Bell's parameter (4.21), the probability of a conclusive event (4.14) and the QBER (4.15) as:

$$S_{\mathrm{CH}} = \frac{A-B}{\mathcal{N}} \tag{A.5a}$$

$$P_{conc} = \frac{1}{2}\frac{B+C}{\mathcal{N}} \tag{A.5b}$$

$$Q_{BER} = \frac{B}{B+C} \tag{A.5c}$$

Standard deviations concerning to the parameters above are equal to:

$$\begin{aligned}
\sigma_{S_{\mathrm{CH}}} &= \sqrt{\frac{\sigma_A^2+B}{\mathcal{N}^2}+\frac{(A-B)^2}{\mathcal{N}^3}} = \sqrt{\frac{\sigma_A^2+B}{\mathcal{N}^2}+\frac{S_{CH}^2}{\mathcal{N}}} \\
\sigma_{Q_{BER}} &= \sqrt{\frac{BC}{(B+C)^3}} = \frac{1}{B+C}\sqrt{Q_{BER}C} \\
\sigma_{P_{conc}} &= P_{conc}\sqrt{\frac{1}{B+C}+\frac{1}{\mathcal{N}}}
\end{aligned} \tag{A.6}$$

A.0.1 Key rate for trusted device case

For the calculation of the standard deviation of the rate let us introduce the following quantity:

$$\mathcal{S} = \frac{(2\log_2 \mathrm{e})(1+2S_{\mathrm{CH}})}{\mathcal{N}\left(\sqrt{1-4S_{\mathrm{CH}}-4S_{\mathrm{CH}}^2}+1-4S_{\mathrm{CH}}-4S_{\mathrm{CH}}^2\right)} \tag{A.7}$$

The rate for the trusted device case can be written as:

$$r = P_{conc}G \tag{A.8}$$

where P_{conc} is the probability of a conclusive event (4.14) and G is defined as:

$$G = 1-\log_2\left(1+\sqrt{1-4S_{\mathrm{CH}}-4S_{\mathrm{CH}}^2}\right)-h_2(Q_{BER}) \tag{A.9}$$

Using the definition (A.5c) for the CH parameter, the probability of a conclusive event and the QBER, we can write the standard deviation for the key rate as:

$$\begin{aligned}
\sigma_r = \sqrt{\sigma_A^2(\mathcal{S}P_{conc})^2 + B\left(\frac{G}{2\mathcal{N}} - P_{conc}\left(\frac{(1-Q_{BER})^2}{C}\log_2\left(\frac{1-Q_{BER}}{Q_{BER}}\right)+\mathcal{S}\right)\right)^2+\cdots} \\
\overline{+\frac{C}{(2\mathcal{N})^2}\left(G+Q_{BER}\log_2\left(\frac{1-Q_{BER}}{Q_{BER}}\right)\right)^2+\mathcal{N}P_{conc}^2\left(\frac{G}{\mathcal{N}}+S_{\mathrm{CH}}\mathcal{S}\right)^2}
\end{aligned} \tag{A.10}$$

A.0.2 Key rate for 1S-DI case

The rate for the 1S-DI case can be written as:

$$r = P_{conc} G \tag{A.11}$$

where G is defined as:

$$G = \eta_B \left[1 - \log_2 \left(1 + \sqrt{1 - 4S_{\mathrm{CH}} - 4S_{\mathrm{CH}}^2} \right) - h_2(Q_{BER}) \right] \tag{A.12}$$

The CH parameter is now equal to:

$$\begin{aligned} S_{\mathrm{CH}} &= \frac{\eta_B [N(a_1,b_1) + N(a_1,b_0) - N(a_0,b_0) - N(\overline{a}_0,b_1)] - N(a_1,b_0) - N(a_1,\overline{b}_0)}{\mathcal{N}} \\ &= \frac{A - \eta_B B}{\mathcal{N}} \end{aligned} \tag{A.13}$$

The quantities B and C are the ones defined in (A.4), while the parameter A become:

$$A = \eta_B \left[N(a_1,b_1) + N(a_1,b_0) \right] - \cdots \tag{A.14}$$

$$- N(a_1,b_0) - N(a_1,\overline{b}_0) \tag{A.15}$$

$$\sigma_A^2 = \eta_B^2 N(a_1,b_1) + \cdots$$

$$+ (\eta_B - 1)^2 N(a_1,b_0) + N(a_1,\overline{b}_0)$$

Then the standard deviation for the key rate is:

$$\begin{aligned} \sigma_r = \sqrt{\sigma_A^2 \left(\frac{\mathcal{S} P_{conc} \eta_B}{\mathcal{N}} \right)^2 + \cdots} \\ \overline{+B \left[\frac{G}{2\mathcal{N}} - \eta_B P_{conc} \left(\mathcal{S}\eta_B + \frac{C}{(B+C)^2} \log_2 \frac{1 - Q_{BER}}{Q_{BER}} \right) \right]^2 + \cdots} \\ \overline{+C \left[\frac{G}{2\mathcal{N}} + \eta_B P_{conc} \left(\frac{Q_{BER}^2}{B} \log_2 \frac{1 - Q_{BER}}{Q_{BER}} \right) \right]^2 + \cdots} \\ \overline{+\mathcal{N} \left[\frac{P_{conc}}{\mathcal{N}} G + \eta_B P_{conc} \left(\mathcal{S} S_{\mathrm{CH}} \right) \right]^2} \end{aligned} \tag{A.16}$$

A.0.3 Key rate for Fully-DI case

The rate for the Fully-DI case can be written as:

$$r = P_{conc} G \tag{A.17}$$

where G is defined as:

$$G = \eta \left[\eta \left(1 - h_2(Q_{BER})\right) - \log_2 \left(1 + \sqrt{1 - 4S_{CH} - 4S_{CH}^2} \right) \right] \tag{A.18}$$

The CH parameter is now equal to:

$$\begin{aligned} S_{\mathrm{CH}} = & \frac{\eta^2 \left[N(a_1, b_1) + N(a_1, b_0) \right]}{\mathcal{N}} + \cdots \\ & + \frac{\eta^2 \left[N(a_0, b_1) + N(\overline{a}_0, b_0) - N(\overline{a}_0, b_1) - N(a_0, b_0) \right]}{2\mathcal{N}} - \cdots \\ & - \frac{\eta \left[N(a_1, b_0) + N(a_1, \overline{b}_0) \right]}{\mathcal{N}} - \cdots \\ & - \frac{\eta \left[N(a_0, b_1) + N(\overline{a}_0, b_1) + N(a_0, b_0) + N(\overline{a}_0, b_0) \right]}{2\mathcal{N}} \end{aligned} \tag{A.19}$$

Let us define the following quantities:

$$\begin{aligned} A &= \eta N(a_1, b_1) - N(a_1, \overline{b}_0) + \cdots & \sigma_A^2 &= \eta^2 N(a_1, b_1) + N(a_1, \overline{b}_0) + \cdots \\ &\quad + (\eta - 1) N(a_1, b_0), & &\quad + (\eta - 1)^2 N(a_1, b_0) \\ B &= N(\overline{a}_0, b_1), & \sigma_B^2 &= B \\ C &= N(a_0, b_1), & \sigma_C^2 &= C \\ D &= N(a_0, b_0), & \sigma_D^2 &= D \\ E &= N(\overline{a}_0, b_0), & \sigma_E^2 &= E \end{aligned} \tag{A.20}$$

The CH parameter (A.19), the probability of a conclusive event (4.14) and the QBER (4.15) can be rewritten as:

$$S_{\mathrm{CH}} = \frac{\eta A - \frac{\eta}{2} \left((\eta + 1)(B + D) - (\eta - 1)(C + E) \right)}{\mathcal{N}} \tag{A.21a}$$

$$P_{conc} = \frac{1}{2} \frac{B + C + D + E}{\mathcal{N}} \tag{A.21b}$$

$$Q_{BER} = \frac{B + C}{B + C + D + E} \tag{A.21c}$$

Then the standard deviation for the key rate is equal to:

$$\sigma_r = \sqrt{\sigma_A^2 \left[\eta^2 \mathcal{S} P_{conc}\right]^2 + \cdots \atop B\left[\frac{G}{2\mathcal{N}} - \eta^2 P_{conc}\left(\frac{\mathcal{S}}{2}(\eta+1) + \log_2\left(\frac{1-Q_{BER}}{Q_{BER}}\right)\frac{1-Q_{BER}}{2\mathcal{N}P_{conc}}\right)\right]^2 + \cdots \atop +C\left[\frac{G}{2\mathcal{N}} + \eta^2 P_{conc}\left(\frac{\mathcal{S}}{2}(\eta-1) - \log_2\left(\frac{1-Q_{BER}}{Q_{BER}}\right)\frac{1-Q_{BER}}{2\mathcal{N}P_{conc}}\right)\right]^2 + \cdots \atop +D\left[\frac{G}{2\mathcal{N}} - \eta^2 P_{conc}\left(\frac{\mathcal{S}}{2}(\eta+1) - \log_2\left(\frac{1-Q_{BER}}{Q_{BER}}\right)\frac{Q_{BER}}{2\mathcal{N}P_{conc}}\right)\right]^2 + \cdots \atop +E\left[\frac{G}{2\mathcal{N}} + \eta^2 P_{conc}\left(\frac{\mathcal{S}}{2}(\eta-1) + \log_2\left(\frac{1-Q_{BER}}{Q_{BER}}\right)\frac{Q_{BER}}{2\mathcal{N}P_{conc}}\right)\right]^2 + \cdots \atop +\mathcal{N}P_{conc}^2\left[\frac{G}{\mathcal{N}} - \eta\mathcal{S}S_{\mathrm{CH}}\right]^2}} \tag{A.22}$$

Threshold detection efficiency for 1sDI case

The threshold detection efficiency for the $\eta_A = 1$ case can be written as:

$$\eta_B = \frac{N(a_1,b_0) + N(a_1,\overline{b}_0)}{N(a_1,b_0) + N(a_1,b_1) - N(a_0,b_0) - N(\overline{a}_0,b_1)} \tag{A.23}$$

where:

$$\begin{aligned} A &= N(a_1,b_0) & \sigma_A^2 &= A \\ B &= N(a_1,\overline{b}_0) & \sigma_B^2 &= B \\ C &= N(a_1b_0) + N(a_1b_1) - \cdots & \sigma_C^2 &= N(a_1b_0) + N(a_1b_1) + \cdots \\ &\quad - N(a_0b_0) - N(\overline{a}_0b_1) & &\quad + N(a_0b_0) + N(\overline{a}_0b_1) \end{aligned} \tag{A.24}$$

Then the standard deviation for the threshold detection efficiency is equal to:

$$\sigma_{\eta_B} = \frac{1}{A+C}\sqrt{A\left(\frac{C-B}{A+C}\right)^2 + B + \sigma_C^2\eta_B^2} \tag{A.25}$$

Threshold detection efficiency for Fully-DI case

The threshold detection efficiency for the $\eta_A = \eta_B = \eta^{th}$ case can be written as:

$$\begin{aligned} \eta^{tr} &= \frac{N(a_1b_0) + N(a_1\overline{b}_0)\frac{1}{2}\left(N(a_0b_1) + N(\overline{a}_0b_1) + N(\overline{a}_0,b_0) + N(a_0,b_0)\right)}{N(a_1b_0) + N(a_1b_1) + \frac{1}{2}\left(N(a_0b_1) + N(\overline{a}_0,b_0) - N(a_0,b_0) - N(a_0b_0)\right)} \\ &= \frac{A+B+C}{A-B+D} \end{aligned} \tag{A.26}$$

where:

$$\begin{aligned}
A &= N(a_1, b_0) + \cdots & \sigma_A^2 &= N(a_1, b_0) + \cdots \\
&\quad + \frac{1}{2}\left(N(a_0, b_1) + N(\overline{a}_0, b_0)\right) & &\quad + \frac{1}{4}\left(N(a_0, b_1) + N(\overline{a}_0, b_0)\right) \\
B &= \frac{1}{2}\left(N(\overline{a}_0, b_1) + N(a_0, b_0)\right) & \sigma_B^2 &= \frac{B}{2} \\
C &= N(a_1, \overline{b}_0) & \sigma_C^2 &= C \\
D &= N(a_1, b_1) & \sigma_D^2 &= D
\end{aligned} \tag{A.27}$$

The standard deviation for the threshold detection efficiency become:

$$\sigma_{\eta^{th}} = \frac{1}{A - B + D}\sqrt{\sigma_A^2\left(\frac{2B + C + D}{A - B + D}\right)^2 + \frac{B}{2}\left(\frac{2A + C + D}{A - B + D}\right)^2 + C + D(\eta^{th})^2} \tag{A.28}$$

APPENDIX B

Entanglement measurements

B.1 Fidelity

The fidelity is the measurement of the closeness of two quantum states with density matrices ρ and σ. It is defined as [104]:

$$F(\rho,\sigma) \equiv \left(\mathrm{Tr}\left(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right)\right)^2 \tag{B.1}$$

In particular, if $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$ are pure states, then

$$F(\rho,\sigma) = |\langle\psi||\phi\rangle|^2 \tag{B.2}$$

Fidelity is a distance measurement with range $0 \leq F(\rho,\sigma) \leq 1$. It can be demonstrated that $F(\rho,\sigma) = 1$ if and only if $\rho = \sigma$.

B.2 Tangle

Let ρ_{AB} be the density matrix of a pair of qubits A and B. The spin-flipped density matrix is defined as:

$$\tilde{\rho}_{AB} = (\sigma_y \otimes \sigma_y)\rho^*_{AB}(\sigma_y \otimes \sigma_y) \tag{B.3}$$

where

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{B.4}$$

is the Pauli matrix. Since ρ_{AB} and $\tilde{\rho}_{AB}$ are positive operators their product $\rho_{AB}\tilde{\rho}_{AB}$ has real and non-negative eigenvalues. Let us take the square root of these eigenvalues in decreasing order: $\lambda_1, \lambda_2, \lambda_3, \lambda_4$. Then the tangle of the density matrix ρ_{AB} is defined as [105]:

$$T(\rho_{AB}) = (\max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4, 0\})^2 \tag{B.5}$$

We can notice that $T(\rho_{AB}) = 0$ corresponds to an unentangled state whereas $T(\rho_{AB}) = 1$ corresponds to a completely entangled state, and the entanglement of formation is a monotonically increasing function of T.

B.3 Purity

The degree of information about the preparation of a quantum state ρ can be characterized by its purity which is defined as [106]:

$$P(\rho) = \mathrm{Tr}(\rho^2) \tag{B.6}$$

The range of purity span from $P(\rho) = 1$, corresponding to a completely pure state, to $P(\rho) = 1/d$, corresponding to a mixed state. d is the dimension of the density matrix ρ.

B.4 Linear entropy

To quantifies the mixedness of a given state ρ we can introduce the linear entropy S_L, which is based on the purity as [107]:

$$S_L(\rho) = \frac{d}{d-1}\left[1 - P(\rho)\right] \tag{B.7}$$

When the state ρ is completely pure we have $S_L(\rho) = 0$ whereas if ρ is completely mixed we have $S_L(\rho) = 1$.

Bibliography

[1] C. H. Bennett, G. Brassard, *et al.*, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, New York, 1984.

[2] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.

[3] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[4] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters*, vol. 94, p. 230504, June 2005.

[5] C. H. Bennett and S. J. Wiesner, "Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[6] F. Dios, J. A. Rubio, A. Rodríguez, and A. Comerón, "Scintillation and beam-wander analysis in an optical ground station-satellite uplink," *Applied optics*, vol. 43, no. 19, pp. 3866–3873, 2004.

[7] V. I. Tatarski, "Wave propagation in a turbulent medium," 1961.

[8] R. L. Fante, "Electromagnetic beam propagation in turbulent media," *Proceedings of the IEEE*, vol. 63, no. 12, pp. 1669–1692, 1975.

[9] R. Fante, "Some new results on propagation of electromagnetic waves in strongly turbulent media," *Antennas and Propagation, IEEE Transactions on*, vol. 23, no. 3, pp. 382–385, 1975.

[10] R. L. Fante, "Electromagnetic beam propagation in turbulent media: an update," *Proceedings of the IEEE*, vol. 68, no. 11, pp. 1424–1443, 1980.

[11] 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 Journal of Physics*, vol. 10, no. 3, p. 033038, 2008.

[12] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein, "How to implement decoy-state quantum key distribution for a satellite uplink with 50 db channel loss," *Physical Review A*, vol. 84, no. 6, p. 062326, 2011.

[13] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New Journal of Physics*, vol. 11, no. 4, p. 045017, 2009.

[14] J. F. Clauser and M. A. Horne, "Experimental consequences of objective local theories," *Phys. Rev. D*, vol. 10, pp. 526–535, Jul 1974.

[15] P. H. Eberhard, "Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment," *Phys. Rev. A*, vol. 47, pp. R747–R750, Feb 1993.

[16] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, "Detection-loophole-free test of quantum nonlocality, and applications," *Phys. Rev. Lett.*, vol. 111, p. 130406, Sep 2013.

[17] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, "Bell violation using entangled photons without the fair-sampling assumption," *Nature*, vol. 497, pp. 227–230, May 2013.

[18] G. Vallone, G. Lima, E. S. Gómez, G. Cañas, J.-A. Larsson, P. Mataloni, and A. Cabello, "Bell scenarios in which nonlocality and entanglement are inversely related," *Phys. Rev. A*, vol. 89, p. 012102, Jan 2014.

[19] G. Vallone, "Einstein-podolsky-rosen steering: Closing the detection loophole with non-maximally-entangled states and arbitrary low efficiency," *Phys. Rev. A*, vol. 87, p. 020101, Feb 2013.

[20] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, Nov 1992.

[21] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," *Phys. Rev. Lett.*, vol. 76, pp. 4656–4659, Jun 1996.

[22] L. Vaidman and N. Yoran, "Methods for reliable teleportation," *Phys. Rev. A*, vol. 59, pp. 116–125, Jan 1999.

[23] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, "Bell measurements for teleportation," *Phys. Rev. A*, vol. 59, pp. 3295–3300, May 1999.

[24] J. T. Barreiro, "Beating the channel capacity limit for linear photonic superdense coding," *Nat Phys*, vol. 4, pp. 282–286, Apr 2008.

[25] M. Lucamarini, G. Vallone, I. Gianani, P. Mataloni, and G. Di Giuseppe, "Device-independent entanglement-based bennett 1992 protocol," *Phys. Rev. A*, vol. 86, p. 032325, Sep 2012.

[26] A. V. Sergienko, *Quantum communications and cryptography.* CRC Press, 2005.

[27] J. Rarity, "Quantum communications and beyond," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1808, pp. 1507–1518, 2003.

[28] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, *et al.*, "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.

[29] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, *et al.*, "Feasibility of 300 km quantum key distribution with entangled states," *New Journal of Physics*, vol. 11, no. 8, p. 085002, 2009.

[30] P. W. Milonni, J. H. Carter, C. G. Peterson, and R. J. Hughes, "Effects of propagation through atmospheric turbulence on photon statistics," *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 6, no. 8, p. S742, 2004.

[31] J. Rarity, P. Tapster, P. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics*, vol. 4, no. 1, p. 82, 2002.

[32] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 9, no. 6, pp. 1541–1551, 2003.

[33] A. Tomaello, C. Bonato, V. Da Deppo, G. Naletto, and P. Villoresi, "Link budget and background noise for satellite quantum key distribution," *Advances in Space Research*, vol. 47, no. 5, pp. 802–810, 2011.

[34] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility analysis for quantum key distribution between a leo satellite and earth," in *Quantum Communication and Quantum Networking*, pp. 96–99, Springer, 2010.

[35] H. Hemmati, *Near-earth laser communications*. CRC Press, 2009.

[36] M. Toyoshima and K. Araki, "Far-field pattern measurement of an onboard laser transmitter by use of a space-to-ground optical link," *Applied optics*, vol. 37, no. 10, pp. 1720–1730, 1998.

[37] A. Tomaello, *Quantum communication channels between earth and space and space to earth*. PhD thesis, Space Sciences, Technologies and Measurements, Sciences and Technologies for Aeronautics and Satellite Applications, 2011.

[38] R. Tyson, *Principles of adaptive optics*. CRC Press, 2010.

[39] V. I. Tatarskii, "The effects of the turbulent atmosphere on wave propagation," 1971.

[40] G. C. Valley, "Isoplanatic degradation of tilt correction and short-term imaging systems," *Applied Optics*, vol. 19, no. 4, pp. 574–577, 1980.

[41] L. C. Andrews and R. L. Phillips, *Laser beam propagation through random media*, vol. 152. SPIE press, 2005.

[42] A. Siegman, "Lasers (university science, mill valley, calif., 1986)," *Chap*, vol. 13, p. 663.

[43] D. L. Fried, "Anisoplanatism in adaptive optics," *JOSA*, vol. 72, no. 1, pp. 52–52, 1982.

[44] R. J. Sasiela, "Electromagnetic wave propagation in turbulence: evaluation and application of mellin transforms," SPIE, 2007.

[45] J. J. Fuensalida, S. Chueca, J. M. Delgado, B. Garcia-Lorenzo, J. M. Rodriguez-Gonzalez, C. K. Hoegemann, E. G. Mendizabal, M. Reyes, M. Verde, and J. Vernin, "Vertical structure of the turbulence above the observatories of the canary islands: parameters and statistics for adaptive optics," in *Proceedings of SPIE*, vol. 5490, pp. 749–757, 2004.

[46] J. A. Louthain and J. D. Schmidt, "Integrated approach to airborne laser communication," in *Remote Sensing*, pp. 71080F–71080F, International Society for Optics and Photonics, 2008.

[47] J. A. Louthain and J. D. Schmidt, "Anisoplanatism in airborne laser communication," *Opt. Express*, vol. 16, no. 14, pp. 10769–10785, 2008.

[48] L. A. Bolbasova and V. P. Lukin, "Modal phase correction for large aperture ground-based telescope with multi-guide stars," in *Proc. SPIE*, vol. 7476, p. 74760M, 2009.

[49] D. L. Fried, "Optical resolution through a randomly inhomogeneous medium for very long and very short exposures," *JOSA*, vol. 56, no. 10, pp. 1372–1379, 1966.

[50] "www.eso.org."

[51] P. Ulrich, "Hufnagel-valley profiles for specified values of the coherence length and isoplanatic angle," tech. rep., MA-TN-88–013, WJ Schafer Associates, 1988.

[52] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, pp. 351–406, May 2001.

[53] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[54] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000.

[55] R. Renner, "Security of quantum key distribution," *International Journal of Quantum Information*, vol. 06, no. 01, pp. 1–127, 2008.

[56] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications*, vol. 3, p. 634, 2012.

[57] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, "Experimental quantum key distribution with finite-key security analysis for noisy channels," *Nature communications*, vol. 4, 2013.

[58] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, "Device-independent quantum key distribution secure against collective attacks," *New Journal of Physics*, vol. 11, no. 4, p. 045021, 2009.

[59] X. Ma and N. Lütkenhaus, "Improved data post-processing in quantum key distribution and application to loss thresholds in device independent qkd," *Quantum Info. Comput.*, vol. 12, no. 3-4, pp. 203–214, 2012.

[60] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, "One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering," *Phys. Rev. A*, vol. 85, p. 010301, Jan 2012.

[61] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," *Phys. Rev. Lett.*, vol. 106, p. 110506, Mar 2011.

[62] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev.*, vol. 47, pp. 777–780, May 1935.

[63] J. S. Bell, "On the einstein-podolsky-rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, 1964.

[64] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969.

[65] J. Renes and R. Renner, "One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys," *Information Theory, IEEE Transactions on*, vol. 58, no. 3, pp. 1985–1991, 2012.

[66] N. Datta and R. Renner, "Smooth entropies and the quantum information spectrum," *Information Theory, IEEE Transactions on*, vol. 55, no. 6, pp. 2807–2815, 2009.

[67] M. Tomamichel, R. Colbeck, and R. Renner, "Duality between smooth min- and max-entropies," *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4674–4681, 2010.

[68] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *Information Theory, IEEE Transactions on*, vol. 55, no. 9, pp. 4337–4347, 2009.

[69] M. Lucamarini, G. Di Giuseppe, and K. Tamaki, "Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states," *Phys. Rev. A*, vol. 80, p. 032327, Sep 2009.

[70] L. Masanes, S. Pironio, and A. Acin, "Secure device-independent quantum key distribution with causally independent measurement devices," *Nat Commun*, vol. 2, no. 238, 2011.

[71] S. J. Jones, H. M. Wiseman, and A. C. Doherty, "Entanglement, einstein-podolsky-rosen correlations, bell nonlocality, and steering," *Physical Review A*, vol. 76, no. 5, p. 052116, 2007.

[72] H. M. Wiseman, S. J. Jones, and A. Doherty, "Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox," *Physical review letters*, vol. 98, no. 14, p. 140402, 2007.

[73] M. Tomasin, "L'entanglement come risorsa nella sperimentazione dell'informazione quantistica," Master's thesis, Department of information engineering, 2012.

[74] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultrabright source of polarization-entangled photons," *Phys. Rev. A*, vol. 60, pp. R773–R776, Aug 1999.

[75] M. Barbieri, C. Cinelli, P. Mataloni, and F. De Martini, "Polarization-momentum hyperentangled states: Realization and characterization," *Phys. Rev. A*, vol. 72, p. 052110, Nov 2005.

[76] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, "Generation of hyperentangled photon pairs," *Phys. Rev. Lett.*, vol. 95, p. 260501, Dec 2005.

[77] K. Chen, C.-M. Li, Q. Zhang, Y.-A. Chen, A. Goebel, S. Chen, A. Mair, and J.-W. Pan, "Experimental realization of one-way quantum computing with two-photon four-qubit cluster states," *Phys. Rev. Lett.*, vol. 99, p. 120503, Sep 2007.

[78] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Experimental demonstration of a hyper-entangled ten-qubit schrödinger cat state," *Nature Physics*, vol. 6, no. 5, pp. 331–335, 2010.

[79] G. Vallone, E. Pomarico, F. De Martini, and P. Mataloni, "Active one-way quantum computation with two-photon four-qubit cluster states," *Physical review letters*, vol. 100, no. 16, p. 160502, 2008.

[80] G. Vallone, E. Pomarico, P. Mataloni, F. De Martini, and V. Berardi, "Realization and characterization of a two-photon four-qubit linear cluster state," *Phys. Rev. Lett.*, vol. 98, p. 180502, May 2007.

[81] N. D. Mermin, "Extreme quantum entanglement in a superposition of macroscopically distinct states," *Phys. Rev. Lett.*, vol. 65, pp. 1838–1840, Oct 1990.

[82] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond bell's theorem," in *Bell's theorem, quantum theory and conceptions of the universe*, pp. 69–72, Springer, 1989.

[83] T. Vértesi, S. Pironio, and N. Brunner, "Closing the detection loophole in bell experiments using qudits," *Phys. Rev. Lett.*, vol. 104, p. 060401, Feb 2010.

[84] S. Massar, "Nonlocality, closing the detection loophole, and communication complexity," *Phys. Rev. A*, vol. 65, p. 032121, Mar 2002.

[85] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993.

[86] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 80, pp. 1121–1125, Feb 1998.

[87] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, 1997.

[88] T. Jennewein, G. Weihs, J.-W. Pan, and A. Zeilinger, "Experimental nonlocality proof of quantum teleportation and entanglement swapping," *Phys. Rev. Lett.*, vol. 88, p. 017903, Dec 2001.

[89] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: Entangling photons that never interacted," *Phys. Rev. Lett.*, vol. 80, pp. 3891–3894, May 1998.

[90] F. Sciarrino, E. Lombardi, G. Milani, and F. De Martini, "Delayed-choice entanglement swapping with vacuum-one-photon quantum states," *Phys. Rev. A*, vol. 66, p. 024309, Aug 2002.

[91] A. Ekert, "Beating the code breakers," 1992.

[92] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, pp. 145–195, 2002.

[93] M. Barbieri, G. Vallone, P. Mataloni, and F. De Martini, "Complete and deterministic discrimination of polarization bell states assisted by momentum entanglement," *Phys. Rev. A*, vol. 75, p. 042317, Apr 2007.

[94] P. G. Kwiat and H. Weinfurter, "Embedded bell-state analysis," *Phys. Rev. A*, vol. 58, pp. R2623–R2626, Oct 1998.

[95] C. Schuck, G. Huber, C. Kurtsiefer, and H. Weinfurter, "Complete deterministic linear optics bell state analysis," *Phys. Rev. Lett.*, vol. 96, p. 190501, May 2006.

[96] S. P. Walborn, S. Pádua, and C. H. Monken, "Hyperentanglement-assisted bell-state analysis," *Phys. Rev. A*, vol. 68, p. 042313, Oct 2003.

[97] G. Vallone and P. Mataloni, "Generation and applications of n-qubit hyperentangled photon states," *Advances in Atomic Molecular and Optical Physics*, vol. 60, pp. 291–314, 2011.

[98] J. D. Franson, "Bell inequality for position and time," *Phys. Rev. Lett.*, vol. 62, pp. 2205–2208, May 1989.

[99] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, "Measurement of qubits," *Phys. Rev. A*, vol. 64, p. 052312, Oct 2001.

[100] "www.idquantique.com."

[101] "www.sequrenet.com."

[102] "www.magiqtech.com."

[103] P. Zoller, T. Beth, D. Binosi, R. Blatt, H. Briegel, D. Bruss, T. Calarco, J. Cirac, D. Deutsch, J. Eisert, *et al.*, "Quantum information processing and communication: Strategic report on current status, visions and goals for research in europe," *The European Physical Journal D*, vol. 36, no. 2, pp. 203–228, 2005.

[104] R. Jozsa, "Fidelity for mixed quantum states," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[105] V. Coffman, J. Kundu, and W. K. Wootters, "Distributed entanglement," *Phys. Rev. A*, vol. 61, p. 052306, Apr 2000.

[106] G. Adesso, A. Serafini, and F. Illuminati, "Entanglement, purity, and information entropies in continuous variable systems," *Open Systems and Information Dynamics*, vol. 12, no. 2, pp. 189–205, 2005.

[107] N. A. Peters, T.-C. Wei, and P. G. Kwiat, "Mixed-state sensitivity of several quantum-information benchmarks," *Phys. Rev. A*, vol. 70, p. 052309, Nov 2004.

List of Publications

The work presented in this thesis has in part been published in the following references.

Journal Papers

[J1] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, R. Ursin, G. Vallone, and P. Villoresi, "Impact of turbulence in long range quantum and classical communications," *Physical review letters*, vol. 109, no. 20, p. 200502, 2012.

[J2] G. Vallone, A. Dall'Arche, M. Tomasin, and P. Villoresi, "Loss tolerant device-independent quantum key distribution," *arXiv preprint arXiv:1310.6664*, 2013.

Conference Proceedings

[P1] G. Vallone, P. Villoresi, I. Capraro, A. Dall'Arche, A. Tomaello, and F. Gerlin, "Experimental study of free-space beam propagation for single-photon quantum communications," in *Quantum Information and Measurement*, Optical Society of America, 2012.

[P2] R. Corvaja, I. Capraro, A. Dall'Arche, N. D. Pozza, F. Gerlin, A. Tomaello, M. Zorzi, A. Assalini, A. Ferrante, G. Pierobon, F. Ticozzi, G. Vallone, and P. Villoresi, "Engineering a long distance free-space quantum channel," in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, ISABEL '11, (New York, NY, USA), pp. 187:1–187:5, ACM, 2011.

[P3] I. Capraro, A. Tomaello, A. Dall'Arche, F. Gerlin, G. Vallone, and P. Villoresi, "Long range beam propagation for quantum communications," *Proc. SPIE*, vol. 8246, pp. 82460H–82460H–7, 2012.

[P4] I. Capraro, A. Tomaello, A. Dall'Arche, and P. Villoresi, "Long-range beam propagation for single-photon communications," *Proc. SPIE*, vol. 8161, pp. 81610C–81610C–8, 2011.

[P5] I. Capraro, D. Bacco, A. Dall'Arche, D. Marangon, F. Gerlin, A. Tomaello, G. Vallone, and P. Villoresi, "Quantum communications along the canary strongly-turbulent optical link," in *Imaging and Applied Optics*, p. PTu1F.4, Optical Society of America, 2013.

Conference submission

[S1] I. Capraro, D. Bacco, A. Dall'Arche, D. Marangon, F. Gerlin, A. Tomaello, G. Vallone, and P. Villoresi, "Quantum communications along optical links with strong turbulence." Invited talk. *AOIM 2013 Stellenbosh (RSA).*, September 2013.

[S2] I. Capraro, D. Bacco, A. Dall'Arche, D. Marangon, F. Gerlin, A. Tomaello, G. Vallone, and P. Villoresi, "Quantum communications with strong turbulent." Talk. *Laser Physics Workshop 2013 Prague.*, July 2013.

[S3] G. Vallone, A. Dall'Arche, M. Tomasin, and P. Villoresi, "Exploiting bell's inequality to extend the device-independent quantum key distribution." Talk. *"Quantum [Un] Speakables II: 50 Years Bell's Theorem" University of Vienna & Austrian Academy of Sciences.*, June 2014.

[S4] I. Capraro, D. Bacco, A. Dall'Arche, D. Marangon, F. Gerlin, A. Tomaello, G. Vallone, and P. Villoresi, "Loss tolerant device-independent quantum key distribution by non-maximally entangled states." Talk. *Quantum 2014, VII workshop ad memoriam of Carlo Novero, Torino.*, May 2014.

[S5] A. Dall'Arche, D. Bacco, D. Marangon, M. Tomasin, F. Gerlin, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, "Quantum and classical resources

for free-space quantum communications." Invited Talk. *Quantum 2014, VII workshop ad memoriam of Carlo Novero, Torino.*, May 2014.

[S6] G. Vallone, A. Dall'Arche, D. Bacco, D. Marangon, M. Tomasin, F. Gerlin, M. Canale, N. Laurenti, and P. Villoresi, "Turbulence as a resource in quantum communications." Invited Talk. *International Conference 'Laser Optics", St.Petersburg, Russia*, June 2014.