Università degli Studi di Padova

Sede Amministrativa: Università degli Studi di Padova
Dipartimento di Ingegneria dell'Informazione (DEI)

CORSO DI DOTTORATO DI RICERCA IN: Ingegneria dell'Informazione

CURRICOLO: Scienza e Tecnologia dell'Informazione (I.C.T.)

CICLO XXIX

Quantum information with polarization and temporal degrees of freedom

Coordinatore: Ch.mo Prof. Matteo Bertocco
Supervisore: Ch.mo Prof. Paolo Villoresi

Dottorando: Marco Tomasin

Quantum information with polarization and temporal degrees of freedom

Abstract

This work deals with creation, manipulation and detection of quantum photon states, in one and two degrees of freedom, encoded in polarization and time-bin basis. A particular quantum state, an entangled state, carries a wide range of implementations, that are impossible via classical tasks, such as teleportation, dense coding, and quantum communication protocols. One of these tasks, quantum cryptography, allows intrinsically secure transmission of information. Nowadays, quantum key distribution is implemented in intercity quantum networks, by using telecommunication fibers to connect nodes within the network. In future scenarios, photons could travel through greater distances, but, due to losses, fiber links need for quantum repeater, a very demanding engineering solution. An alternative way, is the use of free-space satellite quantum networks.

Here we focus on polarization and time bin degrees of freedom (DOFs) of the photons as a resource for quantum information. In particular we study the possibility to share an hyper-entangled state in polarization and time-bin DOFs between two spatially separated users. In addition we study a new tomographic method, based on compressed sensing, to recover the density matrix of a quantum state when prior information are available.

Typical implementation of time-bin photon source, based on Franson's scheme, suffers on intrinsic loophole. To overcome that we experimentally demonstrated that with a time-bin source it is possible to obtain a very high visibility in order to violate a chained Bell inequality.

Interference at single photon level through satellite-ground channels is presented here, showing that, temporal encoding is preserved along turbulent channels. With this experiment we show that temporal encoding can be use for a future implementation of satellite quantum communication.

Finally, to complete this work, we demonstrate a new method to certified the randomness of a source, useful in many task, such as quantum cryptography by using a polarization entangled photons source.

Quantum information with polarization and temporal degrees of freedom

Sommario

Questo lavoro è incentrato sulla creazione, manipolazione e rivelazione di fotoni, in uno o due gradi di libertà, codificati nel dominio del tempo o della polarizzazione. L'entanglement quantistico può essere usato per una vasta gamma di applicazioni che non sono possibili classicamente, come il teletrasporto quantistico, il denscoding e la crittografia quantistica. Quest'ultima, fornisce un grado di sicurezza incondizionato, poichè basata su leggi fisiche. Attualmente, le reti di comunicazione quantistica sono state implementate a livello cittadino utilizzando fibre ottiche per le telecomunicazioni. In uno scenario futuro, sarà necessario raggiungere distanze maggiori, ma a causa delle alte perdite, soluzioni basate su link in fibra saranno difficili da implementare. Un'alternativa è quella di utilizzare reti satellitari per le comunicazioni quantistiche.

In questo lavoro ci focalizziamo sulla realizzazione di una sorgente di fotoni hyper-entangled in tempo e polarizzazione. La particolarità di questa sorgente è la possibilità di condividere lo stato tra due utenti spazialmente separati. Inoltre, abbiamo sviluppato un algoritmo di tomografia quantistica basato sul compressed sensing, per la ricostruzione di uno stato con un numero molto limitato di misure. Per poter funzionare, questo algoritmo ha bisogno di informazioni sullo stato di partenza.

Successivamente, vedremo come il loophole dovuto alla postselezione in una sorgente di fotoni entangled in time-bin, può essere superato con una buona implementazione del setup ottico. Infatti nel nostro esperimento è stato possibile raggiungere una visibilità molto elevata, che ha permesso di violare le disuguaglianze di Bell concatenate.

Vedremo inoltre, la possibilità di utilizzare fotoni codificati nel dominio temporale in un canale satellite-terra. Infatti, abbiamo dimostrato che la turbolenza non rovina lo stato inviato, aprendo la strada a futuri sviluppi basati sulla codifica temporale.

Infine, per completare questo lavoro, una sorgente di fotoni entangled in polarizzazione è stata utilizzata per dimostrare un nuovo metodo per la certificazione della randomicità di una sorgente.

Contents

Introduction 1

1 Quantum communications and Quantum protocols 4
- 1.1 Classical communication . . . 5
- 1.2 Quantum bit . . . 5
- 1.3 Entanglement . . . 8
- 1.4 EPR paradox . . . 11
- 1.5 Bell inequality . . . 12
- 1.6 Quantum communication protocols . . . 16

2 Hyper-Entanglement 22
- 2.1 Polarization Entanglement . . . 23
- 2.2 Time bin entanglement . . . 28
- 2.3 Generation of Hyper-Entanglement in two degrees of freedom . . . 32
- 2.4 Experimental setup . . . 34
- 2.5 Results . . . 42
- 2.6 Conclusion . . . 46

3 Efficient Quantum Tomography 48
- 3.1 Classical compressed sensing . . . 49
- 3.2 Quantum tomography via compressed sensing . . . 51
- 3.3 Fast reconstruction for a state with prior information . . . 53
- 3.4 Result for simulation and real cases . . . 58
- 3.5 Conclusion . . . 65

4 High visibility time-bin entanglement for Chained Bell inequality 66
4.1 Loophole in time bin entanglement . . . 67
4.2 CH chained inequality . . . 73
4.3 Experimental setup . . . 76
4.4 Stabilization . . . 78
4.5 Result . . . 82
4.6 Future implementation . . . 85
4.7 Conclusion . . . 88

5 Interference from satellite 90
5.1 Description of the experiment . . . 91
5.2 Experimental result . . . 95
5.3 Interferometer visibility . . . 100
5.4 Conclusion . . . 103

6 Certified Quantum randomness 105
6.1 QRNG . . . 106
6.2 Up-certified quantum random-number generator . . . 108
6.3 Experimental realization . . . 110
6.4 Conclusion . . . 113

7 Conclusion 115

Appendix A Proof of the min-entropy bound 117
A.1 Uncertainty principle . . . 117
A.2 Proof of the bound . . . 118

References 129

List of Figures

1.1 The source S produces pairs of photons, sent to A and B. The measurements a and b are chosen by the experimenter. $D+$ is the detector relative to a detection of $+1$, $D-$ is the detector relative to a detection of -1. Image from Wikipedia[1]. 14

2.1 Polarization entangled photon generated by a type II SPDC crystal 24

2.2 Encoding in the temporal DOF. The apparatus consists of an unbalanced Michelson interferometer with a short and a long arm. After the interferometer, the photon is in a coherent superposition of the two possible events $|S_p\rangle$ and $|L_p\rangle$. The relative phase θ_e depends on unbalancement between the two arms. Realized with ComponentLibrary[2]. 30

2.3 Time-bin coincidence in function of the phases θ_A and θ_B. The phase is expressed in relation to the shift of the positioner, $\phi = 2\pi \cdot 2\Delta L/\lambda$, where ΔL is the shift and λ is the wavelength of the photons. Only the Alice's phase is changed by moving the positioner by a 20 nm steps, over a 900 nm range. 32

2.4 Time-bin coincidence distribution with respect to the laser pulses. (Top ideal case, bottom experimental acquisition) 33

2.5 Setup of the hyperentanglement source. A detailed version of the SPDC source can be found in fig.2.6. Realized with ComponentLibrary[2]. 35

2.6 Detail of the setup for the generation of polarization entanlged photon pairs. Lens $L_1 = 75mm$ is used to focus the infrared beam of the pulsed laser on the SHG crystal. Lens $L_2 = 200mm$ is used to collimate the SHG beam. Realized with ComponentLibrary[2]. 36

2.7 In this figure we can see the plots for pump and idler/signal waists. All the distances are take from the same fixed point (the position of the SPDC crystal). 37
2.8 The fast scan in fig. (a) was obtained by moving the slider on the long arm of Alice's interferometer. The Bob's slider was stopped. This scan provides a coarse position of the minimum. The fine scan, fig. (b), provides a better position of the minimum. In this case, the position of the minimum has been found around 339 nm. At this point, the phases of Alice and Bob are set equal to zero, $\theta_A = \theta_B = 0$. 39
2.9 In this figure we can see destructive and constructive interference in the central peak. The visibility in this case, was $V = (\max - \min)/(\max + \min) \approx 94\%$. 39
2.10 Decimate synchronization pulses are sent to Alice (A) and Bob (B) time to digital converters. Black lines indicate trigger synchronization events, red lines indicate photons detection on Alice side and with green lines photons detection on Bob side. In the ideal case, the same time interval, T, has to be measured in Alice and Bob's TDCs with the same value. But due to different internal clock drift, Bob's time interval T_B differs from Alice's time interval T_A. To recover a correlation a stretching is apply to Bob's time tags. 40
2.11 Without any correction (top), the differences between correlated trigger pulses on Alice an Bob, are spread on a very large time interval, precluding a reconstruction of the state. If the time is corrected (bottom), the differences between correlated trigger pulses are very narrow distributed. In this case it is possible to reconstruct a time correspondence between Alice and Bob. 42
2.12 Real and imaginary part of polarization entangled state 43
2.13 Real and imaginary part of time-bin entangled state 45
2.14 Real and imaginary part of hyper-entangled state. Numeric label correspond to ordered basis states $\{|HHSS\rangle, |HHSL\rangle, |HHLS\rangle, |HHLL\rangle, |HVSS\rangle, .., |VVLL\rangle\}$ 47

3.1 Spectrum of a signal with only s frequencies. CS provide an exact reconstruction with only $s\log(n)$ randomly chosen measurements. 51
3.2 Available volume of physical states compatible with the only constraint $\mathrm{Tr}(\mathbf{A}\rho) = a$ for different values d of the space dimension. 56
3.3 Projection of an observable onto a qubit. The white circle represents the all possible observables that give the same projection. The bigger the circle, the smaller the information obtains from observable A. 58

3.4 Fidelity as a function of the number of measurements for three different estimators. The simulated state is an ideal hyper-entagled state. As we can see, our method (best sequence) requires less measurements than the standard method (random sequence) to converge to the final value. When the parameters of eq. 3.19 and eq. 3.20 are optimized, the three estimators give about the same results. We note that Lasso estimator perform little better than the others. Error bars on Best lines are zero because in this simulation we don't add any noise, and the result is deterministic because the measurement set is the same. 62
3.5 Fidelity as a function of the number of measurements for a noisy state. The simulated state is an noisy hyper-entagled state, with color noise $p_c = 0.05$ and white noise $p_w = 0.1$ (see eq.3.22 and 3.23). 62
3.6 Fidelity as a function of the number of measurements for the simulated GHZ state. 63
3.7 Fidelity as a function of the number of measurements for hyper-entanglement experimental state. As we can see, the reconstruction with our methods overshot the final fidelity. This can be explained by the fact that CS try to find a low rank solution which corresponds to a pure state. However, with few measurements it is difficult to estimate the noise, and this fact leads to a purest recovered state than the real state. 63
3.8 Real density matrix from experimental state recover with only 12 measurements with our method (on the left) and with standard method (on the right). Imaginary part can be neglected. 64

4.1 LHV model for time-bin experiment. 69
4.2 In this example, the green and red regions give the values for the hidden variable for which $a = M_-$ and $b = M_+$ hold. The brown area, where the regions overlapped, corresponds to the hidden variables for which both $a = M_-$ and $b = M_+$ hold. The value of this area is equal to the integral 4.8. 71
4.3 Setup of the time-bin entanglement source. Realized with ComponentLibrary[2]. . 77
4.4 In this figure we can see the distribution of the singles. In each channel, the first three peaks refer to time-bin state. The other three peaks refer to singles used to stabilize the interferometers. 80

4.5 In this figure we can see the effect of the stabilization algorithm. When the stabilization is off, the phase drift is very slow. This is due to the positioner that is very stable, thanks to a very precise feedback control. In addition, the interferomenter is protected from air flow with a box. When we stabilize the interferometer with our methods, we achieve a stability for a long time. The value of P_{ratio} is bounded because the visibility on the singles detection are not maximized, due to a alignment difficulties. 81

4.6 Time distribution of singles and coincidences counts. The red bar on singles graph represents the time interval within an event is suitable for coincidence. The coincidences graph represent the coincidences between single events within the red bars, in a window of $0.81\,ns$. 82

4.7 Raw coincidence counts between detectors A and B for different values of phases (red data). The blue data represent the coincidence counts between the orthogonal output of detector A, which is obtained by shifting the phase of A by π, and B. . . 83

4.8 Time-bin setup to avoid LHV model. Realized with ComponentLibrary[2]. 86

4.9 Router for photon pulses. Realized with ComponentLibrary[2]. 86

4.10 Output 1(2) shows the distribution of the singles between two laser pulses on the first(second) output port of the balanced MZI (fig.4.8, $1\,bin = 81\,ps$. The bottom plot, shows how the ratio between the two peaks, $R_{12} = Peak_1/(Peak_1 + Peak_2)$. At 200 s the stabilization of the interferometer was lost by the PID, but after some seconds, it got back to properly work. 88

5.1 Distribution of pulse train at MLRO. Blu pulses are the high-energy pulses for laser ranging measurements, the red pulses are the ones used to generate qubits. 92

5.2 In the top panel we can see the satellite radial velocity, $v_r(t)$, measured for Beacon-C satellite. Its value ranges from -6 to $+6$ km/s as a function of time during a single passage. In the bottom panel, we can see a schematic of the experimental setup. An unbalanced MZI with the two $4f$ systems used for the generation of the state and the measurement of the interference. In the small panel it is shown the typical expected detection pattern of time-bin encoding, where the number of counts N_c in the central peak varies according to the kinematic phase θ imposed by the satellite. 93

5.3 In fig.A is represented the scheme of the unbalanced Mach-Zehnder interferometer with the two $4f$-system. In fig.B we can see the images of the primary mirror obtained with only the short or long arm opened. 94

5.4 Kinematic phase and interference pattern. In the top we show the measured satellite distance and the predicted kinematic phase $\phi(t)$ estimated by eq. 5.2 as a function of time for a passage of the Ajisai satellite. Shaded area represents the temporal window of data acquisition. In the bottom we show the kinematic phase $\phi(t)$ and theoretical probability $P_c(t)$ in the shaded area. The interference patter is modulated according to the value of $\phi(t)$ determined by the satellite velocity. 96

5.5 Constructive and destructive single photon interference [Beacon-C satellite, 11.07.2015 h 1.33 CEST]. (A) Histogram of single photon detections as a function of time $\Delta = t_{meas} - t_{ref}$ realized by selecting only the returns characterized by $\phi(\mod 2\pi) \in [4\pi/5, 6\pi/5]$ that lead to constructive interference. The solid line shows the tri-Gaussian fit. By evaluating the Gaussian integrals we obtained the counts $N_l = 112\pm11$ for the sum of lateral peaks and $N_c = 196\pm14$ for the central one. (B) Histogram of single photon detections realized by selecting only the returns characterized by $\phi(\mod 2\pi) \in [-\pi/5, \pi/5]$. Here, $N_l = 112\pm11$ and $N_c = 46\pm7$. (C) Histogram of single photon detections without any selection on the phase. As expected, the interference is completed washed out and we measured $N_c = 1245\pm35$ and $N_l = 1306 \pm 36$, fully compatible with $P_c = 1/2$. In all panels, the dotted red lines represent the expected counts in case of no interference. 97

5.6 Experimental interference pattern. Experimental probabilities P_c^{exp} as a function of the kinematic phase measured for three different satellites. By fitting the data we estimate the visibilities $V_{exp} = 67\pm11\%$ for Beacon-C, $V_{exp} = 53\pm13\%$ for Stella, and $V_{exp} = 38\pm4\%$ for Ajisai. The dashed lines correspond to the theoretical value of P_c predicted by Eq. 5.1. The points are obtained by considering ten intervals of the phase defined by $\mathcal{I}_j = [(j1/10)\pi,\ (j + 1/10)\pi]$. For each interval we selected the data corresponding to $\phi(\mod 2\pi) \in \mathcal{I}_j$: from such data we determined the experimental probability of detection in the central peak P_c^{exp} and we averaged the corresponding phase ϕ. We note that at the point $\phi = 0$ and $\phi = 2\pi$ the same subset of data was selected 99

5.7 Visibility in function of rtt. Left panel shows the visibility obtained with the old configuration. Right panel shows the visibility obtained with the new one. 101

5.8 Experimental setup used to evaluate the term $\delta\theta(\tau)$. Realized with ComponentLibrary[2]. 102

6.1 Scheme of the QRNG. The state ρ_A is the source of randomness that can be correlated with a larger system E. An initial true random seed of length $t(m)$ is used to switch between the $\{\hat{\mathcal{M}}_z\}$ and $\{\hat{\mathcal{N}}_x\}$ POVMs, from which the variables Z and X are extracted. Z is used to generate the random sequence, while X is used to evaluate how many true random bits can be extracted by Z. Y represents the final true random sequence. 109

6.2 Scheme of experimental setup. 111

6.3 Average experimental rate for the qubit QRNG. Blue circles represent the experimental average rate $\widetilde{r}$ of true random bits per measurement, while the continuous red line is the theoretical prediction with $\rho_X = \sum_{x=0}^{1} = p_x|x\rangle\langle x|$ where $p_0 = 0.9973$ and $p_1 = 0.0027$. The shaded red area represents the theoretical standard deviation of the rate, while gray rectangles show the experimental standard deviation of the rate. Green crosses show the classical min-entropy estimated on the Z random variable. The asymptotic limit $H_\infty(Z)$ is evaluated on the state $\rho_Z = \sum_{z=0}^{1} P_z|z\rangle\langle z|$ with $P_0 = 0.5020$ and $P_1 = 0.4980$. 112

6.4 Average experimental rate for the ququart QRNG. For notations, see fig.6.3. In this case $\rho_X = \sum_{x=0}^{3} p_x|x\rangle\langle x|$ with $p_0 = 0.9937$, $p_1 = 0.00359$, $p_2 = 0.00266$ and $p_3 = 1 - p_0 - p_1 - p_2$. For ρ_Z we have $\rho_Z = \sum_{z=0}^{3} P_z|z\rangle\langle z|$ with $P_0 = 0.2527$, $P_1 = 0.2412$, $P_2 = 0.2608$ and $P_3 = 0.2453$. 113

List of Tables

1.1 Depending on the values of the two bits x and y, Alice applies a transformation to the state $|\Phi^+\rangle$. At the end Alice and Bob share one of the four Bell states. 16

3.1 First 12 measurements from the best sequence find by our methods. 61
3.2 Entanglement measurements for the state recovered with 12 measurement by using our method. The linear entropy is lower compared to the recovered state with 144 measurements. See fig. 3.7. 64
3.3 Entanglement measurements for the state recovered with 12 measurement by using standard compressed sensing. 65

4.1 Results for the set of measurements, with N= 3. $S^3_{LHV,i}$ correspond to the value predicted by a local hidden variable model. The reported $S^3_{CH,i}$ has been calculated from the raw coincidence. 84
4.2 Results for the set of measurements, with N=4. $S^4_{LHV,i}$ correspond to the value predicted by a local hidden variable model. The reported $S^4_{CH,i}$ has been calculated from the raw coincidence. 85
4.3 Results for the set of measurements, with N= 5. $S^5_{LHV,i}$ correspond to the value predicted by a local hidden variable model. The reported $S^5_{CH,i}$ has been calculated from the raw coincidence. 85

5.1 Values of $P_c^{(\exp)}$ for constructive and destructive interference obtained from the passage of Beacon-C satellite, 11.07.2015 h 1.33 CEST. 98
5.2 Visibilities and ranges for three satellite, Beacon-C, 11.07.2015, h 1.33 CEST; Stella, 12.07.2015, h 3.08 CEST; Ajisai, 12.07.2015, h 3.42 CEST. 98

5.3 Source mean photon per pulse for three satellite, Beacon-C, 11.07.2015, h 1.33 CEST; Stella, 12.07.2015, h 3.08 CEST; Ajisai, 12.07.2015, h 3.42 CEST. 100

To Alice, Bob and especially to Eve,
whose life has made hard by the first two...

...to Chiara and my family

Acknowledgments

Desidero ringraziare il Prof. Paolo Villoresi per avermi dato un'altra volta la possibilità di lavorare in questo campo, raggiungendo dei risultati molto importanti. Lo ringrazio anche per le varie discussioni avute al di fuori del mondo della ricerca. Ringrazio inoltre il Dr. Giuseppe Vallone, per avermi supportato e sopportato per tutto questo tempo, scontrandosi più volte con la mia testardaggine. Durante il mio lavoro è stato di fondamentale aiuto. Un ringraziamento speciale va a Davide Marangon, per essere stato sempre disponibile nell'aiutarmi. Ringrazio di cuore tutti gli altri colleghi: Matteo Schiavon, con il quale ho condiviso in questi tre anni laboratorio, viaggi, conferenze e idee; Daniele Dequal e Andrea Stanco per le interessanti discussioni, anche in ambito musicale e fotografico e per le idee di business; Francesco Vedovato, Elia Mantoan e Francesco Raffaelli per l'aiuto che mi hanno dato negli esperimenti; Costantino Agnesi, Marco Avesani, Alberto Donazzan, Luca Calderaro, Giacomo Pantaleoni, Mirko Pittaluga, e tutti gli altri colleghi del Luxor. Infine desidero ringraziare Chiara, la mia famiglia e tutti i miei amici che in questi tre anni mi hanno sempre sostenuto.

Introduction

At the beginning of the last century, scientists were working to a new, challenging, but counter intuitive theory, quantum mechanics. Over the years, many optical quantum experiments have been proposed and realized to create, manipulate and measure quantum systems. Even though the correspondence between theory predictions and experimental results was very strong, there were lots of doubts about the presence of an inherently statistical theory that could describe the nature like quantum mechanics, as proposed by Einstein, together with Podolski and Rosen, in their famous paper published in 1935. Many years later, in 1964, John Bell showed, by simple inequalities, that experimental prediction of quantum mechanics are not consistent with the assumption made by EPR. Many tests of Bell inequalities have been carried out, always showing a result that confirm quantum mechanics predictions. However, in these tests, several problems in experimental design affect the validity of the experimental findings. These problems, called loopholes, could change Bell inequality allowing a classical violation of them. Provide an experiment without these loopholes, is very important in order to make a contradiction with local realism.

Violation of Bell's inequalities can be used by two users to exchange secure information by a new

cryptographyc paradigm, quantum key distribution (QKD). This is the task which exchanges cryptographic keys between users in an unconditionally secure way, because its security is based on physics principles. The security of classical cryptography instead, is based on mathematical algorithms. The difficulty that an eavesdropper has to obtain information depends on the available computing capacity. If a quantum computer is built in the future, the computing power will be enough to make obsolete and insecure the classical cryptographic system used today.

QKD exchanges a random secure secret key between two users, Alice and Bob. This key, which is known only to Alice and Bob, can be used to encrypt and decrypt messages shared between them. If an eavesdropper intercepts the key, Alice and Bob will detected anomalies in process, and then the communication will be aborted. Nowadays, QKD devices are commercially available. These devices distribute quantum key within intercity distances, trough optical fiber links, but due to optical attenuation, they are limited in transmission distance. For long distances, moving terminals and satellite links are currently investigating. The study of satellite links is essential for the extension of quantum networks over a worldwide scale.

In view of these arguments, the aim of this thesis is to explore different degrees of freedom (DOF) of the photons in order to provide new tools or tests for quantum information protocols, useful for transmission and analysis of quantum states, or for testing a particular source of quantum states.

Let's now introduce a small resume of the contents presented in the chapters. In the first Chapter, we report a brief summary of the basic concepts of quantum information used trough this thesis. Chapter 2 introduces the experimental realization of an hyper-entangled photon source, with polarization and time-bin degrees of freedom. The aim of this source is to share an hyper-entangled state between two spatially separated users. Time-bin entanglement needs a time reference share between the two users to recover the state. We design the system in order to obtain a very precise time synchronization between the two parties. The solution adopted, allowed to share an hyper-entangled state with a 96% fidelity to the ideal state.

In chapter 3 we introduce a new method to recover a density matrix of a quantum state, based on compressive sensing. This method, when prior information are available, allows a faster recovery of the state than traditional methods.

In chapter 4 we report an experimental demonstration of the violation of chained Bell inequality for a time-bin entangled source. Time-bin source suffers from an intrinsic loophole due to postselection on the detected photon. To violate a Bell inequality additional assumptions are needed. One of these is the requirement of high visibility, in order to obtain a greater violation. With our setup we prove that is possible to achieve such high visibility, and we show that we are able to violate chained Bell inequality with 6, 8 and 10 terms.

In chapter 5 we report the principal result obtained in the experiment conducted at Matera Laser ranging observatory, where we prove for the first time that time-bin encoding of the photon is preserved along satellite-ground quantum channel. We have seen that interference at single photon level between two temporal modes was observed along a path that includes a rapidly moving retroreflector on a satellite and with a length up to 5000 km. This experiment also demonstrate that the relative motion of the satellite with respect to the ground induces a varying phase that modulates the interference pattern.

In chapter 6 we will introduce a new method that provide a bound for the conditional min-entropy of a random variable Z. The bound for the conditional min-entropy can be used to directly compute the conditional min-entropy of the random variable Z, by using the classical random variable X. This term represents the amount of true randomness that can be extracted from Z. We test this method with a polarization entangled photon source.

In the last chapter, finally, we summarize the main results of these works.

1

Quantum communications and Quantum protocols

Experimental implementations showed in this thesis, describe exchange of quantum information between users exploiting temporal degree of freedom (DOF) of photons only, or with polarization DOF. In this chapter, an introduction to quantum information science is provided, focusing on the mathematical tools useful to understand the work presented in the following chapters.

Quantum communications are a revolutionary extension of classical communications and first we will see the difference between them. Afterwards, we will focus on entanglement, a physical phenomenon which cannot be explained with classical physic. To show that, we will introduce Bell in-

equality and its experimental implementation. Finally, some interesting quantum protocol scheme, are presented.

1.1 Classical communication

The first scheme of classical communication was provide by Shannon and Waver in the 1949, and consists on a sender (Alice), composed by an information source and an encoder, a classical channel, where noise can be added, and finally a receiver (Bob), composed by a decoder and a destination. When Alice decides to send a message to Bob, she chooses a message which is encoded and sent through the classical channel. At this point, the message can be subject to external noise. Finally, the message is decoded and delivered to Bob. All the information exchanged, is carried by classical signals, such as electric pulses or radio waves. These signals can assume two distinct values to represent a bit, the basic unit of information used to represent logical levels "0" and "1".

1.2 Quantum bit

Quantum communications differ from classical communications by the use of quantum state to deliver information from a source to a destination. Qubit (short for quantum bit), the quantum counterpart of the bit, can be defined as a state of a two dimensional Hilbert space, with a orthogonal basis defined by states $\{|0\rangle, |1\rangle\}$. The ket symbol $|\cdot\rangle$ represents a column vector, and the bra $\langle\cdot|$ its conjugate transpose. The combination of the two, $\langle\cdot|\cdot\rangle$ represents the internal product.

A general state of a two dimensional quantum system, can be a simultaneous superposition of both:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α and β are complex amplitudes, such that $|\alpha^2| + |\beta^2| = 1$. The state $|\psi\rangle$ represents a qubit

and, different than bit, is a superposition of two different states.

When a measure is perform on $|\psi\rangle$, the state collapses in the state $|0\rangle$ or $|1\rangle$ with a probability equals to the square of the parameters, α^2 and β^2 respectively. This means that, when we perform a measurement on a quantum state, the result cannot be decided a priori. In experimental physics, states $|0\rangle$ and $|1\rangle$ correspond to spins of an electron, up $|\uparrow\rangle$ and down $|\downarrow\rangle$, or to polarization of a photon, horizontal $|H\rangle$ or vertical $|V\rangle$.

Projective measurements

Experimental apparatus, used to manipulate quantum system of particles, are designed to provide a measure of energy, polarization, position and other of those particles. All these measurable quantities represent a self-adjoint operator O, called observables. A quantum observable doesn't represent a classical property, which has a definite value as result. The outcome of a quantum observable can be one of all the possible values that the observed property can assume.

In general, an observable A is an hermitian operator, which spectral decomposition can be written as:

$$A = \sum_i a_i |a_i\rangle\langle a_i|$$

where the eigenvalues a_i are the possible results of measurements, and $|a_i\rangle$ are the respective eigenvectors.

A classical set of observables that forms a basis for the two dimensional Hilbert space, is the set of

Pauli observables.

$$I = \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_x = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.1}$$

$$\sigma_y = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.2}$$

With these matrices, the density matrix of a quantum state can be written as

$$\rho = \frac{1}{2} \sum_i S_i \sigma_i \tag{1.3}$$

where S_i are the result of the measurements $S_i = Tr\{\rho\sigma_i\}$.

Each Pauli matrix can be defined in function of projective measurements, and for polarization quantum state can be written as:

$$\sigma_0 = P_H + P_V \qquad \sigma_1 = P_+ + P_- \tag{1.4}$$

$$\sigma_2 = P_L - P_R \qquad \sigma_3 = P_H - P_V \tag{1.5}$$

where $P_a = |a\rangle\langle a|$ and

$$|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \tag{1.6}$$

$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) \qquad |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle). \tag{1.7}$$

In matrix form, $|H\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|V\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. When we perform a projective measurement P_a on a quantum state $|\psi\rangle$, it collapses onto the state $|a\rangle$ with probability $|\langle a|\psi\rangle|^2$. In the next chapters we

will see how take these measurements in practical experiments.

1.3 Entanglement

Let us now introduce a distinctive property of quantum mechanics, without a counterpart in classical world, the entanglement. Two or more quantum systems are entangled when they show correlation that can be explained only with quantum mechanics. When we have a quantum system of a pair of entangled particles, a measurement on one, instantaneously changes the state of the other, regardless the distance between them. From a mathematical point of view, quantum states are entangled if the state of the system cannot be expressed as a tensor product of the single states.

$$|\Phi\rangle \neq |\Phi_A\rangle \otimes |\Phi_B\rangle \tag{1.8}$$

The following state, instead,

$$|\Phi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right)$$

describes a pair of quantum systems A and B that are entangled. If the qubit in the system A is determined to $|0\rangle$ or $|1\rangle$, the qubit of system B assumes a definite value. Typical entangled states are the Bell states. These states form a basis for a two dimensional Hilbert space $H = H_A \otimes H_B$, and they are:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B\right) \tag{1.9}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B\right) \tag{1.10}$$

In practical experiment, we need some tools to quantifies the quality of the generated quantum state, and for that, we use three measurements: fidelity, purity and linear entropy. The fidelity[9] is the measurement of the distance between two quantum state ρ and σ. It is defined by

$$F(\rho,\sigma) = \left(\mathrm{Tr}\left[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right]\right)^2 \tag{1.11}$$

The range of the fidelity is $0 \leq F(\rho,\sigma) \leq 1$, and $F(\rho,\sigma) = 1$ if and only if $\rho = \sigma$.
If the two states are pure, $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$, then

$$F(\rho,\sigma) = |\langle\psi|\phi\rangle|^2 \tag{1.12}$$

Another useful measure, is the purity[10], that quantify how pure a quantum state is. The purity is defined as

$$P(\rho) = \mathrm{Tr}\left[\rho^2\right]. \tag{1.13}$$

If the state ρ is pure, $P(\rho) = 1$, while for a maximally mixed state is $P(\rho) = 1/d$, where d is the dimension of the state.

To measure the mixedness of a state, a measurement related to purity can be used. Linear entropy[11] is defined as

$$S_L(\rho) = \frac{d}{d-1}(1 - \mathrm{Tr}\left[\rho^2\right]) \tag{1.14}$$

where the normalization ensures that the linear entropy ranges is $0 \leq S_l(\rho) \leq 1$.

Source of entangled photons

Photons can be entangled in different DOFs, such as polarization, time and orbital angular momentum. In this thesis, we study two of these DOFs, polarization and time. One of the most popular source of

entangled photon is spontaneous parametric down conversion (SPDC). When a photon enters into SPDC crystal, with low probability, is splitted into a pair of photons correlated in polarization. The process is spontaneous, in the sense that there isn't any other photon that interacts in the process; is parametric, because the phase of the output fields depend on the phase of the input field and finally, the frequencies of the two generated photons are lower than the frequency of the pump[22]. Polarization entangled photons are generated by a superposition of two polarizations that can take each photon of the pair. Advantages of polarization encoding reside on the facts that polarization can be easily generated, manipulated and measured by simple, economic and stable optical devices.

Another way to generate entangled photons is by their temporal degree of freedom. We can generate temporal entangled photons in two way. The first, energy-time entangled photons source, was proposed by Franson in 1989[75], and is generated by a continous laser source with a coherence time equals to τ, that pumps a SPDC crystal. Each correlated photon from the SPDC crystal is sent to an unbalanced interferometer, where the difference of the two paths ΔT is imposed to be greater than the coherence time of the photons, but lesser than the coherence time of the pump laser. This means that the pair of photons are emitted at the same time and the uncertainty imposed by the pump makes undistinguishable the two paths of the interferometer that each photons can take. Time-bin describe a slightly different process. In this generation scheme, photons are emitted in a sequence of well defined pulses. In time-bin encoding the source is a pulsed laser, which has a very small coherence time τ. The condition used in energy-time, $\tau >> \Delta T$, cannot hold, and to resolve this problem the solution is to implement an unbalanced interferometer along the path of the pump laser. The path difference in this interferometer has to be equal to the path difference of the other two interferometers. In this way, the pump interferometer creates a superposition of two coherent state, and the uncertainty in time emmission is reestablished.

1.4 EPR paradox

The weird property that two entangled particles remain perfectly correlated over long distances, was investigated by Einsten, Podolsky and Rosen (EPR) in their famous paper[3]. Their interpretation affirmed that quantum mechanics contradicts three hypothesis:

Realism: "if without disturbing in any way a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity"

Locality: "the real factual situation of the system S_2 is independent on what is done on the system S_1, which is spatially separated from the former"

Completeness: "every element of the physical reality must have a counterpart in the physical theory"

and, as a consequence, they affirmed that quantum mechanics is not complete. In their paper, to demonstrate the above statements, they proposed an experiment called EPR paradox, that can be synthesized as follow. An EPR photon pair, namely a quantum entangled photon pair, are described by the state

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|H_A H_B\rangle + |V_A V_B\rangle). \tag{1.15}$$

When Alice measures the first particles, and she obtains $|H\rangle$ (or $|V\rangle$), the same result will be obtained, instantaneously and regardless the position, by Bob if he uses the same observable. But, if Bob measures the state with an incompatible observable, the result is undetermined. This means that the measure of Alice instantaneously modifies the Bob's state, and, as a consequence, we can say that two non commuting observables cannot have simultaneously realty. It seems that Alice sends to Bob information about the measure. But, the theory of relativity, developed by Einstein some years before, says that nothing, information included, can travel faster than the light. They called this effect "spooky

action at a distance", saying that, if relativity is maintained, the quantum description is not complete. To resolve this paradox, EPR proposed the presence of local hidden variable (LHV) that described the behavior of the two particles. The LHV theory, adds to quantum mechanics, the requirements to be consistent with local realism.

1.5 Bell inequality

About thirty years later EPR paper, John Bell demonstrated that LHV model was incorrect. His method consists in a inequality that takes into account expectation values from entangled state measurements. The prediction that can be obtained by a LHV theory differs from experimentally result performed with spin-1/2 particles. A few years later, Clauser, Horne, Shimony and Holt (CHSH) proposed a more accessible experimental implementation on entangled system.

Now we see a review on Bell's inequalities, from a mathematical point of view. To explain that, we can think about an experiment where Alice and Bob share a pair of entangled particles. Alice and Bob each have two devices that can perform independently and simultaneously, a measurement on their particle. Each measurement outcome can assume the value $+1$ or -1 (for Alice we have $A_{1,2} = \pm 1$, for Bob $B_{1,2} = \pm 1$). For a LHV theory, the Bell inequality can be written as:

$$S = E(A_1 B_1) + E(A_1 B_2) + E(A_2 B_1) - E(A_2 B_2) \leq 2 \tag{1.16}$$

where $E(A_j B_i)$ is the expectation value of when Alice measures A_j and Bob B_i. The LHV can be view as a parameter λ that influence the outcome of a measurement. We can rewrite

$$\begin{aligned} A_1 &= A_1(\lambda) \qquad B_1 = B_1(\lambda) \\ A_2 &= A_2(\lambda) \qquad B_2 = B_2(\lambda). \end{aligned} \tag{1.17}$$

We assume that $p(\lambda)$ represents the probability distribution of the hidden variable $\lambda \in \Lambda$, where Λ is the probability space

$$\int_\Lambda p(\lambda)\mathrm{d}\lambda = 1, \tag{1.18}$$

and $E(A_j(\lambda)B_i(\lambda))$

$$E(A_j(\lambda)B_i(\lambda)) = \int_\Lambda A_j(\lambda)B_i(\lambda)p(\lambda)\mathrm{d}\lambda. \tag{1.19}$$

meaning that the observed values of Alice and Bob, depend on the local chosen measurement and on the hidden variable λ. The Bell parameter (eq.1.16) now becomes

$$\begin{aligned}
S &= \int_\Lambda A_1(\lambda)B_1(\lambda)p(\lambda)\mathrm{d}\lambda + \int_\Lambda A_1(\lambda)B_2(\lambda)p(\lambda)\mathrm{d}\lambda \\
&+ \int_\Lambda A_2(\lambda)B_1(\lambda)p(\lambda)\mathrm{d}\lambda - \int_\Lambda A_2(\lambda)B_2(\lambda)p(\lambda)\mathrm{d}\lambda \\
&= \int_\Lambda (A_1(\lambda)B_1(\lambda) + A_1(\lambda)B_2(\lambda) + A_2(\lambda)B_1(\lambda) - A_2(\lambda)B_2(\lambda))p(\lambda)\mathrm{d}\lambda \\
&= \int_\Lambda (A_1(\lambda)(B_1(\lambda) + B_2(\lambda)) + A_2(\lambda)(B_1(\lambda) - B_2(\lambda))p(\lambda)\mathrm{d}\lambda
\end{aligned}$$

Each measurement can assume the value ± 1 and if we consider the terms $(B_1(\lambda) + B_2(\lambda))$ and $(B_1(\lambda) - B_2(\lambda))$, one of them is equal to zero. This means that we can bound the Bell parameter with

$$S = \int_\Lambda (A_1(\lambda)(B_1(\lambda) + B_2(\lambda)) + A_2(\lambda)(B_1(\lambda) - B_2(\lambda))p(\lambda)\mathrm{d}\lambda \leq 2. \tag{1.20}$$

Experimentally, the value $E(A_j(\lambda)B_i(\lambda))$ can be found as

$$E(A_jB_i) = \frac{N_{++} - N_{+-} - N_{-+} + N_{--}}{N_{++} + N_{+-} + N_{-+} + N_{--}} = P_{++} - P_{-+} - P_{+-} + P_{--} \tag{1.21}$$

where, for example, N_{++} is the number of particles that give $+1$ as outcome for Alice and Bob, and

P_{++} the relative probability. When Alice measures a photon with a polarizer of angle α we have

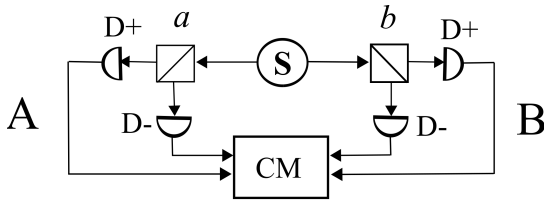


Figure 1.1: The source S produces pairs of photons, sent to A and B. The measurements a and b are chosen by the experimenter. $D+$ is the detector relative to a detection of $+1$, $D-$ is the detector relative to a detection of -1. Image from Wikipedia[1].

$$|+1_A\rangle = \cos(\alpha)|V\rangle - \sin(\alpha)|H\rangle \qquad |-1_A\rangle = \sin(\alpha)|V\rangle + \cos(\alpha)|H\rangle \tag{1.22}$$

while for Bob, when he measures a photon with angle β

$$|+1_B\rangle = \cos(\beta)|V\rangle - \sin(\beta)|H\rangle \qquad |-1_B\rangle = \sin(\beta)|V\rangle + \cos(\beta)|H\rangle. \tag{1.23}$$

The probabilities, in function of α and β can be evaluated as

$$P_{++}(\alpha,\beta) = |\langle +1_A|\langle +1_B|\Phi\rangle|^2 = \frac{1}{2}\cos^2(\alpha-\beta) \tag{1.24}$$

$$P_{--}(\alpha,\beta) = |\langle -1_A|\langle -1_B|\Phi\rangle|^2 = \frac{1}{2}\cos^2(\alpha-\beta) \tag{1.25}$$

$$P_{-+}(\alpha,\beta) = |\langle -1_A|\langle +1_B|\Phi\rangle|^2 = \frac{1}{2}\sin^2(\alpha-\beta) \tag{1.26}$$

$$P_{+-}(\alpha,\beta) = |\langle +1_A|\langle -1_B|\Phi\rangle|^2 = \frac{1}{2}\sin^2(\alpha-\beta) \tag{1.27}$$

The expected value $E(A_j(\lambda)B_i(\lambda))$ of eq.1.21 becomes

$$\begin{aligned} E(A_\alpha B_\beta) &= P_{++}(\alpha,\beta) - P_{-+}(\alpha,\beta) - P_{+-}(\alpha,\beta) + P_{--}(\alpha,\beta) \\ &= \cos^2(\alpha-\beta) - \sin^2(\alpha-\beta) = \cos(2(\alpha-\beta)) \end{aligned}$$

Consider now the state 1.15. Alice chooses for A_1 to measure the angle $\alpha_1 = 0$ and for A_2 the angle $\alpha_2 = \pi/4$. Bob chooses for B_1 to measure the angle $\beta_1 = \pi/8$ and for B_2 the angle $\beta_2 = -\pi/8$. The Bell parameter is

$$\begin{aligned} S &= E(A_{\alpha_1}B_{\beta_1}) + E(A_{\alpha_1}B_{\beta_2}) + E(A_{\alpha_2}B_{\beta_1}) - E(A_{\alpha_2}B_{\beta_2}) \\ &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} - (-\frac{\sqrt{2}}{2})) = 2\sqrt{2} \end{aligned}$$

a result that is outside the bounds placed by eq.1.16 for LHV theory. This violation means that quantum mechanics cannot be considered a LHV theory.

The first experiment on Bell inequality was carried out by Stuart Freedman and John Clauser in 1972[6], showing a violation of Bell inequality. Then, in 1982 Alain Aspect[7] performs the first experiment by closing a locality loophole. In quantum science, a loophole refers to leak in experimental design that can invalidate an experimental result, as a violation of Bell inequality. For example, in optical experiments, the most common loophole is the detection loophole, due to the fact that the efficiency of detectors are less than 100%. The undetected photons, can invalidate the result of a Bell test, that can be considered valid if the efficiency is greater than 83%. Generally, optical experiments have an efficiency less than 30%. With such performances, in order to violate Bell inequality, it is necessary to assume that the undetected photons have the same statistic of the detected ones. There are other loopholes to treat when a quantum experiment is developing. In particular, Franson experiment suffers from a loophole due to postselection on the photons coincidence. This loophole is analyzed in chapter 4. In 2015 three different experimental groups[8,4,5], performed independently a free-loophole Bell test, showing in a definitive way the incorrectness of LHV model.

1.6 Quantum communication protocols

In this section we will review some protocols that are based on quantum entanglement, and, for this reason, they they do not have a classical counterpart.

Dense coding

For example, Alice can use an entangled state to send Bob two classical bits of information by sending a single qubit of the entangled state. This protocol is called dense coding[33,34,35], and works as follows. Alice and Bob share the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \tag{1.28}$$

and suppose that Alice has two classical bits, x and y, to send to Bob. Initially, Alice and Bob have agreed some operations that Alice will perform depending on the values of x and y. These operations modified only the Alice's qubit, corresponding to a final shared state described in tab.1.1.

Bits	State	Operation	Final state
$x = 0\ y = 0$	$\|\Phi^+\rangle$	$(\sigma_0 \otimes \sigma_0)\|\Phi^+\rangle$	$\|\Phi^+\rangle$
$x = 0\ y = 1$	$\|\Phi^+\rangle$	$(\sigma_3 \otimes \sigma_0)\|\Phi^+\rangle$	$\|\Phi^-\rangle$
$x = 1\ y = 0$	$\|\Phi^+\rangle$	$(\sigma_1 \otimes \sigma_0)\|\Phi^+\rangle$	$\|\Psi^+\rangle$
$x = 1\ y = 1$	$\|\Phi^+\rangle$	$(i\sigma_2 \otimes \sigma_0)\|\Phi^+\rangle$	$\|\Psi^-\rangle$

Table 1.1: Depending on the values of the two bits x and y, Alice applies a transformation to the state $|\Phi^+\rangle$. At the end Alice and Bob share one of the four Bell states.

Then, Alice sends to Bob her qubit, and, at this point, Bob can perform a Bell state measurement. With this measurement, Bob can measure which Bell state he has, deducing the value of the two qubits transmitted by Alice.

Quantum Teleportation

Another application of entangled state is the quantum teleportation [36,37,38,39,40]. This protocol refers to the possibility to send a quantum bit by sending only two classical bits. This is useful when Alice wants to transmit an unknown qubit to Bob, but there isn't any quantum channel where transmit it. As for dense coding, Alice and Bob need a shared Bell entangled state

$$|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \tag{1.29}$$

that is provided by a third part, Charlie. The unknown state that Alice wants to teleport to Bob is $|\psi\rangle = \alpha|0_A\rangle + \beta 1_A$, and the total system can be written as

$$|\psi\rangle|\Phi^+_{AB}\rangle = (\alpha|0_A\rangle + \beta 1_A)\frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle). \tag{1.30}$$

If we expand we obtain

$$\begin{aligned}|\psi\rangle|\Phi^+_{AB}\rangle &= \frac{1}{\sqrt{2}}(\alpha|0_A 0_A 0_B\rangle + \alpha|0_A 1_A 1_B\rangle + \beta|1_A 0_A 0_B\rangle + \beta|1_A 1_A 1_B\rangle)\\ &= \frac{1}{2}\left[|\Phi^+_{AA}\rangle(\alpha|0_B\rangle + \beta|1_B\rangle) + |\Phi^-_{AA}\rangle(\alpha|0_B\rangle + \beta|1_B\rangle)\right.\\ &\left.-|\Psi^+_{AA}\rangle(\alpha|1_B\rangle + \beta|0_B\rangle) + |\Psi^-_{AA}\rangle(\alpha|1_B\rangle - \beta|0_B\rangle)\right].\end{aligned}$$

The unknown state $|\psi\rangle$ and the qubit of the entangled state $|\Phi^+_{AB}\rangle$ of Alice, can be written in function of the four Bell states, while for Bob, his qubit of the entangled state $|\Phi^+_{AB}\rangle$ can be written in a similar way to the original qubit holds by Alice.

Alice performs a Bell measurement on her part of the system, and communicate to Bob the result of the measurement with two classical bit. As a consequence, Bob can now discriminate between the four states $\alpha|0_B\rangle \pm \beta|1_B\rangle$ and $\alpha|1_B\rangle \pm \beta|0_B\rangle$, by applying a unitary transformation to his qubit,

in order to obtain the state

$$|\psi_B\rangle = \alpha|0_B\rangle + \beta|1_B\rangle. \tag{1.31}$$

The unitary transformations are

$$\begin{aligned}
|\Phi^+_{AA}\rangle &\Rightarrow \sigma_0(\alpha|0_B\rangle + \beta|1_B\rangle) \Rightarrow |\psi_B\rangle \\
|\Phi^-_{AA}\rangle &\Rightarrow \sigma_3(\alpha|0_B\rangle - \beta|1_B\rangle) \Rightarrow |\psi_B\rangle \\
|\Psi^+_{AA}\rangle &\Rightarrow \sigma_1(\alpha|1_B\rangle + \beta|0_B\rangle) \Rightarrow |\psi_B\rangle \\
|\Psi^-_{AA}\rangle &\Rightarrow i\sigma_2(\alpha|1_B\rangle - -\beta|0_B\rangle) \Rightarrow |\psi_B\rangle
\end{aligned}$$

Entanglement swapping

Another process, called entanglement swapping, allows to entangle particles that have no common past. For example, if the particles A and B hold by Alice and Bob have never interacted, A and B can become entangled if A is entangled with a third system hold by Charlie, and also B is entangled by Charlie. Suppose that the entangled state between Alice and Charlie is described by the state $|\Psi^-\rangle_{AC1}$ and that Charlie and Bob share the state $|\Psi^-\rangle_{C2B}$. With $C1$ and $C2$ are indicated the two particles hold by Charlie. The state that describes the entire system is

$$|\Psi\rangle_{AC1C2B} = |\Psi^-\rangle_{AC1} \otimes |\Psi^-\rangle_{C2B}. \tag{1.32}$$

This state can be expanded[13] as

$$\begin{aligned}
|\Psi\rangle_{AC1C2B} = \frac{1}{2}\big[&|\Psi^+\rangle_{AB} \otimes |\Psi^+\rangle_{C1C2} - |\Psi^-\rangle_{AB} \otimes |\Psi^-\rangle_{C1C2} \\
&-|\Phi^+\rangle_{AB} \otimes |\Phi^+\rangle_{C1C2} + |\Phi^-\rangle_{AB} \otimes |\Phi^-\rangle_{C1C2}\big].
\end{aligned}$$

Charlie can perform a Bell state measurement on his two qubits, and in this way, $C1$ and $C2$ become entangled. For example, suppose that Charlie performs a Bell measurement that gives the state $|\Phi^+\rangle_{C1C2}$ as result.
As a consequence, the resulting state between Alice and Bob is then proportional to

$$(\mathbb{1}_{AB} \otimes |\Phi^+\rangle_{C1C2}\langle\Phi^+|_{C1C2})|\Psi\rangle_{AC1C2B} \propto |\Phi^+\rangle_{AB} \otimes |\Phi^+\rangle_{C1C2}.$$

The above equation means that Alice and Bob share an entangled state. Finally, Charlie tells Bob to apply one of the four Pauli matrices in order to transform the shared state between Alice and Bob in a well defined Bell state. At the end of the process, the entangle between Charlie and Bob is destroyed. This protocol is at the heart of quantum repeater[14], a fundamental device to propagate a quantum entangled state over long distances.

Such applications require true random number generators. Quantum physics can be exploited to provide a trusted randomness source. Indeed, the measurements of a quantum system are used as source of bits.

Quantum Key Distribution - QKD

Quantum key distribution is a protocol that shares a random secret key over a public channel, which can be used to encrypt and decrypt messages shared between two users, Alice and Bob. The security of the process is guaranteed by the properties of quantum meachanics. An eavesdropper cannot recover any information from the key share between the parties without perturbing their state. In this way the parties detect the intrusion and abort the communication.

The first QKD protocol was proposed in 1984 by Bennett and Brassard. In this protocol the bits of the key are encoded into two pairs of orthogonal states (qubits) chosen between two bases, X and Z. Alice chooses two strings of random classical bits, $a = a_1, .., a_n$ and $b = b_1, ..b_n$. The first, a, is

used to choose which bit of the two basis send to Bob, and the second, b, indicate the base. A typical set of qubits is:

$$|\Phi_{00}\rangle = |0\rangle$$

$$|\Phi_{10}\rangle = |1\rangle$$

$$|\Phi_{01}\rangle = |+\rangle$$

$$|\Phi_{11}\rangle = |-\rangle$$

where $|\Phi_{xy}\rangle$ indicates that Alice send the bit x encoded in the base y. The qubits are not mutually orthogonal, in this way, the state cannot be determine uniquely with a single measurement.

Then, Alice sends the sequence of qubits $|\Phi_{ab}\rangle$ to Bob. At this point, Bob chooses randomly a sequence b', that corresponds to the basis in which measure the qubits. At the end Bob get the sequence of bit a'. The sequences a and a' are now differents, meaning that Alice and Bob hold different keys, the raw keys. Using a classical channel Alice and Bob compare the basis used in the transmission and detection. They discard the bits obtained with different basis, while the bits obtained with same basis are the shared sifted key. When the two basis, in transmission and detection, are identical the correlation between the sent and received qubits is very strong. If the two qubits are different, it means that an eavesdropper gain some information about the state or that the channel is noisy. To estimate the presence of an eavesdropper, Bob publicly announces to Alice a random subset of bits of the sifted key. Then, if there are more than d different bits, they discard the key and restart the protocol. The parameter d is chosen to apply information reconciliation and privacy amplification algorithms in order to obtain n' shared secret bits from the original n. This protocol is called BB84.

Starting from BB84 and using different states and bases it is possible to derive other QKD protocols, like the simple B92, which uses only two states, or the EPR protocol, where Alice and Bob share a set of entangled states[24].

Secure data transmission plays a foundamental role in everyday life, from bank account security to online payment or medical analysis. In a future scenario QKD could be the solution to prevent attack from an eavesdropper with an extraordinary power computation (e.g. with a quantum computer) that can be used to broke classical cryptographic systems. In this prospective, chapter 5 present a study of the satellite-ground channel for temporal encoding for a future use in satellite QKD.

2

Hyper-Entanglement

In quantum mechanics, entanglement plays an important role in implementations or experimental tests of quantum information theory. Algorithms and fundamental tests of quantum mechanics are increasingly requiring large number of qubits. Hence, it is necessary to add more qubits to quantum states in order to take full advantages of quantum mechanics. For instance, increasing the number of qubits, allows a strong violation of Bell's inequality[16]. The number of qubits increases with enhance the number of entangled particles[12], but the complexity of experiments greatly increase. An efficient way to achieve that consists on encode more than one qubit in each particle, exploiting different degrees of freedom (DOFs) of particles[17,18,19]. Particles encoded in this way are called hyperentangled. Hyperentanglement offers practical advantages, as low threshold detection efficiency[15]. This lower

bounds, as shown by Massar[20], decrease exponentially with the dimension of Hilbert space. In addition, with only two particles, hyperentanglement allows to generalize Greenberger - Horne - Zeilinger (GHZ) theorem[21].

As we saw in chapter 1, some quantum information protocols, such as teleportation[36,37,38,39,40], dense coding[33,34,35], entanglement swapping[38,41,42,43], cryptography[44], need the discrimination between the four orthogonal Bell states. However, with linear optics, a complete deterministic discrimination between the four Bell states is not possible. A way to achieve a complete Bell state analysis is enlarging the size of the Hilbert space and using hyperentangled states[45,46,47,48].

In this chapter we study in a deep way, how generate entangled in polarization and time-bin temporal DOFs, and how to combine these two DOFs to generate an hyper-entangled state. Some of the results presented in this chapter are published in the master thesis of Raffaelli[124].

2.1 Polarization Entanglement

A classical method used to generate entangled photon in polarization, is by spontaneous parametric down conversion (SPDC)[23]. This is a nonlinear optical process where an higher energy photon, called pump photon, is down-converter in two lower energy photons, called signal and idler photons. When an electric field interacts in a dielectric medium, leads a polarization of the dielectric. Photons inside dielectric medium can decay into a photon pair if some conditions are met. The first condition is that, due to the nonlinear nature of the SPDC process, this appears only in medium where the second-order contribution is greater than zero. In our experiment we use a Beta-barium borate (BBO) crystal which is a negative uniaxial crystal, and exhibits higher transparency and nonlinearities. The total energy of the generated photons, has to be equal to the energy of the pump photon, then

$$\omega_P = \omega_s + \omega_i. \tag{2.1}$$

In addition, the signal and idler photons, have to satisfy a condition on the phases. The sum of their wave vectors must be equal to the pump wave vector,

$$\vec{k}_P = \vec{k}_s + \vec{k}_i. \tag{2.2}$$

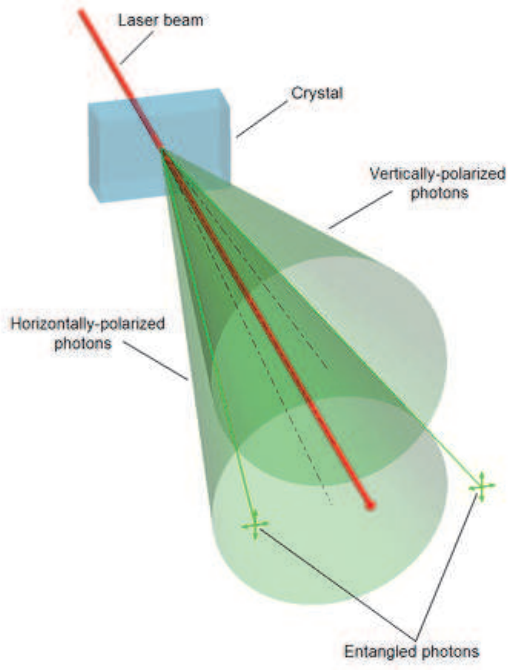


Figure 2.1: Polarization entangled photon generated by a type II SPDC crystal

This is called phase matching condition, and in BBO crystal, when pump photon has extraordinary polarization, idler and signal can have the same ordinary polarization (Type I) or they are orthogonal polarized, one ordinarily, and the other extraordinarily (Type II). A more detailed description, from a quantum mechanical point of view can be found here[32]. When these conditions are met, idler and signal photons are strongly correlated in energy and polarization DOFs. The emission directions of down-converter photons are distributed along cones, and wave vectors of a pair of photons are sym-

metrical emitted with respect to pump wave vector. In this experiment, photon pairs need to be distinguished by polarization, therefore we try to reach a complete indistinguishability in other DOFs. Single mode fibers are used as spatial filter for the modes, and bandpass filter for wavelength filtering. By tilting the angle of the BBO crystal, it is possible to change the angle between the two emission cones, in order to create intersection between them. The configuration when the cones touch each other in two points is called non collinear, and it is the configuration chosen for our experiment. In the intersection points, it is not possible to infer the polarization of the photons. In this points, the state of the photons is in a superposition of two orthogonal polarizations. If we consider a Type II crystal, the state of the photons pair is a generalized Bell state:

$$|\Psi'\rangle = \frac{1}{2}\left(|H_A V_B\rangle + e^{i\phi}|V_A H_B\rangle\right) \tag{2.3}$$

where the phase ϕ can be set up experimentally by tilting the crystal. In the experiment the phase is set to $\phi = \pi$ obtaining the state

$$|\Psi\rangle = \frac{1}{2}\left(|H_A V_B\rangle - |V_A H_B\rangle\right). \tag{2.4}$$

Polarization measurement

Photon measurement is carry out by a transformation of the photons with linear optics[25]. When dealing with polarization states, transformation of qubits can be done with birefringent crystals. Wave retarders are the most important, in particular half and quarter wave plates are used to easily manipulate linear and circular polarizations. These wave retarders introduce a phase shift of π, for half wave plate, or $\pi/2$, for quarter wave plate, between ordinary and extraordinary components of electric field. In function of their fast axes angles, half and quarter wave plates rotate photons polarization, between linear and circular one.

Another important component is the polarizing beamsplitter (PBS), which is a beamsplitter where the horizontal polarization is transmitted and the vertical one is reflected (o vice versa).

To project the photons onto the desired state, we use a quarter wave plate, an half wave plate and a polarizing beamsplitter, placed in front of each other. An easy way to show polarization measuring, is by using the Jones calculus. The basic idea is that half and quarter wave plates, can be described by $2x2$ matrices[26]

$$W_h(\theta) = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ -\sin(2\theta) & -\cos(2\theta) \end{pmatrix}, \tag{2.5}$$

$$W_q(\phi) = \frac{1}{\sqrt{2}} \begin{pmatrix} i - \cos(2\phi) & \sin(2\phi) \\ \sin(2\phi) & i + \cos(2\phi) \end{pmatrix} \tag{2.6}$$

where θ and ϕ are the angles of optical axes for half (h), and quarter (q) wave plate. The matrix of a PBS can be expressed by projection operators:

$$P_H = |H\rangle\langle H| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad P_V = |V\rangle\langle V| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \tag{2.7}$$

where P_H is the projection with respect to transmitted photons, and P_V to reflected photons. In our case the PBS projects onto $|H\rangle$ state. Now, the projection state for a single photon is

$$\begin{aligned} |\Psi'_{\theta,\phi}\rangle &= W_q(\phi) \cdot W_h(\theta) \cdot |H\rangle \\ &= h(\theta,\phi)|H\rangle + v(\theta,\phi)|V\rangle, \end{aligned} \tag{2.8}$$

where

$$h_{\theta,\phi} = \frac{1}{\sqrt{2}}\left(i\ \cos(2\theta) - \cos(2\phi - 2\theta)\right) \tag{2.9}$$

$$v_{\theta,\phi} = \frac{1}{\sqrt{2}}\left(-i\ \sin(2\theta) + \sin(2\phi - 2\theta)\right) \tag{2.10}$$

For two photons, the projection state becomes

$$\begin{aligned} |\Psi''_p\rangle &= |\Psi'_{\theta_1,\phi_1}\rangle \otimes |\Psi'_{\theta_2,\phi_2}\rangle \\ &= h_{\theta_1,\phi_1} h_{\theta_2,\phi_2} |HH\rangle + h_{\theta_1,\phi_1} v_{\theta_1,\phi_1} |HV\rangle \\ &+ v_{\theta_1,\phi_1} h_{\theta_2,\phi_2} |VH\rangle + v_{\theta_1,\phi_1} v_{\theta_2,\phi_2} |VV\rangle. \end{aligned} \tag{2.11}$$

The probability of obtain the state $|\Psi''_p\rangle$ from $|\Phi\rangle$, is

$$p = |\langle \Psi''_p | \Phi \rangle|^2. \tag{2.12}$$

As a consequence, the average number of coincidences counts, observed when the wave plates are set with angles $(\theta_1, \phi_1, \theta_2, \phi_2)$, is

$$\mathcal{C}_p = \mathcal{N} |\langle \Psi''_p | \Phi \rangle|^2, \tag{2.13}$$

where n is the total count rate. For example if we consider the probability to obtain the state $|HH\rangle$ from the state 2.4, we set the angle of the wave-plate as $(\theta_1, \phi_1, \theta_2, \phi_2) = (0, 0, 0, 0)$, and we obtain

$$p = |\langle \Psi''_{(0,0,0,0)} | \Psi \rangle|^2 = \left| \frac{1}{\sqrt{2}}(i-1)\frac{1}{\sqrt{2}} \langle HH | HH \rangle \right|^2 = \frac{1}{2}. \tag{2.14}$$

The state $|H\rangle$ is obtained with $(\theta, \phi) = (0, 0)$, $|V\rangle$ is obtained with $(\theta, \phi) = (45, 0)$, $|+\rangle$ is obtained with $(\theta, \phi) = (22.5, 45)$, $|-\rangle$ is obtained with $(\theta, \phi) = (-22.5, 45)$, $|R\rangle$ is obtained with $(\theta, \phi) =$

$(22.5, 0)$, and $|L\rangle$ is obtained with $(\theta, \phi) = (22.5, 90)$.

Walk-off compensation

When a photon pair is generated inside a SPDC crystal, idler and signal photons are subjected to transverse and longitudinal walk-off due to crystal birefringent and to orthogonal polarization between them. This effect increases the distinguishability between the generated photons, decreasing their entanglement.

Transverse walk-off refers to tranversal shift applied to photons with extraordinary polarization. In a birefringent crystal, Pointing vector of extraordinary wave makes an angle greater than zero with the wave vector, but, for ordinary wave, Pointing vector has the same direction of wave vector.

Longitudinal walk-off is always due to birefringency of crystal, but in this case ordinary and extraordinary wave are delayed in time, one relative to each other. This effect is due to the different refractive index between extraordinary and ordinary waves.

The common solution for these problems, is to use a $\lambda/2$ waveplate to rotate the polarization of the photons by 90° and a second BBO crystal with half thickness[*] of the SPDC crystal to introduce the same effects on the ex-ordinary (now extraordinary due to rotation) wave.

2.2 Time bin entanglement

Time bin entangled indicates photon pairs entangled in temporal degree of freedom where their time of emission is well defined[28]. Time-bin entanglement is more robust for long distance transmission than polarization entanglement, which suffer from depolarization due to birefringence in optical fiber[27]. Here we will describe how to share a time-bin entangled state between two spatially separated users, Alice and Bob.

[*]The down-conversion process can appear all along the crystal, and in mean, the photon pair cross half of its thickness.

To generate a photon pair encoded in time-bin, we need to pump a SPDC crystal with a pulsed laser. Due to the low coherence time τ of the pump, an unbalanced interferometer, with a paths difference equals to ΔL, is inserted along its path, before the crystal. The output state of the interferometer is a superposition of two temporal modes, delayed by $\Delta T = \Delta L/c$ respect to each other. The state of the photon that impinges on the crystal is:

$$|\Phi_p\rangle = \frac{1}{\sqrt{2}}\left(|S_p\rangle + e^{i\theta_e}|L_p\rangle\right) \tag{2.15}$$

where the phase θ_e has to be consider when we will introduce the stabilization of the measurement interferometers. The state $|S\rangle$ indicates the short path, and $|L\rangle$ the long path of interferometer. When this photon passes through the crystal, and generates a down-converter photon pair, the state of the pair is a Bell state:

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}\left(|S_A S_B\rangle + e^{i\theta_p}|L_A L_B\rangle\right) \tag{2.16}$$

where A and B indicates the two photons, and θ_p the phase of the SPDC photons introduced by the pump interferometer.

Time-bin measurement

As we will see here and in the next sections, we've used three interferometers to generate and manipulate time-bin states. The first interferometer is used as pump, and at the receiver stations, Alice and Bob use two interferometers with the same path difference ΔL of the pump one. The output of these two measurement interferometers are

$$|t_A\rangle = \frac{1}{\sqrt{2}}\left(|S_A\rangle + e^{i\theta_A}|L_A\rangle\right) \tag{2.17}$$

$$|t_B\rangle = \frac{1}{\sqrt{2}}\left(|S_B\rangle + e^{i\theta_B}|L_B\rangle\right). \tag{2.18}$$

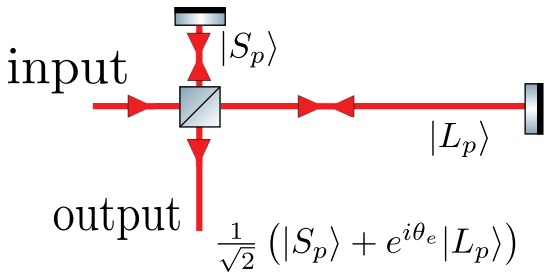


Figure 2.2: Encoding in the temporal DOF. The apparatus consists of an unbalanced Michelson interferometer with a short and a long arm. After the interferometer, the photon is in a coherent superposition of the two possible events $|S_p\rangle$ and $|L_p\rangle$. The relative phase θ_e depends on unbalancement between the two arms. Realized with ComponentLibrary[2].

The phases θ_A and θ_B are set by a nanometric positioner by varying the position of the mirror on the long arm of the interferometers. The state of the photon pair after these interferometers is:

$$\begin{aligned}|\Phi_e\rangle = &|S_pS_A, S_pS_B\rangle + e^{i\theta_A}|S_pL_A, S_pS_B\rangle + e^{i(\theta_A+\theta_B)}|S_pL_A, S_pL_B\rangle + e^{i\theta_B}|S_pS_A, S_pL_B\rangle \\ &+ e^{i\theta_p}|L_pS_A, L_pS_B\rangle + e^{i(\theta_p+\theta_A)}|L_pL_A, L_pS_B\rangle \\ &+ e^{i(\theta_p+\theta_A+\theta_B)}|L_pL_A, L_pL_B\rangle + e^{i(\theta_p+\theta_B)}|L_pS_A, L_pL_B\rangle\end{aligned}$$

where θ_A and θ_B are the phases of Alice and Bob interferometers. Two photons interference arises when the delay acquired by the photons inside the interferometers cannot be used to reconstruct the path take by the photon. For example, consider the photons state $|S_pL_A, S_pS_B\rangle$. This means that the pump photon is emitted at time t_p, Alice's photon is detected at time t_A, Bob's photon at time t_B. The difference $t_A - t_p$ means that the Alice's photon takes a short path and a long one (for the moment we doesn't know the order), but the difference $t_B - t_p$ tells us that the Bob's photon takes short paths in both interferometers. The pump photon is the same for Alice and Bob, and this means that Alice's photon takes the long path on the second interferometer. In this way, we are able to reconstruct the paths of the two photons, that is short for pump, long for Alice and short for Bob, because they are the only paths that can determined these arrival time. When one can distinguish the path takes

by the photons, no interference occurs. Interference occurs when the arrival times are postselected, taking only the events for which the delays acquired through interferometers are indistinguishable. A first selection can be done by removing those events that take different paths in the measurement interferometers. This state is

$$\begin{aligned}|\Phi^{ps}\rangle =&|S_pS_A, S_pS_B\rangle + e^{i(\theta_A+\theta_B)}|S_pL_A, S_pL_B\rangle \\ &+e^{i\theta_p}|L_pS_A, L_pS_B\rangle + e^{i(\theta_p+\theta_A+\theta_B)}|L_pL_A, L_pL_B\rangle\end{aligned}$$

and correspond to events that are in coincidence. In fig.2.4 it is possible to see how these temporal states are distributed. This distribution shows times difference between Alice and Bob detection times, with respect to the time of emission of the pump photon. Events in central peak are the sum of the states $|S_pL_A, S_pL_B\rangle$ and $|L_pS_A, L_pS_B\rangle$, and are the only events for which we cannot reconstruct the path taken by the photons. Interference now occurs at this point, as a result of a superposition of indistinguishable events. The state of the selected photons in the central peak is:

$$|\Phi_{tb}\rangle = |S_AS_B\rangle + e^{i\theta}|L_AL_B\rangle$$

which corresponds to a Bell state. The phase $\theta = \theta_A + \theta_B - \theta_p$ depends on the value assumed by the phases of the three interferometers.

As a consequence, when the phase θ_p is corrected by the stabilization of the interferometers (see subsection 2.4.1), the coincidence rate depends on the value of θ_A and θ_B (see Fig. 2.3):

$$\mathcal{C} \propto \cos^2 \frac{(\theta_A + \theta_B)}{2} \tag{2.19}$$

To set the phases of Alice and Bob, the positioner are moved to the desired position by this relation:

$$\theta_{A/B} = \frac{2\pi 2\Delta L}{\lambda_r} \tag{2.20}$$

where ΔL is the shift of the slider, and $\lambda_r = 808\ nm$ the wavelength of the down-converted photons.

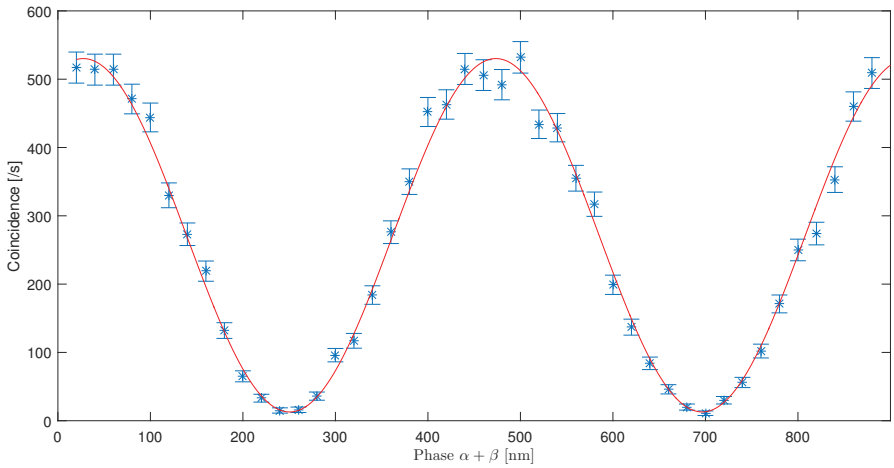


Figure 2.3: Time-bin coincidence in function of the phases θ_A and θ_B. The phase is expressed in relation to the shift of the positioner, $\phi = 2\pi \cdot 2\Delta L/\lambda$, where ΔL is the shift and λ is the wavelength of the photons. Only the Alice's phase is changed by moving the positioner by a 20 nm steps, over a 900 nm range.

2.3 Generation of Hyper-Entanglement in two degrees of freedom

Hyperentangled state can be generate by entangling two photons in different degrees of freedom. A formal definition of hyperentangled state can be found here[31]. Consider two photons, and n independent DOFs, $\{a_j\}$ for A and $\{b_j\}$ for B with $j = 1, .., n$, each of which spans a two-dimensional Hilbert space for photons A and B. This means that each photon can encode n qubits. A state $|\phi\rangle$ is

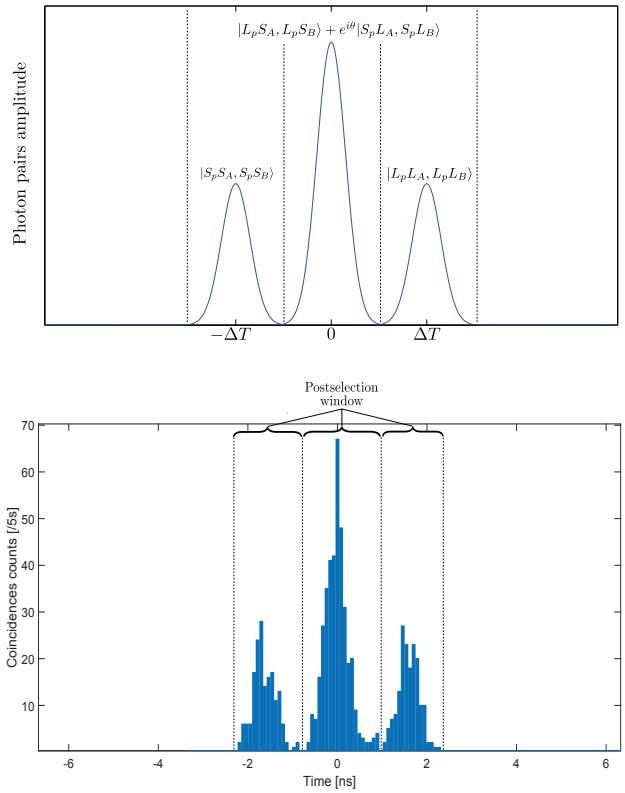


Figure 2.4: Time-bin coincidence distribution with respect to the laser pulses. (Top ideal case, bottom experimental acquisition)

separable in the hyperentangled sense if

$$\exists\, j \quad \text{such that} \quad |\phi\rangle = |\phi_1\rangle_{a_j I}|\phi_2\rangle_{b_j J} \tag{2.21}$$

where $\{I, J\}$ represents a generic bi-partition of the set $T_i = \{a_1, b_1, ..., a_n, b_{,n}\} \setminus \{a_j, b_j\}$, so that $I \cup J = T$ and $I \cap J = \emptyset$. A 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 eq. 2.21

With our experiment, we generate an hyperentangled state in two degrees of freedoms, polarization

and time-bin, encoding four qubits into two photons. The ideal state can be written as:

$$|\Psi_{HE}\rangle = \frac{1}{2}\left(|H_A V_B\rangle + e^{i\theta_p}|V_A H_B\rangle\right) \otimes \left(|S_A S_B\rangle + e^{i\theta_t}|L_A L_B\rangle\right) \tag{2.22}$$

To obtain such state we combine the generation of polarization entangled photon pair, with the generation of time-bin entangled photon pair.

2.4 Experimental setup

The laser source used in our experiment is a pulsed laser at 808nm, 76MHz repetition rate and $\sim 150 fs$ pulse width coming from a Ti:Sa mode-locked oscillator, with an average power of 2W. The Ti:Sa oscillator beam is used to pump a SHG crystal (with a thickness of 2 mm), which generates pulses at 404nm. The light at 404nm passes through a free-space unbalanced Michelson interferometer (see Fig. 2.2), called pump interferometer, where the output state is describe in eq. 2.15 and finally pumps a SPDC crystal (with a thickness of 2 mm). The photons produced at 808 nm are sent through a walk-off compensation crystal and then through a polarimeter, composed by a quarter wave plate, an half wave plate and a polarizing beamsplitter (PBS). Then, the photons are injected in two free-space unbalanced Michelson interferometers, the Alice and Bob's measurement interferometers, whose unbalancement is identical to the pump interferometer. The mirrors on the long paths of these two interferometers, unlike the pump interferometer, are mounted on piezoelectric translators, that are used to stabilize and change the phase of the interferometers. Finally, the photons are coupled into single mode fibers and directed toward two single photon avalanche photodiodes (SPADs). We used the Excelitas Single Photon Counting Modules, with 40% of photon detection efficiency at $808\ nm$, a dark counts of about 100 photons per second and about $40\ ns$ of dead time. To tag each detection event, we used the quTools time-to-digital converter, quTAG, with $81\ ps$ resolution.

Initial photon pairs generation of this source was about 12000 pair/s for a pump power of about

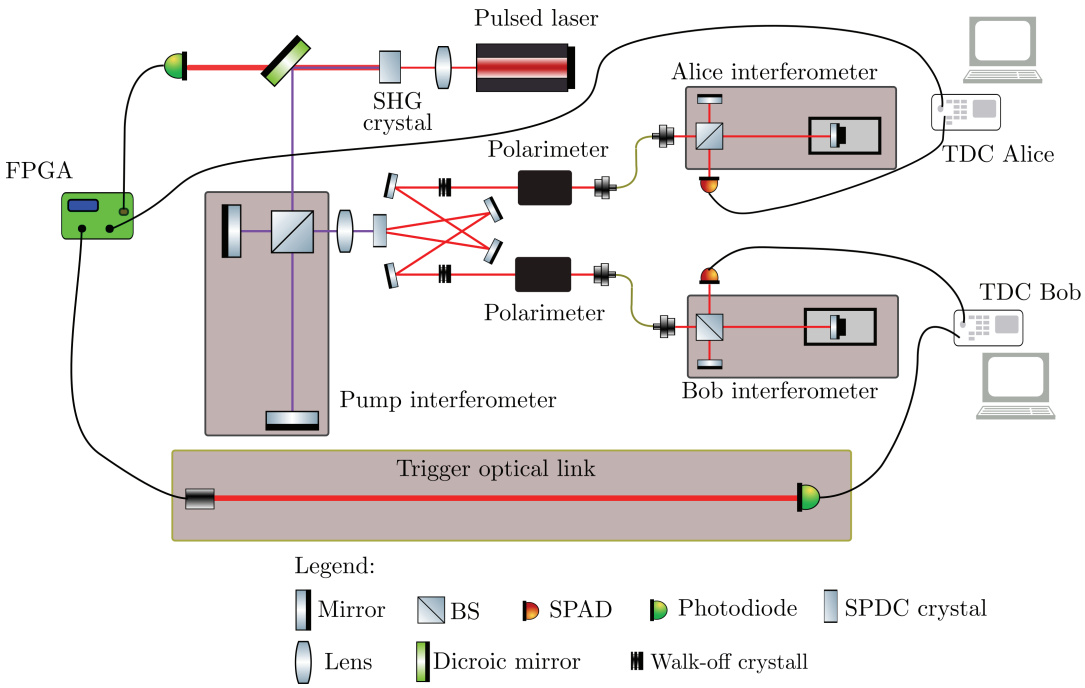


Figure 2.5: Setup of the hyperentanglement source. A detailed version of the SPDC source can be found in fig.2.6. Realized with ComponentLibrary[2].

$300mW$ (this rate is calculated at the output of the SPDC crystal). If we consider the further losses introduced by Michelson interferometers, the rate is low and to increase it, we perform an improvement, by optimizing the waist diameter of the pump and idler/signal photon beam. As described by Ling[72], the emission pair rate $\widetilde{R}_T$ can be written as

$$\widetilde{R}_T \propto \frac{1}{w^2(1/r + 2r)^2} \tag{2.23}$$

where w is the waist of collected idler/signal photon beams, and $r = w_p/w$ is the ratio between the pump and the idler/signal beams. The maximum emission rate is achieved when $r = 1/\sqrt{2}$. In fig. 2.7 it is possible to see the x-y waist of the pump, focused on the SPDC crystal with a $L_3 = 500mm$ lens focal (see the detail on SPDC generation on fig. 2.6). The pump beam is elliptical, and this prob-

lem comes from the generation of the SHG beam by the BiBO crystal, as described by Smith[73]. In fig. 2.7 we can see the beam waist of the idler/signal beam. To obtain this graphs, we measure the beam waist of a continuous wave laser at frequency 808 nm (the same of idler/signal photons), injected from the output of the fiber collimators (see fig. 2.6). The focal length of L_3 has been chosen to satisfied the

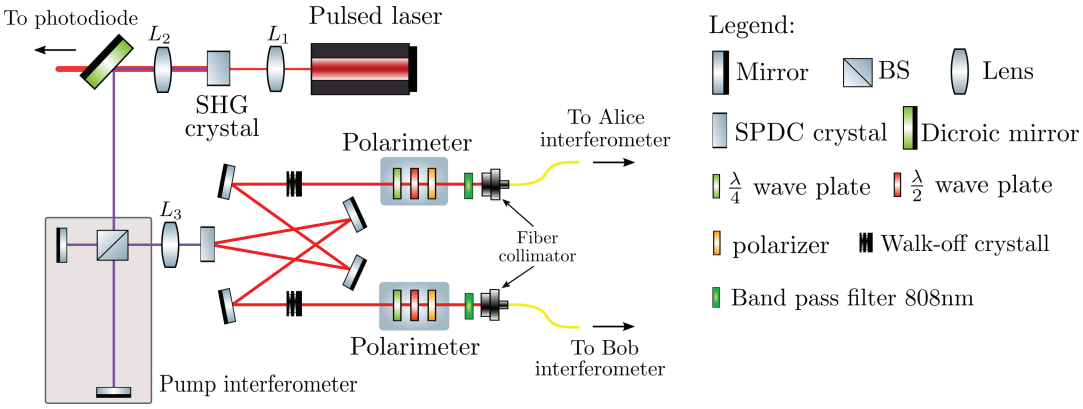


Figure 2.6: Detail of the setup for the generation of polarization entanlged photon pairs. Lens $L_1 = 75mm$ is used to focus the infrared beam of the pulsed laser on the SHG crystal. Lens $L_2 = 200mm$ is used to collimate the SHG beam. Realized with ComponentLibrary[2].

ratio $r = 1/\sqrt{2}$, by considering as pump waist the mean of x-y waist, $w_p = \frac{123.3+81.1}{2} = 102.2\mu m$. The optimal waist for idler/signal photons is $w = w_p/r = w_p/\sqrt{2} \approx 144\mu m$. In our experiment, the idler/signal photons have a waist of $w_{i,s} = 153.3\mu m$, and we can say that the relation $r = w_p/w_{i,s}$ is quite satisfied. With this configuration, the photon pairs generation is about 35000 pair/s with a pump power of 300mW. A future improvement, could be an optimization of the pump beam shape in order to obtain a better photons collection. We note that when the pump beam enters in the interferometer, then, at the output the waists of the short and long arms can be consider equivalent. In fact, the waist of the collimated pump is equal to $w_p^{col} = 1.2mm$, for which the Rayleigh length is equal to several meters. Since the path difference between short and long arms is $\Delta L = L - S = 60cm$, at the output the mode of two beams can be consider equivalent. In

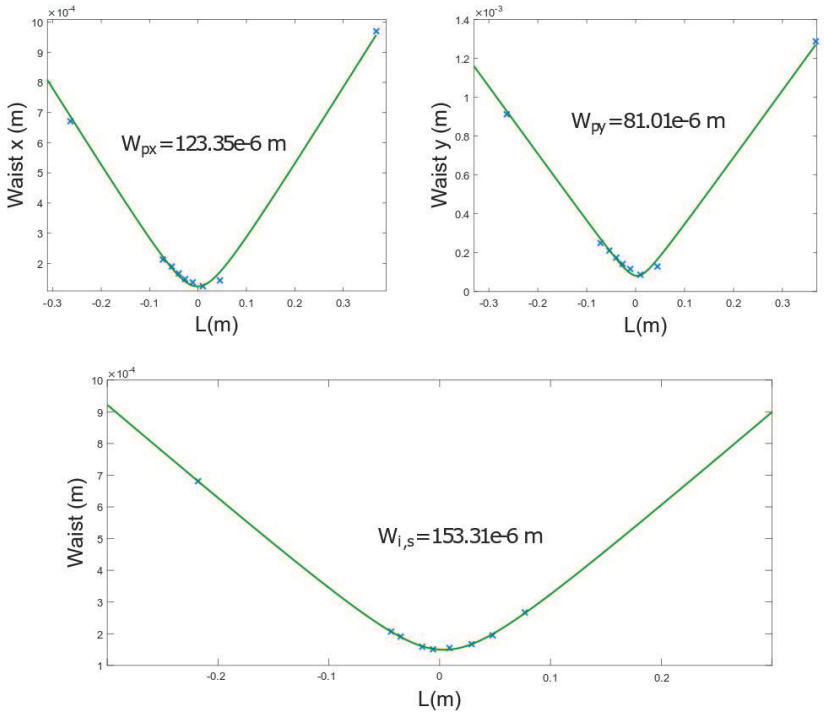


Figure 2.7: In this figure we can see the plots for pump and idler/signal waists. All the distances are take from the same fixed point (the position of the SPDC crystal).

addition, to get a better visibility[†] on the entangled state, we use narrow bandpass $3nm$ filter centered at $808nm$. The visibility of the source in $\pm$ basis is $\approx 98\%$.

2.4.1 Stabilization

Time-bin coincidence rate as we have seen in eq.2.19, depends on phase values of the three interferometers. These values are determined by the path differences between long L and short S arms of the interferometers and by the wavelength λ of the photons. The total phase introduced by an interfero-

[†]Visibility is defined as $V = (\max - \min)/(\max + \min)$, where max and min refers to max and min value of interference

meter is:

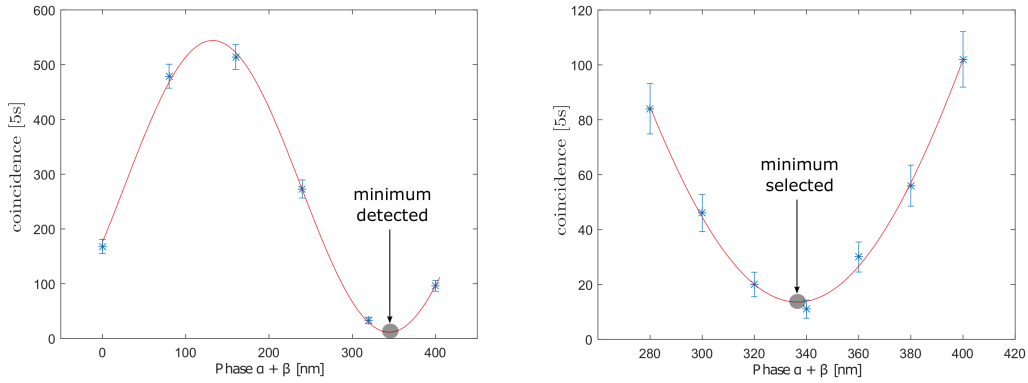
$$\theta = \frac{2\pi(L-S)}{\lambda} \tag{2.24}$$

Consider that the length difference between the two paths is affected by temperature changing, and the laser source has a small wavelength drift. These facts lead to an unstable system, and to compensate it we stabilize the interferometer phase with a passive methods. Active stabilization methods for interferometer performs better, but require a more complicated experimental setup[29,30]. Phase variations, in our case, are in the order of tens seconds for cycle. This means that the unstable interference pattern moves from a maximum to another in tens second. The basic idea is to set, before each measurement, the difference phase between Alice and Bob's interferometers in order to compensate the phase of the pump interferometer. Each measurement lasts up to 6 seconds, and in this time the interferometer can be considered stable.

In practice, before every time-bin measurement, we do:

- a fast scan of the coincidence pattern, by changing the phase value of Alice's interferometer (Bob's phase is not changed)
- fit the pattern with a sine curve, and find the minimum, that correspond to the value where the difference between Alice and Bob's phases compensates the pump phase
- a fine scan around the point calculated above, to find a precise position of the minimum
- the new position correspond to the phase of Alice $\theta_A = 0$, and we set the phase of Bob to $\theta_B = 0$.

In this way, for each measurement we have the same phase reference. The acquisition time is fixed to 5 second, and to increase the statistic of the outcome, we perform the same measurement repeatedly, following the above procedure each time.



(a) Fast scan (b) Fine scan

Figure 2.8: The fast scan in fig. (a) was obtained by moving the slider on the long arm of Alice's interferometer. The Bob's slider was stopped. This scan provides a coarse position of the minimum. The fine scan, fig. (b), provides a better position of the minimum. In this case, the position of the minimum has been found around 339 nm. At this point, the phases of Alice and Bob are set equal to zero, $\theta_A = \theta_B = 0$.

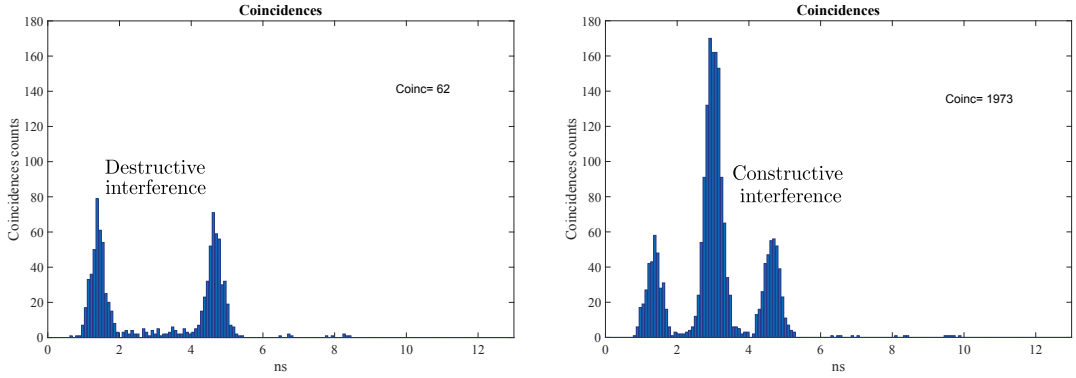


Figure 2.9: In this figure we can see destructive and constructive interference in the central peak. The visibility in this case, was $V = (\max - \min)/(\max + \min) \approx 94\%$.

2.4.2 Synchronization

The aim of this experiment is to build a source of hyperentangled photon in polarization and time-bin encoding, whit spatially separated measurement stations, for a future implementation on a free space optical link. When pulsed laser is used to generate time-bin entangled photon pairs, detection of these

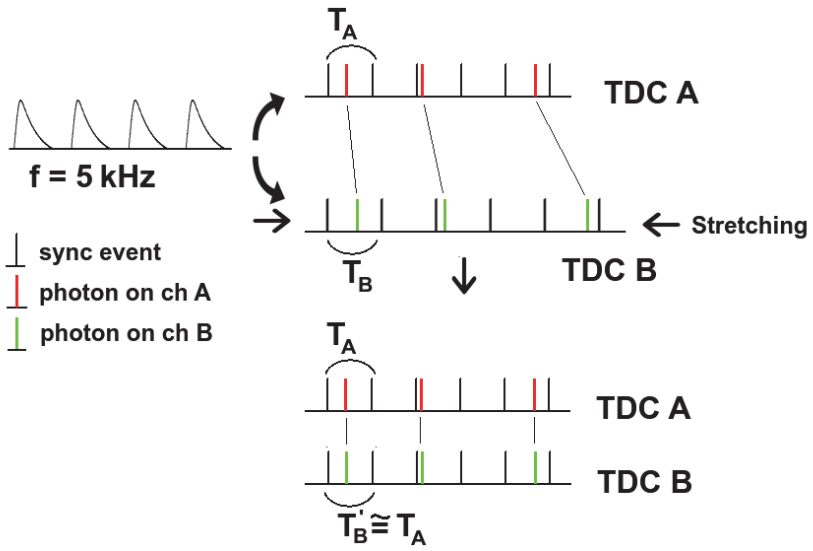


Figure 2.10: Decimate synchronization pulses are sent to Alice (A) and Bob (B) time to digital converters. Black lines indicate trigger synchronization events, red lines indicate photons detection on Alice side and with green lines photons detection on Bob side. In the ideal case, the same time interval, T, has to be measured in Alice and Bob's TDCs with the same value. But due to different internal clock drift, Bob's time interval T_B differs from Alice's time interval T_A. To recover a correlation a stretching is apply to Bob's time tags.

photon pairs have to be synchronized with the emission of the pump photons. Until the measurement stations are spatially near, they can use the same TDC to recorder detection time of the photons. In our setup, photons are detected by SPADs, which send a TTL signal to TDC when a photon is received. TDC can measure time lapsed between pulses (the arrival times of the photons), and converts them into temporal tags, an unsigned integer number with a resolution of $81ps$ (1 bin). TDC, due to its temperature and internal clock drifts, cannot measure events time with absolute accuracy. In other words, this instrument provides different outputs for the same time interval measured, in function of environment changes. Then, when the two receivers are spatially separated, each of them use its TDC and so, the measured time intervals drift in a different way between the two TDCs. But, in order to reconstruct the hyperentangled state, we need a correlation between photon detections in separate stations. The solution that we adopt consists on synchronize two different TDCs by a shared

reference time. A small part of the pulsed laser output, is sent to a photodiode and used as a trigger signal. The analog output of the photodiode is decimate, from 76 MHz to 5 kHz, and split by an FPGA into two signals. One is keep by Alice's TDC, which is located in the same place of the laser and it is used as local reference, and the order is sent to Bob's TDC by an optical link. This is composed by a laser modulated by the decimate trigger and a photodiode, which output is set to TTL level and sent to Bob's TDC.

To reconstruct hyperentangled state with two different TDCs, a subnanosecond accuracy between them is needed. Temporal correlation between Alice and Bob triggers are provided by a shutter on the pump laser output. When a measurement starts, shutter opens, and the trigger pulses are sent to TDCs. Alice and Bob can now create a correspondence between their received trigger pulses. The last thing to do, is the stretching of time intervals (see Fig. 2.10). We divide the entire array of time events, in fixed slots of dimension m, where the first and the last events are trigger pulse. The value of m is selected such that slots have dimension of few milliseconds, to avoid time drift in bigger time intervals. Then, we have used Alice's trigger as reference to transform Bob's time intervals:

$$t_i^B \rightarrow (t_i^B - t_0^B) \left[\frac{t_{i+m}^B - t_i^B}{t_{i+m}^A - t_i^A} \right] + t_i^A \rightarrow t_i'^B, \tag{2.25}$$

where t_i^B is the i-th trigger event on Bob side, and t_i^A the corresponding trigger event on Alice side. With this transformation, time recorded by Bob's TDC has a very well correspondence respect with time recorded by Alice's TDC. As we can see in Fig. 2.11, if we don't correct time intervals, we don't have a time correlation between the same events in different TDCs due to different drift of Bob's internal clock.

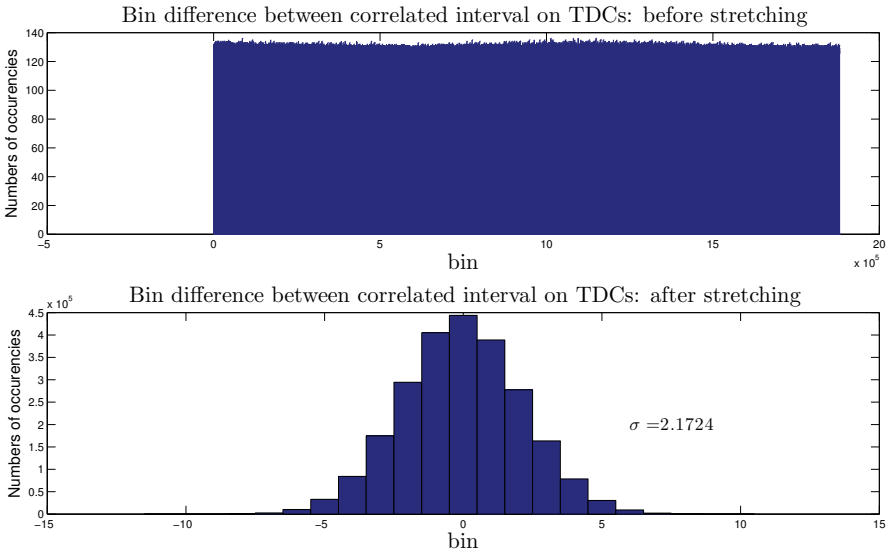


Figure 2.11: Without any correction (top), the differences between correlated trigger pulses on Alice an Bob, are spread on a very large time interval, precluding a reconstruction of the state. If the time is corrected (bottom), the differences between correlated trigger pulses are very narrow distributed. In this case it is possible to reconstruct a time correspondence between Alice and Bob.

2.5 Results

The ideal state that we want to generate is

$$|\Psi_{HE}\rangle = \frac{1}{2}\left(|H_A V_B\rangle - |V_A H_B\rangle\right) \otimes \left(|S_A S_B\rangle - |L_A L_B\rangle\right). \tag{2.26}$$

Distribution of hyper-entangled state between separate users has been tested first for each separate DOF of the state. We begin the analysis by considering the distribution between two separate stations of polarization entangled state. We have verified that the down-converted photon pair is in a superposition of the two states $|HV\rangle$ and $|VH\rangle$ by observing the density matrix of the generated state. To recover this density matrix we have compute a complete quantum tomography on the photon after the SPDC crystal, leaving out Alice and Bob's interferometers. The reconstruction of the density

matrix was performed with a maximum-likelihood algorithm[26]. The coincidence measurements were taken in a window of 25 seconds, with a coincidence window of 1.6 ns. Data has been taken by two distinguished computers, one for each measurement station, and then shared to recover the state.

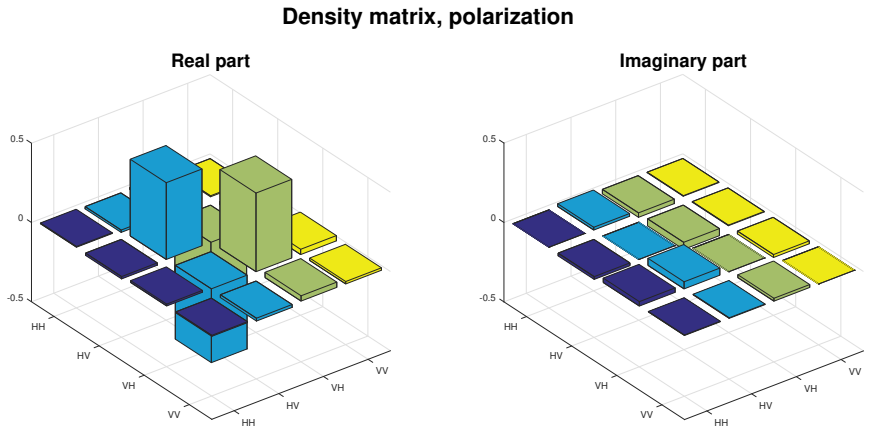


Figure 2.12: Real and imaginary part of polarization entangled state

The expected Bell state is $|\Psi^-\rangle = |HV\rangle - |VH\rangle$ which density matrix $\rho_P = |\Psi^-\rangle\langle\Psi^-|$ is

$$\rho_P = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{2.27}$$

The recovered density matrix by quantum tomography is:

$$\hat{\rho}_P = \begin{bmatrix} 0,005 & -0,014+0,017i & 0,011-0,027i & -0,006-0,003i \\ -0,014-0,017i & 0,484 & -0,465-0,044i & -0,017-0,003i \\ 0,011+0,027i & -0,465+0,044i & 0,495 & 0,033-0,018i \\ -0,006+0,003i & -0,017+0,003i & 0,033+0,018i & 0,016 \end{bmatrix} \tag{2.28}$$

To quantify the quality of the reconstructed state $\hat{\rho_P}$ compare to the ideal state ρ we use the three measurements described in chapter 2, where the error is computed with MonteCarlo simulation, by considering coincidence count distributed with Poisson distribution:

Fidelity	$F(\hat{\rho_P}, \rho_P) = 0.95 \pm 0.01$
Purity	$P(\hat{\rho_P}) = 0.92 \pm 0.02$
Linear Entropy	$S_L(\hat{\rho_P}) = 0.10 \pm 0.02$

In fig.2.12 we can see the graphical representation of the density matrix.

To verify time-bin distribution, we remove the polarization measurement devices. Then the density matrix has been recovered as describe for polarization state.

The expected Bell state is $|\Phi^-\rangle = |SS\rangle - |LL\rangle$ which density matrix $\rho_T = |\Phi^-\rangle\langle\Phi^-|$ is

$$\rho_T = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} \tag{2.29}$$

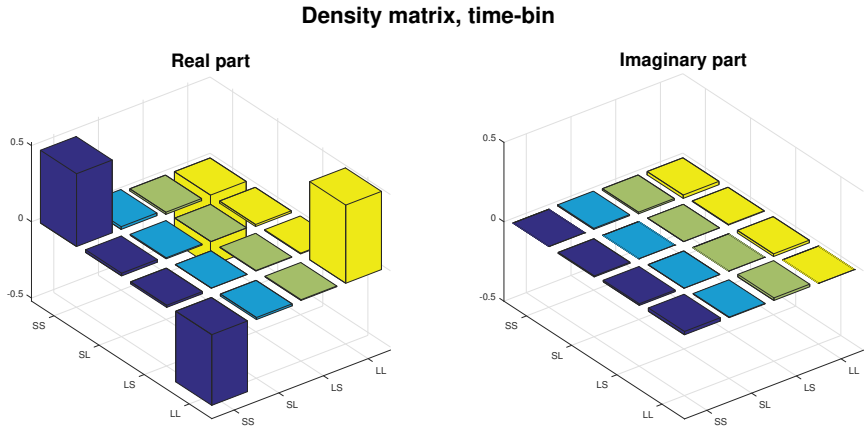


Figure 2.13: Real and imaginary part of time-bin entangled state

The recovered density matrix by quantum tomography is:

$$\hat{\rho}_P = \begin{bmatrix} 0,477 & 0,017+0,006i & -0,013-0,010i & -0,463-0,021i \\ 0,017-0,006i & 0,007 & 0,001 & -0,013-0,003i \\ -0,013+0,010i & 0.001 & 0,003 & 0,004-0,016i \\ -0,463+0,021i & -0,013+0,003i & 0,004+0,016i & 0,513 \end{bmatrix} \tag{2.30}$$

As for the polarization state, compare $\hat{\rho_T}$ with the ideal state ρ we use the three measurements:

Fidelity	$F(\hat{\rho_T}, \rho_T) = 0.96 \pm 0.02$
Purity	$P(\hat{\rho_T}) = 0.92 \pm 0.03$
Linear Entropy	$S_L(\hat{\rho_T}) = 0.10 \pm 0.03$

In fig.2.13 we can see the graphical representation of the density matrix.

As we can see above, the two states are well distributed between the two parties. At this point,

after we verify that the singles DOFs are well recovered, we perform an analysis on the distributed hyper-entangled state. The coincidences rate of the hyper-entangled source is of about 2600 coincidences/sec. A full tomography of n qubit requires $m = 4^n$ measurements setting. In our case $n = 4$ and a full tomography requires $m = 256$ measurements, but, due to laser instability we were unable to perform all the required measurements. In fact, the maximum number of measurements taken before a laser fault are $m' = 144$. With this set, as described in chapter 3, we can recover the density matrix by quantum tomography via compressed sensing. Here, we report the recovered matrix of the distributed hyper-entangled state (see fig. 2.14), and the parameters that describe the quality of the state.

Fidelity	$F(\hat{\rho^{144}_{HE}}, \rho^{ID}_{HE}) = 0.96 \pm 0.01$
Purity	$P(\hat{\rho^{144}_{HE}}) = 0.94 \pm 0.02$
Linear Entropy	$S_L(\hat{\rho^{144}_{HE}}) = 0.11 \pm 0.02$

2.6 Conclusion

In this chapter I have described the realization of an hyper-entangled photons source in polarization and time-bin DOFs. The distinctive feature of this source is that it works for users that are spatially separated to each other. This has been possible because of the precise time reference shared between the two users. The source has been tested between two fully separated users within laboratory distances. The results show that the distributed state is a very good approximation of the ideal desired. A future step, can be the use of this source to send quantum states through separated places, in order to implement quantum algorithm, as quantum dense coding or quantum teleportation, for long range distribution of hyper-entanglement photons.

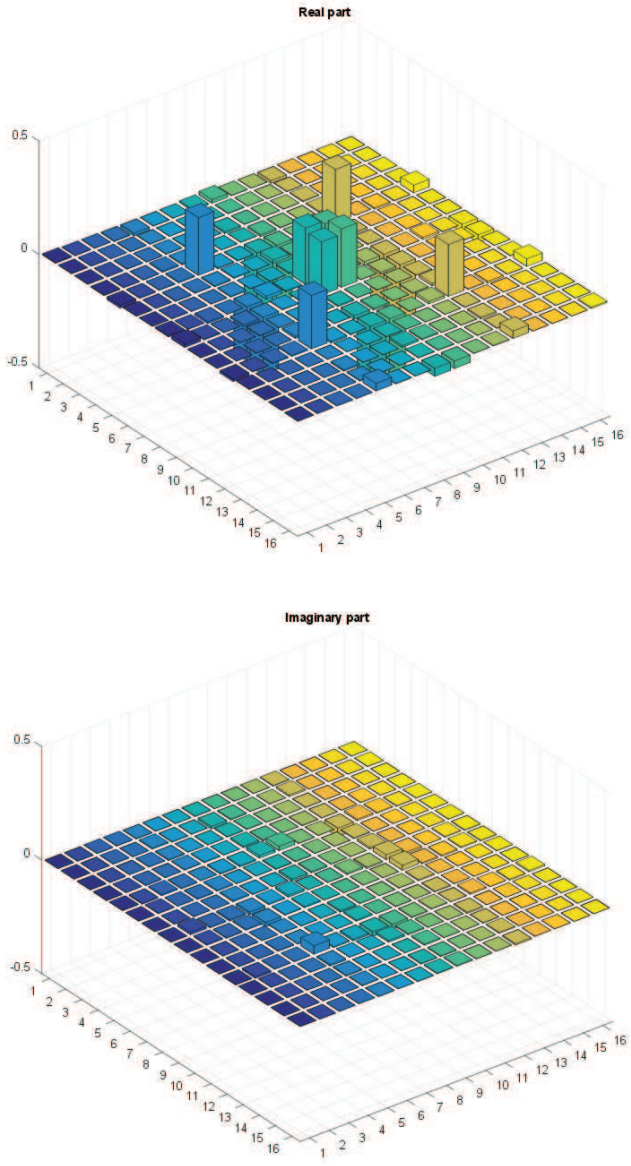


Figure 2.14: Real and imaginary part of hyper-entangled state. Numeric label correspond to ordered basis states $\{|HHSS\rangle, |HHSL\rangle, |HHLS\rangle, |HHLL\rangle, |HVSS\rangle, .., |VVLL\rangle\}$

3

Efficient Quantum Tomography

The accurate and efficient reconstruction of a quantum state is an important tool in quantum information science. Quantum tomography is the well know process used to reconstruct the density operator ρ of a unknown quantum state [54,53,26]. Performing a complete tomography with standard techniques, such as maximum likelihood [50,54], Bayesian mean [51,49] or linear regression estimation [52], requires a set of measurements that span the Hilbert space of the quantum state. If the density matrix of the state has dimension d, the number of required measurements is d^2. It means that the reconstruction of density matrix rapidly increases in complexity with the dimension of the system, carrying a prohibitively time-consuming procedures. For high dimensional states, the realization of the fully quantum tomography requires a lot of resources. As a consequence, efficiency methods for recover density matrix are needed.

A recent methods from classical signal processing science, called compressive sensing, can be exploited to recover a density matrix of a quantum state, when the matrix ρ has low rank (says r): in this case ρ can be reconstructed with $O(rd\log^2 d)$ [57] measurements, or even with $O(rd)$ [55]. We develop a new methods for a fast recover of the state in terms of measurements needed. We experimentally test our method with a two-photon hyperentangled state and compare it to existing protocols. Our method can be extremely useful in applications where one needs a rapid recovery of the states or when applied to large dimension states. In this chapter, first we review compressed sensing from a classical point of view and then we apply this technique to the quantum case. Then we show that compressive sensing can be considerably improved, in terms of the number of required measurements.

3.1 Classical compressed sensing

Reconstruct a signal from sampling measurement, in general, is an impossible task if no prior assumptions about the signal are provided. The well-know Nyquist-Shannon's theorem provides a sufficient condition for sampling rate, to reconstruct a signal with a limited bandwidth [1]. The theorem tells us that if we want to recover all the information about an unknown signal, with the prior knowledge only about its maximum frequency, we need to sampling the signal with twice this frequency. However, when the information are carried only by few frequency, sampling at such high rate could be a waste of resource. In the early 2000, E. Candès et al. [58,59], provided a novel sampling paradigm, called compressed sensing (CS), that allows to recover certain signals from fewer samples respect than conventional techniques. The theory of CS depends on principles:

- Sparsity, means that the information of the original signal is smaller than implied by its bandwidth. In other words, it means that CS relies on signal that have a concise representations in a proper basis $\mathcal{B}$.
- Incoherence, means that signal with a sparse representation over $\mathcal{B}$ must be spread out in the

measurements domain.

The term sparse means that the entries of the vector are all zero except for few elements. After data acquisition, CS uses computational power to numerical reconstruct the full signal from the small amount of sample data.

Let we see the general idea of the protocol[60]. Consider a vector $f \in \mathbb{R}^n$, where $f = \mathcal{B}x$, with x a sparse vector. When we measure a subset of the n coefficients of f, data acquired can be write as:

$$y_k = \langle f, \mathcal{A}_k \rangle, \qquad k \in M \tag{3.1}$$

where $\langle \cdot \rangle$ is the measurement operator, $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_n\}$ is the measurement basis and $M \subset \{1, 2, ..., n\}$ is a subset of cardinality $m < n$.
CS provides a reconstruction $f^* = \mathcal{B}x^*$, where x^* is the solution to the convex optimization program:

$$\min_{x' \in \mathbb{R}^n} ||x'||_{l_1} \qquad \text{s.t.} \quad y_k = \langle \mathcal{A}_k, \mathcal{B}x' \rangle, \quad \forall k \in M \tag{3.2}$$

with $||x||_{l_1} = \sum_i |x_i|$ the l_1-*norm*.
The solution x^* is provably exact if f is sufficiently sparse.

An example is the reconstruction of the spectrum (see Fig. 3.1) of an ideal musical instrument that can reproduce a lot of frequencies sound, says n, but at the moment it reproduces only few frequencies, says s. This spectrum is defined by only s parameters, that are much smaller than n, the numbers of parameters that describe the entire spectrum. To reconstruct such spectrum with Nyquist-Shannon's theorem, we need a lot of samples, not less than $f_{max}/2$, because the theorem reconstruct generic signals. On the other hand, CS algorithm (eq. 3.2) provides, with only $s \log(n)$ randomly chosen measurements in time domain, an exact recovery of the signal with high probability[58]. At finally, when we need for reconstruct a sparse signal in the frequency domain, CS provide complete information

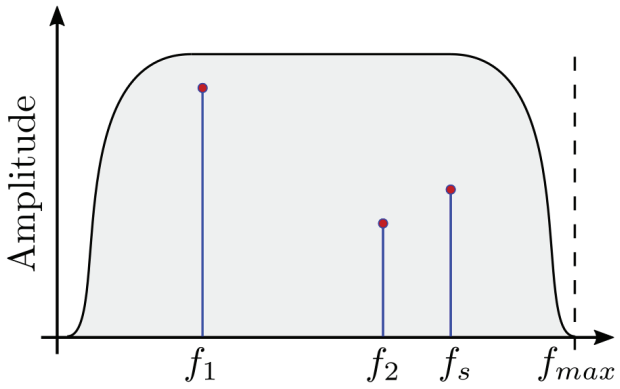


Figure 3.1: Spectrum of a signal with only s frequencies. CS provide an exact reconstruction with only $s\log(n)$ randomly chosen measurements.

about an unknown signal using fewer measurements than traditional methods.

3.2 Quantum tomography via compressed sensing

Now, we return to the quantum world. When we deal with general quantum state, they have support on an r-dimensional space, with $r < d$, meaning that the density matrix is sparse in some basis and, if the state is subjected to some noise, it can be approximated to a matrix of rank r. This is a strong analogous to the CS classical case, but, in order to apply CS to quantum tomography, some changes have to be considered. First, in classical CS, the norm used in minimization procedure is the l_1*-norm*. Quantum states are described by matrices, and to find a sparse solution the l_1*-norm* is replaced with the *trace norm*, defined as

$$||A||_* = \text{trace}(\sqrt{A^*A}) = \sum_i \sigma_i \tag{3.3}$$

where σ_i are the singular values of matrix A, which is used to minimize the rank of the matrix[61,62]. In addition, Pauli matrices are used as measurement operator, because they are incoherent with respect

to $every$ matrix with rank r [62,63]. At this point, CS can be apply to recover an unknown quantum state with rank r by randomly chosen only $rd\log^2(d)$ Pauli measurements [57]. This method has already been tested experimentally [65,69] also with projective measurements [64].

Consider a quantum state ρ of n-qubit, with dimension $d = 2^n$. For such state, the corresponding Pauli matrices σ_k^n, are of the form $\sigma_k^n = \otimes_{i=1}^n \sigma_i$, with $\sigma_i \in \{\sigma_0, \sigma_1, \sigma_2, \sigma_3\}$. Then, if we randomly choose m of these Pauli matrices, and measure the state obtaining the result $\mathrm{Tr}\left[\rho\sigma_k^n\right] = a_k$, the solution ρ^* of the convex problem

$$\min ||\rho'||_* \qquad s.t. \quad \mathrm{trace}(\rho) = 1, \quad \mathrm{trace}(\rho'\sigma_k^n) = a_k, \quad k = 1, ..., m \tag{3.4}$$

is unique with probability exponentially small in c if the number of measurements is equal to $m = crd\log^2(d)$.

A recent work by Kalev [56] shows that if density matrix is constrained to be positive, it is possible to use any optimization method to search the low rank density matrix.

In our works we use condition on trace ($\mathrm{trace}(\rho) = 1$), together with minimization of trace norm, that can be considered a surrogate of positivity for density matrix. In fact, the trace of a matrix correspond to the sum of its eigenvalues. In addition, when a matrix is hermitian, as for density matrix, trace norm is equal to the sum of the absolute values of the eigenvalues of the matrix. This means that when we minimize the sum of the absolute values of eigenvalues, and at the same time their signed sum is constrained to be a positive number, solution gives positive eigenvalues.

Under influence of noise, like when we take data from an experiment, problem described in 3.4, should be replaced by the following [64]

$$\min ||\rho'||_* \qquad s.t. \quad \mathrm{trace}(\rho) = 1, \quad \sum_{k=1}^{m} \left[\mathrm{trace}(\rho'\sigma_k^n) - a_k\right]^2 \leq \epsilon, \tag{3.5}$$

where ϵ corresponds to experimental data error, and can be estimated by

$$\epsilon = \sum_{k=1}^{m} \omega_k^2, \tag{3.6}$$

where ω_k is the standard deviation of a_k.

We use this method to recover the density matrix of hyperentagled state, that we saw in the chapter 1. To solve the convex problem 3.4, we use SDPT3[70] a semidefinite-quadratic-linear solver for Matlab, modeled with CVX[71].

3.3 Fast reconstruction for a state with prior information

In this section we see how we adapt techniques from compressive sensing to develop an experimentally efficient method for fast recovery of a density matrix when prior information are available. This technique is based on a modified version of the compressive sensing method: while in the original CS the measurements are chosen at random, we will show that specific choices of the measurement sequence improve significantly the efficiency of the reconstruction. The idea is that when an experiment is delineate, design scheme of the source provides general information about the experimental generated state, that typically is well approximated by an ideal one.

When compressive sensing is used to recover a density matrix, is assumed that the density matrix is sparse. Such assumption is legitimate only if we have information of the quantum state we would like to generate: however, all available information is only partially used in standard compressive sensing. On the other hand, our method fully exploits such prior information to considerably improve compressing sensing for quantum state reconstruction.

Indeed, based on such prior information, we find a method that gives a measurements sequence for a fast state reconstruction in terms of the required number of measurements. This methods has been tested experimentally and via simulations.

In other words, our methods using the information on which quantum state we aim to generated, find a measurement set in order to obtain a further improvement on the efficiency of the tomography, namely reduces the number of measurements required to obtain a fair estimation of the state fidelity. The basic idea is that each measurement reduces the numbers of compatible (i.e. satisfying the constraint in eq. 3.4) density states in a different way depending on the measurement result a_k. Generic states ρ on a d dimensional Hilbert space can be written as

$$\rho = \frac{\mathbb{1}}{d} + \vec{r} \cdot \vec{\Gamma} \,, \tag{3.7}$$

where $\vec{r}$ is the Bloch vector and Γ_k are linear independent matrices with these properties

- $\mathrm{Tr}(\Gamma_j \Gamma_k) = \frac{d-1}{d} \delta_{jk} \,, \qquad j,k = 1, \ldots, D \equiv d^2 - 1 \,,$
- $\mathrm{Tr}(\Gamma_k) = 0 \,,$
- $\Gamma_k = \Gamma_k^* \,,$

Physical states are characterized by the equation $\mathrm{Tr}(\rho^2) = \frac{1+(d-1)\vec{r}^2}{d} \leq 1$, corresponding to the D-ball with radius $\vec{r}^2 \leq 1$. Consider now a qudit and an observable A,

$$A = \mathrm{Tr}(A)\frac{\mathbb{1}}{d} + \vec{s} \cdot \vec{\Gamma} \tag{3.8}$$

where $\mathrm{Tr}(A) = 1$ and $|\vec{s}| = 1$, if A is a projector onto a pure state. The constraint $\mathrm{Tr}(A\rho) = a$, that corresponds to the probability to project A onto ρ, can be written as:

$$\vec{r} \cdot \vec{s} = \frac{\delta}{1 - \frac{1}{d}} \,, \tag{3.9}$$

where we have defined $\delta = a - \mathrm{Tr}(A)/d$.

This equation defines an hyperplane in the $\mathbb{R}^D$ space. The intersection of such hyperplane with the D-ball gives rise to a $(D-1)$-ball of radius

$$R = \sqrt{|\vec{s}| - (\vec{r}\cdot\vec{s})^2} = \sqrt{1 - \frac{\delta^2}{(1-1/d)^2}} \leq 1\,. \tag{3.10}$$

This means that physical states compatible with the constraint $\mathrm{Tr}(A\rho) = a$ lies within the above ball. The bigger the volume of the ball, the large the compatible physical states. As a consequence, the information is inversely proportional to the volume of the ball. What we are looking for, is to find which observable A gives the lowest volume. The volume of such ball is given by

$$V_{S_{d^2-2}} = \frac{\pi^{d^2/2-1}}{\Gamma(d^2/2)} R^{d^2-2} \tag{3.11}$$

It is easy to see that the available volume is maximal if and only if $a = \mathrm{Tr}(A)/d$ and its value is given by $V_{\max} = \frac{\pi^{d^2/2-1}}{\Gamma(d^2/2)}$. For values of a different from $\mathrm{Tr}(A)/d$ the available volume is reduced and the ratio between $V_{S_{d^2-2}}$ and $V_{\max}$ is given by

$$\frac{V_{S_{d^2-2}}}{V_{\max}} = R^{d^2-2}\,. \tag{3.12}$$

Observables giving a smaller volume of compatible states are thus more informative. Thus, observables with expectation values deviating from $1/d$ give more stringent and informative constraints on the state. In fig.3.2 we can see how the volume of compatible states with the constraint $\mathrm{Tr}(\mathbf{A}\rho) = a$ changes in function of a. For instance, if we consider the case $d = 2$, we see that the measurements $\mathrm{Tr}(\mathbf{A}\rho) = 0$ or $\mathrm{Tr}(\mathbf{A}\rho) = 1$ are those that minimize the volume. In other words, if we project a single qubit ρ_2 onto A with a probability $\mathrm{Tr}(\mathbf{A}\rho_2) = 1$ (0), the state of the qubit will be $\rho_2 = |A\rangle\langle A|$ $(|A^\perp\rangle\langle A^\perp|)$, but if the probability is $\mathrm{Tr}(\mathbf{A}\rho_2) = 0.5$ there are a lot of possible states that satisfy the constraint.

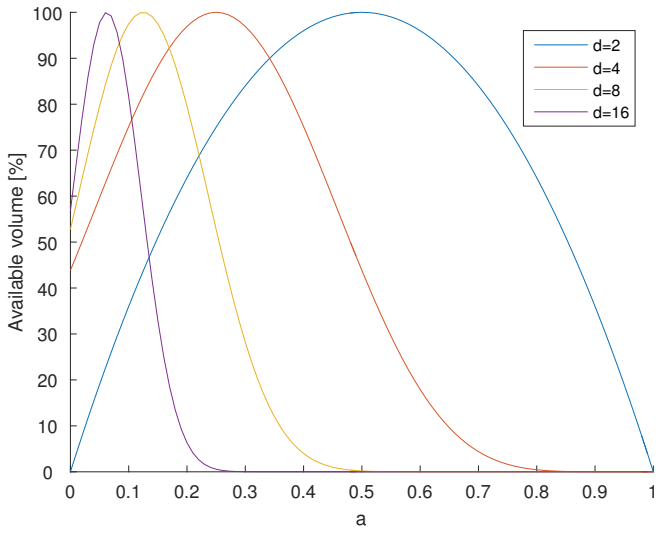


Figure 3.2: Available volume of physical states compatible with the only constraint $\mathrm{Tr}(\mathbf{A}\rho) = a$ for different values d of the space dimension.

For states of higher dimension, we see that the less informative observable are those with expectation values near $1/d$.

Such intuition can be extended to a set of different measurements. Let's consider N measurements defined by the linear independent vectors $\vec{s}_k$. Each measurement gives the constraint $\mathrm{Tr}(\rho A_k) = a_k$, or

$$\vec{r} \cdot \vec{s}_k = \frac{a_k - \mathrm{Tr}(A)/d}{1 - 1/d} \equiv \gamma_k \tag{3.13}$$

Since the vectors $\vec{s}_k$ are linearly independent, the vector $\vec{r}$ can be written as

$$\vec{r} = \sum_{k=1}^{N} c_k \vec{s}_k + \vec{S}_\perp \,, \tag{3.14}$$

where $\vec{S}_\perp \cdot \vec{s}_k = 0, \forall k$. The coefficient c_k can be easily find as

$$c_k = \sum_j (\Lambda^{-1})_{kj} \gamma_j \,, \tag{3.15}$$

where

$$\begin{aligned} \Lambda_{jk} &= \vec{s}_j \cdot \vec{s}_k \\ &= \frac{1}{d-1} \left[d \,\mathrm{Tr}(A_j A_k) - \mathrm{Tr}(A_j)\mathrm{Tr}(A_k) \right] \end{aligned} \tag{3.16}$$

In matricial form we can write $\mathbf{c} = \Lambda^{-1}\boldsymbol{\gamma}$. Since $\vec{r}$ must satisfy the constraint $|\vec{r}| \leq 1$, then

$$|\vec{r}|^2 = |\vec{S}_\perp|^2 + \boldsymbol{\gamma}^T \Lambda^{-1} \boldsymbol{\gamma} \leq 1 \tag{3.17}$$

such that

$$|\vec{S}_\perp| \leq \sqrt{1 - \boldsymbol{\gamma}^T \Lambda^{-1} \boldsymbol{\gamma}} \tag{3.18}$$

The N constraints $\mathrm{Tr}(A_k \rho) = a_k$ reduce the space of the compatible states to a $(d^2 - N - 1)$-ball with radius $|\vec{S}_\perp|$. The volume of such ball is minimized when $\boldsymbol{\gamma}^T \Lambda^{-1} \boldsymbol{\gamma}$ is maximum. Then, the algorithm orders the sequence of measurements in order to maximize at each step the term $\boldsymbol{\gamma}^T \Lambda^{-1} \boldsymbol{\gamma}$.

From the above observation, it is clear that, if the quantum state to be generated is known, it is possible to find what is one of the measurement set that would give more information on the density matrix. By using a sequence of measurements that contain such highly informative observables, it is possible to improve the efficiency of the compressive sensing method. Such sequence will realize a super-compressive sensing reconstruction of the quantum state, requiring less measurements compared to normal compressive sensing method.

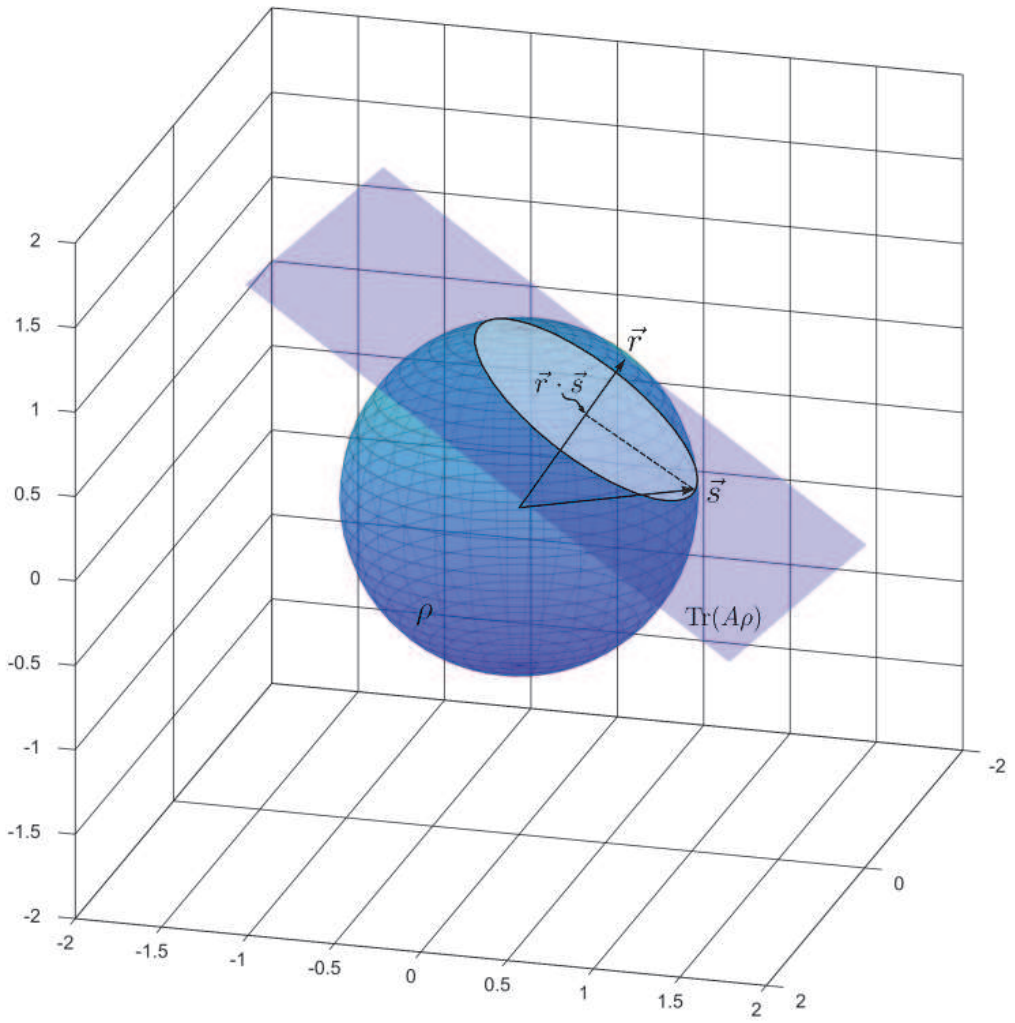


Figure 3.3: Projection of an observable onto a qubit. The white circle represents the all possible observables that give the same projection. The bigger the circle, the smaller the information obtains from observable A.

3.4 Result for simulation and real cases

In this section we will see the results from simulation and from experimental data. The best sequence has been computed as described in the previous section, and has been tested with an ideal hyper-

entangled and GHZ states[21]. Then the density matrix of the ideal state is recovered via CS quantum tomography with the best sequence measurement and compared to normal CS quantum tomography (with random sequence measurement). To prove the robustness of our methods, test was performed with three different estimators. The first is that described in eq. 3.4, the other two are the Dantzig estimator[67]

$$\rho_D = arg\min_X ||X||_{\text{tr}} \; s.t. \; ||M^*(M(X) - y)|| \leq \lambda \tag{3.19}$$

and the Lasso estimator[68]

$$\rho_L = arg\min_X \left[\frac{1}{2}||A(X) - y||_2^2 + \mu||X||_{\text{tr}}\right] \tag{3.20}$$

where $M(X) = (\text{Tr}(A_1X), \ldots, \text{Tr}(A_NX))$ and $y = (b_1, \ldots, b_N)^*$. These estimators are convex function constrained by convex constrains, so methods of convex programming guarantee that the solution can be found efficiently[62]. We add trace normalization condition for each estimators. In addition our method has been tested also with depolarized hyperentangled state.

The ideal hyper-entangled state is

$$|\Psi_{HE}\rangle = \frac{1}{2}\left(|HV\rangle - |VH\rangle\right) \otimes \left(|SS\rangle - |LL\rangle\right). \tag{3.21}$$

To simulate standard CS tomography, we chose a complete random set of measurements, obtained from a combination of the projectors into the states $\{|H_P\rangle, |V_P\rangle, |D_P\rangle, |L_P\rangle\}$ in polarization, where $|D_P\rangle = 1/\sqrt{2}(|H_P\rangle + |V_P\rangle)$ and $|L_P\rangle = 1/\sqrt{2}(|H_P\rangle + i|V_P\rangle)$, and $\{|L_G\rangle, |S_T\rangle, |D_T\rangle, |L_T\rangle\}$, in time-bin, where $|D_T\rangle = 1/\sqrt{2}(|L_G\rangle + |S_T\rangle)$ and $|L_T\rangle = 1/\sqrt{2}(|L_G\rangle + i|S_T\rangle)$. Then, the result of each measurements has been computed simulating the measurement on the ideal state (3.21). Finally, the state has been recovered via CS and to quantify the quality of the recovered state we use the

*Parameters λ and μ are optimized on simulation trials[62].

fidelity between the recovered and the simulated states. For each estimator, we compute 32 simulation with different random sets.

The first projector of our sequence has been chosen by minimizing eq.3.12. Then the others projectors, has been calculated minimizing eq. 3.18. The only difference with standard CS tomography is that we choose a ordered set of measurements instead of a random one. To prove the robustness of our methods, we have simulated the reconstruction of a depolarized hyper-entangled state, as described in fig. 3.5. Depolarization has been added to each DOF of the hyper-entangled state:

- POLARIZATION

$$\rho_p = (1 - p_c - p_w)|\Phi_p\rangle\langle\Phi_p| + p_c\rho_p^c + p_w\frac{\mathbb{1}}{4} \tag{3.22}$$

  where $|\Phi_p\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$, and $\rho_p^c = |HV\rangle\langle HV| + |VH\rangle\langle VH|$

- TIME-BIN

$$\rho_t = (1 - p_c - p_w)|\Phi_t\rangle\langle\Phi_t| + p_c\rho_t^c + p_w\frac{\mathbb{1}}{4} \tag{3.23}$$

  where $|\Phi_t\rangle = \frac{1}{\sqrt{2}}(|SS\rangle - |LL\rangle)$, and $\rho_p^c = |SS\rangle\langle SS| + |LL\rangle\langle LL|$

In our simulation color and white noise are supposed independent and assume a value of $p_c = 0.05$ for color noise and $p_w = 0.1$ for white noise.

In fig. 3.6, we report the comparison between our methods and standard CS tomography for a GHZ state

$$|\Psi_{GHZ}\rangle = |0000\rangle + |1111\rangle. \tag{3.24}$$

This state has a sparse matrix, and we use that to prove that our methods is independent of density matrix type. As we can see the fidelity convergence in this case is faster than the hyper-entanglement reconstruction, because the density matrix of the state $|\Psi_{GHZ}\rangle$ has less numbers of coefficient greater

than zero than the hyper-entangled state $|\Psi_{HE}\rangle$ (eq. 2.26). Density matrix of $|\Psi_{GHZ}\rangle$ state has only 4 elements different from 0, instead density matrix of $|\Psi_{HE}\rangle$ has 16 elements different from 0. If we use a random set for the GHZ state, from the figure 3.6 we see that the error bars are bigger than the other cases. This can be explained by the fact that for the GHZ state, there is a lower number of measurements that give information about the only 4 elements greater than 0, and if we choose a random sequence, the probability that all of these occur on the first measurement is lower and, as a consequence, the recovery of the state is slower. On the other hand, if some of these informative measurement occur first, the recovery is faster, because to recover the GHZ state, are needed a lower number of measurements.

N	Projector A	$\mathrm{Tr}(A\rho)$
1	$\|H_P V_P\rangle\|L_G L_G\rangle$	$0,25$
2	$\|H_P V_P\rangle\|S_T S_T\rangle$	$0,25$
3	$\|V_P H_P\rangle\|L_G L_G\rangle$	$0,25$
4	$\|V_P H_P\rangle\|S_T S_T\rangle$	$0,25$
5	$\|H_P V_P\rangle\|L_T L_T\rangle$	$0,25$
6	$\|H_P V_P\rangle\|D_T D_T\rangle$	0
7	$\|V_P H_P\rangle\|D_T D_T\rangle$	0
8	$\|V_P H_P\rangle\|L_T L_T\rangle$	$0,25$
9	$\|D_P D_P\rangle\|L_G L_G\rangle$	0
10	$\|D_P D_P\rangle\|S_T S_T\rangle$	0
11	$\|L_P L_P\rangle\|L_T L_T\rangle$	0
12	$\|L_P L_P\rangle\|L_G L_G\rangle$	0

Table 3.1: First 12 measurements from the best sequence find by our methods.

We can see that our method performs better than standard CS tomography with random sequence of measurements. We would like to stress, that this method cannot be applied to a generic random quantum state. In this case the performance is the same as for standard CS technique. The best sequence measurement can be found only if one can access to full information about the state. In table 3.1 is reported the first 12 measurements obtained with our methods, and the expectation values of the

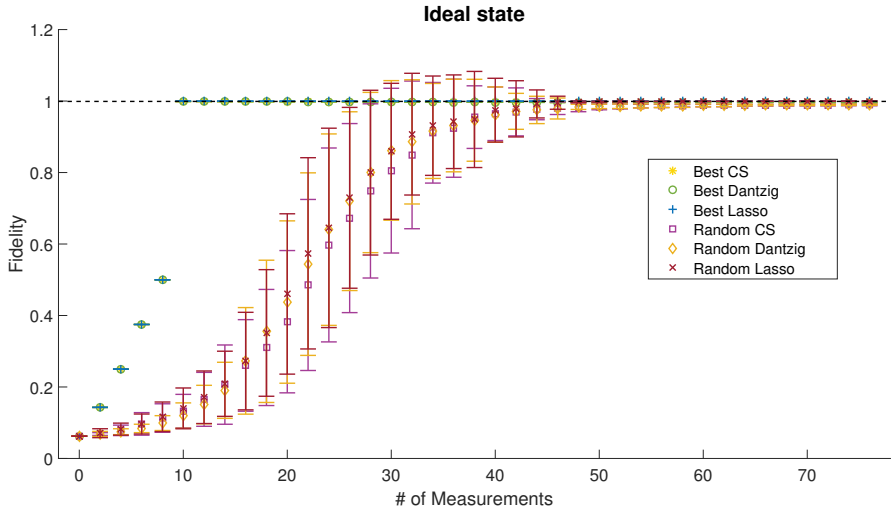


Figure 3.4: Fidelity as a function of the number of measurements for three different estimators. The simulated state is an ideal hyper-entagled state. As we can see, our method (best sequence) requires less measurements than the standard method (random sequence) to converge to the final value. When the parameters of eq. 3.19 and eq. 3.20 are optimized, the three estimators give about the same results. We note that Lasso estimator perform little better than the others. Error bars on Best lines are zero because in this simulation we don't add any noise, and the result is deterministic because the measurement set is the same.

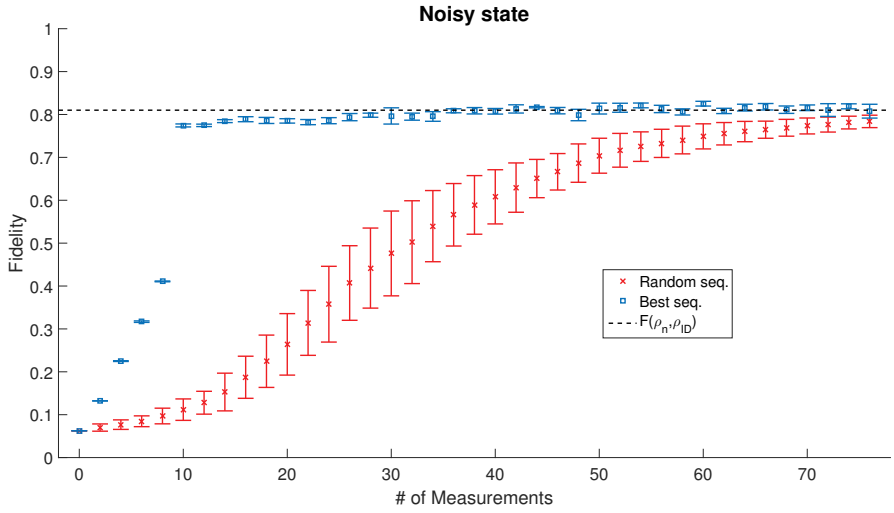


Figure 3.5: Fidelity as a function of the number of measurements for a noisy state. The simulated state is an noisy hyper-entagled state, with color noise $p_c = 0.05$ and white noise $p_w = 0.1$ (see eq.3.22 and 3.23).

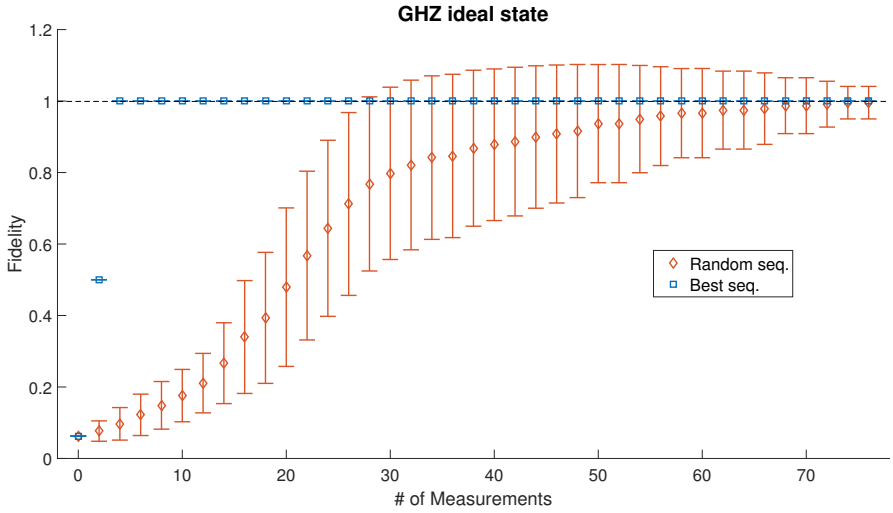


Figure 3.6: Fidelity as a function of the number of measurements for the simulated GHZ state.

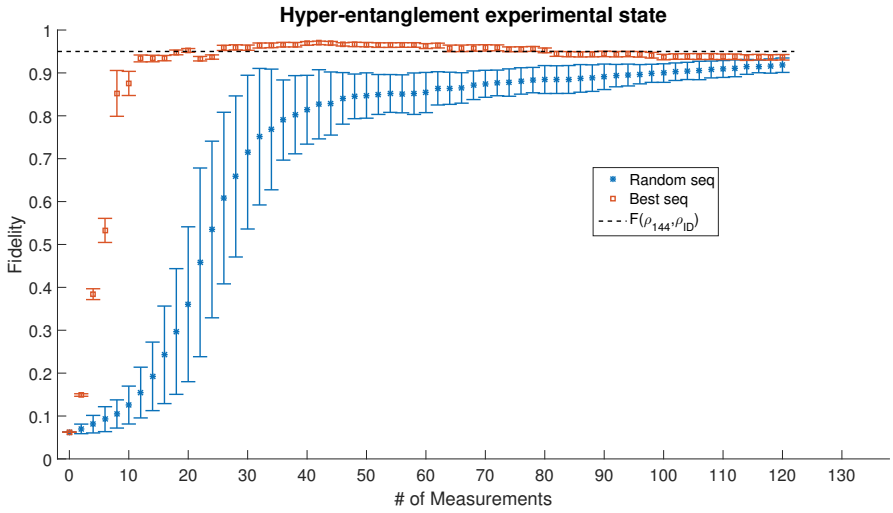


Figure 3.7: Fidelity as a function of the number of measurements for hyper-entanglement experimental state. As we can see, the reconstruction with our methods overshot the final fidelity. This can be explained by the fact that CS try to find a low rank solution which corresponds to a pure state. However, with few measurements it is difficult to estimate the noise, and this fact leads to a purest recovered state than the real state.

projectors. We see that these first measurements are those with higher expectation values (within our set there aren't measurements with expectation values greater than 0.25) or lower. No measurements

with expectation values between 0 and 0.25 are presented.

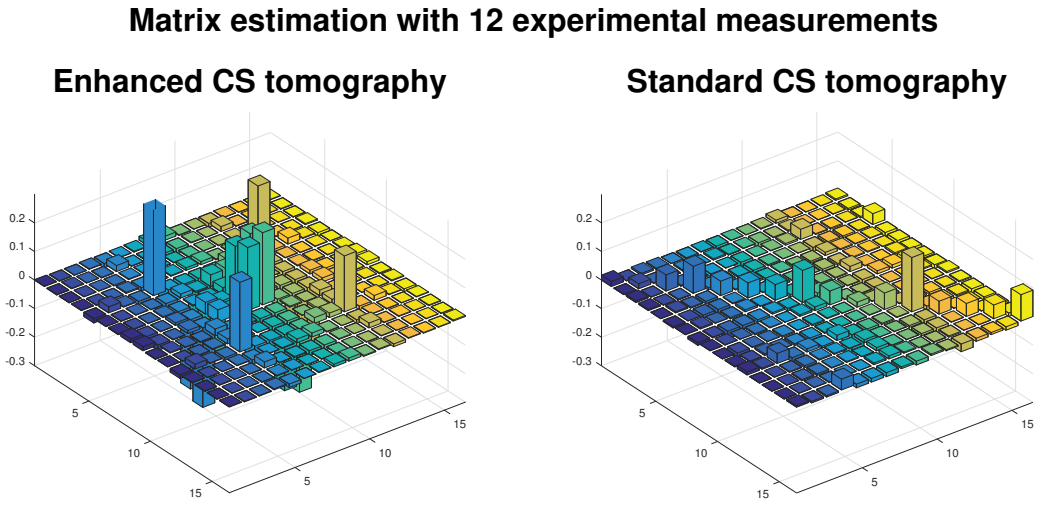


Figure 3.8: Real density matrix from experimental state recover with only 12 measurements with our method (on the left) and with standard method (on the right). Imaginary part can be neglected.

In figure 3.8 we can see the comparison between recovered experimental state by our method and by standard CS tomography. With only 12 measurements our method give a very good estimation of the real state compare to standard CS. The quality of the recovered state ρ_{12} with 12 measurements is reported in tab.3.2, while for standard CS in tab.3.3, where ρ_{HE} is the ideal hyper-entangled state.

Fidelity	$F(\rho_{12}, \rho_{HE})$	0.94 ± 0.01
Purity	$P(\rho_{12})$	0.97 ± 0.01
Linear Entropy	$S_L(\rho_{12})$	0.03 ± 0.01

Table 3.2: Entanglement measurements for the state recovered with 12 measurement by using our method. The linear entropy is lower compared to the recovered state with 144 measurements. See fig. 3.7.

Fidelity	$F(\rho_{12}^{ST}, \rho_{HE})$	0.15 ± 0.06
Purity	$P(\rho_{12}^{ST})$	0.16 ± 0.06
Linear Entropy	$S_L(\rho_{12}^{ST})$	0.90 ± 0.07

Table 3.3: Entanglement measurements for the state recovered with 12 measurement by using standard compressed sensing.

Fidelity between the state ρ_{12} and the state recover with all 144 measurement ρ_{144} is

$$F(\rho_{12}, \rho_{144}) = 0.99 \pm 0.01 \tag{3.25}$$

showing that ρ_{12} is a good estimation of the final state.

3.5 Conclusion

In this chapter we have seen that it is possible to recover a density matrix with few measurements respect standard compressive sensing tomography. This method can be very useful in the situation where one knows an estimation of the expected state. With this information it is possible to find an ordered set of measurements that gives a very fast reconstruction of the state via quantum CS tomography. The ordered measurement set that we have found was tested with different estimators and noisy states, showing that the fast convergence are preserved. In addition we prove that our method works also for a real case. With only few measurements (12 in experimental case) we are able to recover the density matrix of an hyper-entangled photon pair with dimension $d = 16$. If we compare our results with standard quantum tomography technique, as maximum likelihood or linear regression estimator tomography, which require $d^2 = 256$ measurements, is very great improvement in term of required resource for state reconstruction.

4

High visibility time-bin entanglement for Chained Bell inequality

The violation of Bell's inequality requires a well designed experiment to validate the result. In energy-time experiment, proposed initially by Franson in 1989[75], there is an intrinsic loophole due to the implementation of the interferometer. To obtain a violation in this type of experiment, a chained Bell[85,78] inequality must be used. However, the bound due to local realism, impose an high visibility on the energy-time entangled state, greater than 94.63%. In this work[66], we show how we can reach such high visibility, with which we can violate a chained Bell inequality with 6, 8 and 10 terms. Some of the results presented in this chapter are published in the master thesis of Mantoan[125].

4.1 Loophole in time bin entanglement

In his well known work[75], Franson proposed a Bell inequality for energy-time entanglement to investigate local realism. The proposed experimental configuration consists in a source of two correlated photons that are generated by SPDC process with a continuous-wave (CW) pump laser. The two generated photons are directed towards two identical unbalanced Mach-Zender interferometers. Into the interferometers, each photon may follows two different paths, which are called long (L) or short (S). The optical paths difference, $\Delta\mathcal{L} = L - S$, satisfies the relation $\tau_c \ll \Delta\mathcal{L}/c \ll \tau_p$, where τ_c and τ_p are the coherence times of the SPDC and pump photons respectively, and c is the speed of light. In this way, no first order interference effect appears on single photon counts. From all two-photons detection, only 50% corresponds to entangled photons. Indeed, by post-selecting those events in which the delay between the two photons detection is lower that $\Delta\mathcal{L}/c$, two photon interference occurs and a Bell inequality can be violated. Those post-selected coincidences correspond to events in which SPDC photons take both the long paths, or both the short ones.

As pointed out in several works[76,77,79], the Franson's scheme suffers from an intrinsic loophole. Indeed a local hidden variable (LHV) model can reproduce the quantum description for the fourth order interference exploiting the discarded events[77,82,84,79,86]. Different approaches are proposed to reach a violation of local realism without the negative effects of postselection. As described in different works[79,83,80,81] modifying the experimental setup, could be a solution to the problem.

As we have already described, in a energy-time experiment, the photon pair can be generated in any point within the coherence time of the pump. In this way, the times emission of photon pairs are undetermined within the coherent time of the pump laser. A time-bin experiment differs from the previous, because the laser pump is pulsed. Before hitting the crystal, the laser pulse is splitted into two pulses. The photon pair are now generated by a superposition of this pulses, therefore the emission times consist in two well defined moments. A similar LHV model introduced for energy-

time entanglement can be used to describe a LHV model for time-bin entanglement.

4.1.1 LHV model for time-bin entanglement

A time bin entanglement experiment requires a postselection procedure, where 50% of the events are discarded in the correlation functions. As explained by Cabello et al.[81], the 50% postselection procedure allows the sub-ensemble of selected events to depend on the phase settings. As a consequence, if all events are included, the Bell inequalities are not violated. This means that a local hidden variable (LHV) model can describe the experiment, as shown by Aerts[77] and Jogenfors[86].

In such experiment, observers have a common reference clock given by the pump pulses. Consider the general time-bin scheme (see chapter 2), where observer sees three different arrival times: $t_0 - \Delta T$ for short-short path (here we call this event early, E), t_0 for short-long and long-short paths (medium, M) and $t_0 + \Delta L$ for long-long path (late, L), where ΔL is the time difference between short and long paths. For each detection time, E, M and L, a measurement indicated by a and b for Alice and Bob, can have two outcomes, $+$ and $-$.

Consider now the probability

$$P(a, b|\phi_A, \phi_B) \tag{4.1}$$

where ϕ_A and ϕ_B are the measurement settings for Alice and Bob. For the detection $M - M$, the probabilities predicted by quantum mechanics are:

$$P(M_+, M_+|\phi_A, \phi_B) = P(M_-, M_-|\phi_A, \phi_B) = \frac{1}{16}\left[1 + \cos(\phi_A + \phi_B\right] \tag{4.2}$$

$$P(M_+, M_-|\phi_A, \phi_B) = P(M_-, M_+|\phi_A, \phi_B) = \frac{1}{16}\left[1 - \cos(\phi_A + \phi_B\right] \tag{4.3}$$

In the others cases, we have

$$P(M_\pm, E_\pm|\phi_A, \phi_B) = P(E_\pm, M_\pm|\phi_A, \phi_B) = \frac{1}{32} \tag{4.4}$$

$$P(M_\pm, L_\pm|\phi_A, \phi_B) = P(L_\pm, M_\pm|\phi_A, \phi_B) = \frac{1}{32} \tag{4.5}$$

$$P(E_\pm, E_\pm|\phi_A, \phi_B) = P(L_\pm, L_\pm|\phi_A, \phi_B) = \frac{1}{32} \tag{4.6}$$

$$P(E_\pm, L_\pm|\phi_A, \phi_B) = P(L_\pm, E_\pm|\phi_A, \phi_B) = 0 \tag{4.7}$$

As a check, the above probabilities, if one consider every possible events, sum to 1:

$$\begin{aligned} p &= 4p_{MM} + 4p_{ME} + 4p_{EM} + 4p_{ML} + 4p_{LM} + 4p_{EE} + 4p_{LL} + 4p_{EL} + 4p_{LE} \\ &= 4\frac{1}{16} + 4\frac{1}{32} + 4\frac{1}{32} + 4\frac{1}{32} + 4\frac{1}{32} + 4\frac{1}{32} + 4\frac{1}{32} + 0 + 0 = 1 \end{aligned}$$

A local hidden variable (LHV) model can explain such correlation in the following way. Consider $\lambda = (\theta, r)$, with θ uniformly distributed between 0 and 2π, and r uniformly distributed between 0 and 1. The outcomes $A(\lambda; \phi_A)$ and $B(\lambda; \phi_B)$ are determined by fig. 4.1

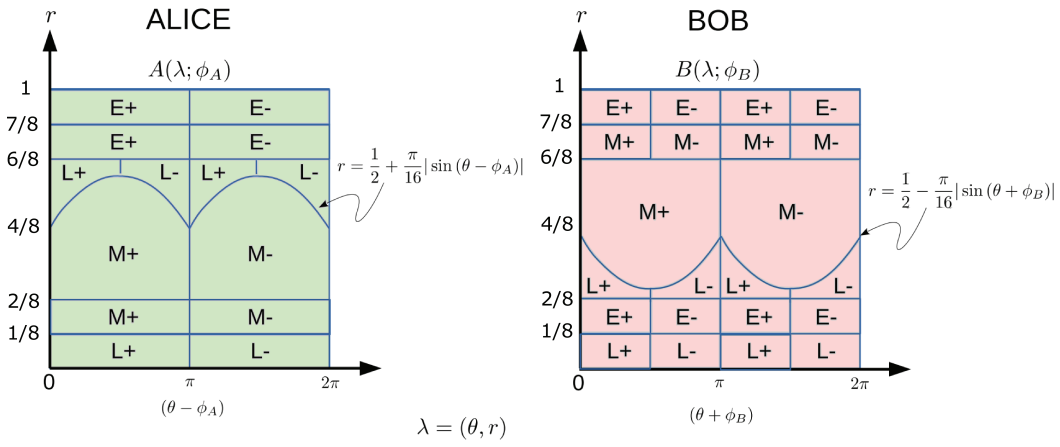


Figure 4.1: LHV model for time-bin experiment.

Given a fixed value (θ, r), the LHV establishes deterministically the outcomes of Alice and Bob in function of ϕ_A and ϕ_B by the functions $A(\lambda; \phi_A)$ and $B(\lambda; \phi_B)$. This model is local, because the outcomes of Alice don't depend on ϕ_B and the outcomes of Bob don't depend on ϕ_A. This model can predict all the outcomes $M_\pm M_\pm$, $E_\pm E_\pm$, $L_\pm L_\pm$, $E_\pm M_\pm$, $M_\pm M_\pm$, $M_\pm L_\pm$, $L_\pm M_\pm$, $E_\pm L_\pm$, $L_\pm E_\pm$.

The probabilities is:

$$P(a, b|\phi_A, \phi_B)_{LHV} = \frac{1}{2\pi} \int_0^{2\pi} \mathrm{d}\theta \int_0^1 \mathrm{d}r \left[A(\theta, r; \phi_A) B(\theta, r; \phi_B)\right]. \tag{4.8}$$

The product $[A(\theta, r; \phi_A) B(\theta, r; \phi_B)]$, is the overlap of the sub-regions of Alice and Bob, that are obtained from fig. 4.1 by considering only the sub-region where $a = \{E_\pm, M_\pm, L_\pm\}$ for Alice, and $b = \{E_\pm, M_\pm, L_\pm\}$ for Bob. In fig. 4.2, it is possible to see a graphical representation of the meaning of integral 4.8.

4.1.2 Theory

A solution to LHV model, is that one has to random fast switching the phase settings and reject pairs of events whose times difference are greater than $L - S$. In this case, the Bell inequality holds for the long-long (LL) events, while a trivial bound is obtained for the short-short (SS) events [86]. Even though this, standard Bell inequalities are insufficient. However, if chained Bell inequalities are used, a non-trivial bound can be obtained. In fact, chaining Bell inequalities allow a stronger quantum violation and make more onerous the requirements of local realism.

We now give more details to explain the above reasoning. The standard Bell inequality for a two separated state systems, as the Clauser-Horne-Shimony-Holt (CHSH), deals with four measurable

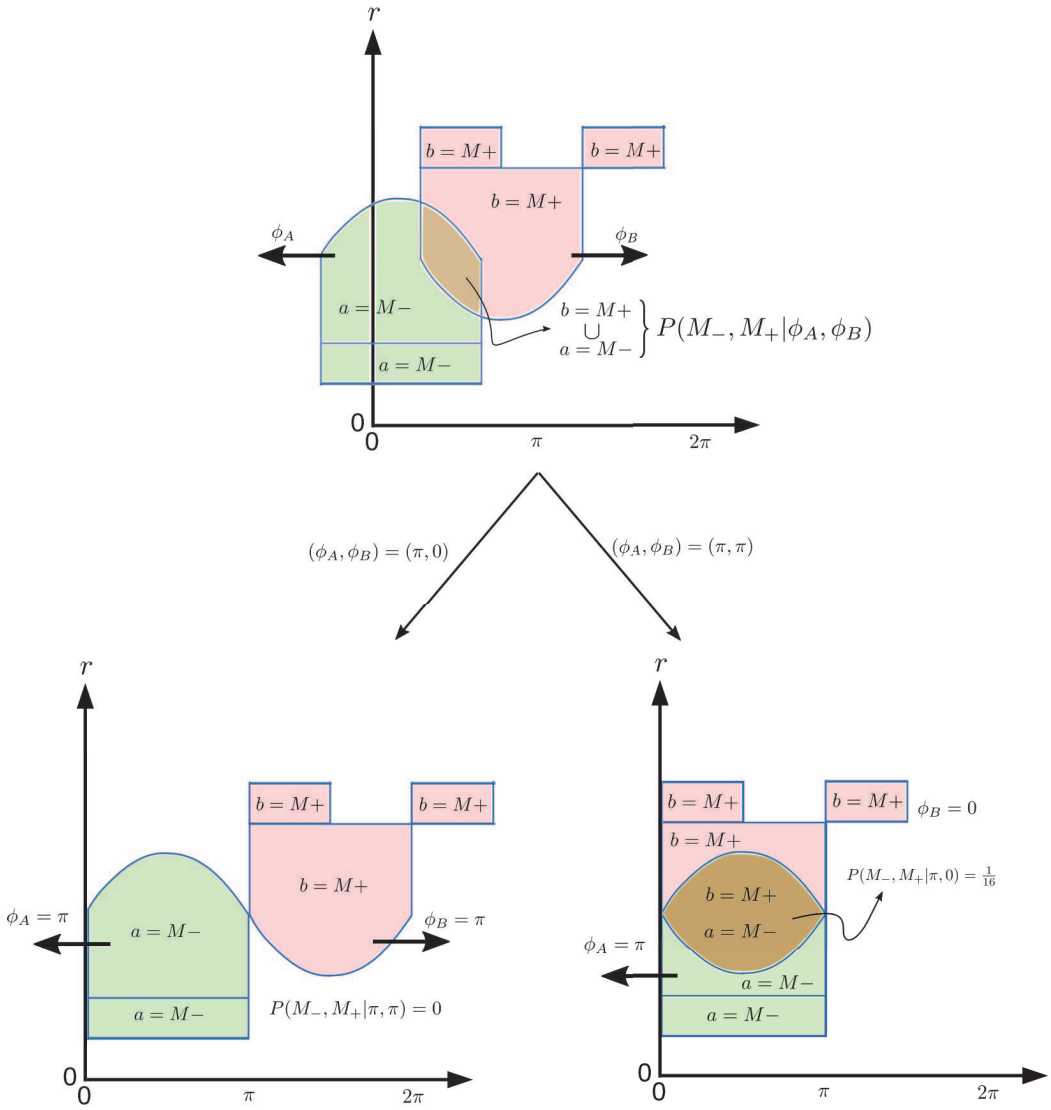


Figure 4.2: In this example, the green and red regions give the values for the hidden variable for which $a = M_-$ and $b = M_+$ hold. The brown area, where the regions overlapped, corresponds to the hidden variables for which both $a = M_-$ and $b = M_+$ hold. The value of this area is equal to the integral 4.8.

quantities:

$$S_{\text{CHSH}} = \langle A_1 B_1 \rangle - \langle A_2 B_2 \rangle + \langle A_2 B_1 \rangle + \langle A_1 B_2 \rangle \tag{4.9}$$

where the terms $\langle A_i B_j \rangle$ are the quantum correlations of particles pairs. If local realism holds[86] in time-bin entanglement experiment, the outcomes obey to

$$S_{re} \leq 3 \tag{4.10}$$

that is higher than the value predicted by quantum mechanics, $S_{qm} = 2\sqrt{2}$.

An useful bound can be obtained if we consider N measurements for each observer. In this case a chained Bell inequality with $2N$ terms can be derived. The Bell parameter is given by

$$S^N = \langle A_N B_N \rangle + \sum_{k=2}^{N} [\langle A_k B_{k-1} \rangle + \langle A_{k-1} B_k \rangle] - \langle A_1 B_1 \rangle \tag{4.11}$$

If A_i and B_j are phase measurement operators, the set of phases that maximize the inequality consist in consecutive measurements separated by an angle of $\theta = \pi/(2N)$. The quantum prediction in this case is

$$S^N_{\mathrm{QM}} = 2N \cos(\frac{\pi}{2N}) \tag{4.12}$$

with a classical bound of $2N - 2$. However, when time-bin is exploited, the realism bound is larger[86] and it is equal to

$$S^N_{\mathrm{LHV}} = 2N - 1 \tag{4.13}$$

and the violation $S^N_{\mathrm{QM}} > S^N_{\mathrm{LHV}}$ can occur for $2N \geq 6$. The above bound is due to the fact that the SS events can be influenced by the phase settings (while the LL sub-ensamble is independent of the phase setting) if the phase switching is performed at a timescale $\Delta\mathcal{L}/c$[84].

To obtain such violation, an high visibility is needed, $V \geq S_{\mathrm{LHV}}/S^N_{\mathrm{QM}}$, anyway greater than 94.63%, a very demanding task for such type of experiment.

4.2 CH CHAINED INEQUALITY

In a typical CHSH experiment, coincidences are simultaneous recorded with four detectors to calculate each terms $\langle A_i B_j \rangle$. For each value of A_i and B_j, the numbers of coincidences are labeled as $N_{++}, N_{+-}, N_{-+}, N_{--}$, where $+$ means that Alice or Bob measures $+1$ and $-$ a measure of -1. The corresponding expectation value is calculated as:

$$\langle A_i B_j \rangle = \frac{N_{++} - N_{+-} - N_{-+} + N_{--}}{N_{++} + N_{+-} + N_{-+} + N_{--}} \tag{4.14}$$

In our experiment we use only two detectors, and the inequality can be written in the CH-Hardy[89] form involving only probabilities. Now we will see how to derive it. The standard CH inequality[87], which correspond to standard Bell inequality, if we assume fair sampling can be rewrite in this form[88]:

$$S_{CH} = p(a_2 b_2) + p(a_1 b_2) + p(a_2 b_1) - p(a_1 b_1) - p(a_2) - p(b_2) \tag{4.15}$$

The CH-Hardy form of the chained Bell inequality is

$$1 - N \leq S_{\mathrm{CH}}^{N} \leq 0 \tag{4.16}$$

where the Bell parameter is given by

$$S_{\mathrm{CH}}^{N} = p(a_N b_N) + \sum_{k=2}^{N} [p(a_k b_{k-1}) + p(a_{k-1} b_k)] - p(a_1 b_1) - \sum_{k=2}^{N} [p(a_k) + p(b_k)] \tag{4.17}$$

The term $p(a_i b_j)$ corresponds to the joint probability of measuring $+1$ on Alice and Bob side respectively.

The single side probabilities $p(a_k)$ and $p(b_k)$, when we assume fair sampling, can be expressed as

$$p(a_k) = p(a_k b_{k-1}) + p(a_k \bar{b}_{k-1}) \tag{4.18}$$

and

$$p(b_k) = p(a_{k-1} b_k) + p(\bar{a}_{k-1} b_k) \tag{4.19}$$

where $\bar{a}_j$ means the -1 outcome. If we replace the terms $p(a_k)$ and $p(b_k)$ in eq.4.17 with 4.18 and 4.19 we can write

$$S^N_{\mathrm{CH},1} = p(a_N b_N) - \sum_{k=2}^{N} [p(a_k \bar{b}_{k-1}) + p(\bar{a}_{k-1} b_k)] - p(a_1 b_1) \tag{4.20}$$

The difference from 4.11 is that, for example, $p(a_i b_j)$ and $p(\bar{a}_i b_j)$ are calculated with two different measurements (to measure $\bar{a}_i$ we need to move the apparatus to obtain the orthogonal state of a_i), instead $\langle A_i B_j \rangle$ is calculated with only one measurement. We note that the inequality holds also when a_k or b_k are replaced by $\bar{a}_k$ and $\bar{b}_k$, because we can arbitrarily define the measurement outcomes with the $+1$ and -1 inverted. From this observation we obtain three others Bell parameters given by

$$S^N_{\mathrm{CH},2} = p(\bar{a}_N \bar{b}_N) - \sum_{k=2}^{N} [p(\bar{a}_k b_{k-1}) + p(a_{k-1} \bar{b}_k)] - p(\bar{a}_1 \bar{b}_1) \tag{4.21}$$

$$S^N_{\mathrm{CH},3} = p(a_N \bar{b}_N) - \sum_{k=2}^{N} [p(a_k b_{k-1}) + p(\bar{a}_{k-1} \bar{b}_k)] - p(a_1 \bar{b}_1) \tag{4.22}$$

$$S^N_{\mathrm{CH},4} = p(\bar{a}_N b_N) - \sum_{k=2}^{N} [p(\bar{a}_k b_{k-1}) + p(a_{k-1} b_k)] - p(\bar{a}_1 b_1) \tag{4.23}$$

By combining the above equation, we can derive the inequality in the CHSH-form

$$\begin{aligned} S^N_{\mathrm{CHSH}} =& S^N_{\mathrm{CH},1} + S^N_{\mathrm{CH},2} - S^N_{\mathrm{CH},3} - S^N_{\mathrm{CH},4} \\ =& \langle A_N B_N \rangle - \sum_{k=2}^{N} [\langle A_k B_{k-1} \rangle + \langle A_{k-1} B_k \rangle - \langle A_1 B_1 \rangle] \end{aligned} \tag{4.24}$$

with

$$|S^N_{\mathrm{CHSH}}| \leq 2N - 2. \tag{4.25}$$

The correlations in 4.24 are defined as

$$\begin{aligned} \langle A_k B_j \rangle &= p(a_k b_j) + p(\bar{a}_k \bar{b}_j) - p(\bar{a}_k b_j) - p(a_k \bar{b}_j) \\ &= 4p(a_k b_j) - 2p(a_k) - 2p(b_j) + 1 \end{aligned} \tag{4.26}$$

The inequality 4.25 cannot be applied to time-bin entanglement due to the post-selection of events (see eq.4.13). Indeed we must distinguish between the short-short (SS) and the long-long (LL) events: the inequality 4.16 holds only for the LL events, while for the SS events we may only derive a trivial bound for CHSH* given by

$$|S^N_{\mathrm{CHSH,SS}}| \leq 2N \tag{4.27}$$

corresponding to the bound in the CH-form†:

$$\frac{1}{2} - N \leq S^N_{\mathrm{CH,SS}} \leq \frac{1}{2} \tag{4.28}$$

The bound is trivial since $S^N_{\mathrm{CHSH,SS}}$ contains $2N$ terms and each of them is bounded from -1 to $+1$.

*due to the fact that the SS events can be influenced by the phase settings, while the LL sub-ensamble is independent of the phase setting[84]

†note that $S^N_{CHSH} = 4S^N_{CH} + 2(N-1)$

Since SS and LL events equally contribute to the coincidences, the Bell parameter is given by the average of the SS and LL Bell parameters, namely $\widetilde{S}^N = \frac{1}{2}S^N_{\rm SS} + \frac{1}{2}S^N_{\rm LL}$. Then the correct inequalities for time-bin encoding are written as

$$|\tilde{S}^N_{\rm CHSH}| \leq 2N - 1 \tag{4.29}$$

and

$$\frac{3}{4} - N \leq \tilde{S}^N_{\rm CH} \leq \frac{1}{4} \tag{4.30}$$

We note that since $S_{\rm CH}$ involves only joint-probabilities and not correlations, the inequality is valid when we use one detector at each side to measure the probabilities $p(a_i b_j)$. Since we have demonstrated that the CHSH form can be derived from the CH form, it implies that also the CHSH inequality holds when one detector at each side is used.

The bound 4.30 is violated by the quantum prediction

$$S^N_{ch,{\rm QM}} = \frac{1}{2} - N \sin^2 \frac{\pi}{4N} \tag{4.31}$$

when $N \geq 3$

4.3 Experimental setup

In order to obtain high visibility, a very stable and precise measurement setup is needed. Experimental setup is similar to the one used for hyper-entangled state generation. The laser source used is a pulsed laser at 808nm, 76MHz repetition rate and $\sim 150 fs$ pulse width coming from a Ti:Sa mode-locked oscillator, with an average power of 2W. The Ti:Sa oscillator beam is used to pump a SHG crystal, which generates pulses at 404nm. The light at 404nm passes through the pump interferometer, where the light are split in two temporal modes and finally pumps a SPDC crystal. The photons produced

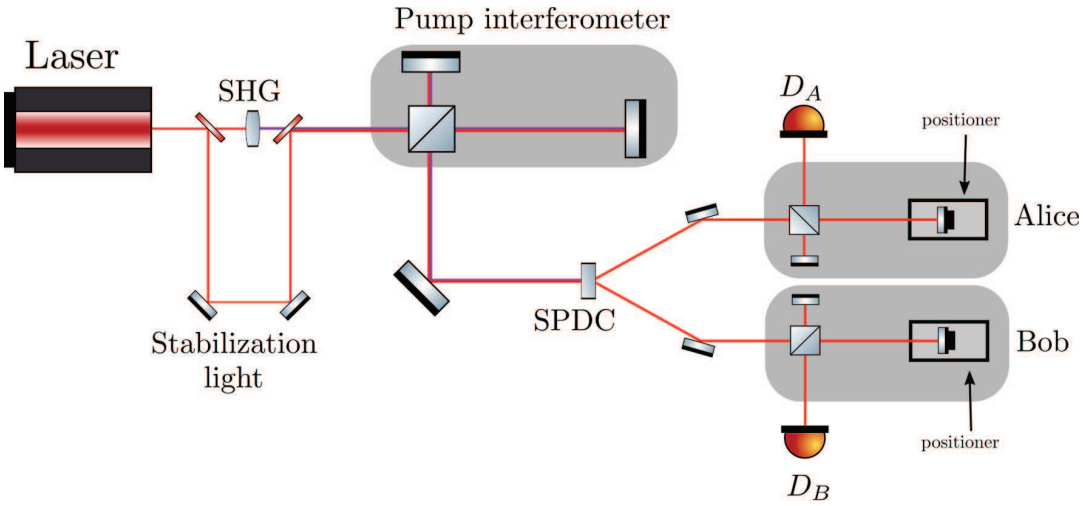


Figure 4.3: Setup of the time-bin entanglement source. Realized with ComponentLibrary[2].

at 808nm are injected in two free-space unbalanced Michelson interferometers, called Alice and Bob interferometer, whose unbalancement is identical to the pump interferometer. The mirrors on the long paths of these two interferometers, unlike the first, are mounted on a piezoelectric translator, that are used to stabilize and change the phase of the interferometers. Finally, the photons are coupled into single mode fiber and directed toward two SPADs. For time acquisition we use a TDC with $81ps$ resolution.

The generated state correspond to

$$|\Psi_e\rangle = \frac{1}{\sqrt{2}} \left(|S_A S_B\rangle - |L_A L_B\rangle \right). \tag{4.32}$$

Maintain a constant phase difference between the two events $|S_A S_B\rangle$ and $|L_A L_B\rangle$ is a crucial task in order to obtain a great visibility on the generated state. To achieve a fixed phase difference, Alice and Bob phases are actively stabilized to the pump phase. This stabilization used a small part of the original oscillator beam, which we call stabilization light. This light is injected in the pump interferometer after an appropriate delay, in order to prevent a detection overlap between the SPDC photons.

The outgoing light is split in two beams, and then, each of them follows the same path of the two SPDC photons. In this way, the second order interference generated through the pump and the Alice (Bob) interferometer can be used to stabilize and compensate the phase. Since the interference pattern depends on the received photons, Alice and Bob interferometers can be stabilized at the same time and independently. A piezoelectric positioner is used to change the phase in each interferometer. During a measurement, the stabilization process is continuously alternate between measurement periods of 3 $sec.$ The stabilization period depends on the number of single events, but, in general, is in the order of 1 $sec.$ In this way it is possible to stabilize not only the phase mismatch introduced in the paths, but also the phase mismatch due to the pump laser. Indeed, the wavelength of the laser pump changes during the experiment due to room temperature variation. These imply a phase state change that affects the visibility of the state. The algorithm can compensate this variation during all the experiment, allowing a good state visibility.

4.4 Stabilization

Now we see in detail how we have stabilized our interferometers[‡]. To prevent instability due to air flows we close the three interferometers inside boxes. In this way interferometers are insensitive to air flows and rumors.

Then, as we have just seen above, Alice and Bob's interferometers have been stabilized using a small part of the original oscillator beam, the stabilization light (see fig. 4.3 and fig. 4.4). The state of the stabilization light after the pump interferometer is $|\Psi_s\rangle = \frac{1}{\sqrt{2}}(|S_p\rangle + e^{i\phi_p}|L_p\rangle)$ where $\phi_p = 2\pi\Delta\lambda/\lambda_{red}$, $\lambda_{red} = 808nm$ and $\Delta\lambda = \text{mod}(|L_p - S_p|, \lambda_{red})$.

After the Alice's interferometer, the state becomes

$$|\Psi_s\rangle = \frac{1}{2}\Big[|S_pS_A\rangle + e^{i\phi_A}|S_pL_A\rangle + e^{i\phi_p}|L_pS_A\rangle + e^{i(\phi_p+\phi_A)}|L_pL_A\rangle\Big]$$

[‡]Is a different from the stabilization algorithm see in chapter 2.

Alice considers only the events corresponding to $|S_pL_A\rangle$ or $|L_pS_A\rangle$ events. By the indistinguishability between the $|L_pS_A\rangle$ or $|S_pL_A\rangle$ case, the measured count rate becomes

$$\mathcal{N}_A \propto \cos^2 \frac{(\phi_A - \phi_p)}{2}. \tag{4.33}$$

Depending on the phase of the Alice interferometer, interference can be constructive or destructive. The same is achieved in Bob interferometer:

$$\mathcal{N}_B \propto \cos^2 \frac{(\phi_B - \phi_p)}{2} \tag{4.34}$$

In this way, it is possible to stabilize, respect to the pump interferometer, the Alice and Bob interferometer at the same time and independently. A piezoelettric positioner is used to change the phase in each interferometer. This positioner has a resolution of a $1\,nm$ and it has a feedback sensor that permits to look the desired position. We set

$$\phi_A = \phi_p + \alpha\,, \qquad \phi_B = \phi_p + \beta\,. \tag{4.35}$$

We note that by this procedure, the entangled state is then stabilized, since the α and β phase can be interpreted as the measured phase. Indeed, the state of the pump photon after the pump interferometer is $|\Psi_e\rangle = |S_p\rangle + e^{i\phi_e}|L_p\rangle$ where $\phi_e = 2\pi\Delta\lambda/\lambda_{SHG} = 2\phi_p$, $\lambda_{SHG} = 404nm$.

Then, the state of the photon pair after the measurement interferometers is

$$\begin{aligned}|\Psi_e\rangle =&|S_pS_A, S_pS_B\rangle + e^{i\phi_A}|S_pL_A, S_pS_B\rangle + e^{i(\phi_A+\phi_B)}|S_pL_A, S_pL_B\rangle + e^{i\phi_B}|S_pS_A, S_pL_B\rangle \\ &+e^{i\phi_e}|L_pS_A, L_pS_B\rangle + e^{i(\phi_e+\phi_A)}|L_pL_A, L_pS_B\rangle \\ &+e^{i(\phi_e+\phi_A+\phi_B)}|L_pL_A, L_pL_B\rangle + e^{i(\phi_e+\phi_B)}|L_pS_A, L_pL_B\rangle \end{aligned} \tag{4.36}$$

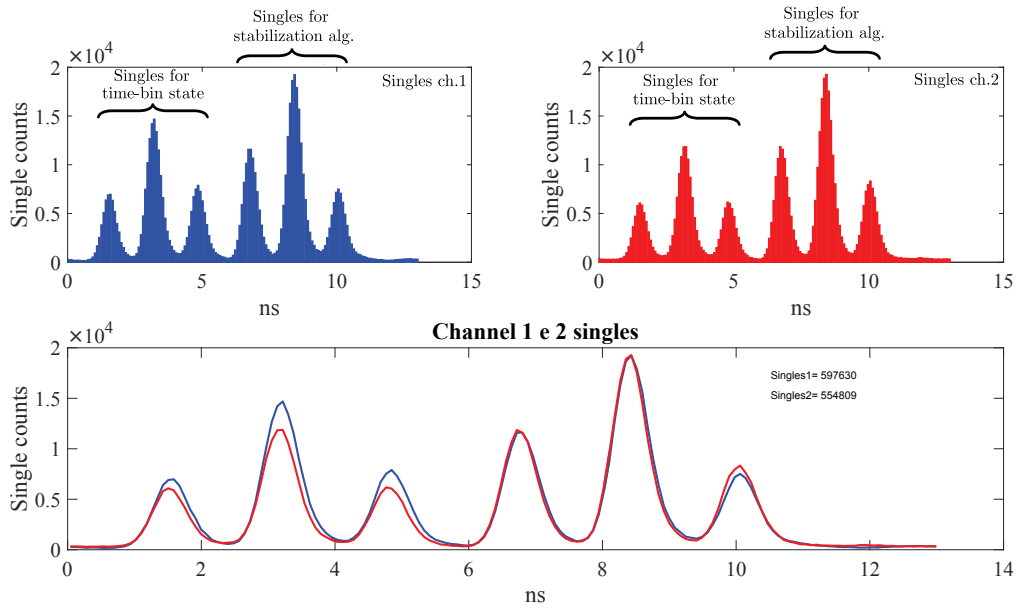


Figure 4.4: In this figure we can see the distribution of the singles. In each channel, the first three peaks refer to time-bin state. The other three peaks refer to singles used to stabilize the interferometers.

where $|i_p k_A, i_p j_B\rangle$ means that the pump photon take the $i \in \{S, L\}$ path, and k_A (j_B) that the Alice (Bob) photon take the $k \in \{S, L\}$ ($j \in \{S, L\}$) path. The two indistinguishable events $|S_p L_A, S_p L_B\rangle$ and $|L_p S_A, L_p S_B\rangle$ give rise to interference. The coincident corresponding to such events are then given by

$$\mathcal{C} \propto \cos^2 \frac{(\phi_A + \phi_B - \phi_e)}{2}$$

From the stabilizer beam we have set $\phi_A = \phi_p + \alpha$, and $\phi_B = \phi_p + \beta$. Since $\phi_p = \phi_e/2$ the offset cancels out and the coincidences varies $\mathcal{C} \propto \cos^2 \frac{(\alpha+\beta)}{2}$.

The stabilization algorithm work as follow (we show how works for Alice, for Bob is the same). We consider the three singles rate from the calibration light ($|S_p S_A\rangle$, is the first peak P_1, $|L_p S_A\rangle$ and $|S_p L_A\rangle$, are the central peak P_C and $|L_p L_A\rangle$ is the last peak P_2). The value of the central peak, P_C, depends on the phase values of the pump and Alice's interferometer ($\phi = \phi_A - \phi_p$, see eq.4.33). As

a consequence we can use the value of P_C as a reference for the phase, but this value can fluctuate due to pump laser instability. But if we consider the ratio

$$P_{ratio} = \frac{P_C}{P_1 + P_2}. \tag{4.37}$$

this is immune to laser fluctuation, because the numerator is proportional to the value of the denominator. Interference can be described by the function $I = I_1 + I_2 + 2g\sqrt{I_1 I_2}\cos\phi$, and if we consider $P_1 = I_1$ and $P_2 = I_2$, we can write

$$P_{ratio} = \frac{P_1 + P_2 + 2g\sqrt{P_1 P_2}\cos\phi}{P_1 + P_2} = 1 + C\cos\phi. \tag{4.38}$$

From the above equation we see the relation between P_{ratio} and the phase ϕ. To stabilize the phase

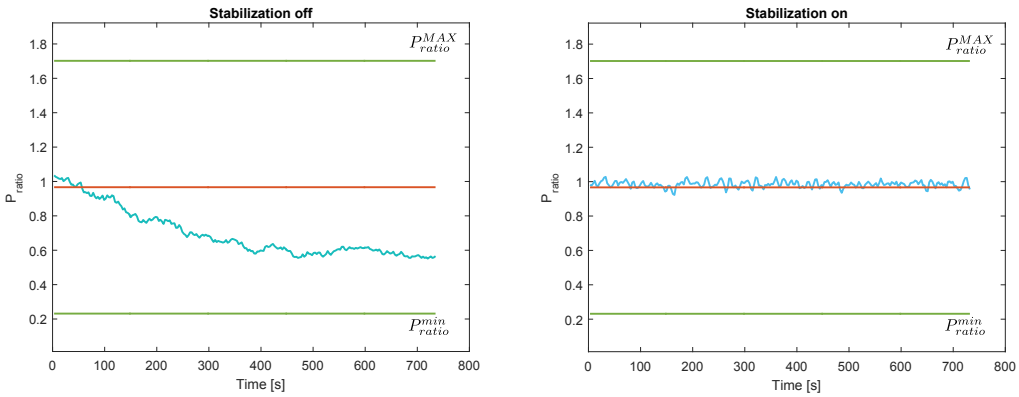


Figure 4.5: In this figure we can see the effect of the stabilization algorithm. When the stabilization is off, the phase drift is very slow. This is due to the positioner that is very stable, thanks to a very precise feedback control. In addition, the interferomenter is protected from air flow with a box. When we stabilize the interferometer with our methods, we achieve a stability for a long time. The value of P_{ratio} is bounded because the visibility on the singles detection are not maximized, due to a alignment difficulties.

we move the positioner in order to keep the position near $P_{ratio} = 1$. In this point we get the maximal sensibility, because in this point the derivative of the function is maximal. When we perform

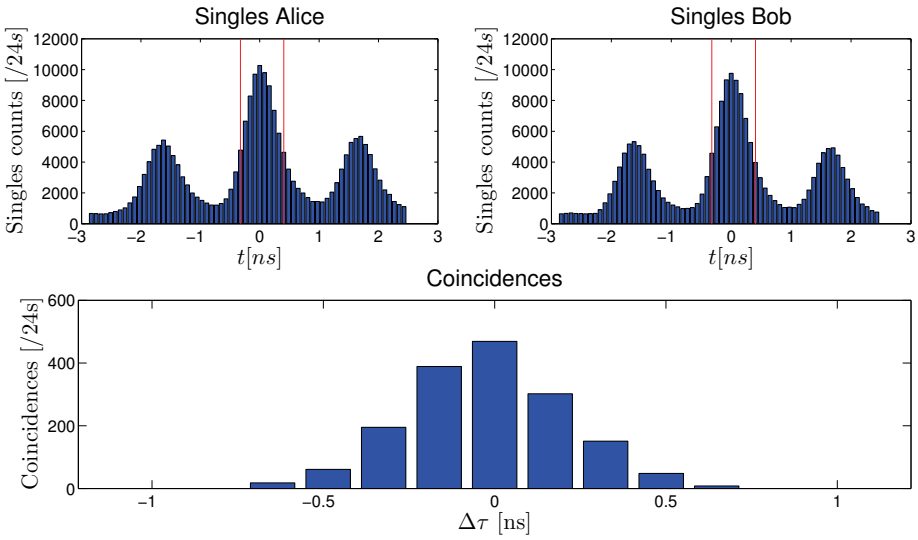


Figure 4.6: Time distribution of singles and coincidences counts. The red bar on singles graph represents the time interval within an event is suitable for coincidence. The coincidences graph represent the coincidences between single events within the red bars, in a window of $0.81\ ns$.

a measurement, for instance when we want to measure α, we know the relation between P_{ratio} and ϕ, and from eq.4.35 we obtain $\phi = \phi_A - \phi_p = \alpha + \phi_p - \phi_p = \alpha$. We also know the relation between a shift ΔL nm of the positioner and the interferometer phase (see eq.2.20), and we can write $\alpha = 2\pi \cdot 2\Delta L/\lambda$. This means that, when we want to measure the phase α, first we stabilize the interferometer by looking the position where $P_{ratio} = 1$, and then move the positioner by ΔL nm. This operation is periodic, since every $3\ sec$ we return to stabilize the interferometer by looking $P_{ratio} = 1$. The stabilization procedure is very fast, generally less than a second, thanks to the fact that single counts have high count rates (we get precise statistics with few measurement).

4.5 Result

In figure Fig.4.6 we show the distribution of the single counts registered on Alice and Bob detectors and the coincidences between them. Thanks to the pulsed pump, it is possible to predict the detection

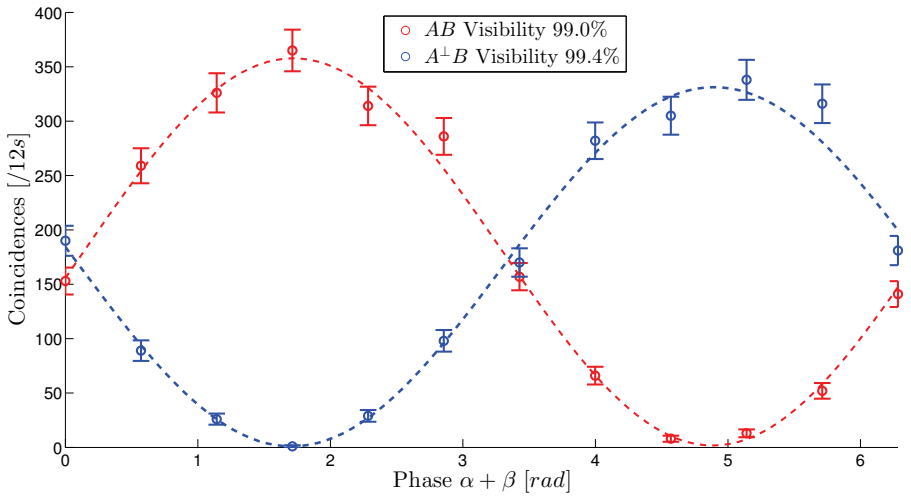


Figure 4.7: Raw coincidence counts between detectors A and B for different values of phases (red data). The blue data represent the coincidence counts between the orthogonal output of detector A, which is obtained by shifting the phase of A by π, and B.

time of every generated photon. As expected the single counts distribute among three different peaks. The temporal window for a "good detection" is indicated by the red bars on the singles graphs. Such temporal window is determined a-priori, by knowing the emission time of the pump beam and using this information as a time-reference. Indeed, the horizontal axis in the upper figure represent the arrival time of the Alice (or Bob) photon with respect the reference time (we set $t = 0$ for the detection corresponding to $|L_A L_B\rangle$ and $|S_A S_B\rangle$ events). The window for "good detection" correspond to the value of t such that $-0.405ns \leq t \leq 0.405ns$ (corresponding to ± 5 bins of our TDC converter). The coincidences are determined by the events on Alice site that are in the same temporal window with an event on Bob site. In Fig.4.6 we show the distribution of the coincidences in function of the time difference $\Delta\tau$ between Alice and Bob events. Note, that, by the definition of coincidence, $|\Delta\tau|$ is lower that the detection window, namely $|\Delta\tau| \leq 0.810ns$.

Thanks to the stabilization algorithm we can achieve a good visibility (see Fig.4.7), up to 99%, obtained by measuring the coincidences in function of the phase $\alpha + \beta$. By the high visibility of

our setup we can obtain a Bell violation of the chained inequalities over the bound imposed by local realism.

We used 3 sets of measurements, composed by 6, 8 and 10 measurements respectively, which correspond to $N = 3, 4, 5$. In the case of 6 measurements, choosing $\theta = \pi/6$ yield the quantum prediction $S^3_{\text{CHSH}} = 5.163$. For 8 measurements, choosing $\theta = \pi/8$ yield the quantum prediction $S^4_{\text{CHSH}} = 7.169$ and finally, for 10 measurements, with $\theta = \pi/10$ the bound become $S^5_{\text{CHSH}} = 9.271$. From the three sets of measurements we obtain the result shown in table 4.1 for $N = 3$, in table 4.2 for $N = 4$, in table 4.3 for $N = 5$. In each table we report the values of every single CH parameter $S^N_{CH,i}$ (see 4.20 to 4.23) and the value of S^N_{CHSH}. As we can see the total violation of S^N_{CHSH} is greater than the singles violation of $S^N_{CH,i}$. This can be explain by the fact that S^N_{CHSH} is the sum of quantities that are repetitively violate. To experimentally calculate the probability values of eq.4.20

$$p(a,b) = \frac{C(a,b)}{C(a,b) + C(\bar{a},b) + C(a,\bar{b}) + C(\bar{a},\bar{b})} \tag{4.39}$$

where $C(a,b)$ is the coincidence obtained for the measurement set a and b. Errors are calculate with error propagation.

i	$S^3_{LHV,i}$	$S^3_{CH,i}$	err_S	Violation
1	0.25	0.289	0.011	3.40σ
2	-2.25	-2.335	0.020	4.15σ
3	-2.25	-2.247	0.020	-0.17σ
4	0.25	0.293	0.012	3.66σ
S^3_{CHSH}	5	5.163	0.033	4.91σ

Table 4.1: Results for the set of measurements, with N= 3. $S^3_{LHV,i}$ correspond to the value predicted by a local hidden variable model. The reported $S^3_{CH,i}$ has been calculated from the raw coincidence.

i	$S^4_{LHV,i}$	$S^4_{CH,i}$	err_S	Violation
1	0.25	0.282	0.011	3.06σ
2	-3.25	-3.299	0.022	2.28σ
3	-3.25	-3.284	0.022	1.59σ
4	0.25	0.302	0.011	4.94σ
S^4_{CHSH}	7	7.169	0.034	4.93σ

Table 4.2: Results for the set of measurements, with N=4. $S^4_{LHV,i}$ correspond to the value predicted by a local hidden variable model. The reported $S^4_{CH,i}$ has been calculated from the raw coincidence.

i	$S^5_{LHV,i}$	$S^5_{CH,i}$	err_S	Violation
1	0.25	0.307	0.009	6.76σ
2	-4.25	-4.304	0.022	2.64σ
3	-4.25	-4.331	0.021	4.01σ
4	0.25	0.327	0.009	8.89σ
S^5_{CHSH}	9	9.271	0.031	8.67σ

Table 4.3: Results for the set of measurements, with N= 5. $S^5_{LHV,i}$ correspond to the value predicted by a local hidden variable model. The reported $S^5_{CH,i}$ has been calculated from the raw coincidence.

4.6 Future implementation

In this section we introduce a further implementation of time-bin entangled source to completely avoid the post-selection loophole. This is possible if one builds an interferometer as described in fig.4.8. The balanced Mach-Zender interferometer works as a router for the input pulses, and the phase α introduced by the phase modulator, is synchronized with the pump pulse laser. The value of α is switched between two values, 0 and π, between the two photon pulses, in a time less than ΔT. The relation between input and output of the MZI can be described as follow.

Consider an initial photon input state

$$|\Psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{4.40}$$

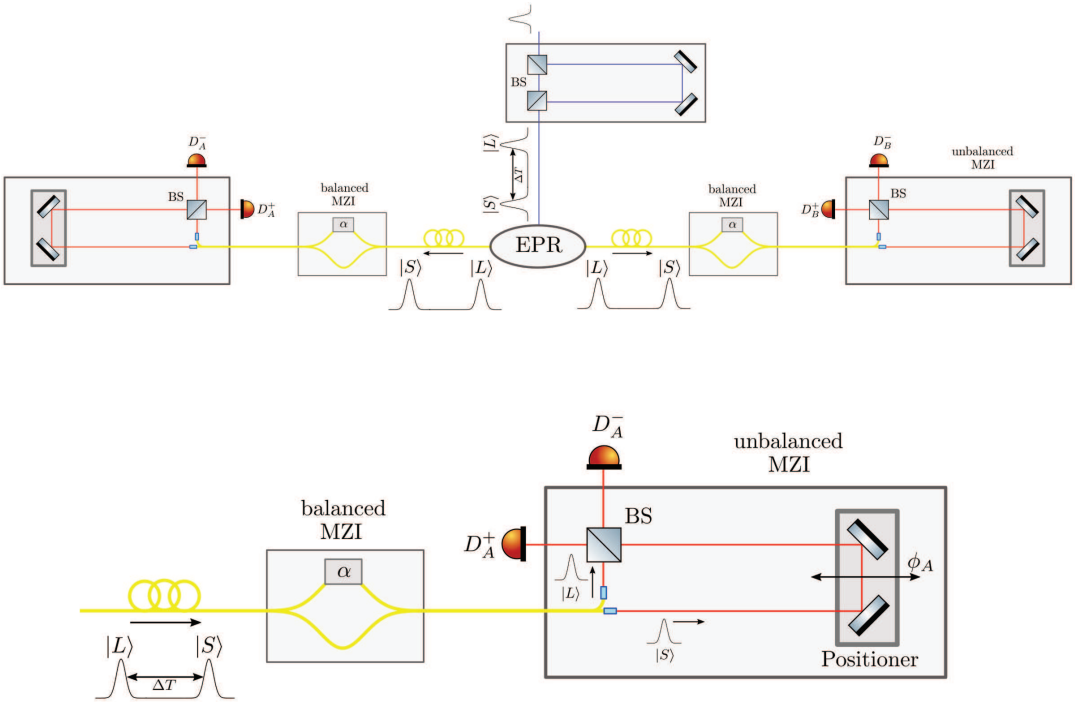


Figure 4.8: Time-bin setup to avoid LHV model. Realized with ComponentLibrary[2].

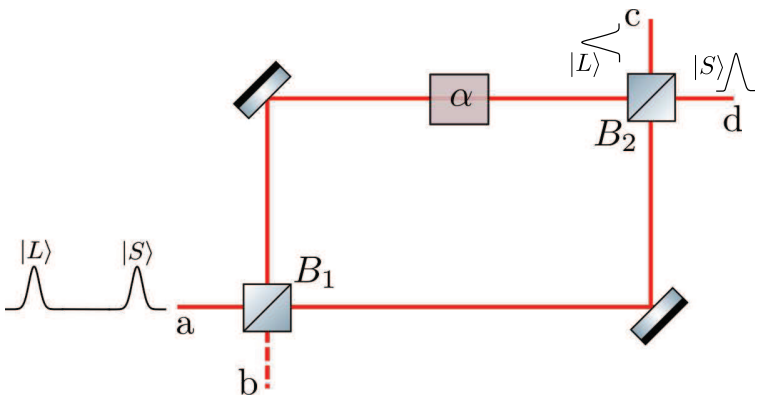


Figure 4.9: Router for photon pulses. Realized with ComponentLibrary[2].

where the photon is in the mode a. Beam splitter and phase modulator are described by

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \qquad P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \tag{4.41}$$

The output state of the MZI in fig. 4.9 is described by

$$|\Psi_{out}\rangle = B_2 P B_1 |\Psi\rangle = \frac{1}{2}\begin{pmatrix} 1 - e^{i\alpha} \\ i + ie^{i\alpha} \end{pmatrix} \tag{4.42}$$

Density matrix of the output state is

$$\rho_{out} = |\Psi_{out}\rangle\langle\Psi_{out}| = \frac{1}{\sqrt{4}}\begin{pmatrix} |1 - e^{i\alpha}|^2 & i(e^{i\alpha} - e^{-i\alpha}) \\ i(e^{i\alpha} - e^{-i\alpha}) & |1 + e^{i\alpha}|^2 \end{pmatrix} \tag{4.43}$$

where the diagonal elements represent the probability that the photon will be measured in the output ports. When $\alpha = \pi$ the photon exits on port c, but when $\alpha = 0$ the photon exits on port d. If we switch the value of α between the two pulses, we are able to send one pulse to an output, and the second to the other output. In this way we are able to route the $|S\rangle$ down-converted photon to the long arm of the unbalanced MZI, and the $|L\rangle$ photon to the short arm. At the output all the photons are detected at the same time , t_0, for both Alice and Bob, and the experiment becomes equivalent to a standard CHSH inequality.

To switch the phase of the balanced MZI we use a fiber phase modulator, with a bandwidth of $10GHz$ (the frequency of the laser pulses is $76MHz$). The switching signal comes from a photodiode that detects all the pump pulses. A custom electrical circuit was made to fit the specifics of the modulator input signal. In order to maintain a perfect separation on the output ports, the switching phase of the balanced MZI has to be stabilized. For that, we implement a PID algorithm, based on the observation of the single photons arrivals. In fact, if the balanced MZI works correctly, the single photons at the output of the unbalanced MZI are distributed in a single peak. Otherwise, if the phase inside the balanced MZI is not set correctly, the singles are distributed over three peaks. The PID algorithm tries to stabilized the phase by looking the position where the ratio between the two lateral

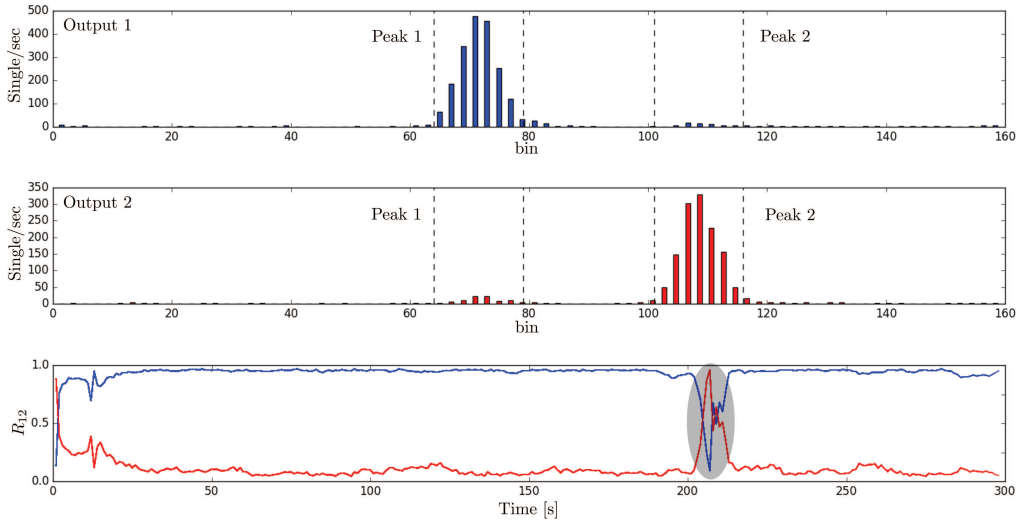


Figure 4.10: Output 1(2) shows the distribution of the singles between two laser pulses on the first(second) output port of the balanced MZI (fig.4.8, 1 $bin = 81\,ps$. The bottom plot, shows how the ratio between the two peaks, $R_{12} = Peak_1/(Peak_1 + Peak_2)$. At 200 s the stabilization of the interferometer was lost by the PID, but after some seconds, it got back to properly work.

peaks and the central peak is minimum. However, it is not possible to look the minimum position, due to the fact that this point is unstable (the PID algorithm, once it reaches the minimum position, doesn't know the direction where to move to stabilize a future drift). In our algorithm, the PID look for a position that is a bit greater of the minimum. Preliminary test on output visibility of the balanced MZI shows that with this approach, it is possible to stabilize the interferometer for a sufficiently long time to acquire measurement data.

In fig. 4.10 we can see how the stabilization algorithm perform on the output of the balanced MZI.

4.7 Conclusion

In this chapter we show that it is possible to reach an high visibility in a time-bin entanglement in order to violate a chained Bell inequality. By using $2N \geq 6$ settings at each measurement station, no local

hidden variable model can reproduce the predictions of a quantum experiments. The postselection loophole, which is present in the case $2N = 4$ (the standard CHSH-Bell inequality), is therefore avoided with the generalized, chained, Bell inequality with $2N \geq 6$.

Note that in order to fully violate the chained Bell inequality, fast switching must be used so that the phase settings at the measurement stations are randomly chosen at least every $\Delta L/c$. This has not been performed by the current experiment, but could be done by using a fast phase modulator, synchronized with the pulse laser, to change the phase within the interferometers. If $2N \geq 3$ is combined with fast switching, all requirements set out by Aerts [84] are fulfilled. In this experiment, we don't consider the space-time separation between the stations for a proper violation of local-realism.

Generally, chained Bell inequalities demand a high experimental visibility ($\geq 94.63\%$). Our experiment fulfills this condition with a visibility of 99% and shows that, despite the difficulties, it is therefore experimentally possible to implement chained Bell inequalities. This opens the door for applications such as device-independent quantum key distribution based on time-bin entanglement without the weaknesses inherent in the original Franson system.

5

Interference from satellite

The aim of quantum networks is to provide transportation of quantum information between physically separate users. Nowadays, implemented quantum networks use telecommunication fibers to connect nodes within the network[120,121,122,123]. The advantages of such systems are that they use the existing fiber links used for classical communication, and that the same fiber can be used to both quantum and classical signal[90,91]. These kind of realizations, however, suffer from optical attenuation due to fiber losses. Intercity quantum networks are already implemented in Tokyo, China and Switzerland. But, to expand a quantum network, over city distances, it is required the connection of them by quantum repeaters, a very demanding engineering solution. An alternative way, is the use of satellite quantum networks. In this years the interest in such field constantly increases, as confirmed by the numerous

article in theoretical [92,93,94] and practical applications [96,95]. Quantum communications along satellite links allow for the realization of quantum protocols over worldwide distances and fundamental test of quantum physics. After the demonstration of the feasibility of satellite-ground link with photons encoded in polarization DOF [97,100], we demonstrate that also temporal encoding can be used in such link, by showing that the temporal DOF is preserved in satellite-ground link [101].

5.1 Description of the experiment

This experiment has been realized at Matera Laser Ranging Observatory (MLRO). This observatory is included in the global satellite laser ranging network, and measures the time of flight of ultrashort light pulses retroreflected by satellite in order to study with high precision satellite orbits, components and temporal variations of Earth gravity field, geocentric positions and motions of ground stations and other. MLRO provides an high energy pulsed laser, which is used to generate pulses of light that are sent to satellites through an high-speed telescope, of 1.5 m diameter, able to precise point and track the satellite. When the light beam hits the orbiting satellite, it is perfectly reflected back by corner cubes* installed on the satellite. Then, the beam light, attenuated by the atmosphere, goes back to the telescope and a detector receives it. The master laser at MLRO is a mode-locking laser that generates a pulse train at a frequency equal to 100 MHz (all the reference times of the system are synchronized with a MASER atomic clock), with a wavelength $\lambda_M = 1064$nm. This pulse train is then amplified in order to obtain a pulsed laser with a repetition rate of 10Hz, a wavelength of $\lambda_L = 532$nm, and an energy of 100mJ per pulse. All the optics for transmit and receive the pulses are optimized at 532 nm. Our system works together with this system, and we use the master laser to generate by a SHG crystal, a pulse train at $\lambda_L = 532$nm, with a frequency of 100 MHz and a energy per pulse equals to 1.1 nJ.

This pulse train is used to generate coherent state $|\Psi_{out}\rangle$ by an unbalanced Mach-Zehnder interfer-

*Corner cube can reflect back an incident beam onto itself, regardless of its orientation

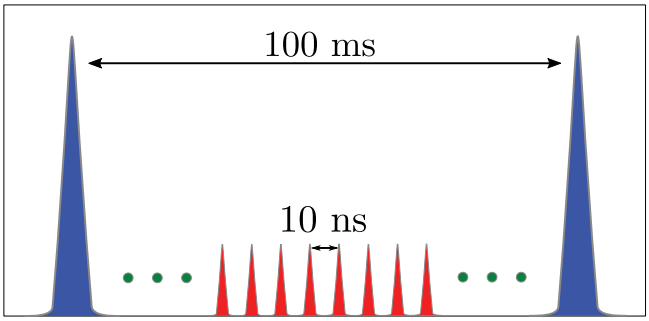


Figure 5.1: Distribution of pulse train at MLRO. Blu pulses are the high-energy pulses for laser ranging measurements, the red pulses are the ones used to generate qubits.

ometer (MZI). The difference between the two arms is of $\Delta L = c\Delta t \simeq 1$ m, with c the speed of light in vacuum and $\Delta t \simeq 3.4$ ns the delay between the two temporal modes outgoing the interferometer. The coherence time of the laser $\tau_c \approx 83$ ps is much shorter than Δt, and this avoid interference at the output of the interferometer. As for the laser ranging technique, the state $|\Psi_{out}\rangle$ is directed to a satellite using the same telescope. The satellite retroreflector redirects the beam back to the ground station, where it is collected and injected into the same MZI used in the uplink. Due to downlink attenuation [98,103], the state collected by the telescope can be written as $|\Psi_r\rangle = (1/\sqrt{2})(|S\rangle - e^{i\phi t}|L\rangle)$, namely, as a superposition of two single-photon wave packets $|S\rangle$ and $|L\rangle$ (the state $|\Psi_r\rangle$ corresponds to the renormalized single-photon part of the state received at the telescope), which correspond to a time-bin encoding. The relative phase $\phi(t)$ is due to the satellite instantaneous radial velocity with respect to the ground, $v_r(t)$. Indeed the satellite motion, at a given instant t, determines a shift $\delta r(t)$ of the reflector radial position, during the separation Δt between the two wave packets. This shift can be estimated at first order as $\delta r(t) \approx v_r(t)\delta t$, and its value may reaches a few tens of micrometers for the satellite that we have used. As a consequence, the satellite motion imposes during reflection the additional kinematic phase $\theta(t) \approx 2\delta r(t)(2\pi/\lambda)$ between $|L\rangle$ and $|S\rangle$, where λ is the pulse wavelength in vacuum. A single MZI for state generation and detection intrinsically ensures the same unbalance of the arms and avoids active stabilization, necessary otherwise with two independent interferometers.

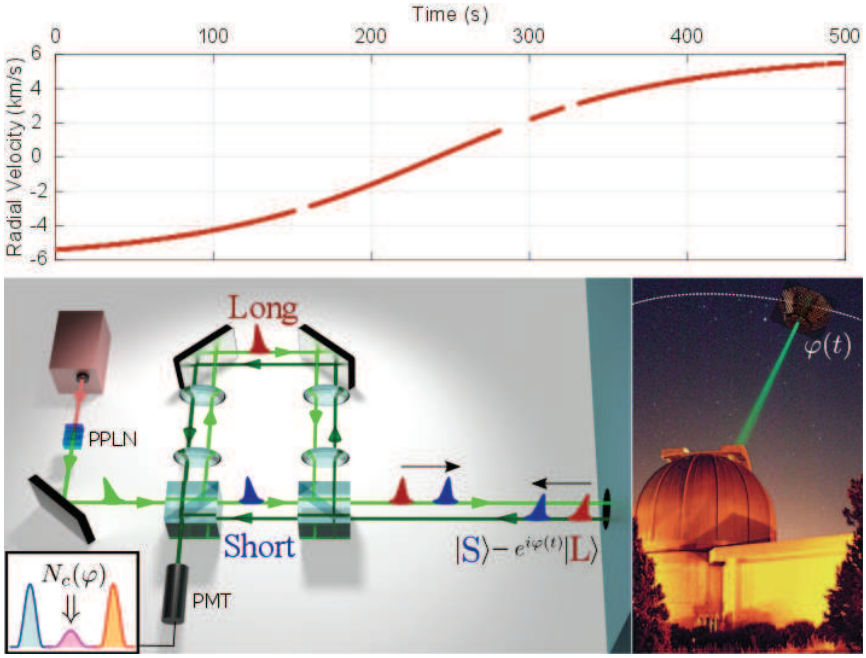


Figure 5.2: In the top panel we can see the satellite radial velocity, $v_r(t)$, measured for Beacon-C satellite. Its value ranges from -6 to $+6$ km/s as a function of time during a single passage. In the bottom panel, we can see a schematic of the experimental setup. An unbalanced MZI with the two $4f$ systems used for the generation of the state and the measurement of the interference. In the small panel it is shown the typical expected detection pattern of time-bin encoding, where the number of counts N_c in the central peak varies according to the kinematic phase θ imposed by the satellite.

In order to obtain interference it is necessary to perfectly match the wavefronts of the wave packets traveling through the short or the long arm. This matching is particularly necessary for the photon beams reflected by the satellite that are subjected to the atmosphere distortion. To this purpose, we have used two $4f$-systems that realize an optical relay of length equal to the path difference between the long and short arm of the MZI. The relay is required to match the interfering beam wavefronts that are distorted by the passage through atmospheric turbulence: otherwise, the latter may cause distinguishability between the two paths, washing out the interference. Each $4f$-systems is composed by two lenses with focal length $f = 12.5\,\text{cm}$ (see fig.5.3A). A single $4f$-systems realize also a mirror transformation on the wavefront, and thus, is necessary to compensate that whit another $4f$-system.

In fig.5.3B it is possible to see the images obtained by blocking the long and the short arm. The two images are comparable (the cross-correlation between them is higher than 0.95, where 1 means identical image), showing that the wavefronts traveling the short or long arm are well matched at the output of the interferometer. At the MZI outputs we expect detection times that follow the well known three-

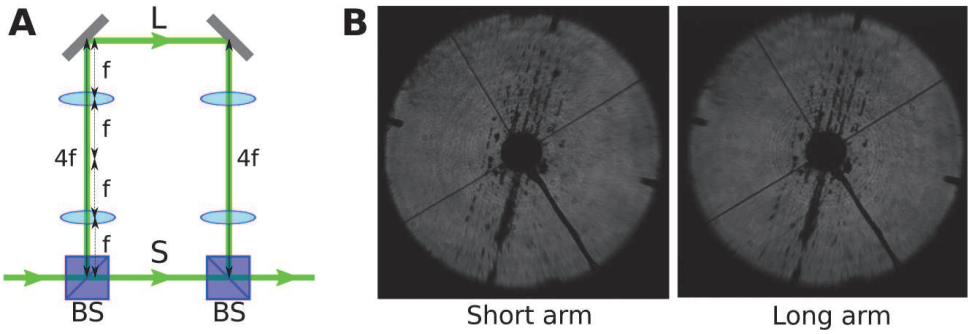


Figure 5.3: In fig.A is represented the scheme of the unbalanced Mach-Zehnder interferometer with the two $4f$-system. In fig.B we can see the images of the primary mirror obtained with only the short or long arm opened.

peak profile (see fig.5.2): the first peak represents the pulse $|S\rangle$ taking again the short arm, while the third represents the delayed pulse $|L\rangle$ taking again the long arm. In the central peak we expect indistinguishably between two alternative possibilities: the $|S\rangle$ pulse taking the long arm and the $|L\rangle$ pulse taking the short arm in the path along the MZI toward the detector. We can say that there is interference at the single photon level when the counts in the central peak differs from the sum of the counts in the lateral peaks.

To measure the interference, we used a photomultiplier tube (PMT), a vacuum phototube which offers single photon detection with greater detection area respect to SPAD, at the cost of less efficiency (about 10%). The PMT is placed at the available port of the MZI (see fig.5.2). For a moving retroreflector, the probability P_c of detecting the photon in the central peak is given by[102]:

$$P_c(t) = \frac{1}{2}\left[1 - \mathcal{V}(t)\cos\phi(t)\right] \tag{5.1}$$

with

$$\phi(t) = \frac{2\beta(t)}{1+\beta(t)}\frac{2\pi c}{\lambda}, \quad \mathcal{V}(t) = \exp\left(-\frac{\lambda^2\phi^2(t)}{8\pi c^2\tau_c^2}\right) \simeq 1 \tag{5.2}$$

We note that for a retroreflector at rest we expect $P_c = 0$. The parameter $\beta(t)$ is defined as $\beta(t) = v_r(t)/c$. The above relation is obtained by time-of-flight calculations together with the Doppler effect that changes the angular frequency of the reflected pulses from $\omega_0 \equiv 2\pi c/\lambda$ to $\omega_0(1-\beta)/(1+\beta)$. The theoretical visibility $\mathcal{V}(t)$ is approximately 1 since the β factor is upper bounded by $3 \times 10^{-}5$ in all the experimental studies cases, while the ratio $\Delta t/\tau_c$ is of the order of 10^2.

5.2 Experimental result

The value of $\theta(t)$ originating from the satellite motion can be precisely predicted on the basis of the sequence of measurements of the instantaneous distance of the satellite, or range r, which is realized in parallel. The range is measured by the strong SLR signal seen above, whit a precise time separation of $\Delta T = 100ms$ between the pulses. After the satellite retroreflection, at the receiver, the measured temporal separation is $\Delta T'$ from which it is possible to determine the instantaneous satellite velocity relative to the ground station $v_r(t)$. This velocity, due to Doppler effect $\Delta T' = \Delta T(1+\beta)/(1-\beta)$, can be estimated as

$$v_r(t) = c\frac{(\Delta T' - \Delta T)}{(\Delta T' + \Delta T)}. \tag{5.3}$$

The separation $\Delta T'$ is related to the range r by

$$\Delta T' = \Delta T + \frac{\Delta r}{c} \tag{5.4}$$

where Δr is the variation of the satellite distance between two subsequent SLR pulses. By measuring the range every 100 ms, it is possible to estimate $v_r(t)$ from which $\phi(t)$ can be derived by using eq.5.2. In fig.5.4, it is shown the passage the measured satellite distance and the estimated $\phi(t)$ for a

passage of the Ajisai satellite. Since $v_r(t)$ is continuously changing along the orbit, the value of $\phi(t)$ is varying accordingly. In the bottom panel of fig.5.4, it is shown the variation of the theoretical output probability $P_c(t)$ along the Ajisai orbit predicted by eq. 5.1. To observe single photon interference,

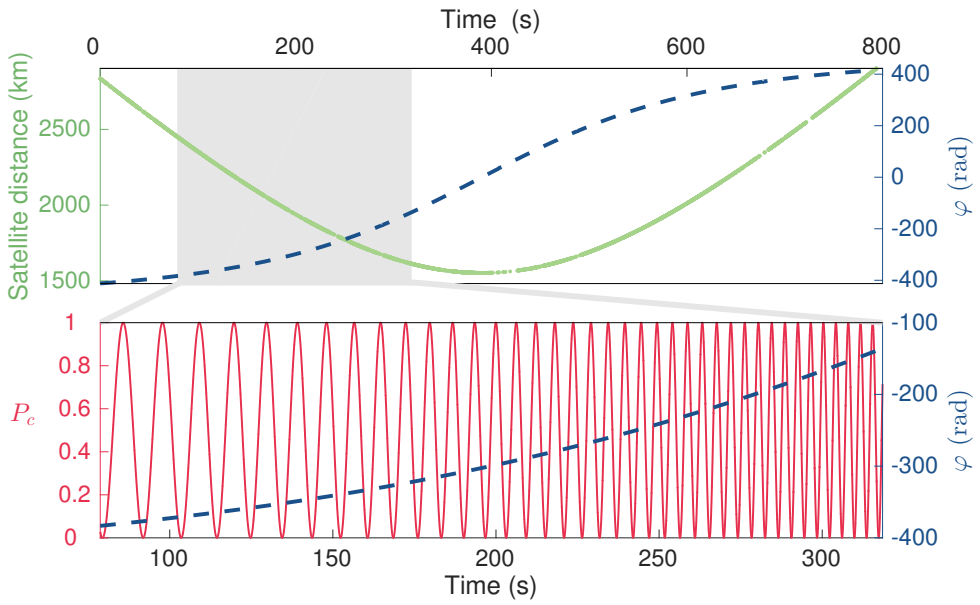


Figure 5.4: Kinematic phase and interference pattern. In the top we show the measured satellite distance and the predicted kinematic phase $\phi(t)$ estimated by eq. 5.2 as a function of time for a passage of the Ajisai satellite. Shaded area represents the temporal window of data acquisition. In the bottom we show the kinematic phase $\phi(t)$ and theoretical probability $P_c(t)$ in the shaded area. The interference patter is modulated according to the value of $\phi(t)$ determined by the satellite velocity.

the receiver requires a very precise temporal synchronization and a strong rejection of the background. The expected instant of arrival of the photons at the MZI output, t_{ref}, can be determined by dividing the time between two consecutive SLR detections in 10^7 subintervals (the number of pulses generate by our system between two SLR pulses). By using a time-to-digital converter with 81 ps resolution, we acquired the start and the stop signals of the laser ranging pulses, together with PMT detections, denote with t_{meas}. By this, we calculate the histogram of the returns in the temporal window of 10 ns between two consecutive pulses as a function of the temporal difference $\Delta = t_{meas} - t_{ref}$ corresponding to a desired value of $\phi(t)$.

In fig.5.5 is reported the constructive and destructive interference in the case of satellite Beacon-C. For the constructive interference (fig.5.5A) we selected the detections corresponding to $\phi(\mod 2\pi) \in [4\pi/5, 6\pi/5]$. For the destructive interference (fig.5.5B), we selected a kinematic phase $\phi(\mod 2\pi) \in [-\pi/5, \pi/5]$. As we can see, the detections in the central peak are, respectively, higher or lower than

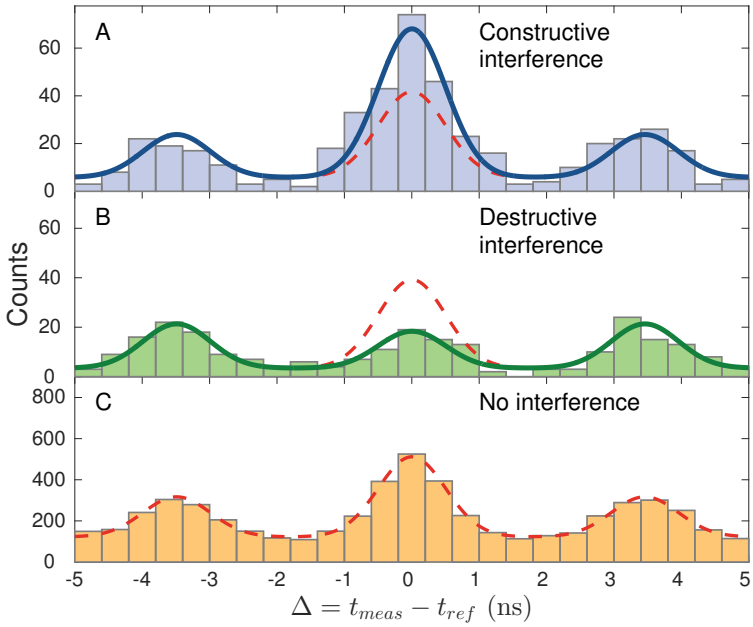


Figure 5.5: Constructive and destructive single photon interference [Beacon-C satellite, 11.07.2015 h 1.33 CEST]. (A) Histogram of single photon detections as a function of time $\Delta = t_{meas} - t_{ref}$ realized by selecting only the returns characterized by $\phi(\mod 2\pi) \in [4\pi/5, 6\pi/5]$ that lead to constructive interference. The solid line shows the tri-Gaussian fit. By evaluating the Gaussian integrals we obtained the counts $N_l = 112 \pm 11$ for the sum of lateral peaks and $N_c = 196 \pm 14$ for the central one. (B) Histogram of single photon detections realized by selecting only the returns characterized by $\phi(\mod 2\pi) \in [-\pi/5, \pi/5]$. Here, $N_l = 112 \pm 11$ and $N_c = 46 \pm 7$. (C) Histogram of single photon detections without any selection on the phase. As expected, the interference is completed washed out and we measured $N_c = 1245 \pm 35$ and $N_l = 1306 \pm 36$, fully compatible with $P_c = 1/2$. In all panels, the dotted red lines represent the expected counts in case of no interference.

the sum of the two lateral peaks (the sum is represented by a dotted red line). In the bottom histogram (fig.5.5C), we report all the data, without any selection on ϕ, showing that no interference occurs (it is the same to take the mean value of the interference). These results show that, in order to prove

the interference effect, it is crucial to correctly predict the kinematic phase ϕ imposed by the satellite motion.

By the data acquired on fig.5.5, we experimentally evaluate the probability $P_c^{(exp)}$ as the ratio between the central peak N_c to twice the sum N_l of the detection associated with the side peaks

$$P_c^{(exp)} = \frac{N_c}{2N_l}. \tag{5.5}$$

In table 5.1 is reported the value of $P_c^{(exp)}$ for constructive and destructive interference, and as we can see, the values deviate with evidence from 0.5, that is the value in the case of no interference.

	$P_c^{(exp)}$
Constructive	0.87 ± 0.10
Destructive	0.20 ± 0.03

Table 5.1: Values of $P_c^{(\exp)}$ for constructive and destructive interference obtained from the passage of Beacon-C satellite, 11.07.2015 h 1.33 CEST.

We also evaluate the experimental probabilities $P_c^{(exp)}$ in function of ϕ, as shown in Figure 5.6 for three different satellites. By fitting the data with $P_c^{(exp)} = \frac{1}{2}(1 - \mathcal{V}_{exp} \cos\phi)$, we estimate the experimental visibilities shown in table 5.2.

Satellite	$\mathcal{V}_{exp}$	Range [km]
Beacon-C	$67 \pm 11\%$	from 1200 to 1500
Stella	$53 \pm 13\%$	from 1100 to 1500
Ajisai	$38 \pm 4\%$	from 1600 to 2500

Table 5.2: Visibilities and ranges for three satellite, Beacon-C, 11.07.2015, h 1.33 CEST; Stella, 12.07.2015, h 3.08 CEST; Ajisai, 12.07.2015, h 3.42 CEST.

We attribute the different visibilities to residual vibrations of the unbalanced MZI between the upgoing and downgoing pulses, since the intrinsic visibility of the interferometer was measured to be above 95%. To improve the visibility it would be necessary to redesign the full interferometric setup

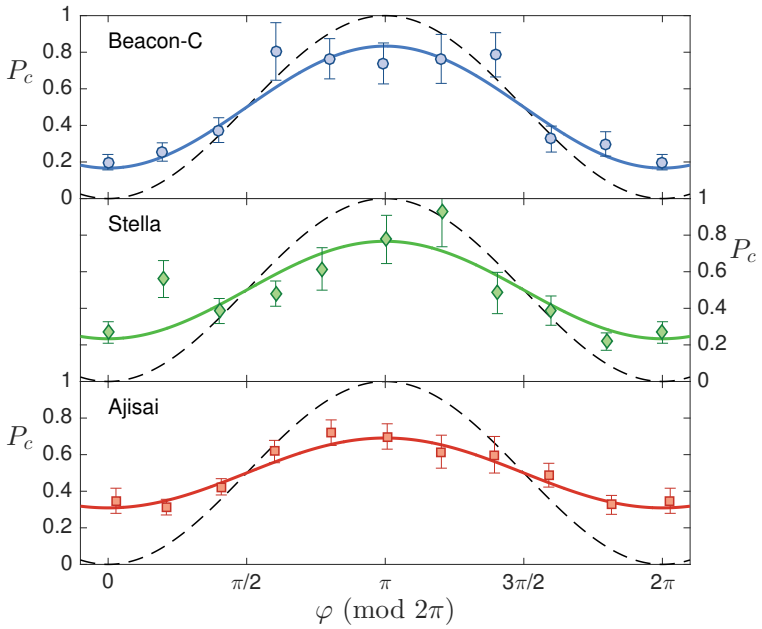


Figure 5.6: Experimental interference pattern. Experimental probabilities P_c^{exp} as a function of the kinematic phase measured for three different satellites. By fitting the data we estimate the visibilities $V_{exp} = 67 \pm 11\%$ for Beacon-C, $V_{exp} = 53 \pm 13\%$ for Stella, and $V_{exp} = 38 \pm 4\%$ for Ajisai. The dashed lines correspond to the theoretical value of P_c predicted by Eq. 5.1. The points are obtained by considering ten intervals of the phase defined by $\mathcal{I}_j = [(j1/10)\pi,\ (j + 1/10)\pi]$. For each interval we selected the data corresponding to $\phi(\mod 2\pi) \in \mathcal{I}_j$: from such data we determined the experimental probability of detection in the central peak P_c^{exp} and we averaged the corresponding phase ϕ. We note that at the point $\phi = 0$ and $\phi = 2\pi$ the same subset of data was selected

to further mitigate this effect. We note that,in the double-pass configuration, the interferometer is sensitive to vibrations with frequency higher than $1/rtt$, where rtt is the round trip time. The rtt for Ajisai has a typically rtt between 10.7 and 16.7 ms, and the other two satellites, instead, have a rtt lower than 10 ms.

In addition we evaluate the mean number of photons μ_{rX} in the received pulses. A general formula which can be used to estimate the detected number of photons per pulse is the radar equation [104]:

$$\mu_{rx} = \mu_{tx}\eta_{tx}G_t\Sigma\left(\frac{1}{4\pi R^2}\right)^2 T_a^2 A_t \eta_{rx}\eta_{det} \tag{5.6}$$

where μ_{tx} is the source mean photon per pulse, η_{tx} is the optical transmission efficiency, G_t is the transmission gain, Σ is the satellite cross section, that depends on corner cube reflectivity and the satellite retroreflective area and the downlink gain, R is the slant distance, T_a is the atmospheric transmissivity, A_t is the telescope area, η_{tx} is the optical receiving efficiency, and $\eta_{det}$is the single photon detector efficiency. At the primary mirror of the receiving telescope, the average μ_{rx} during the data acquisition are shown in table 5.3. From these values we may conclude that interference was probed

Satellite	μ_{rx}
Beacon-C	$7 \times 10^{-}4$
Stella	$9 \times 10^{-}4$
Ajisai	$2 \times 10^{-}4$

Table 5.3: Source mean photon per pulse for three satellite, Beacon-C, 11.07.2015, h 1.33 CEST; Stella, 12.07.2015, h 3.08 CEST; Ajisai, 12.07.2015, h 3.42 CEST.

at the single photon level.

5.3 Interferometer visibility

In this section we see how the interferometer instability affects the visibility of the interference. The basic idea is that when the coherent state pass through the interferometer at time t, the phase between the short and the long arm is equal to $\theta(t)$. Then, as we saw previously, when the beam hits the satellite an additional phase ϕ is added between the two temporal modes. Finally, when the beam returns to the interferometer, we can have two scenarios. In the first (ideal), the phase of the interferometer doesn't change during the round trip time τ of the beam (this correspond to a perfect stabilized interferometer). In this case, the two temporal modes acquire a phase of $-\theta(t+\tau) = -\theta(t)$ between them, canceling out the contribution of the first phase. In the second scenario (real), the phase of the interferometer changes during the round trip time. This means that the two temporal modes acquire a phase $-\theta(t+\tau) \neq -\theta(t)$ different from the first, and at the end, we have a residual phase equal to

$\theta(t) - \theta(t+\tau)$.

For simplicity, we assume that the phase variation is linear, the phase difference depends only on the value of τ, namely $\theta(t) - \theta(t+\tau) = \delta\theta(\tau)$. The probability of detect a photon in the central peak, in function of ϕ and τ can be written as

$$P_c(\phi, \tau) = \frac{1 - V_0 \cos(\phi + \delta\theta(\tau))}{2}, \tag{5.7}$$

and the visibility as

$$V(\tau) = P_c(\pi, \tau) - P_c(0, \tau), \tag{5.8}$$

where $P(\pi, \tau)$ is the maximal value of the probability, $P(0, \tau)$ the minimum and V_0 the nominal visibility of the interferometer. From the two equations above we obtain:

$$\begin{aligned} V(\tau) &= \frac{1 - V_0 \cos(\pi + \delta\theta(\tau))}{2} - \frac{1 - V_0 \cos(\delta\theta(\tau))}{2} \\ &= \frac{-V_0 \cos(\pi + \delta\theta(\tau)) + V_0 \cos(\delta\theta(\tau))}{2} \\ &= \frac{V_0}{2}(\cos(\delta\theta(\tau)) + \cos(\delta\theta(\tau))) = V_0 \cos(\delta\theta(\tau)). \end{aligned} \tag{5.9}$$

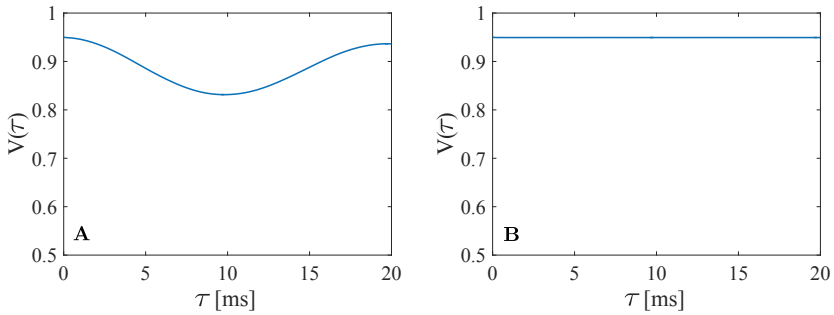


Figure 5.7: Visibility in function of rtt. Left panel shows the visibility obtained with the old configuration. Right panel shows the visibility obtained with the new one.

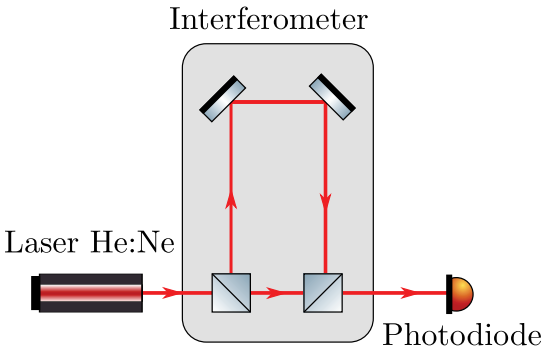


Figure 5.8: Experimental setup used to evaluate the term $\delta\theta(\tau)$. Realized with ComponentLibrary[2].

To experimentally evaluate the term $\delta\theta(\tau)$, we use a continuous single mode He:Ne laser with a coherence time of hundreds of nanoseconds, greater than $\Delta t \approx 3.5\ ns$ (the time difference between short and long arm). The He:Ne laser is sent to the same interferometer used in MLRO. At the output of the interferometer we used a photodiode to measure the interference(see Fig. 5.8). In this case, the two beams interfere at the output of the unbalanced MZI and, from the output intensity, it is possible to recover the value $\delta\theta(\tau)$. We estimate the phase θ (this is an estimation because we cannot recover the absolute value of the phase) and the visibility in this way:

$$
\begin{aligned}
V_i &= \frac{\max(I(t)) - \min(I(t))}{\max(I(t)) + \min(I(t))} \\
\theta(t)_{HeNe} &= \arcsin\left((\frac{2I(t)}{\max(I(t)) + \min(I(t))} - 1)/V_i \right) \\
\theta(t)_{green} &= \theta(t)_{HeNe} \frac{632.8}{532}
\end{aligned}
$$

The last, is the conversion to get the phase relative to the green laser used at MLRO. Then

$$
\delta\theta(\tau, t)_{green} = \theta(t)_{green} - \theta(t+\tau)_{green}
$$

and from 5.9[†]

$$V(\tau, t) = V_n \cos(\delta\theta(\tau, t)_{green}).$$

The mean value of the visibility is then

$$V(\tau) = \frac{1}{T}\int_0^T V(\tau, t)dt.$$

In our case the nominal visibility of interferometer is $V_n \propto 95\%$. The data is acquired in a configuration similar to the one used to take data from the satellite, where the mirrors of the long arm were mounted on a translation stage. In addition we test a new configuration, where the mirrors of the long arm are fixed with rigid steel rods to the other mirror of the interferometer. In fig.5.7A we can see how the value of the round trip time τ influences the visibility. For $rtts$ near 10 ms, a typical value for the satellite that we consider, we have the lower visibility. Fig.5.7B shows the visibility with the new configuration, and, as we can see, the stability of the interferometer is significantly increased.

5.4 Conclusion

In this chapter we have seen that interference at single photon level between two temporal modes was observed along a path that includes a rapidly moving retroreflector on a satellite and with a length up to 5000 km. We have experimentally demonstrated that the relative motion of the satellite with respect to the ground induces a varying phase that modulates the interference pattern. Up to this experiment, the only photon DOF exploited in long distance free-space quantum communications was the polarization. We have demonstrated that atmospheric turbulence isn't detrimental for time-bin encoding in long-distance free-space propagation. Indeed, the two temporal modes are identically

[†]Here we consider the dependence on t to calculate the mean value.

distorted by the propagation in turbulent air[99]. The fundamental point is to careful match the two patterns of the two arms, as shown in fig.5.3.

6

Certified Quantum randomness

In this chapter we will see how an entangled photon source can be used to test and demonstrate an efficient method to extract true randomness from a quantum random number generator. Nowadays, random numbers have important roles in a lot of fields, like scientific simulation, cryptography and fundamental physics experiments[118]. Random number generators based on classical physics provide a source of pseudorandom numbers. Indeed, these generators use methods derived from deterministic algorithms, which use as initial point a small string of bits, the seed. At the end of the procedure,

the output is a long sequence of bits that obey to a random distribution. The main advantages of such methods are the fast generation of random numbers and the possibility to reproduce the output string of bits, if one knows the initial seed. But for some critical applications, unpredictability is a fundamental requisite, as for cryptography or lottery. Such applications require true random number generators. Quantum physics can be exploited to provide a trusted randomness source. Indeed, the measurements of a quantum system are used as source of bits. On the other hand, when the quantum system isn't in a pure state or when it is correlated with other systems, an eavesdropper could obtain some information about the outputs of the measurements. In this way the output bits are not all truly random, but a fraction of these can be considered as random in classically way, i.e. known to the eavesdropper. Theoretical analyses about the security and the truly randomness of the process, have been provided only recently[110,111,112]. It has been shown that true random numbers can be achieved by using of randomness expansion[113,114] or amplification protocols[115,116] based on the violation of Bell inequalities. The first indicates a protocol ables to generate true random numbers by starting with a short but perfect random seed. The second refers to a protocol where the initial seed can be weaker, but greater than zero randomness, at the cost of lower output rate. Although these methods are able to generate perfect randomness, they are very onerous under the experimental implementation. Indeed, the only way to obtain perfect randomness is to enforce conditions of nonlocality and nonsignalling between two parties that violate a Bell inequality[110].

6.1 QRNG

Here we see how a generic QRNG works (for an exhaustive review see here[117]). Consider a d-level quantum system A prepared in a state ρ_A and a random variable Z, which is obtained by measuring the state ρ_A with a d-outcome measurement $\mathbb{Z}$, where each outcome is obtained with a probability P_z. Classical min-entropy $H_\infty(Z)$ quantifies the minimal number of true random bits that can be

extracted from each measurement when ρ_A is pure

$$H_\infty(Z) = -\max_z \left[\log_2 P_Z\right] \tag{6.1}$$

where $P_Z = \mathrm{Tr}\left[\mathbb{Z}\rho_A\right]$. However, this quantity doesn't quantify the real amount of true randomness that can be extracted from a real quantum process. When the state ρ_A is not pure, we can consider that the system A is correlated with a quantum system E. In this scenario it is necessary to estimate the quantity of information that the system E has on the random variable Z. The quantity of true random bits independent from the system E that can be extracted from Z, is given by the conditional min-entropy $H_{min}(Z|E)$, and the probability that an eavesdropper holding the system E guesses Z is

$$p_{guess} = (Z|E) = 2^{-H_{min}(Z|E)}. \tag{6.2}$$

Let we see an example. Consider an eavesdropper, Eve, who holds the quantum system $|\Phi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ and sends to Alice one of the two photons as the system she uses for the randomness extraction. When Alice measures in the $\{H, V\}$ basis, classical min-entropy of the random bit is is perfect, because the two outcomes $|H\rangle$ and $|V\rangle$ are equally probable. But, due to perfect correlation in the $|\Phi\rangle$ state, Eve knows the output of Alice's measurements. In this way, the bit held by Alice can be predicted with certainty by Eve, destroying the randomness. In this case, the probability that Eve has to guess the output is $p_{guess}(Z|E) = 1$.

Here we proposed a method, based on the uncertainty principle, to estimate the conditional min-entropy and the true randomness that ca be obtained by a given source. We also proposed an experimental test showing that, when the system is measured by the conjugate observables $\mathbb{Z}$ and $\mathbb{X}$, it is possible to obtain a bound on the conditional min-entropy given by

$$H_{min}(Z|E) \geq \log_2 d - H_{1/2}(X) \tag{6.3}$$

where d is the dimension of the Hilbert space and $H_{1/2}$ is the max-entropy of $\mathbb{X}$ outcomes (see appendixA and Vallone et al.[119]). The measurement $\mathbb{Z}$ is used to generate the random variable Z, and $\mathbb{X}$ is used to stabilized the amount of true randomness contained in Z. In this protocol no assumptions are used on the source state ρ_A: Eve can have full control on the source and the environment E. Then only assumption to obtain the bound 6.3 is that Eve has no access to measurement devices and that the devices performs a given POVM that are only sensitive to a subspace of dimension d.
This method offers the advantage that no Bell inequality violation is required, but to certify the randomness it is only needed to measure the system in two conjugate bases. In addition, starting with a seed of true randomness, our protocol is able to expand the randomness by taking into account all possible side quantum information possessed by Eve.

6.2 Up-certified quantum random-number generator

In real application, is impossible to prepare the state of the system A in a perfect pure state $|\psi\rangle_A$. In this case the entropies $H_\infty(Z)$ and $H_{min}(Z|E)$ can be different. In the real scenario, our method bounds the effective achievable randomness without requiring any assumption on the source. Even if Eve has complete control over the source ρ_A, the bound given in 6.3 evaluates the amount of true randomness bits that can be extracted from Z.
If we consider the initial example, when Eve sends to Alice one photon of a two-photon maximally entangled state, she can predict the output of Alice's measurements. The state hold by Alice, is a mixed state described by $\rho_A = 1/2\mathbb{1}_2$ and the max entropy is $H_{1/2}(X) = 1$. As a consequence, the bound on the min-entropy is $H_{min}(Z|E) \geq 0$ and $p_{guess}(Z|E) \leq 1$. This means that Eve can predict with certainty the "random" number of Alice, so, no true random bits can be extracted. In order to utilize the bound 6.3 in a practical way, we need to estimate the max-entropy of the source ρ_A. The POVM $\hat{\mathcal{M}}_z$ and $\hat{\mathcal{N}}_x$ cannot be measure at the same time, because they are incompatible. To avoid this

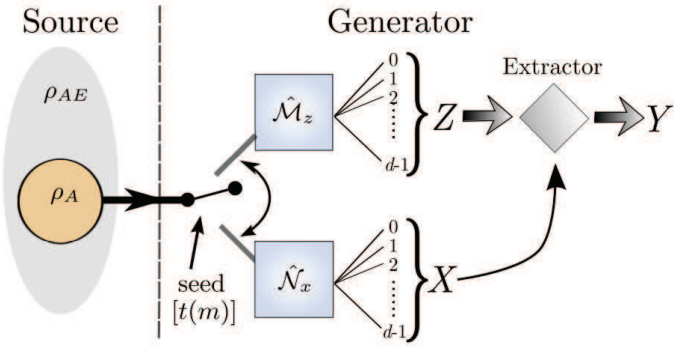


Figure 6.1: Scheme of the QRNG. The state ρ_A is the source of randomness that can be correlated with a larger system E. An initial true random seed of length $t(m)$ is used to switch between the $\{\hat{\mathcal{M}}_z\}$ and $\{\hat{\mathcal{N}}_x\}$ POVMs, from which the variables Z and X are extracted. Z is used to generate the random sequence, while X is used to evaluate how many true random bits can be extracted by Z. Y represents the final true random sequence.

problem, it is possible to switch randomly between $\hat{\mathcal{M}}_z$ and $\hat{\mathcal{N}}_x$ during the random generation (see fig.6.1). These measurements are initially chosen by using a seed of true randomness that our method is able to expand. From this point of view, our method can be seen as a random number expansion protocol. In the experimental demonstration, since we are interested in demonstrating the physical principles, we did not use active switches to change between the two bases (we first measured the Z sequence and afterwards the X sequence).

Let us now see how estimate the max-entropy. Let m be the total number of measurements. We decide that, over m, the number of measurements in the POVM $\{\hat{\mathcal{N}}_x\}$ will be $n_X = \lceil\sqrt{m}\rceil$. As a consequence the probability of measuring in the $\mathbb{X}$ basis is approximately $1/\sqrt{m}$.
The outcome probabilities in the $\mathbb{X}$ basis are given by $p_x = \mathrm{Tr}_A\left[\hat{\mathcal{N}}_x\rho_A\right]$ and the asymptotic lower bound of the in-entropy is $H_{min}(Z|E) \geq q - H_{1/2}(X)$. Experimentally we need to estimate the max-entropy $H_{1/2}(X)$ by using the n_X outcomes. If we denote by n_x (note the difference between n_X and n_x subscript) the number of outcomes such that $X = x$, we can estimate the max-entropy

by using the Bayesian estimator defined by Holste[105]

$$\widetilde{H}_{1/2}(\{n_x\}) = 2\log_2\left[\frac{\Gamma(n_X+d)}{\Gamma(n_X+d+\frac{1}{2})}\sum_{x=0}^{d-1}\frac{\Gamma(n_x+\frac{3}{2})}{\Gamma(n_x+1)}\right] \tag{6.4}$$

Then, given m measurements, the number of extracted random bits are the outputs of the $\mathbb{Z}$ measurement, given by $m - n_X$. Due to the bound, only $(m-n_X)\left[q - H_{1/2}(X)\right]$ are true random bits.

The generation rate of the random bits per measurement is

$$\widetilde{r}(\{n_x\}) = \frac{b_{sec}}{m}, \tag{6.5}$$

where b_{sec} is the number of generated true random bits:

$$b_{sec} = (m-n_X)\left[q - H_{1/2}(\{n_x\})\right] - t(m), \tag{6.6}$$

where $t(m)$ is the number of bits required for the seed, $t(m) = \left\lceil \log_2 \frac{m!}{n_X!(m-n_X)!}\right\rceil$.

When $m \to +\infty$, the seed length is given by $t(m) \approx \sqrt{m}\log_2\sqrt{2}$, the estimator $\widetilde{H}_{1/2}(\{n_x\}) \approx H_{1/2}(X)$. When the number of extracted random bits are quadratically larger than the initial seed bits, the generator expands the initial random bits and part of them i fed as a new seed.

6.3 Experimental realization

My contribution in this experiment was mainly in the realization of the source. The source used to test our method is very similar to the one described in chapter 3 (see fig.6.2). A spontaneous parametric down conversion crystal is used to generate a photon pair. The nonlinear crystal is pumped by femtosecond laser pulses with a 76MHz repetition rate. The generated state is $|\psi\rangle = |HV\rangle - |VH\rangle$,

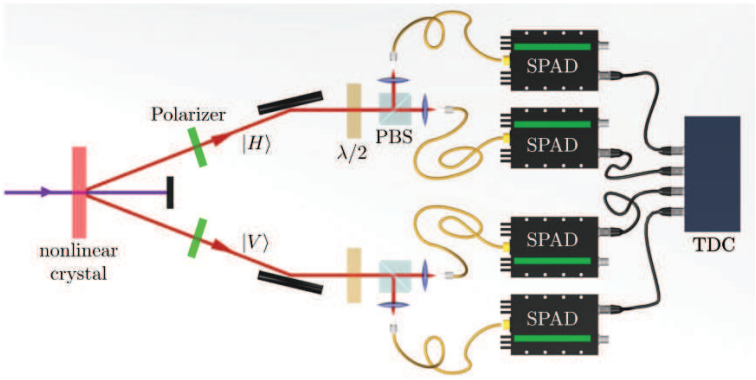


Figure 6.2: Scheme of experimental setup.

and polarising beam splitters select the polarization of the photons. To change between the two basis $\mathbb{Z}$ and $\mathbb{X}$ an half-wave plate is used.

For the generation of the single qubit, the $|H\rangle$ photon is used as a trigger: its detection means the presence of the photon $|V\rangle$ on the other side. This source can provide a rate of photon pairs of 12kHz. Practical applications require higher rate, but in our case, we are interested on the demonstration of the method.

This source has been used as a QRNG to test our algorithm, in two different ways. First we analyze the source as a single qubit QRNG, where a photon of the pair, measured in the $|H\rangle$ state is used as trigger, while the second represents the signal. To generate the random variables Z and X, the signal photon is measured in the basis $\mathbb{Z} = \{|+\rangle, |-\rangle\}$ and $\mathbb{X} = \{|H\rangle, |V\rangle\}$, where $|\pm\rangle = 1/\sqrt{2}(|H\rangle \pm |V\rangle)$. To estimate the classical max-entropy $\widetilde{H}_{1/2}(\{n_x\})$ and the rate $\widetilde{r}(\{n_x\})$ we used the sequences X and Z, which are obtained by choosing $n_X = \lceil\sqrt{m}\rceil$ measurements in the $\mathbb{X}$ basis and $n_Z = m - n_X$ in the $\mathbb{Z}$ basis. In fig.6.3 is reported the average rate $\widetilde{r}$ and its standard deviation experimentally evaluated over 200 different X sequences of n_X bits. The experimental rates can be compared with the predicted average rate $\langle\widetilde{r}\rangle = \sum_{n_x} = \Pi(\{n_x\})\widetilde{r}(\{n_x\})$, obtained by averaging $\widetilde{r}(\{n_x\})$ over the

multinomial distribution

$$\Pi(\{n_x\}) = \frac{n_X!}{n_0!n_1!...n_{d-1}!} p_0^{n_0} p_1^{n_1} ... p_{d-1}^{n_{d-1}} \tag{6.7}$$

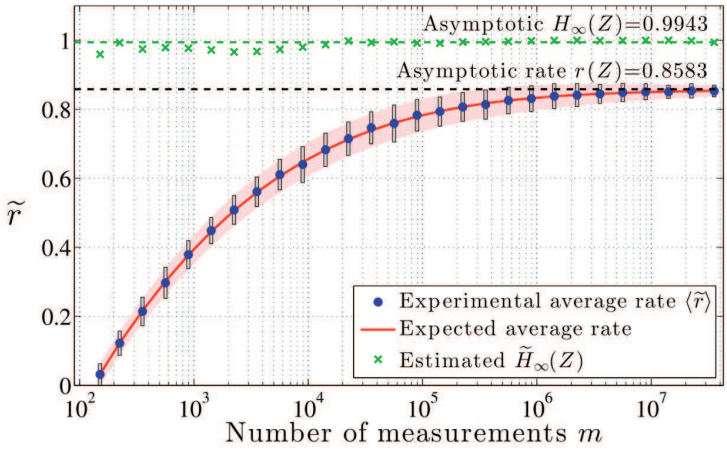


Figure 6.3: Average experimental rate for the qubit QRNG. Blue circles represent the experimental average rate $\widetilde{r}$ of true random bits per measurement, while the continuous red line is the theoretical prediction with $\rho_X = \sum_{x=0}^{1} = p_x|x\rangle\langle x|$ where $p_0 = 0.9973$ and $p_1 = 0.0027$. The shaded red area represents the theoretical standard deviation of the rate, while gray rectangles show the experimental standard deviation of the rate. Green crosses show the classical min-entropy estimated on the Z random variable. The asymptotic limit $H_\infty(Z)$ is evaluated on the state $\rho_Z = \sum_{z=0}^{1} P_z|z\rangle\langle z|$ with $P_0 = 0.5020$ and $P_1 = 0.4980$.

Then we use our source as as a four-level system, namely ququart, QRNG. The $\mathbb{Z}$ and $\mathbb{X}$ bases are respectively give by $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$, and $\{|HV\rangle, |VV\rangle, |HH\rangle, |VH\rangle\}$. The number of measurements are chosen in the same way as indicate for the qubit. As for the qubit, in fig.6.4, we can see for each m, the average rate $\widetilde{r}$ and its standard deviation evaluated over 200 different experimentally X sequences of $n_X(m)$ bits.

From the figures, we see that when m are greater than 10^6, the rate is very close to the asymptotic bound $r(Z)$. In the case of ququart, we obtain an asymptotic bound $r(Z)^4 = 1.685$ bits per measurement, compared with the value of $r(Z)^2 = 0.8583$ achieved with the qubit QRNG. In addition we have evaluated, for qubit and ququart, the classical min-entropy $\widetilde{H}_\infty(Z)$ evaluated on a sequence

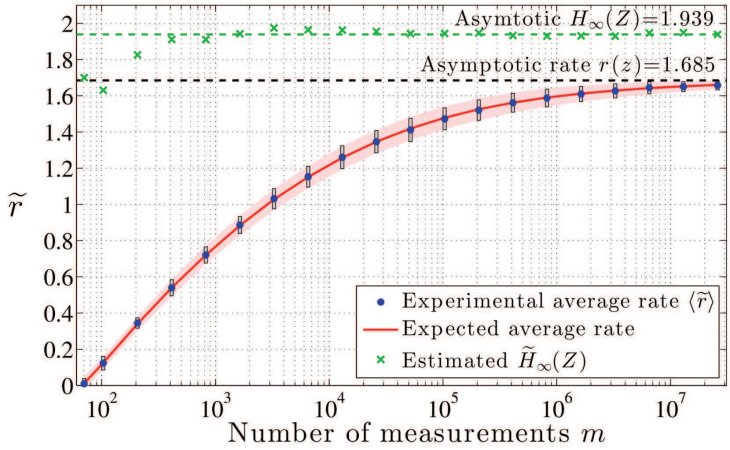


Figure 6.4: Average experimental rate for the ququart QRNG. For notations, see fig.6.3. In this case $\rho_X = \sum_{x=0}^{3} p_x|x\rangle\langle x|$ with $p_0 = 0.9937$, $p_1 = 0.00359$, $p_2 = 0.00266$ and $p_3 = 1 - p_0 - p_1 - p_2$. For ρ_Z we have $\rho_Z = \sum_{z=0}^{3} P_z|z\rangle\langle z|$ with $P_0 = 0.2527$, $P_1 = 0.2412$, $P_2 = 0.2608$ and $P_3 = 0.2453$.

Z with n_Z bits. In the fig.6.3 and 6.4, we see that between $H_\infty(Z)$ and $\widetilde{r}$ there is a gap: this represents the possible knowledge that may have an adversary holding the system E. The limit $H_\infty(Z)$ is often taken as the amount of true randomness used to calibrate the extractor. But this is incorrect, because even if the output string appears statistically good, possible side information held by Eve is not completely erased.

6.4 Conclusion

With the methods proposed in this chapter, we provided a bound by eq.6.3, that can be used to directly compute the conditional min-entropy $H_{min}(Z|E)$ of the random variable Z, by using the classical random variable X. This term represents the amount of true randomness that can be extracted from Z. The variables Z and X are obtained by measuring the system in two mutually unbiased bases. The assumption that we have made is that the measurement devices are trusted. It is important to stress that, if the source does not generate a perfect pure state (as always happens for experimental

applications), the randomness extracted by standard methods (by measuring the system in a single basis) is not a true randomness, because an eavesdropper can have, partially or full, information about the generated random bits.

7

Conclusion

This thesis shows some new applications with temporal and polarization degrees of freedom (DOFs) of the photons for quantum information.

This work started, in chapter 2, with the study and the realization of an hyperentangled photon source in temporal and polarization DOFs. A nanosecond synchronization was studied to share between spatial separated users a precise time reference in order to reconstruct the time-bin state. This solution can be used in future implementation to distribute hyperentangled state with free-space communica-

tion link.

In chapter 3, we presented a new quantum tomographic method to reconstruct a density matrix with very few measurements. This method can be applied very efficiently when prior information on the quantum state are available. This is the case when we deal with quantum state in a laboratory, where we know the implementation of the experiment.

In chapter 4, we proposed a time-bin photon source with high visibility. This source was used to violate different chained Bell inequalities with 6, 8 and 10 terms. In this way, we have demonstrated that with this setup is possible to overcome the postselection loophole. In addition, a future implementation of the measurement interferometers is proposed.

In chapter 5, we reported the results obtained in the transmission of time-bin encoded photons along satellite-ground channel. We proved that atmospheric turbulence is not detrimental for time-bin encoding, if a careful match of the received beam is carried out. This experiment attests to the viability of photon temporal DOF for fundamental test of physics and quantum communication in space.

In chapter 6, with the use of a polarization entangled source, we demonstrate a new method to certify the randomness of a quantum random number generator.

Finally, a personal consideration. In the last years, quantum information had an impressive progress, both in theoretical and experimental studies. Recently, European Commission has announced plans to launch a flagship project to incentive quantum technologies. This is a great opportunity to expand and propose new research in quantum information field for a better knowledge of the world around us.

A

Proof of the min-entropy bound

In this section we see how derive the bound 6.3. First we start by reviewing the uncertainty relation for min- and max- conditional entropies[107,108,109].

A.1 Uncertainty principle

Consider a three quantum system composed by A, B and E, with ρ_{ABE} a tripartite state. Define $\mathbb{Z}$ and $\mathbb{X}$ as two POVMs on A with elements $\{\hat{\mathcal{M}}_z\}$ and $\{\hat{\mathcal{N}}_x\}$, and a random outcomes Z and X

encoded in two orthonormal bases $\{|z\rangle\}$ and $\{|x\rangle\}$.

Then the uncertainty principle is written as

$$H_{min}(Z|E)_\rho + H_{max}(X|B)_\rho \geq q, \tag{A.1}$$

where the min-entropy[106] and max-entropy[106] are evaluated on the postmeasurement states $\rho_{ZE} = \sum_z |z\rangle\langle z| \otimes \mathrm{Tr}_{AB}\left[\hat{\mathcal{M}}_z \rho_{ABE}\right]$, $\rho_{XB} = \sum_x |x\rangle\langle x| \otimes \mathrm{Tr}_{AE}\left[\hat{\mathcal{N}}_x \rho_{ABE}\right]$ and

$$q = \log_2 \frac{1}{c}, \qquad c = \max_{z,x} ||\sqrt{\hat{\mathcal{M}}_z}\sqrt{\hat{\mathcal{N}}_x}||^2_\infty. \tag{A.2}$$

The parameter c is the maximum overlap between the two POVMs, and q quantifies the incompatibility of the measurements. If $\hat{\mathcal{M}}_z$ and $\hat{\mathcal{N}}_x$ are projective measurements corresponding to mutually unbiased bases in dimension d, then $c = \frac{1}{d}$.

A.2 Proof of the bound

In a QRNG, Alice measures its system ρ_A by using a POVM measurement $\mathbb{Z} \equiv \{\hat{\mathcal{M}}_z\}$. The choose of POVM measurements is for a generic scenario, but projective measurements are more practical. The state ρ_A can be described by $\rho_A = \mathrm{Tr}_E[\rho_{AE}]$, meaning that ρ_A is correlated with an external system E. The outcome of the POVM can be expressed by an orthonormal basis $\{|z\rangle_A\}$, such that the state after the measurement is $\rho_{ZE} \equiv \sum_z |z\rangle\langle z| \otimes \mathrm{Tr}_A\left[\hat{\mathcal{M}}_z \rho_{AE}\right] = \sum_z P_z |z\rangle\langle z| \otimes \rho_E^z$, where ρ_E^z is normalized. The min-entropy $H_{min}(Z|E)$, evaluated over ρ_{ZE} gives the Eve's knowledge about the possible outcomes of the $\mathbb{Z}$ measurement. To bound the min-entropy $H_{min}(Z|E)$ and as a consequence the guessing probability 6.2, Alice sometimes, measures her system with a different POVM $\mathbb{X}$. Indeed, by using eq.A.1, and by considering the system B as a trivial space, the uncertainty relation becomes $H_{min}(Z|E) \geq -H_{max}(X)$, where the max-entropy must be evaluated on the state

$\rho_X \equiv \sum_x p_x |x\rangle\langle x|$, with $p_x = \mathrm{Tr}_{AE}\left[\hat{\mathcal{N}}_x \rho_{AE}\right]$. In this case $H_{max}(X) = 2\log_2 \mathrm{Tr}\left[\sqrt{\rho_X}\right]$ [106], that is $H_{1/2}(X)$, the Rényi entropy of order $1/2$ of the classical outcome X. Our result can be summarized as:

$$H_{min}(Z|E) \geq q - H_{1/2}(X) \tag{A.3}$$

where q is equal to $\log_2 d$ in case of conjugate observables in d dimensions.

Bibliography

[1] Wikipedia, www.wikipedia.com.

[2] Componentlibrary by alexander franzen, licensed under a creative commons attribution-noncommercial 3.0 unported license, www.gwoptics.org/componentlibrary, https://creativecommons.org/licenses/by-nc/3.0/.

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

[4] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

[5] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M.l S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam. Strong loophole-free test of local realism*. *Phys. Rev. Lett.*, 115:250402, Dec 2015.

[6] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28:938–941, Apr 1972.

[7] A. Aspect, P. Grangier, and G. Roger. Experimental tests of realistic local theories via bell's theorem. *Phys. Rev. Lett.*, 47:460–463, Aug 1981.

[8] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, Oct 2015. Letter.

[9] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[10] A. Gerardo, A. Serafini, and F. Illuminati. Entanglement, purity, and information entropies in continuous variable systems. *Open Systems and Information Dynamics*, 12(02):189–205, 2005.

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

[12] N. Linden, S. Popescu, and S. Popescu. On multi-particle entanglement. *Fortschritte der Physik*, 46(4-5):567–578, 1998.

[13] X. Ma, S. Zotter, J. Kofler, R. Ursin, T. Jennewein, C. Brukner, and A. Zeilinger. Experimental delayed-choice entanglement swapping. *Nat Phys*, 8(6):479–484, Jun 2012.

[14] J. Jin, M. Grimau Puigibert, L. Giner, J. A. Slater, M. R. E. Lamont, V. B. Verma, M. D. Shaw, F. Marsili, S. W. Nam, D. Oblak, and W. Tittel. Entanglement swapping with quantum-memory-compatible photons. *Phys. Rev. A*, 92:012329, Jul 2015.

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

[16] A. Cabello. Bipartite bell inequalities for hyperentangled states. *Phys. Rev. Lett.*, 97:140406, Oct 2006.

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

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

[19] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. G¨uhne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan. Experimental demonstration of a hyper-entangled ten-qubit schr¨odinger cat state. *Nature Physics*, 6:331–335, 2010.

[20] S. Massar. Nonlocality, closing the detection loophole, and communication complexity. *Phys. Rev. A*, 65:032121, Mar 2002.

[21] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Going Beyond Bell's Theorem*, pages 69–72. Springer Netherlands, Dordrecht, 1989.

[22] Mark Beck. *Quantum Mechanics: Theory and Experiment*. Oxford University Press, 2012.

[23] Malvin Carl Teich Bahaa E. A. Saleh. *Fundamentals of Photonics, 2nd Edition*. Wiley, 2007.

[24] I. L. Chuang M. A. Nielsen. *Quantum Computation and Quantum Information*. Cambridge, 2010.

[25] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001.

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

[27] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin. Time-bin entangled qubits for quantum communication created by femtosecond pulses. *Phys. Rev. A*, 66:062308, Dec 2002.

[28] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin. Distribution of time-bin entangled qubits over 50 km of optical fiber. *Phys. Rev. Lett.*, 93:180502, Oct 2004.

[29] D. Grassani, M. Galli, and D. Bajoni. Active stabilization of a michelson interferometer at an arbitrary phase with subnanometer resolution. *Opt. Lett.*, 39(8):2530–2533, Apr 2014.

[30] K. Huang, H. Le Jeannic, J. Ruaudel, O. Morin, and J. Laurat. Microcontroller-based locking in optics experiments. *Review of Scientific Instruments*, 85(12), 2014.

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

[32] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge Uni- versity Press, 1995.

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

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

[35] M. Horodecki and M. Piani. On quantum advantage in dense coding. *Journal of Physics A: Mathematical and Theoretical*, 45(10):105306, 2012.

[36] 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.*, 70:1895–1899, Mar 1993.

[37] 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.*, 80:1121–1125, Feb 1998.

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

[39] R. Valivarthi, M. Puigibert, Q. Zhou, G. H. Aguilar, V. B. Verma, F. Marsili, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel. Quantum teleportation across a metropolitan fibre network. *Nat Photon*, 10(10):676–680, Oct 2016. Letter.

[40] Q. Sun, Y. Mao, S. Chen, W. Zhang, Y. Jiang, Y. Zhang, W. Zhang, S. Miki, T. Yamashita, H. Terai, X. Jiang, T. Chen, L. You, X. Chen, Z. Wang, J. Fan, Q. Zhang, and J. Pan. Quantum teleportation with independent sources and prior entanglement distribution over a network. *Nat Photon*, 10(10):671–675, Oct 2016. Letter.

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

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

[43] R. Jin, M. Takeoka, U. Takagi, R. Shimizu, and M. Sasaki. Highly efficient entanglement swapping and teleportation at telecom wavelength. *Scientific Reports*, 5:9333 EP –, Mar 2015. Article.

[44] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[45] 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*, 75:042317, Apr 2007.

[46] Paul G. Kwiat and Harald Weinfurter. Embedded bell-state analysis. *Phys. Rev. A*, 58:R2623–R2626, Oct 1998.

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

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

[49] R. Blume-Kohout. Optimal, reliable estimation of quantum states. *New Journal of Physics*, 12(4):043034, 2010.

[50] R. Blume-Kohout. Hedged maximum likelihood quantum state estimation. *Phys. Rev. Lett.*, 105:200504, Nov 2010.

[51] V. Bužek, R. Derka, G. Adam, and P.L. Knight. Reconstruction of quantum states of spin systems: From quantum bayesian inference to quantum tomography. *Annals of Physics*, 266(2):454 – 496, 1998.

[52] B. Qi, Z. Hou, L. Li, D. Dong, G. Xiang, and G. Guo. Quantum state tomography via linear regression estimation. *Scientific Reports*, 3:3496 EP –, Dec 2013. Article.

[53] K. Banaszek, G. M. D'Ariano, M. G. A. Paris, and M. F. Sacchi. Maximum-likelihood estimation of the density matrix. *Phys. Rev. A*, 61:010304, Dec 1999.

[54] Z. Hradil. Quantum-state estimation. *Phys. Rev. A*, 55:R1561–R1564, Mar 1997.

[55] T. Heinosaari, L. Mazzarella, and M. M. Wolf. Quantum tomography under prior information. *Communications in Mathematical Physics*, 318(2):355–374, 2013.

[56] A. Kalev, R. L. Kosut, and I. H. Deutsch. Quantum tomography protocols with positivity are compressed sensing protocols. *Npj Quantum Information*, 1:15018 EP –, Dec 2015. Article.

[57] D. Gross, Y. K. Liu, S. T. Flammia, S. Becker, and J. Eisert. Quantum state tomography via compressed sensing. *Phys. Rev. Lett.*, 105:150401, Oct 2010.

[58] E. J. Candes, J. Romberg, and T. Tao. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *IEEE Transactions on Information Theory*, 52(2):489–509, Feb 2006.

[59] D. L. Donoho. Compressed sensing. *IEEE Transactions on Information Theory*, 52(4):1289–1306, April 2006.

[60] E. J. Candes and M. B. Wakin. An introduction to compressive sampling. *IEEE Signal Processing Magazine*, 25(2):21–30, March 2008.

[61] M. Fazel. *Matrix rank minimization with applications*. PhD thesis, Stanford University, 2002.

[62] S. T. Flammia, Gross. D., Liu. Y. K., and Eisert J. Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators. *New Journal of Physics*, 14(9):095022, 2012.

[63] Y. K. Liu. Universal low-rank matrix recovery from pauli measurements. In J. Shawe-taylor, R.s. Zemel, P. Bartlett, F.c.n. Pereira, and K.q. Weinberger, editors, *Advances in Neural Information Processing Systems 24*, pages 1638–1646. 2011.

[64] W. Liu, T. Zhang, J. Y. Liu, P. X. Chen, and J. M. Yuan. Experimental quantum state tomography via compressed sampling. *Phys. Rev. Lett.*, 108:170403, Apr 2012.

[65] C. A. Riofrio, D. Gross, S. T. Flammia, T. Monz, D. Nigg, R. Blatt, and J. Eisert. Experimental quantum compressed sensing for a seven-qubit system. *arXiv:1608.02263*.

[66] M. Tomasin, E. Mantoan, J. Jogenfors, G. Vallone, J. Larsson, and P. Villoresi. High-visibility time-bin entanglement for testing chained bell inequalities. *arXiv:1612.03602*.

[67] E. Candes and T. Tao. The dantzig selector: Statistical estimation when p is much larger than n. *Ann. Statist.*, 35(6):2313–2351, 12 2007.

[68] M. A. T. Figueiredo, R. D. Nowak, and S. J. Wright. Gradient projection for sparse reconstruction: Application to compressed sensing and other inverse problems. Technical report, IEEE Journal of Selected Topics in Signal Processing, 2007.

[69] F. Tonolini, S. Chan, M. Agnew, A. Lindsay, and J. Leach. Reconstructing high-dimensional two-photon entangled states via compressive sensing. *Scientific Reports*, 4:6542 EP –, Oct 2014. Article.

[70] Sdpt3, www.math.nus.edu.sg/ mattohkc/sdpt3.html.

[71] Cvx, cvxr.com.

[72] A. Ling, A. Lamas-Linares, and C. Kurtsiefer. Absolute emission rates of spontaneous parametric down-conversion into single transverse gaussian modes. *Phys. Rev. A*, 77:043834, Apr 2008.

[73] Devin Hugh Smith. An ultrafast source of polarization entangled photon pairs based on a sagnac interferometer, 2009.

[74] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

[75] J. D. Franson. Bell inequality for position and time. *Phys. Rev. Lett.*, 62:2205–2208, May 1989.

[76] J. D. Franson. Inconsistency of local realistic descriptions of two-photon interferometer experiments. *Phys. Rev. A*, 61:012105, Dec 1999.

[77] S. Aerts, P. Kwiat, J. Larsson, and M. Z˙ukowski. Two-photon franson-type experiments and local realism. *Phys. Rev. Lett.*, 83:2872–2875, Oct 1999.

[78] J. Larsson and R. D. Gill. Bell's inequality and the coincidence-time loophole. *EPL (Europhysics Letters)*, 67(5):707, 2004.

[79] J. Larsson. Loopholes in bell inequality tests of local realism. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424003, 2014.

[80] G. Lima, G. Vallone, A. Chiuri, A. Cabello, and P. Mataloni. Experimental bell-inequality violation without the postselection loophole. *Phys. Rev. A*, 81:040101, Apr 2010.

[81] A. Cabello, A. Rossi, G. Vallone, F. De Martini, and P. Mataloni. Proposed bell experiment with genuine energy-time entanglement. *Phys. Rev. Lett.*, 102:040401, Jan 2009.

[82] L. De Caro and A. Garuccio. Reliability of bell-inequality measurements using polarization correlations in parametric-down-conversion photon sources. *Phys. Rev. A*, 50:R2803–R2805, Oct 1994.

[83] G. Carvacho, J. Cariñe, G. Saavedra, Á. Cuevas, J. Fuenzalida, F. Toledo, M. Figueroa, A. Cabello, J. Larsson, P. Mataloni, G. Lima, and G. B. Xavier. Postselection-loophole-free bell test over an installed optical fiber network. *Phys. Rev. Lett.*, 115:030503, Jul 2015.

[84] S. Aerts, P. Kwiat, and M. Zukowski. Two-Photon Franson-Type Experiments and Local Realism 4, § ˙. pages 1–4, 1999.

[85] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, Oct 1970.

[86] J. Jogenfors and J. Larsson. Energy-time entanglement, elements of reality, and local realism. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424032, 2014.

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

[88] G. Vallone, I. Gianani, E. B. Inostroza, C. Saavedra, G. Lima, A. Cabello, and P. Mataloni. Testing hardy's nonlocality proof with genuine energy-time entanglement. *Phys. Rev. A*, 83:042105, Apr 2011.

[89] D. Boschi, S. Branca, F. De Martini, and L. Hardy. Ladder proof of nonlocality without inequalities: Theoretical and experimental results. *Phys. Rev. Lett.*, 79:2755–2758, Oct 1997.

[90] C. Holloway, E. Meyer-Scott, C. Erven, and T. Jennewein. Quantum entanglement distribution with 810 nm photons through active telecommunication fibers. *Opt. Express*, 19(21):20597–20603, Oct 2011.

[91] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X*, 2:041010, Nov 2012.

[92] N. Hosseinidehaj and R. Malaney. Gaussian entanglement distribution via satellite. *Phys. Rev. A*, 91:022304, Feb 2015.

[93] W. Thacker and A. Gupta. Quantum controlled error-correction teleportation (qcect) scheme for satellite control and communication. *arXiv:1512.00139*, Dec 2015.

[94] F. Gerlin, N. Laurenti, G. Naletto, G. Vallone, P. Villoresi, L. Bonino, S. Mottini, and Z. Sodnik. Design optimization for quantum communications in a gnss intersatellite network. In *Localization and GNSS (ICL-GNSS), 2013 International Conference on*, pages 1–6, June 2013.

[95] Elizabeth Gibney. Chinese satellite is one giant step for the quantum internet, 2016.

[96] K. Günthner and et al. Quantum-limited measurements of optical signals from a geostationary satellite. *arXiv:1608.03511*, Aug 2016.

[97] 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*, 10(3):033038, 2008.

[98] C Bonato, A Tomaello, V Da Deppo, G Naletto, and P Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):45017, 2009.

[99] 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. *Phys. Rev. Lett.*, 109:200502, Nov 2012.

[100] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi. Experimental satellite quantum communications. *Phys. Rev. Lett.*, 115:040502, Jul 2015.

[101] G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, and P. Villoresi. Interference at the single photon level along satellite-ground channels. *Phys. Rev. Lett.*, 116:253601, Jun 2016.

[102] G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, and P. Villoresi. Supplemental material:interference at the single photon level along satellite-ground channels. *Phys. Rev. Lett.*, 116:253601, Jun 2016.

[103] Timothy C. Ralph Hans-A. Bachor. *A Guide to Experiments in Quantum Optics, 2nd, Revised and Enlarged Edition*. Wiley, 2004.

[104] j. Degnan. *Geodyn. Ser.*, 25(233), 1993.

[105] D Holste, I Große, and H Herzel. Bayes' estimators of generalized entropies. *Journal of Physics A: Mathematical and General*, 31(11):2551, 1998.

[106] R. Konig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, Sept 2009.

[107] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106:110506, Mar 2011.

[108] J. M. Renes and J. Boileau. Conjectured strong complementary information tradeoff. *Phys. Rev. Lett.*, 103:020402, Jul 2009.

[109] M. Berta, M. Christandl, R. Colbeck, J. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nat Phys*, 6(9):659–662, Sep 2010.

[110] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, Apr 2010.

[111] C. Dhara, G.e Prettico, and A. Acín. Maximal quantum randomness in bell tests. *Phys. Rev. A*, 88:052116, Nov 2013.

[112] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[113] U. Vazirani and T. Vidick. Certifiable quantum dice. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 370(1971):3432–3448, 2012.

[114] S. Pironio and S. Massar. Security of practical private randomness generation. *Phys. Rev. A*, 87:012336, Jan 2013.

[115] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín. Full randomness from arbitrarily deterministic events. *Nature Communications*, 4:2654 EP –, Oct 2013. Article.

[116] R. Colbeck and R. Renner. Free randomness can be amplified. *Nat Phys*, 8(6):450–453, Jun 2012.

[117] Garcia-Escartin J.C. Herrero-Collantes M. Quantum random number generators. *arXiv:1604.03304*.

[118] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang. Quantum random number generation. *Npj Quantum Information*, 2:16021 EP –, Jun 2016. Review Article.

[119] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A*, 90:052327, Nov 2014.

[120] M Peev, C Pacher, R Alléaume, C Barreiro, J Bouda, W Boxleitner, T Debuisschert, E Diamanti, M Dianati, J F Dynes, S Fasel, S Fossier, M Fürst, J-D Gautier, O Gay, N Gisin, P Grangier, A Happe, Y Hasani, M Hentschel, H Hübel, G Humer, T Länger, M Legré, R Lieger, J Lodewyck, T Lorünser, N Lütkenhaus, A Marhold, T Matyus, O Maurhart, L Monat, S Nauerth, J-B Page, A Poppe, E Querasser, G Ribordy, S Robyr, L Salvail, A W Sharpe, A J Shields, D Stucki, M Suda, C Tamas, T Themel, R T Thew, Y Thoma, A Treiber, P Trinkler, R Tualle-Brouri, F Vannel, N Walenta, H Weier, H Weinfurter, I Wimberger, Z L Yuan, H Zbinden, and A Zeilinger. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[121] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z. Han, and G. Guo. Field experiment on a robust hierarchical metropolitan quantum cryptography network. *Chinese Science Bulletin*, 54(17):2991–2997, 2009.

[122] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011.

[123] D Stucki, M Legré, F Buntschu, B Clausen, N Felber, N Gisin, L Henzen, P Junod, G Litzistorf, P Monbaron, L Monat, J-B Page, D Perroud, G Ribordy, A Rochas, S Robyr, J Tavares, R Thew, P Trinkler, S Ventura, R Voirol, N Walenta, and H Zbinden. Long-term performance of the swissquantum quantum key distribution network in a field environment. *New Journal of Physics*, 13(12):123001, 2011.

[124] Raffaelli Francesco. Quantum communications with hyper-entangled states between indipendent terminals, 2014.

[125] Manton Elia. Entangled states on one or more degrees of freedom and their application to fundamental physics, 2015.