Universidade de Aveiro Departamento de Física
2016

Álvaro José
Caseiro de Almeida

Comunicações Quânticas em Fibras Óticas

Quantum Communications in Optical Fibers

Universidade de Aveiro Departamento de Física
2016

Álvaro José Caseiro de Almeida

Comunicações Quânticas em Fibras Óticas

Quantum Communications in Optical Fibers

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Engenharia Física, realizada sob a orientação científica do Doutor Armando Humberto Moreira Nolasco Pinto, Professor Associado do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, e coorientação do Doutor Paulo Sérgio de Brito André, Professor Associado do Departamento de Engenharia Eletrotécnica e de Computadores do Instituto Superior Técnico da Universidade de Lisboa.

Apoio financeiro da Fundação para a Ciência e a Tecnologia através da bolsa de investigação SFRH/BD/79482/2011 e POPH/FSE.

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

POPH
QUALIFICAR É CRESCER.

QREN
QUADRO DE REFERÊNCIA ESTRATÉGICO NACIONAL
PORTUGAL 2007.2013

GOVERNO DA REPÚBLICA PORTUGUESA

UNIÃO EUROPEIA
Fundo Social Europeu

o júri / the jury

presidente / president

Doutor Nuno Miguel Gonçalves Borges de Carvalho
Professor Catedrático do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro

vogais / examiners committee

Doutor João de Lemos Pinto
Professor Catedrático do Departamento de Física da Universidade de Aveiro

Doutor Gonçalo Nuno Marmelo Foito Figueira
Professor Auxiliar do Departamento de Física do Instituto Superior Técnico da Universidade de Lisboa

Doutor José Maria Longras Figueiredo
Professor Auxiliar do Departamento de Física da Faculdade de Ciências e Tecnologia da Universidade do Algarve

Doutor Helder Manuel Paiva Rebelo Cerejo Crespo
Professor Auxilar do Departamento de Física e Astronomia da Faculdade de Ciências da Universidade do Porto

Doutor Armando Humberto Moreira Nolasco Pinto
Professor Associado do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro (Orientador)

agradecimentos / acknowledgments

Para que o trabalho apresentado nesta tese tivesse sido possível foi necessário o contributo de várias pessoas e entidades a quem gostaria de agradecer. O meu primeiro agradecimento vai para o meu orientador, o professor Armando Nolasco Pinto, pela orientação científica que me deu ao longo de todo o doutoramento. Agradeço-lhe as inúmeras discussões e sugestões para a melhoria do trabalho, bem como a exigência e o acompanhamento contínuos. Ao meu coorientador, o professor Paulo André, agradeço a disponibilidade que sempre demonstrou, bem como todo o acompanhamento, sempre que dele necessitei. Aos meus colegas Nuno Silva, Nelson Muga e Gil Fernandes, que trabalharam quase diariamente comigo, agradeço por todas as discussões, pelas sugestões e por todo o apoio que me deram ao longo destes anos. Foram incansáveis. Ao Eng. João Prata agradeço toda a ajuda prestada nas experiências laboratoriais, sempre que esta lhe foi solicitada. Sem dúvida que deu um contributo extremamente importante. Agradeço ainda de forma particularmente especial ao meu colega Luís Martins, que mesmo após deixarmos de ser colegas de trabalho, sempre se mostrou disponível para inúmeras discussões e sugestões para a melhoria do meu trabalho, mantendo igualmente a colaboração científica. Ao Nelson Filipe agradeço também as inúmeras sugestões feitas, principalmente ao nível da componente de simulação do trabalho. Também os meus colegas Fernando Guiomar, André Albuquerque, Nikola Paunković, Ricardo Loura, Aleksandar Stojanovic, Daniel Macedo, Steven Carneiro, Luís Seabra, João Gonçalves e Vanessa Duarte merecem o meu agradecimento pela colaboração a vários níveis. Ao professor Rubens Viana Ramos e aos doutores Guilherme Barreto Xavier, Andreas Poppe e Rupesh Kumar Subramanian, agradeço todas as sugestões e discussões feitas ao longo deste percurso. Agradeço ainda a todos os meus colegas do Grupo de Comunicações Óticas do Instituto de Telecomunicações por todos os momentos que passámos em conjunto e aos muitos amigos que fiz em Aveiro. Quero agradecer ainda à Universidade de Aveiro pela formação que me deu e igualmente ao Instituto de Telecomunicações por me ter disponibilizado excelentes condições para a realização do meu trabalho, a todos os níveis. Agradeço também à Fundação para a Ciência e a Tecnologia pelo suporte financeiro fundamental que me concedeu, através da bolsa de doutoramento SFRH/BD/79482/2011 e, ainda, aos projetos de investigação QuantTel (Ref.: IT/LA), QuantPrivTel (Ref.: PTDC/EEA-TEL/103402/2008), P-Quantum (Ref.: PEst-OE/EEI/LA0008/2011), SCCQ (Ref.: Ação Integrada E91/12) e CV-Quantum (PEst-OE/EEI/LA0008/2013). Finalmente, quero agradecer à Luciana por todo o apoio e, à minha família, por tudo.

Palavras Chave

Fibra ótica, estatística dos fotões, mistura de quatro ondas, detetor de fotões únicos, polarização, comunicação quântica.

Resumo

Nesta tese começou-se por propor a realização de uma fonte de fotões probabilística baseada no processo estimulado de mistura de quatro ondas (FWM). Implementou-se essa fonte no laboratório e caracterizou-se experimentalmente a sua distribuição estatística. Depois, estudou-se experimentalmente o impacto do processo estimulado de FWM num sinal quântico que se propaga na mesma fibra ótica. Por fim, foi verificada experimentalmente a violação da desigualdade de Clauser-Horne-Shimony-Holt (CHSH) usando pares de fotões entrelaçados, que foram obtidos a partir do processo espontâneo de FWM num ciclo de Sagnac.

Estudou-se a evolução da taxa de erro de bits quânticos (QBER) num sistema sem controlo de polarização, quando este grau de liberdade é usado para codificar a informação. Verificou-se que a QBER aumenta com o comprimento da fibra de transmissão. Verificou-se ainda que o aumento da QBER era devido às variações aleatórias da polarização dos fotões. Derivou-se um modelo para a estimativa rigorosa da QBER e desenvolveu-se um método automático de compensação das rotações aleatórias da polarização. O método foi validado numericamente e experimentalmente, num sistema de transmissão com 40 km, verificando-se que consegue compensar as rotações que os fotões sofrem durante a sua propagação em fibras óticas.

Finalmente, implementou-se um protocolo de compromisso quântico entre duas entidades não confiáveis. Na codificação foram usados dois estados de polarização (SOPs) não ortogonais. Como canal quântico entre as duas entidades foi primeiro considerado que o emissor e o recetor se encontravam lado a lado, depois que estes estavam separados por 8 km e finalmente que se encontravam a 16 km um do outro. A implementação do protocolo foi feita com uma taxa de sucesso nas medidas superior a 93%, muito acima do limite teórico mínimo de 85%. Implementou-se ainda a melhor estratégia para que o compromisso pudesse ser falseado, tendo sido confirmada experimentalmente a sua segurança com uma confiança de 7 desvios padrão.

Keywords Optical fiber, photon statistics, four-wave mixing, single-photon detector, polarization, quantum communication.

Abstract

This thesis begins by proposing the implementation of a probabilistic photon source based on the stimulated four-wave mixing (FWM) process. This source was implemented experimentally and characterized in terms of its statistical distribution. Next, the impact of the stimulated FWM process in a co-propagating quantum signal was studied experimentally. Finally, the violation of Clauser-Horne-Shimony-Holt (CHSH) inequality was experimentally verified using polarization-entangled photon pairs, which were obtained from the spontaneous FWM process in a Sagnac loop.

The experimental evolution of the quantum-bit error rate (QBER) in a system without control of polarization, using this degree of freedom to encode information, was studied. It was found out that the QBER increases with the length of the transmission fiber. It was also verified that the increase in the QBER was due to the random rotation of photon's polarization. A model for the rigorous estimation of the QBER was derived and developed an automatic method to compensate the random rotations of polarization. The method was validated numerically and experimentally, in a transmission system with 40 km, showing that it can compensate for the rotations that photons suffer during propagation in optical fibers.

Finally, a quantum bit commitment (QBC) protocol between two untrusted entities was implemented. The encoding was performed using two nonorthogonal states of polarization (SOPs). As quantum channel between the two entities, it was first assumed that the transmitter and the receiver were side by side, and after that, they were separated by 8 km and finally, that they were 16 km from each other. The implementation of the protocol was performed with a success rate in measurements exceeding 93%, well above the theoretical security limit of 85%. The best strategy for deceiving the commitment was also implemented, and its security experimentally confirmed with a confidence of 7 standard deviations.

“*O tempo dura bastante para aqueles que sabem aproveitá-lo.*”

Leonardo Da Vinci

Aos meus pais.

Contents

List of Acronyms

Notation	Description
AOM	Acousto-Optic Modulator
AWG	Arrayed Waveguide Grating
B92	Bennett 1992
BB84	Bennett-Brassard 1984
BS	Beam-Splitter
CHSH	Clauser-Horne-Shimony-Holt
CW	Continuous-Wave
DARPA	Defense Advanced Research Projects Agency
DSF	Dispersion-Shifted Fiber
DWDM	Dense Wavelength-Division Multiplexing
ECL	External Cavity Laser
EDFA	Erbium Doped Fiber Amplifier
EM	Expectation-Maximization
EPC	Electronic Polarization Controller
EPR	Einstein-Podolsky-Rosen
FPGA	Field-Programmable Gate Array
FWHM	Full-Width at Half Maximum
GD	Group Delay
HNLF	Highly-Nonlinear Fiber
HWP	Half-Wave Plate
IEEE	Institute of Electrical and Electronics Engineers
LP	Linear Polarizer
LWPF	Low-Water-Peak Fiber
MC	Microcontroller
MDI	Measurement-Device-Independent
MLE	Maximum-Likelihood Estimation

MUX	Multiplexer
MZM	Mach-Zehnder Modulator
NFAD	Negative-Feedback Avalanche Diode
OC	Optical Coupler
ONA	Optical Network Analyzer
OS	Optical Switch
OSA	Optical Spectrum Analyzer
PBS	Polarization-Beam Splitter
PC	Polarization Controller
PDC	Parametric Down-Conversion
PDL	Polarization-Dependent Loss
PMD	Polarization-Mode Dispersion
PNS	Photon-Number Splitting
PRBS	Pseudo-Random Bit Sequence
PSCF	Pure Silica-Core Fiber
QBC	Quantum Bit Commitment
QCM	Quantum-Cloning Machine
QBER	Quantum-Bit Error Rate
QKD	Quantum Key Distribution
QND	Quantum Non-Demolition
QRNG	Quantum Random Number Generator
QWP	Quarter-Wave Plate
RLP	Rotatable Linear Polarizer
SECOQC	Secure Communication based on Quantum Cryptography
SSMF	Standard Single-Mode Fiber
SNSPD	Superconducting Nanowire Single-Photon Detector
SOP	State of Polarization
SPAD	Single-Photon Avalanche Detector
SRATE	Success Rate
TDM	Time-Division Multiplexing
TLS	Tunable Laser Source
VOA	Variable Optical Attenuator
WDM	Wavelength-Division Multiplexing
ZDW	Zero-Dispersion Wavelength

List of Figures

List of Tables

List of Symbols

Symbol	**Designation**
$+$	Rectilinear basis
$\times$	Diagonal basis
$\|0\rangle$	Quantum state of bit 0
$\|0^{\perp}\rangle$	Quantum state orthogonal to $\|0\rangle$
$\|\tilde{0}\rangle$	Quantum state at an angle $-\pi/8$ from $\|0\rangle$
$\|1\rangle$	Quantum state of bit 1
$\|1^{\perp}\rangle$	Quantum state orthogonal to $\|1\rangle$
$\|\tilde{1}\rangle$	Quantum state at an angle $-\pi/8$ from $\|1\rangle$
$\|-45\rangle$	Diagonal quantum state of bit 0
$\|+45\rangle$	Diagonal quantum state of bit 1
$\|\psi\rangle$	Vector of a general quantum state (also known as *ket* in Dirac notation)
$\langle\psi\|$	Vector of a general quantum state (also known as *bra* in Dirac notation)
$\langle\psi_1\|\psi_2\rangle$	Inner product between vectors $\|\psi_1\rangle$ and $\|\psi_2\rangle$
$\|\psi_1\rangle\|\psi_2\rangle$	Tensor product of $\|\psi_1\rangle$ and $\|\psi_2\rangle$
$\langle\psi_1\|s\|\psi_2\rangle$	Inner product between vectors $\|\psi_1\rangle$ and $s\|\psi_2\rangle$
$\mathbb{I}$	Identity matrix
i, j, k	Natural numbers ($\mathbb{N}^0$)
α	Confidence level
α_{ϖ}	Attenuation in a VOA
α_{f}	Fiber attenuation coefficient
γ	Nonlinear coefficient of an optical fiber
δ	Deviation
$\Delta\beta$	Phase-matching condition
$\Delta\mathrm{B}$	Conditional branch
ΔS_A	Standard deviation of the state S_A
ΔS_B	Standard deviation of the state S_B
$\mathcal{E}_{\mathrm{d}}$	Optical contribution to noise
η	Efficiency of photon generation
η_{ν}	Combined efficiencies of a VOA and a SPAD
η_{B}	Total losses in the detection side
η_{D}	Quantum efficiency of a SPAD

η_{F}	Total efficiency of an optical fiber
η_{ϖ}	Efficiency of a VOA
$\theta, \phi, \phi_0, \varphi$	Rotation angles
κ	Security parameter
λ	Hidden variable
λ_0	Zero-dispersion wavelength
λ_{i}	Idler wavelength
λ_{p}	Pump wavelength
λ_{s}	Signal wavelength
Λ	Probability space
μ	Average number of photons per pulse
μ_0	Mean value of a binomial distribution when measuring $\|0\rangle$
μ_1	Mean value of a binomial distribution when measuring $\|1\rangle$
μ_{coh}	Average number of coherent photons
μ_{th}	Average number of thermal photons
ν	Carrier frequency
$\hat{\rho}$	General mixed state
ρ_{n}	Probability to detect n photons
σ	Standard deviation of S in relation to 2
σ_0	Standard deviation when measuring $\|0\rangle$
σ_1	Standard deviation when measuring $\|1\rangle$
σ_0^2	Variance of a binomial distribution when measuring $\|0\rangle$
σ_1^2	Variance of a binomial distribution when measuring $\|1\rangle$
σ_S	Standard deviation of S
τ_{g}	Duration of the gate window in a SPAD
$\|\psi_\phi\rangle$	Input quantum state
ω_{i}	Idler frequency
ω_{p}	Pump frequency
ω_{s}	Signal frequency
$A(a, \lambda)$	Expected value of system A
a	Parameter of system A
a_0, a_1	Complex numbers
$\|a_0\|^2, P(0)$	Probability of finding a qubit in state $\|0\rangle$
$\|a_1\|^2, P(1)$	Probability of finding a qubit in state $\|1\rangle$
$A_{\nu,n}$	No-click efficiency
A_{w}	Amplitude
$\mathcal{B}_s$	Orthonormal basis
$B(a, \lambda)$	Expected value of system B
b	Parameter of system B
$\|b\rangle$	Blank quantum state
C	Coincidence counts
C_0	Background coincidence counts
C_-	Minimum number of counts
C_+	Maximum number of counts

$\hat{C}_0$	Commitment basis to 0
$\hat{C}_1$	Commitment basis to 1
$\hat{C}_{\text{ch}}$	Commitment to cheating observable
C_{D}	Single counts in a SPAD
c	Speed of light in vacuum
D_{p}	Polarization-mode dispersion parameter
d	Precision in the estimation of the QBER
d_{r}	Relative precision of the estimated QBER
E	Correlation function between two quantum systems
e_{r}	Number of errors
f_ν	Experimental frequencies of the no-click events for the efficiency η_ν
f_{rep}	Repetition rate
G	Fidelity
G_{P}	Fidelity when using a Poissonian distribution
G_{th}	Fidelity when using a thermal distribution
$g^{(2)}(0)$	Second-order coherence function
$\|H\rangle$	Horizontal quantum state
$\|H\rangle_{\text{s}}\|H\rangle_{\text{i}}$	Horizontal signal-idler photons pair
L	Fiber length
L_{eff}	Effective fiber length
$L_n^a(z)$	Generalized Laguerre polynomials
M	Number of thermal states
M_{0°	Matrix of a wave plate set a 0°
M_{45°	Matrix of a wave plate set a 45°
M_{EPC}	Matrix of an electronic polarization controller
M_{F}	Rotation matrix of a SOP inside an optical fiber
N_{θ_0}	Number of 0's detected when setting θ_0
N_{θ_1}	Number of 1's detected when setting θ_1
N_{F}	Number of frames
$N_{\text{F}}^{\text{Max}}$	Maximum number of control qubits in one frame
N_{i}	Number of iterations
N_{r}	Number of control qubits expected to be received
N_{r}^*	Number of control qubits effectively received
N_{s}	Number of qubits sent
n	Number of photons
$n(s)$	Total number of photons detected when state $\|s\rangle$ was sent
$n(j\|s)$	Number of results j measured when sending state $\|s\rangle$
n_{c}	Number of control qubits in one frame
$n_{\text{c}}(0)$	Number of control qubits in the first frame
n_{ch}	Total number of photons detected when measuring in $\hat{C}_{\text{ch}}$
n_{d}	Number of data qubits in one frame
$n_{\text{d}}(0)$	Number of data qubits in the first frame
p_0	Probability of occurrence of white-noise when receiving a 0
p_1	Probability of occurrence of white-noise when receiving a 1

p_ν^{off}	No-click probability
p_{ch}	Conditional probability when measuring in $\hat{C}_{\text{ch}}$
P_{d}	Probability of detection
P_{dc}	Probability to have dark counts in a SPAD
P_{click}	Probability of click in a single-photon detector
P_{i}	Idler power
$P_{N_{\text{r}}}(e_{\text{r}})$	Probability to have e_{r} errors in N_{r} detections
P_{P}	Photon statistics following a Poissonian distribution
$P_{\text{p}}(0)$	Initial pump power
$P_{\text{Q}}(0)$	Initial quantum signal power
$P_{\text{s}}(0)$	Initial signal power
P_{t}	Probability of transmission of a quantum state through a LP
P_{th}	Photon statistics following a thermal distribution
$p(\lambda)$	Probability distribution of the hidden variable
Q	Mandel parameter
QBER	Quantum-bit error rate
$\widehat{\text{QBER}}$	Estimated QBER
$\widehat{\text{QBER}}_{(0)}$	Initial guess for the estimated QBER
QBER^{opt}	Optical QBER
$\text{QBER}^{\text{non-opt}}$	Non-optical QBER
QBER_{LB}	Lower bound of the QBER
QBER_{UB}	Upper bound of the QBER
QBER_{Min}	Minimum value set for the QBER
QBER_{Max}	Maximum value set for the QBER
$q(j\|s)$	Statistics of results j measured when the state $\|s\rangle$ is sent
R^2	Coefficient of determination
$R_{\text{click}}^{\text{c}}$	Rate of control clicks
S	Bell's entropy parameter
S_1	Small step size in a wave plate
S_2	Medium step size in a wave plate
$S(\lambda_0)$	Dispersion slope at the ZDW
S^{max}	Maximum value for Bell's entropy parameter
S_A, S_B	Noncommuting quantum states
SRATE	Success rate
$\text{SRATE}^{\text{non-opt}}$	Non-optical success rate
$\text{SRATE}^{\text{opt}}$	Optical success rate
$\|s\rangle$	Quantum state
$\hat{s}_{\text{f}}$	Stokes vector of an output quantum state
$\hat{s}_{\text{i}}$	Stokes vector of an input quantum state
$\|T_\theta\rangle$	Transmission state of a LP
t_0	Drift time of the index difference between the fast and slow axes
t_{d}	Drift time of polarization
t_{r}	Time to transmit N_{r} qubits
V	Visibility

$\lvert V\rangle$	Vertical quantum state
$\lvert V\rangle_{\mathrm{s}}\lvert V\rangle_{\mathrm{i}}$	Vertical signal-idler photons pair
Var	Variance
V_{Max}	Maximum voltage of a wave plate
V_{Mean}	Mean voltage of a wave plate
V_{Min}	Minimum voltage of a wave plate
$z_{\alpha/2}$	$100(1-\frac{\alpha}{2})$th percentile of a standard normal distribution

Chapter 1

Introduction

The Internet traffic is entering the zettabyte[1] era, with 1.1 zettabytes of information expected to be transmitted in 2016 [2]. This exponential growth, is mainly due to society's increasing dependence in telecommunication networks. Moreover, the need for security is also increasing due to a growing number of services in banking [3], cloud computing [4] or military [5], making this field one of the most relevant topics to research. Security was identified as one of the strategic areas for European Union's H2020 program, supporting projects in information and communication technologies [6].

Current cryptographic protocols like the Rivest-Shamir-Adleman (RSA) scheme [7] are based on the low computational capacity to solve complex mathematical problems, requiring a large number of bits to maintain security [8]. However, due to the increasing capacity in the processing power and the apparent rise of quantum computers [9–14], which are under research to become universal [15–20], the security of classical cryptographic protocols can be compromised [21]. Within this scope, quantum cryptography appears as a possible solution to provide an increased security for the future communication systems [22, 23]. One advantage of quantum cryptography, and in particular of quantum key distribution (QKD), is allowing to refresh the key at a milliseconds rate [24–26]. More important is the fact that its security is guaranteed by the laws of quantum mechanics, being impossible to make copies of data encoded in a quantum state [27, 28]. The detection of an eavesdropper is also possible since the act of measuring a quantum state changes it, thus revealing his presence [22].

Despite the importance of QKD, quantum cryptography is part of a broader field called quantum communication, which includes for example, quantum teleportation [29, 30], quantum computation [20, 31], quantum communication complexity [32, 33], quan-

[1] Eric Schmidt, former Google CEO, said at the Techonomy conference in Lake Tahoe, CA, in 2010, that between the dawn of civilization and 2003 we created 5 exabytes of information, the same amount that we have created since then every two days and which is increasing [1].

tum super dense coding [34, 35], quantum error correction [36, 37] or quantum bit commitment [38, 39]. Due to this broad range of research topics and applications, quantum communications require the study and development of new and enabling technologies. Ultimately, the aim is to develop solutions that will benefit people and help everyone having higher privacy in communications or storage of information [3, 4, 40, 41].

1.1 Objectives

With this thesis we aim to develop new technologies for quantum communications through the study of the generation, transmission and detection of single and entangled photons. The work will be performed under the scope of the following objectives:

1. Study of alternative methods for the development of novel photon sources to be used in quantum communication applications. We also intend to characterize the statistics of the photon source.

2. Development of quantum communication systems with information encoded in photons' polarization.

3. Implementation of quantum protocols using the developed quantum communication systems.

1.2 Main Contributions

The main achievements reported in this thesis are detailed next:

1. We have implemented experimentally a probabilistic photon source generating few-photons, which is based on the stimulated four-wave mixing (FWM) process in optical fibers [42]. Then, we have characterized experimentally the source statistics [43]. Thereafter, we have studied the impact of the stimulated FWM process on a co-propagating coherent quantum signal in a wavelength-division multiplexed (WDM) lightwave system [43]. Finally, we have implemented experimentally a source of entangled-photon pairs based on the spontaneous FWM process [44]. Using this source, we verified experimentally the violation of Clauser-Horne-Shimony-Holt (CHSH) inequality [44].

2. A theoretical model for the rigorous estimation of the quantum-bit error rate (QBER) in polarization control schemes was derived [45]. A polarization control algorithm was developed and then validated, both numerically and experimentally. It

was found that the method allows an automatic and continuous control of random rotations of photons polarization after transmission through optical fibers.

3. We have implemented experimentally a new quantum bit commitment (QBC) protocol in optical fibers using two nonorthogonal states of polarization [46]. The encoding scheme used the polarization of photons. The protocol allows to establish commitments between two parties which do not know or do not trust each other. The optimal cheating strategy and the security of the protocol were also analyzed.

1.3 Scientific Output

The main achievements from the work resulted in the following publications.

1.3.1 Journal Papers

9. **Álvaro J. Almeida**, Nelson J. Muga, Nuno A. Silva, João M. Prata, Paulo S. André, and Armando N. Pinto, "Continuous control of random polarization rotations for quantum communications", *submitted to IEEE/OSA Journal of Lightwave Technology, Jan., 2016.*

8. **Álvaro J. Almeida**, Aleksandar D. Stojanovic, Nikola Paunković, Ricardo Loura, Nelson J. Muga, Nuno A. Silva, Paulo Mateus, Paulo S. André, and Armando N. Pinto, "Implementation of a two-state quantum bit commitment protocol in optical fibers", *Journal of Optics*, vol. 18, no. 1, p. 015202, Dec., 2015.

7. Luís P. Martins, **Álvaro J. Almeida**, Nuno A. Silva, Paulo S. André, and Armando N. Pinto, "A different way to verify the violation of the WWZB inequality", *The European Physical Journal D*, vol. 68, no. 228, pp. 1–5, Aug., 2014.

6. Ricardo Loura, **Álvaro J. Almeida**, Paulo S. André, Armando N. Pinto, Paulo Mateus, and Nikola Paunković, "Noise and measurement errors in a practical two-state quantum bit commitment protocol", *Physical Review A*, vol. 89, no. 5, p. 052336, May, 2014.

5. Armando N. Pinto, Nuno A. Silva, **Álvaro J. Almeida**, and Nelson J. Muga, "Using quantum technologies to improve fiber optic communication systems", *IEEE Communications Magazine*, vol. 8, no. 51, pp. 42–48, Aug., 2013.

4. Gil M. Fernandes, **Álvaro J. Almeida**, Manfred Niehus, and Armando N. Pinto, "Theoretical analysis of multimodal four-wave mixing in optical microwires", *IEEE/OSA Journal of Lightwave Technology*, vol. 31, no. 2, pp. 195–202, Jan., 2013.

3. Luís P. Martins, **Álvaro J. Almeida**, Paulo S. André, and Armando N. Pinto, "Photon-pair states and violation of CHSH inequality", *Microwave and Optical Technology Letters*, vol. 54, no. 11, pp. 2454–2461, Nov., 2012.

2. **Álvaro J. Almeida**, Nuno A. Silva, Paulo S. André, and Armando N. Pinto, “Four-wave mixing: Photon statistics and the impact on a co-propagating quantum signal”, *Optics Communications*, vol. 285, no. 12, pp. 2956–2960, Jun., 2012.

1. Nuno A. Silva, **Álvaro J. Almeida**, and Armando N. Pinto, “Interference in a quantum channel due to classical four-wave mixing in optical fibers”, *IEEE Journal of Quantum Electronics*, vol. 48, no. 4, pp. 472–479, Apr., 2012.

1.3.2 National and International Conferences

27. **Álvaro J. Almeida**, Nuno A. Silva, Nelson J. Muga, Paulo S. André, and Armando N. Pinto, “Determining the number of bits required for the estimation of the QBER in quantum communication systems”, in *Proc. of 10th Conference on Telecommunications (CONFTELE)*, Aveiro, Portugal, Sep., 2015, pp. 1–4.

26. **Álvaro J. Almeida**, Bruno D. Tibúrcio, Nelson J. Muga, Nuno A. Silva, and Armando N. Pinto, “Comunicações seguras usando a luz”, in *Feira de Ciências “À DESCOBERTA DA LUZ” IYL2015/Portugal*, Viana do Castelo, Portugal, May, 2015.

25. **Álvaro J. Almeida**, Ricardo Loura, Paulo S. André, Armando N. Pinto, Paulo Mateus, and Nikola Paunković, “Noise and measurement errors in a practical two-state quantum bit commitment protocol in optical fibers”, in *Conference on Quantum Cryptography (QCRYPT)*, Paris, France, Sep., 2014, pp. 1–3.

24. **Álvaro J. Almeida**, Luís P. Martins, Paulo S. André, and Armando N. Pinto, “Verification of the violation of WWZB inequality using Werner states”, in *Proc. of International Commission for Optics (ICO-23)*, Santiago de Compostela, Spain, Aug., 2014, pp. 1–6, and *Journal of Physics: Conference Series*, vol. 605, no. 1, p. 012036, Apr., 2015.

23. Armando N. Pinto, Nuno A. Silva, **Álvaro J. Almeida**, and Nelson J. Muga, “Using single photons to improve fiber optic communication systems”, in *Proc. of SPIE 9286, 2nd International Conference on Applications of Optics and Photonics (AOP2014)*, Aveiro, Portugal, vol. 9286, May, 2014, p. 92861B.

22. **Álvaro J. Almeida**, Ricardo Loura, Nikola Paunković, Nuno A. Silva, Nelson J. Muga, Paulo Mateus, Paulo S. André, and Armando N. Pinto, “A brief review on quantum bit commitment”, in *Proc. of SPIE 9286, 2nd International Conference on Applications of Optics and Photonics (AOP2014)*, Aveiro, Portugal, vol. 9286, May, 2014, p. 92861C.

21. **Álvaro J. Almeida**, Nuno A. Silva, Nelson J. Muga, Paulo S. André, and Armando N. Pinto, “Calculation of the number of bits required for the estimation of the bit error ratio”, in *Proc. of SPIE 9286, 2nd International Conference on Applications of Optics and Photonics (AOP2014)*, Aveiro, Portugal, vol. 9286, May, 2014, p. 928607.

20. **Álvaro J. Almeida**, Luís P. Martins, Paulo S. André, and Armando N. Pinto, "Photon-pair states and violation of CHSH inequality", in *Conference on Quantum Cryptography (QCRYPT)*, Waterloo, Canada, Aug., 2013, p. 1.

19. **Álvaro J. Almeida**, Nelson J. Muga, Nuno A. Silva, Aleksandar D. Stojanovic, Paulo S. André, Armando N. Pinto, José M. Mora, and José C. Capmany, "Enabling quantum communications through accurate photons polarization control", in *Proc. of Encontro Ibero-Americano em Óptica and XII Encontro Ibero-Americano sobre Óptica, Lasers e Aplicações (RIAO/OPTILAS)*, Porto, Portugal, Jul., 2013, pp. 1–8.

18. **Álvaro J. Almeida**, Daniel J. Macedo, Nuno A. Silva, Nelson J. Muga, Paulo S. André, and Armando N. Pinto, "Quantum communication using polarization-encoded photons in optical fibers", in *Proc. of 9th Conference on Telecommunications (CONFTELE)*, Castelo Branco, Portugal, May, 2013, pp. 205–208.

17. **Álvaro J. Almeida**, Nuno A. Silva, Paulo S. André, and Armando N. Pinto, "Four-wave mixing: Photon statistics and the impact on a co-propagating quantum signal", in *Conference on Quantum Cryptography (QCRYPT)*, Singapore, Sep., 2012, pp. 1–3.

16. **Álvaro J. Almeida**, Nuno A. Silva, Paulo S. André, and Armando N. Pinto, "Impact of FWM process on the statistics of a co-propagating quantum signal in a WDM light-wave system", in *Proc. of International Conference on Transparent Optical Networks (ICTON)*, Coventry, England, Jul., 2012, pp. 1–4.

15. **Álvaro J. Almeida**, Nuno A. Silva, Paulo S. André, and Armando N. Pinto, "Experimental characterization of the photon statistics of four-wave mixing photon source", in *Proc. of European Conference on Networks and Optical Communications and Conference on Optical Cabling and Infrastructure (NOC/OC&I)*, Vilanova i la Geltrú, Spain, Jun., 2012, pp. 142-147.

14. **Álvaro J. Almeida**, Nelson J. Muga, Nuno A. Silva, Paulo S. André, and Armando N. Pinto, "Long-term time evolution measurements of polarization drift in optical fibers", in *Proc. of Symposium on Enabling Optical Networks and Sensors (SEONS)*, Porto, Portugal, Jun., 2012, pp. 1–4. [**Selected as Best Student Paper on Optical Communications**]

13. Armando N. Pinto, **Álvaro J. Almeida**, Nuno A. Silva, Nelson J. Muga, and Luís P. Martins, "Engineering quantum communication systems", in *Proc. of SPIE 8440, SPIE Photonics Europe*, Brussels, Belgium, vol. 8440, Apr., 2012, p. 84400B.

12. Gil M. Fernandes, **Álvaro J. Almeida**, and Armando N. Pinto, "Nonlinear phase and parametric gain in optical fiber microwires", in *Proc. of Symposium on Enabling Optical Networks (SEON)*, Aveiro, Portugal, Jul., 2011, pp. 1–4.

11. **Álvaro J. Almeida**, Luís P. Martins, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, "Correlated photon-pair generation in a highly nonlinear fiber using spontaneous

FWM”, in *Proc. of Symposium on Enabling Optical Networks (SEON)*, Aveiro, Portugal, Jul., 2011, pp. 1–4.

10. Armando N. Pinto, **Álvaro J. Almeida**, Nuno A. Silva, Nelson J. Muga, and Luís P. Martins, “Optical quantum communications: an experimental approach”, in *Proc. of SPIE 8001, International Conference on Applications of Optics and Photonics (AOP)*, Braga, Portugal, May, 2011, p. 80011M.

9. Nelson J. Muga, **Álvaro J. Almeida**, Mário Ferreira and Armando N. Pinto, “Optimization of polarization control schemes for QKD systems”, in *Proc. of SPIE 8001, International Conference on Applications of Optics and Photonics (AOP)*, Braga, Portugal, May, 2011, p. 80013N.

8. Gil M. Fernandes, **Álvaro J. Almeida**, Manfred Niehus, and Armando N. Pinto, “Measurement of the diameter of an optical fiber microwire using stimulated four-wave mixing”, in *Proc. of SPIE 8001, International Conference on Applications of Optics and Photonics (AOP)*, Braga, Portugal, May, 2011, pp. 1–7.

7. **Álvaro J. Almeida**, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, “Single-photon source using stimulated FWM in optical fibers for quantum communication”, in *Proc. of SPIE 8001, International Conference on Applications of Optics and Photonics (AOP)*, Braga, Portugal, May, 2011, p. 80013W.

6. Nelson J. Muga, **Álvaro J. Almeida**, Mário Ferreira, and Armando N. Pinto, “Critical issues in polarization encoded quantum key distribution systems”, in *Proc. of IEEE, International Conference on Computer as a Tool and 8th Conference on Telecommunications (EUROCON&CONFTELE)*, Lisbon, Portugal, Apr., 2011, pp. 1–4.

5. Nuno A. Silva, **Álvaro J. Almeida**, and Armando N. Pinto, “Statistical characterization of a single-photon source based on stimulated FWM in optical fibers”, in *Proc. of IEEE, International Conference on Computer as a Tool and 8th Conference on Telecommunications (EUROCON&CONFTELE)*, Lisbon, Portugal, Apr., 2011, pp. 1–4.

4. **Álvaro J. Almeida**, Steven R. Carneiro, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, “Polarization-entangled photon pairs using spontaneous four-wave mixing in a fiber loop”, in *Proc. of IEEE, International Conference on Computer as a Tool and 8th Conference on Telecommunications (EUROCON&CONFTELE)*, Lisboa, Portugal, Apr., 2011, pp. 1–4.

3. **Álvaro J. Almeida**, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, “Single-photon source based on FWM with adjustable linear SOP”, *Revista do Departamento de Electrónica, Telecomunicações e Informática*, Universidade de Aveiro, vol. 5, no. 2, Jun., 2010, pp. 151–155.

2. **Álvaro J. Almeida**, Steven R. Carneiro, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, "Time coincidence of entangled photon pairs using spontaneous four-wave mixing in a fiber loop", in *Proc. of Symposium on Enabling Optical Networks (SEON)*, Porto, Portugal, Jun., 2010, pp. 1–2.

1. **Álvaro J. Almeida**, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto, "Fiber-optical communication system using polarization-encoding photons", in *Proc. of European Conference on Networks and Optical Communications and Conference on Optical Cabling and Infrastructure (NOC/OC&I)*, Faro, Portugal, Jun., 2010, pp. 127–132.

1.3.3 Patents

1. Armando N. Pinto, **Álvaro J. Almeida**, Nelson J. Muga, Nuno A. Silva, Paulo S. André, and João M. Prata, "Sistema de Comunicações Quânticas e Método de Operação", 201510000099867, December, 30, 2015.

1.4 Outline

This thesis is divided in six chapters and is organized as follows:

- Chapter 2 presents the state-of-the-art of quantum communications under the scope of the present work, along with the basic principles necessary to understand the physical concepts in this thesis and the encoding and decoding principles.
- Chapter 3 describes the implementation of a few-photons source based on stimulated FWM process and its photon number distribution. The impact of the FWM process on a co-propagating quantum channel is also studied. The spontaneous FWM process is used to generate entangled-photon pairs to verify the violation of CHSH inequality.
- Chapter 4 presents a method to control polarization of photons in real time through the estimation of the QBER of the system. The theoretical model for the estimation of the QBER is derived and the method is validated numerically and experimentally.
- Chapter 5 shows the implementation of a quantum bit commitment protocol using two nonorthogonal states. The noise and measurement errors in its practical implementation are evaluated and its security assessed. An experimental validation of the protocol is presented.
- Chapter 6 summarizes the main results of this thesis and presents suggestions for future work.

This thesis also includes a list of acronyms, a list of figures, a list of tables and a list of symbols.

References

[1] M. Kirkpatrick, "Google CEO Schmidt: "People Aren't Ready for the Technology Revolution"," August 2010, [Online; posted 04-August-2010].

[2] Cisco, "Cisco visual networking index: Forecast and methodology, 2014–2019," www.cisco.com, Accessed January 14, 2016.

[3] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, "An experimental implementation of oblivious transfer in the noisy storage model," *Nat. Commun.*, vol. 5, p. 3418, Mar. 2014.

[4] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of blind quantum computing," *Science*, vol. 335, no. 6066, pp. 303–308, Jan. 2012.

[5] S. Naguleswaran, "A new paradigm for secure military communications: Quantum information processing," in *Military Communications and Information Systems Conference (MilCIS 2010), Canberra, Australia*, Nov. 9–11, 2010, pp. 1–5.

[6] "Post-quantum cryptography for long-term security (PQCRYPTO)," http://cordis.europa.eu/project/rcn/194347_en.html, [H2020-EU.2.1.1., from 2015-03-01 to 2018-03-01, ongoing project - Reference: 645622], Accessed January 14, 2016.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983.

[8] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management – part 1: General (revision 3)," NIST, Special Publication 800-57, 2012.

[9] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, E. M. Chapple, C. Enderud, J. P. Hilton, K. Karimi, E. Ladizinsky, N. Ladizinsky, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, C. J. S. Truncik, S. Uchaikin, J. Wang, B. Wilson, and G. Rose, "Quantum annealing with manufactured spins," *Nature*, vol. 473, no. 7346, pp. 194–198, May 2011.

[10] N. Jones, "Computing: The quantum company," *Nature*, vol. 498, no. 7454, pp. 286–288, Jun. 2013.

[11] S. Boixo, T. F. Rønnow, S. V. Isakov, Z. Wang, D. Wecker, D. A. Lidar, J. M. Martinis, and M. Troyer, "Evidence for quantum annealing with more than one hundred qubits," *Nat. Phys.*, vol. 10, no. 3, pp. 218–224, Mar. 2014.

[12] T. F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A. Lidar, and M. Troyer, "Defining and detecting quantum speedup," *Science*, vol. 345, no. 6195, pp. 420–424, Jul. 2014.

[13] T. Lanting, A. J. Przybysz, A. Y. Smirnov, F. M. Spedalieri, M. H. Amin, A. J. Berkley, R. Harris, F. Altomare, S. Boixo, P. Bunyk, N. Dickson, C. Enderud, J. P. Hilton, E. Hoskinson, M. W. Johnson, E. Ladizinsky, N. Ladizinsky, R. Neufeld, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, S. Uchaikin, A. B. Wilson, and G. Rose, "Entanglement in a quantum annealing processor," *Phys. Rev. X*, vol. 4, no. 2, p. 021041, Apr. 2014.

[14] E. Cohen and B. Tamir, “Quantum annealing - foundations and frontiers,” *Eur. Phys. J. Special Topics*, vol. 224, no. 1, pp. 89–110, Feb. 2015.

[15] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, “Adiabatic quantum computation is equivalent to standard quantum computation,” *SIAM J. Comput.*, vol. 37, no. 1, pp. 166–194, Apr. 2007.

[16] J. Cai, A. Miyake, W. Dür, and H. J. Briegel, “Universal quantum computer from a quantum magnet,” *Phys. Rev. A*, vol. 82, no. 5, p. 052309, Nov. 2010.

[17] M. Van den Nest, “Universal quantum computation with little entanglement,” *Phys. Rev. Lett.*, vol. 110, no. 6, p. 060504, Feb. 2013.

[18] A. D. Córcoles, E. Magesan, S. J. Srinivasan, A. W. Cross, M. Steffen, J. M. Gambetta, and J. M. Chow, “Demonstration of a quantum error detection code using a square lattice of four superconducting qubits,” *Nat. Commun.*, vol. 6, p. 6979, Apr. 2015.

[19] M. Gimeno-Segovia, P. Shadbolt, D. E. Browne, and T. Rudolph, “From three-photon Greenberger-Horne-Zeilinger states to ballistic universal quantum computation,” *Phys. Rev. Lett.*, vol. 115, no. 2, p. 020502, Jul. 2015.

[20] M. Veldhorst, C. H. Yang, J. C. C. Hwang, W. Huang, J. P. Dehollain, J. T. Muhonen, S. Simmons, A. Laucht, F. E. Hudson, K. M. Itoh, A. Morello, and A. S. Dzurak, “A two-qubit logic gate in silicon,” *Nature*, vol. 526, no. 7573, pp. 410–414, Oct. 2015.

[21] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997.

[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[23] D. J. Bernstein, J. Buchmann, and E. Dahmen, *Post-Quantum Cryptography*, 1st ed. Springer, Nov. 2009.

[24] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, “Efficient decoy-state quantum key distribution with quantified security,” *Opt. Express*, vol. 21, no. 21, pp. 24 550–24 565, Oct. 2013.

[25] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, “A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing,” *New J. Phys.*, vol. 16, no. 1, p. 013047, Jan. 2014.

[26] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, “High-rate measurement-device-independent quantum cryptography,” *Nature Photon.*, vol. 9, no. 6, pp. 397–402, Jun. 2015.

[27] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[28] D. Dieks, “Communication by EPR devices,” *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.

[29] H. Takesue, S. D. Dyer, M. J. Stevens, V. Verma, R. P. Mirin, and S. W. Nam, “Quantum teleportation over 100 km of fiber using highly-efficient superconducting nanowire single photon detectors,” *Optica*, vol. 2, no. 10, pp. 832–835, Oct. 2015.

[30] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, “Advances in quantum teleportation,” *Nature Photon.*, vol. 9, no. 10, pp. 641–652, Oct. 2015.

[31] C. R. Laumann, R. Moessner, A. Scardicchio, and S. L. Sondhi, “Quantum annealing: The fastest route to quantum computation?” *Eur. Phys. J. Special Topics*, vol. 224, no. 1, pp. 75–88, Feb. 2015.

[32] P. Trojek, C. Schmid, M. Bourennane, Č. Brukner, M. Żukowski, and H. Weinfurter, “Experimental quantum communication complexity,” *Phys. Rev. A*, vol. 72, no. 5, p. 050305, Nov. 2005.

[33] A. Montina, “Communication complexity and the reality of the wave function,” *Mod. Phys. Lett. A*, vol. 30, no. 1, p. 1530001, Jan. 2015.

[34] S. Sazim and I. Chakrabarty, “A study of teleportation and super dense coding capacity in remote entanglement distribution,” *EPJ D*, vol. 67, p. 174, Aug. 2013.

[35] C. Zheng, Y. Gu, W. Li, Z. Wang, and J. Zhang, “Complete distributed hyper-entangled-bell-state analysis and quantum super dense coding,” *Int. J. Theor. Phys.*, pp. 1–9, Jul. 2015.

[36] E. M. Kessler, I. Lovchinsky, A. O. Sushkov, and M. D. Lukin, “Quantum error correction for metrology,” *Phys. Rev. Lett.*, vol. 112, no. 15, p. 150802, Apr. 2014.

[37] B. M. Terhal, “Quantum error correction for quantum memories,” *Rev. Mod. Phys.*, vol. 87, no. 2, pp. 307–346, Apr. 2015.

[38] R. Loura, Á. J. Almeida, P. S. André, A. N. Pinto, P. Mateus, and N. Paunković, “Noise and measurement errors in a practical two-state quantum bit commitment protocol,” *Phys. Rev. A*, vol. 89, no. 5, p. 052336, May 2014.

[39] E. Adlam and A. Kent, “Device-independent relativistic quantum bit commitment,” *Phys. Rev. A*, vol. 92, no. 2, p. 022315, Aug. 2015.

[40] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, “Practical quantum key distribution with polarization entangled photons,” *Opt. Express*, vol. 12, no. 16, pp. 3865–3871, Aug. 2004.

[41] G. D. Paparo, M. Müller, F. Comellas, and M. A. Martin-Delgado, “Quantum Google in a complex network,” *Sci. Rep.*, vol. 3, no. 2773, pp. 1–16, Oct. 2013.

[42] Á. J. Almeida, N. A. Silva, N. J. Muga, and A. N. Pinto, “Single-photon source using stimulated FWM in optical fibers for quantum communication,” in *Proc. SPIE 8001*, May 3, 2011, p. 80013W.

[43] Á. J. Almeida, N. A. Silva, P. S. André, and A. N. Pinto, "Four-wave mixing: Photon statistics and the impact on a co-propagating quantum signal," *Opt. Commun.*, vol. 285, no. 12, pp. 2956–2960, Jun. 2012.

[44] Á. J. Almeida, S. R. Carneiro, N. A. Silva, N. J. Muga, and A. N. Pinto, "Polarization-entangled photon pairs using spontaneous four-wave mixing in a fiber loop," in *Proc. of International Conference on Computer as a Tool (EUROCON), IEEE, Lisbon, Portugal*, Apr. 27-29, 2011, pp. 1–4.

[45] Á. J. Almeida, N. J. Muga, N. A. Silva, J. M. Prata, P. S. André, and A. N. Pinto, "Continuous control of random polarization rotations for quantum communications," *submitted to J. Lightwave Technol.*, Jan. 2016.

[46] Á. J. Almeida, A. D. Stojanovic, N. Paunkovic, R. Loura, N. J. Muga, N. A. Silva, P. Mateus, P. S. André, and A. N. Pinto, "Implementation of a two-state quantum bit commitment protocol in optical fibers," *J. Opt.*, vol. 18, no. 1, p. 015202, Jan. 2016.

Chapter 2

Quantum Communications

2.1 Introduction

In the late 1960s, Stephen Wiesner had the idea of using quantum mechanics to make bank notes impossible to counterfeit[1]. He wrote his idea in a work called *'Conjugate Coding'*, which he submitted to *Institute of Electrical and Electronics Engineers (IEEE) Transactions on Information Theory*. However, the paper was rejected for publication, possibly because it was not understood by the editors and reviewers at that time. This event came to confirm that quantum mechanics was not yet comprehended by everyone. On the other side of the story, Stephen Wiesner and Charles Bennett have been colleagues during their undergraduate studies at Brandeis University, and even after following different paths, they kept in touch. This allowed Bennett to know about Wiesner's idea, which would be valuable for the future. During the following years, Bennett mentioned the idea to some people, however never received the right feedback from anyone [1].

The next significant event was when Charles Bennett met Gilles Brassard in a conference in Puerto Rico, in 1979[2]. Bennett saw in the conference program that a talk about relativized cryptography was scheduled to be given by Brassard and thought he could be interested in Wiesner's ideas. And in fact, that is what happened! Fortunately, from that conversation resulted a collaboration that would give rise to quantum cryptography [1].

During the following years the two exchanged several ideas, until in 1982 they published the first paper where the term *quantum cryptography* was indeed introduced [2]. Moreover, this paper triggered the publication of Wiesner's *'Conjugate Coding'*, in 1983 [3]. An year after, Bennett and Brassard proposed the very first quantum protocol for quantum key distribution (QKD), which would become known as Bennett-Brassard 1984 (BB84) [4].

[1] On September 12th, 2012, in a phone conversation between Charles Bennett and Stephen Wiesner, audible by all participants of QCRYPT - 2nd International Conference on Quantum Cryptography, taking place in Singapore, Wiesner said that the first time he had the idea of making quantum bank notes was in 1967.

[2] 20th Annual IEEE Symposium on the Foundations of Computer Science.

Nevertheless, in the 1980s quantum cryptography did not receive any particular attention. Then, in 1989 another breakthrough event for quantum cryptography took place, with the first transmission of quantum information in a free-space link of 32.5 cm [5, 6]. In 1991 Artur Ekert presented a different way of seeing quantum cryptography, making use of quantum correlations usually known as quantum entanglement. That work gave rise to the first quantum protocol for the use of entangled photons, nowadays known as Ekert 1991 (E91) [7].

Since those groundbreaking achievements for quantum cryptography, many quantum protocols have been proposed. In 1992, Bennett presented a simplification of BB84 protocol, by establishing that only two nonorthogonal states would be enough to guarantee the security of the transmission. This is probably the most simple protocol and it is known as Bennett 1992 (B92) [8]. In the next year, the first experimental demonstration of quantum cryptography in optical fibers using polarized photons was accomplished [9] and the experimental and practical limits determined [10]. A so-called 4+2 protocol, combining the advantages of BB84 and B92 protocols, was proposed in 1995 [11]. The BB84 protocol was also generalized to six states, allowing higher noise in the system [12]. A solution to help in photon-number splitting (PNS) attacks[3] was presented in 2003, in a different type of protocol called decoy-state [14]. A protocol similar to BB84, but more secure against PNS attacks, was proposed in 2004, being known as Scarani-Acín-Ribordy-Gisin 2004 (SARG04) [15]. With the development of increasingly robust protocols, most of the security problems were solved. However, the detection system remained vulnerable to attacks. To solve that problem, in 2012 a new protocol called Measurement-Device-Independent (MDI) was proposed, which claims to avoid all types of attacks to the detection system, being a major improvement for quantum cryptography [16].

In recent years, quantum bit commitment (QBC) is receiving a great interest, both theoretically and experimentally, mostly potentiated by an increasingly broader range of applications [17–21]. QBC is a fundamental primitive in cryptography with several applications, such as coin flipping [22–25], secure voting [26, 27], oblivious transfer [28, 29] or zero-knowledge proofs [30]. The notion of bit commitment was presented by Manuel Blum in 1981 [31] and the concept of commitment formalized only in 1988 [32]. A QBC protocol claimed by the authors to be unbreakable by both parties was proposed in 1993 [33]. However, a few years later a no-go theorem proved that unconditionally secure QBC was impossible unless relativistic effects were used [34, 35]. In order to evade the no-go theorem in [34, 35], a new classical bit commitment protocol based on cryptographic constraints imposed by special relativity was proposed [36]. This protocol has the merit of being unconditionally secure against classical or quantum attacks. Later, a QBC protocol using quantum and relativistic effects was proposed [37] and proven secure both in the presence of loss [38] and in the presence of perfect devices [39]. The protocol was recently implemented experimentally [40, 41]. Although not unconditionally secure, an ex-

[3] It is well known that many experimental implementations use non ideal single-photon sources. This means that photons in the laser pulses are distributed in a probabilistic way and most of the pulses contain no photons, some pulses contain one photon, and a few pulses contain two or more photons. When the pulses contain more than one photon, an eavesdropper, usually called Eve, can split some of them and transmit the remaining ones without introducing detectable errors. This strategy is known as PNS attack [13].

perimental demonstration of a practical QBC protocol using BB84 and whose security is based on current technological limitations, was also presented [42]. The technological limitations considered are the lack of non-demolition measurements and long-term stable quantum memories. A two-state version of the protocol was also proposed [43], addressing several constraints of a practical implementation presented recently [44].

For the implementation of unconditionally secure quantum protocols, the use of single or entangled photon sources is required [45, 46]. However, obtaining a true single-photon source is not trivial and most of the experimental implementations use probabilistic approximations [47]. The most simple photon source is obtained with an attenuated laser [15]. The stimulated FWM process was also used to obtain a probabilistic photon source [48–53] and the spontaneous FWM process was employed to generate polarization-entangled photon pairs [54, 55] and heralded photon sources [56, 57]. The process of parametric down-conversion (PDC) can also be used in quantum communications, both to generate a heralded single photon source or even an entangled photon source [58–61]. Quantum entanglement has also applications in the realization of quantum repeaters [62, 63].

The capabilities of a quantum communication system are strongly related with the capability of detecting photons. Current photon detectors are still far from ideal. However, there has been an enormous progress in this field [46]. Nowadays, there are several types of detectors, which have been used in many experimental demonstrations of quantum communication, like Single-Photon Avalanche Detectors (SPADs) [64], Superconducting Nanowire Single-Photon Detectors (SNSPDs) [65] or a recently developed Negative Feedback Avalanche Diode (NFAD) [66].

With the theoretical and the experimental knowledge from building and implementing quantum protocols along the years, research moved to the development of quantum networks. In early 2000s, the *Defense Advanced Research Projects Agency* (DARPA) started to work in the world's first quantum network [67]. Between 2003 and 2008, a number of European institutions have worked in a large quantum communication project named *Secure Communication based on Quantum Cryptography* (SECOQC). In the framework of this project, a quantum network was established in Vienna [68]. China also developed a quantum network that was demonstrated in 2009 [69]. The *SwissQuantum* network was implemented in Geneva between 2009 and 2011, proving the reliability of the quantum layer over a long period of time [70]. In 2010, several institutions from Japan and Europe tested a QKD network in Tokyo [71]. In 2016, China expects to launch a hack-proof 2000 km quantum communication network from Beijing to Shanghai [72].

Quantum communication using point-to-point fiber links is limited to only a few hundred kilometers due to attenuation [73–75]. Free-space links in the ground also suffer from limitations due to Earth's curvature and atmospheric attenuation and turbulence [76]. Through the use of quantum repeaters, it may be possible to extend considerably these limits, however at the cost of high complexity, at least for now [62, 77, 78]. Studies with the goal of space quantum communications started almost 20 years ago and promise to make possible to reach much broader distance ranges [79–86]. A fully operational satellite QKD system was demonstrated recently, using BB84 protocol [87]. Quantum teleportation of a photonic qubit over 100 km of optical fiber was also achieved, confirming the feasibility of long-distance quantum communication [88]. The first satellite carrying an entangled photon source is scheduled to be launched in 2016 [89].

Apart from all theoretical and experimental developments, the field of quantum communications includes several technologies which have reached the commercial level, such as SPADs, SNSPDs, QKD systems, quantum random number generators (QNRGs) or even preliminary quantum computers [90].

2.2 Basics of Quantum Information

After a brief resume of the state-of-the-art of quantum communications, in this section, we present some of the basic elements necessary to understand the principles behind its security. Then, we introduce the key elements for quantum communication systems, namely some quantum protocols, the source of photons, the encoding scheme, the quantum channel and finally the decoding scheme.

2.2.1 The Qubit

The basic unit in classical information theory is called *bit*. Analogously, the basic unit in quantum information is the quantum bit, or *qubit* [91]. In the quantum-mechanical view, a qubit can be represented as a two-level system with two states, $|0\rangle$ and $|1\rangle$, in the same way as the classical bit can assume two values, '0' or '1'. The two states must form an orthogonal basis in the two-dimensional Hilbert space given by $\{|0\rangle, |1\rangle\}$. However, contrary to the classical bit, the qubit can be found in a superposition of the two basis states as,

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle \quad \text{with} \quad |a_0|^2 + |a_1|^2 = 1, \tag{2.1}$$

where a_0 and a_1 are, in general, complex numbers and $|a_0|^2$ and $|a_1|^2$ are the probabilities of finding the qubit in state $|0\rangle$ and $|1\rangle$, respectively [92]. For the particular case of a_0 and a_1 being real numbers, the qubit can be visualized as a unit vector on the plane, as shown in Fig. 2.1.

For a single qubit with an arbitrary state, like the one described by Eq. (2.1), it is not possible to determine with a single measurement both coefficients, a_0 and a_1, with 100% certainty. However, if we perform a measurement in the computational basis of the qubit, there are two possible measurement outcomes, $|0\rangle$ and $|1\rangle$, which are obtained with a certain probability [92],

$$P(0) = |a_0|^2 \quad \text{and} \quad P(1) = |a_1|^2. \tag{2.2}$$

Regarding qubits measurement, there are several rules which need to be considered, namely [92]:

1. For any qubit preparation there exists a basis in the qubit's Hilbert space which allows to obtain measurement results with a probability of unity,

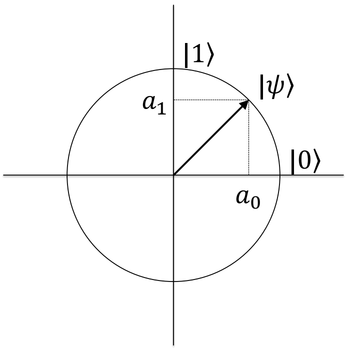

Figure 2.1: Representation of a qubit as a unit vector on the plane.

2. The result of a single measurement on an arbitrary state of unknown preparation is random,

3. It is impossible to determine the preparation basis for an arbitrary and unknown single qubit.

2.2.2 Encoding Qubits in Polarization

In principle, a qubit can be encoded in any degree of freedom of the photon [47]. In this work, the encoding was performed in the polarization of single photons, whose qubit states can be mapped to horizontal $|H\rangle$ and vertical $|V\rangle$ polarizations as,

$$|0\rangle \longrightarrow |H\rangle, \tag{2.3a}$$

$$|1\rangle \longrightarrow |V\rangle. \tag{2.3b}$$

There are, however, other states of polarization (SOPs) which can be used to represent the qubit, such as:

$$|0\rangle \longrightarrow |-45\rangle = \frac{1}{\sqrt{2}}\Big[|H\rangle - |V\rangle\Big] \tag{2.4a}$$

$$|1\rangle \longrightarrow |+45\rangle = \frac{1}{\sqrt{2}}\Big[|H\rangle + |V\rangle\Big]. \tag{2.4b}$$

2.2.3 The Heisenberg Uncertainty Principle

The Heisenberg Uncertainty Principle [93] is probably the best known result of quantum mechanics and a criterion of security for quantum cryptography. The principle prohibits the measurement of a quantum state using two bases simultaneously. Thus, if we cannot know the result of the simultaneous measurement with two bases, we say that they do not commute. In this case, considering that S_A and S_B are two noncommuting states, if we first measure S_A and then S_B, the measurement of the last will not be performed with certainty. Therefore, if we have a given number of identical quantum states, $|\psi\rangle$, then measure S_A on some states and S_B in others, the standard deviation of the results S_A (ΔS_A) times the standard deviation of the results S_B (ΔS_B) satisfy the inequality,

$$\Delta S_A \Delta S_B \geq \frac{|\langle\psi|[S_A, S_B]|\psi\rangle|}{2}, \tag{2.5}$$

where $[S_A, S_B] = S_A S_B - S_B S_A$ is the commutator of S_A and S_B [92]. From this result, we can conclude that an eavesdropper trying to learn a quantum state needs to choose only a measurement basis and if its choice is not compatible with those of Alice (the sender) and Bob (the receiver), it will introduce disturbance and unveil itself. Next, we will exemplify particular examples of this principle.

In order to encode or decode information, Alice and Bob can use two nonorthogonal bases. One basis is called rectilinear and is defined as $+ = \{|H\rangle, |V\rangle\}$. The other basis is called diagonal and is defined as $\times = \{|-45\rangle, |+45\rangle\}$. Now, let us assume that Alice uses the rectilinear basis to encode a bit in the state $|H\rangle$ and Bob performs the measurement using the diagonal basis. In this case, the probability for him to obtain $|{+45}\rangle$ is given by

$$|\langle H|{+45}\rangle|^2 = |\langle H|\tfrac{1}{\sqrt{2}}(|H\rangle + |V\rangle)|^2 = \tfrac{1}{2}|\langle H|H\rangle + \langle H|V\rangle|^2 = \frac{1}{2}. \tag{2.6}$$

The probability to obtain $|{-45}\rangle$ is given by

$$|\langle H|{-45}\rangle|^2 = |\langle H|\tfrac{1}{\sqrt{2}}(|H\rangle - |V\rangle)|^2 = \tfrac{1}{2}|\langle H|H\rangle - \langle H|V\rangle|^2 = \frac{1}{2}. \tag{2.7}$$

Since Heisenberg's Uncertainty Principle forbids the measurement in two bases simultaneously, if the measurement basis is different from the preparation basis the result is random and presents equal probabilities. From the results of Eqs. (2.6) and (2.7) it is straightforward to conclude that

$$|\langle{+45}|H\rangle|^2 = |\langle{-45}|H\rangle|^2 = |\langle V|{+45}\rangle|^2 = |\langle V|{-45}\rangle|^2 = |\langle{+45}|V\rangle|^2 = |\langle{-45}|V\rangle|^2 = \frac{1}{2}. \tag{2.8}$$

If Alice and Bob use the same basis, then the result of the measurement is deterministic according to

$$\langle H|H\rangle = \langle V|V\rangle = \langle{-45}|{-45}\rangle = \langle{+45}|{+45}\rangle = 1, \tag{2.9}$$

or

$$\langle H|V\rangle = \langle V|H\rangle = \langle{-45}|{+45}\rangle = \langle{+45}|{-45}\rangle = 0. \tag{2.10}$$

Moreover, security also comes from the fact that in quantum mechanics the act of measuring the state of a qubit changes it, collapsing it from its superposition of $|0\rangle$ and $|1\rangle$ to a specific state [92].

2.2.4 The No-Cloning Theorem

The no-cloning theorem is one of the pillars for security in quantum cryptography, which states that it is not possible to create a perfect copy of a single qubit [94]. A simple proof of the theorem can be shown as follows. By definition, an ideal quantum-cloning machine (QCM) would be able to copy a qubit, $|\psi\rangle$, arbitrarily prepared, to another blank qubit, $|b\rangle$, without changing or destroying the initial qubit, as shown in Fig. 2.2.

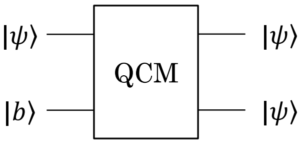

Figure 2.2: Diagram of a QCM.

Following this figure, the process of cloning a quantum state can be written as [95]

$$|\psi\rangle|b\rangle \Longrightarrow |\psi\rangle|\psi\rangle. \tag{2.11}$$

If we consider that the input state $|\psi\rangle = |V\rangle$, then we have that

$$|V\rangle|b\rangle \Longrightarrow |V\rangle|V\rangle, \tag{2.12}$$

which means that a copy was created successfully and the machine works perfectly. Moreover, if we use for example the superposition state given by Eq. (2.4b) as initial state, we have

$$\begin{aligned}|{+45}\rangle|b\rangle = \frac{1}{\sqrt{2}}\Big[|H\rangle + |V\rangle\Big]|b\rangle \Longrightarrow \frac{1}{\sqrt{2}}\Big[|H\rangle + |V\rangle\Big]\frac{1}{\sqrt{2}}\Big[|H\rangle + |V\rangle\Big] = \\ \frac{1}{2}\Big[|H\rangle|H\rangle + |H\rangle|V\rangle + |V\rangle|H\rangle + |V\rangle|V\rangle\Big],\end{aligned} \tag{2.13}$$

which is different from the state that would be expected from a perfect QCM, given by,

$$|{+45}\rangle|b\rangle \Longrightarrow |{+45}\rangle|{+45}\rangle. \tag{2.14}$$

The difference between the results of Eqs. (2.13) and (2.14) clearly demonstrates the impossibility to make perfect copies from arbitrary input quantum states. However, nothing prohibits making approximate copies of a quantum state with optimal fidelity, or perfect copies with the largest probability [96]. Since an eavesdropper cannot perform perfect copies of a quantum state, the protocol implemented between Alice and Bob should guarantee that the fidelity of Eve's copies do not gives her more information than what Alice and Bob can share [92].

2.2.5 Entanglement

The concept of entanglement is one of the most interesting in quantum mechanics, not having, however, an equivalent in the classical world [45]. Two particles are called entangled if their wave function cannot be separated, *i.e.*, if they are in a superposition state such as,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\Big[|H\rangle|H\rangle + |V\rangle|V\rangle\Big]. \tag{2.15}$$

Therefore, any measurement performed on the state of one particle would change the other, no matter how far they are separated [45].

Note that entanglement is not restricted to two-particle systems and can be seen as a fundamental property of many-particle systems. Up to now, multi-particle entangled states having 14 qubits [97] and eight-photon entangled systems [98] were already observed. These achievements pave the way to the realization of quantum computers [99, 100], quantum simulations [101, 102] and many other tasks in quantum communication [45].

2.3 Quantum Protocols Based on Polarization Encoding

In this section, we present the quantum protocols which served as a basis for this work. The first one to be described is the BB84 protocol, which was also the first discrete-variable coding protocol to be proposed [4]. Then, we present the B92 protocol [8]. This protocol uses only two nonorthogonal states, but at the same time is less secure than BB84. Finally, we describe a two-state QBC protocol, which can give increased security to people which do not know or do not trust each other [43]. In the description of the three protocols we consider that bits are encoded in the polarization of photons.

In Fig. 2.3 we show the most general scheme of a quantum communications system. Alice shares a quantum channel with Bob. Eve might want to eavesdrop the quantum channel to gain access to the secret information. However, her presence can be revealed since she causes errors when measuring the quantum information. The public channel is used to perform classical operations which do not share any secret data.

2.3.1 The BB84 Protocol

The BB84 protocol is by far the most known and the most implemented protocol in quantum cryptography [4]. Not only because it was the first to be proposed but also due to the trade-off between experimental complexity and security, this makes it ideal for real-world implementations. This protocol has been well studied during the years, being also the basis for many other protocols [47].

A schematic diagram of this protocol is shown in Fig. 2.4.

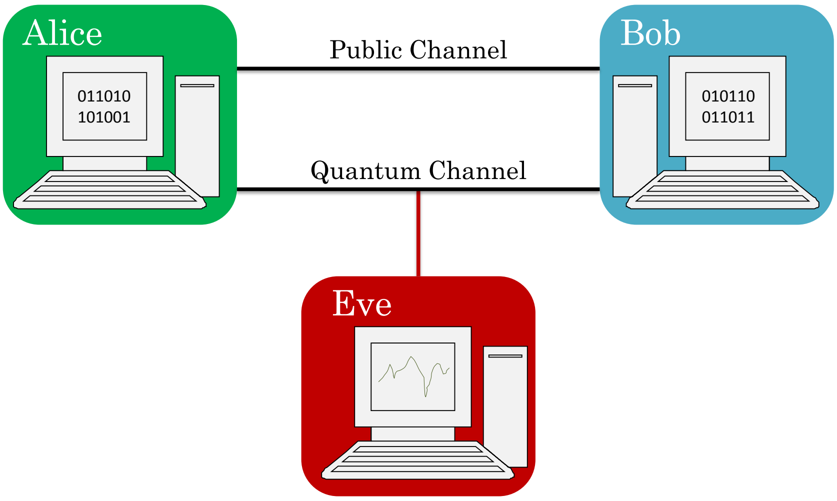

Figure 2.3: General scheme of a quantum communication system.

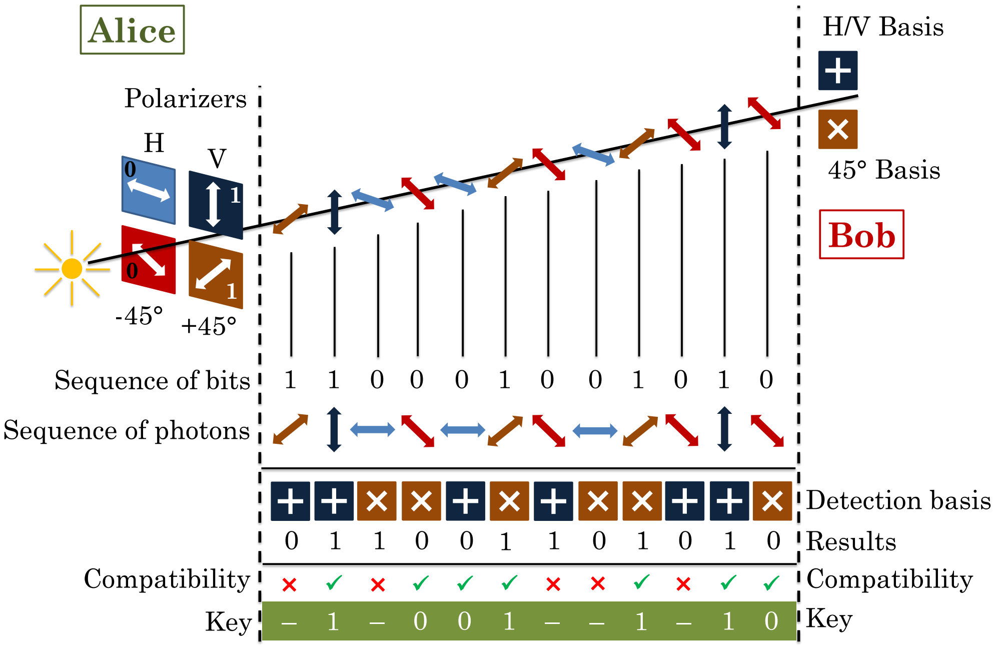

Figure 2.4: General scheme of BB84 protocol using polarization encoding.

The protocol works as follows:

1. Alice generates a random sequence of bits, with ‘0’s and ‘1’s;
2. Then, she randomly generates the basis to encode each bit;
    a) The bases can be the rectilinear, represented by $+ = \{|H\rangle, |V\rangle\}$ or the diagonal, represented by $\times = \{|-45\rangle, |+45\rangle\}$;
3. Photons are transmitted through the quantum channel;

4. Bob chooses, also randomly, the measurement bases and records the bits and the bases used;
5. After all qubits are transmitted, a public discussion is performed in order to determine the secret key;
6. Bob publicly says which bases he used to measure the qubits received;
7. Alice confirms which bases correspond to the ones she used to encode the bits;
8. Bob randomly reveals some of the qubits received;
9. Alice confirms which ones are correct in order to estimate the channel QBER and to apply an error correction procedure,
10. Finally, after privacy amplification, the secret key is obtained from the non-revealed qubits.

The unconditional security of the BB84 protocol was already proven in many papers, using different arguments [103–111].

2.3.2 The B92 Protocol

The B92 protocol was proposed as a simplification of BB84. With this protocol, Bennett showed that it is possible to achieve security in encryption using only two quantum states, as long as they are nonorthogonal [8].

A schematic diagram of the functioning of this protocol is shown in Fig. 2.5.

The protocol's description is the following:

1. Alice generates a random sequence of bits, with '0's and '1's;
2. Then, she randomly generates the basis to encode each bit;
    a) The bases can be the rectilinear, represented by $+ = \{|H\rangle, |V\rangle\}$ or the diagonal, represented by $\times = \{|-45\rangle, |+45\rangle\}$;
3. Photons are transmitted through the quantum channel;
4. Bob chooses, also randomly, the measurement bases and records the bits received;
5. Bob tells Alice which basis he have used for each measurement in a public discussion;
6. Alice confirms which bases are correct;
7. Alice and Bob keep the results from the conclusive measurements and discard the rest;
    a) These are the results that will be used to obtain the secret key;

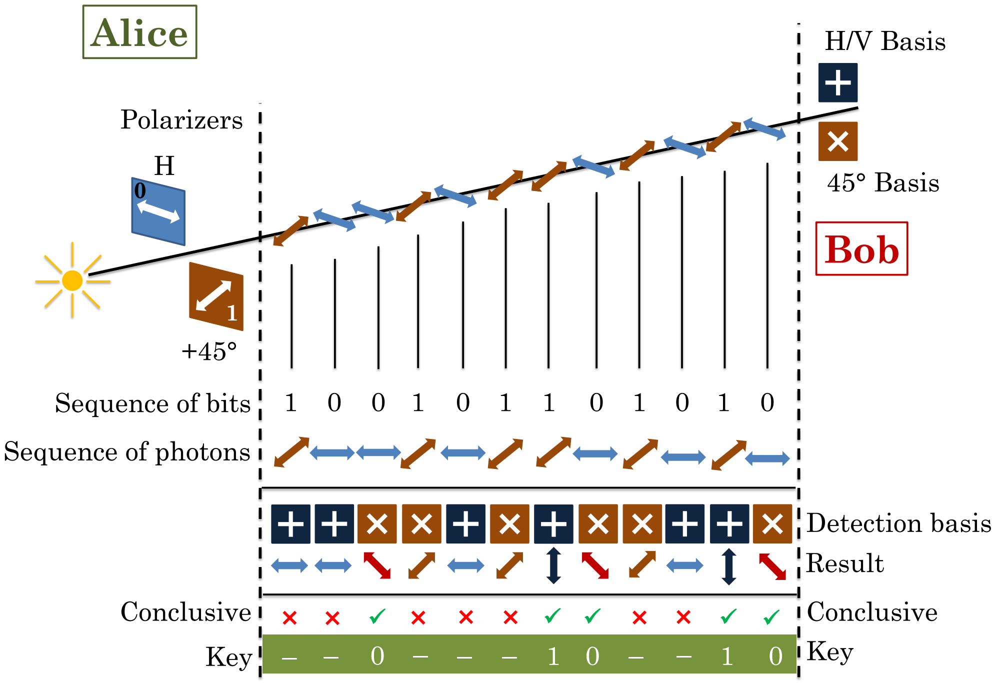

Figure 2.5: General scheme of B92 protocol using polarization encoding.

8. Bob and Alice test the key by revealing some qubits randomly in order to check their parity,

9. Finally, they obtain the secret key from the non-revealed qubits.

Since this protocol uses only two states, *e.g.* $|H\rangle$ and $|+45\rangle$, the establishment of the secret key is based on conclusive measurements. The possible measurement results for the two states, when Bob uses $+$ and $\times$ bases are shown in Fig. 2.6.

	ALICE	BOB		
Case	*Polarization*	*Basis*	*Result*	*Conclusive ?*
1.	↔	+	↔	NO
2.	↔	×	↗	NO
3.	↔	×	↖	YES
4.	↗	+	↔	NO
5.	↗	+	↕	YES
6.	↗	×	↗	NO

Figure 2.6: Detection scheme in B92 quantum protocol based on polarization encoding.

From this figure we can see that Bob obtains conclusive results (without knowing what Alice sent him) in two cases, namely:

i. Bob selects the diagonal basis and measures the state $|-45\rangle$ (Case **3.**), and

ii. Bob selects the rectilinear basis and measures the state $|V\rangle$ (Case **5.**).

If Bob selects the rectilinear basis and measures the state $|H\rangle$, this is an inconclusive result for him, since he cannot know if Alice sent the state $|H\rangle$ (Case **1.**) or the state $|+45\rangle$ (Case **4.**). Likewise, if Bob selects the diagonal basis and measures the state $|+45\rangle$, this is also an inconclusive result for him, since he cannot know if Alice sent the state $|H\rangle$ (Case **2.**) or the state $|+45\rangle$ (Case **6.**).

The unconditional security of the B92 protocol under different scenarios was already proved in several works [112–117].

2.3.3 The QBC Protocol

A QBC protocol is a cryptographic primitive that allows two mistrustful parties to exchange quantum information. Generally, this protocol consists in two phases: *commitment* and *opening*. In the commitment phase, Alice makes the commitment to a value of a bit, '0' or '1'. This means that Alice selects only one measurement basis, at a certain time. After the commitment, Alice finalizes the protocol by revealing her choice to Bob, at the opening phase, in a later moment in time. The commitment can be seen for example as a promise that Alice will do a given action in the future, for example to buy a house from Bob for a given price [43].

In order to be secure, the protocol has to fulfill three requirements:

1. Alice cannot change her commitment later in time, mainly in the opening phase, and due to that, the protocol is considered *binding*;

2. Bob cannot have knowledge on Alice's commitment before the opening phase, defining the property of *concealing*,

3. If both are honest, *i.e.*, if they execute the protocol according to the rules, then Bob will read Alice's commitment successfully, defining its *viability*.

This protocol is of particular interest in situations where the two parties are in different locations, do not know or do not trust each other.

In Fig. 2.7 is shown the scheme of a QBC protocol for the case when Bob sends $|H\rangle$ and $|+45\rangle$ states and Alice measures in H/V basis. Fig. 2.8 shows the case when Alice measures in 45° basis.

The protocol runs as follows:

1. Bob generates a random sequence of bits, with '0's and '1's;

2. Then, he chooses a sequence of photons which he will use to encode each one of the bits;

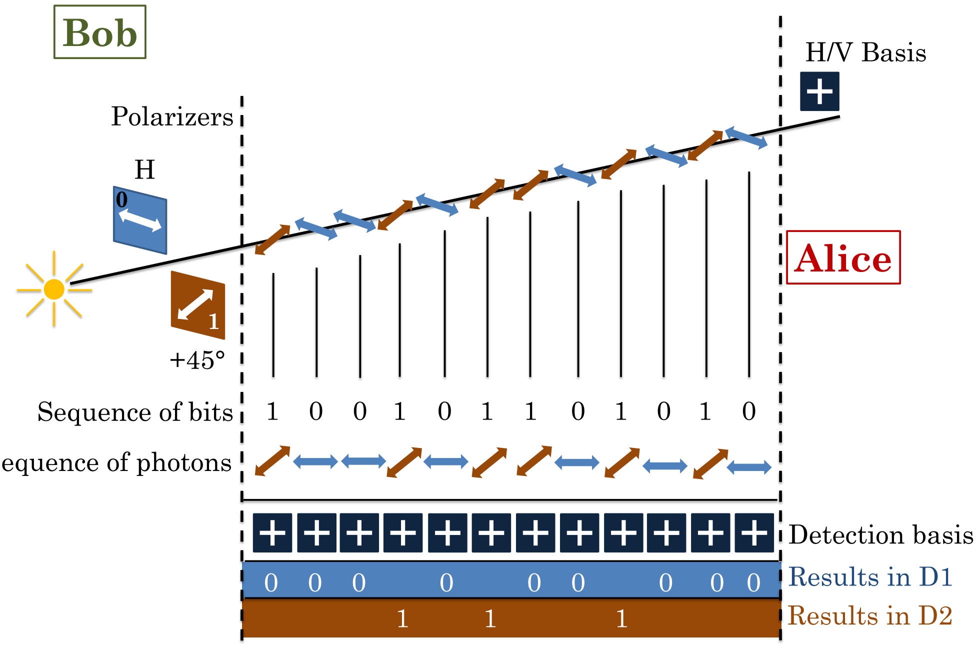

Figure 2.7: Encoding and decoding schemes in a QBC protocol for the case when Bob sends $|H\rangle$ and $|+45\rangle$ states and Alice measures in H/V basis.

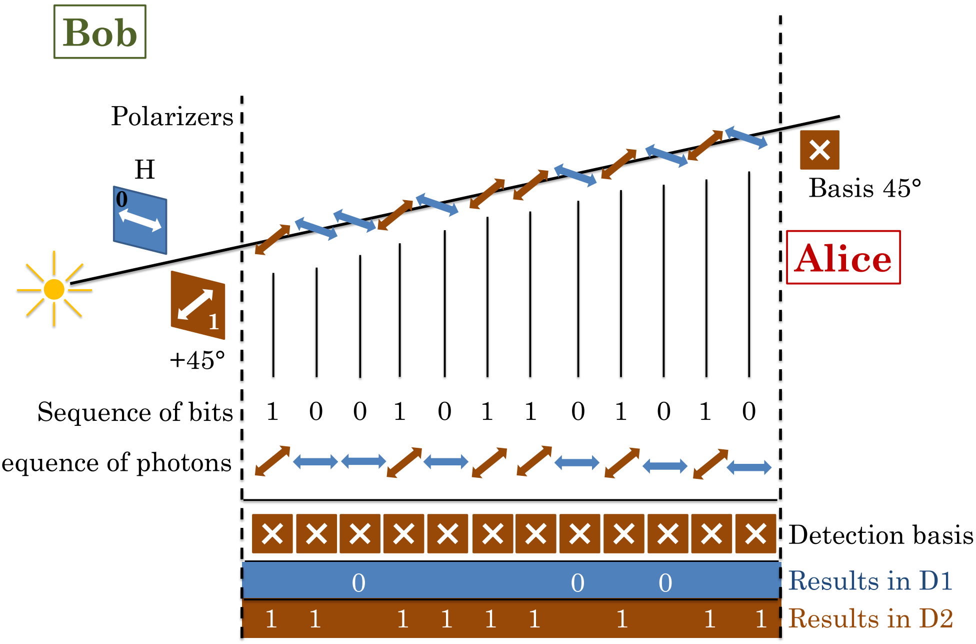

Figure 2.8: Encoding and decoding schemes in a QBC protocol for the case when Bob sends $|H\rangle$ and $|+45\rangle$ states and Alice measures in 45° basis.

a) The SOPs of the photons are obtained from two bases, rectilinear, $+ = \{|H\rangle, |V\rangle\}$ and diagonal, $\times = \{|-45\rangle, |+45\rangle\}$;

  b) The bit '0' will be encoded in the $|H\rangle$ SOP and the bit '1' will be encoded in the $|+45\rangle$ SOP;

3. Photons are transmitted to Alice through the quantum channel;

4. Alice randomly chooses one of the measurement basis for the commitment to all photons and records the results of each detector;

5. After all photons are measured, Alice sends the results and the corresponding commitment basis to Bob;

6. Bob performs a statistical test of Alice's results,

7. Based on the result of the test, Bob accepts or discards Alice's commitment.

Since in a QBC protocol the strength of the commitment is based on a statistical analysis of Alice's results by Bob, in order to have an accurate statistics and to be able for Alice to pass Bob's test, all measurements, either in detector 1 (D1) or detector 2 (D2), need to be considered.

The unconditional security of QBC was proven impossible unless relativistic effects were considered [34, 35, 118]. Unconditionally secure QBC protocols based on quantum and relativistic effects were proposed, taking also advantage of some assumptions [37–39].

2.4 The Quantum Communications System

In this section, we will describe part of the quantum communications system, see Fig. 2.9, that we will use in the work of this thesis.

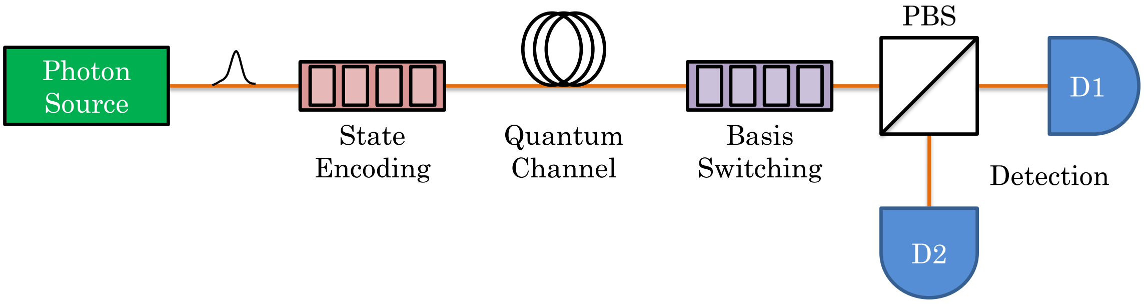

Figure 2.9: Schematic diagram of a quantum communications system. PBS - Polarization-beam splitter; D1 - Detector 1; D2 - Detector 2.

The system includes five main sections: (i) photon generation, (ii) encoding, (iii) the transmission channel, (iv) decoding and (v) detection. First, we start by describing the characteristics of the photon source. Second, we present the encoding scheme, which uses the polarization of photons. As a quantum channel we consider an optical fiber and describe its main characteristics and drawbacks. On the receiver's side, we describe the decoding scheme and finally we present the detection devices.

2.4.1 The Photon Source

A photon source is a key element for quantum communications. The most simple to obtain, and therefore the most used, is a highly attenuated laser source [46].

The key characteristic of probabilistic photon sources is the fact that they present a probability to generate photons which is different from 1. They are also seen as approximations of true single photon sources. The photon number distribution in these sources can follow, for example, Poissonian (coherent) statistics or thermal (incoherent) statistics. In practice that means there are different probabilities to emit 0, 1, 2 or more photons. The different probabilities to emit photons are due to fluctuations from the so-called photon noise [119].

As it was said, the most common sources which are used in quantum experiments are the ones obtained from an attenuated laser. In this case, the distribution of photons follows a Poissonian statistics and therefore they are also called Poissonian photon sources [119]. Through the use of the stimulated FWM process it is possible to obtain a source which obeys thermal statistics for a low number of photons per pulse and which is called thermal photon source [50, 53]. Whenever the average number of photons per pulse generated by these sources is much smaller than 1, they can be used in quantum communication experiments. Therefore, the vast majority of quantum protocols already includes the possibility of non-ideal photon sources [47].

The probability distribution of the number of photons (n) for Poissonian and thermal sources, considering different average numbers of photons per pulse, μ, is shown in Fig. 2.10. From this fugure we can take two main conclusions. First, we can see that if the average number of photons per pulse is equal to 0.1, the distribution of photons in both sources is similar. Moreover, at this photon rate either Poissonian or thermal sources can be used to demonstrate quantum communications systems. The second conclusion is observed when the average number of photons per pulse is equal to 1. In this case, we verify that the thermal source presents a larger number of fluctuations. This is due to the bosonic character of photons, which follow the Bose-Einstein distribution [119].

2.4.2 The Encoding Scheme

As was discussed in the schemes representing the three quantum protocols, classical bits can be encoded in the photon's polarization. Next, we will show the correspondence between bits and quantum states in the rectilinear and diagonal basis and one scheme to encode two nonorthogonal SOPs, see Fig. 2.11. In Fig. 2.11(a), the correspondence between classical bits and quantum states is shown, both for rectilinear and diagonal bases. The rectilinear basis (H/V basis) allows bits to be encoded in two orthogonal states, $|H\rangle$ and $|V\rangle$. The bit '0' can

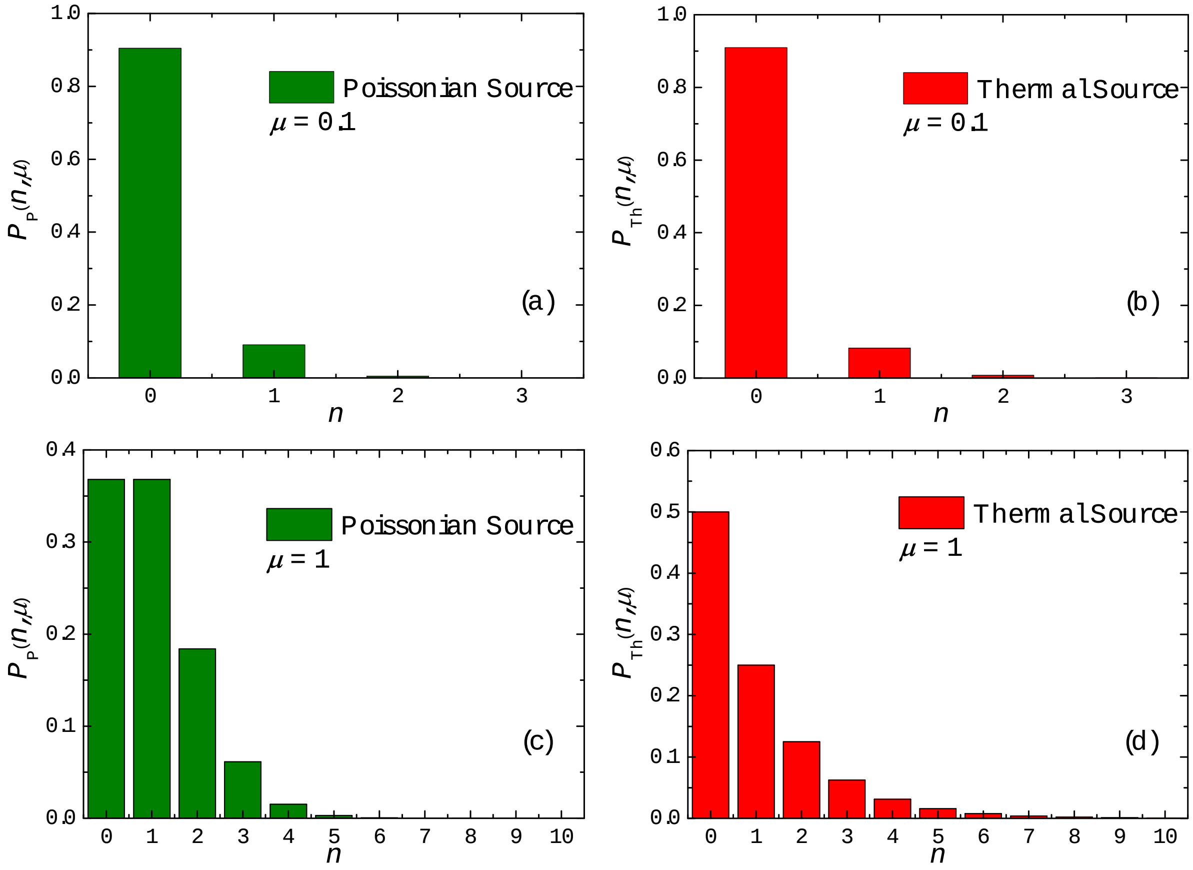

Figure 2.10: Probability distribution of the number of photons, n, for Poissonian (P_P) and thermal (P_{Th}) photon sources, (a)-(b) when the average number of photons per pulse, $\mu = 0.1$ and (c)-(d) when the average number of photons, $\mu = 1$.

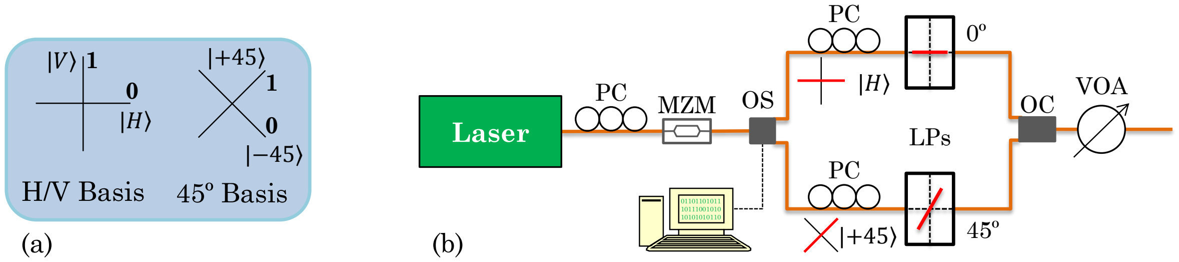

Figure 2.11: (a) Correspondence between bits and states in the rectilinear and the diagonal basis and (b) method to encode two nonorthogonal SOPs.

be encoded in the $|H\rangle$ SOP and the bit '1' can be encoded in the $|V\rangle$ SOP. The diagonal basis (45° basis) also allows bits to be encoded in two orthogonal states, $|-45\rangle$ and $|+45\rangle$. The bit '0' can be encoded in the $|-45\rangle$ SOP and the bit '1' can be encoded in the $|+45\rangle$ SOP.

Fig. 2.11(b) shows the scheme to generate two nonorthogonal SOPs, $|H\rangle$ and $|+45\rangle$. The $|H\rangle$ SOP is obtained from the rectilinear basis and the $|+45\rangle$ SOP is obtained from the diagonal basis (in red). A laser is modulated using a Mach-Zehnder Modulator (MZM) and reaches an optical switch (OS). The polarization controller (PC) after the laser allows to maximize the number of photons that output from the MZM. The OS is connected to a computer which generates classical bits, '0' and '1', at random. Whenever a '0' is generated, the OS allows a photon to go to the upper arm, and if a '1' is generated it goes to the lower arm. Then, one linear polarizer (LP) is set at each arm of the OS. In the upper arm, the LP has its transmission axis with an angle of 0° and the LP in the lower arm has its transmission axis at 45°. The PC before each LP is used to adjust the polarization of the photons with its transmission axis. Therefore, whenever a photon passes through the upper arm it will generate a $|H\rangle$ SOP and whenever a photon passes through the lower arm it will generate a $|+45\rangle$ SOP. After the LPs, photons pass through an optical coupler (OC) and are attenuated using a variable optical attenuator (VOA) in order to reach the near single-photon regime.

If instead of generating two nonorthogonal SOPs one wants to generate orthogonal states, that can be achieved simply by setting the angle of the lower polarizer at 90°. In this case, whenever a photon passes through the lower arm it will be generated a $|V\rangle$ SOP.

2.4.3 The Quantum Channel

The first experiments on quantum communications were performed using the free space as a quantum channel [5, 6]. However, optical fibers have the advantage of guiding more easily the photons and, due to that, they are more commonly used. One important drawback which is present in optical fibers is the attenuation, that varies with the wavelength [75]. Fig. 2.12 shows the attenuation spectrum for a standard single-mode fiber (SSMF) and a low-water-peak fiber (LWPF). Looking at this figure one can see that the minimum attenuation for a SSMF occurs in the C-band, *i.e.*, in the wavelength range between 1530 nm and 1565 nm. At 1550 nm, the value for the attenuation is approximately 0.2 dB/km [121]. Because of this, this region is also called the 1550 nm telecommunications window. For the loss in the fiber contribute mainly the concentration of the OH ion, with the major impact at 1383 nm, and the Rayleigh scattering [121]. Looking at the LWPF spectrum, one can see that it was possible to eliminate almost completely the water peak, which facilitates wavelength division multiplexing (WDM) schemes [120]. Up to date, the lowest fiber attenuation achieved is 0.1484 dB/km, in a pure silica-core fiber (PSCF) [122].

When polarization-encoded photons travel through an optical fiber there are mainly four problems which can affect them during transmission. The first problem causes the rotation of polarization by an angle which is related to Berry's phase [123, 124]. The second problem is fiber's birefringence, which is due to the loss of circular symmetry [125]. The third problem is the polarization-mode dispersion (PMD), which is due to a random evolution of the magnitude and the orientation of the birefringence vector along the fiber [126]. The last problem can be obtained from polarization-dependent losses (PDL) in the fiber. In the presence of PDL, two SOPs loose the relative angle between each other after propagation through an optical fiber [127]. To mitigate these problems, a robust polarization control method should be used at the output of the fiber link.

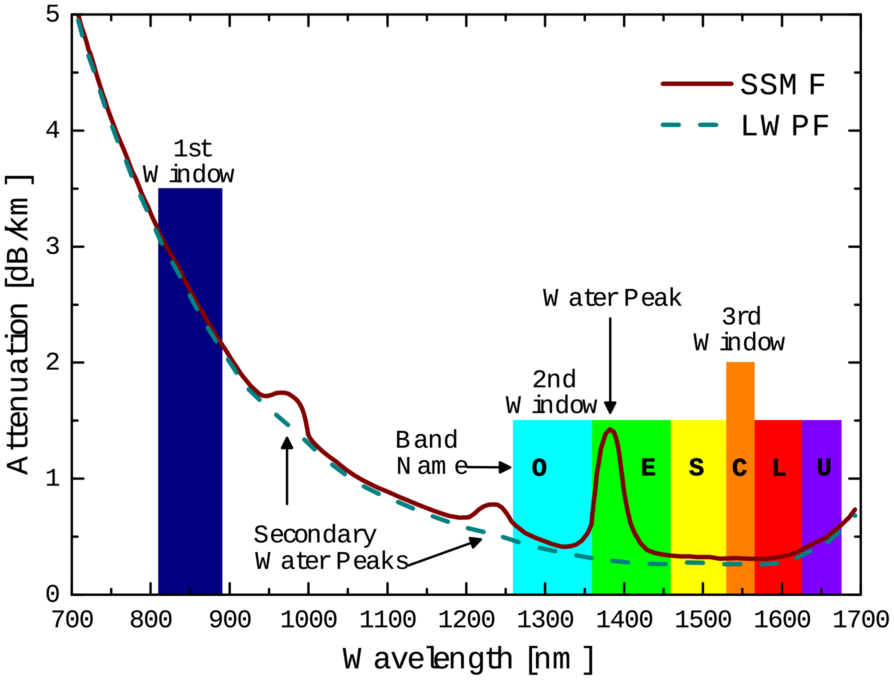

Figure 2.12: Attenuation spectrum for a standard single-mode fiber and a low-water-peak fiber [120].

2.4.4 The Decoding Scheme

Basis Selection

On the receiver's side, the 'rule' is that Bob should be able to select randomly and independently from Alice the measurement basis. In Fig. 2.13, we present two possible schemes for detection.

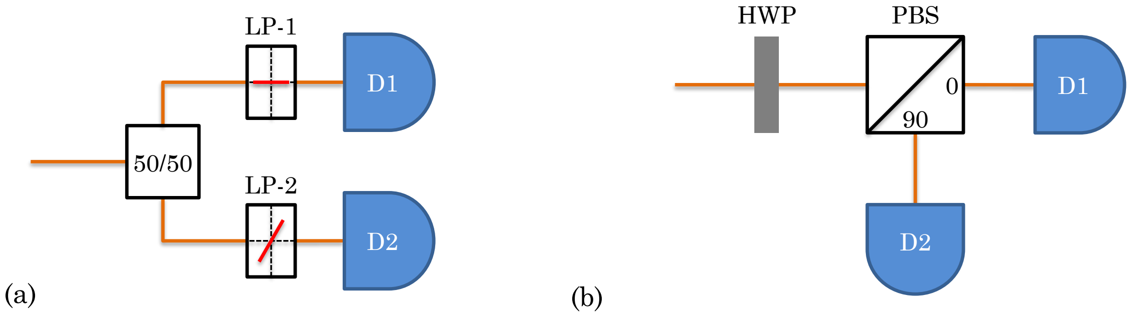

Figure 2.13: (a) Decoding scheme for two SOPs sent assuming a random selection of the basis by a 50/50 beam splitter. (b) Decoding scheme for two SOPs sent assuming the selection of the basis by a wave plate.

Fig. 2.13(a) shows the detection scheme for two nonorthogonal SOPs. In this case, a 50/50 beam splitter works as a random selector of the measurement basis, together with two linear polarizers, one set at 0° (LP-1) and the other at 45° (LP-2). If one photon encoded in the $|H\rangle$ SOP reaches the beam splitter, it has two possibilities: (i) if it goes to the upper arm, it will pass through LP-1 and reach the detector (D1) with 100% probability (in the ideal case); (ii) if it goes to the lower arm, there is a 50% probability to pass LP-2 and reach the detector (D2) and a 50% probability to be absorbed by the linear polarizer. If one photon encoded in the $|+45\rangle$ SOP reaches the beam splitter, there are also two possibilities: (i) if it goes to the upper arm it has a 50% probability to pass LP-1 and to reach the detector (D1) and also a 50% probability to be absorbed; (ii) if it goes to the lower arm, the state has a 100% probability to pass LP-2 (in the ideal case) and to reach the detector (D2). In order to detect orthogonal SOPs such as $|H\rangle$ and $|V\rangle$, one needs only to set the angle of LP-2 at 90°.

Figure 2.13(b) shows a different possibility to decode the information carried out by one state, through the use of a half-wave plate (HWP) and a PBS. The angle of the wave plate can be set at 0° or 45°. The PBS has two output ports, one at 0° and the other at 90°. When Bob sets the HWP at 0°, in practice he is choosing the rectilinear basis. For this case, and sending $|H\rangle$ or $|+45\rangle$ SOPs, there are two possibilities: (i) if Alice sends one photon encoded in $|H\rangle$ state, then it will have a 100% probability of being detected in D1 (in the ideal case); (ii) if Alice sends one photon encoded in the $|+45\rangle$ state, then it will have a 50% probability to be detected in D1 and a 50% probability to be detected in D2. If Bob sets the wave plate at $2\theta = 45°$, in practice he is selecting the diagonal basis. Similarly, for this case, there are two possibilities: (i) if Alice sends one photon encoded in the $|H\rangle$ state, then it will have a 50% probability to be detected in D1 and a 50% probability to be detected in D2; (ii) if Alice sends one photon encoded in the $|+45\rangle$ state, then it will have a 100% probability to be detected in D2 (in the ideal case). It is also possible to detect other combinations, like, for instance, when sending $|V\rangle$ or $|-45\rangle$ SOPs, simply by setting the HWP to $2\theta = 90°$ and $2\theta = -45°$, with similar results. Note that in order to achieve the random selection of the measurement basis, the wave plate must be controlled by a random number generator [128].

Photon Detection

The successful implementation of quantum protocols is highly dependent on the detection capabilities. Apart from the ability to detect photons, it is expected that an ideal single-photon detector presents many other features, such as 100% detection efficiency; no dark-count rate, no dead time and no time jitter. Besides that, an ideal single-photon detector would be able to distinguish the number of photons in an incident pulse, known as photon-number resolution, and would be also asynchronous [46]. Current photon detectors are still far from reaching all the characteristics presented above. However, remarkable advances have been made towards reaching an ideal single-photon detector [46].

In the market there are several types of detectors which have been used in the vast majority of experimental demonstrations in quantum communications, such as SPADs [64], SNSPDs [129] or NFADs [66]. SPADs are the most commonly used single-photon detectors. In addition to their affordable prices, they are very compact, making them practical to be used either in the laboratory or in real-world implementations. This type of detectors still presents a low detection efficiency, but the major problem is related to afterpulses, which results in the occurrence of spontaneous dark counts after the detection of a photon [64]. As an advantage, these detectors work at approximately room temperatures. SPADs usually work in the so-called Geiger mode. In this mode, a single photon can trigger a macroscopic current pulse, which allows the detector to sense the arrival of the photon. In practice, the Geiger-mode operation consists of several steps, namely: (i) arming the device by biasing it above a breakdown voltage, (ii) triggering an avalanche with an incident photon, (iii) quenching the avalanche by lowering the bias, and (iv) re-arming the device by again biasing above the breakdown voltage [130].

One important contribution for degrading the detector's performance are dark counts. These counts can be created for example from thermal excitation or tunneling processes [131]. One way to decrease its rate in SPADs is to operate the detector in a gated mode. In this mode, the detector is biased at a certain voltage which is slightly below the breakdown voltage. To activate the detector, a gate pulse is applied in order to increase the detector bias above the breakdown voltage for a short period of time, typically within nanoseconds [131].

2.5 Summary

As a relatively new field of study in science, quantum communications have reached surprisingly good results. The fact that the absolute security of quantum protocols is guaranteed by quantum mechanics gives even more interest to its continuous development. Even if most of the theoretical proposals are far beyond current technological capacities, the advances are also very important. Therefore, it should not be a surprise if quantum communications are available to everyone in the near future.

In this chapter, we started with the state-of-the-art of quantum communications, which led us to the current status of quantum systems and networks. Then, we presented some basic concepts in quantum information necessary to understand the encoding scheme and the security of quantum communications. We described the three protocols which served as a basis for this work, namely the BB84, the B92 and a QBC protocol. In the last part of the chapter we described all elements in a quantum communications system, from the source, to the encoding scheme, the quantum channel and the decoding scheme. With these tools we are now able to move on to a practical implementation.

References

[1] G. Brassard, "Brief history of quantum cryptography: A personal perspective," in *Theory and Practice in Information-Theoretic Security, 2005. IEEE Information Theory Workshop on*, Oct. 2005, pp. 19–23.

[2] C. H. Bennett, G. Brassad, S. Breidbard, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology: Proceedings of CRYPTO '82*, 1982, pp. 267–275.

[3] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing.* New York: IEEE Press, 1984, pp. 175–179.

[5] C. H. Bennett and G. Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working," *SIGACT News*, vol. 20, no. 4, pp. 78–80, Nov. 1989.

[6] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[7] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[8] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[9] A. Muller, J. Breguet, and N. Gisin, "Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km," *Europhys. Lett.*, vol. 23, no. 6, pp. 383–388, Aug. 1993.

[10] J. Breguet, A. Muller, and N. Gisin, "Quantum cryptography with polarized photons in optical fibres: Experiment and practical limits," *J. Mod. Opt.*, vol. 41, no. 12, pp. 2405–2412, Dec. 1994.

[11] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. Lett.*, vol. 51, no. 3, pp. 1863–1869, Mar. 1995.

[12] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, Oct. 1998.

[13] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug. 2000.

[14] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, Aug. 2003.

[15] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, p. 057901, Feb. 2004.

[16] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, Mar. 2012.

[17] E. Adlam and A. Kent, "Deterministic relativistic quantum bit commitment," *Int. J. Quantum Inf.*, vol. 13, no. 5, p. 1550029, Aug. 2015.

[18] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, "Practical relativistic bit commitment," *Phys. Rev. Lett.*, vol. 115, no. 3, p. 030502, Jul. 2015.

[19] E. Adlam and A. Kent, "Device-independent relativistic quantum bit commitment," *Phys. Rev. A*, vol. 92, no. 2, p. 022315, Aug. 2015.

[20] K. Chakraborty, A. Chailloux, and A. Leverrier, "Arbitrarily long relativistic bit commitment," *Phys. Rev. Lett.*, vol. 115, no. 25, p. 250501, Dec. 2015.

[21] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, pp. 1–32, 2015.

[22] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, "Experimental quantum coin tossing," *Phys. Rev. Lett.*, vol. 94, no. 4, p. 040501, Jan. 2005.

[23] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, "Experimental loss-tolerant quantum coin flipping," *Nat. Commun.*, vol. 2, p. 561, Nov. 2011.

[24] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, "Experimental plug and play quantum coin flipping," *Nat. Commun.*, vol. 5, p. 3717, Apr. 2014.

[25] S. Zhang and Y. Zhang, "Quantum coin flipping secure against channel noises," *Phys. Rev. A*, vol. 92, no. 2, p. 022313, Aug. 2015.

[26] J. A. Vaccaro, J. Spring, and A. Chefles, "Quantum protocols for anonymous voting and surveying," *Phys. Rev. A*, vol. 75, no. 1, p. 012333, Jan. 2007.

[27] A. Broadbent and A. Tapp, "Information-theoretically secure voting without an honest majority," Cryptology ePrint Archive, Report 2008/266, 2008.

[28] Y.-B. Li, Q.-Y. Wen, S.-J. Qin, F.-Z. Guo, and Y. Sun, "Practical quantum all-or-nothing oblivious transfer protocol," *Quantum Inf. Process.*, vol. 13, no. 1, pp. 131–139, Jan. 2014.

[29] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, "An experimental implementation of oblivious transfer in the noisy storage model," *Nat. Commun.*, vol. 5, p. 3418, Mar. 2014.

[30] H. Kobayashi, "General properties of quantum zero-knowledge proofs," in *Theory of Cryptography*, ser. Lecture Notes in Computer Science, R. Canetti, Ed. Springer Berlin Heidelberg, 2008, vol. 4948, pp. 107–124.

[31] M. Blum, "Coin flipping by telephone." in *CRYPTO*, A. Gersho, Ed. U. C. Santa Barbara, Dept. of Elec. and Computer Eng., ECE Report No 82-04, 1981, pp. 11–15.

[32] G. Brassard, D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *J. Comput. Syst. Sci.*, vol. 37, no. 2, pp. 156–189, Oct. 1988.

[33] G. Brassard, C. Crepeau, R. Jozsa, and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties," in *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, 1993, pp. 362–371.

[34] H.-K. Lo and H. F. Chau, "Is quantum bit commitment really possible?" *Phys. Rev. Lett.*, vol. 78, no. 17, pp. 3410–3413, Apr. 1997.

[35] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Phys. Rev. Lett.*, vol. 78, no. 17, pp. 3414–3417, Apr. 1997.

[36] A. Kent, "Unconditionally secure bit commitment," *Phys. Rev. Lett.*, vol. 83, no. 7, pp. 1447–1450, Aug. 1999.

[37] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," *Phys. Rev. Lett.*, vol. 109, no. 13, p. 130501, Sep. 2012.

[38] S. Croke and A. Kent, "Security details for bit commitment by transmitting measurement outcomes," *Phys. Rev. A*, vol. 86, no. 5, p. 052309, Nov. 2012.

[39] J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner, "Secure bit commitment from relativistic constraints," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4687–4699, Jul. 2013.

[40] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, "Experimental bit commitment based on quantum communication and special relativity," *Phys. Rev. Lett.*, vol. 111, no. 18, p. 180504, Nov. 2013.

[41] Y. Liu, Y. Cao, M. Curty, S.-K. Liao, J. Wang, K. Cui, Y.-H. Li, Z.-H. Lin, Q.-C. Sun, D.-D. Li, H.-F. Zhang, Y. Zhao, T.-Y. Chen, C.-Z. Peng, Q. Zhang, A. Cabello, and J.-W. Pan, "Experimental unconditionally secure bit commitment," *Phys. Rev. Lett.*, vol. 112, no. 1, p. 010504, Jan. 2014.

[42] A. Danan and L. Vaidman, "Practical quantum bit commitment protocol," *Quantum Inf. Process.*, vol. 11, no. 3, pp. 769–775, Jun. 2012.

[43] R. Loura, Á. J. Almeida, P. S. André, A. N. Pinto, P. Mateus, and N. Paunković, "Noise and measurement errors in a practical two-state quantum bit commitment protocol," *Phys. Rev. A*, vol. 89, no. 5, p. 052336, May 2014.

[44] Á. J. Almeida, A. D. Stojanovic, N. Paunkovic, R. Loura, N. J. Muga, N. A. Silva, P. Mateus, P. S. André, and A. N. Pinto, "Implementation of a two-state quantum bit commitment protocol in optical fibers," *J. Opt.*, vol. 18, no. 1, p. 015202, Jan. 2016.

[45] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Mod. Phys.*, vol. 81, no. 2, pp. 865–942, Apr. 2009.

[46] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, Jul. 2011.

[47] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Jul. 2009.

[48] P. F. Antunes, A. N. Pinto, and P. S. André, "Single-photon source by means of four-wave mixing inside a dispersion-shifted optical fiber," in *Proc. of Frontiers in Optics*. Optical Society of America, Oct. 2006, p. FMJ3.

[49] N. A. Silva, N. J. Muga, and A. N. Pinto, "Influence of the stimulated Raman scattering on the four-wave mixing process in birefringent fibers," *J. Lightwave Technol.*, vol. 27, no. 22, pp. 4979–4988, Nov. 2009.

[50] N. A. Silva, N. J. Muga, and A. N. Pinto, "Effective nonlinear parameter measurement using FWM in optical fibers in a low power regime," *IEEE J. Quant. Electron.*, vol. 46, no. 3, pp. 285–291, Mar. 2010.

[51] Á. J. Almeida, N. A. Silva, N. J. Muga, and A. N. Pinto, "Fiber-optical communication system using polarization-encoding photons," in *Proc. of 15th European Conference on Networks and Optical Communications and 5th Conference on Optical Cabling and Infrastructure, NOC/OC&I*, Jun. 8-10, 2010, pp. 127–132.

[52] Á. J. Almeida, N. A. Silva, N. J. Muga, and A. N. Pinto, "Single-photon source using stimulated FWM in optical fibers for quantum communication," in *Proc. SPIE 8001*, May 3, 2011, p. 80013W.

[53] Á. J. Almeida, N. A. Silva, P. S. André, and A. N. Pinto, "Four-wave mixing: Photon statistics and the impact on a co-propagating quantum signal," *Opt. Commun.*, vol. 285, no. 12, pp. 2956–2960, Jun. 2012.

[54] H. Takesue and K. Inoue, "Generation of polarization-entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop," *Phys. Rev. A*, vol. 70, no. 3, p. 031802, Sep. 2004.

[55] Á. J. Almeida, S. R. Carneiro, N. A. Silva, N. J. Muga, and A. N. Pinto, "Polarization-entangled photon pairs using spontaneous four-wave mixing in a fiber loop," in *Proc. of International Conference on Computer as a Tool (EUROCON), IEEE, Lisbon, Portugal*, Apr. 27-29, 2011, pp. 1–4.

[56] J. B. Spring, P. S. Salter, B. J. Metcalf, P. C. Humphreys, M. Moore, N. Thomas-Peter, M. Barbieri, X.-M. Jin, N. K. Langford, W. S. Kolthammer, M. J. Booth, and I. A. Walmsley, "On-chip low loss heralded source of pure single photons," *Opt. Express*, vol. 21, no. 11, pp. 13 522–13 532, Jun. 2013.

[57] N. A. Silva and A. N. Pinto, "Comprehensive characterization of a heralded single photon source based on four-wave mixing in optical fibers," *Opt. Commun.*, vol. 327, pp. 31–38, Sep. 2014.

[58] X. Ma and H.-K. Lo, "Quantum key distribution with triggering parametric down-conversion sources," *New J. Physics*, vol. 10, no. 7, p. 073018, Jul. 2008.

[59] C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, T. Zhong, L. Wang, X. Hu, R. D. Horansky, V. B. Verma, A. E. Lita, R. P. Mirin, F. Marsili, M. D. Shaw, S. W. Nam, G. W. Wornell, F. N. C. Wong, J. H. Shapiro, and D. Englund, "Entanglement-based quantum communication secured by nonlocal dispersion cancellation," *Phys. Rev. A*, vol. 90, no. 6, p. 062331, Dec. 2014.

[60] P. S. Michelberger, T. F. M. Champion, M. R. Sprague, K. T. Kaczmarek, M. Barbieri, X. M. Jin, D. G. England, W. S. Kolthammer, D. J. Saunders, J. Nunn, and I. A. Walmsley, “Interfacing ghz-bandwidth heralded single photons with a warm vapour raman memory,” *New J. Phys.*, vol. 17, no. 4, p. 043006, Apr. 2015.

[61] F. Kaneda, B. G. Christensen, J. J. Wong, H. S. Park, K. T. McCusker, and P. G. Kwiat, “Time-multiplexed heralded single-photon source,” *Optica*, vol. 2, no. 12, pp. 1010–1013, Dec. 2015.

[62] S. Bäuml, M. Christandl, K. Horodecki, and A. Winter, “Limitations on quantum key repeaters,” *Nat. Commun.*, vol. 6, p. 6908, Apr. 2015.

[63] A. Khalique and B. C. Sanders, “Practical long-distance quantum key distribution through concatenated entanglement swapping with parametric down-conversion sources,” *J. Opt. Soc. Am. B*, vol. 32, no. 11, pp. 2382–2390, Nov. 2015.

[64] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, “Advances in InGaAs/InP single-photon detector systems for quantum communication,” *Light Sci. Appl.*, vol. 4, p. e286, May 2015.

[65] P. Rath, O. Kahl, S. Ferrari, F. Sproll, G. Lewes-Malandrakis, D. Brink, K. Ilin, M. Siegel, C. Nebel, and W. Pernice, “Superconducting single photon detectors integrated with diamond nanophotonic circuits,” *Light Sci. Appl.*, vol. 4, p. e338, Oct. 2015.

[66] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, “Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency,” *Appl. Phys. Lett.*, vol. 104, no. 8, p. 081108, Feb. 2014.

[67] C. Elliott, “Building the quantum network,” *New J. Phys.*, vol. 4, no. 1, p. 46, Jul. 2002.

[68] 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 J. Phys.*, vol. 11, no. 7, p. 075001, Jul. 2009.

[69] 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,” *Chin. Sci. Bull.*, vol. 54, no. 17, pp. 2991–2997, Jun. 2009.

[70] 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 J. Phys.*, vol. 13, no. 12, p. 123001, Dec. 2011.

[71] 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*, vol. 19, no. 11, pp. 10 387–10 409, May 2011.

[72] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441–442, Apr. 2014.

[73] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, "Entanglement distribution over 300 km of fiber," *Opt. Express*, vol. 21, no. 20, pp. 23 241–23 249, Oct. 2013.

[74] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photon.*, vol. 9, no. 3, pp. 163–168, Mar. 2015.

[75] N. Gisin, "How far can one send a photon?" *Front. Phys.*, vol. 10, no. 6, p. 100307, Oct. 2015.

[76] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144km," *Nat. Phys.*, vol. 3, no. 7, pp. 481–486, Jul. 2007.

[77] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Ultrafast and fault-tolerant quantum communication across long distances," *Phys. Rev. Lett.*, vol. 112, no. 25, p. 250501, Jun. 2014.

[78] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon, "Entanglement over global distances via quantum repeaters with satellite links," *Phys. Rev. A*, vol. 91, no. 5, p. 052325, May 2015.

[79] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.

[80] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "Quantum cryptography: A step towards global key distribution," *Nature*, vol. 419, no. 6906, p. 450, Oct. 2002.

[81] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, no. 1, p. 82, Oct. 2002.

[82] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," *IEEE J. Sel. Top. Quantum Electron.*, vol. 9, no. 6, pp. 1541–1551, Nov. 2003.

[83] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger, "Influence of satellite motion on polarization qubits in a space-earth quantum communication link," *Opt. Express*, vol. 14, no. 21, pp. 10 050–10 059, Oct. 2006.

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

[85] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New J. Phys.*, vol. 15, no. 2, p. 023006, Feb. 2013.

[86] T. Scheidl, E. Wille, and R. Ursin, "Quantum optics experiments using the international space station: A proposal," *New J. Phys.*, vol. 15, no. 4, p. 043008, Apr. 2013.

[87] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, no. 4, p. 040502, Jul. 2015.

[88] H. Takesue, S. D. Dyer, M. J. Stevens, V. Verma, R. P. Mirin, and S. W. Nam, "Quantum teleportation over 100 km of fiber using highly-efficient superconducting nanowire single photon detectors," *Optica*, vol. 2, no. 10, pp. 832–835, Oct. 2015.

[89] N. Horiuchi, "View from... QCMC 2014: Expanding ambitions," *Nature Photon.*, vol. 9, no. 1, pp. 13–14, Jan. 2015.

[90] (http://www.idquantique.com), (http://www.magiqtech.com), (http://www.quintessencelabs.com), (http://www.sequrenet.com), (http://aureatechnology.net), (http://www.scontel.ru), (http://www.smartquantum.com), (http://www.dwavesys.com), Accessed January 14, 2016.

[91] B. Schumacher, "Quantum coding," *Phys. Rev. A*, vol. 51, no. 4, pp. 2738–2747, Apr. 1995.

[92] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, Dec. 2010.

[93] W. Heisenberg, "Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik," *Zeitschrift für Physik*, vol. 43, no. 3, pp. 172–198, Mar. 1927.

[94] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, pp. 802–803, Oct. 1982.

[95] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, "Quantum cloning," *Rev. Mod. Phys.*, vol. 77, no. 4, pp. 1225–1256, Oct. 2005.

[96] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, and L.-Z. Mu, "Quantum cloning machines and the applications," *Phys. Rep.*, vol. 544, no. 3, pp. 241–322, Nov. 2014.

[97] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, "14-qubit entanglement: Creation and coherence," *Phys. Rev. Lett.*, vol. 106, no. 13, p. 130506, Apr. 2011.

[98] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, "Observation of eight-photon entanglement," *Nature Photon.*, vol. 6, no. 4, pp. 225–228, Apr. 2012.

[99] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 45–53, Mar. 2010.

[100] B.-C. Ren and F.-G. Deng, "Hyper-parallel photonic quantum computation with coupled quantum dots," *Sci. Rep.*, vol. 4, p. 4623, Apr. 2014.

[101] I. M. Georgescu, S. Ashhab, and F. Nori, "Quantum simulation," *Rev. Mod. Phys.*, vol. 86, no. 1, pp. 153–185, Mar. 2014.

[102] G. Evenbly and G. Vidal, "Class of highly entangled many-body states that can be efficiently simulated," *Phys. Rev. Lett.*, vol. 112, no. 24, p. 240502, Jun. 2014.

[103] D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," in *Advances in Cryptology — CRYPTO '96*, ser. Lecture Notes in Computer Science, N. Koblitz, Ed. Springer Berlin Heidelberg, 1996, vol. 1109, pp. 343–357.

[104] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," *eprint arXiv:quant-ph/9912053*, Dec. 1999.

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

[106] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.

[107] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, May 2001.

[108] M. Koashi and J. Preskill, "Secure quantum key distribution with an uncharacterized source," *Phys. Rev. Lett.*, vol. 90, no. 5, p. 057902, Feb. 2003.

[109] H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," *EPJ D*, vol. 41, no. 3, pp. 599–627, Mar. 2007.

[110] T. Tsurumaru and K. Tamaki, "Security proof for quantum-key-distribution systems with threshold detectors," *Phys. Rev. A*, vol. 78, no. 3, p. 032302, Sep. 2008.

[111] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, no. 4, p. 045018, Apr. 2009.

[112] Z. Quan and T. Chaojing, "Simple proof of the unconditional security of the Bennett 1992 quantum key distribution protocol," *Phys. Rev. A*, vol. 65, no. 6, p. 062301, May 2002.

[113] K. Tamaki, M. Koashi, and N. Imoto, "Security of the Bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel," *Phys. Rev. A*, vol. 67, no. 3, p. 032310, Mar. 2003.

[114] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally secure key distribution based on two nonorthogonal states," *Phys. Rev. Lett.*, vol. 90, no. 16, p. 167904, Apr. 2003.

[115] K. Tamaki and N. Lütkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel," *Phys. Rev. A*, vol. 69, no. 3, p. 032316, Mar. 2004.

[116] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, "Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse," *Phys. Rev. A*, vol. 80, no. 3, p. 032302, Sep. 2009.

[117] M. Lucamarini, G. di Giuseppe, and K. Tamaki, "Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states," *Phys. Rev. A*, vol. 80, no. 3, p. 032327, Sep. 2009.

[118] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner, "Reexamination of quantum bit commitment: The possible and the impossible," *Phys. Rev. A*, vol. 76, no. 3, p. 032328, Sep. 2007.

[119] B. Lounis and M. Orrit, "Single-photon sources," *Rep. Prog. Phys.*, vol. 68, no. 5, pp. 1129–1179, May 2005.

[120] J. M. Senior, *Optical Fiber Communications: Principles and Practice, 3rd ed.*, J. M. Senior and M. Yousif Jamro, Eds. Pearson Education Limited, 2009.

[121] G. Agrawal, *Nonlinear Fiber Optics, 5th ed.*, G. Agrawal, Ed. Academic Press, 2013.

[122] K. Nagayama, M. Kakui, M. Matsui, T. Saitoh, and Y. Chigusa, "Ultra-low-loss (0.1484 dB/km) pure silica core fibre and extension of transmission distance," *Electron. Lett.*, vol. 38, no. 20, pp. 1168–1169, Sep. 2002.

[123] R. Y. Chiao and Y.-S. Wu, "Manifestations of Berry's topological phase for the photon," *Phys. Rev. Lett.*, vol. 57, no. 8, pp. 933–936, Aug. 1986.

[124] A. Tomita and R. Y. Chiao, "Observation of Berry's topological phase by use of an optical fiber," *Phys. Rev. Lett.*, vol. 57, no. 8, pp. 937–940, Aug. 1986.

[125] H. Kogelnik, R. M. Jopson, and L. E. Nelson, "Polarization-mode dispersion," in *Optical Fiber Telecommunications IV-B: Systems and Impairments*, 4th ed., I. P. Kaminow and T. Li, Eds. Academic Press, Apr. 2002, ch. 15, pp. 725–861.

[126] J. P. Gordon and H. Kogelnik, "PMD fundamentals: Polarization mode dispersion in optical fibers," *Proc. Natl. Acad. Sci. U.S.A.*, vol. 97, no. 9, pp. 4541–4550, Apr. 2000.

[127] N. Gisin and B. Huttner, "Combined effects of polarization mode dispersion and polarization dependent losses in optical fibers," *Opt. Commun.*, vol. 142, no. 1-3, pp. 119–125, Feb. 1997.

[128] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, "Experimental evidence of quantum randomness incomputability," *Phys. Rev. A*, vol. 82, no. 2, p. 022102, Aug. 2010.

[129] F. Mattioli, Z. Zhou, A. Gaggero, R. Gaudio, S. Jahanmirinejad, D. Sahin, F. Marsili, R. Leoni, and A. Fiore, "Photon-number-resolving superconducting nanowire detectors," *Supercond. Sci. Technol.*, vol. 28, no. 10, p. 104001, 2015.

[130] M. Itzler, X. Jiang, M. Entwistle, K. Slomkowski, A. Tosi, F. Acerbi, F. Zappa, and S. Cova, "Advances in InGaAsP-based avalanche diode single photon detectors," *J. Mod. Opt.*, vol. 58, no. 3-4, pp. 174–200, Jan. 2011.

[131] M. A. Itzler, R. Ben-Michael, C.-F. Hsu, K. Slomkowski, A. Tosi, S. Cova, F. Zappa, and R. Ispasoiu, "Single photon avalanche diodes (SPADs) for 1.5 μm photon counting applications," *J. Mod. Opt.*, vol. 54, no. 2-3, pp. 283–304, Jan. 2007.

Chapter 3

Photon Sources for Systems based on Discrete Variables

3.1 Introduction

SINGLE-photon sources find a wide range of applications in the field of quantum information [1]. Quantum cryptography, which could very well be the first real-world application of quantum mechanics, is one of the main motivations for its continuous study [2]. As shown in Chapter 2, probabilistic photon sources can be obtained from an attenuated laser [3–5] or parametric down-conversion (PDC) [6, 7]. The use of an attenuated laser is one of the most common and simple approximations [8]. However, there are other methods to generate probabilistic photon sources which are equally simple and valid, like the use of the four-wave mixing (FWM) process [9–17].

In this chapter, we show the implementation of a probabilistic photon source based on the stimulated FWM process and the characterization of its photon statistics. Next, we show results from the study of the impact of the FWM in a quantum signal co-propagating in the system. Finally, we show the implementation of an entangled-photon source using the spontaneous FWM process. With this source we demonstrate the violation of Clauser-Horne-Shimony-Holt (CHSH) inequality.

3.2 The Four-Wave Mixing Process

The FWM process is a nonlinear effect described by the third-order nonlinear susceptibility in optical fibers [18]. Its origin lies in the nonlinear response of bound electrons to an optical field crossing the fiber [18]. Depending on the implementation, it is possible to obtain both a spontaneous and stimulated process from the FWM [13, 19]. Fig. 3.1 shows the single-pump configuration in the stimulated FWM process, when the pump and the signal waves are sent co-polarized to an optical fiber. When pump (λ_{p}) and signal (λ_{s}) waves are sent together to

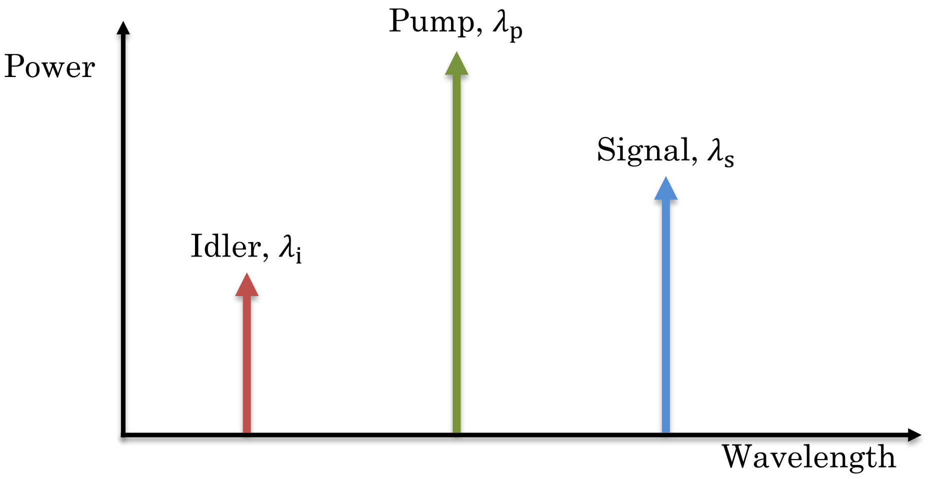

Figure 3.1: Schematic diagram of the signals involved in the single-pump stimulated FWM process in optical fibers.

an optical fiber, they will interact and generate a third wave, which is called idler (λ_i). The frequency of the three waves should then follow the equation,

$$2\omega_p = \omega_s + \omega_i, \tag{3.1}$$

where $\omega_{\{p,\,s,\,i\}} = 2\pi c/\lambda_{\{p,\,s,\,i\}}$, with c representing the speed of light [20].

In the spontaneous FWM process only the pump wave is sent to the fiber, generating correlated photons in a broad spectrum, as shown in Fig. 3.2. The correlated signal-idler

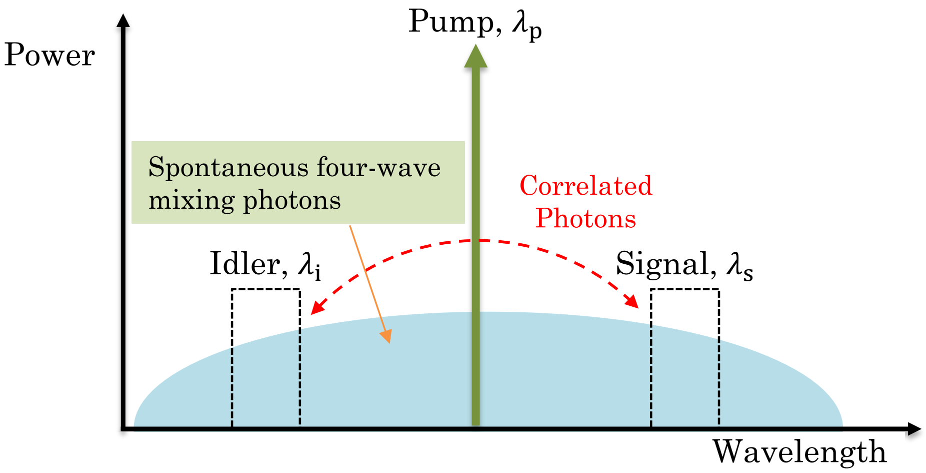

Figure 3.2: Schematic diagram of the signals involved in the single-pump spontaneous FWM process in optical fibers.

photons should verify Eq. (3.1) and their wavelengths can be selected using optical filters.

After this brief introduction, we will now focus on the stimulated FWM process with the aim of generating a probabilistic photon source. As we have said, the generation of idler photons from this source is obtained with the stimulated FWM process. A very important characteristic of the idler wave is that the average number of photons generated in that wave depends on the power sent to the fiber. In order to control it, we can set different powers in the pump and signal waves.

In order to verify the effective generation of the idler wave from the stimulated FWM process, we have implemented the experimental setup shown in Fig. 3.3. In the experiment, the pump ($\lambda_p = 1549.32\,\text{nm}$) and signal ($\lambda_s = 1550.92\,\text{nm}$) waves were obtained from a tunable laser source (TLS) and from an external cavity laser (ECL), respectively. The pump power was set as 13.45 dBm and the signal power as 9.45 dBm. The two waves were coupled in a 50/50 coupler and then reached a linear polarizer (LP). Two polarization controllers (PC-1 and PC-2) were used to adjust the polarization of the photons in order to send both waves co-polarized into a dispersion-shifted fiber (DSF) with a length of 8886 m. The co-polarization of the two waves is necessary to guarantee maximum efficiency in the generation of idler photons [19]. Data were obtained with an Optical Spectrum Analyzer (OSA).

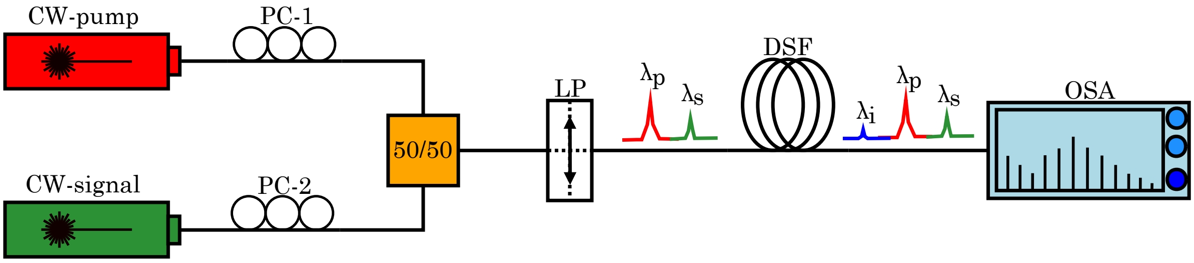

Figure 3.3: Schematics of the experimental setup used to generate idler photons from the stimulated FWM process.

In Fig. 3.4 we show the spectrum of the three waves involved in the stimulated FWM process. This spectrum allows us to draw two main conclusions. First, we verify that the idler wave was effectively generated at a much lower power than the pump and signal waves. Second, we conclude that the idler wave was generated at the expected wavelength, since it verifies Eq. (3.1). Note that the slight differences between the wavelengths set and registered are due to errors in the measurement device.

After verifying the efficient generation of the idler wave, we then wanted to be sure that we were able to control the average number of photons in it. The average number of photons is directly related to the power of the wave, *i.e.*, the larger the power, the larger will the number of photons in the wave be. To determine the optical power of the idler wave we can use

$$P_i(L) = (\gamma P_p(0) L_{\text{eff}})^2 P_s(0) \exp(-\alpha_f L)\eta, \tag{3.2}$$

where γ is the nonlinear parameter of the fiber, $P_p(0)$ and $P_s(0)$ are the input pump and signals powers, respectively, L_{eff} is the effective fiber length[1], α_f is the fiber attenuation coefficient, L is

[1] Length of the fiber where signals can effectively interact. In the absence of losses, $\alpha_f = 0$, and $L_{\text{eff}} = L$ [18].

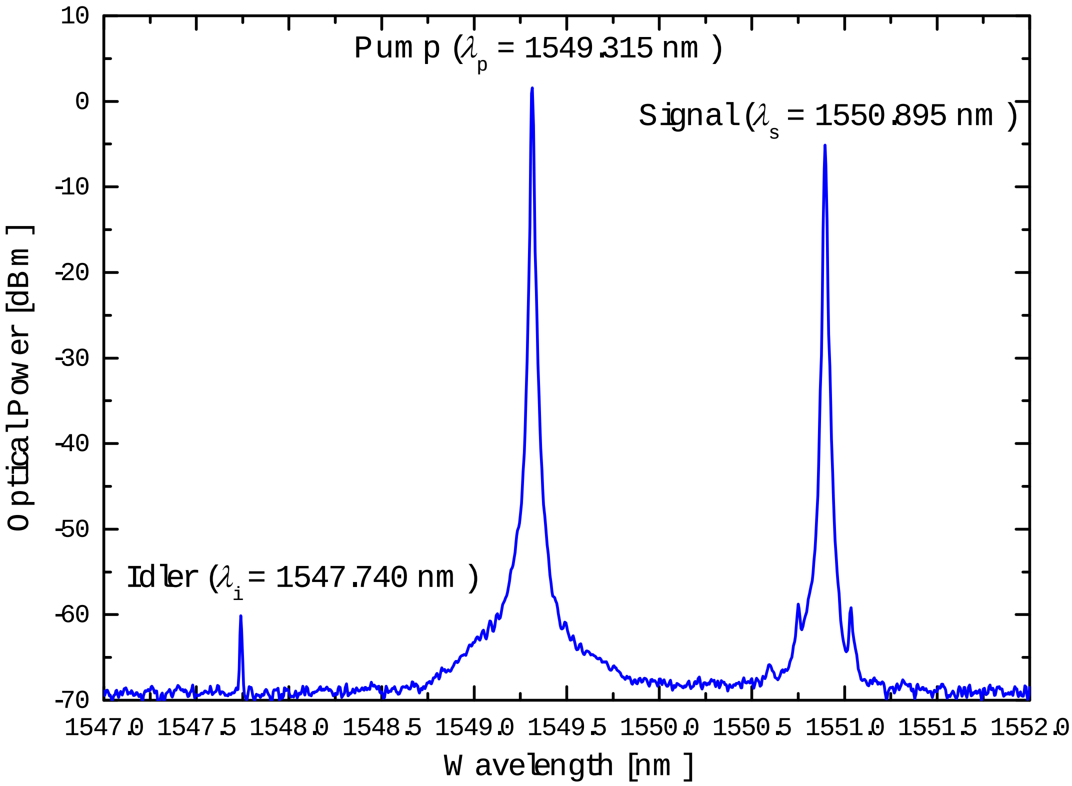

Figure 3.4: Optical spectrum of the three waves involved in the stimulated FWM process, obtained using an OSA.

the fiber length and η is the efficiency of photon generation [21, 22]. The effective fiber length can be calculated from [21, 22]

$$L_{\text{eff}} = \frac{1 - \exp\left(-\alpha_{\text{f}} L\right)}{\alpha_{\text{f}}}. \tag{3.3}$$

Moreover, the efficiency of photon generation is calculated from [21, 22]

$$\eta = \frac{\alpha_{\text{f}}^2}{\alpha_{\text{f}}^2 + \Delta\beta^2}\left[1 + \frac{4\exp(-\alpha_{\text{f}} L)\sin^2(\Delta\beta L/2)}{(1 - \exp(-\alpha_{\text{f}} L))^2}\right], \tag{3.4}$$

where the phase-matching condition is given by

$$\Delta\beta = -\frac{2\pi c \lambda_0^3}{\lambda_{\text{p}}^3 \lambda_{\text{s}}^2}(\lambda_{\text{p}} - \lambda_0)(\lambda_{\text{p}} - \lambda_{\text{s}})^2 S(\lambda_0)\,, \tag{3.5}$$

and $S(\lambda_0)$ represents the dispersion slope of the fiber at the zero-dispersion wavelength (ZDW) [21, 22].

With the experimental setup shown in Fig. 3.3, we have measured the optical power of the idler photons assuming different powers in the signal wave. The first step to define the wavelength of the pump wave was to determine the ZDW of the fiber, which we have done using an Optical Network Analyzer (ONA). This is important due to the fact that if the pump is too far from the ZDW, the efficiency of the process will be very small. In practice, what we have measured with the ONA was the group delay (GD) of the fiber as a function of the wavelength. The ZDW of an optical fiber is the wavelength where the derivative of the GD is null. The spectrum obtained is shown in Fig. 3.5. From the measurement we found that the ZDW is $\lambda_0 = 1550.34$ nm. As described in [23], the maximum efficiency of the FWM process is obtained when the pump is sent at the ZDW of the fiber. However, if we set the pump at the ZDW, according with our model, see Eqs. (3.4) and (3.5), the efficiency of the process is both maximum and constant, independently of λ_s. Nevertheless, in order to obtain the value of the fiber nonlinear parameter, usually λ_p is slightly deviated from λ_0, which is also in the validity region of our model. Due to this, we have chosen $\lambda_p = 1552.32$ nm. For the signal wavelength we have started with $\lambda_s = 1552$ nm and then changed it in steps of 0.5 nm.

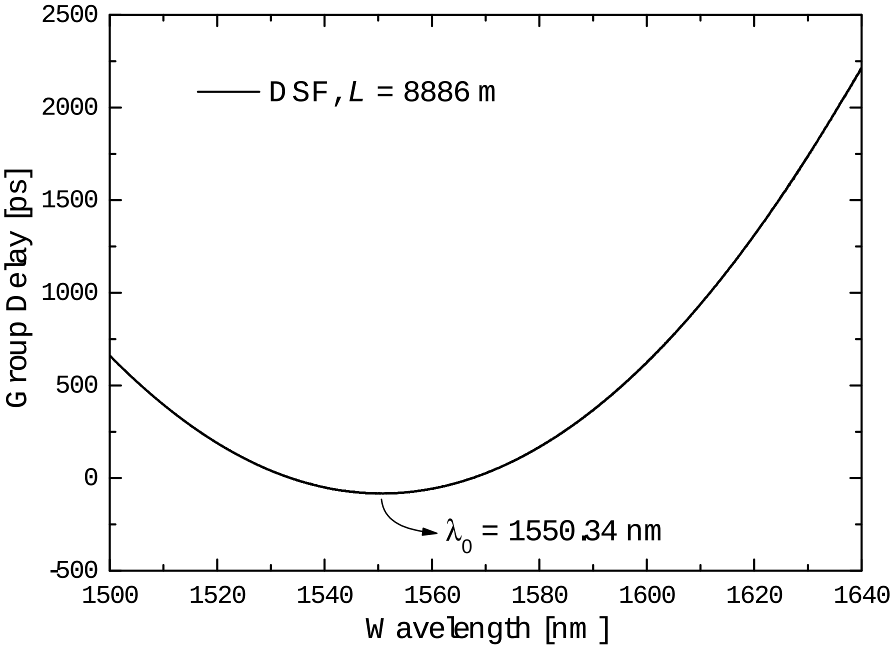

Figure 3.5: Spectral measurement of the group delay as a function of the wavelength in a DSF.

The experimental results for the optical power of the idler photons as a function of the signal wavelength are shown in Fig. 3.6. The results were fitted with Eq. (3.2), which is also shown in Fig. 3.6. A good match between experimental and theoretical data is observed. From the theoretical fit we were able to determine the nonlinear parameter as $\gamma = 2.03 \pm 1 \times 10^{-5}\ \mathrm{W}^{-1}\mathrm{km}^{-1}$ and the dispersion slope at the ZDW as $S(\lambda_0) = 0.050 \pm 8.1 \times 10^{-4}\ \mathrm{ps\,m}^{-2}\,\mathrm{km}^{-1}$. The theoretical fit was obtained with an adjusted R-squared parameter, $R^2 = 0.9988$.

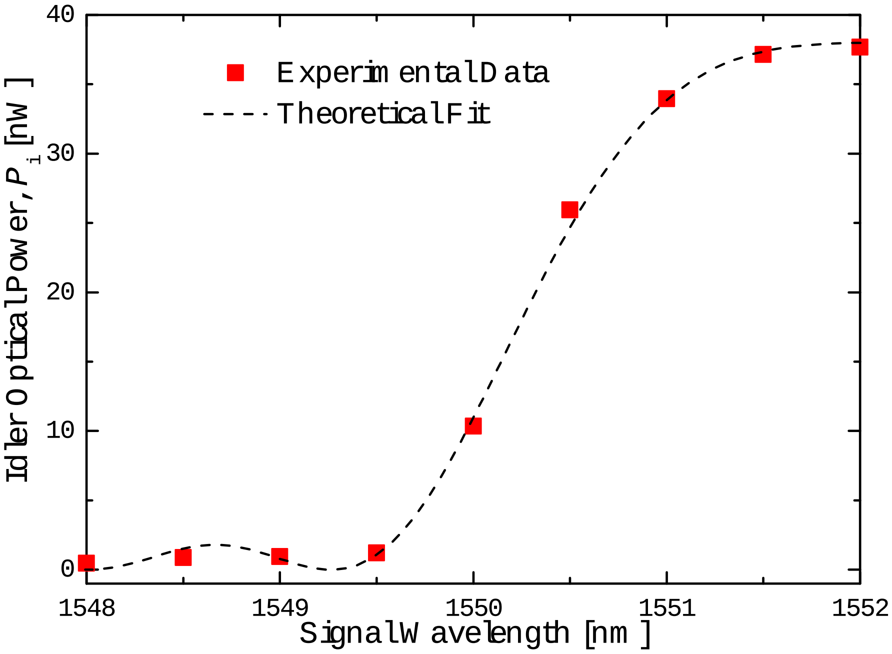

Figure 3.6: Experimental results for the idler optical power as a function of the signal wavelength. The theoretical fit was obtained from Eq. (3.2).

3.3 Probabilistic Photon Source based on Stimulated FWM

The implementation of a probabilistic photon source based on the stimulated FWM process was first demonstrated in [9, 10]. Following these works, we simplified significantly the implementation of the source and improved its efficiency. Fig. 3.7 shows the schematics of the experimental setup which can be used in a practical implementation of a photon source based on the stimulated FWM process. As shown in Fig. 3.3, pump and signal waves are sent co-polarized to a DSF, where the idler photons are generated. The signal wave is modulated using a Mach-Zehnder Modulator (MZM) to produce pulses which will be able to be detected with a Single-Photon Avalanche Detector (SPAD). The filters after the DSF are used to remove the pump and signal waves, so that only the idler wave is detected.

3.3.1 Photon Statistics of the FWM Photon Source

The characterization of the statistics of a photon source is of major importance so that one can know its true nature [2]. Different techniques have been used to do this task, such as quantum tomography [24, 25], time-multiplexing techniques [26] or using photomultiplier tubes [27]. A different approach using on/off SPADs operating in the Geiger mode, assisted by

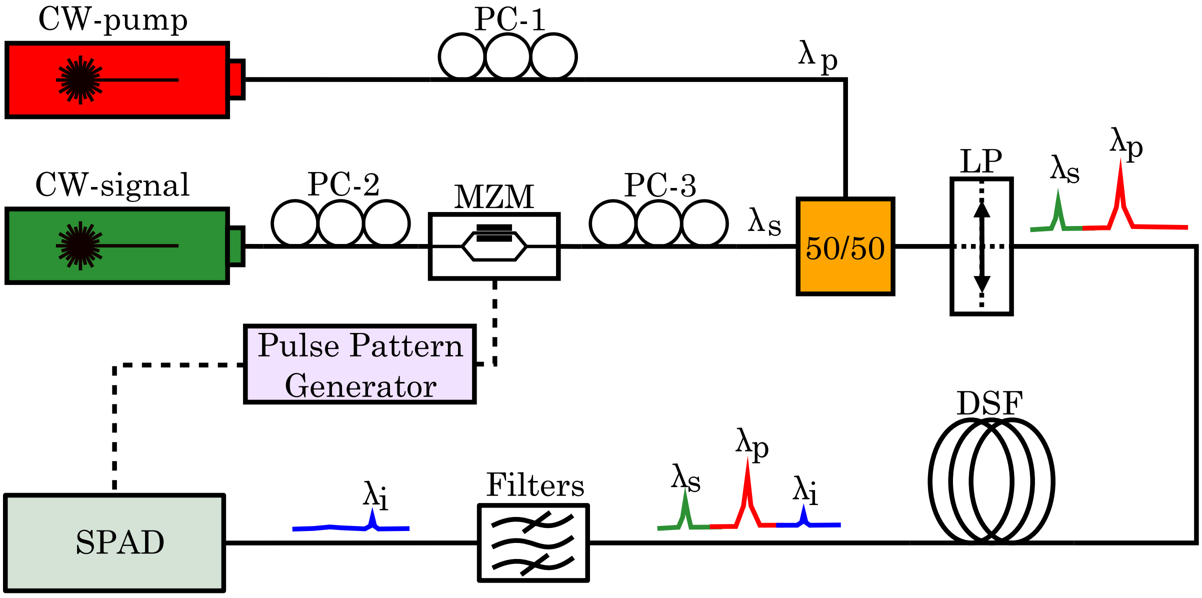

Figure 3.7: Schematics of the experimental setup used to generate photons from the stimulated FWM process in optical fibers.

the maximum-likelihood estimation (MLE) method and the expectation-maximization (EM) algorithm, was also used [28].

For the characterization of the statistics of the stimulated FWM photon source we will use the method described in [28]. To do so, we combined experimental measurements with a numerical reconstruction method, which we will explain next in detail.

Experimental Setup

The first step to determine the statistics of the FWM photon source is to measure the count rate in the detector for different numbers of idler photons generated. The schematics of the experimental setup used for the measurements is shown in Fig. 3.8. The setup is the same as depicted in Fig. 3.7, except for a variable optical attenuator (VOA) which was inserted before the SPAD. The VOA combined with the SPAD can be seen as a variable efficiency detector, since the SPAD has a fixed quantum efficiency. Next, we present the description of the experimental setup.

A pump from a continuous-wave (CW) TLS, centered at $\lambda_\text{p} = 1550.918\,\text{nm}$, passes through a polarization controller (PC-1), before being coupled (50/50) with an optical signal from an ECL centered at $\lambda_\text{s} = 1547.715\,\text{nm}$. This second optical signal passes through another polarization controller (PC-2) and is externally modulated (MZM) to produce optical pulses with a full-width at half maximum (FWHM) of approximately 1 ns and a repetition rate of $f_\text{rep} = 1.22\,\text{MHz}$. After modulation, the signal passes through PC-3, in order to ensure that it will be co-polarized with the pump at the output of the linear polarizer (LP). The two optical signals are launched into a DSF, where the idler photons are generated through FWM. The DSF

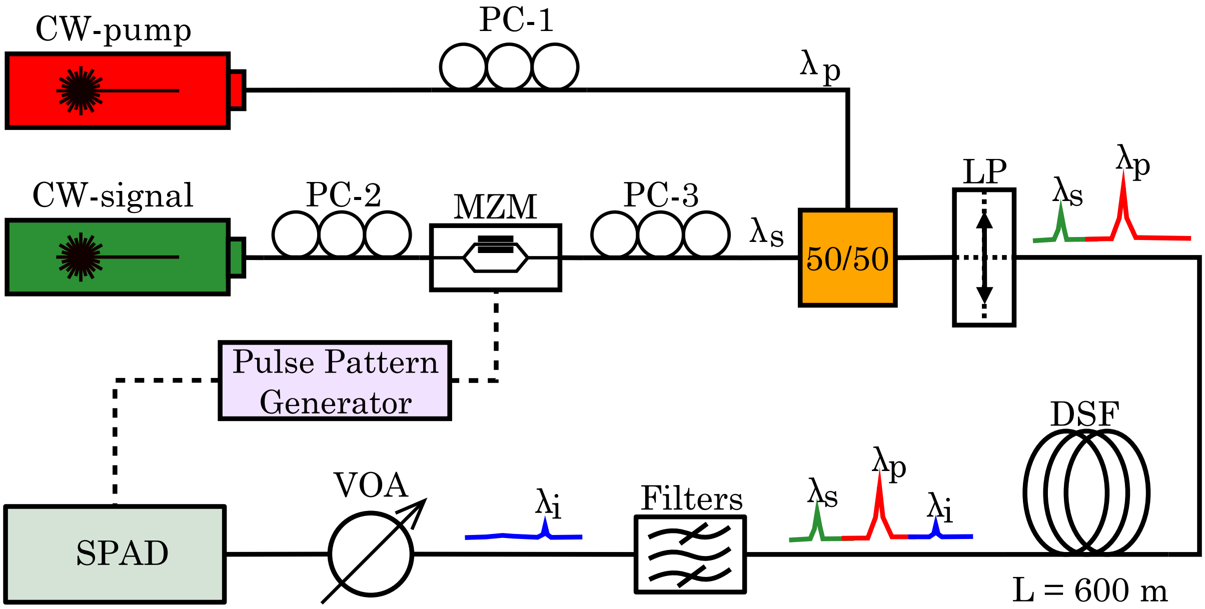

Figure 3.8: Schematics of the experimental setup used to obtain the statistics of FWM photon source.

has a ZDW, $\lambda_0 \approx 1550\,\text{nm}$, a dispersion slope at the ZDW, $S(\lambda_0) \approx 0.071\,\text{ps}\,\text{m}^{-2}\,\text{km}^{-1}$, length, $L = 600$ m, attenuation, $\alpha_{\text{f}} \approx 0.2\,\text{dB/km}$, and a nonlinear coefficient, $\gamma \approx 2.3\,\text{W}^{-1}\text{km}^{-1}$. After the fiber, two cascaded flat-top dense wavelength-division multiplexing (DWDM) optical filters with a 100 GHz passband width and centered at 1552.43 nm are used to suppress the pump and signal waves. The idler photons pass through the filters and the VOA and reach a SPAD operating in the Geiger mode. Before the measurements, the gate duration and the deadtime were set as 5 ns and 10 μs, respectively. The quantum detection efficiency and the probability of having dark counts in the SPAD were measured as $\eta_{\text{D}} \approx 10\%$ and $P_{\text{dc}} = 2.55 \times 10^{-5}$, respectively.

Numerical Reconstruction Method

The numerical method used for reconstruction of the photon statistics through on/off detection was first introduced in [29] and then experimentally implemented in [28]. An on/off detection can also be seen as click/no-click events occurring in the detector. Therefore, as described in [28], the statistics of the no-click events in the SPAD is given by

$$p_\nu^{\text{off}}(\eta_\nu) = (1 - P_{\text{dc}}) \sum_{n=0}^{N} (1 - \eta_\nu)^n \rho_n \,, \tag{3.6}$$

where η_ν, with $\nu = 1 \ldots K$, are the values of the combined efficiencies of the SPAD and the VOA, and ρ_n is the probability to detect n photons. In order to find the solution for ρ_n it can be used the MLE method and the EM algorithm, since the model is linear and the parameters are positive [28]. Therefore, solving Eq. (3.6) gives

$$\rho_n^{(i+1)} = \frac{\rho_n^{(i)}}{\sum\limits_{j=1}^{K} A_{jn}} \sum_{\nu=1}^{K} f_\nu \frac{A_{\nu n}}{p_\nu^{\mathrm{off}}[\{\rho_n^{(i)}\}]}, \tag{3.7}$$

where $A_{\nu n} = (1 - P_{\mathrm{dc}})(1 - \eta_\nu)^n$, f_ν denotes the experimental frequencies of the no-click events for the efficiency η_ν, and $p_\nu^{\mathrm{off}}[\{\rho_n^{(i)}\}]$ represents the no-click probability obtained from the reconstructed distribution $\{\rho_n^{(i)}\}$ [28]. In the numerical algorithm we set the upper limit in the sum of Eq. (3.6) to $N = K - 1 = 30$, where K are the different combined efficiencies considered. This allows the verification of the condition

$$\sum_{n=0}^{N} \rho_n \approx 1. \tag{3.8}$$

The reliability of this method was confirmed in several works, showing that it is robust against fluctuations in the values of η_ν, even if the detectors present values as low as 10 % [30–32]. Also, the reconstruction of the photon statistics can be obtained with very high values of fidelity [30].

Probability Distribution of Poissonian and Thermal Light Sources

It is common that the statistics of photon sources follow Poissonian or thermal distributions. For example, the light from a stable laser is a wave with constant amplitude and phase which is represented as a coherent state [33, 34]. The number of photons in such a state is a variable that fluctuates according to a Poissonian distribution, which is given by

$$P_{\mathrm{P}}(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}, \tag{3.9}$$

where $P_{\mathrm{P}}(n, \mu)$ is the probability of measuring n photons, given a mean measured photon number, μ [35].

The light emitted by a black-body or a lamp is know as thermal light, since many independent emitters contribute for the final signal, *i.e.* it is a superposition of many incoherent waves [33, 34]. The thermal distribution is described as [36–38]

$$P_{\mathrm{th}}(n, \mu) = \frac{\mu^n}{(1 + \mu)^{n+1}}. \tag{3.10}$$

The statistics of the photons in a source can be characterized in terms of the second-order coherence function. This function can be defined as [39, 40]

$$g^{(2)}(0) = 1 + \frac{Q}{\mu}, \tag{3.11}$$

where Mandel's Q parameter is written as [40, 41]

$$Q = \frac{\mathrm{Var}}{\mu} - 1. \tag{3.12}$$

The variance and the mean photon number are obtained, respectively, from

$$\mathrm{Var}^{(N_\mathrm{i})} = \sum_{n=0}^{N} \left(n - \mu^{(N_\mathrm{i})}\right)^2 \rho_n^{(N_\mathrm{i})}, \tag{3.13}$$

and,

$$\mu^{(N_\mathrm{i})} = \sum_{n=0}^{N} n\rho_n^{(N_\mathrm{i})}, \tag{3.14}$$

where N_i represents the number of iterations.

Using the value of $g^{(2)}(0)$ it is possible to obtain an immediate characterization of the source. If $g^{(2)}(0) = 0$, we are in the presence of a perfect single-photon source, since Var= 0. Measuring a $g^{(2)}(0) < 1$ confirms the nonclassical nature of the source, while $g^{(2)}(0) \geq 1$ it confirms its classical nature. A $g^{(2)}(0)=1$ (Var= μ) corresponds to Poissonian statistics of the source and a $g^{(2)}(0) = 2$ (Var= 2μ) corresponds to thermal statistics, such as the spontaneous Raman scattering [11, 40, 42].

Another way to compare the numerically reconstructed data with the theoretically expected results is with a multimode field equation that combines coherent and incoherent light [43–45]. This equation, which represents the convolution of M thermal states, allows to obtain the distribution of photons and has the form

$$\rho_n(\mu_\mathrm{th}, \mu_\mathrm{coh}, M) = \frac{\mu_\mathrm{th}^n}{(1+\mu_\mathrm{th})^{n+M}} \exp\left(-\frac{\mu_\mathrm{coh}}{1+\mu_\mathrm{th}}\right) L_n^{M-1}\left(-\frac{\mu_\mathrm{coh}}{\mu_\mathrm{th}(1+\mu_\mathrm{th})}\right), \tag{3.15}$$

where $L_n^a(z)$ are the generalized Laguerre polynomials [45]. In this equation, μ_th represents the average number of thermal photons in each thermal state and μ_coh is the average number of coherent photons [43, 45, 46]. Substituting Eq. (3.15) in Eq. (3.6) we can now write the theoretical no-click probability as [45]

$$\begin{aligned} p_\nu^\mathrm{off}(\eta_\nu, \mu_\mathrm{th}, \mu_\mathrm{coh}, M) = (1 - P_\mathrm{dc}) \sum_{n=0}^{\infty} (1-\eta_\nu)^n \rho_n(\mu_\mathrm{th}, \mu_\mathrm{coh}, M) = \\ (1 - P_\mathrm{dc}) \frac{1}{(1+\eta_\nu\mu_\mathrm{th})^M} \exp\left(-\frac{\eta_\nu\mu_\mathrm{coh}}{1+\eta_\nu\mu_\mathrm{th}}\right). \end{aligned} \tag{3.16}$$

From Eq. (3.16) one can also discriminate two different cases. The first case is verified when $\mu_{\mathrm{th}} \to 0$ and describes a Poissonian statistics for the distribution of photons. The second case appears when $\mu_{\mathrm{coh}} \to 0$ and describes a thermal statistics for the distribution of photons. Note that the average number of photons at the fiber output is $\mu = M\mu_{\mathrm{th}} + \mu_{\mathrm{coh}}$, where $M\mu_{\mathrm{th}}$ represents the expectation value of the photons in M thermal states [45–47].

In order to measure the accuracy between the reconstructed data and the theoretical results obtained from the multimode field equation we will use the fidelity, which can be written as [28, 45]

$$G = \sum_{n=0}^{N} \sqrt{\rho_n \rho_n^{(N_{\mathrm{i}})}}\,, \tag{3.17}$$

where ρ_n is the theoretical distribution and $\rho_n^{(N_{\mathrm{i}})}$ is the numerically reconstructed distribution, obtained at the last iteration.

To compare the reconstructed statistics for the non-click events (in Eq. (3.6)) with the theoretically expected one (in Eq.(3.16)) we will use simply the deviation, which can be obtained from

$$\delta = \sum_{n=0}^{N} |p_\nu^{\mathrm{off}}(\eta_\nu, \mu_{\mathrm{th}}, \mu_{\mathrm{coh}}, M) - p_\nu^{\mathrm{off}}(\eta_\nu)|\,. \tag{3.18}$$

Reconstruction of the Photon Statistics

The reconstruction of the statistics of the photons from the stimulated FWM photon source was performed considering a number of iterations, $N_{\mathrm{i}} = 1.22 \times 10^6$, *i.e.*, we have considered the number of iterations equal to the pulse repetition rate [28].

The first step for the reconstruction of the statistics of the source is to determine the efficiency of the VOA. This is required to obtain the combined efficiency between the VOA and the SPAD, necessary for the numerical reconstruction algorithm. The efficiency of the VOA was obtained simply by varying its attenuation and comparing the output and input powers. In Fig. 3.9, we present the efficiency of the VOA as a function of its attenuation for 31 points, which were the same used in the numerical reconstruction method. We have fitted the results with an exponential function and obtained that $\eta_\varpi = 0.602 \exp\left(-\alpha_\varpi/1.032\right) - 0.002$, where α_ϖ represents the attenuation in the VOA. The fit was obtained with $R^2 = 0.9993$.

Next, we have used the experimental setup shown in Fig. 3.8 to measure the photon counts in the SPAD as a function of the efficiency of the VOA. The same procedure was performed for seven different signal powers, considering the pump power fixed. Then, we have used the algorithm previously described for the numerical reconstruction of the experimental data.

In Fig. 3.10, we plot the fidelity values obtained from each numerical reconstruction as a function of the average number of photons per pulse at the output of the source, for Poissonian and thermal distributions. As can be seen from Fig. 3.10(a), when the pulse carries a low number of photons, *i.e.*, when $\mu \lesssim 2$, the fidelity for both Poissonian and thermal statistics is close to 100%, with relatively higher values for the last. However, looking at Fig. 3.10(b)

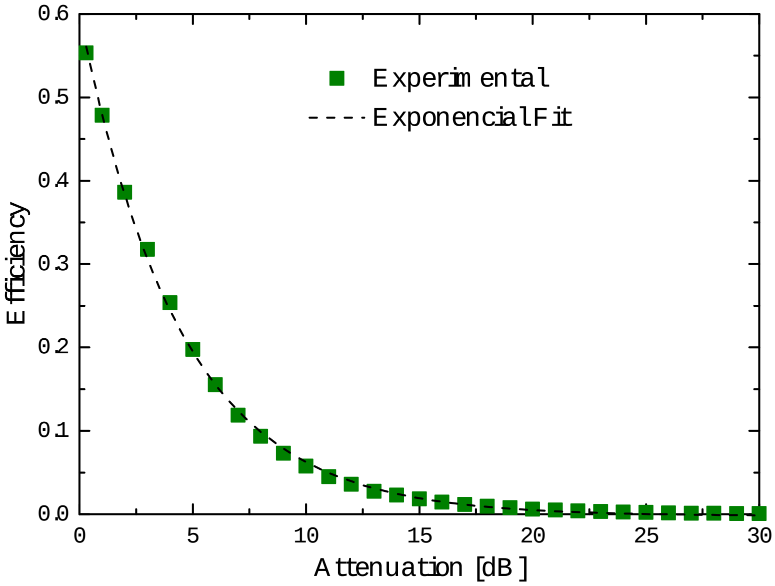

Figure 3.9: Efficiency of the VOA as a function of its attenuation.

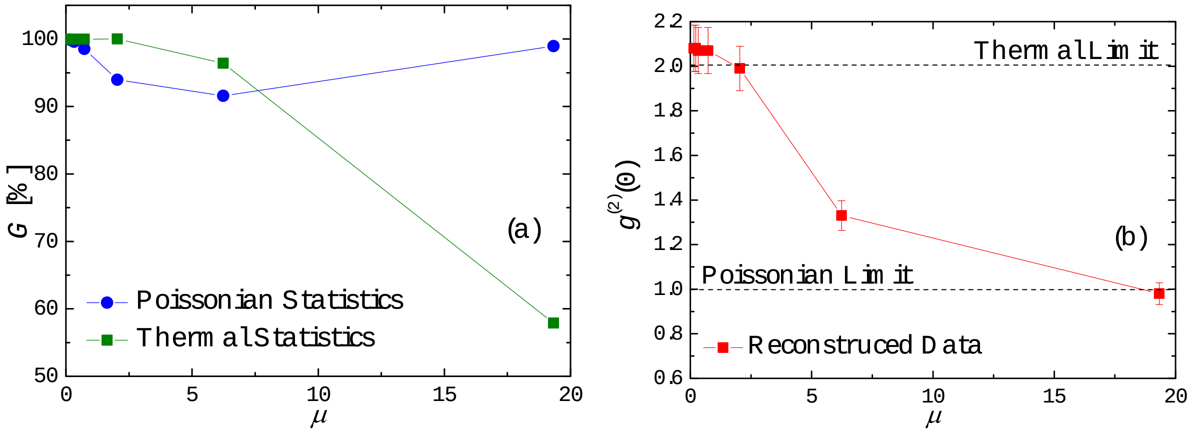

Figure 3.10: (a) Fidelity and (b) second-order coherence function obtained from the reconstructed data as a function of the average number of photons per pulse at the output of the source. The pump and signal powers used in each case are presented in Table 3.1. The error bars in (b) represent a 5% deviation in relation to each value.

it is possible to conclude without any doubts that in this case the statistics of the source is thermal, since $g^{(2)}(0) \approx 2$. The fact that $g^{(2)}(0)$ presents some values slightly larger than 2 is due to experimental errors and inaccuracy in the numerical method used. As μ increases, the Poissonian statistics arises. This can be seen more clearly from $g^{(2)}(0)$ in Fig. 3.10(b). From the results obtained, we can conclude that the statistics of the source goes from thermal, at a low power regime (which corresponds also to a low number of photons in each pulse), to Poissonian, in a high power regime (higher number of photons in each pulse). A thermal statistics can be explained by the fact that spontaneous processes dominate in a low power regime. When μ is increased in the signal, the stimulated processes become more significant and the idler photons follow a Poissonian statistics.

The powers of the pump and the signal at the fiber input are presented in Table 3.1. The average number of photons per pulse on the idler wave at the fiber output, as obtained from numerical reconstructions, are also shown.

Table 3.1: Pump and signal powers at the input of the fiber and corresponding μ at the output of the source. The fidelities obtained from Poissonian, G_{P}, and thermal, G_{th}, reconstructions, along with the second-order coherence function, $g^{(2)}(0)$, are also presented.

$P_{\mathrm{p}}(0) = 4.20\,\mathrm{dBm}$				
$P_{\mathrm{s}}(0)$ [dBm]	μ	G_{P} [%]	G_{th} [%]	$g^{(2)}(0)$
-39.2	0.15	99.90	99.99	2.08
-37.2	0.22	99.81	99.99	2.08
-33.2	0.33	99.59	99.99	2.07
-28.9	0.73	99.52	98.99	2.07
-24.2	2.04	93.97	100	1.99
-21.5	6.24	91.57	96.41	1.33
-18.9	19.33	98.95	57.87	0.98

From the results in Fig. 3.10 we verify that there is a region where the distribution of the photons is neither Poissonian nor thermal. In this case, we can say that we are in a multithermal regime, described by Eq. (3.15). This way, we have fitted the numerically reconstructed data with Eq. (3.15). In Fig. 3.11 we present the reconstructed photon statistics using Eq. (3.7), along with the best fit from Eq. (3.15), for three of the numerical reconstructions. The no-click probabilities from Eq. (3.6) and the best fits from Eq. (3.16) are also plotted.

In Table 3.2, we summarize the values for μ_{coh}, μ_{th}, M, μ and G, corresponding to Figs. 3.11(a), 3.11(c) and 3.11(e). A first look on the results clearly shows that the statistics of the idler photons generated depends significantly on the power of the signal, as we have

Table 3.2: Parameters obtained from the fit to Figs. 3.11(a), 3.11(c) and 3.11(e).

Figure	μ_{coh}	μ_{th}	M	μ	G [%]
3.11(a)	4.13×10^{-9}	0.33	1	0.33	99.99
3.11(c)	2.69	2.03	2	6.75	99.37
3.11(e)	21.24	-0.15	13	19.32	99.97

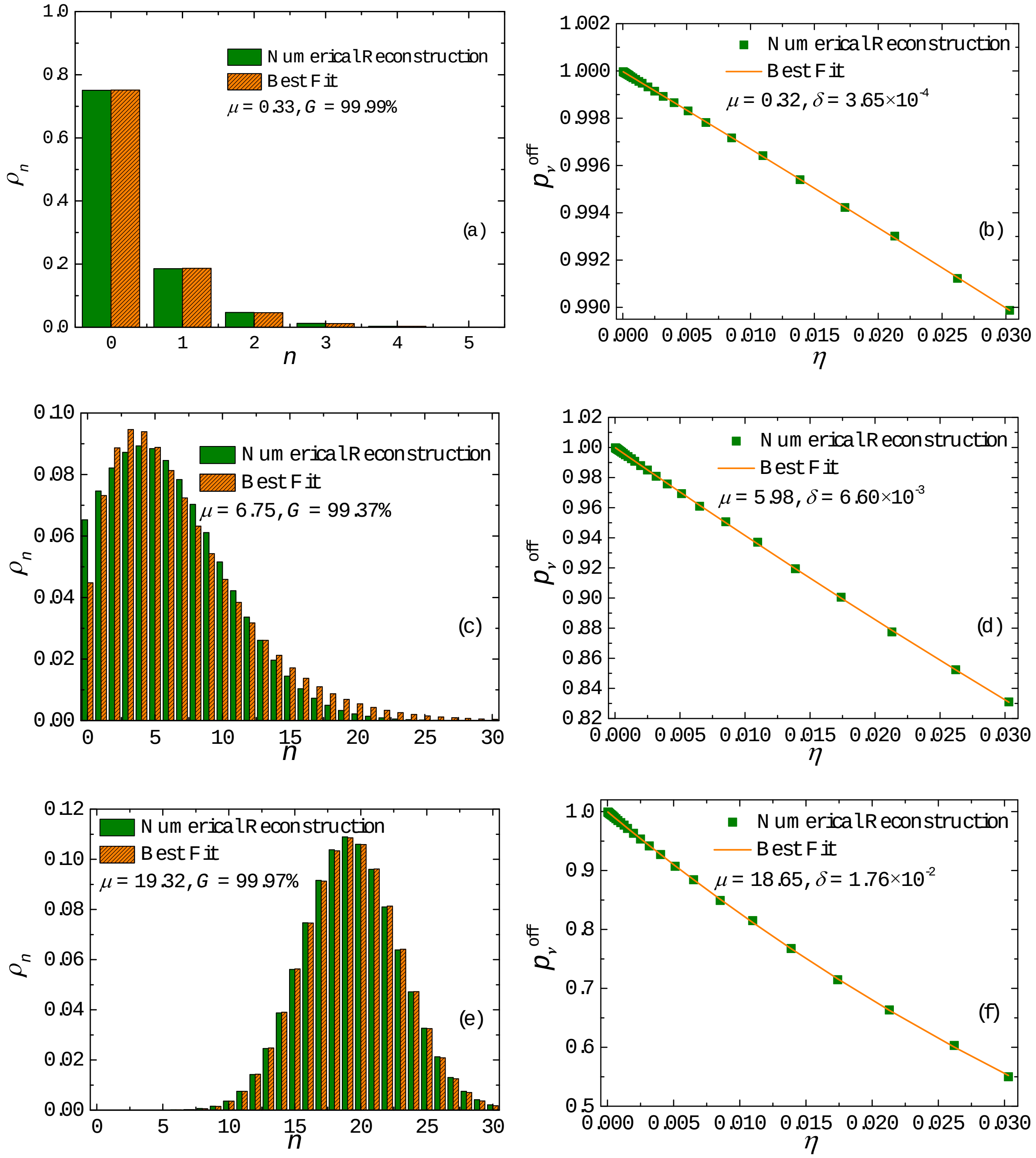

Figure 3.11: Numerical reconstruction of the statistics of the stimulated FWM photon source. *Left side:* Reconstructed photon statistics from Eq. (3.7) and best theoretical fits obtained from Eq. (3.15). *Right side:* No-click probabilities from Eq. (3.6) and best theoretical fits obtained from Eq. (3.16). The pump power at the input of the fiber was set as $P_{\text{p}}(0) = 4.20\,\text{dBm}$ and the signal powers at the input of the fiber were $P_{\text{s}}(0) = -39.2\,\text{dBm}$ in Figs. 3.11(a) and 3.11(b), $P_{\text{s}}(0) = -21.5\,\text{dBm}$ in Figs. 3.11(c) and 3.11(d), and $P_{\text{s}}(0) = -18.9\,\text{dBm}$ in Figs. 3.11(e) and 3.11(f).

seen before. In an analysis to Table 3.2 and Fig. 3.11(a) we conclude that all idler photons generated inside the DSF obey thermal statistics ($\mu_{\text{th}} = 0.33$), since $\mu_{\text{coh}} \to 0$ and $M = 1$. Multithermal statistics can be observed in Fig. 3.11(c), which includes both thermal ($\mu_{\text{th}} = 2.03$) and coherent ($\mu_{\text{coh}} = 2.69$) photons. The last case, which is plotted in Fig. 3.11(e), shows the typical Poissonian statistics, since the majority of the idler photons are coherent ($\mu_{\text{coh}} = 21.24$), due to stimulated processes. The negative sign in the average number of thermal photons was due to numerical errors. We observe an increase in the number of thermal modes, from 1 to 13, as the signal power increases. This occurs due to an increase on the stimulated processes also. Looking at the high values of fidelity (G), an high accuracy between the reconstructed data and the theoretical fits can be confirmed. From the no-click probabilities as a function of the combined efficiencies of the VOA and the SPAD, a good agreement between reconstructed data and theoretical fits is observed, see Figs. 3.11(b), 3.11(d) and 3.11(f). The accuracy between reconstructed and theoretical data is also confirmed by the low deviation values, calculated from Eq. (3.18).

In summary, from the results presented in this section, we verified that in a low signal power regime the idler photons generated from the stimulated FWM process follow a thermal statistics. With an increase in the signal power, the statistics changes to multithermal, until it reaches the Poissonian statistics in a high power regime. It is important to note that the thermal statistics arises mainly due to spontaneous processes that dominate in a low power regime, while the Poissonian statistics dominates in a high power regime due to the presence of stimulated processes [25, 44].

3.4 Impact of FWM in a Co-Propagating Quantum Signal

Transparency in fiber optical networks is a very important aspect for high-speed communications systems [48]. Therefore, the study of the coexistence of quantum and classical signals in the same network is of major importance [49].

The impact of FWM in the QKD system performance was already studied in terms of the quantum-bit error rate (QBER) and the secret key rate [50]. Next, we present a study of the impact of the FWM process in the statistics of a co-propagating coherent quantum signal in a wavelength-division multiplexing (WDM) lightwave system. The study follows the same method used for the characterization of the statistics of the stimulated FWM photon source.

3.4.1 Reconstruction of the Photon Statistics

Experimental Setup

In Fig. 3.12, we present the schematics of the experimental setup used to determine the impact of the stimulated FWM process in the statistics of a coherent quantum signal, co-propagating in the system. To do that, we inserted an additional quantum signal in the setup

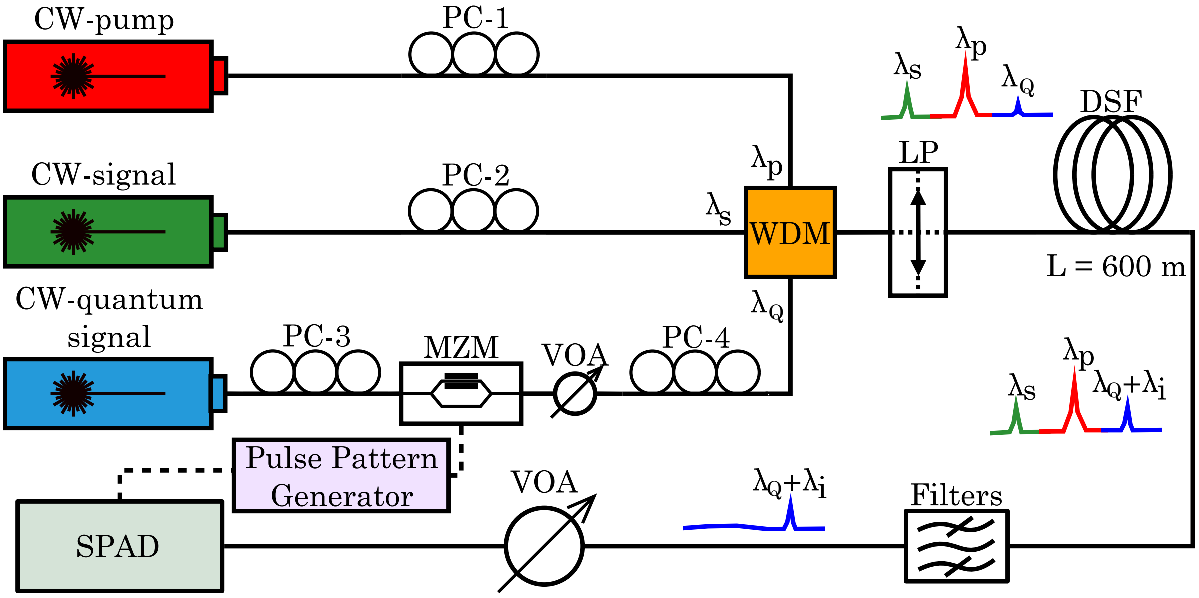

Figure 3.12: Schematics of the experimental setup. The dashed lines represent electrical signals and the solid lines the optical path.

shown in Fig. 3.8. This signal, centered at $\lambda_Q = 1554.13\,\text{nm}$, was modulated (MZM) and then attenuated until the single photon level, in the same way as the signal in the previous experiment. The three waves were sent co-polarized to the DSF, where the idler wave was generated at $\lambda_i = \lambda_Q$. After the fiber, the pump and the signal photons were suppressed by two cascaded flat-top DWDM optical filters with a FWHM of 100 GHz, providing a total isolation of about 100 dB. The idler photons from the FWM process together with the photons from the quantum signal were transmitted through the filters and reached the SPAD. The measurement method applied was the same used in the determination of the statistics of the FWM photon source, by changing the attenuation in the VOA.

Reconstructed Data

Before discussing the reconstructed data it is important to note that since the quantum signal was obtained from an attenuated laser source, its statistics should follow a Poissonian distribution at the fiber input, as demonstrated in several works [28, 44, 47]. We also note that the quantum signal was sent at the same wavelength where the idler photons were generated in order to study the worst case scenario of interference between the two signals.

As for the previous case, in Fig. 3.13(a) we present the fidelity values obtained from Eq. (3.17), for each numerical reconstruction, as a function of the average number of photons per pulse obtained at the output of the source and for the two distributions tested. As can be seen from this figure, when the quantum signal carries a low number of photons per pulse, *i.e.*, when $\mu \lesssim 2.5$, the spontaneous processes from FWM-generated photons dominate and the

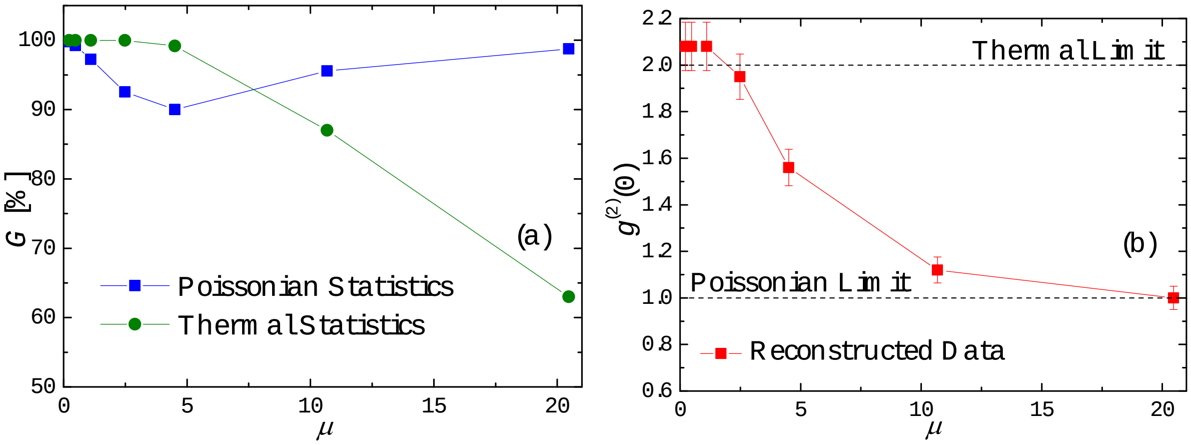

Figure 3.13: (a) Variation of the fidelity and the (b) second-order coherence function with the average number of photons per pulse at the output of the source. The error bars in (b) represent a 5% deviation in relation to each value.

statistics will be seen as thermal. When $2.5 \lesssim \mu \lesssim 11$, we obtained a superposition between the two statistics, *i.e.*, a multithermal statistics. For $\mu \gtrsim 11$, we verified that the spontaneous processes generated from FWM were not enough to dominate over the statistics of the quantum signal, which remained Poissonian. In Fig. 3.13(b), we present the second-order coherence function obtained from Eq. (3.11), for each numerical reconstruction, as a function of the average number of photons per pulse at the output of the source and for the same two distributions. It can be seen in Fig. 3.13(b) that $g^{(2)}(0)$ goes from 2 (thermal statistics) to 1 (Poissonian statistics), as μ evolves from a low number of photons per pulse, $\mu \lesssim 2.5$, to a higher number, $\mu > 11$. These results are according with the theoretical prediction for the $g^{(2)}(0)$ parameter [51]. The main parameters used in Fig. 3.13 are displayed in Table 3.3.

Table 3.3: Pump, signal and quantum signal powers at the input of the fiber, and correspondent μ at the output of the source. The fidelities obtained from thermal, G_{th}, and Poissonian, G_{P}, reconstructions, along with the parameter $g^{(2)}(0)$ are also presented.

$P_{\text{p}}(0) = 1.70$ dBm; $P_{\text{s}}(0) = -12.50$ dBm				
$P_{\text{Q}}(0)$ [dBm]	μ	G_{P} [%]	G_{th} [%]	$g^{(2)}(0)$
-70.21	0.23	99.80	99.99	2.08
-66.68	0.48	99.24	99.99	2.08
-62.93	1.10	97.23	99.99	2.08
-59.42	2.48	92.53	99.99	1.95
-57.24	4.51	90.00	99.16	1.56
-52.84	10.68	95.57	87.02	1.12
-51.72	20.47	98.75	62.99	1.00

In Fig. 3.14, we present the results from the numerical reconstruction obtained from Eq. (3.7) and the best fit using Eq. (3.15), for three different cases. The no-click probabilities are also shown together with the best fits obtained from Eq. (3.16). The results shown in this figure tell us that the final statistics obtained from the mixing of photons from the quantum signal and the FWM-generated also depend on the power of the quantum signal at the fiber. To help in the evaluation of the results, in Table 3.4 we present the values for μ_{coh}, μ_{th}, M, μ and G, for each case. Looking at the results in Fig. 3.14(a), we can see that all photons received are thermal, since $\mu_{\mathrm{coh}} \to 0$ and $M = 1$. This result indicates that the spontaneous processes from the FWM dominate over the quantum signal, thus presenting a thermal statistics. In the second case, for a higher power in the quantum signal, shown in Fig. 3.14(c), we observe a multithermal statistics, since μ_{coh} and μ_{th} are both different from zero, with a larger contribution from coherent photons from the quantum signal. In the last case, shown in Fig. 3.14(e), we can see that the majority of the photons follow a Poissonian distribution, since $\mu_{\mathrm{coh}} \gg n_{\mathrm{th}}$, which tells us that the quantum signal dominates over the FWM. In Table 3.4, we can also verify that the number of modes, M, increases with the increasing in the quantum signal power, which leads to a stimulated-photon regime. From the results of the fidelity, G, we confirm the accuracy between numerically reconstructed data and the theoretically expected ones. Looking at the no-click probabilities in the right side of Fig. 3.14, we verify also a high accuracy between the reconstructed data and the theoretical fits, which can be confirmed from the deviation values, δ.

Table 3.4: Parameters obtained from the fit to Figs. 3.14(a), 3.14(c) and 3.14(e).

Figure	μ_{coh}	μ_{th}	M	μ	G [%]
3.14(a)	1.61×10^{-8}	0.22	1	0.22	99.99
3.14(c)	7.08	0.84	5	11.27	99.34
3.14(e)	18.72	0.11	21	21.05	98.04

From this study, we concluded that when the quantum signal is set at a low power regime, the spontaneous processes generated from FWM dominate. This can be problematic for security in some quantum communication experiments, since in this case the receiver was expecting Poissonian-distributed photons from the quantum signal and measures thermally-distributed ones. If the quantum signal is generated with a higher power its statistics will dominate over the FWM, but at the same time it can also threaten the security of the protocol, since the average number of photons per pulse is higher and that can be advantageous for an eavesdropper.

At last, we highlight that the results described in Sections 3.3 and 3.4 are according with the theoretical data presented in [51].

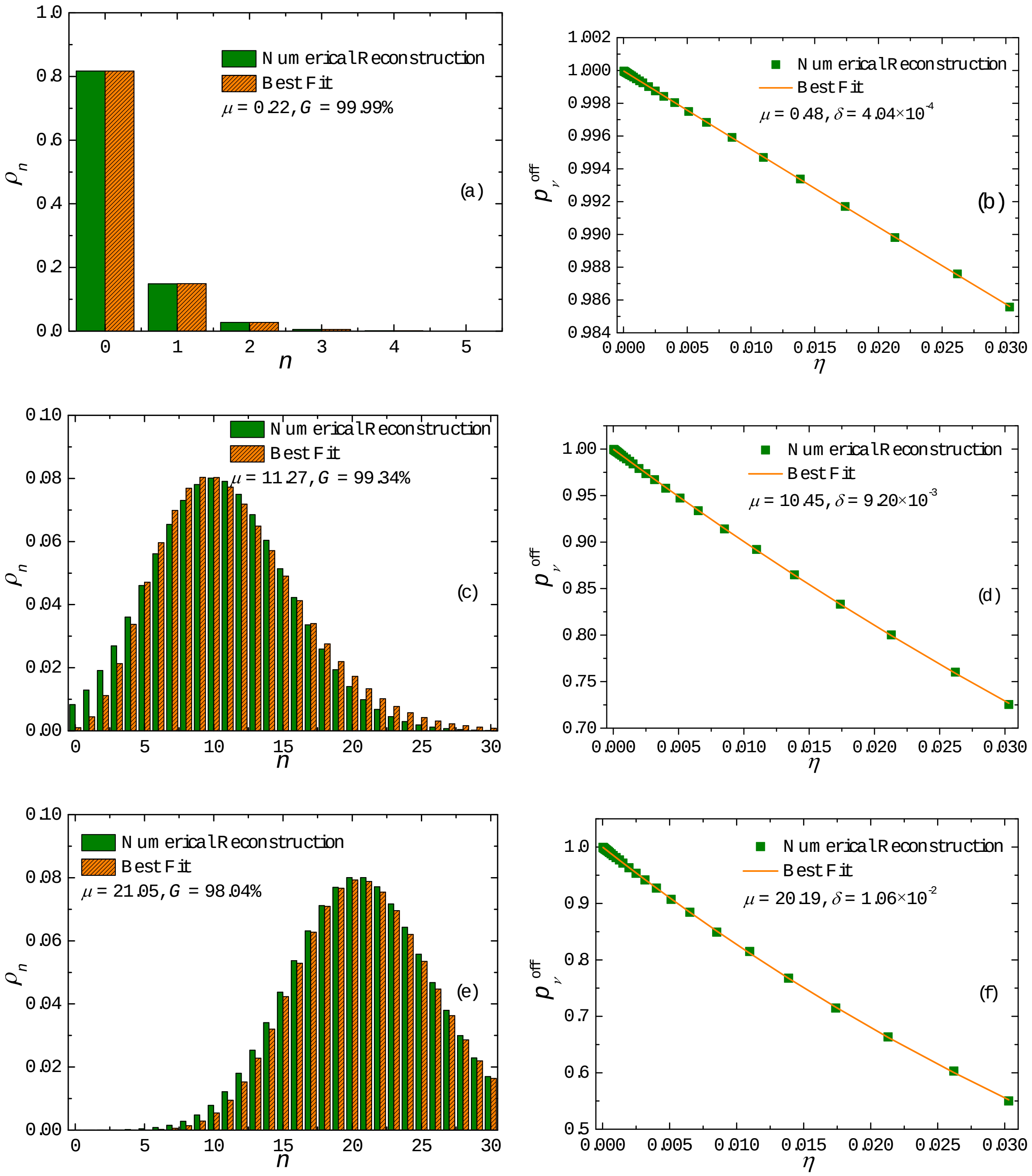

Figure 3.14: Numerical reconstruction of the statistics of a quantum signal in the presence of FWM . *Left side:* Reconstructed photon statistics from Eq. (3.7) and best fits obtained from Eq. (3.15). *Right side:* No-click probabilities from Eq. (3.6) and theoretical fits obtained from Eq. (3.16). The pump and signal powers at the input of the fiber were $P_\mathrm{p}(0) = 1.70\,\mathrm{dBm}$ and $P_\mathrm{s}(0) = -12.5\,\mathrm{dBm}$, and the quantum signal power at the input of the fiber presented the values, $P_\mathrm{Q}(0) = -70.21\,\mathrm{dBm}$ in Figs. 3.14(a) and 3.14(b), $P_\mathrm{Q}(0) = -52.84\,\mathrm{dBm}$ in Figs. 3.14(c) and 3.14(d), and $P_\mathrm{Q}(0) = -51.72\,\mathrm{dBm}$ in Figs. 3.14(e) and 3.14(f).

3.5 Entangled-Photon Source based on Spontaneous FWM

In this section, we present a method to generate polarization-entangled photon pairs through the spontaneous FWM procces in a Sagnac fiber loop. Then, the photon pairs will be used to verify the violation of the CHSH inequality and demonstrate the feasibility of our source of photon pairs.

3.5.1 The CHSH Inequality

With the development of quantum mechanics, mostly in the 1920s and 1930s, a new point of view, markedly different from the classical proposal, came to light. Contrary to the classical view, quantum mechanics stated that an unobserved particle does not posses definite physical properties before a measurement is performed over it. Many physicists disagreed with this view, which was seriously put in question by the famous Einstein, Podolsky and Rosen (EPR) paper [52]. In their paper, Einstein, Podolsky and Rosen proposed a thought experiment to demonstrate that quantum mechanics was not able to provide a complete description of physical reality. Instead, some local hidden variables should be supplemented to make the theory complete. In 1964, John S. Bell presented an experiment to clarify the problem, verifying that the EPR argument was not validated by nature [53]. Bell presented a set of inequalities that should be satisfied by all local hidden variables theories, but not by quantum mechanics. For the inequality to be valid, there are two assumptions that should be followed, namely:

1. *Realism:* all objects have to be in a definite state, which exists independently of the observation.
2. *Locality:* the effects of local actions, such as measurements, cannot travel faster than the speed of light. Then, the measurement made in one does not influence the result of another measurement instantaneously.

In 1969, Clauser, Horne, Shimony and Holt proposed a Bell-type inequality which is easier to demonstrate experimentally [54]. This inequality is called CHSH.

In order to find a condition for violation of CHSH inequality, we start by stating Bell's theorem, which can be written as [53, 55]:

$$E(a,b) = \int_{\lambda \in \Lambda} p(\lambda) A(a,\lambda) B(b,\lambda) \mathrm{d}\lambda, \tag{3.19}$$

where Λ is the probability space, λ are the hidden variables, with A and B being two physical quantities, while a and b are the axes at which A and B are projected. From Eq.(3.19) we can obtain the degree of correlation by measuring different polarizer angles as [56]

$$E(\theta_1,\theta_2) = \frac{C_{\theta_1,\theta_2} + C_{\theta_1^{\perp},\theta_2^{\perp}} - C_{\theta_1,\theta_2^{\perp}} - C_{\theta_1^{\perp},\theta_2}}{C_{\theta_1,\theta_2} + C_{\theta_1^{\perp},\theta_2^{\perp}} + C_{\theta_1,\theta_2^{\perp}} + C_{\theta_1^{\perp},\theta_2}}. \tag{3.20}$$

where $C_{\{\mathrm{A,B}\}}$ are the coincidences between Alice and Bob's polarizers. The angles θ_1 and $\theta_1^{\perp}$ are angles in Alice's polarizer and θ_2 and $\theta_2^{\perp}$ are angles at Bob's polarizer. From the different settings of the polarizers' angles, the CHSH inequality can be written as [54]

$$S = E(\theta_1,\theta_2) - E(\theta_1,\theta_2') + E(\theta_1',\theta_2) + E(\theta_1',\theta_2') \leq 2, \tag{3.21}$$

and requires 16 measurements to be determined.

Quantum mechanics allows to obtain a maximum value for S when measuring a particular set of polarizer angles, as shown in Fig. 3.15. Then, the expectancy values for CHSH inequality are given by

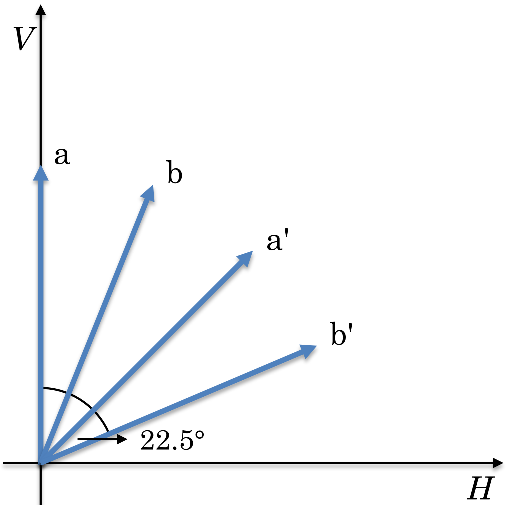

Figure 3.15: Polarizer angles for maximal S.

$$E(\theta_1,\theta_2) = E(\theta_1',\theta_2) = E(\theta_1',\theta_2') = \frac{1}{\sqrt{2}}, \tag{3.22}$$

and

$$E(\theta_1,\theta_2') = -\frac{1}{\sqrt{2}}. \tag{3.23}$$

Substituting Eqs. (3.22) and (3.23) in Eq. (3.21) we find that the maximum value for S according to quantum mechanics is

$$S^{\max} = \frac{1}{\sqrt{2}} - \left(-\frac{1}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} = 2\sqrt{2}. \tag{3.24}$$

Associated with each measurement is a given uncertainty, which can be calculated from [57]

$$\sigma_S = \sqrt{\sum_{i=1}^{16} C_i \left(\frac{\partial S}{\partial C_i}\right)^2}. \tag{3.25}$$

The violation of CHSH inequality is observed if $S > 2$. However, in order to statistically claim the violation of CHSH inequality, excluding statistical fluctuations in the measurement, we need to calculate the standard deviation in relation to the maximum value,

$$\sigma = \frac{S-2}{\sigma_S}, \tag{3.26}$$

and σ must be larger than 3 to be statistically valid [58].

3.5.2 Experimental Validation

After presenting the theory for CHSH inequality, in this subsection we are going to describe the experimental setup which was used in the verification of the inequalities' violation using polarization-entangled photon pairs.

Experimental Setup

The experimental setup used in the verification of the violation of CHSH inequality, through the generation of polarization-entangled photon pairs from the spontaneous FWM process, is shown in Fig. 3.16.

The description of the experimental setup is as follows. A CW pump from a TLS centered at 1550.918 nm passes through a polarization controller (PC-1) and is modulated using a MZM. Then, the sidebands of the pulses are eliminated with a 100 GHZ fixed flat-top DWDM optical filter. Another polarization controller (PC-2) and a linear polarizer (LP) are used to align the polarization of the photons with the input of a 4-ports PBS, which is set at 45°. The PBS sets a Sagnac loop [59] which includes two polarization controllers (PC-3 and PC-4) and a 150 m highly-nonlinear fiber (HNLF). A detailed scheme of the Sagnac loop used to generate the polarization-entangled photon pairs is shown in Fig. 3.17. The pump pulse inputs at port 3 of the PBS at an angle of 45° and will be split into horizontal (H) and vertical (V) polarization components, each one having equal optical power. The pump power must be chosen in order to make the probability of generating simultaneously two pairs very low. The H component propagates in the loop in the counterclockwise direction and generates signal-idler photon pairs in the state $|H\rangle_{\mathrm{s}}|H\rangle_{\mathrm{i}}$ when interacting with the optical fiber. Likewise, the V component propagates in the loop in the clockwise direction and generates signal-idler photon pairs in the state $|V\rangle_{\mathrm{s}}|V\rangle_{\mathrm{i}}$. Note that the difference between the refractive indices of the H and V components in the fiber should be null or very small, in order to produce the same number of

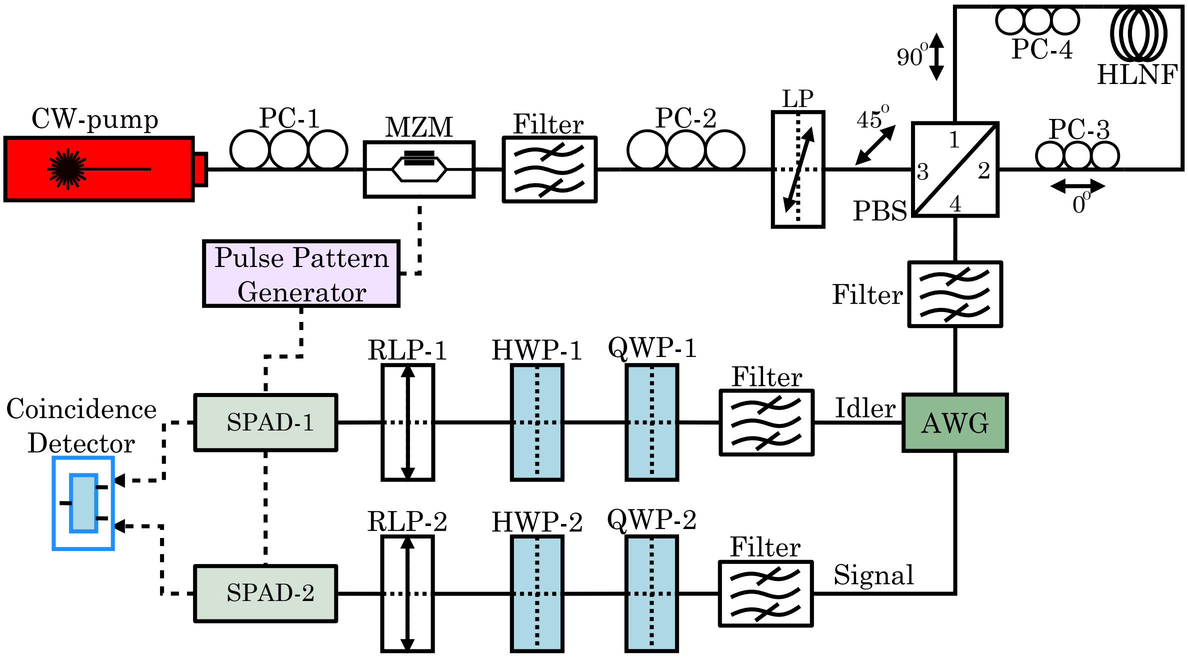

Figure 3.16: Experimental scheme used for polarization-entangled-photon-pair generation through spontaneous FWM and coincidence detection.

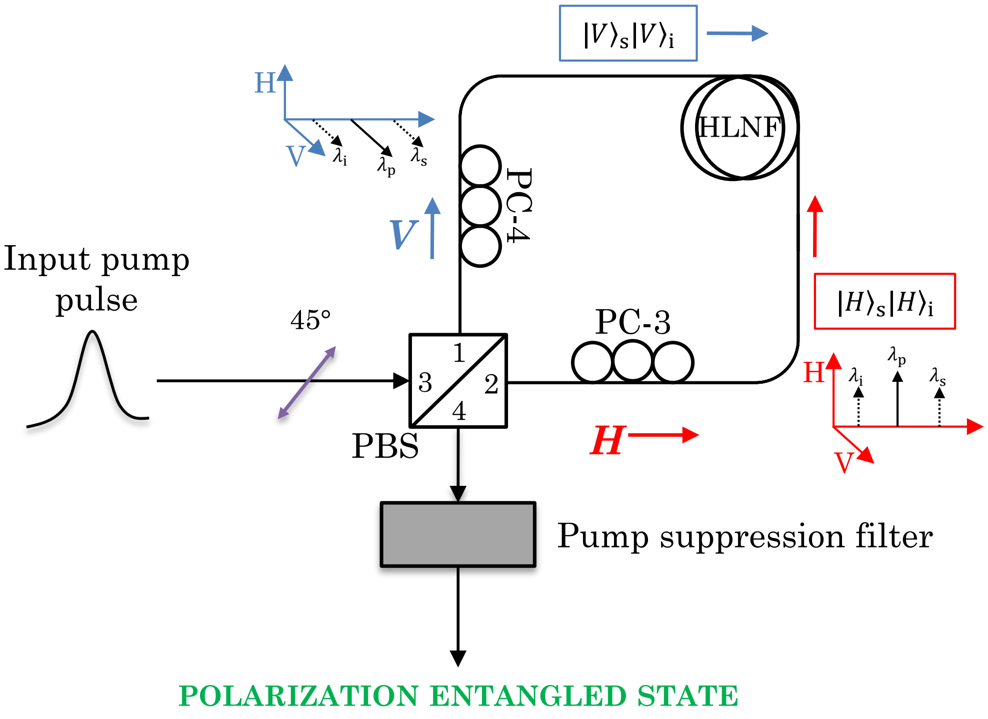

Figure 3.17: Generation of polarization-entangled photon pairs in a Sagnac loop.

photon pairs independently of the position of the fiber where they are generated. To guarantee that the generated photon pairs properly output from the loop it is necessary to adjust the two polarization controllers (PC-3 and PC-4). After the PBS is necessary to eliminate the pump photons, which can be done using an optical filter. After the filter we can obtain, at last, the polarization entangled state given by

$$|\psi\rangle = \tfrac{1}{\sqrt{2}}\big(|H\rangle_{\mathrm{s}}|H\rangle_{\mathrm{i}} + |V\rangle_{\mathrm{s}}|V\rangle_{\mathrm{i}}\big). \tag{3.27}$$

The HNLF has a nonlinear coefficient, $\gamma \approx 10.5\,\mathrm{W}^{-1}\mathrm{km}^{-1}$ and the ZDW, $\lambda_0 \approx 1550\,\mathrm{nm}$. The pump power at the input of each arm of the loop was $P_{\mathrm{p}} = 3.42\,\mathrm{dBm}$. Then, an arrayed waveguide grating (AWG) with a 100 GHz channel spacing is used to send signal photons to one path and idler photons to another, at the wavelengths of $\lambda_{\mathrm{s}} = 1547.715\,\mathrm{nm}$ and $\lambda_{\mathrm{i}} = 1554.134\,\mathrm{nm}$, respectively. A cascade of flat-top fixed DWDM optical filters is then used to assure that only signal or idler photons pass through the respective path and all other wavelengths are suppressed. In order to adjust the SOP of signal and idler photons, we have used a quarter-wave plate (QWP) and a half-wave plate (HWP), so that the two photons experience the same polarization change after they were separated by the AWG. Then, each photon that is transmitted through the rotatable linear polarizer (RLP-1 and RLP-2) is detected using a SPAD. SPAD-1 (id200) has a dark-count probability per time gate, $t_{\mathrm{g}} = 2.5\,\mathrm{ns}$, of $P_{\mathrm{dc}}^{(1)} = 5 \times 10^{-5}\,\mathrm{ns}^{-1}$, and a quantum detection efficiency, $\eta_{\mathrm{D}}^{(1)} \approx 10\%$ [60]. SPAD-2 (id201) has a dark-count probability per time gate, $t_{\mathrm{g}} = 2.5\,\mathrm{ns}$, of $P_{\mathrm{dc}}^{(2)} = 5\times10^{-6}\,\mathrm{ns}^{-1}$, and a quantum detection efficiency, $\eta_{\mathrm{D}}^{(2)} \approx 10\%$ [61]. A deadtime of $10\,\mu\mathrm{s}$ was applied to each detector in order to avoid afterpulses. Finally, the electric signals from the SPADs were sent to a coincidence detector for coincidence measurements. The coincidence detector has a time resolution of 82.3 ps, which is smaller than the time gate window, allowing to distinguish single counts from coincidence counts within the gate.

Experimental Results

As we have mentioned, to verify the violation of CHSH inequality it is required to measure the coincidence rate for 16 combinations of the RLPs. Therefore, we have selected the following fixed angles for each RLP: θ_1 = -45°, 0°, 45°, 90° and θ_2 = 22.5°, 67.5°, 112.5°, -22.5°. The procedure was the same for each measurement, *i.e.*, we have fixed the angle of one RLP and rotated the angle of the other from 0° to 180°, in steps of 22.5.

In Fig. 3.18, we present coincidence and single counts collected during 20 s when varying the angle of the RLP-2 (θ_2), while the angle of the RLP-1 (θ_1) was fixed for 0°, 45°, 90° and -45°. In Fig. 3.19, we show coincidence and single counts collected during a 20 s interval when varying the angle of the RLP-1 (θ_1), while the angle of the RLP-2 (θ_2) was fixed for values 22.5°, 67.5°, 112.5° and -22.5°. From the experimental results there are several conclusions to discuss. The first one is related to the fact that we show coincidence and single counts. This happens because not all photons generated from our source are entangled. Also, one major difference

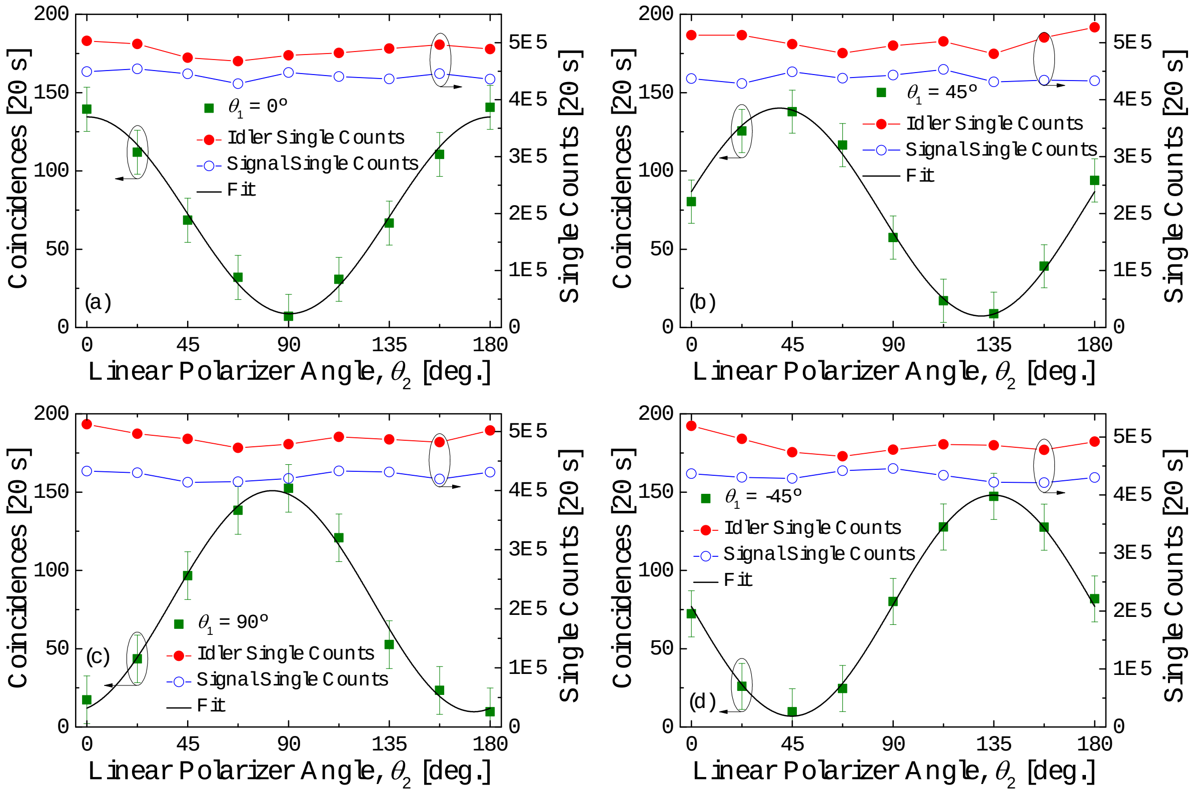

Figure 3.18: Coincidence and single counts as a function of θ_2, while (a) $\theta_1 = 0°$, (b) $\theta_1 = 45°$, (c) $\theta_1 = 90°$ and (d) $\theta_1 = -45°$ were kept fixed. The solid curve is a sinusoidal fit to the experimental data. Error bars are a 5% deviation in relation to the maximum value, in each case.

between coincidence and single photons is that the former present a sinusoidal behavior, while the later show a constant one. Since photon pairs are entangled in the polarization, when they reach the RLP only some of them will pass, *i.e.*, only the ones whose polarization is aligned with the axis of the RLP. When this happens, a maximum number of counts will be detected in the SPAD. When the polarization of the entangled photon is orthogonal with the axis of the RLP, a minimum number of counts will be registered. Regarding single photons, since they are in a superposition state with horizontal and vertical components, they will not be affected by changes in the RLPs, therefore presenting a nearly constant behavior. An higher rate of idler single counts is due to spontaneous Raman scattering, which creates much more noise photons in the idler than in the signal [19, 62].

In the literature, there exist several methods to fit the experimental results for coincidences, either using cosine [63, 64], sine [65], or other functions [66]. To fit the coincidence rate, C, we will use a cosine-type expression of the form

$$C = C_0 + A_{\mathrm{w}} \cos(\theta_i - \xi)^2, \tag{3.28}$$

where C_0 represents the background counts, A_{w} is the amplitude and ξ represents its phase, with

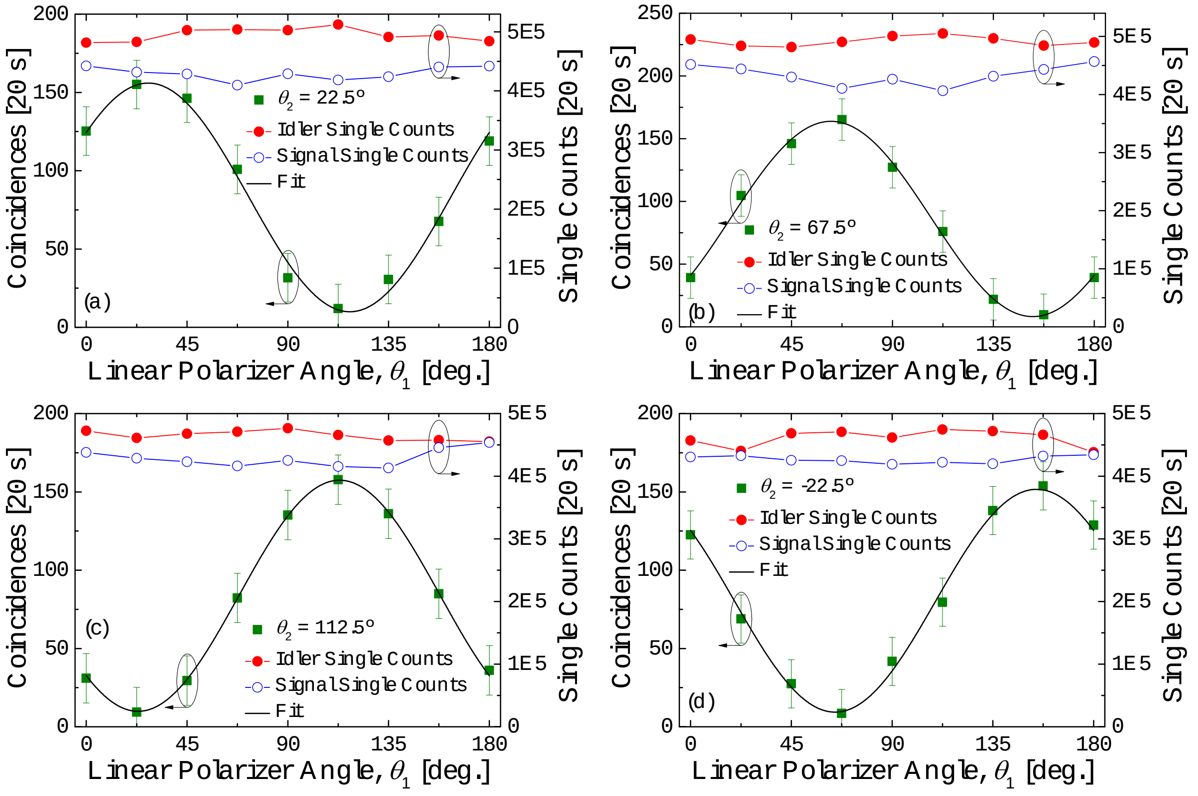

Figure 3.19: Coincidence and single counts as a function of θ_1, while (a) $\theta_2 = 22.5°$, (b) $\theta_2 = 67.5°$, (c) $\theta_2 = 112.5°$ and (d) $\theta_2 = -22.5°$ were kept fixed. The solid curve is a sinusoidal fit to the experimental data. Error bars are a 5% deviation in relation to the maximum value, in each case.

$i = 1, 2$. The parameters obtained from fittings to Figs. 3.18 and 3.19 are shown in Table 3.5. Looking at the values of R^2 in this table, we can see that Eq. (3.28) allows to fit the data with

Table 3.5: Fitting parameters from Eq. (3.28) to the coincidence counts in Figs. 3.18 and 3.19.

Figure	C_0 [counts]	A_w [counts]	ξ [°]	R^2
3.18(a)	8.80	125.65	0.42	0.9878
3.18(b)	7.33	132.77	39.34	0.9882
3.18(c)	9.76	141.16	82.75	0.9892
3.18(d)	6.92	141.15	134.79	0.9952
3.19(a)	9.93	146.02	27.70	0.9869
3.19(b)	8.15	155.69	62.60	0.9959
3.19(c)	9.89	147.57	113.14	0.9991
3.19(d)	9.36	142.28	154.54	0.9903

high accuracy, for all cases shown in the two figures.

The next step is to calculate the expectancy values from Eq. (3.20), in order to determine Bell's parameter, S. The experimental results obtained from the 16 combinations measured, and which are plotted in Figs. 3.18 and 3.19, are shown in Table 3.6. From the data in this table we calculated the expectancy values as: $E(0°, 22.5°) = 0.5460$, $E(0°, 67.5°) = -0.6545$, $E(45°, 22.5°) = 0.6962$ and $E(45°, 67.5°) = 0.5732$. With these values we obtained that

Table 3.6: Single (N_{θ_1}, N_{θ_2}) and coincidence counts (C) as a function of polarizer angles (θ_1 and θ_2).

θ_1 [°]	θ_2 [°]	N_{θ_1} [Hz]	N_{θ_2} [Hz]	C [counts]
0	22.5	102660	122880	131
90	112.5	102660	120060	138
0	112.5	97620	129000	39
90	22.5	105360	125880	40
45	22.5	102840	125280	133
-45	112.5	105840	119220	135
45	112.5	103260	123480	17
-45	22.5	102720	116040	31
0	67.5	103920	123420	26
90	-22.5	98880	126780	31
0	-22.5	101700	121500	138
90	67.5	97980	127980	135
45	67.5	101340	119940	127
-45	-22.5	101880	124740	131
45	-22.5	102660	117240	41
-45	67.5	99300	123780	29

$$S = 0.5460 + 0.6545 + 0.6962 + 0.5732 = 2.4699. \tag{3.29}$$

Next, we calculated the uncertainty in the value of S using Eq. (3.25), giving $\sigma_S = 0.0862$. At last, we have that Bell's parameter is given by $S = 2.4699 \pm 0.0862$. The standard deviation of S was calculated from Eq. (3.26) as

$$\sigma = \frac{2.4699 - 2}{0.0862} = 5.45. \tag{3.30}$$

This result allowed us to demonstrate the violation of CHSH inequality by more than 5 standard deviations of measurement uncertainty.

Another important parameter to analyze is the visibility, which can be calculated from

$$V = \frac{C_+ - C_-}{C_+ + C_-}, \tag{3.31}$$

where C_+ and C_- are the maximum and minimum number of counts, respectively [67]. The visibility was calculated for each set of data in Figs. 3.18 and 3.19 and is summarized in Table 3.7. The results shown in Table 3.7 show high visibility values, $V > 87\%$, which tells us that our source produces entangled-photon pairs with a strong correlation.

Table 3.7: Visibility of the experimental results shown in Figs. 3.18 and 3.19, calculated from Eq. (3.31).

Figure	θ_1 [°]	Visibility [%]	Figure	θ_2 [°]	Visibility [%]
3.18(a)	0	90.33	3.19(a)	22.5	87.87
3.18(b)	45	87.97	3.19(b)	67.5	88.97
3.18(c)	90	88.06	3.19(c)	112.5	88.74
3.18(d)	-45	87.60	3.19(d)	-22.5	89.50

3.6 Summary

In optical communications, the FWM process can be either an impairment or an advantage. For the generation of photons, it proved to be worthy when used in a low power regime. This happens because the distribution of photons generated with this source follows a thermal statistics, which is very similar to the Poissonian statistics obtained from an attenuated laser source, when $\mu \ll 1$. While an attenuated photon source requires only a laser and a VOA, the stimulated FWM photon source is a bit more complex, since it requires two lasers, a coupling component and a DSF. On the other hand, the spontaneous FWM process can be used in the generation of high-purity entangled photon pairs or in heralded single-photon sources.

From the experiments presented in this chapter we demonstrated that the FWM process is an important tool for the generation of entangled photon pairs. Moreover, it can also be used with success in proof-of-principle demonstrations of probabilistic photon sources, which are key elements for quantum communications.

References

[1] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, Jul. 2011.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[3] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. C. Bienfang, D. Su, R. F. Boisvert, C. W. Clark, and C. J. Williams, "Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s," *Opt. Express*, vol. 14, no. 6, pp. 2062–2070, Mar. 2006.

[4] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security," *Opt. Express*, vol. 15, no. 13, pp. 8465–8471, Jun. 2007.

[5] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Long-distance Bell-state analysis of fully independent polarization weak coherent states," *J. Lightwave Technol.*, vol. 31, no. 17, pp. 2881–2887, Sep. 2013.

[6] E. Waks, E. Diamanti, and Y. Yamamoto, "Generation of photon number states," *New J. Phys.*, vol. 8, no. 1, p. 4, Jan. 2006.

[7] A. Soujaeff, T. Nishioka, T. Hasegawa, S. Takeuchi, T. Tsurumaru, K. Sasaki, and M. Matsui, "Quantum key distribution at 1550 nm using a pulse heralded single photon source," *Opt. Express*, vol. 15, no. 2, pp. 726–734, Jan. 2007.

[8] M. Dusek, N. Lutkenhaus, and M. Hendrych, "Quantum cryptography," *In: Progress in Optics, E. Wolf (Elsevier)*, vol. 49, pp. 381–454, 2006.

[9] P. F. Antunes, A. N. Pinto, and P. S. André, "Single-photon source by means of four-wave mixing inside a dispersion-shifted optical fiber," in *Proc. of Frontiers in Optics.* Optical Society of America, Oct. 2006, p. FMJ3.

[10] P. F. Antunes, P. S. André, and A. N. Pinto, "A simple and inexpensive single-photon source by means of four-wave-mixing and attenuation," in *Proc Conf. on Telecommunications - CONFTELE*, Peniche, Portugal, May 2007, pp. 255–257.

[11] E. A. Goldschmidt, M. D. Eisaman, J. Fan, S. V. Polyakov, and A. Migdall, "Spectrally bright and broad fiber-based heralded single-photon source," *Phys. Rev. A*, vol. 78, no. 1, p. 013844, Jul. 2008.

[12] Á. J. Almeida, G. G. Fernandes, and A. N. Pinto, "Single-photon source with adjustable linear SOP," in *Proc. of VII Symposium On Enabling Optical Networks and Sensors - SEONS, Nokia-Siemens Networks, Amadora, Portugal*, Jun. 26 2009.

[13] N. A. Silva, N. J. Muga, and A. N. Pinto, "Influence of the stimulated Raman scattering on the four-wave mixing process in birefringent fibers," *J. Lightwave Technol.*, vol. 27, no. 22, pp. 4979–4988, Nov. 2009.

[14] N. A. Silva, N. J. Muga, and A. N. Pinto, "Effective nonlinear parameter measurement using FWM in optical fibers in a low power regime," *IEEE J. Quant. Electron.*, vol. 46, no. 3, pp. 285–291, Mar. 2010.

[15] Á. J. Almeida, N. A. Silva, N. J. Muga, and A. N. Pinto, "Fiber-optical communication system using polarization-encoding photons," in *Proc. of 15th European Conference on Networks and Optical Communications and 5th Conference on Optical Cabling and Infrastructure, NOC/OC&I*, Jun. 8-10, 2010, pp. 127–132.

[16] Á. J. Almeida, N. A. Silva, N. J. Muga, and A. N. Pinto, "Single-photon source using stimulated FWM in optical fibers for quantum communication," in *Proc. SPIE 8001*, May 3, 2011, p. 80013W.

[17] Á. J. Almeida, N. A. Silva, P. S. André, and A. N. Pinto, "Four-wave mixing: Photon statistics and the impact on a co-propagating quantum signal," *Opt. Commun.*, vol. 285, no. 12, pp. 2956–2960, Jun. 2012.

[18] G. Agrawal, *Nonlinear Fiber Optics, 5th ed.*, G. Agrawal, Ed. Academic Press, 2013.

[19] Q. Lin, F. Yaman, and G. P. Agrawal, "Photon-pair generation in optical fibers through four-wave mixing: Role of Raman scattering and pump polarization," *Phys. Rev. A*, vol. 75, no. 2, p. 023803, Feb. 2007.

[20] H. Takesue and K. Inoue, "Generation of polarization-entangled photon pairs and violation of Bell's inequality using spontaneous four-wave mixing in a fiber loop," *Phys. Rev. A*, vol. 70, no. 3, p. 031802, Sep. 2004.

[21] N. Shibata, R. P. Braun, and R. G. Waarts, "Phase-mismatch dependence of efficiency of wave generation through four-wave mixing in a single-mode optical fiber," *IEEE J. Quant. Electron.*, vol. 23, no. 7, pp. 1205–1210, Jul. 1987.

[22] N. A. Silva, N. J. Muga, and A. N. Pinto, "Effective nonlinear parameter measurement using FWM in optical fibers in a low power regime," *IEEE J. Quant. Electron.*, vol. 46, no. 3, pp. 285–291, Mar. 2010.

[23] K. Inoue, "Four-wave mixing in an optical fiber in the zero-dispersion wavelength region," *J. Lightwave Technol.*, vol. 10, no. 11, pp. 1553–1561, Nov. 1992.

[24] Y. Zhang, K. Kasai, and M. Watanabe, "Investigation of the photon-number statistics of twin beams by direct detection," *Opt. Lett.*, vol. 27, no. 14, pp. 1244–1246, Jul. 2002.

[25] P. L. Voss, R. Tang, and P. Kumar, "Measurement of the photon statistics and the noise figure of a fiber-optic parametric amplifier," *Opt. Lett.*, vol. 28, no. 7, pp. 549–551, Apr. 2003.

[26] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, "Photon-number resolution using time-multiplexed single-photon detectors," *Phys. Rev. A*, vol. 68, no. 4, p. 043814, Oct. 2003.

[27] G. Zambra, M. Bondani, A. S. Spinelli, F. Paleari, and A. Andreoni, "Counting photoelectrons in the response of a photomultiplier tube to single picosecond light pulses," *Rev. Sci. Instrum.*, vol. 75, no. 8, pp. 2762–2765, Aug. 2004.

[28] G. Zambra, A. Andreoni, M. Bondani, M. Gramegna, M. Genovese, G. Brida, A. Rossi, and M. G. A. Paris, "Experimental reconstruction of photon statistics without photon counting," *Phys. Rev. Lett.*, vol. 95, no. 6, p. 063602, Aug. 2005.

[29] D. Mogilevtsev, "Diagonal element inference by direct detection," *Opt. Commun.*, vol. 156, no. 4-6, pp. 307–310, Nov. 1998.

[30] A. R. Rossi, S. Olivares, and M. G. A. Paris, "Photon statistics without counting photons," *Phys. Rev. A*, vol. 70, no. 5, p. 055801, Nov. 2004.

[31] G. Zambra and M. G. A. Paris, "Reconstruction of photon-number distribution using low-performance photon counters," *Phys. Rev. A*, vol. 74, no. 6, p. 063830, Dec. 2006.

[32] G. Brida, M. Genovese, M. Gramegna, A. Meda, F. Piacentini, P. Traina, E. Predazzi, S. Olivares, and M. G. A. Paris, "Quantum state reconstruction using binary data from on/off photodetection," *Adv. Sci. Lett*, vol. 4, no. 1, pp. 1–11, Jan. 2011.

[33] B. Lounis and M. Orrit, "Single-photon sources," *Rep. Prog. Phys.*, vol. 68, no. 5, pp. 1129–1179, May 2005.

[34] M. Oxborrow and A. G. Sinclair, "Single-photon sources," *Contem. Phys.*, vol. 46, no. 3, pp. 173–206, May 2005.

[35] S. D. Poisson, *Recherches sur la probabilité des jugements en matière criminelle et matière civile.* Bachelier, Aug. 1837, vol. 55.

[36] S. N. Bose, "Plancks gesetz und lichtquantenhypothese," *Z. Phys*, vol. 26, no. 1, pp. 178–181, Dec. 1924.

[37] A. Einstein, "Quantentheorie des einatomigen idealen gases," *Sitzungsber. Preuss. Akad. Wiss. Phys. Math. Kl.*, pp. 261–267, Jul. 1924.

[38] A. Einstein, "Quantentheorie des einatomigen idealen gases (zweite abhandlung)," *Sitzungsber. Preuss. Akad. Wiss. Phys. Math. Kl.*, pp. 3–10, Jan. 1925.

[39] R. J. Glauber, "The quantum theory of optical coherence," *Phys. Rev.*, vol. 130, no. 6, pp. 2529–2539, Jun. 1963.

[40] R. Loudon, *The Quantum Theory of Light.*, Loudon, R., Ed. Oxford University Press, 2000.

[41] L. Mandel, "Sub-poissonian photon statistics in resonance fluorescence," *Opt. Lett.*, vol. 4, no. 7, pp. 205–207, Jul. 1979.

[42] J. A. Slater, J.-S. Corbeil, S. Virally, F. Bussières, A. Kudlinski, G. Bouwmans, S. Lacroix, N. Godbout, and W. Tittel, "Microstructured fiber source of photon pairs at widely separated wavelengths," *Opt. Lett.*, vol. 35, no. 35, pp. 499–501, Feb. 2010.

[43] B. R. Mollow and R. J. Glauber, "Quantum theory of parametric amplification. I," *Phys. Rev.*, vol. 160, no. 5, pp. 1076–1096, Aug. 1967.

[44] M. Martinelli and P. Martelli, "Laguerre mathematics in optical communications," *Opt. Photon. News*, vol. 19, no. 2, pp. 30–35, Feb. 2008.

[45] G. Brida, M. Genovese, A. Meda, S. Olivares, M. G. A. Paris, and F. Piacentini, "Constrained MaxLik reconstruction of multimode photon distributions," *J. Mod. Opt.*, vol. 56, no. 2-3, pp. 196–200, Jan. 2009.

[46] R. Noé, "Optical amplifier performance in digital optical communication systems," *Elect. Eng.*, vol. 83, no. 1, pp. 15–20, Feb. 2001.

[47] T. Li and M. C. Teich, "Photon point process for traveling-wave laser amplifiers," *IEEE J. Quant. Electron.*, vol. 29, no. 9, pp. 2568–2578, Sep. 1993.

[48] J. Berthold, A. A. M. Saleh, L. Blair, and J. M. Simmons, "Optical networking: Past, present, and future," *J. Lightwave Technol.*, vol. 26, no. 9, pp. 1104–1118, May 2008.

[49] T. J. Xia and G. Wellbrock, "Optical channel speeds for future transport networks," in *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, ser. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, vol. 8310, Dec. 2011, p. 16.

[50] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, no. 4, p. 045012, Apr. 2009.

[51] N. A. Silva, Á. J. Almeida, and A. N. Pinto, "Interference in a quantum channel due to classical four-wave mixing in optical fibers," *IEEE J. Quant. Electron.*, vol. 48, no. 4, pp. 472–479, Apr. 2012.

[52] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev.*, vol. 47, no. 10, pp. 777–780, May 1935.

[53] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics*, vol. 1, no. 3, pp. 165–200, 1964.

[54] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, no. 15, pp. 880–884, Oct. 1969.

[55] J. S. Bell, "On the problem of hidden variables in quantum mechanics," *Rev. Mod. Phys.*, vol. 38, no. 3, pp. 447–452, Jul. 1966.

[56] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities," *Phys. Rev. Lett.*, vol. 49, no. 2, pp. 91–94, Jul. 1982.

[57] D. Dehlinger and M. W. Mitchell, "Entangled photons, nonlocality, and Bell inequalities in the undergraduate laboratory," *Am. J. Phys.*, vol. 70, no. 9, pp. 903–910, Sep. 2002.

[58] F. Pukelsheim, "The three sigma rule," *Am. Stat.*, vol. 48, no. 2, pp. 88–91, May 1994.

[59] V. Vali and R. W. Shorthill, "Fiber ring interferometer," *Appl. Opt.*, vol. 15, no. 5, pp. 1099–1100, May 1976.

[60] id Quantique, “id 200-single-photon detection module: Operating guide, version 2.2,” http://www.idquantique.com/images/stories/PDF/id201-single-photon-counter/id200-operating.pdf, Accessed January 14, 2016.

[61] id Quantique, “id 201-single-photon detection module: Operating guide, version 4.0,” http://www.idquantique.com/images/stories/PDF/id201-single-photon-counter/id201-operating-guide.pdf, Accessed January 14, 2016.

[62] Q. Lin, F. Yaman, and G. P. Agrawal, “Photon-pair generation by four-wave mixing in optical fibers,” *Opt. Lett.*, vol. 31, no. 9, pp. 1286–1288, May 2006.

[63] J. Chen, K. Fook Lee, C. Liang, and P. Kumar, “Fiber-based telecom-band degenerate-frequency source of entangled photon pairs,” *Opt. Lett.*, vol. 31, no. 18, pp. 2798–2800, Sep. 2006.

[64] C. Liang, K. F. Lee, M. Medic, P. Kumar, R. H. Hadfield, and S. W. Nam, “Characterization of fiber-generated entangled photon pairs with superconducting single-photon detectors,” *Opt. Express*, vol. 15, no. 3, pp. 1322–1327, Feb. 2007.

[65] M. A. M. Versteegh, M. E. Reimer, K. D. Jöns, D. Dalacu, P. J. Poole, A. Gulinatti, A. Giudice, and V. Zwiller, “Observation of strongly entangled photon pairs from a nanowire quantum dot,” *Nat. Commun.*, vol. 5, p. 5298, Oct. 2014.

[66] Q. Zhou, W. Zhang, J. Cheng, Y. Huang, and J. Peng, “Polarization-entangled Bell states generation based on birefringence in high nonlinear microstructure fiber at 15 μm,” *Opt. Lett.*, vol. 34, no. 18, p. 2706, Sep. 2009.

[67] S. Dürr, T. Nonn, and G. Rempe, “Fringe visibility and which-way information in an atom interferometer,” *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5705–5709, Dec. 1998.

Chapter 4

Transmission of Polarization-Encoded Information Through an Optical Fiber

4.1 Introduction

The evolution and control of polarization, after transmission through an optical fiber, have been under study for several decades [1–3]. In classical systems, the control of polarization can be performed manually, using polarization controllers (PCs) [4, 5], or automatically, through electro-optic devices [6–8]. However, in practical implementations, only the automatic methods are suitable to be used [6, 9]. Contrary to classical communications, the control of polarization in quantum communications systems should be non-intrusive, in order to preserve the quantum information [10]. In terms of polarization control, quantum communications also started by incorporating passive solutions [11–14]. The continuous control of polarization in quantum communications systems was only possible after the rise of electronic polarization controllers (EPCs) [15]. The use of EPCs allowed schemes based on monitoring count rates [16], the visibility [17] or Stokes parameters [18] to be implemented to achieve an automatic control of polarization. However, these first proposals had the need to interrupt quantum communication for the control of polarization. Then, methods which allowed the control of polarization at the same time as quantum communication takes place, were soon proposed [10, 19, 20]. Still, these methods shown some limitations due to polarization de-correlation or crosstalk [21], apart form requiring additional classical signals and hardware [10, 20]. Another method using alternating sequences of quantum and classical pulses, while monitoring the quantum-bit error rate (QBER), was also a subject of study [22, 23]. This proposal allows uninterrupted quantum communication but requires the use of two different lasers. Automatic polarization compensation using three quantum signals time-multiplexed was proposed in [24]. The polarization control is achieved by monitoring detector's count rates, which are used as a feedback signal to an EPC. Another method of polarization control which monitors the QBER and uses it as a feedback signal to an EPC was presented in [25]. In this technique, the polarization control is only performed when the QBER exceeds a threshold value and during this phase, the quantum communication is interrupted.

In this chapter, we describe a theoretical model for the accurate estimation of the QBER of the system. Then, we present a method to control polarization in real time, while monitoring the QBER of the system. Moreover, we perform a numerical simulation and an experimental validation to demonstrate its feasibility. The method uses frames containing both control and data qubits which are obtained from quantum signals. This way, it avoids the use of classical signals and additional hardware in the system.

4.2 System of Quantum Communications

Before starting to describe the QBER model, we will study the evolution of the QBER in a system which does not includes control of polarization. With this, we intend to model the evolution of the QBER in order to use it in a numerical simulation. We implement a transmission scheme which uses an attenuated laser source and the encoding is performed in the polarization of photons. To synchronize the emitter and the receiver we will study two different configurations, one using a synchronization pulse co-propagation in the fiber and another sending the pulse counter-propagating. Finally, in this section, we demonstrate the feasibility of an encoding/decoding scheme after the photons were generated from the stimulated four-wave mixing (FWM) process.

4.2.1 Transmission Scheme using a Synchronization Pulse Co-Propagating

The scheme of the experimental setup used in the measurement of the QBER is shown in Fig. 4.1. Next, we present its description. In the emitter, Alice uses a tunable-laser source (TLS) centered at $\lambda_\mathrm{p} = 1550.92\,\mathrm{nm}$, which is externally modulated with a Mach-Zehnder Modulator (MZM) to produce optical pulses with a full-width at half maximum (FWHM) of approximately 1 ns and a repetition rate of 100 kHz. Then, a 50/50 beam splitter (BS) produces two pulses where classical bits will be encoded in photon's polarization. Two acousto-optic modulators (AOM-1 and AOM-2) are used as a switch and controlled with a microcontroller (MC). A polarization-beam splitter (PBS) is then used to generate two orthogonal linear states of polarization (SOPs), one defining the $|H\rangle$ SOP and the other defining the $|V\rangle$ SOP. When the MC sends a bit '0', the AOM-1 allows one photon at the $|H\rangle$ SOP to be sent and when it sends a bit '1', the AOM-2 allows a photon at the $|V\rangle$ SOP to be sent. Two polarization controllers

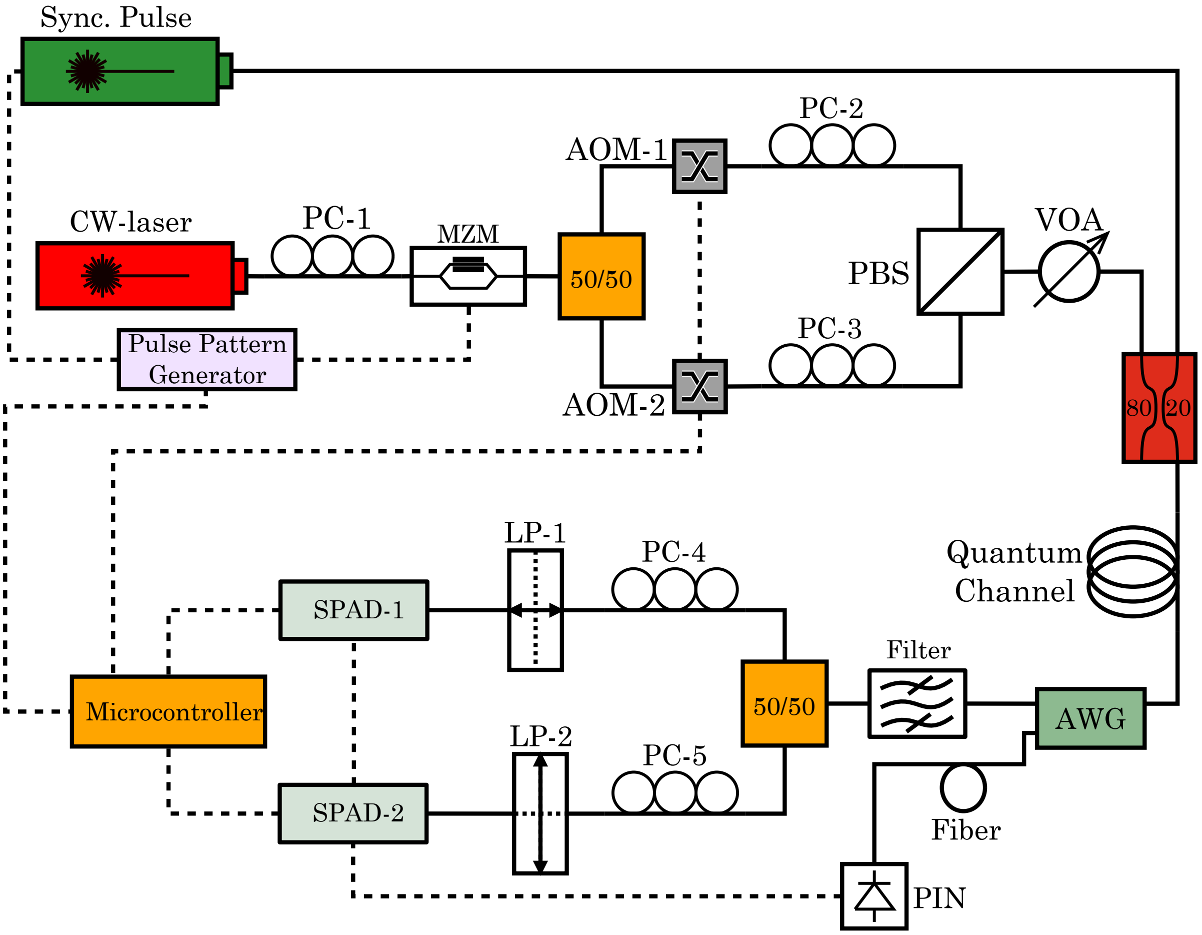

Figure 4.1: Scheme of the experimental setup used to measure the QBER in a polarization-encoding system in optical fibers. The synchronization signal is sent co-propagating. (Solid lines - optical fibers; dashed lines - electrical cables.)

(PC-2 and PC-3) are used to align the polarization of the photons with the axes of the PBS. After passing through the PBS, all pulses are attenuated with a variable-optical attenuator (VOA) in order to generate an average number of photons per pulse, $\mu \approx 0.1$. Then, the photons are transmitted through the quantum channel (an optical fiber) and reach Bob. Bob has another 50/50 BS and two linear polarizers (LPs), LP-1 set at 0° and LP-2 set at 90°. The polarization controllers, PC-4 and PC-5, allow to initially adjust the polarization of the photons with the axes of the LPs. Finally, photons are detected using two single-photon avalanche diodes (SPADs). SPAD-1 (id200) has a dark-count probability per time gate, $t_\mathrm{g} = 5\,\mathrm{ns}$, of $P_\mathrm{dc}^{(1)} = 6.50 \times 10^{-5}\,\mathrm{ns}^{-1}$ and a quantum detection efficiency, $\eta_\mathrm{D}^{(1)} \approx 10\,\%$. SPAD-2 (id201) has a dark count probability per time gate, $t_\mathrm{g} = 5\,\mathrm{ns}$, of $P_\mathrm{dc}^{(2)} = 2.55 \times 10^{-5}\,\mathrm{ns}^{-1}$ and a quantum detection efficiency $\eta_\mathrm{D}^{(2)} \approx 10\,\%$. A classical signal from an external-cavity laser (ECL), centered at $\lambda_\mathrm{s} = 1547.72\,\mathrm{nm}$ and that works as a synchronization signal, is inserted in a 80/20 optical coupler (OC) and sent to the quantum channel. This signal is externally modulated with the same frequency of the quantum signal, with the help of the pulse pattern generator. After the fiber, classical and quantum signals are separated using an arrayed-waveguide grating (AWG) with a 200 GHz channel separation. Then, an additional optical fiber is used to compensate path differences in order to synchronize the arrival of photons from the quantum signal with the opening of the detector's gate window. The filter after the AWG is used to avoid that photons from the synchronization pulse reach the SPAD. The detection of the synchronization pulse is performed with a classical detector (PIN) which give the trigger to both SPADs. The SPADs are connected to the MC, which compares the qubits received with the ones sent, in order to calculate the QBER.

The instantaneous QBER of the transmission can be simply defined as the ratio between the wrong bits, e_r, over the total number of bits received, N_r [26]

$$\widehat{\mathrm{QBER}} = \frac{e_\mathrm{r}}{N_\mathrm{r}}. \tag{4.1}$$

The number of errors can be due to dark counts in the SPADs, noise and imperfections in the fiber link and other transmission impairments such as polarization rotation [26].

For the estimation of the $\widehat{\mathrm{QBER}}$ we have sent a pseudo-random bit sequence (PRBS) with a length, $F_\mathrm{S} = 2^{17}$ bits, through different fiber lengths. First, we considered a back-to-back situation, using only a 1 m optical fiber, then a 8 km and finally a 20 km optical fiber. The results of the measurements for a 3-hours run are shown in Fig. 4.2. From the results shown in

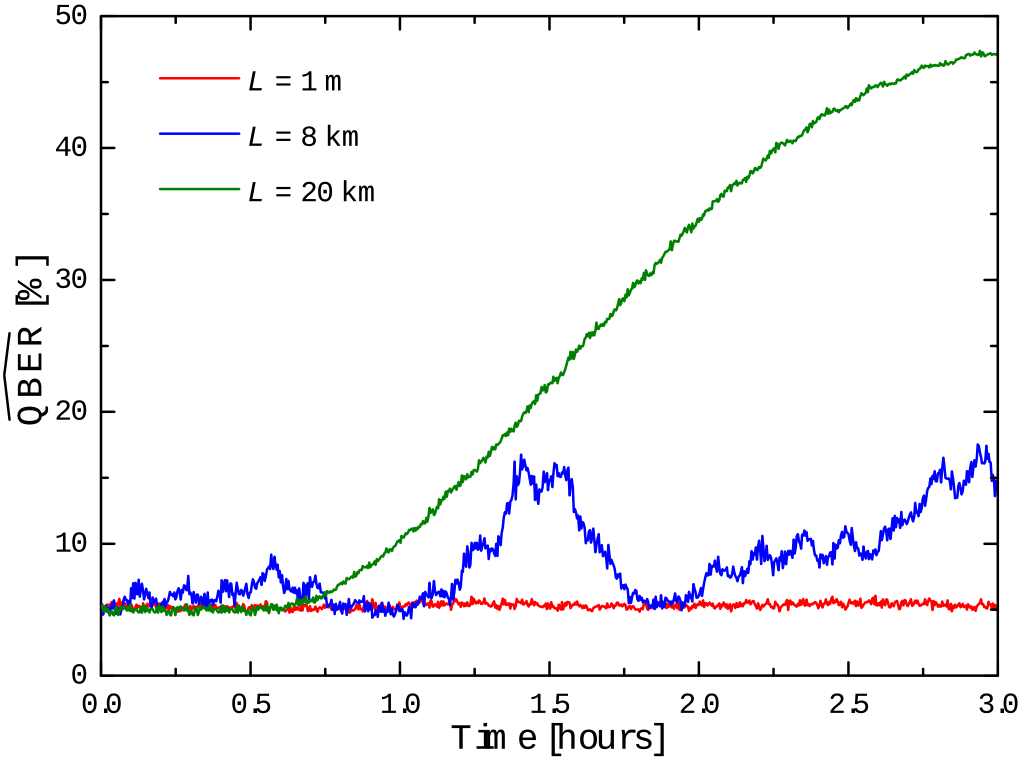

Figure 4.2: Evolution of the $\widehat{\mathrm{QBER}}$ with time for different fiber links working as transmission channel, when sending the synchronization pulse co-propagating.

this figure, we can see that in the back-to-back situation the $\widehat{\text{QBER}}$ remains constant during the full run and it is expected to behave like that, unless some perturbation is applied to the system. When the photons needed to travel through a long-distance optical fiber, we can see that the $\widehat{\text{QBER}}$ has a different evolution from the back-to-back situation. The first observation is that the evolution of the $\widehat{\text{QBER}}$ depends on the fiber length that the photons need to travel. Then, we verify that with increasing the fiber length, the variation of the $\widehat{\text{QBER}}$ also increases. This is due to the fact that the polarization of the photons evolves randomly during transmission through the optical fiber, and is as large as the fiber length. In practice, this random evolution gives rise to a random number of errors in detection. Another aspect which is worth discussing is the initial value for the $\widehat{\text{QBER}}$. As we can see, the system started from a $\widehat{\text{QBER}}$ value near 5%, which is a bit higher than expected. The main contribution for this value were cross-talk photons from the synchronization signal which were not totally filtered. We noticed that the cross-talk photons contributed with about 30% of the total counts. This value was obtained by measuring the counts that reached the detectors when only the synchronization signal was active.

4.2.2 Transmission Scheme using a Synchronization Pulse Counter-Propagating

One way to decrease the cross-talk counts in detection is to send the synchronization pulse in a counter-propagating direction, as shown in Fig. 4.3. In this case, the synchronization pulse entered in the AWG, passed through the quantum channel and then outputted from the 80/20 BS, before being detected in the PIN, which gave the trigger to both SPADs. Using this setup, the same measurements as for the previous case were performed. The results are shown in Fig. 4.4. Looking at the experimental results shown in this figure, we can see that the main difference is in the background $\widehat{\text{QBER}}$, which decreased from about 5% to nearly 1%. This is due to a much larger suppression of the cross-talk counts. In fact, even when sending the synchronization pulse in the counter-propagating direction it is not possible to completely avoid cross-talk counts, since the AWG has a limited non-adjacent channel isolation. However, through the use of this scheme it is possible to reduce the cross-talk counts from 30% to only about 4%. Regarding the variation of the $\widehat{\text{QBER}}$ with time, we can see that it presents an evolution that is similar to what is observed in Fig. 4.2, which is a constant behavior in the back-to-back situation and a random behavior when an optical fiber is used to transmit the photons.

From these two experiments we were able to obtain two main conclusions: first, it was clear that cross-talk between channels should be avoided, since it degrades the quality of the transmission; second, we noticed that since the polarization of the photons changes randomly when they travel through an optical fiber, it is mandatory to use a polarization control scheme in order to maintain the error rate as stable and as low as possible.

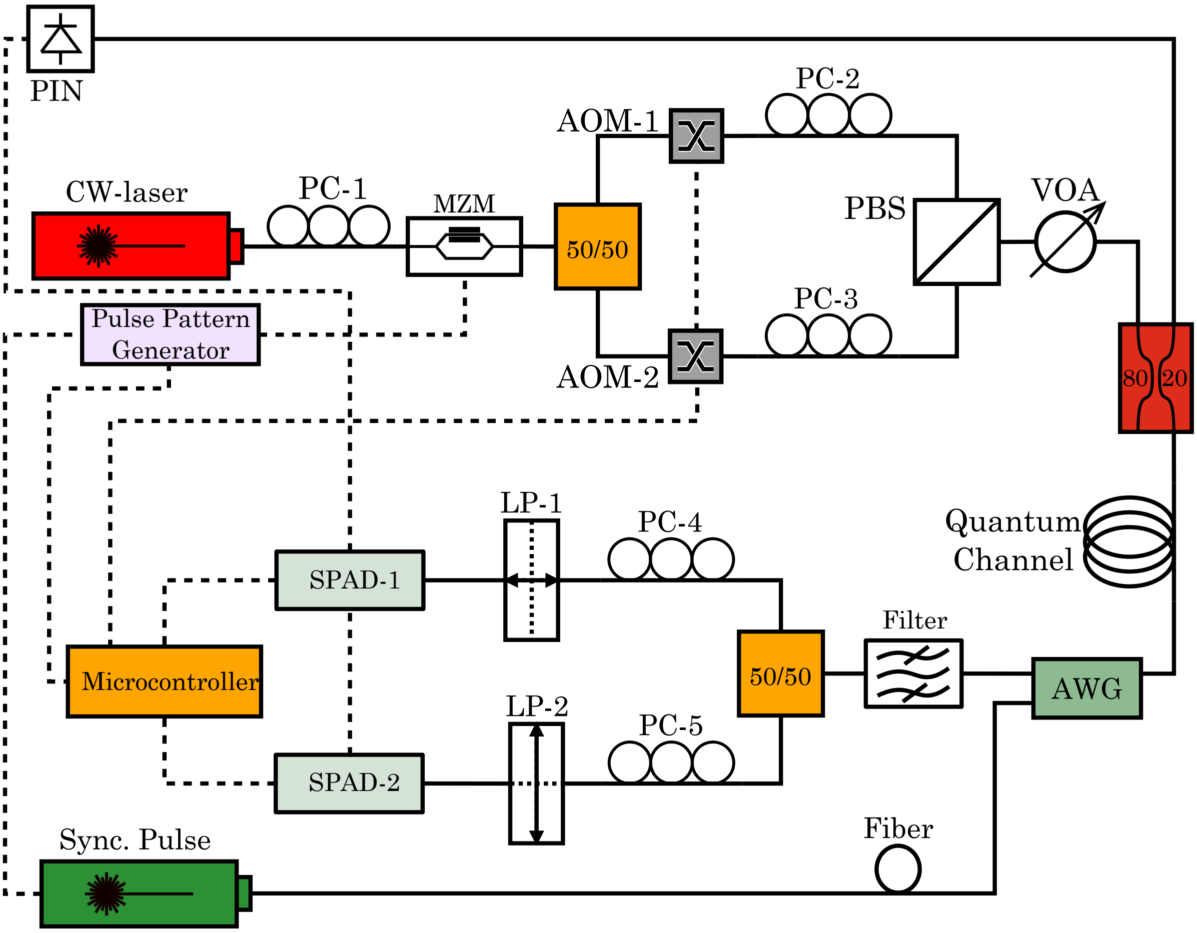

Figure 4.3: Scheme of the experimental setup used to measure the QBER in a polarization-encoding system in optical fibers. The synchronization signal is sent counter-propagating. (Solid lines - optical fibers; dashed lines - electrical cables.)

4.2.3 Encoding, Transmission and Detection of Polarization-Encoded Photons

Next, we want to demonstrate the feasibility of an encoding/decoding system of quantum communications, using the stimulated FWM photon source presented in Chapter 3. To do that, we implemented the experimental setup shown in Fig. 4.5. Following the description of the scheme in Fig. 3.7, after the generation of photons from the stimulated FWM process, we have used a polarization controller (PC-4) and a linear polarizer (LP-2) to make sure that all photons that outputted from the source were linearly polarized. The average number of photons per pulse at the output of the source, μ, was adjusted to approximately 0.2. A half-wave plate (HWP) was used to do the encoding in photon's polarization. Then, the photons were transmitted through a quantum channel (an optical fiber) and reached a 50/50 BS. In each arm of the BS was a polarization controller (PC-5 and PC-6), a linear polarizer (LP-3

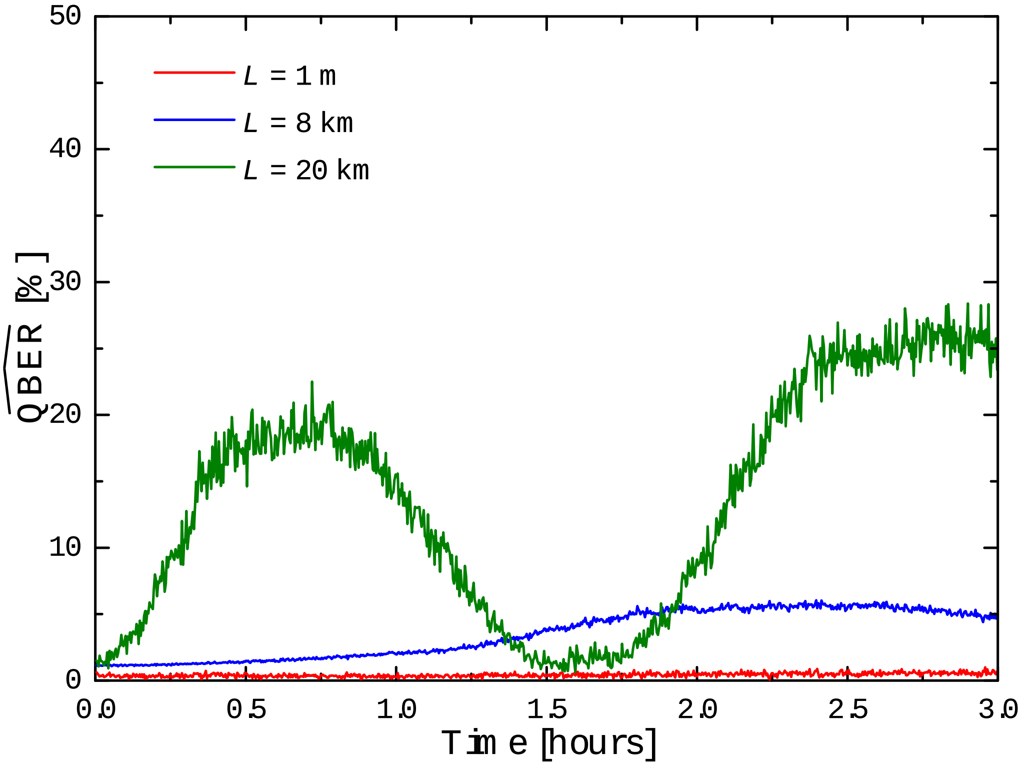

Figure 4.4: Evolution of the $\widehat{\text{QBER}}$ with time for different fiber links working as transmission channel, when sending the synchronization pulse counter-propagating.

and LP-4) and two SPADs. The two linear polarizers were set at 0° (LP-3) and 45° (LP-4). SPAD-1 (id200) has a dark-count probability per time gate, $t_{\mathrm{g}} = 5\,\mathrm{ns}$, of $P_{\mathrm{dc}}^{(1)} = 6.50\times10^{-5}\,\mathrm{ns}^{-1}$ and a quantum detection efficiency, $\eta_{\mathrm{D}}^{(1)} \approx 10\,\%$. SPAD-2 (id201) has a dark count probability per time gate, $t_{\mathrm{g}} = 5\,\mathrm{ns}$, of $P_{\mathrm{dc}}^{(2)} = 2.55\times10^{-5}\,\mathrm{ns}^{-1}$ and a quantum detection efficiency $\eta_{\mathrm{D}}^{(2)} \approx 10\,\%$. In this experiment, the synchronization between the arrival of photons and the opening of the gate was performed directly from the Pulse Pattern Generator.

Theoretical Model

In order to derive a theoretical model for the rate of photons that are expected to be received when using the experimental scheme shown in Fig. 4.5, we need to consider all devices from the photon source to detection. Therefore, as we have determined in Section 3.3, when the FWM source generates a low number of photons per pulse, $\mu \ll 1$, its statistical distribution will follow a thermal statistics [27, 28]. In this case, the probability of a pulse to carry n photons is given by [29–31]

$$P_{\mathrm{th}}(n,\mu) = \frac{\mu^n}{(1+\mu)^{n+1}}. \qquad (4.2)$$

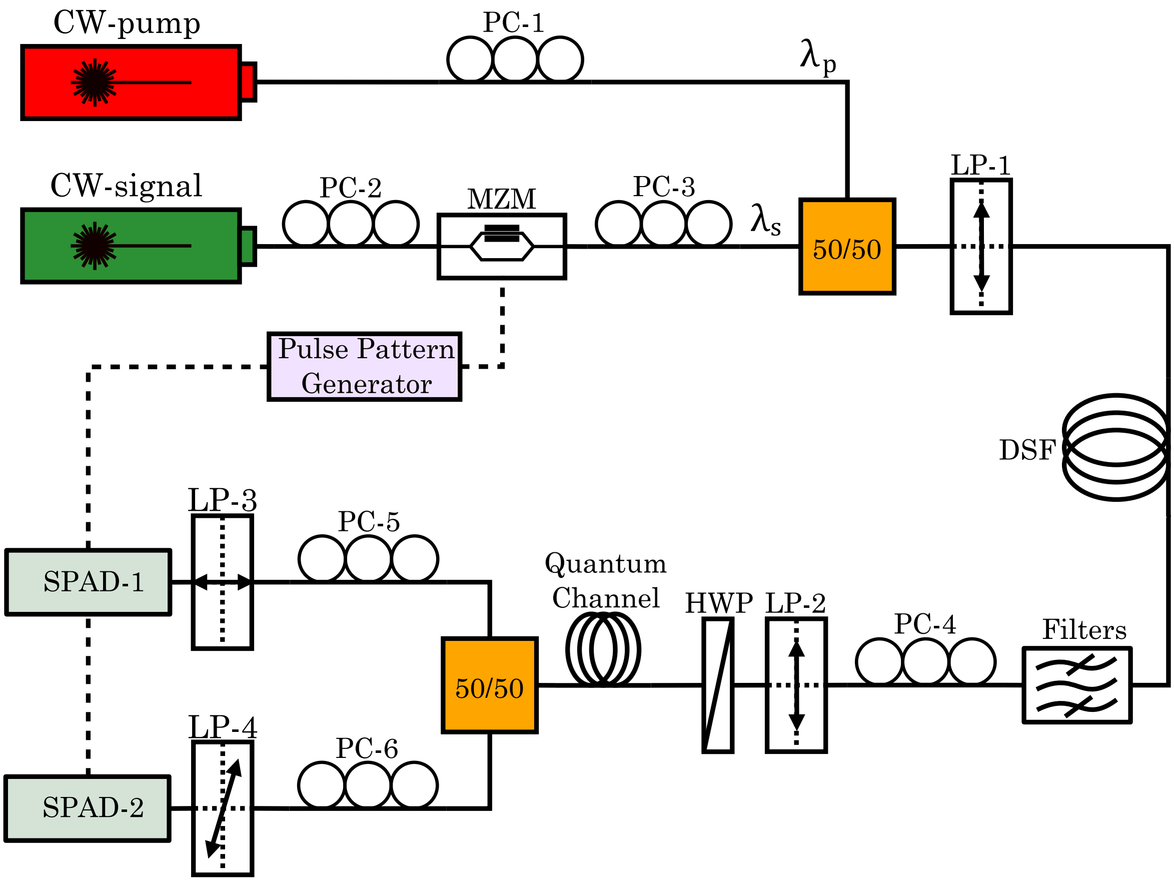

Figure 4.5: Schematics of the experimental setup used to generate, encode, transmit and detect photons from the stimulated FWM. (Solid lines - optical fibers; dashed lines - electrical cables.)

Moreover, it is know that an avalanche can be triggered only when the SPADs receive at least one photon [32]. The probability of a pulse to carry at least one photon is then written as

$$P(n \geq 1, \mu) = 1 - P_{\mathrm{th}}(0, \mu). \tag{4.3}$$

When substituting Eq. (4.2) in Eq. (4.3) we obtain

$$P(n \geq 1, \mu) = 1 - \frac{1}{(1+\mu)}. \tag{4.4}$$

After passing through the quantum channel, the contribution from attenuation should be included and then Eq. (4.4) is now written as

$$P(n \geq 1, \mu) = 1 - \frac{1}{(1+\eta_{\mathrm{F}}\mu)}, \tag{4.5}$$

where

$$\eta_{\rm F} = 10^{-\alpha_{\rm f} L/10}, \tag{4.6}$$

with $\alpha_{\rm f}$ and L being the attenuation coefficient and the length of the quantum channel, respectively [33].

After transmission through the quantum channel, photons pass through a 50/50 BS, which will generate two beams with independent statistics. Therefore, Eq. (4.5) can be rewritten as [34]

$$P(n \geq 1, \mu) = 1 - \frac{1}{(1 + \frac{\eta_{\rm F}\mu}{2})}. \tag{4.7}$$

After passing through the BS, each beam finds a PC and a LP. The PCs allow to compensate for polarization rotations in the quantum channel, while the LPs work as polarization analyzers. This way, the LPs will transmit photons in the state $|T_\theta\rangle$, which is given by

$$|T_\theta\rangle = \cos(\theta)|H\rangle + \sin(\theta)|V\rangle. \tag{4.8}$$

In Eq. (4.8), $|H\rangle$ and $|V\rangle$ represent horizontally and vertically polarized SOPs, respectively, and the transmission axis forms an angle θ with the horizontal [35]. We assume an input state of the form

$$|\psi_\phi\rangle = \cos(\phi)|H\rangle + \sin(\phi)|V\rangle, \tag{4.9}$$

where ϕ represents the rotation angle of the SOP [2]. The probability of transmission of the state through the LP is given by

$$P_{\rm t} = |\langle T_\theta|\psi_\phi\rangle|^2. \tag{4.10}$$

Substituting Eqs. (4.8) and (4.9) in Eq. (4.10), we obtain

$$P_{\rm t} = \frac{1}{2}\Bigg(1 + \cos(2\theta)\cos(2\phi)\Bigg) + 2\cos(\theta)\cos(\phi)\sin(\theta)\sin(\phi). \tag{4.11}$$

In the SPADs, the photons will have a probability to be detected which is given by

$$P_{\rm d} = P(n \geq 1, \mu)P_{\rm t}. \tag{4.12}$$

Using Eqs. (4.7) and (4.11) and adding the contributions from losses in the fiber, losses in the connectors and the quantum efficiency of the detectors, Eq. (4.12) can be written as

$$P_{\rm d} = \Bigg(1 - \frac{1}{(1 + \frac{\eta_{\rm F}\eta_{\rm B}\eta_{\rm D}\mu}{2})}\Bigg)\Bigg(\frac{1}{2}\Bigg(1 + \cos(2\theta)\cos(2\phi)\Bigg) + 2\cos(\theta)\cos(\phi)\sin(\theta)\sin(\phi)\Bigg), \tag{4.13}$$

where $\eta_{\rm B} = 10^{-L_{\rm B}/10}$, with $L_{\rm B}$ representing the total losses in each arm between the BS and the SPAD and $\eta_{\rm D}$ is the quantum detection efficiency of each detector. The probability of a detector to click can be calculated from

$$P_{\rm click} = P_{\rm d} + P_{\rm dc}\tau_{\rm g} - P_{\rm d}P_{\rm dc}\tau_{\rm g}, \tag{4.14}$$

where $P_{\rm dc}$ is the probability of having a click due to detector's dark counts and $\tau_{\rm g}$ is the time gate window [33]. Finally, the probability of click can be written in terms of the effective counts in the detectors as

$$C_{\rm D} = f_{\rm rep} P_{\rm click}, \tag{4.15}$$

where $f_{\rm rep}$ is the pulse repetition rate [33].

Experimental Results

In this section, we will present and discuss the experimental results obtained from the implementation of the experimental scheme shown in Fig. 4.5.

Before starting the measurements, we have performed an initial calibration of the system, *i.e.*, at the output of the photon source we have maximized the counts for two nonorthogonal linear SOPs. First, the HWP was set at 0° and PC-5 was adjusted in order to measure the maximum number of counts in SPAD-1, with the transmission axis of the LP-3 at 0°. Then, the HWP was set at 45° and PC-6 adjusted to give the maximum count rate in SPAD-2, with the transmission axis of LP-4 also at 45°. After the initial calibration, the HWP was rotated back again to 0° and we started to register the photon counts in the SPADs every 15°. For the quantum channel we have considered four different cases: back-to-back (1 m), 20 km, 40 km and 60 km of optical fiber.

In Fig. 4.6, we present the average number of counts registered with the SPADs, during a 20 s interval, as a function of the HWP angle, θ, along with the theoretical fits given by Eq. (4.15). From the results in Fig. 4.6 there are several conclusions to discuss. The first one and the most important is that we were able to encode and then decode correctly the polarization of photons, after transmission through a long-distance quantum channel. This can be seen from the fact that we were able to recover a given polarization at the receiving side, as it was encoded by the sender. The second conclusion comes from the match between the experimental results and the theoretically expected ones, obtained from Eq. (4.15). Looking at Eq. (4.8), we can see that the maximum number of counts is found when the input polarization is aligned with the transmission axis of the LP and the minimum is found when they are orthogonal to each other. This is what is observed from the experimental results. Comparing the plots for different fiber lengths, we can see that the average number of counts decreases with the fiber length, which is due to fiber attenuation.

In Table 4.1, we present the values of ϕ and R^2, obtained from the theoretical fit to the experimental results, along with the visibility of each SOP, calculated from Eq. (3.31). From the results present in this table, we can confirm the good adjustment between theoretical results and experimental data, as can be seen from the high values of R^2. Looking at the values of ϕ, we can see that the angles of the SOPs detected are very close to their initial angles, *i.e.*, 0° for $|H\rangle$ SOP and 45° for $|+45\rangle$ SOP. This tells us that the theoretical model used to describe the experimental data is accurate and was validated. From the high visibility values obtained, we can conclude that all SOPs are practically linear, even after transmission through a 60 km

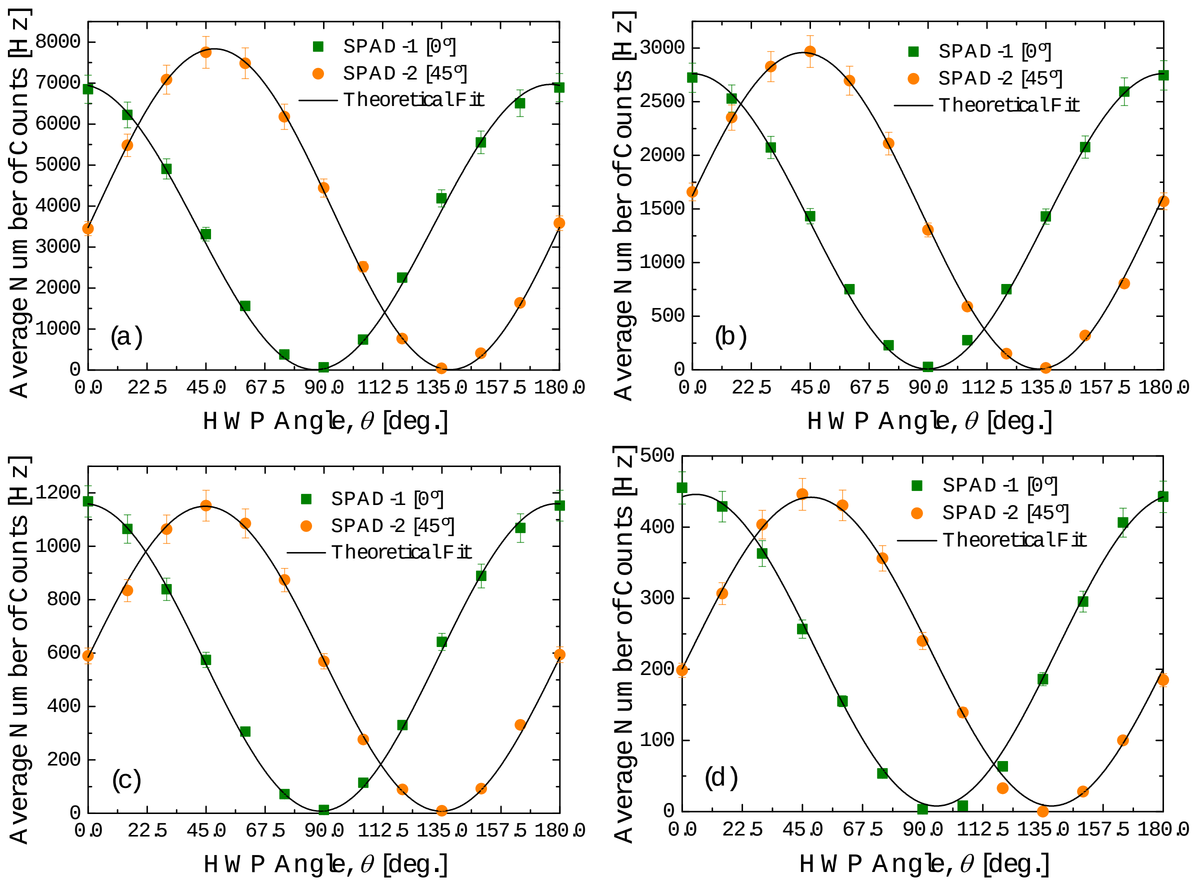

Figure 4.6: Average number of photon counts as a function of the HWP angle after propagation through (a) 1 m, (b) 20 km, (c) 40 km and (d) 60 km of optical fiber. The black line is the theoretical fit obtained from Eq. (4.15). The pump and signal optical powers at the DSF input were $P_p(0) = 3.42$ dBm, and $P_s(0) = -25.77$ dBm, respectively. The error bars represent a 5% deviation in relation to each value.

Table 4.1: Fitting parameters from Eq. (4.15) to the results in Fig. 4.6, for each SOP and corresponding visibility values calculated with Eq. (3.31).

	$\vert H\rangle$			$\vert +45\rangle$		
L (km)	ϕ (°)	R^2	V (%)	ϕ (°)	R^2	V (%)
0.001	-3.35	0.9967	98.13	48.26	0.9993	99.03
20	-0.20	0.9980	98.04	42.27	0.9989	99.71
40	-1.32	0.9982	97.93	44.72	0.9982	99.99
60	5.12	0.9962	98.56	48.21	0.9968	99.97

quantum channel, which allows us to establish an encoding/decoding scheme.

4.3 Real-Time Polarization Control Method

In this section, we present a method to control polarization in real time which uses frames where both control and data qubits are obtained from a quantum signal. This way, the use of classical signals and additional devices in the system is not necessary. The method is based in the Clopper-Pearson confidence interval and allows a rigorous and efficient estimation of the QBER. The number of qubits in each frame and which are used in estimation of the QBER is optimized continuously, allowing to maximize the bandwidth of data to transmit. Next, we will describe a system used in quantum communications and how to incorporate the real-time polarization control method.

4.3.1 System Description

A typical system used in quantum communications can be seen in Fig. 4.7. For the description of the system we assume a BB84-type quantum protocol, using the polarization as encoding scheme. Alice includes a few-photons source and a polarization-encoding device. In this device, data bits, which are obtained from a random generator, are encoded in the polarization of photons, using two nonorthogonal bases. The bases to encode the bits are randomly chosen by Alice, from the rectilinear and the diagonal bases. Then, the qubits are transmitted through the quantum channel and reach Bob. Bob chooses the measurement bases also randomly, and independently from Alice. The detection of photons is performed with SPADs, each one detecting one logical symbol. When each detector clicks separately, we have single clicks, and when they click simultaneously, we will have the so-called double clicks. Since we cannot distinguish between a double click from two sent photons, one photon and a dark count, and two dark counts, we discard them. Bob's measurements are sent to a data processor and treated according to the protocol to implement.

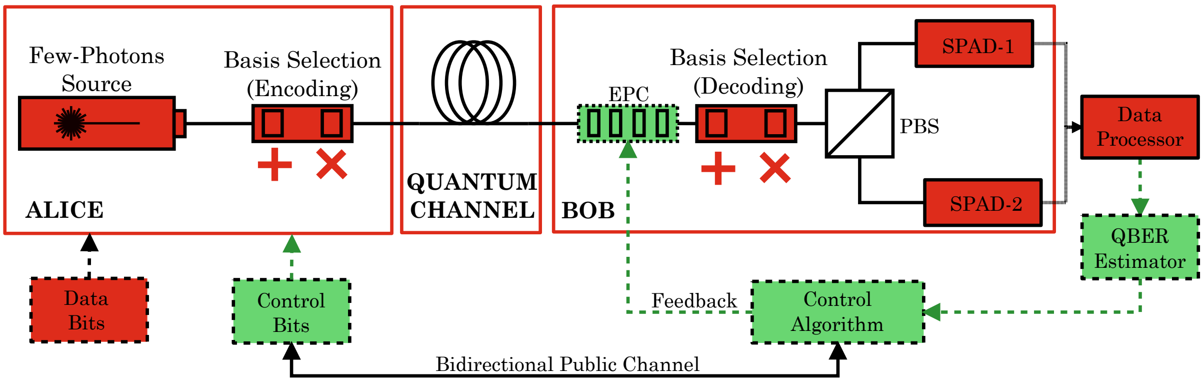

Figure 4.7: Schematic draw of a system employed in quantum communications using single photons (in red - solid lines), and the proposed system for compensation of polarization (in green - dashed lines). EPC: Electronic Polarization Controller, D: Detectors.

The transmission method is based on frames which contain control and data qubits, both obtained from quantum signals (see Fig. 4.8). The continuous control of polarization is achieved through the use of a feedback system containing a QBER estimator, a control algorithm and an EPC. The QBER is estimated from the control qubits received. In order to assure that control and data qubits present the same QBER, it is required that their statistics are the same, not only in terms of logical values but also regarding coding bases. This way, the two must form a deterministic sequence of bits. Next, we present a theoretical model for the rigorous estimation of the QBER.

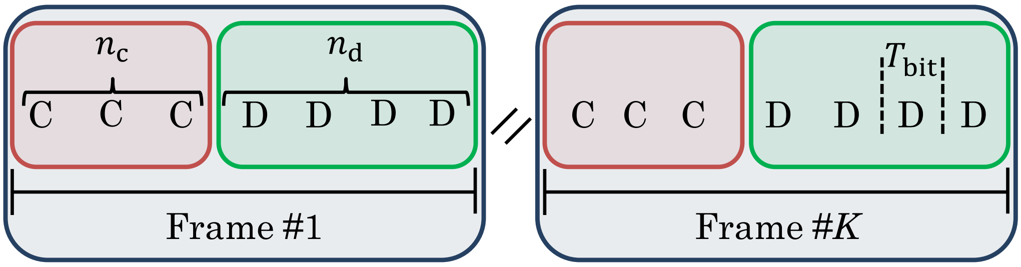

Figure 4.8: Structure of an infinite sequence of qubits of control (C) and data (D). In each frame there are n_c qubits of control and n_d qubits of data. The period of one bit is represented by T_{bit}.

4.3.2 Theoretical Model for QBER Estimation

Limiting Bounds for the QBER

Following Eq. (4.1), we can generalize the QBER by defining it as

$$\text{QBER} = \lim_{N_r \to \infty} \frac{e_r}{N_r}, \tag{4.16}$$

assuming that the number of qubits to receive is nearly infinite [26]. However, for practical purposes an infinite number of qubits cannot be used. Therefore, we have to consider an estimation of the QBER which is based on a finite number of qubits as shown in Eq. (4.1). Therefore, the first problem is to calculate N_r such that $\widehat{\text{QBER}} \approx \text{QBER}$.

We start by assuming that, in the system, errors occur independently from each other. Then, the number of errors can be written as $e_r = \sum_{i=1}^{N_r} e_i$, where e_i is a random Bernoulli variable, assuming the value 1 when there is an error and the value 0 when there is no error. Based on this assumption, e_r is defined as a random binomial variable.

The probability to detect wrongly e_r qubits in N_r detections is given by [36]

$$P_{N_\mathrm{r}}(e_\mathrm{r}) = \frac{N_\mathrm{r}!}{e_\mathrm{r}!(N_\mathrm{r}-e_\mathrm{r})!}\mathrm{QBER}^{e_\mathrm{r}}(1-\mathrm{QBER})^{N_\mathrm{r}-e_\mathrm{r}}. \tag{4.17}$$

When less than N errors occur in N_r qubits received, Eq. (4.17) can be expanded to the cumulative binomial distribution function and we obtain

$$P(e_\mathrm{r} \leq N) = \sum_{e_\mathrm{r}=0}^{N} \frac{N_\mathrm{r}!}{e_\mathrm{r}!(N_\mathrm{r}-e_\mathrm{r})!}\mathrm{QBER}^{e_\mathrm{r}}(1-\mathrm{QBER})^{N_\mathrm{r}-e_\mathrm{r}}. \tag{4.18}$$

Nevertheless, Eq. (4.18) depends on the QBER, which is an unknown parameter of the system. Then, we aim at finding the smallest value for N_r which ensures that the QBER is within the limiting bounds, $\mathrm{QBER}_\mathrm{LB} \leq \mathrm{QBER} \leq \mathrm{QBER}_\mathrm{UB}$, with probability $1-\alpha$, where $\mathrm{QBER}_\mathrm{LB}$ is the lower QBER bound, $\mathrm{QBER}_\mathrm{UB}$ is the upper QBER bound and α is the confidence level in the estimation of the $\widehat{\mathrm{QBER}}$.

One way to calculate the limiting bounds for the QBER is through the Clopper-Pearson confidence interval, which is an exact method based on inverting the equal-tailed binomial test [37]. The upper bound is found by solving the equation [37–39]

$$\sum_{k=0}^{e_\mathrm{r}} \frac{N_\mathrm{r}!}{k!(N_\mathrm{r}-k)!}\mathrm{QBER}_\mathrm{UB}^{k}(1-\mathrm{QBER}_\mathrm{UB})^{N_\mathrm{r}-k} = \frac{\alpha}{2}, \tag{4.19}$$

while the lower bound is obtained from [37–39]

$$\sum_{k=e_\mathrm{r}}^{N_\mathrm{r}} \frac{N_\mathrm{r}!}{k!(N_\mathrm{r}-k)!}\mathrm{QBER}_\mathrm{LB}^{k}(1-\mathrm{QBER}_\mathrm{LB})^{N_\mathrm{r}-k} = \frac{\alpha}{2}. \tag{4.20}$$

The solution for Eqs. (4.19) and (4.20) is given by the quantiles of beta distributions as [38, 39]

$$\mathrm{QBER}_\mathrm{UB}(N_\mathrm{r}, e_\mathrm{r}, \alpha) = \beta(1-\tfrac{\alpha}{2}, e_\mathrm{r}+1, N_\mathrm{r}-e_\mathrm{r}), \tag{4.21}$$

and

$$\mathrm{QBER}_\mathrm{LB}(N_\mathrm{r}, e_\mathrm{r}, \alpha) = \beta(\tfrac{\alpha}{2}, e_\mathrm{r}, N_\mathrm{r}-e_\mathrm{r}+1). \tag{4.22}$$

Since Eqs. (4.21) and (4.22) are difficult to solve using computational methods closer to hardware, it is preferable to use approximations. Therefore, for values of $N_\mathrm{r} \gtrsim 40$ [39], the asymptotic expressions for $\mathrm{QBER}_\mathrm{UB}$ and $\mathrm{QBER}_\mathrm{LB}$ up to $\mathcal{O}(N_\mathrm{r}^{-3/2})$ are given by

$$\mathrm{QBER}_\mathrm{UB} = \widehat{\mathrm{QBER}} + N_\mathrm{r}^{-1/2} z_{\alpha/2}\left[\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}})\right]^{1/2} + \frac{1}{3N_\mathrm{r}}\left[2\left(\tfrac{1}{2}-\widehat{\mathrm{QBER}}\right)z_{\alpha/2}^2 + (2-\widehat{\mathrm{QBER}})\right], \tag{4.23}$$

and

$$\mathrm{QBER_{LB}} = \widehat{\mathrm{QBER}} - N_\mathrm{r}^{-1/2} z_{\alpha/2} \left[\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}})\right]^{1/2} + \frac{1}{3N_\mathrm{r}}\left[2\left(\tfrac{1}{2}-\widehat{\mathrm{QBER}}\right)z_{\alpha/2}^2 - (1+\widehat{\mathrm{QBER}})\right], \quad (4.24)$$

where $z_{\alpha/2}$ is the $100(1-\frac{\alpha}{2})$th percentile of a standard normal distribution [37, 38].

After having the expressions for the two QBER limiting bounds, now we can simulate the evolution of $\widehat{\mathrm{QBER}}$ with N_r. Results for a single estimation of the $\widehat{\mathrm{QBER}}$ for each N_r, alongside the upper and lower bounds calculated from Eqs. (4.23) and (4.24), respectively, are shown in Fig. 4.9. In the simulation, we have considered that QBER = 10 %. The theoretical bounds obtained from Eqs. (4.23) and (4.24) when $\widehat{\mathrm{QBER}} = 10\,\%$ are also plotted. Looking at the results, the immediate conclusion is that the $\widehat{\mathrm{QBER}}$ tends to the QBER value as N_r increases. Also, we verify that the estimated and the expected bounds are in a good agreement. Finally, we found that in only about 3 % of the cases the interval estimated for the QBER does not includes the real value of the QBER, which is within the defined confidence level of 5 %.

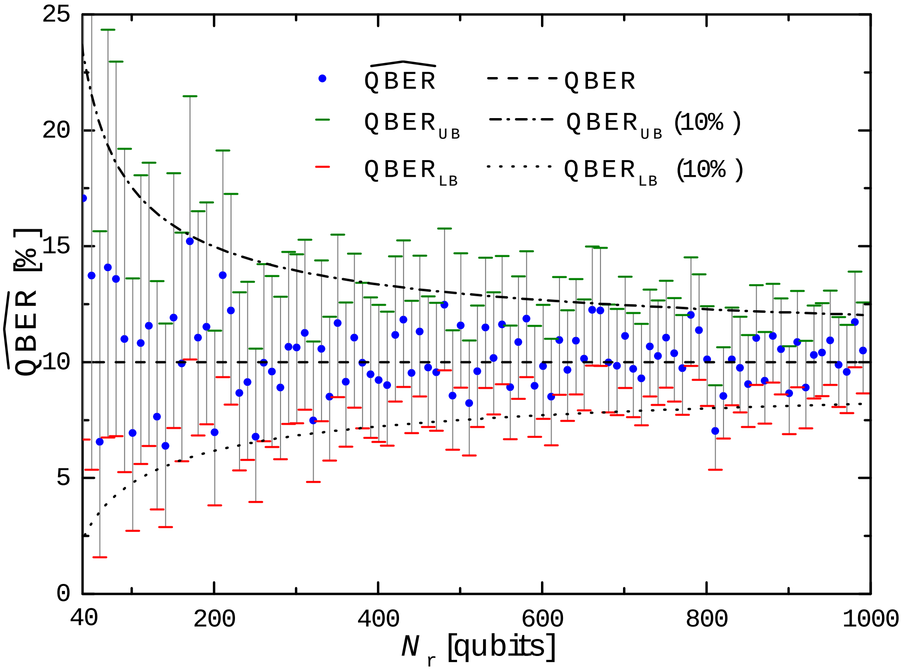

Figure 4.9: A single estimation of the $\widehat{\mathrm{QBER}}$ for each N_r along with the upper and lower bounds obtained from Eqs. (4.23) and (4.24), respectively. The theoretical expectancies for upper (dot-dashed line) and lower (dotted line) bounds assuming in the same equations that $\widehat{\mathrm{QBER}} = 10\,\%$ are also shown. The confidence level was set as $\alpha = 0.05$.

Another plot of interest is the behavior of the $\widehat{\mathrm{QBER}}$ when we fix the number of bits received. This allows us to conclude about the accuracy in the estimation. In Fig. 4.10 we show the simulation of different trials of the $\widehat{\mathrm{QBER}}$ when $N_\mathrm{r} = 500$ qubits, together with the upper and lower bounds from Eqs. (4.23) and (4.24), respectively. The results in this figure tell

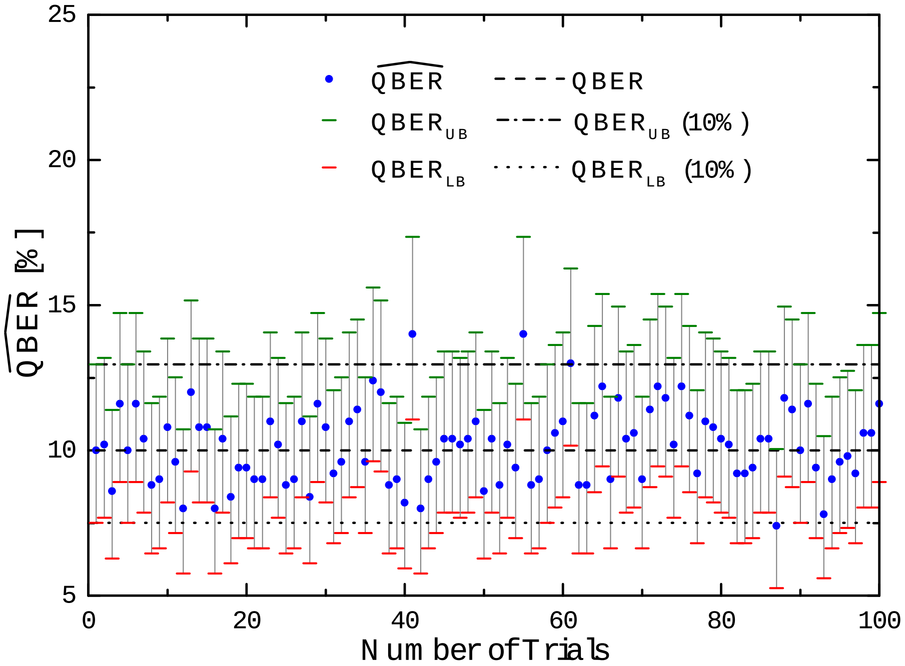

Figure 4.10: Different trials of $\widehat{\text{QBER}}$ along with the upper and lower bounds obtained from Eqs. (4.23) and (4.24), respectively, when $N_{\text{r}} = 500$ qubits. The theoretical expectancies for upper (dot-dashed line) and lower (dotted line) bounds using the same equations, when $\widehat{\text{QBER}} = 10\,\%$, are also shown. The confidence level is $\alpha = 0.05$.

us that the $\widehat{\text{QBER}}$ can be estimated accurately and that in only $3\,\%$ of the trials the upper or lower bounds do not include the QBER value. The theoretical bounds for the case when the $\widehat{\text{QBER}} = 10\,\%$ are also in good agreement with the calculated ones.

Next, we will show how to calculate the minimum number of control qubits, N_{r}, which are required for the accurate estimation of the QBER.

Calculation of the Minimum Value for N_{r}

The length between the upper and lower bounds and which defines the precision in the estimation of the QBER, is given by

$$d = \text{QBER}_{\text{UB}} - \text{QBER}_{\text{LB}}, \tag{4.25}$$

where QBER_{UB} and QBER_{LB} are obtained from Eqs. (4.23) and (4.24), respectively. If $N_{\text{r}} \to \infty$, the asymptotic expansion for the expected length of the $1 - \alpha$ Clopper-Pearson interval gives [39]

$$d = 2z_{\alpha/2}N_\mathrm{r}^{-1/2}(\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}}))^{1/2} + N_\mathrm{r}^{-1} + N_\mathrm{r}^{-3/2}(\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}}))^{-1/2}\times \\ \frac{z_{\alpha/2}}{18}\left(z^2_{\alpha/2} - \frac{5}{2} - 17(\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}})) - 13(\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}}))z^2_{\alpha/2}\right) + \mathcal{O}(N_\mathrm{r}^{-2}). \quad (4.26)$$

If we consider only the terms up to the first order, Eq. (4.26) is now written as

$$d \approx 2z_{\alpha/2}N_\mathrm{r}^{-1/2}(\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}}))^{1/2} + N_\mathrm{r}^{-1}. \quad (4.27)$$

Since the parameter d represents an absolute length, we introduce the variable d_r, which gives the length between upper and lower bounds relative to the $\widehat{\mathrm{QBER}}$ and which is defined as

$$d_\mathrm{r} = \frac{d}{\widehat{\mathrm{QBER}}}. \quad (4.28)$$

Solving now Eq. (4.27) for a given d_r, it is possible to find the minimum value for N_r as

$$N_\mathrm{r} = \left\lceil \frac{2z^2_{\alpha/2}\widehat{\mathrm{QBER}}(1-\widehat{\mathrm{QBER}})}{(d_\mathrm{r}\widehat{\mathrm{QBER}})^2} \right\rceil + \\ \left\lceil \frac{2z_{\alpha/2}\sqrt{z^2_{\alpha/2}\widehat{\mathrm{QBER}}^2(1-\widehat{\mathrm{QBER}})^2 + d_\mathrm{r}\widehat{\mathrm{QBER}}^2(1-\widehat{\mathrm{QBER}})} + d_\mathrm{r}\widehat{\mathrm{QBER}}}{(d_\mathrm{r}\widehat{\mathrm{QBER}})^2} \right\rceil, \quad (4.29)$$

where $\lceil x \rceil$ is the ceiling function that gives the smallest integer greater than or equal to x.

Since we have already the expression to calculate N_r, next we will describe how to calculate its minimum value in a system where the QBER is unknown. The steps are the following:

1. we calculate N_r assuming an initial guess for $\widehat{\mathrm{QBER}}$, named $\widehat{\mathrm{QBER}}_{(0)}$;
2. we estimate the $\widehat{\mathrm{QBER}}$ of the system through the measurement of the number of errors, e_r, in N_r qubits, using Eq. (4.1),
3. using the value of $\widehat{\mathrm{QBER}}$ from the previous step a new value for N_r is calculated from Eq. (4.29).

We note that these steps can be applied iteratively until a stable N_r is found.

In order to evaluate the robustness of the method we have solved Eq. (4.29) numerically, assuming different values for the initial guess. The results of the simulation are shown in Fig. 4.11, considering that the expected value of the error rate is 10%. From the analysis of this figure we can see that it is possible to find the minimum value for N_r only after one iteration, regardless of the initial guess. We add that the method was also tested for small error rates, showing that is works up to values of the order of 10^{-3}, which makes it clearly suitable for quantum communication systems.

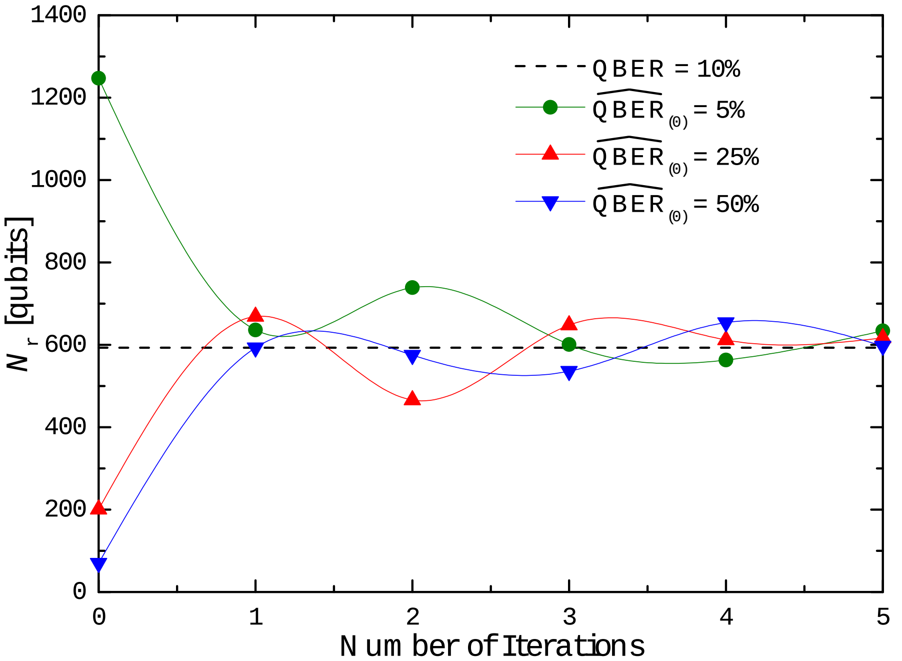

Figure 4.11: Total number of qubits received N_r as a function of the number of iterations. We assumed three different values for the initial guess, $\widehat{\text{QBER}}_{(0)}$, when QBER $= 10\,\%$. The confidence level is $\alpha = 0.05$ and $d_\text{r} = 0.5$.

At last, we will verify if the method is really effective in the control of polarization and determine also its operation range, assuming actual parameters.

Effectiveness of the Method

For this last task, we start by defining the frequency rate of control clicks in the detectors, which can be obtained from

$$R^\text{c}_\text{click} = \frac{N_\text{r}}{t_\text{r}}, \tag{4.30}$$

where t_r is the time to transmit the N_r control qubits. Equation (4.30) can also be written as

$$R^\text{c}_\text{click} = P_\text{click} f_\text{rep} \frac{n_\text{c}}{n_\text{c} + n_\text{d}}, \tag{4.31}$$

where f_rep is the repetition rate of the qubits and n_c and n_d are the number of control and data qubits in each frame, respectively. The probability to have a click in Bob's detectors was defined in Eq. (4.14). In this equation, to calculate the probability of detection we assume that qubits are generated from a highly attenuated laser source with an average number of photons per pulse μ. Therefore, the probability of detection is described by a Poissonian distribution and is given by [33]

$$P_\text{d} = 1 - e^{(-\eta_\text{F}\eta_\text{D}\mu)}. \tag{4.32}$$

If we equalize Eqs. (4.30) and (4.31) and rearrange the final expression, we obtain t_r as

$$t_\mathrm{r} = \frac{N_\mathrm{r}}{P_\mathrm{click} f_\mathrm{rep} \frac{n_\mathrm{c}}{n_\mathrm{c}+n_\mathrm{d}}}. \tag{4.33}$$

Equation (4.33) can also be written in terms of the number of control qubits that must be sent by Alice, N_s, as

$$t_\mathrm{r} = \frac{N_\mathrm{s}}{f_\mathrm{rep}}, \tag{4.34}$$

where N_s is given by

$$N_\mathrm{s} = \frac{N_\mathrm{r}}{P_\mathrm{click} \frac{n_\mathrm{c}}{n_\mathrm{c}+n_\mathrm{d}}}. \tag{4.35}$$

Equation (4.35) is particularly important due to the impact of losses in optical fibers and other components, but also due to the low quantum detection efficiencies. These factors lead to a number of qubits detected considerably smaller than the number of qubits sent and therefore should to be quantified.

Moreover, the drift time of polarization can be calculated from [40]

$$t_\mathrm{d} = \frac{2t_0}{3\nu^2 D_\mathrm{p}^2 L}, \tag{4.36}$$

where t_0 represents the drift time of the index difference between the fast and slow axes of a particular fiber, which depends on environmental conditions; $\nu = c/\lambda_\mathrm{p}$ and represents the frequency of the signal, with c being the speed of light and λ_p being the wavelength of the pump photons, and the term D_p is the polarization-mode dispersion (PMD) coefficient of the fiber. For the control of polarization to be effective, it is necessary that the condition $t_\mathrm{r} \ll t_\mathrm{d}$ is verified. In order to verify the validity range of this condition we made Eq. (4.33) equal to Eq. (4.36) and solved it numerically. The parameters which were considered are shown in Table 4.2.

In Fig. (4.12) we plot the drift time of polarization and the time to receive the N_r bits as a function of the fiber length. From this figure we were able to check that $t_\mathrm{r} = t_\mathrm{d}$ occurs for $L = 538\,\mathrm{km}$. This result tells us that the condition $t_\mathrm{r} \ll t_\mathrm{d}$ is verified for several hundreds of kilometers, which confirms that the polarization control method is able to work far beyond current transmission distances of quantum communication fiber links.

In the next subsection we will describe the polarization control algorithm used in the implementation of the method.

4.3.3 Polarization Control Algorithm

A schematic diagram of the polarization control algorithm is shown in Fig. 4.13. Next, we will present a detailed description of each step.

Table 4.2: Parameters used to plot Fig. (4.12).

Parameter	Value
μ	0.2 photons/pulse
P_{dc}	$1 \times 10^{-6}\,\mathrm{ns}^{-1}$
N_{r}	1247 qubits
D_{p}	$0.2\,\mathrm{ps}/\sqrt{\mathrm{km}}$
α_{f}	0.2 dB/km
t_0	$8.5 \times 10^6\,\mathrm{s}$
ω	193.4 THz
λ	1550 nm
f_{rep}	10 MHz
$n_{\mathrm{c}}(0)$	25 %
$n_{\mathrm{d}}(0)$	75 %
η_{D}	10 %
$\widehat{\mathrm{QBER}}$	5 %
τ_{g}	5 ns
α	0.05
d_{r}	0.5

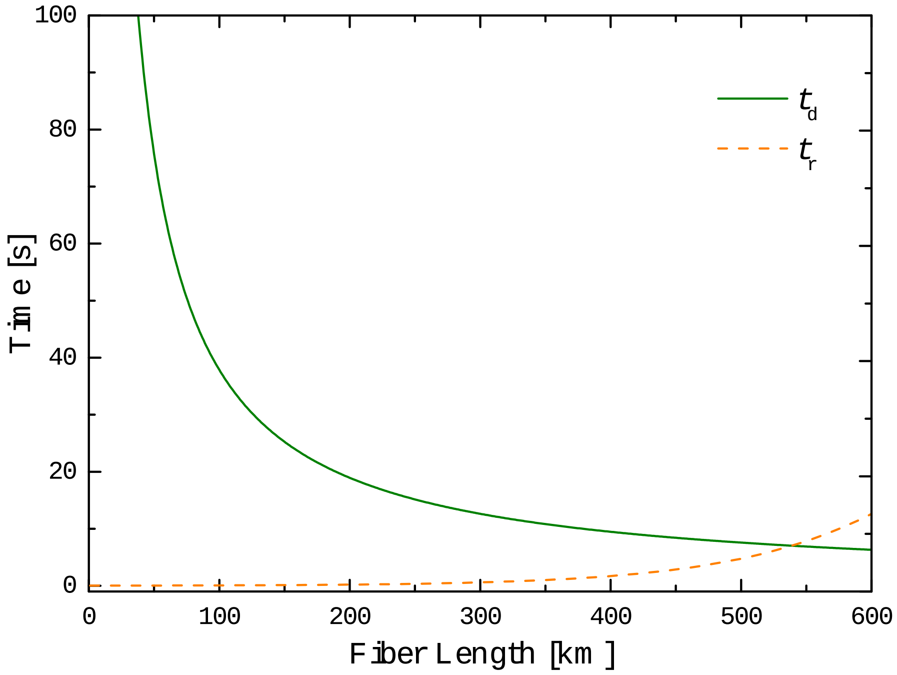

Figure 4.12: Drift time of polarization and time to receive the N_{r} qubits as a function of the fiber length.

The algorithm is based on Bob, which is the master, and has the input parameters shown in Table 4.3. The algorithm runs as follows:

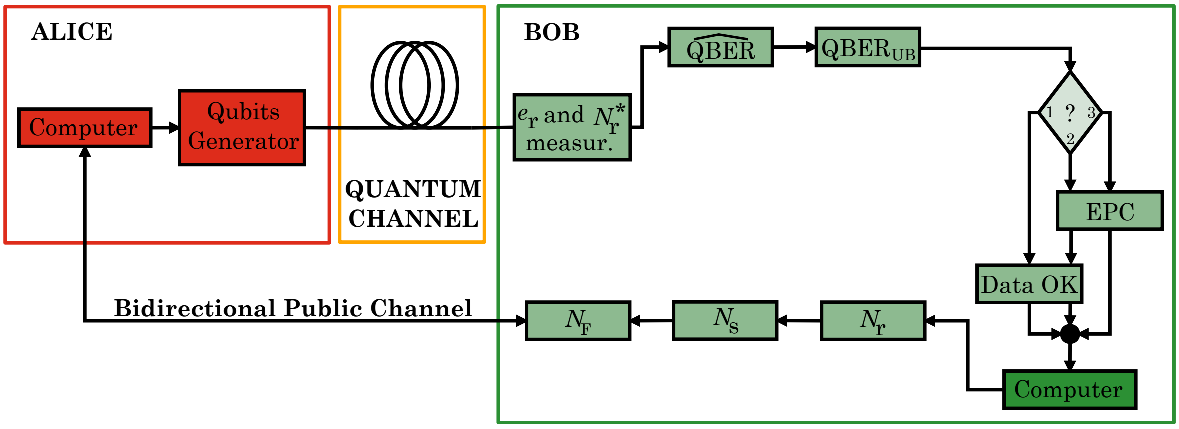

Figure 4.13: Schematic diagram of the polarization control algorithm.

Table 4.3: Input parameters for the polarization control algorithm.

Parameter	Description
QBER_{Min}	Minimum value for que QBER. Below this value the estimation of the QBER is not under the confidence level.
QBER_{Max}	Maximum value for the QBER, which is usually defined by the upper layer quantum protocol.
F_S	Frame size.
N_s^{Max}	Maximum number of control qubits in one frame.
d_r	Relative precision of the $\widehat{\text{QBER}}$.
α	Confidence level in the estimation of the QBER.
$\widehat{\text{QBER}}_{(0)}$	Initial guess for the $\widehat{\text{QBER}}$.
P_{dc}	Probability of having dark counts in the detector.
τ_{g}	Detection time of the detector gate window.
α_{f}	Fiber attenuation coefficient.
L	Fiber length.
η_{D}	Quantum efficiency of the detector.
μ	Average number of photons per pulse.
ΔB	Conditional branch that allows to switch between EPC's wave-plates.

1. The input parameters are inserted in Bob's computer.

2. Bob calculates N_r from Eq. (4.29) in order to estimate the $\widehat{\text{QBER}}$ with a given confidence level, α.

3. Using the value of N_r from Eq. (4.35), Bob calculates the number of qubits that Alice must send, N_s, for him to receive N_r, assuming that $n_c = N_s^{\text{Max}}$.

4. With N_s and N_s^{Max}, Bob calculates the number of frames which are required to send the

control qubits according to

$$N_{\mathrm{F}} = \left\lceil \frac{N_{\mathrm{s}}}{N_{\mathrm{s}}^{\mathrm{Max}}} \right\rceil . \tag{4.37}$$

5. Bob sends the values of F_{S}, $N_{\mathrm{s}}^{\mathrm{Max}}$, N_{s} and N_{F} to Alice through a bidirectional public channel.

6. Alice receives the values sent by Bob, generates the N_{s} qubits and transmits them to Bob through the quantum channel.

7. Bob performs a measurement in the qubits received, which are defined as N_{r}^{*}. At this point there are two cases that must be considered:

   a) If $N_{\mathrm{r}}^{*} < N_{\mathrm{r}}$, it will be obtained a lower precision in the estimation of the $\widehat{\mathrm{QBER}}$. If this happens, it means that the real parameters of the system are slightly different from the ones initially inserted. However, Bob can compensate it by increasing the N_{s} parameter, whenever this occurs in five consecutive times.

   b) If $N_{\mathrm{r}}^{*} > N_{\mathrm{r}}$ in five consecutive times, it means that the system is consuming unnecessary bandwidth with control qubits. In this case, Bob decreases the N_{s} parameter.

8. Using N_{r}^{*} and knowing the control sequence, Bob calculates the error rate from the equation $\widehat{\mathrm{QBER}} = e_{\mathrm{r}}/N_{\mathrm{r}}^{*}$, and then the $\mathrm{QBER}_{\mathrm{UB}}$ from Eq. (4.23).

Next, the algorithm finds a decision stage where $\mathrm{QBER}_{\mathrm{UB}}$ is the input parameter and verifies the following conditions:

1. if $\mathrm{QBER}_{\mathrm{UB}} < \mathrm{QBER}_{\mathrm{Min}}$, there is no action in the EPC and the data qubits received are valid;

2. if $\mathrm{QBER}_{\mathrm{Min}} \leq \mathrm{QBER}_{\mathrm{UB}} \leq \mathrm{QBER}_{\mathrm{Max}}$, the EPC will actuate and the data qubits received are valid,

3. if $\mathrm{QBER}_{\mathrm{UB}} > \mathrm{QBER}_{\mathrm{Max}}$, the EPC will actuate and during this time the data qubits received are discarded.

In order to perform the control of polarization we have used an EPC with four waveplates driven electrically (PolaRITE$^{\mathrm{TM}}$ II/III from General Photonics) [41]. The control of each waveplate is based on a minimization Hill-Climbing algorithm [42] as shown in Fig. 4.14.

The Hill-Climbing algorithm can be used for searching a maximum or minimum in a relatively simple way. In our case, we will use it to find the minimum of the $\widehat{\mathrm{QBER}}$. The algorithm works as follows:

1. The voltage of each waveplate is set at the mean value, $V_{\mathrm{Mean}} = 75\,\mathrm{V}$, to avoid reaching the minimum ($V_{\mathrm{Min}} = 0\,\mathrm{V}$) or maximum ($V_{\mathrm{Max}} = 150\,\mathrm{V}$) values, where the EPC can induce errors in transmission. However, if the limiting voltages are reached it is possible to perform a shift of $\pi/4$, due to the periodical behavior of the waveplates.

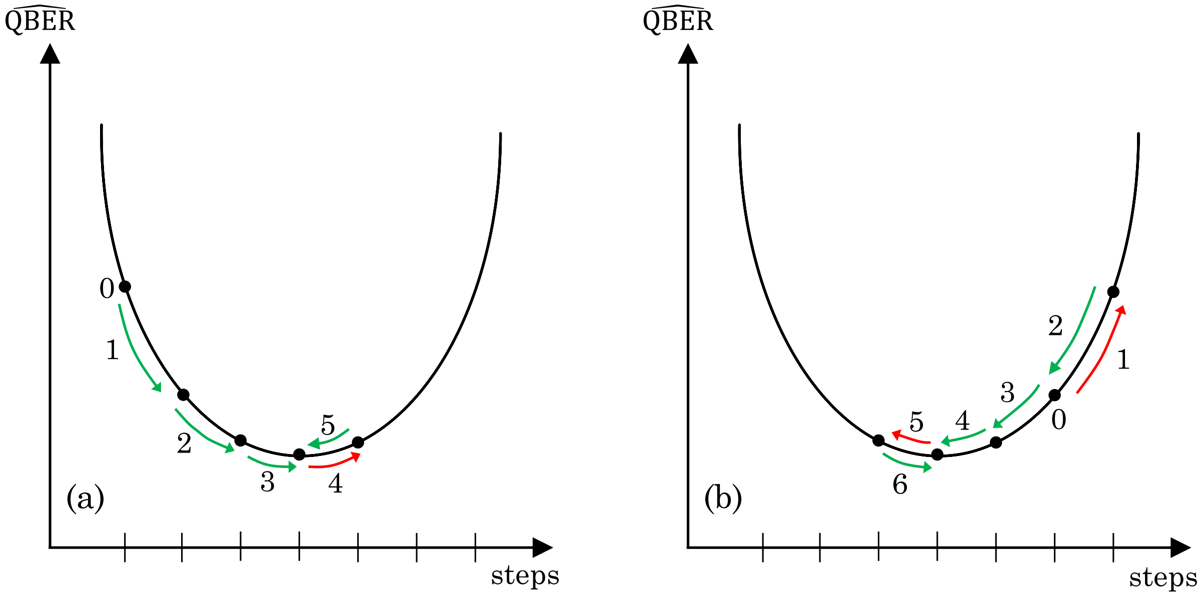

Figure 4.14: Working principle of the Hill-Climbing algorithm. (a) In this example, we assume that the $\widehat{\text{QBER}}$ is at step 0. After moving the waveplate, lower $\widehat{\text{QBER}}$ values are obtained (steps 1 to 3), until in step 4 a higher $\widehat{\text{QBER}}$ is obtained. In this case, the waveplate moves back one step (step 5) in order to get as close as possible to the minimum. (b) In this example, we assume that after the first step the $\widehat{\text{QBER}}$ increases (after increasing the wave plate voltage), which means that the waveplate is moving in the wrong direction. In this case, the voltage is decreased until a minimum value is found (steps 2 to 6.)

2. The voltage of the first waveplate is increased by a given step and the $\widehat{\text{QBER}}$ is estimated. If the $\widehat{\text{QBER}}$ decreases, we continue to increase the waveplate voltage. If the $\widehat{\text{QBER}}$ increases we move back one step.

3. If the variation of the $\widehat{\text{QBER}}$ in the last three iterations is smaller than ΔB, the algorithm jumps to the next waveplate.

In the algorithm, we define two step sizes for the voltage of the waveplates. These are defined by $S_1 = ((\text{QBER}_{\text{Max}} - \text{QBER}_{\text{Min}})/2) + \text{QBER}_{\text{Min}})$ and $S_2 = \text{QBER}_{\text{Max}}$. Based on the two step sizes, there are three cases which are considered:

1. if $\widehat{\text{QBER}} \leq S_1$ we use a step size of $V_{\text{Max}}/100$ in order to slightly optimize the $\widehat{\text{QBER}}$ and do not induce perturbations;

2. if $S_1 < \widehat{\text{QBER}} \leq S_2$ we use a step size of $V_{\text{Max}}/50$ to avoid surpassing the QBER_{Max},

3. if $\widehat{\text{QBER}} > S_2$ we use a step size of $V_{\text{Max}}/10$ to rapidly decrease the error rate.

4.3.4 Numerical Validation

After describing the polarization control algorithm, in this subsection we will show results of a numerical simulation of its implementation, using MATLAB® software. The input parameters for the algorithm are shown in Table 4.4.

Table 4.4: Parameters used to plot Fig. (4.15).

Parameter	Value
μ	0.2 photons/pulse
P_{dc}	$1\times10^{-6}\,\mathrm{ns}^{-1}$
α_{f}	0.2 dB/km
F_{S}	2^{17} bits
f_{rep}	10 MHz
L	100 km
$N_{\mathrm{s}}^{\mathrm{max}}$	25 %
η_{D}	10 %
$\widehat{\mathrm{QBER}}_{(0)}$	50 %
$\mathrm{QBER}_{\mathrm{Max}}$	11 %
$\mathrm{QBER}_{\mathrm{Min}}$	2 %
τ_{g}	5 ns
α	0.05
$\Delta\mathrm{B}$	2 %
d_{r}	0.5

For the complete simulation of the communications scheme, there are four main parts to consider. First, we consider that Alice uses a probabilistic photon source from an attenuated laser, whose photon statistics follows a Poissonian distribution given by Eq. (3.9). Then, we generate two orthogonal SOPs, $|H\rangle$ and $|V\rangle$. The photons are transmitted through the fiber, and their SOPs will suffer random rotations. Such rotations can be modeled in the 3-dimensional Stokes space, following a general rotation matrix given by

$$M_{\mathrm{F}} = \begin{bmatrix} \cos(\theta) & -\sin(\theta)\cos(\phi_0) & \sin(\theta)\sin(\phi_0) \\ \sin(\theta)\cos(\phi) & \cos(\theta)\cos(\phi_0)\cos(\phi)-\sin(\phi_0)\sin(\phi) & -\cos(\theta)\sin(\phi_0)\cos(\phi)-\cos(\phi_0)\sin(\phi) \\ \sin(\theta)\sin(\phi) & \cos(\theta)\cos(\phi_0)\sin(\phi)+\sin(\phi_0)\cos(\phi) & \cos(\phi_0)\cos(\phi)-\cos(\theta)\sin(\phi_0)\sin(\phi) \end{bmatrix}, \tag{4.38}$$

where ϕ, ϕ_0 and θ are three independent random variables [43]. The variables ϕ and ϕ_0 vary uniformly between 0 and 2π whereas $\cos(\theta)$ varies uniformly between -1 and 1.

After the optical fiber, photons pass through the EPC and Bob randomly selects the measurement basis, before photons are detected using SPADs. The matrix representation of the

EPC is given by [44]

$$M_{\mathrm{EPC}} = M_{45^\circ}(\varphi_4) M_{0^\circ}(\varphi_3) M_{45^\circ}(\varphi_2) M_{0^\circ}(\varphi_1), \tag{4.39}$$

where $M(\varphi_{1\ldots4})$ are the waveplate matrices of the EPC in Stokes space and are written as

$$M_{0^\circ}(\varphi_1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\varphi_1) & -\sin(\varphi_1) \\ 0 & \sin(\varphi_1) & \cos(\varphi_1) \end{bmatrix}, \tag{4.40}$$

$$M_{45^\circ}(\varphi_2) = \begin{bmatrix} \cos(\varphi_2) & 0 & \sin(\varphi_2) \\ 0 & 1 & 0 \\ -\sin(\varphi_2) & 0 & \cos(\varphi_2) \end{bmatrix}, \tag{4.41}$$

$$M_{0^\circ}(\varphi_3) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\varphi_3) & -\sin(\varphi_3) \\ 0 & \sin(\varphi_3) & \cos(\varphi_3) \end{bmatrix}, \tag{4.42}$$

and

$$M_{45^\circ}(\varphi_4) = \begin{bmatrix} \cos(\varphi_4) & 0 & \sin(\varphi_4) \\ 0 & 1 & 0 \\ -\sin(\varphi_4) & 0 & \cos(\varphi_4) \end{bmatrix}. \tag{4.43}$$

The full control of a given input SOP, $\hat{s}_{\mathrm{i}}$, can be achieved if the nonlinear equation given by

$$M_{\mathrm{F}} M_{\mathrm{EPC}} = \mathbb{I} \tag{4.44}$$

holds, in a way that the final SOP, $\hat{s}_{\mathrm{f}}$, becomes equal to the input one, according to

$$\hat{s}_{\mathrm{f}} = M_{\mathrm{F}} M_{\mathrm{EPC}} \hat{s}_{\mathrm{i}}. \tag{4.45}$$

Considering an optical fiber with 100 km in length, we have performed a simulation of the evolution of the $\widehat{\mathrm{QBER}}$ with time, which is shown in Fig. 4.15. In the simulation, we have considered that $\widehat{\mathrm{QBER}}_{(0)} = 50\,\%$, since this is the worst case scenario for the error rate. From Fig. 4.15 it is possible to verify that after actuating in the EPC the $\widehat{\mathrm{QBER}}$ soon decreased for values smaller than $\mathrm{QBER}_{\mathrm{Max}}$ and after only about 5 s it decreased below $\mathrm{QBER}_{\mathrm{Min}}$. At about 14 s we introduced a strong perturbation in the system by deliberately increasing the number of errors. This perturbation simulates environmental changes, bending or external pressure in the fiber. However, as can be seen from the result, the algorithm soon reduced the $\widehat{\mathrm{QBER}}$ to the target value. After the control of polarization, the algorithm was also able to keep the $\widehat{\mathrm{QBER}}$ below $\mathrm{QBER}_{\mathrm{Min}}$ for most of the time. From the numerical simulations we were able to conclude that the polarization control method is both effective and robust in real-time control of polarization.

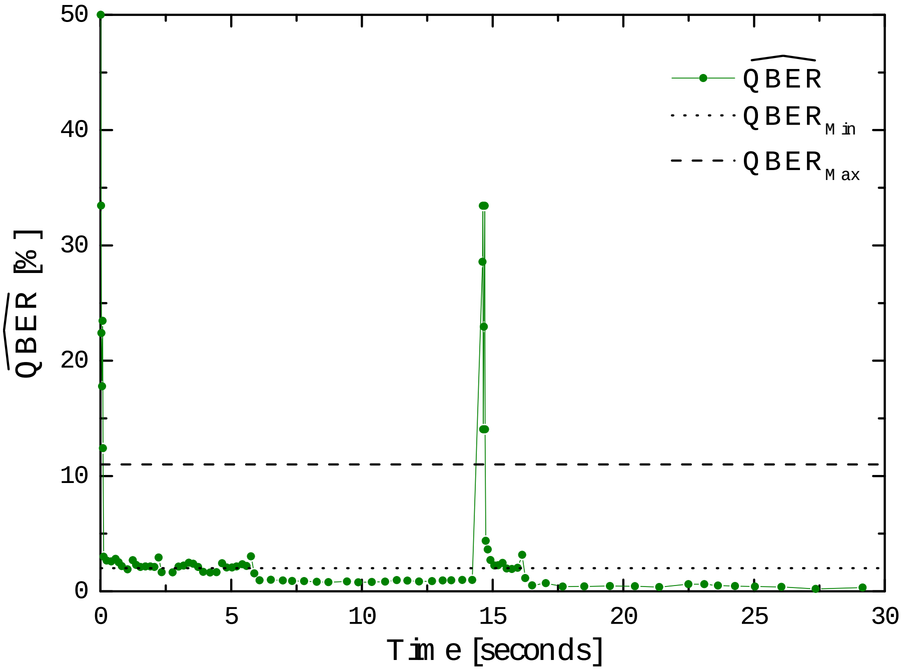

Figure 4.15: Simulation results for the evolution of the $\widehat{\text{QBER}}$ with time after photons are transmitted through a 100 km optical fiber.

4.3.5 Experimental Validation

Finally, we will show results of an experimental validation of the method. First, we describe the experimental setup used in the implementation and then we present and evaluate the experimental results.

Experimental Setup

The scheme of the experimental setup used in a proof-of-principle demonstration of the method is shown in Fig. 4.16. The description of the setup is the following: Alice used a TLS at $\lambda_{\text{p}} = 1550.92$ nm to produce optical signals. Then, the signal passes through a polarization controller (PC-1) and pulses are produced with a MZM. Each pulse has a FWHM of approximately 1 ns and a repetition rate of 100 kHz. The generation of two orthogonal SOPs, $|H\rangle$ and $|V\rangle$, is achieved by using PBS-1, PC-2 and PC-3. The optical switch (OS-1) is connected to a computer which runs an algorithm that randomly generates classical bits, '0' and '1'. When a '0' is transmitted to the switch, the upper arm will be activated and the $|H\rangle$ SOP will be sent. When a '1' is transmitted to the switch, the lower arm will be activated and the $|V\rangle$ SOP will be transmitted. The two polarization controllers, PC-2 and PC-3, are used to align the polarization of the photons with the axes of PBS-1. The average number of photons is then decreased to about 0.2 using a VOA. Alice sends the encoded photons through a 40 km quantum channel and reaches Bob. A HWP was inserted before the optical fiber in order to be possible to introduce a strong perturbation in the polarization of the photons by rotating it by a random angle.

Bob uses an EPC, another polarization-beam splitter (PBS-2) and two detectors, SPAD-1 and SPAD-2. The two detectors are InGaAs/InP avalanche photodiodes operating in a gated Geiger mode. SPAD-1 (id200) has a dark count probability per time gate, $t_\mathrm{g} = 5\,\mathrm{ns}$, of $P_\mathrm{dc}^{(1)} = 4.47 \times 10^{-4}\,\mathrm{ns}^{-1}$ and a quantum detection efficiency, $\eta_\mathrm{D}^{(1)} \approx 10\,\%$. SPAD-2 (id201) has a dark count probability per time gate, $t_\mathrm{g} = 5\,\mathrm{ns}$, of $P_\mathrm{dc}^{(2)} = 2.07 \times 10^{-4}\,\mathrm{ns}^{-1}$ and a quantum detection efficiency $\eta_\mathrm{D}^{(2)} \approx 10\,\%$. To compensate for random rotations of polarization, we have used the algorithm described in Section 4.3.3, implemented in LabView$^\mathrm{TM}$. A second computer is connected to a $\widehat{\mathrm{QBER}}$ estimator (a MC) and to the EPC. The computer runs the algorithm and acts in each squeezer of the EPC, having two possible changes for its voltage, $V_{1\ldots4}\pm$, '+' for increase and '-' for decrease.

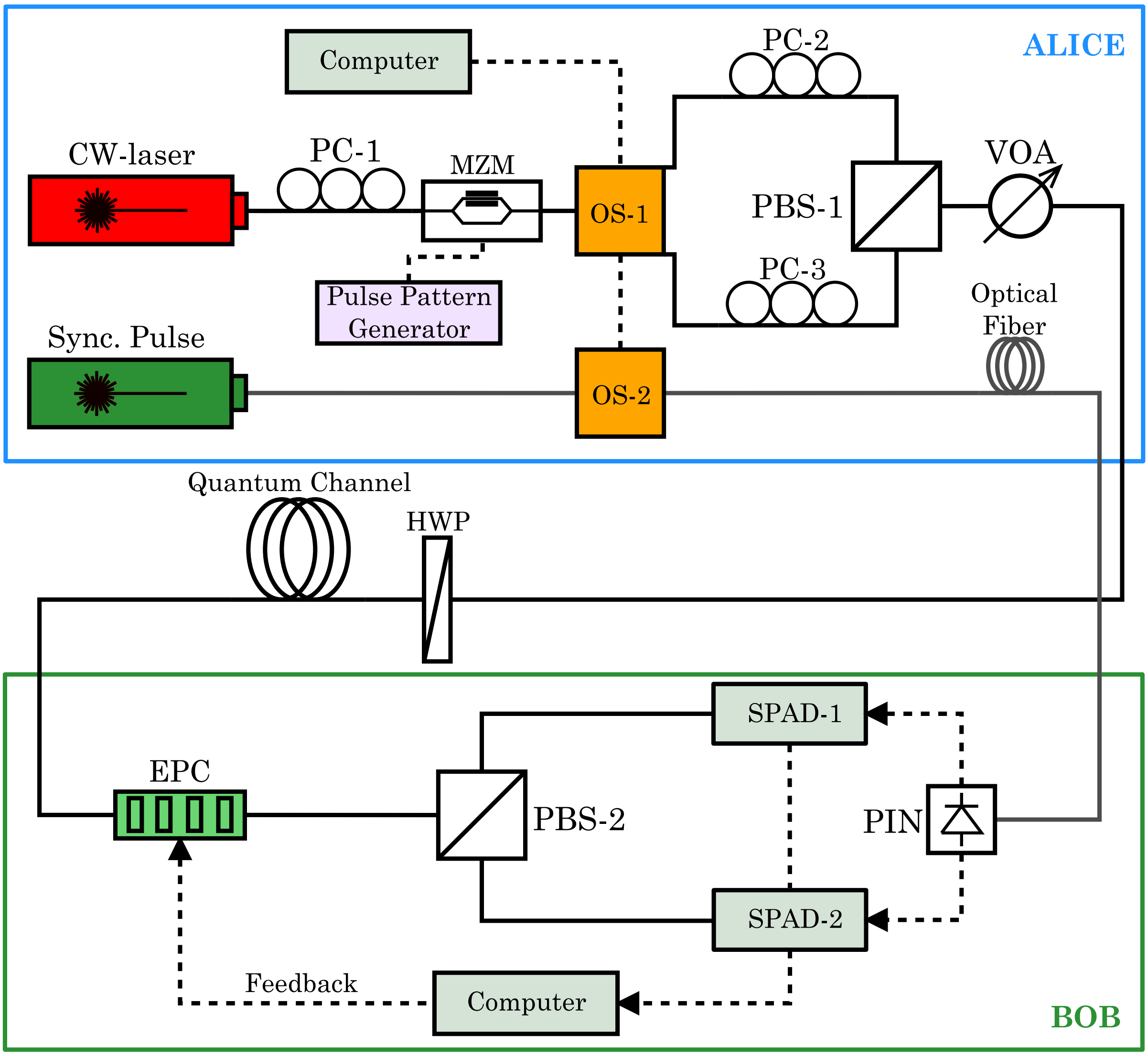

Figure 4.16: Scheme of the experimental setup for the proof-of-principle demonstration of the method. (Solid lines - optical fibers; dashed lines - electrical cables.)

The synchronization between Alice and Bob was achieved using a laser, an optical fiber and a classical detector (PIN), which gave the trigger to the SPADs. The synchronization laser was set at $\lambda_s = 1547.72\,\text{nm}$. The optical fiber was of the same length of the quantum channel in order to allow the synchronization. However, in order to compensate smaller differences it was also possible to make small adjustments in the opening time of the detectors' gate windows. An optical switch (OS-2) working at the same frequency repetition rate of the quantum signal (100 kHz) was also used in the synchronization signal. This way, we guaranteed that the detector opened the gate window only whenever a photon reached it. In this experiment we have chosen to use an additional laser and a fiber to achieve synchronization in order to avoid cross-talk completely.

Experimental Results

Alice generated frames containing 2^{17} bits and sent them to Bob through the quantum channel. Before starting to transmit photons, we have adjusted all PCs in order to achieve the lowest error rate. The system was set to run and after about 30 minutes we rotated the HWP before the fiber in order to introduce a perturbation in photon's polarization. A plot of the evolution of the $\widehat{\text{QBER}}$ with time is shown in Fig. 4.17. Looking at the results in this figure, we can see that the polarization control algorithm was able to keep the $\widehat{\text{QBER}}$ at low values, most of the time way below QBER_{Max}. After applying the external perturbation we verified that

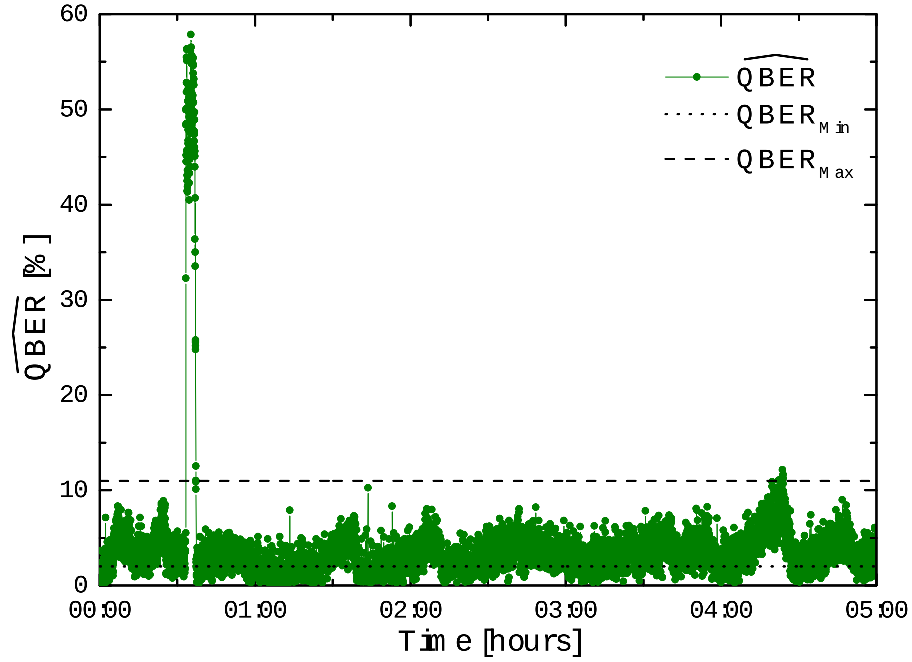

Figure 4.17: Experimental results on the evolution of the $\widehat{\text{QBER}}$ with time, including an external perturbation after about 30 minutes running. The quantum channel used was a 40 km optical fiber. The theoretical limits were defined as $\text{QBER}_{\text{Min}} = 2\,\%$ and $\text{QBER}_{\text{Max}} = 11\,\%$.

the $\widehat{\mathrm{QBER}}$ was increased to about $50\,\%$. However, after about 2 minutes the $\widehat{\mathrm{QBER}}$ decreased to the target value and remained stable for more than 4 hours. The average $\widehat{\mathrm{QBER}}$ during the 5-hours running whenever $\widehat{\mathrm{QBER}} \leq \mathrm{QBER}_{\mathrm{Max}}$ was $3.2\,\%$. Regarding the average number of control qubits sent per frame, we obtained that $N_{\mathrm{s}} = 12.5\,\%$.

The results allowed us to conclude that the polarization control algorithm was indeed effective in the control of polarization and can be used in a long run transmission, even after using a quantum channel with several kilometers in length. Also, it was demonstrated that this method allows uninterrupted transmission of secure data. The recover time is inline with the characteristic time expected when using a low repetition rate, as used in this experiment. One way to improve this time is to increase the repetition rate of the system.

4.3.6 Summary

The QBER of the transmission is highly dependent on the evolution of polarization during propagation through an optical fiber. Moreover, some other effects contribute to the error rate, such as dark counts in detectors or cross-talk counts from auxiliary channels. Apart from proper filtering, a dynamic polarization control scheme should be used to guarantee a constant error rate, or if necessary, to compensate for unexpected changes in the system. From the polarization control scheme presented in this chapter we were able to demonstrate such a control scheme.

Considering that for the accurate estimation of the QBER a certain number of qubits is required, the proposed model allowed us to determine its minimum number. At the same time, the robustness of the polarization control scheme was demonstrated even for the case where long-distance fiber links are used, both numerically and experimentally.

References

[1] R. Ulrich, “Polarization stabilization on single-mode fiber,” *Appl. Phys. Lett.*, vol. 35, no. 11, pp. 840–842, Dec. 1979.

[2] J. N. Damask, *Polarization Optics in Telecommunications*, J. N. Damask, Ed. Springer, 2005.

[3] A. Kumar and A. Ghatak, *Polarization of Light With Applications in Optical Fibers*, 1st ed. SPIE Press, Jan. 2011.

[4] N. J. Muga, A. N. Pinto, M. F. S. Ferreira, and J. R. Ferreira da Rocha, “Uniform polarization scattering with fiber-coil-based polarization controllers,” *J. Lightwave Technol.*, vol. 24, no. 11, pp. 3932–3943, Nov. 2006.

[5] G. Corrielli, A. Crespi, R. Geremia, R. Ramponi, L. Sansoni, A. Santinelli, P. Mataloni, F. Sciarrino, and R. Osellame, “Rotated waveplates in integrated waveguide optics,” *Nat. Commun.*, vol. 5, p. 4249, Jun. 2014.

[6] M. Martinelli, P. Martelli, and S. M. Pietralunga, “Polarization stabilization in optical communications systems,” *J. Lightwave Technol.*, vol. 24, no. 11, pp. 4172–4183, Nov. 2006.

[7] B. Koch, R. Noé, D. Sandel, and V. Mirvoda, “Versatile endless optical polarization controller/tracker/demultiplexer,” *Opt. Express*, vol. 22, no. 7, pp. 8259–8276, Apr. 2014.

[8] K. Kikuchi, “Electronic polarization-division demultiplexing based on digital signal processing in intensity-modulation direct-detection optical communication systems,” *Opt. Express*, vol. 22, no. 2, pp. 1971–1980, Jan. 2014.

[9] A. Hidayat, B. Koch, H. Zhang, V. Mirvoda, M. Lichtinger, D. Sandel, and R. Noé, “High-speed endless optical polarization stabilization using calibrated waveplates and field-programmable gate array-based digital controller,” *Opt. Express*, vol. 16, no. 23, pp. 18 984–18 991, Nov. 2008.

[10] G. B. Xavier, N. Walenta, G. Vilela de Faria, G. P. Temporão, N. Gisin, H. Zbinden, and J. P. von der Weid, “Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation,” *New J. Phys.*, vol. 11, no. 4, p. 045015, Apr. 2009.

[11] A. Muller, J. Breguet, and N. Gisin, “Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km,” *Europhys. Lett.*, vol. 23, no. 6, pp. 383–388, Aug. 1993.

[12] J. Breguet, A. Muller, and N. Gisin, “Quantum cryptography with polarized photons in optical fibres: Experiment and practical limits,” *J. Mod. Opt.*, vol. 41, no. 12, pp. 2405–2412, Dec. 1994.

[13] K. J. Gordon, V. Fernandez, G. S. Buller, I. Rech, S. D. Cova, and P. D. Townsend, “Quantum key distribution system clocked at 2 GHz,” *Opt. Express*, vol. 13, no. 8, pp. 3015–3020, Apr. 2005.

[14] X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. C. Bienfang, D. Su, R. F. Boisvert, C. W. Clark, and C. J. Williams, “Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbit/s,” *Opt. Express*, vol. 14, no. 6, pp. 2062–2070, Mar. 2006.

[15] X. Steve Yao, “Dynamic control of polarization of an optical signal,” U.S. Patent US 6 576 886, 06 10, 2003.

[16] Z. Yuan and A. J. Shields, “Continuous operation of a one-way quantum key distribution system over installed telecom fibre,” *Opt. Express*, vol. 13, no. 2, pp. 660–665, Jan. 2005.

[17] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, “Experimental long-distance decoy-state quantum key distribution based on polarization encoding,” *Phys. Rev. Lett.*, vol. 98, no. 1, p. 010505, Jan. 2007.

[18] J. Chen, G. Wu, Y. Li, E. Wu, and H. Zeng, “Active polarization stabilization in optical fibers suitable for quantum key distribution,” *Opt. Express*, vol. 15, no. 26, pp. 17 928–17 936, Dec. 2007.

[19] G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, “Full polarization control for fiber optical quantum communication systems using polarization encoding,” *Opt. Express*, vol. 16, no. 3, pp. 1867–1873, Feb. 2008.

[20] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, “Stable quantum key distribution with active polarization control based on time-division multiplexing,” *New J. Phys.*, vol. 11, no. 6, p. 065004, Jun. 2009.

[21] N. J. Muga, M. F. S. Ferreira, and A. N. Pinto, “QBER estimation in QKD systems with polarization encoding,” *J. Lightwave Technol.*, vol. 29, no. 3, pp. 355–361, Feb. 2011.

[22] I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, “Proof-of-concept of real-world quantum key distribution with quantum frames,” *New J. Phys.*, vol. 11, no. 9, p. 095001, Sep. 2009.

[23] X. F. Mo, I. Lucio-Martinez, P. Chan, C. Healey, S. Hosier, and W. Tittel, “Time-cost analysis of a quantum key distribution system clocked at 100 MHz,” *Opt. Express*, vol. 19, no. 18, pp. 17 729–17 737, Aug. 2011.

[24] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, “Continuous operation of high bit rate quantum key distribution,” *Appl. Phys. Lett.*, vol. 96, no. 16, p. 161102, Apr. 2010.

[25] H.-F. Zhang, J. Wang, K. Cui, C.-L. Luo, S.-Z. Lin, L. Zhou, H. Liang, T.-Y. Chen, K. Chen, and J.-W. Pan, “A real-time QKD system based on FPGA,” *J. Lightwave Technol.*, vol. 30, no. 20, pp. 3226–3234, Oct. 2012.

[26] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[27] N. A. Silva, Á. J. Almeida, and A. N. Pinto, “Interference in a quantum channel due to classical four-wave mixing in optical fibers,” *IEEE J. Quant. Electron.*, vol. 48, no. 4, pp. 472–479, Apr. 2012.

[28] Á. J. Almeida, N. A. Silva, P. S. André, and A. N. Pinto, "Four-wave mixing: Photon statistics and the impact on a co-propagating quantum signal," *Opt. Commun.*, vol. 285, no. 12, pp. 2956–2960, Jun. 2012.

[29] S. N. Bose, "Plancks gesetz und lichtquantenhypothese," *Z. Phys*, vol. 26, no. 1, pp. 178–181, Dec. 1924.

[30] A. Einstein, "Quantentheorie des einatomigen idealen gases," *Sitzungsber. Preuss. Akad. Wiss. Phys. Math. Kl.*, pp. 261–267, Jul. 1924.

[31] A. Einstein, "Quantentheorie des einatomigen idealen gases (zweite abhandlung)," *Sitzungsber. Preuss. Akad. Wiss. Phys. Math. Kl.*, pp. 3–10, Jan. 1925.

[32] G. Ribordy, N. Gisin, O. Guinnard, D. Stucki, M. Wegmuller, and H. Zbinden, "Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: Current performance," *J. Mod. Opt.*, vol. 51, no. 9-10, pp. 1381–1398, Sep. 2004.

[33] A. Trifonov, D. Subacius, A. Berzanskis, and A. Zavriyev, "Single photon counting at telecom wavelength and quantum key distribution," *J. Mod. Opt.*, vol. 51, no. 9-10, pp. 1399–1415, Sep. 2004.

[34] P. D. Townsend and I. Thompson, "A quantum key distribution channel based on optical fibre," *J. Mod. Opt.*, vol. 41, no. 12, pp. 2425–2433, Dec. 1994.

[35] E. J. Galvez, C. H. Holbrow, M. J. Pysher, J. W. Martin, N. Courtemanche, L. Heilig, and J. Spencer, "Interference with correlated photons: Five quantum mechanics experiments for undergraduates," *Am. J. Phys.*, vol. 73, no. 2, pp. 127–140, Feb. 2005.

[36] A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes, Fourth Edition.* McGraw-Hill Higher Education, 2002.

[37] L. D. Brown, T. T. Cai, and A. DasGupta, "Interval estimation for a binomial proportion," *Stat. Sci.*, vol. 16, no. 2, pp. 101–133, May 2001.

[38] M. Thulin, "Coverage-adjusted confidence intervals for a binomial proportion," *Scand. J. Stat.*, vol. 41, no. 2, pp. 1–10, Jun. 2014.

[39] M. Thulin, "The cost of using exact confidence intervals for a binomial proportion," *Electron. J. Stat.*, vol. 8, no. 1, pp. 817–840, Jun. 2014.

[40] M. Karlsson, J. Brentel, and P. A. Andrekson, "Long-term measurement of PMD and polarization drift in installed fibers," *J. Lightwave Technol.*, vol. 18, no. 7, p. 941, Jul. 2000.

[41] G. P. Corporation, "PCD-M02 – Polarization Controller," http://www.generalphotonics.com/index.php/product/pcd-m02-polarization-controller, Accessed January 4, 2016.

[42] A. Treiber, "A fully automated quantum cryptography system based on entanglement for optical fibre networks," Master's Thesis, University of Vienna, 2009.

[43] Q. Lin and G. P. Agrawal, "Vector theory of stimulated Raman scattering and its application to fiber-based Raman amplifiers," *J. Opt. Soc. Am. B*, vol. 20, no. 8, pp. 1616–1631, Aug. 2003.

[44] E. Collett, *Polarized Light in Fiber Optics.* SPIE Press, 2004.

Chapter 5

Implementation of a Quantum Bit Commitment Protocol

5.1 Introduction

The implementation of quantum protocols is based on the exchange and measurement of quantum signals between two entities [1]. While protocols for quantum key distribution (QKD) allow the two entities to generate and share a secret key, quantum primitives like bit commitment are also very important for information-processing protocols [2].

Quantum bit commitment (QBC) was shown to have much more potential than its classical counterpart [3]. Unfortunately, it was proved that not even the laws of quantum mechanics allow us to build unconditionally secure QBC without considering further assumptions [4, 5]. Pushed by these works, a new classical bit commitment protocol based on cryptographic constraints imposed by special relativity was proposed [6]. This protocol already had the merit of being unconditionally secure against classical or quantum attacks. Later, unconditionally secure QBC protocols using quantum and relativistic properties were proposed and demonstrated experimentally [7–12]. However, despite being unconditionally secure, in practice these protocols are also very difficult to implement. Because of that, QBC protocols whose security is based on current technological limitations have been also proposed. In [13], a practical QBC protocol using four states was presented. This proposal showed the feasibility of the protocol, but the implementation was not secure, since the quantum-bit error rate (QBER) was higher than 20%. Later, a two-state version of the protocol was also presented [14]. These protocols are much easier to implement and at the same time can be considered unconditionally secure, as long as current technological limitations are not solved.

In this chapter, we present an experimental implementation of the QBC protocol proposed in [14, 15]. We have considered two nonorthogonal quantum states encoded in polarization and transmitted through optical fibers. Its security lies in the nonexistence of stable long-term quantum memories and perfect non-demolition measurements, in a foreseeable future.

5.2 The QBC Protocol

5.2.1 What is Bit Commitment?

Bit commitment is a protocol between two untrusted parties, Alice and Bob, which consists of two phases: commitment and opening. In the commitment phase, Alice commits to a value of a bit (‘0’ or ‘1’) at a certain moment in time, without Bob learning the value of the bit. Later, Alice finalizes the protocol by revealing her choice to Bob.

To better understand the functionality of bit commitment protocol we can compare it with that of a safe, as shown in Fig. 5.1. Following this figure, first Bob asks Alice for her to commit to a value of a bit, ‘0’ or ‘1’. Then, she writes her choice on a piece of paper, locks it on a safe and sends the safe to Bob while keeping the key to herself. This is called the commitment phase. In the opening phase, Alice reveals her commitment to Bob. For Bob to know about Alice’s commitment, she simply sends the key to him to open the safe and read the number in the piece of paper.

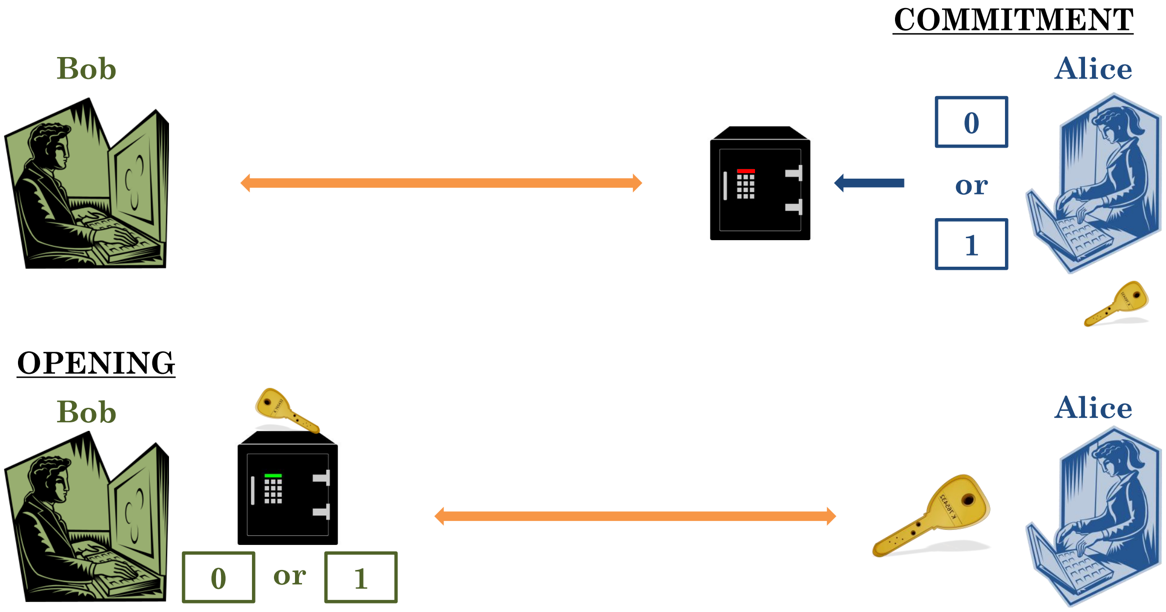

Figure 5.1: Schematic representation of bit commitment protocol.

Bit commitment is an important cryptographic primitive which allows to perform tasks such as secure coin flipping, zero-knowledge proofs or oblivious transfer [14]. In the next subsection we are going to describe our QBC protocol which uses two nonorthogonal states of polarization (SOPs) in the encoding, an optical fiber as quantum channel and two nonorthogonal bases in decoding.

5.2.2 Definition of the Protocol

As we have described in the previous subsection, contrary to QKD in this protocol it is Alice who makes the commitment, while Bob initializes it by preparing the sequence of bits to send (see Fig. 5.1). In order to be feasible, the protocol needs to fulfill three security requirements. Namely, it needs to be:

1. **Binding** - Alice cannot change her commitment later in time, in particular during the opening phase;
2. **Concealing** - Bob cannot learn Alice's commitment before the opening phase,
3. **Viable** - if Alice and Bob are honest, Bob will open Alice's commitment with success.

In this protocol, we use the qubit states $|0\rangle$ and $|1\rangle$ which are nonorthogonal to each other, such that $\langle 0|1\rangle = \cos(\pi/4)$. We denote the states orthogonal to $|0\rangle$ and $|1\rangle$ by $|0^{\perp}\rangle$ and $|1^{\perp}\rangle$, respectively, so that $\langle 0^{\perp}|0\rangle = 0$ and $\langle 1^{\perp}|1\rangle = 0$. This way, we define two orthonormal bases $\mathcal{B}_0 = \{|0\rangle, |0^{\perp}\rangle\}$ and $\mathcal{B}_1 = \{|1\rangle, |1^{\perp}\rangle\}$, which define two orthogonal observables that we call $\hat{C}_0$ and $\hat{C}_1$ and that can be written as

$$\hat{C}_0 = 0 \cdot |0\rangle\langle 0| + 1 \cdot |0^{\perp}\rangle\langle 0^{\perp}|, \tag{5.1a}$$

$$\hat{C}_1 = 1 \cdot |1\rangle\langle 1| + 0 \cdot |1^{\perp}\rangle\langle 1^{\perp}|. \tag{5.1b}$$

For the commitment, Alice uses one of the two observables defined in Eq. (5.1). Since the angle between the two states (which is also the angle between the two bases) is $\pi/4$, the probability to have a mismatch between the state sent and the state measured is 1/2 if the measurement basis differs from the preparation basis [16].

Next, we discuss the factors which contribute to the QBER. The two factors are, namely:

1. **Optical noise** - which represents the effects that change the quantum state of the photon during propagation;
2. **Non-optical noise** - which represents imperfect single-photon sources, finite detector efficiencies and detectors' dark counts.

The optical noise is modeled by a depolarizing channel model [17].

In the protocol we consider four phases, which run as follows:

1. **Initialization:** First, Bob generates a random sequence of classical bits and encodes them in one of two SOPs, $|0\rangle$ or $|1\rangle$. Then, he sends them to Alice and keeps the record of each state.

2. **Commitment:** Right after receiving a photon from Bob, Alice performs a measurement on it (in order to increase security she should announce the arrival times of each photon). She should measure the state of all photons sent by Bob in one of the two observables, $\hat{C}_0$ or $\hat{C}_1$. If Alice wants to commit to '0', she uses $\hat{C}_0$. If she wants to commit to '1', then she uses $\hat{C}_1$ to measure on all photons.

3. **Opening:** In this phase, Alice reveals her commitment to Bob by informing him about the observable she measured and the measurement results that she obtained.

4. **Validation:** Finally, Bob performs a goodness-of-fit test[1] to check if Alice's measurements are statistically coherent or not. Based on this test he will decide on the acceptance of Alice's commitment.

There are several schemes that Bob can use to validate Alice's results. Here, we will consider the so-called binomial test [19], as described next.

a) Let $p_i(j|s)$, with $i, j, s \in \{0, 1\}$, be the conditional probability that Alice obtains the result j when measuring the observable $\hat{C}_i$ on the state $|s\rangle$.

b) Then let $n_i(j|s)$ be the number of results j measured by Alice using observable $\hat{C}_i$ whenever the state $|s\rangle$ was sent, and define

$$q_i(j|s) = \frac{n_i(j|s)}{n_i(s)}. \tag{5.2}$$

c) In this case, the sets $\{q_i(j|0)\}_{i,j\in\{0,1\}}$ and $\{q_i(j|1)\}_{i,j\in\{0,1\}}$ form sets of statistical data.

Now, let's suppose that Alice is committing to '0'. We can define the probability that a binomial distribution with probability of success $p_0(0|0)$ produces the statistics $\{q(i,j|0)\}_{i,j\in\{0,1\}}$, as $P(q_i(j|0)||p_0(0|0))$ and analogously for $P(q_i(j|1)||p_0(1|1))$. For Bob to accept Alice's commitment, he will check if $P(q_i(j|0)||p_0(0|0)) > \kappa$ or if $P(q_i(j|1)||p_0(1|1)) > \kappa$, where κ is a threshold value which will be determined by him. Therefore, for viability purposes, it must be required that if Alice commits to '1', she must be unable to pass the test of committing to '0'. This requirement is satisfied as long as the protocol is secure against a cheating Alice. In Section 5.4 we analyze possible choices of the security parameter κ and show that the protocol is indeed secure against a cheating Alice [14].

5.2.3 White-Noise Model for the Optical Contribution to Noise

In order to analyze the optical contribution to noise, we consider a white-noise model given by a depolarizing channel, $\mathcal{E}_{\mathrm{d}}$, with a given probability, p,

$$\mathcal{E}_{\mathrm{d}}(\hat{\rho}) = (1-p)\hat{\rho} + p\frac{\mathbb{I}}{2}, \tag{5.3}$$

[1] A goodness-of-fit test describes how well a statistical model fits on a set of measurements [18].

where $\hat{\rho}$ is a general mixed state representing the initial qubit state and $\mathbb{I}$ denotes the identity matrix.

When Alice measures $\hat{C}_0$, the conditional probabilities are given by

$$p_0(0|0) = 1 - \frac{p}{2}, \tag{5.4a}$$
$$p_0(1|0) = \frac{p}{2}, \tag{5.4b}$$
$$p_0(0|1) = 1/2, \tag{5.4c}$$
$$p_0(1|1) = 1/2. \tag{5.4d}$$

If Alice measures $\hat{C}_1$, the conditional probabilities are given by

$$p_1(0|0) = 1/2, \tag{5.5a}$$
$$p_1(1|0) = 1/2, \tag{5.5b}$$
$$p_1(0|1) = \frac{p}{2}, \tag{5.5c}$$
$$p_1(1|1) = 1 - \frac{p}{2}. \tag{5.5d}$$

We recall that $n_i(j|s)$, with $i, j, s \in \{0, 1\}$, denotes the number of results j obtained when measuring the observable $\hat{C}_i$ on the state $|s\rangle$. Then, consider that $n_i(s)$ is the total number of photons which were detected when the state $|s\rangle$ was sent and the measurement observable was $\hat{C}_i$. If Alice performs the measurements on all photons using only one of the two observables, the statistics of her measurements will approach to the corresponding conditional probabilities in Eqs. (5.4) and (5.5), due to the law of large numbers. Looking at Eq. (5.4a) we can see that it represents the optical contribution for the success rate (SRATE) and Eq. (5.4b) represents the optical contribution for the QBER, when measuring the observable $\hat{C}_0$ in the state $|0\rangle$ (and analogously for Eqs. (5.5c) and (5.5d)). In this case we say that Alice is honest. Then we can write that

$$\frac{n_0(0|0)}{n_0(0)} \approx p_0(0|0) = 1 - \frac{p}{2} = \mathrm{SRATE}_0^{\mathrm{opt}}, \tag{5.6a}$$
$$\frac{n_0(1|0)}{n_0(0)} \approx p_0(1|0) = \frac{p}{2} = \mathrm{QBER}_0^{\mathrm{opt}}, \tag{5.6b}$$
$$\frac{n_1(0|1)}{n_1(1)} \approx p_1(0|1) = \frac{p}{2} = \mathrm{QBER}_1^{\mathrm{opt}}, \tag{5.6c}$$
$$\frac{n_1(1|1)}{n_1(1)} \approx p_1(1|1) = 1 - \frac{p}{2} = \mathrm{SRATE}_1^{\mathrm{opt}}. \tag{5.6d}$$

If the statistics of Alice's measurements approaches Eq. (5.4), Bob accepts a commitment to '0' and if the statistics approaches Eq. (5.5), Bob accepts a commitment to '1'. Otherwise, Bob will abort the protocol.

5.2.4 Technological Limitations to Guarantee the Protocol's Security

As we have said, the security of this protocol is based on current technological limitations. These limitations are, namely, the nonexistence of stable long-term quantum memories and the incapability of performing ideal quantum non-demolition (QND) measurements. Next, we explain how these limitations are used to guarantee the security of the protocol.

One of the most interesting tasks that a cheating Alice would like to be able to do was the ability to postpone her commitment until the opening phase. However, in order to do that she will need a stable long-term quantum memory to store the qubits received by her and measure them only immediately before the opening phase. Despite recent efforts, such quantum memories are still far from existing [20–22].

The protocol also requires that Alice announces the arrival times of the qubits. However, if Alice wants to cheat and delay the commitment, she must perform a QND measurement to detect the presence of a photon without destroying it or affecting its state. Currently, ideal QND measurements are also impossible to achieve [23–26]. Furthermore, even if Alice was capable of performing a QND measurement, she would need to have access to a stable long-term quantum memory in order to perform her measurements later in time.

There are, however, other aspects that should be accounted for the implementation of the protocol to be considered secure. It is well know that an ideal single-photon source is quite difficult to obtain [1]. Therefore, Bob normally uses probabilistic sources generating a small number of photons in each pulse, in order to prevent the photon-number splitting (PNS) attack [27]. A problem for security occurs if a pulse contains more than one photon, since in that case all of them will be in the same SOP. If this happens, Alice can split two photons and measure $\hat{C}_0$ on one photon and $\hat{C}_1$ on another. In this way, she can have results consistent with both commitments and send only one of the results to Bob at her choice. To avoid this problem, it is expected that the emission rate of multi photons is much smaller than the emission rate of single photons. Finally, we also assume that Bob does not have access to Alice's laboratory, and since she reveals her commitment only during the opening phase, Bob does not get any knowledge about her measurements before that phase.

5.2.5 Optimal Cheating Strategy for Alice

Contrary to QKD, in the proposed QBC protocol the eavesdropper can be Alice herself. Therefore, from the point of view of her measurements, we can also discuss the optimal cheating strategy that she can use for single-photon measurements.

We start by defining the optimal cheating observable, which is the observable whose eigenbasis is rotated by -$\pi/8$ from $\mathcal{B}_0$ [28–31]. Then, the cheating observable, $\hat{C}_{\text{ch}}$, is defined by mutually orthogonal vectors, $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$, such that the angle between $|0\rangle$ and $|\tilde{0}\rangle$, and the angle between $|1\rangle$ and $|\tilde{1}\rangle$ is $\pi/8$ and is written as

$$\hat{C}_{\text{ch}} = 0\cdot|\tilde{0}\rangle\langle\tilde{0}| + 1\cdot|\tilde{1}\rangle\langle\tilde{1}|. \tag{5.7}$$

Therefore, if Alice obtains the result '0', which corresponds to vector $|\tilde{0}\rangle$, she infers that the state sent by Bob was $|0\rangle$. In the same way, if she obtains the result '1', which corresponds to state $|\tilde{1}\rangle$, she infers that the state sent by Bob was $|1\rangle$. We can now define the conditional probabilities for the cheating observable, in the ideal case as

$$p_{\text{ch}}(0|0) = |\langle 0|\tilde{0}\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right), \tag{5.8a}$$

$$p_{\text{ch}}(1|0) = |\langle 0|\tilde{1}\rangle|^2 = \sin^2\left(\frac{\pi}{8}\right), \tag{5.8b}$$

$$p_{\text{ch}}(0|1) = |\langle 1|\tilde{0}\rangle|^2 = \sin^2\left(\frac{\pi}{8}\right), \tag{5.8c}$$

$$p_{\text{ch}}(1|1) = |\langle 1|\tilde{1}\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right). \tag{5.8d}$$

In this particular case, the SRATE is obtained from the probability to infer 0 when the state sent by Bob was $|0\rangle$, and the same for the case when the state sent by Bob was $|1\rangle$. Since the situation is symmetric, the two probabilities are equal.

In terms of probabilities for the optical contribution (opt), $\text{SRATE}_{\text{ch}}^{\text{opt}}$ and $\text{QBER}_{\text{ch}}^{\text{opt}}$ are written as

$$\text{SRATE}_{\text{ch}}^{\text{opt}}(0) = \frac{n_{\text{ch}}(0|0)}{n_{\text{ch}}(0)} \approx p_{\text{ch}}(0|0) = 0.8536, \tag{5.9a}$$

$$\text{QBER}_{\text{ch}}^{\text{opt}}(0) = \frac{n_{\text{ch}}(1|0)}{n_{\text{ch}}(0)} \approx p_{\text{ch}}(1|0) = 0.1464, \tag{5.9b}$$

$$\text{QBER}_{\text{ch}}^{\text{opt}}(1) = \frac{n_{\text{ch}}(0|1)}{n_{\text{ch}}(0)} \approx p_{\text{ch}}(0|1) = 0.1464, \tag{5.9c}$$

$$\text{SRATE}_{\text{ch}}^{\text{opt}}(1) = \frac{n_{\text{ch}}(1|1)}{n_{\text{ch}}(0)} \approx p_{\text{ch}}(1|1) = 0.8536. \tag{5.9d}$$

From Eqs. (5.9b) and (5.9c), we can verify that the maximum error rate allowed by the protocol is around 15%. This tells us that if the error induced by an honest Alice is similar to the error of a cheating Alice, the two strategies are indistinguishable, and the protocol cannot be performed.

5.3 Experimental Implementation of the Protocol

5.3.1 Experimental Setup

The scheme of the experimental setup used to implement the QBC protocol presented is shown in Fig. 5.2.

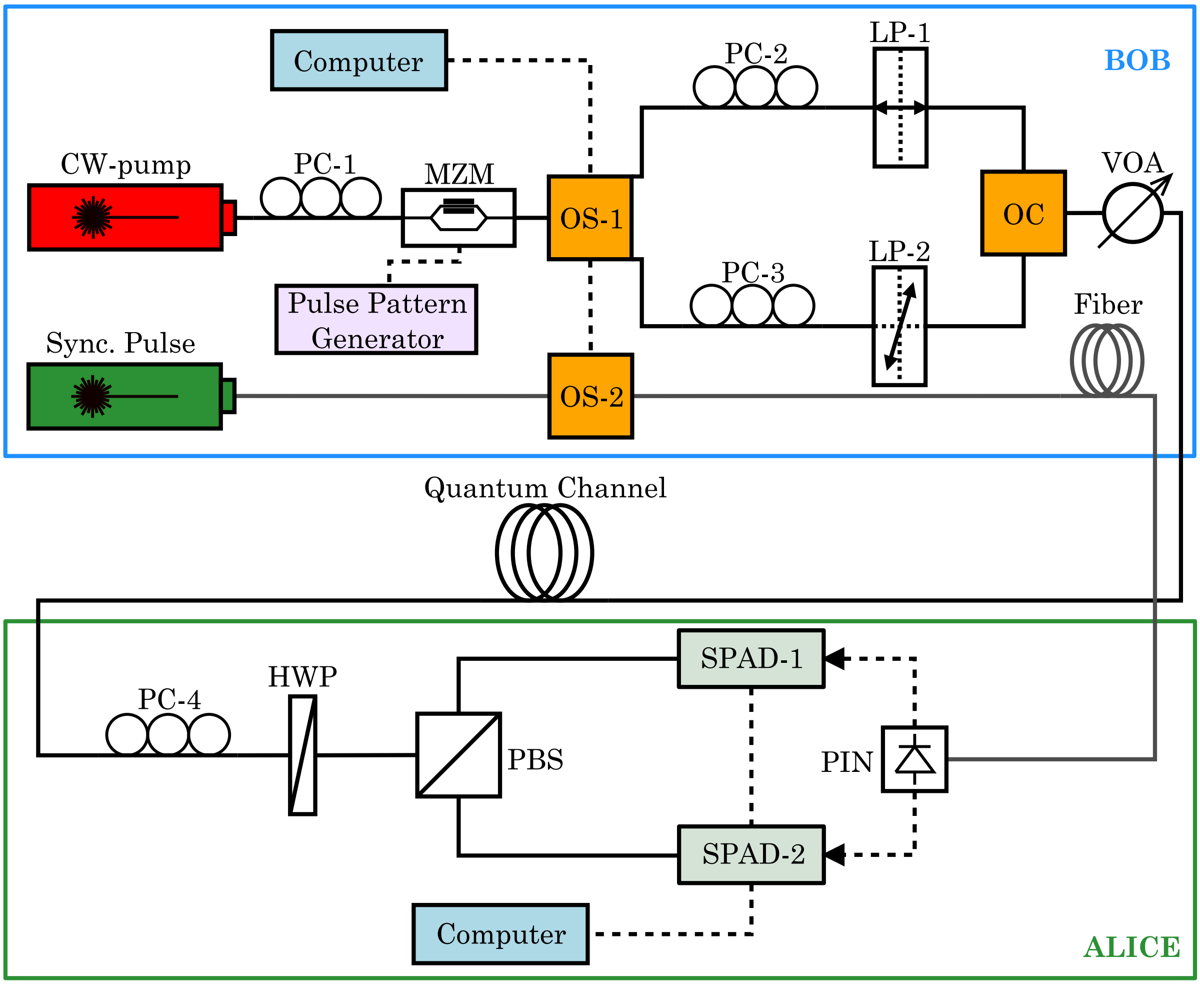

Figure 5.2: Experimental setup used in the proof-of-principle demonstration of the two-state QBC protocol proposed.

The sender, Bob, uses a continuous-wave (CW) pump at $\lambda_p = 1550.92$ nm which is externally modulated with a Mach-Zehnder Modulator (MZM) to produce optical pulses with a full-width at half maximum (FWHM) of approximately 1 ns and a repetition rate of 100 kHz. A polarization controller (PC-1) is used to maximize the number of photons at the output of the

MZM. Then, classical bits are encoded in two nonorthogonal SOPs. In the upper arm, bits are encoded at the $|H\rangle$ SOP through the use of a linear polarizer (LP-1) whose transmission axis is set at 0°. In the lower arm, bits are encoded at the $|{+45}\rangle$ SOP using another linear polarizer (LP-2), this one set at 45°. Using an optical switch (OS-1), if a '0' is received the upper arm is activated, if a '1' is received it is the lower arm which is activated. Then, both pass through a 50/50 optical coupler (OC). After the encoding part, pulses are attenuated with a variable optical attenuator (VOA) to generate 0.2 photons per pulse, in average. Then, photons are transmitted through the quantum channel (an optical fiber). The receiver, Alice, uses a half-wave plate (HWP) to select the commitment basis. The wave plate is set at $2\theta = 0°$, for selecting the rectilinear basis ($\hat{C}_0$), $2\theta = 45°$ to select the diagonal basis ($\hat{C}_1$), or $2\theta = -22.5°$ to choose the optimal cheating basis ($\hat{C}_{\text{ch}}$). A polarization-beam splitter (PBS) allows to discriminate between 0° and 90°. The polarization controller (PC-4) before the HWP is used to compensate random rotations of polarization in the optical fiber. The detection of photons is performed with two single-photon avalanche diodes (SPAD-1 and SPAD-2). SPAD-1 (id200) has a dark count probability per time gate, $t_{\text{g}} = 5$ ns, of $P_{\text{dc}}^{(1)} = 6 \times 10^{-5}\,\text{ns}^{-1}$, and a quantum detection efficiency, $\eta_{\text{D}}^{(1)} \approx 7\%$. SPAD-2 (id201) has a dark count probability per time gate, $t_{\text{g}} = 5$ ns, of $P_{\text{dc}}^{(2)} = 3\times10^{-5}\,\text{ns}^{-1}$, and a quantum detection efficiency, $\eta_{\text{D}}^{(2)} \approx 9\%$. The synchronization between Alice and Bob is achieved by using another laser ($\lambda_{\text{s}} = 1547.72$ nm) set at the same repetition rate of the quantum signal and an optical fiber also with the same length of the quantum channel. Another optical switch (OS-2) guarantees that the classical signal is sent to Alice only when the qubit is also sent. These pulses are detected using a classical detector (PIN), which gives trigger to both SPADs. As in previous experiment, we have used an additional laser and fiber to avoid cross-talk counts completely.

5.3.2 Experimental Results

Alice Measuring $\hat{C}_0$ and $\hat{C}_1$

To demonstrate the implementation of the proposed QBC protocol, we have performed measurements of both $\hat{C}_0$ and $\hat{C}_1$, using different quantum channel lengths. We considered two types of measurements for each observable. When the basis of Alice's measurement observable $\hat{C}_i$ (with $i \in \{0, 1\}$) coincides with the basis $\mathcal{B}_s$ (with $s \in \{0, 1\}$) from which the state was prepared by Bob, we call this a 'measurement in equal bases'. When they are different, we call it a 'measurement in different bases'.

The sequence of bits to encode was obtained from a pseudo-random binary sequence (PRBS) with size 2^{17}. In a single run, we have sent the full sequence of bits and recorded the results from the ones who have reached the detectors. For the quantum channel, we have considered three different fiber lengths: 0 km, 8 km and 16 km.

In Fig. 5.3, we show the measurement results for both $\hat{C}_0$ and $\hat{C}_1$ in five different runs.

Looking at the experimental data in this figure, we can see that the measurement probability

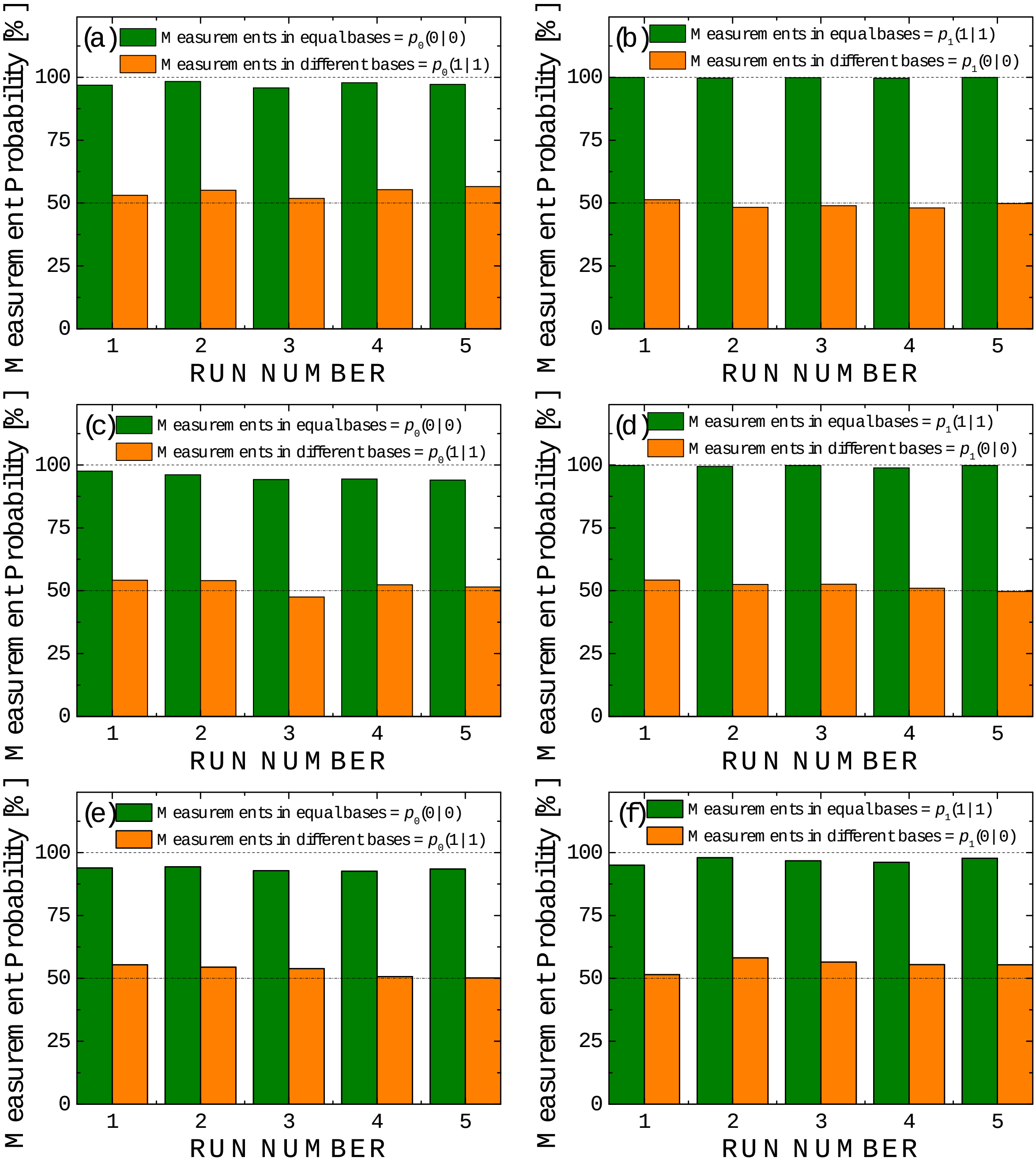

Figure 5.3: Experimental results of the measurement probability for five different runs obtained when Alice committed to $\hat{C}_0$ and $\hat{C}_1$. Figures (a) and (b) show the results for 0 km, figures (c) and (d) present the results for 8 km and figures (e) and (f) present results for 16 km. The dashed lines represent the theoretical value for measurements in equal bases (100%) and the dash-dotted line represents the theoretical value for measurement in different bases (50%).

when equal bases were used is always higher than 93%. Therefore, these results are way above the minimum theoretical security limit of 85.36%. The measurement probability when different bases were used is always close to 50%. This was the expected result, since there is a probability of 50% to detect a photon in each detector. In Table 5.1, we present the success rates for $\hat{C}_0$ and $\hat{C}_1$, obtained from the results in Fig. 5.3. From this table, we can verify that as larger the fiber length, smaller is the success rate when measuring in equal bases. This is due to the fact that with the increase on the fiber length it is more difficult to adjust polarization and therefore the system is more susceptible to errors.

Table 5.1: Success rates for $\hat{C}_0$ and $\hat{C}_1$ when measuring in equal and in different bases.

	SRATE when measuring in equal bases (%)		**SRATE when measuring in different bases (%)**	
Fiber Length (km)	$\hat{C}_0$	$\hat{C}_1$	$\hat{C}_0$	$\hat{C}_1$
0	97.18	99.81	54.37	49.30
8	95.25	99.54	51.92	51.99
16	93.43	96.73	52.91	55.41

The SRATEs and the QBERs are a consequence of both optical and non-optical noise. Therefore, we can write that

$$\mathrm{SRATE}_i = \mathrm{SRATE}_i^{\mathrm{opt}} + \mathrm{SRATE}_i^{\mathrm{non-opt}}, \tag{5.10a}$$

$$\mathrm{QBER}_i = \mathrm{QBER}_i^{\mathrm{opt}} + \mathrm{QBER}_i^{\mathrm{non-opt}}, \tag{5.10b}$$

with $i = 0$, 1. The optical noise is given by Eqs. (5.4) and (5.5), having a significant impact on the results. On the other hand, the non-optical noise does not depend on the state emitted by Bob nor on the observable measured by Alice, but it does depends on the result obtained. The non-optical QBER can be written as

$$\mathrm{QBER}_i^{\mathrm{non-opt}} = \frac{P_{\mathrm{dc}}^{(j)}}{\mu\eta_{\mathrm{F}}\eta_{\mathrm{D}}^{(j)}}, \tag{5.11}$$

with $i = 0$, 1 and $j = 1$, 2.. In Eq. (5.11), $P_{\mathrm{dc}}^{(j)}$ is the probability to have dark counts in each detector, μ is the average number of photons per pulse and $\eta_{\mathrm{D}}^{(j)}$ is the quantum efficiency of each detector. The term η_{F} represents the total efficiency of the fiber and is given by Eq. (4.6). From Eqs. (5.4), (5.5) and (5.11), Eq. (5.10b) can be rewritten as

$$\mathrm{QBER}_i = \frac{p_i}{2} + \frac{P_{\mathrm{dc}}^{(j)}}{\mu\eta_{\mathrm{F}}\eta_{\mathrm{D}}^{(j)}}, \tag{5.12}$$

including both optical and non-optical contributions.

In addition to Fig. 5.3, we can plot the average QBER over the five runs for each fiber length. The results are shown in Fig. 5.4. The theoretical fit to the results was obtained from

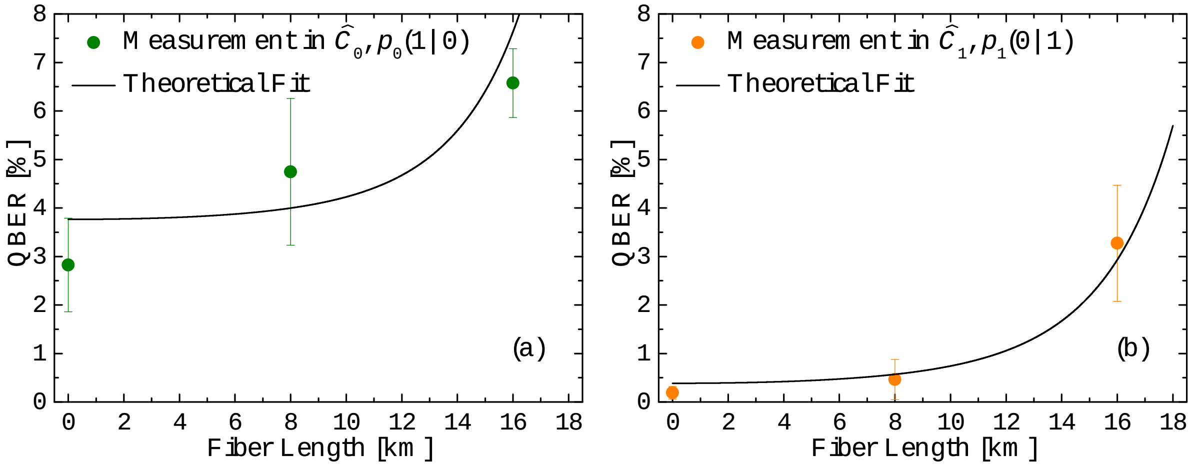

Figure 5.4: Average QBER as a function of the fiber length when measuring (a) $\hat{C}_0$ (QBER$_0$) and (b) $\hat{C}_1$ (QBER$_1$), along with the theoretical fit from Eq. (5.12). The error bars represent the standard deviation of the experimental values.

Eq. (5.12), considering p_i as the fitting parameter. From the fit we obtained that $p_0 = 6.3\times10^{-2}$ and $p_1 = 3.7\times10^{-3}$. The correlation coefficient between experimental and theoretical data was $R^2 = 0.7827$ when $\hat{C}_0$ was measured and $R^2 = 0.9587$ when $\hat{C}_1$ was measured. From the results in Fig. 5.4, the first conclusion that we can take is that the QBER increases with the fiber length, as expected. It is also possible to see that the experimental results are within the theoretical security limit for the QBER, which is about 15%. The difference between the QBER values in the measurements with $\hat{C}_0$ and $\hat{C}_1$ is due to several factors. First, the dark count probabilities are different in the two detectors, since $P_{\text{dc}}^{(1)} = 6\times10^{-5}\,\text{ns}^{-1}$ for SPAD-1 and $P_{\text{dc}}^{(2)} = 3\times10^{-5}\,\text{ns}^{-1}$ for SPAD-2. Then, the quantum efficiencies of the two detectors are also different, with $\eta_{\text{D}}^{(1)} \approx 7\%$ for SPAD-1 and $\eta_{\text{D}}^{(2)} \approx 9\%$ for SPAD-2. Finally, we note that the losses in each arm of the PBS were also slightly different.

Next, we can calculate the probability of occurrence of white noise, p_i. This can be obtained from Eq. (5.12), which can be rewritten as

$$p_i = 2\left(\text{QBER}_i - \frac{P_{\text{dc}}^{(j)}}{\mu\eta_{\text{F}}\eta_{\text{D}}^{(j)}}\right). \tag{5.13}$$

Using Eq. (5.13) and the experimental results from Fig. 5.4, where QBER$_i$ is the average value of the five runs for each fiber length, we plot p_i in Fig. 5.5.

As also shown in Fig. 5.4, Fig. 5.5 indicates that in the measurement of $\hat{C}_0$ the noise is higher and increases with the fiber length, due to the same reasons presented in the analysis of Fig. 5.4.

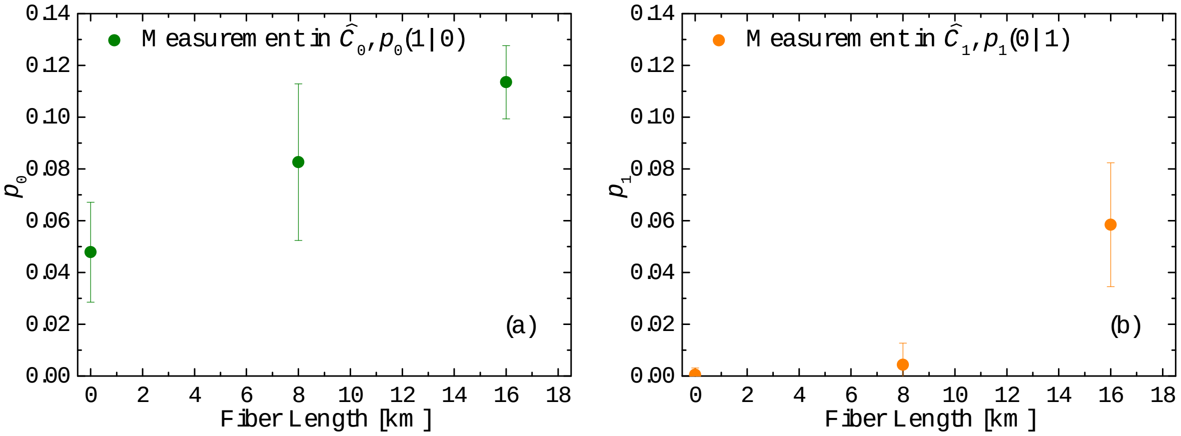

Figure 5.5: Calculated values for (a) p_0 and (b) p_1 as a function of L, using Eq. (5.13). The error bars represent the standard deviation of the experimental data.

Alice Measuring $\hat{C}_{\text{ch}}$

In order to verify the optimal cheating strategy for Alice, instead of $\hat{C}_0$ or $\hat{C}_1$ we performed measurements of $\hat{C}_{\text{ch}}$. The results are shown in Fig. 5.6. From these results we can verify that there is a good agreement between experimental and theoretically expected data. The average success rates for the measurement probability of the optimal cheating strategy are summarized in Table 5.2.

Table 5.2: Average success rates for the optimal cheating strategy when measuring zeros and ones.

Fiber Length (km)	**SRATE when measuring zeros (%)**	**SRATE when measuring ones (%)**
0	83.12	81.11
8	82.50	75.74
16	80.01	73.83

As we have done for measurements with $\hat{C}_0$ and $\hat{C}_1$, we can plot the average QBER over the five runs for each fiber length, when measuring $\hat{C}_{\text{ch}}$. The results are shown in Fig. 5.7. From the theoretical fit we obtained that $p_0 = 0.4$ and $p_1 = 0.344$. The correlation coefficient between experimental and theoretical data is $R^2 = 0.5305$ when measuring ones in $\hat{C}_{\text{ch}}$ and $R^2 = 0.8267$ when zeros were measured in $\hat{C}_{\text{ch}}$.

Using Eq. (5.13) and the experimental results from Fig. 5.7 we plotted the variation of p_{ch} with the fiber length, which is shown in Fig. 5.8. As shown in Fig. 5.5, from these results we can also verify that the noise increases with the fiber length, presenting larger values, since the QBER for the cheating strategy is also larger.

One of the conclusions from the experiment to test the optimal cheating strategy for Alice

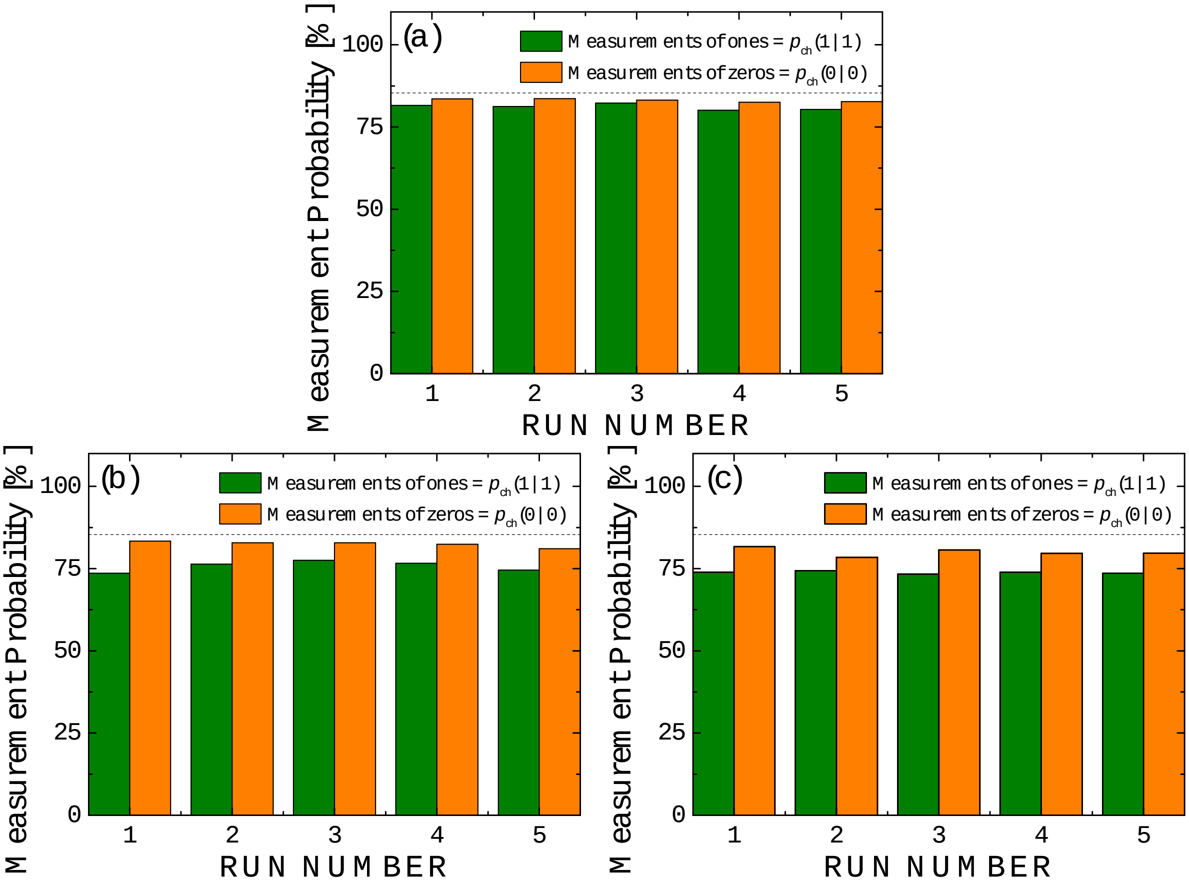

Figure 5.6: Experimental results of the measurement probability for five different runs obtained from the measurements in $\hat{C}_{\text{ch}}$, when (a) $L = 0\,\text{km}$, (b) $L = 8\,\text{km}$ and (c) $L = 16\,\text{km}$. The dashed line represents the theoretical value for measurements of both zeros and ones, which is at 85.36%.

is that the QBER is slightly larger than the theoretical value. This is due to the difficulty to set the HWP at exactly $2\theta = -22.5°$ and due to the unavoidable optical noise. A difference between measurements of ones and zeros is also observed in the average QBERs. This is also due to different dark-count probabilities, different quantum efficiencies in the two detectors and different fiber losses in each arm of the PBS. It is worth to highlight that errors due to bad alignment also exist when measuring $\hat{C}_0$ and $\hat{C}_1$. However, since it is easier to align the linear polarizers for those two measurements, we can assume that when measuring $\hat{C}_0$ and $\hat{C}_1$ this type of error is negligible.

5.4 Security Against a Cheating Alice

In this subsection we analyse the security of the protocol against a cheating Alice. The first thing to do is to use the experimental results of Alice's measurements in observables $\hat{C}_0$ and $\hat{C}_1$ to establish Bob's quantitative validity criterion. Then, we use the experimental results obtained

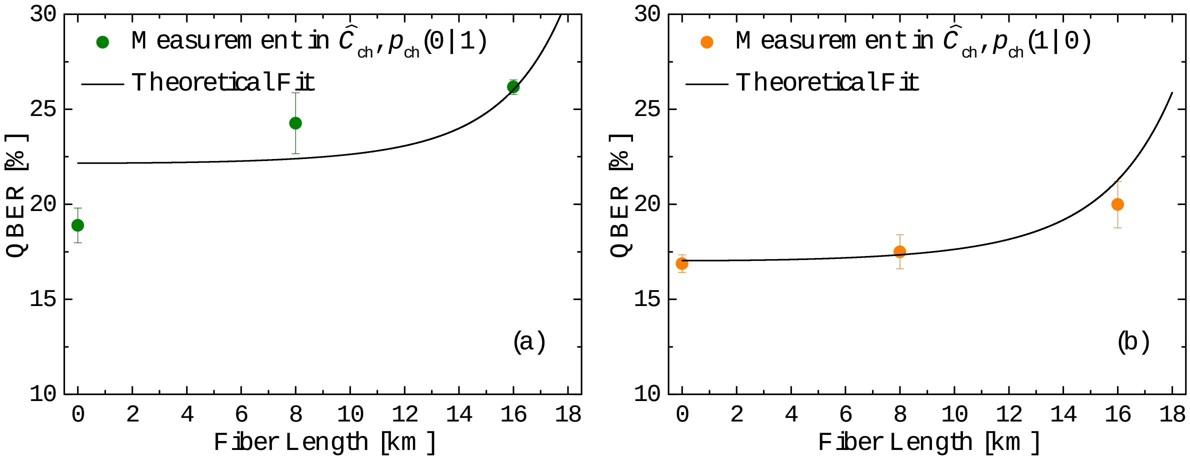

Figure 5.7: Average QBER as a function of the fiber length when measuring (a) ones in $\hat{C}_{\text{ch}}$ and (b) zeros in $\hat{C}_{\text{ch}}$. The theoretical fit from Eq. (5.12) is also shown. The error bars represent the standard deviation of the experimental values.

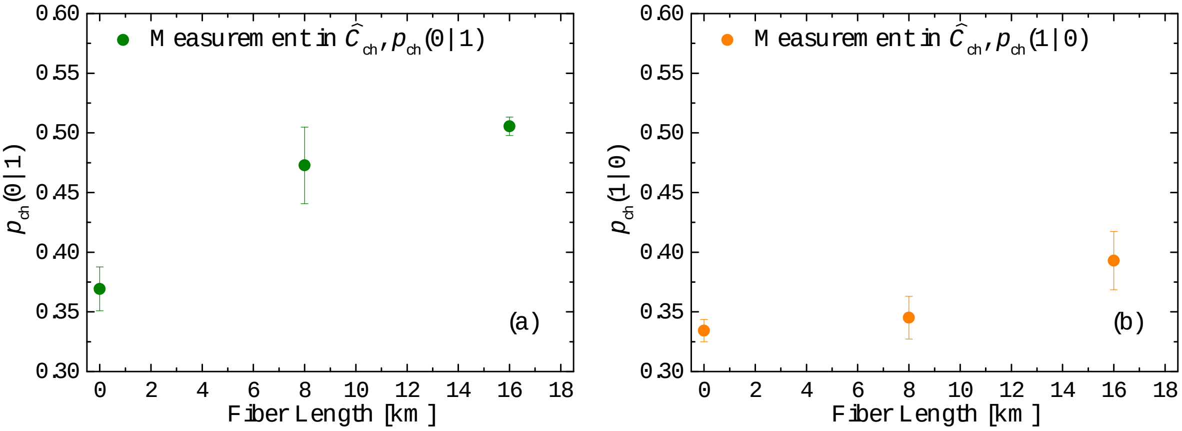

Figure 5.8: Calculated values for (a) $p_{\text{ch}}(0|1)$ and (b) $p_{\text{ch}}(1|0)$ as a function of L, using Eq. (5.13). The error bars represent the standard deviation of the experimental values.

from a cheating Alice and show that they would not pass such criterion, which demonstrates the security of the protocol.

First, we describe the way Bob forms the viability criterion introduced in the definition of the protocol. The probability that an honest Alice committing to $\hat{C}_0$ obtains $n_0(0|0)$ times the value '0' when measuring $n_0(0)$ photons in state $|0\rangle$ is given by a binomial distribution with mean value

$$\mu_0 = n_0(0)p_0(0|0), \tag{5.14}$$

and variance

$$\sigma_0^2 = n_0(0)p_0(0|0)(1 - p_0(0|0)). \tag{5.15}$$

The probability that an honest Alice committing to $\hat{C}_0$ obtains $n_0(1|1)$ times the value '1' when measuring $n_0(1)$ photons in state $|1\rangle$ is given by a binomial distribution with mean value

$$\mu_1 = n_0(1)p_0(1|1), \tag{5.16}$$

and variance

$$\sigma_1^2 = n_0(1)p_0(1|1)(1 - p_0(1|1)). \tag{5.17}$$

For a sufficiently large $n_0(0)$ and $n_0(1)$, this binomial distribution will behave like a normal distribution when considering the same parameters. Then, the binomial test described before reduces to the $68 - 95 - 99.7$ rule for significance levels of 32%, 5% and 0.3%, respectively. If we consider a significance level of 0.3%, it means that Bob accepts Alice's statistics whenever $|0\rangle$ was sent if

$$n_0(0|0) \in [\mu_0 - 3\sigma_0, \mu_0 + 3\sigma_0]. \tag{5.18}$$

The Eq. (5.18) ensures that if an honest Alice wants to commit to '0' she has approximately 99.7% chance of having part of her data accepted by Bob. In terms of the security parameter, κ, introduced in Section 5.2.2, this corresponds to the calculation of

$$\kappa = \Pr[n_0(0|0) = \mu_0 - 3\sigma_0], \tag{5.19}$$

where Pr is the probability. Immediately afterwards, Bob tests the statistics of Alice's measurements when $|1\rangle$ was sent and accepts them if

$$n_0(1|1) \in [\mu_1 - 3\sigma_1, \mu_1 + 3\sigma_1], \tag{5.20}$$

which in terms of the security parameter corresponds to the calculation of

$$\kappa = \Pr[n_0(1|1) = \mu_1 - 3\sigma_1]. \tag{5.21}$$

At last, Bob validates Alice's full commitment only if the conditions in Eqs. (5.18) and (5.20) are satisfied. For a significance level of 0.3%, this means that Bob will not accept the commitment from an honest Alice in only about 6 times at each 1000.

From the results in Fig. 5.3 we can calculate the conditional probabilities in Eq. (5.4), which are

$$p_0(0|0) = 0.934, \tag{5.22a}$$

$$p_0(1|0) = 0.066, \tag{5.22b}$$

$$p_0(0|1) = 0.471, \tag{5.22c}$$

$$p_0(1|1) = 0.529. \tag{5.22d}$$

Since in the case of Fig. 5.3 Bob registered about $n_0(0) \approx n_0(1) \approx 350$ measurement outcomes on average, we can calculate from Eqs. (5.14) and (5.15) that

$$\mu_0 = 326.9, \tag{5.23a}$$

$$\sigma_0 = 4.64, \tag{5.23b}$$

$$\mu_1 = 185.15, \tag{5.23c}$$

$$\sigma_1 = 9.34. \tag{5.23d}$$

Therefore, the condition in Eq. (5.18) gives $[\mu_0 - 3\sigma_0, \mu_0 + 3\sigma_0] = [312.98, 340.82]$ and the condition in Eq. (5.20) gives $[\mu_1 - 3\sigma_1, \mu_1 + 3\sigma_1] = [157.13, 213.17]$.

Next, we calculate the probability of a cheating Alice to pass the previous test. From the results shown in Fig. 5.6 we are able to calculate the conditional probabilities, which are

$$p_{\text{ch}}(0|0) = 0.8, \tag{5.24a}$$

$$p_{\text{ch}}(1|0) = 0.2, \tag{5.24b}$$

$$p_{\text{ch}}(0|1) = 0.262, \tag{5.24c}$$

$$p_{\text{ch}}(1|1) = 0.738. \tag{5.24d}$$

Using Eq. (5.14), we obtain that $n_0(0)p_{\text{ch}}(0|0) = 280$. Since $280 \notin [312.98, 340.82]$, the statistics from a cheating Alice would not be accepted by Bob as a valid commitment to '0'. In the same way, using Eq. (5.16) we obtain that $n_0(1)p_{\text{ch}}(1|1) = 258.3$. Since $258.3 \notin [157.13.98, 213.17]$, the statistics from a cheating Alice would also not be accepted by Bob as a valid commitment to '1'. Note that even if we had chosen $[\mu_0 - 7\sigma_0, \mu_0 + 7\sigma_0]$ and $[\mu_1 - 7\sigma_1, \mu_1 + 7\sigma_1]$ as the acceptance intervals, to increase the chance of an honest Alice being rightfully accepted, a cheating Alice would, on average, still fail to pass that test. This comes from the fact that substituting the respective values we obtain $[\mu_0 - 7\sigma_0, \mu_0 + 7\sigma_0] = [294.42, 359.38]$ and $[\mu_1 - 7\sigma_1, \mu_1 + 7\sigma_1] = [119.77, 250.53]$, which allows to conclude that they still exclude the statistics from a cheating Alice. Note that by using such a larger standard deviation we also increase the chance of an honest Alice to be accepted.

We note that even if Alice had ideal detectors, with 100% efficiency and no dark counts, that would not help her cheating. The reason for this is that ideal detectors will only improve the results of $\hat{C}_0$ and $\hat{C}_1$ used to establish Bob's numerical verification criterion, reducing them to the case of optical noise only, given by Eqs. (5.4) and (5.5). In other words, this means that Bob's verification criterion would be tighter than if non-ideal detectors were used. However, while ideal detectors improve the probability for Alice to cheat, that will not be enough to compromise the security of the protocol. By assuming the "noisy" verification criterion given by Eq. (5.18), for the experimental values given by Eqs. (5.22) and (5.23) and perfect cheating statistics given by Eq. (5.8), the significance level for the protocol's security is still of the order of 10^{-8}, corresponding to a 6σ security criterion.

From this demonstration, we are able to conclude that if the protocol is secure against a cheating Alice, then it is also viable. This means that if Alice is honest and is trying to commit to ‘0’, she can never pass the test of committing to ‘1’.

5.5 Summary

In this chapter, we presented a QBC protocol based on two nonorthogonal SOPs sent through optical fibers. Classical bits were encoded in photon’s polarization and transmitted through different fiber lengths. Results were presented for Alice committing both to ‘0’ and to ‘1’ and compared with theoretically expected results, showing good agreement. We also presented results for the optimal cheating strategy for Alice and demonstrated a validity criterion for Bob to accept or reject Alice’s commitment.

The implementation of this QBC protocol assumed some technological limitations, which means that it is not unconditionally secure. However, there are still two good reasons for implementing this protocol. The first one is that stable long-term quantum memories and ideal non-demolition measurements are not going to be feasible in a foreseeable future. The second reason is supported by the fact that this protocol is much easier to implement in a real-world scenario than relativistic QBC protocols.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Jul. 2009.

[2] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, pp. 1–32, 2015.

[3] E. Hänggi and J. Wullschleger, "Tight bounds for classical and quantum coin flipping," in *Theory of Cryptography*, ser. Lecture Notes in Computer Science, Y. Ishai, Ed. Springer Berlin Heidelberg, Mar. 2011, vol. 6597, pp. 468–485.

[4] H.-K. Lo and H. F. Chau, "Is quantum bit commitment really possible?" *Phys. Rev. Lett.*, vol. 78, no. 17, pp. 3410–3413, Apr. 1997.

[5] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Phys. Rev. Lett.*, vol. 78, no. 17, pp. 3414–3417, Apr. 1997.

[6] A. Kent, "Unconditionally secure bit commitment," *Phys. Rev. Lett.*, vol. 83, no. 7, pp. 1447–1450, Aug. 1999.

[7] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," *Phys. Rev. Lett.*, vol. 109, no. 13, p. 130501, Sep. 2012.

[8] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, "Experimental bit commitment based on quantum communication and special relativity," *Phys. Rev. Lett.*, vol. 111, no. 18, p. 180504, Nov. 2013.

[9] Y. Liu, Y. Cao, M. Curty, S.-K. Liao, J. Wang, K. Cui, Y.-H. Li, Z.-H. Lin, Q.-C. Sun, D.-D. Li, H.-F. Zhang, Y. Zhao, T.-Y. Chen, C.-Z. Peng, Q. Zhang, A. Cabello, and J.-W. Pan, "Experimental unconditionally secure bit commitment," *Phys. Rev. Lett.*, vol. 112, no. 1, p. 010504, Jan. 2014.

[10] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, "Practical relativistic bit commitment," *Phys. Rev. Lett.*, vol. 115, no. 3, p. 030502, Jul. 2015.

[11] E. Adlam and A. Kent, "Deterministic relativistic quantum bit commitment," *Int. J. Quantum Inf.*, vol. 13, no. 5, p. 1550029, Aug. 2015.

[12] E. Adlam and A. Kent, "Device-independent relativistic quantum bit commitment," *Phys. Rev. A*, vol. 92, no. 2, p. 022315, Aug. 2015.

[13] A. Danan and L. Vaidman, "Practical quantum bit commitment protocol," *Quantum Inf. Process.*, vol. 11, no. 3, pp. 769–775, Jun. 2012.

[14] R. Loura, Á. J. Almeida, P. S. André, A. N. Pinto, P. Mateus, and N. Paunković, "Noise and measurement errors in a practical two-state quantum bit commitment protocol," *Phys. Rev. A*, vol. 89, no. 5, p. 052336, May 2014.

[15] Á. J. Almeida, A. D. Stojanovic, N. Paunkovic, R. Loura, N. J. Muga, N. A. Silva, P. Mateus, P. S. André, and A. N. Pinto, "Implementation of a two-state quantum bit commitment protocol in optical fibers," *J. Opt.*, vol. 18, no. 1, p. 015202, Jan. 2016.

[16] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, "Eavesdropping on quantum-cryptographical systems," *Phys. Rev. A*, vol. 50, no. 2, pp. 1047–1056, Aug. 1994.

[17] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[18] J. R. Taylor, *An Introduction to Error Analysis: The Study of Uncertainties in Physical Measurements*, 2nd ed. University Science Books, 1997.

[19] S. Siegel, *Nonparametric Statistics for the Behavioral Sciences.* McGraw-Hill Series in Psychology, Tokyo: McGraw-Hill Kogakusha, 1956.

[20] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, D. J. Twitchen, J. I. Cirac, and M. D. Lukin, "Room-temperature quantum bit memory exceeding one second," *Science*, vol. 336, no. 6086, pp. 1283–1286, Jun. 2012.

[21] K. Saeedi, S. Simmons, J. Z. Salvail, P. Dluhy, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, J. J. L. Morton, and M. L. W. Thewalt, "Room-temperature quantum bit storage exceeding 39 minutes using ionized donors in Silicon-28," *Science*, vol. 342, no. 6160, pp. 830–833, Nov. 2013.

[22] M. Zhong, M. P. Hedges, R. L. Ahlefeldt, J. G. Bartholomew, S. E. Beavan, S. M. Wittig, J. J. Longdell, and M. J. Sellars, "Optically addressable nuclear spins in a solid with a six-hour coherence time," *Nature*, vol. 517, no. 7533, pp. 177–180, Jan. 2015.

[23] W. J. Munro, K. Nemoto, R. G. Beausoleil, and T. P. Spiller, "High-efficiency quantum-nondemolition single-photon-number-resolving detector," *Phys. Rev. A*, vol. 71, no. 3, p. 033819, Mar. 2005.

[24] B. R. Johnson, M. D. Reed, A. A. Houck, D. I. Schuster, L. S. Bishop, E. Ginossar, J. M. Gambetta, L. Dicarlo, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf, "Quantum non-demolition detection of single microwave photons in a circuit," *Nat. Phys.*, vol. 6, no. 9, pp. 663–667, Sep. 2010.

[25] R. J. Sewell, M. Napolitano, N. Behbood, G. Colangelo, and M. W. Mitchell, "Certified quantum non-demolition measurement of a macroscopic material system," *Nature Photon.*, vol. 7, no. 7, pp. 517–520, Jul. 2013.

[26] N. Didier, J. Bourassa, and A. Blais, "Fast quantum nondemolition readout by parametric modulation of longitudinal qubit-oscillator interaction," *Phys. Rev. Lett.*, vol. 115, no. 20, p. 203601, Nov. 2015.

[27] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug. 2000.

[28] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy," *Phys. Rev. A*, vol. 56, no. 2, pp. 1163–1172, Aug. 1997.

[29] R. W. Spekkens and T. Rudolph, “Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol,” *Quant. Inf. Comp.*, vol. 2, no. 1, pp. 66–96, Dec. 2002.

[30] M. Williamson and V. Vedral, “Eavesdropping on practical quantum cryptography,” *J. Mod. Opt.*, vol. 50, no. 13, pp. 1989–2011, Jul. 2003.

[31] L. Dan, P. Chang-xing, Q. Dong-xiao, H. Bao-bin, and Z. Nan, “A new attack strategy for BB84 protocol based on, Breidbart basis,” in *Communications and Networking in China, 2009. ChinaCOM 2009. Fourth International Conference on*, Aug. 2009, pp. 1–3.

Chapter 6

Conclusions and Future Work

The work presented in this thesis focused on three major topics: (i) the implementation of a probabilistic and of an entangled photon source and the characterization of the source statistics, (ii) a dynamic method to control polarization in fiber-based schemes and (iii) the implementation of a quantum bit commitment protocol. In all cases, we have presented theoretical descriptions validated by experimental realizations. In this chapter, we present an overview of the work developed and summarize the main conclusions. Finally, we present directions for future work.

6.1 Conclusions

In Chapter 2, we started by presenting a brief review of the state-of-the-art of quantum communications. Then, we introduced some basic concepts of quantum information, mostly related with the security criteria. We have presented and described the Bennett-Brassard 1984 (BB84), Bennett 1992 (B92) and quantum-bit commitment (QBC) protocols, since they were used as a basis for this work. Finally, we have described the main components of a quantum communications scheme, namely the photon source, the encoding scheme, the quantum channel and the decoding scheme.

Chapter 3 of this thesis was devoted to the experimental implementation of a probabilistic and an entangled photon source. After a brief introduction to the four-wave mixing (FWM) process, we have demonstrated that this process could be obtained experimentally in a simple way, using it to determine the nonlinear coefficient of a dispersion-shifted fiber (DSF). This coefficient was obtained from the fit to the variation of the idler optical power as a function of the signal wavelength detuning, which shown to agree with the model proposed. Then, we have presented a method to determine the source statistics, which consisted in two steps: the measurement of the photon counts for different detection efficiencies and a numerical reconstruction based on the maximum-likelihood estimation (MLE) method and the expectation-maximization (EM) algorithm. The results obtained allowed us to conclude, in a general way, that the statistics of the source depends on the type of process which allows the generation of photons. If the generation process is spontaneous, the statistics of the source will be thermal, but if the process is stimulated the statistics will follow a Poissonian distribution. The spontaneous process was obtained when the signal power was low, thus presenting a thermal statics, changing to Poissonian when the signal power was high and the stimulated process dominated. For intermediate values of power, the statistics of the source follows a multithermal distribution, *i.e.*, a distribution which accounts with photons generated from spontaneous processes and others from stimulated processes. We have also concluded that when the average number of photons per pulse is much lower than one, the statistical distribution of the source is equivalent to the one which is obtained from an attenuated laser. Therefore, this source can be also used in proof-of-principal demonstrations of quantum communications. Then, we have studied the impact of the FWM process in a co-propagating quantum signal. As it is demonstrated in several works, the statistics of an attenuated laser source is always Poissonian, independently of the number of photons produced, since they were generated from stimulated processes. Therefore, we have used the same method as for previous case to determine the statistics of the attenuated photon source when it is in the presence of the FWM process. In order to verify the maximum impact of FWM, the idler photons were generated in the same wavelength of the quantum signal. We verified that when the quantum signal is set at a low power, the spontaneous processes from FWM dominate, leading to a thermal statistics. This can lead to security problems in some quantum communication experiments, since in this case the receiver is expecting Poissonian-distributed photons from the quantum signal and measures thermally-distributed ones, which can be interpreted as an effect of an eavesdropper. If the quantum signal is generated at higher power regimes, its statistics will dominate over the FWM, but at the same time it can also threaten the security of the protocol, since the average number of photons per pulse is higher and that can be advantageous for an eavesdropper to get information from the encoded qubits. Finally, we have demonstrated results which confirmed the violation of Clauser-Horne-Shimony-Holt (CHSH) inequality. For that, we have generated entangled-photon pairs in a Sagnac fiber loop and calculated the correlation between the two photons of the pair for different polarization configurations. The violation of the inequality was observed for more than 5 standard deviations, obtained from the value of Bell's parameter, $S = 2.469 \pm 0.0862$.

In Chapter 4, we have studied the evolution of the quantum-bit error rate (QBER) of the system in two different cases, first when no control of polarization was present and then using a polarization control method. We verified that, in a system without control of polarization, the QBER changes randomly with time and that variation is as higher as longer the transmission fiber. We have also studied the impact of cross-talk in the QBER, verifying that it is extremely important that it can be minimized as much as possible. Next, we have implemented a system of quantum communications using the FWM process as a photon source. Information was encoded in the photons' polarization, transmitted through an optical fiber and then decoded. We have verified that the visibility of the states-of-polarization (SOPs) detected was higher than 97%, even after photons were transmitted through 60 km of fiber. Finally, we have presented an automatic polarization control scheme based on monitoring the QBER of the system. We have derived a theoretical method to estimate the QBER in a rigorous way and which is based on the Clopper-Pearson confidence interval. The transmission system was based on the use of frames containing both qubits for the estimation of the QBER and qubits carrying quantum information. We have determined the minimum number of qubits for the accurate estimation of the QBER and demonstrated numerically that the method is capable of controlling polarization even after photons were transmitted through a long distance quantum channel. An experimental validation of the method was obtained using an optical fiber with 40 km as a quantum channel.

In Chapter 5, we have presented a QBC protocol which was based on two nonorthogonal SOPs to encode information. The encoding of classical information was performed in photons polarization and the quantum channel was an optical fiber. Results were obtained for three different cases, one where the sender and the receiver were side by side, other when they were separated by an 8 km optical fiber and other when they were 16 km apart. In all cases, we verified a successful implementation of the protocol, *i.e.*, within the theoretical security limits established. The success rate (SRATE) in the measurement of the results was higher than 93%, assuring that the implementation of the protocol was performed securely, *i.e.*, above the theoretical minimum of 85%. Finally, we have evaluated the optimal cheating strategy for Alice and discussed the security of the protocol, concluding that the implementation of the protocol is secure with a confidence up to 7 standard deviations.

6.2 Future Work

Related to the work presented in this thesis, some topics can be considered for future research. These topics are described next.

- The length of the quantum channel can be increased in order to test the functionality of the polarization control method presented in Chapter 4 when subjected to larger variations of polarization. The security of the implementation of the protocol described in Chapter 5 can also be tested for a larger separation between Alice and Bob.

- Most of the experiments presented in this thesis are proof-of-principle demonstrations. Therefore, the repetition rate of the data was relatively slow. It would be interesting to use higher transmission rates, in order to verify the behavior of the transmission scheme. One way to do it is through the use of field-programmable gate arrays (FPGAs) instead of microcontrollers (MCs).

- All experiments presented in this thesis were performed in a laboratorial environment. It might be interesting to move to a field environment in order to confirm their robustness in a real-world implementation.

- A security analysis model can be derived in order to determine the optimal number of photons per pulse to use in each experiment. Moreover, the impact of that optimal number of photons in the experimental results can be verified, namely in the transmission rate.

- The security of the protocol presented in Chapter 5 is based on current technological limitations. Therefore, the possibility to develop a scheme to make its implementation unconditionally secure can be investigated, removing its dependence from technological limitations.

Appendices

Appendix A

Characteristics of the Experimental Components

In this Appendix, we present the general characteristics of the components used in the laboratorial experiments.

Table A.1: Components used in the experiments.

Name	**Model**	**Company**	**Range**
Acousto-Optic Modulator	26027-2-1.55-LTD	Neos	0 - 27.12 MHz/1520 - 1570 nm
Arrayed-Waveguide Grating	MUX-W40	Gemfire	100GHz/1530.33 - 1561.42 nm
Classical Detector	11982A	Hewlett-Packard	1200 - 1600 nm
Coincidence Detector	TTM-8000	Austrian Institute of Technology	1 ps - 82.3 ps
Dispersion-Shifted Fiber	FutureGuide®-DS	Fujikura	1550 nm/2 $W^{-1}km^{-1}$
Electronic Polarization Controller	PolaRITE II/III	General Photonics	1260 - 1650 nm
External Cavity Laser	ECL1560/01	Anritsu	-7 - 11.76 dBm/1500 - 1620 nm
Fiber Polarization Controllers	FPC032	Thorlabs	1260 - 1625 nm
Half Waveplate	RZBH-1550	Thorlabs	1550±10 nm
Highly Nonlinear Fiber	Standard	OFS Fitel	1550 nm/10.5 $W^{-1}km^{-1}$
Linear Polarizer	OLPOL-155	Opto-Link	1550±40 nm
Mach-Zehnder Modulator	OC48	SDL	0-2.5 GHz
Microcontroller	dsPIC33FJ64GP802	Microchip	Up to 40 MIPS
Optical Coupler	OLCPL-155	Opto-Link	1550±40 nm
Optical Filter	LTFDWS-1C37	Gemfire	100 GHz/1547.72 nm
Optical Filter	LTFDWS-1C33	Gemfire	100 GHz/1550.92 nm
Optical Filter	LTFDWS-1C29	Gemfire	100 GHz/1554.13 nm
Optical Spectrum Analyzer	Q8384	Advantest	600 - 1700 nm
Optical Switch	Nanona	BATi	Up to 1 MHz
Pattern Generator	HP70841B	Hewlett-Packard	0.1-3 Gbit/s
Polarization-Beam Splitter	OLCS-155	Opto-Link	1550±40 nm
Quarter Waveplate	RZBQ-1550	Thorlabs	1550±10 nm
Rotating Linear Polarizer	PCB-2.5-1550	Thorlabs	1500 - 1600 nm
Single-Mode Fiber	OS2	Corning	1550 nm

Table A.1: Components used in the experiments.

Name	**Model**	**Company**	**Range**
Single-Photon Avalanche Detector	id 200	id Quantique	0 - 4 MHz/900 - 1700 nm
Single-Photon Avalanche Detector	id 201	id Quantique	0 - 8 MHz/900 - 1700 nm
Tunable Laser Source	TLS/C	Anritsu	10.5 - 13.5 dBm/1527.41 - 1657.13 nm
Variable Optical Attenuator	VA4 Series	JDS Fitel	0 - 70 dB
Wavelength-Division Multiplexing	OLWDM-F-156	Opto-Link	1550±5 nm

Appendix B

Laboratorial Pictures

In this Appendix, we show some pictures of the experimental schemes implemented in the laboratories of the Instituto de Telecomunicações, in Aveiro.

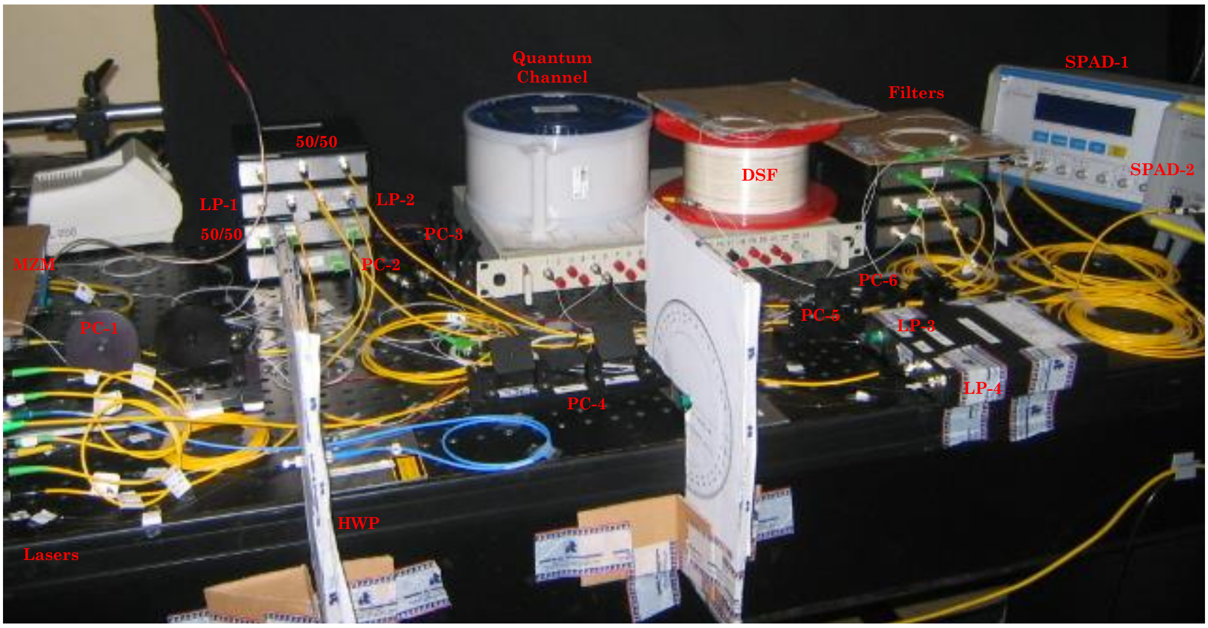

Figure B.1: First experimental setup used in the generation of the four-wave mixing photon source (which was later simplified to Fig. 3.7) and in the encoding/transmission/decoding of polarization-encoded photons (which was later simplified to Fig. 4.5).

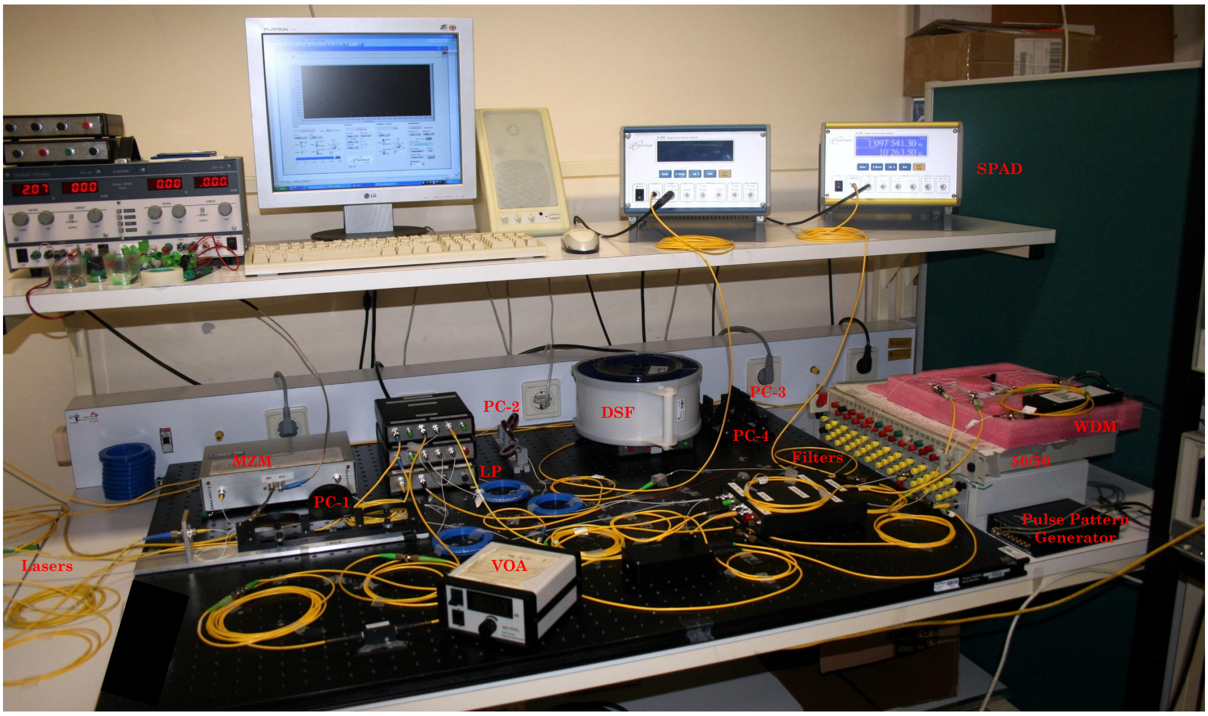

Figure B.2: Experimental setup used in the characterization of the four-wave mixing photon source statistics (Fig. 3.8) and in the study of the impact of four-wave mixing in a co-propagating quantum signal (Fig. 3.12).

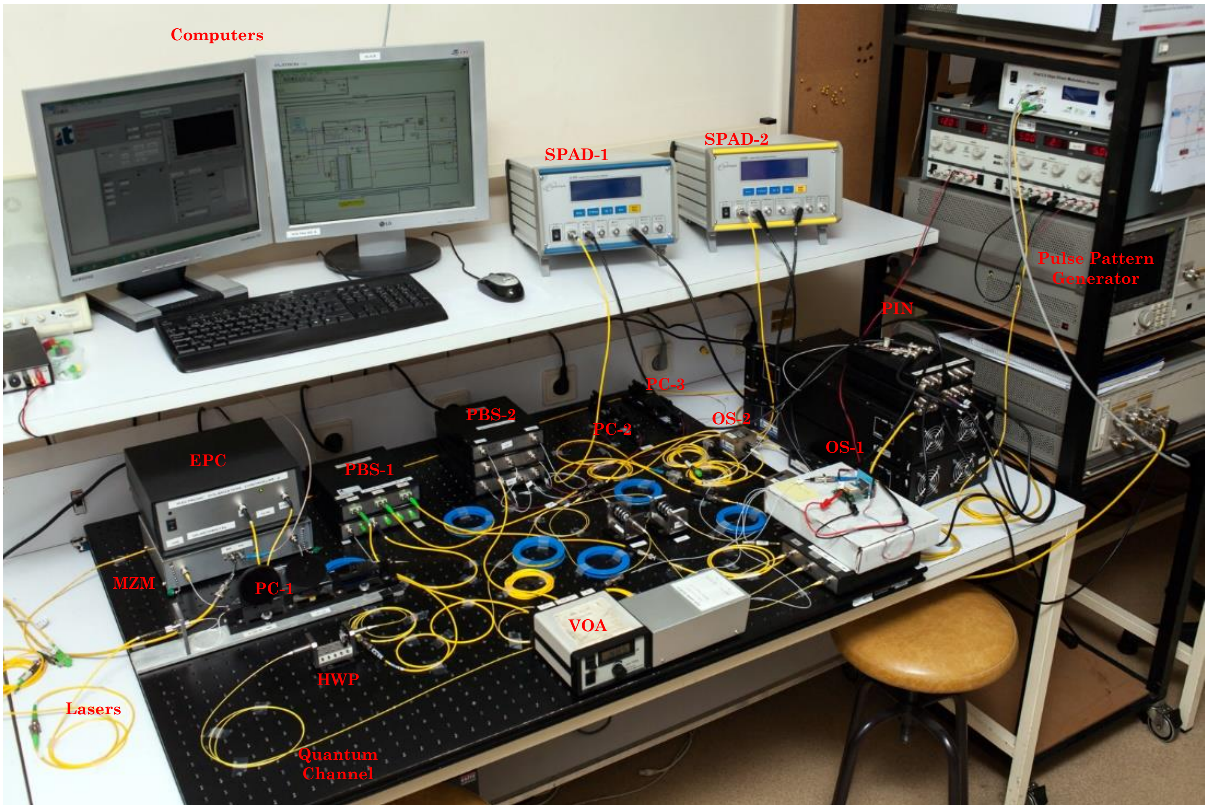

Figure B.3: Experimental setup used in the implementation of the real-time polarization control method (first version of Fig. 4.16).

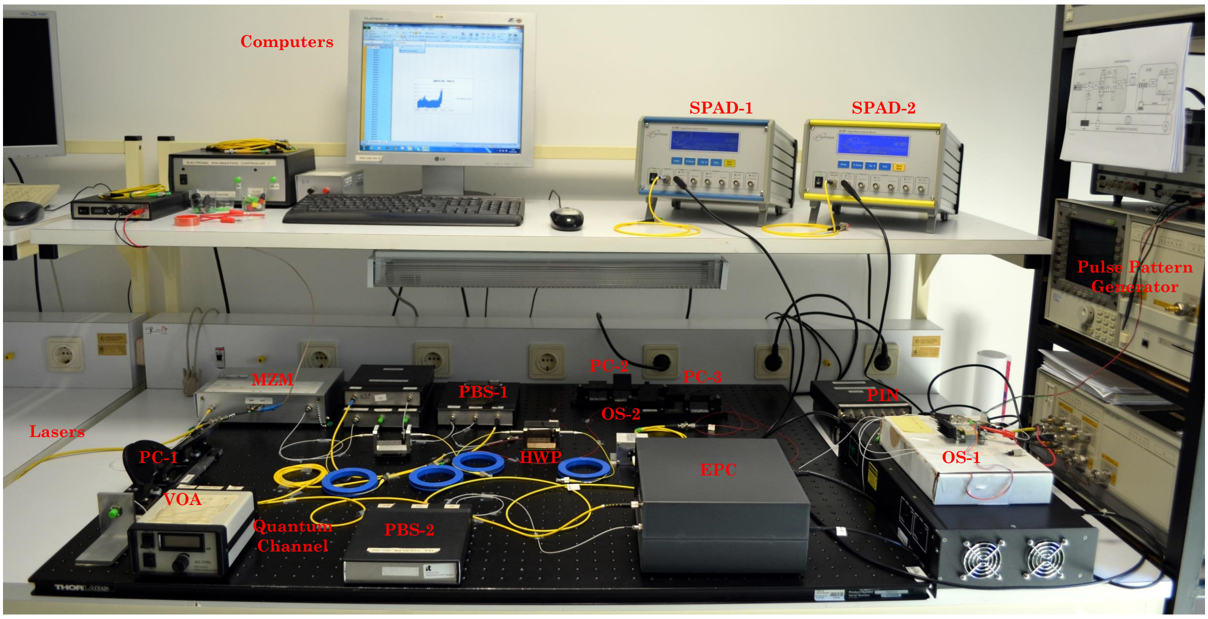

Figure B.4: New assembly of the experimental setup used in the implementation of the real-time polarization control method (Fig. 4.16).

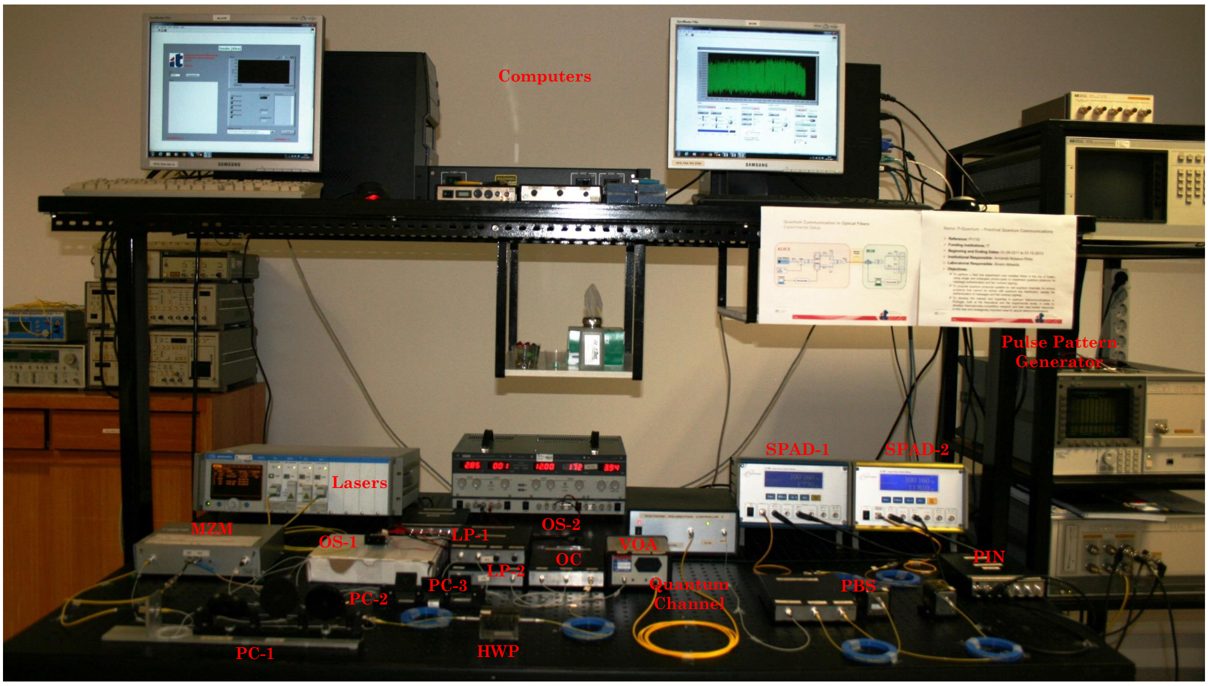

Figure B.5: Experimental setup used in the implementation of the quantum bit commitment protocol (first version of Fig. 5.2).

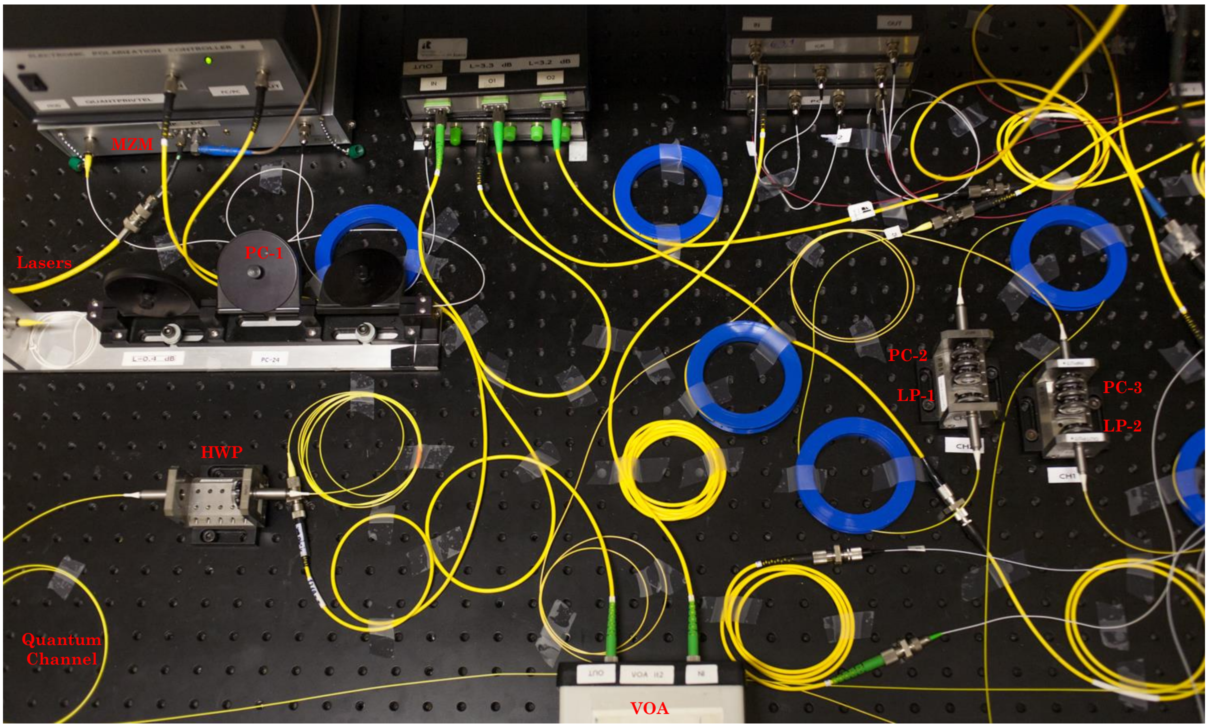

Figure B.6: Top view of the experimental setup used in the implementation of the quantum bit commitment protocol (which was later simplified to Fig. 5.2).