Guilherme Barreto Xavier

Practical Assets for Fiber Optical Quantum Communications

TESE DE DOUTORADO

Thesis presented to the Postgraduate Program in Electrical Engineering of the Departamento de Engenharia Elétrica, PUC-Rio as partial fulfillment of the requirements for the degree of Doutor em Engenharia Elétrica

Advisor: Prof. Jean Pierre von der Weid

Rio de Janeiro
March 2009

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Guilherme Barreto Xavier

Recursos Práticos para Comunicações Quânticas em Fibras Ópticas

Tese apresentada como requisito parcial para obtenção do título de Doutor pelo Programa de Pós-Graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica do Centro Técnico Científico da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Dr. Jean Pierre von der Weid
Orientador
Centro de Estudos de Telecomunicações - PUC-Rio

Dr. Hugo Zbinden
Université de Genève

Dr. Paulo Henrique Souto Ribeiro
UFRJ

Dr. Guilherme Penello Temporão
Centro de Estudos de Telecomunicações - PUC-Rio

Dra. Patrícia Lustoza de Souza
Centro de Estudos de Telecomunicações - PUC-Rio

Stephen Patrick Walborn
UFRJ

Djeisson Hoffmann Thomas
Centro de Estudos de Telecomunicações - PUC-Rio

Prof. Jose Eugenio Leal
Coordenador(a) Setorial do Centro Técnico Científico - PUC-Rio

Rio de Janeiro, 04 de Março de 2009

Guilherme Barreto Xavier

Guilherme B. Xavier graduated in Electrical Engineering at Pontifical Catholic University of Rio de Janeiro (PUC-Rio) in mid-2003, moving on to obtain the degree of Mestre in Engenharia Elétrica in 2005, in the field of modulation schemes for frequency encoded quantum key distribution. After starting his PhD, he went to KTH in Stockholm staying for one and a half years as an exchange PhD student. After return in the end of 2007, he carried on research in PUC-Rio to complete work for the PhD thesis. His research interests include (but are not limited to) quantum communications, quantum optics, and optical telecommunications metrology.

Bibliographic data

Xavier, Guilherme Barreto

Practical Assets for Fiber Optical Quantum Communications / Guilherme Barreto Xavier; advisor: Jean Pierre von der Weid. – 2009.

129 f. : il. ; 30 cm

Tese (Doutorado em Engenharia Elétrica)–Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2009.

Inclui bibliografia

1. Engenharia Elétrica – Teses. 2. Comunicações quânticas. 3. Distribuição Quântica de Chaves. 4. Fibras Ópticas. 5. Geração Quântica de Números Aleatórios. 6. Codificação em Polarização I. Weid, Jean Pierre von der. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. III. Título.

CDD: 621.3

Acknowledgements

To my advisor Jean Pierre von der Weid, for all the help, advice, friendship and discussions we had over these four years.

To Anders Karlsson, for welcoming me with open arms at KTH, and for all the nice talks and patiently explaining lots of cool stuff about entanglement and Sweden.

To my best friend and wife, Bruna, who has had the patience to endure me through the PhD, and who gave me priceless support.

A special thanks to my family specially my parents Alvaro and Luiza and my brother Bernardo, who always supported what I did and understood the sacrifices I had to make to get this work finally completed.

Many thanks to the people from the Optoelectronics group from CETUC/PUC-Rio: Djeisson, Janaína, Andy, Rogério, Tarcísio, Fernando, Marçal, Gustavo, Tito, Daniela and Douglas. Many thanks to Thiago, Giancarlo and Temporão who directly contributed to many of the results. A final thanks to Amalia, for all the help with the bureaucracy.

To the colleagues from KTH who received me very well, for providing a great working environment and who were always there for a friendly chat, Marcin, Qin, Christian, Simeon, Sebastian, Isabel, Maria, Johan, Rahul and Prof. Gunnar Bjork. A special thanks to Sèbastien for being a good friend, for advising me through the day-to-day work and for all the help settling in. A nice tap on the back to my new colleagues from Hefei, Wei and Tao. Last but not least, thanks to Walter from ACREO always ready to lend us equipment when we needed the most, specially the fiber splicer.

To Nino from the University of Geneva for the measurements done for the polarization-encoded QKD experiment. Many thanks to Profs. Hugo Zbinden and Nicolas Gisin for the helpful discussions and for the single-photon counting

module lent.

To all my friends who understood my absence during many months towards the end of the thesis. A special thanks to my sister-in-law Paula.

To everyone from LabSem in PUC-Rio, and to all the Professors and staff from CETUC and the Electrical Engineering department.

To CAPES and CNPq for the financial support.

This thesis was not a one-man work. A special thanks again to all those that contributed directly and indirectly to the results presented here!

Resumo

Guilherme Barreto Xavier. **Recursos Práticos para Comunicações Quânticas em Fibras Ópticas.** Rio de Janeiro, 2009. 129p. Tese de Doutorado - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

As comunicações quânticas estão rapidamente integrando-se às redes de fibras ópticas, entretanto muitos desafios de engenharia ainda existem para essa aglutinação. Esta tese discute algumas soluções práticas para a melhoria de aplicações reais em comunicações quânticas em fibras ópticas. No primeiro experimento uma fonte de pares de fótons emaranhados não-degenerados, de banda-estreita, empregando conversão espontânea paramétrica descendente (CEPD) é utilizada para demonstrar a viabilidade da distribuição quântica de chaves (DQC) através de 27 km de fibras ópticas, com o canal de sincronismo presente na mesma fibra com uma separação de 0.8 nm em comprimento de onda. A outra demonstração utilizou uma fonte heráldica de fótons únicos também baseada em CEPD para a realização de DQC através de 25 km de fibras ópticas com a utilização do protocolo de decoy states pela primeira vez. Houve também um estudo dos impactos gerados por ruído Raman espontâneo causado por um canal óptico clássico presente na mesma fibra que o canal quântico. Um protocolo para gerar números verdadeiramente aleatórios em um sistema de DQC independente da taxa de transmissão do sistema é proposto, e um experimento prova-de-princípio demonstra a idéia. Finalmente um sistema de controle automático de polarização é utilizado para a realização de uma sessão de DQC através de 16 km de fibras ópticas utilizando codificação em polarização, mesmo sob a presença de um embaralhador rápido do estado de polarização.

Palavras-chave

Comunicações Quânticas, Distribuição Quântica de Chaves, Fibras Ópticas, Geração Quântica de Números Aleatórios, Codificação em Polarização.

Abstract

Guilherme Barreto Xavier. **Practical Assets for Fiber Optical Quantum Communications.** Rio de Janeiro, 2009. 129p. Tese de Doutorado - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Quantum communications is quickly becoming integrated within fiber optical networks and still many engineering challenges remain towards this interweaving. This thesis deals with some practical solutions toward improving real-world applications in quantum communications within optical fibers. In the first experiment, a non-degenerate narrowband entangled pair single-photon source based on spontaneous parametric down-conversion (SPDC) is used to show the feasibility of performing quantum key distribution (QKD) through 27 km of optical fiber, with the synchronization channel wavelength multiplexed in the same fiber with a channel spacing of just 0.8 nm. A second experiment uses a heralded single-photon source also based on SPDC to perform QKD over 25 km of optical fiber with the decoy state modification for the first time. Then there is a study of the problems caused by spontaneous Raman induced noise due to the presence of a classical signal in the same fiber as the quantum channel. A protocol to generate truly random numbers in a QKD setup independent of the system's transmission rate is proposed, and a proof-of-principle experiment demonstrates the idea. Finally an automatic polarization control system is used to perform a QKD session over 16 km of optical fiber using polarization encoding, even in the presence of a fast polarization scrambler.

Keywords

Quantum Communications, Quantum Key Distribution, Fiber Optics, Quantum Random Number Generation, Polarization Encoding.

Summary

Figure list

Abbreviation list

ADSL - Asynchronous Digital Subscriber Line

AOM - Acousto-Optical Modulator

APD - Avalanche Photo-Diode

APCS - Automatic Polarization Control System

ASE - Amplified Spontaneous Emission

AWG - Array Waveguide Grating

BSF - Band Stop Filter

CHSH - Clauser Horne Shimony Holt

CW - Continuous Wave

DFB - Distributed Feedback

DG - Delay Generator

DM - Dichroic Mirror

DPSS - Diode Pumped Solid State

DS - Dispersion-Shifted

DWDM - Dense Wavelength Division Multiplexing

EA - Electro-Absorption

EPR - Einstein Podolsky Rosen

FBG - Fiber Bragg Grating

FC - Fiber Coupler

FM - Faraday-Michelson

FPGA - Field Programmable Generator Array

FWM - Four Wave Mixing

FWHM - Full Width at Half-Maximum

GHZ - Greenberger Horne Zeilinger

HSPS - Heralded Single Photon Source

HWP - Half Wave Plate

MZ - Mach-Zehnder

PBS - Polarizing Beam Splitter

PCF - Photonic Crystal Fiber

PD - Photo Diode

PMF - Polarization Maintaining Fiber

PNS - Photon Number Splitting

PPLN - Periodically Poled Lithium Niobate

QBER - Quantum Bit Error Rate

QIT - Quantum Information Theory

QKD - Quantum Key Distribution

QRNG - Quantum Random Number Generator

SOP - State of Polarization

SPAD - Single-Photon Avalanche Diode

SPDC - Spontaneous Parametric Down-Conversion

TC - Time Chopper

TDC - Time-Discriminator Circuit

WCP - Weak Coherent Pulse

WCS - Weak Coherent State

WDM - Wavelength Division Multiplexing

XPM - Cross Phase Modulation

1
Introduction

During the beginning of the last century the long open problem of blackbody radiation was finally explained by Max Planck. Back then no one could foresee that this apparently little problem of classical science would open up a whole new world in theoretical physics. We have come a long way in our understanding of the quantum world and yet there is still so much that we do not understand about what truly happens before a measurement is performed [1].

Even though we are still ignorant to some aspects of quantum physics, what we know of it has helped us immensely through the development of new technologies that have had major impacts on mankind, such as electronics and optoelectronics [2,3]. However, all these developments employed semi-classical approaches in the sense that electrons and photons were still treated mostly macroscopically. With the development of Quantum Information Theory (QIT) [4,5,6] applications were created with the requirement that quantum states are handled individually, such as quantum cryptography [7], quantum teleportation [8] and quantum computation [9].

QIT takes many of its concepts from Classical Information Theory (CIT) [10] with the main difference that instead of discrete classical states (distinct voltage levels, for instance) quantum states are used. Many possible quantum states can be used for QIT, such as the polarization state of a photon [5], or the spin of an electron [11]. Within binary systems in CIT the two possible states that information can be represented in are called bits, and in QIT qubits become the analogue. At first sight this may not seem like a huge difference, however upon closer inspection we notice that, due to quantum theory, the two states may be in a coherent superposition. Furthermore, depending on how the measurement of the states are performed, deterministic or probabilistic results are obtained. These are fundamental principles for QIT.

The focus of this thesis is on quantum communications and, as such, we are interested only in the photon as our quantum information carrier due to its naturally low decoherence probability during its time of flight [7] Several experiments which have been done to solve some of the experimental issues in quantum communications within optical fibers are discussed. These experiments include single-photon transmission using an entangled photon-pair source (idler measured locally, signal transmitted through the fiber) with a classical reference timing channel with a 0.8 nm separation from the quantum channel within the same 27 km of standard single-mode optical fiber. There is also the first experimental demonstration of the decoy state protocol with a heralded single-photon source, an analysis of the impact for quantum communications of spontaneous Raman induced noise, generated from classical channels in optical fibers, a protocol to generate truly random numbers for variable rate Quantum Key Distribution (QKD) systems that also dismisses the usage of quantum random number generators, and finally, the first experimental demonstration of polarization encoded QKD in optical fibers with real-time continuous birrefringence compensation. All these experiments demonstrate improvements to experimental quantum communications in optical fibers, with a slight bias towards polarization coding.

This thesis is organized as follows: Chapter II gives a brief introduction to quantum communications for the beginners in the field, chapter III deals with the two experiments performed in Anders Karlsson's group during the author's stay at KTH in Stockholm, while chapter IV deals with Raman noise measurements and the random number protocol. Finally Chapter V discusses the polarization encoded QKD experiment performed together with the Group of Applied Physics of the University of Geneva led by Nicolas Gisin. Chapter VI provides the conclusions and future perspectives.

2
An Introduction to Quantum Communications

2.1.
Introduction

Nowadays we take the simple act of communications for granted. Mobile phones are ubiquitous everywhere in the majority of countries in the world. Twenty years ago, or perhaps even less, most people would consider impossible for someone to make a phone call while in a taxi ride from any street in Johannesburg to another person standing in line in a bank in Helsinki. Modern communications have made the world smaller, changing many different aspects of society, from economics to human relationships.

The definition of the word communication according to the New Oxford American Dictionary is "the imparting or exchanging of information or news"'. There are many different forms of communication, both verbal and non-verbal, and it encompasses many different fields of study. Of course we only attain here to the engineering side of communication, that is, we only deal with systems that encode the information in a suitable manner, to be sent in a communication channel, and then to be decoded at the receiver.

In 1948 Claude Shannon published a landmark paper [10] in which many mathematical concepts for the theory of modern digital communication were laid out. Several important concepts such as, channel capacity, source entropy and communication in the presence of noise were introduced in this paper. In Fig. 1 the most basic components of a communication system are displayed: the information to be transmitted (represented by binary digits here, as it is usually the case), the modulator, the communication (or transmission) channel and finally the demodulator, where the information is recovered at the receiver. As usual in the quantum communication literature, we use the names Alice for the transmitter, Bob for the receiver and Eve (not yet present in Fig. 1) for the eavesdropper.

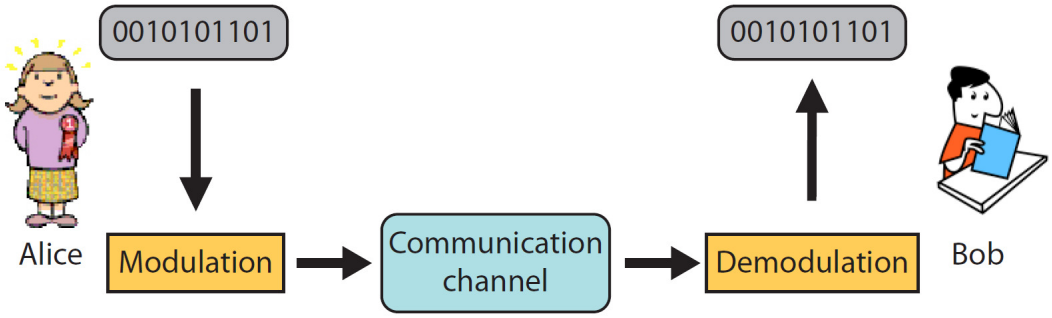

Figure 1 - Typical elements of a communication system. Information (represented here in its most usual form, binary digits) is modulated into an appropriate form for transmission through a communication channel by Alice. Bob demodulates it obtaining the same information Alice transmitted (in the absence of errors).

Of course the elements shown in Fig. 1 are just the basic building blocks of a communication system. Each block shown can be expanded into very complex systems [12], and many different types of modulation-demodulation schemes exist, both analog and digital. Using different schemes, different transmission rates may be obtained with the same communication channel between Alice and Bob. One example of such an improvement, was the adoption of ADSL (Asynchronous Digital Subscriber Line), which improved considerably the data transmission rate over ordinary copper twister-pair cables, allowing broadband internet access without a new installed infrastructure [13].

The field of modern classical communications has experienced major improvements since the times of Heinrich Hertz and Guglielmo Marconi. Recently, major research efforts on telecommunications are focused on improving both the accessibility of the Internet (especially in developing countries) and higher data rates allowing high-definition content to be delivered reliably, among other subjects.

2.2.Quantum physics and information

Quantum physics was born from the explanation of the blackbody radiation by Max Planck in 1900, followed soon by Albert Einstein's theory to explain the photo-electric effect in 1905. The energy of the electromagnetic wave is quantized and only dependent on its wave frequency as given by the famous

equation E = hν where h is Planck's constant and ν is the frequency. This result is one of the foundations of quantum physics [14]

These quantized packets of energy were first called light quanta by Einstein, with the name photon being coined by Gilbert N. Lewis in 1926 [15] Nowadays there is a whole field dedicated to the manipulation and study of the quantum effects of single photons and its interaction with matter called quantum optics [16,17,18]. Quantum physics is a broad field, but the focus of this thesis remains solely within quantum optics. There have been many landmark experiments on this field, exalting many features of quantum physics, and to name but a few please see [8,19,20,21].

Information was mathematically quantified by Shannon [10] but only classical systems were considered, to carry and process information. Good examples for these systems and widely used today, are different voltage levels inside an electronic circuit or the amplitude (or phase) of a classical light pulse (Shannon's paper concerns digital information. We do not consider the analog case, although it is also an information carrier). Although many discrete levels are possible, we move on considering only the binary case. Now, what if we employ a quantum system to store and process a single bit of information instead of a classical one? From what we know of quantum physics we can be sure to expect different results, and as we will see this is definitely the case.

We may ask ourselves: what is a quantum system? And what are the differences between quantum and classical systems? We could simply say that such a system is one that displays quantum effects, such as wave-particle duality and has a probability of being detected dependent on a wavefunction. Another definition is one that has not suffered decoherence. Decoherence is the coupling of a quantum system to the environment, leading to information loss [22]. The system loses its quantum properties since it entangles with many degrees of freedom of the environment. Another definition of decoherence is when the environment destroys the coherence between the states of a quantum system [23]. As a consequence, quantum systems can be very fragile, since any interaction with the environment leads to information loss. This is a critical problem, especially in quantum computation [9].

In the case of quantum communication, single-photons are the natural information carriers, and fortunately for this field, they do not decohere easily in

optical fibers or in free-space [5,7]. The actual practical limitation is photon absorption, which limits the transmission distance when combined with detector noise. And unlike in classical optical communications, there is no simple way to increase the transmission distance through the use of optical amplifiers. So far it seems there are only problems and no advantages in quantum communications over classical systems, but as we shall see, the nature of the states employed in quantum communications allows feats of communication that are impossible through purely classical means. Quantum communication is also necessary for the transfer of quantum information between quantum computers.

2.3.Qubits

The fundamental unit of information is the bit, short for binary digit [10]. In an analogous way the fundamental unit of quantum information is the quantum bit, or qubit for short [5,6,9]. As we mentioned above, a qubit is represented by a quantum state, just like a classical state holds a bit of information. And also, just like two distinct levels of a classical system represent a bit, two different states of a quantum system compose a qubit. Now is where the differences begin. A qubit can be represented as an unitary state vector in a bi-dimensional complex Hilbert space. Any degree of freedom of a quantum system can be used, such as spin, polarization, phase, frequency, etc… Let us use the polarization of a photon to represent our qubit. Since it is represented by a vector, we need to choose a basis in the Hilbert space to write our state. Let the kets shown in Fig. 2 $|H\rangle$ and $|V\rangle$, that is, horizontal and vertical polarization states respectively, be our basis. The state $|\psi\rangle$ can be written as a linear combination of the kets forming the orthonormal basis as $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$. The complex numbers α and β are the probability amplitudes of obtaining $|H\rangle$ and $|V\rangle$ when a projective measurement is performed on $|\psi\rangle$. The corresponding probabilities of obtaining $|H\rangle$ and $|V\rangle$ are $|\alpha^2|$ and $|\beta^2|$ where the probabilities must add up as $|\alpha^2| + |\beta^2 = 1|$.

The first major difference between classical and quantum systems comes from a simple observation of Fig. 2. When a projective measurement is performed

on $|\psi\rangle$ only two possible outcomes are obtained, $|H\rangle$ or $|V\rangle$ and as mentioned above, the probabilities of obtaining each result depend on the state $|\psi\rangle$. A simple way to visualize this is shown in the inset of Fig. 2 displaying the state $|\psi\rangle$ going through a polarizing beam splitter (PBS), with the state $|V\rangle$ reflected, and $|H\rangle$ transmitted, with the probability of each outcome depending on α and β. Clearly the original state is destroyed and all we are left with is a measurement result. Therefore, the trivial act of performing a measurement as we do everyday on classical systems is completely different in the quantum world. The only way to realize the measurement preserving the original state is aligning the measurement basis (that is, aligning either the H or V axis of the PBS) with the state $|\psi\rangle$. Geometrically this can be seen referring again to Fig. 2 where $|\psi\rangle$ is aligned with one of the axis of the orthonormal basis spanned by the PBS. This issue is the main concept behind quantum key distribution [7]. This discussion was done assuming $|\psi\rangle$ is a single-photon state.

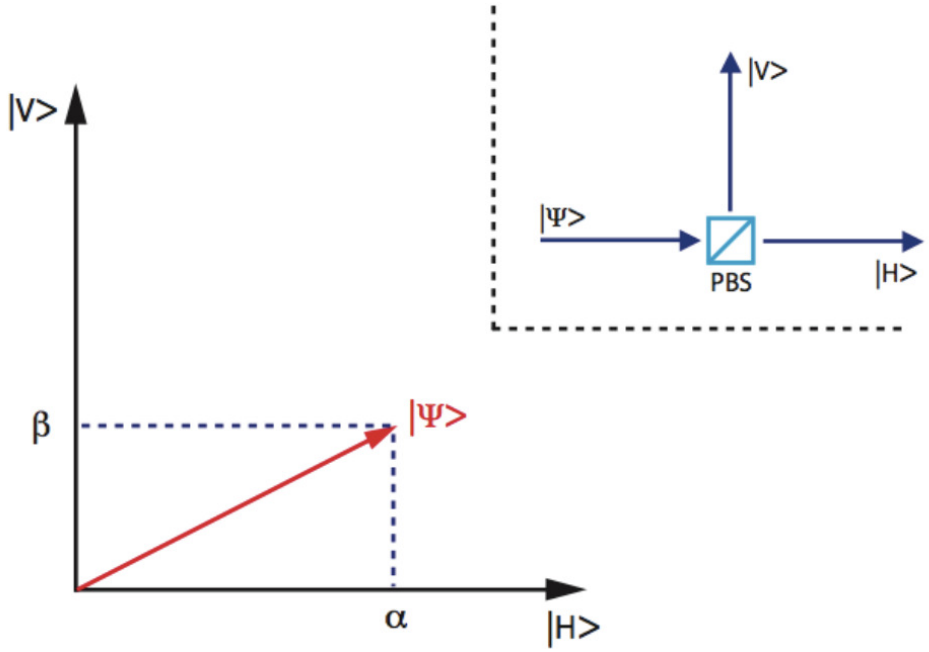

Figure 2 - Graphical representation of the state of polarization $|\psi\rangle$. Inset shows what happens to $|\psi\rangle$ after a polarizing beam splitter (PBS).

What seems to be a major drawback is what gives quantum information its power. While a bit, independent of how it is stored, is always either 0 or 1, a qubit

can be in a coherent superposition of two states. We can therefore rewrite the state $|\psi\rangle$ in a more general form:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

It is the same state as presented before, however this time it is written in terms of the more general states $|0\rangle$ and $|1\rangle$, representing any two quantum states comprising an orthonormal basis in a bi-dimensional Hilbert space. This state is in a quantum superposition, since before a measurement is performed, it is in both states $|0\rangle$ and $|1\rangle$ simultaneously. This is unique in the quantum theory and there is no classical analog. It also reinforces the fact that different results are obtained depending on how the measurement is performed. As we mentioned above, the polarization of a photon is a good example of a physical system to store a qubit. Other examples include the photon's phase, the spin of an electron or atomic states [9].

2.4. Single-photon sources

The natural candidates for the transport of quantum information are single photons. Without going into too much detail single-photons can be represented as the photon number state $|1\rangle$ where $|n\rangle$ represents a state with *n* photons. For more details please see [16,18] Nevertheless single-photon states can be easily manipulated using standard commercial optical components such as wave-plates, beam splitters and modulators. We would like to encode each qubit in single-photon states (this is crucial for the security of quantum key distribution), however this is not an easy feat. There is still no ready-to-use source which outputs a single-photon on demand.

The simplest source we can use is to take a laser and attenuate it. In fact this is the most widely used source in quantum communication experiments until the beginning of this decade [7] and in all current commercial implementations of quantum key distribution [24,25].

This is a very simple and cheap source, however it has some problems. A laser is indeed a good choice, due to its long coherence length and narrow spectrum. The issue we need to consider is that the probability to obtain a given number of photons within the coherence time follows a poissonian distribution:

$$p(n) = \frac{e^{-\mu}\mu^{n}}{n!} \tag{2.2}$$

where n is the number of photons, and μ is the average number of photons. μ is related to the average power of the light source. In practice what is done is to employ an attenuated pulsed laser, or a continuous-wave (CW) laser with an external amplitude modulator and an optical attenuator. The problem with this source is that the number of photons on each pulse is random, according to Eq. 2.2. It is impossible to know *a priori* the number of photons in each pulse, all we know is the average photon number μ. For μ = 1 photons / pulse, we obtain an equal probability of 36.8 % of obtaining a pulse with zero photons (vacuum state) or one photon. Since all probabilities must add up to unity, the probability of obtaining a pulse with two or more photons is 26.4 %. Clearly this is not a good single-photon source because we have no control when a single-photon pulse is emitted. The pulses emitted by the attenuated laser are called weak coherent pulses (WCPs), since each pulse is in a coherent state [7].

A different type of single-photon source that has gained notoriety is the one based on semiconductor quantum dot structures. A quantum dot has the same principle of a quantum well [2], which is a sandwich of two different semiconductor structures with different band-gap energies, thus providing a one dimensional electron confinement. The quantum dot follows the same idea, except that the geometry provides three dimensional confinement, thus generating a similar energy level distribution of an isolated atom. A single quantum dot, is in principle, an excellent source of narrowband high-coherence single-photons. The major difficulty is to grow just a single-dot in a semiconductor structure [26] and the fact that all are unique, emitting photons with distinct wavelengths. In practice many dots are grown, since it is difficult to obtain such a type of control during the growth process. When a current pulse is applied to excite the dots, many of them emit simultaneously, degrading the performance of the source. One successful solution is to place the dot inside a cavity, which works as a filter, therefore selecting emission of a single dot [26,27]. Their widespread use remains limited since no commercial products exist yet, keeping their use restricted to research groups that have access to semiconductor growth facilities. Nevertheless quantum dots remain a good candidate for true single-photon sources in the future.

In order to explain another important type of single-photon source, based on spontaneous parametric down-conversion (SPDC) in a non-linear $\chi^{(2)}$ medium, first we need a small section briefly explaining non-linear optics.

2.4.1.Non-linear optics

Non-linear optics is the field that deals with phenomena that occur in a medium that depends non-linearly on the incident optical power. When an optical field interacts with a dielectric medium, the electromagnetic wave induces a dipole polarization in the medium, which generates a new electromagnetic field. The electric polarization *P* of the medium can be written as a function of the electric field *E* as [28]:

$$P = \varepsilon_0 \chi^{(1)} E + \varepsilon_0 \chi^{(2)} E^2 + \varepsilon_0 \chi^{(3)} E^3 + \ldots \tag{2.3}$$

where $\chi^{(n)}$ is the medium's susceptibility tensor of order *n,* and ε_0 is the vacuum's electric permissivity. As we can observe from Eq. 2.3 for low-power electric fields only the linear term is important. However, as the field strength increases, the non-linear terms become significant. As we also see, the non-linear response depends both on the field strength and the material's susceptibility, therefore different materials will yield different non-linear responses. There is also a further consideration that, depending on the structure of the medium, even or odd orders susceptibilities may vanish. For example centrosymmetric crystals do not exhibit even order susceptibilities.

If we consider only the $\chi^{(2)}$ component, and there are two optical fields with different frequencies ω_1 and ω_2 combining in the non-linear medium (Fig. 3), the resulting second-order polarization becomes:

$$P^{(2)} = \varepsilon_0 \chi^{(2)} \left(E_1 + E_2 \right) \tag{2.4}$$

where $E_1 = E_a \cos \omega_1 t$ and $E_2 = E_b \cos \omega_2 t$ Substituting back into (2.4) we obtain, after simple trigonometric manipulation:

$$P^{(2)} = \frac{1}{2}\varepsilon_0 \chi^{(2)}\{[E_a^2(1+\cos 2\omega_1 t) + E_b^2(1+\cos 2\omega_2 t) + E_a E_b[\cos(\omega_1 - \omega_2) + \cos(\omega_1 + \omega_2)]\} \quad (2.5)$$

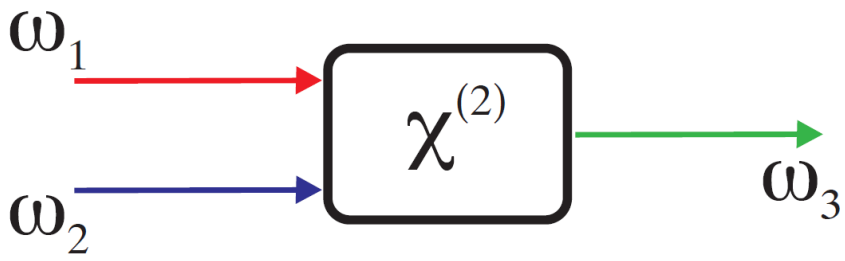

Figure 3 - Two optical fields with frequencies ω_1 and ω_2 combining in a non-linear medium to produce ω_3.

From Eq. (2.5) we have the following terms: the harmonics $2\omega_1$, $2\omega_2$ and the sum and difference terms $\omega_1 + \omega_2$ and $\omega_1 - \omega_2$. The sum and difference terms are of special consideration to us, as they give rise to many different effects. They yield the processes *sum-frequency generation* and *difference-frequency generation*. If we set $\omega_1 = \omega_2 = \omega_p$ that is, we have a single input optical field of frequency ω_p called the pump giving rise to $\omega_3 = 2\omega_p$. This can be verified by simply using $E_1 = 2E_1 \cos \omega_p t$ in Eq. 2.4. This particular case is called Second Harmonic Generation (SHG) [28] and it is widely used to double the frequency of an optical signal.

Focusing again on single-photon sources, the non-linear process we are most interested in is the so-called Spontaneous Parametric Down-Conversion (SPDC). This process is basically the inverse of the one shown on Fig. 3 as we have a single pump field at the input ω_p of a non-linear medium (typically a crystal), and two fields at the output ω_s and ω_i, called signal and idler respectively. However this process cannot be explained purely with classical theory. What happens is that photons from the pump interact with the vacuum field (a quantum phenomenon), generating both signal and idler fields [16]. It is a spontaneous process, since it depends on the vacuum fluctuations. The success probability for this process is quite low, typically of the order of 10^{-6} hence high pump powers are typically used. To increase the conversion efficiency, longer

crystals may be used as well as tighter focusing conditions [29]. Another way to improve the conversion is to use waveguides such that the optical field stays highly confined throughout the crystal length, increasing the intensity and also the non-linear effect [30].

The crystals that have been typically used for experiments on SPDC are BBO (Beta Barium Borate or β-BaB_2O_4), KTP (Potassium Titanium Oxide Phosphate or $KTiOPO_4$) and $LiNbO_3$ (Lithium Niobate). Another problem with SPDC is due to the fact that the wavelengths and polarization of the idler and signal can be different. When they are propagating inside the crystal, they travel at different velocities due to the wavelength and polarization dependence on the refractive index. In collinear propagation they cannot be in phase along the length of the crystal, due to destructive interference and thus generating no output. In order to compensate this, phase-matching is needed.

Phase-matching can be obtained geometrically in a birefringent crystal. Birefringence is the phenomenon in which a material's refractive index varies depending also on the optical field polarization, besides the optical field frequency. Thus, it is possible to have phase-matching between signal and idler fields depending on their directions of propagation. This scheme is limited however, since only a very specific set of parameters (wavelengths, polarizations and crystal optical properties) allows effective phase-matching between pump, signal and idler, that is, $\Delta k = k_s + k_i - k_p = 0$. Another limitation is that it is not usually possible to use the strongest components of the susceptibility tensor $\chi^{(2)}$, due to the geometry of the conversion process [31]. This process is called birefringent phase-matching.

Birefringent phase-matching is possible in two situations [31]. In the first, the pump's polarization is aligned with the crystal's extraordinary axis, and the signal and idler are produced parallel to the crystal's ordinary axis. This is called type-I phase-matching. The other type is when the pump is once again extraordinary, and the idler and signal are produced with orthogonal polarizations between each other. In this case the signal maintains the pump's polarization, and the idler comes out parallel to the ordinary axis. This process is called type-II phase matching. In type-II it is not possible to obtain spot-like collinear emission for both signal and idler, due to the different beam polarizations [31]. It is highly desirable to obtain collinear emission due to ease of alignment, and efficient

coupling to optical fibers. In type-I birefringent phase-matching, collinear spot-like emission is possible to obtain albeit for a restricted set of frequencies.

As just discussed birefringent phase-matching can be limited due to the stringent requirements to obtain it. A more efficient approach is called *quasi-phase matching* [29,30,31]. In this procedure the sign of the non-linear tensor $\chi^{(2)}$ is periodically flipped along the length of the crystal. This sign flipping is achieved through appllication of a strong electrical field periodically along the cyrstal, in a process called periodic poling. The idea behind quasi-phase matching is that when the idler and signal photons created in the beginning of the crystal begin to drift out of phase, the sign of $\chi^{(2)}$ is reversed, and then the signal and idler photons are brought back in phase, thus increasing the generated intensity. The sign fipping is repeated along the entire crystal (Fig. 5). For a periodically poled crystal the phase-matching condition is given by:

$$k_p = k_s + k_i + K \qquad |K| = \frac{2\pi}{\Lambda} \tag{2.6}$$

where K is the effective grating-type k-vector and Λ is the poling period [30]. This approach is more flexible than birefringent phase-matching, since more frequency combinations are possible by simply changing the poling period Λ. Furthermore the converted wavelengths may be tuned within a certain range, through variation of the crystal's temperature.

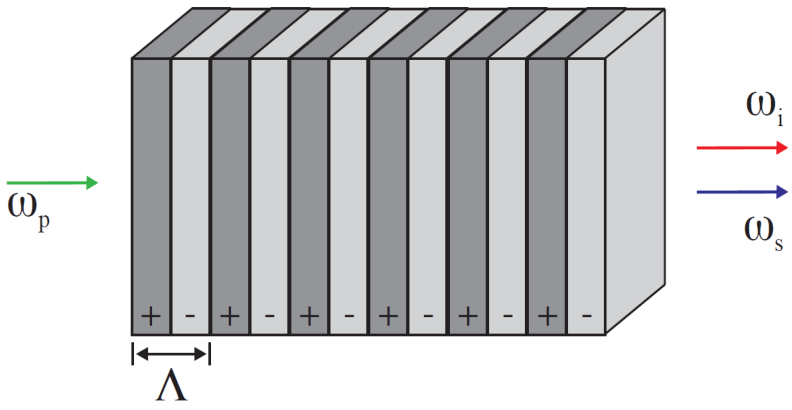

Figure 4 - A periodically poled crystal. The signs indicate where the non-linearity $\chi^{(2)}$ is negative and positive. Shown are also the input optical field ω_p and the outputs ω_s and ω_i.

We can use a non-linear crystal and the process of SPDC to produce a single-photon source [32]. The simplest is the Heralded Single Photon Source (HSPS), in which the detection of a photon "heralds" the presence of the other [32, 33, 34]. Usually in an HSPS, the crystal poling is designed such that the idler can be detected by a high-efficiency detector, thus providing a timing reference for the other photon (signal) with high probability. This conversion is normally non-degenerate. A more detailed description of an HSPS will be given in chapter 3.

2.4.2. Entangled single-photon pair sources

Another type of single-photon source using non-linear crystals is the one which produces entangled photon pairs [35]. Entanglement is one of the key features of quantum physics, and it is at the heart of quantum information [1,5,6,9]. When two quantum particles are said to be entangled it means that their wavefunction is not separable, for example:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2\right) \tag{2.7}$$

Eq. (2.7) represents an entangled state since we cannot write it in a separable form. The indexes 1 and 2 represent two field modes. Compare (2.7) with:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_1|0\rangle_2 - |1\rangle_1|1\rangle_2\right). \tag{2.8}$$

(2.8) is separable since we can write it as $|\psi\rangle = \frac{1}{\sqrt{2}}|1\rangle_1\left(|0\rangle - |1\rangle\right)_2$, therefore it is not an entangled state. Entangled states are remarkable in the sense that each particle of the pair carries no information individually. It is only the state of the pair which is meaningful. The two wavefunctions displayed above were not normalized. Rewriting (2.7) as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b\right) \tag{2.9}$$

where the subscripts *a* and *b* mean which photon of the pair we are referring to. From (2.9) we see that if we choose to measure simply particle *a* or *b*, we have a

50 % chance of obtaining 1 or 0 as the result, assuming measurement in the computational basis. The results are therefore random, and one simple example of such a case is the measurement of a single-photon in the diagonal polarization state with the H-V axis of a polarizing beam splitter. However if we perform correlation measurements between the photons of the pair, the results obtained will not be random. From (2.9) we see that every time we obtain a measurement result of 1 from one photon, the other one will yield 0 and vice-versa. What is special about the entangled state is that the correlations hold even when the particles are separated, providing a "non-local" character to quantum physics. Albert Einstein, Boris Podolsky and Nathan Rosen were unhappy with this thought, and as such, they proposed a "gedanken" experiment later called the EPR paradox [36], which questioned whether quantum physics was a complete theory. The EPR paradox remained an open philosophical problem until John Bell's discovery of an inequality (which bears his name today) [1], and later adapted by Clauser, Horne, Shimony and Holt [37] for experimental tests demonstrating that quantum physics is indeed non-local [19, 38, 39].

For quantum communications there are four entangled states which are extensively used, the so-called Bell states:

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_a\left|1\right\rangle_b \pm \left|1\right\rangle_a\left|0\right\rangle_b\right) \tag{2.10}$$

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_a\left|0\right\rangle_b \pm \left|1\right\rangle_a\left|1\right\rangle_b\right) \tag{2.11}$$

As we can see, the maximally entangled singlet state (2.9) is in fact $\left|\psi^{-}\right\rangle$, one of the Bell states. For instance these states are used in quantum teleportation [8]. Also note that the Hilbert space of these states double to 4 dimensions, since we now have two quantum particles, each belonging to a 2-dimensional Hilbert space. There are entangled states with more dimensions, comprised more particles. For example, one particular class of 3 particle entangled state is the Greenberger-Horne-Zeilinger state (GHZ) [40]:

$$\left|GHZ\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left|0\right\rangle\left|0\right\rangle + \left|1\right\rangle\left|1\right\rangle\left|1\right\rangle\right) \tag{2.12}$$

It was briefly explained what entangled states are, however how can we produce them? There are many different ways, depending on which type of particles one would like to entangle. We focus here on entanglement of photons, since it is the main concern of this thesis. One relatively simple way to produce polarization entangled photon pairs is through the usage of SPDC. For example it is possible to use type-II conversion in a single BBO crystal, however it was not very efficient due to the fact that the overlap of the light cones produced by both polarizations was small [35]. An improvement to this source was done in 1999, introducing the idea of using two crystals, orthogonally oriented between themselves, with each crystal producing one polarization, H or V, and the pump polarization oriented at 45º (Fig. 5) [41]. Note in Fig. 5 that each crystal produces pairs of photons with parallel polarizations, $|H\rangle|H\rangle$ in the first, and $|V\rangle|V\rangle$ in the second. Therefore the state is:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_a|V\rangle_b + e^{i\phi}|V\rangle_a|H\rangle_b\right) \tag{2.13}$$

where the phase α comes from the pump. If we use an additional birefringent phase shifter in the pump, we can tune the value of α, and with a half-wave plate in either the signal or idler path, we can produce any of the four Bell states. In order to have the maximally entangled state, the setup needs to be carefully aligned and balanced, such that the probabilities of conversion for both H and V polarizations are equal.

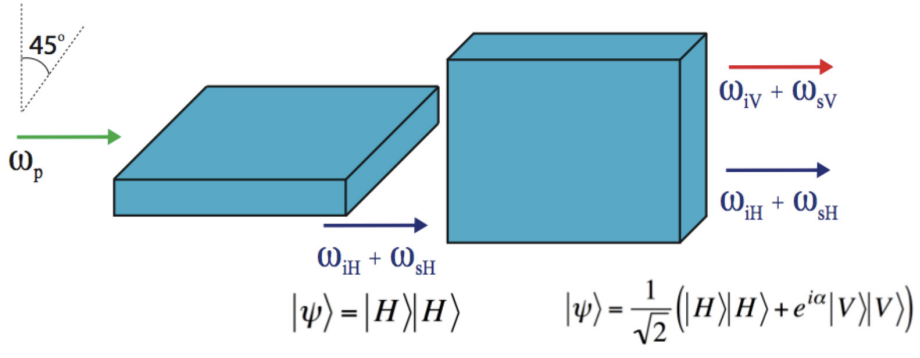

Figure 5 - Generation of the maximally entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle|V\rangle + e^{i\phi}|V\rangle|H\rangle\right)$ employing two non-linear crystals, with the pump polarization oriented at 45º.

We have only mentioned polarization-entangled photon pair sources thus far, however another important class of photon entanglement is called energy-time entanglement [40]. Due to phase matching conditions, and energy conservation, once one photon is detected (signal or idler), the other will be detected within the two-photon correlation time, which is of the same order as the single-photon coherence time [42]. This time is dependent upon the bandwidth of the down-converted photons. In order to prepare temporally entangled photons each generated photon is sent through identical separate unbalanced Mach-Zehnder interferometers (MZ), with the long arm much longer than the coherence time of the emitted photons in order to prevent single-photon interference. In addition the long arms in both sides have a phase-shifter adjusted to ϕ_1 and ϕ_2 (Fig. 6). This scheme was originally devised by Franson [43]. If a coincidence is detected, it means that photons took either the long-long path (L-L), or the short-short (S-S). Again, we can only be sure of that, if the MZ interferometer unbalance is much greater than the coherence length of the photons. Another restriction is that the coincidence gate used, needs to be much shorter than the coherence time. Effectively what happens is that the long-long and short-short paths interfere, and by varying the phase shifters, interference curves are obtained which violate Bell's inequality [42]. The entangled wave function described by the setup in Fig. 6 is:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|L\rangle_1|L\rangle_2 + e^{i\phi}|S\rangle_1|S\rangle_2\right) \tag{2.14}$$

where $\phi = \phi_1 - \phi_2$ and is very similar to what we have seen before, except that the degree of freedom used is now time.

If the continous-wave (CW) laser used in the Franson experiment described above is replaced by a short pulsed pump laser, then we get what is called time-bin entanglement [7]. In this case, the pump passes through an interferometer with one arm much longer than its pulse width, before being focused on a non-linear crystal. After the interferometer, we have two pump pulses separated in time, and the state of the pump is $\alpha|short\rangle_p + \beta|long\rangle_p$. α and β can be controlled with a variable beam splitter employed at the pump interferometer, which also includes a phase shifter in the long arm. Both pulses pass through the crystal. If down-conversion occurs through SPDC, then the entangled state is [40]:

$$|\psi\rangle = \alpha|short\rangle_1|short\rangle_2 + \beta|long\rangle_1|long\rangle_2 . \quad (2.15)$$

Changing the ratio of the beamsplitters in the pump interferometer, and varying the phase shifter all time-bin Bell states can be prepared [40].

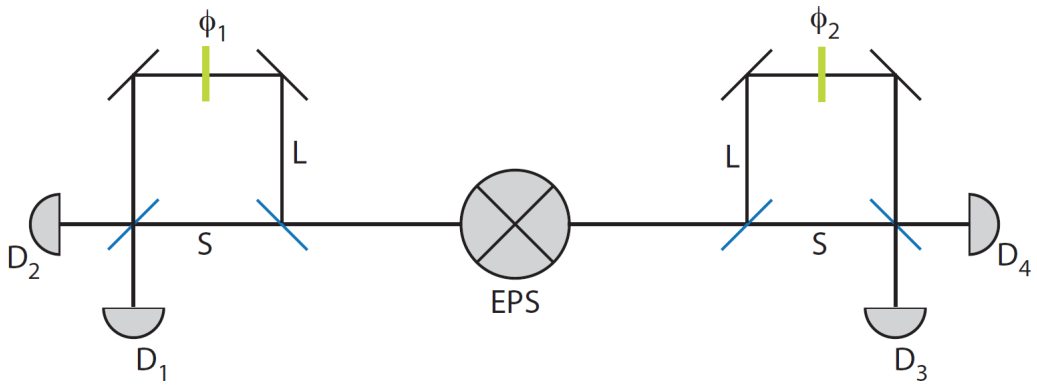

Figure 6 - Scheme for a Franson-type interferometry setup. EPS: Entangled photon source; L and S: Long and short interferometer arms respectively; D_x: Single photon detectors; ϕ_x: Phase shifters.

2.4.3. Generation of single-photon pairs in optical fibers

As discussed below, optical fibers are a very practical way to send single-photons between two parties. The single photons produced by the sources based on SPDC discussed above, may need to be transported by optical fibers in many cases. As a result, considerable work has been done to improve the sources for optimal coupling into optical fibers [44]. Another approach which is very promising, would be the generation of single photons already inside an optical fiber, thus removing all possible coupling problems.

The idea is to use another non-linear effect, called Kerr effect (associated with the $\chi^{(3)}$ tensor) [28] to generate four-photon scattering events (four-wave mixing). Two pump photons of frequency ω_p scatter in the fiber due to the Kerr effect and generate simultaneously two photons at frequencies ω_i (idler) and ω_s. Energy conservation requires that $2\omega_p = \omega_i + \omega_s$ and obviously the two original pump photons are destroyed in the process. Other advantages of using optical fibers as the non-linear medium are the low losses of modern fibers (0.2 dB km^{-1} at 1550 nm), small confinement cross-sections (of the order of 50 μm^2) and the

fact that the fiber can be made many kilometers long [45]. These properties compensate the fact that the Kerr effect is relatively weak. The process is also phase-matched as long as the pump is tuned close to the zero-dispersion wavelength of the fiber [46].

Polarization entangled photons have been produced using these sources [47, 48], and also time-bin entanglement [48]. Finally, there have also been experiments using photonic crystal fibers (PCFs) as the non-linear medium [49, 50] instead of dispersion-shifted commercial (DS) fibers like the ones in [46, 47]. PCFs can have higher non-linear coefficients per unit length than commercial fibers, thus having the possibility to yield brighter sources in the future.

2.5. Single-photon detectors

None of the practical aspects of quantum communications would be possible without the detection of a single-photon. In the past, single-photon detection was mostly based photomultipliers. Nowadays the best choice for practical applications are detectors based on avalanche photo-diodes (APDs), since they are easily portable and do not require cryogenic temperatures to work [51]. There are other options to detect single-photons, such as up-conversion [52] and superconducting nano-wire detectors [53, 54]. Furthermore if one wishes to work on mid-far infrared wavelengths, up-conversion detectors seem to be the most effective way to go [55].

We will focus on APDs since all work done in this thesis uses these detectors. In short they have been very successful in many experiments in quantum information and quantum optics so far, but as we shall see, there is still room for improvement. Si APDs cover the region from around 400 nm up to around 1000 nm. For longer wavelengths our choice remains with Ge (best choice for 1300 nm) or InGaAs (the only choice for 1550 nm). Si APDs outperform Ge and InGaAs APDs. However they are limited to wavelengths up to around 1000 nm. As we will see, for quantum communications, the 1550 nm region is highly desirable.

Regardless of the type of diode used, the basic procedure of how an APD detects a single-photon is as follows: The APD is reverse biased until it is below the breakdown voltage value (which depends on the material of the diode and

operating temperature). The breakdown voltage is negative, since we are applying a reverse bias, so that all the times the detector is below the breakdown voltage it means it can generate an avalanche. At this point the diode is in a situation that if a single-photon successfully gets absorbed and generates an electron-hole pair, a macroscopic electric current is produced, which can be easily detected [51]. After this, some procedure to quench the avalanche must take place, otherwise the diode may be destroyed due to overheating.

Basically, single-photon avalanche detectors (SPADs) can be divided in three operating modes: passive, active and passive gated modes. As just mentioned, all three modes share a similarity: the diode operates near the limit of the reverse breakdown voltage. In passive mode, the diode is reverse biased at slightly below the breakdown voltage, in series with a large resistor R_L (typically many kΩ). In this condition, the probability that the diode generates an avalanche is extremely high. Any photon that is absorbed in the active region of the diode, or an electron-hole pair generation due to thermal excitation causes an avalanche. Avalanches generated by thermal emissions, when no photons are absorbed, produce false counts known as dark counts. This is basically noise, and causes errors in a possible quantum communication process taking place. After the avalanche current flows, the large resistor R_L causes a voltage drop on the diode removing it from the breakdown region. This quenches the avalanche and the current drops. The voltage across R_L is reduced, causing the voltage applied to the APD to rise, bringing it back to the breakdown region again, ready to generate another avalanche (Fig. 7a). There is also another small resistor in series with the APD (50 Ω) which, generates a voltage pulse. This pulse is detected by the discriminating electronics and generates an output formatted pulse that can be sent to a counter or a computer for data analysis.

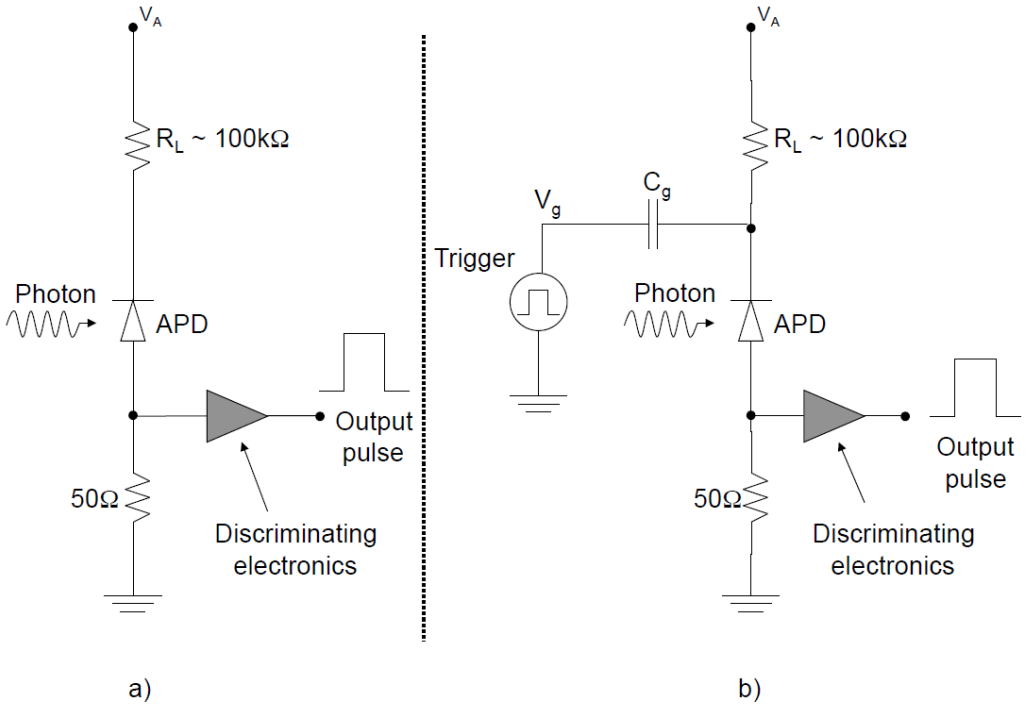

Figure 7 - Part a) shows the circuit used to detect single photons in passive mode, while part b) is the circuit for passive gated mode operation. Capacitor C_g in part b) is used to decouple the DC voltage between the circuit and the pulse generator.

APDs used in active mode employ the same basic procedure and circuit as Fig. 7a. The difference is that there is some additional circuitry to detect the avalanche, quickly pulling the APD from the breakdown region and allowing it to recover, much faster than in passive mode. Since the diode recovers faster there is a considerable performance gain [51].

Both active and passive methods are only usable when we do not know the precise arrival time of the single photons. If one wishes to employ them in a syncronized system, such as in a quantum communication scheme, then another method is necessary. It is called passive gated mode, or just Geiger mode [7]. It is depicted in Fig. 7b, and it basically uses the same circuitry as the passive mode with one small modification: a trigger (or gate) pulse is added to the bias voltage V_A. In this mode the diode is slightly above the breakdown voltage (hence, outside of the breakdown region) by adjusting V_A. A very narrow pulse (T_{FWHM} of around 2 ns) of amplitude V_g is added to V_A such that $V_g + V_A$ is greater than the breakdown voltage (Fig. 8). The APD is then inside the breakdown region for a very brief period of time. During the gate, the APD has a high probability of

generating an avalanche, whether through an absorbed photon or a thermal transition.

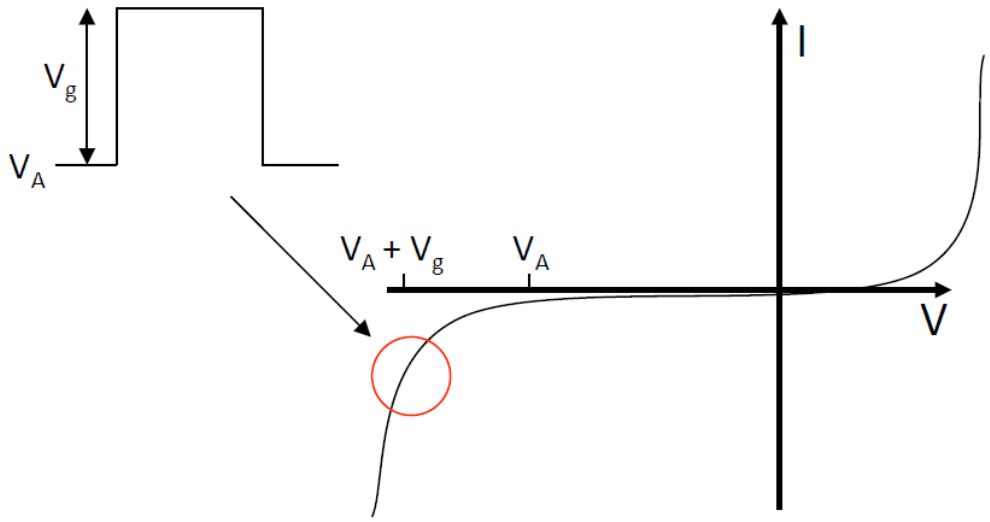

Figure 8 - Typical current-voltage curve for an avalanche photo-diode. V_A is the breakdown voltage and V_G is the amplitude of the gate pulse applied. The red circle shows where the diode is placed for the gate pulse's duration.

The clear advantage of Geiger mode is that it can be used in a synchronized scheme, since we can greatly increase the probability that an absorbed photon generates an avalanche during a brief period of time. Furthermore, the performance in Geiger mode is much better than in passive mode for InGaAs and Ge detectors [56]. The problem with Geiger mode is the afterpulsing effect, caused by trapped carriers in the semiconductor lattice, increasing the probability of a detection given that a count already occurred [51, 56]. For this reason, the upper bound for the gate repetition rate is around 1MHz for InGaAs APDs. Recently there have been considerable improvements employing much faster repetition rates with standard Geiger mode InGaAs APDs, with similar dark count and afterpulse probabilities[57, 58]. Nevertheless dark counts in detectors are the main factor limiting the distance in secure quantum communications [7]

2.6. The quantum communication channel

As discussed in the beginning of this chapter (Fig. 1) there must be a physical communication channel between Alice and Bob so that they can communicate. This holds for both classical and quantum communication systems.

They typically fall into two categories, guided and unguided media. For classical systems guided media examples are coaxial cables, twisted-pair cables, waveguides and optical fibers, while unguided typically refers to free-space connections, such as satellite, microwave radio and free-space optical links. For quantum systems this simple division also applies, however since we are currently limited to using photons as quantum information carriers, we are restricted to using optical fibers for guided media, and free-space optics for unguided.

As we shall see, one clear distinction between quantum and classical systems is that one cannot make a copy of an unknown quantum state, which is completely counter-intuitive at first glance. We make copies of information all the time, working at our computer, or perhaps just jotting down a recipe for a cake we may have seen on television. In the quantum world, arbitrary copying is not allowed, and this is one of the remarkable consequences of storing information on quantum states. It is also the main argument behind quantum cryptography (please see next section). For the same reason no broadcast communication has been done so far within a quantum communication framework.

The good news is that there is nothing fundamentally different for the channel between a classical and a quantum system. Any channel capable of sending classical optical signals is also capable of sending single photons. Therefore the standard commercial hardware used in classical optical communications, such as modulators, optical couplers, fibers, etc... may be employed in quantum systems with little or no modifications. From a commercial point of view this is outstanding, since it is possible in principle, to integrate quantum systems into existing commercial optical networks. We will discuss this point further, specially in Chapter 4.

Employing free-space as the optical channel is a good option, as long as we properly prepare the beam to keep it collimated during transmission. The main advantage of using this channel is that it is quick to assemble and run (and comparatively cheap), when there is no available installed fiber between Alice and Bob. The obvious drawback is that a direct line of sight is needed between Alice and Bob, and it is limited in the distance (in the best case) by the Earth's curvature. Nevertheless there have been quite a few experiments using free-space optics [59, 60]. They work around 780 nm to take advantage of the higher efficiency of Si APDs. One important factor to consider is the attenuation of the

channel, and in the case of these systems, it is heavily dependent on weather conditions. Fortunately, what may be a heavily attenuated channel for one specific wavelength, may not be for another one [61]. In fact, a study has shown that quantum communications in wavelengths in the mid-far infrared (4.6 μm) is possible, and it will perform better than 780 nm in certain fog conditions [62]. The main problem with longer wavelengths is that up-conversion detectors need to be used, which add considerable noise.

2.6.1. Optical fibers

Optical fibers have become very important in our lives, even if we may not be aware of it. When we send an email, talk on the phone, stream a movie on the internet or just casually browse webpages we can be sure that there is a high probability that all or part of the information is being sent and received through optical fibers. Their extremely high capacity to carry information has enabled them to become the main communication channel nowadays, for high-density traffic.

An optical fiber is basically a dielectric cylindrical waveguide composed of silica. Its basic structure is composed of a core where most of the light is guided, and a cladding wrapped around the core [63] (Fig. 9). Both the core and the cladding are made of silica, however they are doped during the fabrication process in a slightly different way such that the refractive index of the core is slightly higher than the index of the cladding. It is obviously higher in order to guide the light, but the reason why it is only slightly higher is to minimize dispersion of the light signal [64]. It is possible to change the refractive index profile in the core $n(x,y)$ (propagation is along the z direction) during the fabrication process, and this gives the fiber many of its light propagation properties [63].

For us there is one property which is of particular interest: the radius of the core. This value will determine, for a particular wavelength, if the propagation of the signal is single or multi-mode. Older optical fibers have a 50 μm diameter core, which supports the propagation of many modes. Each mode has a slightly different frequency, which leads to multi-modal dispersion and has severely limited the transmission rates and distance of early lightwave systems [63]. They are not good for quantum communications either, as the different modes couple easily acting on the qubit, causing decoherence [7].

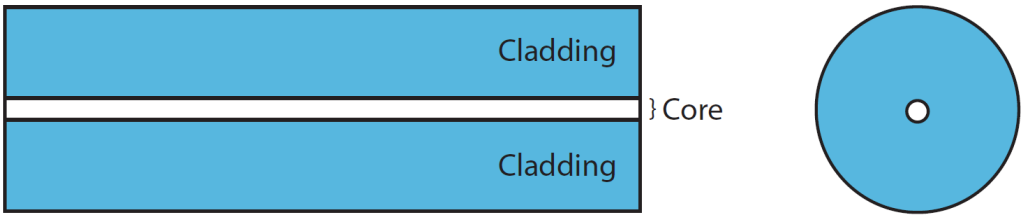

Figure 9 - Basic optical fiber structure. The protection coatings have been omitted from the figure. Right part is simply the profile view of the fiber.

Newer fibers have much smaller cores, to support single-mode propagation. Standard single-mode telecom fibers (SMF-28) have a core diameter around 8 μm, for operation at the wavelength of 1550 nm. They support single-mode operation for wavelengths as low as 1200 nm, after which they become multi-mode. Fortunately, for some quantum optics applications, commercial single-mode optical fibers are available for visible light.

The attenuation of an optical signal inside the fiber is dependent on its wavelength. There have been three main operating wavelengths for telecom applications since optical fibers were developed: the first window was around 800 nm, since the first semiconductor light sources and detectors operated in this region. The loss is around 2 dB/km in this region. At 1300 nm, the loss is 0.35 dB/km, and when sources and detectors appeared in this wavelength, there was a considerable improvement. However the lowest loss is at 1550 nm, (0.2 dB/km), and the entire optical communications industry works in this region today. It also happened that optical amplifiers based on erbium doped fibers also work at 1550 nm \[64].

The index of refraction is wavelength dependent, therefore any real signal of finite bandwidth will disperse as it propagates along the fiber. This phenomenon is known as chromatic dispersion and it is a limitation for classical communication systems. Its effects can be reduced by using light sources with narrower linewidths, or working on regions of the fiber with lower dispersion (SMF-28 fiber has zero-dispersion around 1310 nm). Chromatic dispersion can also be compensated with short pieces of special fibers with high negative dispersion coefficients [64]. For quantum communication using weak coherent states generated from semiconductor lasers, chromatic dispersion is not an issue, since the bandwidth of the source is very small, and the distances involved

(typically 150 km max) are relatively short. For SPDC sources, it can be a problem since the bandwidth can be quite large (tens of nanometers) [7].

There is one final issue with optical fibers that is of critical importance for quantum communication. When they are fabricated optical fibers are never perfectly cylindrical, therefore they display slight asymmetries in their geometrical structure. This residual asymmetry leads to birefringence along the fiber. The resulting birefringence at a position *L* along the fiber depends on how asymmetric the fiber is at that particular place. Therefore residual birefringence changes randomly throughout the length of the fiber cable. Birefringence changes the state of polarization (SOP) of an optical signal, because of the delay introduced by the index variation between two orthogonal polarization components of the signal. We can then say that the input state $|H\rangle$ will come out as $|Random_{SOP}\rangle$ at the end of an optical fiber. So far this does not look like a major problem, since we could just place a manual fiber polarization controller (a set of half-wave plates and a quarter-wave plate) at the end of the fiber to undo the rotations caused on the light signal, and transform $|Random_{SOP}\rangle$ back into $|H\rangle$.

Unfortunately birefringence created from asymmetries during fabrication do not remain unchanged forever, as any mechanical forces to the fiber cause changes to the local birefringence. Basically any forces upon the fiber, like twisting or bending, change the output polarization state. In fact, just moving a small piece of fiber on the workbench during an experiment is enough to completely change the SOP! Any experiments with optical fibers that are dependent on the polarization state, must be performed with the utmost care that the fiber is not touched after the experiment is aligned. Still, this looks like an easily remedied situation, in most cases, as we could run the experiment with the entire fiber fixed, and just use a manual polarization controller at the end of the fiber like mentioned before.

What actually restricts the use of manual polarization control is that temperature also changes the birefringence of the fiber. Therefore, in practice, it is impossible to have the fiber birefringence unchanged as a function of time. We should change our output polarization state to $|Random_{SOP}(t)\rangle$ to indicate that it is time dependent. A simplified picture of the problem is shown in Fig. 10. Clearly,

this presents a major impairment for quantum communication, as long as the polarization degree of freedom of the single photon is used to encode information. An experiment in which polarization based quantum communication is implemented was performed in this thesis, using a fiber with active stabilization. We will return to this problem in chapter 5. More comments on optical fibers will be made in chapter 6 in the context of the impact of noise generated from Raman scattering inside a fiber, by a classical optical channel operating at a different wavelength than the quantum signal.

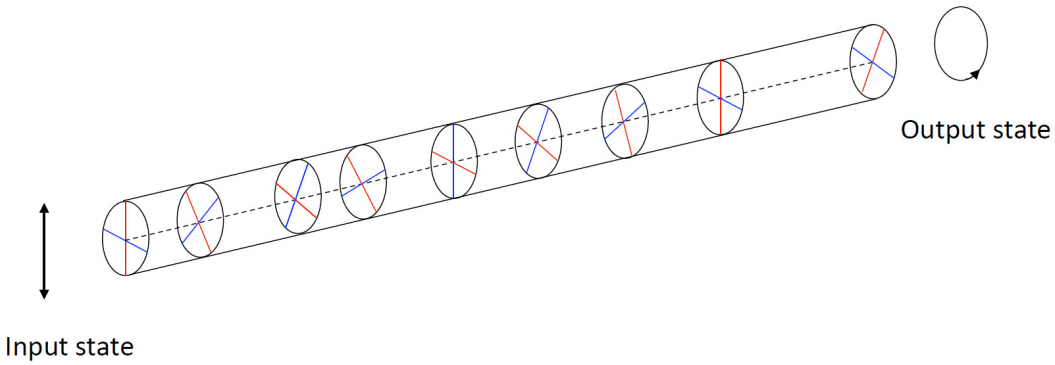

Figure 10 - Birefringence in an optical fiber is a function of mechanical stresses and temperature fluctuations along its length, causing random polarization rotations of an input polarization state. We see in the figure for example, a vertical state randomly transforming into a circular state after propagation.

Even though there were transmissions using polarization encoding in optical fibers in the past [65], phase encoding [66,67] quickly became the dominant form of transmission [68,69].

2.7. Quantum Key Distribution

Since all experiments performed in this thesis deal with Quantum Key Distribution (QKD) it is worth giving a brief explanation of how it works. QKD (also called quantum cryptography) was based on initial ideas by Stephen Wiesner on how to make money impossible to counterfeit using spin qubits, somehow stored on the bills themselves [70]. Charles Bennett and Gilles Brassard, took upon these ideas and developed a protocol to share cryptographic keys between two remote parties with absolute security, built upon the laws of quantum physics [71].

Cryptography is the science of encrypting information before transmission through a communication channel, such that, if this information is intercepted by someone else than the intended receiver, the intercepted message is unintelligible. The intended receiver has a decoding key, which allows him to recover the original information upon reception of the encrypted message. The algorithm to encrypt the message may be known, however without the decoding key, the eavesdropper has no way (ideally) to decode the message.

For the moment, let us assume that the same key can be used to encrypt and decrypt the message, and as we will see this is the case for quantum cryptography. The main issue here is how can both the transmitter and receiver (henceforth referred to as Alice and Bob respectively) agree on an encrypting / decrypting key prior to the information exchange. From a security point of view this is not a trivial matter. There is no way that Alice can send the key to Bob with 100 % confidence that the message will not be read. In fact this is a feature of classical information theory because information can be copied at will without destroying the original content. Therefore the most secure way that they can perform the key exchange is if they meet in-person. If they have never met before, this is clearly a problem as they need to be sure that a spy (we shall call her Eve from now on, following the trend in all QKD literature) is not taking the place of Alice and Bob. Some form of authentication is thus required (this is true for all cryptographic protocols, classical or quantum). Even if Alice and Bob know each other, an extremely clever and ingenious Eve could be using a perfect disguise and fool one of the parties. This is the most remarkable feature of Eve, we always assume she is infinitely smart and has access to technology that ordinary human beings have not even heard of (Eve is, of course, still limited by the laws of physics.

One of the simplest cryptographic algorithms, called Vernam's cipher, is also fully secure [5]. It can not be cracked independently of what Eve does, however there are three conditions for absolute security. First, the encrypting / decrypting key must be truly random and as long as the message itself (if the message consists of 1 million bits, then the key must be 1 million bits long). The randomness requirement can be solved with available quantum random number generators (we shall discuss this in detail in chapter 4). The second requirement is that, in order for Vernam’s cipher to be secure, the key can only be used once. Therefore, if we wish to send a second message consisting of 1 million bits,

another key of 1 million bits must be generated and shared. The final requirement is that clearly, Alice and Bob must share the same key prior to transmission.

The cipher goes as follows: Alice generates a random key (private key) the size of the message she intends to send to Bob in the future. She somehow securely shares a copy of the key with Bob. She performs a logic XOR operation (modulo-2 addition) bit by bit of the message she intends to encrypt with the key, obtaining the encrypted message, which is sent to Bob through the communication channel. Bob receives the encrypted message, and in possession of his copy of the private key generated by Alice, simply performs the same XOR operation bit by bit, decrypting the message (Fig. 11).

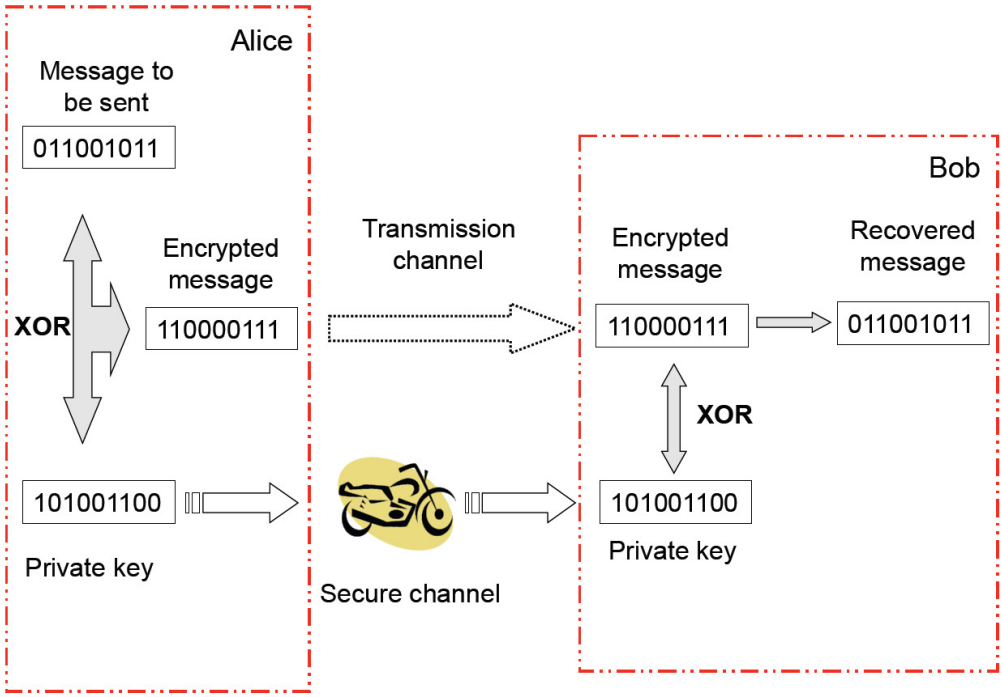

Figure 11 - Scheme of Vernam's cipher. Note that we used a trusted courier as the secure channel here, which in principle is not a good choice. Adapted from [72].

Vernam's cipher although simple has been proven to offer *unconditional security* [5, 7], as long as the three requirements mentioned above are met. Requirements one and two are not an issue at all, they can be dealt with. The problem is the final requirement, how can Alice send a copy of the key to Bob knowing that no one has tampered with it? Note that no classical method of transmission can absolutely guarantee this, not even meeting face to face. It is always possible that Eve comes up with a clever way of fooling the key delivery

system, no matter how sophisticated or fool-proof it might seem. The answer lies within quantum physics.

2.7.1. No-cloning theorem

Let us say that we would like to clone an arbitrary unknown qubit. This is a perfectly possible operation with a classical bit, so it should be possible to realize on a quantum system. For someone not familiar with quantum physics it is very surprising that in reality, an unknown quantum state cannot be cloned [73].

Let us assume that we have a perfect cloning machine [5]. And that we would like to clone the two orthogonal quantum states $|0\rangle$ and $|1\rangle$. Our cloning machine works as follows:

$$|0\rangle|\mathit{Initial}\rangle \rightarrow |0\rangle|0\rangle|\mathit{Final}_0\rangle \tag{2.16}$$

$$|1\rangle|\mathit{Initial}\rangle \rightarrow |1\rangle|1\rangle|\mathit{Final}_1\rangle \tag{2.17}$$

$|\mathit{Initial}\rangle$ and $|\mathit{Final}_{1,0}\rangle$ are the initial and final states of the cloning machine respectively. What Eqs. (2.16) and (2.17) show is that the cloning machine takes the input states $|0\rangle$ and $|1\rangle$, preserves the original and creates a copy on the output, with the machine ending the cloning procedure at state $|\mathit{Final}_{1,0}\rangle$. So far this seems to work. Let us try copying the state $a|0\rangle + b|1\rangle$ which is in an arbitrary linear superposition of the two orthogonal states $|0\rangle$ and $|1\rangle$:

$$(a|0\rangle + b|1\rangle)|\mathit{Initial}\rangle \rightarrow a|0\rangle|0\rangle|\mathit{Final}_0\rangle + b|1\rangle|1\rangle|\mathit{Final}_1\rangle \tag{2.18}$$

where we simply used the linearity of quantum physics [73]. This is, however, not the same state as what the cloning machine should do:

$$(a|0\rangle + b|1\rangle)|\mathit{Initial}\rangle \rightarrow (a|0\rangle + b|1\rangle)(a|0\rangle + b|1\rangle)|\mathit{Final}\rangle \tag{2.19}$$

We can conclude that no perfect cloning machine exists for an arbitrary unknown quantum state, however it is possible to clone orthogonal states. The fundamental concept for QKD comes from this fact.

The no-cloning theorem tells us that it is not possible to make copies of quantum states at will. And what if we use quantum states to share the key between Alice and Bob in the Vernam's cipher? Not even Eve can violate the non cloning theorem as she would need to violate the laws of quantum physics themselves! This is the basic idea behind Quantum Key Distribution. Its name comes from the fact that it is a protocol to securely distribute keys for the Vernam's cipher. In fact, as we will see, the quantum transmission is only a part of the entire protocol, though a crucial one.

Quantum cryptography is different from all other cryptographic schemes, because it relies on physical principles, instead of mathematical ones. Vernam's cipher, although fully secure, is not a practical scheme for most uses due to the key sharing problem. Other cryptographic schemes based on difficult mathematical problems were developed to be used in less-sensitive applications, such as on-line banking and shopping. One of the most popular is the RSA, based on the difficult-to-solve prime number factorization problem [5]. RSA is widely used because it manages to use a public-key scheme, different from Vernam's private key, solving the key-sharing problem with the difficult problem of prime-factorization. As said above, the problem of cracking the code is difficult to solve but not *impossible.* RSA is vulnerable to increasing computational power, which according to Moore's law, roughly doubles every 2 years [74]. Furthermore an algorithm (Shor's) has been developed for factorization of prime numbers, if the processing is done on a quantum computer [9]. It is worth noting that many modern cryptographic schemes used today (in many cases that we are not even aware of) are based on RSA. The development of the quantum computer poses a considerable threat to classical cryptography. Fortunately for QKD, security proofs have been drawn even when facing attacks from an eavesdropper equipped with a quantum computer [5,7].

2.7.2. BB84

QKD revolves around a protocol called BB84, named after its inventors Bennett and Brassard [71]. As in the original proposition, polarization encoding will be used in the explanation, as it is also simpler to visualize. As explained before most modern QKD systems employ phase coding to avoid the problems caused by random birefringence changes in the fiber. Another reason to start with BB84 to explain QKD is that it is still widely used today, although there have been modifications to improve it.

Alice generates a random number of the same size of the message to be transmitted, using a quantum random number generator (QRNG) [75]. A QRNG uses a quantum process (which is truly random) to generate random numbers, a common example is sending a single photon through a beamsplitter, and observing to which output port it exits. The topic of QRNGs will be discussed thoroughly in chapter 4.

She uses four linear polarization states to send each bit: $|V\rangle$, $|H\rangle$, $|+45\rangle$ and $|-45\rangle$, corresponding to the linear polarization states vertical, horizontal, +45º and -45º respectively. The idea is that she has two bases with maximum overlap: the rectilinear basis V / H, and the diagonal basis +45º / -45º, and she chooses one of them for each transmitted qubit. She proceeds in the following way: each bit of the generated random sequence (this is the key to be sent to Bob) gets randomly assigned to one of the two bases with a 50\% chance for each one. Depending on the bit value, 0 or 1, one of the two states of the basis is prepared and sent. The correspondence between states and logical levels is chosen, for instance so that in the rectilinear basis H corresponds to 0, V corresponds to 1, and in the diagonal basis, -45º is 0 and +45º is 1.

The QRNG sequence is used create the bits forming the random key and to choose randomly between the bases. This assignment is shown in the table below:

Random bits	State	Bit sent
00	H	0
01	V	1
10	-45º	0
11	+45º	1

As we will see below, we employ the two different bases to fool Eve. Alice then encodes each bit of the key according to the table above using a polarization modulator (e.g. a half-wave plate) on a single-photon from her source. For the sake of this explanation let us assume that she has a perfect single-photon source. The photons (with the encoded random bits) are sent to Bob through the communication channel (free-space or optical fiber). When Bob receives the photons, he must randomly choose between the rectilinear and diagonal measurement bases, for each photon received, *independently from Alice.* He needs a random number generator of his own for this task. This point is crucial, Bob must be able to choose his basis in a totally unbiased and independent manner. To continue with the protocol, Alice and Bob need a classical communication channel (it can be public) between them. Since the channel has losses, not every photon will be detected by Bob and he uses the public channel to inform Alice which photons he has detected, and which basis he has chosen. The entire system is synchronized and each qubit sent has an unique time stamp for identification. Eve is perfectly capable of listening this communication (since it is classical) and it is not a security problem, as long as the channel cannot be modified.

Alice then discards each bit that Bob measured in a basis different from the one she sent, and keeps those that Bob used the same measurement basis. She tells Bob the time stamps of the bit she is keeping and likewise he discards all other bits other than the ones Alice kept. Because of the way a measurement works in quantum physics, Alice and Bob know that if they used different bases for preparation and measurement, then they cannot be sure if Bob's measured bit is the same that Alice sent. Only when the bases are the same Alice knows that Bob received the same bit she prepared (not taking into account imperfections and errors yet).

Let us now analyze what Eve can do. Her objective is to read the key while it is being transmitted, so she can later intercept the encrypted message, decrypt it and obtain the information Alice is attempting to send to Bob. She has perfect equipment and advanced technology, but she cannot bend quantum physics laws. Each bit of information Alice prepared and sent is encoded on a single photon, which Eve intercepts and measures. After measurement the single photon is lost, and Eve must send a new one to Bob (two identical photons in every degree of freedom are indistinguishable) to mask her presence. How does Eve choose to

measure the polarization state of the single photons? Remember that one cannot measure a quantum object arbitrarily. Even if she knows that Alice is preparing the single photons in the rectilinear and diagonal bases, Eve needs to choose between one of them to perform a correct measurement. Since Alice is using a *quantum* random number generator that Eve has no access to, she must guess which basis Alice chooses for each photon. On average, Eve will succeed half of the times. When a wrong basis is used, Eve has a 50 % chance of measuring the photon incorrectly (Each photon in the opposite basis, will be at an angle of 45º with the axis of the other basis, thus having a probability of $\cos^2 45 = 1/2$ of going to either port of the polarizing beam splitter). Therefore if Eve intercepts and resends each single photon transmitted, she causes a 25 % error rate in the transmitted string [7]. The general idea of the BB84 protocol is summarized in Fig. 12.

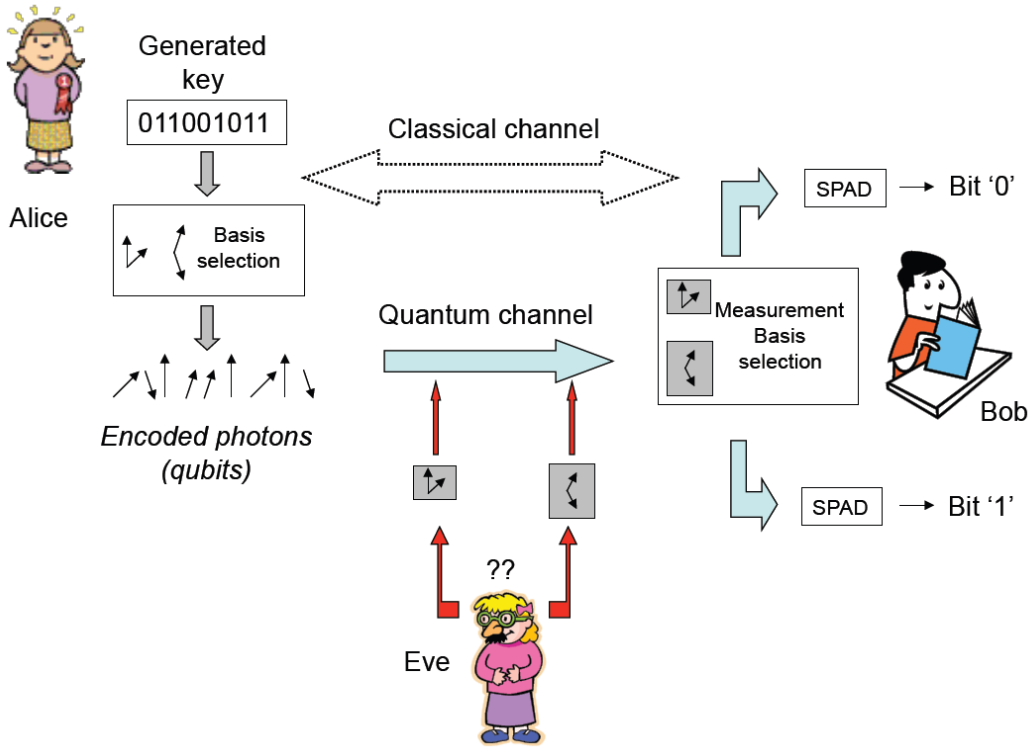

Figure 12 - BB84 protocol. PBS: Polarizing beam splitter. Adapted from [72].

The process that Alice and Bob undertake to verify which bits should be kept according to the bases used, is called basis reconciliation. Following it, they sacrifice some of the bits, by verifying them over the public channel so that the error rate can be measured and Eve's presence tested. If there is no detection of Eve, they follow on through an error correction process (to remove errors coming

from imperfect optical components, detectors dark counts, etc...) in which more bits have to be lost, and finally privacy amplification, a procedure to reduce any information Eve may have gained (she may have only measured a few photons keeping her presence below the error threshold) [76]. Privacy amplification is also a process that needs to discard more bits. In the end, Alice and Bob end up with a key, that is much shorter than the original one Alice transmitted, but they can be sure that Eve has no knowledge of it.

There are general security proofs for QKD for many different types of attacks, and in many different situations [7]. The quantum bit error rate threshold (QBER, essentially the same as bit error rate, that is total number of wrong qubits / total number of qubits) that Alice and Bob can still distill a secure key in spite of Eve's attacks is approximately 11 %, assuming coherent attacks using a quantum computer. As long as the QBER is below this value, Alice and Bob can still obtain a secure key, while successfully using privacy amplification to reduce Eve's information to zero. Obviously any reliable QKD system must therefore operate at QBER values considerably lower than 11 % in the absence of Eve. Properly aligned systems with reasonable transmission distances, typically have QBERs of 1-2 %. The maximum secure distance obtained is limited mainly by the dark count probability of the detector, since a decrease of the probability of a photon successfully arriving on the detectors reduces the signal to noise ratio, increasing the QBER [7].

3
Integration within Classical Networks and the Decoy State Implementation

Both experiments explained here were performed during the author's stay with Anders Karlsson's group at KTH between July 2006 and December 2007. They were both based on single-photon sources from spontaneous parametric down-conversion processes in Periodically Poled Lithium Niobate (PPLN) crystals. The first one uses an entangled source of photon-pairs owned by Alice, with one photon detected locally, and the other one transmitted through 27 km of single-mode fiber to Bob. The other key feature of this experiment was that the synchronization classical channel was implemented in the same fiber as the single photons with a channel separation of 0.8 nm. The other experiment employed a heralded single photon source in a QKD experiment using phase coding and the decoy state modification. It was the first experiment to use a sub-poissonian single-photon source with the decoy state protocol.

3.1. Narrowband entangled photon pair source used in a DWDM environment

A practical feature of quantum communication is that we do not need anything other than common commercial optical fibers to use as the quantum channel between Alice and Bob. This is a major advantage to deploy quantum communications in commercial environments since we can use the fibers already installed between two different locations. In order to optimize the use of available resources, classical optical systems typically employ Wavelength Division Multiplexing (WDM) such that each channel (centered each at, λ_1, λ_2,… λ_n) occupies a finite bandwidth. Many modern systems work in a DWDM environment (Dense Wavelength Division Multiplexing) with a channel spacing of 0.8 nm at 1550 nm. It is a quite common practice for the operator who owns the fiber to rent just a single wavelength channel, if the renter desires, such that maximum usage is obtained. Modern filters based on fiber Bragg gratings (FBGs)

or array waveguide gratings (AWGs) ensure that each channel does not interfere with the other. Care must still be taken with non-linear effects happening in the fiber based on the $\chi^{(3)}$ non-linearity, such as four-wave mixing (FWM) and Cross-phase modulation (XPM) [77].

It is therefore, of practical interest, to be able to send quantum signals alongside classical channels inside an optical fiber, since it is more feasible in a commercial sense, to use an optical fiber populated with live traffic, than to require a dark fiber for a quantum communication session. There is another reason to share the quantum communication with classical signals in the same fiber, as both Alice and Bob need to be synchronized. As mentioned in the end of chapter II each qubit sent needs to have a time stamp, and for this matter, the clock signal generated by Alice has to be sent to Bob. In addition to that, the clock signal is normally used to gate the InGaAs SPAD operating in Geiger mode (as it is usually the case for 1550 nm quantum communications). One other reason to multiplex classical and quantum channels in the same fiber would be to implement active polarization control [78]. In this case two channels are required to be used as feedback for the control system. We shall return to this point in Chapter 5.

The source is an improved version of previous efforts by the KTH group on this subject [79,80]. It is a polarization-entangled source of photon pairs, employing two PPLN crystals in an H-V configuration [41], each one being 50 mm long [81]. The motivation for the use of long crystals is to obtain a higher photon pair generation rate, which is proportional to $\sqrt{L}$, and a narrow emission bandwidth, proportional to 1/*L*, where *L* is the crystal's length [82]. To the best of our knowledge this was the first time such long crystals were used in this configuration.

The source is depicted in Fig. 13. We employ a continuous-wave Nd:YAG DPSS (diode pumped solid state) laser, emitting at the wavelength of 532 nm. This laser has an internal laser diode at 808 nm used to pump a Nd:YAG crystal, which generates 1064 nm light, then passing through a non-linear crystal (KTP typically) and gets frequency doubled to 532 nm through second-harmonic generation. The laser beam output goes through a BG39 short-pass filter, to eliminate any residual emission at 808 nm from the diode laser pumping the Nd:YAG crystal, which would be catastrophic to this experiment, as the crystals

are quasi-phase matched for the conversion $532 \rightarrow 809 + 1555\,\text{nm}$. Any photon generated from the pump at 808 nm could be successfully detected degrading the correlation between photon pairs. After the filter we use a half-wave plate (HWP) to rotate the linear polarization of the laser beam.

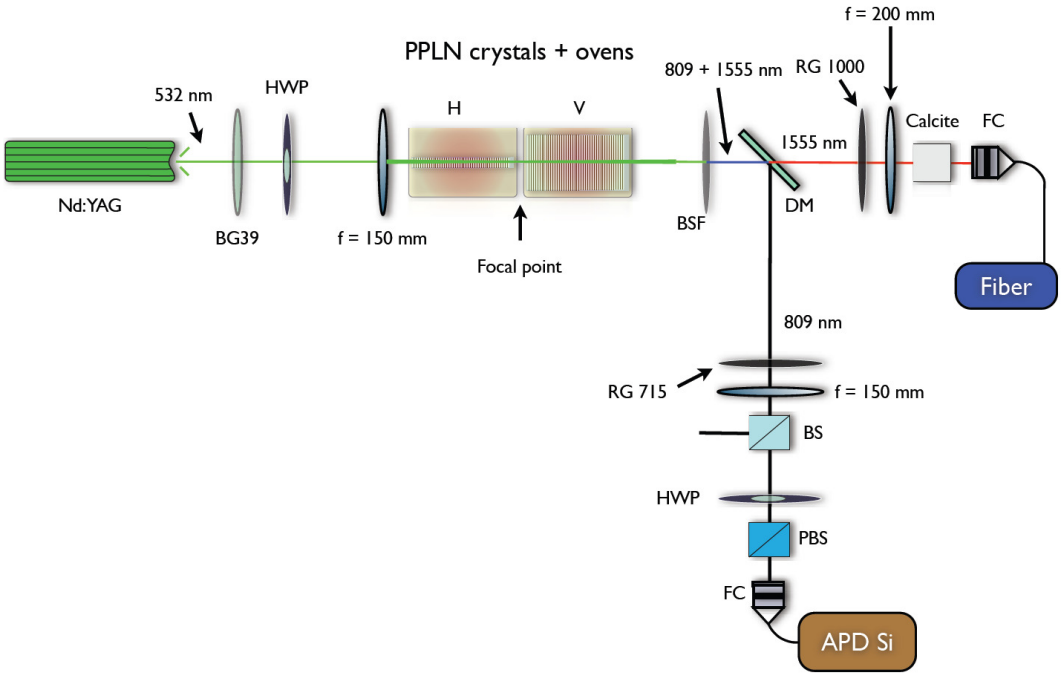

Figure 13 - Entangled single-photon pair source used in the DWDM experiment. HWP: Half-wave plate; BSF: Band-stop filter; DM: Dichroic mirror; BS: Beamsplitter; PBS: Polarizing beamsplitter; FC: Fiber coupler.

The light is rotated to 45º to generate equal probability of conversion in each crystal (since one crystal axis of conversion is oriented in the H direction, and the other in the V direction), and passes through an achromatic doublet lens (focal length = 150 mm) to focus the pump in the middle of both crystals. The crystals generate collinear type-I down-converted light, giving the advantage of better coupling to optical fibers than the cone-like emission in some type-II sources [35]. After the crystals a band-stop filter (BSF) is inserted to remove the pump photons. A dichroic mirror (DM) is used to split the down-converted wavelengths, so that each one may be properly coupled to single-mode fibers. The 809 nm photons are detected by Si APDs (Perkin-Elmer) with 60 % quantum efficiency, operating in passive (free-running) mode. The 1555 nm photons are transmitted via 27 km of SMF-28 (Standard) single-mode telecom fiber to Bob. A home-made InGaAs SPAD module (using an avalanche diode from Epitaxx) with

18\% quantum efficiency working in Geiger mode, is gated by a detection occurring in Alice's Si APD.

The quantum state generated by the source is [81]:

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|V(\omega_s)\rangle|V(\omega_i)\rangle + e^{i\varphi}|H(\omega_s)\rangle|H(\omega_i)\rangle\right) \quad (3.1)$$

and $\omega_i + \omega_s = \omega_p$ must be satisfied. ω_p, ω_i and are the frequencies of the pump, idler and signal respectively, and φ is the total phase difference between two polarization components.

The 809 nm photons are locally analyzed by Alice using a passive beamsplitter, to perform the basis choice, and a combination of polarizing beam splitters. The entire analyzing setup is not indicated in Fig. 13, but one extra PBS is missing in the 809 nm arm, which would be connected to the other output of the BS. Also one more half-wave plate is needed on the other arm to convert the D/A (+45º/-45º) basis back to H/V. Four detectors are also needed, two at each PBS. We analyze the state manually rotating the half-wave plate just before the PBS in the idler arm, as indicated in the figure. The down-converted wavelengths can be slightly tuned by changing the temperature of the ovens containing the crystals.

After the down-converted photons are split by DM, they need to be focused into single-mode optical fibers. Because of the input focusing length, the beams are diverging at the output of the crystal and need to be collimated before going through all other components. Because of the different divergence of the beams, different lenses were used, (f_s = 200 mm and f_i = 150 mm), so that each collimated beam gets coupled with a focusing angle matching the numerical aperture of the fibers. In order to remove any residual pump photons that did not get blocked by the BSF filter, we use additional filters in each arm (RG 715 for the idler and RG 1000 for the signal). As mentioned before the 809 nm photon goes through a BS, then a HWP-PBS combination to analyze the state. The photon is finally coupled to a single-mode fiber through FC (containing a short focal length aspheric lens, a fiber holder and a multi-axis translation stage).

A block of calcite is placed on the 1555 nm arm, to compensate the chromatic dispersion generated in the crystals from the fact that the generated wavelengths are so different. In the second crystal V(809) and V(1555) photons

are generated and will separate in time. In the first crystal H(809) and H(1555) photons are emitted, which go through the second crystal generating further dispersion. The net result is that the delay between H(809) and H(1555) is 11 ps larger than the one between V(809) and V(1555) [81]. We use the calcite then, to slow down V(1555) with respect to H(1555), so that the delay between V(1555) and H(1555) with respect to their corresponding idlers is the same. The time of 11 ps is comparable to the calculated 16 ps coherence time of the down-converted photons, which leads to a 75\% visibility decrease in the D/A basis compared to the H/V basis [81]. The piece of calcite gives a 15 ps group delay difference between H and V components, therefore we use a 3-meter long piece of polarization maintaining fiber (PMF), giving a -4 ps group delay difference (slow axis of PMF is aligned to fast axis of calcite). The PMF also allowed us to fine tune the phase difference φ between the two polarization components, by applying a local mechanical strain to the fiber. The PMF is not shown in Fig. 13 for the sake of clarity.

One issue that was discovered about the source employing long crystals is the temperature instabilities between the two ovens. This causes drifts of φ as a function of time due to refractive index changes. These drifts are proportional to the crystal length, and therefore we have severe constraints in that respect since we are using long crystals. It was calculated that a temperature drift of 0.1ºC results in a phase shift between signal and idler polarizations of the order of π, destroying the correlations in the diagonal basis. Our temperature control system, along with isolation of the two crystals inside a transparent box to stop airflow in the room, was just enough to keep the system stable to perform the measurements (several minutes). In order to improve the stability of the source, it would be necessary to replace it by a single-crystal setup [83,84].

In Fig. 14 the entire experimental setup is shown. The signal photon (809 nm) is coupled into a single-mode fiber and detected by a passive-gated Si based APD (Perkin Elmer SPCM AQR-14). Upon successful detection, the Si APD outputs a short electrical pulse (approximately 30 ns wide, 3V amplitude) that goes through a delay generator (DG), which is also used to shorten the pulse width to 10 ns, and then is used to modulate a DFB (distributed feedback laser) with an EA (electro-absorption) modulator built-in (15 dB extinction ratio and 2.5 GHz bandwidth). Each incoming electrical pulse generates an optical one (trigger

signal) with 10 ns width at 1555.75 nm (the laser center wavelength). A circulator (C) and fiber Bragg grating (FBG) centered at the laser wavelength is used to provide additional filtering to remove amplified spontaneous emission (ASE) from the laser. We did not have the FBG installed in the beginning as we only found out that the filtering provided by the wavelength division multiplexers was insufficient when the complete setup was running. In order to relax the filtering requirements we shifted the trigger pulse in time by 50 ns using the delay generator. The signal passes through a single WDM filter module (working as a band-pass filter with 0.5 nm full width-at-half maximum - FWHM, and 0.2 nm flat-top bandwidths), and is then multiplexed at another WDM module with the 1555 nm photon coming from the source (already coupled to single-mode fiber). The 1555 nm photon goes through a 100 m long optical delay consisting of a single-mode fiber cable. This delay is the fiber cable linking the two labs (although located next to each other) where Alice and Bob were located.

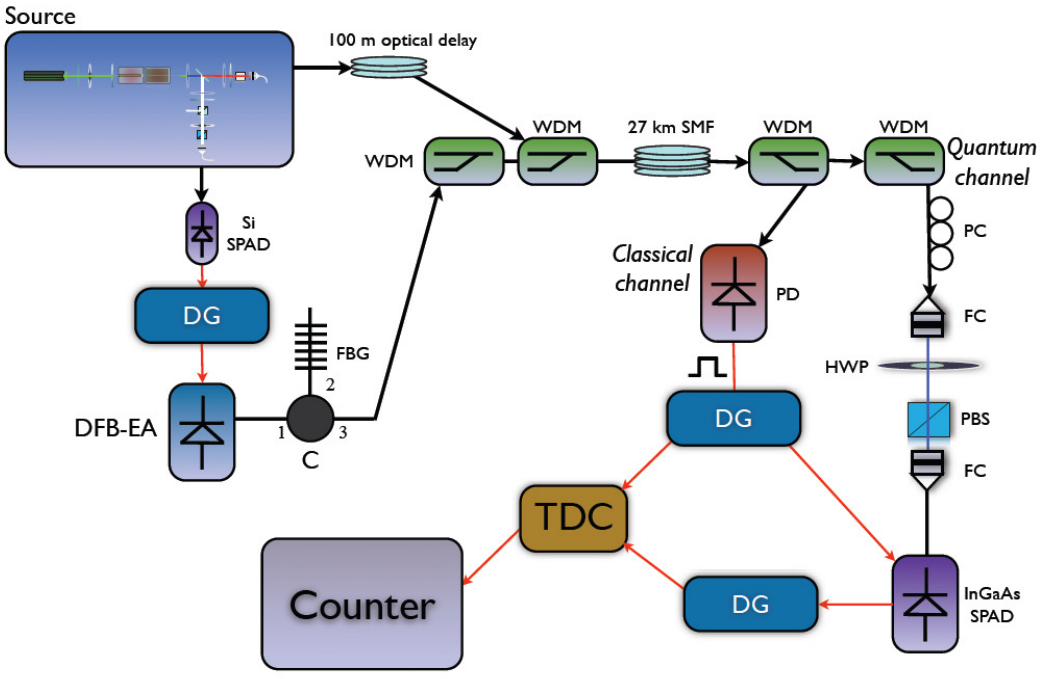

Figure 14 - Complete experimental setup. SPAD: Single photon avalanche detector; DG: Delay generator; DFB-EA: Distributed feedback laser with electro-absorption modulator; FBG: Fiber Bragg grating; WDM: Wavelength division multiplexer; SMF: Single-mode fiber; PC: Polarization controller; PD: Photo-diode; TDC: Time-discriminator circuit. Black lines represent optical fibers, red lines account for electrical connections, and the blue one is free-space.

Both the quantum bit, and the classical pulse are transmitted through 27 km of single-mode fiber, and go through another pair of WDMs working as demultiplexers this time. The classical pulse is reflected in the first WDM, while the quantum signal goes through the other WDM for extra filtering. The classical pulse is detected by a home-made photo-diode (PD, bandwidth of 1 GHz), and its output pulse is connected to another channel of our DG. The 1555 nm photon goes through a manual polarization controller (PC), and a fiber coupler with a collimator before passing a half-wave plate, a PBS and back to fiber again through another coupler. This is done so that the single-photon polarization can be analyzed. The polarization controller is used to adjust the incoming polarization state so that it is linear before going through the HWP. The single photon is then connected to the InGaAs SPAD, which is triggered by one of the outputs of the DG conditioned by the classical trigger pulse. Finally the output of the InGaAs detector passes another channel of the DG, and is connected to one of the inputs of a time-discriminator circuit (TDC) we built to artificially narrow down the gate window. The TDC essentially performs the AND logical operation, with the output of the InGaAs APD and the output of the delayed version of the the trigger pulse (as shown in Fig. 14). Since in a SPDC source, the signal and idler are strongly correlated in time, we can be certain when we should open the detection window (compare this with a weak coherent pulsed source, where the single photon can be anywhere within the attenuated pulse). What we do is to use an AND operation with both pulses, with a smaller overlap between them than the 2.5 ns minimum gate window of the InGaAs APD, through the proper adjustment of the DGs. The price to pay is the loss of some photons (around 20 % for an effective gate window of 1.5 ns), however we simply increased the pump power to compensate. We saw a benefit of a few % gain in all visibility measurements in coincidence counts between signal and idler when using the TDC.

Initially we perform a measurement with only one crystal pumped (although the entire source was aligned, e.g. the focal point of the pump beam in between the crystals), and connected the InGaAs SPAD to detect the 1555 nm photons directly after the fiber coupler at Alice's side. The maximum rate of detection of photon pairs with only the V crystal pumped at a power of approximately 3 mW is $R_c = 25 \times 10^3\ s^{-1}$, with the single count rate at 809 nm $R_s = 0.8 \times 10^6\ s^{-1}$, yielding a conditional detection probability R_c / R_s of around 3 %.

Taking into account the quantum efficiency of the InGaAs SPAD (18 %), we have a corrected probability of detection of 16 %, with no WDM filters present. We measure the accidental (uncorrelated) count rate by triggering the InGaAs SPAD with an external clock at the same single frequency, and we obtained R_a = 0.9 x 10^3 s^{-1}, giving a raw visibility of $V_v = (R_c - R_a) / (R_c+R_a)\$ = 93 %. The spectrum at 1555 nm of the down-converted photons is obtained using an optical spectrum analyzer in place of the InGaAs detector, employing a long integration time and pumping the crystal with maximum power (Fig. 15).

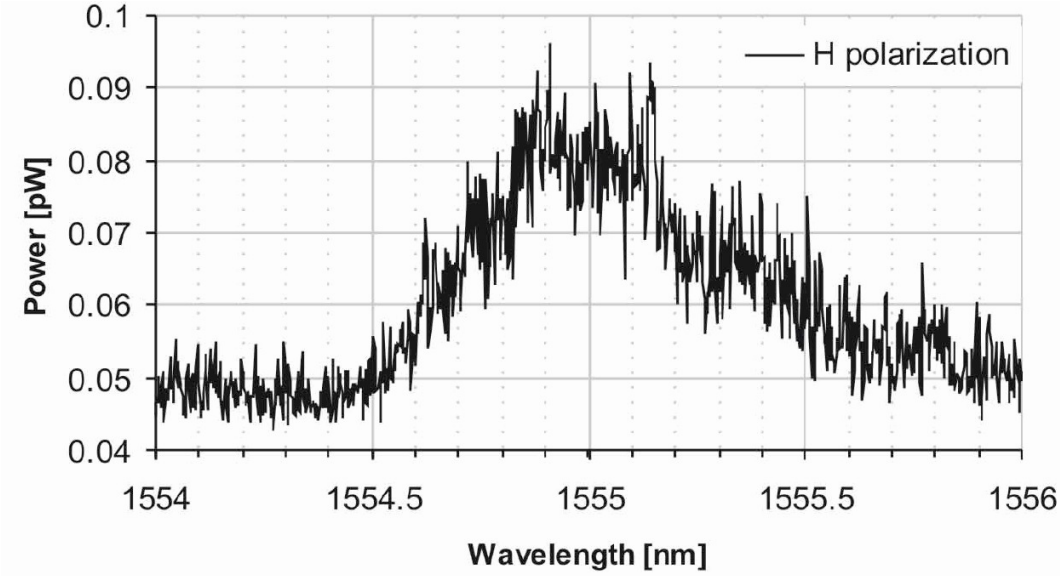

Figure 15 - Spectrum for the 1555 nm down-converted photons, obtained for horizontal polarization without conditional gating at 809 nm. The FWHM is approximately 0.8 nm. Background is the noise level from the optical spectrum analyzer.

For the next step, we pump both crystals (rotating the pump's polarization so that both crystals generate down-converted photons) with the entire setup connected and we measure the visibility curves by using the 809 nm photons as triggers and detecting the 1555 nm ones as a function of Bob's HWP angle with the 100 m fiber cable in place of the optical link (Fig. 16). Synchronization of the system is done by means of an electrical coaxial cable, and a delay generator. The incident pump power on the crystals was of about 4 mW, single count rate of 1.1 x 10^6 s^{-1} at 809 nm and only one WDM filter was used. The coincidence rate R_c dropped by a factor of about three, due to losses in the WDM, and the insertion loss in the free-space polarization analyzer at Bob's side. Measured raw visibilities for each of the four possible polarization states of the signal (809 nm) were V_H =

94 %, V_V = 90 %, V_D = 87 % and V_A = 89 %, for H, V, D and A polarizations respectively. The average predicted QBER from the four visibility curves is 5 %.

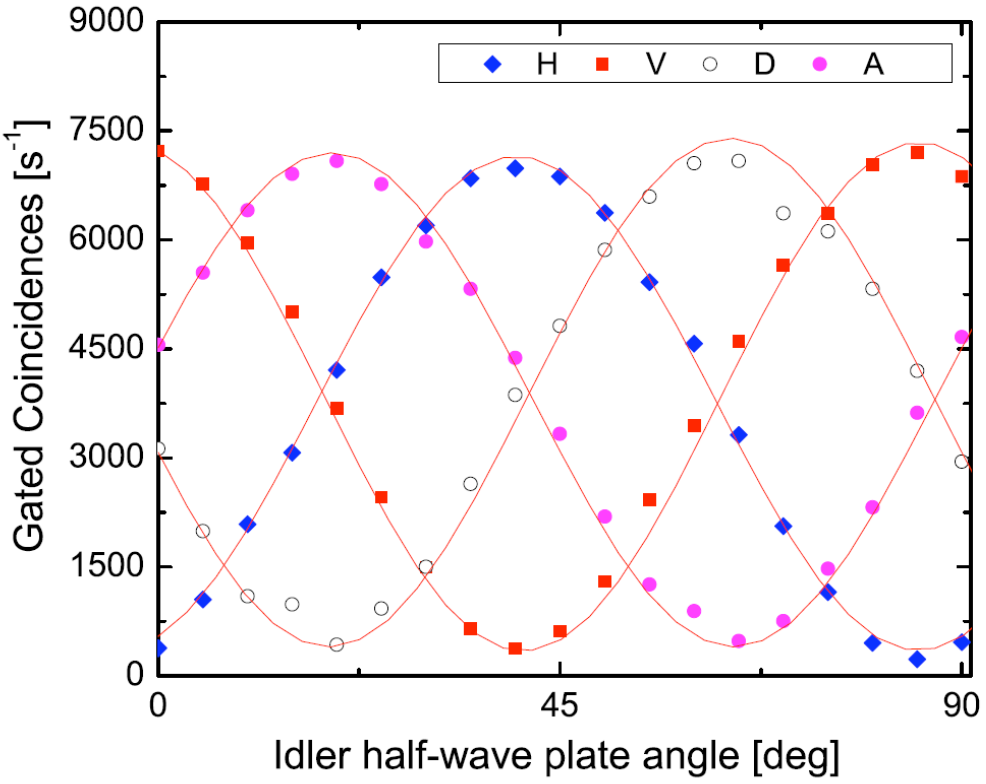

Figure 16 - Visibility curves using coincidence counts as a function of the idler half-wave plate setting for each of the four polarization states of the signal photons (H, V, D and A). Curves show a best fit.

The final part of the experiment is to perform the same visibility measurements with the entire setup connected as in Fig. 14, including the 27 km of SMF, the four WDM filters and the trigger pulses (at 1555.75 nm) sent in the fiber together with the single-photons at 1555 nm. The same incident pump power is used as in the previous part, therefore a single count rate of 1.1 x 10^6 s^{-1} is kept at 809 nm. The coincidence count rate dropped to 1.1 x 10^3 s^{-1} due to the extra attenuation provided by the 27 km fiber link (6 dB), and insertion losses from the other WDMs (3 dB). The raw visibilities for this case decreased to V_H = 85 %, V_V = 85 %, V_D = 83 % and V_A = 85 %. This decrease is due to the losses and trigger channel leakage which we could not fully remove. In hindsight, one of the causes of noise in this experiment could have been Raman spontaneous scattering, which is discussed in the next chapter. The estimated QBER from these curves is around

8\%, averaged over all four polarization states. The polarization state of the idler photons was stable enough for a few minutes, so that the visibility curves could be obtained.

It was shown in this experiment that distribution of single-photons in a quantum network environment (with 0.8 nm channel spacing) is possible, while sending the trigger signal in the same fiber. At the time this work was published, there was only one experiment using the same channel spacing [85]. We have successfully performed the experiment with a narrowband SPDC source, which is a benefit for compatibility with the narrow channels of classical optical networks, and is less sensitive to the effects of chromatic dispersion inside the optical fiber.

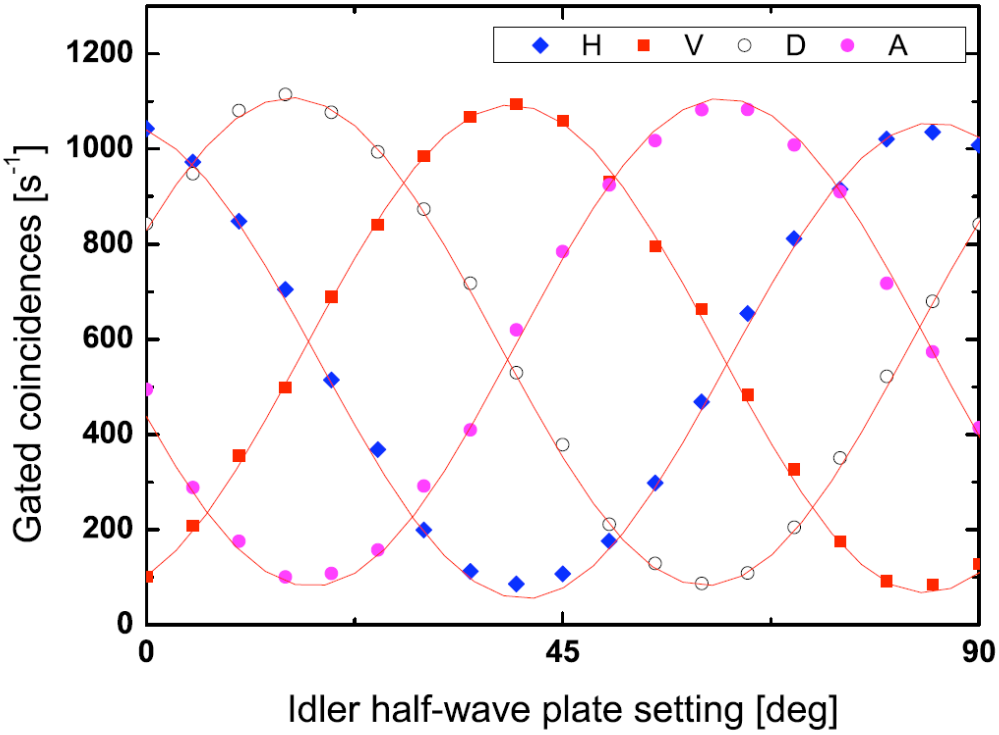

Figure 17 - Visibility curves after 27 km of single-mode fiber using coincidence counts as a function of the idler half-wave plate setting for each of the four polarization states of the signal (H, V, D and A). Curves show a best fit.

3.2. Experimental QKD with a Heralded Single-Photon Source and the Decoy State Modification

Even though there have been extensive proofs of security for QKD [86,87,88], there is one type of attack Eve can perform which takes advantage of realistic photon sources called the photon number splitting (PNS) attack [89-90].

This type of attack can succeed against sources that emit multi-photon states, and for this reason only QKD schemes using perfect single-photon sources are secure against this type of attack. All current photon sources employed in quantum communications are approximations to the ideal single-photon source, with the attenuated laser generating weak coherent states (WCS) being the worst. Depending on the average photon number per pulse chosen (typically 0.1), WCS sources may be used for secure QKD, but there is a large vacuum component (empty pulses, around 90 % of the total) which severely limits the transmission rate. If the average photon number is higher, then the multi-photon component (pulses containing two photons or more) increases considerably, and the PNS attack becomes possible. In fact for secure QKD, the following condition must apply [89,91].

$$y > p_{multi} \tag{3.1}$$

We shall now describe the idea behind the PNS attack: Eve monitors the quantum communication channel between Alice and Bob, and performs a quantum non-demolition measurement (QND) [92] to find out how many photons are in each pulse. Remember that Eve has access to technology that is not even developed yet, as long as it is physically feasible. Every instant a single-photon pulse is detected by Eve, she simply blocks it and all the times a multi-photon pulse is detected, she splits it keeping one photon for herself and forwarding the other to Bob. Eve stores her photon in a quantum memory (this was far-fetched technology when the PNS attack was first mentioned, but it is getting more and more practical [93,94]) and awaits until the basis choices are revealed by Alice and Bob over the public channel. Then she measures the photons with full certainty, obtaining full information about the key. If this is all Eve does, Bob will clearly realize something is wrong, since all single-photon pulses are not reaching him (we are assuming he does not have photon-number resolving detectors, but he realizes that less pulses are being detected). The PNS attack becomes more difficult to detect when the source has a large multi-photon component, in other words, a low quality single-photon source is being used by Alice. Eve is obviously smarter than that. In order to disguise her presence, she replaces the part of the communication channel after the point of her interception by a lossless channel (for example a perfect teleportation apparatus). Eve's presence can be

more easily masked if the loss and multi-photon component are higher. These two conditions can be summarized by Eq. (3.1), and the PNS attack is summarized in Fig. 18.

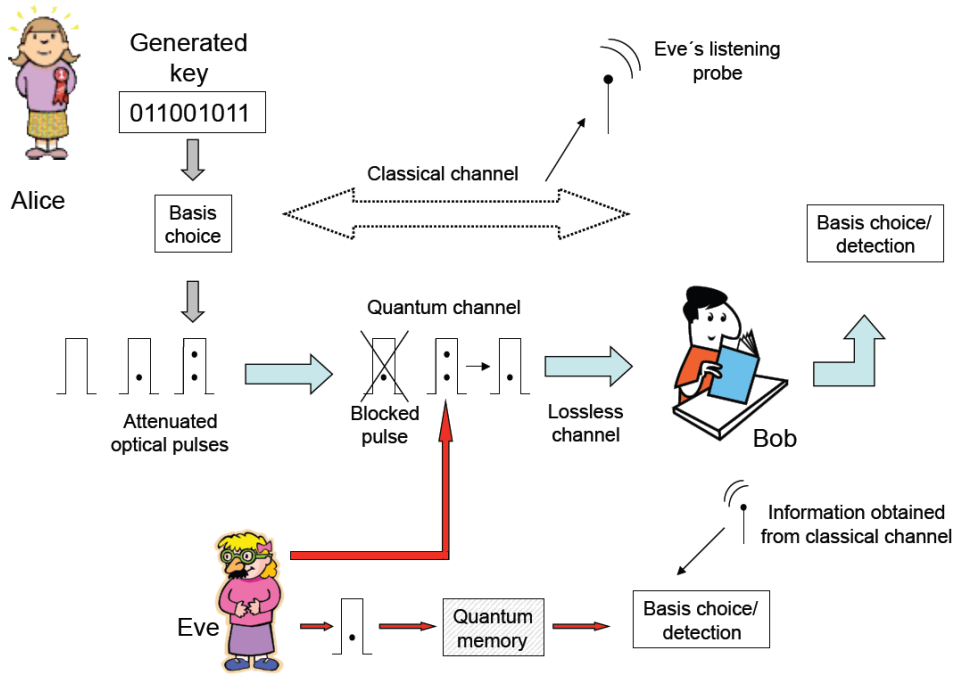

Figure 18 - PNS attack scheme. Adapted from [72].

The PNS attack defines what is the actual secure transmitted distance, even if the reachable distance is much higher. For example, using the experimental data from [95], Brassard *et al* [89] have shown that the secure transmitted distance was zero, even though the experiment managed to share a key through 30 km, using an average photon number per pulse of 0.2. The large vacuum component of the source used (attenuated pulsed laser) causes difficulties for this type of source, as well as the multi-photon probability. One solution is to use a source based on SPDC processes, since the vacuum component and the multi-photon probabilities are both smaller. Indeed, changing the source used in [95] and using the same data for the optical fiber and detectors used, Brassard *et al* [89] have shown that a secure distance of 68 km could be achieved with a SPDC source.

From the results mentioned above, it seems that sources based on weak coherent states are not secure enough against a technologically superior Eve, and that SPDC-based sources seem to be a solution. However, even today they are much more expensive and complex than an attenuated pulsed laser. Fortunately a

major breakthrough came in 2003 with the idea of decoy states developed by Hwang [91] and later improved [96,97].

The decoy state method is based in the idea that Alice sends multi-photon pulses on purpose to Bob, in order to trick Eve in performing a PNS attack. The key to this method is that Eve cannot predict if a multi-photon pulse was intentionally generated by Alice, or if it is a source imperfection, thus she will perform the PNS attack on all multi-photon pulses. The protocol works as follows: Alice randomly chooses between different intensity levels for each pulse being sent. We shall refer here only to the three-state protocol [96] in which Alice sends vacuum, signal and decoy pulses with 0, μ and μ' average photon numbers respectively, where $\mu' > \mu$\$. She can change which type of pulse she wishes to send by using a variable optical attenuator. Other important parameters are the counting rates (or yield) measured by Bob Y_0, Y_μ and $Y_{\mu'}$. After all the pulses are sent out, Bob informs through the public channel which pulses caused clicks on the detectors, and which did not. Alice knows which type of pulse was sent each time, and from the results informed by Bob, she can deduce the counting rates for each type of pulse.

Let us now look at it from another perspective. If Eve blocks all the single-photon pulses, the transmittance of multi-photon pulses should be abnormally high when compared to the single-photon ones. In other words, the normalized counting rates (over the number of pulses) for multi-photon pulses will be higher than single-photon pulses. Alice and Bob can calculate a lower bound for the single-photon counting rate of single-photon states and an upper bound of the quantum bit error rate of single-photon states. They can then discover if Eve is attempting the PNS attack. The decoy state idea has dramatically improved the secure transmission distance [97]. This is just the general idea of the decoy state method, for a more rigorous discussion please see [91,96,97]. For experimental realizations please see [59,98].

Decoy states represent a major improvement for the security of systems using attenuated pulsed lasers as the single-photon source. But what about a source based on SPDC? A heralded single-photon source (HSPS) is in principle a perfect single-photon source, since for every detected signal photon, there is a corresponding idler photon. A practical HSPS, however, will have losses, and

those will create empty pulses. Multi-photon pulses are also created due to high intensity pump powers though this probability is much lower than sources with weak coherent states. Nevertheless it was shown that the decoy state method can improve the secure transmitted distance of an HSPS too [99,100,101]. This experiment then combines an HSPS with the decoy state method performing a QKD session over an optical fiber link [34].

The experiment was done in Stockholm as a collaboration between KTH and the University of Science and Technology of China from Hefei, with the group of Guang-Can Guo. The source was assembled at KTH and when it was ready, members from Hefei brought in their phase-coding setup and electronics to perform a QKD session. We shall first describe the HSPS we built for the experiment. Originally a 20 mm long PPLN crystal with a waveguide was used in the HSPS, for the same conversion of $532 \rightarrow 809 + 1555\,\text{nm}$. A great deal of time was spent adapting the oven containing the crystal to the optical setup. After spending some more time aligning the optics, we discovered that the conversion was completely off from the specified. Although the brightness was clearly much superior than the long crystals used in the narrowband source experiment, the the wavelength was not compatible with optical fiber transmission (emission was at around 1200 nm for the idler). We made the quick decision of replacing the waveguide with one of the 50 mm long PPLN crystals used in the previous experiment explained in the previous section, especially since, as mentioned, the entangled source of photon-pairs would move on to a single-crystal configuration.

The scheme for our HSPS is shown in Fig. 19. The pump is a Nd:YAG DPSS laser. The pump beam is focused in the middle of the PPLN crystal using a 150 mm focal length achromatic doublet lens. This focal length was chosen after some attempts based on the focusing conditions of the previous experiment. However, no collimating lens was used to the output down-converted beams, and instead we placed the dichroic mirror (DM), filters and fiber couplers very close to crystal, so that the beams did not diverge too much. The fiber coupler (FC) is composed of a short focal length aspheric lens, a multi-axis translation stage and optical fiber holder. The signal FC was placed at half the distance from the DM when compared to the idler FC, in order to compensate the beam divergences in

the coupling. We also tried using extra collimating lenses but the final results were approximately the same, so we opted for the simpler setup.

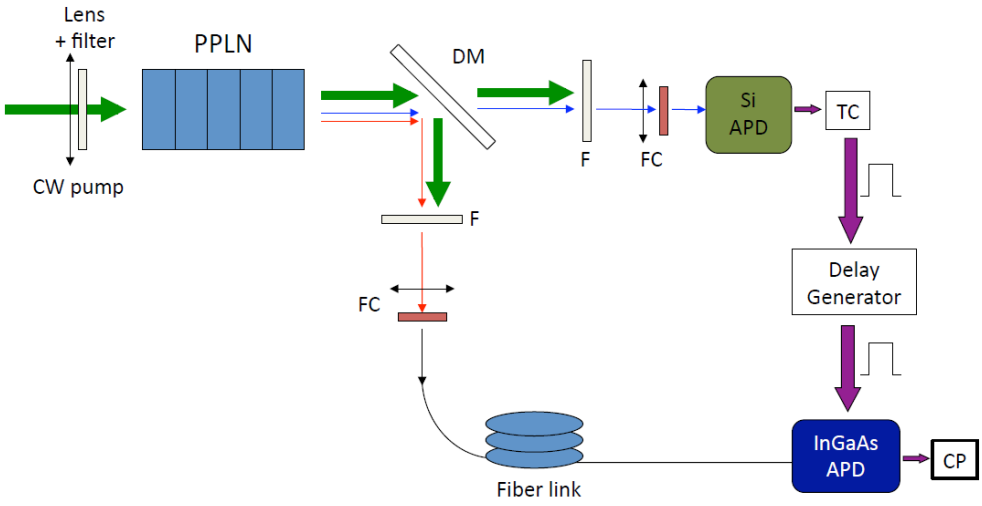

Figure 19 - Heralded single photon source used in the experiment. PPLN: Periodically-poled lithium niobate crystal; DM: Dichroic mirror; F: Filter; FC: Fiber coupler with aspheric lens and multi-axis translation stage; TC: Time chopper; CP: Counter and processing. Green, blue and red arrows represent pump, signal (809 nm) and idler (1555 nm) respectively. A HWP is used to adjust the pump polarization before the crystal (not shown).

After the DM, two bulk filters are used to remove the pump from the signal and idler beams (RG 715 and RG 1000 respectively). Both beams are coupled to single-mode optical fibers before arriving at the Si and InGaAs detectors. The Si APD was the same as the one used in the previous experiment (Perkin Elmer), while the InGaAs APD operating in Geiger mode was changed (IdQuantique id200). It has a quantum efficiency of 7.5 % and 2.5 ns gates were used. After the Si APD we employed a Time Chopper (TC), used to insert a dead time after each detection. It is necessary because in order to change the average idler photon number per detection window we need to change the pump power, and as a consequence the signal photon rate. When we do so, we change the triggering rate in the InGaAs APD, and the dark count probability also changes. Therefore, with a deadtime, the InGaAs triggering rate did not rise as fast as the number of detections by the Si APD, and our set up did not see the difference in the dark count probability when we changed between , μ and μ' . The output of the TC is connected to a delay generator, and finally to the trigger input of the

InGaAs APD. The idler photon, after coupling, will go through the optical fiber until before detection by the InGaAs APD.

The initial step is to characterize the HSPS, and we employed the same method as in [102] described in detail in [103]. We would like to know what type of photon distribution our source emits. When using a CW pump, as long as the coherence time Δt_c of the down-converted photons is shorter than the gate width, a large number of independent down-conversion processes will take place, resulting in a poissonian distribution [103]. One important parameter for the characterization of a single-photon source is the second-order auto-correlation function at zero-time delay [16,103]:

$$g^{(2)}(0) = \frac{2P_{m\geq 2}}{P_{m\geq 1}^2} . \qquad (3.2)$$

If $g^{(2)}(0) = 1$ we have a poissonian source, $g^{(2)}(0) < 1$ it is sub-poissonian and and finally $g^{(2)}(0) > 1$ super-poissonian [16]. $P_{m\geq k}$ is the probability to find at least *k* photons within a gate period, which can be written as:

$$P_{m\geq k} = P^{cor} P_{m\geq k-1}^{acc} + (1 - P^{cor}) P_{m\geq k}^{acc} \qquad (3.3)$$

where P^{cor} is the correlated rate of photon pairs, which is the probability of detecting an idler photon (heralded) given that a signal photon (heralding) has been detected. If there are no losses in the system (perfect coupling and components), then $P^{cor} = 1 \cdot P_{m\geq k}^{acc}$ is the probability that at least *k* accidental photons fall within a gate period, that is, uncorrelated photons. Since the accidental photons are not correlated, the pump is CW and the coherence time of the down-converted light is much smaller than the gate width, the distribution of these photons is poissonian. As we will see, our source fall within these conditions, since the emitted coherence time is around 10 ps, and the gate width is 2.5 ns. Therefore, $P_{m\geq k}^{acc}$ can be written as [102,103]:

$$P_{m\geq k}^{acc} = 1 - \sum_{i=0}^{k-1} \frac{\mu^i}{i!} e^{-\mu}, \qquad (k \geq 2) \qquad (3.4)$$

where μ is the average photon number per gate, $\mu = R_i \cdot \Delta t_{gate}$, R_i is the mean photon number per second, is the gate width of the detector. We denote r_c the coincidence count rate; r_s the Si APD single counting rate; r_i the InGaAs detector single counting rate (using random triggering, whose frequency is R_0); R_0 is the heralding rate which can be different from r_s due to the dead time of the detector / delay generator; η_i (η_s) and d_i (d_s) are the detection efficiency and dark count probability of idler and signal detectors respectively; R_i (R_s) is the photon number per gate present in the fiber before detection.

Using the steps shown in [103] we can write:

$$R_s = \frac{1}{\eta_i \Delta t_{gate}} \ln \frac{R_0 - d_i}{R_0 - r_i} \tag{3.5}$$

$$P^{cor} = 1 - \frac{R_0 - r_c}{R_0 - d_s} e^{\eta_s R_s \Delta t_{gate}} \tag{3.6}$$

All the parameters in Eqs. (3.5) and (3.6) can be measured in the experiment yielding the values of P^{cor} and R_s. Writing expressions for the probability to detect *n* photons, vacuum, the single-photon, and substituting the values of $ P^{cor} and R_s into those expressions (steps outlined in [103]) we can calculate the photon number distribution of our source as shown in the table below for two different trigger frequencies (or in other words, pump power) after the time chopper, 200 and 650 kHz, corresponding to μ and μ' respectively. The intensity is the average number of photons per detection window and p_0, p_1 and p_2 correspond to the vacuum, single and two-photon probabilities per detection window:

Trigger (kHz)	Intensity	p_0	p_1	p_2	$g^{(2)}(0)$	P^{cor}
200	0.588×10^{-3}	0.727	0.273	1.600×10^{-4}	4.56×10^{-3}	0.273
650	5.532×10^{-3}	0.698	0.300	1.655×10^{-4}	3.53×10^{-2}	0.298

From these results we clearly see that our source exhibits sub-poissonian characteristics $g^{(2)}(0) < 1$ and very low multi-photon probability, showing that we have an improvement when compared to a weak coherent source. A photo of part of the source is shown in Fig. 20:

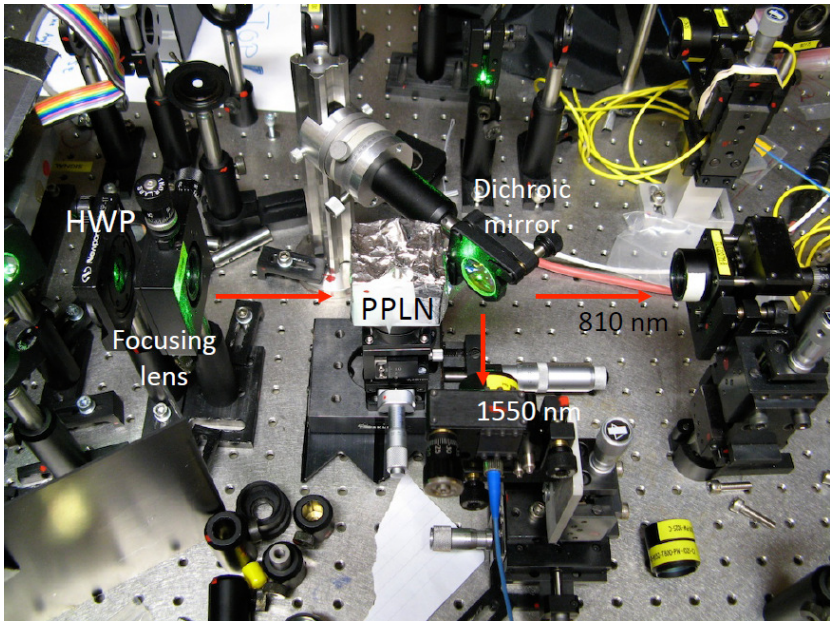

Figure 20 - Picture of part of the source. The pump laser, electronics and detectors are not shown.

Taking the data obtained from the source characterization and using the same method from [99,100,101] and as shown in [34, 103], we plot the key generation rate vs the total losses comparing several different schemes:

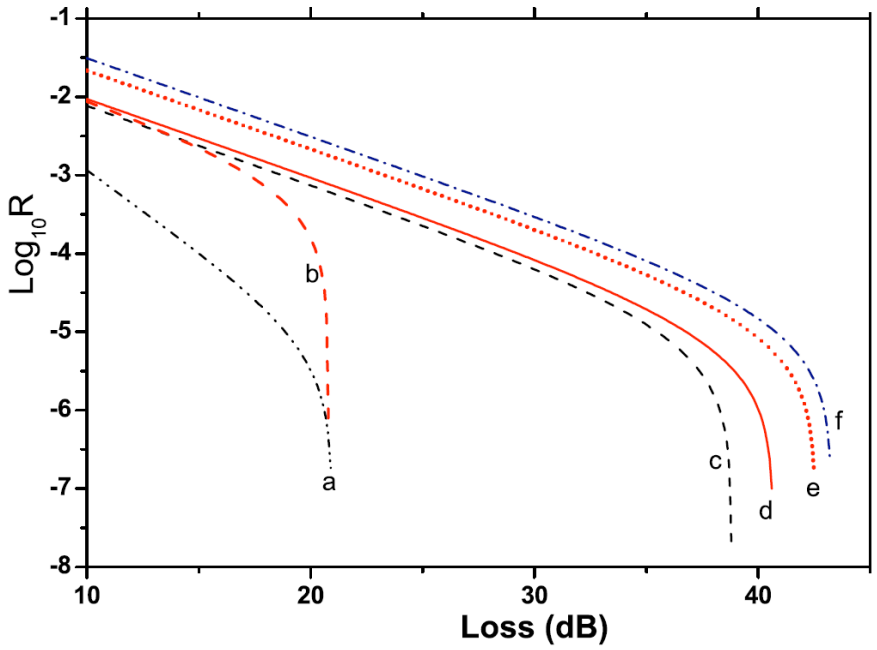

Figure 21 - Numerical simulation for the key generation rate vs total loss for the following schemes: a) WCS source without decoy state; b) HSPS without decoy state; c) WCS with decoy state method (optimal values for used for each point); d) HSPS with decoy state with P^{cor} = 30 %, μ = 5.88 x 10^{-4} and μ' = 5.53 x 10^{-3}, values taken from our source

characterization; e) HSPS with decoy state and with P^{cor} = 70\%, and μ and μ' values as before; f) the ideal single-photon source.

Fig. 21 clearly that shows our scheme outperforms an attenuated pulsed laser source using optimized decoy states. Curve e) shows what could be obtained if an HSPS with P^{cor} = 70\% was used with the same values for μ and μ' as our source. Such an HSPS was recently demonstrated [104] using narrow filters, therefore it is technologically feasible, and its performance comes very close to the ideal single-photon source. Optimizing our source we obtained $P^{cor} = 40\ \%$ in [103]. The entire experimental setup is shown in Fig. 22:

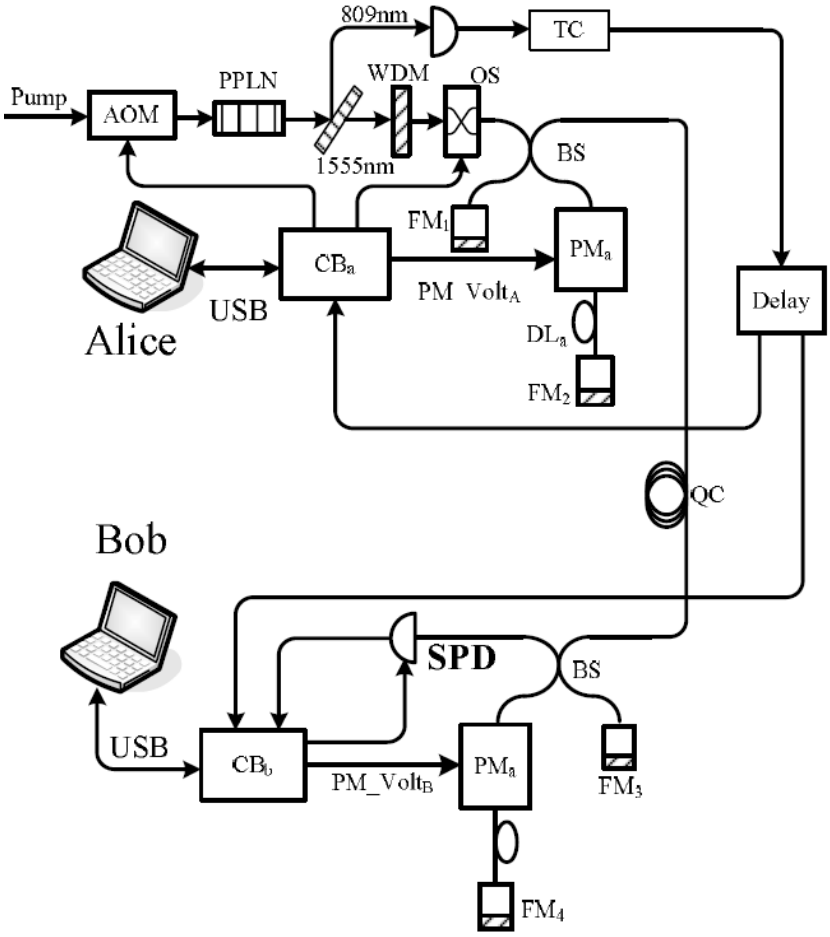

Figure 22 - Complete experimental setup of QKD with an HSPS using the decoy state method. AOM: Acousto-optical modulator; PPLN: Periodic poled lithium niobate; WDM: Wavelength division multiplexer; OS: Optical switch; TC: Time chopper; BS: Beam splitter; PM: Phase modulator; FM: Faraday mirror; CB: Control board; DL: Delay line; SPD Single photon detector.

The QKD phase-coding setup is based on a one-way Faraday-Michelson (F-M) system [105], using four states with one detector scheme, making it immune to time-shift [106] and faked-states [107] attacks, with the disadvantage of losing half of the photons. This scheme is also immune to birefringence changes like the "Plug and play" setup, but it has the advantage of being one-way.

In order to create the decoy states, we could simply place a fiber-pigtailed amplitude modulator after the 1555 nm signal coupling. However, as we will discuss below, our system has too much loss, and the > 3 dB insertion loss in commercial optical amplitude fiber-based modulators for 1550 nm was too much. Therefore we placed an Acousto-optical modulator (AOM) in the pump beam path before the crystal. One problem we would have is how to create the vacuum state in this configuration, because we would lose all triggering signal by fully attenuating the pump. We then inserted a fiber pig-tailed optical switch with 0.6 dB loss to change between μ_0 (vacuum) and μ states, and the AOM changing between μ and μ' states. As mentioned before the electronic time chopper (TC) was necessary to keep the same dark count probability, while changing the pump's power with the AOM to generate μ and μ'.

The F-M system was intended to be used originally with a WCS source, and therefore the attenuation at Alice does not matter as she can simply adjust her attenuator accordingly. For an HSPS *any* attenuation means less photons arriving at Bob. The F-M configuration + HSPS is even more restrictive at that, since the signal passes twice through the phase modulators when compared to a standard phase scheme. Right from the start, loss was one of the most difficult issues with this experiment. That is the reason why we had to minimize losses, the best as possible. Another major issue was the coherence length of the source required to obtain interference in the interferometers. The interferometers were designed to be used with an attenuated pulsed laser, which has a very narrow linewidth. The length mismatch between the two interferometers was too long as we observed visibilities of less than 10 % with the HSPS, which makes any quantum communication session unfeasible. Using a classical broadband light source centered around 1550 nm, connecting the two interferometers in series, measuring the spectrum of such source in an optical spectrum analyzer and observing the fringes generated we estimated the length mismatch to be on the order of 1 cm. Using the spectrum of our HSPS (Fig. 23), we estimated that the required length

mismatch should be in the order of 2-3 mm. Even though the crystal is the same as in the previous experiment, we obtained a brighter source when comparing the optical power from the two spectra (this one and the spectrum of the entangled photon-pair source using two crystals) due to optimized focusing conditions and coupling, to a much simpler configuration of the source, and to less optical components involved.

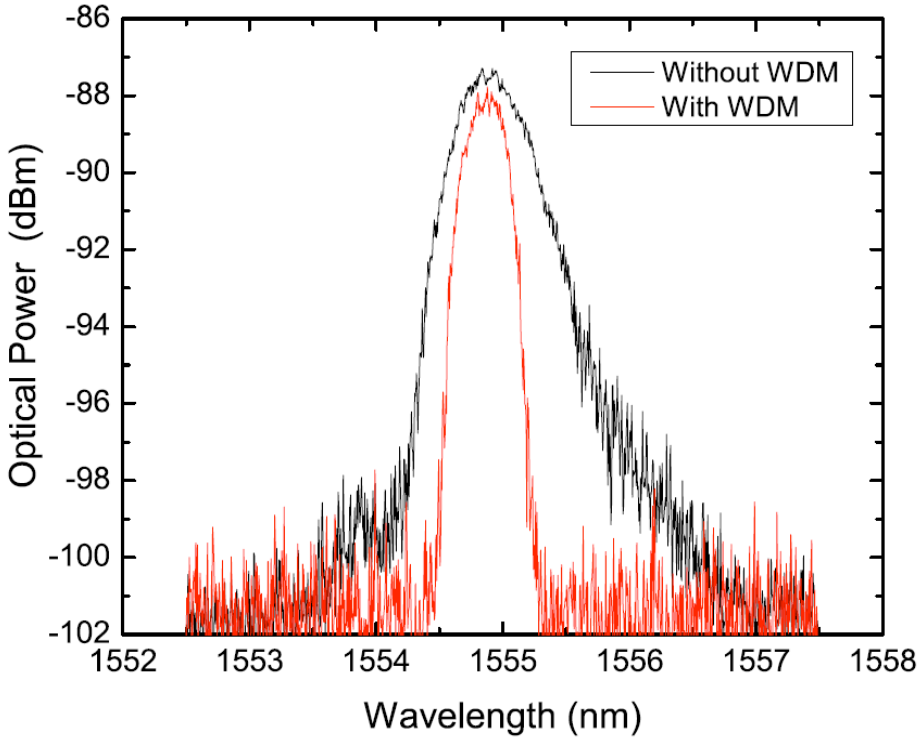

Figure 23 - Spectrum of the down-converted idler photons with (red) and without (black) WDM filter.

In order to adapt the interferometers to our source we decided to open up their thermally insulated boxes, cut one of them, and use a fiber splicer to adjust the lengths. It was a trial-and-error procedure, since we had to get the length adjusted to within less than 2 mm. After we managed to adjust it (we checked with the broadband light source and spectrum analyzer), the visibility curve had improved considerably, but it was not good enough, since high QBERs were obtained even with no fiber. We finally used a WDM filter (from the previous experiment) to narrow down the spectrum of the HSPS as shown in Fig. 23. We had to bear with a total loss of almost 3 dB (insertion loss + narrower spectrum), but it was the only way to get a good visibility (> 95 %) to perform the experiment.

The average photon number per 2.5 ns gate is for each intensity: [μ', μ, μ_0] = [5.532 x 10^{-3}, 0.588 x 10^{-3}, 0.577 x 10^{-5}], and due to an imperfect isolation ratio of the optical switch (20 dB), our vacuum state is a bit higher than just the dark counts. The ratio between the number of states sent for each type was 10:4:1. The interferometers were built inside thermal insulated containers, and they were stable enough for usage for only a few seconds. There was no active temperature controllers built-in. In order to improve the insulation we made a larger box filled with styrofoam pieces and placed both interferometer containers inside. The stability improved to around 1 min, which is clearly not enough for a QKD session, therefore we adopted a scan and transmission mode [105] in which we transmit blocks of key, then stop the transmission, scan the interferometer to measure the visibility adjusting the voltage bias of the phase modulators. This has the negative effect of dropping the overall key transmission rate, but no active control is required.

Alice and Bob are connected by 25 km of standard SMF-28 optical fiber, with a total loss of 5dB. Unlike the previous experiment, we did not send the trigger pulses in the fiber along with the quantum signals. We were so limited in terms of loss, that we would not be able to use the set of 4 DWDM filters. Therefore the synchronization was done using electrical cables and a delay generator to match the times. We estimated the required delay for the fiber. Then we made a quick search around that value until we found the coincidence peak. During a measurement of 200 minutes (the actual key transmission time is 70 minutes, without the scan time), the total QBER for μ (μ') was 6.43 % (6.88 %), and we obtained 30.90 x 10^3 sifted key bits out of a total of 84.60 x 10^3 coincidence counts after a total loss of 36 dB (fiber + QKD setup after fiber coupling). Finally, 3.77 \times 10^3 secure key bits can be distilled, which agrees well with the theory, as shown in Fig. 24, using the simulation model described in references [97,99,100].

Our final key rate is lower than most QKD systems due to the high loss present in the optical setup. Many things could be done to decrease the loss, such as replacing the F-M system by a Mach-Zehnder configuration [7], using polarization encoding, using a standard two-detectors scheme and replacing the InGaAs detector by a newer model with higher quantum efficiency and lower dark counts. All in all, we could gain 15 dB which would make our experiment more

reliable for long distance transmission or higher key rates. However as a proof-of-principle experiment we showed that QKD with an HSPS with the decoy-state method is feasible, and offers performance gains over standard decoy-state with a WCS source.

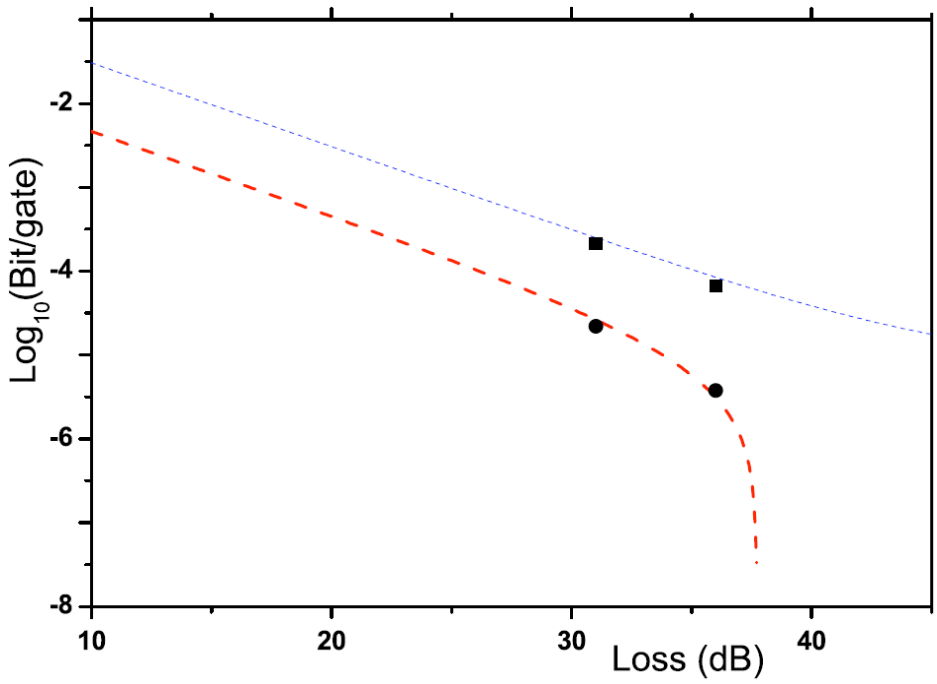

Figure 24 - Theoretical curves for the coincidence count rate (dotted blue line) and final secure key rate (dashed red line). The dots and squares are the experimental results at a total loss of 31 (optical fiber removed) and 36 dB (25 km of spooled SMF-28 fiber connected).

4
Raman Noise and Random Number Generation

Both experiments presented here were performed after the author's return to Rio de Janeiro, from January 2008 until the end of the same year. They present results which aim to support quantum communications in optical fibers (as is the case of the Raman noise study), or in general as in the case of the random number generation experiment.

4.1. Simultaneous Classical and Quantum Communications in Optical Fibers

In order for QKD to move from the lab or niche commercial applications to mainstream usage, co-existence of quantum and classical channels inside the same optical fiber is of paramount importance. Severe care must be taken in the transmission of a classical signal in a fiber with a single-photon detector at the other end. The isolation of most commercial telecom components (filters, couplers, etc...) is of the order of 30 dB, which means that out of a typical signal power of 0 dBm (1mW), there are still too many photons falling on the detector. Careful filtering is therefore critical to a successful quantum and classical communication in the same optical fiber.

The work presented here came during preparation for the experiment with polarization control in the next chapter. While using the reference classical channels for polarization control, a source of noise was noticed, and originally we believed it was cross-talk from the WDM filters. We realized it was only present when the fiber was connected, therefore it must be a scattering effect of the classical channels along the fiber. We decided to investigate this effect further and the results are presented here.

Our initial attempts were to mimic the polarization control setup first used by our group in [78], in which the control channels were used in a counter-propagating manner to the quantum channel. This was reasonable enough in order to minimize cross-talk effects. As we will show, in this situation a problem which

can arise is Rayleigh backscattering [77] from the classical signals generated in the fiber, as well as reflection in optical connectors, from the amplified spontaneous emission (ASE) of the lasers used. Although all lasers concentrate most of their emission power on a center wavelength with narrow bandwidth, a small percentage of light is emitted as broadband noise called ASE, which can be tens of nanometers wide centered on the emission wavelength. ASE (as the center wavelength) will scatter back as it propagates along the fiber through Rayleigh backscattering, and reflect from connectors as well. The problem is that a part of the backscattered ASE will fall within the quantum channel wavelength, causing noise in the quantum transmission. Rayleigh backscattering can be removed filtering the ASE section corresponding to the quantum signal bandwidth out of the laser spectrum as shown in Fig. 25, using a fiber Bragg grating. Without the fiber connected it is possible to verify that all cross-talk and reflections from fiber optical connectors have been removed. When the fiber is added to the setup, a considerable amount of noise appears and this is what we wish to investigate.

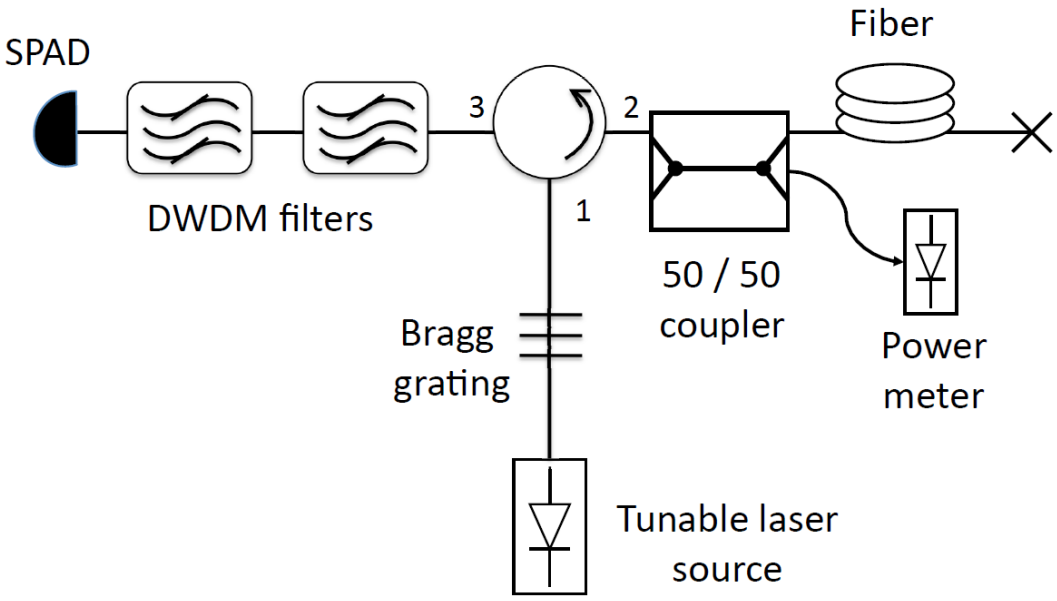

Figure 25 - Experimental setup to investigate noise generated from Raman spontaneous scattering. SPAD: Single photon avalanche detector; DWDM: Dense wavelength division multiplexer. The Bragg grating center wavelength is 1546.12 nm.

In the experiment to characterize the counter-propagating noise, we employed a tunable laser source operating in CW (continuous wave) mode to scan between 1475 and 1640 nm (a combination of two tunable lasers were used). In series with the laser is a fiber Bragg grating, designed to reflect the wavelength

1546.12 nm, which is the wavelength of the quantum channel in our polarization control experiment. Therefore by placing the Bragg grating, we remove the ASE component corresponding to the quantum channel from the tunable laser source spectrum. It is then connected to port 1 of an optical circulator, going to port 2 as shown in Fig. 25, is split in two by a 50/50 coupler with one output going to an optical fiber, and the other one to a power meter. The power meter is necessary to normalize the output power of the laser, since it is not constant for all wavelengths. The output of the optical fiber is an angled connector, and just before it bends of small radii were made to the fiber, to remove any reflections from the connector, which might disrupt the measurements results. Any photons returning along the fiber arrive at port 2 of the circulator and get forwarded to port 3, passing the two DWDM filters in tandem, and then arrive at the SPAD. These filters are in fact multiplexers / demultiplexers (they are passive components, so they are a multiplexer or a demultiplexer depending on which way they are connected), having one common port and 4 four wavelength ports (1545.32, 1546.12, 1546.92 and 1547.12 nm). All input light at the common port will get split in wavelength according to the other four ports, and vice-versa. In our experiment, light coming from port 3 of the circulator is connected at the common port of the first DWDM, whose 1546.12 nm port is connected to the common port of the second DWDM and finally the 1546.12 nm port is connected to the SPAD. Both DWDMs are simply used here as filters to the 1546.12 nm channel, but in the polarization control experiment the first DWDM was used to split the quantum (1546.12) and classical channels (1545.32 and 1546.92). Fig. 26 presents the measured results with 8 km of dispersion shifted (DS) and 7.5 km of standard SMF-28 optical fiber. The dark counts have been subtracted as we want to show only the effects of Raman noise.

The first thing which jumps out from this measurement is that the intensity of the counts obtained is, on average one order of magnitude higher than the dark count level of most commercial InGaAs SPADs (10^{-5} dark counts per 1 ns gate). 1 mW of input power is a typical level for many telecom systems, and sometimes it can be even more. It was verified that appropriate filtering was used by removing the fiber, and checking that we only had dark noise level for all input wavelengths. The experiment was made using two separate fiber spools, one composed of 8 km of DS fiber, and the other of 7.5 km of SMF-28. Clearly this

noise is being generated inside the optical fiber by the presence of a single CW classical channel. The first thought was of a non-linear effect, however as is shown in Fig. \27, the intensity of the noise varies linearly with the optical power. After considerable research and thought, we concluded that the phenomenon responsible is Raman spontaneous scattering, which is a linear effect [77]. The reason why the noise intensity is higher in the DS fiber, is due to difference in fiber core radii. Interestingly, we came to the correct conclusion that the effect we were observing is Raman spontaneous scattering independently of the works of other groups who first identified it [108, 109].

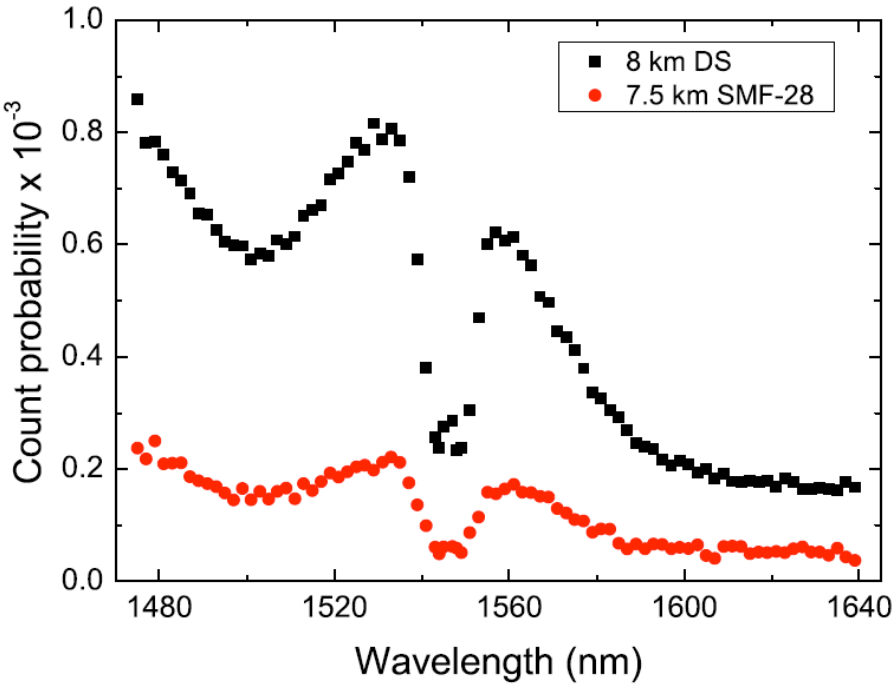

Figure 26 - Count probability per 1 ns gate for 1 mW (0 dBm) of input CW optical power as a function of the tunable laser wavelength. Dark counts have been subtracted.

Raman scattering works in the following manner: a photon while in its time-of-flight inside a fiber may be absorbed by one of the many SiO_2 atoms that make up the fiber's lattice. It is then re-emitted at a longer wavelength, and to conserve energy and momentum, a phonon is absorbed by the lattice (anti-Stokes), or is re-emitted at a shorter wavelength, and a phonon is consumed in the process (Stokes). For this reason Raman is a type of inelastic scattering, while Rayleigh's scattering is elastic since no phonons are involved and therefore no wavelength conversion takes place [77]. Another important result showing the linearity of the noise is presented in Fig. 27. As we can clearly observe the noise intensity is

linear through a broad variation of input power, which is among the typical levels used in telecom. The difference in intensity between different wavelengths is simply because as we observed, the Raman noise intensity is wavelength dependent.

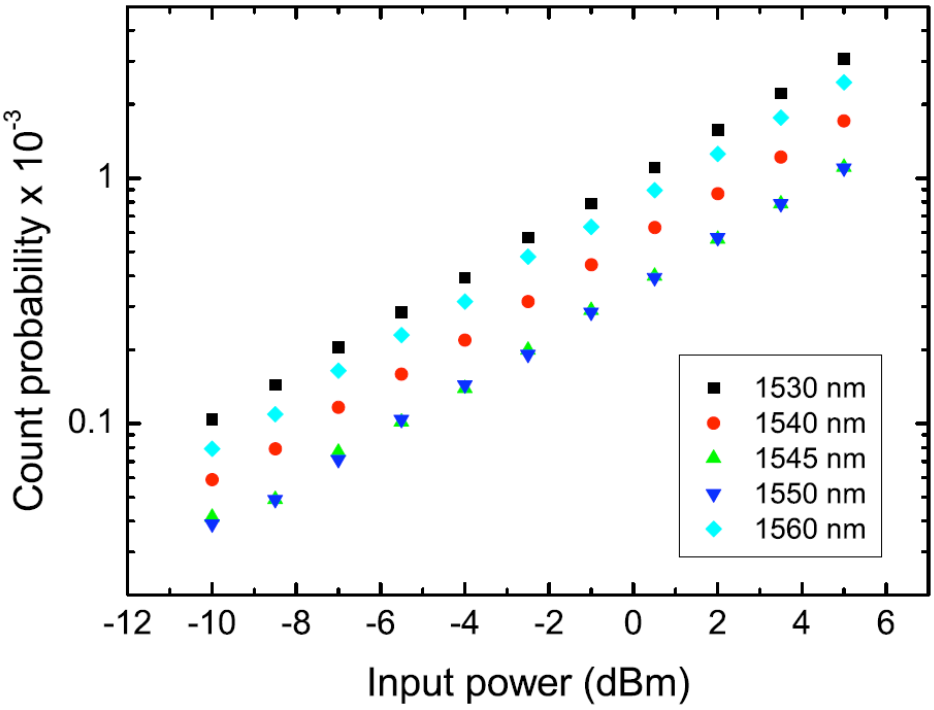

Figure 27 - Count probability per 1 ns gate for the counter propagating setup for 8 km of DS fiber as a function of input power and wavelength.

The spectra of one of the DWDMs (both of them have the same characteristics) is shown in Fig. 28. Since they are standard for the ITU-T telecom grid (0.8 nm spacing), their spectra is of the flat-top type with 0.4 nm FWHM (full-width at half maximum). The extinction ratio between adjacent channels is of the order of 40 dB. This measurement was performed using a tunable laser as the light source, and an optical spectrum analyzer connected after the DWDM. The output fiber of the laser was connected to the common port of the DWDM, and each wavelength port was connected to the spectrum analyzer in turn, yielding the four spectra shown in the figure.

So far we have seen the noise contribution in only one direction, the counter-propagating one. This is one possible configuration we may have while using a quantum channel in a fiber with live traffic being transmitted. In fact, this could have been the most sought after configuration, since it makes filtering easier due to the fact that channels are counter-propagating. Unfortunately, according to

the results we have shown, any quantum communication session is impossible with the noise levels presented. The first experiment presented in the previous section used a separate channel in the same fiber as the single-photons, providing trigger information for the single-photon detector. In that case there was no noise generated due to Raman scattering because the trigger signals consisted of optical pulses separated in time from the single-photons. At the end of this section comments will be made regarding to what can be done to minimize the effects of Raman spontaneous scattering induced-noise when propagating classical and quantum channels in the same fiber.

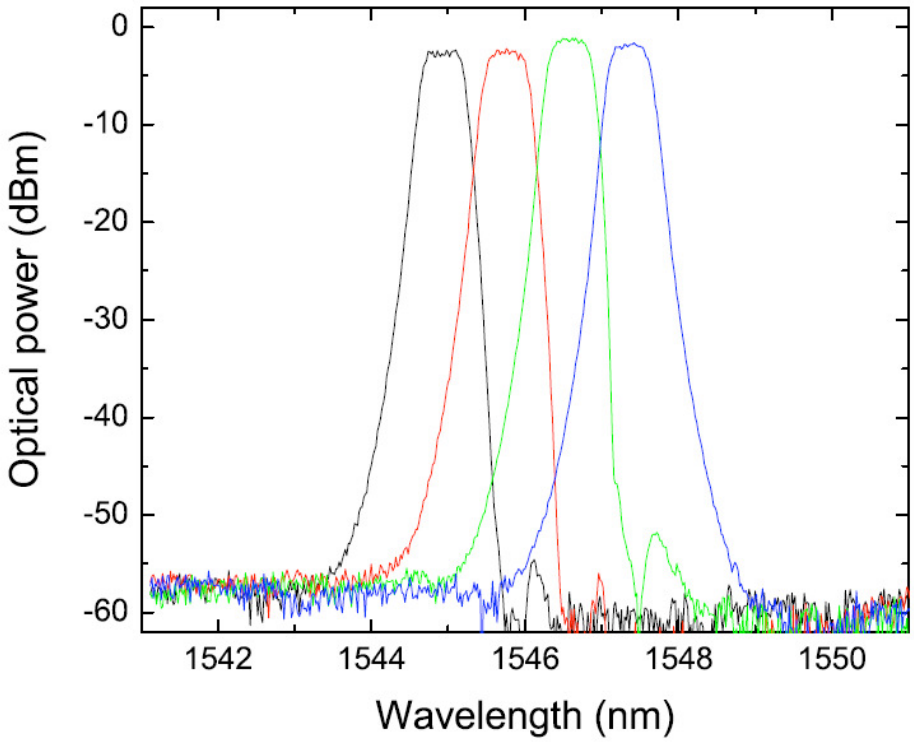

Figure 28 - Spectra of each DWDM channel measured with a tunable laser source and an optical spectrum analyzer.

What can we expect when we wish to co-propagate a classical and a quantum channel along the same fiber? This is the objective of the next measurement in respect to Raman spontaneous scattering. The experimental setup is presented in Fig. 29. We have employed the same combination of two tunable laser sources (yielding a total scan spectrum between 1475 and 1640 nm). The filtering needs to be more stringent in this configuration since we are shining a classical light source directly at the detector, which can easily saturate or even

destroy the SPAD. Once again, even though the center wavelength of the laser will not coincide with the quantum channel (1546.12 nm), a component of the ASE from the laser corresponding to the quantum wavelength (the power of the ASE in respect to the center peak can range between -30 to -50 dB depending on the laser quality) falls *directly* on the detector. The first step we take to protect against this is to place a fiber Bragg grating, centered at 1546.12 nm, in series with the tunable laser to remove that ASE component. The power is split in two in a fiber coupler, to monitor the tunable laser power. The signal passes through the fiber, then through a circulator connected as shown in the figure. Port number 2 of the circulator has a fiber Bragg grating connected with the end reflection of the fiber removed by using an angled connector and several small bends on the fiber just before it. This grating is centered on the quantum channel wavelength to improve the filtering provided by the two DWDMs. Finally port 3 is connected to the two DWDM filters in the same configuration as before.

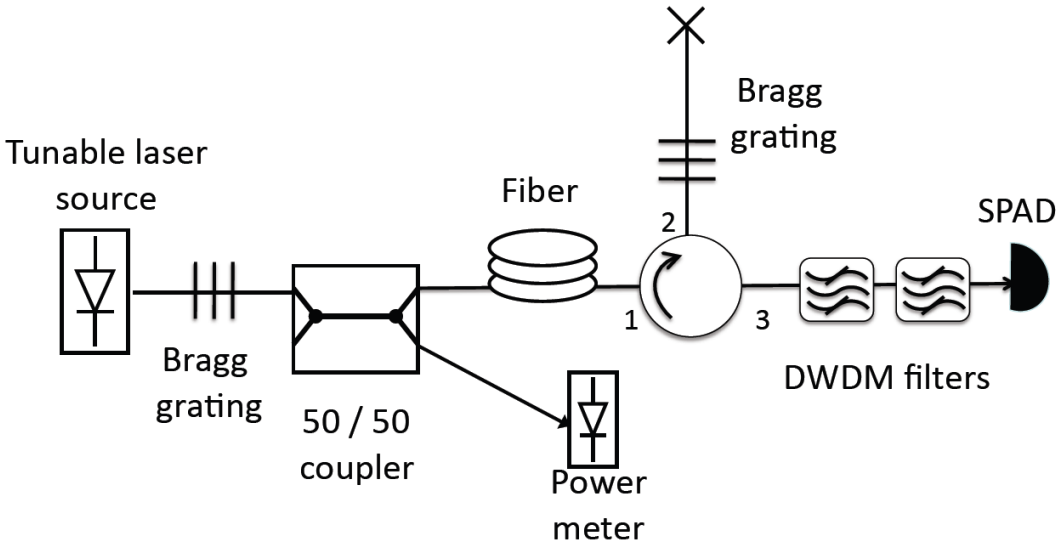

Figure 29 - Setup for characterizing co-propagating Raman noise.

Even by taking the extra filtering precautions we did not manage to remove all cross-talk noise, since we saw that without the fiber connected, the level of counts on the detector was a bit higher than the dark noise level. When we connected the fiber we could still see a noticeable difference so we nevertheless observe the effects of Raman noise. In order to correct the curves however, we did two measurements, one without the fiber, and the other with the fiber connected.

The two curves were subtracted in order to obtain only the Raman noise contribution (Fig. 30).

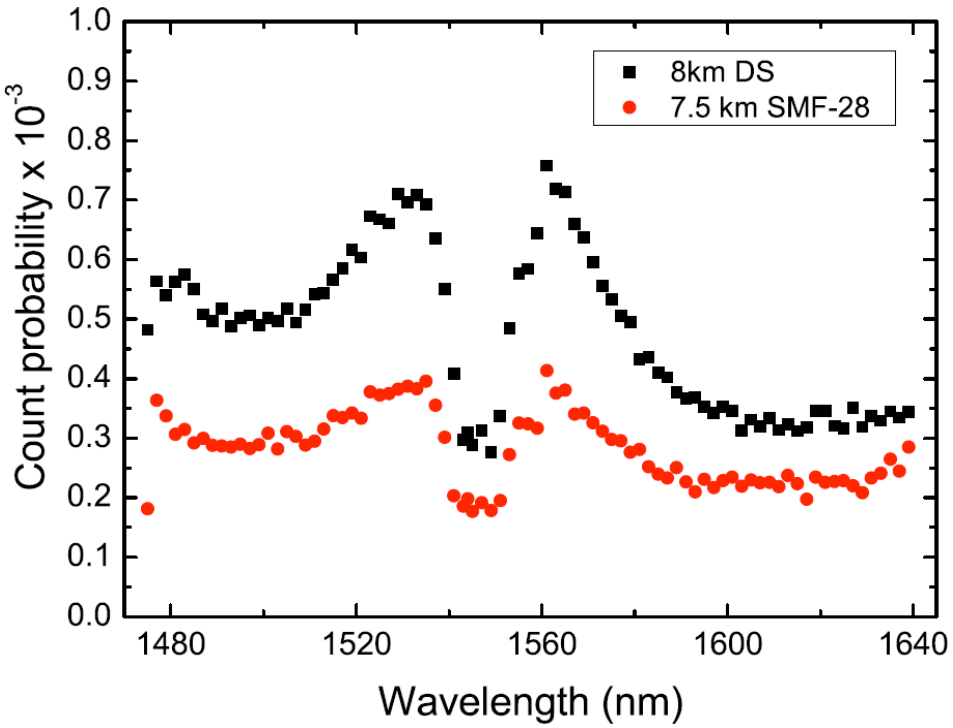

Figure 30 - Count probability per 1ns gate for 1mW (0dBm) of input CW optical power as a function of the tunable laser wavelength. Dark counts + counts from cross-talk have been subtracted.

We clearly notice that the order of magnitude of both co and counter-propagating setups is the same, as it would be expected for Raman spontaneous scattering. We can also observe almost the same difference between using DS and SMF-28 fibers, once again owning to the difference in fiber core radii. The most important result is that since the noise contribution in both configurations is roughly the same, there is little to no benefit in using one configuration or the other in principle. Based on this conclusion, we should then prefer the counter-propagating setup, as the cross-talk filtering is easier. Unfortunately the counter-propagating setup does not support the idea of shutting down the classical channel when the single-photon is to be transmitted, eliminating all Raman noise, due to the fact that this "dark pulse" would never be in sync with the single photon (they are counter-propagating).

Our results show that the photon counts contribution from Raman for a 1 mW input CW laser power is, on average, one-two orders of magnitude higher

than the dark count rate of commercial InGaAs SPADs, which makes quantum communication unfeasible. There are steps we can use to minimize Raman spontaneous scattering impact while performing quantum transmission in fibers simultaneously with live commercial traffic. The first clear measure to take is to lower the input power. Since the noise contribution is linear, a 10 dB reduction in input power yields a 10 dB reduction in noise. It is possible to use -10 dBm input power depending on the transmission distance, and even so, Erbium Doped Fiber Amplifiers can be used to amplify the classical channel, after it is demultiplexed. Such an experiment was performed (in fact it was the first experiment we know of done with 0.8 nm spacing in optical fibers) [85]. The authors however do not discuss Raman noise at all, or mention any noise contributions in their system. The other alternative is to use much narrower filters, to minimize the noise (since it is broadband). Very narrow filters are possible with today's technology, such as 10 pm bandwidth [110]. Since the filters we used have a bandwidth of around 0.4 nm, we can expect a reduction by a factor of 40 in the noise. In order to use a much narrower filter the source must be equally narrow, such as an attenuated pulsed laser. On the other hand sources based on SPDC have typically many nanometers bandwidth, which would be very inefficient to use together with a very narrow filter. One final solution is to temporarily shut down the classical channel when the single-photon is transmitted. This idea can remove all Raman noise, and we successfully used it in the polarization control experiment explained in the last chapter. Unfortunately this is not a practical solution for commercial classical optical communication systems, since: a) too much adaptation of classical systems is needed to ensure synchronization is kept, no data is lost, etc\ldots; b) the lasers when turned on from zero current have a long transient time until they stabilize, making any modulation directly to zero current unfeasible at rates beyond 2.5 Gb/s [64]. Most modern fiber systems operate at 10 or 40 Gb/s.

Of course, all the above discussion was done considering one classical channel only, while many channels are routinely used in wavelength multiplexed systems in order to reuse a single optical fiber. If we only consider Raman spontaneous noise, it will grow linearly with the number of channels used. However, other effects come into play in multi-channel systems such as four-wave mixing (FWM) and cross-phase modulation (XPM). FWM is non-linear in nature, and will generate frequency combinations that depend on three frequencies

(e. g. $\omega_4 = \omega_1 + \omega_2 - \omega_3$), and can fall exactly in the quantum channel wavelength. The transmission of a quantum channels inside a fiber populated with several classical channels is a far from trivial feat, and further investigation is expected in this area.

4.2. Quantum Random Number Generation Protocol

One of the central requirements for security in QKD is that Alice and Bob must be able to generate their measurement basis choices in such a way that Eve with all her technological prowess cannot predict the values they choose. The only way to perform such a task is to use a random number generator. Although it sounds like a simple problem to solve, the generation of random numbers is a non-trivial matter. Let us think about this for a moment, how can we generate a random number inside a computer (the command "rand" for example, exists in many programming languages)? Once we begin to ponder it, we can see that it is impossible for a deterministic machine such as a computer, to generate a truly random value. What programming commands such as "rand" do, is to take an initial value known as a seed, perform a mathematical algorithm on it, and give the user the result as a random number [111]. In fact the only random component of these numbers is the seed. Clearly the quality of the random number generator depends upon the seed. In modern computers, a typical seed is the time of the day the rand command is run. Another seed which is sometimes used is the content of the last network packet present in the computer's Ethernet port when the rand command is typed. This last seed example is clearly more suited for the task since it is much harder to predict than the current time of the day. If we decided to use this as a random number generator for QKD, clearly we should use the last packet present in the network port as our seed choice, as the time of the day is too easy for Eve to predict. But can we be certain that Eve will not be able to guess our random numbers? The answer is no, since *in principle*, Eve could be eavesdropping in the entire network, and predict the packets being read by Alice and Bob's software-based random number generator.

The more we think about it, the more obvious it becomes that software-based random number generators are not the way to go when we want protection against an eavesdropper with unlimited access to technology. There are physical

processes which can give better seeds, such as chaotic process like noise fluctuations in a resistor. This is definitely harder to predict by Eve, but once again not impossible. What can we use that Eve cannot predict? Fortunately for us there are processes in nature that are truly random, and thus unpredictable. The answer of course, is given by quantum physics. The basic foundations of quantum physics tell us that given that the wavefunction of a particle is known, we can only then speak of the particle in terms of probabilities. If we can perform a measurement on a degree of freedom of a quantum particle with maximum uncertainty, then we have ourselves a random number which cannot be predicted.

Such a device is called a quantum random number generator (QRNG), and there have been successful devices built recently using the idea of which port a photon exits a beamsplitter [112, 113] and the time-of-arrival of a photon [114, 115]. These generators provide truly random numbers and if they are not used as a seed provider, but rather their output sequence is directly used to choose the basis (and in Alice's case to generate the actual key itself), then Eve has no way to guess the numbers. If it is used to generate seeds, and then expanded using a mathematical algorithm, the sequence generated in this way is no longer truly random and for this matter not secure [111]. Therefore to be complete foolproof against Eve, the QRNG must provide the random bits in the rate the system requires to operate, without any expansion of the random number sequence. Rates of Mbit/s is achievable with commercial QRNGs [24]. However there have been recent experiments with high-rate QKD, reaching Gbit/s data rates [54, 116], and it will likely become the standard in the near future. We present here a protocol which generates random numbers for QKD independent of the rate required, and furthermore, it only requires small modifications to the hardware, as it is based on the detectors already used in a typical QKD setup. It can fully replace QRNGs in the case of QKD with an entangled photon pair source or an HSPS, and can replace Bob's QRNG for a standard QKD setup.

We will first briefly explain how QKD works with an entangled photon pair source. Such a source produces entangled-photon pairs (we will use polarization entanglement as our example, but it works for any other degree of freedom). One photon of the pair is sent to Alice and the other to Bob as shown in Fig. 31. Let us assume the wavefunction generated by the source is

$|\psi\rangle = 1/\sqrt{2}\left(|H\rangle_a|V\rangle_b + |V\rangle_a|H\rangle_b\right)$ where the subscripts *a* and *b* stand for the photons going to Alice and Bob respectively. The basic idea behind this protocol relies on the fact that the photons going to Alice and Bob are entangled. It is a well known fact, that due to entanglement if Alice uses the same measurement basis as Bob (through polarization modulators PM_A and PM_B, which work as automatic wave plates) their measurement results will always be correlated, that is, for our wavefunction if Alice measures H, Bob will obtain V and vice-versa. The remarkable about this, is that *any* identical measurement basis yields perfect correlations. Ekert in 1991 realized this could be used for QKD if the measurement choices are performed at random and independently by Alice and Bob, hence each of them needs a QRNG [117]. It is possible to remove the requirement of QRNGs, by employing a passive basis choice at both Alice and Bob's stations, however four (or more) detectors are required [118]. The protocol briefly runs as follows: for each incoming photon of the pair, Alice and Bob choose a random measurement basis and record the results. After the photons are received they publicly reveal over a classical communications channel the measurement bases chosen for each detected photon. Like in BB84, they discard all values where incompatible measurement bases were used. The standard steps of BB84 now follow: Eve's presence verification, error correction and privacy amplification. This scheme has the advantage of having another security check: the violation of Bell's inequalities [1, 117]. If Eve attempts to perform an attack there will no longer be a violation of Bell's inequalities from the photon's correlations and therefore Eve is caught. In practice a modified version of Bell's inequalities called the Clauser-Horne-Shimony-Holt inequality (CHSH) [37] is used, since it allows a check of violation using directly measurable quantities. This scheme is secure even if Eve has control of the source [5].

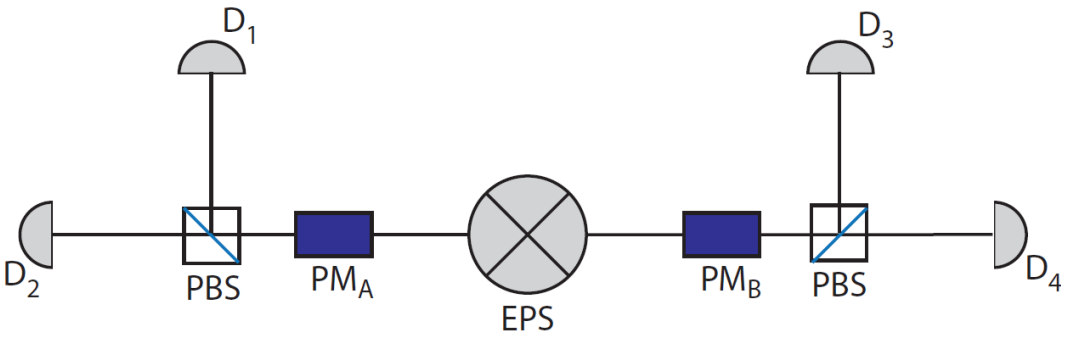

Figure 31 - Scheme for QKD with an entangled-photon source based on the E91 protocol. PBS: Polarization beam splitter; PM: Polarization modulator; EPS: Entangled photon source.

Our protocol is therefore meant to be used to perform the random choices required on an Ekert based QKD protocol with active-basis choices. We will later extend it to be used with BB84 with an HSPS for both Alice and Bob, or just Bob in the case of standard BB84. A recent theoretical modification [119] shows that three bases are needed at Alice, but Bob can use two (when compared to the original case that both need three) for QKD and a full check of the CHSH inequality. It runs as follows: In our proposal both Alice and Bob have a clock generator each, working asynchronously from each other. This signal can be easily generated within modern electronics already used in a QKD setup. The main idea is to generate the random numbers based on the number of clock pulses between consecutive photon detections, that is, between consecutive generations of electrical pulses in the output of their detectors. Since the entangled source may not be trusted, the following procedure is performed: initially, both Alice and Bob block their detector inputs and wait for the first dark count, thus obtaining random and independent integers equal to the number N_{A0} (N_{B0} for Bob) of clock pulses until either detector has fired. Alice (Bob) will proceed to calculate N_{A0} mod 3 \ (N_{B0} mod 2) and choose one of the 3 (2) needed bases for the first transmitted qubit depending on the result. The detector inputs are opened, the quantum transmission starts and they count the number of pulses N_{A1} (N_{B1}) until the next detection, perform N_{A1} mod 3 (N_{B1} mod 2), choose the basis for the next qubit and so on, where a random number $N_{AT(BT)}$ will be obtained between detections *T-1* and *T*. Since the times of detection follow an exponential distribution [114,115], the generated sequence will be random. As long as we can assume Eve is not looking inside the detectors (However, Eve can still ``hear'' the detection clicks without gaining any information, in exactly the same way as in the standard BB84 protocol), she will not be able to guess the bases used, as required in all QKD protocols. The scheme is presented in Fig. 32 for the particular case of the E91 protocol with polarization coding in optical fibers. Our protocol is independent of the coding method, and can be readily applied to phase coding systems.

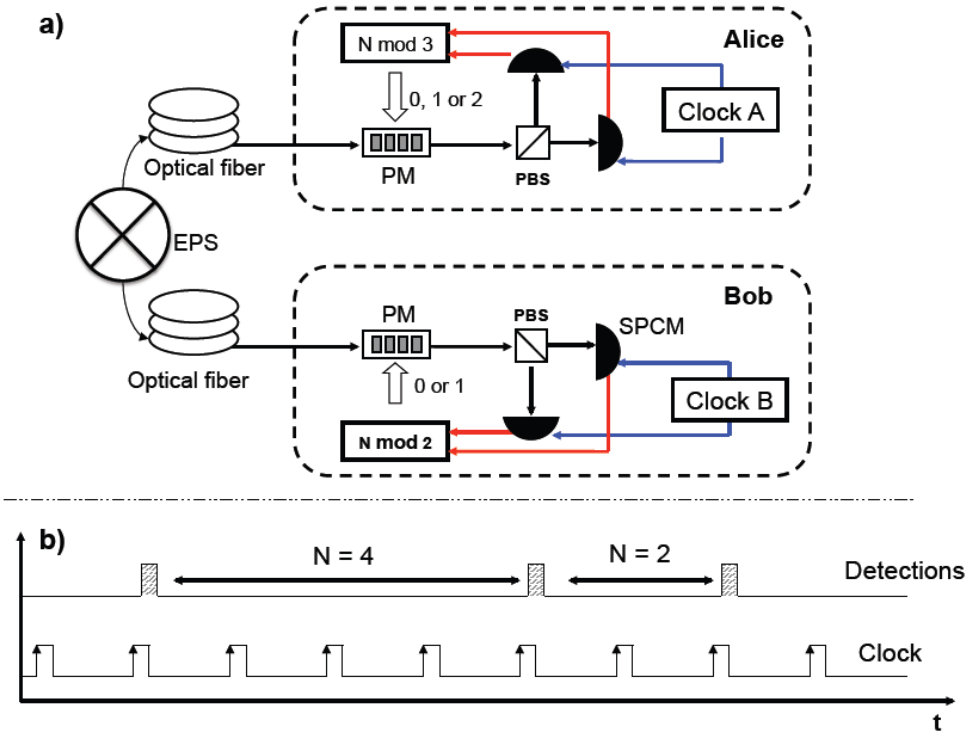

Figure 32 - Schematics of our proposal applied to the Ekert (E91) protocol. Black arrows represent optical connections, while blue and red ones depict electrical cables. EPS - Entangled photon source; PM - Polarization modulator; PBS - Polarizing beam splitter; SPCM - Single photon counting module. The master clock synchronizing Alice and Bob, as well as QKD electronics are omitted for the sake of clarity. b) Illustrative representation of the waveforms from the detection and clock pulses.

We can also extend this idea to the BB84 protocol if Alice has a HSPS, since she will have one detector yielding a trigger signal to pinpoint that an idler photon was created which is sent to Bob. Once again they also each have a local clock generator which they use as a timing reference. Alice performs her basis choices calculating N_{AT} mod 4 and converting the 4-valued number into two random bits. Bob performs the same procedure as before, he begins to count the N_{B0} number of clocks before any photons are transmitted until he detects a dark count (once again he blocks the detector input), and calculates N_{B0} mod 2 to determine the first basis to be used. He then proceeds calculating N_{BT} mod 2 for each received photon. Finally if the standard BB84 scheme is to be used with an attenuated pulsed laser source, then only Bob can use our protocol to generate random numbers. Since Alice does not detect the photon she does not have available to her a quantum event to be used as a random generator. In principle she can use a quantum non-demolition measurement (QND) and verify if a photon

is emitted by her laser, and with a local clock generator use this event to create a random number. The technology to perform such a measurement is not yet practical, therefore we shall only leave this case here as a possibility.

Let us now discuss what are Eve's options in cracking such a scheme. Her objective is to try to predict which bases Alice and Bob will use in the E91 protocol, or just Bob in BB84. Short of intercepting the photons (in which case her presence is revealed anyway through non-violation of the CHSH inequality), the simpler attack she can attempt is to perform a QND predicting the time instants a photon is passing through the fiber links to Alice and Bob. Assuming the QND is successful, Eve can try to predict the basis choices Alice and Bob will choose. Several factors come into play now. First of all detectors are not perfect, and if we assume real detectors are used (quantum efficiencies less than unity) then detections are randomized. This may not be enough to counter Eve, and it is not future-proof since detectors with extremely high efficiencies may appear in the future. What Alice and Bob can do is to use a local clock with a much higher resolution than the gate width of the detector (2.5 ns is a typical value for InGaAs SPADs). This way they add an extra degree of randomness to the system by detecting where in the gate pulse the photon arrives. If the coherence length of the photons is longer than the gate width (tricky in SPDC based sources), then Alice and Bob can be sure the time of arrival of the photon inside the gate window is truly random. In addition to this, the photons need to be single-mode inside the detection window, such that they are spatially indistinguishable. This is the only way to be immune against Eve. If this is not possible the best that can be done is to use a local clock, not only with a high-resolution, but also with jitter (in practice all clock signals exhibit some degree of jitter), to further randomize results.

If we now consider the poissonian probability of existing n photons inside a detection window with μ photons per pulse $p(n) = e^{-\mu}\mu^n / n!$, the probability of detecting a photon on the N_{th} gate window can be written as:

$$P(N) = (1-\mu\eta)^{N-1} \cdot \mu\eta \tag{3.7}$$

where η is the detection efficiency. From the poissonian distribution we can rewrite the probability of detecting a photon as:

$$P = 1 - e^{-\mu\eta} \tag{3.8}$$

Equation (3.8) can be interpreted simply as having a perfect non-resolving photon number detector with an external loss given by the detection efficiency. We can now use Eq. (3.8) to write the probability of detection as:

$$P(N) = \left(e^{-\mu\eta}\right)^{N-1} \cdot \left(1 - e^{-\mu\eta}\right) \tag{3.9}$$

Finally from Eq. (3.9) we write the probabilities of detecting photons in odd and even detection windows, summing over *N* for both cases:

$$P_{EVEN} = \frac{1}{1 + e^{\mu\eta}} \tag{3.10}$$

$$P_{ODD} = \frac{1}{1 + e^{-\mu\eta}} \tag{3.11}$$

From these two equations we note that the probability of odd and even detection events are different. This means the sequence generated from *N* mod 2 will be unbalanced in terms of zeros and ones. The above formulation was done using the gate window itself as the time unit. Intuitively it is easy to see that the bias will diminish if a higher resolution clock is used, vanishing completely at the limit of infinite high resolution, which reinforces the idea of using such a clock as explained before. Post-processing classical procedures can be used to balance the sequence [113], however the price we have to pay for this is a shortened sequence.

We can also extend the previous discussion to the case with light sources with thermal statistics. In this case the probability to find *N* photons per detection window with μ photons per window on average is [16]:

$$p(n)\frac{\mu^n}{(\mu+1)^{n+1}} \tag{3.12}$$

Using the same line of reasoning as before, we can arrive at the following probabilities for odd and even events:

$$P_{EVEN} = \frac{1}{\mu\eta + 2} \tag{3.13}$$

$$P_{ODD} = \frac{\mu\eta + 1}{\mu\eta + 2} \tag{3.14}$$

The probabilities for odd and even events once again differ, but the unbalance in the sequence can be made to vanish if a higher-resolution clock is used as explained before. Two proof-of-principle experiments were performed to demonstrate the idea, the first one uses a simple setup of a fiber pigtailed CW semiconductor laser (λ = 1549.32 nm) in series with a calibrated attenuator, which is then connected to an InGaAs SPAD, to which we triggered at a constant frequency using an external pulse generator. The results of this experiment have been presented in [120]. The output of the APD is connected to a fast A/D card (analog to digital) plugged into a computer. The trigger output from the pulse generator is connected to a second input of the same A/D card, and the data acquisition software we wrote counts the number of trigger pulses between each consecutive detection. Therefore we assemble the statistics of arrival times of single photons.

We employed a trigger frequency of 100 kHz, with an average photon number per detection window of 0.1, a typical value for QKD. The gate width used was 20 ns, which is quite wide compared to many QKD experiments. The reason for this is due to a timing problem in our APD, which reduces the quantum efficiency for narrow gate widths. Therefore, 20 ns was used in order to increase the quantum efficiency. Dark counts were also increased (10^{-4} per 1ns gate) but it is not as major issue as this is a proof-of-principle experiment. We obtained 500 x 10^3 counts and plotted the histogram of the times of arrival (Fig. 33). As expected the probability distribution of the arrival times is exponential since the probability to obtain *n* photons in a gate window follow a poissonian law [112].

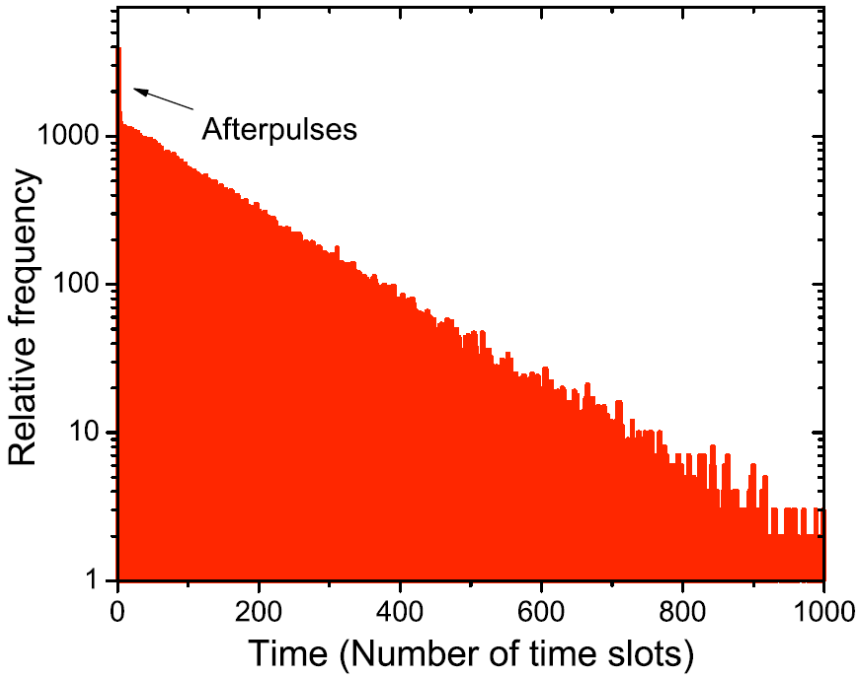

Figure 33 - Measured histogram of the number of time slots between two consecutive successful detections for μ = 0.1.

Observing the figure we notice two things. The first is that the reason for the unbalance comes from the exponential shape of the distribution itself, since it is always more probable for an odd event to occur than for an even one, and the slope of the distribution depends on the average photon number. The other is the clear point out of the curve in the first bin (the bins have been graphically enlarged to make the first bin stand out). Through simulations and other experimental runs, we have deduced the first bin is a result of afterpulsing. There is a current study going on to characterize afterpulses in SPADs using this technique [121].

The sequence which generated the histogram is used to create our random sequence through the $N \bmod 2$ operation, giving us a sequence of zeros and ones. The first question that comes to mind is, how random is our sequence. The first test we attempt is to calculate and plot the normalized auto-correlation function of the sequence. One of the requirements for randomness is that the sequence does not present patterns, and the auto-correlation function is a good test against repetitions (Fig. 34). As we can observe from the measurements, the function only displays a single central peak, with the rest being uncorrelated, a good sign that the sequence has no patterns. This is not a full guarantee that our

sequence is random, but it already points in the right direction. The sequence balance ratio is of 0.974 between zeros and ones.

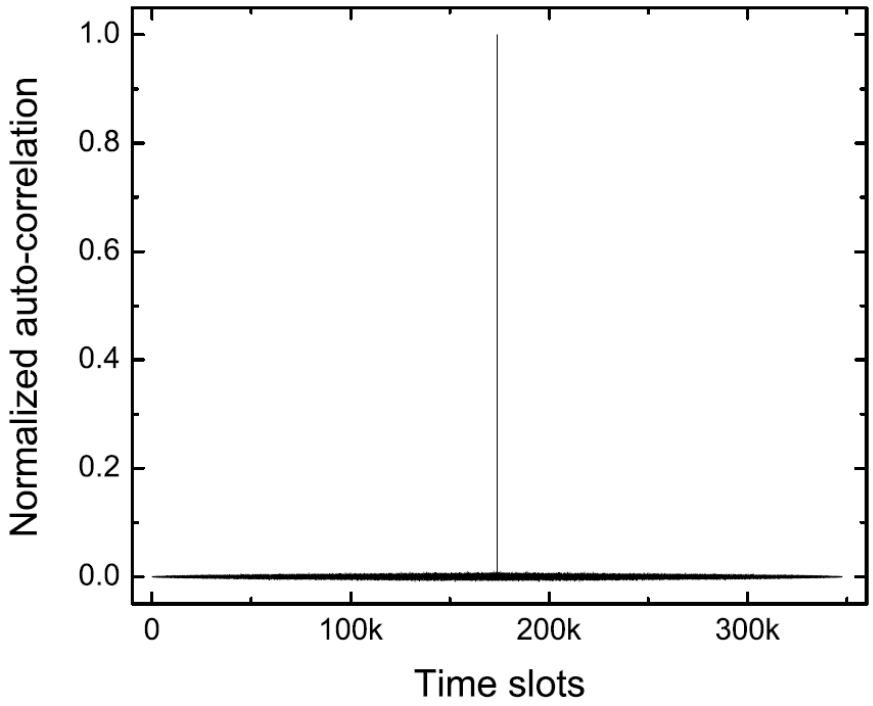

Figure 34 - Normalized auto-correlation for the random sequence generated from the distribution from Fig. 33.

There is a standard test suite to verify the randomness of a number developed by NIST and freely available on the Internet [122]. It is composed of 13 tests to be applied to a sequence, and each test gives a result called a p-value. As long as the p-value is larger than the confidence value α (for cryptographic applications, $\alpha = 0.01$), then the sequence is random with a very high probability [122]. The test expects a balanced random sequence, and if that is not the case, many of the tests fail. We generated two sequences of 1 million bits each (the number of bits required for a single run of the test) in order to perform the test twice. We increased the average photon number to $\mu = 0.4$ in order to speed up the measurement, otherwise the time taken for the data acquisition would be too long. The reason why time seems to be of an issue here is due to inefficiency in our data acquisition setup. The sequence balance ratio dropped to 0.944 due to the photon number increase, and as such, it does not pass in the NIST test. We balanced it using the simple procedure of XORing our sequence with a 0101… sequence, which is equivalently to flipping the bit assignments at each detection (even stops being zero and becomes one). The sequence was successfully balanced having

now a ratio of 0.9996 which is good enough for the NIST test. The results are presented in the table below:

NIST test	P-value 1	P-value 2
Frequency	0.496504	0.972877
Block-frequency	0.186886	0.618073
Cumulative-sums forward	0.712049	0.496736
Cumulative-sums reverse	0.300269	0.524704
Runs	0.060592	0.948969
Longest runs	0.130525	0.425877
Rank	0.365876	0.981847
DFFT	0.600927	0.129989
Universal	0.792907	0.087627
Apen	0.110230	0.406134
Serial 1	0.447454	0.566796
Serial 2	0.867164	0.399266
Linear complexity	0.956506	0.424975

These results clearly show our sequence is random according to the NIST test demonstrating the feasibility of our scheme. As a second proof-of principle experiment we used a SPDC process to create the photons used for the random number generation. This experiment represents what would be used in an Ekert-type QKD protocol. The results of this experiment have been published with a few improvements in [123]. We used a 20 mm long Periodically-Poled Lithium Niobate (PPLN) crystal pumped by a 532 nm CW Nd:YAG laser. The crystal is identical to the ones used in the two experiments of Chapter III, except that it is shorter. Therefore it provides type - I quasi-phase matching for $532 \rightarrow 809 + 1555\,\text{nm}$ when the crystal is heated at approximately 90ºC, this temperature is slightly different than the one used for the longer crystal in the previous experiments. The experimental setup is presented in Fig. 35. The pump light passes through an optical attenuator, and then goes through a half-wave plate to adjust the pump's polarization before the crystal. It is then focused on the 20 mm long crystal using an achromatic doublet lens L with a 100 mm long focal length. The beam is focused in the middle of the crystal, and the output beam is

collimated by an identical lens before the prism P, used to spatially split the generated beams and the pump. A bulk filter (RG 715) is placed before the fiber coupler (FC) to remove any residual pump light from the detector. An aspheric lens (f = 11 mm) is used to focus the signal beam on a standard 780 nm single mode fiber (SMF), mounted on a multi-axis translation stage. The fiber is connected to a Si Avalanche Photo Detector (Id Quantique ID100-MMF50). The output from the detector is finally connected to an A/D card (20 MSamples/s), which is attached to a personal computer to process the data. This time, we used the internal clock of the A/D card as our timing clock. The optical attenuator was adjusted so that a 150 kHz detection rate was obtained with optimized coupling. The measured input optical pump power on the crystal for that rate is 9.8 mW. The experiment we perform here is a perfect representation of Alice in the case where she uses a heralded single-photon source. It also represents the basic building block of the E91 protocol, with the source located somewhere between Alice and Bob. Our setup can therefore be easily upgraded into a single-crystal entangled photon pair source [84,124].

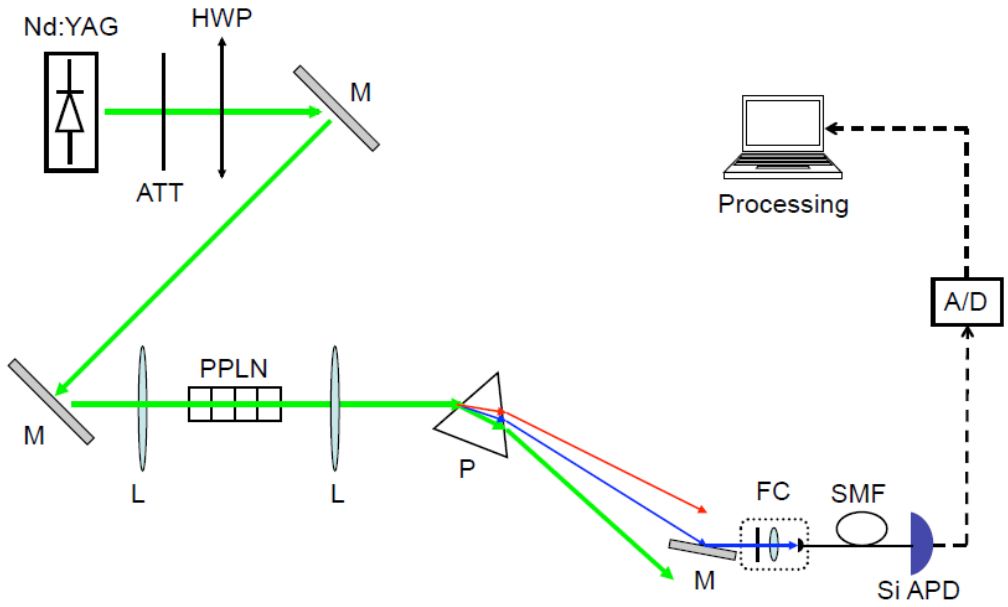

Figure 35 - Experimental setup: ATT: Optical attenuator; HWP: Half-wave plate; M: Mirror; L: Lens; PPLN: Periodically-poled lithium niobate; P: Prism; FC: Fiber coupler, here consisting of a multi-axis translation stage (not shown here), RG 715 high-pass filter, 11 mm focal length aspheric lens and fiber holder; SMF: 780 nm single mode optical fiber; APD: Avalanche photon detector; A/D: Analog to digital converter. The green, red

and blue arrows represent the pump, idler and signal beams respectively. The dashed lines represent electrical cables.

The next step is the NIST set of randomness tests. We generated a sequence of 20 million bits at 150 kHz count rate, using the previously described *N* mod 2 procedure. Since the clock resolution was limited by the A/D card sampling rate (20 MHz) it was not enough to entirely remove the bias, as discussed before. We applied the same balancing procedure with the XOR operation and increased the balance from 0.9968 to 0.9995, which was enough to pass the tests. The results for the 13 tests are presented in Fig. 36, which indicates that our sequence is random with a very good degree of confidence.

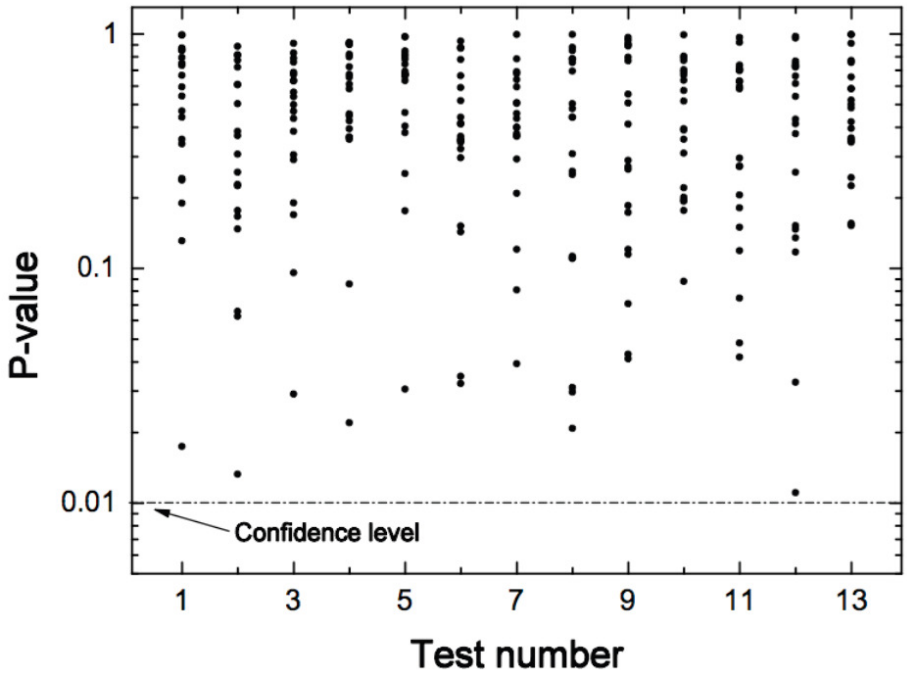

Figure 36 - P-values plotted for the NIST test suite individual tests for the 20 million bit generated sequence after bias removal. Each dot represents a run of 1 million bits for a particular test. The results are all above the confidence value for cryptography applications. The tests are: 1 - Frequency; 2 - Block frequency; 3 - Cumulative-sums forward; 4 - Cumulative-sums reverse; 5 - Runs; 6 - Longest runs; 7 - Rank; 8 - DFFT; 9 - Universal; 10 - Approximate entropy; 11 - Serial 1; 12 - Serial 2; 13 - Linear complexity.

A scheme was presented to perform true random basis choices for the E91 protocol which is based on the hardware which is already present in any QKD system. It may also be extended to be used by Bob in the BB84 protocol, or even Alice, if she uses a heralded single photon source. Our proposal has the advantage

of being readily scalable ``on-the-fly'' with the transmission rate without any active changes from the user, as long as high-resolution local clocks are used. Therefore, it could be used in future entangled based QKD networks [125] or any quantum cryptography system which employs a variable key rate. The protocol can be implemented with simple modifications and it replaces true RNGs for the active basis choices, decreasing the building cost of a practical QKD setup. We have shown that the generated sequence is indeed random like we expected, and supports our idea of random number generation in QKD systems. If Alice and Bob employ asynchronous clock generators with a timing resolution higher than the detection jitter of the single-photon counting modules, and the light source coherence time is longer than the detection window, then Eve cannot gain any information on the basis selection.

5
Transmission of Polarization Encoded Qubits in Optical Fibers

5.1. Introduction

The first experimental demonstration of QKD was done over a 30-cm free-space distance using polarization encoding [76]. There were some experiments with polarization encoding in optical fibers [65], however due to residual birefringence in optical fibers, phase encoding was adopted [66, 67]. Phase encoding became the dominant for of transmission in optical fibers [68, 69]. Free-space QKD has still used polarization encoding extensively however [59, 118].

Interestingly polarization encoding usage in optical fibers has grown in recent years [98, 125, 126, 127, 128, 129, 130, 131], and this trend is expected to grow. Some of them employed active polarization control [98, 128, 131], however all of these control methods are time-multiplexed with the key transmission. Another interesting way to make the transmission polarization insensitive is to make use of the idea of decoherence-free subspaces [22]. When any linear combination of the entangled states $\left|\psi^{+}\right\rangle$ and $\left|\psi^{-}\right\rangle$ are transmitted in an optical fiber, they are immune to birefringence fluctuations (as long as both photons are measured), and thus well suited for polarization encoded QKD [132]. However, the requirement to generate and detect both photons increase the complexity of the source and of the detection system, as well as being more sensitive to fiber loss [129].

An active polarization control system was developed within our group recently [78]. It differs from the control schemes used above in the sense that it operates continuously because it is wavelength multiplexed. It has the advantage of being able to compensate very fast birefringence fluctuations in the fiber, such as those present in aerial cables. The experiment was performed together with the group of Nicolas Gisin from the University of Geneva as a joint collaboration [133].

5.2. Control theory

Work on the idea of active polarization control for QKD began as early as 2005, from some simulation results showing that very closed spaced wavelengths have a high correlation in respect to rotations induced from birefringence fluctuations [134]. Since a control system obviously requires a feedback, why not use a classical channel close to the wavelength of the quantum bits to supply the necessary information? Early tries were made using a single control channel as feedback, however results were unsuccessful because we came to the conclusion that one single channel (containing a single element of information, which is simply the intensity of the light after a polarizer) was only enough to control orthogonal states. The conclusion was made that two channels were needed (each channel launched in the fiber with non-orthogonal polarizations) for full real-time control. Indeed we built such a system later using this idea [78].

BB84 using polarization encoding requires that four states are sent, typically $|H\rangle$, $|V\rangle$, $|+45\rangle$ and $|-45\rangle$. In an optical fiber the relation between the output polarization state and the input one is given by where U_F is the unitary operator representing the rotations caused by random birefringence fluctuations in the fiber. As shown in [78] feedback provided by two reference channels is enough to perform the unitary transformation U_T, where $U_T = U_F^{-1}$. This transformation undoes the unitary rotation caused by the fiber such that the output quantum state is: $|\psi\rangle_{OUT} = U_T U_F |\psi\rangle_{IN} = |\psi\rangle_{IN}$.

As we have mentioned, the two classical control channels have a different wavelength than the quantum channel, and in fact U_F is wavelength dependent. Therefore we can intuitively think that the control cannot be perfect since the unitary transformations for control and quantum wavelengths will be different. While it may not be perfect, under certain conditions *good enough*. As we have shown, as long as the fiber mean group delay is of the order of 1 ps or less, and the channel spacing is sufficiently small (0.8 nm), the QBER contribution due to the control system stays under 1 % during the vast majority of the time [78]. As was shown there are other possible control schemes [134], like using a single wavelength channel with two polarization components split within two amplitude

modulation frequencies, or combining both the wavelength separation method with the double amplitude modulation frequency within a single channel method, and taking the mean result. This method yields the best possible results, however it requires a more complex setup. We opted to use the wavelength separation option using two channels with no amplitude modulation as it is conceptually simpler to implement. It naturally fits in the ITU-T wavelength grid with channel spacing of 0.8 nm (Fig. 37). It also gives the same control performance as the method with a single channel and the double amplitude modulation according to simulations performed [135].

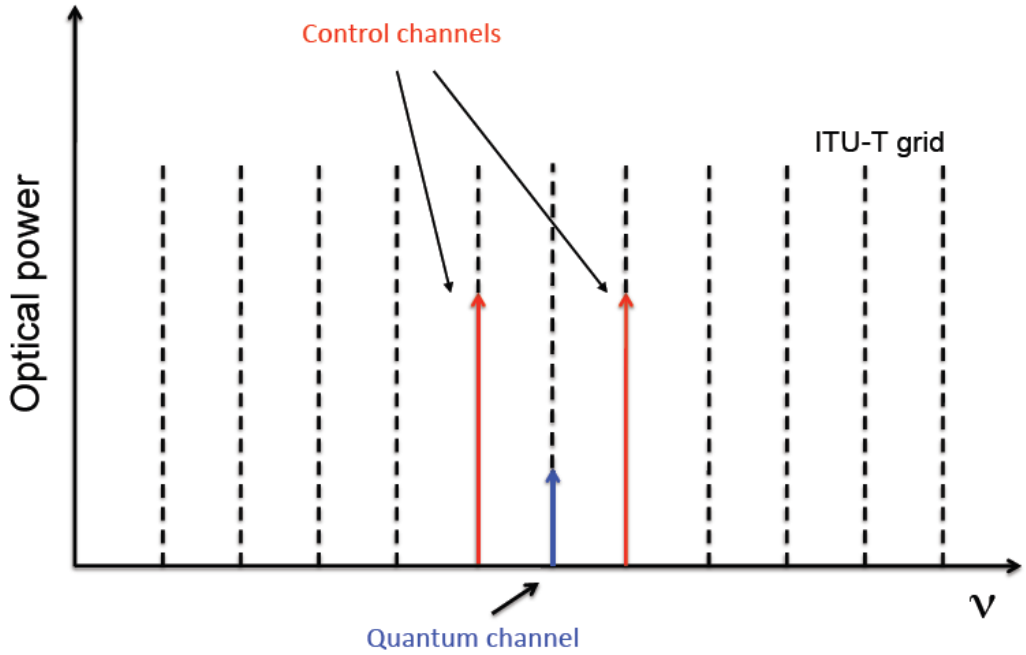

Figure 37 - Schematics showing the I_TU-T frequency grid (dashed black lines), the control channels (red) and the quantum channel (blue).

5.3. The experiment

The experiment is extensively based on the control system used in [78]. Based on the results of the Raman noise measurements presented in the previous chapter, one major change was needed. The original experiment was performed in a counter-propagating direction (single photons and classical channels work counter-propagatively). In that experiment noise was not a major issue because only a demonstration of the control scheme in the single-photon counting regime was required. For QKD, from our Raman measurements, the option to shut down

the side channel control lasers would not work counter-propagatively. Therefore we switched to a co-propagating configuration, even though the filtering requirements are steeper. The polarization control prototype was designed and assembled at PUC-Rio, fit in a standard 19-inch rack with 2U (units) height. It includes the optical components necessary for the polarization control, and the processing and driving electronics. The complete setup is shown in Fig. 38. The automatic polarization control system (APCS) is represented by the dashed orange line in the setup figure (A picture of the prototype is shown in Fig. 39). The electronics controlling the QKD setup supplied by the Geneva group is based on a previously used "plug and play" setup [68]. In the "plug and play" scheme Bob sends classical pulses to Alice, who then attenuates the signal to the single photon level, modulates them (including basis choice) and sends these attenuated pulses back to Bob, who finally performs his measurement basis choices and records the results from his detectors. Due to the "plug and play" configuration , Bob sends the trigger pulses to Alice, and the QKD electronics used in our experiment have to work in this way. Therefore we used a standard telecom DFB laser (Distributed Feedback) as the synchronization channel sending pulses from Bob to Alice (λ_S = 1547.72 nm) counter-propagating with the quantum and classical control channels.

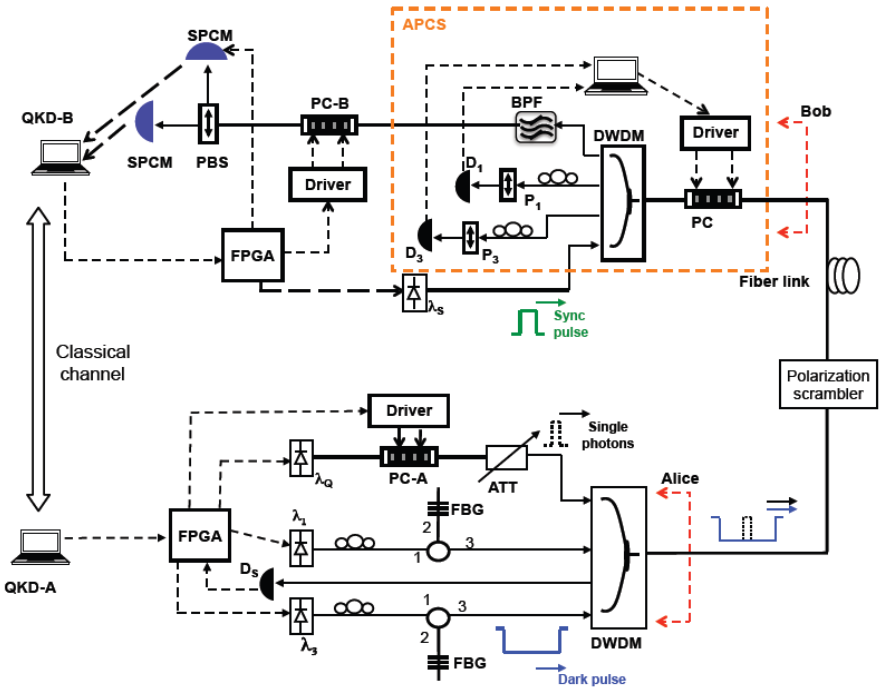

Figure 38 - Experimental setup for the polarization encoded QKD experiment. QKD-A and QKD-B: Alice and Bob's computers; FPGA: Field programmable gate array; D_S, D_1 and

D_3: Classical detectors; FBG: Fiber Bragg grating; PC-A and PC-B: Alice and Bob's $LiNbO_3$ polarization controllers; ATT: Optical attenuator; DWDM: Dense wavelength division multiplexer; P_1 and P_3: Polarizers; BPF: Band-pass filter; PBS: Polarizing beam splitter; SPCM: Single photon counting module. APCS: Automatic polarization control system. Solid lines represent optical fibers, while dashed ones are electrical connections. The direction of pulses is indicated in the figure.

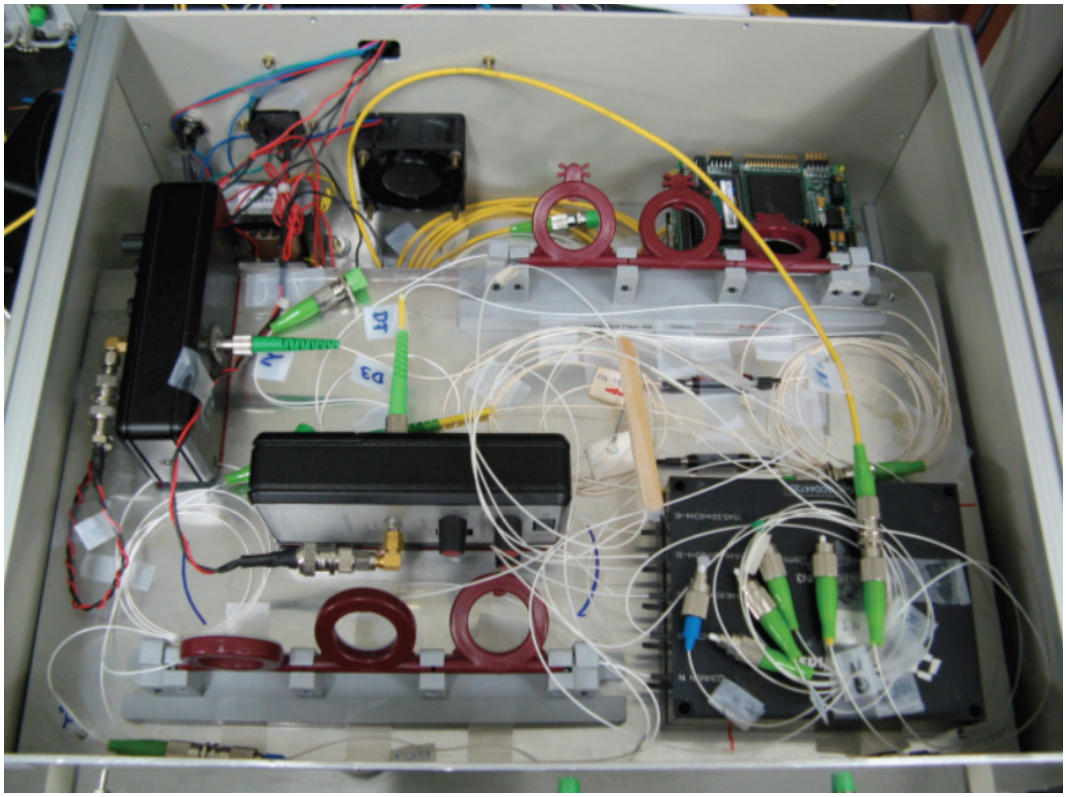

Figure 39 - Picture of the prototype. Clearly visible are the optical components: The polarization controllers, polarizers, detectors and the DWDMs. The electronics (power supplies, drivers and control CPU) are underneath the optics and thus not shown.

The two classical control channels are also composed of DFB lasers at wavelengths λ_1 = 1545.32 nm and λ_3 = 1546.92 nm. The quantum channel uses a pulsed attenuated DFB laser centered at λ_Q = 1546.12 nm. All three channels are multiplexed at Alice's setup using a commercial DWDM multiplexer with 1.4 dB insertion loss and an extinction ratio of at least -35 dB between adjacent channels and -45 dB between non-adjacent ones. Each side channel employs a circulator with a FBG centred at λ_Q to remove any ASE noise generated from the respective lasers, which would fall on the SPCM at Bob's side, rendering QKD impractical. A measurement of the spectra of the DWDMs is shown in Fig. 40.

As discussed before there are two main noise contributions we need to counter in order to perform a successful QKD session. The first is caused by "real" components, such as filters with finite extinction ratios and lasers emitting light outside of their center wavelength. The second contribution comes from the fiber itself, in the form of non-linear effects (Alice and Bob are connected by 16 km of standard optical fibers in our experiment) . The circulators with the Bragg gratings and the DWDMs used in the setup took care of the noise coming from cross-talk and imperfect components. In order to remove the Raman spontaneous contribution (the main form of in-fiber generated noise in our case), we created a short dark slot, in which the pseudo-single photon pulse is transmitted, of 13.5 ns by suppressing the laser current thus reducing the power to -90 dBm. We took this approach since, as mentioned in Chapter IV, the Raman spontaneous scattering induced is linear, and thus harder to remove by simply attenuating. Our method completely removes the Raman noise contribution, and it does not compromise the control performance since we use a low-pass filter on the detection side (not shown in Fig. 38). Fortunately for this experiment, the Raman noise contribution according to our measurements is smallest the closer the spacing between the classical and quantum channels (Fig. 41).

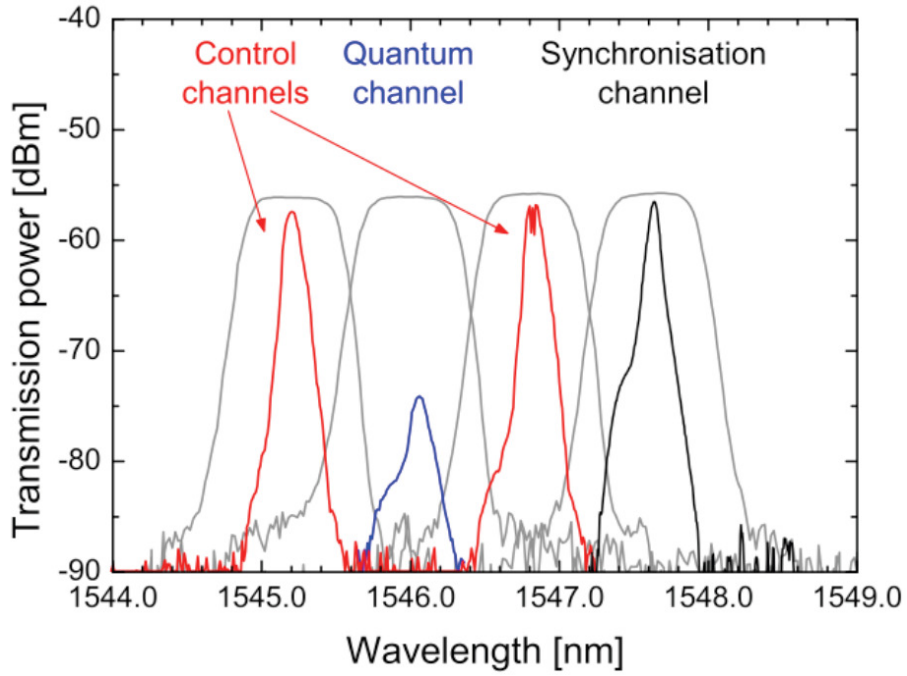

Figure 40 - Emission spectra of the two polarization control lasers (red), quantum channel laser (blue) and synchronization laser (black) aligned to 4 adjacent channels of the ITU-T band between 1545.32 and 1547.72 nm. The transmission spectra of the respective DWDM channels are shown as grey lines. Measurement performed by N. Walenta.

To temporally synchronize with Alice, Bob generates 1 ns long pulses with a repetition frequency of 5 MHz. These clock signals are transmitted in trains of 300 pulses in the same fiber as the quantum and classical side channels to Alice using a DFB laser centered at λ_Q = 1546.92 nm. In principle, backscattered photons from the synchronization pulses would induce noise in the quantum channel due to Raman and crosstalk from Rayleigh backscattering. However, these effects are not relevant in our setup since, at Alice, we delay the incoming signals by 50 ns in order to gain time to synchronize her internal clock with the incoming pulses before triggering the emission of the quantum signals. This delay acts as storage for the synchronization pulses such that no intersection of quantum signals and backscattered light takes place in the transmission fiber. We verified that the synchronization pulses did not affect the noise on the SPCMs at Bob.

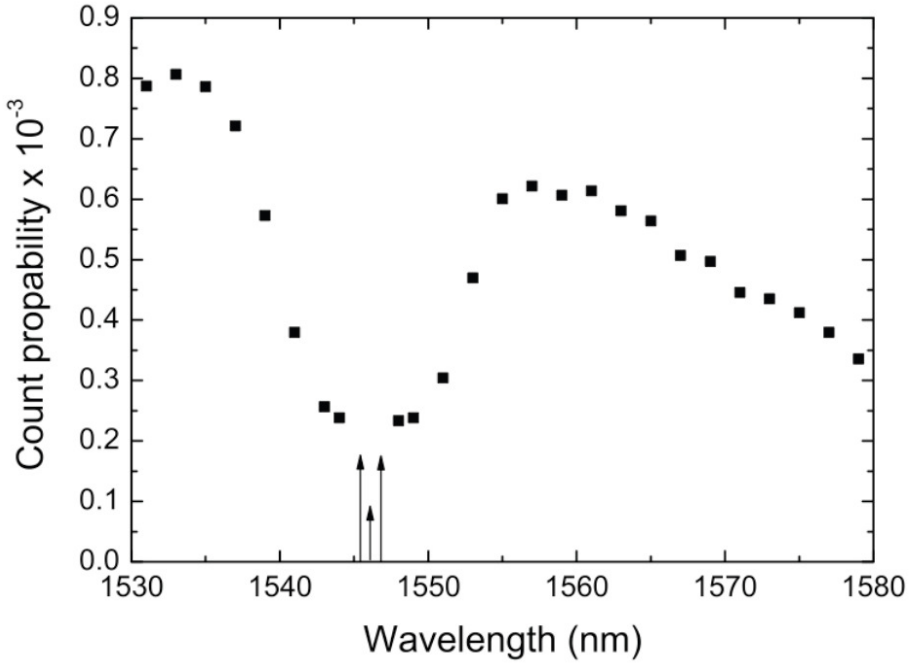

Figure 41 - Zoomed version of Fig. 27. The three arrows at the bottom represent the classical and quantum channels.

The SOP (State of polarization) of the faint laser pulses is modified with a fast $LiNbO_3$ fiber pig-tailed electro-optic polarization controller (PC-A, EOSPACE), with the modulating electrical signal generated from a FPGA (Field Programmable Gate Array) passing through a high voltage electronic driver (V_π approximately 50 V). This controller switches between the four distinct SOP needed in the BB84 protocol. An identical set of $LiNbO_3$ controller and driver is

used by Bob to change between the two measurement bases (PC-B). The modulator in our setup was able to change between orthogonal polarization states within 10 ns, as shown in Fig. 42. This measurement was performed by modulating the polarization state of a CW laser with one of the $LiNbO_3$ controllers, passing the optical signal through a polarizer and measuring the signal intensity with a p-i-n photodiode. From this we verify that our modulation speed is compatible with the 5 MHz repetition frequency generated from the electronics.

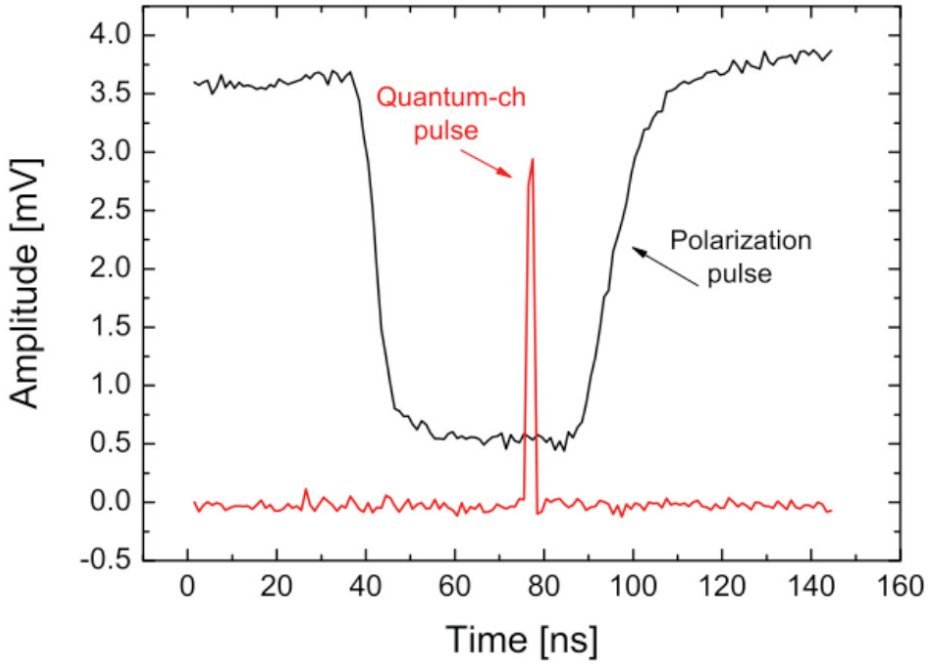

Figure 42 - Intensity measurements of a polarization pulse (black), and the quantum channel signal (red), operating on classical power levels. The polarization pulse was taken after a polarizer, with a CW laser, while switching the SOP between two orthogonal values, and back to the original. The quantum channel pulse is included here as a reference, showing that it is much narrower than the polarization bit. Measurement performed by N. Walenta.

The classical side channels are separated by the DWDM and pass through linear polarizers with their optical axis adjusted to be non-orthogonal using manual polarization controllers [78]. Their optical intensities after the polarizers are measured by classical p-i-n photodiodes and fed to the control computer for processing. Its control algorithm maximizes the intensity of both control channels at the same time by changing the polarization state of the optical signals before splitting at the DWDM. By maximizing both side channel intensities simultaneously the original input polarization states are recovered. The whole

setup is controlled by personal computers that send out the necessary electrical signals to the optical components to perform a QKD session, and perform the classical procedures required by BB84. The classical channel between Alice and Bob was realized with an USB connection between both systems.

Before performing a quantum transmission, the entire setup is calibrated by adjusting the polarization of the quantum channel as well as both side channels. For the quantum channel, two manual polarization controllers (not shown in Fig. 38) before PC-A and PC-B were used to align the input polarization state with the $LiNbO_3$ polarization modulator for identical maximum rotations on the Poincaré sphere. Another manual polarization controller (also not shown in figure 38) is placed at Bob after his PC-B to align the state to the axis of the subsequent polarizer.

The polarization states of the side channel lasers were set with two manual controllers to be non-orthogonal. We have improved on the previous scheme in such a way that the control will work properly as long as the side-channels are non-orthogonal, but not necessarily maximally overlapped as it used to be the case [78], which makes the system more robust and considerably easier to align than before. The alignment procedure only needs to be done once, before initializing the transmission. We note that this adjustment could be performed automatically by employing additional $LiNbO_3$ controllers, and as such, our system could be used in a commercial environment where no manual intervention is needed.

After alignment of the entire system we tested the performance of the setup initially with the stabilization system installed but not active. Alice's quantum signals were attenuated to obtain an average of μ = 0.1 photons per pulse. With a side channel laser power of -7.4 dBm each, but without the stabilization system running and the polarization scrambler turned off, the prepared states yielded a visibility of 97.2 % corresponding to a minimal QBER of 1.4 %. The measured QBER was 1.6 %, with an optical share $QBER_{opt}$ = 0.7 % which is caused by the detection of photons in the wrong detector, mainly due to the limited 22 dB extinction of Bob's polarizing beam splitter. Another share of $QBER_{det}$ = 0.1 % is caused by noise counts due to the SPCMs and a share of $QBER_{side}$= 0.8 % is caused by noise due to crosstalk and photons generated by Raman scattering in the side channels. With the stabilization system active, the total QBER increased by 1.1 %. This can be ascribed to an increase in the optical

share $QBER_{opt}$ due to fluctuations of the polarization state inherently induced by the stabilization algorithm.

Before demonstrating QKD we characterize the performance of the stabilization system even in the presence of fast polarization changes using the scrambler. A voltage ramp can be applied to each piezo crystal, which performs a polarization rotation of 2π back and forth on the Poincaré sphere at a tunable frequency. As such, a scrambling frequency of 1 Hz means a polarization rotation of 4π per second. It should be noted that such extreme polarization fluctuations are rarely expected in normal environments.

In order to reduce the influence of detector and side channel noise to less than 0.1 % during the following characterization, we increase the average photon number to μ = 1.0 per pulse. We constantly prepare the same state at Alice and measure in the corresponding basis at Bob, in order to eliminate any possibility of errors induced by the polarization modulators. Figure 43 then shows the optical share $QBER_{opt}$ measured at different voltage ramp frequencies applied to the scrambler. Each point is averaged over 50 measurements, with 1 million photon pulses sent from Alice to Bob per measurement. The results show that $QBER_{opt}$ stays constantly under 6 % for scrambling frequencies up to 16 π/s, and increasing the rotations to 40 π/s, $QBER_{opt}$ has an average of 7.5 %, well below the limit of 11% [7].

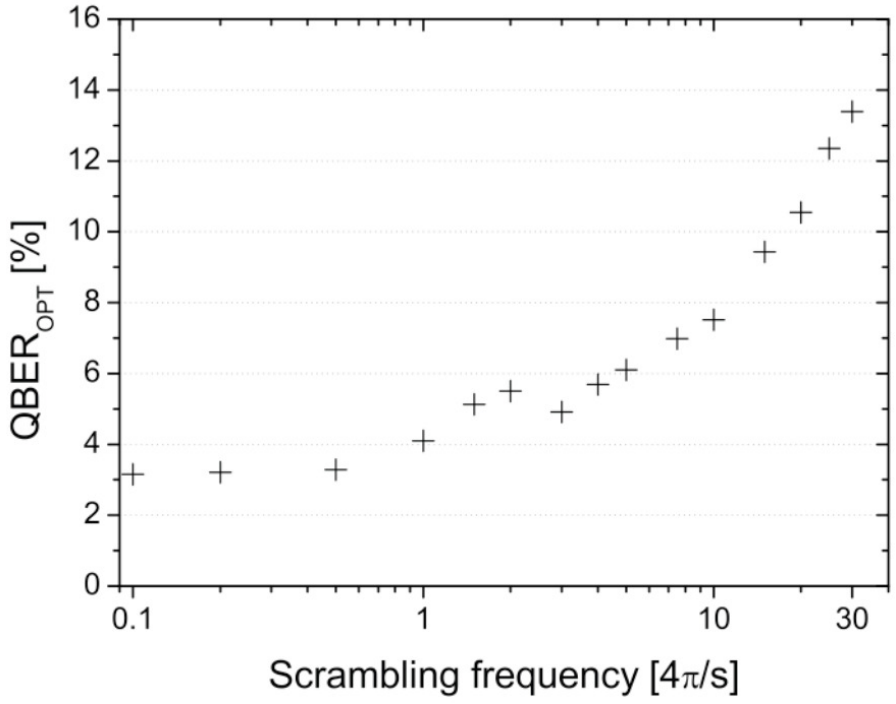

Figure 43 - The optical share $QBER_{opt}$ as a function of the scrambling frequency demonstrating the stabilization capability of the control system under rapid polarization changes. Each value is averaged over 50 measurements, with 1 million photon pulses sent per measurement. Measurement performed by N. Walenta.

To demonstrate the applicability of the stabilization system for QKD under the condition of random polarization changes, as it occurs in aerial fibres or under thermal or mechanical stresses, we replaced the piezo-electric scrambler by a manual polarization modulator. Unfortunately, an electronic problem with Bob's polarization modulator PC-B reduced the stability and extinction of its modulation during a key exchange at 5 MHz. This forced us to simulate a random key exchange by measuring Alice's randomly prepared qubits first in one basis at Bob and then, in a subsequent measurement, in the other basis. In Fig. 44 both measurements are combined on top of each other with black points indicating key exchanges with measurements in Bob's first basis and red points in the second, respectively. This problem, along with errors in the alignment, is also the reason for the slightly increased QBER during the key exchange demonstration.

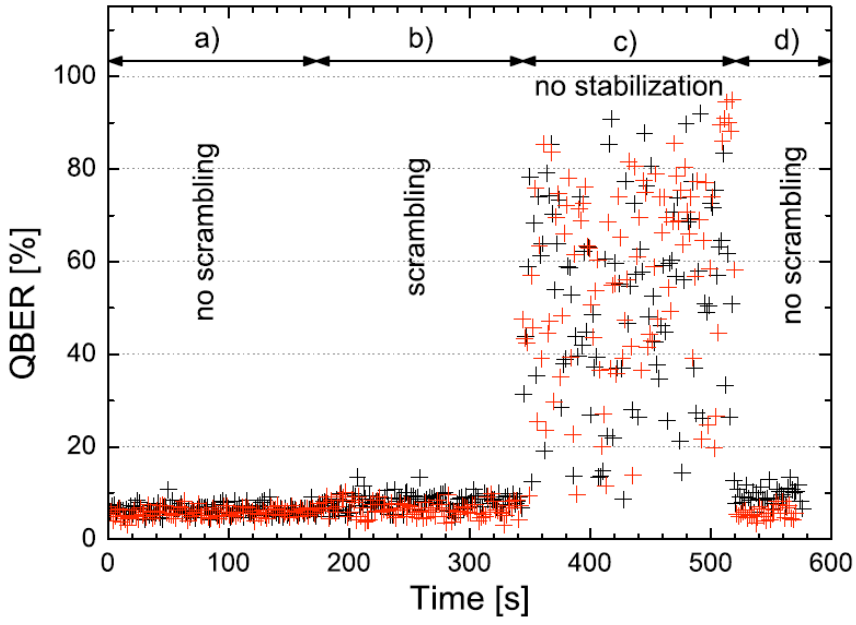

Figure 44 - QBER as a function of time under different conditions. a) No polarization scrambling. b) Polarization scrambling with active stabilization. c) Polarization scrambling without stabilization system. d) Re-stabilization after the system is reactivated. Each point corresponds to 1 million sent qubits. Black and red points distinguish measurements in different bases at Bob (see text for details). Measurement performed by N. Walenta.

Still, figure 44 shows the effectiveness of the stabilization system when the polarization state is randomly scrambled in the order of a few rad/s. Again, each point represents a key exchange of one million sent qubits. In the first section of the figure, (part a) keys are distributed with the stabilization system running but without any polarization scrambling. In the second section (part b) the average QBER increases by only 1.2 % during the key exchange although the polarization states are continuously and randomly scrambled. By comparison, without the stabilization system the QBER would increase dramatically with an average of around 50 % (part c) making any quantum key distribution impossible. The last section (part d) reveals that the system is able to re-stabilize immediately when it is reactivated.

The scheme implemented here demonstrates that it is possible to achieve real-time continuous control of the polarization state of single photons along a 16 km long optical fiber link, with an active polarization scrambler connected in series. We have demonstrated the feasibility of quantum key distribution employing polarization encoded qubits in optical fibers, in situations where the SOP of the transmitted photons is subject to fast random variations. The scheme was assembled using only standard off-the-shelf telecom components, and can be used with other single-photon sources, such as those based on SPDC. Furthermore our setup allows other applications requiring polarization encoding in long-distance quantum communications in optical fibers.

6
Conclusions and future developments

The field of quantum communications is losing its status of just “cool” physics and ground-breaking experiments to having real-world practical applications, and thus starting to integrate within the field of engineering. This is just one more example of fields becoming ever more multi-disciplinary. This field-merging trend is likely to continue for a long time and it is one more way of demonstrating that science has no boundaries.

For many engineers, quantum physics is something very far away from regular day-to-day activity, only mentioned at a general physics course as part of most elementary curricula. For others, some deeper knowledge is required to work in fields such as electronics or optics. Still for most engineers, to deal with individual quanta used to sound like work that only physicists would do. This statement could not sound more wrong in the age of miniaturization we are moving towards. Everyday devices shrink, computers get more powerful and technology gets more widespread use. With this comes a price: As components features get smaller and smaller the semi-classical physics that govern their behavior, and which has served us so well since the invention of the transistor, may no longer be valid. A full quantum picture is needed, and many theoretical aspects are already solved. We already know many different ways of how quantum information and processing works, and which operations it can perform. Many experiments have been done with successful and important results, however integration within systems outside of the lab are still lacking. Until a few years ago there had been few trials performed in real-world conditions.

This picture is steadily changing, however, as the commercial applications begin to see a need to use quantum information as well as its classical counterpart. The most clear example of this is quantum key distribution since digital security gets many headlines in the news nowadays. QKD is not yet ready for widespread use, but when we compare the latest research results compared to 10-15 years ago

we can see how much it has advanced. It is difficult to predict where we will be 15 years from now in QKD, but we can only expect to see its use more diffused.

This thesis, written in an electrical engineering department, is one more attempt to bridge the worlds of engineering and experimental physics. As such, it was written mostly with an engineering point of view focusing on how the experiments were done. In Chapter 2 a brief introduction to quantum communications was given, with the aim of aiding newcomers to understanding the engineering problems of experimental quantum communications. It is not meant as a self-contained introduction, and references are given as appropriate. Readers seeking to know more are encouraged to look into those.

Chapter 3 contains the main results of the two experiments the author took part in during his stay at KTH in Stockholm. The first experiment used a narrowband non-degenerate entangled photon pair source, with the signal photon detected locally by Alice, and the idler sent to Bob over 27 km of SMF-28 optical fiber. The synchronization signal is sent through the same fiber using wavelength multiplexing with a channel separation of only 0.8 nm, making it compatible with optical networks. The visibility results achieved show that QKD is possible with such a setup. The other experiment involved the construction and characterization of a non-degenerate heralded single-photon source, to be used in a QKD experiment with the decoy state method implemented. This was the first time decoy states were used experimentally with a source based on SPDC. Results matched the theoretical predictions, and in spite of our lossy setup, a successful key exchange was achieved with satisfactory results.

In Chapter 4 the results from the two main experiments performed at PUC-Rio after the author's return from Stockholm. The first is a study of Raman induced noise generated from a classical channel onto a quantum channel, both present in the same optical fiber. This study was motivated when the setup for the polarization control experiment presented in Chapter 5 was being initally tested. The study showed that transmission of classical and quantum channels simultaneous in the same fiber is non-trivial, but possible with current technology. Solutions to minimize the impact of Raman noise, such as narrower filters, and low transmitted powers were suggested. The other experiment was based on an idea that came up one day on a lab discussion on how to generate truly random numbers. The protocol we designed can generate truly random numbers

independently of the rate the system works on, and is secure against Eve's attacks. A proof-of-principle experiment was performed demonstrating the validity of the idea.

Finally Chapter 5 presented an experiment done in collaboration with the GAP-Optique, from the University of Geneva. The prototype of the automatic polarization control system was assembled and tested at PUC-Rio, and the quantum key exchange done at Geneva. Results are very promising, showing that it is possible to transmit secure keys with polarization-encoded qubits using our prototype even in the presence of fast polarization changes applied to the single-photons via a polarization scrambler.

The results presented in this work leave a few doors open. The polarization control system we developed can be used in future experiments requiring polarization encoding in optical fibers, such as long-distance Bell-state measurements. It is also possible to do a polarization encoded key exchange in an installed fiber cable subjected to strong polarization fluctuations such as an aerial cable. It also is worthwhile to study the Raman noise issue further, performing simulations and measurements with fiber spools of different lengths, as well as characterizing other non-linear effects. Finally one other route to pursue is a theoretical analysis of the security of the random number generation protocol.

7
Bibliography

[1] HERBERT N. Quantum Reality. **Anchor Books**. New York, 1985.

[2] STREETMAN B. G. Solid State Electronic Devices, Third Edition. **Prentice-Hall International**, Eaglewood Cliffs, N. J., 1990.

[3] SALEH A. B.; TEICH C. M. Fundamentals of Photonics, **Wiley**, New York, 1991.

[4] BENNETT C. H.; SHOR P.W. Quantum Information Theory, **IEEE Transactions on Information Theory**, Vol. 44, No. 6, 1995.

[5] BOUWMEESTER D.; EKERT A. and ZEILINGER A. The physics of quantum information. **Springer**, New York, 2001.

[6] LO H-K.; POPESCU S. and SPILLER T. Introduction to Quantum Computation and Information, **World Scientific**, Danvers, Maryland, 1998.

[7] GISIN N. et al, Quantum Cryptography, **Reviews of Modern Physics**}, Vol. 74, p. 145-195, 2002.

[8] BOUWMEESTER D. et al, Experimental Quantum Teleportation, **Nature (London)** Vol. 390, pp.575-579, 1997.

[9] NIELSEN M. and CHUANG I. Quantum Computation and Information, **Cambridge University Press**, Cambridge, 2002.

[10] SHANNON C. E. A Mathematical Theory of Communication, **Bell System Technical Journal**, Vol. 27, pp. 379-423, 623-656, 1948.

[11] IMAMOGLU A. et al, Quantum information processing using quantum dot spins and cavity QED, **Physical Review Letters**, Vol. 83, pp. 4204, 1999.

[12] HAYKIN S., Communication Systems 4th Edition, **Wiley**, 2001.

[13] KYEES P. J.; MCCONNELL R. C. and SISTANIZADEH K., ADSL: a new twister-pair access to the information highway, **IEEE Communications Magazine**, Vol. 33, 52, 1995.

[14] COHEN-TANNOUDJI C.; DIU B. and LALOË F., Quantum Mechanics Vol. 1, **Wiley-VCH**, Paris, France 1977.

[15] LEWIS G. N., The conservation of photons, **Nature (London)**, Vol. 118, 874, 1926.

[16] FOX M., Quantum optics: an introduction, **Oxford University Press**, Great Britain, 2006.

[17] VEDRAL V., Modern foundations of quantum optics, **Imperial college press**, London, Great Britain, 2005.

[18] MANDEL L. and WOLF E., Optical coherence and quantum optics, **Cambridge University Press**, New York, USA, 1995.

[19] ASPECT A.; GRANGIER P and ROGER G., Experimental tests of realistic local theories via Bell's theorem, **Physical Review Letters**, Vol. 47, 460, 1981.

[20] BEUGNON J. et al, Quantum interference between two single photons emitted by independently trapped atoms, **Nature (London)** Vol. 440, 779, 2006.

[21] DELÈGLISE S. et al, Reconstruction of non-classical cavity field states with snapshots of their decoherence, **Nature (London)** Vol. 455, 510, 2008.

[22] LIDAR D. A. and WHALEY K. B., Decoherence-free subspaces and subsystems, **arXiv:quant-ph/0301032v1**, 2003.

[23] ZUREK W. H., Decorerence, einselection and the quantum origins of the classical, **Reviews of Modern Physics** Vol. 75, 715, 2003.

[24] www.idquantique.com

[25] www.magiqtech.com

[26] YOUNG R. J.; ELLIS D. J. P.; STEVENSON M. R.; BENNETT A. J.; ATKINSON P.; COOPER K.; RITCHIE D. A. and SHIELDS A. J., Quantum-dot sources for single photons and entangled photon pairs, **Proceedings of the IEEE**, Vol. 95, 1805, 2007.

[27] STRAUF S. et al, High-frequency single-photon source with polarization control, **Nature Photonics**, Vol. 1, 704, 2007.

[28] BOYD R. W., Non-linear optics, **Academic Press**, San Diego, USA, 2003.

[29] LJUNGGREN D., Entanglement in quantum communication: Preparation and characterization of photonic qubits, **PhD thesis**, KTH Stockholm, 2006.

[30] TANZILLI S.; TITTEL W.; DE RIEDMATTEN H.; ZBINDEN H.; BALDI P.; DE MICHELI M.; OSTROWSKY D. B. and GISIN N., PPLN waveguide for quantum communication, **European Physical Journal D**, Vol. 18, 155-160, 2002.

[31] TENGNER M., Photonic qubits for quantum communications: Exploiting photon-pair correlations; from theory to applications, **PhD thesis**, KTH Stockholm, 2008.

[32] HONG C. K. and MANDEL L., Experimental realization of a localized one-photon state, **Physical Review Letters**, Vol. 56, 58, 1986.

[33] FASEL S.; ALIBART O.; TANZILLI S.; BALDI P.; BEVERATOS A.; GISIN N. and ZBINDEN H., High-quality asynchronous heralded single-photon source at telecom wavelength, **New Journal of Physics**, Vol. 6, 163, 2004.

[34] WANG Q.; CHEN W.; XAVIER G.; SWILLO M.; ZHANG T.; SAUGE S.; TENGNER M.; HAN Z.-F.; GUO G.-C. and KARLSSON A., Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source, **Physical Review Letters**, Vol 100, 090501, 2008.

[35] KWIAT P. G.; MATTLE K.; WEINFURTER H.; ZEILINGER A.; SERGIENKO A. V. and SHIH Y., New High-Intensity Source of Polarization-Entangled Photon Pairs, **Physical Review Letters**, Vol 75, 4337, 1995.

[36] EINSTEIN A.; PODOLSKY B. and ROSEN N., Can quantum-mechanical description of physical reality be considered complete?, **Physical Review**, Vol. 47, 777, 1935.

[37] CLAUSER J. F.; HORNE M. A.; SHIMONY A. and HOLT A. R., Proposed Experiment to Test Local Hidden-Variable Theories, **Physical Review Letters**, Vol. 23, 880, 1969.

[38] WEIHS G.; JENNEWEIN T.; SIMON C.; WEINFURTER H. and ZEILINGER A., Violation of Bell's inequality under strict Einstein locality conditions, **Physical Review Letters**, Vol. 81, 5039, 1998.

[39] TITTEL W.; BRENDEL J.; ZBINDEN H. and GISIN N., Violation of Bell's inequalities by photons more than 10 km apart, **Physical Review Letters**, Vol. 81, 3563, 1998.

[40] PAN J.-W.; CHEN Z.-B.; \.ZUKOWSKI M.; WEINFURTER H. and ZEILINGER A., Multi-photon entanglement and interferometry, arXiv:0805.2853v1 [quant-ph], 2008.

[41] KWIAT P. G.; WAKS E.; WHITE A. G.; APPELBAUM I. and EBERHARD P. H., Ultrabright source of polarization-entangled photons, **Physical Review A**, Vol. 60, R773, 1999.

[42] KWIAT P. G.; STEINBERG A. M. and CHIAO R. Y., High-visibility interference in a Bell-inequality experiment for energy and time, **Physical Review A**, Vol. 47, R2472, 1993.

[43] FRANSON J. D., Bell inequality for position and time, **Physical Review Letters**, Vol. 62, 2205, 1989.

[44] LJUNGGREN D. and TENGNER M., Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode optical fibers, **Physical Review A**, Vol. 72, 062301, 2005.

[45] WANG L. J.; HONG C. K. and FRIBERG S R, Generation of correlated photons via four-wave mixing in optical fibres, **Journal of optics B: Quantum and semiclassical optics**, Vol. 3, 346, 2001.

[46] LI X.; VOSS P. L.; SHARPING J. E. and KUMAR P., Optical-fiber source of polarization entangled photons in the 1550 nm telecom band, **Physical Review Letters**, Vol. 94, 053601, 2005.

[47] LI X.; LIANG C.; LEE K. F.; CHEN J.; VOSS P. L. and KUMAR P., Integrable optical-fiber source of polarization-entangled photon pairs in the telecom band, **Physical Review A,** Vol. 73, 052301, 2005.

[48] TAKESUE H. and INOUE K., Generation of-1.5 μm band time-bin entanglement using spontaneous fiber four-wave mixing and planar light-wave circuit interferometers, **Physical Review A**, Vol. 72, 041804(R), 2005.

[49] RARITY J. G.; FULCONIS J.; DULIGALL J.; WADSWORTH W. J. and RUSSELL P. ST. J., Photonic crystal fiber source of correlated photon pairs, **Optics Express**, Vol. 13, 534, 2005.

[50] FULCONIS J.; ALIBART O.; O'BRIEN J. L.; WADSWORTH W. J. and RARITY J. G., Nonclassical interference and entanglement generation using a photonic crystal fiber pair photon source, **Physical Review Letters**, Vol. 99, 120501, 2007.

[51] KARLSSON A.; BOURENNANE M.; RIBORDY G.; ZBINDEN H.; BRENDEN J.; RARITY J. and TAPSTER P., A single-photon counter for long-haul telecom, **IEEE Circuits & Devices Magazine**, Vol. 15, pp. 34-40, 1999.

[52] THEW R. T.; TANZILLI S.; KRAINER L.; ZELLER S. C.; ROCHAS A.; RECH I.; COVA S.; ZBINDEN H. and GISIN N., Low jitter up-conversion detectors for telecom wavelength GHz QKD, **New Journal of Physics**, Vol. 8, 32, 2006.

[53] GOL'TSMAN G. N.; OKUNEV O.; CHULKOVA G.; SEMENOV A.; SMIRNOV K.; VORONOV B.; DZARDANOV A.; WILLIAMS C. and SOBOLEWSKI R., Picosecond superconducting single-photon optical detector, **Applied Physics Letters**, Vol. 79, 705, 2001.

[54] TAKESURE H.; NAM W. S.; ZHANG Q.; HADFIELD R. H.; HONJO T.; TAMAKI K. and YAMAMOTO Y., Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, **Nature Photonics**, Vol. 1, 343, 2007.

[55] TEMPORÃO G.; TANZILLI S.; ZBINDEN H.; GISIN N.; AELLEN T.; GIOVANNINI M. and FAIST J., Mid-infrared single-photon counting, **Optics Letters**, Vol. 31, 1094, 2006.

[56] RIBORDY G.; GAUTIER J. D.; ZBINDEN H. and GISIN N., Performance of InGaAs/InP avalanche photodiodes as gated-mode counters, **Applied Optics**, Vol. 37, 2272, 1998.

[57] NAMEKATA N.; SASAMORI S. and INOUE S., 800 MHz single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating, **Optics Express**, Vol. 14, 10043, 2006.

[58] YUAN Z. L.; KARDYNAL B. E.; SHARPE A. W. and SHIELDS A. J., High speed single photon detection in the near infrared, **Applied Physics Letters**, Vol. 91, 041114, 2007.

[59] MANDERBACH-SCHMITT T., et al, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, **Physical Review Letters**, Vol. 98, 010504, 2007.

[60] HUGHES R. J.; NORDHOLT J. E.; DERKACS D. and PETERSON C. G., Practical free-space quantum key distribution over 10 km in daylight and at night, **New Journal of Physics**, Vol. 4, 43, 2002.

[61] COLVERO C. P., Análise experimental de sistemas de comunicação ópticas no espaço livre em diferentes comprimentos de onda, **PhD thesis**, PUC-Rio, Rio de Janeiro - Brazil, 2006 (available in portuguese only).

[62] TEMPORÃO G. P.; ZBINDEN H.; TANZILLI S.; GISIN N.; AELLEN T.; GIOVANNINI M.; FAIST J. and VON DER WEID J. P., Feasibility study of free-space quantum key distribution in the mid-infrared, **Quantum Information and Computation**, Vol. 8, 1, 2008.

[63] KAISER G., Optical fiber communications third edition, **McGraw Hill**, USA, 2000.

[64] AGRAWAL G. P., Fiber-optic communication systems second edition, **Wiley interscience**, USA, 1997.

[65] BREGUET J.; MULLER A. and GISIN N., Quantum cryptography with polarized photons in optical fibers: Experiment and practical limits, **Journal of Modern Optics**, Vol. 41, 2405, 1994.

[66] BENNETT C. H., Quantum cryptography using any two nonorthogonal states, **Physical Review Letters**, Vol. 68, 3121, 1992.

[67] TOWNSEND P. D.; RARITY J. G. and TAPSTER P. R., Single photon interference in 10 km long optical fibre interferometer, **Electronics Letters**, Vol 29, 634, 1993.

[68] STUCKI D.; GISIN N.; GUINNARD O.; RIBORDY G. and ZBINDEN H., Quantum key distribution over 67 km with a plug & play system, **New Journal of Physics**, Vol. 4, 41, 2002.

[69] GOBBY C.; YUAN Z. L. and SHIELDS A. J, Quantum key distribution over 122 km of standard telecom fiber, **Applied Physics Letters**, Vol. 84, 3762, 2004.

[70] WIESNER S., Conjugate coding, **ACM SIGACT News**, Vol. 15, 78, 1983.

[71] BENNETT C. H. and BRASSARD G., Quantum cryptography: Public key distribution and coin tossing, **Proceedings of the IEEE international conference on computers, systems and signal processing**, Bangalore, India, December 1984.

[72] XAVIER G. B, Esquemas de modulação para distribuição quântica de chaves com codificação por freqüência, **Master thesis**, PUC-Rio, Rio de Janeiro - Brazil, 2005 (available in portuguese only).

[73] WOOTERS W. K. and ZUREK W. H., A single quantum cannot be cloned, **Nature (London)**, Vol. 299, 802, 1982

[74] SCHALLER R. R., Moore's law: past, present and future, **IEEE Spectrum**, Vol. 34, 52, 1997.

[75] STEFANOV A.; GISIN N.;, GUINNARD O.; GUINNARD L. and ZBINDEN H., Optical quantum random number generator, **Journal of Modern Optics**, Vol. 47, 595, 2000.

[76] BENNETT C. H.; BESSETTE F.; BRASSARD G.; SALVAIL L. and SMOLIN J., Experimental quantum cryptography, **Journal of Cryptology**, Vol. 5, 3, 1992.

[77] AGRAWAL G. P., Nonlinear fiber optics third edition, **Academic Press**, San Diego, USA, 2001.

[78] XAVIER G. B.; VILELA DE FARIA G.; TEMPORÃO G. P. and VON DER WEID J. P., Full polarization control for fiber optical quantum communication systems using polarization encoding, **Optics Express**, Vol. 16, 1867, 2008.

[79] PELTON M.; MARSDEN P.; LJUNGGREN D.; TENGNER M.; KARLSSON A.; FRAGEMANN A.; CANALIAS C. and LAURELL F., Bright, single-spatial-mode source of frequency non-degenerate, polarization-entangled photon pairs using periodically poled KTP, **Optics Express**, Vol. 12, 3573, 2004.

[80] LJUNGGREN D.; TENGNER M.; MARSDEN P. and PELTON M., Theory and experiment of entanglement in a quasi-phase-matched two-crystal source, **Physical Review A**, Vol. 73, 032236, 2006.

[81] SAUGE S.; SWILLO M.; ALBERT-SEIFRIED S.; XAVIER G. B.; WALDEBACK J.; TENGNER M.; LJUNGGREN D. and KARLSSON A., Narrowband polarization-entangled photon pairs distributed over a WDM link for qubit networks, **Optics Express**, Vol. 15, 6926, 2007.

[82] LJUNGGREN D. and TENGNER M., Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers, **Physical Review A**, Vol. 72, 062301, 2005.

[83] FEDRIZZI A.; HERBST T.; POPPE A.; JENNEWEIN T and ZEILINGER A., A wavelength-tunable fiber-coupled source of narrowband entangled photons, **Optics Express**, Vol. 15, 15377, 2007.

[84] SAUGE S.; SWILLO M.; TENGNER M. and KARLSSON A., A single-crystal source of path-polarization entangled photons at non-degenerate wavelengths, **Optics Express**, Vol. 16, 9701, 2008.

[85] LIANG C.; LEE K. F.; CHEN J. and KUMAR P., Distribution of fiber-generated polarization entangled photon-pairs over 100 km of standard fiber in OC-192 WDM environment, postdeadline paper, **Optical Fiber Communications Conference - OFC 2006**}, paper PDP35, 2006.

[86] LO H.-K. and CHAU H. F., Unconditional security of quantum key distribution over arbitrarily long distances, **Science**, Vol. 283, 2050, 1999.

[87] LÜTKENHAUS N., Security against individual attacks for realistic quantum key distribution, **Physical Review A**, Vol. 61, 052304, 2000.

[88] KOASHI M. and PRESKILL J., Secure quantum key distribution with an uncharacterized source, **Physical Review Letters**, Vol. 90, 057902, 2003.

[89] BRASSARD G., LÜTKENHAUS N., MOR T. and SANDERS B. C., Limitations on practical quantum cryptography, **Physical Review Letters**, Vol. 85, 1330, 2000.

[90] LUTKENHAUS N. and JAHMA M., Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack, **New Journal of Physics**, Vol. 4, 44, 2002.

[91] HWANG W.-Y., Quantum Key Distribution with high loss: toward global secure communication, **Physical Review Letters**, Vol. 91, 057901, 2003.

[92] GRANGIER P.; LEVENSON J. A. and POIZAT J.-P., Quantum non-demolition measurements in optics, **Nature (London)**, Vol. 396, 537, 1998.

[93] CHEN S.; CHEN Y.-A.; ZHAO B.; YUAN Z.-S.; SCHMIEDMAYER J. and PAN J.-W., Demonstration of a stable atom-photon entanglement source for quantum repeaters, **Physical Review Letters**, Vol. 99, 180505, 2007.

[94] DE RIEDMATTEN H.; AFZELIUS M.; STAUDT M. U.; SIMON C. and GISIN N., A solid-state light-matter interface at the single-photon level, **Nature (London)**, Vol. 456, 773, 2008.

[95] MARAND C. and TOWNSEND P. D., Quantum key distribution over distances as long as 30 km, **Optics Letters**, Vol. 20, 1695, 1995.

[96] WANG X.-B. Beating the photon-number-splitting attack in practical quantum cryptography, **Physical Review Letters** Vol. 94, 230503, 2005.

[97] LO H.-K., MA X. and CHEN K., Decoy state quantum key distribution, **Physical Review Letters**, Vol.94, 230504, 2005.

[98] PENG C.Z. et al, Experimental long-distance decoy-state quantum key distribution based on polarization encoding, **Physical Review Letters**, Vol. 98, 010505, 2007.

[99] WANG Q.; WANG X.-B. and GUO G.-C., Practical decoy-state method in quantum key distribution with a heralded single-photon source, **Physical Review A**, Vol. 75, 012312, 2007.

[100] WANG Q., and KARLSSON A., Performance enhancement of a decoy-state quantum key distribution using a conditionally prepared down-conversion source in the Poisson distribution, **Physical Review A**, Vol. 76, 014309, 2007.

[101] WANG Q.; WANG X.-B.; BJORK G. and KARLSSON A., Improved practical decoy state method in quantum key distribution with parametric down-conversion source, **Europhysics Letters**, Vol. 79, 40001, 2007.

[102] TENGNER M. and LJUNGGREN D., Characterization of an asynchronous source of heralded single photons generated at a wavelength of 1550 nm, **arXiv:0706.2985 [quant-ph]**, 2007.

[103] WANG Q.; CHEN W.; XAVIER G.; SWILLO M.; ZHANG T.; SAUGE S.; TENGNER M.; HAN Z.-F.; GUO G.-C. and KARLSSON A., Robust quantum cryptography with a heralded single-photon source based on the decoy state method, **arXiv:0803.3643v1 [quant-ph]**, 2008.

[104] ZAVRIYEV A. and TRIFONOV A., in **Proceedings of single photon workshop 2007**, Turin, Italy.

[105] MO X.-F.; ZHU B.; HAN Z.-F.; GUI Y.-Z. and GUO G.-C., Faraday-Michelson system for quantum cryptography, **Optics Letters**, Vol. 30, 2632, 2005.

[106] ZHAO Y.; FRED FUNG C.-H.; QI B.; CHEN C. and LO H.-K., Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, **Physical Review A**, Vol. 78, 042333, 2008.

[107] MAKAROV V. and SKAAR J., Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols, **Quantum information and computation**, Vol. 8, 0622, 2008.

[108] SUBACIOUS D.; ZAVRIYEV A. and TRIFONOV A., Backscattering limitation for fiber-optic quantum key distribution systems, **Applied Physics Letters**, Vol. 86, 011103, 2005.

[109] NWEKE N. I. et al, Experimental characterization of the separation between wavelength-multiplexed quantum and classical communications channels, **Applied Physics Letters**, Vol. 87, 174103, 2005.

[110] HALDER M.; BEVERATOS A.; THEW R. T.; SCARANI V.; SIMON C. and ZBINDEN H., Entangling independent photons by time measurement, **Nature Physics**, Vol. 3, 692, 2007.

[111] PARK S. K. and MILLER K. W., Random number generators: good ones are hard to find, **Communications of the ACM**, Vol. 31, 1192, 1988.

[112] JENNEWEIN T.; ACHLEITNER U.; WEIHS G.; WEINFURTER H. and ZEILINGER A., A fast and compact quantum random number generator, **Review of Scientific Instruments**, Vol. 71, 1675, 2000.

[113] STEFANOV A.; GISIN N.; GUINNARD O.; GUINNARD L. and ZBINDEN H., Optical Quantum Random Number Generator, **Journal of Modern Optics**, Vol. 47, 595, 2000.

[114] STIPCEVIC M. and MEDVED ROGINA B., Quantum random number generator based on photonic emission in semiconductors, **Review of Scientific Instruments**, Vol. 78, 045104, 2007.

[115] DYNES J. F.; YUAN Z. L.; SHARPE A. W. and SHIELDS A. J., A high speed, postprocessing free, quantum random number generator, **Applied Physics Letters**, Vol. 93, 031109, 2008.

[116] DIXON A. R.; YUAN Z. L.; DYNES J. F.; SHARPE A. W. and SHIELDS A. J., Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate, **Optics Express**, Vol. 16, 18790, 2008.

[117] EKERT A. K., Quantum cryptography based on Bell's theorem, **Physical Review Letters**, Vol. 67, 661, 1991.

[118] LING A.; PELOSO M. P.; MARCIKIC I.; SCARANI V.; LAMAS-LINARES A. and KURTSIEFER C., Experimental quantum key distribution based on a Bell test, **Physical Review A**, Vol. 78, 020301(R), 2008.

[119] ACÍN A.; MASSAR S. and PIRONIO S., Efficient quantum key distribution secure against no-signalling eavesdroppers, **New Journal of Physics**, Vol. 8, 126, 2006.

[120] XAVIER G. B.; FERREIRA DA SILVA T.; VILELA DE FARIA G.; TEMPORÃO G. P. and VON DER WEID J. P., A simple scheme for random number generation in quantum key distribution systems, Proceedings of AQIS 2008, Seoul, South Korea, 2008.

[121] FERREIRA DA SILVA T.; XAVIER G. B. and VON DER WEID J. P., **in preparation**.

[122] RUSHKIN A. et al, **Nist Special Publication 800-22**, available at http://csrc.nist.gov/groups/ST/toolkit/rng/index.html, 2001.

[123] XAVIER G. B.; FERREIRA DA SILVA T.; VILELA DE FARIA G.; TEMPORÃO G. P. and VON DER WEID J. P., Practical Random Number Generation Protocol for Entanglement-Based Choice Quantum Key Distribution, **Quantum Information & Computation**, Vol. 7, 0683, 2009.

[124] LIM H. C.; YOSHIZAWA A.; TSUCHIDA H. and KIKUCHI K., Stable source of high quality telecom-band polarization-entangled photon-pairs based on a single, pulse-pumped, short PPLN waveguide, **Optics Express**, Vol. 16, 12460, 2008.

[125] LIM H. C.; YOSHIZAWA A.; TSUCHIDA H. and KIKUCHI K., Distribution of polarization-entangled photonpairs produced via spontaneous parametric down-conversion within a local-area fiber network: Theoretical model and experiment, **Optics Express**, Vol. 16, 14512, 2008.

[126] POPPE A. et al, Practical quantum key distribution with polarization entangled photons, **Optics Express**, Vol. 12, 3865, 2004.

[127] TANG X. et al, Experimental study of high speed polarization-coding quantum key distribution with sifted-key rates over Mbits/s, **Optics Express**, Vol. 14, 2062, 2006.

[128] CHEN J.; WU G.; LI Y.; WU E. and ZENG H., Active polarization stabilization in optical fibers suitable for quantum key distribution, **Optics Express**, Vol. 15, 17928, 2007.

[129] CHEN T.-Y.; ZHANG J.; BOILEAU J.-C.; JIN X.-M.; YANG B.; ZHANG Q.; YANG T.; LAFLAMME R. and PAN J.-W., Experimental quantum communication without a shared reference frame, **Physical Review Letters**, Vol. 96, 150504, 2006.

[130] HUBEL H.; VANNER M. R.; LEDERER T.; BLAUENSTEINER B.; LORUNSER T.; POPPE A. and ZEILINGER A., High-fidelity transmission

of polarization encoded qubits from an entangled source over 100 km of fiber, **Optics Express**, Vol. 15, 7853, 2007.

[131] TREIBER A.; POPPE A.; HENTSCHEL M.; FERRINI D.; LORUNSER T.; QUERASSER E.; MATYUS T.; HUBEL H. and ZEILINGER A., Fully automated entanglement-based quantum cryptography system for telecom fiber networks, **arXiv:0901.2725 [quant-ph]**.

[132] BOILEAU J.-C; LAFLAMME R.; LAFOREST M. and MYERS C. R., Robust quantum communication using a polarization-entangled photon pair, **Physical Review Letters**, Vol. 93, 220501, 2004.

[133] XAVIER G. B.; WALENTA N.; VILELA DE FARIA G.; TEMPORÃO G. P.; GISIN N.; ZBINDEN H. and VON DER WEID J. P., Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation, **New Journal of Physics**, Vol. 11, 045015, 2009.

[134] MACEDO J. F. and VON DER WEID J. P., Time domain PMD simulations in optical fibers and emulators, **Proceedings WFOPC - IEEE / LEOS Workshop of fibres and optical passive components 2005**, pp. 176, Palermo, Italy, 2005.

[135] XAVIER G. B.; MACEDO J. F. and VON DER WEID J. P., Polarization control scheme using a DWDM guard channel for quantum cryptography, *unpublished*.

[136] VILELA DE FARIA G.; FERREIRA J.; XAVIER G. B.; TEMPORÃO G. P. and VON DER WEID J. P., Polarisation control schemes for fibre-optics quantum communications using polarisation encoding, **Electronics Letters**, Vol. 44, 228, 2008.

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo