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.

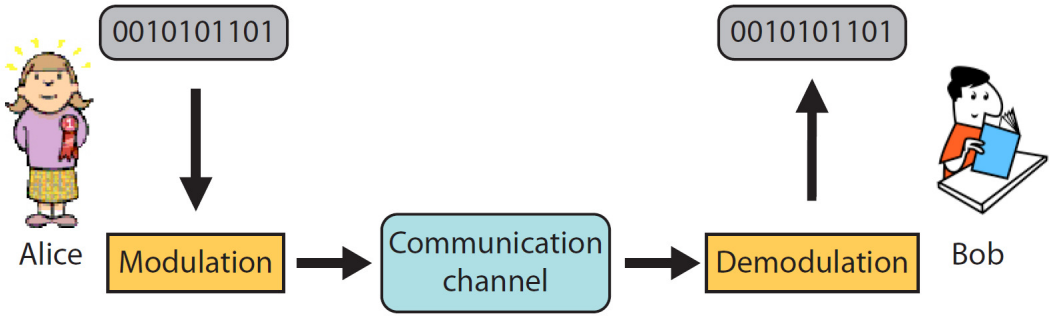

Figure 1 - Typical elements of a communication system. Information (represented here in its most usual form, binary digits) is modulated into an appropriate form for transmission through a communication channel by Alice. Bob demodulates it obtaining the same information Alice transmitted (in the absence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

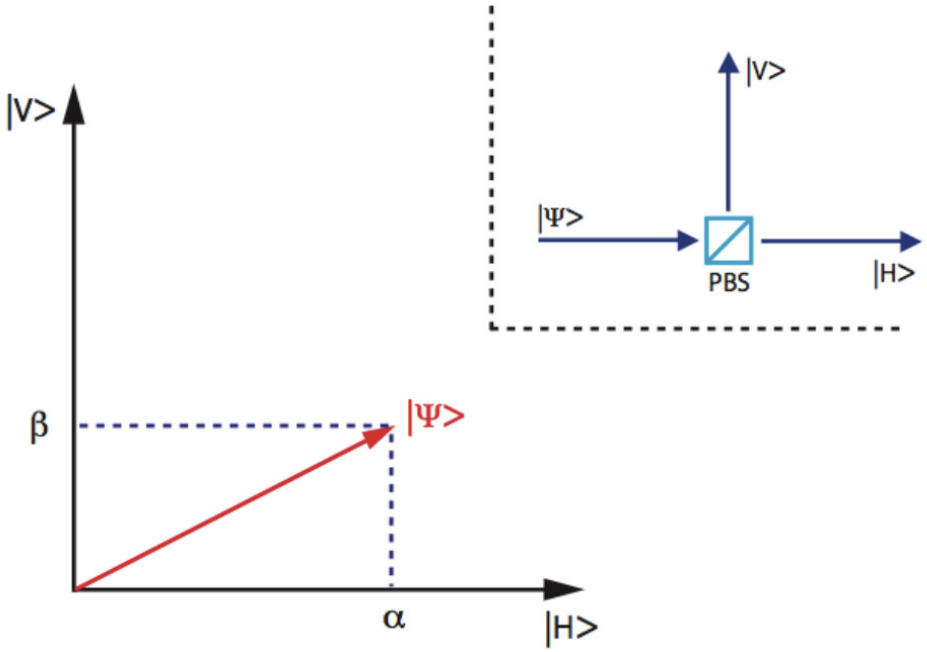

Figure 2 - Graphical representation of the state of polarization $|\psi\rangle$. Inset shows what happens to $|\psi\rangle$ after a polarizing beam splitter (PBS).

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:

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

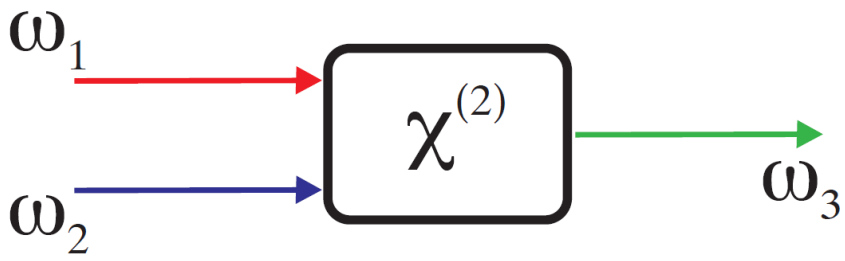

Figure 3 - Two optical fields with frequencies ω_1 and ω_2 combining in a non-linear medium to produce ω_3.

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.

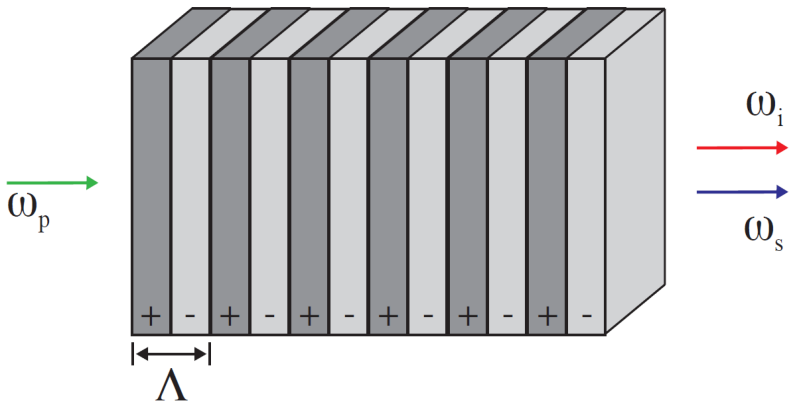

Figure 4 - A periodically poled crystal. The signs indicate where the non-linearity $\chi^{(2)}$ is negative and positive. Shown are also the input optical field ω_p and the outputs ω_s and ω_i.

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.

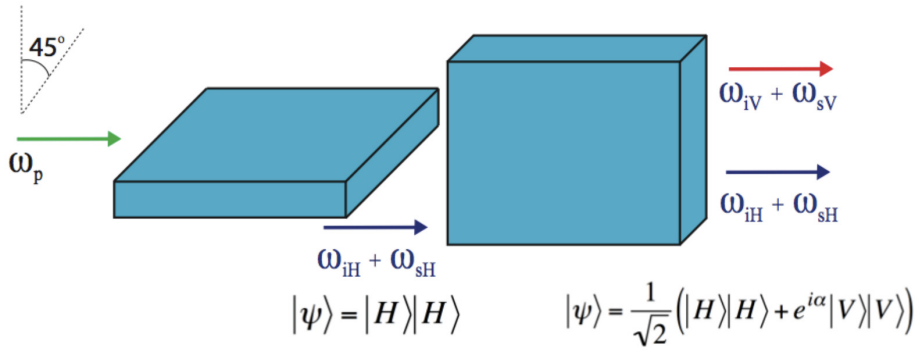

Figure 5 - Generation of the maximally entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle|V\rangle + e^{i\phi}|V\rangle|H\rangle\right)$ employing two non-linear crystals, with the pump polarization oriented at 45º.

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].

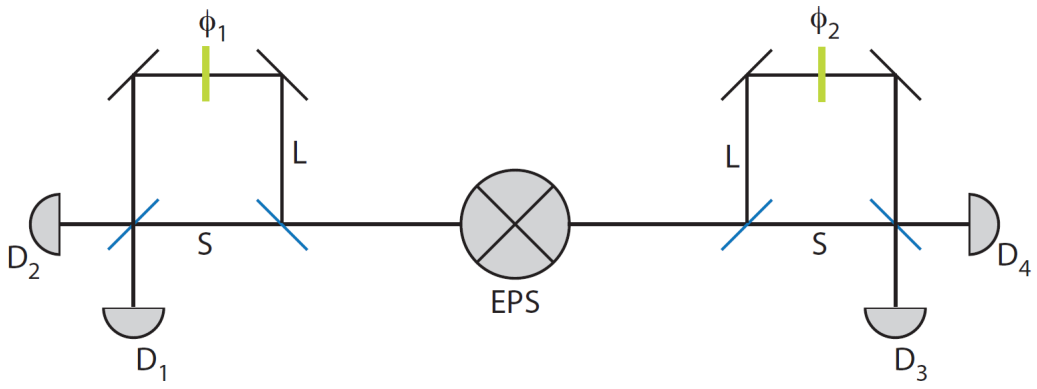

Figure 6 - Scheme for a Franson-type interferometry setup. EPS: Entangled photon source; L and S: Long and short interferometer arms respectively; D_x: Single photon detectors; ϕ_x: Phase shifters.

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.

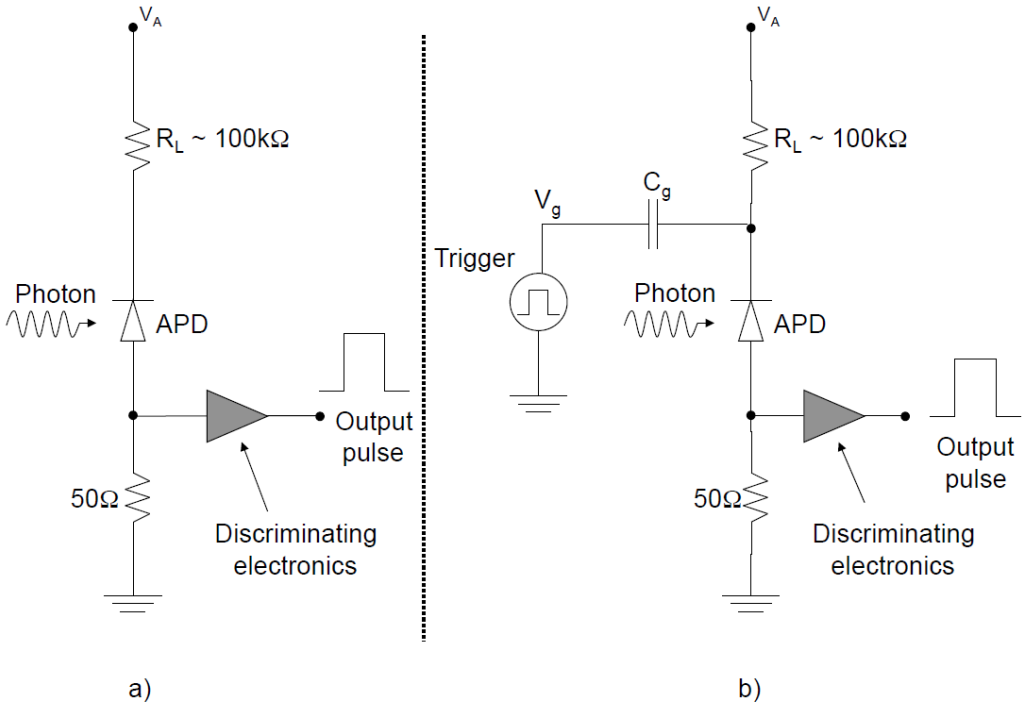

Figure 7 - Part a) shows the circuit used to detect single photons in passive mode, while part b) is the circuit for passive gated mode operation. Capacitor C_g in part b) is used to decouple the DC voltage between the circuit and the pulse generator.

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.

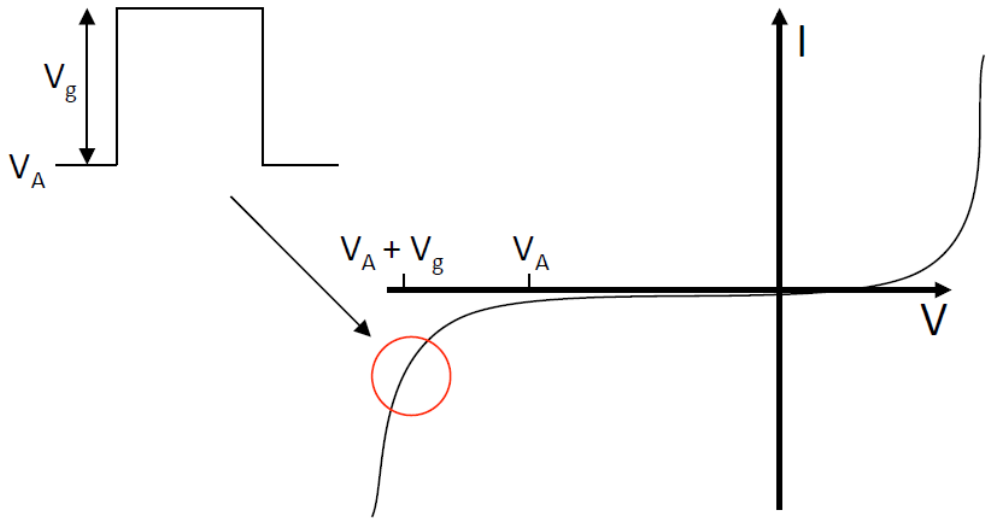

Figure 8 - Typical current-voltage curve for an avalanche photo-diode. V_A is the breakdown voltage and V_G is the amplitude of the gate pulse applied. The red circle shows where the diode is placed for the gate pulse's duration.

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].

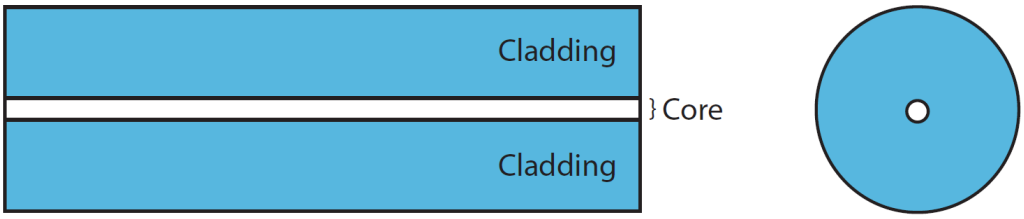

Figure 9 - Basic optical fiber structure. The protection coatings have been omitted from the figure. Right part is simply the profile view of the fiber.

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.

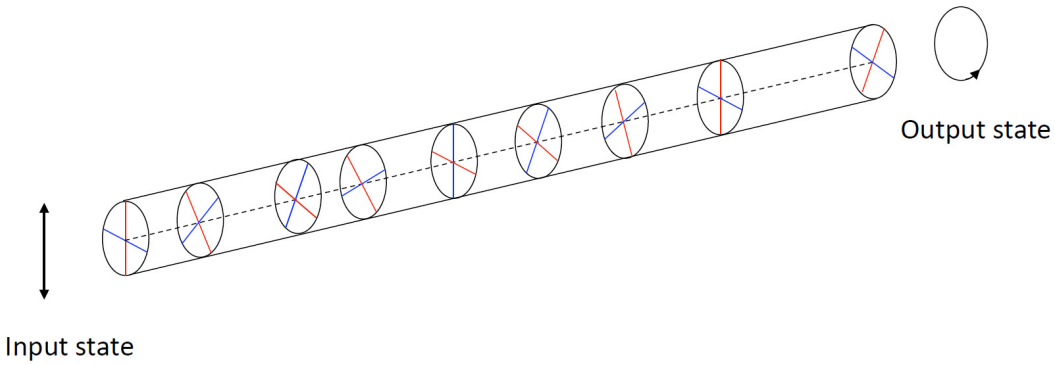

Figure 10 - Birefringence in an optical fiber is a function of mechanical stresses and temperature fluctuations along its length, causing random polarization rotations of an input polarization state. We see in the figure for example, a vertical state randomly transforming into a circular state after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

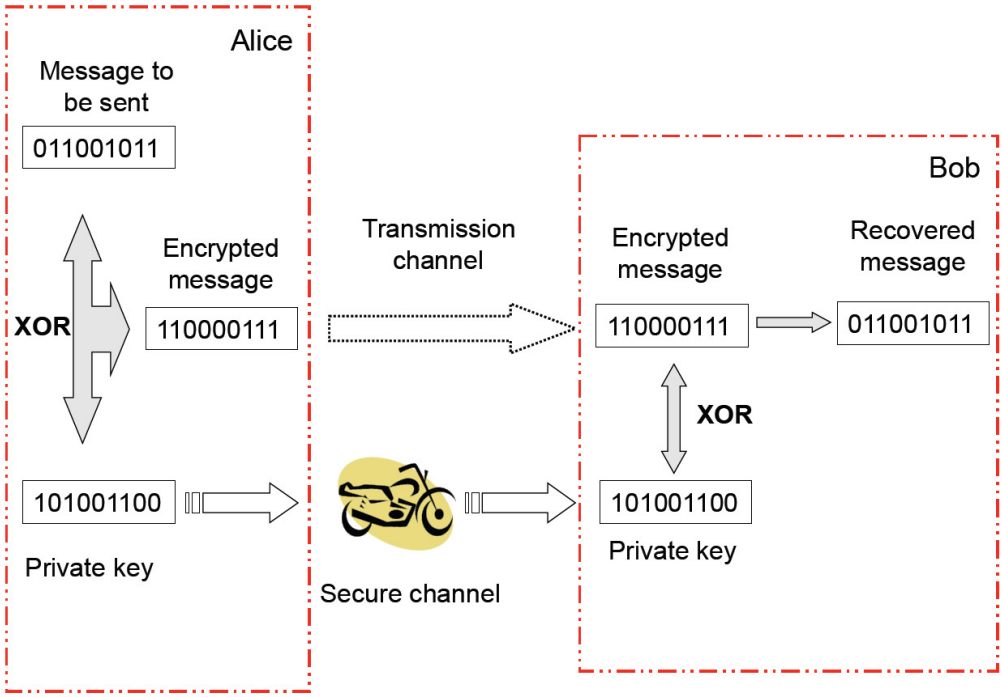

Figure 11 - Scheme of Vernam's cipher. Note that we used a trusted courier as the secure channel here, which in principle is not a good choice. Adapted from [72].

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:

$$|0\rangle|Initial\rangle \rightarrow |0\rangle|0\rangle|Final_0\rangle \tag{2.16}$$

$$|1\rangle|Initial\rangle \rightarrow |1\rangle|1\rangle|Final_1\rangle \tag{2.17}$$

$|Initial\rangle$ and $|Final_{1,0}\rangle$ 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 $|Final_{1,0}\rangle$. 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 $|1\rangle$:

$$(a|0\rangle + b|1\rangle)|Initial\rangle \rightarrow a|0\rangle|0\rangle|Final_0\rangle + b|1\rangle|1\rangle|Final_1\rangle \tag{2.18}$$

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

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

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.

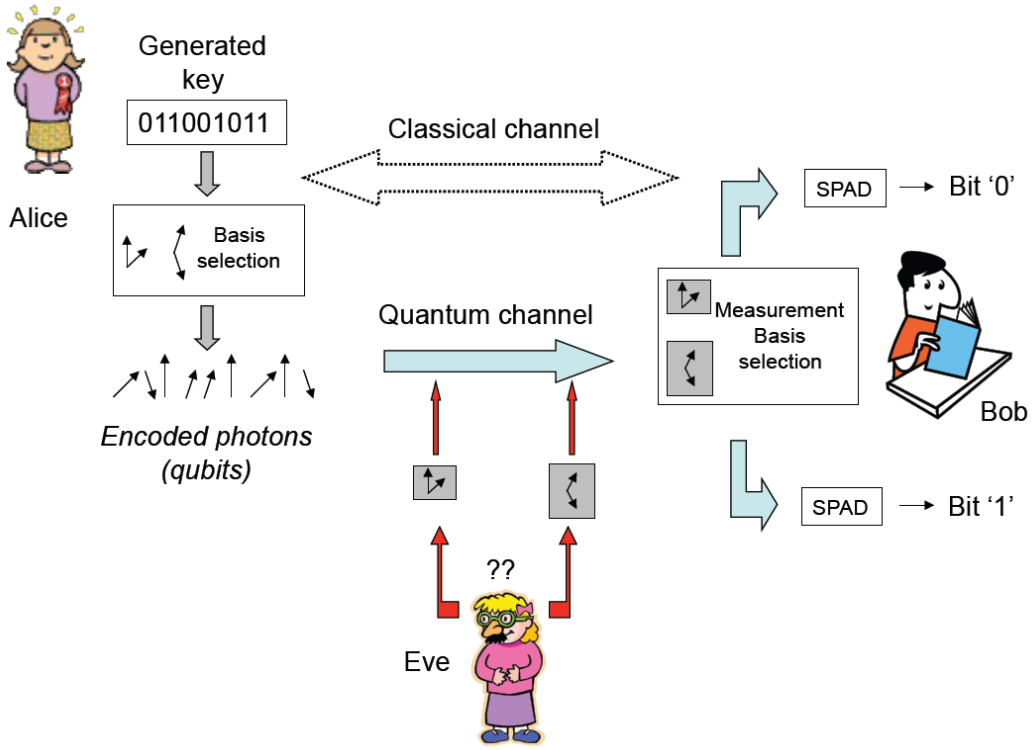

Figure 12 - BB84 protocol. PBS: Polarizing beam splitter. Adapted from [72].

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].