ICFO-INSTITUT DE CIÈNCIES FOTÒNIQUES

&

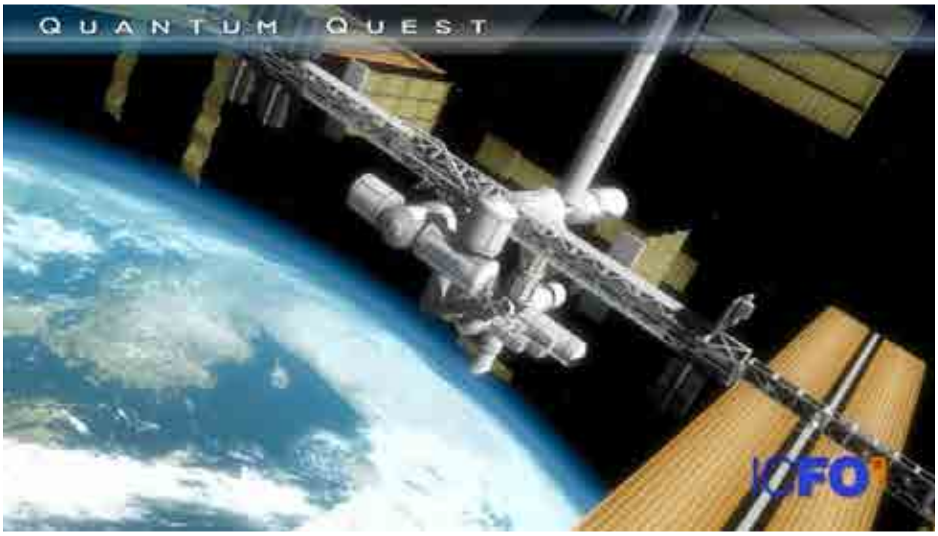
UPC-UNIVERSITAT POLITÈCNICA DE CATALUNYA

# Integrated photonic transmitters for secure space quantum communication

MARC JOFRE

**Thesis Advisor: Prof. Valerio Pruneri**

**PhD Thesis - 2013**


QUANTUM QUEST
ICFO

*To my family*

*The real voyage of discovery*
*consists not in seeking new landscapes,*
*but in having new eyes.*
**Marcel Proust**

# Abstract

An important issue in today's information society is the security of data transmission against potential intruders, which always put at risk the confidentiality. Current methods to increase security require that the two parties wishing to transmit information, exchange or share one or more security keys. Once the key has been identified, the information can be transferred in a provable secure way using a one-time pad, i. e. the key length is as long as the plaintext. Therefore, the security of the information transmission is based exclusively on the security of the key exchange. Quantum cryptography, or more precisely quantum key distribution (QKD), guarantees absolutely secure key distribution based on the principles of quantum physics, according to which it is not possible to measure or reproduce a state (e.g. polarization or phase of a photon) without being detected. The key is generated out from the measurement of the information encoded into specific quantum states of a photon, named qubits. For example, a qubit can be created using properties such as the polarization or the phase of a photon.

Achieved goals of this thesis are the development of a new class of high speed integrated photonic sources for applications in quantum key distribution systems, capable of producing unprecedented qubit rates ($100$ Mbps - $1$ Gbps) and transmitting those over larger distances than those achieved so far ($>$ $200$ km). More specifically the work has been focused on developing faint pulse sources which can be used in very demanding environmental conditions, such as those in Space. For the development of these sources, apart from the optical design, essential is the opto-mechanical engineering as well as the integration with the electron-

ics. One of the objectives was to achieve very high level of integration and power efficiency, e.g. volumes and power consumption between 10 and 100 times smaller than those typical of a laboratory experiment. Moreover, work in related parts of a whole QKD transmission system has been carried out. In particular, a new scheme for a compact, fast and simple random number generator has been demonstrated successfully achieving a random number generation rate of 1.1 Gbps. Also, during the course of this thesis, the development and engineering of a free-space QKD optical link has been initiated.

This thesis makes use of novel ideas to alternatively demonstrate proof-of-concept experiments, which could then further develop into commercial products. To this end, close collaborations with world-wide leading companies in the field have been established. The Optoelectronics Group at ICFO has been involved in current European Space Agency (ESA) projects to develop a small footprint and low power consumption quantum transceiver and a high-flux entangled photon source.

# Resum

En l’actual societat del coneixement és important la seguretat en la transmisson de dades contra potencial intrusos, els quals sempre posen en risc la confidencialitat. Mètodes actuals per incrementar la seguretat requereixen que les dos parts que volen transmetres informació, intercanviin o comparteixin una o més claus. Una vegada la clau ha estat identificada, la informació pot ser transferida de forma provadament segura utilitzant ”‘one-time pad”’. Per tant, la seguretat en la transmissió de la informació es basa exclusivament en la seguretat en l’intercanvi de la clau. La criptografia quàntica, o més precisament distribució de clau quàntica (QKD), garanteix absolutament la seguretat de la distribució de la clau basant-se en els principis de la física quàntica, segons la qual no és possible mesurar o reproduïr un estat (p. e. la polarització o fase d’un fotó) sense ser detectat. La clau es genera a partir de les mesures de la informació codificada en estat quàntics del fotó, anomenats qubits. Per exemple, un qubit pot ser creat utilitzant propietats com la polarització o fase d’un fotó.

Els objectius aconseguits d’aquesta tesis són el desenvolupament d’una nova classe d’emissors fotònics d’alta velocitat per a aplicacions en sistemes de distribució de clau quàntica, capaços de produïr velocitats de qubit sense precedents (100 Mbps - 1 Gbps) i transmetre’ls a través de distàncies més llunyanes que les aconseguides fins ara ($>$ 200 Km). Més en concret el treball s’ha centrat en el desenvolupament de fonts de pulsos atenuats que poden ser usades en condicions ambientals molt extremes, com les presents a l’Espai. Per al desenvolupament d’aquestes fonts, apart del disseny òptic, importantíssim es l’enginyeria optomecànica com també la integració amb la electrònica. Un dels objectius ha estat acon-

seguir un molt alt nivel de integració i eficiència de potència, p. e. volums i consums de potència entre 10 i 100 vegades més petits que els típics en experiments de laboratori. Ademés, s'ha realitzat treball en altres parts relacionades amb un sistema de transmissió QKD. En particular, un nou esquema per a un generador de números aleatori compacte, ràpid i simple ha estat positivament demostrat aconseguint velocitats de generació de números aleatoris de 1.1 Gbps. També, el desenvolupament i enginyeria d'un enllaç òptic per a QKD en espai lliure ha estat iniciat durant aquesta tesis.

Aquesta tesis utilitza idees novedoses per a demostrar experiments de prova de concepte, els quals poden esdevenir en productes comercials. Per a aquest fi, s'han establert col·laboracions amb empreses internacionals líders del sector. A més a més, el Grup d'Optoelectrònica de ICFO ha estat invol·lucrat en projectes de la Agència Espacial Europea (ESA) per a desenvolupar un transceptor quàntic de tamany reduït i baix consum de potència, el qual també conté una font de fotons entrellaçats d'alt flux.

# Acknowledgments

I herewith would like to thank everyone who helped me advance in the difficult task that has been pursuing this work.

I must thank, first of all, my supervisor Prof. Valerio Pruneri, for helping me at every stage of this thesis, giving me useful advises in decision making situations. In addition, I would like to thank him for being a valuable source of ideas and motivation as well. Also I would like to acknowledge Prof. Morgan W. Mitchell, Prof. Juan P. Torres, Prof. Marcos Curty and Prof. Rupert Ursin, whom I had the opportunity to work with and gratefully expanding the completeness in different fields. Without their help, this work would have never been fulfilled, and therefore I am deeply indebted to them.

Working in the nice atmosphere at ICFO, headed by Prof. Lluís Torner, has a clear impact on the quality of the achieved results. Thence, I would like to thank the colleagues at ICFO who have rendered my daily routine much more pleasant. Especially to all the Nanophotonics - Optoelectronics group for never giving up the idea of kindly kidding me and making work more bearable. Also, thank all the personnel of the eWorkshop, mWorkshop and PPL who definitely contributed with their continuous work to the accomplishment of this thesis.

I ought to acknowledge as well the ICFO PhD program for giving me the possibility to pursue a PhD degree and everything that this entails for my formation, both as an engineer and as a person.

Last, but not least, I am indebted to my family and life-friends, I know that I have counted with their affection every single day during these years, hence I want to thank them for their permanent support.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 Quantum optics

Quantum optics deals with the study of the nature and effects of light as quantized photons. According to quantum theory, an electro-magnetic field at optical frequencies may be not only considered as a wave but also as a stream of particles called photons, hence it is quantized. Fundamental characteristics allowing to work in the quantum domain at optical wavelengths are convenient sources and detectors, and energy spacing of the quantum levels larger than the thermal energy [1–3].

The average photon flux of an optical beam can have a well-defined value determined by the intensity, which corresponds to an average detector count rate. But, considering more in detail the detection time intervals between photons, statistical fluctuations arise from the fact that the optical beam is quantized. Thus, in quantum optics, it is of relevant interest to infer the intrinsic photon number statistics of the light beam more than the average photon number.

To measure the photon statistics, high efficiency detectors are required. With such detectors, the photon-counting statistics give a true measure of the incoming photon statistics, with a fidelity that increases as the efficiency of the detectors increases. Otherwise, in the limit of very low efficiencies, the time intervals between the photo-electrons becomes completely random, and the counting statistics are Poissonian for all possible incoming distributions.

### 1.1.1 Photon statistics and detection theory

A photon flux can be classified into three different photon number statistics, meaning the number of photons per given interval when having enough time resolution: Poissonian, Super-Poissonian and Sub-Poissonian.

We will focus in coherent light beam which have Poissonian photon number statistics. For instance, the output of strongly attenuated lasers can be best approximated by a Poissonian distribution, no matter which statistics has the laser in a non-attenuated regime [4]. The Poissonian and exponential distributions are related. If the number of counts follows a Poissonian distribution, then the interval between individual counts follows an exponential distribution.

Thus, when single photon counters are used in coherent light beams, Poissonian timing statistics arise. Single photon detectors generate a detection pulse whenever an electron pair is generated and if followed by timing analysis equipment, they provide photon-counts statistics. Electron pairs can be generated due to photo-electron pairs in the signal as well as background photons; while electron pairs can also be generated from electron recombination, generating dark counts. In photon-count systems, all forms of loss and inefficiency will tend to degrade the photon-count statistics to the Poissonian case. In order to correctly treat the information generated by the single photon detectors, the statistic properties of the different involved contributions has to be fully understood. In particular, if it is considered the count statistics detected in a given time, signal photons, background photons as well as dark counts are uncorrelated and follow Poissonian photon number statistics.

Considering attenuated pulsed coherent light beams, the photon number statistics of the different pulses follows Poissonian statistics but the time window of expected signal detections is limited to the time width of the pulse. Instead, the background noise and dark counts are distributed over time and thus, those detections outside the expected timing window for the signal photons can be filtered out by software algorithms and detector-gating techniques.

Given a coherent signal state with mean photon number $\bar{n}$, the yield $Y_i$ of an $i$-photon is the conditional probability of a detection event, over a transmission line with transmission $\eta_i$, at the receiver side given that the transmitter sends out an $i$-photon state. Note that $Y_0$ is the background rate, which includes the detector dark count and other background contributions such as stray light. Thus, the yield of an $i$-photon state mainly comes from two parts, background and true signal. Assuming that the background counts are independent of the signal photon detection, $Y_i$ is given by

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \cong Y_0 + \eta_i \tag{1.1}$$

where $Y_0$ and $\eta_i$ are small. Typically the detections are limited to specific time windows, thus the yield of background is the product of background rate $R_b$ and the time window width $\tau_c$, $Y_0 = R_b\tau_c$. Also, in common transmission lines (i.e, free-space or optical fibers) the transmission is independent of the particular state $i$-photon, thus common to any $i$-photon, $\eta = \eta_i$.

The gain $Q_i$ of an $i$-photon is the product of the probability of sending out an $i$-photon state and the conditional probability that lead to a detection event. The gain of the $i$-photon state $Q_i$ is given by

$$Q_i = Y_i \frac{\bar{n}^i}{i!} e^{-\bar{n}} \tag{1.2}$$

Thus, the gain $Q_{\bar{n}}$ of a coherent state with mean photon number $\bar{n}$ is given by

$$Q_{\bar{n}} = \sum_{i=0}^{\infty} Y_i \frac{\bar{n}^i}{i!} e^{-\bar{n}} = Y_0 + 1 - e^{-\eta\bar{n}} \tag{1.3}$$

## 1.2 Quantum communication

Quantum communication (QC) is based on the generation, transmission and detection of quantum states (qubits) of individual entities that act as carriers, such as photons. In the last two decades, QC has steadily gained importance and attention for different reasons. On the one hand, in state-of-the-art free-space optical communication links, the increasing bit rate and the substantial loss, due to atmospheric scattering and intrinsic diffraction, significantly reduces the energy (i.e. the number of photons) the bits are encoded with. This tendency toward the so-called single photon regime makes the quantum nature emerge and to be considered as essential. This regime is also typical for the new generation deep-space links [5]. On the other hand, information is physical and any processing of information is always performed by physical means, hence when working at the quantum regime a fundamental new discipline arises which is commonly know as quantum theory of information [6]. Quantum physics allows the construction of qualitatively new systems with no classical counterpart, i.e. new types of logic gates (quantum computation), secure cryptosystems (quantum key distribution), teleportation of information (quantum teleportation). Thus, the realization of quantum communication is of paramount importance in many quantum information applications, certainly in high bit rate long-distance quantum communication systems non-trivial issues emerge.

At present, photons are suitable carrier entities for long-distance quantum communication. Other systems such as atoms or ions are being studied thoroughly, however their applicability is not practical within the near future. In long-distance communications, the inevitable losses on the channel constitute an important source of noise, in that an absorbed quantum in the signal cannot be detected by the receiver. In modern fiber-based optical communication, this issue is overcome by the use of repeaters or amplifiers which, respectively, measure and regenerate the signal or amplify its intensity. For quantum channels, however, these processes are unsatisfactory as the level of the added noise acts to destroy the quantum information carried. Firstly, any measurement of the qubit leads to a change of at least some of the possible states of the qubit. Secondly, amplification to generate copies of the quantum state is a more subtle process, in that it does not include a measurement and so does not reveal any information about the state. It is, nevertheless, impossible to accurately copy the unknown state of a quantum system. This is known as the no-cloning theorem [7, 8].

In practice, there are two media that can propagate photons: optical fibers and free-space. Each of these two possible choices implies the use of the corresponding appropriate wavelength. For optical fibers, the classical telecom choices are 1300 nm and 1550 nm and hence any real-world-application of quantum communication in fibers showed to work at this wavelengths. For free-space the favored choice is at shorter wavelengths, around 800 nm, where efficient detectors exist and diffraction is lower.

### 1.2.1 Free-space quantum communication

In many applications, free space optical (FSO) communications is the technology of choice to transmit information, especially when fiber optical cabling is not easily achievable or its installation is too expensive [9]. Compared to radio frequency (RF) techniques, its main advantages lie in high data rates (up to several Gbps), minimum free space losses due to the small optical beam divergence and absence of regulatory issues thanks to the low interference level [10–12]. Therefore FSO communication is favorable for high data-rate, long-range point-to-point links, where the terminal size, mass, and power consumption are subjected to strong limitations, such is the case of aeronautical or space platforms.

Optical fiber link losses (0.2 dB/km) or atmospheric free-space attenuation (0.1 dB/km), and current photon-detector technology limit QC on Earth to around 200 km [13], while those problems are less severe in Space (line-of-sight limitation). Thus, a versatile global QC system will combine fiber, free-space and Space transmission to overcome the current limit due to loss.

Quantum information, on a photon, may be encoded through several degrees of freedom. Table 1.2.1 summarizes the possible approaches, listing the advantages and disadvantages of each of them. Thus, a convenient encoding for free-space quantum communication is based on polarization since this degree of freedom can be sent through the atmosphere with very high quality.

One of the most relevant free-space quantum communication demonstration is described in reference [14]. The Canary Islands (Spain) were chosen as location for the inter-island link to be established between a transmitter at the Observatorio Roque de los Muchachos on the island of La Palma and a receiver at the Observatorio del Teide on the neighboring island of Tenerife, $144$ km apart. The established quantum channel through the atmosphere can be considered a worst case scenario for a space-to-ground link from the atmospheric turbulence point of view. As a matter of fact the overall end-to-end loss of this horizontal atmospheric link is about $25$-$35$ dB, which is comparable to the link loss between a LEO satellite and a ground receiver (although at a much longer link distance). Effects caused by atmospheric turbulence (e.g. random rotation of single photon's polarization, time-of-arrival jitter due to fluctuations of the optical path) have been demonstrated to be tolerable in terms of potential quantum state decoherence [15].

Free-space transmission is highly representative of Space transmission. Thus, an intermediate milestone, certainly, is free-space QC and in particular to achieve practical polarization control and synchronization with adequate signal to noise ratio. The ultimate milestone is the demonstration of a QC protocol in a satellite-to-ground down-link configuration [16]. This link will be a very important ingredient in the realization of a global QC scheme. Furthermore, the unique features of Space offer extremely long propagation paths to explore the limits of the validity of quantum physics principles. In particular Space QC can potentially offer a unique test bed of quantum entanglement over a distance exceeding $1000$ km, which is not feasible on the ground.

### 1.2.2 Synchronization techniques

In QC systems, a common issue is the electronic synchronization between the source and the receiver, i.e. the capability of identifying each optical detection with the corresponding emitted qubit. Moreover, accurate synchronization to timescales shorter than the time duration of a transmission

| Degree of freedom | Expected behavior in atmospheric transmission | Experimental advantage | Experimental challenge |
|---|---|---|---|
| Polarization | Well tested in atmospheric turbulence and it is essentially not affected. | Straight forward. | Polarization alignment of birefringent elements and surfaces in the channel and rotation of the sender and receiver. |
| Phase/Time bin | Not tested in turbulent atmosphere. In principle, it could work. | Only a well defined polarization transmitted, possibly polarization independent channel. | Active stabilization of unbalanced interferometers at the source and the receivers. |
| Spatial mode | Not expected to function in turbulent atmosphere since any wave-front distortion leads to decoherence. | No polarization dependence. | Perfect compensation of the wave-front distortions required. |
| Frequency bin | Not tested in atmosphere, but could work. | No polarization dependence. | Phase of the states are a inherent function of time (not constant) and therefore the paths might need to be stabilized interferometrically. |
| Continuous variables. | Not tested in atmosphere, but could work. | Simple sources and detectors. | Loss tolerance presently only to about 10 dB. |

Table 1.1: Types of encoding of quantum information on a photon.

pulse is necessary in order to maintain a narrow time window to filter the background and dark counts from single-photon detectors. A typical time window $\tau_c$ is chosen to be slightly larger than the detector time jitter, which is of the order of $\tau_d = 500$ ps, and pulse time width or coherence time of the signal. This requires establishing a common time base or synchronization between the transmitter and the receiver.

It is not convenient to digitally sample the single-photon detectors, recording whether there was a detection or not, at a given rate since most of the samples will present no detection. This results in too much data to be processed in a very low efficient manner and computationally difficult. Instead, it is common to use time-tagging hardware, which records only positive detections giving them a unique time-stamp. Using time-tagging hardware, for the synchronization, two issues have to be addressed. First the detection instances will have an unknown time offset $\Delta T$ with respect the emission times of the transmitter. Second, clocks drift one respect the other mainly because practical clock performances and atmospheric time-of-arrival fluctuations, interpreted as a relative frequency accuracy $\Delta u$.

### Relevant theory of time-of-arrival fluctuations in free-space

Pulse broadening can be calculated from knowledge of the two-frequency mutual coherence function (MCF) [17]. The two-frequency MCF is an important quantity by itself as it provides a measure of the coherence bandwidth and the coherence time. The coherence bandwidth limits the speed of transmission without distortion, while the coherence time is the necessary time in order that the transmission channel changes significantly. At optical frequencies, $1$ ns pulses can be considered narrow-band thus no distortion and no pulse broadening is a limiting impairment for the transmission.

The turbulent atmospheric optical channel can be characterized, to a first approximation, as a log-normal fading channel having a large coherence bandwidth ($\geq 10$ GHz), a long coherence time ($\geq 1$ ms), negligible multi path time dispersion ($\leq 1$ ps) and a significant dispersion in space and spatial frequency [18]. But, beam spreading induced by turbulence limits the average far-field beam width of a collimated laser beam. Thus, a narrow transmitter beam can suffer significant loss of antenna gain. In addition, turbulence may induce angle-of-arrival (phase) fluctuations which limit the energy collection capability of a diffraction-limited receiver observing a single or few spatial modes. Furthermore, turbulence-induced scintillations can degrade communication performance significantly through deep signal fades.

### Initialization of data receiving

In a practical QC implementation, the clocks can be coarsely synchronized by conventional means (e.g. using the network time protocol), so it can be assumed that $\Delta T$ will not exceed a few hundred milliseconds. Other techniques rely on GPS signals or using bright pulses.

Practical clocks (rubidium and crystal oscillators) have a limited frequency accuracy (instead of clocking at $10$ MHz they might clock at $10.01$ MHz) and a limited stability (is the variation over time of the output frequency). Rubidium clocks have a relative frequency accuracy of $10^{-11}$, while standard crystal oscillators have a relative frequency accuracy of $10^{-4}$ and a stability of $10^{-6}$ to $10^{-7}$. In time-stamp applications, what matters, is the relative frequency difference between the two clocks $\Delta u$ and the time offset $\Delta T$. The detection time $t'$, given the transmitter time $t$, is connected via

$$t' = (t + \Delta T) \cdot (1 + \Delta u) \tag{1.4}$$

To date, there are different practical ways to achieve clock synchronization in QC among the two parties, the transmitter and the receiver. One is to use time-stamp hardware with stabilized local software-controlled phase-lock loop clocks driven by the detected photon signal [19] (in particular for correlated photon pairs see [20]) or by the ultra precise global position system (GPS) signal [21]. The other method is to make use of a classical synchronization channel between the transmitter and the receiver. In particular for defined time-of-arrival systems a periodic bright pulse, of a different wavelength, can be used as precursor to open a time gate for the subsequent signal photon [22,23].

**Pilot signal synchronization:** allows the receiver to synchronize its local oscillator to the carrier frequency and phase of the received signal from the transmitter. When an unmodulated carrier component is transmitted along with the information-bearing signal, the receiver employs a phase-locked loop (PLL) to acquire and track the carrier component. The PLL is designed to have a narrow bandwidth so that it is not significantly affected by the presence of frequency components for the information-bearing signal.

In practice, the selection of the bandwidth of the PLL involves a trade-off between speed of response and noise in the phase estimate. On the one hand, it is desirable to select the bandwidth of the loop to be sufficiently wide to track any time variations in the phase of the received carrier. On the other, a wide band PLL allows more noise to pass into the loop, which corrupts the phase estimate. Typically, phase noise introduces a jitter of few ps using standard PLL.

**Periodic synchronization signal:** the transmitter emits a strong light pulse, which acts as a synchronization light (SL) on each or at some clock cycles. After a certain time delay $t$, a data burst is launched towards the receiver. At the receiver, the arrival time of the SL is used as a reference time to turn on a timing gate in which a data burst is expected. In general, the SL is detected by a photo detector (PD) and a constant fraction discriminator (CFD) to generate the time reference. The amplitude of the output of the PD is directly proportional to the intensity of the light. In free-space, the intensity of the SL varies due to the atmospheric disturbance, so does the pulse height of the output of the PD. The CFD minimizes the effect of amplitude fluctuations in the input signal. The trigger time of a CFD is nearly independent of the amplitude of input pulse [22]. A certain time delay $t$ is needed to account for the limited bandwidth of the pulse detection and gating triggering components at the receiver, as well as to reduce background noise due to the synchronization pulse, even if implemented at different wavelengths.

This works for defined time-of-arrival systems, where a specific timing frame for the data transmission is employed.

**GPS driven stabilized local clocks:** uses local oven-stabilized $10$ MHz clocks driven by the ultra precise global position systems (GPS) signal. Synchronization down to $1$ ns can be achieved. In order to initially synchronize the received data, a correlation computation can be performed. Correlation computations are efficiently performed by Fast Fourier Transform (FFT) algorithms.

**Detected photon signal driven clocks:** an algorithm to detect the time and frequency differences of independent clocks based on observation of the photon pulses, in particular for correlated photons in EPS systems [20]. It is a non decision-directed method, since signals are treated as random variables, where synchronization is obtained out of the received signal. This method applies to cases where detection times of photons at the receiver location are recorded, and information is identified based on these time stamps. This method requires stable and synchronous clocks to be used for the time stamping. As long as the signal events are initially identified, the drift of the clocks can be tracked directly form the detected signal (tracking algorithm). In this simplest form, where signals events can be identified, a moving average of the time difference $\Delta t = t_i - t_j$ between signal events can be used to track a drift of the reference time between the two sides.

It is practical to retrieve the initial time offset $\Delta T$ by computing a correlation from a data set of time duration $T_a$. $\Delta T$ has to be estimated with an uncertainty $\delta\tau_c$, smaller than $\tau_c$. It is needed to average $n$ time differences $\Delta t$, given by

$$n = \left(\frac{\tau_d}{2\sqrt{2\ln 2}\delta\tau_c}\right)^2 + 1 = \left(\frac{\sigma}{\delta\tau_c}\right)^2 + 1 \qquad (1.5)$$

where $\sigma$ is the time standard deviation of the jitter. Assuming that the jitter has a Gaussian time distribution statistic, $\tau_d = 2\sqrt{2\ln 2}\sigma$. To obtain $n$ signal detections the time synchronization data set $T_a = n/R_b$, where $R_b$ is the expected signal detection rate. Therefore, during $T_a$ the two clocks should not frequency drift more than $\tau_c/T_a$, so that signal events fall in the expected time window $\tau_c$. This translates into a system specification relative frequency accuracy given by $\Delta u \leq \tau_c / \left(n/R_b\right)$.

In order to compute the relative frequency difference $\Delta u$, two clock data sets separated in time by $T_s$ are used. The larger $T_s$, the faster the refining correction algorithm finishes, but the longer the initial synchronization sequence has to be. The relative frequency difference has to be know with an uncertainty such that along the time $T_a$ an event does not fell outside the time resolution bin, given by $T_a \cdot \delta u \leq \delta\tau_c$. Once the time offset $\Delta T$ is known with an accuracy $\delta\tau_c$, the relative frequency difference $\Delta u$ is known with an accuracy $\delta u \approx \sqrt{2}\delta\tau_c/T_s$.

### Noise filtering

In order to reduce the background and dark count rates, there are three main methods: spectral, spatial and temporal filtering. Dichroic and optical interference filters reduce background-noise by strongly attenuating spectral contributions outside an operating bandwidth, typically 3 nm. Clearly, the spectral components of the signal are within this operation bandwidth. Spatial filtering is related to the effective field-of-view (FOV) of the receiver system. The receiver FOV is the resultant of a receiving telescope system and detector's spatial acceptance characteristics. Commonly, the FOV of the receiver system is adjusted to allocate the diameter of the signal spot at the receiver plus some extra marging around to account for beam wandering and the alignment tracking capabilities of the whole system. The temporal filtering, or time gate filtering, consists in blocking noise photons arriving outside the expected narrow time window. The narrower the time gate is, the more efficiency this method can achieve. However, a narrow time gate requires precise synchronization between the sender and receiver. The parameter which limits how narrow the time window can be is the timing jitter (particularly the detectors' jitter).

## 1.3 Quantum key distribution

Cryptography consists of algorithms and protocols that can be used to ensure the confidentiality, the authenticity and the integrity of communications. Quantum cryptography is an application of quantum information that has already reached the level of commercial maturity. Processing with off-the-shelf commercial systems already available. Securing today's encrypted data against future cracking is the driving motivation for quantum cryptography. The target market expands over the next $15$ years from niche users such as governments, defense and research institutes to encompass commercial organizations needing to protect confidential customer information, e.g. large financial, accountancy and law firms. Quantum key distribution (QKD) makes use of quantum optics to guarantee unconditional secure communication [24–26]. It enables two or more parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt information. QKD is part of the broader field of quantum cryptography, which is fundamented in quantum information.

The security of QKD relies on the foundations of quantum mechanics, in contrast to the public key distribution protocol which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping or guarantee of key security. QKD is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret random key. QKD guarantees absolutely secure key distribution based on principles of quantum physics [24, 25], since it is not possible to measure or reproduce a state (e.g. polarization or phase of a photon) without being detected [7, 8, 27]. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. The key can be generated from the measurement of the information encoded into specific quantum states of a photon (qubits), using properties such as the polarization or the phase. An important and unique property of QKD is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superposition or quantum entanglement and transmitting information in quantum states, a communication system can be implemented which detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is unconditionally guaranteed to be secure, otherwise no secure key is possible and communication is aborted.

In QKD systems, one is interested in maximizing three quantities - the secure key generation rate; the tolerable error rate known as quantum bit error rate (QBER); and, closely related, the maximal secure distance. QKD schemes employ single photons sent through a quantum channel, plus classical communications over a public channel to generate a secure shared key. The most common schemes are known as the BB84 protocol [28] and Ekert91 [29]. Although single photon sources may be very useful for quantum computing, they are not strictly required for QKD [30, 31]. A relevant feature of QKD is that the security is linked to the one-time-pad transmission, i.e. the key has to be used once and has to be equal or similar in size to the information being transmitted. This, and the relative difficulty of generating true single photons, motivates also other approaches based on conventional light sources, such as faint pulse sources. Another way of performing QKD is exploiting entanglements, i.e. quantum correlations between photons (signal and idler) generated from the same photon (pump). Entangled photon sources allow distributing random but perfectly correlated sequences between two distant points.

### 1.3.1 QKD protocol principles

Generally, a QKD implementation starts by sending to the receiver, Bob, a long sequence of qubits. Without loss of generality it can be considered that the transmitter, Alice, has generated these qubits considering at least two non-orthogonal quantum measurement basis; i.e. qubits encoded into vertical-horizontal or circular right - circular left polarization basis. Bob, for each single qubit, randomly selects one of the measurement basis and records the obtained results as either $0$ or $1$, as agreed with Alice. Then, in the bases announcement stage, Bob publicly reveal the measurement bases and corresponding qubits detected, but not the specific state measured. The key shared at this point is called the raw key.

Alice and Bob generate the shared sifted key, which corresponds to keeping as valid the detections in which Alice and Bob made compatible choices of bases, which in average is half of the time. Unavoidably, the shared sifted random key will be very similar but not completely equal - in perfect conditions they would be identical, but due to experimental imperfections or eavesdropping, there will be some error ratio QBER. Alice announces a subset of qubits and their values and Bob also returns the bits he received of this subset. At this point, Alice and Bob can estimate the QBER and so work out the maximum amount of information a third party, Eve, can access of their shared random keys. These are interesting results, but on their own they are not enough to solve the key distribution problem. It could be disastrous if Eve learns even a small part of the cryptographic key: she could then read part - perhaps a critical part - of the secret message Alice wants to send. Because errors and background noise can never completely be avoided, Alice and Bob can never guarantee that Eve has no information at all about their keys - communication errors and eavesdropping cannot be distinguished, and so to be on the safe side Alice and Bob have to assume that all discrepancies are due to Eve.

Privacy amplification is a cryptographic version of error correction, which allows Alice and Bob, who start with similar shared sifted random keys, about which Eve has some information, to make shorter shared random keys which are identical, about which Eve no longer has any information. Though classical privacy amplification can be used for either the Bennett-Brassard or the Ekert protocols, it turns out that entanglement-based cryptography allows privacy amplification to be carried out directly at the quantum level. This is more efficient, and has other advantages. In particular, when the technology is fully developed, it will allow quantum

| $E_\mu$ | $f\left(E_\mu\right)$ |
|---|---|
| $0.01$ | $1.16$ |
| $0.05$ | $1.16$ |
| $0.1$ | $1.22$ |
| $0.15$ | $1.35$ |

Table 1.2: Example of the performance of the bidirectional error reconciliation protocol [32] as a ratio with respect to the Shannon limit.

cryptography to be carried out over arbitrarily long distances by using quantum repeater stations along the communication route.

Thus, the optimum ratio between minimum number of bits that Alice and Bob have to reveal, to perform the privacy amplification that enables the error correction and removal of Eve knowledge, are $N_{corr}^{Shannon}$ bits. $N_{corr}^{Shannon}$ bits are needed to correct a key of length $n$, given according to Shannon by

$$\frac{N_{corr}^{Shannon}}{n} = H_2\left(E_\mu\right) \tag{1.6}$$

$E_\mu$ is the QBER of the sifted key generated from the signal state with mean photon number $\mu$ and $H_2$ is the binary Shannon entropy, given by

$$H_2\left(e_1\right) = -e_1 \log_2\left(e_1\right) - \left(1-e_1\right)\log_2\left(1-e_1\right) \tag{1.7}$$

It is not trivial to approach the Shannon limit with error correction codes which use unidirectional classical communication only. Fortunately, a more efficient bidirectional code exists [32], which uses $f\left(E_\mu\right) N_{corr}^{Shannon}$ bits for error correction with a correction factor $f\left(E_\mu\right)$, which is the ratio of actually needed revealed bits to the corresponding number given by the Shannon limit $N_{corr}^{Shannon}$, listed in Table 1.2. These codes are known as information reconciliation techniques (e.g., Cascade [32]) which leak out minimal information to correct those bits that do not match at Alice and Bob.

In QKD transmission performance characterization tests, it is convenient to implement all steps of QKD but computing the lower bound for the secure key rate $R$ instead of the highly computationally privacy amplification step. $R$ takes into account the efficiency of the protocol $q$, Alice pulse rate $N/t$, gain of the signal states $Q$, error ratio QBER and the correction efficiency $f(x)$.

## 1.3.2 Bennet Brassard 1984 protocol

The first protocol for QKD was BB84 [28], which was proposed in $1984$ and experimentally demonstrated in $1992$ [33] by Charles H. Bennett (IBM) and Gilles Brassard (University of Montreal). BB84 is a prepare-and-measure protocol, meaning that Alice simply prepares a sequence of single photon signals and transmits them to Bob. Bob immediately measures those signals; thus, no quantum computation or long-term storage of quantum information is necessary, only the transmission of single photon states.

BB84 protocol has been proven to be unconditionally secure [34, 35]. For the proof to be valid, the source has to emit a single photon per qubit, although it can be extended to be used with currently more practical single-photon-approximated faint pulse sources [36–38].

### Single photon sources

Single-photon emitters have been considered for applications in quantum information processing, quantum cryptography and quantum metrology. For the sake of integration, it is of great interest to stimulate single-photon emission by electrical excitation as demonstrated for quantum dots [39]. Another alternative is to make use of radiative transitions between electronic levels of a single atom or molecule [40].

For single photon sources, the secure key generation rate $R^{single}$ for the limit of long keys, is given by

$$R^{single} \geq q\frac{N}{t}\left\{Q_1\left[1 - H_2\left(e_1\right)\left(1 + f(e_1)\right)\right]\right\} \tag{1.8}$$

where $q$ depends on the implementation (1/2 for the BB84 protocol and $\approx\ 1$ for efficient BB84 protocol), $N$ is the total number of the pulses sent in time $t$, $e_1$ is the QBER for the single photons, $Q_1$ is the gain of single photon signals, $f(x)$ is the bi-direction error correction efficiency and $H_2(e_1)$ is the binary Shannon information function.

The cut-off QBER, such that $R^{single} \geq 0$, is about $11\%$. However, one can verify quantum correlations up to $25\%$.

### Faint pulse sources

Attenuated laser pulses sources or faint pulse sources (FPSs), on average, emit less than one photon per pulse. They are often used in practical QKD systems. The performance limitations of attenuated pulse systems had initially led to believe that single photon sources would be mandatory for building efficient QKD systems. However, the introduction of the decoy-state protocol [36–38] made possible a much tighter bound for the key generation rate, achieving an almost linear dependency of the latter on the channel transmittance. In this way, the technologically much simpler faint pulse systems can offer comparable QKD security with respect to single photon sources.

Furthermore, when using realistic sources implemented by attenuating the pulses, after key distillation, the security is just as good with faint laser pulses as with multi-photon signal sources (Fock states) [24].

### Decoy-state protocol

The protocol introduces some decoy-states, consisting of states that do not differ in any physical characteristic but in the mean photon number (average number of photons per pulse). From now on, distinctions are made for signal and decoy states although they could all be named decoy states; this is so in order to be consistent with common literature. Signal refers to the state with higher mean photon number, while decoy refers to the other states with lower mean photon numbers. Even though introducing decoy states will reduce the overall transmission rate, they allow to better estimate the bounds of $Q_1$ and $e_1$, from the detections at Bob. Thus, obtaining a lower bound for the key generation rate $R$, allowing a larger maximum distance or higher transmission loss. Also, decoy states are useful to detect eavesdropping attacks, by computing the ratio between signal pulses gain $Q_\mu$ and decoy-states gain $Q_\nu$. Thus in a decoy-state protocol what actually matters is to estimate $Q_1$, $e_1$ and $Y_0$, which is common for all states.

The lower bound for the key generation rate $R^{decoy}$ is given by

$$R^{decoy} \geq R_s + R_{\nu_1} + R_{\nu_2} + ... \tag{1.9}$$

where $R_s$ is the $R$ generated from the signal states, $R_{\nu_1}$ is the $R$ generated from the decoy 1 states, and so on. It is always beneficial to generate $R$ independently for the different states. For a matter of clarity, $R_s$ is given by

$$max\left\{q\frac{N_\mu}{t}\left\{-Q_\mu f\left(E_\mu\right)H_2\left(E_\mu\right)+Q_0+Q_1\left[1-H_2\left(e_1\right)\right]\right\},0\right\} \tag{1.10}$$

$\mu$ is the mean photon number of the signal states, $q$ depends on the implementation (1/2 for the BB84 protocol and $\approx 1$ for efficient BB84 protocol), $N_\mu/t$ is the rate of signal states sent (Alice pulse rate times the relative ratio of signal pulses sent), $Q_\mu$ is the gain of the signal states, $E_\mu$ is the QBER for the signal states, $Q_0$ is the gain of the vacuum states sent by Alice [41], $Q_1$ is the gain of single photon states, $e_1$ is the error rate of single photon states, $f\left(x\right)$ is the bi-direction error correction efficiency (taken as $1.16$ [42], for an error rate of $1\%$) as a function of error rate, and $H_2\left(x\right)$ is the binary Shannon information function. Then $R_{\nu_1}$ is given by

$$max\left\{q\frac{N_{\nu_1}}{t}\left\{-Q_{\nu_1} f\left(E_{\nu_1}\right)H_2\left(E_{\nu_1}\right)+Q_0+Q_1\left[1-H_2\left(e_1\right)\right]\right\},0\right\} \tag{1.11}$$

where $N_{\nu_1}/t$ is the rate of decoy state 1 sent (Alice pulse rate times the relative ratio of decoy state 1 pulses sent), $\nu_1$ is the decoy state 1 with mean photon number $\nu_1$; and so on for the following used decoy states.

In order to estimate the yield of vacuum states $Y_0$, single photons yield $Y_1$, and the error ratio of single photons, $e_1$, lower or upper bounds have to be found, respectively. The more decoy states used, better estimations can be performed on the parameters $Y_1$, $Y_1$ and $e_1$, although having one signal state and two decoy states is very similar as using infinite decoy states when considering the asymptotic key generation case. The general and optimum estimation solution is to compose a linear system of equations to be solved numerically. In [42], a suboptimal analytical estimation solution is presented, valid when considering weak coherent phase randomized pulses with fix mean photon number for the different signal and decoy states. When considering a signal state $\mu$ and two decoy states $(\nu_1, \nu_2)$, bounds are given by

$$Y_0^{L_{bound}} = max\left\{\frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, 0\right\} \tag{1.12}$$

$$\begin{aligned} Y_1^{L_{bound}} &= \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} \\ &\cdot \left(Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \cdot (Q_\mu e^\mu - Y_0^{L_{bound}})\right) \end{aligned} \tag{1.13}$$

$$Q_1^{L_{bound}} = \mu e^{-\mu} Y_1^{bound} \tag{1.14}$$

$$e_1^{U_{bound}} = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^{L_{bound}}} \tag{1.15}$$

where $L_{bound}$ and $U_{bound}$ stand for lower and upper bound, respectively. $e_d$ is the probability that a photon is wrongly detected, typically $0.01$ and independent of transmission loss, it is related to misalignments and finite performance of optical components. $Q$ is the gain and $E$ is the QBER of correspondent states $(\mu, \nu_1, \nu_2)$. The QBER for a state with mean photon number $\bar{n}$ is given by

$$E_{\bar{n}} = \frac{e_0 Y_0 + e_d(1 - e^{-\eta\bar{n}})}{Q_{\bar{n}}} \tag{1.16}$$

where $e_0$ is the error rate of background. Typically, $e_0$ is independent of the signal and random, $e_0 = 1/2$.

This suboptimal analytical solution is based on using the decoy states to estimate the three relevant parameters with respect to the signal state. For the proposed analytical solution, there is an important difference between using one decoy state (signal and decoy state), two decoy states (signal and two decoy states) or having a vacuum state. Notice that having a perfect vacuum state is difficult experimentally since most optical components used to select a specific intensity have a finite extinction ratio, thus it is preferable to use the estimations without accounting for a vacuum state (even though these give a slightly higher SKR).

In the decoy-state protocol the optimized rate, for a given distance, is

$$R \approx -\eta\mu f\left(e_d\right) H_2\left(e_d\right) + \eta\mu e^{-\mu}\left[1 - H_2\left(e_d\right)\right] \tag{1.17}$$

This is true for a low background yield $(Y_0 << \eta)$ and small transmittance $\eta << 1$ (typical values are $Y_0 = 10^{-5}$ and $\eta = 10^{-3}$). Then, the key generation rate is optimized when $\mu = \mu_{opt}$, which satisfies

$$\left(1 - \mu_{opt}\right) e^{-\mu_{opt}} = \frac{f\left(e_d\right) H_2\left(e_d\right)}{1 - H_2\left(e_d\right)} \tag{1.18}$$

Usually $\mu_{opt}$ is around $0.5$, and the key generation rate and distance are pretty stable against even a 20% change of $\mu$.

It is important to stress that, as pointed out in [43], there is an optimal $\mu$ depending on the transmission losses. Concentrating on the optimal choice of the expected photon number which yields the maximal gain rate; the gain drops roughly exponentially with the length of the transmission before it starts to drop faster due to the increasing influence of the dark counts. The initial behavior is mainly due to the multi-photon component of the signals while the influence of the error-correction part is small.

### 1.3.3 Other protocols

There is a large collection of other QKD protocols such as entanglement-based [29], other prepare-and-measure protocols and variations of BB84. A fairly complete revision of all of them can be found in [24, 25] and a detailed security analysis of practical QKD devices in [26, 44].

## 1.4 Random number generators

Random numbers form sequences of numbers or symbols that lack any pattern. A random number generator (RNG) is a computational or physical device designed to generate random numbers. The need for random numbers in research and technology was recognized very early [45], and has motivated electronic and photonic advances [46–48].

RNGs can be classified in pseudo-RNGs (PRNGs), computational algorithms, and true-RNGs (TRNGs), physical devices designed to generate a sequence of numbers or symbols that lack any pattern. Moreover, TRNG can be subdivided into classical RNGs (CRNGs), based on classical hardware devices, and quantum RNGs (QRNGs) based on the intrinsic randomness of quantum observables. Algorithms can rapidly produce pseudo-random outcomes, series of numbers that mimic most properties of true random numbers while quantum random number generators (QRNGs) exploit intrinsic quantum randomness to produce true random numbers. Single-photon QRNGs are conceptually simple but produce few random bits per detection. In contrast, vacuum fluctuations are a vast resource for QRNGs: they are broad-band and thus can encode many random bits per second. Direct recording of vacuum fluctuations is possible, but requires shot-noise-limited detectors, at the cost of bandwidth.

Random numbers support critical activities in advanced economies, including secure communications [25, 49, 50], numerical simulation [51] and quantitative finance [52]. Cryptography requires true random numbers to generate keys, but how many depends on the encryption scheme. The unconditionally secure one-time-pad scheme is the most demanding of all; it requires as many random bits as there are bits of information to be encrypted. Many security applications have failed or been severely compromised because their RNGs failed to be sufficiently random. The larger the random number sequence rate the larger the communication bit rate. It is thus essential to increase the RNG rate so that future demands for ever-increasing communication rate, currently $10$ Gbps, $40$ Gbps and in the near future $100$ Gbps per channel, will be met. Modern lotteries and gambling machines are all based on the use of random numbers to guarantee a uniform winning probability. It must not be possible for a player to increase his probability to win by discovering a bias towards certain outcomes in the game procedure. Financial simulation techniques, such as Monte Carlo simulations, are statistical based behavioral approaches that apply predetermined probability distributions and random numbers to estimate risky outcomes. By tying the various cash flow components in a financial model together in a mathematical model and repeating the process several times, the financial analyst can develop a probability distribution of project returns. From the distribution of returns, a financial analyst can determine not only the expected value of the return but also the probability of achieving or surpassing a given return. From a more research and development application perspective, scientists have devised techniques relying on random numbers to model and simulate complex systems. These techniques are fast, yield high accuracy results, thus essential for modern numerical simulations. There are also many experiments in research laboratories in the fields of quantum communication and information, which rely on the use of random generation sources.

For this reason, there has been intense effort to develop practical true RNGs, to replace existing pseudo-random methods. Quantum random number generators (QRNGs) employ a true source of randomness known to science, the randomness embedded into quantum physics. Recently, it has been shown that quantum physics also can be used to verify the randomness of entanglement-based generators [53,54]. Examples of demonstrated QRNGs include two-path splitting of single photons [55], photon-number path entanglement [56], time of generation or counting of photons [57–61], fluctuations of the vacuum state using homodyne detection techniques [62, 63] as well as interferometric schemes [64, 65]. Current commercial RNGs devices are based in: quantum single photon detector array [66], CMOS metastability, noise signal by using stochastic physical phenomenon of electrons trapped in the silicon nitride layer of a transistor, arrival detection time of photons of a cw operated laser, reversed bias semiconductor junction and thermal or Johnson noise and transistor noise [67]. Current patents on TRNG are: a light beam illuminating a detector array [48], chaotic laser signal [68], wave diffraction using high-order grating [69], detection of light as photon detection events [70], single photon going to a single-mode coupler [71], electrical noise [47, 72], laser beam splitting in homodyne detection [73].

### 1.4.1 Randomness principles

Randomness corresponds, ideally, to having a totally unpredictable sequence, which entails both low correlation and high entropy. At a more fundamental level, any classical system is no such thing as true randomness because it admits in principle a deterministic description and thus appears random as a consequence of a lack of knowledge about its fundamental description. Quantum theory is, on the other hand, fundamentally random, thus a true potential resort for generating random numbers. Even though, in a real device the intrinsic randomness of quantum systems is necessarily mixed-up with an apparent randomness that results from noise or lack of control of the device.

Post-processing algorithms can be used to remove bias from a sequence of quantum random numbers affected by bias. The simplest unbiasing procedure was first proposed by von Neumann [74]. More advanced random numbers data refining algorithms are hash functions and randomness extractors. A hash function is any algorithm or subroutine that maps large data sets of variable length to smaller data sets of a fixed length. A good hash function should map the expected inputs as evenly as possible over its output range. That is, every hash value in the output range should be generated with roughly the same probability. Note that this criterion only requires the value to be uniformly distributed, not random in any sense. Cryptographic hash functions, such as Whirlpool [75], have even stronger uniformity guarantees than checksums or fingerprints, and thus can provide very good general-purpose hashing functions. A randomness extractor [76, 77], as Trevisian's extractor [78], is based on a family of hash functions with the property that for any variable with enough entropy, the output is uniformly distributed. A common practice is to use cryptographic hash functions for the purpose of randomness extraction. A main reason for this practice is that cryptographic hash functions are readily available in software and hardware implementations, and are required by most cryptographic applications for purposes other than randomness extraction. Therefore, it is attractive and convenient to use them for random bit extractions.

### 1.4.2 Randomness measures and tests

Randomness, as opposed to unpredictability, is held to be an objective property. Also, what appears random to one observer may not appear random to another. One of the intriguing aspects of random processes is that it is hard to know whether a process is truly random or a quantitative measure of randomness. RNGs are the basic tools in many applications therefore as in any relevant task performed by a device, the user has to know his tool [79]. Clearly, an objective characterization of any RNG wanted to be used in a specific task will always be required. Even, QRNGs may be imperfect in a practical setting. For example, as time goes on, a QRNG may become biased when the probability of one outcome is not equal to the probability of the other outcome.

The quality of the randomness required for different applications varies. For example, creating a nonce in some protocols need only uniqueness of use of a random sequence. On the other hand, generation of a master key requires a higher quality, more entropy. And in the case of one-time pad encryption, the information-theoretic guarantee of perfect secrecy only hold if the key material is obtained from a true random source with high entropy. Two main requirements for a RNG are identified: the random numbers generated should have good statistical properties; and the knowledge of subsequences of random numbers shall not enable to compute predecessors or successors or to guess them with non-negligible probability.

A numeric sequence is said to be statistically random when it contains no recognizable patterns or regularities [80]. Statistical randomness does not necessarily imply true randomness. There are many practical but not complete measures of statistical randomness for a binary sequence. These include measures based on frequency, discrete transforms, statistical, or a mixture of these. When a supposedly random sequence generated from a RNG starts to fail a test decisively, a p-value of the test usually converges to $0$ or $1$ exponentially fast as a function of the sample size of the sequence used.

Correlation and entropy values are useful parameters to characterize a random sequence generated by a RNG. However, correlation and entropy usually cannot be directly measured as a physical magnitude, i.e. voltage, but have to be estimated numerically. As a rule of thumb, computing the autocorrelation of a sequence is a statistical method that looks for periodicity in a data set. While, computing entropy estimates the amount of uncertainty of the sequence. Inconveniently, numerical estimation of correlation and entropy only operate on properties of random variables but not of observed random numbers, hence they do not completely validate the randomness present in the sequence but only statistically. Although, recently a QRNG was proposed which also allows to verify the generated sequence is random [53]. The proposed QRNG takes advantage of quantum entanglement and violation of Bell inequality measurements showing that the non-local correlations can be used to certify the presence of genuine randomness, providing a bound for the entropy generated.

## 1.5 Aims of the thesis

Despite the achievements of quantum communication experiments, the distances over which entanglement can be distributed in a single section, i.e. without a quantum repeater in-between, are by far not of a global scale. Experiments based on present fiber technology have demonstrated that qubits can be sent to $200$ km in the field, but no improvements by orders of magnitude are to be expected. On the other hand, optical free-space links could provide a unique solution to this problem since they allow in principle for much larger propagation distances of photons due to the low absorption of the atmosphere in certain wavelength ranges.

Free-space optical links have been studied and successfully implemented already for several years for their application in quantum cryptography based on faint classical laser pulses. A next crucial step was demonstrated, namely the distribution of quantum entanglement via a free-space link, which was verified by violating a Bell inequality between two distant receivers without a direct line of sight between them. However, terrestrial free-space links suffer from obstruction of objects in the line of sight, from possible severe attenuation due to weather conditions and aerosols and, eventually, from the Earth's curvature. They are thus limited to distances typically of the same order as the fiber links. To fully exploit the advantages of free-space links, it will be necessary to use space and satellite technology. By transmitting or receiving either photons from a satellite, qubits can be distributed over truly large distances and thus would allow quantum communication applications on a global scale. A significant advantage of satellite links is that the attenuation of a link directly upwards to a satellite is comparable to about 5-8 km horizontal distance on ground. Proof-of-principle experiments for such distances in free space exist for weak laser pulses. Several studies are currently underway and suggest the feasibility of space-based experiments based on current technologies [81, 82].

Nevertheless, many of the goals to be achieved in free-space quantum communication are shared with fiber-based technology.

- The first task of this thesis is to develop a new class of high speed integrated photonic sources for applications in free-space QKD systems, capable of producing unprecedented qubit rates (100Mbps - 1Gbps) and transmitting those over larger distances than those achieved so far ($>$ 200km). Two new FPs schemes have been implemented and its performance measured. These sources can be used in future free-space QKD link experiments.

- The second task of the thesis is to use novel schemes for quantum random number generation. In particular, high random number generation rates and low cost devices are to be achieved. The final aim of this task is to develop a QRNG product, thus collaboration with industry will be established.

- Another objective is to implement a free-space QKD system for mobile platforms. The work presented in the final part of this thesis was driven by a proposed application of implementing for the first time a free-space quantum communication between moving platforms, over a short distance (1 km).

## 1.6 Thesis outline

In **Chapter 2**, a proposed faint pulse source based on proven high speed lithium niobate modulators is described and the technical foundations of the design are analyzed. Mainly, the performance of the amplitude modulator and the polarization modulator are described. The technical details of the other building blocks of the source, e.g. laser diode and calibrated variable optical attenuator, are also presented. Finally, the relevant QKD parameters of the source were experimentally measured and discussed. In **Chapter 3**, a demonstrated faint pulse source based on semiconductor optical amplifiers is described in detail. Mainly, the source is based on semiconductor optical amplifiers operating as switching devices with high extinction ratio to select the output polarization state. Furthermore, a complete analysis of the security of the source in terms of QKD is presented, based on calculations of the indistinguishability of the generated optical states. Finally, a QKD transmission measurement is presented, which clearly reflects the achieved performance of the source. In **Chapter 4**, a proposed random number generator is described and the physics foundations which is based on are analyzed. It extracts random bits from vacuum using optical independent amplification. Finally, a statistical testing of the randomness is performed to qualify the device up to current validation methods. In **Chapter 5**, a free-space QKD system is presented and technical details described. Firstly, an automatic operating faint pulse source is described, also consisting of a polarization control system suitable for free-space links. Secondly, a compact mechanical polarization receiver attached to a tracking receiving telescope was developed. Requirements and procedures for QKD system data synchronization and processing is presented. Finally, in **Chapter 6**, several conclusions on the thesis work and possible future work directions are presented.

# Chapter 2

# $LiNbO_3$ modulators based QKD source

It is important to develop faint pulse sources and systems for QKD which can generate high key rates. In this Chapter, a proposed faint pulse source based on proven high speed lithium niobate modulators is described and the technical foundations of the design are analyzed. Mainly, the performance of the amplitude modulator and the polarization modulator are described. The technical details of the other building blocks of the source, e.g. laser diode and calibrated variable optical attenuator, are also presented. Finally, the relevant QKD parameters of the source were experimentally measured and discussed.

## 2.1 The integrated faint pulse source

One of the integrated faint pulse source (FPS) developed in our laboratory [83] for QKD consists of commercially available space-qualified discrete components; single semiconductor distributed-feedback (DFB) laser diode (LD) emitting a continuous pulse train at 100 MHz followed by integrated (waveguide) amplitude (AM) and polarization (PM) lithium niobate ($LiNbO_3$) modulators, shown in Fig. 2.1.

The pulse train generated by the LD is sent through a polarization

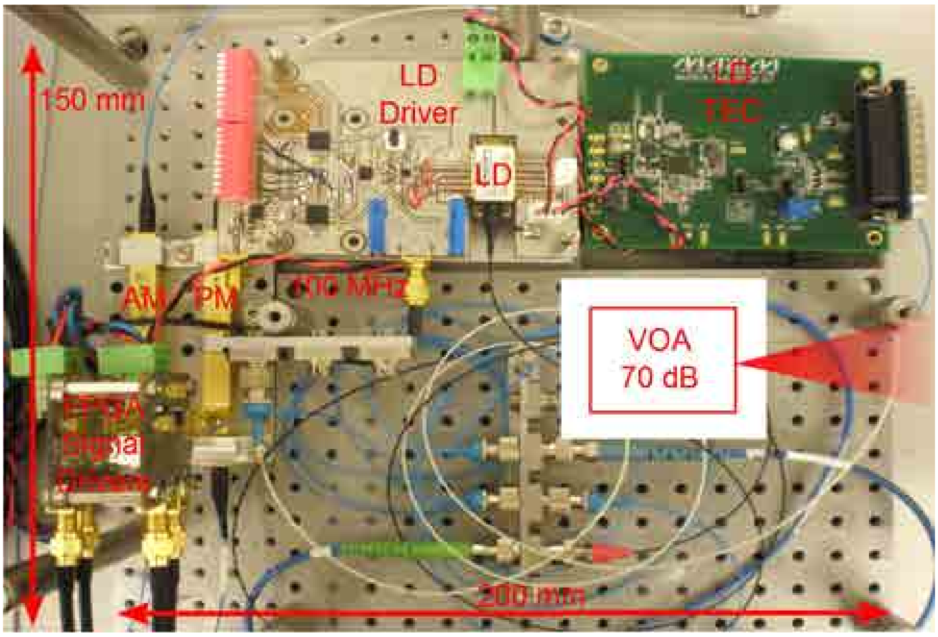


Figure 2.1: Scheme of the QKD source inside a $200$mm x $150$mm box. (LD Driver) denotes the electrical current pulse generation, (LD TEC) the laser diode temperature controller driver, (LD) the laser diode, (FPGA Signal Driver) the electronic digital-to-analog drivers for the modulators, (AM) an amplitude modulator, (PM) a polarization modulator and (VOA) a variable optical attenuator.

maintaining fiber (PMF) into the AM (a Mach-Zehnder modulator in LiNbO$_3$) that generates three different levels of intensity. Note that if the LD were driven in pure continuous wave (CW) mode (no pulse train) and externally modulated to generate the intensity pulses, two potential issues would occur: (i) pulses with different energies (number of photons) would unavoidably have different temporal and spectral shapes due to the nonlinear electro-optic response (optical output as a function of driving voltage) of the AM; (ii) there would be phase coherence between the pulses due to the relatively long coherence time (narrow spectrum) of a DFB structure, thus increasing the vulnerability of the QKD transmission [84].

After the AM, the pulses are injected into the PM through a PMF. The PM a waveguide LiNbO$_3$ phase modulator with the PMF input axis oriented at $45°$with respect to the optical axis. In this way, the two orthogonal equal amplitude polarization components of the electromagnetic field that propagates in the crystal experience a refractive index difference, which is proportional to the voltage applied to the modulator. By applying different voltages one can thus change the state of the output polarization, in particular to linear $+45°$, $-45°$, right-handed circular and left-handed circular. The optical pulses present a spectrum within the acceptance bandwidth of the two modulators, so that amplitude and polarization modulation can be achieved with sufficient extinction ratio.

## 2.2 LiNbO$_3$ electro-optical modulators: Pockels effect

LiNbO$_3$ is a uniaxial trigonal $3m$ crystal whose refractive indices change when an electric field is applied. This is known as Pockels effect, shown in Figure 2.2. LiNbO$_3$ electro-optic modulators' typical parameters are: electrode gap $10\mu$m, $r_{33} = 30$pm/V, $n_e = n_{33} = 2.24$, $r_{13} = 4$pm/V and $n_0 = n_{13} = 2.16$. Hence, the change of ordinary and extraordinary refractive index when a $V_\pi$ is applied corresponds to

$$n_0\left(E\right) \approx n_0 - \frac{1}{2}n_0^3 r_{13} E = 2.16 - 2.02 \cdot 10^{-6} E \tag{2.1}$$

$$n_e\left(E\right) \approx n_e - \frac{1}{2}n_e^3 r_{33} E = 2.24 - 1.69 \cdot 10^{-5} E \tag{2.2}$$

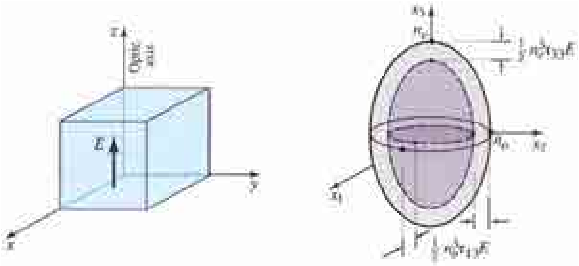


Figure 2.2: Modification of the index ellipsoid of a trigonal $3m$ crystal such as LiNbO$_3$ resulting from the application of a steady electric field along the direction of the optic axis [85].

### 2.2.1 Relevant transmission line theory

To achieve high speed modulation with a LiNbO$_3$ modulator, by applying an electric signal, requires a good matching of the microwave signal field and the optical field propagation speeds. The microwave signal is applied on impedance matched electrodes conforming a transmission line. The voltage in a transmission line corresponds to

$$V(z) = V^+ \left[e^{-j\beta z} + \rho(0)e^{e^{j\beta z}}\right] \tag{2.3}$$

where $V^+ = V_G/2$, $V_G$ is the voltage supplied by the generator, $\beta = 2\pi/\lambda$ and $\rho = |\rho|\, exp\left(j\theta\right)$. Open- or short-ended transmission lines have $|\rho\left(0\right)| = 1$, while a matched load one produces $\rho = 0$. In particular, an open-ended transmission line produces a voltage and current distribution given by

$$V = 2V^+ \cos(\beta z) \tag{2.4}$$

$$I = -2j\frac{V^+}{Z_0}\sin(\beta z) \tag{2.5}$$

For low frequencies, where the wavelength is much longer than the modulator electrodes length, in an open-ended transmission line, the voltage of the standing wave is twice the one as for a matched transmission line. Hence, not loading the electrodes allows to use lower generator voltages but the bandwidth is limited by the length of the electrodes. Without termination impedance, its input's frequency dependence can be modeled as a lossy open transmission line equivalent to a RC circuit. When matching the electrodes impedance, using a termination impedance, the needed generator voltage doubles, but the bandwidth is much larger, i.e. 10 GHz-40 GHz.

### 2.2.2 Temperature stability

The half-wave voltage $V_\pi$ is the drive voltage necessary to produce $180°$optical phase shift. Dependence on temperature of the $V_\pi$, is given by the expression

$$V_\pi = \frac{\lambda S}{2n^3 r_{33} L\Gamma} \tag{2.6}$$

where $\lambda$ is the optical wavelength, $S$ is the electrode gap, $n$ is the refractive index, $r_{33}$ is the electrooptic coefficient, $L$ is the electrode length, and $\Gamma$ is the electric field/optical field overlap factor. The electrode gap and length are only weakly temperature dependent [86]. For X-cut Y-propagating modulators, the electrode gap can be expected to contract $\sim 4 \cdot 10^{-6}$ m/m-K as the temperature is decreased. Likewise, the electrode length will be reduced $\sim 16 \cdot 10^{-6}$ m/m-K as the temperature is lowered. For typical electrode gaps ($10\mu$ m) and electrode lengths ($10$ mm), the refractive index $n$ is also temperature dependent as $(1/n)dn/dt =$

$3.18 \times 10^{-6}$/K [87]. The overlap factor, $\Gamma$, is negligibly affected by temperature and does not need to be considered. The temperature dependence of the electro-optic coefficient, $r_{33}$ is $(1/r)dr/dt = 0.00049$/K over the temperature range of $293$K to $473$K [88]. This same value can be used to extrapolate to below room temperatures. Thus, the variation of the half-wave voltage over temperature is given by

$$\frac{1}{V_\pi}\frac{\Delta V_\pi}{\Delta T} \approx -\frac{5.20 \times 10^{-4}}{\Delta T} \tag{2.7}$$

where no $\lambda$ temperature dependence has to be considered nor for the overlap factor. Thus, around $1.04\%$ variation of the $V_\pi$ is expected for a $20°$C variation [89].

A PMF is used at the input of LiNbO$_3$ modulators. The reason for this is that LiNbO$_3$ devices are polarization sensitive and a particular polarization is required at the input. This approach has been shown to be useful for commercial devices operating over the temperature range of $-20°$to $+80°$. Issues can arise when extreme temperature variations are encountered because of the vastly different temperature coefficient of expansion (TCE's) of the various materials. Typical room-temperature TCE's are $200$, $16$, and $0.5$ ($\times 10^{-6}$m/m-K) for urethane adhesive, LiNbO$_3$ ($y$-axis), and optical fiber, respectively [90].

Some fully extended studies for LiNbO$_3$ modulators dependence over temperature have been carried out, in particular at around $800$ nm in [89, 91,92]. The frequency response shows no degradation due to temperature dependence. Methods for accurately measuring $V_\pi$ voltage parameter are shown in [93].

The DC bias voltage point is more temperature dependent, effect known as bias drift, therefore has to be actively controlled or calibrated. The bias drift is due to electron carriers screening causing an effective voltage largely different from the applied bias voltage in the long term (hours). Thus once in the steady state, desired small voltage bias variations will be correctly supported while large desired voltage bias variations will initiate a new electron carrier screening. X-cut modulators show a higher stability than Z-cut ones, in particular temporal stability, in the order of thousand of hours [94]. Instead, Z-cut configurations exhibit lower driving voltage and higher bandwidth, but X-cut ones exhibit more stability and lower chirp. Optical fiber modulators are of great interest to space flight projects for communications and LIDAR applications. Due to harsh environment and long duration for most missions, space flight applications have a unique set of demands for photonics parts [95].

### 2.2.3 Amplitude modulator

The AM used in the presented source was selected to be space-qualified working at around $800$ nm. The DC uncoupling capacitor for the amplitude modulator was removed to double the effective electrical signal voltage. Hence, the RF input accepts DC voltages and the DC input can be just grounded.

In terms of QKD performance, the more accurate the voltage driving the larger the secure key rate (SKR), given an optimum mean photon number for the different signal and decoy states. The variation on the mean photon number for the signal state and decoy-states due to optical power variation is given by

$$\frac{\Delta \bar{n}}{\bar{n}} = \frac{\Delta P}{P} \tag{2.8}$$

Possible sources of optical power variation could be due to the AM driving voltage, insertion loss (IL) of the connectors and attenuation variation of the variable optical attenuator. Assuming that the latter will not present attenuation variations, the IL variations will be compensated by working slightly off the AM's maximum transmission point. Then, the optical power variations due to the driving electronics accuracy are approximately given by

$$\frac{\Delta P}{P} = 10^{\mathrm{ER}/10} \frac{\Delta V}{V_\pi} \tag{2.9}$$

where $ER = 25$ dB is the typical maximum extinction ratio of an AM in CW LD operation, the half-wave voltage $V_\pi = 1.5V$ and $\Delta V$ is the voltage accuracy of the driving electronics.

Usually $\mu_{optm}$ is around $0.5$, and the key generation rate and distance are pretty stable against even a $\Delta\mu = 20\%$. Then, the maximum power variation acceptable is $\Delta P/P = \Delta\mu = 20\%$, requiring a driving voltage accuracy better than $\Delta V/V_\pi = 0.06\%$

### 2.2.4 Polarization modulator

The polarization modulator described in this thesis is a waveguide LiNbO$_3$ phase modulator where the polarization maintaining fiber (PMF) input axis is oriented at 45°with respect to the optical axis. In this way, the two orthogonal equal amplitude polarization components of the electromagnetic field that propagates in the crystal experience a refractive index difference, which is proportional to the voltage applied to the modulator. By applying different voltages one can thus change the state of the output polarization, in particular linear $+45°$, $-45°$, right-handed circular and left-handed circular. The particular polarization modulator is a Z-cut Ti:LiNbO$_3$ embedded strip waveguide fabricated by diffusing titanium into a lithium niobate substrate to increase its refractive index in the region of the strip. The refractive indexes given by the provider are TM mode (extra-ordinary, fast axis $n_e = 2.17$) and TE mode (ordinary, slow axis $n_0 = 2.25$), and the optical chip length is 71mm.

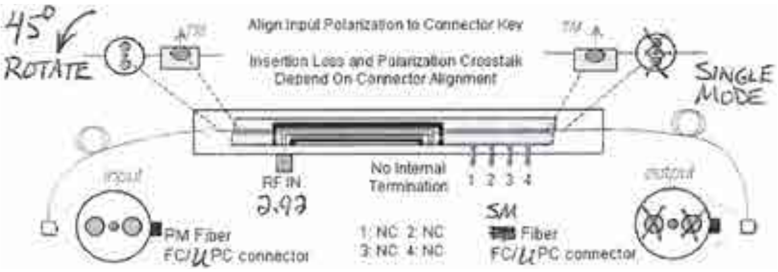


Figure 2.3: Optical connectorization schematic of the PM.

In order to achieve a good SKR generation in QKD systems, the figure of merit is the QBER. The QBER is directly related to the physical parameter the qubits are encoded with. In the current source, the qubits are encoded on the polarization state of the photons. Generally, the QBER is given by

$$\text{QBER} = 1 - \cos^2(\Delta\theta) \tag{2.10}$$

where $\Delta\theta$ is the angular misalignment with respect to the desired polarization state. A common design value for QBER is $0.01$. Hence a polarization maximum angle difference of $\Delta\theta = 0.1$rad (5.74°) can be tolerated.

The PM used is capable of producing any polarization state along a full circle of the Poincare sphere, consisting in a full $2V_\pi$ voltage scan of the driving voltage. The driving voltage accuracy is given by

$$\frac{\Delta\theta}{\theta} = \pi\frac{\Delta V}{V_\pi} \tag{2.11}$$

where the half-wave voltage $V_\pi = 1.5$V. Thus the driving voltage accuracy has to be lower than $\Delta V = 3.18\%$, respect to $V_\pi$. Regarding the applied voltage to polarization state generated performance, its variation can be assessed with the angle to intensity relation when using a polarizer in analyzer configuration, given by

$$\Delta\theta \approx \frac{\Delta P}{2P} \tag{2.12}$$

where $P$ is the power intensity of light exiting the modulator and $\Delta P$ is the intensity variation after the step ($P$ as an approximation, can be taken as $P = \Delta P_{step}/cos^2((\pi/V_\pi)\Delta V_{step})$ and $\Delta P$ as the power fluctuation once the step as shown in Fig. 2.7 (a) and (b)). This power variation can be translated into QBER increase by

$$\frac{1}{2}(1 - \cos(2\Delta\theta)) \approx \frac{1}{2}\left(1 - \cos\left(\frac{\Delta P}{P}\right)\right) \tag{2.13}$$

as derived above in (Eq. 2.10). Thus, the tolerable optical power variation is $\Delta P/P = 20.03\%$

### Polarization modulator PMD

An impairment of the current PM configuration is the degradation of degree-of-polarization (DOP), directly related to the QBER, due to the optical bandwidth of the input optical pulses which undergo polarization mode dispersion (PMD) along the PM. The introduced PMD in the PM is due to the refractive index difference between the ordinary and extraordinary refractive indices already at a static operation.

The required DC voltage to achieve a static compensation of the refractive indices by applying a DC offset is too high, hundreds of Volts. Besides dielectric breakdown might be present, occurs in air at an electric field strength of about $E_{max} = 3 \times 10^6$V/mm. Instead, an external PMD compensation can be achieved using a matched-length PMF patchord which undoes the phase rotations introduced by the PM. First, phase rotation was experimentally measured using the extrema counting measurement [96].

The LD current driver controller was used to apply a low frequency modulation triangular signal to the driving current of the LD, through the LD controller modulation input, in order to generate a frequency sweep. DFB LD emits at the frequency $\nu_0$ corresponding to

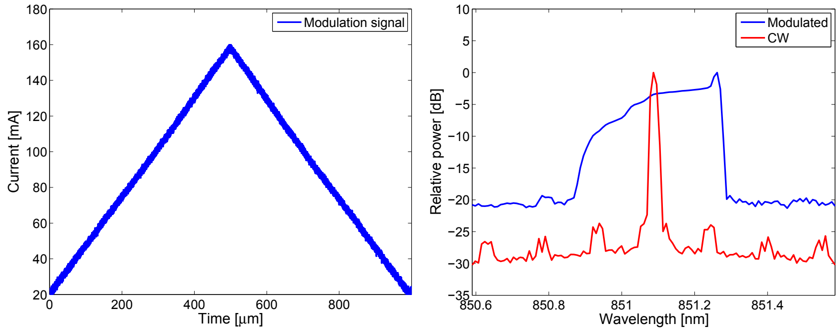
$$\nu_0 = \frac{c}{2\Delta\mu_e} m \tag{2.14}$$

where $c$ is the speed of light in vacuum, $\Delta$ is the period of the grating, $\mu_e$ is the effective refractive index and $m = 1, 2$ stands for first- or second-order grating. The effective refractive index depends on the optical frequency and on the carrier density, which also holds dynamically under modulation conditions and it clearly indicates the relation between a modulation of the carrier density and the modulation of the optical frequency [97].

In Figure 2.4 (a) is shown the current modulation $1$ kHz triangular signal and in Fig. 2.4 (b) the generated optical frequency sweep as a spectrum measurement. A frequency sweep of $0.45$ nm, $186.85$ GHz, is produced.

It is convenient to introduce the mean differential group delay $\Delta\tau$ introduced by PMD. $\Delta\tau$ can be determined by extrema counting as

$$\Delta\tau = \frac{N_e \lambda_{start} \lambda_{stop}}{2(\lambda_{stop} - \lambda_{start}) v} \tag{2.15}$$



**(a)** Current triangular modulation signal.

**(b)** Generated optical frequency sweep.

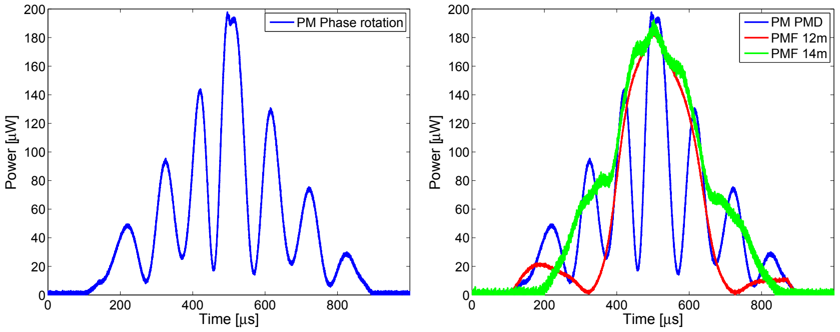
Figure 2.4: The LD is driven in current with a $1$ kHz triangular signal (a) to produce a LD optical output frequency sweep (b).

where $\lambda_{start}$ and $\lambda_{stop}$ are the ends of the wavelength sweep, $N_e$ represents the number of transmission extrema (peak and valleys) across the scan, and $v$ is the speed of light in the medium. $\Delta\tau$ is related to $\Delta\theta = \Delta\tau 2\pi\Delta\nu$, where $\Delta\nu$ is the optical frequency bandwidth.

In Figure 2.5 (a) are shown the phase rotations introduced by the PM. Notice that the number of rotations have to be considered only in the corresponding range of the rising current ramp. In Figure 2.5 (b) are shown the phase rotations produced by the PM and the corresponding compensations by using different length PMF fibers at the output of the PM, properly aligned in terms of polarization with respect to the bulk chip of the PM.

The PM produces a phase rotation of $3.5-4$ cycles during the positive raising of the current ramp of the modulation signal, which accounts for a low $9.7\%$ QBER. The compensating PMF fiber patchord of $14$ m long only produces $1.5$ phase rotation cycles, producing a better $1.4\%$ QBER.

An alternative solution is to acquire a PM which propagates in Y-cut, the optical mode propagates along $z$, where there is no $\Delta_n$ for the static situation because the projected $x$ and $y$ E fields have the same refractive



**(a)** Phase rotation produced by the PM.

**(b)** Compensated phase rotation using PMF fiber of different lengths.

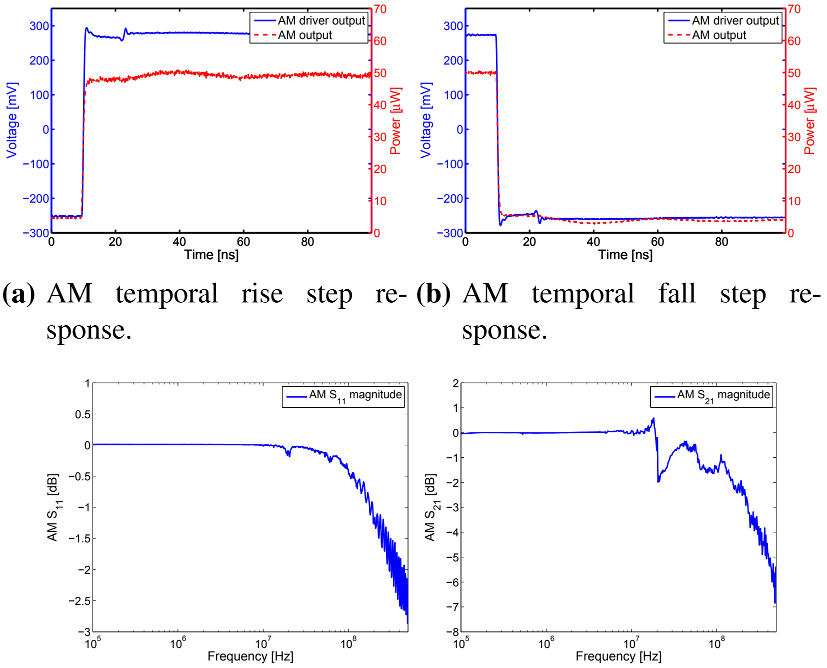
Figure 2.5: PM phase rotations. Different PM PMD compensation results using PMF fibers.

index $n_o$. Nevertheless, when an electric field is applied a difference in the refractive indices appears but with a lower nonlinear coefficient, thus higher driving voltages would be required.

### 2.2.5 Modulators' driving response

The temporal step response was measured using as voltage input to the modulators a square wave of $1$ MHz, $1.088$ GS/s, and $500$ mVpp from a waveform generator and the output was sampled with an oscilloscope. For the frequency response measurement, a network analyzer was used scanning from $100$ kHz to $500$ MHz with calibration data and $0$ dBm RF power.

Top rows in Figs 2.6 and 2.7 show the temporal profiles of the applied voltage steps rise/fall applied to the AM and PM, respectively, as well as the generated optical outputs. The voltage-stair-step produced on the driving voltages is due to the reflection of the transmitted driving signals through the $0.5$ m SMA-coaxial cable. Therefore, in order to avoid this



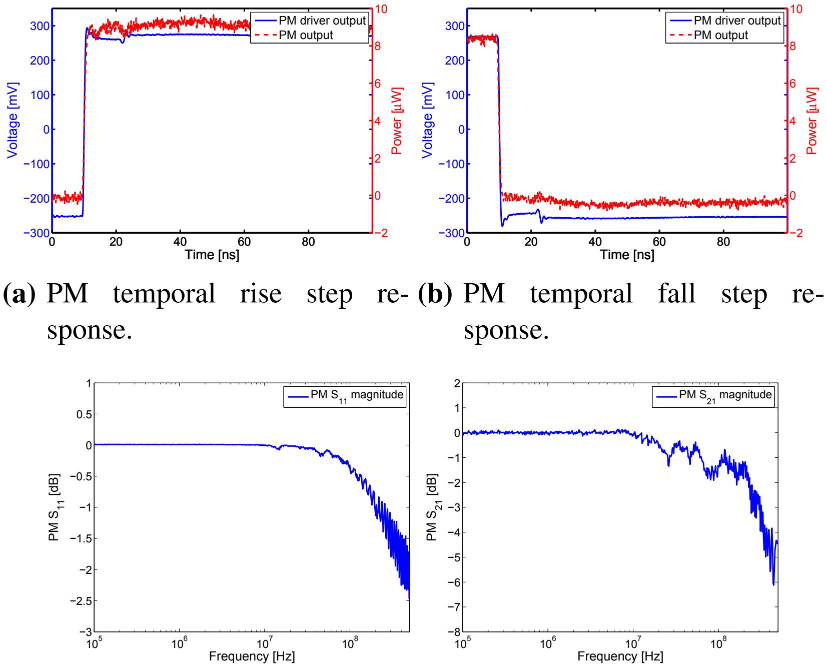
**(a)** AM temporal rise step response.

**(b)** AM temporal fall step response.

**(c)** AM S$_{11}$ parameter magnitude.

**(d)** AM electro-optics S$_{21}$ parameter magnitude.

Figure 2.6: AM RF temporal and frequency response.



**(a)** PM temporal rise step response.

**(b)** PM temporal fall step response.

**(c)** PM S$_{11}$ parameter magnitude.

**(d)** PM electro-optic S$_{21}$ parameter magnitude.

Figure 2.7: PM RF temporal and frequency response.

| Achieved performance | AM |
|---|---|
| $V_\pi$ temperature variation ($\Delta T = 20$°C) | $1.04\%$ |
| $V_\pi$ frequency variation (100KHz-50MHz) | $1.46\%$ |
| Driver voltage accuracy $\Delta V/V_m$ (Rise/Fall) | 2.40%/2.30% (avoiding reflection peaks) |
| Achieved voltage accuracy | 4.9%/4.8% |
| Specified voltage accuracy | $0.06\%$ |
| Modulator output accuracy (Rise/Fall) | 5.63%/5.36% |
| Power intensity frequency variation (100KHz-10MHz/50MHz) | 2.28%/13.90% (avoiding peaks) |
| Achieved power intensity accuracy (100KHz-50MHz) (Rise/Fall) | 19.53%/19.26% |
| Specified power intensity accuracy | $20\%$ |

Table 2.1: Operational specifications compliance for the AM, in order to achieve a power intensity level accuracy lower than $20\%$.

| Achieved performance | PM |
|---|---|
| $V_\pi$ temperature variation ($\Delta T = 20$°C) | $1.04\%$ |
| $V_\pi$ frequency variation (100KHz-50MHz) | $1.71\%$ |
| Driver voltage accuracy $\Delta V/V_m$ (Rise/Fall) | 2.50%/2.20% (avoiding reflection peaks) |
| Achieved voltage accuracy | 5.25%/4.95% |
| Specified voltage accuracy | $3.18\%$ |
| Modulator output accuracy (Rise/Fall) | 3.24%/4.60% |
| Polarizations state frequency variation (100KHz-10MHz/50MHz) | 1.83%/16.82% (avoiding peaks) |
| Achieved polarization state accuracy (100KHz-50MHz) (Rise/Fall) | 20.06%/21.42% |
| Specified polarization state accuracy | $20.03\%$ |

Table 2.2: Operational specifications compliance for the PM, in order to achieve QBER lower than $1\%$.

voltage-stair-step the transmission lines connecting the control electronics and the modulators have to be short.

Table 2.1 summarizes the goal and the achieved performance specifications for the AM, while in Table 2.2 are summarized the ones for the PM. The achieved performances are either fulfilled or close to the requirements.

In order to stay within the required operational specifications for both modulators, the length of the transmission lines connecting the driving electronics to the modulators have to be shorter than $10$ cm. Furthermore, the operation of the AM requires a driving voltage accuracy better than $600$ ppm, while the PM requires better than $3\%$. Moreover, the temporal DC stability of the modulators was measured to be larger than $5$ minutes.

## 2.3 Variable optical attenuator

For the implementation of a QKD system using decoy-state protocol, besides four different polarization states, the FPS source should generate three intensity levels (optimally $1/2$, $1/8$ and $0$ photons in average per pulse [42]). Using a variable optical attenuator (VOA), it is possible to operate in the single photon regime. The photon energy at $850$ nm is $E_{ph} = 2.3386 \cdot 10^{-19}$ J. The optical pulse duration $\approx 400$ ps and the pulse peak power $3.5$ mW, corresponding to $1.4$pJ energy per pulse. Thus, a number of photons per pulse $\approx 6 \cdot 10^{6}$. In order to get a mean photon number for the signal state of $\mu = 0.5$, which is an optimum mean number for distances of interest [42], the VOA has to introduce an optical attenuation of the order of $70$dB.

The chosen FPS wavelength ($850$ nm) is optimum for free space operation considering attenuation (due to scattering, absorption and diffraction) and single-photon detector's quantum efficiency [98].

## 2.4 FPGA signal drivers

A proper electronic control of the different intensities and polarization states generated is fundamental in order to achieve a low QBER. The signal driver designed of the AM is able to output 3Vpp and the PM driver 6Vpp on high impedance of the oscilloscope. The synchronization and setting of the different optical components of the source was implemented by an automatic control which is split into two working operations. The control system first synchronizes and calibrates the driving signals timings and amplitudes to the AM and PM. Secondly, it uses the retrieved driving voltages to produce the required intensity and polarization states for the BB84+decoy protocol.

## 2.5 Relevant QKD parameters measurements

Figure 2.8 (a) shows the train of optical pulses generated by the laser diode when driven by electrical pulses of 1 ns at 100 MHz. The resulting optical pulse duration is about 400 ps. Since the obtained CW train of optical pulses are all generated in the same way, they can be assumed to be indistinguishable thus having no side-channel information. Furthermore, the short optical pulse duration of 400 ps (small duty cycle) has the advantage to increase the signal to noise ratio since the measurement window (detection time) in the receiver can be reduced. The DFB laser diode is driven in direct modulation with a strong RF driving signal with 24mA DC bias current, far below threshold 36mA, thus producing highly similar optical pulses and jitter as low as 100ps, rise time 65ps and fall time 129ps, as shown in Figure 2.8 (b). Furthermore, the optical pulse bandwidth is small enough to enter the acceptance bandwidth of the subsequent polarization modulator.

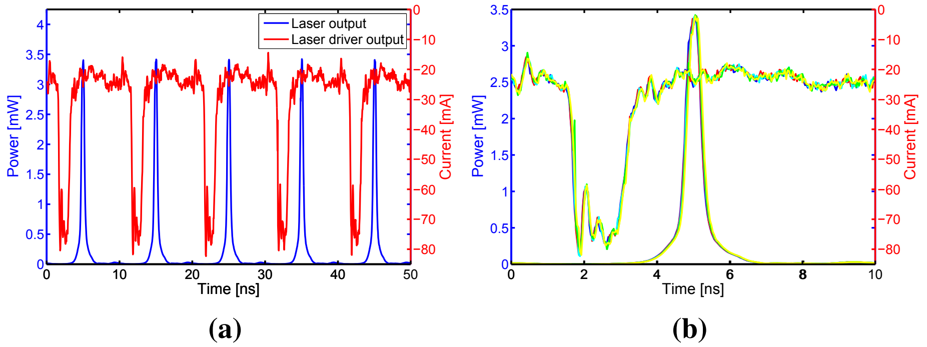
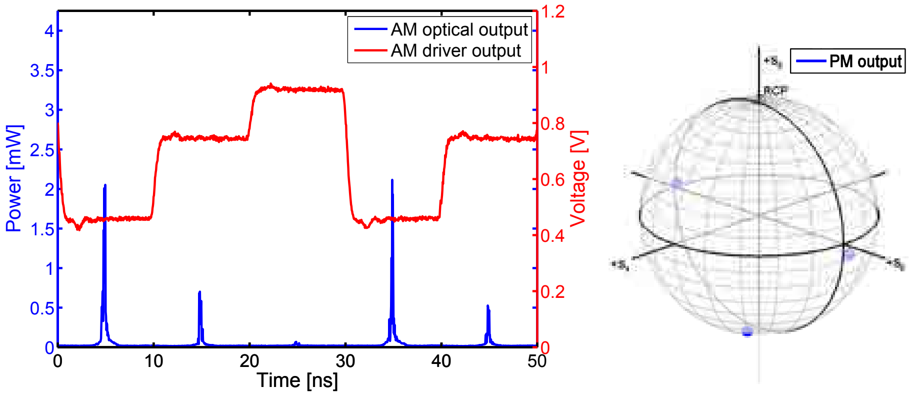


Figure 2.8: Laser diode output and laser driver output results. (a) Generated CW train of optical pulses at 100 MHz experimental results. (b) Time distribution of five pulses from the laser diode and the laser driver.

Figure 2.9 (a) shows the three different intensity optical pulses generated after the AM. The attenuations for the medium and low level of intensity pulses are about 4.65 dB and 14.76 dB, with respect to the high intensity pulse. While Figure 2.9 (b) shows the four polarization states generated after the PM, as measured with a terminating rotating waveplate polarimeter. The RF modulating signal is driven at 100 MHz, in this way, chirp produced at the pulse edges of the RF driving voltage is avoided and intensity and polarization indistinguishability is obtained.



(a)

(b)

Figure 2.9: Amplitude and polarization modulators experimental results. (a) Amplitude modulator experimental results. (b) Different polarization states are generated (shown on the Poincare sphere), in particular it is shown four polarization states: +45°, −45°, right-handed circular and left-handed circular; sufficient to implement a BB84 protocol.

Table 2.3 summarizes the characteristics of the driving RF and corresponding optical pulses for the three levels of intensity, suitable for a decoy-state protocol. The modulator ”ON” window has a duration of at least 5 ns, much larger than that of the optical pulse. Therefore, only the amplitude of the optical pulse changes, while the temporal and spectral shape remain unaltered. In addition low driving voltages are needed, making the design suitable for electronic integration with low electrical power consumption drivers.

Table 2.4 summarizes the RF voltages driving the PM generating the

| Pulse | AM driver RF signal [mV] | Optical attenuation [dB] |
|---|---|---|
| High intensity level | $460$ | $0$ (reference) |
| Medium intensity level | $745$ | $4.65$ |
| Low intensity level | $920$ | $14.76$ |

Table 2.3: Relevant parameters of three generated pulse intensity levels with the amplitude modulator. The RF driving voltages needed are below $1$ V, which are suitable to be integrated.

| Polarization | PM driver RF signal [V] | QBER |
|---|---|---|
| $+45°$ | $0$ | $10.66\%$ |
| $-45°$ | $1.56$ | $10.04\%$ |
| Right-handed circular | $0.81$ | $10.65\%$ |
| Left-handed circular | $-0.76$ | $10.10\%$ |

Table 2.4: Relevant parameters of four polarization states generated with the polarization modulator. Again, the RF driving voltages needed are low (below $1.5$ V), which are suitable to be integrated. The obtained QBER is just sufficient for QKD protocols, but it can be further improved using PMD compensation.

four orthogonal states. In the same table, QBER values for the four different polarization states are given. The QBER values obtained, without PMD compensation, are just sufficient for QKD protocols, but it can be further improved using PMD compensation. As for the AM case, low driving voltages are needed, suitable for integration with low power consumption and inexpensive electronics.

## 2.6 Summary

Starting from commercially available and space-qualifiable components, it is possible to build an integrated transmitter capable of generating the several intensity and polarization states required for decoy-state QKD.

The experimental demonstration has been carried out at $850$ nm with $100$ MHz modulation rates. However, taking into consideration that the modulators bandwidth can go well beyond $10$ GHz and operate also at other wavelengths (e.g. $1550$ nm), the source can be easily scalable to higher bit rates, the upper limit being probably given by the laser diode itself, and other transmission systems (e.g. optical fibers).

# Chapter 3

# Semiconductor optical amplifiers based QKD source

Reliable and simple-operation photonic sources are of relevant interest for applications in harsh environments, such those encountered in Space. In this Chapter, a demonstrated faint pulse source based on semiconductor optical amplifiers is described in detail. The source is based on semiconductor optical amplifiers operating as switching devices with high extinction ratio to select the output polarization state. Furthermore, a complete analysis of the security of the source in terms of QKD is presented, based on calculations of the indistinguishability of the generated optical states. Finally, a QKD transmission measurement is presented, which clearly reflects the achieved performance of the source.

## 3.1 The compact faint pulse source

The integrated faint pulse source (FPS) [99] consists of space-qualified discrete components, shown in Fig. 3.1. A single semiconductor laser diode (LD) emits a continuous train of optical pulses at $100$ MHz, equally split to four outputs using three in-fiber single-mode $1x2$ couplers. Each fiber output is followed by an integrated semiconductor optical amplifier (SOA). The four bare fibers to the coupling tube are accurately positioned on a custom opto-mechanical mount to simultaneously achieve the correct launching to the polarizers substrate sheet as well as to introduce a desired 70 dB coupling-loss to work in the single-photon regime at the end of the output bare fiber. Each polarizer is accurately oriented to produce one of the four polarizations (0°, 90°,45°and −45°) required for BB84 protocol. Finally, the output fiber can be connected to the corresponding optical link interface (e.g. a telescope for free-space communication or optical fiber for terrestrial links).

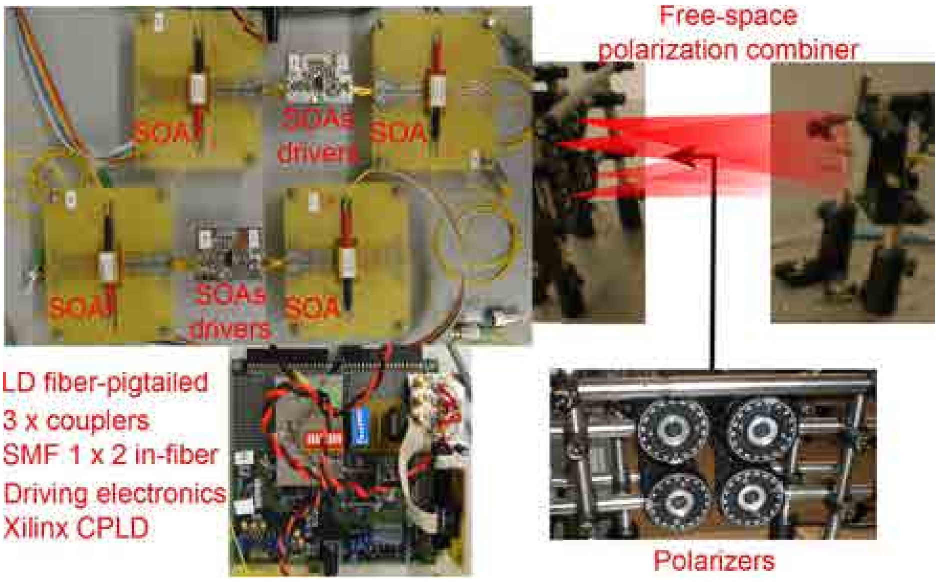


Figure 3.1: Scheme of the QKD source. (LD) denotes a laser diode, (C) a single-mode in-fiber $1x2$ coupler, (SOA) a semiconductor optical amplifier, (P) a free-space thin-film polarizer and (BF) a single-mode bare fiber.

The distributed feedback (DFB) LD source is directly modulated at 100 MHz by a train of electrical pulses of about 1 ns duration. Single-mode $1x2$ in-fiber couplers perform the task of passively splitting the continuous optical pulse train into four equal outputs, while sufficiently preserving the polarization state linearity generated by the LD, before entering the SOAs. Each SOA performs the double task of spatial switching and amplitude modulation; it selects a specific fiber output while, by changing the driving current, it generates the three intensity levels needed for the decoy state protocol. Note that the spatial switching among the four fiber outputs is then transformed in polarization modulation, according to the scheme described above, by going through different polarizing patterns of the polarizers substrate. In this way intensity and polarization modulation can be achieved with high extinction ratio (ER), without the need of using polarization maintaining fibers (PMFs) and PMF couplers or the complexity of having to maintain a specific input polarization state or high degree of polarization (DOP) along the whole optical assembly. Usually, the common parameter of interest for a SOA is the gain. However in this case the frequency response to an electrical signal is equally important, in particular for the time and spectral indistinguishability of the pulses with different polarizations and energy levels.

The main reason of using SOAs as active switching and intensity selection devices is their high ER ($>20$ dB) which is highly desirable when implementing 3-state decoy protocol. SOAs outperform other solutions such as Mach-Zehnder or electro-absorptive modulators which have lower ER when operated with optical pulses as input signal. Finally, thin-film polarizers achieve high degree-of-polarization (DOP) of the order of $99.68\%$, being a remarkable specification in order to ensure an adequate quantum bit error ratio and thus high efficiency of secure key generation rate. Polarization modulators can not achieve such a high DOP.

### 3.1.1 Source assembly

The DFB LD fiber-pigtail is connected to a $1x2$ coupler. At each output of the coupler a second $1x2$ coupler is connected, to have the output split into four similar outputs. Each of these outputs is connected to a fiber coupled SOA. At the fiber output of each SOA, an adjustable collimator is placed to interface correctly into the polarization combiner module. The four collimators are on kinematic mounts on a self-assembled mechanical structure. The distance from the mechanical structure to the output coupling bare fiber, forming the polarization combiner module, is around $80$ cm. All four collimators are placed within a circular area of $10$ cm diameter, in order to have the output beams within the input NA of the coupling SMF fiber (NA=$0.13$). Furthermore, following each output collimator a thin-film free-space polarizer is placed on a rotation mount in order to generate the four different polarizations ($0°$, $90°$, $+45°$and $-45°$).

The four SOAs are soldered to custom PCB boards for the RF driving signals. The control electronics are implemented using a Xilinx CPLD with analog output drivers, SMA connected close to the SOA pins in order to avoid relevant effects of impedance matching (less than $5$cm). Notice that a simple solution for impedance matching is not possible because the SOA presents an equivalent input impedance similar to a diode, thus of around $3\Omega$ in parallel with a $2$ pF capacitor; and the driving signals have an electrical bandwidth of $50$ MHz (from DC to $50$ MHz first harmonic).

A continuous periodic sequence, driving the four SOAs, is used to set the intensity level of a single SOA while the other three SOAs remain in the OFF state. The sequence is periodic as shown in Table 3.1.1 to facilitate the synchronization identification at the receiver. Obviously, in a real implementation of a QKD transmission the sequence has to be totally random and secure. Moreover, the three intensity levels correspond to optimal values reported in [42]: a high intensity level state which is set to produce $1/2$ average photon per pulse by adjusting the coupling efficiency to the output bare fiber; then a second intensity level is set to produce $1/8$ average photon per pulse and the third level is set as nearly vacuum (the SOA is switched OFF).

The sequence contains programmed symbols. A symbol is considered as a pair SOA and intensity (SOAx,Intensity), where each SOA corresponds to the generation of a particular polarization state. The sequence is repeated infinitely without dead times, outputting the signaling to the SOA drivers through a data bus at $100$ MHz. The sequence contains $12$ symbols, all possibilities in a $3$-state decoy BB84 protocol: (SOA1,low), (SOA2,medium), (SOA3,high), (SOA4,low), (SOA1,medium), (SOA2,high), (SOA3,low), (SOA4,medium), (SOA1,high), (SOA2,low), (SOA3,medium) and (SOA4,high).

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SOA/Polarization | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Intensity | 3 | 2 | 1 | 3 | 2 | 1 | 3 | 2 | 1 | 3 | 2 | 1 |

Table 3.1: 12-symbols periodic sequence stored in the Xilinx CPLD board. A symbol is considered as a pair SOA and intensity, where each SOA corresponds to the generation of a particular polarization state. The sequence is repeated infinitely without dead times, outputting the signaling to the SOA drivers through a data bus at $100$ MHz.

## 3.2 Source indistinguishability

The goal of QKD is to allow distant parties to securely share a common key in the presence of an eavesdropper. Therefore, it is important to demonstrate a system to generate pulses that differ only in polarization and intensity, considering a decoy state BB84 protocol, while being indistinguishable in the other degrees of freedom. Potential side-channel leakage could come from other degrees of freedom that characterize the quantum state of photons, such as arrival time, optical frequency, and spatial mode. Hence, in security applications, it is mandatory to estimate the side-channel information leaked to adjust the degree of privacy amplification to implement at the reconciliation step.

The proposed FPS ensures a high degree of indistinguishability among the different intensity and polarization pulses. Also, it ensures phase incoherence of consecutive generated states. Side-channel information allows an eavesdropper to gain knowledge about the key without introducing errors. A quantitative measure of the amount of information, directly accessible by a single, immediate measurement on one pulse, is the mutual information on the spatial, temporal and spectral shapes.

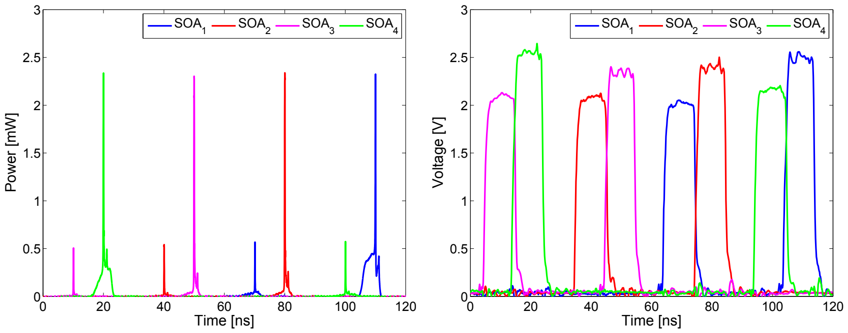
Due to issues of ensuring simultaneous switching (temporal information), LD manufacturing (spectral information) differences, a single LD outperforms the achievable security of the qubits sent by the source compared to using more than one LD. Furthermore, using a DFB LD generates short optical pulses close to transform limited pulses which ensures the correct functionality and minimum additional distortion of any subsequent optical devices and components. The time duration and spectral bandwidth product of the generated pulses is $0.56$, very close to the theoretical value for transform limited Gaussian pulses ($0.44$). In this way, phase incoherence of consecutive generated optical pulses, which otherwise would be detrimental for the link security [44], is achieved.

### 3.2.1 Measurements on indistinguishability

A $8$ GHz amplified photodiode and a $4$ MHz resolution Fabry-Perot interferometer were used for the temporal and spectral measurements on indistinguishability, respectively. Figure 3.2 shows the generated optical intensity states required to implement the decoy state protocol, for the four different SOAs, as well as the driving signals, loaded with $50\Omega$ for monitoring purposes.

The assembled analog drivers for the SOAs allow to manually set the DC bias current and the modulation current for each of the three intensity levels, independently for each SOA. Both the DC bias current and modulation currents should be programmable: DC current bias between $15$ mA - $35$ mA and modulation currents between $0$ mA - $70$ mA. Note that the driving currents were adjusted independently such that the peak optical intensities are similar for the different SOAs, shown in Fig. 3.2(b). It is clear that the optical pulses from the SOAs have amplified spontaneous emission (ASE) noise reducing the indistinguishability of the different states, seen at the bottom part of the optical pulses shown in Fig. 3.2(a). ASE has a larger bandwidth than the signal, thus ASE can be mitigated by using proper filters and/or selection of SOAs. In fact, SOAs $2$ and $3$ produce nearly identical pulses without the use of any filter. Figure 3.3 shows the generated optical pulses reducing the ASE from each SOA filtering with a $3$ nm interference filter.

Figure 3.4 shows the temporal and spectral shapes of pulses with same intensity level and four different polarization states, filtered ASE, where an offset has been introduced in the vertical axis only for visualization



**(a)** Optical output. **(b)** Driver output.

Figure 3.2: (a) Generated optical pulses, as required for the implementation of the decoy state BB84 protocol. Note that the driving currents are such that the peak optical intensities from the four SOAs are similar, although ASE is present which reduces the degree of indistinguishability. (b) Driving signals (monitored on an oscilloscope with $50\Omega$ input impedance). The sequence of the driving signals follow the periodic sequence stored in the CPLD electronic controller.

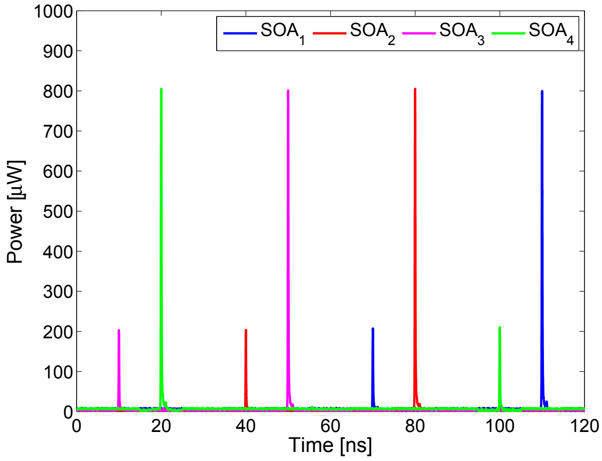


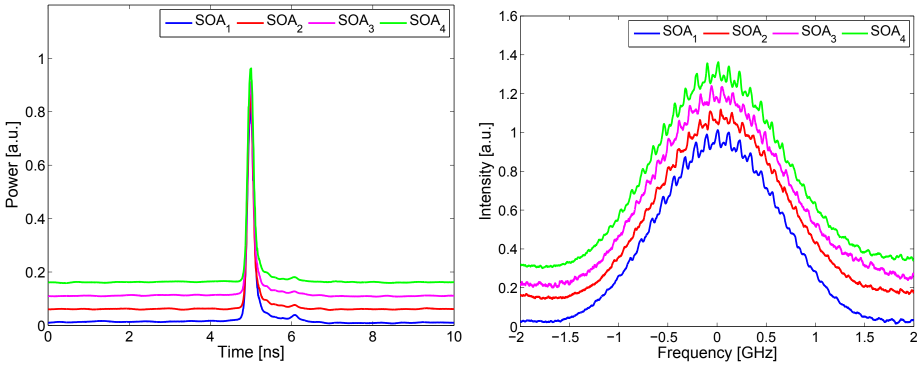
Figure 3.3: Generated optical pulses after extensively removing ASE using a 3nm interference filter with central peak wavelength of $852$ nm. Hence, producing nearly identical directly increases the degree of indistinguishability of the different optical states.

purposes otherwise the pulses would highly overlap in intensity.

The modulator "ON" window has duration of at least $5$ ns, much larger than that of the optical pulse. Therefore, only the amplitude of the optical pulse changes, while the temporal and spectral shapes remain unaltered. As expected, Fig. 3.4 shows the high degree of similarity of the pulses indicating minimal pulse distortion due to the SOAs. The mutual information computed is commented below:

- Spatial: The coupling output fiber also serves as a spatial filter, removing higher order modes. Because of the short length of the output SMF fiber (few centimeters) there might be still information transmitted by the fiber cladding. However this information leakage $I(S:B)$ would be of the order of $10^{-5}$ bits per pulse.

- Spectral: The mutual information between the bit value $B$ and the spectra $F$ is $I(F:B) = 1.75 \cdot 10^{-3}$ bits per pulse.



**(a)** Temporal profiles.

**(b)** Spectral profiles.

Figure 3.4: Temporal (a) and spectral (b) profiles for pulses with same intensity level (high) and four different polarization states, where an offset has been introduced in the vertical axis only for visualization purposes. As expected, these show a high degree of similarity, indicating minimal distortion of the pulses.

- Temporal: The mutual information between the bit value $B$ and the temporal shape $T$ is $I(T : B) = 1.92 \cdot 10^{-3}$ bits per pulse, when removing the ASE. If the ASE is not removed, considering the generated optical pulses from the four particular SOAs available, the mutual information computes to $I(T : B) = 7.25 \cdot 10^{-2}$ bits per pulse, mainly because of high levels of ASE in SOAs 1 and 4. If SOAs were pre-selected to have low ASE the $I(T : B)$ could achieve the $10^{-3}$ bits per pulse order.

The level of indistinguishability is directly reflected on the amount of secure key rate (SKR) that has to be removed in the privacy amplification step, in order to ensure security. The amount of bits to be removed when filtering with interference filters ($10^{-3}$ bits per pulse) can be achieved without using an interference filter but pre-selecting four SOAs with similar low ASE values. Considering the above values for $I(S : B)$, $I(F : B)$ and $I(T : B)$ the according information leakage is small compared to the information leakage indicated by the QBER of the contribution of pulses with more than one photon.

## 3.3 QKD system performance

A consistent method to determine the performance of a source is to implement a measurement of a QKD transmission. Mainly, the system performance is determined by the QBER, regarded that the detection subsystem part has high fidelity performance. However, it has to be taken into account that such a measurement does not reflect security issues, side-channel information leakage, that could reduce the effective key generation rate.

### 3.3.1 Synchronization electronics

A central electronic system, shown in Fig. 3.5, provides synchronized signals to the transmitter (Alice) and receiver (Bob). Synchronization entails that all signals are generated from the same central clock or completely synchronized clocks, which results with no relative frequency drifts between signals. The required signals are: clock, (SOA,intensity) data bus, $10$ MHz reference and repeating re-synchronization initial signal. The clock indicates the pulse repetition frequency to modulate the LD. At the same rate at least four bits are required to select which of the SOA and which of the three intensities through the data bus (SOA,intensity). It is required to have the capability to program a time delay between the clock and (SOA,intensity) selection with minimum resolution of $1$ ns and a dynamic range of $10$ ns. The central system also provides a synchronized copy of the clock at $10$ MHz (sinusoidal to drive an AC coupled $1$ K$\Omega$ termination with $1$ Vpp) and generates a repeating re-synchronization initial pulse signal where a rising edge (matched to $50\Omega$ higher than $500$ mV, better $2$ V) is generated every $99072$ symbols when working at a clock frequency of $100$ MHz (ideally this factor should be programmable). The re-synchronization signal produces a sharp rising edge (below $1$ ns) with pulse width of $50$ ns - $150$ ns at the start of the sequence and is repeated every specified number of symbols. The rise time jitter for the synchronization signal has to be smaller than $1$ ns.

### 3.3.2 Measurement statistics

In QKD systems, the performance parameter of relevance is the QBER. In order to correctly estimate the achieved QBER performing measurements, some statistics considerations have to be taken into account. QBER is the ratio between erroneous detections $e$ and total detections $N$, sum of good detections $N_c$ and $e$, only considering sifted qubits. In a correctly performing system a sufficiently good QBER and low dark count rate (noise) can be expected. In this situation of interest the approximation $N_c >> e$ is valid and $N \approx N_c$. For convenience, QBER can be expressed in the natural logarithm as QBER$_{ln} = \ln e - \ln N_c$. Then, the variance is

$$\sigma^2_{\text{QBER}_{ln}} = \left(\frac{\partial \text{QBER}_{ln}}{\partial e}\right)^2 \sigma_e^2 + \left(\frac{\partial \text{QBER}_{ln}}{\partial N_c}\right)^2 \sigma^2_{N_c} \tag{3.1}$$

where $\sigma_e^2$ and $\sigma_{N_c}^2$ are the variances of $e$ and $N_c$, respectively. The partial derivatives are

$$\frac{\partial \text{QBER}_{ln}}{\partial e} = \frac{1}{e} \tag{3.2}$$

$$\frac{\partial \text{QBER}_{ln}}{\partial N_c} = \frac{-1}{N_c} \tag{3.3}$$

Photon counting statistics considering Poissonian states obey $\sigma_n^2 = n$. Substituting into (Eq. 3.1), considering $N_c >> e$, $\sigma^2_{\text{QBER}_{ln}} \approx 1/e$ and the standard deviation $\Delta\text{QBER}_{ln} \approx 1/\sqrt{e}$. Expressed in decibels units $\Delta\text{QBER}_{dB} = 2(10/\ln 10)\Delta\text{QBER}_{ln}$.

In particular, considering $20$ dB QBER with an uncertainty of $1$ dB requires around $2000$ sifted photons. This only includes sifted qubits, but raw qubits are detected which are in general twice the number of sifted ones, doubling the required number of detected qubits to $4000$. Furthermore, four states are monitored (e.g. polarization states) in BB84, quadrupling the number of required total detections per channel. Hence, around $16000$ measurements would be required for a good estimation of the QBER using detected qubits evaluating four polarization states.

### 3.3.3 QKD parameters measurement

Figure 3.5 shows the setup used for the decoy state BB84 transmission measurement. The output bare fiber was connected to a free-space collimator pointing to the polarization-sensitive detection module, a.k.a. “Bob module” commonly used for polarization-encoded QKD. The polarization detection fidelity is defined as the ratio between erroneous detected polarization states to total detected polarization states. Fidelity defines the capability to correctly resolve the received polarization states. In particular, the assembled receiver module used in the experiment has $7.9 \times 10^{-3}$ fidelity. Alice’s and Bob’s time references were synchronized using a classical channel providing a $10$ MHz clock signal. The detections from the single-photon avalanche detectors (SAPD) were recorded by a timetagging unit and then transferred to a computer to derive the relevant parameters (e.g. lower bound secure key rate (LBSKR), raw key rate (RKR) and quantum bit error ratio (QBER)). The parameters of interest were extrapolated using enough accumulated detections in a burst mode operation, which for high RKR it accounted for about 100 ms while for the lowest RKR it accounted for 16.6 minutes. The timetagging unit allows 10 Mcps transmission to the computer, by direct memory access (DMA), and also it has a timestamp resolution of 78.125 ps. Accounting for 500 ps jitter of SAPD (Perkin Elmer SPCM-AQ4C), 100 ps jitter and 400 ps of the width of the generated optical pulses, a 1 ns time window was implemented by software, allowing to reduce the background noise.

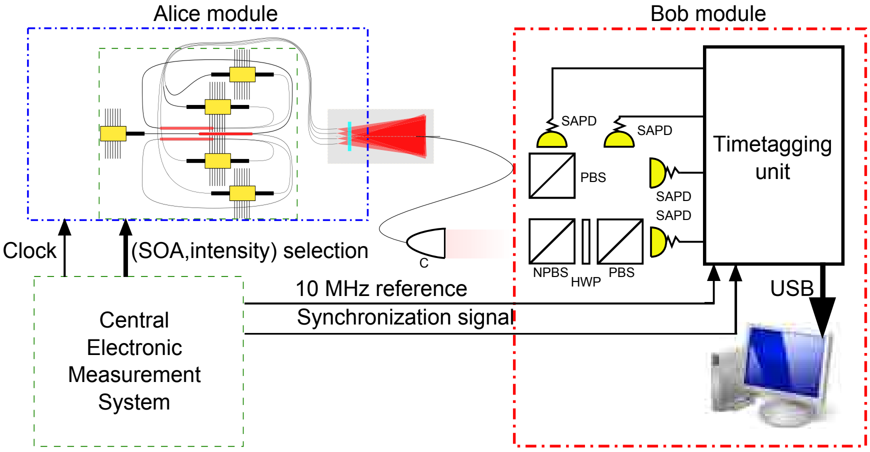


Figure 3.5: Scheme of the QKD measurement setup. Alice module is composed of the FPS also providing a common clock signal of 10 MHz in order to synchronize Alice and Bob modules. (C) denotes a fiber to free-space collimator, (NDF) a neutral density filter, (NPBS) a non-polarizing beamsplitter, (HWP) a half-wave plate, (PBS) a polarizing beamsplitter and (SAPD) a single-photon detector.

The free-space link was emulated in the laboratory by placing different neutral density attenuators along the propagation path from Alice (the source) to Bob (the receiver). Then rates and performances of the QKD decoy state BB84 protocol were measured using the presented source. In the implementation of the BB84 protocol, only single-photon pulses contribute to the secure key, while in the 3-state decoy state protocol the full range of intensities should be considered. All but privacy amplification was implemented, were the lower bound for the secure key generation rate can be obtained as demonstrated in [37, 38].

Figure 3.6 shows the detected RKR and QBER, and the resulting LBSKR, for different link attenuations. In the transmission measurement the detectors' efficiency was set to $50\%$, $2$ dB were accounted for losses due to the transmitting and receiving optical setup with a background yield of $5.58 \times 10^{-4}$. The background yield $Y_0$ includes the detectors' dark count and other background contributions from stray light [42] and is the major cause for the drop in secure key rate at large distances. As expected, for signal rates well above the noise floor the RKR decreases exponentially as the attenuation increases, so does the LBSKR. When the signal rate decreases the noise starts to dominate, so the QBER increases rapidly as well as the LBSKR, until the QBER is $> 0.11$ when the LBSKR drops completely to zero. In particular, results for the emulated decoy state BB$84$ protocol transmission, for a particular attenuation of $6$ dB, are shown in Table $3.3.3$. Achieved LBSKR of $3.64$ Mbps with a QBER as low as $1.14 \times 10^{-2}$ for an attenuation of $6$ dB while the achieved LBSKR became $187$ bps for an attenuation as high as $35$ dB.

## 3.4 Summary

It has been shown that a single photon source based on an attenuated laser diode for QKD applications can be built based on a novel scheme including semiconductor optical amplifiers. The source is capable of generating pulses of different polarization distributed over four states and three intensity levels required for decoy state BB84 protocol. A lower bound secure key rate of $3.64$ Mbps with a quantum bit error ratio as low as $1.14 \times 10^{-2}$ for an attenuation of $6$ dB.

Given the relatively low driving voltages of the SOAs, the laser diode and the other integrated optical components, the proposed transmitter is potentially low power consumption, highly integrable and stable. The ex-

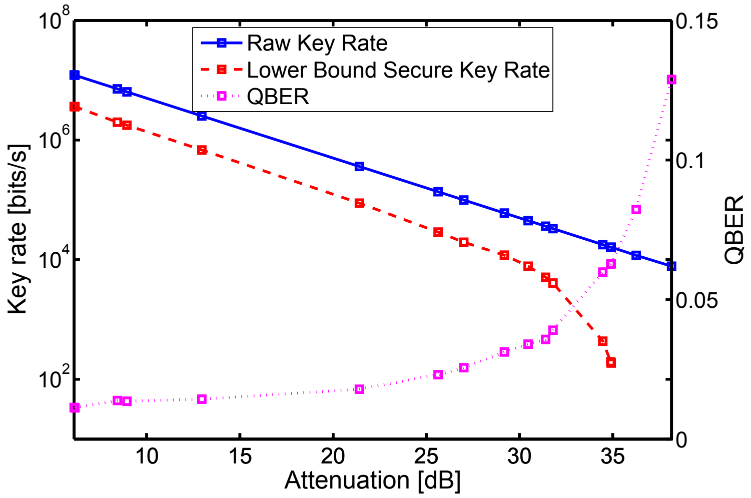


Figure 3.6: QKD BB84 implementing decoy states transmission results. Raw Key Rate (blue solid line), Lower Bound Secure Key Rate (red dashed line) and QBER (magenta dotted line). The detectors' efficiency was set to $50\%$, background yield $5.58 \times 10^{-4}$, 2 dB were accounted for losses due to the transmitting and receiving optical systems.

| Parameter | Value | Parameter | Value |
|---|---|---|---|
| Attenuation | 6 dB | $Q_\mu$ | $1.18 \times 10^{-1}$ |
| $\mu$ | $0.5$ | $Q_{v_1}$ | $1.8 \times 10^{-2}$ |
| $\nu_1$ | $6.6 \times 10^{-2}$ | $Q_{v_2}$ | $3 \times 10^{-3}$ |
| $\nu_2$ | $2 \times 10^{-3}$ | $e_\mu$ | $1.14 \times 10^{-2}$ |
| $R_{secure}$ | $3.64$ Mbps | $f\left(E_\mu\right)$ | $1.16$ |

Table 3.2: Summary of the QKD results for a BB84 transmission, implementing the decoy state protocol. The obtained values are for a $6$ dB attenuation, where $\mu$, $\nu_1$ and $\nu_2$ are the signal, decoy 1 and decoy 2 (ideally vacuum) states. The computed values are the gains for the signal $Q_\mu$, decoy 1 $Q_{\nu_1}$, decoy 2 $Q_{\nu_2}$ states and the QBER for the signal states $e_\mu$. Finally the lower bound of the secure key rate $R_{secure}$, for the presented source, is $3.64$ Mbps with a QBER as low as $1.14 \times 10^{-2}$ while a $R_{secure}$ of $187$ bps for an attenuation as high as $35$ dB.

perimental demonstration has been carried out at $850$ nm, for the implementation in free-space links, with $100$ MHz generation rates. However, taking into consideration that the SOA's bandwidth can go well beyond $10$ GHz and operate also at other wavelengths (e.g. $1310$ nm and $1550$ nm for fiber transmission), the source is scalable to higher bit rates, the upper limit probably being set by the laser diode itself.

# Chapter 4

# Pulsed semiconductor laser based random number generator

Random numbers support critical activities in advanced economies, including secure communications, numerical simulation and quantitative finance. In this Chapter, a proposed random number generator is described and the physics foundations which it is based on are analyzed. It extracts random bits from vacuum using optical independent amplification. Finally, a statistical test of the randomness is performed to qualify the device utilizing standard validation methods.

## 4.1 True random number generators

Although any quantum measurement provides some randomness, a practical source must be simultaneously fast, inexpensive, and robust. For this purpose, fluctuations of the quantum vacuum are very attractive because the electric field amplitude is a continuous quantity, a single measurement can yield many true random bits. True vacuum is also perfectly white, uncorrelated, and broadband; the quantum field renews its random value arbitrarily quickly. Guaranteeing true vacuum is far from trivial, however; any scattered light will contribute a non-random component to the field measurement. Homodyne detection based schemes [62, 63, 73] guarantee that the signals originate in vacuum noise. The method relies on the vacuum noise fluctuations as homodyne detection schemes, and at the same time achieves high bandwidth, because the requirement for shot-noise-limited detection is removed.

Relative to demonstrated methods for RNG and achieved speeds, it is proposed a device highly integrated, using commercially available components, but also has other advantages [100]. In particular, the strong current modulation, well above and below threshold, ensures true randomness from vacuum. This active gain control allows a single device to have both a short coherence time, for rapid extraction of uncorrelated random bits, and a high signal level. In this way, standard photodiodes can be used. Furthermore, due to the high power of the signal pulses, the signal-to-noise ratio (SNR) is high. Hence, several random bits per detection event can be generated, limited by the classical noise of the measurement equipment. It is the first time that current gain modulation is used in a QRNG.

## 4.2 Device operation

A distributed feedback (DFB) laser diode (LD) is used as the oscillator, providing single-mode operation and high modulation bandwidth. The DFB LD is directly modulated at around $100$ MHz by a train of $\sim 1$ ns electrical pulses. A polarization-maintaining, all-fiber unbalanced Mach-Zehnder interferometer (MZI) with a relative delay of $t_{\text{lp}} \approx 10$ ns provides stable single-mode operation of the interferometer, as shown in Fig. $4.1$.

The LD is set with $24$ mA DC bias current, far below its threshold value of $36$ mA. Phase-randomized coherent optical pulses of $400$ ps time width and $3.5$ mW peak power are produced. A $30$ dB optical isolator (OI) is placed just after the LD to avoid back reflections into the oscillator cavity. Then, the linearly polarized optical pulses are split in power using a polarization maintaining coupler (PMC) with a fixed coupling ratio. In one of the output ports of the PMC, a $2$ m polarization maintaining

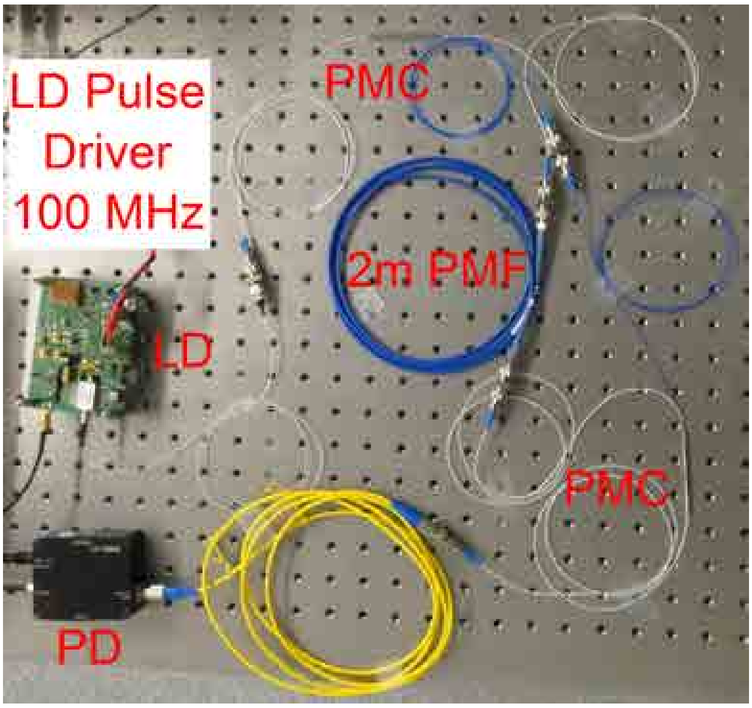


Figure 4.1: (LD Pulse Driver) denotes the electrical pulse generator to directly modulate the laser, (LD) laser diode, (PMF) polarization maintaining fiber, (PMC) polarization maintaining coupler, a temporal delay in one arm of the interferometer is introduced by a 2 m long PMF and (PD) is a fast photodiode.

fiber (PMF) patchcord is connected, which corresponds approximately to the equivalent length of the pulse repetition frequency (PRF). Both arms of the interferometer are connected to a second PMC where the interference between pulses takes place. The overall interferometer setup, at the output, has power coupling ratios of $T_{12}^2 \approx 49.8\%$ and $R_{12}^2 \approx 40.3\%$, and polarization isolation of $23.98$ dB and $25.23$ dB for the two arms. At one of the output ports of the interferometer, a $150$ MHz photodiode is connected to collect the different interfering optical pulses which are processed by a fast oscilloscope. The oscilloscope is operated with a $200$ MHz bandwidth for the input channel, triggered by the system clock reference.

The path delay difference of the interferometer can be adjusted to temporally overlap subsequent pulses. On the one hand, the time delay between interfering pulses can be controlled by fine tunning the propagation properties of the long arm of the interferometer to change the parameter $\phi_{loop}$. For instance, by changing the temperature of the optical fiber one can produce a refractive index change and also thermal expansion of a wavelength for a $0.03$°C temperature change, corresponding to $4.25$ fs. Albeit, the time adjustment range achievable is limited compared to the pulse repetition period $\sim 10$ ns. On the other hand, the interferometer can be temperature stabilized to within $0.01$°C to keep the parameter $\phi_{loop}$ fix and the PRF changed to increase or decrease the time between successive pulses. The time delay difference between both arms of the MZI is related to the PRF as $\Delta t = 1/\text{PRF}$, which allows an accurate and larger time adjustment range. The path delay difference of the interferometer was adjusted by setting the PRF at $97.6$ MHz.

## 4.3 Laser physics analysis

In semiconductor lasers the laser dynamics depends sensitively on the charge carrier densities, set by the DC current bias, which provide the optical gain [101]. The noise due to spontaneous emission is the dominant noise source in laser diodes (LD) which presents thermal light characteristics. Since the spontaneous emission noise extends over a large wavelength range, it can be considered as a white noise source with a delta-function autocorrelation.

The average spontaneous emission rate $R_{sp}$, is the number of spontaneously generated photons per unit of time within the considered oscillating laser mode. Not considering structural factors of the LD cavity which are not numerically relevant, $R_{sp}$ is approximated by $R_{sp} \approx g n_{sp} c_0/n = 10^{12} s^{-1}$, $g \approx 100$ cm$^{-1}$ is the gain of the fundamental mode and $n_{sp} \approx 1.5...2.5$ is the inversion factor. While, $S$ is the number of photons in the cavity, which derives from the laser equation rates. For a single-facet LD, given an output power $P$, $S$ is given by

$$S = \frac{nP}{h\nu c_0 \alpha_m} \tag{4.1}$$

where $h$ is the Planck's constant, $\nu$ is the optical center frequency, $n = 3.6$ is the refractive index of the guiding layer of the LD, $c_0$ is the speed of light in vacuum and $\alpha_m$ is the facet loss defined as

$$\alpha_m = \frac{1}{2nL} \ln\left(\frac{1}{R}\right) \tag{4.2}$$

where $L = 300\mu$m is the typical cavity length and $R = 30\%$ is the reflectivity of the exiting facet mirror.

The phase change $\Delta\phi_i$ due to a single spontaneous emission event alters $S$ from the steady-state value. When $S$ is altered Fig. 4.2, the LD undergoes damped relaxation oscillations, which return $S$ to a steady-state [102].The principle of superposition holds, thus the total phase change for many spontaneous emission events overlapping in time is the sum of the individual phase changes.

If the average spontaneous emission rate is $R_{sp}$, the average phase change is

$$\langle \Delta\phi \rangle = -\frac{\alpha R_{sp} t}{2S} \tag{4.3}$$

where $t$ is time and $(1+\alpha^2)$ is the linewidth enhancement factor, typically for semiconductor laser diodes $\alpha \approx 4.6 - 6.2$. The overall average spontaneous emission causes a field intensity change equivalent to adding one

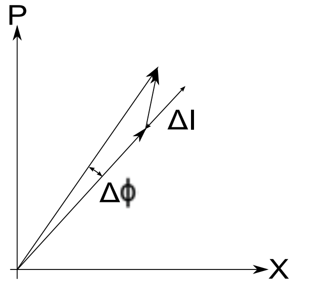


Figure 4.2: Phase $\Delta\phi$ and optical intensity $\Delta I$ instantaneous changes of the optical field caused by a single spontaneous emission event. The intensity increases and the phase change has a random value.

photon to the mode. However, it produces a large change of the number of photons of several hundreds. Due to the random spontaneous emission events, the phase $\phi$ executes Brownian motion and has a Gaussian probability distribution, with a variance

$$\left\langle \Delta\phi^2 \right\rangle = \frac{\alpha R_{sp}(1+\alpha^2)t}{2S} \tag{4.4}$$

Considering operating the laser diode below threshold with a typical output power $P \approx 100\mu$W and a renewal time $t = 10$ns, the average phase change is $\langle\Delta\phi\rangle \approx -10$ rad and the variance is $\langle\Delta\phi^2\rangle \approx 50.68$ rad$^2$. These settings produce a phase variation which covers the whole $2\pi$ range.

It is desired to operate the laser below threshold to obtain large phase variations in a given time $t$. Then, it is convenient to amplify the optical field to a macroscopic value to allow high signal-to-noise ratio measurements. Electrical injected current into the laser produces a time transition-state with known associated time-scale dynamics. The relevant time-scale dynamics are given by the electronic relaxation rate $\Gamma_s$, the optical relaxation rate $\gamma_s$ and the resonant coupling frequency $\omega_r$. The desired time-scale dynamics are such that allow to generate an optical pulse by direct current modulation. A convenient generated pulse is the one that has reduced overshot and a short time width so that the laser can rapidly be taken below threshold again. The lower the DC bias current the more phase variation produced but the time-scale-dynamics become slower.

Figure 4.3 shows the train of optical pulses generated by the laser diode when driven by electrical pulses of $1$ ns at $100$ MHz repetition rate. The resulting optical pulse duration is about $400$ ps. The laser is biased using a DC current of $24$ mA, far below threshold $36$ mA, and it is directly modulated using a strong RF current of $50$ mA (peak value) so that the optical pulse is generated [97].

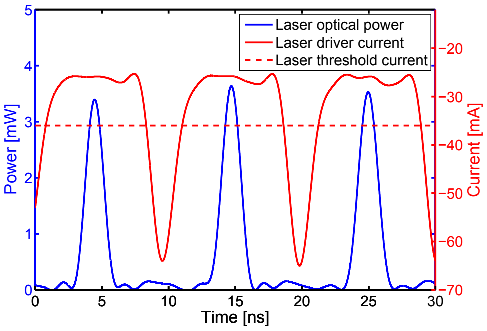


Figure 4.3: Laser diode output and laser driver output results. Laser driver output (upper curve, right axis) produces few-ns, negative-going pulses which drive the DFB laser briefly above threshold. The laser output (lower curve, left axis), shows pulses with $100$ MHz repetition rate and sub-ns duration.

The method operates on the field within a single mode of a semiconductor diode laser. The spontaneous emission behaves like thermal light, thus it has a Gaussian probability density distribution [97]. The LD acts as an amplifier for the spontaneous emission field which is also dependent on the existing cavity mode field. In turn, the spontaneous emission field has an impact both in the intensity noise and in the phase noise of the LD. The laser is first operated far below threshold, producing simultaneously strong attenuation of the cavity field and input of amplified spontaneous emission (ASE). This attenuates to a negligible level any prior coherence, while the ASE, itself a product of vacuum fluctuations, contributes a masking field with a true random phase. The laser is then briefly taken above threshold, to rapidly amplify the cavity field to a macroscopic level. When the laser is taken above threshold, the equilibrated field is amplified, limited by gain depletion [103], to produce observed output powers of $P \approx 3.5$ mW or $1.5 \times 10^7$ photons/ns. The amplification is electrically-pumped and thus phase-independent. Due to gain saturation, the resulting field has a predictable amplitude but a true random phase. The cycle is repeated, producing a stream of phase-randomized, nearly identical optical pulses. As shown in Fig. 4.1, interference of subsequent pulses converts the phase randomness into a stream of pulses with random energies, which is directly detected and digitized.

During the attenuation phase, the cavity field is described by the Langevin equation:

$$\frac{d}{dt}a = -i\omega a - \frac{1}{2}\gamma a + \Gamma, \tag{4.5}$$

where $a$ is the field operator for the mode, $\omega$ is its angular frequency, $\gamma$ is the (energy) decay rate and $\Gamma = \gamma^{1/2}a_{\rm res} + \Gamma_{\rm ASE}$ is a noise operator, with $a_{\rm res}$ a reservoir mode. The first term is from attenuation [104], and the second from ASE. $\gamma = \gamma_{\rm cav} + \gamma_{\rm mat}$ follows: The cavity contribution is $\gamma_{\rm cav} = -c_0/(2nL)\ln(R) = 5 \times 10^{10}$ s$^{-1}$, where $c_0$ is the speed of light in vacuum, $R$ is the out-coupler reflectivity, $n$ is the refractive index, and $L$m is the cavity length. The material contribution $\gamma_{\rm mat}$ ranges from $c\alpha/n \approx 10^{11}$ s$^{-1}$ at zero current to $\gamma_{\rm mat} = -\gamma_{\rm cav}$ at threshold. Here $\alpha \approx 10^4$cm$^{-1}$ is the intrinsic absorption of GaAs at $852$nm [105]. Interpolating, at $70\%$ threshold current, $\gamma \approx 10^{11}$ s$^{-1}$, or about $400$ dB/ns. This renders completely negligible any prior coherence in the cavity, and the remaining field is an equilibrium between ASE and attenuation. The phase of this field is a true quantum random variable, its value determined by ASE which is driven by vacuum fluctuations.

Considering the speed limits of this technique, even at a modulation rate of 10 GHz, i.e., an attenuation time of $\sim$ 50 ps, the attenuation is 20 dB. The field contribution remaining from the previous pulse is $6 \times 10^{-4}$ photons, or $\approx 10$ bits below the vacuum fluctuations. The physics of the process can thus support QRNG rates in excess of $100$ Gbps.

## 4.4 Characterization of the coherence of the laser pulses

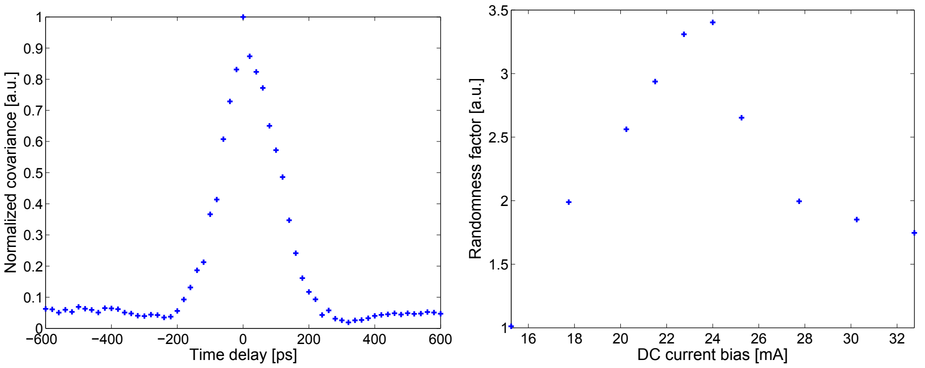
The interferometric setup allows to determine the first order coherence properties of the laser pulses, described by the correlation functions $G(\tau) \equiv \int dt \, \langle \, \hat{E}^{(-)}(t)\hat{E}^{(+)}(t+\tau) \, \rangle$, or its normalized version $g(\tau) \equiv G(\tau)/G(0)$. Here $\hat{E}^{(\pm)}$ are the positive- and negative-frequency parts of the emitted field $\hat{E}$ and integrals are taken over the duration of the pulse. The pulse energies $G(0)$ are narrowly distributed, and $g(t_{\mathrm{rep}})$ has near-unit magnitude and random phase, where $t_{\mathrm{rep}}$ corresponds to the time between successive pulses given by the PRF. Subsequent pulses have very similar envelopes and random phases $\phi$. The interferometer output is $\hat{E}_{\mathrm{out}}(t) = T_{12}\hat{E}(t) + R_{12}\hat{E}(t+t_{\mathrm{lp}})$ where $T_{12}, R_{12}$ indicate combined transmission and reflection coefficients through the two splitters. If the pulse energy in both arms of the interferometer is defined as $u_i \equiv R_{12}^2 G(0)$ and $v_{i+1} \equiv T_{12}^2 G(0)$, the energy at the output port of the interferometer, $u_i^{(\mathrm{out})} \equiv \int dt \, \langle \, \hat{E}_{\mathrm{out}}^{(-)}(t)\hat{E}_{\mathrm{out}}^{(+)}(t) \, \rangle_i$ is given by

$$u_i^{(\mathrm{out})} = u_i + v_{i+1} + 2|g(t_{\mathrm{lp}})|\sqrt{u_i v_{i+1}} \cos\left(\phi_i - \phi_{i+1} - \phi_{\mathrm{lp}}\right) \tag{4.6}$$

where $\phi_{\mathrm{lp}} = \omega t_{\mathrm{lp}}$ is the phase introduced by the delay loop.

First, the interferometer length and DC current working point are optimized to find the largest variance of interfered pulse energies, as shown in Fig. 4.4. Figure 4.4(a) shows the time difference adjustment tolerance with respect to the optimum, which strongly depends on the time width of the interfering pulses. In particular, for the generated optical pulses the tolerance is of around $200$ ps, equivalently around $2$ MHz detuning. Figure 4.4(b) shows the relative variance of interfered pulse energies. The largest variance is found for $24$ mA, which is below threshold $36$ mA.

The relevant statistics are measured as follows (data shown in Fig. 4.5(a)): narrow distributions of $u_i$ and $v_{i+1}$ are directly observed by block-

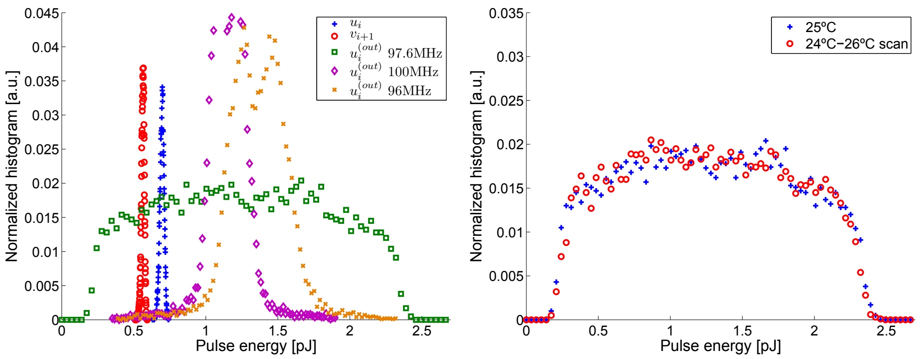


**(a)** Temporal overlapping adjustment.

**(b)** LD bias current optimum working point.

Figure 4.4: Adjustment of the parameters of the RNG. (a) Temporal overlapping adjustment with respect the optimum time delay difference. The time difference can be fine tuned by modifying the pulse repetition frequency. (b) LD bias current working point adjustment. Notice that the optimum value, $24$ mA is below threshold, $36$ mA.

ing one or the other path. Interference leads to a broadening of the observed distribution, with the broadest distribution corresponding to $t_{\text{rep}} = t_{\text{lp}}$. From the width of the $u_i^{(\text{out})}$ distribution and the mean values of $u_i, v_{i+1}$, the interference visibility is $|g(t_{\text{lp}})| \approx 90.22\%$. To demonstrate that the laser pulses are phase-uncorrelated, statistics are collected both for $\phi_{\text{lp}}$ fixed, and for $\phi_{\text{lp}}$ swept over several $\pi$, obtained by heating the fiber loop during acquisition. Results, shown in Fig. 4.5(b), are statistically identical, indicating the absence of phase relation between subsequent pulses.



**(a)** Input and output statistics.

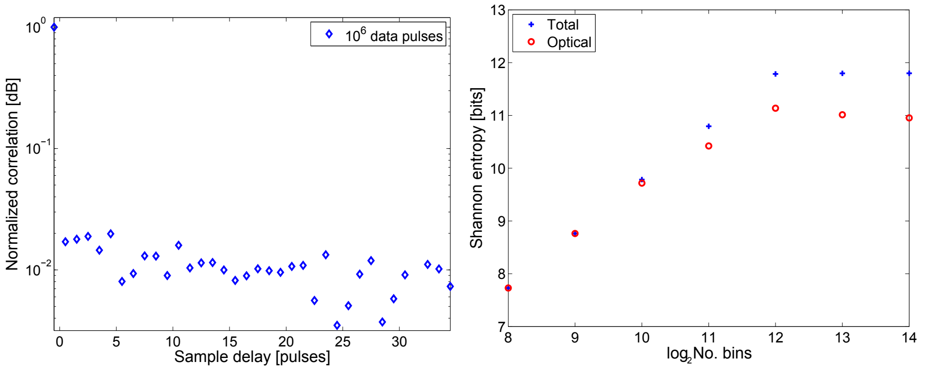
**(b)** Statistics for different temperature settings.

Figure 4.5: Inter-pulse interference measured by output energy distributions. (a) Distributions for: individual pulse energies $u_i$,$v_{i+1}$, interfering pulse energies $u_i^{(\text{out})}$ under different PRF and hence different $t_{\text{rep}}$. (b) Output pulse energy histogram for delay-loop temperatures of 25 °C (fixed), and 24 °C to 26 °C (scanned). Loop phase has no observable effect on the distribution, indicating statistical independence of the pulses' phases.

## 4.5 Statistical testing

The output of the photodiode was highpass filtered with a cutoff frequency of $40$ MHz and digitized using the waveform integration function of an oscilloscope with input bandwidth $200$ MHz, sampling speed of $2.5$ Gsps and a 12-bit analog-to-digital converter (ADC). The $10$ ns time range setting, compliant with the PRF, and sampling speed of the oscilloscope permits to acquire $25$ samples over a pulse. The oscilloscope translates the multiple samples per pulse to a single measurement. The nearly uniform distribution of observed energies permits the use of equally-sized encoding bins, and facilitates calibration. Records of $10^6$ output pulses were collected in order to characterize the statistical correlations of the acquired raw data and to determine the number of extractable random bits per pulse. The normalized correlation of successive samples as a function of sample delay of the raw data is computed as the modulo-N circular auto-correlation for finite length sequences and it is normalized to the maximum, shown in Fig. 4.6(a). The correlation of data samples follows a delta-function like behavior which indicates an uncorrelated sequence with low impact of drifts in the device. The quantum random bit content of the recorded signal is determined as follows: The pulse distribution of Fig. 4.5 is divided into $2^b$ equally-sized bins and the Shannon entropy is calculated. As shown in Fig. 4.6(b), the entropy increases linearly with $b$, up to the value $b = 12$, where it saturates to $11.8$ bits of entropy. The same procedure, applied to the detection noise, finds the classical noise entropy. Subtracting the noise entropy, the quantum optical noise contribution reaches a level of $11.1$ bits per pulse at $b = 12$. Multiple samples per pulse achieves larger accuracy when used together with higher resolution ADC. This allows to better bound the contribution of the classical noise and thus permits to extract more true random bits per pulse.

The observed classical noise, however random it may appear, could in principle be the result of a completely predictable process. Indeed, randomness tests (described below) detect patterns in the recorded classical noise. To completely remove these patterns, the entropy of the classical noise places an upper bound on the information it can contain. Then this



**(a)** Normalized correlation of raw data. **(b)** Total entropy of detected pulses and entropy of optical contribution

.

Figure 4.6: Measured correlation and entropy of acquired pulses. (a) Normalized correlation of successive samples as a function of sample delay of the raw data. The correlation data samples follows a delta-function like behavior indicating a random sequence. (b) Total entropy, calculated from the measured distribution. Distribution is divided into $2^b$ bins, from which the Shannon entropy is calculated. Optical contribution, up to $11.1$ bits per pulse, is found by subtracting entropy of the measured electronic noise.

quantity of information is removed, using cryptographic hash functions, from the combined quantum and classical noise [62]. Here, the Whirlpool hash function is used [75]; other standard randomness extractors could have also been employed [76, 77]. These cryptographic functions mix the input data bits, increasing the theoretically secure entropy per bit at the cost of losing output bits. The reduction factor of the hash function applied to the collected raw bits is $1.08$. As a result, the random bit generation rate of the current device accounts to $1.11$ Gbps.

All tests of randomness from TestU01 [80] have been performed. Considering the optical pulse data set, some test fail when applied to the raw data set, while they were successfully passed when applied to the hashed data set. Confirming that the hashing removes any remaining predictable behavior and increases the entropy per bit. Instead, the classical noise data set fails some tests both before and after hashing, using the same hashing factor.

## 4.6 Summary

In summary, high-bandwidth extraction of random bits from quantum vacuum fluctuations using optical amplification was demonstrated. The use of strong attenuation followed by amplification guarantees that the signal originates from quantum noise, and provides macroscopic signals compatible with the highest bandwidth detection. With commercially-available components, over $1$ Gbps true random number generation was demonstrated. The QRNG device is low in power consumption, is robust, and can be easily automated allowing it to have a long operational lifetime. Consideration of the laser physics indicates that rates above $10$ Gbps and even $100$ Gbps are possible. The high random number generation rate extends the practical applications of this method to erode the dominance of currently used classical RNG choices. The method can be applied to high speed secure communication, to the gambling industry and to cryptography.

# Chapter 5

# Free-space QKD system

Free-space QKD is a major research line in global quantum communication applications. In this Chapter, a free-space QKD system is presented and technical details described. First, an automatic operating faint pulse source is described, also consisting of a polarization control system suitable for free-space links. Second, a compact mechanical polarization receiver attached to a tracking receiving telescope was developed. Finally, requirements and procedures for QKD system data synchronization and processing is presented.

## 5.1 System overview

Free-space QKD attracts attention for global quantum communication because of its low-transmission loss, compared to fiber-transmission systems. Although, a major milestone in free-space QKD systems is the possibility to achieve successful transmission with moving targets, such as satellites. An intermediate milestone, which represents a major success in its own right, is the achievement of the conditions for polarization control along the space channel and the synchronization with adequate signal to noise ratio. The ultimate milestone is the demonstration of a QKD protocol in a satellite-to-ground downlink or ground-to-satellite uplink configuration.

All free-space QKD systems experimentally implemented involve links between static terminals. However, a mobile QKD system would be a significant step towards more realistic scenarios, like the transmission of secure data between vehicles, aircrafts and space-to-ground or intra-satellite quantum communication.

The different parts of a QKD system for mobile platforms, where the transmitter (Tx) is in motion with respect to a static receiver (Rx) are presented. The system is part of the EXTRA project, which aims to build a 1 km free-space quantum communication link, where the transmitter (Alice) is placed on a mobile platform and the receiver (Bob) is a fixed tracking telescope. The Tx is constituted by a faint pulse source, a feedback system for source and polarization calibration, and a pointing/tracking system using a galvanometric optical scanner (galvo) compensated in polarization. The Rx is based on a catadioptric telescope which is used to collect the photons emitted by the Tx and deliver them to a polarization analyzer module (Bob). Finally, synchronized data is processed to perform QKD reconciliation step.

## 5.2 Transmitter source

The source integrated into the transmitter system is based on $\text{LiNbO}_3$ modulators [83]. A computerized control for the calibration step for the amplitude modulator and polarization modulator would be desirable for the faint pulse source (FPS), in order to operate in the foreseen field test experiments. The developed automatic control is split into two working operations. First, the control system calibrates and sets the parameters of involved devices. Second, it generates the correct driving signals needed for the FPS source to implement a QKD transmission. In Table 5.1 the different characteristics of the parameters to be controlled for each active device conforming the source are described.

The source is based on an already proposed scheme, but a polarization controller (PC) and a calibration feedback loop were added, shown in Fig. 5.1. The optical output of the PC is collimated to 6mm $1/e^2$ diameter and

| Device | Parameters | Goal | Drifts | Time scale | Inputs |
|---|---|---|---|---|---|
| Laser diode | Optical pulse peak power. | Constant absolute optical pulse peak power for the cw train of optical pulses. | Absolute optical pulse peak power variation. | Months. | DC current bias and RF current pulses. |
| Amplitude modulator | DC bias voltage and RF driving voltages. | Constant absolute optical pulse peak power for the different intensity levels. | DC bias point and RF voltages for the different intensity levels. | Seconds. | DC voltage input and RF voltage input. |
| Polarization modulator | RF driving voltages. | Constant relative polarization states but absolute orthogonality of the states. | RF voltages for the different polarization states. | Seconds. | RF voltage input. |
| Polarization controller | Different stages' voltages. | Constant absolute position of the different polarization states on the Poincare sphere and pointing mirrors compensation. | TBD. | TBD and at least 1 kHz to compensate for the steering mirrors. | Digital voltage signal. |
| Steering mirrors | - | Pointing polarization compensation. | Minutes | 1 kHz. | Digital voltage signal. |

Table 5.1: Different devices' parameters to be controlled and associated drifts.

a $0.09$mrad divergence. The feedback loop consist on picking-off optical signal using a non-polarizing beamsplitter. The probe signal is fed into a polarizer followed by a photodiode to convert optical intensity into a voltage signal that can be processed by electronic hardware. Through the transmission branch of the non-polarization beamsplitter, the beam is attenuated to the single photon level with a calibrated neutral density filter.

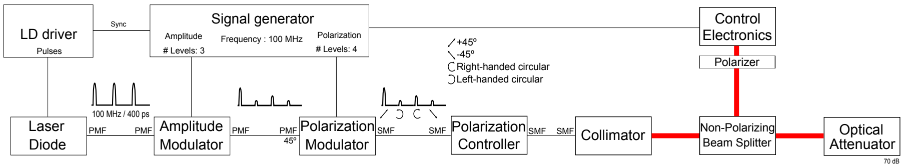


Figure 5.1: FPS source scheme. The source is based on an already proposed scheme, but a calibration feedback loop was added. The feedback loop consist on picking-off optical signal using a non-polarizing beamsplitter. The probe signal is fed into a polarizer followed by a photodiode to convert optical intensity into a voltage signal that can be processed by electronic hardware.

The calibration control consists in an integrator-probe signal configuration. It uses a low frequency probe signal which is coherently detected with a low speed photodiode and analog-to-digital converter (ADC) (accepts up to $2$ Vpp). The calibration algorithm feeds a $800$ Hz sinusoidal tone with adjustable amplitude, mounted on the value of an integrator, the gain of the integrator can be positive or negative. Higher tone frequencies are not desirable because they would introduce a non-negligible phase delay which would cause the algorithm of coherent detection to fail.

The optical input signal consists of a train of pulses at $100$ MHz modulated by the tone and integrator value, through either the AM or the PM. The optical power in the zero harmonic (DC carrier) is almost as high as that in the first $100$ MHz harmonic, because the optical pulses have around $10\%$ duty-cycle. Thus, it is convinient to only use the zero harmonic and filter out the higher harmonics (otherwise they would have to be demodulated down to DC). At the input of the ADC, before the single-ended to differential converter, a low pass filter DC-$1.9$MHz is placed to remove the signal modulated at the first harmonic that the photodiode is able to detect. Issues working at DC include a much higher noise, otherwise DC could be rejected and a RF power detector could be used to demodulate the first harmonic.

The calibration algorithm searches for the maximum and the minimum of the modulators' transfer functions. Once they have been retrieved a squared cosine function is assumed to compute the transfer function curve. The algorithm monitors the power of the detected tone, being proportional to the slope of the transfer function, while the integrator value is scanned. The algorithm stops when a zero is detected, practically the value is below an indicated noise level. The value at which the integrator stops is stored. Taking into account the sign of the gain of the integrator a minimum or maximum is differentiated. The integrator integrates, since the start of algorithm, the value of the slope times the gain. The slope is retrieved by using the sinusoidal probe signal.

$$I \propto \int m\left(t\right) k \tag{5.1}$$

where $I$ stand for integrator, $m\left(t\right)$ is the current slope of the transfer function, it is function of the time since the integrator moves the working point on the transfer function and $k$ is the gain of the integrator. When placed at the positive slope part of the optical transfer function ($cos\left(x\right)^2$), a negative value of the integrator gain will go to lower values thus converging to a minimum while a positive gain value will converge to a maximum. When placed at the negative slope part of the optical transfer function, a negative value of the integrator will converge to a maximum and a positive value of the gain of the algorithm will converge to a minimum. To know when the searching algorithm is done it can be checked whether the previous value (or average values) of the integrator converges.

In order to have the adaptive algorithm running in the FPGA a minimum SNR is needed. The SNR will be determined by the product of the measured probe signal power ($800$ Hz) and the integrator coefficient gain. The ADC accepts up to $\pm 2$V and it is mapped using a unsigned short int (0-$65535$), thus the resolution is around $61\mu$V.

## 5.3 Link polarization control

A polarization steerable system was developed assembled with a fiber polarization controller (PC) and a galvanometric scanner, both controlled by a digital signal processor (DSP) board [106]. The system implements the control of the polarization state, which is decoupled from the pointing direction of the galvo, by compensating with the PC the polarization transformation induced by the galvo through a feed-forward control scheme. Hence, the method presented can be extended to similar systems where it is needed to decouple the system general state of polarization from other transformations.

The integrated system implemented makes use of commercially available components, shown in Fig. 5.2. A fiber-pigtailed laser diode (LD) at $850$ nm generates a single polarization state with a high degree of polarization (DOP) into the PC. The output of the PC is properly launched into the galvo system (GV) using a fiber to free-space collimator (C). A dichroic mirror (DCM), placed before the galvo, reflects the signal from the beacons to be imagined on the CCD through an imaging optics system. Finally, the two imaged beacons on the CCD are processed by a digital signal processor (DSP) to compensate relative angle rotations of the receiver with respect to the transmitter, and galvo polarization transformations at a rate of $\sim 20$ ms.

### 5.3.1 Receiver orientation angle

The relative Tx-Rx orientation angle $\chi$ is retrieved by imaging the receiver through the galvanometer system and computing the apparent rotation angle. This imaging task is facilitated by two beacons, one brighter than the other, mounted on either side of the receiver. Figure 5.3(a) sketches the angle measurement algorithm. $\chi$ is the angle between the center vertical axis of the CCD image and the clockwise angle to the brighter spot. The rotation $\chi$ is converted into Mueller matrix formalism.

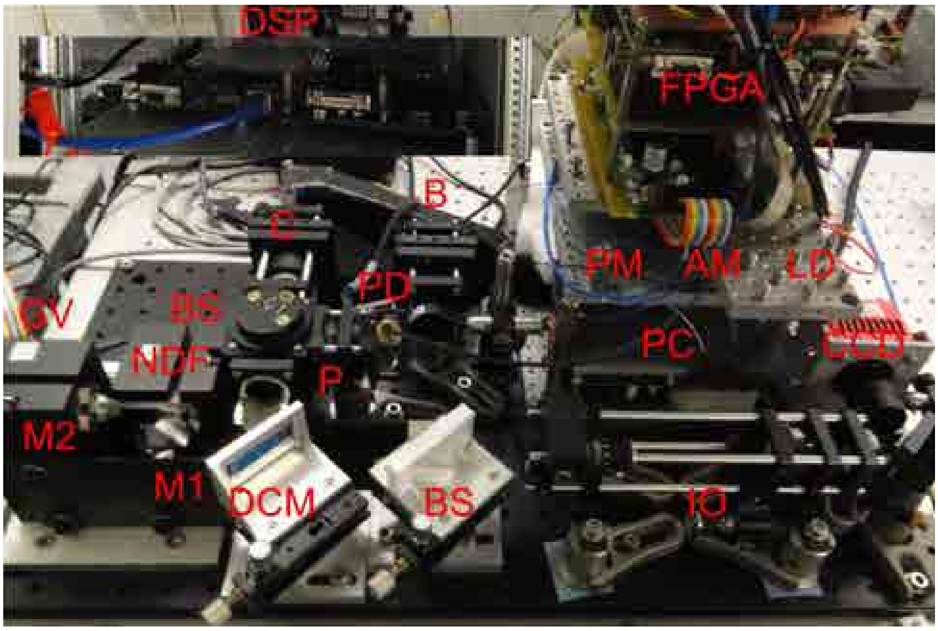


Figure 5.2: Transmitter optical system scheme. (LD) denotes the laser diode, (AM) amplitude modulator, (PM) polarization modulator, (PC) polarization controller, (C) fiber-collimator, (BS) non-polarizing beamsplitter, (P) polarizer, (PD) photodiode, (NDF) neutral density filter, (GV) galvanometric scanner with (M1) mirror 1 and (M2) mirror 2, (DCM) dichroic mirror, (IO) imaging optics, (CCD) charge-coupled device camera, (FPGA) field-programmable gate array, (DSP) digital signal processor and (B) transmitter beacon.

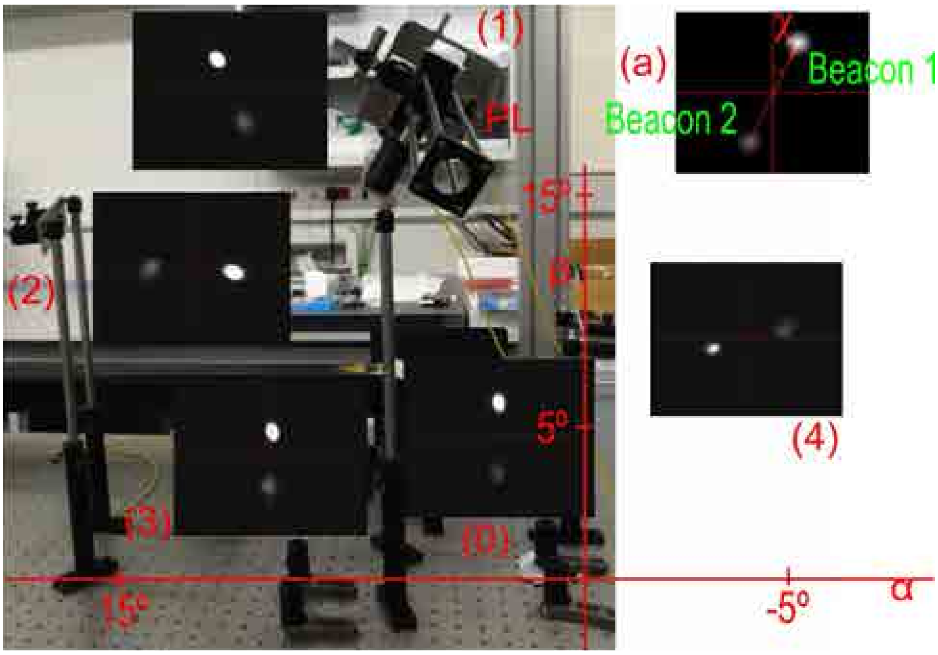


Figure 5.3: Imaged beacons to retrieve the Tx-Rx relative angle rotation $\chi$. (a) The angle is computed between the central vertical axis of the CCD image and the clockwise angle to the brighter beam spot. Notice that one of the beams is brighter than the other to easily identify both spots. Five pointing directions are considered with galvo mirrors' angles and (PL) polarimeter.

### 5.3.2 Polarization compensation

The mobile polarization analyzer system consists of a polarimeter (PL) with two $639$ nm fiber-collimated laser beacons mounted on opposite sides pointing to the transmitter. The two beacons are imaged using a charge-coupled device (CCD) camera to retrieve any relative angle rotation between the receiver PL and the transmitter galvo. The PL consists of a rotating quarter-wave plate, a fixed polarizer and a photodiode with $\pm 0.25°$azimuth and ellipticity angle accuracy. The laser beacons are mounted at $60$ mm radius with respect the center aperture of the PL and are collimated to a $1$ mm beam waist.

Five pointing directions were considered to quantify the performance of the system, with arbitrary placements and rotations of the receiver PL. The target pointing directions are described by the angles of the galvo mirrors and receiver orientation rotation, grouped in the triplet ($\alpha$,$\beta$,$\chi$). Figure 5.3(0) shows the zero pointing which corresponds to (0°,0°,0°), considering it as the reference. The other four pointing directions shown in Fig. 5.3 are: (1) pointing 1 ($3.56$°,$12.19$°,$336.47$°), (2) pointing 2 ($18.66$°,$8.37$°,$93.06$°), (3) pointing 3 ($7.99$°,$-0.13$°,$4.01$°) and (4) pointing 4 ($-4.03$°,$3.30$°,$243$°).

A manual polarization controller was added before the PC in order to generate different input polarization states, taking them as reference at the zero pointing. Four extra different pointing directions with arbitrary receiver rotations have been considered, taking four different polarization states measurements at each pointing direction. The error angle $\Delta\epsilon$ is defined as the absolute arc angle between the final polarization state and the reference polarization state at the zero pointing direction as

$$\Delta\epsilon = \left| \frac{1}{2} \cos^{-1} \Big( \cos\left[2\left(\theta_{px} - \theta_{pz}\right)\right] \cos\left[2\left(\varphi_{px} - \varphi_{pz}\right)\right] \Big) \right| . \tag{5.2}$$

$\theta_{px}$ and $\varphi_{px}$ are azimuth and ellipticity for a particular final pointing direction, and $\theta_{pz}$ and $\varphi_{pz}$ are azimuth and ellipticity for the zero pointing, considering an initial polarization state.

Figure 5.4 shows the error angles measured with the receiving PL, separated in columns by pointing directions. They are identified in color markers for compensated and uncompensated system operation. Blue-circle marker for Tx-Rx and galvo compensation, green-diamond marker for galvo compensation, cyan-square marker for Tx-Rx compensation or red-cross marker for no compensation. Error angles are plotted in logarithmic scale, $10 \cdot \log_{10}(\Delta\epsilon)$, for clearer visualization of error angles close to $0$ rad.

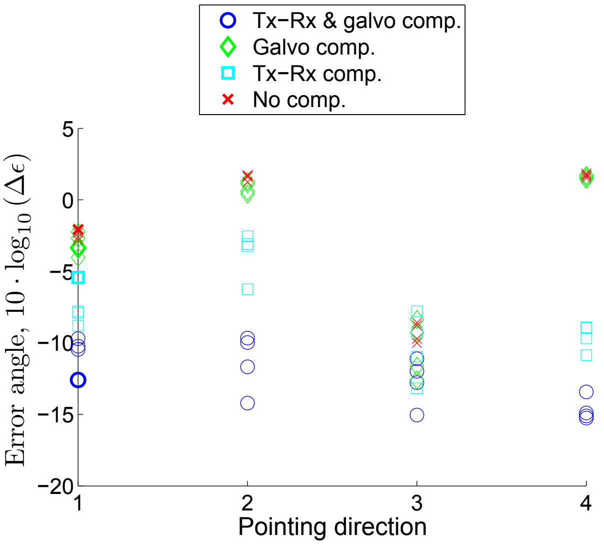


Figure 5.4: Error angle for different polarization states. The polarization states are measured with the receiving polarimeter. Different compensation configurations are presented, compensation of the Tx-Rx and galvo (blue-circle marker), galvo compensation (green-diamond marker), Tx-Rx orientation (cyan-square marker) and no compensation (red-cross marker). For each pointing direction and each compensation configuration, four different polarization states are used, taking as reference the zero pointing. Error angles are plotted in logarithmic scale, $10 \cdot \log_{10}(\Delta\epsilon)$, for clearer visualization of error angles close to $0$ rad. When the system performs the compensation, the error angle is below $0.2$ rad.

From Figure 5.4 it can be seen that the error angle due to the galvo for different pointing directions is small. In contrast, the error angle when not compensating for the Tx-Rx rotation angle is directly proportional to $\chi$. When the system performs the compensation, the error angle is smaller than $0.2$ rad. The main contribution to the error angle when compensating is due to system calibration loss due to drifts both in the SMF fibers and PC, and small pointing misalignment between the Tx and Rx along the line of propagation due to the manual placement of the PL. The performance appears to be limited by hysteresis in the PC actuators, which is largely but not completely canceled by our min-to-max driving strategy. A driving strategy based on a tracking control of hysteretic piezoelectric actuator using adaptive rate-dependent controller [107] could reduce this error significantly. $0.1$ is probably the lower limit given by the typical DOP degradation of commercial PCs. Typically, PC performance is limited by the polarization dependent loss (PDL) to about $0.1$ rad, while other parameters such as state-of-polarization (SOP) resolution and accuracy are well below this limit, $< 0.01$ rad and $< 0.002$ rad respectively. A common performance parameter in quantum communication applications is the quantum bit error ratio (QBER). QBER is defined as the number of correct sorted qubits to the number of detected qubits in the proper measuring bases, thus correct and wrong sorted qubits [25, 108]. The relation between the QBER and the error angle follows a squared cosine function as QBER$= 1 - \cos^2(\Delta\epsilon)$. The upper error angle of $0.2$ rad corresponds to $3.95\%$ QBER, while an improved driving strategy could achieve $0.1$ rad or $1\%$ QBER. Most quantum protocols run with QBERs lower than $11\%$, thus the performance achieved is compliant with quantum key distribution protocols and validates the system to be used in free-space quantum communication links.

## 5.4 Receiver optical system

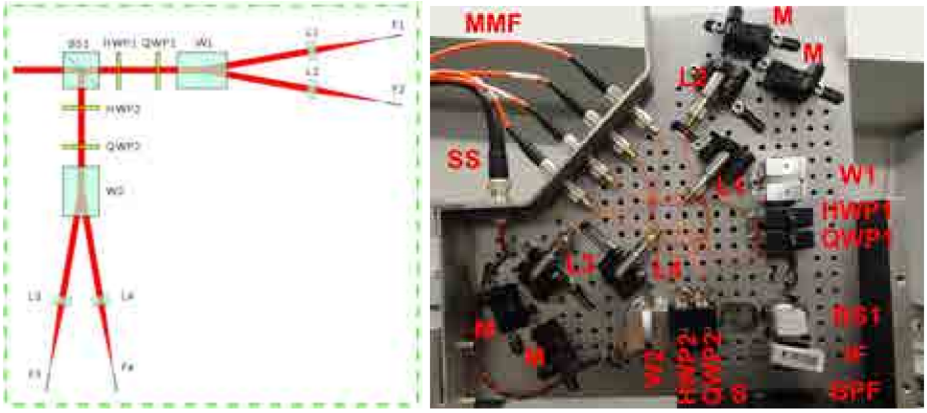
The telescope is a F/10 Meade LX200-ACF catadioptric telescope mounted on a motorized Alt/Az mount for pointing/tracking. The $200$ mm aperture of the telescope matches the diameter of the transmitter signal beam at $1$ Km distance. As a result, the geometrical loss is minimum, $2$ dB. Beyond the focal plane of the telescope, the signal beam is collimated by a lens producing an output optical beam $3$ mm in diameter. The telescope has an effective focal length of $750$ mm. With this configuration, the angular size of the pixels of the CCD camera are comparable to the optical angular resolution of the galvo scanner. The field-of-view (FOV) is $0.78°$x $0.64°$which corresponds to a rectangular area of $14x11$ m at a distance of $1$ km. The telescope has an axially symmetric design which allows to reduce polarization aberrations [109]. It is equipped with two beacon lasers, to provide information about the spatial orientation with respect the transmitter. Furthermore, an automatic tracking system using the internal stepper-motors of the telescope was developed.

The collimated output of the telescope impinges on a $45°$oriented mirror on a kinematic mount to correctly point the beams to the polarization receiver module and the telescope tracking sub-system. The tracking is based on processing the imaged beacon, from the transmitter, using a CCD and a fast DSP.

### 5.4.1 Polarization receiver module

The polarization receiver module is responsible to decode the polarization state of the received qubits, known as Bob module. A Galilean beam expander (GBE) is placed outside the Bob module to match the input optical beam diameter to the beam diameter required by the free-space to fiber couplers of the multimode fiber-coupled single-photon avalanche photodiodes (SAPDs).

A compact modular design was built based in optical optimization and mechanical model design, shown in Fig. 5.5. The input optical beam is 3 mm in diameter ($1/e^2$), $851$nm operational wavelength and $< 3$ nm bandwidth FWHM. The input signal is in the single-photon regime encoded in polarization ($+45°$, $-45°$, circular right and circular left polarization states). The detectors are multimode-fiber coupled with $62.5\mu$m core FC/PC connector. Polarization beam splitter cubes are not used because although they present enough polarization extinction ratio (PER) in the transmission branch (200:1), they usually have low PER (20:1) for the reflection branch. Instead, Wollaston prism present high PER $(10000{:}1)$ for both polarizations. A Wollaston prism is composed of two geometrically identical wedges of quartz or calcite (which are birefringent, or doubly-refracting materials) cut in a way that their optical axes are oriented perpendicular when they are cemented together to form the prism. The ordinary ray in the first half of the prism becomes the extraordinary ray in the second half, and vice versa [110]. Therefore, the two output beams in a Wollaston polarizer exit with a beam deviation from normal.



**(a)** Optical design.

**(b)** Opto-mechanical design.

Figure 5.5: Bob system design. (BPS) denotes band-pass filter, (IF) interference filter, (BS) beamsplitter, (QWP) quarter-wave plate, (HWP) half-wave plate, (W) wollaston prism, (M) mirror, (L) lens coupler, (MMF) multimode fiber, (SS) shutter signal and (S) shutter. (a) Optical system optimization using Zemax software. (b) Opto-mechanical design for correct placement, alignment and reliability. Overall size is $< 20$x$20$x$10$ cm$^3$ and $< 6$ kg weight.

The most important parameter in order to build a high performance Bob module is to achieve a high PER ($> 20$ dB) and just almost as important is to have a high coupling ratio ($> 90\%$). Since the beam is collimated and there are no focusing lenses in the system, the precision-alignment-demanding component are the fiber couplers, specially in tilt adjustment. Once aligned, the maximum permitted changes have been identified to be $0.02°$and $500\mu m$ for the input beam.

### Mechanical box

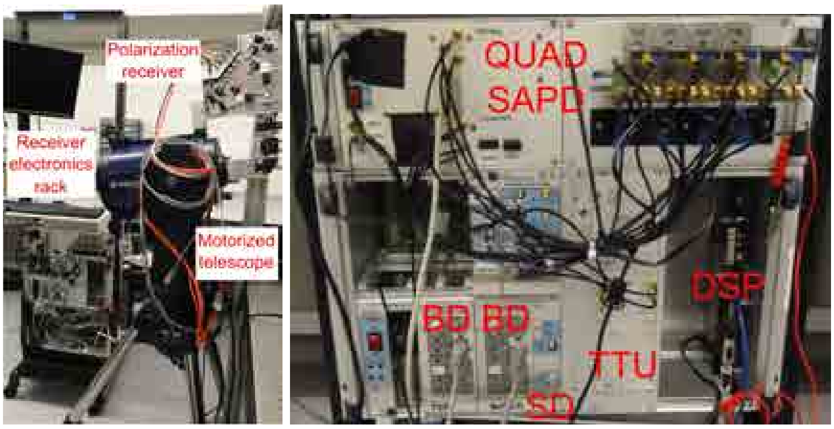
The polarization receiver module was built in a custom aluminum box attached to the output of the telescope, shown in Fig. 5.5(b). The box is light-weight and closed to avoid surrounding light and the qubits are coupled to output MMFs. The MMF were covered with black-out material to avoid light into the output MMF fibers which reach the detectors.

The temperature range for space application requires parameters and functional stability in the range from $-55$ to $+125$°C. The worst case, in terms of first approximation of thermal expansion, is taking the largest dimension of the base (116mm) and the maximum allowed displacement for a collimator $1.7$mm. Considering space requirements, the thermal expansion coefficient has to be smaller than $\alpha_T < 150 \cdot 10^{-6}\ K^{-1}$. Aluminum has a thermal expansion coefficient of $\alpha_T = 23 \cdot 10^{-6}\ K^{-1}$.

The mechanical box is made of aluminum with black absorptive material in the inside walls and the aluminum color for the outside in order to reflect as maximum the incident light and have less thermal expansion. The buried beds on the base have a depth of $250 - 300\mu m$. Special attention is taken to prevent the surrounding light from entering the closed box by placing the base on a larger base with screw-holes at the ends to screw the encapsuling cover.

## 5.5 Data synchronization and processing

The received qubits decoded in polarization are sent through MMF to the detection electronics, Fig, 5.6(a). The receiving electronics were assembled in a portable rack mount, shown in Fig. 5.6(b). A four channel single-photon avalanche photodiode (SAPD) detects the received qubits and generates a time accurate pulse to the timetagging unit (TTU) independently for each channel. The TTU detects with $78.125$ ps time resolution the edge of the pulses generated by the detectors and timestamps the detections. Data is temporally stored in an internal FIFO memory consisting of the pair (channel,timestamp). Data is continuously dump to the computer through direct memory access (DMA) feature at 10 Msps (stamps per second).



**(a)** Receiver system. **(b)** Receiver system electronics.

Figure 5.6: Receiver system assembled in a portable rack. (QUAD SAPD) denotes a four channel single-photon avalanche photodiodes, (TTU) timetagging unit, (DSP) digital signal processor, (SD) optical shutter driver and (BD) beacon driver. A protection logic circuit was added to the QUAD SAPD to avoid burning off the detectors if too much light goes into. The protection system shuts down the SAPDs module and closes the optical shutter at the polarization receiver.

Most of the computational processing of the data is performed on the computer, while the DSP handles the fast fine tracking of the telescope.

### 5.5.1 Data synchronization

Data synchronization is continuously performed in-line, not requiring dead times for processing, implementing the detected photon signal driven clocks technique. The algorithm requires an initial synchronization sequence known to Alice and Bob (public) to find the initial $\Delta T$ and relative frequency difference $\Delta u$.

Initially, $\Delta T\,(1+\Delta u)$ is unknown but the term can be effectively retrieved by computing the cross correlation between the detected and original sequence of length $T_a$. Typically, the time gate window is $\tau_c = 1$ ns, the detector jitter $\tau_d = 500$ ps and $R_b = 1.5$ Mbps expected signal detection rate. In order to estimate the center of the time differences, with an uncertainty $\delta\tau_c = 0.1$ ns (one order of magnitude better than the $\tau_c$ window), it is needed to average $n$ time differences given by

$$n = \left(\frac{\tau_d}{2\sqrt{2\ln 2}\delta\tau_d}\right)^2 + 1 \approx 6 \tag{5.3}$$

where $\sigma$ is the standard deviation of the jitter, that assuming that the jitter has a Gaussian time distribution statistics, is related to the jitter as $\tau_d = 2\sqrt{2\ln 2}\sigma$. To maintain two clocks synchronized within $\tau_c$ after a $\tau_e$, a relative frequency difference lower than $\tau_c/\tau_e$ is required. Thus, for a time period of $n/R_b = 4\mu$s, the clock should not drift such that an event leaves the time window, which translates into a relative frequency difference accuracy given by $\tau_c/(n/R_b) = 250$ ppm, achievable with crystal oscillators.

Then, the algorithm has to correctly estimate $\Delta T$ and $\Delta u$ separately. First, $\Delta u$ is estimated by computing the relation $(\Delta T_1 - \Delta T_2)\,/T_s$ between two sequences of length $T_a$ separated in time by $T_s$. Once $\delta u$ is known, timestamps can be corrected for the frequency drift $(1+\Delta u)$ and $\Delta T$ computed. $\Delta T$ needs to be known to a better uncertainty than the time gate window (1 ns).

### Synchronization on moving platforms

On a moving platform, there will be varying Doppler shifts which change the frequency difference $\Delta u$ and the time offset $\Delta T$, but can be tracked and corrected for.

In the limit where the speed of the wave is much greater than the relative speed of the source and observer (the case with electromagnetic waves, light), the relationship between observed frequency $f$ and emitted frequency $f_0$ is given by

$$f = \left(1 - \frac{v_{s,r}}{c}\right) f_0 \tag{5.4}$$

where $v_{s,r}$ is the velocity of the source relative to the receiver (negative when the source is moving towards the receiver, positive when moving away), $c$ is the speed of light. Thus, the frequency change is given by

$$\Delta f = -\frac{v_{s,r}}{c} f_0 \tag{5.5}$$

Considering satellite motion ($\pm 3 - 5$ km/s), which would be the extreme situation of interest, the relative frequency difference change is of $13.33$ ppm. Given an emitted frequency of $f_0 = 100$ MHz, the frequency change is $f = 1.3$ KHz.

Considering the synchronization requirements shown before and considering satellite motion, the relative frequency difference is increased by $13.33$ ppm. This extra relative frequency difference, together with the maximum relative frequency difference due to standard crystals oscillators ($100$ ppm), is lower than the maximum acceptable frequency difference $250$ ppm. Moreover, the gate window should be enlarged only by $177.3$ ps.

### 5.5.2 Data processing

The QKD transmission follows the protocol scheme shown in Fig. 5.7. First, the transmitter is calibrated, both for the source devices as well as for the link polarization control sub-system. In parallel, the transmitter and the receiver are oriented to point each other. Then, the tracking is turned on and the synchronization data sequence is transmitted, insure success. Finally, the random secure QKD data sequence is sent.

Since neither the source nor the link polarization control have continuous calibration, the QKD transmission is stopped after a certain time. Again, the whole procedure is repeated but the tracking algorithm runs

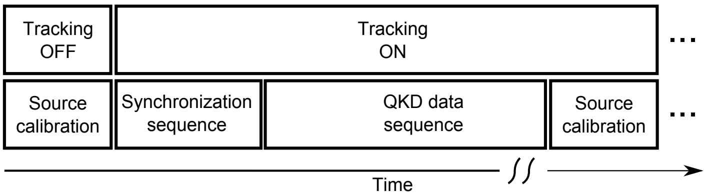


Figure 5.7: QKD transmission protocol scheme. First the transmitter is calibrated while initial pointing for the tracking is carried out. Then, the tracking is turned on and the synchronization sequence is transmitted first and then the random secure QKD data. Due to calibration drifts at the transmitter, the whole procedure is repeated indefinitely, although the tracking is continuously running.

continuously. Each, complete procedure lasts 15 minutes. Source calibration takes 4 minutes, synchronization sequence 1 minute and QKD transmission 10 minutes.

In faint pulse source systems, it is convenient to compute clock synchronization and QKD reconciliation at the transmitter. Mainly because the receiver has detected much less qubits than those sent by the transmitter. Hence, the classical channel data transmission requirements are lower. Furthermore, it is practical to encode the timetag information in a compressed Poisson rate-dependent algorithm [111, 112]. This is particularly interesting in ground-to-satellite applications, where the downlink transmission speed is strongly limited or the available transit time of the satellite reduced.

## 5.6 Summary

An automatic calibrated faint pulse source based on $LiNbO_3$ modulators has been assembled and incorporated in a complete free-space optical transmitter system. Also, it has been demonstrated a steerable optical system based on a feed-forward control with decoupled control of the polarization state. It is possible to assemble the system from commercially available components. The system is able to compensate the particular galvo polarization transformation which depends on the pointing direction and the relative orientation rotation of the receiver.

A complete receiving system, considering the optics and the electronics, has been assembled. The clock synchronization technique relies on the detected photons clock driving technique because it is more robust, reliable and straight forward to implement. Otherwise a pilot signal synchronization technique can be though as the back-up solution or even can be concurrent with the detected photons clock driving algorithm. Finally, a simple QKD transmission protocol has been proposed considering the technical performances of the involved transmitter and receiver assembled.

# Chapter 6

# Conclusions

QKD has been routinely demonstrated across optical fiber links of more than $200$ km, and over $144$ km line-of-sight free-space links, establishing the feasibility of ground-to-satellite quantum communication. QKD is well-aligned with the trend toward increasing capacity of optical fiber networks through greater transparency. This raises the possibility that quantum cryptography could be incorporated into future networks to provide security at the physical layer level for new applications.

This thesis has explored new schemes of faint pulse sources (FPSs) for free-space QKD. First, two polarization-encoded high-speed sources suitable for Space have been demonstrated. Following the extensive work on direct laser diode modulation, a novel random number generator scheme has been invented. The device is simple, fast and highly competitive solution for true random number generation. Finally, initial work on the implementation of a complete QKD system for mobile platforms has been carried out.

The work in Chapter 2 demonstrates implementation of FPSs with commercially available optical devices. The source is based on waveguide $LiNbO_3$ modulators. $LiNbO_3$ modulators definitely allow to reach transmission speeds higher than $40$ Gbps, until technical impairments decrease the performance achieved with the source. Also, advanced calibration techniques are required for long-term operation which increase the overall cost and complexity of the source.

A much simpler and robust FPS is described in Chapter 3. It is based on semiconductor optical amplifiers which select which output polarization state is transmitted. This scheme achieves a very high QBER performance, despite the high number of optical components and devices required and the assembly of a custom opto-mechanical mount.

Together with the sources work, a new true random number generator (TRNG) has been designed and implemented in Chapter 4. It is based on extraction of random bits from vacuum using optical-independent amplification. It has a high potential to gain a market share from classical RNG devices because it is simple, integrated and fast. Furthermore, this research has initiated a ERC-funded project, called MAMBO. The project aims at developing a QRNG product which outperforms current commercial solutions, in particular, increasing the generation speed and identifying the ultimate limitations of the invented scheme.

Finally, the work in Chapter 5 presents work towards a convenient implementation of a complete QKD system for mobile platforms, such as in ground-to-satellite links. An automatically calibrated FPS source has been assembled in a light-weight transmitter system for convenient integration in a highly dynamic mobile platform. A fundamental aspect of this system is the capacity to overcome the technical issues of polarization-encoded communication in a changing polarization-reference-frame system. The control of the polarization state of a signal while the beam is steered in real time has been successfully demonstrated. Future work will include the final engineering of the different parts of the receiver. A research effort for the whole link experiment will definitely contribute to enhance current QKD technologies and advance the field of quantum communication in free-space.

# Bibliography

[1] M. Fox, *Quantum Optics: An Introduction*. Oxford University Press, 2006.

[2] M. Scully and M. Zubairy, *Quantum optics*. Cambridge University Press, 1997.

[3] R. Loudon, *The Quantum Theory of Light, Third Edition*. Oxford University Press, 2000.

[4] Y. Hu, X. Peng, T. Li, and H. Guo, "On the Poisson approximation to photon distribution for faint lasers," *Physics Letters A*, vol. 367, pp. 173–176, 2007.

[5] H. Hemmati and I. B. Djordjevic, "Deep-Space Optical Communications: Future Perspectives and Applications," *Proc. IEEE*, vol. 11, pp. 2020–2039, 2011.

[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, C. U. Press, Ed., 2000.

[7] W. K. Wootters and W. H. Zurek, "A Single Quantum Cannot be cloned," *Nature*, vol. 299, pp. 802–803, 1982.

[8] D. Dieks, "Communication by EPR devices," *Physics Letters A*, vol. 92, pp. 271–272, 1982.

[9] T. H. Carbonneau and D. R. Wisely, "Opportunities and challenges for optical wireless: the competitive advantage of free

space telecommunications links in today's crowded marketplace," *Wireless Technologies and Systems: Millimeter-Wave and Optical, Proc. SPIE*, vol. 3232, pp. 119–128, 1998.

[10] T. Garlington, J. Babbitt, and G. Long, "Analysis of Free Space Optics as a Transmission Technology," Tech. rep., U.S. Army Information Systems Engineering Command (USAISEC), Transmission Systems Directorate, Tech. Rep. WP No. AMSEL-IE-TS-05001, 2005.

[11] D. O'Brien, G. Faulkner, K. Jim, E. Zyambo, D. Edwards, M. Whitehead, P. Stavrinou, G. Parry, J. Bellon, M. Sibley, V. Lalithambika, V. Joyner, R. Samsudin, D. Holburn, and R. Mears, "High-speed integrated transceivers for optical wireless," *Communications Magazine, IEEE*, vol. 41, no. 3, pp. 58–62, Mar 2003.

[12] C. Davis, I. Smolyaninov, and S. Milner, "Flexible optical wireless links and networks," *Communications Magazine, IEEE*, vol. 41, no. 3, pp. 51–57, Mar 2003.

[13] T.-Y. Chen, J. Wang, Y. Liu, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "200km Decoy-state quantum key distribution with photon polarization," *arXiv:0908.4063v1*, 2009.

[14] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojeck, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, pp. 481–486, 2007.

[15] D. Y. Vaylyev, A. A. Semenov, and W. Vogel, "Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality," *Phys. Rev. Lett.*, vol. 108, p. 220501, 2012.

[16] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Fedrizzi, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lutkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch, V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, and A. Zeilinger, "Space-quest: Experiments with quantum entanglement in space," *Europhysics News*, vol. 40, no. 3, pp. 26–29, 2009.

[17] C. Y. Young, L. C. Andrews, and A. Ishimaru, "Time-of-arrival fluctuations of a space–time gaussian pulse in weak optical turbulence: an analytic solution," *Appl. Opt.*, vol. 37, no. 33, pp. 7655–7660, 1998.

[18] V. Chan, "Coding for the turbulent atmospheric optical channel," *Communications, IEEE Transactions on*, vol. 30, no. 1, pp. 269–275, Jan 1982.

[19] J. G. Rarity, P. R. Tapster, and P. M. Gorman, "Secure free-space key exchange to 1.9km and beyond," *Journal of Modern Optics*, vol. 48, pp. 1887–1901, 2001.

[20] C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Clock synchronization by remote detection of correlated photon pairs," *New Journal of Physics*, vol. 11, p. 045011, 2009.

[21] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Free-Space distribution of entanglement and single photons over 144 km," *Nature Phys.*, vol. 3, p. 481, 2007.

[22] Q.-L. Wu, Z.-F. Han, E.-L. Miao, Y. Liu, Y.-M. Dai, and G.-C. Guo, "Synchronization of free-space quantum key distribution," *Optics Communications*, vol. 275, pp. 486–490, 2007.

[23] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, pp. 1–14, 2002.

[24] M. Dusek, N. Lutkenhaus, and M. Hendrych, "Quantum Cryptography," *Progress in Optic*, vol. 49, pp. 381–454, 2006.

[25] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews Modern Physics*, vol. 74, pp. 145–195, 2002.

[26] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, 1301, 2008.

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

[28] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, December 1984.

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

[30] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum Cryptography with Entangled Photons," *Phys. Rev. Lett.*, vol. 84, pp. 4729–4732, 2000.

[31] N. Gisin and N. Brunner, "Quantum cryptography with and without entanglement," *Arxiv*, 2008.

[32] G. Brassard and L. Salvail, "Secret Key Reconciliation by Public Discussion," *Advances in Cryptology - EUROCRYPT '93*, vol. 765/1994, pp. 410–423, 1994.

[33] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[34] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, 2000.

[35] D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," *Advances in Cryptography - Proceedings of Crypto '96 (Springer-Verlag)*, pp. 343–357, 1996.

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

[37] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, 230503, no. 23, p. 4, Jun 2005.

[38] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, p. 230504, Jun 2005.

[39] M. Nothaft, S. Hohla, F. Jelezko, N. Frunhau, J. Pflaum, and J. Wrachtrup, "Electrically driven photon antibunching from a single molecule at room temperature," *Nature Comm.*, vol. 3, p. 628, 2012.

[40] W. E. Moerner, "Single-photon sources based on single molecules in solids," *New J. Phys.*, vol. 6, p. 88, 2004.

[41] H.-K. Lo, "Getting something out of nothing," *Quantum Information and Computation*, vol. 5, no. 4&5, pp. 413–418, Mar 2005.

[42] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” *Phys. Rev. A*, vol. 72, no. 1, p. 012326, Jul 2005.

[43] N. Lütkenhaus, “Security against individual attacks for realistic quantum key distribution,” *Phys. Rev. A*, vol. 61, no. 5, p. 052304, Apr 2000.

[44] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” *Quant. Inf. Comput.*, vol. 5, pp. 325–360, 2004.

[45] F. Galton, “Dice for statistical experiments,” *Nature*, vol. 42, pp. 13–4, 1890.

[46] R. Corporation, Ed., *A Million Random Digits with 100,000 Normal Deviates*. The Free Press, 1955.

[47] T. Kanai, M. Tarui, and Y. Yamada, “Random number generator,” *International patent WO2010090328*, 2009.

[48] G. Ribordy and O. Guinnard, “Method and apparatus for generating true random numbers by way of a quantum optics process,” *US patent 2007127718*, 2007.

[49] N. Cerf and L.-P. Lamooureux, “Network distributed quantum random number generation,” *International patent GB2473078*, 2009.

[50] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*. Wiley Publishing, Inc., 2010.

[51] N. Metropolis and S. Ulam, “The Monte Carlo Method,” *J. Am. Statist. Assoc.*, vol. 44, pp. 335–341, 1949.

[52] S. Banks, P. Beadling, and A. Ferencz, “FPGA Implementation of Pseudo Random Number Generators for Monte Carlo Methods

in Quantitative Finance," in *Proceedings of the 2008 International Conference on Reconfigurable, Computing and FPGAs, RECONFIG'08*. IEEE Computer Society Washington, DC, USA, 2008, pp. 271–276.

[53] S. Pironio and *et al.*, "Random numbers certified by Bell's theorem," *Nature*, vol. 464, pp. 1021–1024, 2010.

[54] R. Colbeck and A. Kent, "Private randomness expansion with untrusted devices," *J. Phys. A: Math. Theor.*, vol. 44, p. 095305, 2011.

[55] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, 2000.

[56] O. Kwon, Y.-W. Cho, and Y.-H. Kim, "Quantum random number generator using photon-number path entanglement," *Appl. Opt.*, vol. 48, pp. 1774–1778, 2009.

[57] M. Stipcevic and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Rev. Sci. Instrum.*, vol. 78, p. 045104, 2007.

[58] P. Bronner, A. Strunz, C. Silberhorn, and J. P. Meyn, "Demonstrating quantum random with single photons," *Eu. J. Phys.*, vol. 30, pp. 1189–1200, 2009.

[59] M. Wayne and P. Kwiat, "Low-bias high-speed quantum number generator via shaped optical pulses," *Optics Express*, vol. 18, no. 9, pp. 9351–9357, 2010.

[60] M. Fürst, H. Weier, S. Nauerth, D. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Optics Express*, vol. 18, no. 12, pp. 13 029–13 037, 2010.

[61] M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," *Applied Physics Letters*, vol. 98, p. 171105, 2011.

[62] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nature Photonics*, vol. 4, pp. 711–715, 2010.

[63] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," *Applied Physics Letters*, vol. 98, p. 231103, 2011.

[64] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Opt. Lett.*, vol. 35, no. 3, pp. 312–314, 2010.

[65] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Physical Review E*, vol. 81, p. 051137, 2010.

[66] (2010) Random number generation using quantum physics. idQuantique White Paper.

[67] G. Taylor and G. Cox, "Digital randomness," IEEE Spectrum, Tech. Rep., 2011.

[68] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photonics*, vol. 2, pp. 728–732, 2008.

[69] W. Gunawan and M. Berhad, "Quantum random number generator based on diffraction of high-order grating," *International patent WO 2010062161*, 2010.

[70] Z. Yuan, J. Dynes, M. R. Stevenson, and A. J. Shields, “Random number generation using photon detection events,” *International patent GB 2457328*, 2009.

[71] Y. Luo and T. C. Kam, “Quantum random number generators,” *International patent KR 20080025151*, 2008.

[72] P. R. Tapster and P. M. Gorman, “Apparatus and Method for Generating Random Numbers,” *US patent 2009013019*, 2009.

[73] A. Trifonov and H. Vig, “Quantum noise random number generator,” *US patent 7284024*, 2007.

[74] J. v. Neumann, “Various techniques used in connection with random digits,” *National Bureau of Standards Applied Mathematics Series*, vol. 12, pp. 36–38, 1951.

[75] P. Barreto and V. Rijmen. (2010) The Whirlpool Hashing Function. [Online]. Available: http://www.larc.usp.br/~pbarreto/WhirlpoolPage.html

[76] Y. Peres, “Iterating Von Neumann’s Procedure for Extracting Random Bits,” *Ann. Stat.*, vol. 20, pp. 590–597, 1992.

[77] N. Nisan and A. Ta-Shma, “Extracting Randomness: A Survey and New Constructions,” *Journal of Computer and System Sciences*, vol. 58, pp. 148–173, 1999.

[78] L. Trevisian, “Extractors and Pseudorandom Generators,” *J. ACM*, vol. 48, pp. 860–879, 2001.

[79] P. Hellekalek, “Good random number generators are (not so) easy to find,” *IMACS*, vol. 46, pp. 485–505, 1998.

[80] P. L’Ecuyer and R. Simard, “TestU01: A C library for empirical testing of random number generators,” *ACM Trans. Math. Softw.*, vol. 33, no. 4, Article 22, p. 40, 2007.

[81] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New J. Phys.*, vol. 4, p. 82, 2002.

[82] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-Distance Quantum Communications with Entangled Photons Using Satellites," *IEEE J. Sel. Top. Quantum Elec.*, vol. 9, pp. 1541–1551, 2003.

[83] M. Jofre, A. Gardelein, G. Anzolin, G. Molina-Terriza, J. P. Torres, M. W. Mitchell, and V. Pruneri, "100 MHz Amplitude and Polarization Modulated Optical Source for Free-Space Quantum Key Distribution at 850 nm," *IEEE Journal of Lightwave Technology*, vol. 29, pp. 2572–2578, 2010.

[84] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Information and Computation*, vol. 8, no. 5, pp. 431–458, 2007.

[85] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics*. Wiley, 2007.

[86] C. McConaghy, M. Lowry, R. Becker, and B. Kincaid, "The Performance of Pigtailed Annealed Proton Exchange $LiNbO_3$ Modulators at Cryogenic Temperatures," *IEEE Phot. Tech. Lett.*, vol. 8, pp. 1480–1482, 1996.

[87] M. V. Hobden and J. Warner, "The temperature dependence of the refractive indices of pure lithium niobate," *Phys. Lett.*, vol. 22, pp. 243–244, 1966.

[88] J. D. Zook, D. Chen, and G. N. Otto, "Temperature dependence and model of the electro-optic effect in $LiNbO_3$," *Appl. Phys. Lett.*, vol. 11, pp. 159–161, 1967.

[89] K. McCammon, J. Morse, D. Masquelier, C. McConaghey, H. Garret, K. Hugenberg, M. Lowry, E. Track, and L. Bunz, "Fiber Optic

Transceiver for Interfacing Digital Superconducting Electronics," in *Dod Fiber Optics Conference*, 1994.

[90] J. S. Browder and S. S. Ballard, "Thermal expansion data for eight optical materials from 60k to 300k," *Appl. Opt.*, vol. 16, pp. 3214–3217, 1977.

[91] T. Fujiwara, T. Kawazoe, and H. Mori, "Temperature dependence of the half-wave voltage in Ti:LiNbO$_3$ waveguide devices at 0.83 $\mu$m," *Jap. Jour. Appl. Phys.*, vol. 29, pp. 2229–2231, 1990.

[92] J. D. Morse, K. G. McCammon, C. F. McConaghey, D. H. Masquelier, H. E. Garret, and M. E. Lowry, "Characterization of lithium niobate electro-optic modulators at cryogenic temperatures," *Proc. SPIE*, vol. 2150, pp. 283–291, 1994.

[93] Y. Di, P. Gardner, and H. Ghafouri-Shiraz, "Methods for measuring the RF half-wave voltage of LiNbO$_3$ optical modulators," *Microwave Opt. Tech. Lett.*, vol. 46, pp. 440–443, 2005.

[94] E. Wooten, K. Kissa, A. Yi-Yan, E. Murphy, D. Lafaw, P. Hallemeier, D. Maack, D. Attanasio, D. Fritz, G. McBrien, and D. Bossi, "A review of lithium niobate modulators for fiber-optic communications systems," *IEEE Sel. Top. Quant. Elec.*, vol. 6, pp. 69–82, 2000.

[95] M. Ott, J. Vela, C. Magee, and H. Shaw, "Reliability of Optical Fiber Modulators for Space Flight Environments," Sigma Research Engineering/NASA Goddard Space Flight Center, Tech. Rep., 2002.

[96] D. Derickson, *Fiber optic: Test and Measurement*. Prentice Hall, 1998.

[97] K. Petermann, *Laser diode modulation and noise*, A. in Optoelectronics, Ed. Kluwer Academic Publishers, 1991.

[98] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," *arXiv:0906.4547v1*, June 2009.

[99] M. Jofre, A. Gardelein, G. Anzolin, W. Amaya, J. Capmany, R. Ursin, L. Penate, D. Lopez, J. L. S. Juan, J. A. Carrasco, F. Garcia, F. J. Torcal-Milla, L. M. Sanchez-Brea, E. Bernabeu, J. M. Perdigues, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri, "Fast optical source for quantum key distribution based on semiconductoroptical amplifiers," *Opt. Express*, vol. 19, no. 5, pp. 3825–3834, Feb 2011.

[100] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," *Optics Express*, vol. 19, pp. 20 665–20 672, 2011.

[101] H. F. Hofmann and O. Hess, "Coexistence of thermal noise and squeezing in the intensity fluctuations of small laser diodes," *JOSA B*, vol. 17, pp. 1926–1933, 2000.

[102] C. H. Henry, "Theory of the Linewidth of Semiconductor Lasers," *IEEE Quant. Electr.*, vol. 18, pp. 259–264, 1982.

[103] Y. Suematsu and S. Arai, "Single-mode semiconductor lasers for long-wavelength optical fiber communications and dynamics of semiconductor lasers," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 6, no. 6, pp. 1436–1449, 2000.

[104] M. J. Collett and C. W. Gardiner, "Squeezing of intracavity and traveling-wave light fields produced in parametric amplification," *Phys. Rev. A*, vol. 30, no. 3, pp. 1386–1391, 1984.

[105] M. D. Sturge, "Optical absorption of gallium arsenide between 0.6 and 2.75 ev," *Phys. Rev.*, vol. 127, no. 3, pp. 768–773, Aug 1962.

[106] M. Jofre, G. Anzolin, F. Steinlechner, N. Oliverio, J. P. Torres, V. Pruneri, and M. W. Mitchell, "Fast beam steering with full polarization control using a galvanometric optical scanner and polarization controller," *Opt. Express*, vol. 20, pp. 12 247–12 260, 2012.

[107] U.-X. Tan, W. T. Latt, F. Widjaja, C. Y. Shee, C. N. Riviere, and A. W. T., "Tracking control of hysteretic piezoelectric actuator using adaptive rate-dependent controller," *Sensors and Actuators A*, vol. 150, pp. 116–123, 2009.

[108] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[109] J. P. McGuire Jr. and R. A. Chipman, "Polarization aberrations. 2. tilted and decentered optical systems," *Applied Opt.*, vol. 33, p. 5101, 1994.

[110] M. Françon and S. Mallick, "Polarization interferometers: applications in microscopy and macroscopy," in *Wiley-Interscience, New York*, 1971.

[111] I. Rubin, "Information Rates and Data-Compression Schemes for Poisson Processes," *IEEE Trans. Information Theory*, vol. 20, pp. 200–210, 1974.

[112] G. Vega, R. Sato, F. Contreras, B. Garcia, M. Platino, A. Lucero, F. Suarez, M. Videla, and O. Wainberg, "Lossless compression of Poisson distributed variable for AMIGA/Auger," *Elsevier*, vol. 1, p. 10, 2011.