TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

MASTERARBEIT

Preparatory Experiments for a Cosmic Bell Test and Satellite-based Quantum Communication

Ausgeführt am

Atominstitut Wien

der Technischen Universität Wien

durch

David Bricher

Matrikelnummer 1026016
Mayerhofgasse 4/10, 1040 Wien

unter Gutachtung von

o. Univ.- Prof. Dr. phil. Anton ZEILINGER

Vienna, May 9, 2016

Contents

Abstract

Based on the superposition principle of quantum mechanics, single particle states can be used to encrypt and decrypt messages for quantum key distribution. The main aim of these quantum communication schemes is to render an unconditionally secure key between two parties, which is today achieved e.g. with weak coherent laser pulses. In systems consisting of more than one particle, the physical phenomenon of quantum entanglement is leading to correlations between those particles over large distances. This quantum effect is suggested to be one of the main approaches for future applications in quantum computation, quantum information and quantum communication. Within this thesis I describe preparatory experiments, that are essential for the realization of two quantum free-space projects, that I have worked on at the Institute for Quantum Optics and Quantum Information in Vienna, which make use of the correlation effects of polarization entangled photons and weak coherent laser pulses.

The Quantum Experiments at Space Scale (QUESS) project pursues the aim to enable an unconditional secure quantum key exchange for the first time between a satellite and different optical ground stations. This experiment is a collaboration of the Austrian and the Chinese Academy of Sciences, whereby the Austrian side is responsible to equip the ground stations within Europe with corresponding polarization analyzation modules. In order to adjust these receiving modules with horizontal optical free-space links, it was my task to develop a satellite mock-up setup, which I describe in this thesis. We have shown that the ground stations of Tenerife and Graz are already well aligned by achieving polarization visibilities that exceed a level of 98% and thus, they are well prepared for future satellite-to-ground communications. Within the second project described, an experimental Bell test is planned to be carried out for the first time with different cosmic light sources in order to close the freedom-of-choice loophole. The realization and preparation of the therefore needed polarization analyzation modules are described in detail in this thesis. In a first laboratory approach we have carried out an experiment with different sources of random numbers in order to test the violation of the Bell inequality. Within each experimental run we have violated the Bell inequality by more than 70 standard

deviations. Thus, we can guarantee a proper alignment for future Bell tests with cosmic sources.

Kurzfassung

Aufbauend auf dem Superpositionsprinzip der Quantenmechanik kann man Zustände von Einzelphotonen dazu verwenden, um geheime Botschaften zu verschlüsseln bzw. zu dechiffrieren. Das vorrangige Ziel von diesen Quantenkommunikationsprotokollen besteht darin, einen abhörsicheren Schlüssel zwischen zwei verschiedenen Parteien auszutauschen, was man heutzutage beispielsweise mit schwachen kohärenten Laserpulsen bewerkstelligen kann. In Systemen, die aus mehr als einem Teilchen bestehen, führt das physikalische Phänomen der Verschränkung zu langreichweitigen Korrelationen zwischen diesen Teilchen. Dieser Effekt der Verschränkung wird als ein Eckpfeiler für die zukünftige Ermöglichung von Anwendungen im Bereich der Quanteninformatik, des Quantencomputers und der Quantenkommunikation angesehen. Diese Arbeit beschreibt vorbereitende Experimente, welche essentiell für die Durchführung von zwei quantenoptischen free-space Projekten sind, an denen ich am Institut für Quantenoptik und Quanteninformation in Wien gearbeitet habe, und die sich den Korrelationseffekten von in der Polarisation verschränkten Photonen und schwachen kohärenten Laserpulsen bedienen.
Das QUESS Projekt (Quantum Experiments at Space Scale) verfolgt das Ziel eines abhörsicheren Quanten-Schlüssel-Austausches, welcher erstmals zwischen einem Satelliten und verschiedenen optischen Bodenstationen bewerkstelligt werden soll. Dieses Experiment stellt eine Kollaboration der Österreichischen und Chinesischen Akademie der Wissenschaften dar, wobei sich die österreichische Seite dazu verpflichtet hat, sich um die Ausrüstung der verschiedenen Bodenstationen mit Polarisations-Analyse-Modulen in Europa zu kümmern. Um diese Empfängermodule mit optischen horizontalen free-space Links richtig zu justieren, bestand meine Aufgabe in der Entwicklung eines Satelliten-Attrapen Systems, welches ich in dieser Arbeit beschreibe. Dabei haben wir in unseren Bodenstationen in Teneriffa und Graz eine Polarisations-Visibility von 98% überschritten, was einer optimalen Präparierung der Analyse-Module entspricht und einen Einsatz für zukünftige Satelliten Experimente ermöglicht.
Innerhalb des zweiten beschriebenen Projekts versucht man das freedom-of-choice Schlupfloch in einem kosmischen Bell-Test Experiment zu schließen. Die Justage und das Verhalten von den dafür verwendeten Polarisations-Analyse-Modulen wer-

den im Detail behandelt. In anfänglichen Labortests haben wir verschiedene Quellen von Zufallszahlen verwendet, um deren Einfluss auf den Ausgang eines Bell-Tests zu studieren. Dabei stellten wir fest, dass die Bellsche Ungleichung bei jedem Durchlauf um mehr als 70 Standardabweichungen verletzt wurde. Die Ergebnisse bestätigen uns eine passende Justage der Analyse-Module für zukünftige Bell-Tests mit kosmischen Quellen.

Chapter 1

Introduction

"God does not play dice with the universe."

- Albert Einstein, The Born-Einstein Letters 1916-55

The above quoted citation is definitely one of the, if not the, most common statement of Albert Einstein towards quantum mechanics. It is fascinating to explore, how the world of quanta differs from what we call the physics of everyday life, and it is even more fascinating to see, in how many different ways mankind is making use of the effects of quantum mechanics. Particle entanglement is one of these surrealistic effects, that Einstein once called "spooky action at a distance". Although many physicists believed, quantum mechanics would be an incomplete theory with a hidden local mechanism as foundation, John Bell came up with a theory in 1964, from which he concluded that no local hidden variable theory can be used to reproduce all properties of quantum mechanics. Unfortunately, Albert Einstein was not alive at the time when Bell published his work. It would be thrilling to see, if he would digress from the above quoted citation.

Until today, it is one of the main aims of the physics society to gain more information about the quantum world and to implement the appearing effects in different scopes of applications. Within this thesis I want to give a closer look insight two experiments, that I have collaborated on over the last year at the Institute for Quantum Optics and Quantum Information in Vienna. The first project, called QUESS, focuses on the exchange of quantum keys via optical satellite-to-ground links, while the second one pursues the goal of closing the freedom-of-choice loophole in a Bell test experiment by the usage of cosmic sources. The following work is structured as follows:

Chapter 2 gives a theoretical introduction in the world of quantum mechanics, whereas the third chapter treats the basic ideas and occurring safety issues of the BB84 protocol for quantum key distribution. In chapter 4 I explain the QUESS experiment and describe in detail the adjustment of a satellite mock-up setup, that was

tested at the optical ground stations in Tenerife and in Graz. The concepts of the EPR paper, as well as John Bell's approach for his famous inequality are discussed in chapter 5. Chapter 6 focusses explicitly on the experimental setup of the planned Bell test experiment with cosmic sources. Beside from the engineering approach, we want to analyze the influence of different random numbers, which are used for the choice of the measurement basis, on the outcome of a Bell test experiment in the laboratory.

Chapter 2

Quantum Entanglement

In the following chapter I will give a short introduction to the theoretical framework of quantum mechanics, which builds the cornerstone of this thesis. Based upon the described concepts, I will also discuss the phenomenon of quantum entanglement.

2.1 Superposition

In the theory of quantum mechanics the state of a system is described by the wave function $|\psi\rangle$. Mathematically seen, we interpret this state as a unit vector in the corresponding Hilbert space. Thus, we can find a basis $|\phi_i\rangle$ with dimension i= 1, ... N, in which the state $|\psi\rangle$ can be expressed as:

$$|\psi\rangle = \sum_{i=1}^{N} c_i \, |\phi_i\rangle \, . \tag{2.1}$$

According to this superposition principle, each state is described as a linear combination of its basis states with complex coefficients c_i fulfilling the relation

$$\sum_{i=1}^{N} |c_i|^2 = 1. \tag{2.2}$$

Each measurement on a quantum system (i.e. an interaction of the system with a classical measurement device) leads to a collapse of the wave function. The outcomes a_i of a measurement are the eigenvalues of an operator of the Hilbert space. The probability of measuring such an eigenvalue is given by the absolute squared projection of the measured state onto the eigenvector k_i of the operator

$$P(a_i) = |\langle k_i|\psi\rangle|^2. \tag{2.3}$$

In the following thesis we will only consider quantum-mechanical two-state systems,

so-called *qubits*, which correspond to the quantum mechanical analogue of the classical bit. In the Dirac notation we can express a qubit as a linear combination of its basis states

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{2.4}$$

As the outcome of the further described experiments mainly depend on the polarization state of photons, we will describe the qubit as a linear combination of two orthonormal polarization states, i.e. we substitute $|0\rangle$ and $|1\rangle$ for $|H\rangle$ and $|V\rangle$. Hence, this photonic qubit can be written in its most general form as

$$|\psi\rangle = \cos\frac{\theta}{2}\,|H\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|V\rangle\,, \tag{2.5}$$

with θ being the zenith and ϕ the azimuth angle for any arbitrary state, that can be visualized on the three-dimensional Poincaré-Sphere (compare figure 2.1).

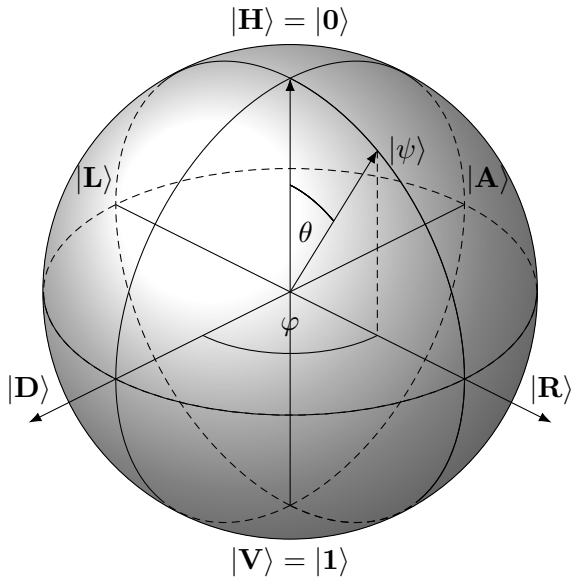

Figure 2.1: The Poincaré-Sphere represents any arbitrary polarization state of a photonic qubit. The axes have been chosen, that horizontal polarization corresponds to the north pole and vertical polarization to the south pole. Rotations around the axes (described by the angles θ and φ) can be accomplished in the experiment by the usage of linear optic devices (e.g. half-wave plates or quarter-wave plates).

In the experiment we can generate any photonic qubit state rather simple by the usage of linear optical devices (e.g. wave plates). The most important polarization states of photonic qubits are quoted in table 2.1.

polarization state	linear combination	named	linear polarization angle
$\|H\rangle$	$\|H\rangle$	horizontal	0°
$\|V\rangle$	$\|V\rangle$	vertical	90°
$\|D\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	diagonal	45°
$\|A\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	anti-diagonal	135°
$\|R\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle + i\,\|V\rangle)$	right-handed circular	-
$\|L\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle - i\,\|V\rangle)$	left-handed circular	-

Table 2.1: Table of the most important polarization states of photonic qubits.

2.2 Entanglement

In order to introduce the concept of entanglement, we consider N noninteracting systems with corresponding Hilbert spaces - their composite quantum system can be described by a Hilbert space, that is formed by the tensor product of its N subsystems

$$\mathcal{H} = \bigotimes_{i=1}^{N} \mathcal{H}_i. \tag{2.6}$$

Assuming $N = 2$ (i.e. a composite system of two qubits) we can build four states, that form an orthonormal basis to the corresponding four-dimensional Hilbert space:

$$\begin{aligned} |\psi\rangle^{\pm} &= \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 \pm |V\rangle_1 |H\rangle_2) \\ |\phi\rangle^{\pm} &= \frac{1}{\sqrt{2}}(|H\rangle_1 |H\rangle_2 \pm |V\rangle_1 |V\rangle_2). \end{aligned} \tag{2.7}$$

These states cannot be written as a tensor product of their subsystem states, i.e. they are not separable. In quantum mechanics such states are called *entangled*.
The above quoted states are better known as the so-called *Bell states*. These states are maximally entangled, which means that the measurement of only one qubit will lead to absolutely random results (i.e. we measure $|H\rangle$ and $|V\rangle$ with the same probability of $\frac{1}{2}$), but a joined measurement of both qubits will always show perfect correlation for $|\phi\rangle^{\pm}$ and anti-correlation for $|\psi\rangle^{\pm}$. Many experiments have shown, that the strength of these correlations does not change over distance [1, 2, 3, 4], which is also known as quantum non-locality.

2.3 No-cloning theorem

In 1982 Wooters and Zurek have been the first one to show, that it is neither possible to generate a perfect copy of an arbitrary unknown quantum state of a qubit nor to amplify a qubit onto a different one, without disturbing the original qubit [5]. This phenomenon is better known as the *no-cloning theorem*. Assume, we are able to use a copying device, which creates an exact copy of an input qubit i onto an output qubit o. The operations of such a device can be formulated as:

$$\begin{aligned} |0\rangle_i |0\rangle_o &\rightarrow |0\rangle_i |0\rangle_o \\ |1\rangle_i |0\rangle_o &\rightarrow |1\rangle_i |1\rangle_o . \end{aligned} \tag{2.8}$$

If we consider the input qubit to be in a superposition state $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, the copying device would generate an entangled state

$$\frac{1}{\sqrt{2}}(|0\rangle_i + |1\rangle_i) |0\rangle_o \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_i |0\rangle_o + |1\rangle_i |1\rangle_o), \tag{2.9}$$

which clearly differs from the desired output state

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle_i + |1\rangle_i) |0\rangle_o \rightarrow \frac{1}{\sqrt{2}}(|0\rangle_i + |1\rangle_i)\frac{1}{\sqrt{2}}(|0\rangle_o + |1\rangle_o) = \\ \frac{1}{2}(|0\rangle_o |0\rangle_i + |0\rangle_o |1\rangle_i + |1\rangle_o |0\rangle_i + |1\rangle_o |1\rangle_i). \end{aligned} \tag{2.10}$$

Although we can see, that it is impossible to create a deterministic quantum cloning device, there are at least probabilistic cloning strategies, which achieve a successful cloning probability of $\frac{5}{6}$ [6].

Chapter 3

Quantum Key Distribution

The classical cryptography is a branch of information science, which aims for the secure rendering of messages between two authorized parties (usually called *Alice* and *Bob*), while preventing any eavesdropping attack by a third party (*Eve*). In general, a message is encoded through additional information from a readable to a desultory state, which is known as the key. Typically, it should not be possible to crack the message without the knowledge of the corresponding key. Today's state of the art is the usage of complex mathematical algorithms in order to encrypt messages. These cryptosystems divide into two classes, depending on whether Alice and Bob use the same key to encrypt and decrypt a message - *symmetric (secret key) cryptosystem*, or differing keys - *asymmetric (public-key) cryptosystem.*

Presumably, the growing technological progress of quantum information science in computer systems will enable these cryptosystems to become cracked in future with very low time effort compared to now. Thus, the field of quantum cryptography is a growing sector in the field of quantum information and communication. The principles of qubit superposition and entanglement (compare chapter 2) can be beneficially used in order to exchange information between two parties, while instantly recognizing any occurring eavesdropper. Any attempt by Eve for obtaining parts of the secret key will lead to additional errors in a QKD protocol, that can be registered by Alice and Bob, e.g. the usage of a one-time-pad protocol enables such a communication to become unconditional secure.

A one-time-pad protocol demands the key to be absolutely random, which can not be achieved with classical but with quantum systems. Furthermore, the secret key must have the same length as the plain-text and any bit of the key can only be used once [7].

Today's quantum cryptographic systems can be experimentally realized either by weak coherent laser pulses (WCP) [8, 9, 10, 11], entanglement [12, 13, 14] or by continuous variables [15, 16]. In the following sections I will describe the principles of

the famous BB84 protocol for weak coherent laser pulses and for entangled photons, which is the theoretical cornerstone for the QUESS experiment, that is described in more detail in the next chapter.

3.1 Coherent state BB84 protocol

Quantum key distribution systems are not restricted to the usage of single photon sources to generate a secret key. It is difficult to realize them experimentally and in some cases even impractical for QKD. Instead, weak coherent laser pulses are used to generate a quantum signal, where the electromagnetic field can be approximated by a monochromatic coherent state with a narrow spectral width. Those single pulses from a weak coherent laser source follow a Poissonian distribution with the probability of having n photons in one pulse

$$P_\mu(n) = \frac{\mu^n}{n!} e^{-\mu}, \tag{3.1}$$

where μ corresponds to the mean number of photons in one pulse and can be adjusted via the laser intensity of the emitter. As it is beneficial to keep the probability of multi-photon emission per pulse as low as possible, μ is usually chosen to be below 1.

In 1984 Bennett and Brassard developed the BB84 protocol, which enables the encoding of classical bits by four different qubits from two mutually unbiased bases [17]. In their work these qubits are described by different polarization states, where $|H\rangle$ and $|D\rangle$ correspond to a binary 0, while $|V\rangle$ and $|A\rangle$ are assigned with 1. Furthermore, the two chosen bases have to be complementary, with the properties:

$$\begin{aligned} \langle H|D\rangle = \langle V|D\rangle = \langle H|A\rangle = \langle V|A\rangle = \frac{1}{\sqrt{2}} \\ \langle H|V\rangle = \langle D|A\rangle = 0. \end{aligned} \tag{3.2}$$

As shown in figure 3.1, Alice sends single photons to Bob, which were randomly prepared in either of the four polarization states, and notes her basis choice. The receiver Bob also chooses randomly one of the two complementary bases $|H, V\rangle$ or $|D, A\rangle$ to measure the incoming photon. Hence, Bob obtains a binary key, which is called the raw key. Additionally, Bob also records his measurement basis. In 50% of the cases Alice and Bob have used the same basis, which is leading to an error rate of 25% for the raw key. Both parties exchange via a classical channel (e.g. the internet) their records of the used bases and reject each qubit, that was prepared in a different basis, than it was measured (basis reconciliation). Thereby, Alice's

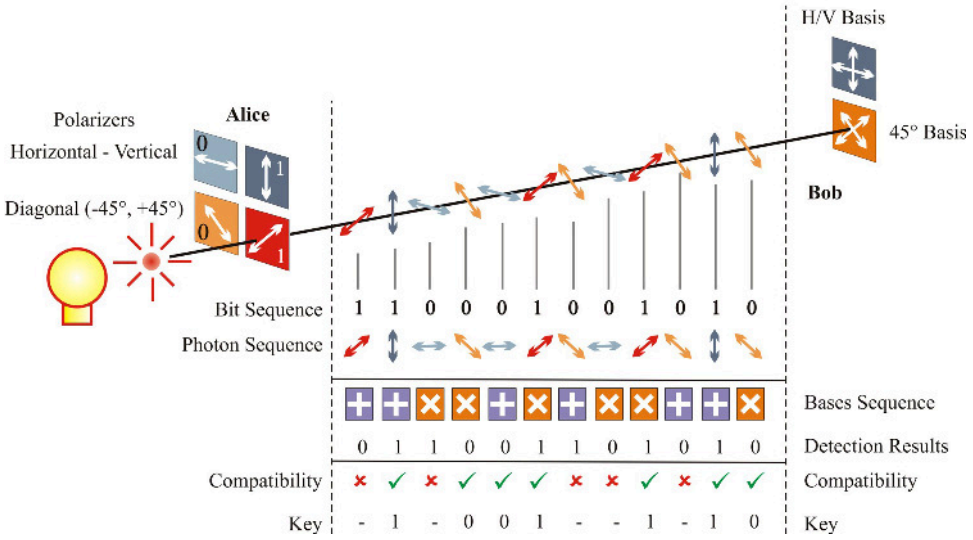

Figure 3.1: Scheme of the coherent state BB84 protocol. Alice emits single photons, which are randomly prepared in one of the four polarization states. Bob measures the incoming photon also randomly in one of the two bases $|H, V\rangle$ or $|D, A\rangle$. After exchanging the selected basis choices, they reject each result, that was measured in a different basis than prepared, leading to the sifted key.

and Bob's retained bit sequence, the so-called sifted key, is identical. Note, that the sole knowledge of the measurement basis does not allow a third party to gain information about the exchanged key.

3.2 Security of the BB84 protocol

In order to guarantee an unconditionally secure key exchange, we have to take into account possible strategies of Eve to disturb the obtained sifted key.
One approach of Eve consists of intercepting some parts of the key. Thereby, Bob's detected bit sequence gets reduced, but it does not compromise the security. Alternatively, Eve could also detect the sent qubit in one of the two complementary bases and resend a copy of the observed state to Bob (intercept-resend strategy). In accordance to the no-cloning theorem Eve only obtains 50% information from the key and increases the error rate in the sifted key by 25% (quantum bit error rate - QBER). The enlarged error rate is registered by Alice and Bob and so they reject the key. In general, Alice and Bob already measure a higher error rate due to inherent noise produced by dark counts and experimental imperfections. Thus, the error can not be distinguished to have come from an eavesdropper or simply from noise. Thereby, all experimental imperfections must be attributed to an eavesdropping attack. In order to reduce the error in the sifted key, the usage of error correction protocols is beneficial. The additional information that an eavesdropper

might have gained from the error correction is erased by a process called privacy amplification [18]. Both procedures result in a shortened sifted key, the secret key, which is unknown to Eve. Shor and Preskill derived a lower bound for the maximal QBER by taking into account any arbitrary eavesdropping attacks possible within the laws of quantum mechanics [19]. The BB84 protocol is secure with a secure key rate of at least $1 - 2H_2(q)$, with q being the QBER in the sifted key and $H_2(q)$ being the binary Shannon entropy:

$$H_2(q) = -q \log_2(q) - (1-q) \log_2(1-q), \tag{3.3}$$

where the secure key rate reaches 0 for $q > 11\%$. A disadvantage of this protocol is that Bob has to ensure, that Alice is not corrupted (in Eve's hand) and therefore he must trust Alice.

Another more powerful method for eavesdropping a quantum key is the photon number splitting (PNS) attack [20, 21, 22]. As described in the previous section weak coherent laser pulses have a probability > 0 to generate more than one photon in a pulse. Eve can make advantage of this fact, by measuring the number of photons Alice transfers to Bob. A measurement of the photon number corresponds to a separate Hilbert space and does not disturb the polarization degree of freedom. With such a *quantum non-demolition measurement* Eve is able to block all pulses that contain a single photon. Whenever she measures more than one photon per pulse, Eve splits one photon off and allocates the rest for the communication between Alice and Bob. Eve keeps all the split photons, waits until Alice and Bob exchange their basis choices and thus, she is able to perform the correct basis measurement on the photons (coherent attack). In order to counteract such PNS attacks one can use so-called decoy-states [23, 8, 9]. Here, additional decoy pulses with different μ, than in the signal pulses are added. As Eve can not distinguish between signal or decoy pulse, she will split off photons from the signal and the decoy states. The different states exhibit different photon number statistics, such that any eavesdropping PNS attack will get recognized by Alice and Bob from the transmission probabilities of the signal and decoy states.

3.3 Entanglement based BB84 protocol

The entanglement based BB84 protocol uses entangled photons instead of attenuated laser pulses to establish a secure key. Those entangled photon pairs are produced e.g. by spontaneous parametric down-conversion (SPDC) in a non-linear crystal and are prepared in the desired Bell state, here $|\psi^-\rangle$. One of the two photons is detected by Alice the other one by Bob, since they share a $|\psi^-\rangle$ state (which

is invariant under polarization rotation), their results show perfect anti-correlation in polarization. In order to achieve a BB84 based protocol, the incoming photons are randomly measured in the $|H, V\rangle$ or $|D, A\rangle$ basis. Experimentally, this can be realized by a 50/50 beam splitter or any active switch. Afterwards, they exchange their basis choice via a classical channel and discard those photons, in which their measurement bases did not coincidence. As the results are perfectly anti-correlated Alice or Bob inverts the bits of the gained key in order to obtain an identical set of bits - the sifted key. As already described for weak coherent laser pulses a secret key of entanglement based QKD can also be extracted by classical error correction codes and privacy amplification. A. Poppe et al. were one of the experimentalists, who have already used such an entanglement based BB84 protocol in a real-world scenario [24]. They exchanged a quantum key produced by an entanglement source, where one photon was measured at the headquarters of the Bank Austria Credit Anstalt and the other one at the City Hall of Vienna.

Chapter 4

Quantum Experiments at Space Scale

The Quantum Experiments at Space Scale (QUESS) project is a collaboration of the Chinese Academy of Science (CAS) and the Austrian Academy of Science (AAS), that wants to establish quantum key distribution according to the BB84 protocol for the first time via a space-earth link from a satellite to optical ground stations. Today, the usage of satellites for free-space quantum communication protocols is the most promising approach to establish a global quantum network, as the key loss is mainly influenced by the propagation of the optical signal through the atmosphere. Although the usage of optical telecom fibers appears to be more feasible, because of the already existing infrastructure, the losses within the fibers and the detection modules are the limiting factors, which do not allow a world-wide quantum key exchange up to now. Based on a cooperation contract, the CAS is responsible for the equipment and the launch of the satellite, while the Austrian Institute for Quantum Optics and Quantum Information will supply three optical ground stations within Europe with receiver modules.
In the following chapter I describe the operating mode of the receiver modules, that are installed at the ground stations. In order to simulate the conditions for a satellite overflight we have tested and adjusted the modules via horizontal free-space links in Graz and Tenerife, whose results are presented at the end of this chapter.

4.1 Satellite setup

The BB84 protocol for quantum key distribution is carried out in the QUESS experiment via an optical link from a satellite to optical ground stations. Although the propagation through the atmosphere is leading to losses of the quantum signal, the *Quantum Key Relay Protocol* should guarantee an unconditional secure key

exchange between two arbitrarily distant ground stations, that are communicating with the same relay.
First, the satellite exchanges a key (K1) with ground station A (e.g. in Europe), while at some later time the satellite generates a different key (K2) with ground station B (e.g. in China). Afterwards, the satellite logically combines both keys with an XOR combination and transmits the result (K0) to both ground stations. Hence, each station can now determine the key of the other station by combining its key with K0, compare figure 4.1

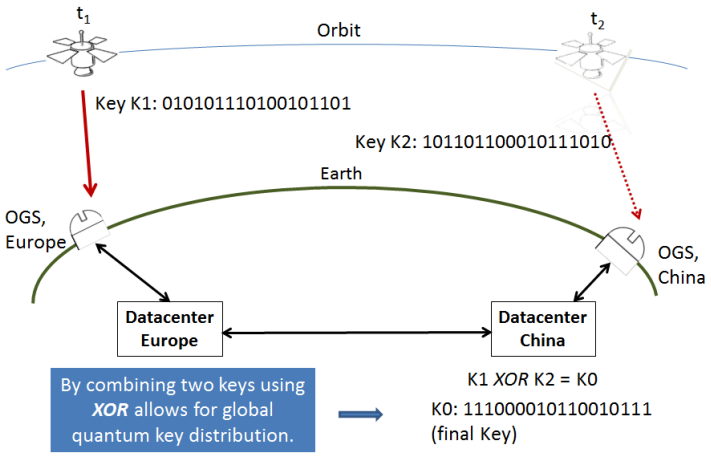

Figure 4.1: Sketch of the planned key exchange between the satellite and two ground stations.

The QUESS satellite will be in a sun synchronous low earth orbit (LEO) at 600 km height and is planned to be equipped with two different photon sources. One is a decoy state source, while the other one uses an entangled photon source. The decoy state source produces randomly polarized attenuated laser pulses (quantum signal) at a wavelength of 850 nm and a repetition rate of 100 MHz. In order to synchronize the clocks of the satellite and the receiver modules, the satellite uses an additional laser, which emits strong laser pulses at a rate of 10 kHz and a pulse length below 1 ns at a wavelength of 532 nm (beacon signal). The usage of a 3 W uplink beacon laser at 671 nm at the ground stations enables a bidirectional tracking with the strong satellite laser.
According to the CAS the launch of the QUESS satellite is scheduled for summer 2016.

4.2 Receiving modules

For the QUESS experiment three different ground stations in Europe (Vienna, Graz and Tenerife) are planned to be equipped with polarization analyzing modules to

enable an optical satellite-to-ground communication. At the ground stations the quantum as well the beacon signal is collected with a telescope and afterwards guided to the polarization analyzing modules, compare figure 4.2. As the telescope in Vienna will be replaced by a bigger version in summer 2016, only the two polarization modules of Graz and Tenerife have been tested by now. The different types of telescopes used at the ground stations are listed in table 4.1.

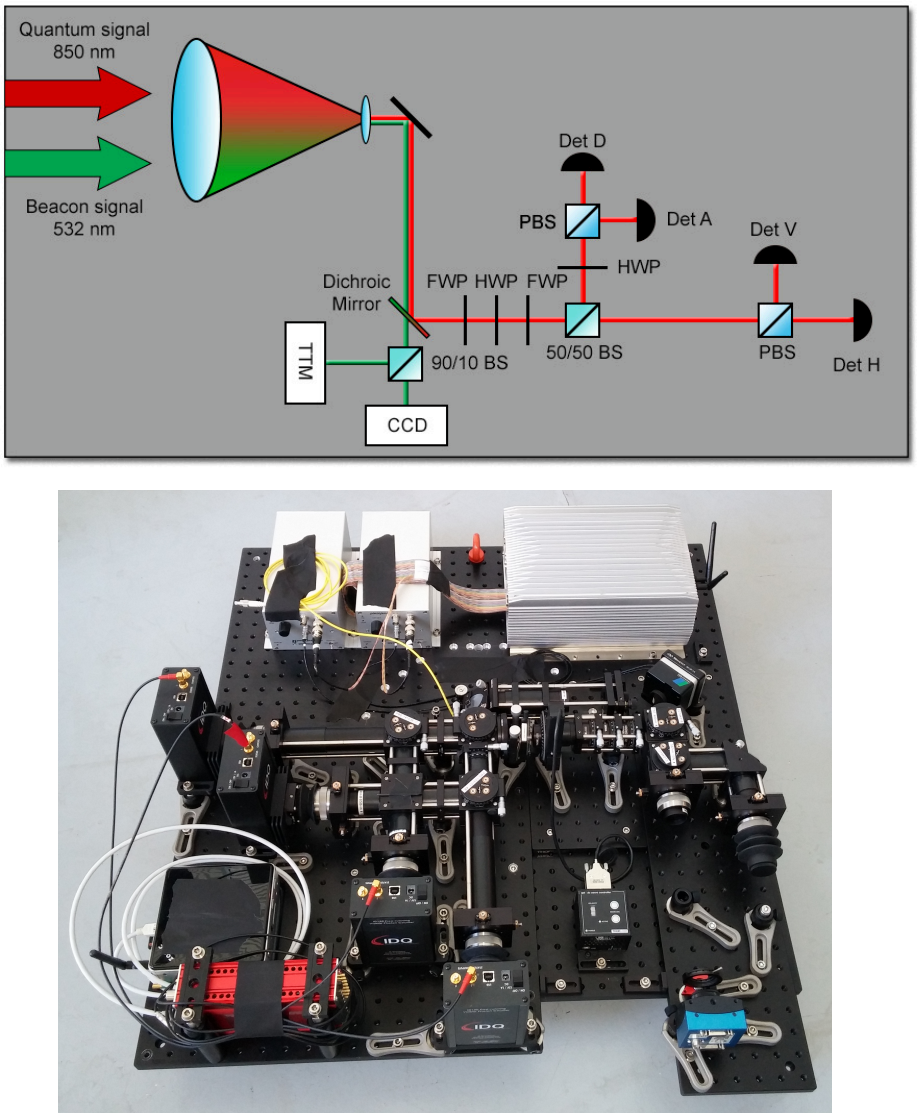

Figure 4.2: Sketch of the quantum and beacon beam propagation in the receiving setup (up) and image of the receiving modules (bottom). For details refer to the main text.

In the analyzation module a dichroic mirror is used to separate the beacon from the quantum signal.

	ø primary mirror	ø secondary mirror	telescope mount type
OGS Vienna	0.30 m	0.12 m	equatorial mount
OGS Graz	0.50 m	0.15 m	altazimuth mount
OGS Tenerife	1.00 m	0.20 m	equatorial mount

Table 4.1: Table of the telescopes used at the three different European Optical Ground Stations

The beacon signal is guided to a 90/10 beam splitter. Thereby, the majority of the beacon signal is focused onto a CCD camera, which is used for tracking purposes. It is necessary to keep the received beacon laser spot on a predefined reference point of the CCD-camera in order to guarantee, that all of the detectors in the quantum path are hit properly. The rest of the beacon signal is fed into a fast detector (transmitted arm), which is connected to a time-tagging unit, that is afterwards used for clock-synchronization.

As the quantum signal should be analyzed randomly in the $|H, V\rangle$ or $|D, A\rangle$ basis, the usage of a 50/50 beam splitter in the quantum analyzation arm is beneficial. The transmitted fraction of the quantum signal propagates to a polarizing beam splitter (PBS). According to their polarization the photons are separated at the PBS and detected at fast avalanche photo diodes. The detected signal corresponds to a measurement in the $|H, V\rangle$ basis. In the reflected arm of the beam splitter the infrared photons first pass a half-wave plate, which rotates their polarization state by 45°. Again, the photons get separated at a PBS and thereby accord to the measurement in the $|D, A\rangle$ basis.

In general, the incident and the reflected beam at a surface of an optical component define a plane, which is called the plane of incidence. Typically, the component of the polarization, which lies within this plane, is termed *p*-polarized, while the component perpendicular to the plane of incidence is called *s*-polarized. Within our receiving module the *s*- and *p*-polarization description corresponds to vertical respectively horizontal polarization. As given in table 2.1, diagonal and anti-diagonal polarization states are expressed as linear combinations of horizontal and vertical polarization, respectively *p*- and *s*-polarization. The reflection of the light beam at an optical device is leading to phase-shifts between the *s*- and *p*-components, i.e. the reflection at an optical device generates disturbances for diagonally or anti-diagonally polarized light, while horizontally or vertically polarized light is not effected. In order to compensate this phase-shift, the usage of devices consisting of birefringent material is beneficial.

The relative orientation between the telescope of the satellite and the telescope of the ground stations alters during a satellite overflight. Thereby, the polarization reference frames of both systems get rotated against each other. In order to compensate

this rotation, we can use a remote-controllable half-wave plate, whose compensation orientation can be determined from the current position of the satellite and the ground station. The half-wave plate only works properly, if the incoming beam is linearly polarized. Thus, we need to use two full-wave plates, which compensate appearing phase-shifts before and after the half-wave plate. The rotation of the wave-plates is chosen such, that the optical axes is parallel to horizontal or vertical polarization, while the tilt of the wave plate is adjusted in order to compensate the unwanted phase-shifts.
In Tenerife the telescope is not constructed for tracking LEO satellites, as the dynamical pointing error would lead to a loss of the signal within the field of view of the detectors. Thus, a fast tip/tilt mirror system is used to compensate the pointing error.

4.3 Satellite signal simulation

Before the satellite is operated in its orbit, we have to guarantee that the analyzation modules at the ground stations are optimally aligned. Thus, we have built up a satellite mock-up setup that generates beacon and quantum signals, that we expect from the satellite. In order to simulate the influence of atmospherical turbulences, we have tested the alignment on horizontal free-space links. On the Canary Islands we have adjusted a horizontal link of 143 km between the islands of Tenerife and La Palma, while the link distance in Graz was about 6 km. Within these link distances we should achieve a similar atmospherical influence, that we would expect from future satellite-to-ground links.
The principal setup, that is used for our satellite mock-up, is shown in figure 4.3. In order to simulate the quantum signal we have used an ultra-short pulsed light source at a wavelength of 850 nm, which enables maximal repetition rates of 100 MHz[1].
In order to set a desired polarization state, the laser pulses are guided to a PBS. The transmitted horizontally polarized component of the pulses is coupled into a polarization maintaining fiber. As the decoy state source at the satellite uses weak coherent laser pulses, we have to attenuate the infrared pulses of our setup. Thus, we use a polarizer in front of the PBS in order to set our incoming amount of horizontally polarized photons. In addition, the rotation of a half-wave plate is chosen such, that the desired polarization state is coupled into the polarization maintaining fiber. The beacon signal has been generated by a strong 10 kHz pulsed laser at 532 nm[2]. In the real experiment the intensity of the beacon signal collected at the ground stations will reach in the worst case (mainly due to the elevation of the

[1]Hamamatsu PLP-10 Picosecond light pulser: PLP-10-085
[2]Roithner diode pumped solid state laser: MPL-III-532-20mW

satellite) 100 pW/m^2, i.e. in order to prepare for this scenario we have to attenuate the beacon laser to comparable intensity levels. Therefore, we have used multiple neutral density (ND) filters, which had to be calibrated before used. The given attenuation of the ND filters from the manufacturer corresponds to a mean value over the full wavelength spectrum, which will lead to slight deviations for 532 nm. The beacon signal propagates to a 90/10 dichroic mirror, where the majority of the signal is coupled into a fiber, while the rest is focused onto a fast diode, which is connected to a time-tagging unit in order to check the signal strength and the repetition rate.

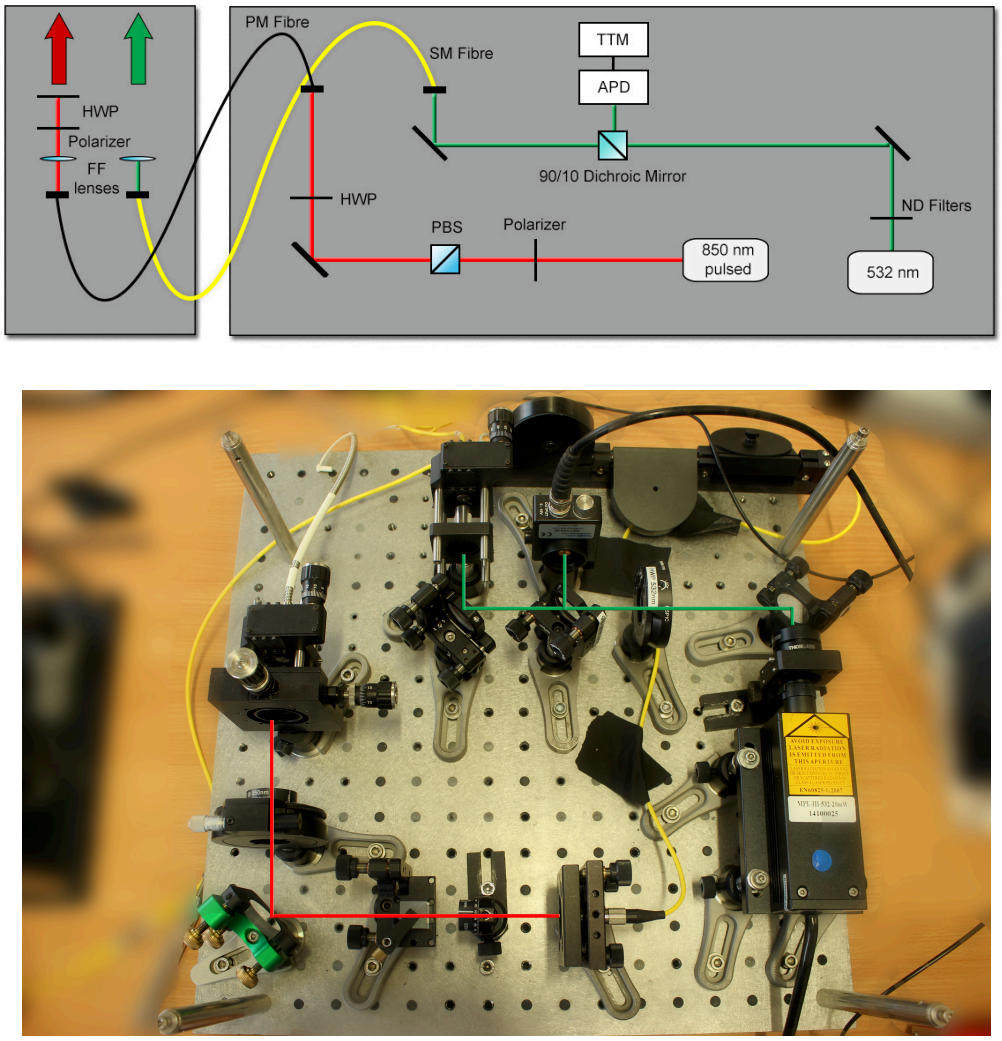

Figure 4.3: Scheme (up) and image (bottom) of the satellite mock-up setup. The quantum signal as well as the beacon signal are coupled into fibers and connected to the transmitting modules. Here, both beams are collimated with fixed-focus lenses and the polarization of the quantum signal is controlled with a polarizer and a remote controllable half-wave plate.

The polarization maintaining as well as the single mode fiber are attached to the transmitting module. Both beams are collimated with fixed-focus lenses. In the quantum signal an additional polarizer guarantees linear polarization and a remote controllable half-wave plate is used in order to adjust different polarization states. In La Palma the transmitting module was attached to a platform, where the beam propagation has been adjusted by tilting the mount of the collimating lens, compare figure 4.4.
The optimal degree of tilting has been achieved by scanning over the entire field of view of the receiving module's detectors and readjusting the tilt until the detected count rates are maximized. In contrast to La Palma, the transmitting module of Graz was attached to a telescope mount. Here, the axis of the telescope can be steered manually, until we achieve an optimal signal propagation direction, which corresponds to maximal count rates at the detectors.

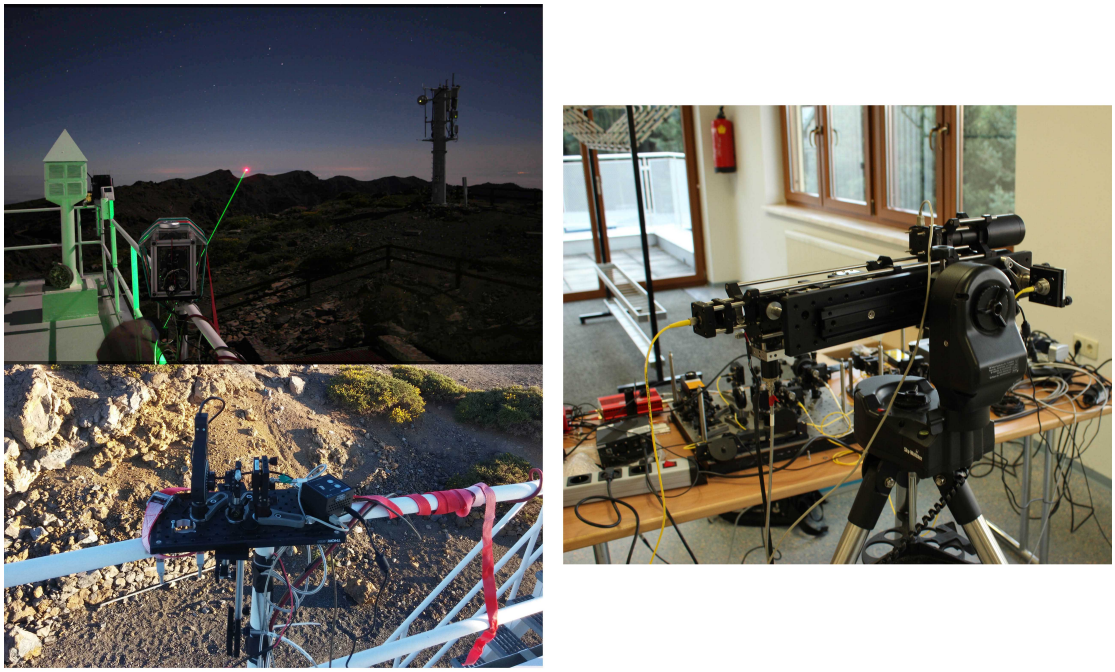

Figure 4.4: Images of the transmitting modules in La Palma (left) and Graz (right).

4.4 Results

After adjusting the satellite mock-up setup properly, the receiving modules have been optimally aligned. By sending different polarization states from the transmitter to the receiving module, it is the main aim to hit all four detectors and to compensate the influence of the divers optical components in the beam path on the polarization,

compare the sketch of the receiving module in figure 4.2. The beam splitter is leading to unwanted polarization phase-shifts in the reflected arm, i.e. it is crucial for a good alignment, that the photons are linearly polarized before they reach the half-wave plate in the $|D, A\rangle$ arm. The figure of merit for adjusting the receiving setup is the contrast, which is given by

$$K_{xy} = \frac{C_x}{C_y}, \tag{4.1}$$

with C_x and C_y being the count rates measured in the polarization state x and the corresponding orthogonal state y.
At first, we want to get rid of unwanted phase-shifts, which appear in the reflected analyzation arm due to the influence of the beam splitter ($|D, A\rangle$ basis). Thus, we insert a polarizer at 45° and tilt the wave plate, until we get rid of the unwanted phase-shifts by maximizing the contrast in the $|D, A\rangle$ basis. Afterwards, we switch the position of the polarizer to horizontal and check the contrast in the $|H, V\rangle$ basis. If the observed contrast is not satisfying enough, it might be improved by rotating the wave plate. Unfortunately, the rotation of the wave plate disturbs again the contrast in the reflected arm, why we have to iteratively change the tilt and the rotation in order to achieve optimal contrasts in both arms.
The same procedure has been carried out for the other wave plate as well, which compensates the polarization phase-shifts that come from the remaining optical devices. Apart from the contrast, another figure of merit is the visibility, which is defined as

$$V = \frac{C_{max} - C_{min}}{C_{max} + C_{min}}, \tag{4.2}$$

with C_{max} being the detected photon count rates in the detector corresponding to the analyzed polarization state and C_{min} the detected counts of the orthogonal polarization state.

4.4.1 Tenerife

The described procedure for the alignment of the receiving module has been performed in Tenerife and in Graz. As it is nearly impossible to completely shield the detectors from background light, we have to consider the dark count events in each detector as well.
In order to determine the contrast and visibility levels of the receiving modules, we use the following strategy - the transmitter prepares the quantum signal in one of the four polarization states, which is sent to the receiver for approximately ten seconds. Then, the beam is blocked and only dark count events are registered by

the detectors. This procedure is revised with each of the four polarization states. Table 4.2 shows the mean count rates, while sending a certain polarization state, as well as the mean dark count rates of the four detectors. In order to determine the error of the count rates, we use Poissonian photon statistics with $\Delta C = \sqrt{C}$.

	H detector [Photons/s]	V detector [Photons/s]	D detector [Photons/s]	A detector [Photons/s]
Dark counts	113 ± 11	119 ± 11	123 ± 11	137 ± 12
H sent	78,811± 281	306 ± 17	41,525 ± 204	42,102 ± 205
V sent	174 ± 13	66,895 ± 259	33,209 ± 182	38,134 ± 195
P sent	39,213 ± 198	37,909 ± 195	68,879 ± 262	318 ± 18
M sent	39,543 ± 199	36,209 ± 190	233 ± 15	72,375 ± 269

Table 4.2: Count rates for optimal alignment in Tenerife.

By subtracting the dark counts from the detected signal events, we achieve the contrasts and the visibilities, that are shown in table 4.3 and figure 4.5. As we can see, the visibilities for the four combinations HV, VH, DA, AD exceed a level of 99%, which corresponds to a very good alignment of our receiving module.

	Contrast	Visibility [%]
HV	422 ± 47	99.53 ± 0.05
VH	1,081 ± 297	99.82 ± 0.05
DA	660 ± 45	99.48 ± 0.06
AD	380 ± 114	99.70 ± 0.05

Table 4.3: Final contrast and visibility for optimal alignment in Tenerife.

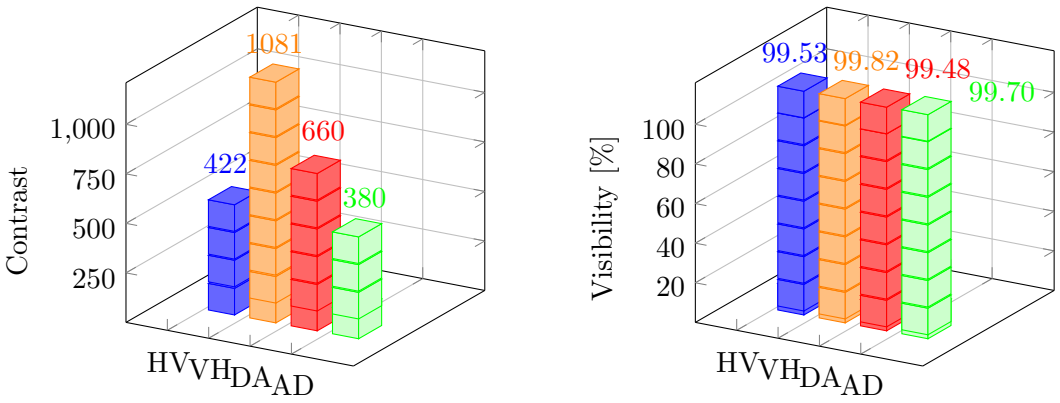

Figure 4.5: Contrast rates (left) and visibilities (right) in the $|H, V\rangle$ and $|D, A\rangle$ basis, measured at the OGS in Tenerife. By achieving visibilities $> 99\%$, we guarantee an optimal alignment of the receiving setup. The corresponding error ranges are given explicitly in table 4.3, as they can not be visualized properly in the plot.

4.4.2 Graz

The same alignment procedure has also been applied to the receiving module in Graz. The results are shown in table 4.5 and in figure 4.6.

	H detector [Photons/s]	V detector [Photons/s]	D detector [Photons/s]	A detector [Photons/s]
Dark counts	218 ± 15	422 ± 21	214 ± 15	162 ± 13
H sent	571,647± 3,589	306 ± 60	307,664 ± 555	193,659 ± 440
V sent	4,216 ± 65	579,656 ± 761	326,400 ± 571	244,286 ± 494
P sent	386,632 ± 622	341,568 ± 584	555,372 ± 745	1,783 ± 42
M sent	429,583 ± 655	370,565 ± 609	2,673 ± 52	437,316 ± 661

Table 4.4: Count rates for optimal alignment in Graz.

Although, we have reached lower contrasts than in Tenerife, the visibility levels still exceed a value of 98%. Consequently, we can conclude, that both receiver modules are optimally aligned and ready for carrying out the planned QUESS experiment.

	Contrast	Visibility [%]
HV	180 ± 4	98.90 ± 0.02
VH	145 ± 2	98.63 ± 0.02
DA	343 ± 9	99.42 ± 0.02
AD	178 ± 4	98.88 ± 0.02

Table 4.5: Final contrast and visibility for optimal alignment in Graz.

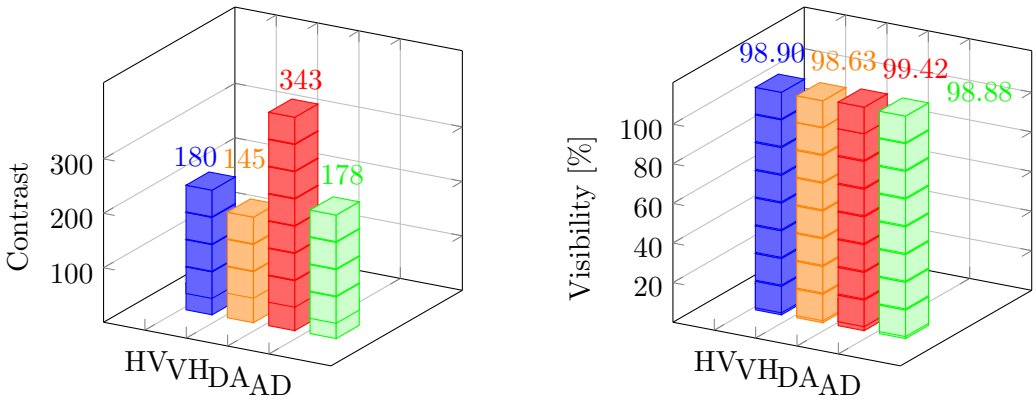

Figure 4.6: Contrast rates (left) and visibilities (right) in the $|H, V\rangle$ and $|D, A\rangle$ basis, measured at the OGS in Graz. As in Tenerife all measured visibilities exceed a value of 98%, which allows the setup to be optimally aligned for the satellite-to-ground communication. The corresponding error ranges are given explicitly in table 4.5, as they can not be visualized properly in the plot.

4.5 Summary

In order to execute the QUESS experiment, we have to guarantee a proper alignment of the receiving modules at the European ground stations in Vienna, Graz and Tenerife. Thus, we have built up a satellite mock-up system, that can be used to adjust the alignment of our receivers respectively to test the quantum and beacon signals on horizontal free-space links. The ground stations of Graz and Tenerife have achieved visibilities $> 98\%$, which correspond to good alignment. In summer 2016 the Viennese ground station will be equipped with a new telescope and the receiving module will also have to be aligned. Additionally, we will check the adjustment of the receiving station in Graz with a satellite mock-up system, that was developed by our Chinese colleagues, before the satellite will be launched in its orbit.

Chapter 5

Quantum Nonlocality

The principles of local realism define our macroscopic world, which obeys the rules of classical physics. Physical objects possess properties that are only influenced by its immediate surrounding at any time and independent of the observation, i.e. measurements are methods to reveil these properties.
The world of quanta does not follow the described classical rules. The outcome of a measurement in quantum mechanics projects the state of an object with a certain probability on an eigenstate of the observable. Measurements of a basis on a superposition state (e.g. a two-level qubit) lead to probabilistic results, that appear to be objectively random. If we consider entangled systems, the measurement outcome of one particle does influence the outcome of the second one, although they can be space-like separated. This weird correlation between the particles is in conflict with our macroscopic world view.
The first scientists, who have identified this phenomenon, were Einstein, Podolski and Rosen in their famous paper of the year 1935 [25]. They raised the question, if the theory of quantum mechanics can become complete. In a thought experiment the scientists have shown, that entangled systems would not accord to the concept on elements of reality, which Einstein famously baptized "spooky action at a distance". In order to prevent quantum mechanics from being an incomplete theory, they believed in additional variables or "hidden" variables to the observers, that should enable a hypothetical completion of quantum mechanics.
Aside from Niels Bohr, who has been an opponent of this publication, the world of science did not further pursue the EPR argument more carefully over the following years. In 1964 (roughly 30 years after the publication of the EPR paper) John Bell proved, that such a complete theory of quantum mechanics with additional local variables could not exist. Clauser, Horn, Shimony and Holt (CHSH) have even showed ways to test Bell's prediction experimentally. A lot of effort from many scientists has been applied to successfully violate the Bell-inequality in the experiment,

but still there may exist so-called *loopholes*, which would allow all experimental violations to be explained by local realistic models.
This chapter will give a review on the EPR paradox as well as a comparison of the results of Bell's theorem with concepts of local realism. Finally, I will discuss three different kinds of loopholes that need to be closed in order to extenuate the influence of local realism in the results of the Bell inequality.

5.1 EPR paradox

In their 1935 published paper Albert Einstein, Boris Podolsky and Nathan Rosen set up three assumptions for physical theories to become complete [25]:

- **completeness:** *"every element of the physical reality must have a counterpart in the physical theory."*
- **elements of reality:** *"if, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of reality corresponding to this quantity."*
- **locality:** *"if two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done to the first system."*

In a thought experiment, that is based on two position-momentum entangled particles, the physicists claimed, that quantum mechanics would not be a complete theory. Assume this two-particle system is space-like separated with the wave function

$$\psi(x_1, x_2) = \int_{-\infty}^{+\infty} e^{(\frac{2\pi i}{h})(x_1 - x_2 + x_0)p} dp, \tag{5.1}$$

where x_1 and x_2 correspond to the positions of the particles and x_0 is some constant. If an observer measures the position x of particle 1, the state of particle 2 is projected onto the position eigenstate $x + x_0$. Thus, the position measurement on one particle guarantees to predict the position of the second particle in an entangled system, without interacting with the second particle. According to the EPR criteria the positions of both particles are elements of reality.
This means, that an observer could measure the position of one particle and the momentum of the second spatially separated particle. Hence, we could predict two eigenvalues from the position and the momentum operator, which are in quantum mechanics non commuting. Here, we definitely get in conflict with quantum theory, since it is not possible to measure the position and the momentum of a particle arbitrarily precise (Heisenberg uncertainty principle).

In 1957 David Bohm referred to the EPR paper in a thought experiment with entangled spin-$\frac{1}{2}$ particles [26]. As this thesis considers polarization entangled photons, I will use the polarization-entangled analogue in order to describe Bohm's work.
Assume, we have the maximally entangled two-photon state:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1 |V\rangle_2 - |V\rangle_1 |H\rangle_2) = \frac{1}{\sqrt{2}}(|D\rangle_1 |A\rangle_2 - |A\rangle_1 |D\rangle_2), \tag{5.2}$$

where both photons are spatially wide separated. The $|\psi^-\rangle$ state is characterized to be invariant under rotations, i.e. independent from the basis measurement of particle 1, we will always find perfect anti-correlation for the second particle. If an observer measures particle 1 in a certain basis, photon 2 will be with certainty in the orthogonal state, when measured in the same basis. Still one has to reconsider that the observer has the free choice to measure the particle either in the $|H, V\rangle$ or in the complementary $|D, A\rangle$ basis. Thus, the outcome of photon 2 in any basis is predetermined without even disturbing it. In accordance to EPR, those complementary states of particle 2 are simultaneous elements of reality. This statement is in strict contradiction with quantum mechanics, as the certain outcome of a measurement in a basis will lead to completely random results in the complementary basis, i.e. in quantum mechanics two complementary states can never be simultaneous elements of reality.

5.2 Bell's theorem

After the publication of the EPR paper in 1935 it took nearly 30 years in order to find a proof for describing quantum mechanics with a theory of local hidden variables. It was John S. Bell, who came up with a theory in 1964, where he generally disproved EPR's approach of a local hidden variable theory [27]. In his argumentation, Bell considers a pair of spin-$\frac{1}{2}$ particles in the singlet spin state, moving in opposite directions:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1 |\downarrow\rangle_2 - |\downarrow\rangle_1 |\uparrow\rangle_2), \tag{5.3}$$

with $|\uparrow\rangle$ and $|\downarrow\rangle$ corresponding to the eigenstate of the spin in z-direction with the eigenvalue +1 respectively -1. Furthermore, Bell assumes, that neither the measurement orientations, nor the results of the measurement devices, can influence each other.
The derivation of Bell's inequality (which can be taken from [27]) results in

$$|E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{c}})| \leq 1 + E^{lhv}(\hat{\mathbf{b}}, \hat{\mathbf{c}}), \tag{5.4}$$

where E^{lhv} corresponds to the expectation value for a joined measurement of two particles. The inequality is fulfilled by any local hidden variable model and is independent of the measurement direction. In quantum mechanics it is maximally violated, if we choose the units vector such that $\hat{\mathbf{a}} \cdot \hat{\mathbf{c}} = 0$ and $\hat{\mathbf{a}} \cdot \hat{\mathbf{b}} = \hat{\mathbf{b}} \cdot \hat{\mathbf{c}} = \frac{1}{\sqrt{2}}$. Hence, we obtain by inserting into equation 5.4

$$\frac{1}{\sqrt{2}} \leq 1 - \frac{1}{\sqrt{2}}. \tag{5.5}$$

From this approach Bell concluded, that theories containing hidden variables in quantum mechanics must have a non-local mechanism, where a measurement device show instantaneous influence on the results of a distant measurement device.

5.3 CHSH inequality

In his inequality John Bell assumes perfect correlation (a perfectly pure $|\psi^-\rangle$ state) as well as a detection efficiency of 100 %, which is hardly feasible in a real experiment. Based on Bell's inequality Clauser, Horn, Shimony and Holt derived an approach, which is not limited through perfect correlation and detection efficiencies [28]. A rigorous derivation is given in [29], which is leading to the CHSH inequality:

$$S^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}, \hat{\mathbf{a}'}, \hat{\mathbf{b}'}) := |E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}'})| + |E^{lhv}(\hat{\mathbf{a}'}, \hat{\mathbf{b}'}) + E^{lhv}(\hat{\mathbf{a}'}, \hat{\mathbf{b}})| \leq 2 \tag{5.6}$$

For the conditions $\hat{\mathbf{a}} = \hat{\mathbf{b}}$ and $E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{a}}) = -1$ the CHSH inequality becomes the original form of Bell's inequality. Restricting our unit vectors to lie in one plane of a three dimensional space, we can substitute them with the corresponding angles α, β, α' and β', leading to a quantum mechanical expectation value $E^{qm}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) = -\cos(\beta - \alpha)$. By choosing $\alpha = 0°$, $\beta = 45°$, $\alpha' = 90°$ and $\beta' = 135°$ we achieve the strongest violation of the CHSH inequality with

$$\begin{aligned} S^{lhv}(\alpha, \beta, \alpha', \beta') &= |-\cos(45°) + \cos(135°)| + |-\cos(45°) - \cos(-45°)| \\ &= |-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}| + |-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}| = 2\sqrt{2} \geq 2. \end{aligned} \tag{5.7}$$

5.4 Loopholes

Naively seen, any violation of the Bell inequality would show, that quantum mechanics is not compatible with local realistic theories. In fact, there is still enough room for conspiracy theories with so-called *loopholes*, which allow the violation to be explained by a local realistic theory. Among the multiplicity of possible loopholes there are two loopholes, that are directly connected to the derivation of the Bell inequality and one that occurs due to detection inefficiencies at the experiment. It is the main aim of the experimentalists to close most of these loopholes. In the next subsection I will give an overview of these three loopholes.

5.4.1 Locality loophole

In the EPR paper locality has been characterized by the fact, that if "*two systems no longer interact, no real change can take place in the second system in consequence of anything done to the first system*" [25]. Jon P. Jarrett divided locality into two different categories [30]. The first one considers the *outcome independence*, which guarantees that the outcome of a measurement on one system does not influence the result of a different space-like separated system. The other category corresponds to the *setting independence*, which does not allow the choice of the measurement settings on one system to influence the outcome of another system.
According to the rules of special relativity (the maximal velocity of a signal is limited by the speed of light) both locality categories can be closed in the experiment by space-like separating every measurement event on one side from the measurement as well as the setting choice on the other side.

5.4.2 Freedom-of-choice loophole

If the setting choice of our measurement device can be influenced by a hidden variable, which defines the properties of the entangled particles or vice versa, we speak of the freedom-of-choice loophole. In order to close this loophole Bell has already suggested to space-like separate the measurement devices and to choose the setting on each side at the last second, before the measurement is carried out [29]. Todays technology enables this loophole to be closed in the experiment by the usage of fast random devices, which determine the measurement settings in a Bell test. It is still crucial, that the output of these devices is truly random. Up to now, the freedom-of-choice loophole makes the plausible assumption, that any hidden variables, that might influence the choice of the measurement settings, are created simultaneously with the entangled particles of the source. Thus, one has to to space-like separate the decision of the measurement settings from the particle emission of an entanglement source in order to close the freedom-of-choice loophole. Nevertheless, one can argue

that the measurement settings have been pre-determined by processes different from the source emission, i.e. any processes from the past could possibly influence the creation of the entangled particles in the source as well as the measurement setting choices.

5.4.3 Fair-sampling loophole

A loophole, that arises in order to experimental imperfections, i.e. a loss in particle collection and detection, is the so-called fair-sampling loophole. As only a fraction of produced particles is observed, this subensemble might not be representative [31]. Local realistic theories with hidden variables can be settled in a way, that the detected subensemble is leading to a violation of the Bell inequality, while the whole system would fulfill it. As showed by Garg and Mermin in 1987, an overall detection efficiency of at least 82.8% is already sufficient to close the fair-sampling loophole in experimental Bell tests using the CHSH inequality [32].
By using non-maximally entangled states, such as for polarization entangled photons

$$|\psi^-\rangle = \frac{1}{\sqrt{1+r^2}}(|H\rangle_1 |V\rangle_2 + r\,|V\rangle_1 |H\rangle_2) \tag{5.8}$$

with $0 \leq r \leq 1$, Eberhard derived a Bell-type inequality, where the fair-sampling loophole can be closed with overall detection efficiencies of at least 66.7% with no background noise [33]. More generally speaking, the lower limit of the detection efficiency for closing the detection loophole depends on the level of background noise, the measurement settings and an adaption of the variable r to the actual efficiency of the setup.

Chapter 6

Towards a "Cosmic Bell" Experiment

Up to date numerous Bell test experiments have been executed, which can close either individual loopholes or several loopholes at the same time [34, 35, 36, 1]. In the last couple of years some of these experiments have proven, that the locality, the freedom-of-choice and the fair-sampling loophole can be closed simultaneously in systems using photon entanglement [37, 38] and electron-spin entanglement [39]. As mentioned in the previous chapter, under the common assumption that hidden variables only appear within the photon production in the source, the freedom-of-choice loophole can be closed by space-like separating the random choices of Alice's and Bob's measurement basis from the creation process of the source photons. Nevertheless, supporters of local hidden variable theories will cling to the freedom-of-choice loophole, as both, the creation process of entangled photon pairs at the source and the measurement setting choices, can still be influenced by hidden variables, which might have been created even before the actual experiment has been carried out. Thus, one has to either rely on the true randomness of todays quantum random number generators, or one has to use random number generators, which are causally disconnected until far in the past.

As proposed by Gallicchio, Friedman and Kaiser [40] cosmic light sources from the very back corners of the universe (e.g. quasars) can be utilized to generate the random basis choice in a Bell test. Quasars are highly energetic and distant objects, that were created shortly after the universe became transparent. If one uses two light emission signals from space-like separated quasars, the decision of the bases settings has been settled 13.8 billion light years ago. Such a "cosmic Bell" experiment would imply a new milestone to exhaust the limits of any hidden local realistic mechanism in the world of quantum mechanics.

A collaboration between the above quoted authors of the "cosmic Bell" paper and

the Institute for Quantum Optics and Quantum Information in Vienna pursue the main goal of performing such a cosmic Bell experiment in the coming years. Before executing the final stage of the experiment with quasars, in a first approach it is beneficial to carry out a Bell test over the rooftops of Vienna, using the light of distant stars as random number generators.

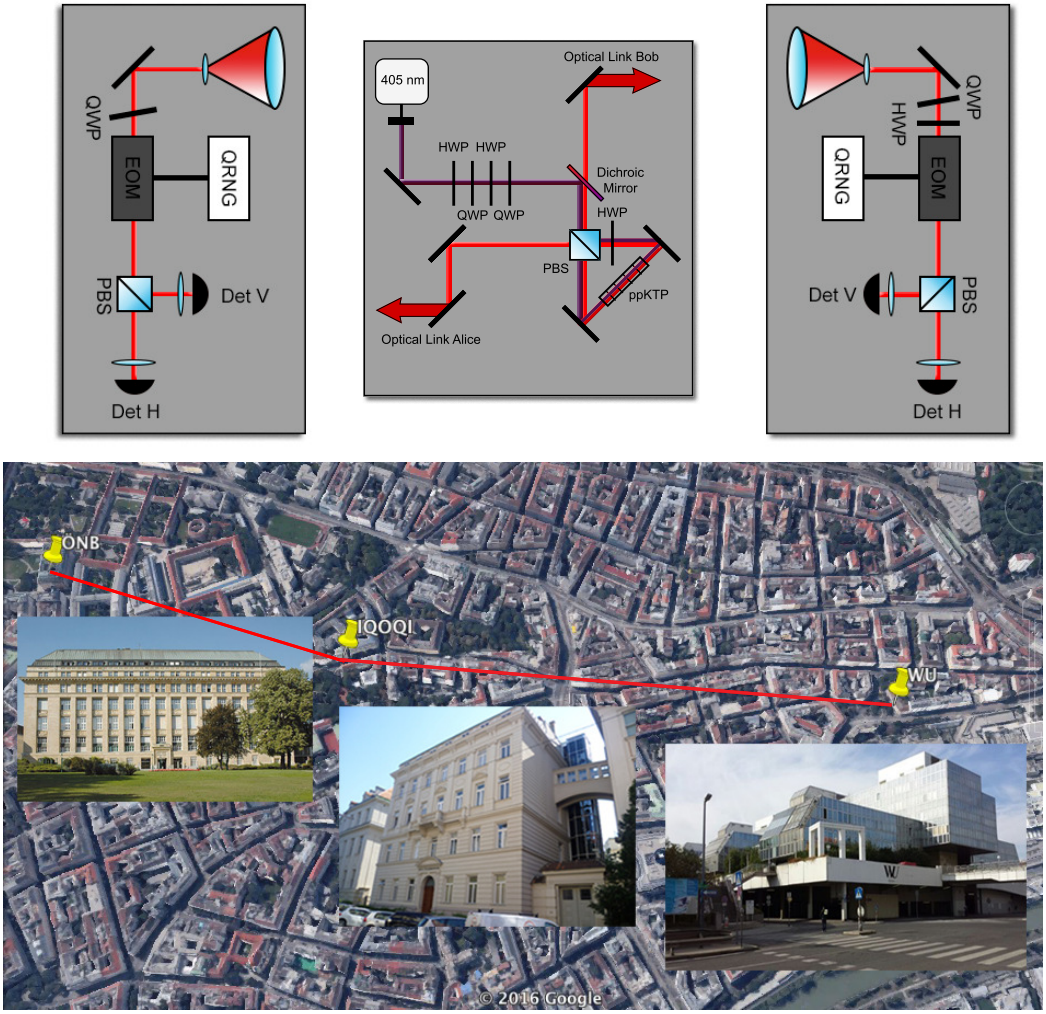

Figure 6.1: Illustration of the planned Bell test experiment, which uses star light as random number generator. The polarization entangled photons are created at the IQOQI Vienna and sent via optical links to the receiver stations. Alice's receiver module is located 0.6 km away from the source at the Austrian National Bank, while Bob's analyzation module is situated at the the former building of the economic university of Vienna (distance to IQOQI 1.2 km).

The entangled photons are created at the institute building and sent via optical free-space links to two opposite situated receiver stations at the Austrian National Bank (ÖNB) and the main building of the former university of economy (WU) in

Vienna. The setup of this Bell test is shown in figure 6.1. The distance between the source and the receiving stations is not identical (distance source - ÖNB 570 m and source - WU 1.18 km). Hence, this asymmetric arrangement has to be reconsidered in the corresponding choices of stars in order to guarantee an appropriate space-like separation. At the receiving stations the photons get collected and a test of the CHSH inequality can be carried out. Therefore, we have to properly align and test the receiving stations in the laboratory at first. In the following chapter I will describe the components of the experimental setup as well as their alignment in detail. Finally, we want to test the alignment of our modules in Bell tests with different random number sources. Furthermore, we want to study, whether the choice of our random numbers does effectively influence the outcome of our experiment.

6.1 The entangled photon source

6.1.1 Spontaneous parametric down conversion

One of the most common and efficient methods to create entangled photon pairs is the usage of spontaneous parametric down conversion (SPDC), describing a second-order non-linear process in crystals [41]. SPDC processes can be considered as the polarization response P of a non-linear medium on an external electric field. Thus, we can write the polarization response as

$$P_i = \epsilon_0[\chi_{ij}^{(1)} E_j + \chi_{ijk}^{(2)} E_j E_k + \chi_{ijkl}^{(3)} E_j E_k E_l + ...], \tag{6.1}$$

with ϵ_0 being the vacuum permittivity and $\chi^{(n)}$ the n^{th} order susceptibility of the non-linear medium.
In quantum optics the down-conversion is described by a three particle process, where high energy pump photons with frequency ω_p create pairs of entangled photons, called signal ω_s and idler ω_i photons. All particles are subject to the conservation of energy and momentum, satisfying the so-called *phase-matching* conditions

$$\omega_p = \omega_s + \omega_i \qquad \text{and} \qquad \hat{\mathbf{k}}_\mathbf{p} = \hat{\mathbf{k}}_\mathbf{s} + \hat{\mathbf{k}}_\mathbf{i}. \tag{6.2}$$

Depending on whether the polarization of signal and idler photons are identical or orthogonal to each other, we speak of type-I or type-II SPDC.
The interaction Hamiltonian of the SPDC process can be described quantum mechanically by using second quantization of the electrodynamic fields. These quantized fields are given by

$$E_j^{(-)} = \epsilon_j \int_V d^3r a_{j,k}^\dagger(\omega_j) e^{i(\hat{\mathbf{k}}_\mathbf{j}\hat{r} - \omega_j t)}, \tag{6.3}$$

where $a^{\dagger}_{j,k}$ is the creation operator with j corresponding either to the signal or idler field and k being the corresponding polarization mode. In contrast to the output modes the pump field can be treated classically

$$E_p^{(+)} = \epsilon_p e^{i(\hat{\mathbf{k}}_\mathbf{p}\hat{r}-\omega_p t)}. \tag{6.4}$$

Hence, we can write the interaction Hamiltonian as

$$\hat{\mathcal{H}}_I = \epsilon_0 \int_V d^3r \chi_2 E_p^{(+)} E_s^{(-)} E_i^{-} + \text{H.c.}. \tag{6.5}$$

For collinear phase-matching (i.e. $\hat{\mathbf{k}}_\mathbf{p} \mid\mid \hat{\mathbf{k}}_\mathbf{s} \mid\mid \hat{\mathbf{k}}_\mathbf{i}$), the signal and idler state are given by

$$|\psi(\omega_s,\omega_i)\rangle = \int d\omega_s d\omega_i \delta(\omega_p-\omega_s-\omega_i)\text{sinc}\left(\frac{\text{L}\Delta\text{k}}{2}\right) \text{a}^{\dagger}_{\text{s,V}}(\omega_\text{s})\text{a}^{\dagger}_{\text{i,H}}(\omega_\text{i})\,|0\rangle\,, \tag{6.6}$$

with $|0\rangle$ being the initial vacuum state, L the length of the nonlinear medium and Δk the phase-mismatch.

Typically bulk nonlinear crystals have a transversal walk-off between signal and idler beams in type-II SPDC processes, which can be compensated by positioning the crystal axis for a given wavelength under an appropriate angle. This technique is better known as birefringent phase matching. The source in our experiment uses a periodically poled crystal, which is composed of alternating domains with poling period Λ. Thereby, the phase-matching condition is expanded by an additional term

$$\hat{\mathbf{k}}_\mathbf{p} = \hat{\mathbf{k}}_\mathbf{s} + \hat{\mathbf{k}}_\mathbf{i} + \frac{2\pi}{\Lambda}. \tag{6.7}$$

This process is also called quasi-phasematching and is used to facilitate the generation of collinear signal and idler beams. In the experiment the quasi-phasematching can be adjusted by an oven, which controls the desired crystal temperature.

6.1.2 Sagnac source of polarization entangled photons

In our experiment the process of SPDC has been used in a polarization Sagnac interferometer, where a periodically poled potassium titanyl phosphate $KTiOPO_4$ (pp-KTP) nonlinear crystal is used for generating polarization entangled photons. The Sagnac source has been assembled and adjusted by my colleague Dominik Rauch. In this thesis I will only briefly describe the functionality of this source.

The input pump laser, chosen at a wavelength of 405 nm, is guided to a polarizing beam splitter (PBS) building the interferometer input. The horizontally polarized component of the pump beam is transmitted at the PBS, while the vertically polar-

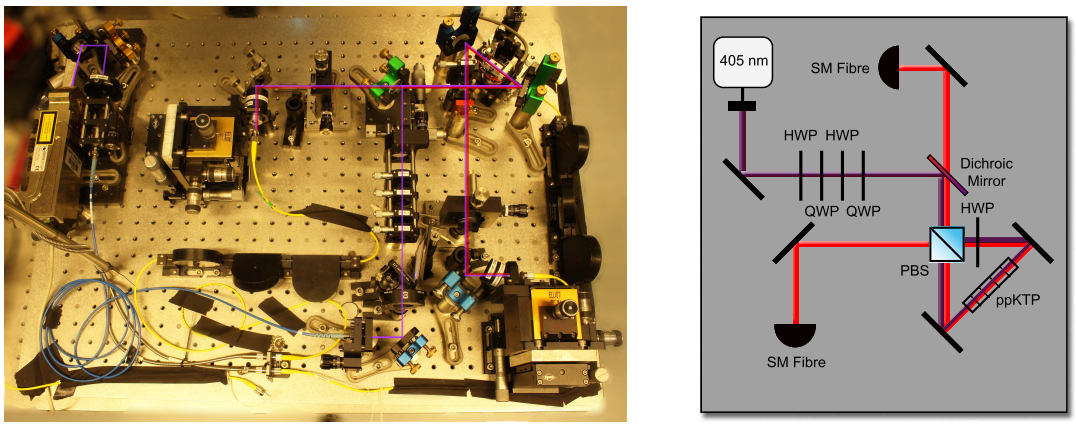

Figure 6.2: (left) Image of the entire source setup used for the generation of entangled photons. (right) Sketch of the most important devices used in the polarization Sagnac interferometer. Ultraviolet laser light is focused onto the ppKTP crystal, which produces pairs of signal and idler photons. According to the propagation direction in the Sagnac loop and their polarization, the photons are transmitted or reflected at a PBS and guided to the analyzation modules. A more detailed description of the Sagnac source can be taken from the main text.

ized component is reflected. $|H\rangle$ polarized photons propagate in the counterclockwise direction of the interferometer and are focused onto the crystal. In the crystal the process of SPDC generates a signal and an idler photon at a wavelength of 810 nm with $|H\rangle_s$ and $|V\rangle_i$ polarization. Afterwards, a half-wave plate rotates the polarization of the photons by 90°. The signal and idler photons propagate back to the PBS and leave it according to their polarization through two different outputs. The photons are coupled into two single mode fibers, which are then guided to the receiving modules.

Contrarily, vertically polarized pump photons, that propagate through the interferometer in clockwise direction, are rotated by the half-wave plate, before creating an additional pair of signal and idler photons. Thus, we obtain a set of horizontally and vertically polarized photons in each output arm of the PBS. With an optimal alignment we erase the "which path" information of the photons and generate the entangled state:

$$|\psi_\phi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_i |V\rangle_s + e^{i\phi} |V\rangle_i |H\rangle_s), \tag{6.8}$$

where the indices i and s correspond to the signal and idler component fraction of the pump beam. In order to adjust the phase ϕ of the entangled state, we have used a set of quarter-, half- and quarter-wave plates. An additional half-wave plate generates the fraction of horizontally or vertically polarized pump beam photons,

that reach the PBS.

6.2 The receiving modules

In order to investigate the violation of the CHSH inequality, the entangled photons are coupled into single mode fibers, which will then be sent via optical free-space links to the two analyzation (receiving) modules, that are located at the ÖNB (Alice) and the main building of the former university of economy (WU) in Vienna (Bob). Before the actual Bell test can be carried out at our receiving stations, we have to align and test the setup in the laboratory. The setup of our receiving modules can be taken from figure 6.3.

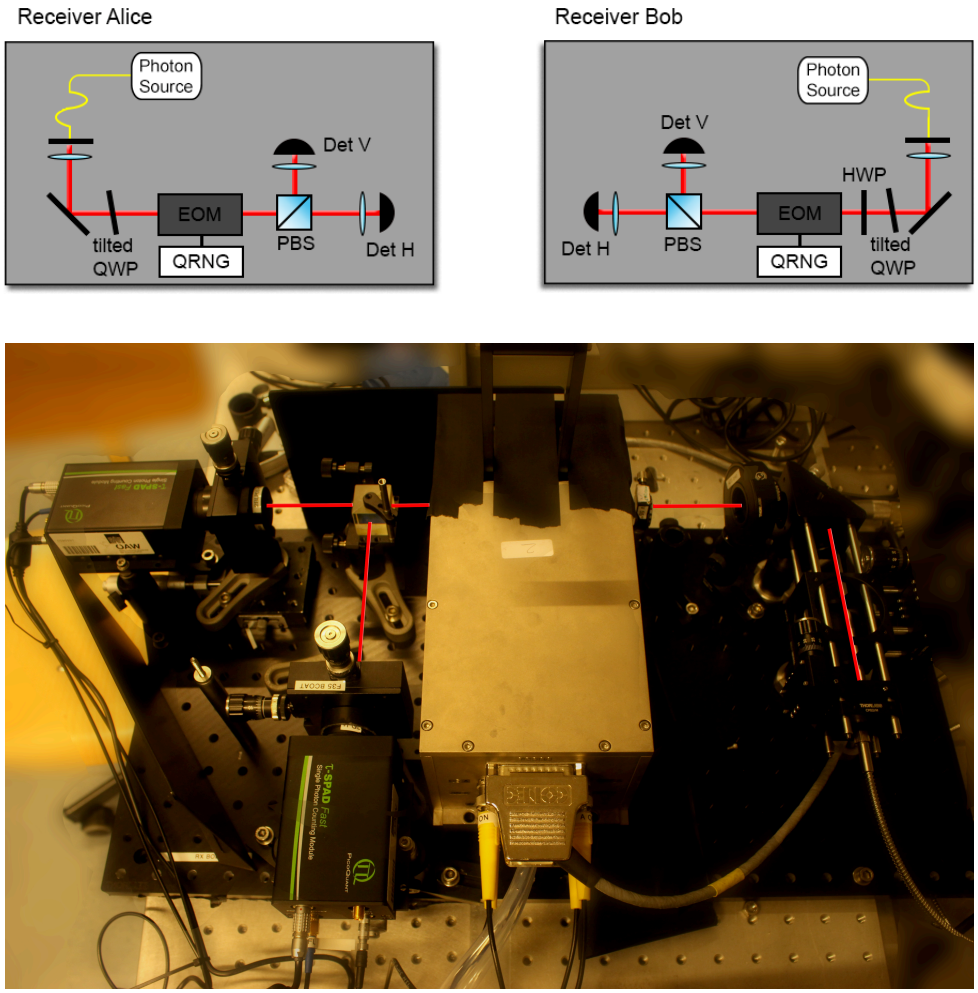

Figure 6.3: Sketches and image of the receiving modules Alice (left) and Bob (right).

In the real experiment the entangled photons have to be collected on each receiving side by a collecting lens (focal length of 40 cm). Additionally, a dichroic mirror

branches off light from a beacon laser, that is focused onto a CCD-camera chip and can be used for tracking the beam position. The entangled photons are not influenced by the dichroic mirror and propagate through the analyzing setup.
In the lab-test we use fixed-focus lenses to directly couple the entangled photons into our receiving modules. In order to simplify the alignment of the setup at the beginning with higher photon count rates, we have used an 810 nm attenuated continuous wave laser before optimizing the adjustment of the setup with entangled photons from the source.
The coupled laser light is collimated and propagates through the electro-optical modulator (Pockels cell). At a polarizing beam splitter the polarization of the photons is analyzed by coupling the transmitted and reflected photons into our detectors. In the following subsections I will describe the individual components of the receiving setups.

6.2.1 Electronics

Single photon detectors

The used detectors (τ-*SPAD-FAST*) are actively quenched silicon avalanche photodiodes (APDs) with a quantum efficiency at a wavelength of 810 nm between 20% and 40% and an active area of 500 μm. The detectors have been chosen, as they offer a very good timing resolution of 150 ps - 400 ps (depending on the wavelength) and a low dark count rate < 200 cps. On each receiving module we use two detectors that are placed in the transmitting (H detector) and the reflecting arm (V detector) of the PBS. The incoming photons are focused onto the active area of the detectors, where they are transferred into 20 ns long nuclear instrumentation module (NIM) electronic signals, that are fed into the FPGA logic.

FPGA logic

The choice, in which measurement basis the source photons are analyzed, depends on our quantum random number generator (QRNG). Different QRNG sources for testing the CHSH inequality are treated in detail in chapter 6.3. The interface between the choice of our actual measurement basis and the generation of corresponding Pockels cell signals is enabled by the usage of a field programmable gate array (FPGA) logic. Here, the QRNG signal is connected to the input signal of the FPGA board and four different output channels are connected to the corresponding inputs of the Pockels cell.
Additionally, the FPGA logic possesses two input ports, that are connected with the detectors. Each incoming signal from a detected photon produces a time stamp, that can be time-delayed within the software of the FPGA logic. Furthermore, the soft-

ware enables the analyzation of coincidence counts, i.e. two photons from different inputs get detected within a chosen coincidence window. By internally time-delaying the signals to each other, we can build for instance coincidences, where only photons have been taken into account, that passed the Pockels cell in the switching mode (compare section 6.2.3).

6.2.2 Polarizing beam splitter (PBS)

In order to analyze the polarization of the incoming photons we use a polarizing beam splitter (PBS). In the lossless case only horizontally polarized photons are transmitted at the PBS, while vertically polarized get reflected. Thus, the detected photons are directly analyzed in the $|H, V\rangle$ basis (i.e. an arbitrary polarization state of the incoming beam is dismembered into its H and V fraction at the PBS). For analyzing the photon polarization states in a different orthonormal basis (e.g. the $|D, A\rangle$ basis), it is convenient to rotate the polarization, before the photons reach the PBS. In the experiment this is achieved by the usage of wave-plates and electro-optic modulators.
As we want to reach a good contrast between the transmitting and the reflecting arm, the PBS has to be well aligned. At first, we fix the PBS on a two axis tip-tilt mount such, that the beam hits the PBS centered. Furthermore, we tilt the up-down axis until the back-reflections of the PBS coincidence with the incoming beam. In order to improve the contrast we place a polarizer in H position in front of the PBS and measure classically the beam power in both arms. By tilting the left-right axis of the mount, we are able to minimize the output power in the reflected arm. By applying this procedure, we achieve in both receiving modules contrasts C_R/C_T of approximately 1/700, which accords to good alignment.

6.2.3 Electro-optic modulator

For the experiment it is essential to use a device, which enables a fast switching of the measurement basis in order to close the freedom-of-choice loophole. The utilization of an electro-optic modulator (EOM) emerges to be beneficial, as it can be used as a retardation plate, which rotates the polarization of the transiting beam, when an electric field is applied. Usually the EOM is a crystal, whose refractive index n changes in dependance of the electric field as [42]

$$n(E) = n_0 + aE + bE^2 + ... \tag{6.9}$$

with n_0 being the refractive index for $E = 0$ and a respectively b being electro-optic constants. The linear variation of the refractive index with the electric field is better known as the Pockels effect, which only occurs in crystals that lack a

center symmetry. The Pockels effect can be well described by the modification of the indicatrix ellipsoid

$$\Delta\eta_i^2 = \Delta\left(\frac{1}{n_i}\right)^2 = \sum_{j=1}^{3} r_{ij}E_j, \tag{6.10}$$

with η_i being the impermeability matrix and r_{ij} the electro-optic matrix. By considering the crystal's main axis system the impermeability matrix has diagonal form. Thus, when no field is applied we can write the refractive index ellipsoid as

$$\frac{x^2}{n_o^2} + \frac{y^2}{n_o^2} + \frac{z^2}{n_e^2} = 1. \tag{6.11}$$

Here, we assume a uniaxial crystal with $n_x = n_y = n_o$, $n_z = n_e$ and $n_o \neq n_e$, which corresponds to typical Pockels cells.

The thereby associated phase change of the polarization of light, that propagates through the crystal, is called Pockels electro-optical effect and is used in so-called Pockels cells. By applying an electric field the elements of the entire impermeability matrix get modified and the indicatrix changes to

$$\begin{aligned}\left[\frac{1}{n_o^2} + \Delta\left(\frac{1}{n_1^2}\right)\right]x^2 + \left[\frac{1}{n_o^2} + \Delta\left(\frac{1}{n_2^2}\right)\right]y^2 + \left[\frac{1}{n_e^2} + \Delta\left(\frac{1}{n_3^2}\right)\right]z^2 \\ +2\left[\Delta\left(\frac{1}{n_4^2}\right)\right]xy + 2\left[\Delta\left(\frac{1}{n_5^2}\right)\right]yz + 2\left[\Delta\left(\frac{1}{n_6^2}\right)\right]xz = 1.\end{aligned} \tag{6.12}$$

It is possible to define a new reference system (x', y', z') in which the impermeability matrix gets diagonal again after the crystal is stressed by an electric field. The change of the refractive index can be taken from figure 6.4. When $E = 0$ the polarization of the light, that travels along the optical axis (z-axis) does not change (the intersection of the indicatrix with a plane perpendicular to the optical axis is a circle with radius n_o), while for E $\neq$ 0 the rotation of the reference frame leads to different velocities of the x' and y' polarization component. Thus, the crystal becomes birefringent and the polarization of the incoming light is rotated, i.e. the crystal acts as a retardation plate.

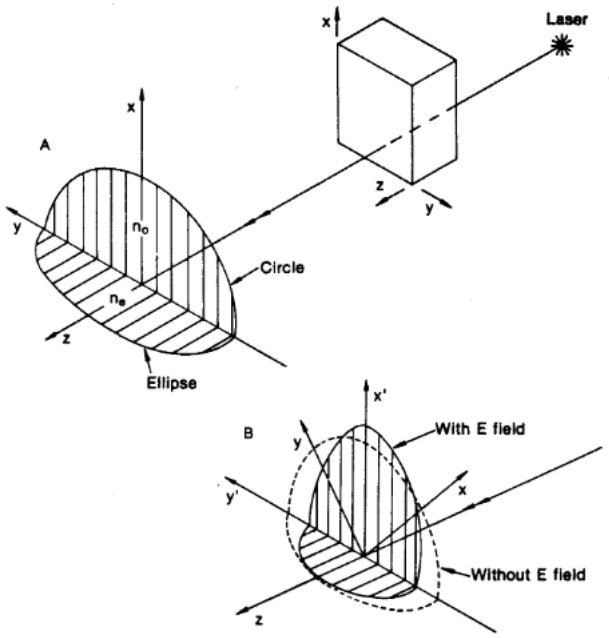

Figure 6.4: Illustration of the Pockels effect [43]. (top) When no electric field is applied, the x and y component of linearly polarized light travels with same velocity $v_x = v_y = c/n_0$ and no birefringence appears along the z-direction. (bottom) When $\mathrm{E} \neq 0$, the rotational symmetry gets lost and the intersection of a plane perpendicular to the z-direction with the indicatrix corresponds to an ellipse. Thus, the velocities of the x' and y' polarization components $v_{x'} = c/n_{x'}$ and $v_{y'} = c/n_{y'}$ differ from each other, i.e. birefringence appears. Both components get superimposed at the end of the crystal, which is leading to a rotation of the initial polarization of the beam.

The used Pockels cell

Each receiving module is equipped with a pair of Rubidium Tytanyl Phosphate (RTP) crystals. The crystals are cut such that the optical path does not overlap with the optical axes but with the crystallographic y-axes. As we use two sequently placed RTP crystals that are rotated against their z-axes by 90° to each other, any birefringence in the optical path is compensated, as long as no external field is applied in the z-direction. The change of polarization can be achieved by the strength of the electric field as well as the rotation of the Pockels cell crystal along the optical path.

Pockels cell driver

The Pockels cell driver consists of an optical head, which contains a high-voltage switching circuit. The chosen model from Bergmann Messgeräte offers high repetition rates as well as fast on- and off switching with low jitter. The state of the system can be controlled by four signals *A-On*, *B-On*, *A-Off*, *B-Off*. Whenever the

driver should apply an electric field to the Pockels Cell, the signals have either to be *A-On* and *B-Off* or *B-On* and *A-Off* (depending on whether applying positive or negative voltage). In order to preserve the Pockels cell from ion wandering effects (i.e. the Pockels cell is in switching mode for longer times), that could easily destroy the crystal, the supplied voltage changes alternately from positive to negative and vice versa. Each time *A* and *B* are both *On* or *Off*, the switching mode is suppressed. The electronic delay between a produced electric signal at the FPGA board and the time until the voltage is applied to the crystal was measured to be approximately 80 ns. Additionally, the optical head is connected with a chiller in order to cool the Pockels cell for high duty cycles.

Alignment of the crystal

The Pockels cell is placed on a four axis tip-tilt mount, which enables a precise adjustment of the crystallographic axes system. As described, it is crucial for the alignment of the crystal, that the optical path is parallel to the crystallographic y-axes. In a first step we try to set our optical path in a way, that the beam travels centered through the Pockels cell. By illuminating the crystal with divergent light, we can see the shadow of the Pockels cell, which simplifies adjusting the beam in the center of the shadow. Furthermore, we use the tip-tilt mount to adjust the position of the crystal such, that any back-reflections of the Pockels cell overlap with the incoming beam. By iteratively applying those two procedures, one can set the basic position of the Pockels cell.

Alignment of the $|H,V\rangle/|D,A\rangle$ Basis

By supplying the Pockels cell with an external electric field, it should act as a half-wave plate that is oriented at 22.5°. This behavior can be achieved by the rotation of the Pockels cell around the optical path as well as the strength of the applied electric field. In order to enable the adjustment during the switching a splitter box was used to supply the Pockels cell with an external 100 kHz trigger signal (continuous switching would damage the Pockels cell), i.e. every 10 μs the Pockels cell changes to the switching state for 100 ns. The detected photons as well as the external trigger signal create time stamps at the FPGA board.
At first, we want to align the beam propagation direction with the crystallographic y-axes. Therefore, we insert a polarizer in H or V polarization position in front of the Pockels cell. When no electric field is applied to the Pockels cell, the incoming polarization state must not be influenced. Thus, we minimize the count rates on the V respectively H detector by changing the tilt of the crystal's mount.
By changing the polarizer position to diagonal, the switching would create an excess

of photons at the H detector, while in the ideal case no photon reaches the V detector, i.e. if the Pockels cell is in switching mode we have a high contrast between the H and the V detector, while both detectors are balanced when the Pockels cell does not switch. In the delay histogram, which can be taken from figure 6.5, we can clearly see the change of the count rates of photons that pass the Pockels cell, while it is switching. Thus, we adjust the rotation of the crystallographic y-axes as well as the strength of the electric field by minimizing the switched photon counts on one detector.

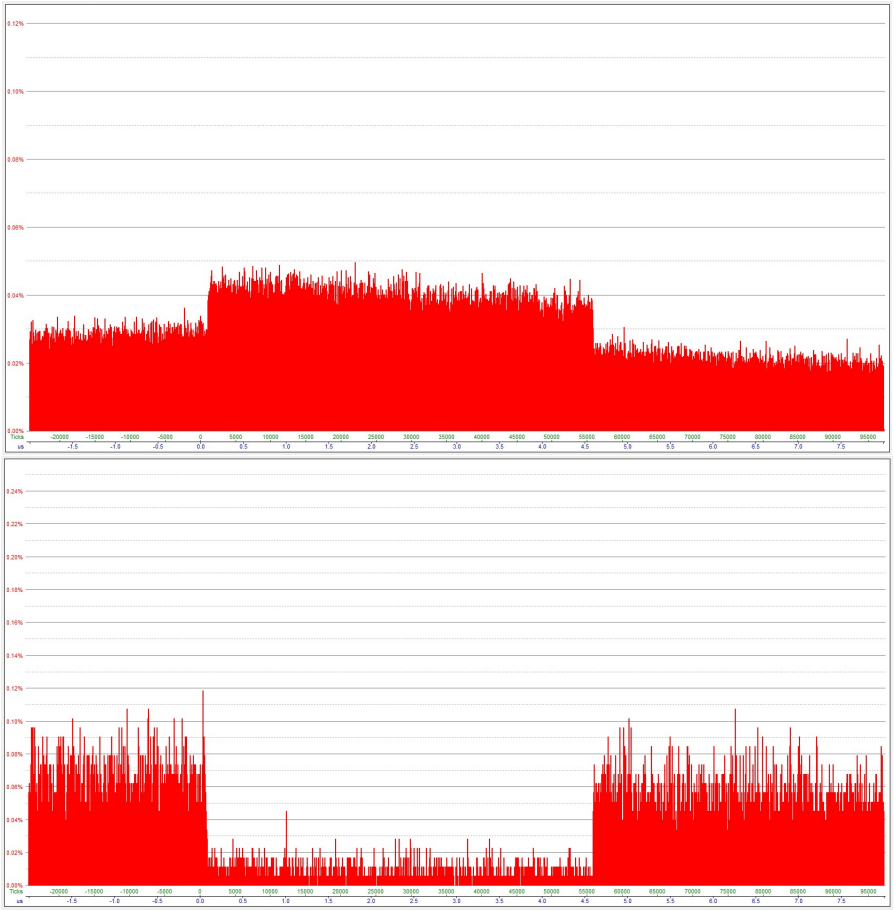

Figure 6.5: Delay histogram of detected photons, while the Pockels cell is in switching mode. In the diagrams the x-axes corresponds to the time delay between the detected photons and the trigger signal, which is supplied to the Pockels cell, and the y-axes to the number of detected photons. Before the photons reach the Pockels cell, they are prepared to diagonal polarization. Photons, which propagate through the Pockels cell, while a voltage is applied, lead to an excess of photons, that are detected at the H detector (upper histogram), while the count rates at the V detector decrease (picture below). Photons, that are not effected by the Pockels cell switching, are randomly equal distributed on both detectors.

Since the alignment of the switching in the $|D, A\rangle$ basis influences the result in the $|H, V\rangle$ basis, we have to revise these steps several times until the contrast in both bases finally converges.

Characterization of the Pockels cell

In order to characterize the switching behavior of the Pockels cell, we have used a pulsed laser beam at 850 nm, which was triggered at 100 kHz. Additionally, a delay line box is placed in between the trigger output channel and the splitter box input. Thereby, we can delay the switching mode of the Pockels cell with respect to the generated laser pulses. We place again a polarizer at diagonal position in front of the Pockels cell and measure coincidences between the trigger signal, that supplies the Pockels cell, and the detected photons from the pulsed source. Stepwise we can manipulate the time-delay of the Pockels cell trigger signal with respect to the laser pulses. Thereby, we can determine the switching time of the Pockels cell from the changing coincidence rates of the H and V detector. The measured contrast between the H and V coincidence rates as a function of the time delay of the trigger signal, that is fed into the Pockels cell, is shown in figure 6.6.

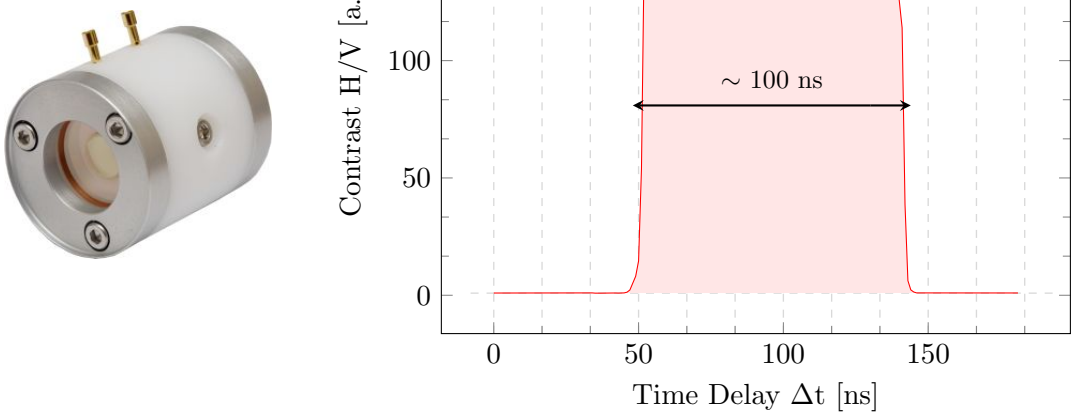

Figure 6.6: (left) Used Pockels cell (right) Switching behavior of the used Pockels cell. The Pockels cell is in switching mode for approximately 100 ns. While the optical rising time of the applied electric field takes approximately 10ns, the drop of the applied field is immediately.

The Pockels cell is switching for a time period of 100 ns, which corresponds to a duty cycle of 1 %. Furthermore, we see, that the Pockels cell takes approximately 10 ns of optical rising time, until the applied electric field is leading to a maximal

contrast in the switching mode. When the field is turned off, the contrast drops immediately, which is a typical behavior for the used crystal. As the used crystal material is piezoelectric, we have to be aware of possible resonance frequencies, that could damage the crystal. By periodically applying voltage in resonance, the piezoelectric effect causes mechanical vibrations in the crystal. These vibrations influence the optical properties of the crystal and can be observed in the "swinging" count rates in both detectors. In the experiment the star light will not produce perfectly periodic signals. Thus, the piezoelectric effect should not be a crucial limiting factor. By generating periodic rectangle signals with a function generator, we have found the resonance to appear at frequencies of approximately 100 kHz, compare figure 6.7.

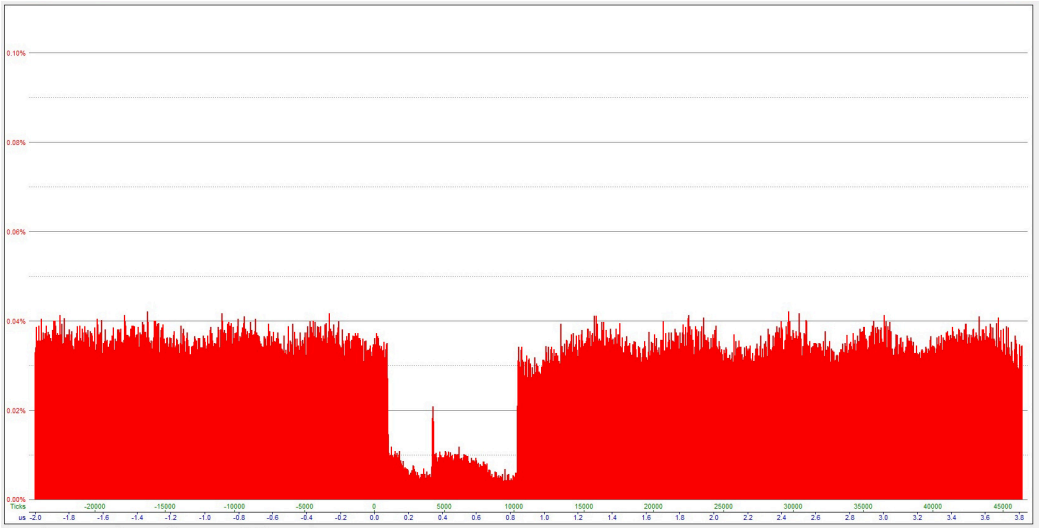

Figure 6.7: Detected photons while the Pockels cell is switching with resonant frequency. Due to the piezoelectric effect mechanical vibrations can appear in the crystal, which are leading to a "swinging" behavior of the count rates, when the voltage is applied in resonance.

Alignment for single photons from the source

As we have adjusted our Pockels cell with an attenuated continuous wave laser, we want to fine tune in a next step the alignment of the Pockels cell with single photons from the entangled source. Thereby, we pump unidirectional into the Sagnac interferometer, which generates a pair of photons, where one photon is directly sent to a detector, while the other one is coupled into the receiving module.
From classical measurements we have determined the losses within the receiving module to correspond to 20%. By forming coincidence pairs within a time window of 2 ns between directly detected photons from the source and photons that propagate through the receiving module, we remark an additional loss of approximately 30%.

This behavior can be concluded from a worse quantum efficiency of our receiver module detectors at a wavelength of 810 nm, compared to the ones that directly detect the source photons.
By optimally aligning both receiving modules for single photons from the source, we achieve maximal contrasts in the $|H, V\rangle$ and the $|D, A\rangle$ basis of approximately 50/1. Thereby, we have set a coincidence window of 60 ns in order to guarantee, that the source photons pass the Pockels cell, while it is in switching mode. Though these contrast values are already sufficient for carrying out the cosmic source experiment, we still suppose even higher contrast values by subtracting accidental coincidences from background counts. Thus, we achieve contrasts in both bases that exceed a level of 100/1.

6.2.4 Adjustment of a polarization reference frame

As a last step in the adjustment of our receivers, we have to establish a common polarization reference frame in both analyzation modules. Therefore, we utilize a fiber polarization controller, or so-called "bat ears", which are attached to the fibers, that connect the source with the corresponding receiving module. In principle, these "bat-ears" are the fiber technological counterpart to a sequence of quarter-, half- and quarter-wave plates and consist of three different coils of fiber. The fiber in the middle coil is twisted twice in order to mimic a half-wave plate, whereas the other coils are only twisted once. All three coils can be rotated around the axis of the input and the output fiber, which enables the tuning of the polarization.
In order to fix our reference frame we place a polarizer in horizontal position right before coupling into the fibers, that are connected with the receivers. Subsequently, we want to maximize the contrast between the H and V detector by rotating the coils of the "bat-ears". In a next step we have to optimize the contrast in the $|D, A\rangle$ basis, without changing the $|H, V\rangle$ contrast. Therefore, we place a retardation plate in front of the Pockels cell, while supplying the receiver with horizontally polarized source photons. The retardation plate is rotated until the contrast in the $|H, V\rangle$ basis is maximized, i.e. the retardation plate does not influence the $|H, V\rangle$ basis. As a next step we change the polarizer to diagonal position. As the FPGA board internally differs photons, that are influenced by the Pockels cell switching, we can adjust a good contrast in the $|D, A\rangle$ basis by tilting the retardation plate. This procedure has been tested with different types of retardation plates. As a best choice has served the usage of quarter-wave plates. Finally, we set a half-wave plate at 11.25° in Bob's receiver module right after the tilted quarter-wave-plate in order to test a maximal violation of the CHSH-inequality.

6.3 Generation of random numbers

In the modern age of technology the usage of random numbers is not only restricted to the field of lottery, but it is essential in many other scopes of applications as in cryptography, computer simulations or in communication. Although random numbers play an important role in our everyday technological life, there is still the question in the room, what characterizes a sequence of numbers being random? There are several statistical approaches, that can test a sequence of numbers on their degree of randomness in form of predictability, but an answer of this question has not been found and will not be further traced in this thesis.
Nevertheless, quantum mechanical processes have already been successfully used in order to generate random numbers, which come close to our ideal conception of random numbers and could replace the so far applied pseudo-random numbers from deterministic algorithms.
The phenomenon of randomness is one of the limiting factors for closing the freedom-of-choice loophole in a Bell test. Our random numbers define, in which polarization basis (e.g. $|H, V\rangle$ or $|D, A\rangle$ basis) we carry out the photon measurement. We can interpret the polarization basis settings as bit sequences, where our nomenclature has been chosen that "0" corresponds to the $|H, V\rangle$ basis, while "1" defines the measurements in the $|D, A\rangle$ basis.
In the following section I will describe the generation process of different types of true and pseudo-random numbers and compare their degree of randomness with divers statistical tests. Furthermore, we want to use these random numbers to analyze the influence of different types of random numbers on the outcome of a Bell test.

6.3.1 Random numbers from cosmic sources

As shortly explained in the introduction of this chapter, the usage of cosmic sources as QRNG in a Bell test lends itself as a beneficial method to suppress approaches of local hidden variable theories in quantum mechanics. In this "cosmic Bell" test incoming light from quasars, that was emitted 13.8 billion years ago, should serve as QRNG. As quasars are very distant objects, they have high red-shifts. Their emission spectra are rather wide, which can be used for the measurement basis choice. According to the wavelength (energy) of the incoming photons from the quasars, they are either transmitted or reflected at a dichroic mirror and focused onto two detectors. Hence, we choose our binary "0" and "1" values in accordance with the responding detector signal. Technically and infra-structurally it is challenging to execute a Bell test with quasars. As the incoming photon flux is rather low, one has to use big telescopes to collect and couple the quasar light into fibers, that are connected to the random number detection module. Furthermore, one has to clar-

ify, that the incoming photons do not originate from different sources (e.g. nearby stars).
Before handling the challenge of generating random numbers from quasars, we will feed our random number detection module with star light at first. Each receiving spot (Alice and Bob) is equipped with a telescope, that collects photons from different space-like separated stars. The setup of the QRNG module is shown in figure 6.8.

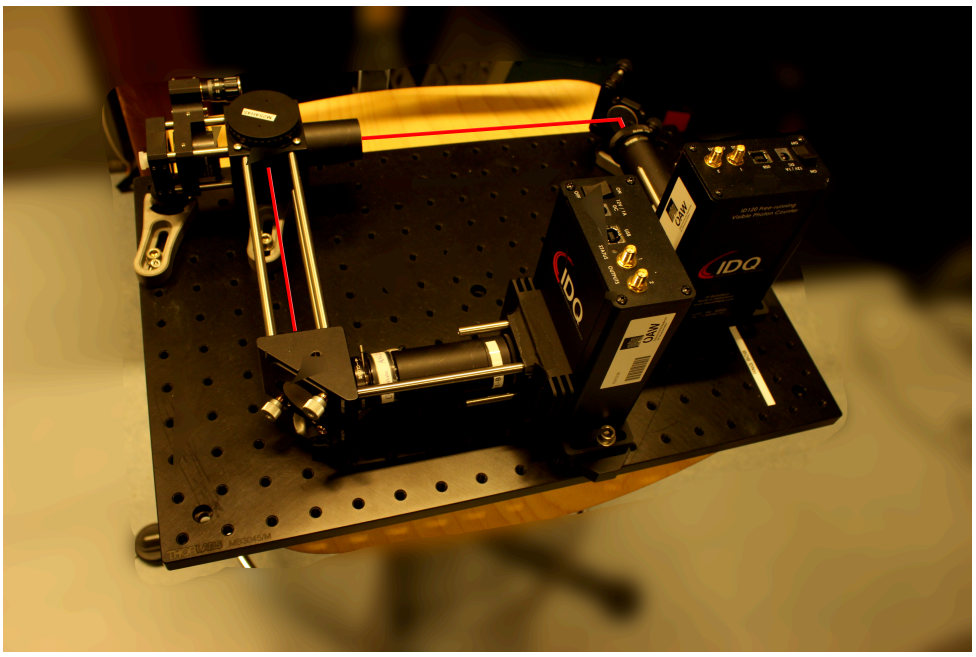

Figure 6.8: Image of the random number detection module. Photons from a tracked star are coupled from a telescope into the detection module. According to their wavelength they are separated at a dichroic mirror. Depending on which detector is hit by a photon, the measurement basis choice corresponds either to the $|H, V\rangle$ or the $|D, A\rangle$ basis.

6.3.2 Random numbers for the lab-test

Before using our cosmic QRNG, we want to analyze, if the choice of our generated random numbers, does effectively influence the outcome of a Bell test. I want to convert publicly well known events into sequences of binary "0"s and "1"s in order to test them on their degree of randomness with the statistical test suite SP-800-22 (offered by NIST), which is a common standard in performing statistical evaluations on random numbers. In the following section I will introduce the different types of random numbers, that have been generated.

6.3.3 True random numbers

In order to compare the outcome of a Bell test, that is fed with true random numbers and pseudo-random numbers, we have to ensure, that we receive binary data samples, which are obtained by physical processes. The Australian National University (ANU) as well as the National Institute of Standards and Technology (NIST) offer publicly available data samples of true random numbers. In the following I will explain the different production processes of their random numbers.

ANU Quantum Random Number Server

The ANU Quantum Random Number Server generates random numbers from the quantum fluctuations of the vacuum [44]. In classical theories vacuum is described as an empty space of matter, while in quantum mechanics the vacuum can be treated as a sea of virtual particles, that are created and annihilated randomly in order to the vacuum's zero-point energy. Single mode laser light at a wavelength of 1550 nm and an output power of some few mW is guided to a 50/50 beam splitter. Here, the beam intensity is equally split up and detected by two homodyne photodetectors. Since the average laser field amplitude α is much higher, than the fluctuation of the vacuum field, the difference between the photo-currents of both detectors is proportional to $\alpha X_\nu(\omega)$ with $X_\nu(\omega)$ being the squared amplitude of the vacuum field. By the usage of the homodyne photodetectors, the contribution of the vacuum fluctuations as quantum noise can be amplified essentially. In order to minimize technical noise frequencies, the photo-currents are demodulated with a RF of 1.6 GHz.

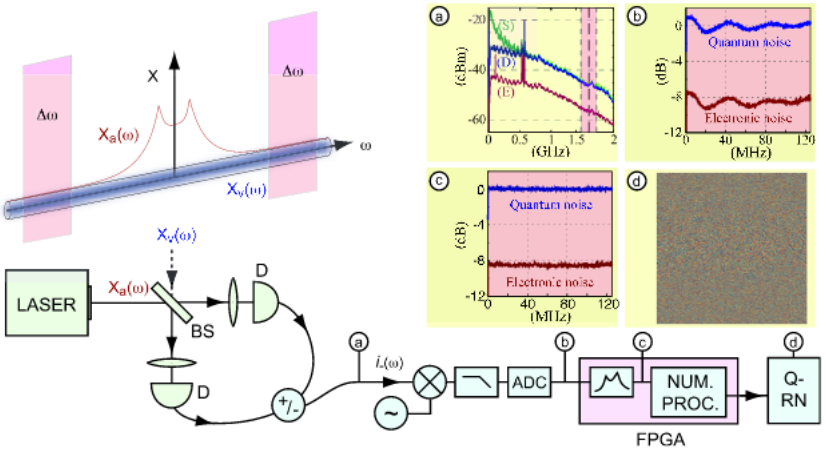

Figure 6.9: Schematic illustration of the generation of true random numbers at ANU [44]. For details refer to the main text.

Thus, the electronic noise differs from the quantum noise by 8.5 dB. The non-uniform electric gain of the noise signal is compensated with a filter function. Finally,

numerical processes are used to convert the quantum noise into digital sequences of random bits. The experimental setup scheme as well as the noise spectra can be taken from figure 6.9.

NIST Randomness Beacon

In a collaboration between the Physical Measurement Laboratory (PML) and the National Institute of Standards and Technology (NIST), the outcomes of loophole-free Bell tests can be used to generate true random numbers, that are unknown to a third party before a certain time [45]. At the moment, the NIST Randomness Beacon consists of two independent commercially available sources of randomness, which offers in intervals of 60 second publical access to full-entropy bit-strings in block of 512 bits. As the bits are known to public after their broadcast, the Randomness Beacon can not be used for cryptographic applications, but it is sufficient to guarantee private randomness for our purposes.

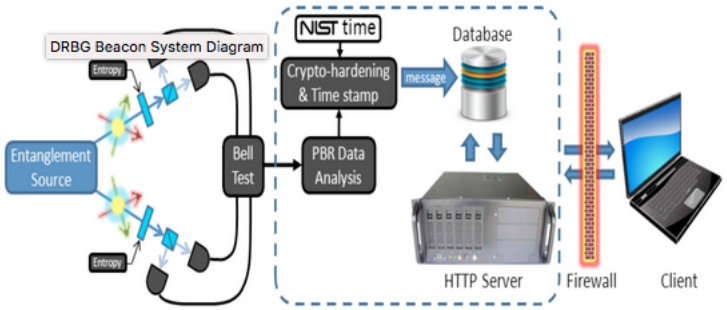

Figure 6.10: Architecture of NIST's Randomness Beacon for generating true random numbers [45].

6.3.4 Pseudo-random numbers

Political speeches: Obama vs. Bush resp. Obama vs. Fischer

In a first test I want to generate sequences of random numbers from politicians speeches. For this reason the measurement basis choice on Alice's side is generated by the speeches, that were held by President Barack Obama during his two legislations. In contrast, Bob's random numbers can be derived from the orations of his precursor George W. Bush. Furthermore, I want also to use the speeches of the Austrian President Heinz Fischer and Barack Obama in an additional Bell test.
The sequences of binary random numbers are created by converting every letter of the speeches into the corresponding bit sequences (e.g. the character "a" corresponds to the binary 01100001). The so won random numbers are produced by an algorithm and correspond to pseudo-random numbers.

FIFA world cup final 1998 vs. 2014

In another approach I want to extract random bit sequences from a video analysis of the last fifteen minutes of the FIFA soccer world cup finals in 1998 and 2014. Therefore, the video is split into 9000 separate images, and we choose a small reference window, from which we determine the mean pixel value and apply on this figure the modulo 2 function in order to get a binary value. The reference window is scanned over the entire image and revised for every picture. Thereby, we achieve a big amount of random binary data.

Atmospheric turbulences

As suggested in the paper of Marangon et al. [46], we can utilize atmospheric turbulences in order to generate random numbers. It takes huge computational effort to approximate the solution of the Navier-Stokes equations for the turbulent atmosphere. Thus, we use the distortion of the incoming wave-front from an optical laser link, that can be analyzed with a camera. For this reason, we have used a video file from a former experiment in Tenerife. Here, a laser-beam has been sent from the cable car station of the Teide to the house wall of the optical ground station (OGS). The thereby filmed video shows the typical speckle pattern, created by the interference of different sets of wave-fronts. Again, we analyze a certain region of interest and set a mean pixel value for each reference frame. In a similar method as suggested in Marangon's paper, the number of pixels within a reference frame, which exceed the mean pixel value, are used to determine a binomial coefficient. Afterwards, the result is transformed into a set of binary values. This procedure is revised for the entire video and used to generate two different sets of random number sequences.

Periodic binaries

In contrast to the generation of random bits, we also want to study the case of periodically changing sequences. By studying small parts of the produced random numbers, we can provide information about their further progression, i.e. the measurement bases get maximally predictable and we widely open the freedom-of-choice loophole. On Alice's side we use the sequence "0101010101..." while on Bob's side we apply the binary code "001001001...".

6.4 Statistical test

In order to analyze the generated binary sequences on their degree of randomness, the usage of different statistical tests is needed. The outcomes of these statistical

tests can be treated with probabilistic theories, that check the predictability of the random bit sequences. There are lots of different approaches for judging the quality of random numbers, why even a detailed analysis can not be seen as "complete". In this thesis I want to analyze the bit sequences with the NIST statistical test suite SP 800-22, which offers 15 different statistical tests [47]. The outcomes of these tests are again random variables with a given probability distribution, which is also called test statistic. This reference distribution offers the possibility to determine a critical value. From the test statistic we can calculate a so-called p-Value, which proves the evidence of coming upon a random number. In our tests the bit sequences fail to be random for a p-Value < 0.01, which corresponds to a confidence level of 99%.
In the following I want to introduce two of the used tests, the other ones are described in detail in [47].
The frequency test surveys the fraction of appearing "0" and "1" bits in our sequences. For increasing sequence lengths the fractions should converge to $\frac{1}{2}$. The FFT test determines the peak heights of the Discrete Fourier Transform of our sequence. If one detects periodic properties like repetitive patterns, than our assumption of randomness fails.
As a consequence of asymptotic approximations, that are crucial in several tests for the determination of the limiting distribution, the choice of the sequence length n, as well as the number of analyzed sequences m are the two essential parameters for carrying out the statistical tests. Thus, the developers suggest to analyze several Mbyte of data to ensure proper statistical test results. Unfortunately, it is not possible for our experiment to use this amount of data for each produced random sequence. Taking for instance into account the random bit sequence derived from all Presidential speeches, that were held by Barack Obama, we only achieve a data sample of 50 Mbyte. Though, this sample size would be sufficient for a proper statistical test, we would need to feed the Pockel's cell with 400 million electronic signals. As the production rate of electronic signals within the Labview software was limited by some 100 Hz, using the whole data file would have taken more than 40 days of experimental time for only one Bell test. Thus, we have used much smaller amounts of data in the experiment, why I have also analyzed sample sizes of half a Mbyte on their degree of randomness.

As we can see in table 6.1 the true random numbers, created at ANU and NIST, pass all statistical tests with a samples size n = 1,000,000 and m = 50. Even for smaller samples of n = 50,000 and m = 10 (these sample sizes are also used for the pseudo-random numbers) the statistical tests show successful results for the random sequences, but some of the tests cannot be carried out any more in order to a lack of statistics (compare table 6.2).
A common way to improve the quality of random bit sequences is given by post-

processing the raw data with some randomness extractor. In principle, this extractor can be seen as a privacy amplification scheme [48, 49]. Thus, we can use a hash function to generate a new random number bit sequence. For simplicity we choose the hash function

$$h(x_j) = \sum_{i=1}^{100} x_{j+i} \mathrm{mod} 2, \tag{6.13}$$

with x_j being a random bit and $j \in \mathbb{N}_0 < \frac{n \cdot m - 100}{100}$. As supposed, the hashing does not influence the statistical test results for the true random number sequences. In contrast, tables 6.4 and 6.5 show a comparison between the test results for the raw and the hashed bit sequences for the random numbers generated by the video of the world cup final 1998 and the speeches of Barack Obama. While the raw data fail in most of the applied tests, the hashing generates new bit sequences, that are able to pass most tests. Thus, we can directly see, how the quality of our generated pseudo-random numbers has improved. The same behavior has been found for the other generated pseudo-random numbers and can be taken from the Appendix.

	ANU		NIST	
	p-Value	proportion	p-Value	proportion
Frequency	0.419	49/50	0.018	48/50
BlockFrequency	0.956	50/50	0.456	49/50
CummulativeSums	0.983	49/50	0.575	47/50
Runs	0.154	50/50	0.983	50/50
LongestRun	0.699	50/50	0.983	49/50
Rank	0.122	50/50	0.699	48/50
FFT	0.996	49/50	0.883	50/50
NonOverlappingTemplate	0.384	47/50	0.740	48/50
OverlappingTemplate	0.883	50/50	0.658	50/50
Universal	0.262	49/50	0.575	49/50
ApproximateEntropy	0.779	50/50	0.534	49/50
RandomExcursions	0.028	36/36	0.067	27/28
RandomExcursionsVariant	0.407	35/36	0.025	27/28
Serial	0.020	50/50	0.740	48/50
LinearComplexity	0.991	49/50	0.319	48/50

Table 6.1: NIST statistical test results for the ANU and NIST Beacon random numbers (n=1,000,000 and m=50).

	ANU short		NIST short	
	p-Value	proportion	p-Value	proportion
Frequency	0.350	10/10	0.911	10/10
BlockFrequency	0.740	10/10	0.350	10/10
CummulativeSums	0.213	10/10	0.350	10/10
Runs	0.350	10/10	0.534	10/10
LongestRun	0.534	10/10	0.350	10/10
Rank	0.213	10/10	0.534	10/10
FFT	0.350	10/10	0.534	10/10
NonOverlappingTemplate	0.740	8/10	0.534	8/10
OverlappingTemplate	0.534	10/10	0.534	10/10
Universal	–	–	–	–
ApproximateEntropy	0.350	10/10	0.350	10/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.350	9/10	0.350	10/10
LinearComplexity	0.534	10/10	0.534	10/10

Table 6.2: NIST statistical test results for the ANU and NIST Beacon random numbers (n=50,000 and m=10).

	ANU hashed		NIST hashed	
	p-Value	proportion	p-Value	proportion
Frequency	0.534	10/10	0.534	10/10
BlockFrequency	0.350	10/10	0.350	10/10
CummulativeSums	0.009	10/10	0.350	10/10
Runs	0.534	9/10	0.122	9/10
LongestRun	0.350	10/10	0.534	10/10
Rank	0.740	9/10	0.350	10/10
FFT	0.018	10/10	0.534	10/10
NonOverlappingTemplate	0.213	8/10	0.066	9/10
OverlappingTemplate	0.534	10/10	0.213	10/10
Universal	–	–	–	–
ApproximateEntropy	0.066	10/10	0.534	10/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.213	10/10	0.740	10/10
LinearComplexity	0.534	10/10	0.911	10/10

Table 6.3: NIST statistical test results for hashed ANU and NIST Beacon random numbers (n=50,000 and m=10).

	WC Final 1998 short		WC Final 1998 hashed	
	p-Value	proportion	p-Value	proportion
Frequency	0.534	8/10	0.350	10/10
BlockFrequency	0.000	4/10	0.740	10/10
CummulativeSums	0.350	7/10	0.122	10/10
Runs	0.000	0/10	0.534	9/10
LongestRun	0.000	1/10	0.911	10/10
Rank	0.534	10/10	0.213	10/10
FFT	0.000	6/10	0.740	10/10
NonOverlappingTemplate	0.000	1/10	0.066	9/10
OverlappingTemplate	0.000	1/10	0.991	10/10
Universal	–	–	–	–
ApproximateEntropy	0.000	2/10	0.350	10/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.000	3/10	0.350	10/10
LinearComplexity	0.350	10/10	0.122	10/10

Table 6.4: Comparison of NIST statistical test results for the raw data and the hashed data from the world cup final 1998 (n=50,000 and m=10). Each failed test is colored red. The hashing dramatically improves the quality of the random numbers, shown in the results of the statistical test. All tests, that were rejected before post processing, finally pass the tests.

	Obama short		Obama hashed	
	p-Value	proportion	p-Value	proportion
Frequency	0.000	0/10	0.122	10/10
BlockFrequency	0.000	0/10	0.911	10/10
CummulativeSums	0.000	0/10	0.122	10/10
Runs	0.000	0/10	0.067	9/10
LongestRun	0.000	0/10	0.350	10/10
Rank	0.000	0/10	0.740	10/10
FFT	0.000	0/10	0.067	9/10
NonOverlappingTemplate	0.000	0/10	0.350	8/10
OverlappingTemplate	0.000	0/10	0.122	10/10
Universal	–	–	–	–
ApproximateEntropy	0.000	0/10	0.067	9/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.000	0/10	0.000	5/10
LinearComplexity	0.213	10/10	0.911	10/10

Table 6.5: Comparison of the NIST statistical test results for raw and hashed data from the binary sequences of Obama's speeches (n=50,000 and m=10). As seen in the result for the random numbers from the world cup final 1998, the hashing improves the quality of the random numbers.

6.5 Results

Our generated random numbers have been converted into electronic signals, which were supplied to the FPGA board, building the interface between the random numbers and the switching behavior of the Pockels cell. Each measurement run has started simultaneously on Alice's and Bob's receiving side and has been performed for approximately 30 seconds with a random number rate of approximately 100 Hz. The received detector counts from the source photons have been time-tagged with the help of the FPGA software and saved in separate data files for Alice and Bob. Afterwards, these files where fed into a program designed by my colleague Liu Bo, which enables the extraction of the cross-correlation functions as well as the characteristic Bell parameter S from the received data, which is exemplified in figure 6.11.

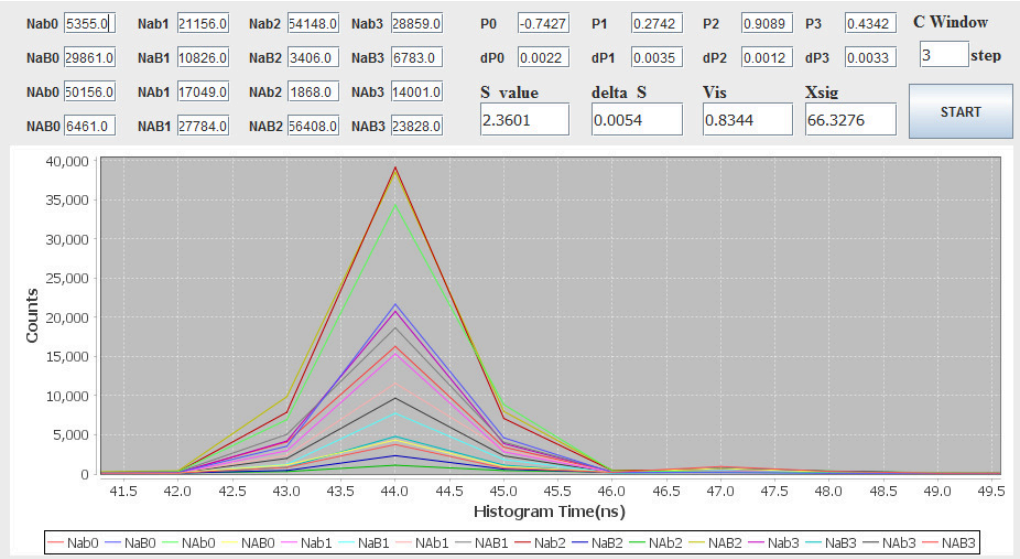

Figure 6.11: Screenshot of the program that is used for the analyzation of the 16 cross-correlation functions. The shown result corresponds to a Bell test, that has been carried out with random numbers, which were generated from atmospheric turbulences. By properly adjusting the time-delay between the different detectors, one obtains the 16 coincidence peaks of a typical measurement, that are shown in the middle graph and can be used to determine the expectation values of the CHSH inequality as well as the corresponding S-value.

Thereby, we have obtained a total number of approximately 35,000 coincidences per run. The 16 coincidence rates within a coincidence window of 3 ns can be used to determine the four expectation values for the CHSH inequality. The expectation values as well as the so won S-value for each set of random number files can be taken from table 6.6 and 6.7.

	E(22.5°, 0°)	E(67.5°, 0°)	E(22.5°, 45°)	E(67.5°, 45°)
Periodic	0.262 ± 0.003	-0.743 ± 0.003	0.903 ± 0.001	0.454 ± 0.004
ANU/NIST	0.294 ± 0.003	-0.771 ± 0.002	0.907 ± 0.001	0.450 ± 0.003
ANU/NIST hashed	0.288 ± 0.003	-0.772 ± 0.002	0.904 ± 0.002	0.444 ± 0.003
Atmospherical Turbulences	0.274 ± 0.004	-0.743 ± 0.002	0.909 ± 0.001	0.434 ± 0.003
Obama/Fischer	0.284 ± 0.003	-0.767 ± 0.002	0.902 ± 0.001	0.447 ± 0.003
Obama/Bush	0.300 ± 0.003	-0.771 ± 0.002	0.904 ± 0.002	0.450 ± 0.003
Obama/Bushed hashed	0.300 ± 0.003	-0.771 ± 0.002	0.904 ± 0.002	0.449 ± 0.003
WC Final 1998/2014	0.294 ± 0.003	-0.775 ± 0.002	0.901 ± 0.002	0.450 ± 0.003
WC Final 1998/2014 hashed	0.300 ± 0.003	-0.773 ± 0.002	0.901 ± 0.002	0.448 ± 0.003

Table 6.6: Determined expectation values of the CHSH inequality for the different random numbers corresponding to a total number of coincidences of approximately 35,000.

	S-value
Periodic	2.361 ± 0.005
ANU/NIST	2.422 ± 0.005
ANU/NIST hashed	2.409 ± 0.005
Atmospherical Turbulences	2.360 ± 0.005
Obama/Fischer	2.400 ± 0.005
Obama/Bush	2.424 ± 0.005
Obama/Bush hashed	2.424 ± 0.005
WC Final 1998/2014	2.420 ± 0.005
WC Final 1998/2014	2.421 ± 0.005

Table 6.7: Resulting S-values for the Bell tests performed with different random number sources.

By using Poissonian photon statistics in the error calculation, the error for the expectation value can be written as

$$\Delta E(\alpha,\beta) = \sqrt{\left[\frac{2\cdot C(\alpha,\beta)_{\parallel}}{(C(\alpha,\beta)_{total})^2}\cdot \Delta C(\alpha,\beta)_{\perp}\right]^2 + \left[\frac{2\cdot C(\alpha,\beta)_{\perp}}{(C(\alpha,\beta)_{total})^2}\cdot \Delta C(\alpha,\beta)_{\parallel}\right]^2}, \tag{6.14}$$

with

$$\begin{aligned} C(\alpha,\beta)_{\parallel} &= C(\alpha,\beta) + C(\alpha^{\perp},\beta^{\perp}) \\ C(\alpha,\beta)_{\perp} &= C(\alpha,\beta^{\perp}) + C(\alpha^{\perp},\beta) \\ C(\alpha,\beta)_{total} &= C(\alpha,\beta)_{\parallel} + C(\alpha,\beta)_{\perp}. \end{aligned} \tag{6.15}$$

Thus, we obtain the error for S to be

$$\Delta S(\alpha_1, \beta_1, \alpha_2, \beta_2) = \sqrt{\Delta E(\alpha_1, \beta_1)^2 + \Delta E(\alpha_1, \beta_2)^2 + \Delta E(\alpha_2, \beta_1)^2 + \Delta E(\alpha_2, \beta_2)^2}. \tag{6.16}$$

As we can deduce from figure 6.12, each of our measurements violates the CHSH-inequality. Thus, we conclude, that the quality of our random numbers does not influence the outcome of the Bell test measurement.

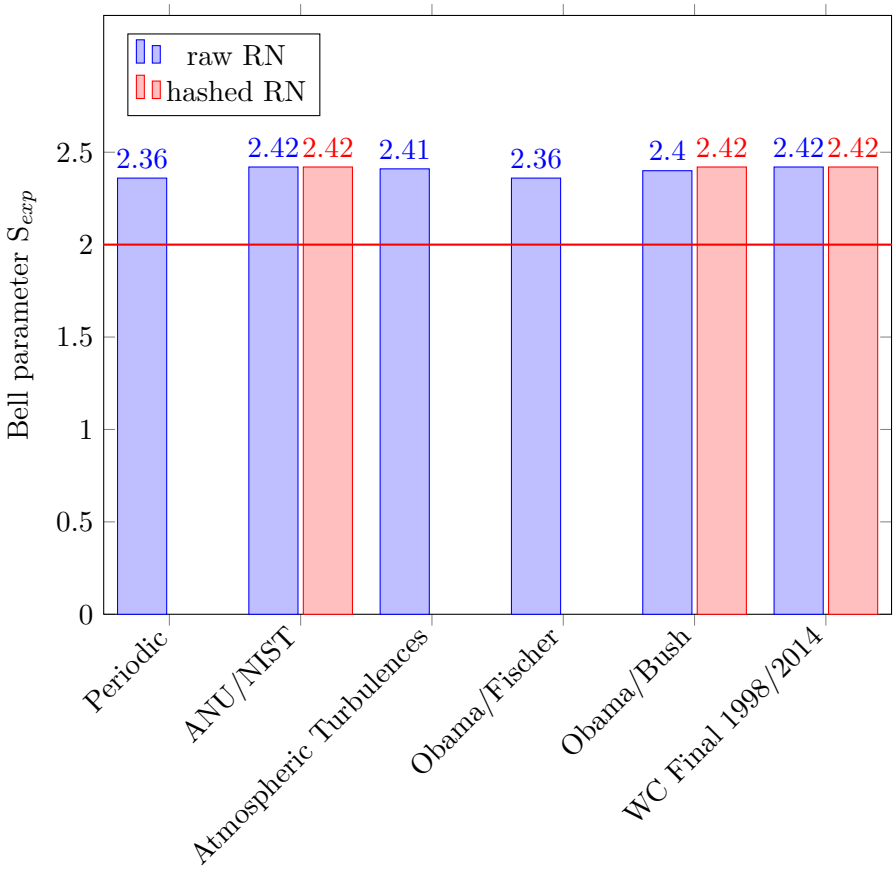

Figure 6.12: Plot of the determined S_{exp} value for different random number sources. As we can see, each of the performed Bell tests is leading to a violation of the CHSH inequality (the limit of 2 is colored red). The corresponding error ranges are given explicitly in table 6.7, as they can not be visualized properly in the plot.

Also the absolutely not random periodic sequences of random data has violated the Bell inequality by more than 72 standard deviations. Nevertheless, we have to be aware, that in this laboratory Bell test we have not closed any loopholes. Accordingly, local hidden variable theories could be used to explain the obtained

results. However, the adjustment of our receiver modules is satisfying for being used in a "cosmic Bell" experiment.

6.6 Summary

Within this experiment we have assembled and analyzed two different receiving modules, that will be used for future Bell test experiments with cosmic sources in order to close the freedom-of-choice loophole. At first the entire setup has been aligned with a continuous wave laser at a wavelength of 810 nm and afterwards fine tuned with source photons of the same wavelength. Thereby, we have achieved contrast rates of at least 50/1 in the $|H, V\rangle$ and $|D, A\rangle$ basis. Furthermore, we have investigated the influence of different random numbers on the outcome of a Bell test in the laboratory. We have seen, that the quality of the random numbers does not influence the violation of the CHSH inequality, also not for totally periodic and predictable random numbers. Consequently, we can conclude that our setup is prepared for carrying out a Bell test experiment, which uses cosmic sources as random number generator.

Chapter 7

Conclusion and Outlook

In this thesis I have shown the preparation, the design and the testing of a transmitting and a receiving module, that are crucial for the execution of two different quantum experiments, which are performed at the Institute for Quantum Optics and Quantum Information in Vienna.
The first experiment, QUESS, plans to enable a quantum key exchange according to the BB84 protocol for the first time via an optical satellite-to-ground link. Thus, we have to equip three different optical ground station in Europe with receiving modules. In order to test those stations, we have built up a satellite mock-up system, that generates similar quantum and beacon signals, that we expect from the satellite. This mock-up setup has been tested on horizontal ground links at the Canary Islands as well as in Graz. Thereby, we were able to adjust our receiving modules up to a visibility $> 98\%$. We are therefore very confident, that the receiving modules are optimally adjusted for future satellite to ground communications. Furthermore, it is planned to check the adjustment with an additional mock-up setup, that has been created by our project partners from the Chinese Academy of Science at the end of April 2016. The launch of the satellite is scheduled for summer 2016.
For the "cosmic Bell" experiment we have developed two receiving setups, that will be used for the execution of a Bell test with cosmic sources. Therefore, we had to characterize, design and test the behavior of our receiving stations (Alice and Bob). Additionally, we have analyzed the outcome of Bell tests in the laboratory, which uses different types of random number sources. In the experiment we have generated several types of true and pseudo-random binary numbers, which were then used as the choice of the receiving modules measurement bases. From the obtained results, we can conclude, that we have achieved a violation of the CHSH inequality for each type of used random numbers. However, we have to be aware, that we have not closed any possible loophole in the performed experiments. Both receiving stations are ready to be used for a Bell type experiment over the rooftops of Vienna, which

uses starlight as random number generator. In future, it is planned to exceed this experiment by using quasar photons as source of randomness, which would close the freedom-of-choice loophole in a way, that has never been achieved experimentally before.

Appendix A

NIST Statistical Tests

	Atm Turb (Alice)		Atm Turb (Bob)	
	p-Value	proportion	p-Value	proportion
Frequency	0.067	7/10	0.009	9/10
BlockFrequency	0.350	10/10	0.534	10/10
CummulativeSums	0.018	8/10	0.009	9/10
Runs	0.000	1/10	0.000	0/10
LongestRun	0.122	10/10	0.534	10/10
Rank	0.350	10/10	0.740	9/10
FFT	0.350	10/10	0.350	10/10
NonOverlappingTemplate	0.000	0/10	0.000	0/10
OverlappingTemplate	0.350	9/10	0.122	9/10
Universal	–	–	–	–
ApproximateEntropy	0.000	0/10	0.000	0/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.000	0/10	0.000	0/10
LinearComplexity	0.911	10/10	0.350	10/10

Table A.1: NIST statistical test results for the random numbers created from atmospherical turbulences (n=50,000 and m=10).

	Periodic 10		Periodic 100	
	p-Value	proportion	p-Value	proportion
Frequency	0.000	0/10	0.000	0/10
BlockFrequency	0.000	0/10	0.000	0/10
CummulativeSums	0.000	0/10	0.000	0/10
Runs	0.000	0/10	0.000	0/10
LongestRun	0.000	0/10	0.000	0/10
Rank	0.000	0/10	0.000	0/10
FFT	0.000	0/10	0.000	0/10
NonOverlappingTemplate	0.000	0/10	0.000	0/10
OverlappingTemplate	0.000	0/10	0.000	0/10
Universal	–	–	–	–
ApproximateEntropy	0.000	0/10	0.000	0/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.000	0/10	0.000	0/10
LinearComplexity	0.000	0/10	0.000	0/10

Table A.2: NIST statistical test results for periodic random numbers (n=50,000 and m=10).

	WC Final 2014 short		WC Final 2014 hashed	
	p-Value	proportion	p-Value	proportion
Frequency	0.122	8/10	0.534	10/10
BlockFrequency	0.000	0/10	0.534	10/10
CummulativeSums	0.035	8/10	0.911	10/10
Runs	0.000	0/10	0.911	10/10
LongestRun	0.000	0/10	0.740	9/10
Rank	0.534	10/10	0.213	10/10
FFT	0.000	3/10	0.350	10/10
NonOverlappingTemplate	0.000	0/10	0.122	9/10
OverlappingTemplate	0.000	0/10	0.122	10/10
Universal	–	–	–	–
ApproximateEntropy	0.000	0/10	0.122	9/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.000	0/10	0.350	10/10
LinearComplexity	0.740	10/10	0.740	10/10

Table A.3: NIST statistical test results for raw and hashed data from the world cup final 2014 (n=50,000 and m=10).

	Bush short		Bush hashed	
	p-Value	proportion	p-Value	proportion
Frequency	0.000	0/10	0.067	9/10
BlockFrequency	0.000	0/10	0.350	10/10
CummulativeSums	0.000	0/10	0.009	9/10
Runs	0.000	0/10	0.000	5/10
LongestRun	0.000	0/10	0.740	10/10
Rank	0.000	0/10	0.350	10/10
FFT	0.000	0/10	0.350	9/10
NonOverlappingTemplate	0.000	0/10	0.035	7/10
OverlappingTemplate	0.000	0/10	0.213	10/10
Universal	–	–	–	–
ApproximateEntropy	0.000	0/10	0.122	8/10
RandomExcursions	–	–	–	–
RandomExcursionsVariant	–	–	–	–
Serial	0.000	0/10	0.122	9/10
LinearComplexity	0.534	10/10	0.740	10/10

Table A.4: NIST statistical test results for raw and hashed data from George Bush's speeches (n=50,000 and m=10).

	Heinz Fischer	
	p-Value	proportion
Frequency	0.000	0/10
BlockFrequency	0.000	0/10
CummulativeSums	0.000	0/10
Runs	0.000	0/10
LongestRun	0.000	0/10
Rank	0.000	0/10
FFT	0.000	0/10
NonOverlappingTemplate	0.000	0/10
OverlappingTemplate	0.000	0/10
Universal	–	–
ApproximateEntropy	0.000	0/10
RandomExcursions	–	–
RandomExcursionsVariant	–	–
Serial	0.000	0/10
LinearComplexity	0.740	10/10

Table A.5: NIST statistical test results from Heinz Fischer's speeches (n=48,000 and m=10).

List of Figures

List of Tables

Bibliography

[1] R. Ursin et al. Entanglement-based quantum communication over 144 km. *Nat Phys*, 3(7):481–486, 2007.

[2] M. Aspelmeyer et al. Long-distance free-space distribution of quantum entanglement. *Science*, 301(5633):621–623, 2003.

[3] K. J. Resch et al. Distributing entanglement and single photons through an intra-city, free-space quantum channel. *Opt. Express*, 13(1):202–209, 2005.

[4] C.-Z. Peng et al. Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication. *Phys. Rev. Lett.*, 94:150501, 2005.

[5] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[6] C. Simon, G. Weihs, and A. Zeilinger. Optimal quantum cloning via stimulated emission. *Phys. Rev. Lett.*, 84:2993–2996, 2000.

[7] G. S. Vernam. Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. *American Institute of Electrical Engineers*, pages 55–109, 1926.

[8] H.-K. Lo, X. Ma, and K. Chen. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.*, 94:230504, 2005.

[9] W.Y. Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.*, 91:057901, 2003.

[10] C.-Z. Peng et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.*, 98:010505, 2007.

[11] T. Schmitt-Manderbach et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, 2007.

[12] T. Jennewein et al. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84:4729–4732, 2000.

[13] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. Free-space quantum key distribution with entangled photons. *Applied Physics Letters*, 89(10), 2006.

[14] C. Erven et al. Entangled quantum key distribution over two free-space optical links. *Opt. Express*, 16(21):16840–16853, 2008.

[15] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, 2002.

[16] J. Lodewyck et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, 76:042305, 2007.

[17] 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*, 175, 1984.

[18] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy Amplification by Public Discussion. *SIAM J. Comput.*, 17(2):210–229, 1988.

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

[20] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, 2000.

[21] M. Dušek, O. Haderka, and M. Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Optics Communications*, 169:103–108, 1999.

[22] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.*, 85:1330–1333, 2000.

[23] X.-B. Wang. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.*, 94:230503, 2005.

[24] A. Poppe et al. Practical Quantum Key Distribution with Polarization Entangled Photons. *Optics Express*, 12:3865–3871, 2004.

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

[26] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky. *Phys. Rev.*, 108:1070–1076, 1957.

[27] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[28] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[29] J. S. Bell. *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press, second edition, 2004.

[30] J. P. Jarrett. On the Physical Significance of the Locality Conditions in the Bell Arguments. *Noûs*, 18(4):569–589, 1984.

[31] P. M. Pearle. Hidden-Variable Example Based upon Data Rejection. *Phys. Rev. D.*, 2:1418–1425, 1970.

[32] A. Garg and N. D. Mermin. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Phys. Rev. D*, 35:3831–3835, 1987.

[33] P. H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A*, 47:R747–R750, 1993.

[34] G. Weihs et al. Violation of bell's inequality under strict einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043, 1998.

[35] M. A. Rowe et al. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409(6822):791–794, 2001.

[36] T. Scheidl et al. Violation of local realism with freedom of choice. *PNAS*, 107:19708, 2010.

[37] M. Giustina et al. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, 2015.

[38] L. K. Shalm et al. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, 2015.

[39] B. Hensen et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[40] J. Gallicchio, A. S. Friedman, and D. I. Kaiser. Testing bell's inequality with cosmic photons: Closing the setting-independence loophole. *Phys. Rev. Lett.*, 112:110405, 2014.

[41] M. H. Rubin et al. Theory of two-photon entanglement in type-ii optical parametric down-conversion. *Phys. Rev. A*, 50:5122–5133, 1994.

[42] G. L. Pedrola. *Beam Propagation Method for Design of Optical Waveguide Devices*. John Wiley & Sons, 2015.

[43] R. Goldstein. Electro-optic devices in review. *Lasers and Applications*, 1986.

[44] 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*, 98(23), 2011.

[45] NIST. NIST Randomness Beacon. `http://www.nist.gov/itl/csd/ct/nist_beacon.cfm`. Accessed: 2016-04-15.

[46] D. G. Marangon, G. Vallone, and P. Villoresi. Random bits, true and unbiased, from atmospheric turbulence. *Scientific Reports*, 4:5490, 2014.

[47] A. Rukhin et al. A statistical testsuite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 Revision 1a (2010). `http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf`.

[48] C. H Bennett et al. Generalized privacy amplification. *Information Theory, IEEE Transactions on*, 41(6):1915–1923, 1995.

[49] X. Ma et al. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A*, 87:062327, 2013.

Acknowledgements

By finalizing this thesis I look back on my years of study as being the most formative time of my life in all kinds of living situations. Without the support of many different people the completion of this work would not have been possible. Herewith, I want to express my sincere gratitude to those people:
At first I want to thank Prof. Anton Zeilinger for giving me the opportunity to conduct my master's thesis at the free-space group of the IQOQI. The IQOQI has not only been a very instructive place for making experiments, but also a great location to discuss with an inspiring group of people the questions of science and everyday life.
Furthermore, I want to thank the free-space group - Thomas Scheidl, Johannes Handsteiner, Thomas Herbst, Dominik Rauch and Liu Bo - for their great support. Whenever something appeared to be unclear to me, you have taken your time to remove all of my ambiguities without hesitation. Beside from the scientific point of view, I have also appreciated the human component, that plays a big role within this group. Especially, I will treasure the exciting time with you on the Canary Islands.
Special thanks to my friends, particularly my room mates, who have spent most of my studying time with me, keeping me grounded and always having an open ear for my troubles.
Finally, I want to thank my family, who has stood behind me throughout my whole life. I thank my father for his support, my sister Patricia for being the dearest sister one can imagine. My deepest gratitude extends to my mother, who has arranged her life primary according to the needs of us children. This work is dedicated to your love and the hard work that you have performed only to fulfill our personal desires.
This work was supported by the Austrian Science Fund (FWF) SFB-FoQuS F-4007, by the QUESS project, by the IQOQI Vienna and by the University of Vienna.