universität wien

DISSERTATION

Titel der Dissertation

A fundamental test and an application of quantum entanglement

angestrebter akademischer Grad

Doktor der Naturwissenschaften (Dr. rer.nat.)

Verfasserin / Verfasser:	Thomas Scheidl
Matrikel-Nummer:	9902354
Dissertationsgebiet (lt. Studienblatt):	Experimentalphysik
Betreuerin / Betreuer:	o. Univ.-Prof. Dr. DDr. h. c. Anton Zeilinger

Wien, am 19. März 2009

Contents

1. Abstract **7**

2. Zusammenfassung **9**

3. Introduction **11**
3.1. Outline of the thesis . . . 12

4. The basics of photonic qubits **15**
4.1. Superposition and Entanglement . . . 15
4.1.1. Superposition . . . 15
4.1.2. Entanglement . . . 15
4.2. Photonic qubits . . . 16
4.3. No-cloning theorem . . . 17
4.4. Density matrices . . . 18
4.5. Measurement . . . 19
4.6. State tomography . . . 19

5. Local realism vs. quantum mechanics **21**
5.1. EPR's argument . . . 22
5.1.1. Bohm version of EPR's thought experiment . . . 23
5.1.2. Bohr's response to EPR . . . 24
5.2. Local realistic theories . . . 24
5.3. Bell's theorem . . . 26
5.3.1. CHSH inequality . . . 28
5.4. Loopholes . . . 29
5.4.1. Bell's assumptions . . . 29
5.4.2. Locality loophole . . . 30
5.4.3. Freedom-of-choice loophole . . . 30
5.4.4. Fair-sampling loophole . . . 31
5.5. Previous experiments . . . 32
5.5.1. 1972 - Freedman and Clauser . . . 32
5.5.2. 1982 - Aspect *et al.* . . . 33
5.5.3. 1998 - Weihs *et al.* . . . 34
5.5.4. 2001 - Rowe *et al.* . . . 36
5.5.5. 2007 - Gröblacher *et al.* . . . 36

5.5.6. 2007 - Ursin *et al.* . . . 37

6. A Bell test under locality and freedom-of-choice conditions **39**
6.1. Required space-time arrangement for the Bell test . . . 40
6.1.1. How to close the locality loophole . . . 40
6.1.2. How to close the freedom-of-choice loophole . . . 43
6.2. Experimental parts . . . 44
6.2.1. Source of entangled photons . . . 44
6.2.2. Quantum Random Number Generator . . . 47
6.2.3. Polarization analyzers . . . 50
6.2.4. Electro-optical modulator . . . 52
6.2.5. Atmospheric free-space quantum channel . . . 59
6.2.6. Optical fiber channel . . . 67
6.2.7. Classical channel . . . 68
6.2.8. Electronics . . . 69
6.2.9. Time-tagging and coarse synchronization . . . 70
6.2.10. Software and fine synchronization . . . 72
6.3. Experimental situation . . . 73
6.3.1. Event durations . . . 74
6.3.2. Final space-time situation . . . 75
6.4. Measurement procedure . . . 77
6.4.1. Aligning the Sagnac source . . . 77
6.4.2. Measuring the attenuation through the quantum channels . . . 78
6.4.3. Establishing a common polarization reference frame . . . 79
6.4.4. Data acquisition . . . 79
6.5. Results . . . 80
6.5.1. Violation of the CHSH inequality . . . 80
6.5.2. State tomography . . . 83
6.5.3. Different space-time scenarios . . . 85
6.6. Conclusion and Outlook . . . 86

7. Quantum cryptography **89**
7.1. Coherent state BB84 protocol . . . 89
7.1.1. Coherent photon states . . . 89
7.1.2. Protocol . . . 90
7.1.3. Security . . . 91
7.2. Entanglement based BB84 protocol . . . 93
7.2.1. Entangled photon states . . . 93
7.2.2. Protocol . . . 93
7.2.3. Security . . . 94

8. Advantages of entanglement based QKD **95**
8.0.4. Theoretical error model . . . 96
8.1. The experiments . . . 97
8.1.1. Source at Alice . . . 99
8.1.2. Source asymmetric in between Alice and Bob . . . 101
8.1.3. Source in the middle . . . 102
8.1.4. Clock synchronization . . . 103
8.2. Conclusion and Outlook . . . 104

A. Preprint **107**

B. C^{++}-Code **123**
B.1. Source code: coincdosv9.cpp . . . 123

C. VHDL-Code **133**
C.1. Source code: compar.vhd . . . 133

D. Acknowledgements **147**

E. List of Publications **149**

F. Curriculum vitae **151**

1. Abstract

This work describes two experiments that are based on correlation measurements between entangled photons, spatially separated by 144 km between the Canary Islands, La Palma and Tenerife.

The first of which contributes to the debate of whether or not quantum mechanical predictions can be described within a local realistic frame, a question that plays a fundamental role in the foundation of quantum mechanics ever since the famous Einstein-Podolsky-Rosen (EPR) "paradox" [1]. The experiment presented is a test of the CHSH form [2] of Bell's inequality [3], simultaneously closing two out of three possible "loopholes" for local realism that can arise in an experimental Bell test. These two loopholes are the *locality* loophole and the *freedom-of-choice* loophole. The latter has not been addressed experimentally so far and was closed for the first time in our experiment by space-like separating the setting choice from the photon pair emission. Unfortunately, the third crucial loophole, i.e., the *fair-sampling* loophole [4], could not be closed due to inefficient photon detection. However, our experiment is the first to close more than one loophole at a time. By violating the CHSH inequality by more than 16 standard deviations with $S_{exp} = 2.37 \pm 0.023$, this is the most conclusive violation of local realism to date and represents an important step towards a completely loophole-free Bell test, which is one of the most significant still-unresolved challenges in fundamental physics.

Within the second experiment described, the intriguing properties of photonic entanglement are exploited for demonstrating entanglement based quantum key distribution (QKD), probably one of the most mature applications in the field of quantum information and quantum communication. In high loss situations, such as in the case of future satellite based or optical fiber based quantum communication networks, it is important to implement the most efficient experimental QKD scheme. It has recently been emphasized [5] that entanglement based quantum key distribution systems can tolerate higher channel losses compared to systems based on weak coherent laser pulses. This is in particular the case when the entangled photon source is located symmetrically between the two receiver stations, called Alice and Bob. We experimentally studied this important advantage by implementing different entanglement based QKD setups on a 144 km free-space link between the two Canary Islands, La Palma and Tenerife. We studied three different configurations that operated at two-photon attenuations of 35 dB, 58 dB and 71 dB, respectively. In these experiments, the entangled photon source was placed either at Alice's location, asymmetrically between Alice and Bob or symmetrically in the middle between Alice and Bob. In addition, we show that our experimental results agree well with the theoretical model devised in [5], which we applied to our experimental parameters. Compared to the expected link attenuations in a low-earth-orbit (LEO) satellite to ground scenario [6], as it might be implemented in a future network, we expect from

our results that entanglement based QKD systems are suitable to be used within either a single-downlink configuration or a configuration with two simultaneous downlinks [7].

2. Zusammenfassung

Diese Arbeit beschreibt zwei Experimente, die auf Korrelationsmessungen zwischen verschränkten Photonen basieren. Die Photonen werden dabei zwischen den kanarischen Inseln La Palma und Teneriffa 144 km räumlich voneinander getrennt.

Das erste Experiment trägt zur Diskussion darüber bei, ob quantenmechanische Vorhersagen innerhalb eines lokal-realistischen Rahmens beschrieben werden können. Diese Frage spielt seit der Veröffentlichung des berühmten Einstein-Podolsky-Rosen "Paradoxons" [1] eine fundamentale Rolle in der Begründung der Quantenmechanik. Das beschriebene Experiment ist ein Test der CHSH Form [2] der Bell'schen Ungleichung [3] und schließt gleichzeitig zwei der drei "Schlupflöcher" für lokalen Realismus, die in einem experimentellen Test der Bell'schen Ungleichung auftreten können. Es sind dies das *Locality* und das *Freedom-of-choice* Schlupfloch. Letzteres wurde bis heute experimentell nicht adressiert und zu allererst in unserem Experiment durch raumzeitliche Trennung der Wahl der Analysatorstellung und der Photonemission geschlossen. Das dritte Schlupfloch, das *Fair-sampling* Schlupfloch [4], konnte wegen zu niedriger Detektionseffizienz leider nicht geschlossen werden. Da unser Experiment jedoch das Erste ist, das mehr als ein Schlupfloch gleichzeitig schließt und die CHSH Ungleichung mit mehr als 16 Standardabweichungen durch $S_{exp} = 2.37 \pm 0.023$ verletzt, repräsentieren unsere Resultate die bis heute schlüssigste Verletzung des lokalen Realismus. Gleichzeitig stellt unser Experiment einen wichtigen Schritt in Richtung eines vollkommen schlupflochfreien Bell Tests dar, eine der bedeutensten ungelösten Herausvorderungen der fundamentalen Physik.

Im zweiten Experiment werden die faszinierenden Eigenschaften verschränkter Photonen ausgenutzt, um die verschränkungsbasierte "Verteilung" quantenkryptographischer Schlüssel (quantum key distribution, QKD) zu demonstrieren. Diese technische Anwendung quantenmechanischer Eigenschaften ist wohl eine der ausgereiftesten im Bereich der Quanteninformation und Quantenkommunikation. Für QKD Experimente bei denen man hohen Abschwächungen im Quantenkanal ausgesetzt ist, wie etwa in zukünftigen satellitenbasierten Netzwerken oder Glasfasernetzwerken, ist es wichtig die effizientesten Systeme zu verwenden. Es wurde kürzlich gezeigt [5], dass QKD mit verschränkten Photonen höhere Abschwächungen tolerieren kann als Systeme die auf schwachen Laserpulsen basieren. Das ist vorallem der Fall, wenn die Quelle verschränkter Photonen symmetrisch zwischen den Empfängerstationen, Alice und Bob, liegt. In unserem Experiment untersuchen wir diesen wichtigen Vorteil eines symmetrischen Systems und implementieren drei unterschiedliche experimentelle Aufbauten. Diese benutzen einen 144 km langen optischen Kanal zwischen den kanarischen Inseln La Palma und Teneriffa und weisen Photonpaar Abschwächungen von 35 dB, 58 dB beziehungsweise 71 dB auf. Dabei wurde die Quelle der verschränkten Photonenpaare entweder direkt bei Alice, asymetrisch zwischen Alice und Bob oder symmetrisch in der mitte zwischen Alice und Bob platziert.

Wir zeigen, dass unsere experimentellen Resultate sehr gut mit dem theoretischen Modell übereinstimmen, welches auf eine aktuelle Arbeit [5] bezogen ist, jedoch an unsere experimentellen Parameter angepasst wurde. Verglichen mit dem zu erwartenden Photonenverlust bei der Übertragung von einem Satelliten im "low-earth-orbit" (LEO) zur Erde [6] geben unsere Resultate Grund zur Annahme, dass verschränkungsbasierte QKD Systeme geeignet sind, solche Übertragungen sowohl in einem Einzel- als auch Doppellink Szenario [7] durchzuführen.

3. Introduction

Quantum mechanics has had enormous success in explaining many of the features of our world. Much of the modern technology operates at a scale, where quantum effects are significant (e.g. the laser, the electron microscope and magnetic resonance imaging). The quantum study of semiconductors led to the invention of the diode and the transistor, which are indispensable for modern electronics. Quantum mechanics is commonly accepted as one of the most precise theories of nature.

Today, quantum mechanical systems find fruitful applications in the rapidly growing fields of quantum information and quantum communication due to their intriguing properties of *superposition* and *entanglement*. In quantum computers [8, 9, 10], although they still are just in their infancy, these properties can be used to perform computations much more efficient than their classical counterparts. Specifically, the problem of integer factorization of large numbers can efficiently be solved using Shor's quantum algorithm [11]. This ability would allow a quantum computer to "break" many of the classical cryptographic systems which are in use today. Hence, the development of a real quantum computer represents a serious security problem for the future "electronic" community.

At the same time, quantum mechanical systems, such as single photons, are already implemented for applications in the field of quantum cryptography. They can be used to establish absolutely secure keys between two communicating parties [12, 13, 14]. Thereby, the security of the keys is based on fundamental quantum physical laws (i.e., the *no-cloning theorem* and the *superposition principle*) and not even a quantum computer could "break" them. Hence, the big goal within the quantum cryptography community is to establish a global quantum communication network, which will require the combination of earth based and satellite based quantum cryptographic systems. Over the last few years, many different systems (e.g. based on weak coherent laser pulses or based on entanglement) were developed and successfully tested in real world applications [15, 16, 17, 18, 19, 20, 21]. Building upon these tests, theoretical models have been developed to infer and compare the performance of the various systems when exposed to channel attenuations as expected in future networks. A recently developed theoretical model [5] indicates that entanglement based systems can bridge the largest distances/attenuations (i.e., up to 70 dB two-photon loss), while systems based on weak coherent laser pulses yield the highes key rates in the low to medium loss regime (i.e., from 0 up to approximately 30 dB). Hence it is suggested that entanglement based systems are best suited for communication from a low-earth-orbit (LEO) satellite to an earth-based receiver station, where the single link attenuation is expected to be 35 dB [6, 7, 5]. It was the motivation for the second experiment described in this thesis to perform quantum key distribution experiments with entangled photons in order to experimentally check the theoretical predictions concerning the secure key rates that can be achieved for different setup configurations and total attenuations.

Despite the enormous success of quantum mechanics, quantum theory was and still is often considered incomplete, because the sometimes weird properties of quantum mechanical systems in combination with the classical concepts of locality and realism, lead to conflicts with the theory of special relativity. After some of these conflicts were first identified by Einstein, Podolsky and Rosen [1], it was John Bell in 1964 who discovered a theorem, which enables to experimentally test whether or not these classical concepts can be restored to quantum mechanics by augmenting it with "local hidden variables".

The so-called "Bell inequality" [3] is based on three assumptions: *realism* (objects possess definite properties prior to and independent of observation), *locality* (space-like separated events cannot causally influence each other), and *freedom of choice* (the choice of measurement settings is free or random). It can be violated with entangled quantum systems, but is fulfilled within any "local hidden variable theory", indicating that hidden variables cannot exist. However, in experimental tests of Bell's inequality, there exist "loopholes", which allow observed violations to still be explained by local realistic theories. In recent years, the aim of a completely loophole-free Bell test still motivates scientists to a number of experiments [22, 23, 24, 25, 26]. Out of the many experiments performed [27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 20], just a few have closed individual loopholes, specifically the locality loophole [36] and the fair-sampling loophole[37]. However, Bell's freedom-of-choice assumption (i.e., the choice of the measurement settings must be "*free or random*" [38]) was commonly ignored not only experimentally but also within general discussions about that topic. Moreover, no experiment to date has closed more than one loophole at a time, but for a definitive statement about the existence of hidden variables, all loopholes must be excluded simultaneously in a single experiment. Strictly speaking, the existence of local hidden variables, and therewith the possibility for a local realistic interpretation of quantum mechanical predictions is still not ruled out definitively. This fact was the motivation for the first experiment described in this thesis, with the aim at performing the most conclusive Bell test, possible with nowadays technology.

3.1. Outline of the thesis

In Chapter 4, I will start with a short introduction to the basics of photonic qubits, which are the quantum systems used in the experiments.

The consecutive Chapter 5 is introduced with the famous work from Einstein, Podolsky and Rosen, followed by the response of some contemporary physicists onto the conclusion of the authors. Afterwards, I will consider the properties of local realistic theories (local hidden variable theories) and how Bell derived his theorem based on the differences between their predictions and the predictions of quantum mechanics. Furthermore, the possible loopholes in a Bell experiment will be discussed, followed by a short historic summary of previous experiments.

The main experiment of this thesis will be described subsequently. Chapter 6 starts with considerations about the space-time requirements for closing the locality and freedom-of-choice loopholes and how these requirements can be implemented experimentally. This is followed by a detailed description of the experimental equipment and the actual experi-

mental setup. After presenting the obtained results, the Chapter closes with a conclusion and outlook paragraph.

Chapter 7 starts with an introduction to quantum cryptography, presenting two important quantum key distribution (QKD) protocols, i.e., the coherent state and the entanglement based protocol.

In Chapter 8, I will present our investigations on entanglement based QKD, starting with a description of the theoretical model devised in [5]. Since the experimental equipment is the same as described in Chapter 6, the second experiment in this thesis will be described right away, followed by the presentation and a subsequent discussion of the obtained results. This Chapter closes again with a conclusion and outlook paragraph.

4. The basics of photonic qubits

In this work, I will exclusively consider two-level quantum systems, called *qubits*. In analogy to a classical bit, it's possible "values" are denoted as the two orthonormal basis states $|0\rangle$ and $|1\rangle$. For simplicity, I will base the following introduction to the basic quantum theoretical concepts on the special case of qubits.

4.1. Superposition and Entanglement

In quantum mechanics the state of a system is given by a normalized vector in a complex vector space $\mathcal{H}$, which is called *Hilbert space*. The Hilbert space of qubits is two-dimensional and it is formed by the orthonormal two-dimensional basis vectors $|0\rangle$ and $|1\rangle$ (also know as *computational basis states*).

4.1.1. Superposition

The *superposition principle* allows us to write a general state of a qubit as a linear combination of the basis states:

$$|Q\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{4.1}$$

with the complex coefficients α, β fulfilling the relation

$$|\alpha|^2 + |\beta|^2 = 1. \tag{4.2}$$

4.1.2. Entanglement

A composite quantum system is described in a Hilbert space which is given by the tensor product of its n subsystem spaces:

$$\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i. \tag{4.3}$$

In the special case of $n = 2$ (i.e., a two-qubit composite system) the states

$$\begin{aligned} |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 \pm |1\rangle_1 \otimes |0\rangle_2) \\ |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |0\rangle_2 \pm |1\rangle_1 \otimes |1\rangle_2) \end{aligned} \tag{4.4}$$

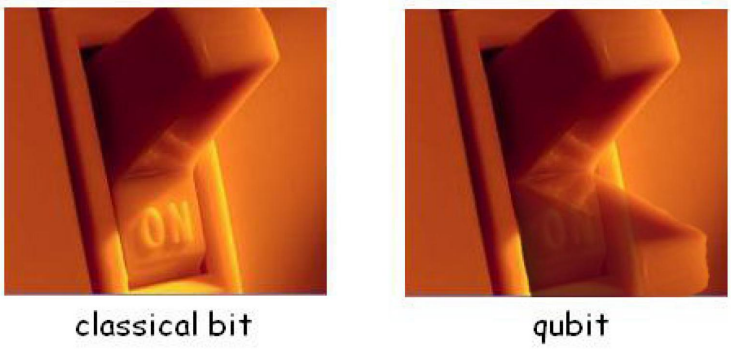

Figure 4.1.: An illustration of the difference between classical bits and qubits. The classical bit is always in a well defined state while qubits can also exist in a superposition of states. (Figure taken from [39])

form an orthonormal basis of the corresponding four-dimensional Hilbert space. These states are not separable, i.e., they cannot be written as a tensor product of their subsystems. In quantum mechanics, such non-separable states are called *entangled*. In contrast, a state of a classical composite system is simply given by the tensor product of its subsystem states and therefore always separable.

The four states (4.4) are called *Bell states*. They are maximally entangled, meaning that a measurement in the computational basis on either qubit will yield a random result (i.e., with probability $\frac{1}{2}$ either $|0\rangle$ or $|1\rangle$), while a joint measurement on both qubits will always reveal perfect correlations (for the $|\Phi^{\pm}\rangle$-states) or perfect anti-correlation (for the $|\Psi^{\pm}\rangle$-states). It will be shown later that these correlations are stronger than could possibly exist in classical systems.

4.2. Photonic qubits

In the experiments described here, the qubit is realized with two orthogonal polarization states of a single photon (e.g. the horizontal polarization state $|H\rangle$ for $|0\rangle$ and the vertical polarization state $|V\rangle$ for $|1\rangle$). Any arbitrary polarization state can be obtained via a superposition of the horizontal and vertical state (see Table 4.1).

The advantage of using photonic qubits is that they can be easily generated, controlled and their states manipulated with rather simple linear optical devices (e.g. wave plates). A convenient way to consider the polarization states and the action of wave plates is to look at the geometrical representation of the polarization states on the *Poincaré-Sphere* (see Figure 4.2). Since the qubit state is normalized (see Equation (4.2)) its state can also be written as

$$|Q\rangle = \cos\frac{\theta}{2}|H\rangle + \mathrm{e}^{i\varphi}\sin\frac{\theta}{2}|V\rangle, \tag{4.5}$$

where the angles θ and φ define a point on the three-dimensional unit sphere, as shown

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 4.1.: The most important polarization states of a photonic qubit. Any polarization state can be obtained via a linear combination of horizontal and vertical polarization. The linear polarization states are often assigned with the corresponding linear polarization angles.

in Figure 4.2. A half wave plate (HWP) rotates the polarization state in the equatorial plane (i.e., the plane of the linear polarization states), while a quarter wave plate (QWP) in general converts linear polarization into elliptical polarization.

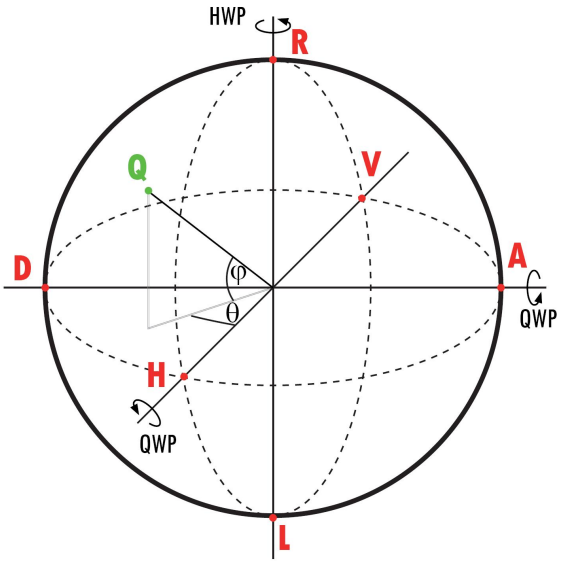

Figure 4.2.: The Poincaré-Sphere for the polarizations states of a qubit. The actions of a half wave plate (HWP) and a quarter wave plate (QWP) on the polarization state can be described by rotations around the corresponding axes, as illustrated in the Figure.

4.3. No-cloning theorem

In quantum mechanics, it is not possible to copy an arbitrary unknown quantum state of a qubit exactly onto a different qubit, while leaving the original qubit undisturbed. This

is known as the *no-cloning theorem* and was first shown in [40]. As illustration, one can imagine a simple copying device which copies the state of one qubit (A) onto another (B) and leaves the original state undisturbed. This device performs the following operations:

$$\begin{aligned} |0\rangle_A|0\rangle_B &\longrightarrow |0\rangle_A|0\rangle_B \\ |1\rangle_A|0\rangle_B &\longrightarrow |1\rangle_A|1\rangle_B. \end{aligned} \tag{4.6}$$

In contrast to a classical bit, the input qubit can be in the superposition state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Due to the linearity of quantum mechanics and Equations (4.6), the copying device would produce the following output for the superposition state:

$$\frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)\,|0\rangle_B \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)\,, \tag{4.7}$$

which is an entangled state and obviously different from the desired output state

$$\begin{aligned} \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)\,|0\rangle_B \quad &\longrightarrow \quad \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A)\,\frac{1}{\sqrt{2}}(|0\rangle_B + |1\rangle_B) \\ &= \quad \frac{1}{2}(|0\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)\,. \end{aligned} \tag{4.8}$$

So generally, a quantum cloning device cannot exist. However, there exist optimal cloning strategies [41] for general states. E.g. a cloning machine where the state of one input qubit is transferred onto two identical output qubits can achieve a successful cloning probability of $\frac{5}{6}$ [42].

4.4. Density matrices

A convenient way for describing quantum systems is the *density matrix* formalism, especially if the system is not known completely. In this case, the system is described by a *mixed state* and its corresponding density matrix is given by

$$\rho_{mixed} = \sum_i p_i |\phi_i\rangle\langle\phi_i|, \tag{4.9}$$

where $|\phi_i\rangle$ is an orthonormal set of states in the corresponding Hilbert space and p_i are the probabilities for the system to be in the state $|\phi_i\rangle$. Since p_i are probabilities, they have to fulfill the relations $0 \leq p_i \leq 1$ and $\sum_i p_i = 1$, which are equivalent to the statement that a density matrix must be Hermitian and its trace must be one:

$$\mathrm{Tr}(\rho_{mixed}) = 1. \tag{4.10}$$

A system is described by a *pure state*, if there exists a measurement whose outcome has a definite value. A pure state $|\psi\rangle$ describes a system completely and therefore, its density matrix can simply be written as the projector

$$\rho_{pure} = |\psi\rangle\langle\psi|, \tag{4.11}$$

Obversely, a density matrix ρ describes a pure state, if and only if $\rho^2 = \rho$.

For a qubit, the density matrix is a Hermitian 2×2 matrix and can thus be written as a linear sum of the *Pauli matrices*:

$$\rho_{qubit} = \sum_{k=0}^{3} c_k \sigma_k, \tag{4.12}$$

with

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{4.13}$$

the constants c_k ($c_0 = \frac{1}{2}$) and the 2×2 identity matrix σ_0.

4.5. Measurement

In quantum mechanics, a measurement is described as an interaction of the quantum system with a classical measurement device. This interaction is characterized by an observable, which is given by a Hermitian operator in Hilbert space. The possible values of an observable are the eigenvalues of the corresponding operator. Formally, a measurement is simply described by a projection of the measured state $|\varphi\rangle$ onto one of the operator's eigenvectors $|k_i\rangle$ corresponding to an eigenvalue c_i. Hence, a measurement operator is also called projector and consequently, such measurements are called *projective measurements*. The probability that a measurement yields a certain eigenvalue c_i is given by

$$p(c_i) = |\langle k_i|\varphi\rangle|^2. \tag{4.14}$$

In the density matrix formalism, the same probability is given by

$$p(c_i) = \mathrm{Tr}\{|k_i\rangle\langle k_i|\rho\}. \tag{4.15}$$

Furthermore, the expectation value for the state $|\varphi\rangle$ and an operator A is given by

$$\langle A\rangle = \langle\varphi|A|\varphi\rangle. \tag{4.16}$$

In comparison, the expectation value of the operator can also be found by calculating the trace over its product with the density matrix ρ of the system.

$$\langle A\rangle_\rho = \mathrm{Tr}\{A\rho\}. \tag{4.17}$$

4.6. State tomography

State tomography is the procedure of experimentally determining the complete density matrix of an unknown quantum state. In the case of two photonic qubits, the polarization

state of the two photons can be fully determined by taking a set of 16 projective measurements [43, 44]. These are given by all possible permutations of the projector $\mu_i \otimes \mu_j =: \mu_{ij}$ $(i, j = 0, 1, 2, 3)$, with

$$\begin{aligned} \mu_0 &= |H\rangle\langle H|, \quad \mu_2 = |D\rangle\langle D| \\ \mu_1 &= |V\rangle\langle V|, \quad \mu_3 = |R\rangle\langle R|. \end{aligned} \tag{4.18}$$

The density operator describing a two-qubit state is a 4×4 matrix with 16 real parameters (of which 15 are independent). The density matrix is often reconstructed using *maximum likelihood estimation*, i.e., searching for the density matrix which maximizes the likelihood of giving the experimental results[1]. For a two-qubit state with a given density matrix ρ, the average number of coincidence counts in the detectors C_{ij}, when measuring the operator μ_{ij}, can be calculated by $C_{ij} = \mathcal{N} \cdot \mathrm{Tr}(\rho \cdot \mu_{ij})$, where $\mathcal{N}$ is a constant that can be obtained from the experimental data. While giving a close fit to the data, the maximum likelihood estimation also guarantees the state to be theoretically valid.

One measure to compare the reconstructed density matrix with a pure target state $|\psi\rangle$ is the fidelity $\mathfrak{F}$, defined as

$$\mathfrak{F} = \langle\psi|\rho|\psi\rangle. \tag{4.19}$$

Furthermore, a useful measure for the amount of entanglement is the concurrence $\mathcal{C}$ [45, 46], which is defined as

$$\mathcal{C} = \max\left\{\sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}, 0\right\}. \tag{4.20}$$

λ_i are, in decreasing order, the eigenvalues of the product of ρ and it's "spin-flipped" version $(\sigma_2 \otimes \sigma_2)\rho^*(\sigma_2 \otimes \sigma_2)$, with the complex conjugated density matrix ρ^* and the Pauli matrix σ_2 (see Equation (4.13)). A more sensitive measure of entanglement is the *tangle* $\mathcal{T}$ which is simply given by the square of the concurrence

$$\mathcal{T} = \mathcal{C}^2. \tag{4.21}$$

For non-entangled states $\mathcal{T} = 0$ and for maximally entangled states $\mathcal{T} = 1$. For a comprehensive discussion of that topic please refer to [45, 46].

[1] Usually, the maximum likelihood estimation is implemented using mathematic computer packages (e.g. `Mathematica` or `MatLab`).

5. Local realism vs. quantum mechanics

In a realistic worldview, such as in classical physics, physical objects posses well defined properties at any time and independent of observation. Measurements are just a tool to reveal those preexisting properties – the measurement outcome is predetermined[1]. There exists only *subjective* randomness, i.e., random results are just due to the lack of knowledge of the observer about the measured system.

It is different in standard quantum mechanics, where a measurement projects the state of an object with a certain probability onto one of the eigenstates of the observable. If the measured state was in a superposition of the observable's eigenstates, the results obtained are *objectively* random – it seems as if the measurement creates and defines the reality of the object. Moreover, quantum mechanics predicts that the properties of an object (e.g. it's momentum or position) can depend on the type of measurement performed on another object that is far apart. Thus, accepting quantum mechanics one must either "*totally abandon the realistic philosophy of most working scientists, or dramatically revise our concept of space-time*" [50].

Starting in 1935 with the famous paper of Einstein, Podolsky and Rosen (EPR) [1] down to the present day, the question of whether quantum mechanical predictions can be explained by realistic theories is of major scientific and philosophic interest. EPR constructed a thought experiment from which they have concluded that the quantum-theoretical description of physical reality is incomplete, because, holding fast to the concept of *elements of reality* would require "spooky action at a distance". However, they believed that quantum mechanics could be completed. Usually, such a hypothetical completion is described by additional variables which are "hidden" to the observer, but should determine *all* properties of a system at any time. A complete version of quantum mechanics should then allow for a local realistic interpretation of quantum mechanical predictions.

Immediately after EPR's publication, Bohr tried to convince the authors that their conclusion is based on a faulty argumentation [51]. However, at this time most physicists ignored the debate between Bohr and Einstein because it seems that to which position to adhere was a matter of personal taste. This situation changed dramatically when 30 years later John Bell in 1964 came up with a conclusive proof [3], that no completed version

[1] In general, the assumption of realism does not only cover deterministic theories, as suggested here, but also covers stochastic theories with probability distributions instead of deterministic outcome functions [47, 48]. However, these can always be modelled by mixing realistic (deterministic) theories and correlations can be explained by a deterministic local hidden variable model if and only if they can be described by a stochastic one [49]. Thus, stochastic theories are equivalent to deterministic theories in the context of violating Bell's inequality and will not be considered in this thesis.

of quantum mechanics with additional local variables can exist. Later, Bell's theoretical work was adapted by Clauser, Horn, Shimony and Holt (CHSH) [2], such that the question whether or not quantum mechanics can be described by local realistic theories could be tested experimentally.

This Chapter starts with a review of EPR's work, followed by a simplified version of their thought experiment formulated by Bohm. Subsequently, I will briefly outline Bohr's argumentation to refute EPR's conclusion. Afterwards, the concept of local realistic theories using hidden variables will be described, which is followed by the derivation of Bell's theorem and a short history of experiments testing local realism vs. quantum mechanics.

5.1. EPR's argument

The pioneering EPR paper [1] was the first work which discussed the intriguing implications of entanglement. They put forward in very clear words criteria that can be used to define a whole class of physical theories, which today is known as the class of *local-hidden-variable* theories.

The argumentation of Einstein, Podolsky and Rosen is based on three vital assumptions about a physical theory [1]:

- **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., 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.*"

They consider an entangled state of two particles, which are, after initial interaction, spatially separated. This bipartite state is of the form:

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

where the variables x_1 and x_2 describe the position of the particles and x_0 is some constant. If an observer chooses to measure the *momentum* of particle 1 and if the result was $+p$, it can be shown [1] that the state of particle 2 would be projected onto the momentum eigenstate that corresponds to the eigenvalue $-p$. That means, from a momentum measurement on particle 1 one could with certainty (i.e., with probability 1) predict the result of a momentum measurement performed on particle 2 – the momentum $-p$ of particle 2 must therefore correspond to an element of reality.

On the other hand, if the observer chooses to measure the *position* of particle 1 and if the result was x, the state of particle 2 would be projected onto the position eigenstate

that corresponds to the eigenvalue $x + x_0$. That means, from a position measurement on particle 1 one could with certainty predict the result $x + x_0$ of a position measurement on particle 2 – its position is therefore also an element of reality.

Depending on the observer's choice either the momentum or the position of particle 2 would be an element of reality. Since particle 1 and 2 are spatially separated and do no longer interact, the outcome of a measurement on particle 2 cannot depend on anything that is done to particle 1 (i.e., EPR's locality assumption). Thus, the momentum and the position of particle 2 must already be determined at the time the particles separate and due to the reality assumption, both momentum and position of particle 2 must be simultaneous elements of reality. Contrary, in quantum mechanics these two cannot be defined simultaneously to arbitrary precision and therefore cannot be simultaneous elements of reality. EPR conclude their paper with the sentences [1]: *"While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."* Unfortunately, they never proposed a concept of how to possibly complete quantum mechanics.

5.1.1. Bohm version of EPR's thought experiment

Directly connected to EPR, David Bohm formulated a similar thought experiment where he considered entangled spin-$\frac{1}{2}$ particles [52]. For the sake of completeness I will shortly review his work here, but instead of considering spin-$\frac{1}{2}$ particles, I will consider polarization entangled photons, since these are the quantum systems used in the experiments described in this thesis.

Suppose we have two photons in the maximally entangled state:

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

and suppose these two photons are widely separated. The state (5.2) is invariant under rotations and has the same form in all orthogonal bases, specifically in the two complementary bases $|H, V\rangle$ and $|D, A\rangle$ (the polarization states are defined in Table 4.1). An observer can now choose to measure photon 1 in any of these complementary bases. Whichever result is found, photon 2 will be with certainty in the orthogonal state when measured in the same basis as photon 1. But, depending on the observers choice about the measurement on photon 1, either a state in the $|H, V\rangle$ or in the $|D, A\rangle$ basis could be predicted with certainty for photon 2 without disturbing it. According to EPR, these complementary states for photon 2 must be simultaneous elements of reality. This is in contradiction with quantum mechanics, because, if the outcome of a measurement in a basis is certain the results of a measurement in the complementary basis will be random. According to quantum mechanics, two complementary states can never be simultaneous elements of reality.

5.1.2. Bohr's response to EPR

Shortly after the EPR paper was published, in which they conclude that quantum theory is incomplete, Bohr commented on it and tried to reveal a flaw in EPR's argumentation [51]. His major objection was that they ascribed certain properties to a quantum system (i.e., its momentum and its position) in the absence of measurement. According to Bohr's views, observing a quantum object involves a physical interaction with a classical measuring device that results in an uncontrollable "disturbance" of both systems. This disturbance causes the momentum (position) of a particle to become uncertain, after the particle's position (momentum) was measured.

For his argumentation, Bohr considered a measurement device where a diaphragm with a slit, like the other parts of the apparatus, is rigidly fixed to a support which defines the space frame of reference. During a position measurement, "*the momentum exchange between the particle and the diaphragm will, together with the reaction of the particle on the other bodies, pass into this common support, and we have thus voluntarily cut ourselves off from any possibility of taking these reactions separately into account in predictions regarding the final result of the experiment, – say the position of the spot produced by the particle on the photographic plate* [which is placed behind the diaphragm]" [51]. In other words, after measuring the position of particle 1 of the EPR state (5.1), its momentum becomes uncertain and consequently we also cannot predict the outcome of a momentum measurement on particle 2. Likewise, we cannot predict the outcome of a position measurement on particle 2 after the momentum of particle 1 was measured. In accordance to EPR's locality assumption, particle 2 is not influenced by anything that is done to particle 1. But the information we have about particle 2 directly depends on the kind of measurement that is performed on particle 1. This is essentially different from the concept of "mechanically disturbing" the particle, because the information, which we base our conclusions on, can change instantaneously since both particles are described by a common wave function.

Bohr therefore considered it as necessary that the experimental setup must be included in the definition of the "element of reality" (see Section 5.1). As a consequence, the existence of simultaneous elements of reality as in the EPR paper would be excluded. However, it seems that exactly this was EPR's main criticism on quantum mechanics. They claimed that "[n]*o reasonable definition of reality could be expected to permit* [that the physical quantity of the second system depends] *upon the process of the measurement carried out on the first system, which does not disturb the second system in any way*" [1].

5.2. Local realistic theories

Not only in former times but even today many physicists hold fast to their classical view of reality. Thus it is of great interest to ask, if EPR's suggestion at the end of their paper can in principle be realized: *Can there exist a local realistic theory, which reproduces all quantum mechanical predictions?* Before we can address this question, we have to consider the properties of such a hypothetical theory.

Realism is a concept in which one can think of the statistical element in the quantum mechanical description as arising, because the measured states are just averages over better defined states. These hypothetical states, often called *dispersion free* states, would not only be described by the quantum mechanical state vector but also by additional *hidden variables* (hv) – hidden in a sense, that they are generally inaccessible for measurements. Consequently, objects would at any time and independent of observation posses definite properties.

The values $A_\psi(\lambda)$ of an observable A for a system in the state $|\psi\rangle$ do then also depend on the hidden variables λ. A random result would be due to the fact that an observer does not know the hidden variables associated with the system and not due to objective randomness, as in standard quantum mechanics. The expectation value of the observable in such a hidden variable model is given by

$$E_A^{hv} = \langle A \rangle_\psi = \int_\Lambda A_\psi(\lambda)\rho_\psi(\lambda)d\lambda. \tag{5.3}$$

Here $\rho_\psi(\lambda)$ is the probability distribution over the space Λ of the hidden variables for the state $|\psi\rangle$, with

$$\int_\Lambda \rho_\psi(\lambda)d\lambda = 1. \tag{5.4}$$

Besides the "elements of reality" assumption in Section 5.1, locality is an inevitable ingredient for a well-defined theory in the sense of EPR [1]. It is therefore reasonable to restrict the properties of the hidden variables to be *local*. Consequently, such realistic theories with local hidden variables are called *local realistic* or *local hidden variable* theories (lhv-theories).

According to the quantum mechanical measurement (see Section 4.5), the expectation value of the observable A for a system in the state $|\psi\rangle$ is given by

$$E^{qm} = \langle A \rangle_\psi = \langle \psi | A | \psi \rangle. \tag{5.5}$$

In the end we want the local realistic model to reproduce the quantum mechanical predictions. Thus, the expectation values resulting from quantum theory (5.5) and from the local realistic model (5.3) should be the same for all measurements we could perform.

Von Neumann wrongly claimed to have proven that such realistic models using hidden variables cannot exist in general [53]. His mathematical proof was based on the assumption, that the expectation values of non-commuting observables for dispersion free states must be additive. Following Bell, von Neumann's proof must be rejected, because it is exactly the additivity of the expectation values of non-commuting observables, which is an intriguing property of quantum mechanical states. It cannot be expected "a priori" from the dispersion free states, which should just reveal the quantum mechanical predictions *when averaged over* [54].

To date, the most complete hidden variable theory was formulated by Bohm [55, 56]. Although his model seems to be able to reproduce all quantum mechanical predictions, there exists an explicit causal mechanism whereby, e.g. for the EPR state (5.1), a measurement on particle 1 directly and instantaneously influences the trajectory of the distant particle 2. As Bell accurately formulated [54]:

" In fact the Einstein-Podolsky-Rosen paradox is resolved in the way which Einstein would have liked least."

5.3. Bell's theorem

After Von Neumann's failed proof and after Bohm's formulation of a non-local hidden variable model, Bell pursued and tried to find another proof whether or not quantum mechanics could be augmented with local hidden variables. In 1964, he came up with his famous theorem, where it is proven that quantum mechanical predictions cannot be reproduced by local hidden variable theories in general [3].

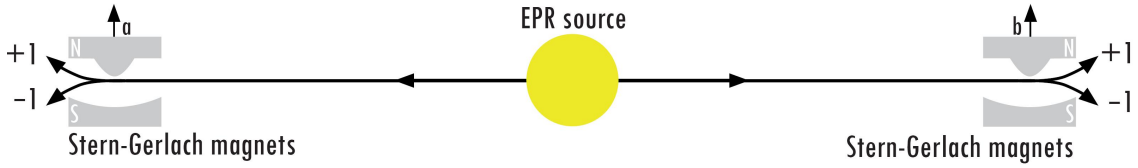

Figure 5.1.: An EPR source emits pairs of spin-$\frac{1}{2}$ particles in an entangled state. Stern-Gerlach magnets analyze the spin along different directions with the possible outcomes ± 1.

Bell considers a pair of spin-$\frac{1}{2}$ particles in the singlet spin state, which freely move in opposite directions:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_1|\downarrow\rangle_2 - |\downarrow\rangle_1|\uparrow\rangle_2), \tag{5.6}$$

where $|\uparrow\rangle$ ($|\downarrow\rangle$) denotes the eigenstate of the spin's z-component with eigenvalue $+1$ (-1). Suppose both particles are measured, using Stern-Gerlach magnets, along directions given by the unit vectors $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$, respectively. The results on both sides will either be $+1$ or -1 and according to quantum mechanics, the results are always anti-correlated when particle 1 and 2 are measured along the same direction. Now Bell assumes that the measurements are made at places remote from one another, such that the orientation of one magnet can neither influence the orientation of nor the result obtained with the other magnet. According to quantum mechanics, the result of a measurement along any direction on particle 2 can be predicted in advance by previously measuring particle 1 along the same direction. Within local hidden variable theories, it follows that the result of any such measurements must be predetermined. According to EPR any component of $\overrightarrow{\sigma}$ is therefore an element of reality, where $\overrightarrow{\sigma} = (\sigma_x, \sigma_z, \sigma_z)$ is the vector of the Pauli matrices (4.13).

From Bell's assumptions it follows that the result A of measuring $\overrightarrow{\sigma_1} \cdot \hat{\mathbf{a}}$ (i.e., a measurement of the spin along $\hat{\mathbf{a}}$) on particle 1 can only depend on the local setting $\hat{\mathbf{a}}$ and on the hidden variables λ. In the same way, the result B of measuring $\overrightarrow{\sigma_2} \cdot \hat{\mathbf{b}}$ on particle 2 only depends on the setting $\hat{\mathbf{b}}$ and λ. The possible measurement results are:

$$A(\hat{\mathbf{a}}, \lambda) = \pm 1, \quad B(\hat{\mathbf{b}}, \lambda) = \pm 1. \tag{5.7}$$

The expectation value for a joint measurement on both particles given by a local realistic theory can therefore be written as

$$E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) = \int_{\Lambda} d\lambda \rho(\lambda) A(\hat{\mathbf{a}}, \lambda) B(\hat{\mathbf{b}}, \lambda). \tag{5.8}$$

This local realistic model should reproduce the quantum mechanical expectation value

$$E^{qm}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) = \langle \psi^- | \overrightarrow{\sigma_1} \cdot \hat{\mathbf{a}} \otimes \overrightarrow{\sigma_2} \cdot \hat{\mathbf{b}} | \psi^- \rangle = -\hat{\mathbf{a}} \cdot \hat{\mathbf{b}}. \tag{5.9}$$

Thus, at first the following obvious relations must be fulfilled:

$$\begin{aligned} E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{a}}) &= E^{qm}(\hat{\mathbf{a}}, \hat{\mathbf{a}}) = -1 \\ E^{lhv}(\hat{\mathbf{a}}, -\hat{\mathbf{a}}) &= E^{qm}(\hat{\mathbf{a}}, -\hat{\mathbf{a}}) = +1 \\ E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{a}}^{\perp}) &= E^{qm}(\hat{\mathbf{a}}, \hat{\mathbf{a}}^{\perp}) = 0. \end{aligned} \tag{5.10}$$

Because $\rho(\lambda)$ is a normalized probability distribution it follows from the first relation in (5.10) that

$$A(\hat{\mathbf{a}}, \lambda) = -B(\hat{\mathbf{a}}, \lambda). \tag{5.11}$$

Then, Equation (5.8) can be rewritten

$$E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) = -\int_{\Lambda} d\lambda \rho(\lambda) A(\hat{\mathbf{a}}, \lambda) A(\hat{\mathbf{b}}, \lambda). \tag{5.12}$$

Since $A^2(\hat{\mathbf{b}}, \lambda) = 1$ and using Equations (5.7), one obtains for another unit vector $\hat{\mathbf{c}}$:

$$\begin{aligned} E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{c}}) &= -\int_{\Lambda} d\lambda \rho(\lambda) [A(\hat{\mathbf{a}}, \lambda) A(\hat{\mathbf{b}}, \lambda) - A(\hat{\mathbf{a}}, \lambda) A(\hat{\mathbf{c}}, \lambda)] \\ &= \int_{\Lambda} d\lambda \rho(\lambda) A(\hat{\mathbf{a}}, \lambda) A(\hat{\mathbf{b}}, \lambda) [A(\hat{\mathbf{b}}, \lambda) A(\hat{\mathbf{c}}, \lambda) - 1]. \end{aligned}$$

Because $A(\hat{\mathbf{a}}, \lambda) A(\hat{\mathbf{b}}, \lambda) \leq 1$ and $A(\hat{\mathbf{b}}, \lambda) A(\hat{\mathbf{c}}, \lambda) - 1 \leq 0$ and using the triangle equation[2], it follows that

$$\begin{aligned} |E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{c}})| &\leq \int_{\Lambda} d\lambda \rho(\lambda) |A(\hat{\mathbf{a}}, \lambda) A(\hat{\mathbf{b}}, \lambda) [A(\hat{\mathbf{b}}, \lambda) A(\hat{\mathbf{c}}, \lambda) - 1]| \\ &\leq \int_{\Lambda} d\lambda \rho(\lambda) |[A(\hat{\mathbf{b}}, \lambda) A(\hat{\mathbf{c}}, \lambda) - 1]| \\ &= \int_{\Lambda} d\lambda \rho(\lambda) [1 - A(\hat{\mathbf{b}}, \lambda) A(\hat{\mathbf{c}}, \lambda)] \\ |E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{c}})| &\leq 1 + E^{lhv}(\hat{\mathbf{b}}, \hat{\mathbf{c}}) \end{aligned} \tag{5.13}$$

This mathematical restriction on local realistic theories is the original form of *Bell's inequality*. It is fulfilled by all local hidden variable models, independent of the choice

[2] *i.e.*, $|x + y| \leq |x| + |y|$.

of the measurement directions. Quantum mechanics maximally violates Equation (5.13), if the unit vectors are chosen such that $\hat{\mathbf{a}} \cdot \hat{\mathbf{c}} = 0$ and $\hat{\mathbf{a}} \cdot \hat{\mathbf{b}} = \hat{\mathbf{b}} \cdot \hat{\mathbf{c}} = \frac{1}{\sqrt{2}}$. Inserting the quantum mechanical expectation value (5.9) for the state (5.6) into Equation (5.13) yields the contradiction

$$\frac{1}{\sqrt{2}} \leq 1 - \frac{1}{\sqrt{2}}. \tag{5.14}$$

From this, Bell himself concluded that in a theory in which hidden variables are added to quantum mechanics, there must be a non-local mechanism whereby a measurement device has an instantaneous influence on the result obtained with another distant measurement device. Such a theory could not be Lorentz invariant. In his eyes, it is also conceivable that quantum mechanical predictions are of limited validity and may apply only to experiments, in which a signal with velocity less than or equal to the speed of light can influence the measurements. In this context, Bell considered it as crucial to perform experiments in which the settings are changed during the flight of the particles, as proposed by Bohm and Aharonov [52].

5.3.1. CHSH inequality

The derivation of Bell's theorem was based on the perfect correlation given in Equations (5.10). In an experiment, these would require perfect measurement devices and a perfectly pure $|\psi^-\rangle$ state, both of them unavailable in practice. In 1969, Clauser, Horn, Shimony and Holt (CHSH) derived an inequality based on Bell's theorem, which does not require perfect correlations and is thus applicable for experiments [2]. Another important but practical difference to Bell's original inequality is that the measurement devices are allowed to fail to register one or both particles.

Here I will not review the original work of Clauser, Horn, Shimony and Holt, but I will follow Bell's more general way to derive the CHSH inequality [57].

Instead of the perfect measurement results (5.7) we now have the averages $\overline{A}(\hat{\mathbf{a}}, \lambda)$ and $\overline{B}(\hat{\mathbf{b}}, \lambda)$ with

$$|\overline{A}(\hat{\mathbf{a}}, \lambda)| \leq 1, \quad |\overline{B}(\hat{\mathbf{b}}, \lambda)| \leq 1. \tag{5.15}$$

For two alternative measurement directions $\hat{\mathbf{a}}'$ and $\hat{\mathbf{b}}'$, we have

$$\begin{aligned} E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}') &= \int_\Lambda d\lambda \rho(\lambda)[\overline{A}(\hat{\mathbf{a}}, \lambda)\overline{B}(\hat{\mathbf{b}}, \lambda) - \overline{A}(\hat{\mathbf{a}}, \lambda)\overline{B}(\hat{\mathbf{b}}', \lambda)] \\ &= \int_\Lambda d\lambda \rho(\lambda)[\overline{A}(\hat{\mathbf{a}}, \lambda)\overline{B}(\hat{\mathbf{b}}, \lambda)(1 \pm \overline{A}(\hat{\mathbf{a}}', \lambda)\overline{B}(\hat{\mathbf{b}}', \lambda)] \\ &\quad - \int_\Lambda d\lambda \rho(\lambda)[\overline{A}(\hat{\mathbf{a}}, \lambda)\overline{B}(\hat{\mathbf{b}}', \lambda)(1 \pm \overline{A}(\hat{\mathbf{a}}', \lambda)\overline{B}(\hat{\mathbf{b}}, \lambda)]. \end{aligned}$$

Using (5.15) one obtains

$$\begin{aligned} |E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}}, \hat{\mathbf{b}}')| &\leq \int_\Lambda d\lambda \rho(\lambda)(1 \pm \overline{A}(\hat{\mathbf{a}}', \lambda)\overline{B}(\hat{\mathbf{b}}', \lambda) \\ &\quad + \int_\Lambda d\lambda \rho(\lambda)(1 \pm \overline{A}(\hat{\mathbf{a}}', \lambda)\overline{B}(\hat{\mathbf{b}}, \lambda), \end{aligned}$$

or

$$|E^{lhv}(\hat{\mathbf{a}},\hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}},\hat{\mathbf{b}}')| \;\leq\; 2 \pm E^{lhv}(\hat{\mathbf{a}}',\hat{\mathbf{b}}') - E^{lhv}(\hat{\mathbf{a}}',\hat{\mathbf{b}}).$$

Written in a more symmetric form, one gets the CHSH inequality:

$$S^{lhv}(\hat{\mathbf{a}},\hat{\mathbf{b}},\hat{\mathbf{a}}',\hat{\mathbf{b}}') := |E^{lhv}(\hat{\mathbf{a}},\hat{\mathbf{b}}) - E^{lhv}(\hat{\mathbf{a}},\hat{\mathbf{b}}')| + |E^{lhv}(\hat{\mathbf{a}}',\hat{\mathbf{b}}) + E^{lhv}(\hat{\mathbf{a}}',\hat{\mathbf{b}}')| \leq 2. \tag{5.16}$$

For $\hat{\mathbf{a}}' = \hat{\mathbf{b}}'$ and assuming perfect anti-correlation $E^{lhv}(\hat{\mathbf{a}},\hat{\mathbf{a}}) = -1$ the CHSH inequality would yield the original form of Bell's inequality (5.13). If we now restrict our unit vectors to lie in one plane in the three dimensional space, we can substitute them with the corresponding angles $\alpha, \beta, \alpha', \beta'$ and the quantum mechanical expectation value becomes $E^{qm}(\hat{\mathbf{a}},\hat{\mathbf{b}}) = -\cos(\beta - \alpha)$. Choosing $\alpha = 0, \beta = 45°, \alpha' = 90°, \beta' = 135°$ results in the strongest violation of the CHSH inequality with

$$\begin{aligned} S^{qm}(\alpha,\beta,\alpha',\beta') &= |-\cos(45°) + \cos(135°)| + |-\cos(45°) - \cos(-45°)| \\ &= \left|-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right| + \left|-\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\right| = 2\sqrt{2} \geq 2 \end{aligned} \tag{5.17}$$

5.4. Loopholes

If a Bell-type inequality is violated by experiment, there may exist *loopholes*, which would allow the obtained violation to still be explained by a local realistic model. There are essentially three loopholes, two of them are directly connected to the assumptions that were made to derive the Bell inequality but one arises from experimental imperfections. To understand them more precisely, let me briefly recall Bell's assumptions for the derivation of his theorem. Afterwards, I will discuss how they are connected to the possible loopholes and how the loopholes can be closed in an experiment.

5.4.1. Bell's assumptions

The most basic assumption is that of realism. Properties of objects should always be predetermined and independent of observation. This implies for a theoretical description that there exist deterministic outcome functions for the results of measurements performed on objects. For the situation considered by Bell, the outcome of the measurement on either particle could in principle depend on the measurement result of the other particle A and B, respectively, on both measurement settings $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ and of course on the hidden variables λ:

$$\textbf{Realism:} \quad A = A(B,\hat{\mathbf{a}},\hat{\mathbf{b}},\lambda), \;\; B = B(A,\hat{\mathbf{b}},\hat{\mathbf{a}},\lambda). \tag{5.18}$$

Realism is an assumption about the physical world and no experiment has yet been proposed, which could directly determine its validity. Today there is no loophole known which can be assigned with this assumption.

Locality is the next assumption and imposes that 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" [1]. Locality can be divided into two separate assumptions [58]. The first of which is called the *outcome independence* assumption, i.e., the result of a measurement on one particle does not influence the result on the other side. The second assumption considers *setting independence* and requires that the measurements are arranged such that the measurement result on one side cannot be influenced by the measurement setting on the other side. From these two assumptions it follows that Equation (5.18) must be rewritten in the form Bell used for the derivation of his theorem (see Equation (5.7)). The locality assumption can formally be emphasized by

$$\textbf{Locality:} \quad A \neq A(B, \hat{\mathbf{b}}), \;\; B \neq B(A, \hat{\mathbf{a}}). \tag{5.19}$$

Bell's third vital assumption requires that the measurement settings for particle 1 and 2 are not influenced by the particle source or generally by the hidden variables. In Bell's original work this was not pointed out explicitly, but in a later work [38] he emphasized that it is important that the settings $\hat{\mathbf{a}}$ and $\hat{\mathbf{b}}$ "*can be considered to be free or random*". This can only be guaranteed, if the corresponding *setting choices* are truly free or random, because then "*they are not influenced by the hidden variables* [and] *the resultant values for* $\hat{\mathbf{a}}$ *and* $\hat{\mathbf{b}}$ *do not give any information about* λ" [38]. Formally this assumption can be written as

$$\textbf{Freedom of choice:} \quad \hat{\mathbf{a}} \neq \hat{\mathbf{a}}(\lambda), \;\; \hat{\mathbf{b}} \neq \hat{\mathbf{b}}(\lambda). \tag{5.20}$$

5.4.2. Locality loophole

This loophole arises in a Bell experiment if the locality assumption is not guaranteed, i.e., if the measurement result on one side can in principle be causally influenced by a physical signal from the measurement or the setting choice on the other side. This is the case in experiments with static setups, because there the settings "*are made sufficiently in advance to allow them to reach some mutual rapport by exchange of signals with velocity less than or equal to that of light*" [38]. According to special relativity, the velocity of a physical signal is limited by the speed of light. If space-time events are *space-like separated*, special relativity guarantees that no physical signal (subluminal or luminal) can travel between them. Thus, the best available way to close the locality loophole in an experiment is to space-like separate every measurement event on one side from both the measurement (outcome independence) and setting choice (setting independence) on the other side.

5.4.3. Freedom-of-choice loophole

The freedom-of-choice loophole arises, if the setting choices could in principle be causally influenced by the hidden variables or vice versa, because then the corresponding settings cannot be considered as free or random, as required by Bell. To close this loophole, Bell imagined an experiment where the two sides are separated by "*a distance of order light minutes* [and the settings] *being freely chosen at the last second by two different experimentalists, or some other random device*" [38]. However, with nowadays technology

the distance required for closing this loophole can be reduced using a fast random device, which determines the measurement settings for the Bell experiment. To guarantee that the output of this random device is truly random, it is further necessary to space-like separate the device's random process from the particle emission. Then, no physical signal from the hidden variables, which are created simultaneously with the particles at the source, can influence the random choices and the corresponding measurement settings give no information about the hidden variables. Without this space-like separation there might be some unknown mechanism which would allow the source of particles to causally influence the processes in the random device[3].

5.4.4. Fair-sampling loophole

A third loophole, often called the fair-sampling loophole, arises from experimental imperfections, i.e., inefficient particle collection and detection. It suggests that, if only a fraction of generated particles is observed, this may not be a representative subensemble [4]. One could then construct a local realistic theory, where the hidden variables influence the chance for the particles of being detected such that the subensemble violates the Bell inequality although the overall ensemble fulfills it. If the CHSH inequality is used for an experimental Bell test, this loophole can be closed if the overall detection efficiency of the experimental setup is at least 82.8% for either particle [59].

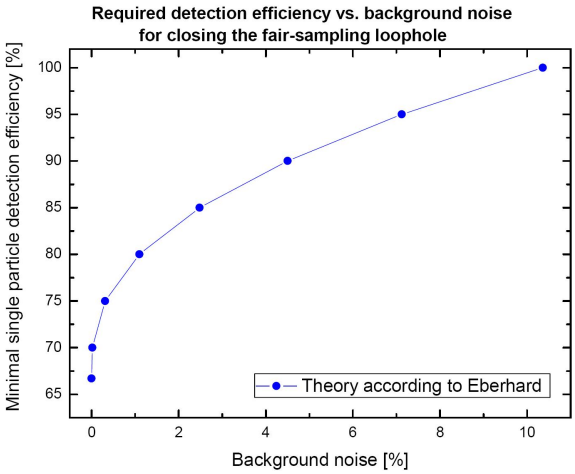

Figure 5.2.: This Figure shows the minimal required single particle detection efficiency for closing the fair-sampling loophole when using an Eberhard-type Bell-inequality [26].

Eberhard realized that this limit can be reduced if one uses non-maximally entangled

[3]It is conceivable that both the source and settings could depend on events in their shared back-ward light cones, so that the settings would still depend on hidden variables. In such "superdeterministic" theories [38, 22], however, choices are never free. "*Perhaps such a theory could be both locally causal and in agreement with quantum mechanical predictions*", as Bell suggests [38].

states [26]. In the case of polarization entangled photons, such a state can be written as

$$|\psi\rangle = \frac{1}{\sqrt{1+r^2}} \left(|H\rangle_1|V\rangle_2 + r|V\rangle_1|H\rangle_2\right), \tag{5.21}$$

with $0 \leq r \leq 1$. Eberhard derived a Bell-type inequality, for which the detection loophole can be closed, if the overall detection efficiency for either particle is at least 66.7%, in the limit of no background noise. Generally, the minimal required efficiency depends on the amount of background noise (see Figure 5.2), and the measurement settings (e.g. for photons the polarization measurement basis) as well as the variable r to violate the inequality must be adapted for the actual efficiency of the experimental setup.

5.5. Previous experiments

Starting in 1972 with an experiment by Freedman and Clauser [27], there have been many experiments performed to test Bell's inequality. The first experiments used cascade transitions in calcium to generate polarization correlated photon pairs. Suffering from very low count rates, the authors were forced to derive more compact inequalities in order to minimize the experimental complexity. As the experiments became more and more accurate, the quantum mechanical predictions were still confirmed. However, the possibility for a local realistic description of quantum mechanics could not be ruled out, because no experiment was able to close the loopholes discussed in Section 5.4. In 1982, Aspect *et al.* [30] performed the first experiment to address the vital time factor in the derivation of Bell's inequality, but the goal to close the locality loophole could not be reached. Based on Aspect's experiment, it was Weihs *et al.* [36] who closed the locality loophole for the first time by space-like separating the required events.

Even though today's photon sources, using parametric down-conversion, are highly efficient, it still seems not possible to close the fair-sampling loophole with photons, because the detection efficiency of state-of-the art single-photon counters is below the minimum requirement for an Eberhard-type Bell inequality of 66.7%. However, in 2001 the fair-sampling loophole was closed by Rowe *et al.* using entangles ions [37]. Their results included almost the whole ensemble of entangled particles but they were not able to close the locality loophole.

To support a short historic summary and to understand the problems that can arise in experimental Bell tests, I will now describe some of the most important experiments performed so far.

5.5.1. 1972 - Freedman and Clauser

Freedman and Clauser used photon pairs with wavelengths of 551.3 nm and 422.7 nm, respectively, emitted in a atomic cascade transition in calcium [27]. The polarization correlated photons were analyzed using polarizers and detected using photomultipliers. The authors recorded the coincidence rate for two-photon detection as a function of the relative angle between the polarizers.

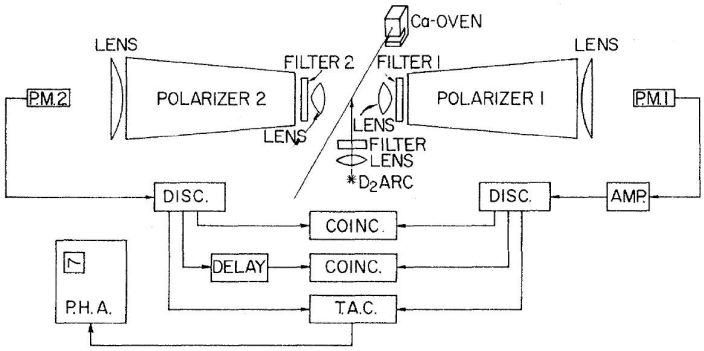

Figure 5.3.: Schematic layout of the experimental setup used by Freedman and Clauser.

To reduce the complexity of the experiment, Freedman and Clauser derived a generalized Bell inequality, simpler and more convenient for their experiment. Testing this inequality required only two different polarizer settings and one measurement without polarizers.

$$\delta = \left| \frac{R(22.5°)}{R_0} - \frac{R(67.5°)}{R_0} \right| - \frac{1}{4} \leq 0, \tag{5.22}$$

with the coincidence rates $R(\alpha)$ for the measurement with polarizers (difference angle α) and R_0 for the measurement without polarizers. Typically obtained coincidence rates ranged from 0.3 s^{-1} to 0.1 s^{-1} and the rate of background coincidences was 0.01 s^{-1} to 0.002 s^{-1}. Measurement runs, each 100 s, were accumulated resulting in a total integration time of 200 h. After background subtraction the authors obtained the result $\delta = 0.050 \pm 0.008$, a clear violation of the inequality (5.22).

Although it was an impressive experiment, considering the technical possibilities at that time, the results cannot rule out local realistic theories, because Bell's assumptions were not experimentally guaranteed.

5.5.2. 1982 - Aspect et al.

Aspect *et al.* [30] realized, that all experiments so far have been performed with static setups in which the polarizers are fixed for the whole measurement run. Using the same atomic cascade transition as Freedman and Clauser, the authors improved on the static setups by implementing an acousto-optical modulator in each arm, which is able to rapidly redirect incident photons from one polarizer to another polarizer by using Bragg-refraction on an ultrasonic standing wave in water. Hence, two polarizers with different orientations could be used in each arm instead of using only one single polarizer [30]. A typical measurement run lasted 12000 s, and testing an inequality similar to the CHSH-inequality yielded the contradiction $0.101 \pm 0.020 \leq 0$.

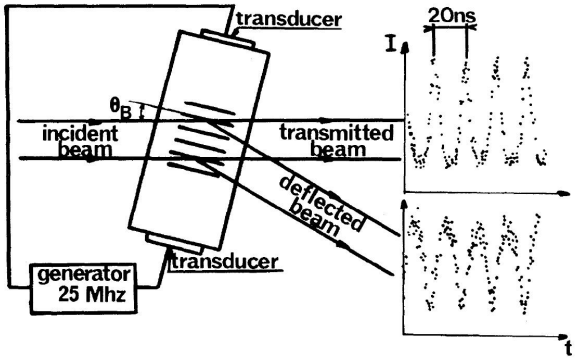

Figure 5.4.: An illustration of the working principle of the acousto-optical switch used by Aspect *et al.* to vary between two different measurement settings.

Aspect argued that in their experiment a detection event on one side was space-like separated from the corresponding measurement orientation change on the other side because the switching period of 10 ns was smaller than the 40 ns photon flight time from the emission to the optical switch. Unfortunately, this wonderful experiment was again not sufficient to close any of the existing loopholes.

The reason therefore was that the switching between the paths to the different polarizers happened quasiperiodic and not truly random. In this case the measurement setting is predetermined long before the corresponding photons are created and thus the setting choices are neither space-like separated from the particle source nor from the detection event on the other side. A short discussion on this experiment was already given in 1986 by Anton Zeilinger [60]. There, the author suggests that "*due to a numerical coincidence between the photon flight time and the switching frequency the time-dependent experiment of Aspect et al. is not conclusive*". However, Aspect *et al.* themselves realized that their experiment was not conclusive and concluded already in their work that a "*more ideal experiment with random and complete switching would be necessary for a fully conclusive argument against the whole class of supplementary-parameter theories obeying Einstein's causality*".

5.5.3. 1998 - Weihs et al.

Weihs *et al.* [36] performed an experiment, which explicitly aimed at closing the locality loophole. They used spontaneous parametric down-conversion in a non-linear crystal to generate polarization entangled photon pairs. In order to achieve a sufficiently large spatial separation between the two observer stations, they sent each photon through a 500 m long optical fiber (250 m of which were left coiled at the source and 250 m were laid out beneath the Innsbruck University science campus), such that the direct distance between the observers was 400 m. For the polarization analysis on both sides, they used electro-optical modulators (EOMs) to switch fast between a polarization rotation of 0°

and 45°, followed by a polarizing beam splitter and two single-photon detectors in each output mode. The EOMs were triggered from independent physical quantum random number generators, sampled at a rate of 10 MHz, to guarantee the randomness of the setting choices. The detection events were recorded using time-tagging units and the coincidence analysis was done long after a measurement run was finished, thus guaranteeing the independence of the two observer stations. Using polarizing beam splitters instead of polarizers enabled them to measure all setting combinations required for testing the CHSH-inequality in one single measurement run.

The authors defined the duration of the measurement as the time from the generation of a random number until the single-photon counter registered a photon. In their case, this time was approximately 100 ns, much shorter than the 1.3 μs separation of the two observers. Weihs and his co-authors violated the CHSH inequality by 30 standard deviations, and thus successfully closed the locality loophole for the first time.

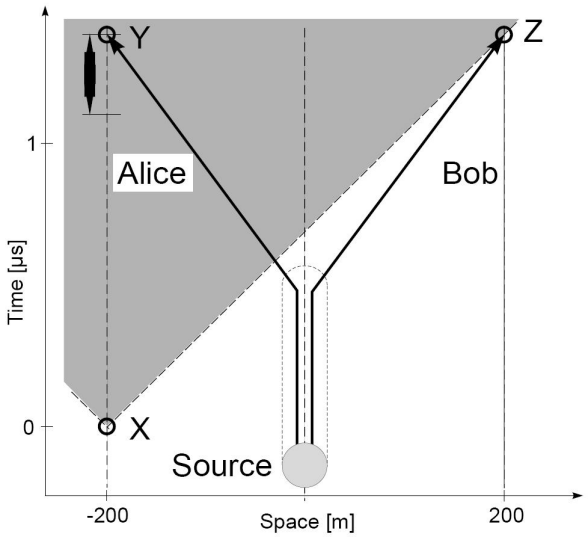

Figure 5.5.: The space-time situation in the experiment by Weihs *et al.* One can see easily that the whole measurement process (indicated by the vertical black bar), including random number generation and detection, lies in the future light cone of the source. Thus the random numbers (i.e., the setting choices) could have been influenced by the hidden variables.

The overall detection and collection efficiency of the experimental setup was 5% and the authors admitted that there are still local realistic interpretations possible, if the detected photon sample is not a faithful representative of the whole ensemble (i.e., the fair-sampling loophole).

As in all previous experiments, it was not discussed in this work either that the freedom-of-choice assumption is also crucial for the derivation of Bell's theorem. It can easily be seen in Figure 5.5 that the actual setting choices were made in the future light cone of the photon emission at the source. Hence, the random numbers cannot be considered as truly free or random, because they could have been influenced by the hidden variables. Obviously, the freedom-of-choice loophole was not closed in this experiment. It is the

motivation for the work presented here to qualitatively repeat the author's achievements and to simultaneously close the freedom-of-choice loophole.

5.5.4. 2001 - Rowe et al.

Rowe *et al.* were the first to close the fair-sampling loophole [37]. They used a pair of $^9Be^+$ two-level entangled ions which are confined along the axis of a linear Pauli trap. The two different states are denoted as $|\uparrow\rangle$ and $|\downarrow\rangle$ and the entangled state is given by

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle |\uparrow\rangle - |\downarrow\rangle |\downarrow\rangle \right). \tag{5.23}$$

The state of an ion was determined by probing the ion with a light pulse from a "detection" laser beam. During this detection pulse, ions in the state $|\downarrow\rangle$ scattered many photons (bright state) and ions in the state $|\uparrow\rangle$ scattered very few photons (dark state). The different states could easily be distinguished with discriminator levels in the number of photons collected with a phototube.

In the language of polarization measurements on photons using polarizers, the state of the ions could be measured along different directions by varying the phase angles of the two detection laser beams. Setting the phase angles $\alpha_1 = -\frac{\pi}{8}$, $\delta_1 = \frac{3\pi}{8}$, $\beta_2 = -\frac{\pi}{8}$ and $\gamma_2 = \frac{3\pi}{8}$ for ion 1 and 2, respectively, enabled the authors violate the CHSH inequality with $S = 2.25 \pm 0.03$. Since essentially any ion could be detected, this experiment successfully closed the fair-sampling loophole.

5.5.5. 2007 - Gröblacher et al.

The experiment by Gröblacher *et al.* aimed not at closing any loophole but it showed that quantum mechanical predictions are not only at variance with local realistic theories but also with a broad class of non-local realistic theories [61]. Their results suggest, that giving up the concept of locality is not sufficient to be consistent with quantum mechanics. It seems to be necessary that also certain features of realism must be abandoned for that purpose.

The authors followed an incompatibility theorem for a class of non-local models formulated by Leggett [62]. They analyzed the assumptions made by Leggett and derived an inequality, suitable for an experimental test of whether quantum mechanics can be described by this class of non-local realistic theories or not. The derived inequality does not explicitly demand locality and thus, measurement outcomes can very well depend on parameters in space-like separated regions. The obtained generalized Leggett-type inequality for non-local hidden variable theories (nlhv theories) reads:

$$S_{nlhv} = |E(\hat{\mathbf{a}}_1, \hat{\mathbf{b}}_1) + E(\hat{\mathbf{a}}_2, \hat{\mathbf{b}}_3)| + |E(\hat{\mathbf{a}}_2, \hat{\mathbf{b}}_2) + E(\hat{\mathbf{a}}_2, \hat{\mathbf{b}}_3)| \leq 4 - \frac{4}{\pi} \left| sin\frac{\varphi}{2} \right|. \tag{5.24}$$

For the inequality to be applied, the unit vectors $\hat{\mathbf{a}}_1$ and $\hat{\mathbf{b}}_1$ have to lie in a plane orthogonal to the plane defined by $\hat{\mathbf{a}}_2$ and $\hat{\mathbf{b}}_2$ with $\angle(\hat{\mathbf{a}}_1, \hat{\mathbf{b}}_1) = \angle(\hat{\mathbf{a}}_2, \hat{\mathbf{b}}_2) = \varphi$ and $\hat{\mathbf{b}}_3 = \hat{\mathbf{a}}_2$ (see Figure 5.6).

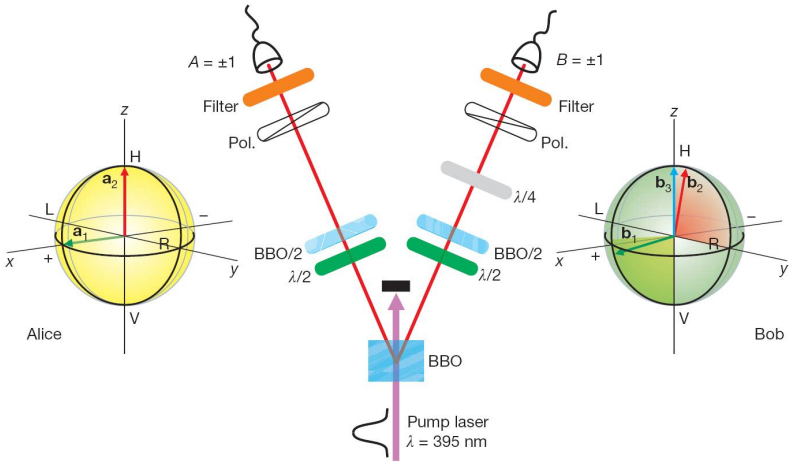

Figure 5.6.: The experimental situation for the test of non-local hidden variable models.

Using polarization entangled photons from spontaneous parametric down conversion the authors were able to violate this inequality with $S_{exp} = 3.8521 \pm 0.0227$ which is 3.2 standard deviations above the non-local realistic bound of $S_{nlhv}^{max} = 3.792$ for the used set of unit vectors. To simultaneously exclude that the obtained correlations could be explained by local realistic theories they used parts of their data to additionally violate the CHSH inequality.

5.5.6. 2007 - Ursin et al.

The experiment by Ursin *et al.* [20] was performed between the Canary Islands, La Palma and Tenerife. I was part of the experimental team performing this experiment during my diploma thesis and although this experiment did not attempt to close any of the loopholes, I want to review it here for several reasons. First, within this experiment the same optical free-space link as in the experiments presented in this thesis was used. Second, entanglement could be successfully verified between photons which were separated by 144 km which today this still is a distance record for free-space entanglement distribution. Additionally, free-space entanglement based quantum key distribution was for the first time successfully demonstrated over such a long distance. All these achievements constitute the cornerstones for the both experiment described in this thesis.

The experiment was conducted on behalf of a proof-of-principle study of the European Space Agency (ESA) with the aim of satellite based quantum communication experiments. The results showed that entanglement can survive such long distances and that ESA's optical ground station (OGS) in Tenerife, originally built for laser communication to and from satellites, is also suitable to receive single-photons. Furthermore, the authors successfully performed quantum key distribution and thus demonstrated, that the intriguing features of entanglement can already be used for 'real world' applications.

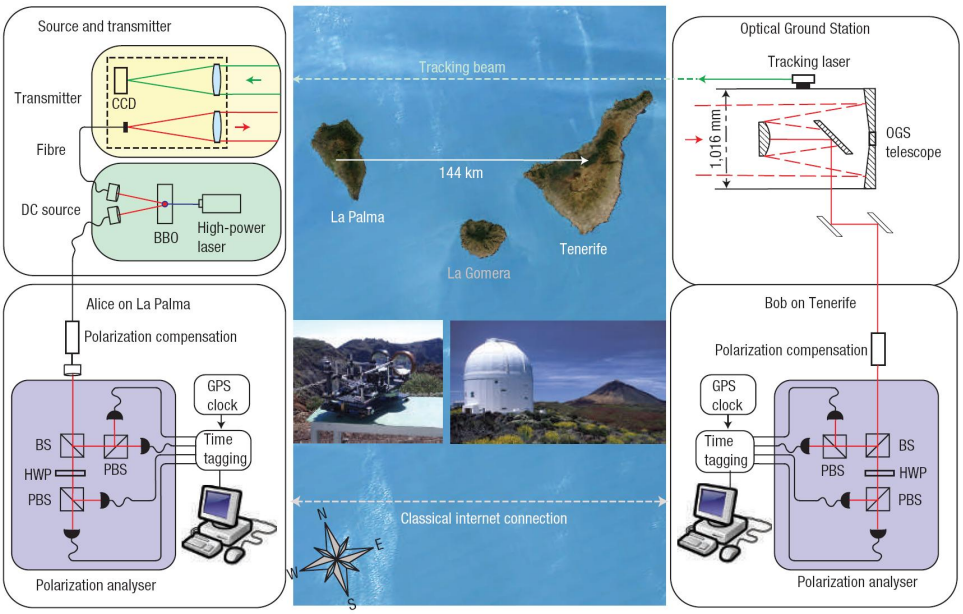

Figure 5.7.: An illustration of the experimental setup in the inter-island experiment from Ursin *et al.*

The experimental setup of this experiment is schematically shown in Figure 5.7. Polarization entangled photon pairs were generated in La Palma via spontaneous parametric down conversion in a non-linear crystal. One photon of each pair was analyzed locally and the other one was sent through a 144 km optical free-space link to Tenerife, where it was received by the OGS telescope. Similar to the experiment by Weihs *et al.*, time-tagging units recorded the detection events on both sides. The analyzer modules passively decided in which basis to analyze incoming photons using a 50/50 beam splitter and thus, this experiment was not able to close any loopholes. However, the CHSH inequality could be violated by 13 standard deviations with $S_{exp} = 2.508 \pm 0.037$, showing that entanglement can survive global distances of up to 144 km without significant loss of quality. Furthermore, the applicability of this setup for quantum communication was demonstrated by generating a quantum cryptographic key. Starting from 417 bits of *raw key* and a quantum bit error ratio of 4.8 % ± 1 %, a *secure key* of 178 bits could be obtained after classical *error correction* and *privacy amplification* .

6. A Bell test under locality and freedom-of-choice conditions

As discussed in Section 5.4, there exist loopholes in an experimental Bell test which allow observed violations of a Bell inequality to still be explained by local realistic theories. Hence, for a definitive statement of whether nature agrees with local realism or quantum mechanics, it is required to close all possible loopholes simultaneously in a single experiment.

The experiment I am going to present in this Chapter is a test of the CHSH-type Bell inequality, with the aim at simultaneously closing the *locality* and the *freedom-of-choice loophole*. For two reasons, its successful realization represents a major step from earlier work towards loophole-free Bell experiments. First, while previous experiments individually closed the locality loophole [36] or the fair-sampling loophole [37], the presented experiment is the first to address the third crucial loophole, i.e. the freedom-of-choice loophole. Second, it is also the first to address two loopholes simultaneously and therefore represents the closest to a loophole-free Bell test to date.

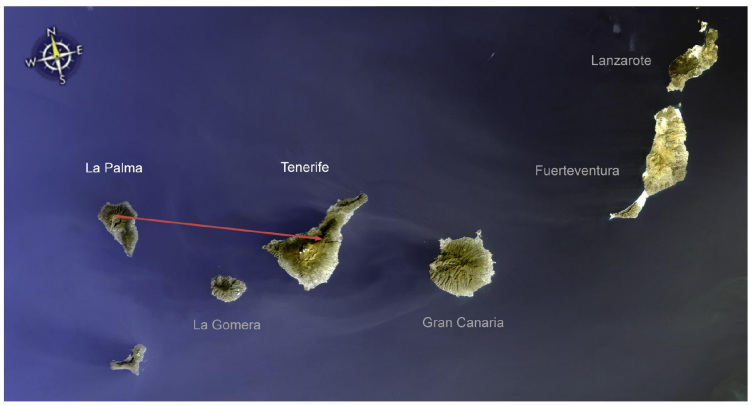

Figure 6.1.: The optical path used in the experiments presented here. (Image by ESA/Envisat.)

The experiment was conducted between the Canary Islands, La Palma and Tenerife, using polarization entangled photons. One photon of an entangled pair was measured next to the source in La Palma, while the other photon was sent through a 144 km free-space link to Tenerife (see Figure 6.1). Although the spatial separation between the observer stations was orders of magnitude larger than actually required for closing the two loopholes, it was easier for us to perform the experiment there, because we were very well

used to the trial sites from previous experiments. Searching for another suitable location and establishing the required infrastructure somewhere else would have been much more complex.

The following sections are structured as follows. With the help of space-time diagrams, I first will consider general space-time arrangements for our purpose. Simultaneously, the requirements to implement such a suitable arrangement experimentally and how it was realized in this work are discussed. Our final setup resulted from many ideas and estimations which can, due to the interdependence of the many experimental parts, hardly be described in a structured and understandable way. Hence, I will describe every experimental part separately and show, why it was implemented correspondingly. Subsequently, I will describe the actual experimental situation from which it should become clear, that the requirements for a Bell test under locality and freedom-of-choice conditions were indeed fulfilled. Within the last sections, I will delineate the measurement procedure and present the experimental results obtained during the measurement campaign.

6.1. Required space-time arrangement for the Bell test

In order to define the required space-time arrangement for our experiment, we first have to consider the basic characteristics of a simple experimental Bell test: Two observers, Alice and Bob, receive (entangled) photons emitted by some *source*. Both choose one out of two possible measurement settings, $\hat{\mathbf{a}}_{1,2}$ and $\hat{\mathbf{b}}_{1,2}$, respectively, and then record their measurement outcome values, A and B. The measurement settings $\hat{\mathbf{a}}_1$, $\hat{\mathbf{a}}_2$, $\hat{\mathbf{b}}_1$ and $\hat{\mathbf{b}}_2$ must be chosen, such that quantum mechanics predicts a violation of the Bell inequality for the correlations obtained between Alice's and Bob's local results.

From the experimental characteristics, we identify the crucial *space-time events* in a Bell experiment which are, together with the corresponding notations, summarized in the following list:

- Alice's and Bob's measurement events $\mathbf{A}$ and $\mathbf{B}$
- Alice's and Bob's setting choice events $\mathbf{a}$ and $\mathbf{b}$
- The photon-pair emission event $\mathbf{E}$

6.1.1. How to close the locality loophole

As discussed in Section 5.4.2, the best available way to close the locality loophole in an experiment is to space-like separate every measurement event $\mathbf{A}$ ($\mathbf{B}$) on one side from both the measurement event $\mathbf{B}$ ($\mathbf{A}$) and setting choice event $\mathbf{b}$ ($\mathbf{a}$) on the other side. Obviously, these space-like separations require the *independence* of Alice's and Bob's measurement devices.

A convenient way to discuss certain space-time arrangements is to look at the corresponding space-time diagrams. A very simple and symmetric space-time diagram is depicted in Figure 6.2. Two photons are transmitted with the vacuum speed of light from

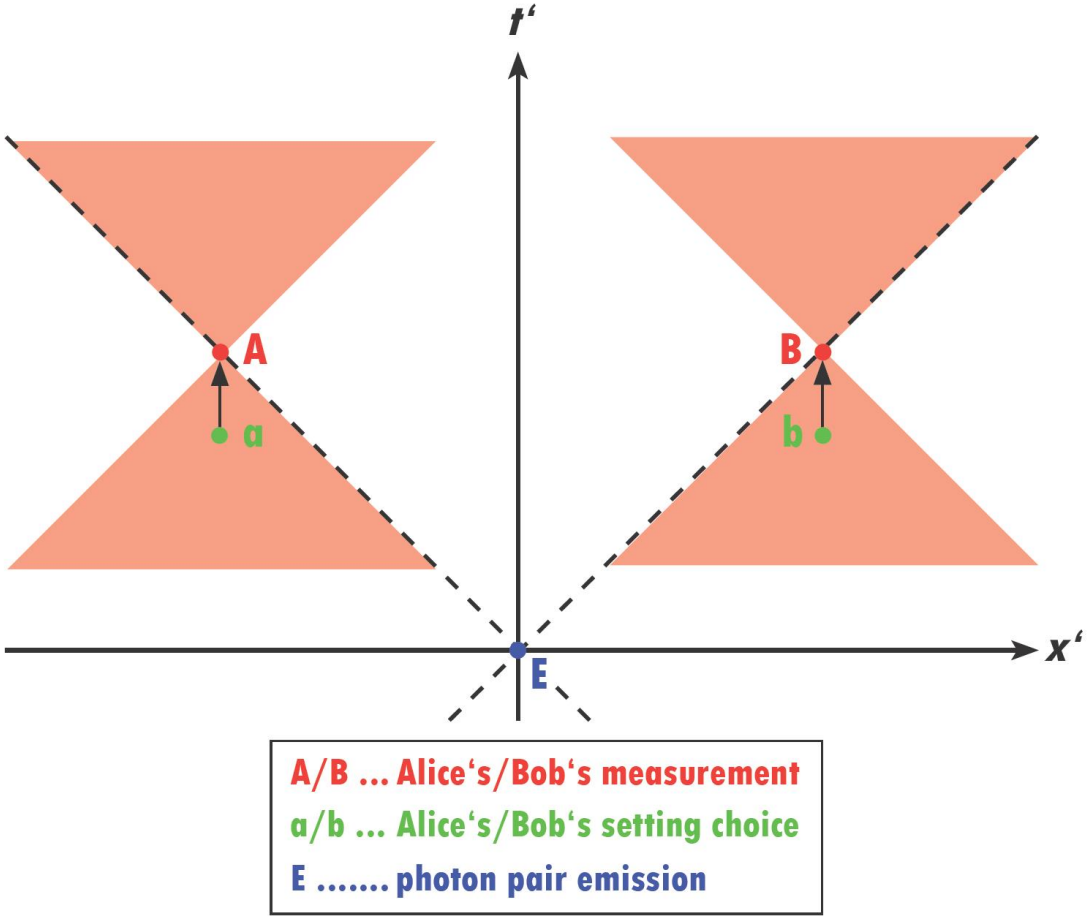

Figure 6.2.: A symmetric space-time diagram. The green dots represent the setting choices. These are made some time before the measurement, are transmitted to the measurement device through some channel and are finally used to implement the measurement setting. The red shaded areas represent the light cones of Alice's and Bob's measurement events. A region outside a light cone is space-like separated from the corresponding space-time event. Contrary, regions inside the future (past) light cone could have been directly influenced by (could directly influence) the corresponding space-time event. It is easy to see that the locality conditions are fulfilled, because the measurement event on one side is space-like separated from both, the measurement and the setting choice event on the other side.

the source to Alice and Bob, respectively. In the reference frame of the source, Alice and Bob detect the photons at the same time. Obviously, the setting choices must be made before the measurement, because the measurement device needs a specific amount of time for adjusting the corresponding setting. Within the depicted scenario, the locality conditions are clearly fulfilled.

The symmetry of the arrangement, however, is not a necessary condition for a Bell test. It is also possible to measure, lets say Alice's photon, right next to the entangled photon source, which results in a totally asymmetric space-time diagram (this situation is qualitatively the same as in our experiment). In such a case, the required space-like separations for closing the locality loophole can only be achieved by inserting a delay line for Alice's photon, which can easily be realized with an optical fiber (see Figure 6.3).

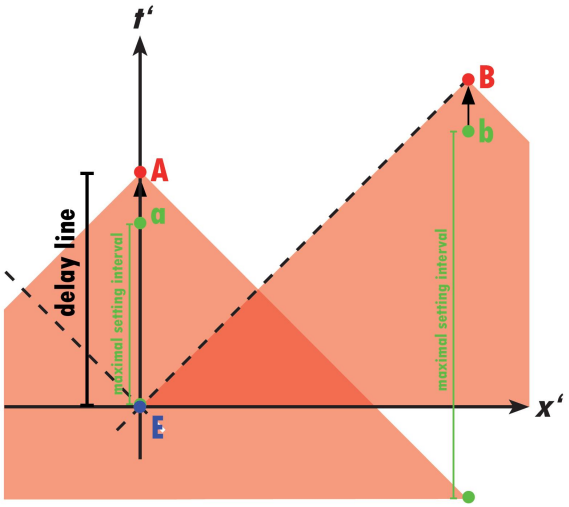

Figure 6.3.: A space-time diagram, where Alice's photon is measured at the location of the photon source. Alice's photon must be delayed in order to achieve space-like separation between the measurement event on one side and both the measurement and the setting choice events on the other side. Additionally, the settings must be chosen randomly. Due to the probabilistic nature of the emission process, the random settings must be refreshed at a rate, such that the required space-like separations are guaranteed for the whole setting interval. In the Figure, the longest allowed setting interval for closing the locality loophole is indicated by the vertical green bar between two consecutive setting choices. Note that Alice's setting choice events lie in the future lightcone of the emission event and thus, the freedom-of-choice loophole is not closed in this scenario.

Besides the required independence of the observer stations, it is also crucial that both measurement devices *randomly* switch between the two different measurement settings. Due to the statistical nature of the photon emission process (see Section 6.2.1), the emission and the random setting choices are not synchronized. Hence, a measurement event can happen with equal probability anywhere within the time interval over which a certain setting is valid (i.e., the time between two consecutive random choices). Hence, closing

the locality loophole imposes that the random settings are refreshed fast enough, such that the required space-like separations are guaranteed for the whole setting interval. The maximal length of the setting interval generally depends on the actual experimental space-time arrangement. Static setups or pseudo-random choices can not be used to guarantee locality, because static setups do not vary the settings and pseudo-random choices are at any time predetermined. Hence, in both cases the choice events are not space-like separated from the measurement on the other side.

In our experiment, Alice and Bob used individual quantum random number generators (QRNGs) (see Section 6.2.2) to decide about their measurement settings. Consequently, the underlying random process represented the setting choice. The random numbers were then used to implement polarization measurements along two different directions, which was achieved by using electro-optical modulators (EOMs) (see Section 6.2.3).

6.1.2. How to close the freedom-of-choice loophole

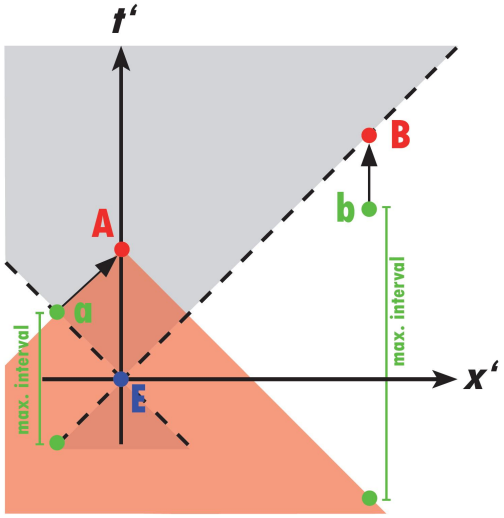

Figure 6.4.: This asymmetric space-time diagram represents a situation, where the locality and freedom-of-choice conditions are guaranteed. The longest allowed time interval between two consecutive settings (vertical green bars) is at Alice restricted most by the freedom-of-choice condition (i.e., space-like separation between the setting choices and the emission event), while at Bob it is restricted most by the locality condition (i.e., space-like separation between the setting choices and Alice's measurement event).

As discussed in Section 5.4.3, it is crucial for closing this loophole that the type of measurement performed is not influenced by the particle source or generally by the hidden variables.

In general, the freedom-of-choice condition can be guaranteed simultaneously with the locality condition, if the random choices, **a** and **b**, are made not only space-like separated

from each other and from the measurement on the other side (i.e., the locality conditions), but also space-like separated from the photon emission event **E**. This condition is already fulfilled within the symmetric situation depicted in Figure 6.2. However, within the asymmetric scenario, this requires to make the random setting choices at Alice some distance apart the measurement in order to "move" them out of the light cone of the emission (see Figure 6.4). Like in the case for closing the locality loophole, the refreshing rate of the random settings must be chosen such that the required space-like separations are guaranteed for the whole setting interval.

In our experiment, we placed Alice's QRNG 1.2 km apart from her measurement device and transmitted the random numbers through a radio channel to Alice where they were used to implement the measurement settings.

I want to remark that space-time events in general have to be represented with vertical bars rather than with points in the space-time diagram, due to the finite duration of the underlying processes. For the locality and freedom-of-choice conditions to be fulfilled, the required space-like separations must be guaranteed for the whole processes.

6.2. Experimental parts

From the above considerations it follows that a Bell test under locality and freedom-of-choice conditions with entangled photons requires specific experimental arrangements. These are an entangled photon source, a device that provides a random output signal, polarization analyzer modules that are able to implement two different measurement settings depending on the random signal, quantum channels for transmitting the photons from the source to the separate observers and a radio channel (or similar) for transmitting the signal from Alice's distant random device to the analyzer module. Furthermore, precise temporal alignment, independent data acquisition and data processing requires lots of electronic equipment and software.

In the following sections I will describe the experimental parts that were used in our final setup. The individual sections start with a short introduction to the underlying theory and/or physical processes followed by a description of their actual experimental implementation.

6.2.1. Source of entangled photons

Spontaneous parametric down conversion

Today, the most efficient way for generating entangled photons is to use the process of spontaneous parametric down conversion (SPDC) in non-linear crystals. Generally, the SPDC process can be described by considering the polarization response P of a nonlinear medium on the electric field of a monochromatic wave $E_i = E_{0i}\cos(\omega t - \hat{\mathbf{r}}\hat{\mathbf{k}})$. P can be expressed in a power series of the applied electric field:

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

with the vacuum permittivity ϵ_0 and the n^{th} order susceptibility $\chi^{(n)}$ of the nonlinear material. Considering a wave with the wave vector $\hat{\mathbf{k}}$ parallel to the z-direction and only regarding first and second order terms, the first component of the polarizability at $z = 0$ is given by

$$P_1 = \epsilon_0 \left[\chi^{(1)} E_{01} \cos \omega t + 2\chi^{(2)} E_{01}^2 + 2\chi^{(2)} E_{01}^2 cos 2\omega t\right]. \tag{6.2}$$

The last term of Equation (6.2) leads to dipole radiation of the medium with frequency 2ω. This process is called *second harmonic generation*. It is a special case of the more general three-wave mixing *up-conversion* process, where two waves with frequency ω_1 and ω_2 interact in a second order nonlinear medium, producing a third wave with frequency $\omega_3 = \omega_1 + \omega_2$. The corresponding reverse process is called *down-conversion*, where the wave with frequency ω_3 interacts with the nonlinear medium and generates the two waves with frequencies ω_1 and ω_2, respectively.

In quantum mechanics, the down-conversion process can be described as a three-photon interaction. A pump photon with frequency ω_p and wave vector $\hat{\mathbf{k}}_p$ splits into a *signal* and an *idler* photon with frequencies and wave vectors ω_s, $\hat{\mathbf{k}}_s$ and ω_i, $\hat{\mathbf{k}}_i$, respectively. Due to conservation of energy and momentum, the so-called *phase-matching conditions* must be satisfied for the three photons involved

$$\omega_p = \omega_s + \omega_i \quad , \quad \hat{\mathbf{k}}_p = \hat{\mathbf{k}}_s + \hat{\mathbf{k}}_i. \tag{6.3}$$

The interaction operator for the general SPDC process is obtained by substituting the classical fields with the corresponding quantum electrodynamic fields. The output modes of the SPDC process are represented by the quantized field

$$E_j^{(-)} = \epsilon_j \int_V d^3r \; a_{j,k}^\dagger(\omega_j) \mathrm{e}^{i(\hat{\mathbf{k}}_j \hat{\mathbf{r}} - \omega_j t)}, \tag{6.4}$$

where $a_{j,k}^\dagger$ is the creation operator of a photon with j standing for either the signal or idler field and k standing for the corresponding polarization mode. Contrary, the strong pump field can still be considered constant and is treated as a classical plane wave $E_p^{(+)} = \epsilon_p \exp[i(\hat{\mathbf{k}}_p \hat{\mathbf{r}} - \omega_p t)]$. With Equation (6.4) the SPDC interaction operator has the form [63]:

$$\mathcal{H} = \epsilon_0 \int_V d^3r \chi^{(2)} E_p^{(+)} E_s^{(-)} E_i^{(-)} + \text{H.c.}, \tag{6.5}$$

where V is the interaction volume and H.c. is the Hermitian conjugate.

Assuming collinear phase-matching along the z axis ($\hat{\mathbf{k}}_p \| \hat{\mathbf{k}}_s \| \hat{\mathbf{k}}_i \| z$), the state of the signal and idler fields in a type-II[1] SPDC process is given by [63]

$$|\Psi(\omega_s, \omega_i)\rangle = \left[\int d\omega_s d\omega_i \delta(\omega_p - \omega_s - \omega_i) \text{sinc}\left(\frac{L\Delta k}{2}\right) a_{s,V}^\dagger(\omega_s) a_{i,H}^\dagger(\omega_i)\right] |0\rangle. \tag{6.6}$$

Here L is the length of the nonlinear medium and $\Delta k = k_p - k_s - k_i$ is the phase-mismatch.

[1] In a type-II process the signal and idler photons will have orthogonal polarization.

In periodically poled crystals, as used in our source, the effective nonlinearity of the medium is inverted with a certain period by the application of a strong electrical field with alternating directions during the crystal growing process. Thus, the phase-matching conditions involve an additional term depending on the crystal's poling period Λ:

$$\hat{\mathbf{k}}_p = \hat{\mathbf{k}}_s + \hat{\mathbf{k}}_i + \frac{2\pi}{\Lambda}. \tag{6.7}$$

This is called *quasi-phasematching* and allows for almost arbitrary phase-matching angles and wavelengths. Specifically, these crystals can be tailored for collinear phase-matching along one of the crystallographic axes. For a type-II SPDC process this means that the orthogonal signal and idler beams do not experience *transversal walk-off* (e.g. as it occurs in entangled photon sources where bulk nonlinear crystals are used), which is of utmost importance for efficient generation of highly entangled photon pairs.

This is because the transversal walk-off effect results in a spatial separation between the two down-converted modes and provides "which-path" information of the signal and idler photons. This in principle enables to gain information about the polarization of a photon when looking at it's path and thus reduces the entanglement quality. Even though this effect can be partly compensated, it generally limits the length of the crystals that can be used.

Consequently, exploiting the quasi-phasematching technique in periodically poled nonlinear media allows to increase the interaction volume V and thus the efficiency of the SPDC process by using long crystals.

Sagnac source of polarization entangled photon pairs

Our source employed SPDC in a periodically poled potassium titanyl phosphate $KTiOPO_4$ (ppKTP) nonlinear crystal, placed inside a polarization Sagnac interferometer (PSI). The PSI source was originally developed by my former colleague Alessandro Fedrizzi and a detailed description of this source can be found in [64]. Here I will give only a short and comprehensive introduction to its working principle.

An illustration of the source is shown in Figure 6.5. The input pump laser with 405 nm wavelength is split into orthogonal polarization components at the dual-wave polarizing beam splitter (dPBS) at the interferometer input. The counter clockwise propagating part of the pump laser generates a signal and idler photon with 810 nm wavelength and with horizontal (H) and vertical (V) polarization, respectively (Figure 6.5a). Their polarization is rotated by 90° after passing a dual-wave half wave plate (dHWP) [65] such that the idler photon (now H-polarized) is transmitted at the dPBS and leaves the interferometer through output 4. The V-polarized signal photon gets reflected at the dPBS and, using a dichroic mirror, it is separated from the pump laser and reflected to output 3. The polarization of the clockwise propagating component of the pump laser is rotated by 90° at the dHWP and also generates a H-polarized signal photon and a V-polarized idler photon at 810 nm (Figure 6.5b). The clockwise propagating V-polarized idler photon gets reflected at the dPBS and leaves the interferometer through output 4. Similarly, the clockwise propagating H-polarized signal photon is transmitted at the dPBS and leaves

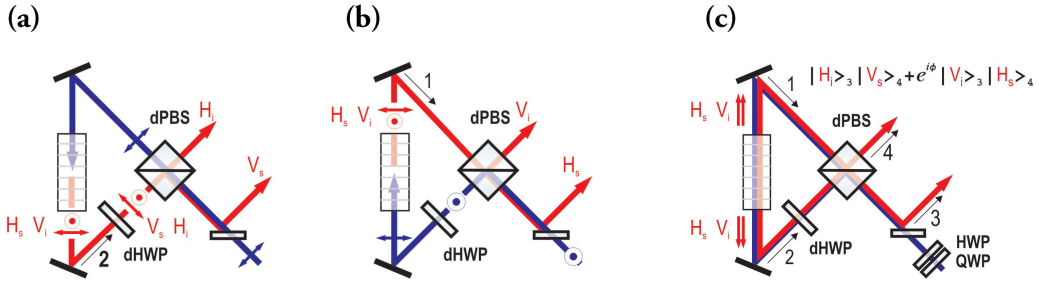

Figure 6.5.: A polarization Sagnac interferometer for the generation of polarization entangled photon pairs. For a detailed description please refer to the main text. (Figures taken from [66])

the interferometer through output 3. If the polarization of the pump laser is chosen, such that half of the intensity gets reflected and half gets transmitted at the dPBS, we are finally left with the entangled state in the two output modes 3 and 4:

$$|\psi_\phi\rangle = \frac{1}{\sqrt{2}}\left(|H_i\rangle_3|V_s\rangle_4 + \mathrm{e}^{i\phi}|V_i\rangle_3|H_s\rangle_4\right). \tag{6.8}$$

The phase ϕ originates from the phase relation between the vertical and horizontal components of the pump laser field and the individual phases picked up by the down-conversion fields in the interferometer. This phase can be manipulated via a half wave plate (HWP) and a quarter wave plate (QWP) in the pump laser beam (Figure 6.5c). In our experiment, the phase was adjusted such that we obtained the maximally entangled Bell state

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|H_i\rangle_3|V_s\rangle_4 - |V_i\rangle_3|H_s\rangle_4\right). \tag{6.9}$$

The photons at the outputs were coupled into single mode optical fibers, which were connected to the quantum channels during the measurements, transmitting the photons to Alice and Bob, respectively.

6.2.2. Quantum Random Number Generator

The functionality of the quantum random number generator (QRNG) developed for this experiment is based on a previous work of my college Thomas Jennewein [67], but its design was improved with respect to operability and stability.

Source of randomness

For the QRNG, we employed the optical process of splitting single photons at a 50/50 beam splitter (BS) as the physical source of randomness. Each individual photon coming from the light source and traveling through the beam splitter, has equal probability to be

either transmitted or reflected. Quantum mechanics predicts that the individual decisions are truly random and independent of each other.

Functionality

As schematically shown in Figure 6.6, the photon source was realized with a blue light emitting diode (LED). The short coherence time of the source ensured that the number of photons per coherence time was $\ll 1$, thus avoiding effects of photon statistic or optical interference onto the behaviour of the QRNG. In each output of the BS, fast photomultipliers (PM) detect the single photons. Small apertures are used in front of the detectors to avoid saturation effects. Subsequently, the detector pulses are combined in a toggle switch (S) which has two states, 0 and 1. If detector PM1 fires, the switch is flipped to state 0, until an event in detector PM2 occurs, switching S back into state 1, and vice versa. The output of the switch toggles between the 0 and 1 state, constituting a binary random signal (see Figure 6.7) with the randomness lying in the times of the transitions. Subsequently, the random signal is sampled periodically at an adjustable rate and converted to TTL[2] levels, using further electronics. The QRNG has two output connectors. One of which is a BNC connector for directly tapping the random TTL signal. The other is a USB connector, wherewith either the QRNG can be controlled via a personal computer or the random signal can be transferred to a personal computer (e.g. using a fast digital I/O board).

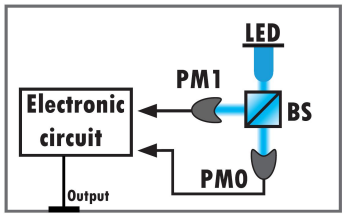

Figure 6.6.: An illustration of our quantum random number generator. A detailed explanation of the functionality is given in the main text.

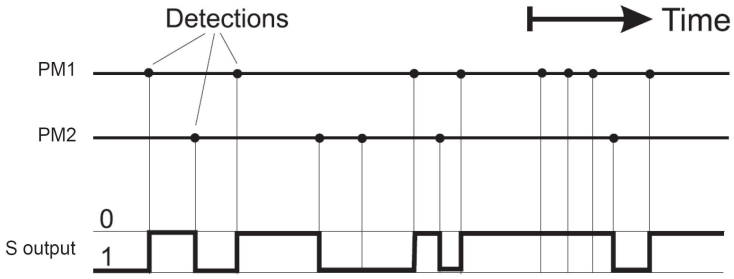

Figure 6.7.: The output of the toggle switch S of the QRNG.

Characterization

Since the timing in our experimental setup was a critical point, we had to know exactly the time the QRNG needed to establish a random state of its output signal. Therefore,

[2] Transistor-transistor logic, with "high" and "low" referring to 0 V and 3.3-5 V, respectively.

the total time delay, resulting from delay in the light source, light path, photomultipliers and further electronics was measured and the value $\tau_{delay} \approx 75$ ns was obtained. In addition, the autocorrelation function of the binary signal had to be considered. This is a measure for the average correlation between the signal at a time t and $t+\tau$. It exhibits an exponential decay of the form

$$A(\tau) = A_0 \mathrm{e}^{-2R|\tau|}, \tag{6.10}$$

where R is the average toggle rate of the random signal, A_0 is a normalization constant and τ is the delay time [68]. The autocorrelation time τ_{ac} is defined as the time for which $A(\tau_{ac}) = \frac{A_0}{\mathrm{e}}$ holds and is thus given by

$$\tau_{ac} = \frac{1}{2R}. \tag{6.11}$$

For the internal toggle frequency of 30 MHz, as used in our QRNG, the autocorrelation time was $\tau_{ac} \approx$17 ns. This means that the time for generating a random signal, starting from a point in time where the output state of the generator may already be known, is given by $(\tau_{delay} + \tau_{ac}) < 100$ ns.

Widely accepted conditions for the randomness of any binary sequence were introduced by Kolmogorov and Martin-Löv. Kolmogorov's considerations are based on the algorithmic complexity of the sequence. He found that a binary sequence is random, if it is "chaotic". Martin-Löv's definition says that a random sequence must be "typical", i.e., no particular random sequence must have any features that make it distinguishable from all random sequences [69, 70].

There exists a wide range of statistical tests to check the randomness of a binary sequence. A very simple and intuitive test is to look if the occurrence of "0's" and "1's" is equally probable. Clearly, the equidistribution by itself is not a criterion for the randomness of the sequence. Another test proofs the distribution of n-bit blocks of a data set, where n is the length of the block. If the data set is sufficiently long, any n-bit block should appear with equal probability. The distribution corresponds to the entropy $H_n = -\sum_i p_i \log_2 p_i$, where p_i is the empirically determined probability for finding the ith block. If the sequence is random, a block of length n should produce n bits of entropy. In the so-called "run test", the number of blocks with consecutive "0's" and "1's" is

File import
File name: Y:\Work\Photon\QRandom\100Mbit0.txt
Date and time: 03/11/08 11:30:56
Bit count 101999184

Balancing
No balancing has been performed
Ones ratio: 50.00%

One Level Entropy Test
Lenght of Blocks: 12
Nb of Blocks: 8499932

Entropie H: 4044.836
Expected value: 4095.000
Standard deviation s: 90.499

The sequence of bits seems to be random because there is only 0.55 s of difference with the expected mean.

Lenght of Blocks: 4
Nb of Blocks: 25499796

Entropie H: 17.789
Expected value: 15.000
Standard deviation s: 5.477

The sequence of bits seems to be random because there is only 0.51 s of difference with the expected mean.

Figure 6.8.: The typical output of the program testing the randomness of our QRNG. Here, the balancing of "0's" and "1's" as well as the entropy H_n for two different block sizes were empirically determined. The results indicate the randomness of the analyzed 100 Mbit random sequence. Tests performed with many other samples showed similar results.

counted. Since the probability is $\frac{1}{2}$ for obtaining either zero or one, the number of blocks found with n concatenated equal bits should be proportional to a $\frac{1}{2^n}$ function.

These statistical tests were applied to samples produced by our QRNG preliminary to the actual experiment in order to illustrate its functionality. The results obtained are in favor with our device as typical results obtained with a testing programm show (see Figure 6.8 and Figure 6.9).

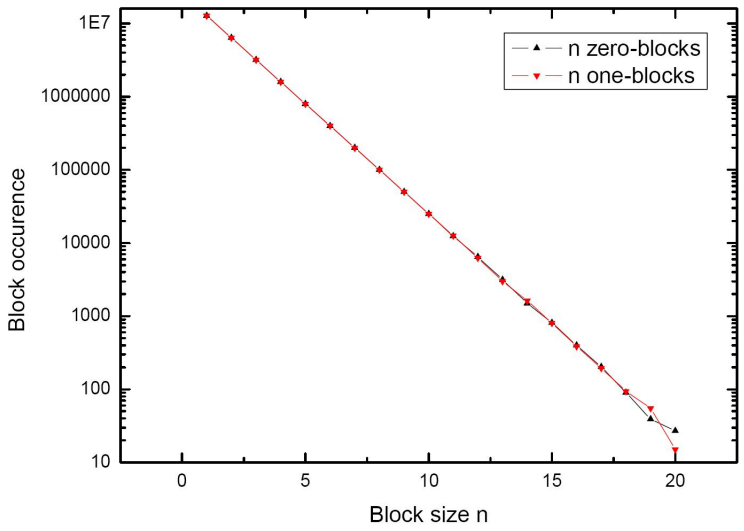

Figure 6.9.: The result of the "run-test" for the same 100 Mbit sample as in Figure 6.8. The slopes of the logarithmically scaled distributions were obtained from a linear fit and are -0.302 ± 0.001 (n zero-blocks) and -0.303 ± 0.002 (n one-blocks). The slight deviation from the ideal value of $-\log(2) = -0.301$ is a consequence of minor differences in the probabilities of finding a zero or a one at the output of the QRNG.

6.2.3. Polarization analyzers

As discussed in Section 6.3, the random numbers must be used to switch randomly between two measurement settings. In the following Section I will discuss for which settings quantum mechanics predicts a violation of the Bell inequality in the case of polarization measurements on entangled photons and how an analyzer module for obtaining the required expectation values can be designed.

CHSH inequality for polarization entangled photons

In our experiment we used the CHSH inequality (5.16) to be violated. In an experiment, it is convenient to use polarizers and simply measure the linear polarization of the entangled photons. In this case, the quantum mechanical expectation value for correlation

measurements on photon-pairs in the state (6.9) only depends on the angles of Alice's and Bob's polarizers, α and β, and is given by

$$E^{qm} = -\cos(2(\alpha - \beta)). \tag{6.12}$$

With this expectation value, quantum mechanics predicts a maximal violation of the CHSH inequality

$$S(\alpha_1, \alpha_2, \beta_1, \beta_2) = |E(\alpha_1, \beta_1) - E(\alpha_1, \beta_2)| + |E(\alpha_2, \beta_1) + E(\alpha_2, \beta_2)| \leq 2 \tag{6.13}$$

for the polarizer settings $\alpha_1 = 22.5°, \alpha_2 = 67.5°, \beta_1 = 0°$ and $\beta_2 = 45°$ with $S^{qm}_{max} = 2\sqrt{2}$.

The four required expectation values are obtained via coincidence measurements between the detection events at Alice and Bob. For each expectation value, four coincidence rates are required:

$$E(\alpha, \beta) = \frac{C(\alpha, \beta) + C(\alpha^\perp, \beta^\perp) - C(\alpha^\perp, \beta) - C(\alpha, \beta^\perp)}{C(\alpha, \beta) + C(\alpha^\perp, \beta^\perp) + C(\alpha^\perp, \beta) + C(\alpha, \beta^\perp)}, \tag{6.14}$$

where $C(\alpha, \beta)$ is the detected coincidence rate with Alice's polarizer at angle α and Bob's polarizer at angle β. Hence, a test of the CHSH inequality requires 16 coincidence measurements when using polarizers. However, using switchable wave-plates and a polarizing beam splitter, it is possible to obtain all 16 coincidence rates within a single measurement run, as will be shown in the next Section.

Analyzer modules

Instead of polarizers we used polarizing beam splitters (PBS) as optical elements for analyzing the polarization of the photons. If correctly aligned, horizontally (H) polarized photons are transmitted at the PBS while vertically (V) polarized are reflected. In this case, any photon with arbitrary polarization is analyzed in the $|H, V\rangle$-basis and will either be transmitted or reflected, with the corresponding probabilities depending on the polarization state. A different orthonormal basis (e.g. the $|D, A\rangle$-basis) for analyzing the linear polarization can be realized by either rotating the PBS or, more convenient, rotate the polarization of the photons before they hit the PBS. In our analyzers, this rotation was implemented using wave plates and electro-optical modulators (see Figure 6.10).

Alice's analyzer consisted of a half wave plate (HWP), a quarter wave plate (QWP), an electro-optical modulator (EOM), a PBS and single photon detectors in each output mode of the PBS. The EOM together with the QWP were aligned for switching between polarization rotations of 0° and 45°, depending on the output of Alice's QRNG (see Section 6.2.4 for details). The HWP at the analyzer input was set to 11.25°. Hence, an incoming photon was in total rotated by either 22.5° or 67.5°. In combination with the PBS, the photons were analyzed in the linear bases $|22.5°, 112.5°\rangle$ or $|67.5°, 157.5°\rangle$, respectively. **Bob's analyzer** was similar to Alice's, besides the missing HWP at the input. An incoming photon was in total rotated by either 0° or 45°, which corresponds to the analyzing bases $|0°, 90°\rangle$ or $|45°, 135°\rangle$, respectively.

Since the measurement bases were actively varied, controlled by the random number generators, our analyzers enabled us to obtain all 16 coincidence rates that are required for testing the CHSH inequality in a single measurement run (see Section 6.2.8 for details).

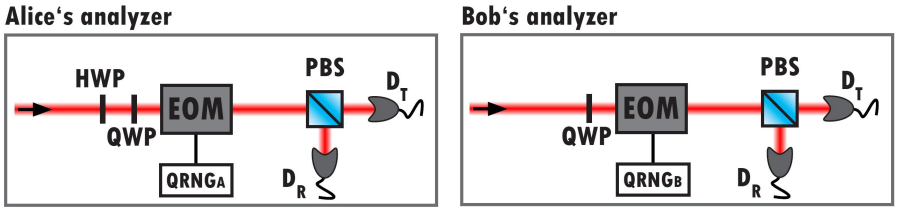

Figure 6.10.: Alice's and Bob's polarization analyzer modules. For details please refer to the main text.

6.2.4. Electro-optical modulator

It was essential to find an electro-optical modulator which was able to implement two different settings depending on the state of the quantum random number generator and to refresh them fast enough, such that the locality and freedom-of-choice conditions could be guaranteed in the experiment.

In this Section, I will start with a short discussion about the electro-optical effect and its implementation for Pockels Cells (i.e., voltage controlled wave plates). Subsequently, I will describe the properties of our electro-optical crystals and how they could be adjusted for our purpose.

Electro-optical effect

Electro-optical materials change their optical properties when exposed to an electrical field [71]. The linear electro-optical effect, i.e., *Pockels effect* [72], is a change in the refractive index, linearly depending on the (static) applied field:

$$\Delta\left(\frac{1}{n^2}\right)_{ij} = \Delta\left(\frac{1}{\epsilon}\right)_{ij} = \Delta\beta_{ij} = r_{ijk}E_k(\omega = 0), \tag{6.15}$$

with the linear dielectric permittivity ϵ_{ij}, the optical indicatrix $\beta_{ij} := \epsilon_{ij}^{-1}$ and the Pockels tensor r_{ijk}. The Pockels effect occurs only in crystals that lack inversion symmetry and thus, these materials are also piezoelectric[3].

A convenient way to consider the electro-optical effect is to look at the optical indicatrix of the material. In the crystal's main axis system, the indicatrix has a diagonal form and the main refractive indices are defined as

$$n_i := \frac{1}{\sqrt{\beta_{ii}}}. \tag{6.16}$$

[3]The piezoelectric effect can cause mechanical vibrations in the crystal when voltage is applied periodically. These vibrations in turn induce an electrical potential and influence the optical properties of the crystal (i.e., piezoelectric ringing). If voltage is applied in resonance frequency with a piezoelectric mode, the crystal can get damaged in the worst case.

The geometrical interpretation of the indicatrix [73] in the main axis system is an ellipsoid (see Figure 6.11) given by the main refractive indices $n_{x,y,z}$:

$$\frac{x^2}{n_x} + \frac{y^2}{n_y} + \frac{z^2}{n_z} = 1. \tag{6.17}$$

In this picture, the optical axes of the crystal are defined by vectors perpendicular to the planes, for which the intersection with the indicatrix is a cycle. If for a material all three main refractive indices are different ($n_x \neq n_y \neq n_z$), two optical axes can be found and the crystal is said to be *biaxial*. If only two indices are different (e.g. $n_x \neq n_y = n_z$) the crystal is *uniaxial*. In both cases, birefringence can be observed along general directions (except those parallel to the optical axes). The corresponding refractive indices are given by the length of the semi-major and semi-minor axes of the intersection ellipse of the indicatrix with the plane perpendicular to the wave vector (see Figure 6.11). In contrast, the indicatrix of an optical isotropic medium ($n_x = n_y = n_z$) is a sphere and no birefringence can be observed.

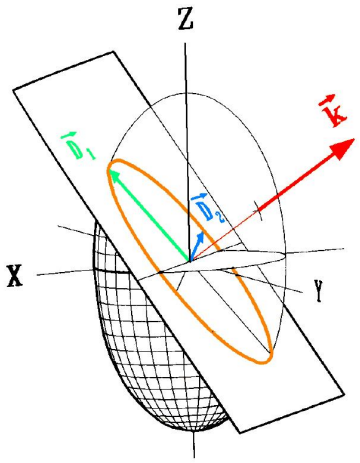

Figure 6.11.: The geometrical interpretation of the indicatrix is an ellipsoid in the crystal's main axis system. (Figure taken from [73].)

An applied electric field changes the refractive index structure and thus the indicatrix of the crystal, given by Equation (6.15). The change of the indicatrix for a longitudinal electro-optical crystal (i.e., the electric field is applied along the light path) is shown in Figure 6.12. Light travels along the optical axis (z-direction) and is not exposed to birefringence in the absence of an electrical field (left part of Figure 6.12). The right part of Figure 6.12 shows the action of an applied field. The crystal becomes birefringent and in general, changes the polarization of light.

If designed appropriately, electro-optical crystals can be used to fabricate voltage-controlled wave plates. In so-called Pockels Cells, the voltage can be adjusted, such that the "fast" and "slow" polarization components exhibit a phase-shift of π ($\frac{\pi}{2}$) and the Pockels Cell acts as a half wave plate (quarter wave plate).

Our Pockels Cell

The Pockels Cells (PoCs) used in our experiment were produced by `Leysop LTD` and consisted of two 4x4x10 mm Rubidium Titanyl Phosphate (RTP) crystals placed in sequence. This material exhibits a low piezoelectric effect but offers a high electro-optical coefficient, enabling half wave switching within nanoseconds and allowing for high switching rates. These crystals are cut such that the optical path is not along the optical axes but along the crystallographic y-axis, a direction that exhibits birefringence even in the absence of an electrical field. However, using a pair of RTP crystals oriented with their z-axes 90° to each other, the birefringence is compensated. In contrast to a longitudinal Pockels Cell, voltage is applied along the z-direction (transversal Pockels Cell), with opposite sign for

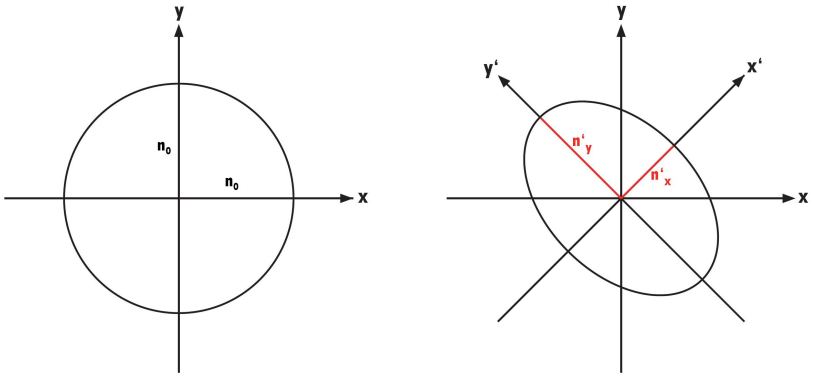

Figure 6.12.: An illustration of the longitudinal Pockels effect, where the electrical field is applied along the optical axis (z-direction). (left) If no field is applied to the crystal, the intersection of the indicatrix with a plane perpendicular to the z-axis is a cycle with $n_x = n_y = n_0$; no birefringence along the z-direction. (right) If an electrical field is applied, the rotational symmetry gets lost and the crystal becomes birefringent. The x' and y' polarization components of light traveling along the z-direction exhibit different speeds, inversely proportional to n'_x and n'_y, respectively. At the end of the crystal these components are superimposed again, resulting in a change of polarization.

the two crystals[4]. This results in a change of polarization, depending on the strength of the electric field and on the orientation of the z-axis (i.e., the rotation of the PoC around the optical path).

Alignment of the optical path

For the alignment of the optical path, it was crucial that it was exactly parallel to the crystallographic y-axis. A common way to achieve this, is to look at the *isogyre pattern* produced by divergent (or diffuse) light illuminating the PoC. Schematically, the Pockels Cell is therefore put in between two crossed polarizers and the light pattern is observed on a screen after the second polarizer.

Light that travels along the desired y-axis exhibits no birefringence in the absence of an electrical field and will be blocked at the second polarizer, while light rays forming a finite angle with this axis will be changed in polarization. This change is rotational symmetric around the y-axis and characteristic for the traveling direction. Along certain directions, light can pass through the second polarizer and in a situation where all directions are equal probable, this will lead to the characteristic interference pattern shown in Figure 6.13. Our Pockels Cell was therefore put onto a four axis tip-tilt mount, which allowed for precise alignment of the crystallographic axes system.

[4]If voltage would be applied with equal sign, the birefringence would always be compensated, due to the crossed configuration and the polarization of light would not be affected by applying an electrical field.

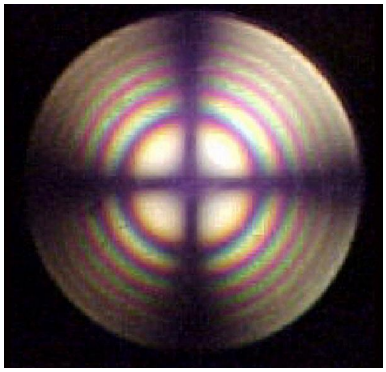

Figure 6.13.: This picture shows an ideally looking isogyre pattern. (Picture taken from http://www.brocku.ca/earthsciences/people/gfinn).

Alignment of the rotation

As discussed in Section 6.2.3, the Pockels Cell should serve as a switchable half wave plate (HWP) oriented at 22.5° (i.e., for polarization rotations of either 0° or 45°). Therefore, the rotation of the crystallographic z-axis (i.e., the rotation of the crystals around the optical path) had to be aligned appropriately. This was accomplished by placing the Pockels Cell in between two polarizers and detecting the signal of a collimated laser diode (5 mW, 810 nm) at the output of the polarizer-PoC-polarizer setup with a fast photodiode. The signal from the photodiode was displayed with an oscilloscope as shown in Figure 6.14.

The input and the output polarizers were set to 0° and 45°, respectively. A signal generator box (splitter box) from the Pockels Cell supplier was used to apply bipolar half wave voltage (±HWV) pulses (100 kHz repetition rate, 200 ns pulse duration and pausing at 0 V between two consecutive pulses) in form of a square wave to the crystals[5].

If the rotation angle was aligned correctly, the input polarization (0°) was rotated by −45° whenever −HWV was applied and the light beam was fully blocked at the output polarizers. Contrary, applying +HWV rotated the input polarization by 45° and the full light intensity could be detected on the photodiode. In between two voltage pulses, the polarization was not rotated by the Pockels Cell and half of the light intensity could pass through the second polarizer.

Reducing the required voltage

Preliminary estimations suggested that a switching rate of at least 200 kHz will be required for our purpose. However, to be on the safe side, we tested our PoC for the highest possible rate. In general, the maximal switching rate of a Pockels Cell is limited by the performance

[5]When positive (negative) half wave voltage is applied (in our case ±1000 V), the induced birefringence is such that the fast and slow polarization component exhibit a phase shift of $\pi(-\pi)$ and the Pockels Cell acts as a have wave plate. Similarly, when positive (negative) quarter wave voltage is applied (±500 V), the phase shift is $\frac{\pi}{2}$ $(-\frac{\pi}{2})$ and the Pockels Cell acts as a quarter wave plate.

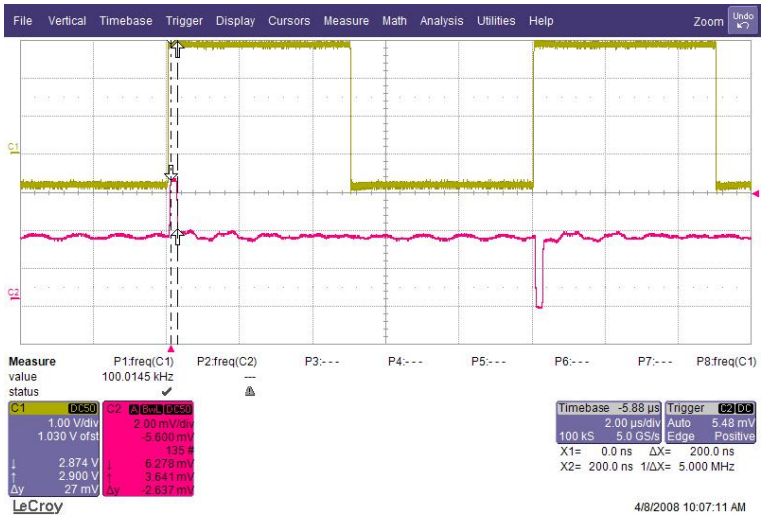

Figure 6.14.: A snapshot of the oscilloscope display, showing the optical switching behaviour of our Pockels Cells, which was placed in between two polarizers as described in the main text. The yellow curve shows the 100 kHz trigger signal, alternately applying positive and negative half wave voltage for 200 ns. This type of operation resulted in a high and low signal on the photodiode (red curve). In between a positive and a negative voltage pulse, no electric field was applied and half of the light intensity reached the photodiode. One can also see slight piezoelectric ringing after a voltage pulse.

of the high voltage supply and by the piezoelectric properties of the crystal, but can be increased by reducing the voltage that has to be applied.

Hence, we investigated a method, where quarter wave voltage (QWV) (instead of half wave voltage) was sufficient for our desired polarization rotations. This method required to simply place a quarter wave plate (QWP) with its optical axis oriented at 22.5° in front of the Pockels Cell. Then, by applying positive quarter wave voltage (+QWV), the PoC acted as an additional QWP at 22.5°, such that the overall effect was the one of a HWP at 22.5°, rotating the polarization of light by 45°. Obversely, applying negative quarter wave voltage (−QWV) made the PoC compensate the action of the QWP, such that the overall polarization rotation was 0°.

Additionally, this method was very convenient to suppress ion wandering effects[6] that may had damaged the crystals when the Pockels Cell was triggered by our quantum random number generator. That is, because a run of n consecutive "0's" ("1's") could occur with a probability of $\frac{1}{2^n}$ (see Section 6.2.2) and would require to continuously apply −QWV (+QWV) to the crystals, since "0" ("1") required a polarization rotation of 0° (45°). However, our QRNG was balanced within the statistical uncertainties such that positive and negative quarter wave voltage were on average applied equally often. Thus, the mean electric field in the crystals was kept zero and ion wandering effects have been

[6]Ion wandering effects occur if high voltages are applied for a relatively long period of time (usually on the order of milliseconds).

suppressed.

Performance of the complete analyzer modules

At first, we tested the performance of the Pockels Cell aligned with the QWP in front of it. The aim was to find the maximal achievable switching rate combined with a high duty cycle[7]. Therefore, the PoC was placed in between two polarizers and the signal of a collimated laser diode (5 mW, 810 nm) was detected at the output of the polarizer-PoC-polarizer setup with a fast photodiode. The first polarizer was set to 0° and the second to 45°, while QWV was applied in form of a bipolar square wave directly switching from +QWV to −QWV and vice versa. This resulted in the highest possible duty cycle, only limited by the optical rise time of the Pockels Cell.

Figure 6.15.: The performance of the Pockels Cell operated at a switching rate of 4 MHz. The yellow curve shows the signal on the photo diode. The Pockels Cell was directly switched from the +QWV to the −QWV state, and vice versa, resulting in a duty cycle of 96.4%, which was only limited by the optical rise time.

A reasonable performance was achieved up to a switching rate of 4 MHz between the positive and negative voltage state, corresponding to an "on-time" of 250 ns per state. The switching quality of the Poc, defined by the contrast of the maximal and minimal signal on the photodiode, was approximately 1:50. This value was mainly limited by the noise of the photodiode. The optical rise time for the switching process was measured to be approximately 9 ns, as shown in Figure 6.15, resulting in a duty cycle of $(1-\frac{9}{250}) = 96.4\%$

[7]The duty cycle is given by the ratio between the time the PoC is in one of the two desired states (i.e., when either +QWV or −QWV is applied) and the time the PoC is in an unwanted state (i.e., within the optical switching process).

As a next and final step we characterized the quality of the complete analyzer setup with the Pockels Cell triggered by the QRNG. The measurements were based on coincidence detection of photon pairs from our SPDC source. Using polarizers, the Sagnac source was aligned to produce signal and idler photons with horizontal (0°) and vertical (90°) polarization, respectively. Both photons were coupled into individual single mode fibers. The signal photon was detected directly with detector D_S, while the idler photon was sent through one of the analyzers (see Figure 6.16). Let us denote the detectors of the analyzer as $D_{T,0}$ and $D_{R,0}$, when the actual random number was "0" and as $D_{T,1}$ and $D_{R,1}$, when the actual random number was "1".

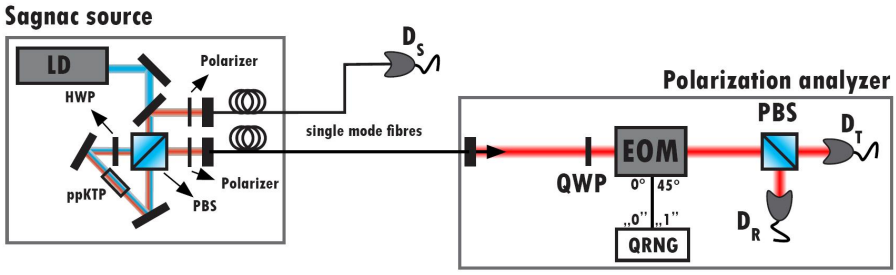

Figure 6.16.: The setup for testing the performance of our polarization analyzers. The polarizers selected signal/idler pairs of either horizontal/vertical or 135°/45° polarization. The performance of the polarization analyzer was quantified by the contrast in the coincidence rates $C_{D_S,D_T} : C_{D_S,D_R}$.

Selecting only those detection events, where the random number was "0", the polarization of the idler photon was rotated by 0° and thus analyzed in the $|0°, 90°\rangle$-basis (how to select detection events for only one of the two possible settings will be explained in Section 6.2.8). In the ideal case, no coincidences should be detected between D_S and $D_{T,0}$, while the coincidence rate between D_S and $D_{R,0}$ should be maximal. Hence, the contrast between these coincidence rates should reach infinity. However, in the realistic case the contrast is limited due to non-perfect switching and background counts. After improving the contrast of the coincidence rates by fine adjustment of the Pockels Cell's orientation using the tip-tilt mount, we were able to obtain a coincidence rate contrast of $C_{D_S,D_{T,0}} : C_{D_S,D_{R,0}} = 1 : 160$.

In order to test the quality of the Pockels Cell's 45° rotation, the same measurement was repeated for the case of a 135° polarized signal and a 45° polarized idler photon. Selecting those detection events, where the idler photon was analyzed in the $|45°, 135°\rangle$-basis (i.e., random number "1"), we obtained a contrast of $C_{D_S,D_{T,1}} : C_{D_S,D_{R,1}} = 1 : 170$.

I want to remark that for obtaining these satisfying results, the toggle frequency of the Pockels Cell could maximally be set to 1 MHz. This was achieved by sampling the random signal every 1 μs. Using higher toggle rates resulted in strange piezoelectric behaviour, which degraded the switching quality significantly. The optical rise time was again measured to be 9 ns, which corresponds to a duty cycle of $(1 - \frac{9}{1000}) = 99.1\%$.

6.2.5. Atmospheric free-space quantum channel

We used the atmosphere as quantum channel for transmitting one photon of an entangled pair from the source in La Palma to the 144 km apart observer Bob in Tenerife. From everyday life we know that the viewing of distant objects strongly depends on the atmospheric conditions. Hence, we had to consider the atmospheric factors that influence the transmission of light. In general, these are scattering, absorption and refractive index fluctuations (*optical turbulence*). Besides the atmospheric effects, there is also the effect of beam spreading in vacuum due to diffraction. Together, these effects can cause extinction of the transmitted light, i.e., preventing photons to reach the receiver. The extinction is given by the Lambert-Beer law:

$$I(\lambda, L) = I_0 \exp(\sigma_{ext}(\lambda) \cdot L), \tag{6.18}$$

with the extinction coefficient $\sigma_{ext} = \sigma_{abs} + \sigma_{scat} + \sigma_{turb}$, given by the sum of the absorption, scattering and turbulence induced loss coefficients [74]. L is the length of the atmospheric path and λ the wavelength of the light.

Vacuum beam spreading

In the paraxial approximation, a light beam which is transmitted into a specific direction is described by a set of Gaussian-beam waves [75]. The intensity profile of the lowest order Gaussian-beam wave (TEM_{00}-mode) propagating in z-direction is given by:

$$I(r, z) = \frac{2P}{\pi\omega^2(z)} \exp\left(-\frac{2r^2}{\omega^2(z)}\right), \tag{6.19}$$

with r denoting the distance from the optical axis and P denoting the power of the light beam. The local $(1/e^2)$ beam radius at distance z is given by

$$\omega(z) = \omega_0 \sqrt{1 + \frac{z^2}{z_R^2}}. \tag{6.20}$$

Here, ω_0 is the minimum beam radius (*beam waist*), which is related to the characteristic beam divergence length (*Rayleigh length*) by $z_R = \frac{\pi\omega_0^2}{\lambda}$ (see Figure 6.17). A beam of finite waist is thus spread as a function of propagation distance even in vacuum, which is a consequence of diffraction.

Absorption and scattering in the atmosphere

Absorption is a process in which electronic, vibrational and/or rotational modes of the atmospheric molecules are excited by incident photons. Hence, the absorption spectra exhibit a series of discrete absorption lines. For light with wavelengths in the visible to near-infrared, vibrational excitations are the major effect.

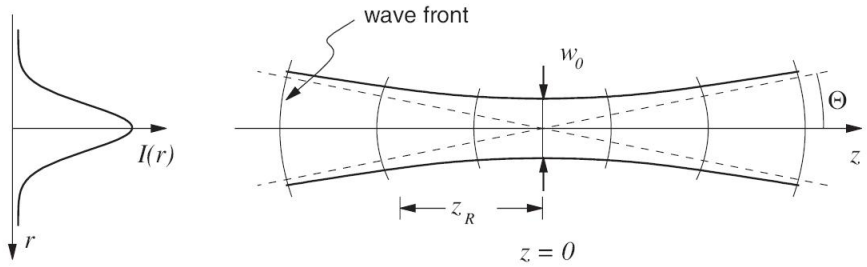

Figure 6.17.: The characteristic parameters of a Gaussian beam: ω_0 is the minimum beam waist, z_R is the Rayleigh length and Θ is the divergence half angle in the limit of $z \to \infty$. (Figure taken from [76].)

Rayleigh scattering is elastic scattering of light on particles and molecules, much smaller than the wavelength, i.e., if

$$x = \frac{2\pi r}{\lambda} \ll 1, \tag{6.21}$$

with the characteristic particle size r and the scattered wavelength λ. It is caused by a displacement of the weakly bound electronic cloud surrounding the gaseous molecule. The amount of scattered light is described by the Rayleigh scattering coefficient, which is inversely proportional to λ^4. Rayleigh scattering is negligible for wavelength larger than 3 μm. Conversely, for light in the visible to near-infrared it gives the sky the blue appearance, because blue light is scattered more than red or green.

Mie scattering[8] describes scattering of light on a spherical object with a size comparable to the wavelength. In the atmosphere, Mie scattering occurs mainly on solid or liquid particles that are suspended in the atmosphere. These particles are called *aerosols* and originate both from natural and man-made sources, can exist in concentrations ranging from 10^{-3}-$10^{11}/\mathrm{cm}^3$ and with sizes roughly between 1 nm and 100 μm.

The wavelength dependent extinction caused by aerosol and atmospheric molecules can be obtained by measuring the optical transmittance through the atmosphere. In Figure 6.18, the optical transmittance of the so-called standard atmosphere for a vertical propagation path between ground and space is shown. Water vapour, CO_2, NO_2, CO, and ozone are the primary radiation absorbers in the atmosphere. Specifically, CO_2 and water vapour absorb radiation at infrared wavelengths [77]. Obviously, the actual attenuation through the atmosphere strongly depends on the local humidity and environmental conditions.

[8] In general, Mie scattering encompasses the general spherical scattering solution (absorbing or non-absorbing) without any limitations with reference to the particle size. It converges at the limit for very large particles to geometric optics, and at the limit for small particles it includes Rayleigh scattering.

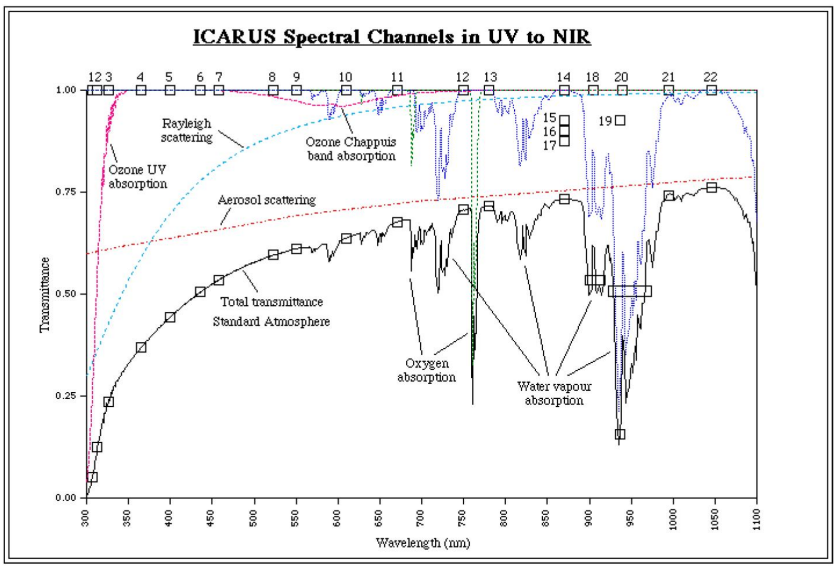

Figure 6.18.: Optical transmittance of the atmosphere for a vertical propagation path between ground and space. (Data from the "Natural Environment Research Council", http://www.soc.soton.ac.uk/RSADU/.)

Optical turbulence

The motion of air is highly turbulent, due to temperature and pressure gradients, resulting in wind shears (i.e. a wind gradient) or convection (for a detailed treatment of this topic please refer to [78, 79]). This causes a temporally and spatially random redistribution of the refractive index n and induces a number of effects on an optical wave related to its temporal intensity fluctuations (scintillations) and phase fluctuations (wavefront distortion). These effects can essentially be split into two categories, i.e., *turbulence induced beam wander* and *turbulence induced beam spreading*.

An important parameter for characterizing the turbulence induced effects is the refractive index structure parameter C_n^2, which is a measure of the fluctuation of n. At least over short time intervals it is reasonable to consider C_n^2 constant at a certain height above uniform terrain. Like in the Hufnagel-Valley 5/7 model [80, 81, 82], C_n^2 can then be described as a function of height.

When talking about **beam wander** [83] one has to distinguish between *long-term* and *short-term* beam wander. The latter originates from the deflection of a finite optical beam on turbulent cells. Since these turbulent cells are flowing across the propagating path, the centroid of the beam is randomly deflected in different directions. If the light beam is observed on a screen it "jumps" around on timescales of some 1 kHz. However, when averaged over time, the intensity's centroid position remains unchanged. The magnitude of the short-term beam wander depends on the refractive index structure parameter and the path length L. It is characterized by the root-mean-square of the beam displacement r_{bw} from the time-averaged center, which is for a collimated Gaussian beam with waist

ω_0 given by:

$$\langle r_{bw}^2 \rangle^{\frac{1}{2}} = \sqrt{2.87 \cdot C_n^2 \cdot L^3 \cdot \omega_0^{-\frac{1}{3}}}. \tag{6.22}$$

When the beam is collected by a telescope, these short-term movements cause the *angle*

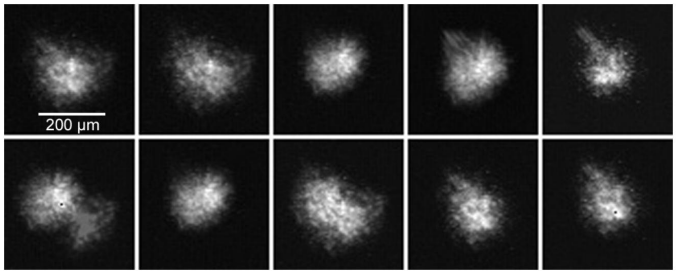

Figure 6.19.: Series of beam images showing the image jitter in the detector's focal plane at the OGS telescope after propagation through the 144 km free-space link between La Palma and Tenerife. The pictures were taken during a previous measurement campaign. The effective focal length of the OGS telescope (1 m diameter) during these measurements was reduced from f = 39 m to f = 5 m with a focal length reducer. The temporal separation between the images was several seconds and the exposure times were a few milliseconds.

of arrival to fluctuate, which results in an *image jitter* in the focal plane of the telescope. During a previous experiment, we measured the image jitter on the same 144 km free-space link between La Palma and Tenerife with a CCD camera in the detector's focal plane (see Figure 6.19).

This is of course a well known phenomenon for astronomers using ground-based telescopes [84], where the achievable angular resolution does not grow indefinitely with the telescope diameter. In contrast to short term beam wander, long-term beam wander is a result of the change in the atmospheric layering, slowly (on timescale of minutes) altering the global temperature and pressure gradients. This affects the time averaged centroid position of the beam to slowly move off its initial position on the screen. In the focal plane of a telescope, this effect also causes the centroid position of the focus spot to move off its initial position. This was also measured in our previous experiment with the same optical setup as for the measurements of the image jitter described above. The result is shown in Figure 6.20.

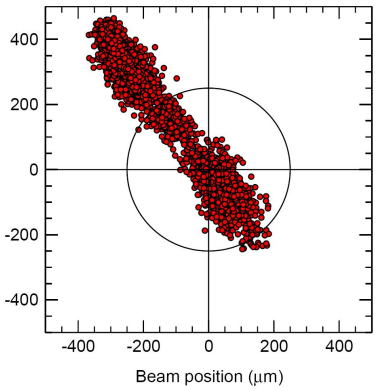

Figure 6.20.: Measurement of the beam centroid positions in the detector focal plane over a full measurement time of 55 min; the circle indicates the detector's active area.

The effect of turbulence induced **beam spreading** must also be divided into *short-term* and *long-term*

beam spreading. The short-term beam waist ω_{st} at the receiver screen can be obtained by taking a picture with an exposure time shorter than the characteristic time between two "jumps". In general, w_{st} is larger than the diffraction limited spot size in vacuum. The long-term beam waist ω_{eff} is a result of the additional short term beam wander (see Figure 6.21) and can be obtained by taking pictures of the beam on the screen with exposure times much larger than the characteristic "jump"-time. The effective long-term beam radius is given by

$$\langle \omega_{\mathrm{eff}}^2 \rangle = \langle \omega_{\mathrm{st}}^2 \rangle + \langle r_{\mathrm{bw}}^2 \rangle. \tag{6.23}$$

Similarly to long-term beam spreading, *image blur* can be observed in the focal plane of a telescope, when taking a picture with long exposure-time. Hence, image blur and image jitter can be seen as the counterparts to beam spreading and beam wander and can be used to quantify turbulence induced effects.

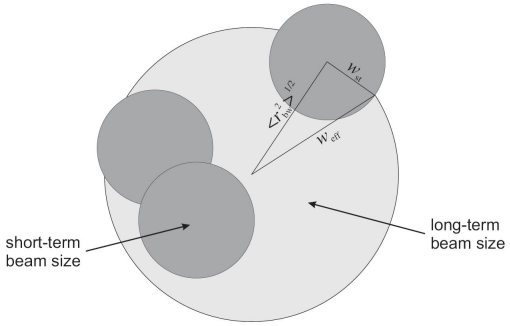

Figure 6.21.: An illustration of the short-term and long-term beam radius: the dark shaded circles represent the short-term beam size ω_{st}; the long-term beam radius ω_{eff} results from additional beam wander and is indicated with the large light circle. (Figure taken from [76].)

Transmitter and receiver telescope

The transmitter telescope in La Palma consisted of an output fiber coupler and a $f/4$ best form lens ($f = 280$ mm). In order to allow fine pointing, the telescope was mounted onto a stable tip-tilt stage, equipped with stepper motors for the horizontal and vertical axis. Furthermore, the output fiber coupler was motorized to provide a means of changing the z-position of the focus. The receiving telescope was the European Space Agency's Optical Ground Station (OGS) in Tenerife, which is a Zeiss 1 meter Ritchey-Chrétien/Coudé telescope. We used the Coudé focus (focal length $f = 39$ m) to set up our analyzer modules.

Since the long-term beam wander causes the beam to drift away from the receiving aperture, the pointing of the transmitter telescope was controlled automatically by a closed loop tracking system[9]. Therefore, a green laser (beacon) was attached to the OGS

[9]Short-term beam wander can be compensated using adaptive-optic systems. However, its implementation would have been very complex and was not established in our setup.

telescope and directed towards La Palma. Using an additional lens at the transmitter with 15 cm diameter and 40 cm focal length, the beacon beam was focused onto a CCD camera. The position of the spot on the CCD was calculated by software and the stepper motors were moved, such that the spot was kept on a fixed position. Likewise, the OGS monitored the position of a beacon laser mounted at the transmitter telescope and adjusted its pointing direction accordingly.

The entangled photons received at the OGS were detected, using avalanche photodiodes (APDs) with an active area of 500 μm. In order to minimize the loss along the path from the receiving aperture through the analyzer modules to the detectors, a suitable optical design for imaging the beam onto the detectors had to be found (see Figure 6.22). The optical design was essentially defined by the maximal expected angle-of-arrival fluctuations (77 μrad), the clear aperture of the Pockels Cell crystals (4 mm), the active area of the detectors (500 μm) and the availability of lenses with certain focal lengths.

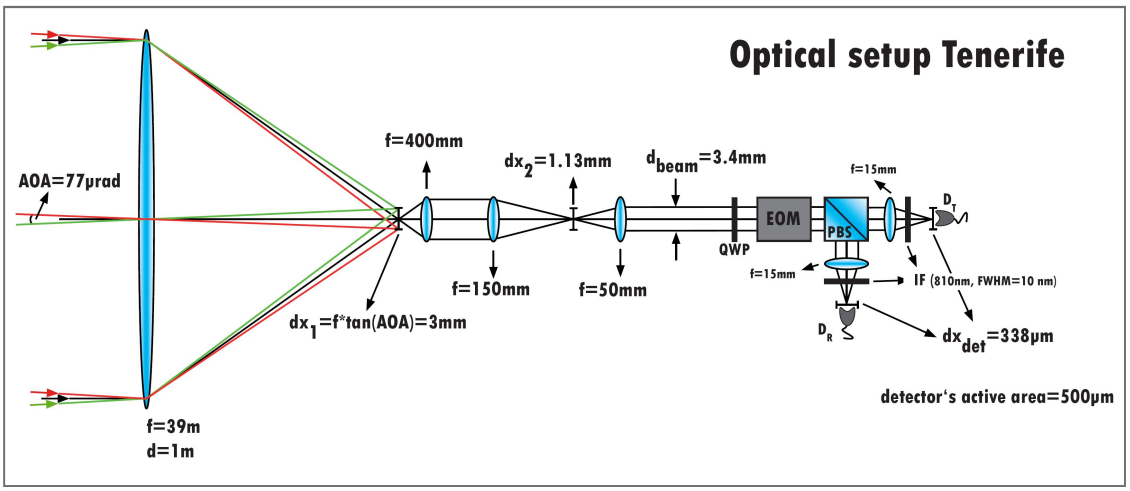

Figure 6.22.: The optical design in the Optical Ground Station (OGS) in Tenerife (not to scale). An incoming beam was collimated appropriately (please refer to the main text for details) and sent through the polarization analyzer module. The lens system was chosen, such that the image jitter at the detector's focal plane dx_{det}, caused by the angle-of-arrival (AOA) fluctuations, was smaller than the active area of the detectors. Interference filters (IF) in front of the detectors were used to reduce background light.

The received beam was collimated after the OGS's Coudé focus (39 m) using a $f = 40$ cm lens to approximately 1 cm diameter, much larger than the aperture of the Pockels Cell crystals (4 mm). Hence, a telescope with magnification 1:3 was used to reduce the beam size to approximately 3.4 mm. Finally, a lens with $f = 15$ mm was used to focus the beam onto the active area of the APD. From previous experiments, we expected maximal angle-of-arrival fluctuations of approximately 77 μrad (see Section "Inter-island link characterization" below). This would cause the spot in the Coudé focus to deviate $\approx \pm 1.5$ mm from the optical axis. However, with our optical design the image jitter in the

Coudé focus was reduced to an image jitter of only ±169 μm in the plane of the APD's active area. Additionally, to minimize background counts coming from the moon or from stars, interference filters for 810 nm with a full-width-half-maximum (FWHM) of 10 nm were put in front of the detectors.

Inter-island link characterization

In a previous measurement campaign, the same 144 km free-space link was characterized with different methods[10](see [86, 76]). Therefore, a strong laser beam at 808 nm was transmitted using a 7 cm diameter lens.

At first, the transmitted spot was projected onto the outside wall of the OGS telescope building and very roughly estimated spot diameters between 3 m and 6 m could be observed by eye. In comparison, in the absence of atmospheric turbulence, the beam would be spread to a radius of only

$$\omega(144000) = 0.035\sqrt{1 + \frac{144000^2}{\left(\frac{\pi \cdot 0.035^2}{0.000000810}\right)^2}} \approx 1.1 \text{ m}, \tag{6.24}$$

due to vacuum beam spreading.

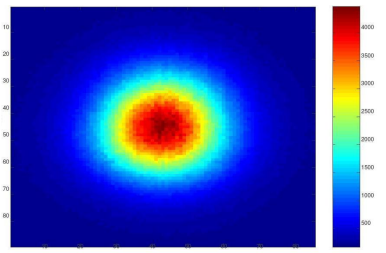

Figure 6.23.: A blurred image of the laser beam, transmitted through the 144 km inter-island link and focused onto a CCD camera at the receiver with $f = 39$ m.

Secondly, the transmitted beam was imaged onto a CCD camera in the Coudé focus and the image blur was observed, as shown in Figure 6.23. From pictures taken with 1 second exposure time, blurred spots of $1/e^2$-width between 0.6 mm (weak turbulence conditions) and 3 mm (strong turbulence conditions) have been observed. The corresponding angle-of-arrival fluctuations of $\Theta_{AOA} = 15.4$ μrad and $\Theta_{AOA} = 77$ μrad could be calculated by

$$\Theta_{AOA} = \frac{\Delta d_{1/e^2}}{f}, \tag{6.25}$$

with the measured $1/e^2$-width $\Delta d_{1/e^2}$ and the focal length of the camera imaging system $f = 39$ m. Additionally, the effective beam waist at the receiver could be calculated via

$$\omega_{eff} = \Theta_{AOA} \cdot L, \tag{6.26}$$

where L is the link distance.

With our link distance of 144 km, the widths of the obtained blurred images correspond to effective spot waists of $\omega_{eff} = 2.2$ m and $\omega_{eff} = 11.1$ m, respectively. Since the receiving telescope's primary mirror M_1 has a diameter of $D_{M_1} = 1$ m, smaller than the smallest obtained effective beam waists, geometrical losses occur at the receiver, which were referred to as turbulence losses L_T. With the additional obstruction due to the

[10]The link has previously also been used for (classical) optical free-space communication experiments [85].

secondary mirror M_2 of the receiving telescope ($D_{M_2} = 0.33$ m), these losses could be calculated with:

$$L_T := \exp\left[-\frac{2(D_{M_2}/2)^2}{\omega_{eff}^2}\right] - \exp\left[-\frac{2(D_{M_1}/2)^2}{\omega_{eff}^2}\right]. \tag{6.27}$$

Consequently, the resulting turbulence losses for the beam waists $\omega_{eff} = 2.2$ m and $\omega_{eff} = 11.1$ m were 10.6 dB and 18.4 dB respectively.

Finally, the end-to-end transmission losses, including turbulence losses, absorption and scattering losses and losses in the optical path of the transmitter and receiver telescope were determined by comparing the intensity of the alignment laser at 808 nm wavelength before the transmitter lens and after the receiving telescope optics in the focal plane, using identical optical power meters. The measured attenuations were 25 db (for $\omega_{eff} = 2.2$ m) and 35 db (for $\omega_{eff} = 11.1$ m), from which ≈4 dB were assigned to losses in the OGS telescope's path. From this, one can determine the attenuation caused by absorption and scattering with ≈10 dB and ≈13 dB, respectively, implying a loss of 0.07 dB/km and 0.09 dB/km. This is in reasonable agreement with values in the literature were values between 0.04 dB/km and 0.08 dB/km at altitudes above 2000 m can be found [87, 17].

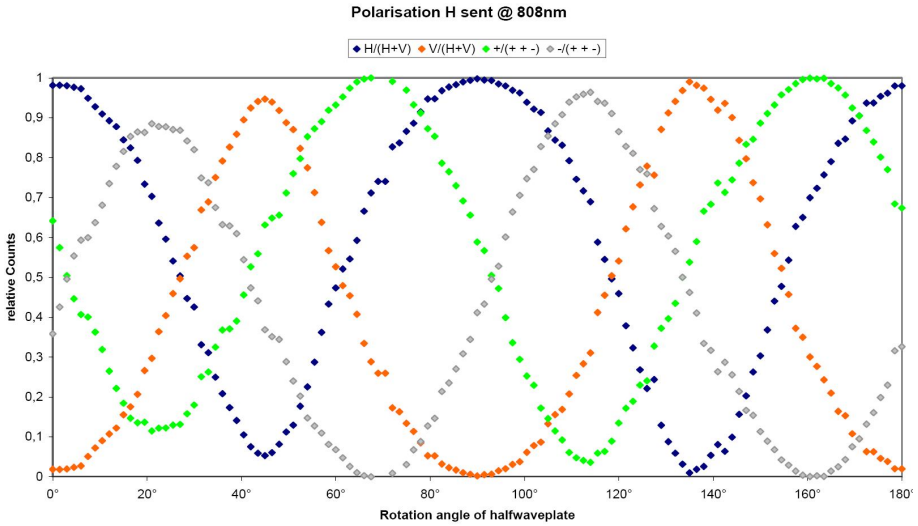

Figure 6.24.: Polarization of 808 nm laser light. The count rates were normalized due to the intensity fluctuations of the free-space link. The visibilities of the four polarization states could be calculated from the upper plot. They were for H 98,0%, for V 99,5%, for +45° 93% and for −45° 99,8%. The reason for the non-sinusoidal shape of the curves can be explained by the non-constant rotation speed of the motorized half wave plate.

The effect of the atmosphere on the polarization was determined by sending polarized photons through the quantum link[11]. For compensation of the polarization disturbances

[11] Especially in the case of multiple scattering, depolarization of the incident light can occur [74]. However,

due to the fiber, which was used in La Palma to connect the photon source to the telescope, the atmosphere and the optics of the receiver telescope, a quarter wave plate and a half wave plate were used in the optical path of the OGS to rotate the polarization back to the polarization vector, which was sent from La Palma. Finally, the polarization was analyzed, using an analyzer module similar to the one used in the experiment described in this thesis. After initial polarization compensation, the half wave plate was rotated, altering the counts in the analyzer outputs (see Figure 6.24). The visibilities of H, V and $-45°$ indicate that the atmospheric disturbance as well as the disturbance of the telescope optics onto the polarization state can be excluded. The low visibility of the $+45°$ polarization could be traced back to misalignment of the corresponding detector.

6.2.6. Optical fiber channel

As discussed in Section 6.3, the delay line for Alice's photon can easily be accomplished using an optical fiber. We therefore decided to use a 6 km long (coiled) single mode fiber from `Nufern` of type 780-HP. The length was chosen in order to exhaust the maximal acceptable two-photon loss in our setup and to have a clear space-like separation between Alice's and Bob's measurements. Using a laser diode at 810 nm, we measured a total attenuation through the fiber of 17 dB. To avoid polarization drift due to temperature change, the fiber was placed in a thermally insulated box and temperature stabilized to $40°\text{C}\pm0.2°\text{C}$.

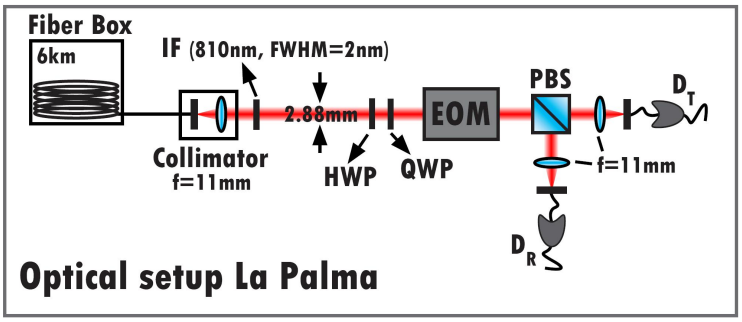

Figure 6.25.: The optical design of the polarization analyzer module after the 6 km fiber channel. The photons were collimated and sent through the analyzer module. Finally they were coupled into multi mode fibers and guided to the detectors. An interference filter (IF) was used after the output collimator to reduce the back ground counts originating from the remaining UV pump light and fluorescence in the SPDC source.

The exact time delay in the fiber was verified via coincidence detection of photon pairs from our SPDC source. Therefore, one photon of a pair was sent through the fiber before

quantitative measurements over horizontal propagation paths in the lower clear atmosphere [88, 89] indicate that the polarization of a propagating wave is only minimally affected, often below the sensitivity of the apparatus.

it was detected, while the other one was detected immediately. Both detection signals were fed into a coincidence logic device where the relative time delay between the input signals could be adjusted by software. A peak in the coincidence rate was found for a relative delay of 29.6 μs.

During the experiment, the output of the fiber channel was directly connected to a collimator lens ($f = 11$ mm) and sent through Alice's polarization analyzer module. The optical design of this setup is depicted in Figure 6.25. In each output mode of the analyzer, fixed-focus lenses with $f = 11$ mm were used to couple the photons to multi mode fibers, which were connected to the detectors. The loss through the analyzer module, including fiber coupling, was measured to be 3 dB. Hence, the overall attenuation through the fiber link could be specified with 20 dB.

6.2.7. Classical channel

For transmitting the random signal from Alice's distant QRNG to the analyzer module, we used a time stable 2.4 GHz AM[12] RF[13] link (1.2 km link distance). AM is a technique used in electronic communication, most commonly for transmitting information via a radio carrier wave. It works by varying the strength of the transmitted signal in relation to the information being sent. The strongest signals of a radio link are on the direct line between transmitter and receiver and always lie in the 1$^{\text{st}}$ *Fresnel Zone*, i.e., a spheroid between the transmitter and receiver antenna. If some part of the signal is reflected from obstacles, it may arrive out of phase with the direct signal and reduce the power of the received signal. Hence, in order to maximize the received signal strength, the line of sight must be kept obstacle free. The radius of the first Fresnel Zone is highest in the center of the RF link and given by

$$r = 17.32\sqrt{\frac{D}{4f}}, \tag{6.28}$$

with the radius r in meters, the total link distance D in kilometers and the transmitted frequency f in gigahertz. For the parameters of our radio link, $r = 6.12$ m could be found. Since the antennas were installed on rooftops and the link was oriented uphill the line of sight was essentially obstacle free.

Using the 1 pps[14] time reference from the global positioning system (GPS), a transmission time of 4.5 μs was measured. 3.9 μs could be assigned to 1.2 km free-space transmission and 0.6 μs to electronics and cables at the RF transmitter and receiver. For clear transmission through the classical channel, the output of the QRNG was set to a toggle rate of 2 MHz.

[12] Amplitude Modulated
[13] Radio Frequency
[14] pulse per second

6.2.8. Electronics

Single photon detectors

Our detectors were actively quenched `PerkinElmer` silicon avalanche photo diodes (APDs) with a quantum efficiency between 25% and 40%. On Alice's side, these were fiber coupled modules consisting of four diodes of which two were used during a measurement and the remaining were used during the alignment.

On Bob's side, the diodes had an active area of 500 μm and the received photons were focused directly onto it. Each diode was mounted in a housing together with a small active quenching circuit. The APDs were biased to around +220 V and cooled to a temperature of about -30°C.

The detection signals were 200 ns long transistor-transistor logic (TTL) pulses and the optical response time of the diodes was specified as 0.5 ns. In [90, 91, 92] more information about single-photon detection and the required electronics can be found.

Pockels Cell driver

The Pockels Cell driver was bought from `Bergmann Messgeräte`. It contained a high-voltage power supply for setting the desired voltage and an "optical head". Within the optical head was the Pockels Cell and a high voltage switching circuit. The principle of the high voltage switching circuit is shown in Figure 6.26. The state of the system is controlled by four signals *On-A*, *Off-A*, *On-B* and *Off-B*[15]. For applying positive voltage

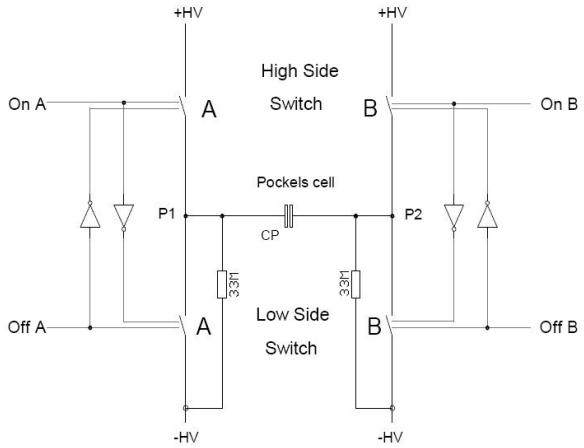

Figure 6.26.: The principle of a double push-pull Pockels Cell driver. *On-A* closes high-side switch A and opens low-side switch A synchronously. Likewise *Off-A* opens high-side switch A and closes low-side switch A synchronously. The control signals for push-pull switch B operate the same. (Figure taken from [93].)

to the crystals, the signals *Off-B* and *On-A* are required. Contrary, the signals *Off-A* and

[15] These signals must be TTL signals ≥3 V.

On-B are required for switching to negative voltage. The electronic delay in the Pockels Cell electronics, i.e., the time from applying a trigger signal until the voltage is applied to the crystals, was measured to be 45 ns.

FPGA logic for generating the Pockels Cell signals

We used a field programmable gate array (FPGA) logic to sample the random sequence from the QRNG and to generate the required signal sequence for the Pockels Cell driver. The FPGA chip was programmed, using `Xilinx Inc.` software and the VHDL source code can be found in Appendix C. The QRNG signal was connected to the input of the FPGA module and was sampled at a rate of 1 MHz (as required for optimal performance of the Pockels Cell). Depending on its state, either the output channels 1 (*On-A*) and 2 (*Off-B*) or the output channels 3 (*On-B*) and 4 (*Off-A*) were simultaneously set to 5 V (see Figure 6.27). These four outputs were then connected accordingly to the four inputs of the Pockels Cell driver.

The remaining four output channels 5-8 of the FPGA module were used to provide NIM[16] signals, wherewith the detectors of the analyzer modules could be identified with the correct polarization analyzing basis, as will be described in the next Section. By delaying and tailoring these signals as depicted in Figure 6.27, detection events that happened within the optical switching process of the Pockels Cell were automatically discarded.

QUAD logic array for correct detector assignment

The 200 ns TTL detection pulses from the two detectors D_T and D_R were converted to 10 ns long NIM pulses (as required for further processing), using constant fraction discriminators (CFDs). Additionally, a copy of each 10 ns pulse could be obtained via a second output of the CFD. Each of the resulting four detection NIM pulses was then combined with one of the four NIM signals from the FPGA module output channels 5-8 in a QUAD 4-Input Logic Unit from `Ortec`. This unit only provides an output if both inputs are simultaneously "high". In the end, a signal at output 1 (2) of the QUAD unit could be identified with a detection event at detector D_T (D_R) when the actual random number was "0". This corresponds to the polarization state $|0°\rangle$ ($|90°\rangle$). Likewise, a signal at the output 3 (4) could be identified with a detection event at detector D_T (D_R) when the actual random number was "1", corresponding to a photon polarization of $|45°\rangle$ ($|135°\rangle$). The correct assignment of the QUAD logic unit output signals with the detected photon polarization can be found in Table 6.1.

6.2.9. Time-tagging and coarse synchronization

The TTL output pulses from the QUAD 4-Input Logic Unit triggered a self designed time-tagging unit which labeled every detection event with a 64-bit tag, containing the channel information and a time-tag with a resolution of 156 ps. Simultaneously, the gathered

[16] Nuclear Instrumentation Module: "low"=0 V, "high"=−0.8 V

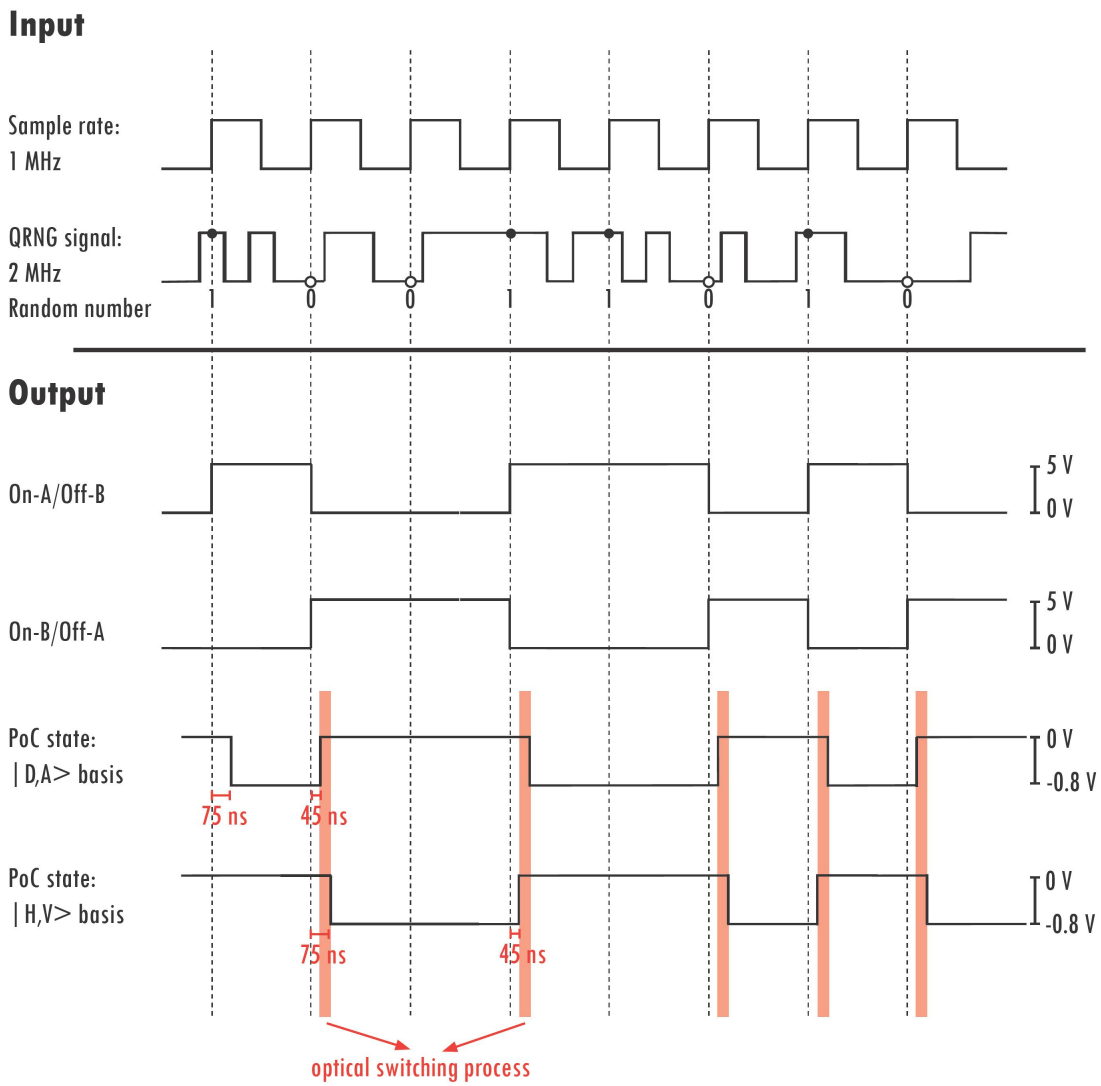

Figure 6.27.: The signal sequence generated by the FPGA module depended on the state of the random input signal. A random number "0" ("1") required simultaneous trigger signals for the Pockels Cell driver at inputs *On-B* and *Off-A* (*On-A* and *Off-B*), directly switching the Pockels Cell to the state −QWV (+QWV). Additionally, *PoC state* NIM signals (i.e., simply the TTL-to-NIM converted version of the Pockels Cell driver signals) were required to identify the detectors with the correct photon polarization. However, before the NIM pulses could be combined with the detector signals (please refer to the main text for details), they had to be delayed for 45 ns with respect to the Pockels Cell trigger signals, due to the electronic delay of 45 ns of the trigger signal in the Pockels Cell driver. Additionally, to discard detection events within the optical switching process, the rising edge of the NIM signals had to be additionally delay by at least 9 ns (i.e. the optical rise time of the crystals), while the falling edge had to remain unchanged. However, for confidence we added 30 ns, resulting in a total delay of the rising edge of 75 ns.

QUAD output	actual random number	detector notation	corresponding polarization
1	"0"	$D_{T,0}$	0°
2	"0"	$D_{R,0}$	90°
3	"1"	$D_{T,1}$	45°
4	"1"	$D_{R,1}$	135°

Table 6.1.: The assignment of the QUAD logic output channels with the detector notation and the actual random number. The actual random number defined the state of the Pockels Cell and with it the actual polarization analyzing basis. Thus, the polarization of the detected photons could be assigned correspondingly.

data was sent to the measurement computer via a National Instruments (NI) PCI-6533 high-speed realtime digital-I/O connection with a maximum clock rate of 2 MHz and a maximum data rate per channel of 2 MBits/s. In order to have a common time reference at both observers, the time-tagging electronics relied on a highly stable 10 MHz signal from a GPS disciplined oscillator.

6.2.10. Software and fine synchronization

A self designed `LabView` program controlled the data acquisition process via the NI card and stored each detector click together with its time-tag on the local hard drive.

After a measurement run, the time-tagging data file from Tenerife was sent to the measurement computer in La Palma via Internet. There, a C^{++} program calculated the cross-correlation functions for all 16 detector combinations in a time range $\pm$500 ns around an adjustable coarse delay (i.e., roughly the difference between the transmission time of the photons through the corresponding quantum channels) with a resolution of 0.5 ns.

The cross-correlation output file was further processed using a self designed `LabView` programm. A peak in the cross-correlation function indicated the correct fine delay Δt for the coincidence evaluation. The coincidence-time window could be adjusted by summing over a certain number of bins in the output file of the C^{++} program. In the experiment, we used a coincidence time-window of 1.5 ns for computing the 16 coincidence count rates required for the CHSH inequality.

Due to a relative drift[17] between the individual time bases (see Figure 6.28), Δt was a time dependent parameter, resulting in a broadening of the coincidence peak. This required to increase the coincidence-time window, which in turn resulted in a reduction of the signal to noise ratio (SNR), due to an increase in accidental coincidences[18]. However, this problem could be overcome by analyzing the time-tagging data in short blocks. By

[17] One major reason for this drift are the inconsistencies of the atmospheric conditions, specifically in the ionosphere. This affects the speed of the GPS signals passing through the earth's atmosphere [94]. The effects of the ionosphere is largest for satellites near the horizon, because then the path through the atmosphere is longer.

[18] The number of accidental coincidences C_{acc} between two detectors can be calculated from the single count rates, S_1 and S_2, and the coincidence-time window τ_{coinc} with $C_{acc} = S_1 \cdot S_2 \cdot \tau_{coinc}$.

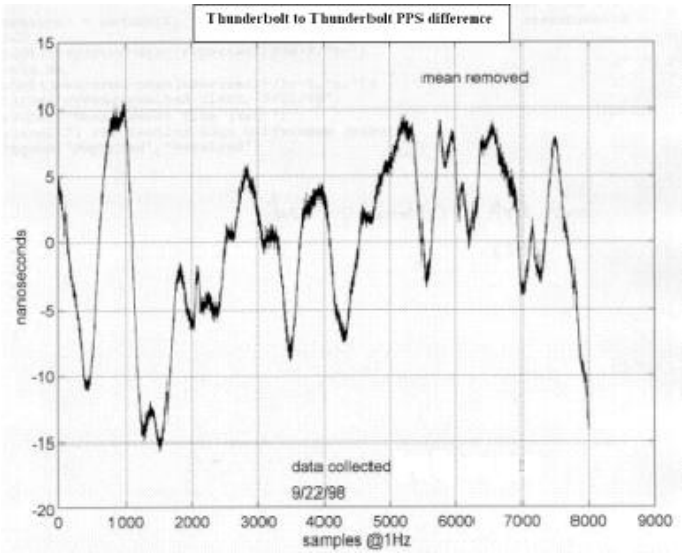

Figure 6.28.: The relative time-drift between the pps signals of two GPS receivers placed next to each other.

recalculating the fine time delay Δt for any individual block enabled our software to compensate the relative drift with an accuracy of 0.5 ns. During the data analysis, we found that a block length of 30 s was reasonable for our purpose.

6.3. Experimental situation

The geographical situation in our experiment is depicted in Figure 6.29. Alice and the source were located on the Roque de los Muchachos in La Palma, approximately 2400 m above sea level. Our laboratory was established in a container placed on the parking lot of the Nordic Optical Telescope (NOT), power and internet access was achieved through the NOT infrastructure. The only reasonable possibility for transferring Alice's quantum random number generator ($\mathrm{QRNG_A}$) to some place apart, was to put it in the service building next to the Residencia. The distance from the service building to our container was 1.2 km. Bob was situated in the OGS building in Tenerife, receiving photons that were transmitted through the horizontal 144 km free-space quantum channel.

Before I describe in detail our experimental situation, I am going to define the durations of the crucial space-time events, which were essentially given by the properties of the corresponding experimental parts described in Section 6.2. From the subsequent discussion of the actual space-time scenario in the source's reference frame, as well as in the reference frame of a moving observer, it should become clear that our experiment indeed fulfilled the locality and freedom-of-choice conditions.

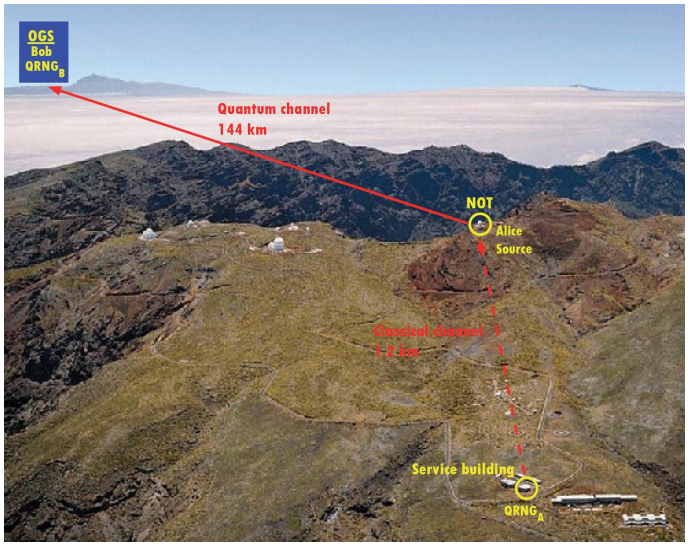

Figure 6.29.: The geographical situation of our experimental configuration. Alice and the entangled photon source were located in La Palma at the NOT parking lot. Alice's quantum random number generator ($QRNG_A$) was located in the service building of the Residencia, 1.2 km apart from Alice and the source. Bob, together with $QRNG_B$ were located in Tenerife 144 km in direct distance to Alice.

6.3.1. Event durations

The following list summarizes the upper bounds for the durations of the crucial space-time events, defined by the physical and technical properties of the used equipment.

Duration of the emission event The coherence length of our pump laser could be seen as the time-uncertainty for a photon-pair emission. Hence, it was used to define the duration $\tau_{emission}$ of the emission event **E**, which was for our pump laser $\tau_{emission} <$ 1 ns.

Duration of the choice event The duration of the choice events **a** and **b** was given by the time the QRNG needed to establish a random state at its output. As discussed in Section 6.2.2, this time could be specified with $\tau_{random} < 100$ ns. Note that the choices (i.e., the actual random numbers) were refreshed at a rate of 1 MHz, as required for optimal operation of the Pockels Cell. Hence, each setting was applied for a 1 μs interval and the required space-like separations had to be fulfilled for the whole interval, as discussed in Section 6.3.

Duration of the measurement event The measurement duration was defined as the time from a photon impact on the detector surface until a classical signal was generated at the detector output (i.e., until the completion of the APD breakdown)[19]. It is given by the optical response time of our detectors and could be specified with $\tau_{det} < 1$ ns.

[19]There is an ongoing debate about when a quantum measurement is finished. Quantum theory by itself

6.3.2. Final space-time situation

The final space-time scenario is illustrated in Figure 6.30a. Bobs photon was guided from the source to the transmitter telescope next to the container, using a 10 m single-mode fiber, and sent to Tenerife via a 143.6 km long free-space channel (479 μs flight time). Measuring Alice's photon immediately after the emission (i.e., already before Bob's photon has actually reached the transmitter telescope) would allow a signal from measurement **A** to travel (with the speed of light in vacuum) to Bob in Tenerife and influence the measurement apparatus before Bob's photon arrives. In this case, the outcome independence assumption would not be guaranteed. However, as discussed in Section 6.3, the space-like separation between **A** and **B** can be restored by inserting a delay line for Alice's photon. In our experiment, this delay line was realized with a 6 km long optical fiber channel, as described in Section 6.2.6, and resulted in a temporal delay of 29.6 μs.

Additionally, the random setting choices on one side had to be space-like separated from both the measurement event on the other side (i.e., setting independence assumption) and from the photon emission event **E** (i.e., freedom-of-choice assumption). At Alice, the latter could only be achieved by transferring the QRNG to a place 1.2 km apart from the photon source and Alice. The random signal was then transmitted to Alice's measurement apparatus via a radio channel (described in Section 6.2.7), with $\approx$ 4.5 μs transmission time (3.9 μs free-space transmission and 0.6 μs delay due to the electronics and cables). Note that in the experiment, the random numbers were refreshed every 1 μs. This means that there existed 7 subsequent random settings that lay outside the light cone of the emission event. However, if the random numbers would be used to implement the settings immediately after their transmission through the radio channel, the corresponding random choices would still have been made inside the light cone of the emission. Hence, we further delayed the random signal at Alice electronically by 24.6 μs. Since the photon emission time is probabilistic, this resulted in a situation where Alice's choice event **a**, corresponding to a given measurement **A**, occurred on average simultaneously with the emission event **E**, i.e., the measurement event occurred on average in the middle of the 1 μs setting interval. This situation also enforced that the choice event **a** is space-like separated from the measurement event **B** on the other side.

Bob was, together with his QRNG, situated in the OGS telescope in Tenerife. There, the space-like separation of the choice events from the emission event could simply be achieved by electronically delaying the random output signal of the QRNG by more than 280 ns, which is the time a hypothetical vacuum signal from the emission event arrives earlier at Bob's analyzer than Bob's photon. This is, because the speed of light in the atmosphere (n=1.0002) is less than the vacuum speed, resulting in a flight time difference of 100 ns. Another 50 ns result from the delay of Bob's photon in the single-mode fiber

has no definitive answer to this question. A commonly accepted interpretation, on which the definition of the measurement duration in this thesis is based, suggests that a measurement is over, as soon as the result is secured in a classical system (i.e., a classical signal,...). Decoherence claims that a measurement is finished once the information is in the environment. Another possible interpretation assumes a connection between quantum measurements and gravity [95, 96], i.e., the measurement is over, after a massive object has been displaced. The characteristic time depends on the displacement distance, the volume and the mass of the displaced object.

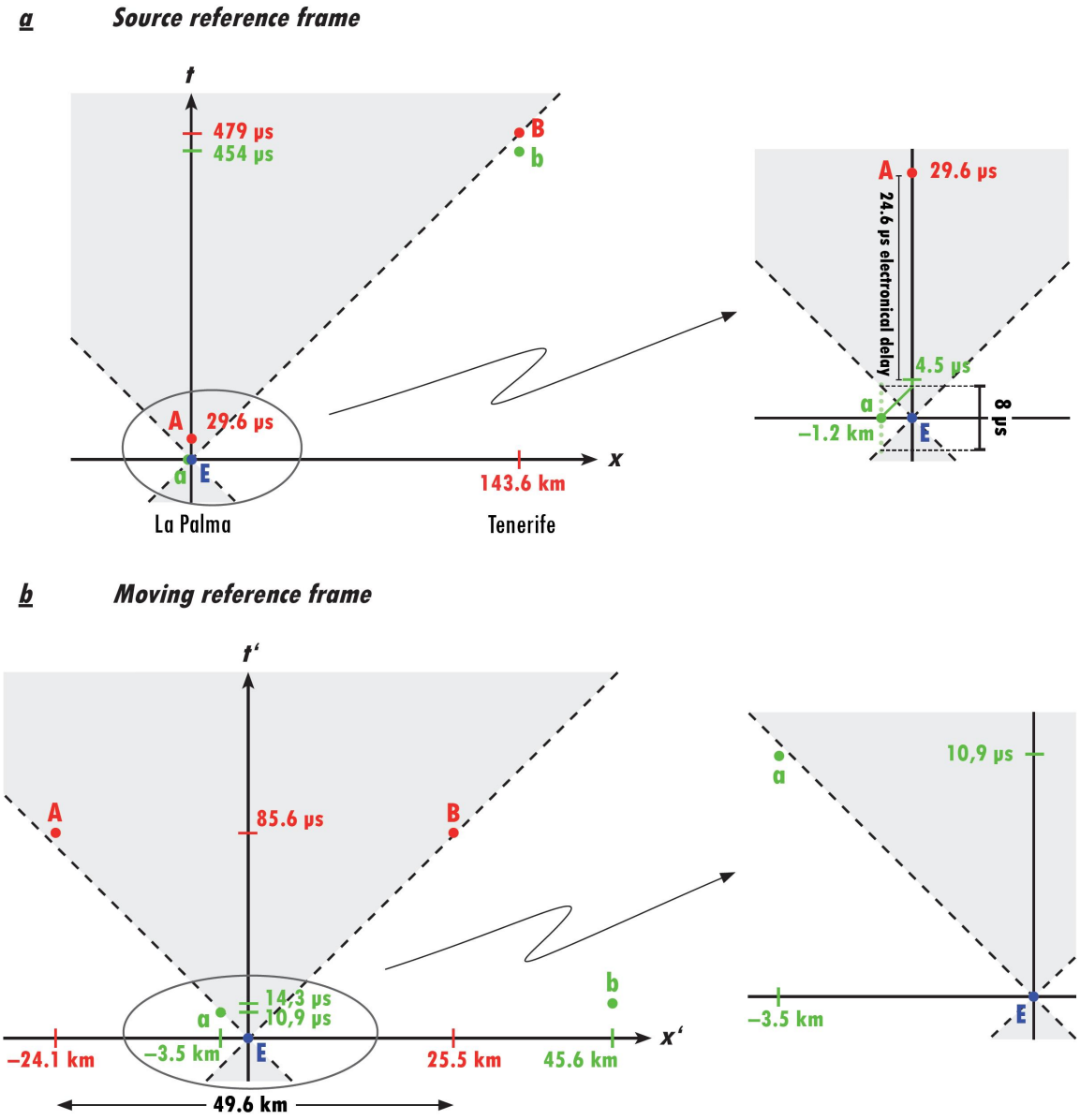

Figure 6.30.: *a*: Source reference frame. Alice's random setting choices (indicated by small green dots in the zoomed part of Figure a), each applied for a 1 μs interval, were transmitted over a 1.2 km classical link, which took 4.5 μs (3.9 μs classical RF link, 0.6 μs electronics). This signal was electronically delayed for 24.6 μs, so that the choice event **a**, corresponding to a given measurement **A**, occurred on average simultaneously with the emission event **E**, i.e., the photon measurement event occurred on average in the middle of the 1 μs setting interval. The choice and emission events were therefore space-like separated. The same electronic delay (24.6 μs) was applied to Bob's choice **b**, so that it was also space-like separated from the source. *b*: Moving reference frame. From the perspective of an observer moving at a speed of $0.938 \cdot c$ parallel to the direction from La Palma (Alice) to Tenerife (Bob), the measurement events, **A** and **B**, occur simultaneously with the emission event approximately in the middle of the two. The locality and the freedom-of-choice loopholes are closed in the source reference frame, and since space-like separation is conserved under Lorentz transformations, they are closed in all reference frames. In the diagrams above, the total uncertainty of the event times is below the thickness of the illustrated points.

from the source to the transmitter telescope and 130 ns result from the delay in the optical path of the OGS telescope. We decided to implement the same delay for Bob's random choices as it was used at Alice, i.e., 24.6 μs. As will be discussed below, this resulted in a quite symmetric space-time diagram within a moving reference frame. This time-delay also guaranteed that the choice event **b** is space-like separated from the measurement event **A**.

Note, that the event durations (see Section 6.3.1) are below the thickness of the illustrated event points on the plot scale of Figure 6.30. Hence, the combined conditions enforced within our setup clearly guaranteed the required space-like separations for performing a Bell test under locality and freedom-of-choice conditions[20].

Moving reference frame

Since Alice's and Bob's measurement events were space-like separated, there exists a moving reference frame in which those events happened simultaneously. Bob's electronic delay was chosen such that in this frame, the setting choices also happen approximately simultaneously (see Figure 6.30b). The speed of this frame with respect to the source reference frame is $v_{ref} = c_0^2 \cdot (t_B; t_A)/(x_B; x_A) = 0.938 \cdot c_0$ (with the vacuum speed of light c_0), using the space-time coordinates of the measurement events $\mathbf{A} = (t_A, x_A) = (29.6\ \mu\text{s}, 0)$ and $B = (t_B, x_B) = (479\ \mu\text{s}, 143.6\ \text{km})$. The relativistic gamma factor is $\gamma^{-1} = 1/(1 - v_{ref}^2/c_0^2)^{1/2} = 2.89$, giving an effective spatial separation of Alice and Bob (La Palma and Tenerife) under Lorentz contraction of $\gamma^{-1} \cdot 143.6\ \text{km} \approx 50\ \text{km}$. Note that, because space-like separation is conserved under Lorentz transformation, the locality and the freedom-of-choice loopholes were closed in all reference frames.

6.4. Measurement procedure

An illustration of the final experimental setup is depicted in Figure 6.31. The individual parts had to be carefully aligned and characterized before a measurement run. Usually the alignment procedure was performed in the same ordering as it will be described below.

6.4.1. Aligning the Sagnac source

Before every measurement run, the Sagnac source was aligned to locally generate the entangled state (6.9). Using 50 mW of pump power, the source produced entangled photon pairs at a rate of 34 MHz, of which 2.5 MHz could be detected locally after they

[20] I want to remark that the geographical setup is not exactly one-dimensional as drawn in Figure 6.30. However, the deviation from an ideal one-dimensional scenario is only about 24°. The real-space distance between Alice's QRNG and Bob is about 100 m less than the sum of the distance between QRNG_A and Alice (1.2 km), and the distance between Alice and Bob (143.6 km). Thus, using the approximated one-dimensional scenario introduces no deviations larger than 0.3 μs (which is well below the 1 μs setting interval) and hence does not effect the space-like separation of the key events.

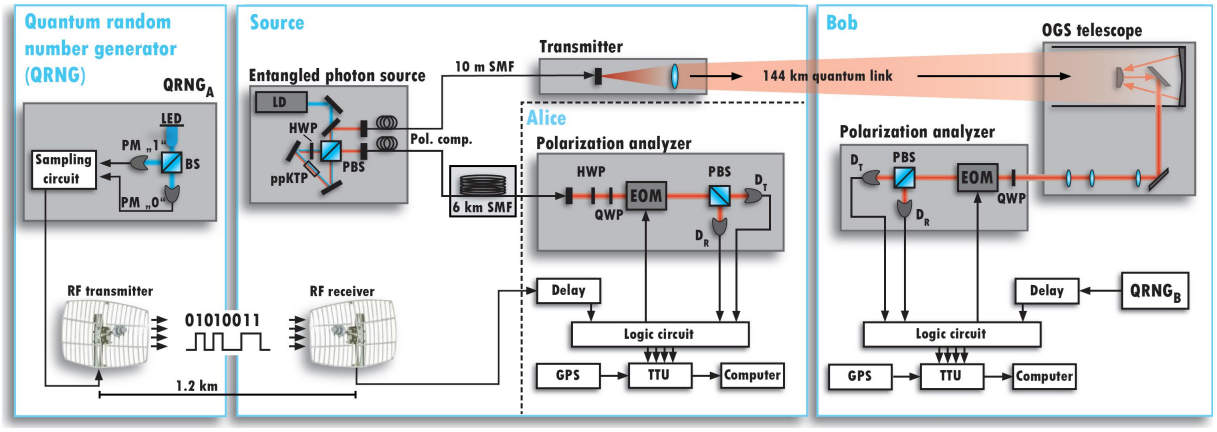

Figure 6.31.: An illustration of the complete experimental configuration of our setup. For a detailed description of the individual parts please refer to the main text in Section 6.2.

were coupled into the single mode fibers[21]. The single mode fibers were later directly connected to the free-space and optical fiber channel. Furthermore, the quality of the generated entangled state was characterized locally by the visibilities in the $|H, V\rangle$ and $|D, A\rangle$ bases. Subtracting accidental coincidences, typical values for the visibilities of 99% in the $|H, V\rangle$-basis and 98% in the $|D, A\rangle$-basis were obtained.

6.4.2. Measuring the attenuation through the quantum channels

After aligning the free-space link using a strong adjustment laser diode, we used the photons from the SPDC source to measure the actual end-to-end link attenuation before a measurement run. Typically, the attenuation, starting from the entangled photon source in La Palma to the detectors at the OGS in Tenerife, was obtained to be 35 dB. However, this is only a rough estimate for the actual attenuation averaged over the total measurement time. In general, the measured attenuation value varied ±3 dB within a (good) measurement night. The "real" average attenuation was later obtained from the number of the coincidences that were detected within a full measurement run.

locally detected coincidence rate	free-space channel attn.	fiber channel attn.	total two photon attn.	expected coincidence rate
2.5 MHz	35 dB	20 dB	55 dB	7.9 Hz

Table 6.2.: The locally detected coincidence rate, the channel attenuations as well as the expected average coincidence rate.

As mentioned in Section 6.2.6, the attenuation through the fiber channel together with

[21] This number could not be measured directly, due to saturation of the detectors, but was inferred from locally detected 250000 photon pairs/s at a pump power of 5 mW and a coupling efficiency of 27%. The coupling efficiency was calculated from the ratio between the coincidence and single count rates.

Alice's analyzer module was 20 dB. Thus, the expected photon-pair attenuation through the whole setup was approximately 55 dB, from which we expected a coincidence rate of ≈8 Hz. To provide a clear overview, I have summarized the above discussed values in Table 6.2.

6.4.3. Establishing a common polarization reference frame

Before starting a measurement run we had to establish a common polarization reference frame between the source, Alice and Bob. Therefore, we used an auxiliary 810 nm laser diode, which was directed at the entangled photon source, such that linearly polarized light was coupled into the output fibers at a well defined single-photon rate. The detector signals were connected to a frequency counter, which in turn was connected to a personal computer, displaying the actual count rates. Note that for the alignment of the reference frame, the HWP in Alice's analyzer module was set to 0°.

First, horizontally polarized light was sent through the corresponding quantum channels to Alice's and Bob's polarization analyzer modules, which were operated in the "random switching mode". With the help of "bat-ears", attached to the fibers which connected the source with the quantum channels (see Figure 6.32), the contrast between the detectors $D_{T,0}$ and $D_{R,0}$ was maximized (see Table 6.1 for details about the detector notation). This guaranteed that a horizontally polarized photon was detected in the horizontal output of the analyzer. Second, 45° polarized photons were sent to Alice and Bob and the contrast between the detectors $D_{T,1}$ and $D_{R,1}$ was maximized, using the same bat-ears. This guaranteed that a 45° polarized photon was detected in the 45° output of the analyzer. However, the alignment for the transmission of the 45° polarization to some degree "destroyed" the alignment for the horizontal polarization. Hence, this procedure had to be repeated (on average 3 to 4 times) until it converged to a point, where both polarizations simultaneously transmitted correctly through the quantum channels. If the entangled photon source initially was aligned to produce the entangled state (6.9), the same state could now be detected between Alice and Bob. At last we set the HWP of Alice's analyzer module back to 11.25°.

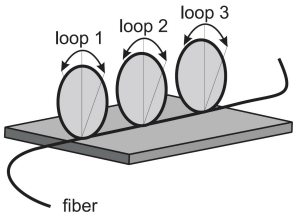

Figure 6.32.: "Bat-ears". Three fiber loops of a few cm in diameter are rotated with respect to each other in order to rotate the polarization of the transmitted photons to the desired state. (Figure taken from [97]).

From the polarization contrast obtained during the alignment we could infer the values for the visibilities of the analyzer modules in combination with the quantum channels. Typically, these visibilities were 99% for the free-space channel together with Bob's analyzer and 97% for the fiber channel together with Alice's analyzer.

6.4.4. Data acquisition

After the shared reference frame was aligned, the alignment laser was switched of and the entangled photon pairs were sent to Alice and Bob. The detector signals were connected

to the time-tagging unit and the measurement programm was activated simultaneously on both sides. A typical measurement run lasted 600 s, limited by polarization drift in the 6 km fiber channel. Even though it was thermally insulated and temperature stabilized we had to realigned the fiber channel after every measurement run, while the free-space quantum channel was observed to be stable over hours.

After a measurement run, Bob's time-tagging data file was sent via internet to Alice's measurement computer where the data analysis was performed (see Section 6.2.10).

6.5. Results

The experimental campaign took place between the 18^{th} of June and the 10^{th} of July 2008. After setting up the experimental equipment for almost 1 week, a dusty cloud moved over from Sahara desert, dramatically reducing the visibility between the islands such that the attenuation through the free-space link was 100%. It lasted nearly another week till the cloud disappeared again. Luckily, the weather conditions in the remaining last week were pretty good and we were able to obtain satisfying results.

6.5.1. Violation of the CHSH inequality

We performed several measurements with the setup described above. At the end, we could accumulate data from 4 measurement runs, 600 s each, performed in two consecutive nights. We obtained a total of 19917 coincidences, corresponding to a coincidence rate of $\frac{19917}{2400} = 8.3$ Hz, in good agreement with the expected value of approximately 8 Hz (see Table 6.2).

The cross-correlation function was calculated using the C^{++} programm and the Bell parameter S was obtained using the self-designed `LabView` program described in Section 6.2.10. The screen-shot of the latter is depicted in Figure 6.33, showing the 16 obtained cross-correlation functions, the corresponding coincidence rates and the resulting S value for one of the 4 measurements.

		Alice			
		$D_{T,0}\hat{=}22.5°$	$D_{R,0}\hat{=}112.5°$	$D_{T,1}\hat{=}67.5°$	$D_{R,1}\hat{=}157.5°$
Bob	$D_{T,0}\hat{=}0°$	1926	539	408	1799
	$D_{R,0}\hat{=}90°$	475	2371	2017	453
	$D_{T,1}\hat{=}45°$	2140	552	1909	562
	$D_{R,1}\hat{=}135°$	625	1893	444	1804

Table 6.3.: The experimentally obtained coincidence count rates for the 16 combinations between Alice's and Bob's detectors.

The accumulated 16 coincidence rates (using a coincidence window of 1.5 ns) for any combination between Alice's and Bob's detectors are shown in Table 6.3. With these

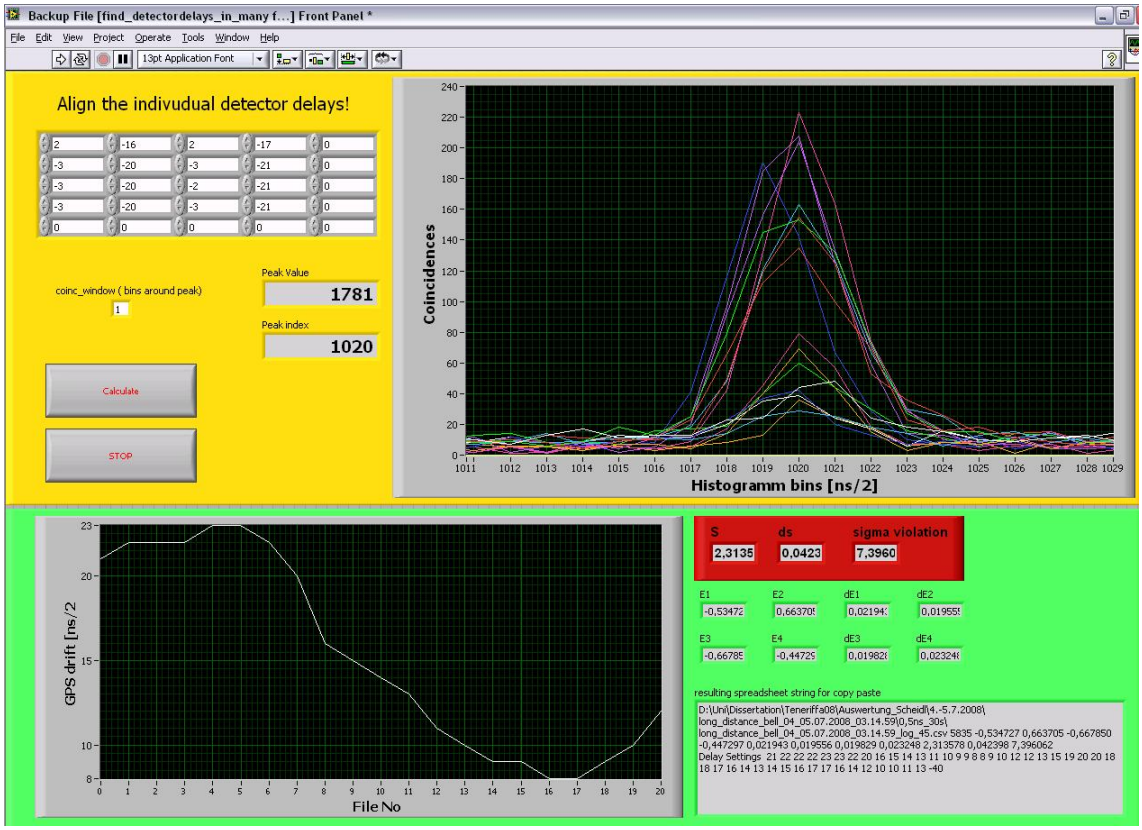

Figure 6.33.: A screen-shot of the `LabView` programm for analyzing the 16 cross-correlation functions. The 16 coincidence peaks of a typical measurement are indicated by the colored lines in the top-right graph. The delay between the individual detectors could be adjusted via the matrix control on the top-left. The relative drift between the time-bases for the actual 600 s measurement is shown in the graph within the green background. The indicator of the actual Bell parameter S for the CHSH inequality is surrounded by a red box.

numbers we could calculate the four expectation values for the CHSH inequality, using Equation (6.14):

$$E(22.5°, 0°) = +0.618 \pm 0.011 \quad (6.29)$$
$$E(67.5°, 0°) = -0.632 \pm 0.011 \quad (6.30)$$
$$E(22.5°, 45°) = +0.548 \pm 0.012 \quad (6.31)$$
$$E(67.5°, 45°) = +0.574 \pm 0.012. \quad (6.32)$$

Inserting these values into the CHSH inequality 6.13 results in an experimentally obtained Bell parameter of

$$S_{exp} = 2.37 \pm 0.023. \quad (6.33)$$

This corresponds to a violation of the local realistic bound 2 of the CHSH inequality by $(2.37 - 2)/0.023 = 16$ standard deviations.

For the error calculation Poissonian photon statistics was used, where the error in the coincidence rate is given by its square root: $\Delta C(\alpha, \beta) = \sqrt{C(\alpha, \beta)}$. After Gaussian error propagation, the error for the expectation values can be calculated from

$$\triangle E(\alpha, \beta) = \sqrt{\left[\frac{2 \cdot C(\alpha, \beta)_{\parallel}}{(C(\alpha, \beta)_{total})^2} \cdot \triangle C(\alpha, \beta)_{\perp}\right]^2 + \left[\frac{2 \cdot C(\alpha, \beta)_{\perp}}{(C(\alpha, \beta)_{total})^2} \cdot \triangle C(\alpha, \beta)_{\parallel}\right]^2}, \quad (6.34)$$

with

$$\begin{aligned} C(\alpha, \beta)_{\parallel} &= C(\alpha, \beta) + C(\alpha^{\perp}, \beta^{\perp}) \\ C(\alpha, \beta)_{\perp} &= C(\alpha, \beta^{\perp}) + C(\alpha^{\perp}, \beta) \\ C(\alpha, \beta)_{total} &= C(\alpha, \beta)_{\parallel} + C(\alpha, \beta)_{\perp}. \end{aligned} \quad (6.35)$$

Subsequently, the error for the S value is given by

$$\triangle S(\alpha_1, \alpha_2, \beta_1, \beta_2) = \sqrt{\triangle E(\alpha_1, \beta_1)^2 + \triangle E(\alpha_1, \beta_2)^2 + \triangle E(\alpha_2, \beta_1)^2 + \triangle E(\alpha_2, \beta_2)^2}. \quad (6.36)$$

Visibility reduction

In our experiment, there were several factors which reduced the measured Bell parameter below the ideal value of $2\sqrt{2}$, including imperfections in the source, polarization analysis and quantum channels. These could be characterized individually by the measured visibilities, which are summarized below:

- $V_{Source} = 99\%$ (98%) was the locally measured visibility of the generated entangled state in the $|H, V\rangle$ ($|D, A\rangle$) basis (accidental counts subtracted).
- $V_{Alice} = 97\%$ was the typical value for the combined visibility of Alice's analyzer module and the 6 km fiber channel, measured before each measurement run.
- $V_{Bob} = 99\%$ was the typical value for the combined visibility of Bob's analyzer module together with the 144 km free-space channel.

- $V_{SNR} = 91\%$ was the limited visibility due to an inherently low signal-to-noise ratio (SNR). This includes both dark counts and multipair emissions at the source for the finally used coincidence window of 1.5 ns and with the actual two-photon attenuation of 55 dB.

The product of these visibilities represents the two-photon visibility of the total setup $V_{setup} = 86\%$, from which one can calculate the expected Bell parameter via $S_{expected} = V_{setup} \cdot S^{qm}_{max} = 2.43$. This is already close to the measured value of $S_{exp} = 2.37$. The small discrepancy could be ascribed to variable polarization drift in Alice's 6 km delay fiber during a measurement run. After optimizing the fiber channel before each measurement, its visibility was observed to fall from initially 97% as low as 87-90% during a measurement run, limiting the useful measurement time in general to 600 s before realignment was required. This was confirmed by the results of a tomographic measurement described below.

6.5.2. State tomography

We also used the same experimental design to perform state tomography and directly measure the entangled state (see Section 4.6). Unlike a Bell test, this tomographic analysis requires no prior knowledge of the polarization orientation of the two-photon state, and therefore does not rely on how well Alice and Bob can establish a shared reference frame. The data for the tomography were acquired in four consecutive 600 s measurements. Note that for the tomographic measurements it was required to remove the HWP from Alice's analyzer.

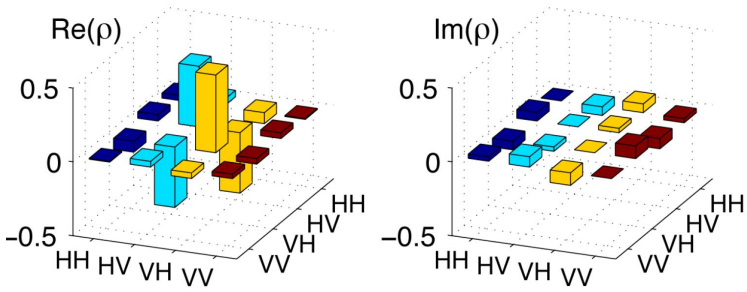

Figure 6.34.: Reconstructed density matrix ρ for Alice's and Bob's nonlocal two-photon state, confirming the entanglement of the widely separated photons. The non-zero imaginary components are mainly due to polarization rotations resulting from imperfections in the alignment of Alice's and Bob's shared reference frame.

The first measurement was performed with both analyzer modules randomly switching between the $|H, V\rangle$ and $|D, A\rangle$ analyzing bases. For the second measurement a quarter wave plate at 45° was placed in front of Alice's analyzer, such that the photons were

analyzed in either the $|R, L\rangle$ or the $|L, R\rangle$ basis, while Bob still analyzed in $|H, V\rangle$ or $|D, A\rangle$. For the third measurement a quarter wave plate at 45° was placed in front of Bob's analyzer as well, such that both analyzers switched between the $|R, L\rangle$ or the $|L, R\rangle$ bases. Finally, the fourth measurement required to remove the quarter wave plate at Alice, but leave it in Bob's analyzer. From these four measurements, we were able to obtain the 16 coincidence rates required for the reconstruction of the density matrix[22]

The measured quantum state demonstrates the entanglement of the widely separated photons, characterized by the measured tangle [46, 44] $\mathcal{T} = 0.68 \pm 0.04$. The optimal fidelity with a maximally entangled state was $\mathfrak{F}_{opt} = 0.91 \pm 0.01$. The reconstructed density matrix (shown in Figure 6.34) predicts a Bell parameter of $S_{tomo} = 2.41 \pm 0.06$, which is in reasonable agreement with the direct Bell measurement. However, we did also calculate the optimal Bell violation that could have been achieved with a perfectly aligned reference frame: $S_{opt} = 2.54 \pm 0.06$. This is close to the Bell value $S_{SNR} = V_{SNR} \cdot 2\sqrt{2} = 2.57$, which is limited only by the SNR, indicating that the polarization errors arose mainly from the difficulties of aligning the shared reference frame rather than from polarization decoherence.

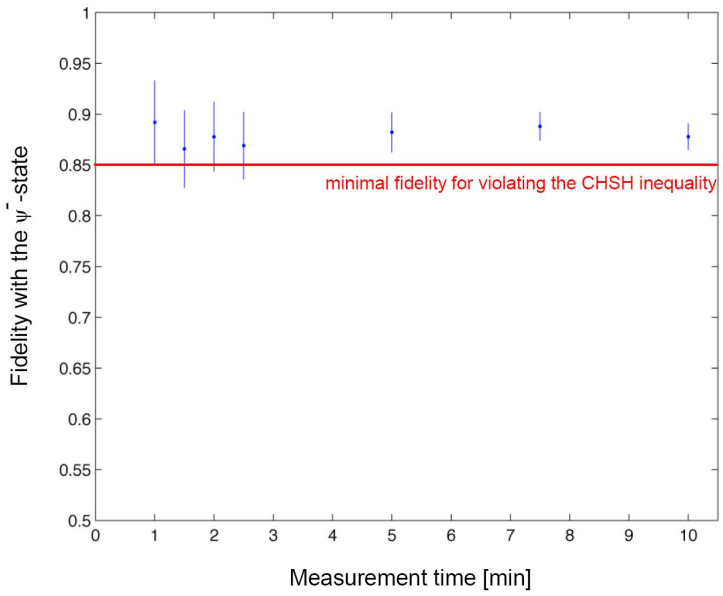

Figure 6.35.: The temporal evolution of the fidelity of the reconstructed state with the desired $|\psi^-\rangle$ state (6.9). The data was analyzed in intervals of 30 s. The red line indicates the minimal fidelity for violating the CHSH inequality.

As discussed in Section 6.2.10, we analyzed our data in blocks of 30 s in order to compensate for the relative drift between Alice's and Bob's time bases. This discrete

[22] Actually, we obtained 32 relevant combinations and thus could perform over-complete state tomography. The additional combinations could be used to improve the statistics of our measurements.

analysis enabled us to characterize the temporal evolution of our tomography results. In Figure 6.35 the fidelity of the reconstructed density matrix with the desired state (6.9) is depicted as a function of accumulation time. One can see that already after 1 minute measurement time the fidelity settled down at approximately 87%, above the limit for violating the CHSH inequality[23]. With increasing accumulation time the number of detected coincidences increased, improving the statistics and decreasing the error, as confirmed by our result.

6.5.3. Different space-time scenarios

We wanted to have a fair comparison between our Bell value obtained under locality and freedom-of-choice conditions and Bell values obtained within scenarios, where these conditions were not guaranteed. For that reason we additionally performed Bell tests with the same experimental setup described above, but within different space-time configurations. The different scenarios are described below:

1. The choices **a** and **b** were made in the past light cone of the emission **E**. This situation was achieved by setting the electronic delays for both Alice's and Bob's random signals to 1.2 ms (compared to 24.6 μs for closing the loopholes). Hence, the random choices were neither space-like separated from the hidden variables emitted by the source nor from the measurement event on the other side and the locality and the freedom-of-choice loopholes were not closed. This situation is true for any experiment, where the measurement settings are not actively and randomly switched.

2. The settings were varied periodically at a rate of 1 MHz, and were thus predictable at any time. This situation is similar to the one in the experiment by Aspect *et al.* [30] and non of the loopholes were closed.

3. The choice events **a** and **b** were made in the future light cone of **E**. This was achieved by removing the electronic delays of Alice's and Bob's random signals and inserting an optical fiber with a length of 1 km before the transmitter telescope of Bob's photon. This was necessary to ensure that Bob's setting choice was made in the future light cone of the source, since the time for establishing a random number was given by approximately 100 ns (see Section 6.2.2). In this situation, the choices could have been influenced by the hidden variables and the freedom-of-choice loophole was not closed. A similar scenario was achieved in the experiment of Weihs *et al.* [36] (see Section 5.5).

The obtained Bell parameters for the scenarios 1.-3. are listed in Table 6.4. The lower quality of these measurements compared to the main result of this work was mainly due to an apparently less efficient free-space link, as we inferred from less data in our time tagging files. Especially for scenario 3., the utilization of an extra optical fiber before the

[23] The minimal visibility of the whole experimental setup must be $V_{min} = \frac{2}{2\cdot\sqrt{2}} = 0.707$ to violate the CHSH inequality. From the visibility, the minimal fidelity can ba calculated by $\mathfrak{F}_{min} = \frac{1+V_{min}}{2} = 0.85$

	settings $\hat{a}$ and $\hat{b}$ ...	obtained Bell value S_{exp}
1.	...were chosen in the past light cone of the emission	2.28 ± 0.04
2.	...were varied periodically	2.23 ± 0.05
3.	... were chosen in the future light cone of the emission	2.23 ± 0.09

Table 6.4.: The results of our Bell test, using the same setup as for the Bell test under locality and freedom-of-choice conditions but within different space-time scenarios, where these conditions were not fulfilled.

free-space link caused an additional loss of 3 dB, reducing the signal to noise ratio. This explains the weak Bell violation of only 2.5 standard deviations.

These results indicate that the temporal ordering of the various events in a Bell experiment has no influence on whether or not the Bell inequality is violated and thus confirm my deep belief that hidden variables do not exist in "reality".

6.6. Conclusion and Outlook

This work presents results from a Bell experiment, exploiting a 144 km free-space link between two Canary islands. In addition to the commonly accepted locality and fair-sampling loopholes, we have addressed another crucial loophole, the freedom-of-choice loophole. This loophole arises if the emission of the photon pairs and the choice of the settings at Alice's and Bob's analyzers are not space-like separated events. Because then, the setting choices could in principle be influenced by the hidden variables via some hypothetical, unknown mechanism and can no longer be considered as "free or random", as required in the derivation of Bell's theorem. One may argue that this loophole is very unlikely and "unrealistic" and is not as crucial as the locality and the fair-sampling loopholes. However, the unlikelihood seems to be a common property of loopholes and within such fundamental questions as hidden variables, any hypothetical influences must be considered. There exists no more or less important loophole, it is either there or not[24].

We violated Bell's inequality by more than 16 standard deviations within an experimental configuration, where the locality and the freedom-of-choice conditions were guaranteed simultaneously. It is the first experiment to close the freedom-of-choice loophole and it is also the first to close more than one loophole in a single experiment. Hence, our results represent the most conclusive falsification of local realism to date. This significantly reduces the set of possible local hidden variable theories. The only models not excluded by our experiment are those based on the fair-sampling loophole and those where the setting choices and the hidden variables in the particle source are ("superdeterministically" [38, 22]) interdependent because of their common past - but the exclusion of the latter appears to be beyond the scope of physics.

There are several possible improvements for future Bell experiments. The most obvious next step is to perform a completely loophole-free Bell test [22, 23, 24, 25, 26]. Even

[24] As the wife, Ruth, of my college Rupert Ursin accurately compared: "A woman can not be a bit pregnant."

though all loopholes have already been closed individually, the best one could do is to close all loopholes simultaneously in a single experiment. Such an experiment would have to qualitatively repeat the achievements of our experiment and to additionally close the fair sampling loophole by ensuring that, in the limit of no background noise, at least 44.5% of all generated particle pairs are detected (see Section 5.4.4) [26]. The detection efficiencies in experiments using photons is usually limited by the low efficiency of the single-photon detectors (typically 10-40%). However, recent developments in the field of superconducting single-photon detectors may resolve the problem of low detection efficiency and open up the way to a loophole-free Bell test. So-called transition-edge sensors (TES) are microcalorimeters (e.g. with tungsten as the absorbing device material) that have photon-number resolving with negligible dark counts. At the superconducting critical temperature these sensors exhibit a steep change in resistance versus temperature, resulting in a very sensitive measure of temperature and enabling precise measurements of the energy of single photons. By including multilayer device structures that enhance the absorbtion of light into the active device material, recently detection efficiencies of 95% have been reported [98] for photons with a wavelength of 1556 nm. Additionally, the photon number resolving capability of TES detectors denotes another big advantage, because it enables one to reduce the noise from multipair emission in a Bell experiment, relaxing the efficiency requirements for a loophole free Bell test [26].

In an ultimate Bell experiment, however, the quantum random number generators should be "replaced" with human observers, who freely and independently decide about their measurement settings. Any influence on the choices would then be moved to the level of consciousness and the superdeterminism argument would completely be led *ad absurdum* (unless human beings are also predetermined). A violation of the Bell inequality would imply, for a deterministic view, that even our free will is conspiratorially correlated with the properties of the measured system. In order to guarantee the required space-like separations in an ultimate Bell test, spatial separations between the observers in the order of light seconds are required, which is not possible with earth based quantum channels. However, it might once be possible using inter-satellite links [7].

7. Quantum cryptography

Quantum cryptography, or *quantum key distribution* (QKD), is a growing branch and the most mature technical application in the field of quantum information and quantum communication. It is a method for distributing secure quantum keys, which can be used to encode messages between two communicating parties. In contrast to classical cryptography, using it's quantum mechanical counterpart enables establishing completely secure keys between two parties, usually called Alice and Bob, and noticing if an eavesdropper is trying to "listen". The underlying fundamental physical principles are the superposition principle for qubits (see Equation (4.1)) and the no-cloning theorem (see Section 4.6), which prohibits to gain information about a quantum state without disturbing it. Thus, any attempt of a potential eavesdropper, Eve, to obtain parts of the secret key will introduce errors in the QKD protocol which will be detected by Alice and Bob. If the secret key is used in a one-time-pad protocol, the entire communication becomes absolutely secure.

A one-time-pad protocol requires that the key is absolutely random, that the secret key must have the same length as the transmitted message and that any bit of the key is used only once [99]. The requirement of absolute randomness cannot be achieved with classical systems. Contrary, it is a fundamental property of quantum mechanical states. However, the perfect security of quantum cryptographic keys generated with one-time-pad protocols comes at the cost of a large consumption of key material, since the key must be as long as the message and can only be used once.

Current QKD architectures [100, 101, 102] can be broadly categorized into systems based either on weak coherent laser pulses (WCP) [103, 104, 105, 19], on entanglement [13, 14, 106, 21] or on continuous variables [107, 108, 109, 110]. The latter will not be considered in this thesis. In the following sections, I will first describe the rather simple principle of the original BB84 protocol [12] and its implementation using weak coherent laser pulses. Subsequently, I will describe the BBM92 variant [14] of the BB84 protocol using entangled photons, which is the scheme that was implemented in the experiments described in Chapter 8.

7.1. Coherent state BB84 protocol

7.1.1. Coherent photon states

Ideally, QKD systems use single photons as qubits to generate a secret key, because this reduces the power of a possible eavesdropper. In practice, real single photon sources are barely available and rather impractical for QKD, thus weak coherent laser pulses are often used as signals. The number of photons contained in one laser pulse follows a Poissonian

distribution with the probability of having n photons in one signal pulse given by

$$p_\mu(n) = \frac{\mu^n}{n!} e^{-\mu}. \tag{7.1}$$

Here μ is the mean photon number per pulse which can be set via the intensity of the laser. Due to the Poissonian statistics there is a non-zero probability of having more than one photon per pulse allowing several powerful eavesdropping attacks. In order to keep the probability for a multi-photon pulse small, μ is usually chosen to be smaller than 1.

7.1.2. Protocol

The BB84 protocol was developed by Bennett and Brassard in 1984 [12] and it requires four different qubit states that form two complementary bases. These states are usually realized with four linear polarization states of a photon, e.g. $|H\rangle$, $|V\rangle$, $|D\rangle$ and $|A\rangle$, with

$$\langle H|D\rangle = \langle V|D\rangle = \langle H|A\rangle = \langle V|A\rangle = \frac{1}{\sqrt{2}} \tag{7.2}$$

$$\langle H|V\rangle = \langle D|A\rangle = 0 \tag{7.3}$$

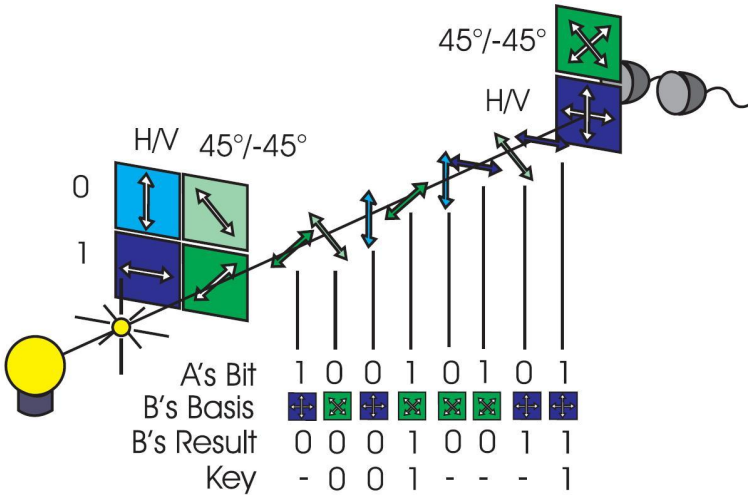

Figure 7.1.: An illustration of the coherent state BB84 protocol. Alice sends polarized single photons, prepared randomly in either of two complementary bases. Bob measures them, again randomly in one of the two bases. After public bases announcement they obtain the sifted key from their data.

As illustrated in Figure 7.1, Alice sends single photons to Bob which were prepared randomly in either of the four polarization states, and records the state of any sent photon. Bob receives and analyzes them with a two channel analyzer, again randomly, in one of the two complementary bases, $|H, V\rangle$ or $|D, A\rangle$. He records his measurement results

together with the basis the corresponding photon was analyzed in. After enough photons have been transmitted Bob communicates publicly with Alice and tells her which photons actually arrived and the corresponding analyzing bases. In return, Alice tells Bob when she has used the same bases to prepare them, because only in these cases Bob obtains the correct result. Assigning the binary values "0" and "1" to the states $|H\rangle/|D\rangle$ and $|V\rangle/|A\rangle$, respectively, leaves Alice and Bob with an identical set of "0"s and "1"s. This set is called the *sifted key*.

7.1.3. Security

What happens if Eve tries to gain information about the key generated between Alice and Bob? The simplest strategy Eve can pursue is to intercept the communication, measure the photons with a two-channel analyzer in one of the two complementary bases and to re-send the photons in the observed state to Bob (*intercept re-send strategy*). Since Eve does not know the bases of the photons, she introduces an error of 25 % in the sifted key due to the no-cloning theorem and Equation (7.2). If Alice and Bob detect an error of 25 % or larger by comparing a subset of the sifted key, they discard the whole key. In practical systems, however, there will always be some inherent noise due to dark counts in the detectors and transmission errors. As it cannot be distinguished whether the errors in the sifted key come from noise in the quantum channel or from eavesdropping activity, they all must be attributed to an eavesdropping attack.

For extracting the final *secure key* from the defective sifted key, classical procedures have to be applied. First, the errors in the sifted key need to be corrected, which is done by classical *error correction* codes (e.g. CASCADE [111] or LPDC [112, 113]). Therefore it is necessary to exchange additional information over the classical (public) channel. To further erase the information a potential eavesdropper might gain during the error correction process, Alice and Bob compress in a second step their corrected strings (e.g. using a hash function). This procedure is called *privacy amplification* [114] and results in a shorter key, the secure key, which is unknown to an eavesdropper. The actual quantum bit error ratio (QBER) in the experimentally obtained sifted key determines the amount of bits that must be discarded during classical error correction and privacy amplification. Consequently, there exists a maximally allowed QBER in order to be able to extract a secure key.

The *lower bound* for the maximal QBER is derived in the Shor and Preskill security proof by considering arbitrary eavesdropping attacks possible within the laws of quantum mechanics. It is shown [115] that the BB84 protocol can be secure with a secure key rate of at least $1 - 2H_2(q)$, where q is the QBER in the sifted key. With the binary Shannon entropy

$$H_2(x) = -x \log_2(x) - (1 - x) \log_2(1 - x), \tag{7.4}$$

the secure key rate reaches 0 if $q \approx 11\%$.

The *upper bound* can be derived by considering only simple individual attacks [116] (e.g. intercept re-send strategy). In the work from Fuchs *et al.* [117] it is shown that the mutual information between Bob and Eve must not be greater than the mutual information

between Alice and Bob, in order to extract a secure key:

$$I_{EB} \leq I_{AB}. \tag{7.5}$$

Thus, the upper bound of the QBER for a potentially safe quantum channel in a BB84 scheme can be calculated by setting $I_{AB} = I_{EB}$ resulting in $q \approx 14.6\%$ [117].

I want to remark that the theoretical bit error limits are only true for ideal algorithms and an infinite number of bits transmitted. In practice one has to consider statistical fluctuations resulting from a finite set of bits which will lower the acceptable QBER.

The PNS attack and the decoy-state QKD protocol

As an example of a very powerful eavesdropping attack I would like to describe the photon number splitting (PNS) attack [118, 119, 116]. Eve measures the number of photons Alice sends to Bob without disturbing the polarization degree of freedom using a *quantum non-demolition measurement* and blocks all single photon pulses. Whenever a signal pulse contains more than one photon, Eve deterministically splits one photon off and forwards the remaining to Bob. Eve keeps all the split photons until Alice and Bob communicate their bases and then performs the correct measurement on all photons (coherent attack). Given the probability that Bob receives a non-empty signal pulse p_{transm} (which depends on the channel transmission η) and the probability for a multi-photon signal pulse p_{multi}, the fraction of the sifted key known to Eve is [119]

$$f_{PNS} = \frac{p_{multi}}{p_{transm}} = \frac{1 - (1+\mu)e^{-\mu}}{1 - e^{-\eta\mu}} \tag{7.6}$$

Consequently, there exists a critical channel transmission below which no secure key can be obtained because f_{PNS} becomes 1 which depends on the mean photon number:

$$\eta_{PNS}^{crit} = 1 - \frac{1}{\mu}\ln(1+\mu). \tag{7.7}$$

For an optimized mean photon number the critical channel loss for the BB84 protocol is ≈ 20 dB.

An effective method to counteract the PNS attack is to use *decoy states*[103, 120, 121]. These are states of various mean photon numbers which are added randomly to the signal pulses. An eavesdropper cannot distinguish between signal and decoy pulses and thus cannot act differently on them. Since the signal states and the decoy states exhibit different photon number statistics (see Equation (7.1)), any photon-number dependent eavesdropping strategy (i.e., the PNS attack) has different effects on the signal states and on the decoy states. Alice and Bob can now separately compute the transmission probability of signal and decoy states and detect, with high probability, any photon-number dependent attack. It can be shown that for the decoy state protocol the critical channel transmission is ≈ 35 dB [19].

7.2. Entanglement based BB84 protocol

7.2.1. Entangled photon states

In contrast to the coherent state schemes, entanglement based QKD uses entangled photon pairs to establish the secure key. These pairs are usually produced via spontaneous parametric down-conversion in a non-linear crystal. The state emitted from a type-II SPDC source can be written as [5]

$$|\Psi\rangle = \cosh^{-2}\chi \sum_{n=0}^{\infty} \sqrt{n+1}\tanh^{n}\chi|\Phi_n\rangle, \tag{7.8}$$

where $|\Phi_n\rangle$ is the state of n photon-pairs, given by

$$|\Phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)^m |n-m,m\rangle_A |m,n-m\rangle_B \tag{7.9}$$

and χ is some interaction constant depending on the nonlinearity of the crystal and the intensity of the pump laser. Defining the polarization states $|H\rangle = |1,0\rangle$ and $|V\rangle = |0,1\rangle$, Equation (7.9) gives for $n = 1$ the basis independent entangled state

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B\right) = \frac{1}{\sqrt{2}} \left(|D\rangle_A |A\rangle_B - |A\rangle_A |D\rangle_B\right). \tag{7.10}$$

From Equation (7.8) it follows that the emission probability for n photon-pairs per pump pulse is given by

$$p_\kappa(n) = \frac{(n+1)\kappa^n}{(1+\kappa)^{n+2}}, \tag{7.11}$$

with $\kappa = \sinh^2\chi$. For continuous wave pumped sources this is the probability for emitting n photon-pairs within the coincidence time window. Consequently, the mean photon-pair number per pump pulse (coincidence time window) μ is given by $\mu = 2\kappa$.

7.2.2. Protocol

Alice and Bob share, in first approximation (neglecting higher order emissions), the entangled state (7.10) emitted by some SPDC source [122]. Using a two channel analyzer, each measures the incoming photons randomly (e.g. using a 50/50 beam splitter or an active switch) in either the $|H,V\rangle$ or the $|D,A\rangle$ basis and records the results and the measurement bases. Afterwards, they publicly communicate which photons they actually detected and the corresponding measurement bases and discard those results in which they accidentally disagreed with the basis. Since the shared entangled state is anti-symmetric in polarization, Alice's and Bob's results are perfectly anti-correlated. Then, they assign the binary values "0" and "1" to the results $|H\rangle/|D\rangle$ and $|V\rangle/|A\rangle$, respectively and after one of them inverts the bits, they obtain an identical set of "0"s and "1"s - the sifted key.

7.2.3. Security

As in the coherent state BB84 scheme 7.1.3, the security of the key will be proven by comparing a subset of the sifted key. Depending on the QBER in the sifted key, a secure key can be extracted with the help of classical error correction codes and privacy amplifications.

In the work from Ma, Fung and Lo [5] it is shown that, applying Koashi and Preskill's security proof [123], secure key generation with entanglement based systems is possible at a rate of at least $\frac{1}{2}\{Q_\kappa[1 - f(q)H_2(q) - H_2(q)]\}$. Here, $f(x)$ is the error correction efficiency, $H_2(x)$ is the Shannon entropy (see Equation (7.4)) and q is the QBER. The probability Q_κ that Alice and Bob detect a photon pair per pump pulse depends on the attenuation in the quantum channels, the dark count rate in the detectors and on the SPDC source specific constant κ. For the SPDC source put exactly in the middle of Alice and Bob (*source-in-the-middle scheme*) and inserting experimental data obtained in the work from Ursin *et al.* (see Section 5.5), it can be calculated that entanglement based QKD can tolerate up to 70 dB total attenuation in the quantum channels (compared to 35 dB for coherent state decoy schemes).

8. Advantages of entanglement based QKD

A most important benchmark for a QKD system is the secure key rate that can be achieved for a given quantum channel attenuation. As discussed in Chapter 7 the distance/attenuation over which a secure key can still be generated is limited for any QKD system due to absorptive losses in the communication channels and detector imperfections. The experimental method which presently offers the best performance in high loss regimes are, with respect to the channel attenuations symmetric entanglement-based systems as recently emphasized theoretically in [5]. There it was specifically shown that the maximal tolerable two-photon attenuation for a pulsed entanglement-based QKD system [20] with the source placed in the middle between the receivers is up to 70 dB (in the case of optimized mean photon number in the limit of an infinite number of key bits). In terms of distance, this is approximately a factor of two more than can be achieved with typical WCP systems, which can tolerate a loss of maximally 35 dB [5, 19].

One solution for extending the communication distance in a QKD network beyond these limits are multi-node networks with key relay centers [124]. In the first stage, where centers will have to be trusted and be connected with point-to-point QKD systems, entanglement could potentially reduce the required number of trusted nodes because it is the only system which allows three-party communication with an untrusted source [125]. In consequence, entanglement-based systems could considerably lower the complexity and cost requirements for a quantum communication network. Ideally, the network nodes could eventually be replaced by quantum repeaters [126], but even though the first working quantum repeater node has recently been demonstrated [127, 128], they still need significant development.

The quantum channels in a future global quantum communication network will mostly consist of optical fibers which are already widely installed. As an alternative, free-space connections will allow to quickly build up connections between parties with direct line-of-sight. Additionally, orbital free-space links, e.g. satellite-to-ground links or inter-satellite links, will allow the efficient global interconnection of regional quantum networks [129, 130]. The attenuation expected for a single link ground connection from a satellite is at least 30 dB, and its feasibility has been shown in first ground-based tests [19, 20]. In the more demanding two-link satellite scenario, QKD systems will have to cope with 60 dB attenuation.

Within the experiments presented in this work, the performance of entanglement-based QKD (see Section 7.2) was tested in an attenuation range from 35 dB to 71 dB. It was the aim to experimentally investigate the theoretically predicted [5] advantage of the symmetric scenario over commonly used asymmetric systems and to compare our results

with the theoretical model investigated in [5].

Two of these experiments were performed within the measurement campaign for the Bell test presented in Chapter 6. Thus, we implemented the same 144 km free-space link between the two Canary Islands, La Palma and Tenerife, and used the same experimental equipment as described in Section 6.2. Note that for performing QKD experiments the half wave plate in Alice's analyzer module (see Section 6.2.3) was removed, such that both analyzers switched randomly between the $|H, V\rangle$-basis and the $|D, A\rangle$-basis. We studied two different setup configurations that operated at two-photon attenuations of 35 dB and 58 dB. Therefore, the entangled photon source was placed either at Alice's location (*source at Alice*) or *asymmetrically in between Alice and Bob*. These two scenarios could be realized by either removing or inserting the 6 km fiber channel (see Section 6.2.6) for Alice's photon.

Additionally, we analyzed the data obtained in a previous Bell experiment [131], where both photons were sent through the 144 km free-space link (i.e., the two-photon attenuation was 71 dB) and put it in the context of our investigation as the *source in the middle* scheme.

8.0.4. Theoretical error model

In practical QKD setups, most errors will actually originate from experimental imperfections, e.g. non-perfect entanglement and higher order photon emissions at the source, noisy quantum channels, imperfect polarization analyzers and photon detectors. A direct estimate of the expected QBER in a quantum optics QKD experiment can be obtained by measuring the total quantum correlation visibility V_{tot}, which has a simple relation to q:

$$q = \frac{1 - V_{tot}}{2} \tag{8.1}$$

and can be obtained from the maxima, N_{max}, and minima, N_{min}, of the observed coincidences:

$$V_{tot} = \frac{N_{max} - N_{min}}{N_{max} + N_{min}}. \tag{8.2}$$

Given that all these parameters are experimentally accessible, one can model the performance of a QKD system. First, a finite coincidence time window τ_c, limited by the timing resolution of the detection apparatus, results in a certain probability to accidentally detect two uncorrelated photons in coincidence, which do not belong to the same pair. Second, the statistical nature of the down-conversion process inherently generates multi-photon emissions within the coherence time of the photons. This also results in uncorrelated detection events at Alice and Bob. Furthermore, the finite coincidence time window leads to uncorrelated accidental coincidences from background light and intrinsic detector dark counts. In addition, imperfections and misalignment in the setup (source, polarization analysis, etc.) introduce systematic errors. In the following, the errors from uncorrelated detection events are characterized by the accidentals visibility V_{acc} and the systematic errors by the system visibility V_{sys}. The total correlation visibility is given by $V_{tot} = V_{sys} \cdot V_{acc}$.

The effect of these error sources on the secure key rate are analyzed analytically within a model devised by X.-F. Ma *et al.* [5], which assumes pulsed operation of the SPDC source. The input parameters for the model are the photon-pair generation rate at the source, the ratio between the coincidence and single rates at Alice and Bob, including detector efficiencies and the system visibility V_{sys}. The model yields an error probability and a secure key gain per pump pulse as a function of total two-photon attenuation in a QKD experiment. As already discussed in Section 7.2.3, a lower bound for the final secure bit rate per pulse R is then calculated using Koashi and Preskill's security analysis [123] via

$$R \geq \frac{1}{2}\{Q_\kappa[1 - f(q)H_2(E) - H_2(q)]\}. \tag{8.3}$$

Here, Q_κ is the coincidence detection probability between Alice and Bob per pump pulse, $\frac{1}{2}$ is the basis reconciliation factor and H_2 is the binary entropy function (7.4). The correction factor $f(q)$ accounts for the fact that practical error correction protocols in general do not perform ideally at the Shannon limit. Instead of assuming $f(q) \approx 1$, we used realistic values for the bidirectional error correction protocol Cascade [111]. Furthermore, for our case of a cw-type[1] SPDC source, the model was adapted to yield a probability per coincidence time window instead of a probability per pump pulse.

Note that Equation (8.3) gives the final secure key rate in the limit of infinite key lengths. However, in a practical implementation the secure key is obtained via error correction and privacy amplification on a finite key, which might compromise the security (see [5, 102] for more details). For simplicity, we will restrict the analysis of our experiments to the infinite bounds.

8.1. The experiments

As mentioned above, we implemented three different experimental QKD scenarios (see Figure 8.1), but only the first and the second were actually performed within this thesis. In all three experiments, one photon of an entangled pair was sent to Bob via a 144 km free-space link, established between the islands of La Palma and Tenerife. The first and the second experiment were both asymmetrical with respect to the different channel losses for Alice and Bob. In the first experiment the SPDC source was placed at Alice (*source at Alice*) and one photon of an entangled pair was measured directly at the source. In the second experiment (*source asymmetric in between Alice and Bob*), Alice's photon was sent through a 6 km single-mode fiber before it was analyzed. In the third scenario both photons were sent via the 144 km free-space link to a common receiver where they were split up and analyzed separately. This can be seen as an effective realization of the *source in the middle* scheme, since we have equal channel losses for Alice's and Bob's photons.

To get an overview about the different scenarios and the corresponding results, please refer to Table 8.1. A detailed discussion will be given in the next sections.

[1] cw stands for continuous wave

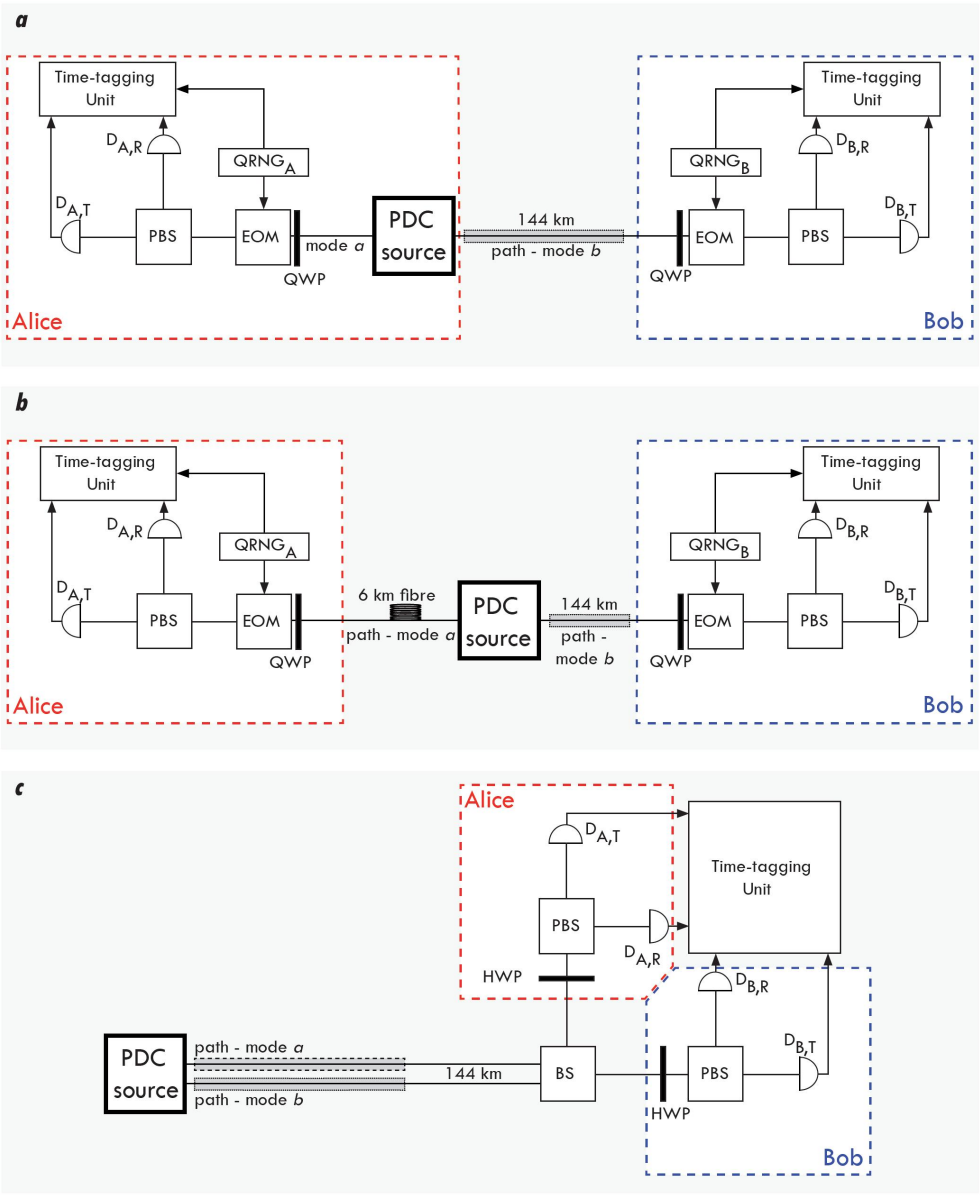

Figure 8.1.: An illustration of the three setups used for the entanglement-based quantum key distribution experiments. The entangled photon source (PDC source) generates entangled photon pairs that were sent via optical fibers and free-space optical links to Alice and Bob, respectively. There they were analyzed and detected, using four avalanche photo detectors $D_{A,T}$, $D_{A,R}$,$D_{B,T}$ and $D_{B,T}$. ***a)*** Alice's photon was analyzed directly at the source after 1 meter of optical fiber and Bob's photon was sent through a 144 km free-space channel. The total two-photon attenuation was 35 dB. ***b)*** Alice's photon is now sent through a 6 km fiber, resulting in a total two-photon loss of 58 dB. In the scenarios ***a)*** and ***b)*** each analyzer module consisted of a polarizing beam splitter cube (PBS), a quarter wave plate (QWP) and an electro optical modulator (EOM) to switch between the complementary bases. The EOMs were triggered by independent quantum random number generators. ***c)*** Both photons were sent through the 144 km free-space channel to one common receiver. There they were split up with a 50/50 beam splitter (BS) and guided to Alice and Bob, who could adjust their analyzing bases, using a HWP and a PBS.

Scenario source...	**Attn.** [dB]	**local pair rate** [MHz]	$\mathbf{V_{tot}}$ [%]	**QBER** [%]	**secure key rate** [bits/s]
... at Alice (Figure 8.1a)	35	0.55	86.2	6.9	24
... asymmetric in between (Figure 8.1b)	58	2.5	86.2	6.8	0.6
... in the middle (Figure 8.1c)	71	1	92	4	0.02

Table 8.1.: A summary of the parameters for the three different experimental scenarios and the corresponding results, i.e., the total two-photon attenuation, the locally detected coincidence rate, the total visibility V_{tot}, the quantum bit error ratio QBER and the finally obtained secure key rate.

8.1.1. Source at Alice

The experimental situation is depicted in Figure 8.1a. The SPDC source [64] was located in La Palma and generated photon pairs in the entangled state (5.2). The photons in modes a and b were coupled into single-mode fibers, Alice's photon in mode a was analyzed and detected locally after only 1 meter of single-mode fiber, while the photon in mode b was sent through a 144 km free-space channel to Tenerife. There it was collected by the 1 meter diameter telescope of the optical ground station (OGS) operated by the European Space Agency ESA and analyzed by Bob.

Each polarization analyzer consisted of a quarter wave plate (QWP) an electro optical modulator (EOM), a polarizing beam splitter (PBS) and two single-photon avalanche diodes. Triggering the EOMs by independent quantum random number generators, the analyzer modules randomly switched between the complementary analyzing bases $|H, V\rangle$ and $|D, A\rangle$ as required for the BBM92 protocol [14]. At Alice and Bob, every detection event (including arrival time, detector channel and EOM setting information) was recorded onto local computer hard disks, using time-tagging units disciplined by the global positioning system (GPS) time standard. Note that using active analyzers which are triggered by a quantum random number generator represents a security advantage over passive QKD systems, because it prevents an eavesdropper from applying certain side-channel attacks (e.g. faked states attack) [5, 132].

In the first scenario implemented, the free-space channel attenuation for photons in mode b was measured to be approximately 32 dB on average (including all optical elements), while only half of the locally measured photons (3 dB) in mode a were lost in Alice's analyzer module. The total two-photon attenuation was therefore 35 dB.

The SPDC source generated entangled photon pairs at an estimated rate of 7 MHz, limited by the peak count rate of Alice's detector system. After single-mode fiber coupling, 550000 coincidences were observed locally, corresponding to a combined coupling and detection efficiency of 28%. The darkcount rate at Alice was 500 Hz while Bob's detectors showed an average of 1200 Hz. For these parameters and a coincidence window of $\tau_c =$

1.5 ns, theory predicts an upper bound of $V_{th} = 94.1\%$ for the total visibility, which includes the initially measured system visibility $V_{sys} = 96\%$ as well as the background and multi-pair emission limited visibility of $V_{acc} = 98\%$. However, the actual visibility of the transmitted entangled state was measured to be $V_{tot} = 86.2\%$ on average. The discrepancy to V_{th} was most probably caused by a polarization drift in the fiber connecting the source with the transmitter telescope during the measurements.

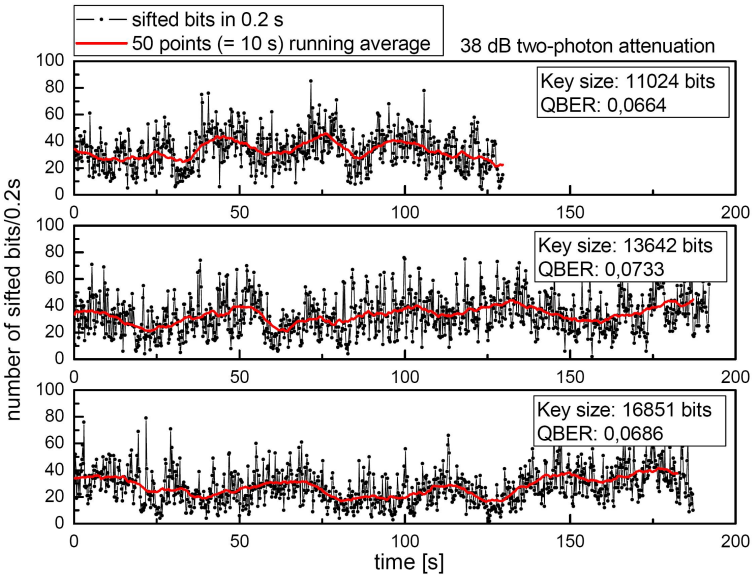

Figure 8.2.: The results of three typical QKD measurements within the source at Alice scheme with a two-photon attenuation of 35 dB. The sifted key rates in 0.2 s are plotted versus measurement time. The strong intensity fluctuations through the free-space link are reflected in the fluctuations of the key rates. Accumulating these three measurements and applying Koashi and Preskill security analysis yielded an average secure key rate of approximately 24 bit/s.

The result of a typical measurement is shown in Figure 8.2. In total, three measurements were performed and sifted keys containing 11024 bits (130 s integration time), 13642 bits (190 s integration time) and 16851 bits (190 s integration time), respectively, were obtained. During a measurement run, the free-space link usually undergoes strong atmospheric turbulence, resulting in a time dependent two-photon attenuation. This is reflected by the time-resolved sifted key rates (see Figure 8.2). The QBERs for these measurement runs of 6.6%, 7.3% and 6.9%, respectively, were obtained by comparing the sifted keys and are in good agreement with the measured overall visibility. Finally, applying Equation 8.3 yields an averaged secure key rate of approximately 24 bits/s. A comparison of the experimentally obtained data point with the theoretically calculated secure key rate as a function of overall link attenuation is shown in Figure 8.4.

8.1.2. Source asymmetric in between Alice and Bob

The second scenario extends the *source at Alice* scheme (see Section 8.1.1), such that the photon in mode a was delayed by 29.6 μs in a 6 km long single-mode fiber (see Figure 8.1b). The attenuation of the fiber was measured to be 17 dB and during this particular measurement series, the free-space link attenuation was 38 dB. Combined with the 3 dB loss in Alice's analyzer, the overall two-photon attenuation was 58 dB. For these experiments, we increased the output of the SPDC source to a pair generation rate of 32 MHz by operating at the maximum available pump laser power of 50 mW. Due to detector saturation, the fiber-coupled and locally detectable pair rate could only be extrapolated to be 2.5 MHz. In this situation, the initial system visibility was $V_{sys} = 94\%$, a slight reduction compared to the 35 dB scenario, caused by the delay fiber. With the same coincidence window ($\tau_c = 1.5$ ns) and darkcount rates (500 Hz at Alice and 1200 Hz at Bob) as in the first experiment, the theoretic upper bound for this scheme turns out to be $V_{th} = 88\%$ and the measured total visibility of the entangled state at the receiver was with $V_{tot} = 86.2\%$ coincidentally the same as in the first scenario.

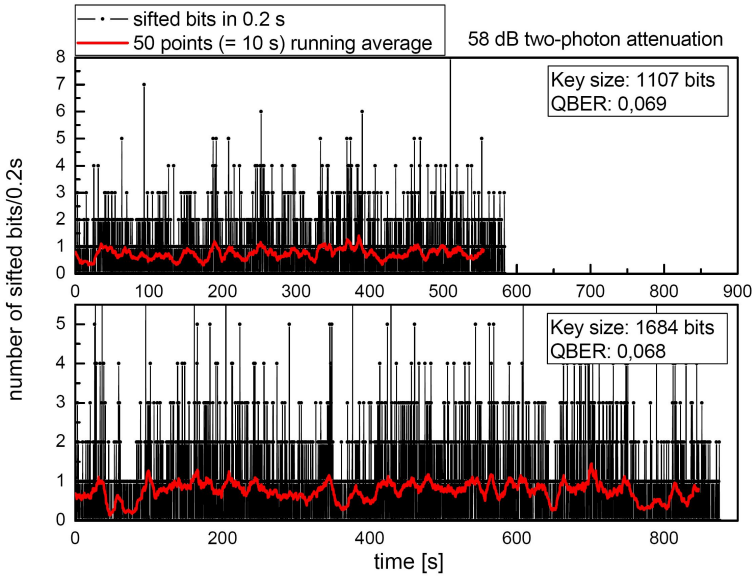

Figure 8.3.: Two typical measurements runs for the scenario shown in Figure 8.1b, where the source was arranged asymmetrically in between Alice and Bob, resulting in a two-photon attenuation of 58 dB. An averaged secure key rate of 0.6 bits/s was obtained.

A typical measurement result is depicted in Figure 8.3. In total, two sifted keys were obtained, containing 1107 bits (580 s integration time) and 1684 bits (880 s integration time). The corresponding QBER was 6.9% and 6.8%, respectively. With these QBERs a secure key rate of 0.6 bits/s could be obtained. For this scenario both the expected visibility and the key rate agree very well to the model (see Figure 8.4).

8.1.3. Source in the middle

The experimental situation for the third, the *source in the middle* scenario, is depicted in Figure 8.1c. The entangled photons in mode a and mode b were coupled into single mode fibers, guided to two separate transmitter telescopes and sent through a 144 km free-space channel to one common receiver in Tenerife. The total two-photon attenuation was measured to be about 71 dB (including all optical components). For a detailed description of the setup please refer to [66].

The source produced photon pairs at a rate of 10 MHz from which 3.3 MHz single photons and 1 MHz photon-pairs were detected locally. Both photons were sent via two telescopes over the 144 km free-space links to Tenerife. On average, 0.071 transmitted photon pairs/s could be detected, using a coincidence window of 1.25 ns. Each detector registered a background count rate of 400 Hz. Accumulating data for a total amount of 10800 seconds we measured an averaged visibility of the transmitted entangled state of $V_{tot} = 92\%$ (with $V_{sys} = 99\%$ and $V_{acc} = 94\%$), which is very close to the theoretic upper bound of $V_{th} = 91.7\%$. Based on these measurements we inferred that a QKD experiment

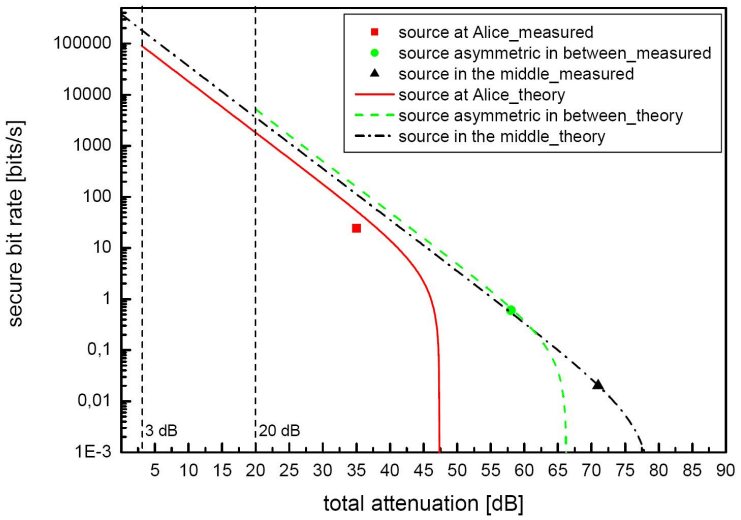

Figure 8.4.: A comparison of the obtained results with the theoretical model described in the main text. The solid curve (*source at Alice*) starts at a two-photon attenuation of 3 dB, which corresponds to the fixed loss in Alice's analyzer module. The dashed curve represents the scheme with the *source asymmetrically between Alice and Bob*, where the attenuation for Alice's fiber channel together with the analyzer module was 20 dB. The dotted-dashed curve is predicted by our model for the *source in the middle* scheme. The three experimentally obtained secure bit rates are depicted as the square, the circle and the triangle, respectively. It is easy to see that the data point for the *source in the middle* scenario (triangle) can not be explained by the models for the asymmetric cases. Similarly, the data point of the experiment with the *source asymmetrically between Alice and Bob* can not be explained by the model for the *source at Alice* scheme. Thus the advantage of the symmetric scenario is clearly verified by our experimental results.

employing a similar setup would have yielded a QBER of approximately 4%. From the coincidence rate and the QBER-dependent performance of the classical key distillation protocols, we estimate that our experiment would have yielded a final secure key rate of approximately 0.02 bits/s (see Figure 8.4). However, the implementation of a full QKD experiment was not possible, because only one receiver station and module was available in Tenerife.

8.1.4. Clock synchronization

As already discussed in Section 6.2.10, our coincidence search algorithm could be utilized to synchronize the individual time bases at Alice and Bob within 0.5 ns during the first two experiments. For the third experiment such a synchronization was not necessary, because one and the same time-tagging system was used for the measurements.

Coincidence events between Alice and Bob were identified by calculating the cross-correlation function of the individual time-tagging data sets. A peak in the cross-correlation function indicated the current time offset Δt between the time scales of the receiver units. Initially, Alice's and Bob's time bases were both disciplined by the GPS time standard. However, the two individual GPS receivers exhibited a relative drift during a measurement run. By analyzing the data in blocks of adjustable length, our software measured

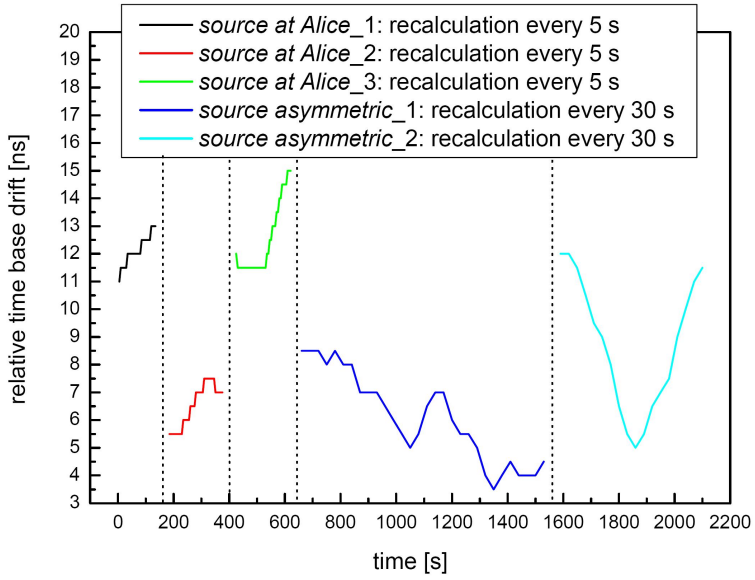

Figure 8.5.: This plot shows the relative drift between Alice's and Bob's local time-tagging systems that were directly disciplined by the global positioning system. Due to the relative drift (vertical axis of the plot), the offset for the coincidence analysis was adapted by recalculating the cross-correlation. For the three measurements within the *source at Alice* scheme the recalculation was performed in steps of 5 s (black, red and green curve), while for the two measurements within the *source asymmetric in between Alice and Bob* scenario it was performed every 30 s (blue and light blue curve).

and compensated for this relative drift with 0.5 ns resolution by temporal alignment of the data blocks. The data of the first experiment described were analyzed in blocks of 5 s length, while the data obtained in the second experiment were analyzed in blocks of 30 s length. The corresponding results concerning the relative drift of Alice's and Bob's time bases are depicted in Figure 8.5.

8.2. Conclusion and Outlook

We experimentally studied entanglement-based QKD in three different scenarios in order to verify the symmetry advantage of such an implementation. This involved placing the source directly at Alice, asymmetrically between Alice and Bob and finally symmetrically between Alice and Bob. The experiments were performed on a 144 km free-space link between the Canary Islands of La Palma and Tenerife. Our results clearly show that in the symmetric case (*source in the middle*) secure keys can still be generated in loss regimes, where the asymmetric systems fail. We also showed that our experimental results agree well with a recently devised theoretical model.

The big future goal of quantum communication is to establish a global quantum communication network. This requires earth-based networks as well as satellite-to-ground and inter-satellite links. Our experiment shows, that satellite-to-ground links can already be realized with state-of-the-art technology, since the expected link attenuation in a low earth orbit (LEO) satellite to ground scenario is 30 dB [133]. Hence, the results suggest that our entanglement based system could be used in either a single-link (*source at Alice*) or even a two-link (*source in the middle*) satellite-to-ground scenario [7]. Additionally, the obtained results proof the feasibility for implementing an existing optical ground station for quantum communication experiments with single photons.

We conclude from our experiments that entanglement based QKD systems will be the systems of choice for a quantum communication network, because entanglement based systems can bridge larger distances and/or attenuations, reducing the number of trusted nodes in a network. Contrarily, WCP systems might be used for short distances if high key rates are required.

A next step is to perform proof-of-principle experiments, actually testing entanglement based or WCP systems using satellite-to-ground links. Already in 2004, the joint mission proposal *Quantum Entanglement in Space* (SpaceQUEST [134]) was submitted to the European Space Agency (ESA) by several European quantum optics groups. The scientific goals of this mission are to demonstrate quantum key distribution on a global scale and to perform test on fundamental quantum physical concepts from space. Three possible scenarios for these proof-of-concept experiments are shown in Figure 8.6. It is suggested to place the transmitter terminal onto the International Space Station (ISS), while the receiver terminals should be installed at suitable optical ground stations. The feasibility of the accommodation of a photonic terminal on the ISS was already devised in 2003 [135] under ESA's *General Studies Programme* (GSP) [6].

In a first experiment, one single downlink might be used to generate a secure key between the satellite and a ground station (Figure 8.6a). Hence, both WCP systems and

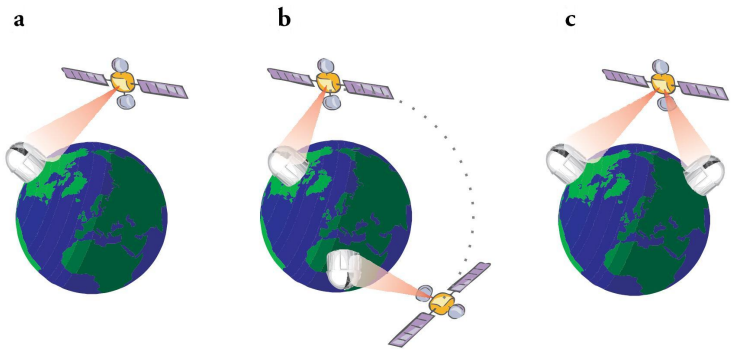

Figure 8.6.: Three potential scenarios of space based quantum communication. (a) One single downlink is used to establish a secure key between a satellite and an earth-based receiver. (b) Two individual secure keys can be established between the satellite and individual ground stations that can establish a link to the ISS. These keys can then be merged to obtain a secure key between the distant observers. (c) Entangled photon pairs are transmitted simultaneously to two separate ground stations via two downlinks. (Figure taken from [66].)

entanglement based systems can be tested within this scenario.

possible ground stations	distance between them
Tenerife ↔ Calar Alto	1638 km
Tenerife ↔ Matera	3309 km
Calar Alto ↔ Matera	1698 km
Calar Alto ↔ Sierra Nevada	76 km

Table 8.2.: Distances between possible ground stations for the two-link scenario depicted in Figure 8.6c. (Table taken from [7].)

If the satellite is trusted, single downlinks could be used to sequentially build up a secrete key between any two ground stations that can establish a communication link with the ISS (Figure 8.6b). Thereby, each of the two ground stations will independently establish a quantum key with the space-based transmitter terminal. Since the space platform has access to both keys, it can send a logical combination of the keys (e.g. logically connected by XOR) via classical communication channels publicly to either of the ground stations, where the key of the other ground station can be generated.

The probable most interesting scenario is depicted in Figure 8.6c, where entangled photons are simultaneously transmitted from the ISS to two ground stations. The link duration now depends on the distance between the stations (see Table 8.2) and on the minimum acceptable elevation angle. In this case, a secrete key can be generated directly between two ground stations without the need to trust the satellite. Additionally, within this scenario entanglement can be tested over distances as large as 3309 km, which are not accessible to ground-based quantum communication schemes.

A. Preprint

Preprint of 'Violation of local realism with freedom of choice', submitted to Nature Physics (2009). It contains a description of the main experimental result of this thesis.

Violation of local realism with freedom of choice

Thomas Scheidl, Rupert Ursin, Johannes Kofler, Sven Ramelow, Xiao-Song Ma,

Thomas Herbst, Lothar Ratschbacher, Alessandro Fedrizzi, Nathan Langford,

Thomas Jennewein & Anton Zeilinger

Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

Faculty of Physics, University of Vienna, Sciences, Boltzmanngasse 5, 1090 Vienna, Austria

The predictions of quantum mechanics can be in striking contradiction with local realism if entanglement exists between distant systems. Bell's theorem shows that local realistic theories, such as classical physics, place a strong restriction on observable correlations between different systems in experiments, giving rise to Bell's inequality[1]. This allows an experimental test of whether nature itself agrees with local realism or quantum mechanics. To derive his inequality, Bell made three assumptions: *realism* (objects possess definite properties prior to and independent of observation), *locality* (space-like separated events cannot causally influence each other), and *freedom of choice* (the choice of measurement settings is free or random). In experimental tests of Bell's inequality, there may be "loopholes" which allow observed violations to still be explained by local realistic theories. Many Bell tests have been performed which violate Bell's inequality[2-13], some which have closed individual loopholes, specifically the locality loophole[11] and the fair-sampling loophole[12]. Another crucial loophole, which has been discussed theoretically in Ref. [14] but not yet addressed experimentally, is related to Bell's freedom-of-choice assumption. Here we report an experiment using entangled photons, which for the first time closes this loophole by randomly switching measurement settings and space-like separating the setting choice from the photon pair emission. There has previously been much experimental and theoretical progress towards a complete loophole-free Bell test (e.g., Refs [14-18]). However, our experiment, which simultaneously closes the locality and the freedom-of-choice loopholes, is the first to close more than one of the three crucial loopholes at the same time. By violating Bell's inequality by more than 16 standard deviations and only relying on the fair sampling assumption, this represents the most conclusive violation of local realism to date.

Quantum entanglement, a concept which was first discussed by Einstein, Podolsky and Rosen[19] and by Schrödinger[20], is the key ingredient for violating Bell's inequality in a test of local realism. A simple experimental Bell test has the following basic characteristics. Two observers, Alice and Bob, receive (entangled) particles emitted by some source. They each choose a *measurement setting*, *a* and *b* respectively, and then

record their measurement *outcome values*, *A* and *B*. To understand more precisely the possible loopholes that can arise in such a test, we now discuss Bell's assumptions in more detail.

Realism is a world view in which measurements just reveal pre-existing properties of physical objects. Following Bell, realism implies that deterministic functions exist for Alice's and Bob's outcome values, which depend on the outcome and setting values of both observers and on a set of "hidden variables"[1], all written as the single parameter λ, i.e. $A = A(a,b,B,\lambda)$ and $B = B(b,a,A,\lambda)$. Realism is an assumption about the physical world and no experiment has yet been proposed which could directly determine its validity. Here, we do not consider stochastic hidden variable theories[21,22], because they are equivalent to deterministic theories in the context of violating Bell's inequality[23].

Locality imposes that 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."[19] Thus, the *joint* assumption of local realism implies that the outcomes only depend on the local settings and the hidden variables, i.e. $A(a,b,B,\lambda) = A(a,\lambda)$ and $B(a,b,B,\lambda) = B(b,\lambda)$. In an experiment, the *locality loophole* arises when Alice's *measurement event* can in principle be causally influenced by a physical (subluminal or luminal) signal from Bob's *measurement event* or Bob's *choice event*, and vice versa. The best available way to close this loophole is to space-like separate every measurement event on one side from both the measurement ("outcome independence"[24]) and setting choice ("setting independence"[24]) on the other side. Then, special relativity ensures that no physical signals between the events can influence the observed correlations. Experimentally, the locality loophole was first addressed by Aspect *et al.*[5], and finally closed by Weihs *et al*.[11]

In Bell's theorem it is crucial that the type of measurement performed is not influenced by the particle source or generally by the hidden variables. Following Bell, this *freedom-of-choice* hypothesis requires that "the variables *a* and *b* can be considered as *free* or *random*"[25]. If the setting choices "are truly free or random, they are not influenced by the hidden variables. Then the resultant values for *a* and *b* do not give any information about λ."[25], i.e. $a \neq a(\lambda)$ and $b \neq b(\lambda)$. If not, then this creates a loophole, one which has not been addressed by any experiment to date. Experimentally, this loophole can be closed if Alice's and Bob's setting values are chosen by a random number generator *and* if no physical signal can travel between their choice events and the particle emission event at the source (i.e., if these events are space-like separated)[14]. Without this space-like separation, the setting choices could in principle have been influenced by hidden variables created at the particle emission event, and the variables *a* and *b* would no longer be "truly free or random". The *freedom-of-choice loophole* has been closed for the first time by our experiment. It is, of course, conceivable that both the source and settings could depend on events in their shared backward light cones, so that the settings would still depend on hidden variables. In such "superdeterministic theories"[14,25], however, choices are never free. "Perhaps such a

theory could be both locally causal and in agreement with quantum mechanical predictions", as Bell suggests[25].

A third loophole, called the *fair-sampling loophole*[26], arises from inefficient particle collection and detection. It suggests that, if only a fraction of generated particles is observed, this may not be a representative subensemble, and an observed violation of Bell's inequality could still be explained by local realism. This loophole was closed by Rowe *et al*. [12]

In our experiment, we performed a Bell test between the two Canary Islands, La Palma and Tenerife, with a link altitude of 2400 m, simultaneously closing the locality and the freedom-of-choice loopholes (detailed layout in Figure 1). A simplified space-time diagram is plotted in Figure 2a. This one-dimensional scenario is in good quantitative agreement with the actual geographical situation (see Supplementary Information).

In La Palma, polarization-entangled photon pairs in the maximally entangled ψ^- singlet state were generated by spontaneous parametric down-conversion. One photon of each pair was sent through a coiled 6 km optical fibre (29.6 μs travelling time) to Alice (located next to the photon source), and the other photon was sent through a 144 km optical free-space link (479 μs travelling time) to Bob in Tenerife. The spatial separation and Alice's fibre delay ensured that the measurement events, denoted as **A** and **B**, were space-like separated from each other ("outcome independence"). To further ensure that the measurement events on one side were space-like separated from the setting choice events on the other ("setting independence"), the setting values, *a* and *b*, were determined by independent quantum random number generators (QRNGs)[27] at appropriate points in space-time (denoted as events **a** and **b**). To switch between two possible polarization measurements, these settings were implemented using fast electro-optical modulators (EOMs) (refreshed every 1 μs). These combined conditions explicitly closed the locality loophole[11].

To simultaneously close the freedom-of-choice loophole, the settings were not only chosen by random number generators and space-like separated from each other, but the corresponding choice events, **a** and **b**, were also arranged to be space-like separated from the photon-pair emission event, denoted as **E** (Fig. 2a). On Alice's side, the QRNG was placed some distance from the photon source (approximately 1.2 km in our experiment). The random setting choices were transmitted via a classical 2.4 GHz AM radio link to Alice and electronically delayed such that, for a given measurement event, the setting choice and the photon emission were always space-like separated and occurred on average simultaneously in the reference frame of the source (see Fig. 2a). On Bob's side, the same electronic delay was applied to the random setting to ensure that his choice occurred before any signal could arrive from the photon emission at the source. These combined measures ensured the space-like separation of the choice and emission events, and thus closed the freedom-of-choice loophole.

Since Alice's and Bob's measurement events were space-like separated, there exists a moving reference frame in which those events happened simultaneously. Bob's

electronic delay was chosen such that, in this frame, the setting choices also happen approximately simultaneously (Fig. 2b). The speed of this frame with respect to the source reference frame is $v_{ref} = c^2 \cdot (t_B - t_A)/(x_B - x_A) = 0.938 \cdot c$ (with the speed of light c), using the space-time coordinates of the measurement events **A** = (t_A,x_A) = (29.6 µs, 0) and **B** = (t_B,x_B) = (479 µs, 143.6 km). The relativistic gamma factor is $\gamma = 1/(1-v_{ref}^2/c^2)^{1/2}$ = 2.89, giving an effective spatial separation of Alice and Bob (La Palma and Tenerife) under Lorentz contraction of $\gamma^{-1} \cdot 143.6$ km ≈ 50 km. Note that, because space-like separation is conserved under Lorentz transformation, the locality and the freedom-of-choice loopholes were closed in all reference frames.

For our Bell test, we used the Clauser-Horne-Shimony-Holt (CHSH) form of Bell's inequality[28]:

$$S(a_1,a_2,b_1,b_2) = |E(a_1,b_1) + E(a_2,b_1) + E(a_1,b_2) - E(a_2,b_2)| \leq 2, \qquad (1)$$

where a_1,a_2 (b_1,b_2) are Alice's (Bob's) possible polarizer settings and $E(a,b)$ is the expectation value of the correlation between Alice's and Bob's local (dichotomic) polarization measurement outcomes. Quantum mechanics predicts a maximum violation of this inequality with $S^{qm}_{max}=2\sqrt{2}$ when Alice and Bob make their measurement choices between appropriate mutually unbiased bases, e.g., with polarization analyzer settings (a_1,a_2,b_1,b_2) = (0°,45°,22.5°,67.5°).

During four 600 s-long measurement runs we detected 19917 photon pair coincidences and violated the CHSH inequality, with $S^{exp} = 2.37 \pm 0.02$ (no background subtraction), by 16 standard deviations above the local realistic bound of 2 (Table 1). This represents a clear violation of local realism in an experimental arrangement which explicitly closes both the locality and the freedom-of-choice loopholes, while only relying on the fair-sampling assumption.

In our experiment, there were several factors which reduced the measured Bell parameter below the ideal value of 2√2, including imperfections in the source, polarization analysis and quantum channels. These can be characterized individually by measured visibilities, which were: for the source, ≈ 99% (98%) in the H/V (45°/135°) basis; for both Alice's and Bob's polarization analyzers, ≈ 99%; for the fibre channel and Alice's analyzer (measured before each run), ≈ 97%, while the free-space link did not observably reduce Bob's polarization visibility; for the effect of accidental coincidences resulting from an inherently low signal-to-noise ratio (SNR), ≈ 91% (including both dark counts and multipair emissions, with 55 dB two-photon attenuation and a 1.5 ns coincidence window). Using these values, one can calculate the expected Bell parameter from the estimated two-photon visibility via $S^{exp} \approx V^{exp} \cdot S^{qm}_{max} \approx 2.43$. The remaining discrepancy with the measured value results mainly from variable polarization drift in Alice's 6 km delay fibre, as confirmed by the results of a tomographic measurement (see Supplementary Information). After optimising the fibre channel before each measurement, its visibility was observed to fall as low as 87-90% during a measurement run, limiting the useful measurement time to 600 s before realignment was required.

In conclusion, we violated Bell's inequality by more than 16 standard deviations, in an experiment simultaneously closing both the locality and the freedom-of-choice loopholes. This represents the most conclusive falsification of local realism to date. A completely loophole-free Bell test will have to both exclude these two loopholes and simultaneously close the fair-sampling loophole by ensuring that, in the limit of no background noise, at least 44.5% of all generated particle pairs are detected[18]. We believe that such an experiment is possible.

Figures and tables.

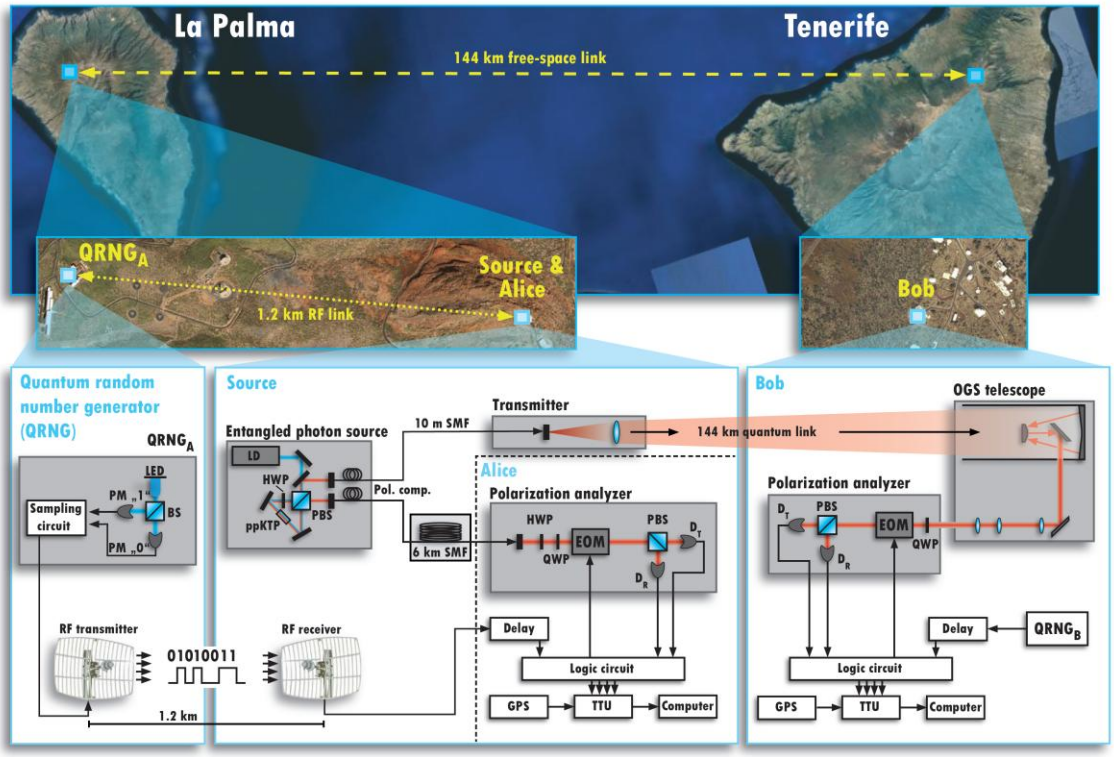

Figure 1| Experimental setup. The Bell experiment was carried out between the islands of La Palma and Tenerife at an altitude of 2400 m. *La Palma*: A 405 nm laser diode (LD) pumped a periodically poled KTP crystal (ppKTP) in a polarization-based Sagnac interferometer, to generate entangled photon pairs in the ψ^- singlet state. One photon per pair was sent through a 6 km long, coiled optical single-mode fibre (SMF) to Alice (located next to the source). Alice's polarization analyzer consisted of half- and quarter-wave plates (HWP, QWP), an electro-optical modulator (EOM), a polarizing beam splitter (PBS) and two photodetectors (D_T, D_R). A quantum random number generator ($QRNG_A$)[27] located at a distance of 1.2 km, consisting of a light emitting diode (LED), a 50/50 beam splitter (BS) and two photomultipliers (PM), generated random bits which were sent to Alice via a 2.4 GHz AM link. The random bits were used to switch the EOM, determining if the incoming photon was measured in the 22.5°/112.5° or 67.5°/157.5° linear polarization basis. A time-tagging unit (TTU), locked to the GPS time standard, recorded every detection event (arrival time, detector channel and setting information) onto a local hard disk. The other photon was guided to a transmitter telescope and sent through a 144 km optical free-space link to Bob on Tenerife. *Tenerife*: The incoming photon was received by the 1 m optical ground station telescope of the European Space Agency. At Bob's polarization analyzer (triggered by an equal but independent quantum random number generator $QRNG_B$), the photons were measured in either the H/V or the 45°/135° linear polarization basis. Bob's data acquisition was equivalent to Alice's. (See also Supplementary Information for details.) [Geographic pictures taken from *Google Earth*.]

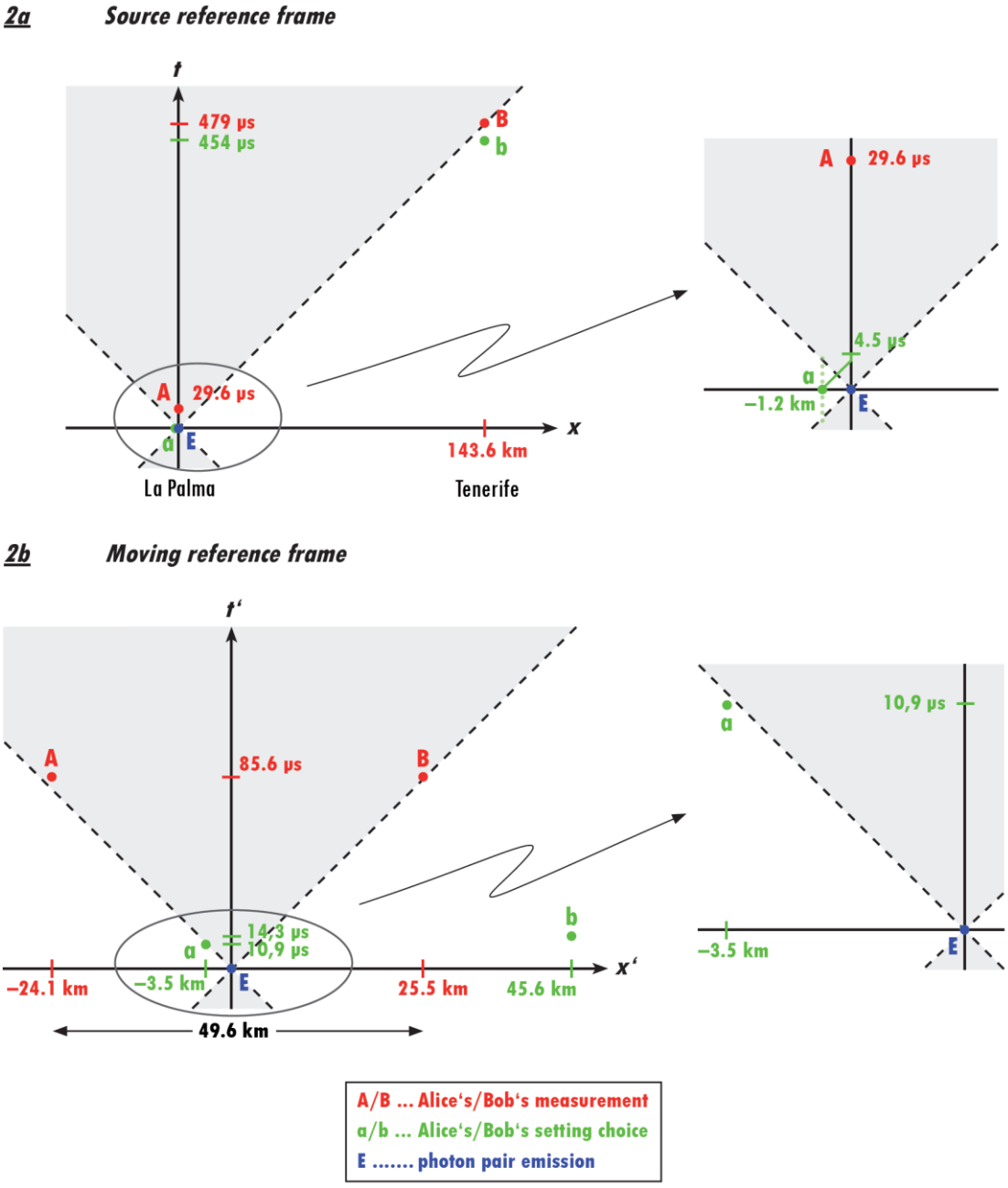

Figure 2| Space-time diagrams. *2a*: Source reference frame. The forward (backward) light cone of the photon emission event **E**, shaded in grey, contains all space-time events which can be causally influenced by **E** (can causally influence **E**). Alice's random setting choices (indicated by small green dots in the zoomed part of figure 2a), each applied for a 1 µs interval, were transmitted over a 1.2 km classical link, which took 4.5 µs (3.9 µs classical RF link, 0.6 µs electronics). This signal was electronically delayed by 24.6 µs, so that the choice event **a**, corresponding to a given measurement **A**, occured *on average* simultaneously with the emission event **E**, i.e., the photon measurement event occurred *on average* in the middle of the 1 µs setting interval. The choice and emission events were therefore space-like separated. The same electronic delay (24.6 µs) was applied to Bob's choice **b**, so that it was also space-like separated from the source. *2b*: Moving reference frame. From the perspective of an observer moving at a speed of 0.938·*c* parallel to the direction from La Palma (Alice) to Tenerife (Bob), the measurement events, **A** and **B**, occur simultaneously with the emission event approximately in the middle of the two. The locality and the freedom-of-choice loopholes are closed in the source reference frame, and since

space-like separation is conserved under Lorentz transformations, they are closed in all reference frames. In the diagrams above, the total uncertainty of the event times is below the thickness of the illustrated points (see Supplementary Information).

Polarizer settings *a, b*	0°, 22.5°	0, 67.5°	45°, 22.5°	45°, 67.5°
Correlation $E(a,b)$	0.62 ± 0.01	0.63 ± 0.01	0.55 ± 0.01	–0.57 ± 0.01
Obtained Bell value S^{exp}	2.37 ± 0.02			

Table 1| Experimental results. We measured the polarization correlation coefficients $E(a,b)$ to test the CHSH inequality[28] under locality and freedom-of-choice conditions. Combining our experimental data, we obtained the value of S^{exp} = 2.37 ± 0.02. Assuming statistical errors and relying only on the fair-sampling assumption, this leads to a violation of local realism by more than 16 standard deviations, thereby simultaneously closing both the locality and the freedom-of-choice loopholes.

Acknowledgements

The authors wish to thank F. Sanchez (Director IAC) and A. Alonso (IAC), T. Augusteijn, C. Perez and the staff of the Nordic Optical Telescope (NOT), J. Kuusela, Z. Sodnik and J. Perdigues of the Optical Ground Station (OGS) as well as J. Carlos and the staff of the Residence of the Observatorio del Roque de Los Muchachos for their support at the trial sites. This work was supported by ESA (contract number 18805/04/NL/HE), the Austrian Science Foundation (FWF) under project number SFB1520, the Doctoral Program CoQuS, the European project QAP, the Austrian Research Promotion Agency (FFG) through the Austrian Space Program ASAP, and the DTO-funded U.S. Army Research Office within the QCCM program.

References

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

[2] Freedman, S. J. & Clauser, J. F. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.* **28**, 938-941 (1972).

[3] Fry, E. S. & Thompson, R. C. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.* **37**, 465-468 (1976).

[4] Aspect, A., Grangier, P. & Roger, G. Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell's inequalities. *Phys. Rev. Lett.* **49**, 91-94 (1982).

[5] Aspect, A., Dalibard, J. & Roger, G. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.* **49**, 1804-1807 (1982).

[6] Ou, Z. Y. & Mandel, L. Violation of Bell's inequality and classical probability in a two-photon correlation experiment. *Phys. Rev. Lett.* **61**, 50-53 (1988).

[7] Shih, Y. H. & Alley, C. O. New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion. *Phys. Rev. Lett.* **61**, 2921-2924 (1988).

[8] Tapster, P. R., Rarity, J. G. & Owens, P. C. M. Violation of Bell's inequality over 4 km of optical fiber. *Phys. Rev. Lett.* **73**, 1923-1926 (1994).

[9] Kwiat, P. G., Mattle, K., Weinfurter, H. & Zeilinger, A. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75**, 4337-4341 (1995).

[10] Tittel, W., Brendel, J., Zbinden, H. & Gisin, N. Violation of Bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.* **81**, 3563-3566 (1998).

[11] Weihs, G. *et al.* Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.* **81**, 5039-5043 (1998).

[12] Rowe, M. A. *et al*. Experimental Violation of a Bell's Inequality with Efficient Detection. *Nature* **409**, 791-794 (2001).

[13] Ursin, R. *et al*. Entanglement-based quantum communication over 144 km. *Nature Physics* **3**, 481-486 (2007).

[14] Kwiat, P. G., Eberhard, P. H., Steinberg, A. M. & Chiao, R. Y. Proposal for a loophole-free Bell inequality experiment. *Phys. Rev. A* **49**, 3209-3221 (1994).

[15] García-Patrón, R. *et al.* Proposal for a Loophole-Free Bell Test Using Homodyne Detection. *Phys. Rev. Lett.* **93**, 130409 (2004).

[16] Simon, C. & Irvine, W. T. M. Robust Long-Distance Entanglement and a Loophole-Free Bell Test with Ions and Photons. *Phys. Rev. Lett.* **91**, 110405 (2003).

[17] Volz, J. *et al.* Observation of Entanglement of a Single Photon with a Trapped Atom. *Phys. Rev. Lett.* **96**, 030404 (2006).

[18] Eberhard, P. H. Background Level and Counter Efficiencies Required for a Loophole-Free Einstein-Podolsky-Rosen Experiment. *Phys. Rev. A* **47**, R747-R750 (1993).

[19] Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777-780 (1935).

[20] Schrödinger, E. Die Gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften* **23**, 807-812; 823-828; 844-849 (1935).

[21] Bell, J. S. in *Foundations of Quantum Mechanics*, pp. 171-181, ed. d'Espagnat, B., New York: Academic (1971).

[22] Clauser, J. F. & Horn, M. A. Experimental consequences of objective local theories. *Phys. Rev. D* **10**, 526-535 (1974).

[23] Fine, A. Hidden variables, joint probabilities, and the Bell inequalities. *Phys. Rev. Lett.* **48**, 291-295 (1982).

[24] Jarrett, J. P. On the physical significance of the locality conditions in the Bell argument. *Noûs* **18**, 569-589 (1984).

[25] Bell, J. S. *Speakable and Unspeakable in Quantum Mechanics*, pp 243-244, Revised Edition. Cambridge University Press (2004).

[26] Pearle, P. M. Hidden-variable example based upon data rejection. *Phys. Rev. D* **2**, 1418-1425 (1970).

[27] Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675 (2000).

[28] Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880-884 (1969).

Supplementary information

Entangled photon source

Entangled photon pairs were generated by type-II down conversion in a 10 mm ppKTP crystal which was placed inside a polarization Sagnac interferometer[1]. Using a 405 nm laser diode with a maximum output power of 50 mW, we generated entangled pairs with a wavelength of 810 nm in the ψ^- Bell state with a production rate of 3.4×10^7 Hz. This number was inferred from locally detected 250000 photon pairs/s at a pump power of 5 mW and a coupling efficiency of 27% (calculated from the ratio of coincidence and singles counts). Furthermore, operation at 5 mW pump power yielded a locally measured visibility of the generated entangled state in the H/V (45°/135°) basis of ≈ 99% (98%) (accidental coincidence counts subtracted). We assumed that the state visibility did not change considerably at 50 mW pump power.

Polarization analyzer modules

As electro optical modulators (EOMs) we used Pockels Cells (PoCs) consisting of two 4x4x10mm RTP crystals (Rubidium Titanyl Phosphate). Since the PoC served as a switchable half-wave plate (HWP) for polarization rotations of 0° and 45°, we aligned the optical axes of the RTP crystals to 22.5°. Additionally, we placed a quarter-wave plate (QWP) with its optical axis oriented parallel to the axis of the RTP crystals in front of the PoC. Applying a positive quarter-wave voltage (+QV) made the PoC act as an additional QWP, such that the overall effect was the one of a HWP at 22.5° which rotates the polarization by 45°. In contrast, applying negative quarter-wave voltage (–QV) made the PoC compensate the action of the QWP, such that the overall polarization rotation was 0°. A self-built FPGA logic sampled the random bit sequence from the quantum random number generator (QRNG) and delivered the required pulse sequence to the PoC driver head. A random bit “0” (“1”) required a polarization rotation of 0° (45°) and –QV (+QV) was applied to the PoC. A given setting was not changed until the occurrence of an opposite trigger signal. However, since our QRNG was balanced within the statistical uncertainties, +QV and –QV were applied on average equally often. As a result, the mean field in the PoC was zero, which allowed continuous operation of the PoC without damaging the crystals, e.g. due to ion-wandering effects. For optimal operation of the PoC, a toggle frequency of 1 MHz was chosen. The rise time of the PoC was measured to be < 15 ns. Thus, to be sure that the switching process had been finished, we discarded all photons which were detected less than 35 ns after a trigger signal. These operating conditions resulted in a switching duty cycle of approximately 97%.

6 km fibre channel

At Alice’s location, the 6 km-long fibre was placed in a thermally insulated box and temperature stabilized to 40°C ± 0.2°C to avoid polarization drift. Despite this, we

had to realign the polarization through the fibre link approximately every 600 s. The fibre attenuation of 17dB and the attenuation of the analyzer module of 3dB resulted in an attenuation of Alice's quantum channel of 20dB.

144 km optical free-space channel

The optical free-space link was formed by a transmitter telescope mounted on a motorized platform and a receiver telescope – the European Space Agency's OGS with a 1 m mirror (effective focal length f = 38 m) located on Tenerife. The transmitter consisted of a single-mode fibre coupler and an $f/4$ best form lens (f = 280 mm). We employed the closed-loop tracking system described in Refs [2, 3]. Using a weak auxiliary laser diode at 810 nm, the attenuation of the free-space link from La Palma (including the 10 m single-mode fibre to the transmitter telescope) to the (free-space) APDs (500 µm active area) at the OGS in Tenerife was measured to be 35dB. Here, the 3dB attenuation through the analyzer module is already included.

The photon-pair attenuation through the whole setup was therefore 20 dB + 35 dB = 55 dB, from which we predicted a coincidence rate of ≈ 8 Hz between Alice and Bob, in good accordance with our measured 19917 coincidences in 2400 s (i.e. 8.3 Hz).

Event durations

In our experiments, we define the event durations as follows: for measurements, the time from a photon impact on the detector surface until the completion of the APD breakdown (< 10 ns for our detectors); for setting choices, the autocorrelation time of the random number generators (= 1/(2*R) ≈ 17 ns for an internal toggle frequency R = 30 MHz[4]); and for the emission event, the coherence time of the pump laser (< 1 ns).

Actual space-time arrangement

The geographical setup is not exactly one-dimensional as drawn in the Figure 2. However, the deviation from an ideal one-dimensional scenario is only about 24°. The real-space distance between Alice's QRNG and Bob is about 100 m less than the sum of the distance between Alice's QRNG and Alice herself (1.2 km), and the distance between Alice and Bob (143.6 km). Thus, using the approximated one-dimensional scenario in Figure 2 introduces no deviations larger than 0.3 µs (which is well below the time for which an individual setting is valid) and hence does not effect the space-like separation of the key events. One can also neglect the refractive index of air at this altitude (1.0002), and the delay due to the optical path in the receiving telescope, each of which only introduces an error of approximately 0.1 µs to the flight time of Bob's photon.

State tomography

We also used the same experimental design to perform tomography and directly measure the entangled state (Figure 1) in the same locality and freedom-of-choice context. The measured quantum state demonstrates the entanglement of the widely separated photons by about 17 standard deviations, characterized by the tangle[4,5] T = 0.68 ± 0.04. It also predicts a Bell parameter of S^{tomo} = 2.41 ± 0.06, which agrees with the direct measurement. However, unlike a Bell test, this tomographic analysis requires no prior knowledge of the polarization orientation of the two-photon state, and therefore does not rely on how well Alice and Bob can establish a shared reference frame. Therefore, we can also calculate the optimal Bell violation that could have been achieved with a perfectly aligned reference frame, S^{opt} = 2.54 ± 0.06, which is close to the Bell value S^{SNR} = 0.91*2√2 ≈ 2.57 that is limited only by the SNR. This indicates that the polarization errors arose mainly from the inaccuracies of aligning the shared reference frame rather than from polarization decoherence.

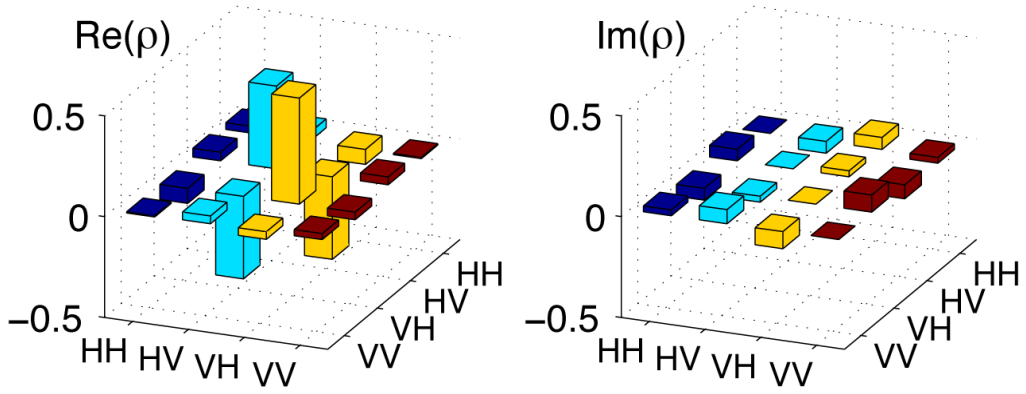

Figure 1| State tomography. Reconstructed density matrix ρ for Alice's and Bob's nonlocal two-photon state, with tangle[5,6] T = 0.68 ± 0.04, confirming the entanglement of the widely separated photons, linear entropy[6] S_L = 0.21 ± 0.03 and optimal fidelity with a maximally entangled state F_{opt} = 0.91 ± 0.01. The measured state predicts a Bell parameter of S^{tomo} = 2.41 ± 0.06, which agrees with the directly measured value, and an optimal violation of S^{opt} = 2.54 ± 0.06 for a rotated set of polarization measurements. The non-zero imaginary components are mainly due to polarization rotations resulting from imperfections in the alignment of Alice's and Bob's shared reference frame.

Different space-time scenarios

For the sake of completeness, we have performed Bell experiments using different space-time arrangements of the relevant events, achieving significant Bell violations in each case (Table 1).

	Settings *a* and *b* …	Our obtained Bell value S^{exp}	Previously performed?
a)	… were chosen in the past light cone of the emission	2.28 ± 0.04	Yes: experiments with static settings
b)	… were varied periodically	2.23 ± 0.05	Yes: Ref. [7]
c)	… were randomly chosen in the future light cone of the emission	2.23 ± 0.09	Yes: Ref. [8]
d)	… were space-like separated from the emission	2.37 ± 0.02	No: presented here for the first time

Table 1|Space-time scenarios. *a)* Choice events **a** and **b** lay in the past light cone of **E** and could have influenced the hidden variables emitted by the source. In addition, the choice event on one side was not space-like separated from the measurement event on the other side. Thus, the locality and the freedom-of-choice loopholes were not closed. This situation is true for any experiment where the measurement settings are not randomly switched. *b)* Settings were varied periodically, and were hence predictable at any time. This situation is similar to the one in Aspect *et al*.[7] *c)* Choice events **a** and **b** lay in the future light cone of the pair emission **E**, and thus could in principle have been influenced by the hidden variables produced by the source, and hence the freedom-of-choice loophole was not closed. The weak Bell violation by 2.5 standard deviations was due to bad weather conditions which resulted in low photon transmission through the free-space link and a low signal-to-noise ratio. A similar scenario was achieved in the experiment of Weihs *et al.*[8] *d)* Scenario of the experiment described in the main text of this paper.

References for Supplementary Information

[1] Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T. & Zeilinger, A. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express* **15**, 15377-15386 (2007).

[2] Ursin, R. *et al*. Entanglement-based quantum communication over 144 km. *Nature Physics* **3**, 481-486 (2007).

[3] Fedrizzi, A. *et al.* Testing quantum communication with photonic Bell states over a 71 dB loss freespace channel. Submitted (2008).

[4] Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H. & Zeilinger, A. A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675 (2000).

[5] Wootters, K. M. Entanglement of Formation of an Arbitrary State of Two Qubits. *Phys. Rev. Lett.* **80**, 2245-2248 (1998).

[6] James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A* **64**, 052312 (2001).

[7] Aspect, A., Dalibard, J. & Roger, G. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.* **49**, 1804-1807 (1982).

[8] Weihs, G. *et al.* Violation of Bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.* **81**, 5039-5043 (1998).

B. C^{++}-Code

Below is the C^{++} code, which was used to calculate the cross-correlation function from the time-tagging files. This routine was written by my college Thomas Jennewein.

B.1. Source code: coincdosv9.cpp

```
//coincidences from a single file
//Thomas Jennewein Sept,2006
//gcc -lm -o coinc_search_singlefile coinc_search_singlefile.c
//einbau von Buffer für Timetags 25.9.2006, notwendig für wenig Zählrate
//Adaptierung für das Einlesen der Daten von LabView Binary, 3. April 2007
//April 2008 Adaptierung für zwei Files, von der neuen Timetag logik, mit eingebauter Korrektur
//Juni2008 Adaptierung für Ausgabe von Koinzidnezhistogram in kurzen Blöcken

#include <stdlib.h>
#include <stdio.h>
#include <errno.h>
#include <math.h>
#include <string.h>



#define binanzahl 2000

signed long histo[27][binanzahl];
// signed long corr[27][binanzahl]; // daraus wurde die Coinc Matrix für jeden Timebin errechnet
signed long coinc_matrix[27];
signed long singles[8];

//Cyclebuffer für Alice tags
double atime_cycle[20];
signed long achan_cycle[20];

double achan, atime, bchan, btime, offset, diff, histwid, bobgps, laufzeit, sss, timetagunit_a, timetagunit_b, gps_tolerance;
signed long maxhisto, maxindex, accumhisto, bj, aj, cycla, outfile_counter;
signed long j, i, k, corr_channel, count_alice, count_bob, outputperiode, gpscycle;
int dummy_chan, gpscycle_input;

//variables for the filter
/*double currentCounts, count1, sum1, count2, sum2, kFilter, kComp, diff1, diff2;
double CP_count, CP_time, CP_factor;
int PC_factor=1;
int prevTag, FilterStartPoints;
int firstTag, firstRefTag, FilterReady;
double ReferenceTagDifference, FilterPoints, GridWidth, ExpectedCounts, MinCount, MaxCount;
double tim, plausibilityLastCount, diff_plaus, zeroTime,last_ref;
*/

//Function for Reading Timetags from File
double getsample(FILE *f) {
  if(fread(&sss,8,1,f)==1) {
  return sss;
  }
  else {return 0;}
}


//Functions for Filter for Correcting Timebase
/*void CalcFilter(double count) {
    if (firstRefTag==0) {
        count1 = count;
        count2 = count;
        CP_count = count;
        firstRefTag = 1;
    return;
    }

    count1 = count1 + (diff1 * kFilter + sum1 * kComp);
    diff1 = (count - count1)/PC_factor;
    sum1 = sum1 + diff1;

    count2 = count2 + (diff2 * kFilter + sum2 * kComp);
    diff2 = count1 - count2;
    sum2 = sum2 + diff2;
    CP_factor = ReferenceTagDifference / (count2 - CP_count);
    CP_count = count2;
    CP_time = CP_time + PC_factor*ReferenceTagDifference;
```

```
}



void InitFilter(void) {
    FilterReady = 0;
    FilterStartPoints = FilterPoints * 5;
    kFilter = 1. / FilterPoints;
    kComp = kFilter * kFilter / 4;
    count1 = 0;
    count2 = 0;
    if (kComp == 0) { sum1 = 0; }
    else { sum1 = ExpectedCounts / kComp; }
    sum2 = sum1;
}

void InitTagSystem(void) {

    ReferenceTagDifference = 1.0 / 10000000.0 * 1000.0; //10 MHz mit Prescaler 1000
    FilterPoints = 3.;
    GridWidth = 0.00000000125;
    ExpectedCounts = ReferenceTagDifference / GridWidth;
    MinCount = ExpectedCounts - 5000.;
    MaxCount = ExpectedCounts + 5000.;

    firstRefTag = 0;
    currentCounts = 0.;
    CP_count = 0;
    CP_time = 0;
    CP_factor = ((ReferenceTagDifference * 1.0) / ExpectedCounts);
    InitFilter();
}

//Lineare interpol
double Interpolate(double tag) {
 return ( CP_time + (tag - CP_count) * CP_factor);

}


double handle_tag(int chn, double time) {
       if (chn == 0) {
          //PlausibilityCheck(time);
          CalcFilter (time);
          //fprintf(stderr,"Bob Ref Tag: %5.0f  differnece= %5.0f \n",time,time-last_ref);
          }
       time = Interpolate(time);
       if (chn == 0) {
          //fprintf(stderr,"corr Bob Ref Tag: %5.10f, diff to pref Ref %5.10f  \n",time,
    time-last_ref);

          //last_ref=time;
          }
 return time;
}
*/


void write_output_file(FILE *f){
     //Formatting the logfile for output
        //fout=fopen(fname_out&"_%d",outfile_counter,"w");
        fprintf(f,"Histogram bin size  %5.10f ns\n \n",histwid/(binanzahl/2)*1e9);
        fprintf(f,"Singles Counts: CH1=%.6d CH2=%.6d CH3=%.6d CH4=%.6d CH5=%.6d\n \n",
    singles[0],singles[1],singles[2],singles[3],singles[4]);
        //fprintf(fout,"Histoelements for all coincidences in single file, : \n");

        //fprintf(fout,"Bin, ");
        for(bj=1;bj<27;bj++)//{fprintf(fout,"Hist%d, ",bj); }
        //fprintf(fout,"\n");

        for(j=1;j<binanzahl+1;j=j+1) {
                fprintf(f,"%f, ",(j-binanzahl/2)*(histwid/(binanzahl/2)*1e9)-(histwid/
    (binanzahl)*1e9));
```

```
                for(bj=1;bj<27;bj++){ fprintf(f,"%d, ",histo[bj][j]);
                                    }
                fprintf(f,"\n");
                }
        fprintf(f,"\n");
        fprintf(f,"\n");
        //fclose(f);
     }

//Main Program
int main(int argc, char **argv) {

const char *fname_alice=argv[5];
const char *fname_bob=argv[6];
//const char *fname_out=argv[7];

char* fname_out=argv[7];
char fname_out2[100];


FILE* falice;
FILE* fbob;
FILE* fout;

if(argc!=9) printf("Not enough Arguments!\n\n Usage: coincdos_vX.X timedelay[s] timewindow
    [s] outperiod(1..inf) accumhisto(1/0) gpscycle A_file B_file fileout measured_cycle");

//InitTagSystem();

//timetagunit=0.00000000125; // hŠngt von der eingesetzten Logik ab! dieser Wert 1.25ns ist
     fŸr die "alte" Logik .

timetagunit_a=(1 / (50000000.0 * 2 * 2 * 4 * 8));//0.00000000015625;
timetagunit_b=timetagunit_a;

fprintf(stderr,"\n ************************************ \n Willkommen bei der
    Koinzidencen-Suche in zwei separate Files.\n Ausgabe wird unterteilt in mehrere Blöcke
    \n Es geht nun los. \n ************************************ \n");
fprintf(stderr,"Filename Alice: %s \n",fname_alice);
fprintf(stderr,"Filename Bob  : %s \n",fname_bob);

if((falice=fopen(fname_alice,"rb")) == NULL) {
                                    fprintf(stderr,"Alice File could not be opened");
                                    exit(0);}

if((fbob=fopen(fname_bob,"rb")) == NULL) {
                                    fprintf(stderr,"Bob File could not be opened");
                                    exit(0);}

//***********  Parameters: **********
  histwid=(double)atof(argv[2]);     //0.5e-7; Halbwertsbreite des Histogrammes
  laufzeit=(double)atof(argv[1]);    //0; //0.00047935;// Grobdelay, guter Wert in
    Teneriffa: 0.0004795015;
  outputperiode=atoi(argv[4]);       // Periode der Ausgabe bezogen auf 1PPS vom GPS Signal
  accumhisto=atoi(argv[3]);          //Akkumulative HIstogramms? oder Histogramm bei jedem
    GPS ZUyklus lÃ¶schen?
  gpscycle_input=atoi(argv[8]);      // gpscycle_input defines the measurement_time =
    (gpscycle-1)/gps_frequncy
  if (gpscycle_input==-1) {gpscycle_input=100000;}  //wenn gpscycle_input = -1, dann soll
    das gesamte File gescannt werden
  fprintf(stderr,"Suchparameter: Grobdelay: %5.10fs; \n Histogramm-Halbreite: %5.10fs; \nO
    utputperiode Anzahl 1PPS: %d. \n Akkumulatives Histogramm: %d\n",laufzeit,histwid,
    outputperiode,accumhisto);
  dummy_chan=7;
  gps_tolerance=5;                 //synchronization tolerance of the two computers
    measured on GPS signals

if(outputperiode<1) {outputperiode=1;}
//********** Start der Suche: **********
for(j=1;j<binanzahl;j=j+1) {
    for(bj=0;bj<27;bj=bj+1)
        {
        histo[bj][j]=0;
    }
```

```
 }

fprintf(stderr,"Histogram bin size  %5.10f ns\n",histwid/(binanzahl/2)*1e9);

fout=fopen("gps_tags.txt","w");

// Find first Bob Timetag
do {
    bchan=getsample(fbob);
    //btime=(double)getsample(fbob)*timetagunit_b;
    btime=(double)getsample(fbob);
    //fprintf(stderr,"Bob Tag: %5.10f Bob Chan:%1.1f  corr = ",btime*timetagunit_b,bchan);
    btime=btime*timetagunit_b; //handle_tag(bchan,btime);
    //fprintf(stderr,"Bob Tag: %5.10f Bob Chan:%1.1f \n",btime,bchan);

 } while(bchan!=6);   //GPS channel = 6

// First Bob Timetag Found
fprintf(stderr,"First Bob-GPS tag found at %5.10f\n",btime);

// Initialisiere atime_cycle und achan_cycle
for(k=1;k<20;k++){
        atime_cycle[k]=0;
        achan_cycle[k]=0;
    }
// Find first Alice GPS Timetag
do {
    do{
        achan=getsample(falice); atime=(double)getsample(falice)*timetagunit_a;
        //if (achan==6){
        //fprintf(stderr,"Alice Tag: %5.10f Alice Chan:%f \n",atime,achan);}
        }while(achan==dummy_chan);

    for(k=1;k<20;k++){
        atime_cycle[k-1]=atime_cycle[k];
        achan_cycle[k-1]=achan_cycle[k];
    }
    atime_cycle[19]=atime;
    achan_cycle[19]=(signed long)achan;
} while(achan_cycle[0]!=6); //GPS channel = 6

fprintf(stderr,"First Alice-GPS found at %5.10f\n",atime_cycle[0]);

offset = btime - atime_cycle[0] + laufzeit;  //GPS Offset + Flugzeit!!! ca0.0005s
//offset=laufzeit; //ohne GPS wird hŠndischer Offset genommen
fprintf(stderr,"First Total offset inklusive GPS + Grobdelay: %5.10f s. \n **********↙
    **********\n",offset);



//Time jitter and ambivalence correction for the 1PPS signal


if (offset>gps_tolerance){
                          // Find next Alice GPS Timetag
                            do {
                                do{
                                    achan=getsample(falice); atime=(double)getsample       ↙
    (falice)*timetagunit_a;
                                    //if (achan==6){
                                    //fprintf(stderr,"Alice Tag: %5.10f Alice Chan:%f \n",  ↙
    atime,achan);}
                                    }while(achan==dummy_chan);
                                for(k=1;k<20;k++){
                                    atime_cycle[k-1]=atime_cycle[k];
                                    achan_cycle[k-1]=achan_cycle[k];
                                }
                                atime_cycle[19]=atime;
                                achan_cycle[19]=(signed long)achan;
                            } while(achan_cycle[0]!=6); //GPS channel = 6
                            fprintf(stderr,"Second Alice GPS found %5.10f\n",atime_cycle    ↙
    [0]);
                          }
if (offset<-gps_tolerance){
```

```
                        // Find next Bob GPS Timetag
                        do {
                             bchan=getsample(fbob);
                             //btime=(double)getsample(fbob)*timetagunit_b;
                             btime=(double)getsample(fbob);
                             //fprintf(stderr,"Bob Tag: %5.10f Bob Chan:%1.1f  corr = ",
    btime*timetagunit_b,bchan);
                             btime=btime*timetagunit_b; // handle_tag(bchan,btime);
                             //fprintf(stderr,"Bob Tag: %5.10f Bob Chan:%1.1f \n",btime,
    bchan);
                         } while(bchan!=6);   //GPS channel = 6

                        // Second Bob Timetag Found
                        fprintf(stderr,"Second Bob GPS tag found %5.10f\n",btime);
}
fout=fopen("bob_cor.txt","w");
offset = btime - atime_cycle[0] + laufzeit;  //GPS Offset + Flugzeit!!! ca0.0005s
//offset=laufzeit; //ohne GPS wird hŠndischer Offset genommen
fprintf(stderr,"New Total offset inklusive GPS + Grobdelay: %5.10f s. \n **********
    ******************\n",offset);

//Loop für Koinzidenssuche
do{
    do{
          bchan=getsample(fbob);
          //btime=(double)getsample(fbob)*timetagunit_b;
          btime=(double)getsample(fbob);
          //fprintf(stderr,"Bob Tag: %5.10f Bob Chan:%1.1f  corr = ",btime*timetagunit_b,
    bchan);

            /*if (bchan==0){
                    if ((btime-last_ref<70000)|(btime-last_ref>90000)) {
             fprintf(fout,"Bob Ref Tag: %5.10f,  differnece= %5.10f \n",btime,btime-
    last_ref);}
             last_ref=btime;

           }*/

          btime=btime*timetagunit_b;//handle_tag(bchan,btime);
          if (bchan==6){
             fprintf(fout,"Bob, 1PPS-Tag=%5.10f\n",btime);
             }

          }while(bchan==dummy_chan);
    if (bchan!=6){
                count_bob = count_bob+1;
                if (bchan==1) {bj=0;}
                if (bchan==2) {bj=1;}
                if (bchan==3) {bj=2;}
                if (bchan==4) {bj=3;}
                if (bchan==5) {bj=4;}
                singles[bj]++;
                }

    if ((bchan==6)) {
                 gpscycle++;

                 if (gpscycle%outputperiode==0){
                 fprintf(stderr,"************************  GPS Bob: %5.10f , GPS Cycle:
     %d **********************\n",btime,gpscycle);
                 bobgps= btime;
                 //Search for (single) Coincidencepeak
                 maxhisto=0;
                 for(j=1;j<binanzahl+1;j=j+1) {
                     if (histo[26][j]>maxhisto) {
                          maxhisto=histo[26][j];
                          maxindex=j;
                          }
                     }
                 fprintf(stderr,"Maxhisto at index: %d, corresponding to time delay: %f
    ns.\n\n",maxindex,((maxindex-(binanzahl/2)+1)*histwid/(binanzahl/2)*1e9 ));

                 //***** Take Values arround peak -> Momentan statisch, muss angepasst
    werden...
```

```
                for(j=0;j<25;j=j+1) {
                        coinc_matrix[1+j] = histo[1+j][maxindex] + histo[1+j][maxindex+
    1]+ histo[1+j][maxindex-1]+histo[1+j][maxindex+2]+histo[1+j][maxindex-2];
                    }

                //**** Print coincidence table
                for(j=0;j<25;j=j+5) {
                        fprintf(stderr,"%.7d %.7d %.7d %.7d %.7d\n",coinc_matrix[1+j],
    coinc_matrix[2+j],coinc_matrix[3+j],coinc_matrix[4+j], coinc_matrix[5+j]);

                }
                k=0;
                for(j=0;j<25;j++){
                    k=k+(long)coinc_matrix[1+j];
                    }
                fprintf(stderr,"Summe Koinzidenzen: %d \n",k);


                fprintf(stderr,"Singles Counts: CH1=%.6d CH2=%.6d CH4=%.6d CH8=%.6d
    CH16=%.6d\n ",singles[0],singles[1],singles[2],singles[3],singles[4]);
                count_alice=0;
                count_bob=0;



                //****** Ausgabe der Counts und Löschen bei jedem GPS Zyklus?
                if (accumhisto==0){
                        //sprintf(fname_out2, "%s_%d", fname_out, outfile_counter);
                     j=sprintf(fname_out2, "%s_%d.csv", fname_out, outfile_counter);
                     fprintf(stderr,"out_filename: %s \n",fname_out2);

                     fout=fopen(fname_out2,"w");
                     write_output_file(fout);
                     fclose(fout);
                     outfile_counter++;
                    for(j=1;j<(binanzahl+1);j=j+1) {
                                        for(k=0;k<26;k=k+1) {histo[1+k][j]=0;}
                                        }
                    for(k=0;k<25;k=k+1) {coinc_matrix[1+k]=0;}

                    for(k=0;k<5;k=k+1) {singles[k]=0;}
                    }
                }
             }
    //  }


    i=0;

    //********************************** Align Tables! ***********************************
    *
    cycla=0;
    do{
            if (cycla<20){
                achan=achan_cycle[cycla];
                atime=atime_cycle[cycla];
                cycla++;
                }
            else{
                do{
                        achan=getsample(falice);
                        atime=(double)getsample(falice)*timetagunit_a;
                        if (achan==6){
                           fprintf(fout,"Alice GPS-Tag %5.10f\n",atime);
                           }

          //}
                        }while(achan==dummy_chan);
                for (k=1;k<20;k++){
                    atime_cycle[k-1]=atime_cycle[k];
                    achan_cycle[k-1]=achan_cycle[k];
                    }
                atime_cycle[19]=atime;
                achan_cycle[19]=(signed long)achan;
```

```
                    }
                i=i+1;
            //fprintf(stderr,"present diff %5.10f \n",(btime-atime-offset));
            diff = (btime-atime-offset);
            if (atime==0) {
                //fprintf(stderr,"present diff %5.10f \n",(btime-atime-offset));
                diff=-2*histwid;
                }
      } while((diff>histwid)); // &(achan!=bchan));

    //*****************************************************************************
    do{
        diff = (btime-atime-offset);
        if ((diff>-histwid)) {
            j=abs((diff/histwid)*(binanzahl/2)+((binanzahl/2)+1));
            if ((bchan >0)&(achan>0)&(achan!=6)&(bchan!=6)) {
                if ((j<binanzahl+1)&(j>-1)) {

                    if (bchan) {
                                    //fprintf(stderr,"coinc found at A %5.10f, B %5.10f \n",atime,btime);
                                    if (achan==1){aj=0;}
                                    if (achan==2){aj=1;}
                                    if (achan==3){aj=2;}
                                    if (achan==4){aj=3;}
                                    if (achan==5){aj=4;}
                                    corr_channel= (aj + bj*5 + 1);
                                    histo[corr_channel][j]++;
                                    histo[26][j]++;
                                   }
                       }
                   }
              }

        if (cycla<20){
            achan=achan_cycle[cycla]; atime=atime_cycle[cycla];   //sa=atime_cycle[cycla]; atime=(1E-9*sa/(1<<18)); achan=(long)sa&0xff;
            cycla++;
        }
        else {
             do{
                    achan=getsample(falice); atime=(double)getsample(falice)*timetagunit_a;
                    if (achan==6){
                             fprintf(fout,"Alice GPS-Tag %5.10f\n",atime);
                              }
                    }while(achan==dummy_chan);
             count_alice=count_alice+1;
             for (k=1;k<20;k++){
                    atime_cycle[k-1]=atime_cycle[k];
                    achan_cycle[k-1]=achan_cycle[k];
                }
            atime_cycle[19]=atime;
            achan_cycle[19]=(signed long)achan;
        }

    } while((diff>-histwid)&(atime>0));

 } while((btime>0)&!(gpscycle>gpscycle_input));// gpscycle defines the measurement time,

  fclose(fout);

    fprintf(stderr,"********************************** \n Suche Abgeschlossen!!! \n ");
    if (accumhisto==1){

        maxhisto=0;
        for(j=1;j<binanzahl+1;j=j+1) {
            if (histo[26][j]>maxhisto) {
                maxhisto=histo[26][j];
                maxindex=j;
            }
            // Warnung!! Immer nur Mitte de s Histogramms!
            //maxindex=200;
        }
```

```
        fprintf(stderr,"Maxhisto at index: %d, corresponding to time delay: %f ns.\n ",
    maxindex,((maxindex-(binanzahl/2)+1)*histwid/(binanzahl/2)*1e9 ));

        //fprintf(stderr,"Histoelements -+10 arround center: ");
        for(j=1;j<22;j=j+1) {
            //fprintf(stderr," %d, ",histo[maxindex+j-11]);
            }
        fprintf(stderr,"\n");

        //***** Take Values arround peak
        for(j=0;j<25;j=j+1) {
                coinc_matrix[1+j] = histo[1+j][maxindex] + histo[1+j][maxindex+1]+ histo[1+
    j][maxindex-1]+histo[1+j][maxindex+2]+histo[1+j][maxindex-2];
            }

        //**** Print coincidence table
        for(j=0;j<25;j=j+5) {
                fprintf(stderr,"%.7d %.7d %.7d %.7d %.7d\n",coinc_matrix[1+j],coinc_matrix
    [2+j],coinc_matrix[3+j],coinc_matrix[4+j],coinc_matrix[5+j]);
                }
        k=0;
        for(j=0;j<25;j++){
            k=k+(long)coinc_matrix[1+j];
            }
        fprintf(stderr,"Summe Koinzidenzen: %d \n",k);

        //Formatting the logfile for output

        j=sprintf(fname_out2, "%s_%s.csv", fname_out, "all");
        fprintf(stderr,"output_filename: %s \n",fname_out2);
        fout=fopen(fname_out2,"w");
        write_output_file(fout);
        fclose(fout);

    }

 fclose(falice);
 fclose(fbob);
 return 0;
}
```

C. VHDL-Code

Below is the VHDL code for implementing the FPGA logic, which sampled the random signal and provided the corresponding Pockels Cell signals (see section 6.2.8). This logic was implemented in a XC9536XL CPLD device from `Xilinx`, using the Foundation Express software from `Xilinx`.

C.1. Source code: compar.vhd

```
1         library IEEE;
2         use IEEE.std_logic_1164.all;
3         use IEEE.STD_LOGIC_ARITH.ALL;
4         use IEEE.STD_LOGIC_UNSIGNED.ALL;
5
6
7         -- produces correct pockels cell signals for switching between
8         -- +/- and H/V analyzer basis triggert by QRNG
9
10        entity compar is
11            port (
12                d: in STD_LOGIC_VECTOR(0 to 7);
13                clk: in STD_LOGIC;
14                sel: in STD_LOGIC_VECTOR (0 to 1);
15                pcsequence: inout STD_LOGIC_VECTOR (0 to 7)
16
17                );
18
19        end compar;
20
21        architecture compar_arch of compar is
22
23        signal dtemp: STD_LOGIC_VECTOR (0 to 7):="00000000";
24        signal sample_rate: STD_LOGIC_VECTOR (0 to 7):="00000101";
25        signal counter: STD_LOGIC_VECTOR (5 downto 0):="000000";
26        signal counter2: STD_LOGIC_VECTOR (5 downto 0):="000000";
27        signal temp: STD_LOGIC:='0';
28        begin
29          p1: process (clk)
30          begin
31
32          if (clk'event and clk='1') then
33              -- input data structure: 1 Bit: QRNG signal
34
35            counter<=counter+1;
36            counter2<=counter2+1;
37
38            if (sel="11") then
39
40
41        -- bipolar pockels cell mode; pockels cell triggert by QRNG
42        -- output data structure: 4 Bits for Pockels Cell Sequence
43        -- and 2 Bits for Pockels Cell State:
44        -- output: pockels cell signals:
45        -- (1)A_on (2)B_on (3)A_off (4)B_off (5)not used (6)sample pulse
46        -- (7)PC_state_+V (+/- basis) (8)PC_state_-V (H/V basis)
47
48
49                    if (counter=sample_rate) then             -- input signal (QRNG) is sampled
50                       if (d/=dtemp) then                     -- with sample_rate
51                           if (d="00000000") then
52                              pcsequence<="01100100";         -- B_on, A_off, sample pulse
53                              dtemp<="00000000";
54                           elsif (d="10000000") then
55                              pcsequence<="10010100";         -- A_on, B_off, sample pulse
56                              dtemp<="10000000";
57                           end if;
58                       else
59                           pcsequence<=(pcsequence or "00000100");  -- leave as it was
60                       end if;
61                    elsif (counter=sample_rate+1) then     -- PC_state output
```

```
 62                                                      -- is delayed for one clock cycle
 63                         counter<="000000";                   -- reset counter
 64                     if (dtemp="00000000") then
 65                         pcsequence<="00000001";          -- PC_state_-V (H/V
        basis)
 66                     elsif (dtemp="10000000") then
 67                         pcsequence<="00000010";          -- PC_state_+V (+/-
        basis)
 68                     end if;
 69                  end if;
 70
 71
 72
 73
 74             elsif (sel="00") then                              -- bipolar mode
 75
 76                    if(counter2="000000" and temp='0') then
 77                        pcsequence<= "10010000";
 78                    elsif(counter2="000001" and temp='0') then
 79                        --temp<='1';
 80                        counter2<="000000";
 81                        pcsequence<= "01100000";
 82                    --elsif (counter2="000000" and temp='1')then
 83                        --pcsequence<= "00100000";
 84                   -- elsif (counter2="000001" and temp='1')then
 85                     -- temp<='0';
 86                        --pcsequence<= "00010000";
 87                    --else
 88                        --pcsequence<="00000000";
 89                    end if;
 90
 91
 92
 93             elsif (sel="10") then     -- unipolar positive mode (+/- basis)
 94
 95                    if(counter2="000000" and temp='0') then
 96                        pcsequence<= "10000010";
 97                    --elsif(counter2="000001" and temp='0') then
 98                        --pcsequence<= "00000010";
 99                    elsif(counter2="000011" and temp='0') then
100                        temp<='1';
101                        pcsequence<= "01000000";
102                    elsif (counter2="000000" and temp='1')then
103                        pcsequence<= "00010010";
104                    --elsif (counter2="000001" and temp='1')then
105                        --pcsequence<= "00000010";
106                    elsif(counter2="000011" and temp='1') then
107                        temp<='0';
108                        pcsequence<= "00100000";
109                    elsif(counter2<="000011") then
110                        pcsequence<="00000010";
111                    else
112                        pcsequence<="00000000";
113                    end if;
114
115
116
117             elsif (sel="01") then      -- unipolar negative mode (H/V basis)
118
119                    if(counter2="000000" and temp='0') then
120                        pcsequence<= "01000000";
```

```
121                     elsif(counter2="000001" and temp='0') then
122                         temp<='1';
123                         pcsequence<= "10000000";
124                     elsif (counter2="000000" and temp='1')then
125                         pcsequence<= "00100000";
126                     elsif (counter2="000001" and temp='1')then
127                         temp<='0';
128                         pcsequence<= "00010000";
129                     else
130                         pcsequence<="00000000";
131                     end if;
132
133
134               end if;
135              end if;
136
137
138
139
140             end process p1;
141
142
143            end compar_arch;
144
145
146
147
148
149
150
151
152
```

Bibliography

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

[2] 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.

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

[4] P. Pearle. Hidden variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, 1970.

[5] X. Ma, C.-H. F. Fung, and H.-K. Lo. Quantum key distribution with entangled photon sources. *Phys. Rev. A*, 76:012307, 2007.

[6] M. Aspelmeyer, M. Pfennigbauer, T. Jennewein, R. Kaltenbaek, M. Lindenthal, H. R. Böhm, J. Petschinka, R. Ursin, C. Brukner, W. Leeb, and A. Zeilinger. Quantum communications in space. Technical Report under contract 16358/02, ESTEC/Contract No. 16358/02/NL/SFe, 2003.

[7] R. Kaltenbaek, M. Aspelmeyer, M. Pfennigbauer, T. Jennewein, C. Brukner, W. R. Leeb, and A. Zeilinger. Proof-of-concept experiments for quantum physics in space. *Proc. of SPIE*, 5161:252–268, 2003.

[8] D. Deutsch and E. Ekert. Quantum computation. *Phys. World*, 11:47–52, 1998.

[9] P. Walther, K. Resch, T. Rudolph, E. Schenck, H. Weinfurterand V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 301:621–623, 2005.

[10] R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445:65–69, 2006.

[11] P. W. Shor. Algorithms for quantum computation: discrete log and factoring. Preprint, 1994.

[12] C. H. Bennett and G. Brassard. Quantum cryptography. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, page 175, New York, 1984. IEEE.

[13] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[14] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[15] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin. *J. Cryptology*, 5:3, 1992.

[16] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Phys. Rev. Lett.*, 84:4729, 2000.

[17] R. J. Hughes, J. E. Nordholt, D. Derkacs, and G.Peterson. Practical free-space quantum key distribution over 10 km in daylight andat night. *New Journal of Physics*, 4:43, 2002.

[18] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics*, 4:41.1–41.8, 2002.

[19] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, 2007.

[20] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantrum communication over 144 km. *Nature Physics*, 3:481 – 486, 2007.

[21] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer. Daylight operation of a free space, entanglement-based quantum key distribution system. *arXive*, 0812.1880v1, 2008.

[22] P. G. Kwiat, H. Eberhard, Philippe, A. M. Steinberg, and R. Y. Chiao. Proposal for a loophole-free bell inequality experiment. *Phys. Rev. A*, 49:3209, 1994.

[23] R. Garcia-Patron, J. Fiurasek, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier. Proposal for a loophole-free bell test using homodyne detection. *Phys. Rev. Lett.*, 93:130409, 2004.

[24] C. Simon and W. T. M. Irvine. Robust long-distance entanglement and a loophole-free bell test with ions and photons. *Phys. Rev. Lett.*, 91:110405, 2003.

[25] J. Volz, M. Weber, D. Schlenk, W. Rosenfeld, J. Vrana, K. Saucke, C. Kurtsiefer, and H. Weinfurter. Observation of entanglement of a single photon with a trapped atom. *Phys. Rev. Lett.*, 96:030404, 2006.

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

[27] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28(14):938–941, 1972.

[28] E. S. Fry and R.l C. Thompson. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 37:465–468, 1976.

[29] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: A new violation of Bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, 1982.

[30] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25):1804–1807, 1982.

[31] Z. Y. Ou and L. Mandel. Violation of Bell's inequality and classical probability in a two-photon correlation experiment. *Phys. Rev. Lett.*, 61(50):50–53, 1988.

[32] Y. H. Shih and C. O. Alley. New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion. *Phys. Rev. Lett.*, 61(26):2921–2924, 1988.

[33] P. R. Tapster, J. G. Rarity, and P. C. M. Owens. Violation of bell's inequality over 4 km of optical fiber. *Phys. Rev. Lett.*, 73:1923, 1994.

[34] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, and A. V. Sergienkoand Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337–4342, 1995.

[35] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.*, 81:3563, 1998.

[36] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of bell's inequality under strict Einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043, 1998.

[37] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409:791 – 794, 2001.

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

[39] R. Prevedel. Experimental realization of a simple entangling gate for quantum computation. Master's thesis, University of Vienna, Austria, October 2005.

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

[41] V. Buzek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54:1844–52, 1996.

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

[43] S. G. G. Stokes. On the composition and resolution of streams of polarized light from different sources. *Trans. Cambridge Philos. Soc.*, 9, 1852.

[44] D. F. V. James, P. G. Kwiat, W. J.Munro, and A. G. White. Measurement of qubits. *Phys. Rev. A*, 64:52312, 2001.

[45] S. Hill and W. K. Wootters. Entanglement of a pair of quantum bits. *Phys. Rev. Lett.*, 78:5022–5025, 1997.

[46] W. K. Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245–2248, 1998.

[47] J. S. Bell. *Foundations of Quantum Mechanics*. New York: Academic, 1971.

[48] J. F. Clauser and M. A. Horne. Experimental consequences of objective local theories. *Phys. Rev. D*, 10(2):526–535, 1974.

[49] A. Fine. Hidden variables, joint probabilities, and the bell inequalities. *Phys. Rev. Lett.*, 48:291–295, 1982.

[50] J. F. Clauser and A. Shimony. Bell's theorem: experimental tests and implications. *Rep. Prog. Phys.*, 41:1881–1927, 1978.

[51] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 48:696–702, 1935.

[52] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky. *Phys. Rev.*, 108(4):1070–1076, 1957.

[53] J. Von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Springer, Berlin, 1932.

[54] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.*, 38:447–452, 1966.

[55] D. Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. I. *Phys. Rev.*, 85(2):166–179, 1952.

[56] D. Bohm. A suggested interpretation of the quantum theory in terms of "hidden" variables. II. *Phys. Rev.*, 85(2):180–193, 1952.

[57] J. S. Bell. Introduction to the hidden-variable question. In B. D'Espagnat, editor, *Foundations of Quantum Mechanics*, pages 171–181, New York, 1971. Academic.

[58] J. P. Jarrett. On the physical significance of the locality conditions in the bell argument. *Noûs*, 18:569–589, 1984.

[59] A. Garg and N.D. Mermin. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Phys. Rev. D*, 35(12):3631–5, 1987.

[60] A. Zeilinger. Testing Bell's inequalities with periodic switching. *Phys. Lett. A*, 118(1):1–2, 1986.

[61] S. Groeblacher, T. Paterek, R. Kaltenbaek, C. Brukner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger. An experimental test of non-local realism. *Nature*, 446:871–875, 2007.

[62] A. J. Leggett. Nonlocal hidden-variable theories and quantum mechanics: An incompatibility theorem. *Found. Phys.*, 33:1469–1493, 2003.

[63] Morton H. Rubin, David N. Klyshko, Y. H. Shih, and A. V. Sergienko. Theory of two-photon entanglement in type-ii optical parametric down-conversion. *Phys. Rev. A*, 50(6):5122–5133, 1994.

[64] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger. A wavelength-tunable, fiber-coupled source of narrowband entangled photons. *Optics Express*, 15:15377–15386, 2007.

[65] T. Kim, M. Fiorentino, and F.N.C. Wong. Phasestable source of polarizationentangled photons using a polarization sagnac interferometer. *Phys. Rev. A*, 73:12316, 2006.

[66] A. Fedrizzi. *Fundamental experiments with a high brightness source of entangled photons*. PhD thesis, University of Vienna, 2008.

[67] T. Jennewein, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Rev. Sci. Instrum.*, 71:1675–1680, 2000.

[68] L. Mandel and E. Wolf. *Optical Coherence and Quantum Optics*. Cambridge University Press, Cambridge, 1995.

[69] A. Compagner. *Am. J. Phys.*, 59:700, 1991.

[70] V. A. Uspenskii, A. L. Semenov, and A. K. Shen. Can an individual sequence of zeros and ones be random? *Russian Math. Surveys*, 45:121, 1990.

[71] E. Hecht. *Optik*. Addison-Wesley (Deutschland) GmbH, 1989.

[72] F. Pockels. *Lehrbuch der Kristalloptik*. Leipzig, 1906.

[73] F. Agullo-Lopez, J. M. Cabrera, and F. Agullo-Rueda. *Electrooptics*. Academic Press, 1994.

[74] D. K. Killinger, J. H. Churnside, and L. S. Rothman. *Atmospheric Optics, OSA Handbook of Optics, Chapter 44.* McGraw-Hill, 1995.

[75] A. Yariv. *Quantum Electronics.* John Wiley, New York, 3rd edition, 1989.

[76] T. Schmitt-Manderbach. *Long distance free-space quantum key distribution.* PhD thesis, Ludwig-Maximilians-Universität München, 2007.

[77] J. A. Curcio, L. F. Drummeter, and G. L. Knestrick. An atlas of the absorption spectrum of the lower atmosphere from 5400 a to 8520 a. *Applied Optics*, 3:1401–1409, 1964.

[78] A. N. Kolmogorov. The local structure of turbulence in an incompressible viscous fluid for very large reynolds numbers. *C. R. (Doki) Acad. Sci. U.S.S.R.*, 30:301–305, 1941.

[79] L.C.Andrews and R.L.Phillips. *Laser Beam Propagation Through Random Media.* SPIE - The International Society for Optical Engineering, 1998.

[80] R. E. Hufnagel. *Propagation through atmospheric turbulence.* The Infrared Handbook, Chap. 6, 1974.

[81] P. B. Ulrich. *Hufnagel-Valley profiles for specified values of the coherence length and isoplanatic angle.* MA-TN-88-013, 1988.

[82] G. C. Valley. Isoplanatic degradation of tilt correction and short-term imaging systems. *Appl. Opt.*, 19:574, 1980.

[83] J. H. Churnside and R. J. Lataitis. Wander of an optical beam in the turbulent atmosphere. *Applied Optics*, 29:926, 1990.

[84] D.L.Fried. Optical resolution through a randomly inhomogeneous medium for very long and very short exposures. *Journal of the Optical Society of America*, 56:1372–1379, 1966.

[85] A. Comeron, J. A. Rubio, and A. Belmonte. Astc inter-island measurement campaign final report. Technical report, Technical University of Catalonia, 1996.

[86] T. Scheidl. Methoden fürFree-Space Quantenkommunikationsexperimente. Master's thesis, University of Vienna, 2005.

[87] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity. A step towards global key distribution. *Nature*, 419:450, 2002.

[88] D. H. Höhn. Depolarization of a laser beam at 6328 a due to atmospheric transmission. *Applied Optics*, 8:367–369, 1969.

[89] J. N. Bradford and J. W. Tucker. A sensitive system for measuring atmospheric depolarization of light. *Applied Optics*, 8:645–647, 1969.

[90] R. G. W. Brown, R. Jones, J. G. Rarity, and K. D. Ridley. Characterization of silicon avalanche photodiodes for photon correlation measurements. 2: Active quenching. *Appl. Opt.*, 26(12):2383–2389, 1987.

[91] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Applied Optics-LP*, 35:1956–1976, 1996.

[92] H. Dautet, P. Deschamps, B. Dion, A. D. MacGregor, D.e MacSween, R. J. McIntyre, C. Trottier, and P. P. Webb. Photon counting techniques with silicon avalanche photodiodes. *Applied Optics-LP*, 32:3894 – 3900, 1993.

[93] T. Bergmann. Electrooptical modulator / pockels cell driver models pcdpp and pcddpp. Technical report, Bergmann Messgeräte, D-82418 Murnau, 2005.

[94] N. Goldovsky and M. Luria. Ionospheric delay contribution to the uncertainty of time and frequency measurements by one-way satellite time transfer method. *Science Direct*, 35:353–362, 2004.

[95] R. Penrose. On gravity's role in quantum state reduction. *Gen. Rel. Grav.*, 28:581, 1996.

[96] D. Salart, A. Baas, J. A.W. van Houwelingen, N. Gisin, , and H. Zbinden. Spacelike separation in a bell test assuming gravitationally induced collapses. *Phys. Rev. Lett.*, 100:220404, 2008.

[97] T. Jennewein. *Quantum Communication and Teleportation Experiments using Entangled Photon Pairs*. PhD thesis, University of Vienna, 2002.

[98] A. E. Lita, A. J. Miller, and S. W. Nam. Counting near-infrared single-photons with 95% efficiency. *Optics Express,*, 16:3032–3040, 2008.

[99] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Am. Inst. Elec. Eng.*, 55:109, 1926.

[100] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74(1):145–195, Mar 2002.

[101] H.-K. Lo and Y. Zhao. Quantum cryptography. *Encyclopedia of Complexity and System Science (to be published by Springer)*, 2008.

[102] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Luetkenhaus, and M. Peev. The security of practical quantum key distribution. *arXiv:0802.4155v2 [quant-ph]*, 2008.

[103] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91(5):057901, Aug 2003.

[104] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Physical Review Letters*, 98(1):010505, 2007.

[105] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A.a Tomita. Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics. *arXiv:0705.3081*, 2007.

[106] C. Erven, C. Couteau, R. Laflamme, and G. Weihs. Entangled quantum key distributionover two free-space optical links. *Opt. Express*, 16(21):16840–16853, 2008.

[107] F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88(5):057902, Jan 2002.

[108] M. Legre, H. Zbinden, and N. Gisin. *Quantum Inf. Comput.*, 6:326, 2006.

[109] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 76(4):042305, 2007.

[110] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Physical Review A (Atomic, Molecular, and Optical Physics)*, 76(5):052323, 2007.

[111] G. Brassard and L. Salvail. Eurocrypt '93: Workshop on the theory and application of cryptographic techniques on advances in cryptology. In *Lecture Notes in Computer Science*, volume 765, pages 410–423, New York, 1994. Springer.

[112] R. G. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, IT-8:21–28, 1962.

[113] D. Pearson. High-speed qkd reconciliation using forward error correction. In *The 7th International Conference on Quantum Communications, Measurement, and Computing*, 2004.

[114] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Comput*, 17:210–229, 1988.

[115] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, 2000.

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

[117] C. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. I. Information boundand optimal strategy. *Phys. Rev. A*, 56:1163–1172, 1997.

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

[119] G. Brassard, N. Luetkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, 2000.

[120] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, 94(23):230503, 2005.

[121] H.-K. Lo, X.-F. Ma, and K. Chen. Decoy state quantum key distribution. *Physical Review Letters*, 94(23):230504, 2005.

[122] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992.

[123] Masato Koashi and John Preskill. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.*, 90(5):057902, Feb 2003.

[124] Romain Alleaume, Jan Bouda, Cyril Branciard, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Langer, Anthony Leverrier, Norbert Lutkenhaus, Philippe Painchault, Momtchil Peev, Andreas Poppe, Thomas Pornin, John Rarity, Renato Renner, Gregoire Ribordy, Michel Riguidel, Louis Salvail, Andrew Shields, Harald Weinfurter, and Anton Zeilinger. Secoqc white paper on quantum key distribution and cryptography. 2007.

[125] Harald Weinfurter and Marek Zukowski. Four-photon entanglement from down-conversion. *Phys. Rev. A*, 64:010102, 2001.

[126] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, 1998.

[127] Bo Zhao, Yu-Ao Chen, Xiao-Hui Bao, Thorsten Strassel, Chih-Sung Chuu, Xian-Min Jin, Jörg Schmiedmayer, Zhen-Sheng Yuan, Shuai Chen, and Jian-Wei Pan. A millisecond quantum memory for scalable quantum networks. *Nature Physics*, 2008.

[128] Mikael Afzelius, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Multimode quantum memory based on atomic frequency combs. pages arXiv:0805.4164v2 [quant–ph], 2008.

[129] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons 1509 200. Practical quantum cryptography for secure free-space communications. *Proc. QCQC 98*, 1509:200, 1999.

[130] R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, and L. Cacciapuoti *et al.* Spacequest: Experiments with quantum entanglement in space. *arXiv:0806.0945*, 2008.

[131] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger. High-fidelity transmission of entanglement over a high-loss freespace channel. *arXiv:0902.2015v1*, 2009.

[132] V. Makarov and D. R. Hjelme. Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, 52:691–705, 2005.

[133] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. In *IEEE Journal of Selected Topics in Quantum Electronics 1541-1551*, 2003.

[134] M. Aspelmeyer. Spacequest: Quantum entanglement in space experiments. *ESA-AO-2004*, 2004.

[135] G. Neckamm M. Aspelmeyer T. Jennewein F. Tiefenbacher A. Zeilinger G. Baister K. Kudielka T. Dreischer M. Pfennigbauer, W. R. Leeb and H. Weinfurter. Accommodation of a quantum communication transceiver in an optical terminal (accom): final report. Technical report, European Space Agency Contract Report, ESTEC, Contract 17766/03/NL/PM, 2005.

D. Acknowledgements

The experiments described in this thesis would not have been possible without the help of so many people. Now it is time to thank all those who made this dissertation finally happen:

First of all I thank my supervisor Rupert Ursin for his scientific support during my whole time as a PhD student. I am grateful that after all the great time we spent together in the office, in the laboratory and on the Canaries my "Chef" also became a dear friend.

I want to express my gratitude to Prof. Anton Zeilinger for providing a research environment of unequaled opportunities and for his enthusiasm for the experiments on the Canaries.

I am thankful to Johannes Kofler for his theoretical and experimental support, for proofreading the first part of this thesis, for the invitation to his promotion *sub auspiciis* but most of all for the many enlightening discussions about whatsoever.

I am greatly indebted to the whole Canary '08 team for their devotional support before, during and after our stay on the Canaries: to Sven Ramelow and Lothar Ratschbacher for building the best windbreak for the transmitter telescope, to Xiao-Song Ma and Thomas Herbst for bravely adjusting the optical setup in the OGS's "pizza oven", to Nathan Langford for his patience and commitment when writing the paper, to Alessandro Fedrizzi for his extraordinary bright entangled photon source and to Thomas Jennewein for his ingenious programming skills and his excellent expertise in electronic engineering.

Thanks to F. Sanchez and A. Alonso, T. Augusteijn, C. Perez and the staff of the Nordic Optical Telescope (NOT), J. Kuusela, Z. Sodnik and J. Perdigues of the Optical Ground Station (OGS) as well as J. Carlos and the staff of the Residence of the Observatorio del Roque de Los Muchachos for their support at the trial sites.

Special thanks to Robert Prevedel for many motivating conversations about the life as a physicist and for his company during the many hours of sporting activities.

Last but not least I want to thank my family for their unconditional support throughout all the years, my girlfriend Alex for her love and understanding during my stay at the Canaries and my friends for always providing a most welcome alternation from workaday life.

Thomas Scheidl, March 2009

E. List of Publications

Articles in refereed journals

- T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter.
  Experimental demonstration of free-space decoy-state quantum key distribution over 144 km
  Phys. Rev. Lett. **98**, 010504 (2007).

- R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger.
  Entanglement-based quantum communication over 144 km
  Nature Physics **3**, 481-486, (2007).

- A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, A. Zeilinger
  High-fidelity transmission of entanglement over a high-loss freespace channel
  Nature Physics (accepted February 2009); arXiv:0902.2015 [quantph].

Submitted

- T. Scheidl, R. Ursin, J. Kofler, S. Ramelow, X.-S. Ma, T. Herbst, L. Ratschbacher, A. Fedrizzi, N. K. Langford, T. Jennewein, A. Zeilinger
  Violation of local realism with freedom of choice
  submitted to Nature Physics (2009); arXiv:0811.3129 [quantph].

- T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein and A. Zeilinger
  Feasibility of 300 km Quantum Key Distribution with Entangled States
  submitted to New Journal of Physics (2009).

Proceedings

- R. Ursin, T. Jennewein, J. Kofler, J. M. Perdigues, L. Cacciapuoti, C. J. de Matos, M. Aspelmeyer, A. Valencia, T. Scheidl, A. Fedrizzi, A. Acin, C. Barbieri, G. Bianco, C. Brukner, J. Capmany, S. Cova, D. Giggenbach, W. Leeb, R. H. Hadfield, R. Laflamme, N. Lutkenhaus, G. Milburn, M. Peev, T. Ralph, J. Rarity, R. Renner, E. Samain, N. Solomos, W. Tittel, J. P. Torres, M. Toyoshima, A. Ortigosa-Blanch,

V. Pruneri, P. Villoresi, I. Walmsley, G. Weihs, H. Weinfurter, M. Zukowski, A. Zeilinger
Space-QUEST: Experiments with quantum entanglement in space
Accepted for the 59th International Astronautical Congress (2008); arXiv:0806.0945v1 [quantph].

F. Curriculum vitae

Curriculum vitae

Mag. Thomas Scheidl
Högelmüllergasse 6/11
1050 Wien

Mobile: +43-676-962-81-53
Email: thomas.scheidl@univie.ac.at
Mailing address: Boltzmanngasse 3, A-1090 Vienna, Austria
Current position: PhD student
Institute for Quantum Optics and Quantuminformation (IQOQI)
Austrian Academy of Sciences

Personal Data

Born	20. November 1979 in Vienna, Austria
Parents	Mag. Kurt Scheidl and Dr. Brigitte Scheidl

Education

1986 - 1990	Volksschule Pabneukirchen
1990 - 1994	Hauptschule Pabneukirchen
1994 - 1998	BORG Perg, branch for natural sciences (Matura in June 1998)
1999 - 2004	Diploma studies of experimental physics, Faculty for Physics, Univerity of Vienna
2004 - 2005	Diploma thesis within the group of Prof. Anton Zeilinger: „*Methoden für Free-Space Quantenkommunikationsexperimente*“
2006 - 2008	PhD studies within the group of Prof. Anton Zeilinger. Thesis: *„A fundamental test and an application of quantum entanglement“*

Research activities

2004-2005	Measurement campaign on an inter-city optical free-space link in Vienna
2005 - 2008	Measurement campaign on the Canary islands of La Palma and Tenerife at ESA‘s Optical Ground Station (OGS), Tenerife, Spain
2006-2007	Development of a fs-pulsed source of non-degenerate entangled photons for multi-photon experiments

Languages

German	Native language
English	Fluent in spoken and written
French	Basics in spoken
Latin	Basics in written