Quantum Communication and Teleportation Experiments using Entangled Photon Pairs

Dissertation zur Erlangung des Grades “Doktor der Naturwissenschaften”

eingereicht von

Mag. Thomas Daniel Jennewein
Institut für Experimentalphysik
der Universität Wien

durchgeführt bei

o. Univ. Prof. Dr. Anton Zeilinger

11th June 2002

Gefördert vom Fonds zur Förderung der wissenschaftlichen Forschung, Projekt Nr. SFB1506, und durch die Europäische Kommission.
## Contents

1 Abstract 7

2 Introduction 9

3 The Basics of Qubits and Quantum Information 11
   3.1 Entanglement .................................. 11
   3.2 Bell’s inequality ................................ 12
   3.3 The qubit .................................... 12
      3.3.1 Polarization of Photons as qubits .......... 13
      3.3.2 Bloch sphere and Poincaré sphere .......... 14
   3.4 Bell-states .................................... 14
   3.5 No-cloning theorem for qubits ................. 15

4 Quantum Key Distribution 17
   4.1 Concept ..................................... 17
   4.2 The Vernam-One-Time-Pad protocol ............. 17
   4.3 Quantum Key Distribution ........................ 18
      4.3.1 Single Qubits: BB84 scheme ................ 19
      4.3.2 Entangled Qubits: Ekert Scheme .......... 21
   4.4 Quantum Key Distribution with Entangled Photons 22
      4.4.1 Adopted BB84 Scheme .................... 22
      4.4.2 Adopted Ekert Scheme .................... 23

5 Quantum Key Distribution in Experiment 25
   5.1 The Hardware of the QKD System ................. 25
      5.1.1 The Optics ................................ 25
      5.1.2 Photon Registration and Coincidence Determination 26
      5.1.3 Performance of the System ............... 27
   5.2 Classical Communication of QKD .................. 27
      5.2.1 Key Sifting ................................ 27
      5.2.2 Security Check ............................ 30
      5.2.3 Simple Classical Error Correction ......... 30
   5.3 Encoding Software ................................ 31
   5.4 Experimental Results and Discussion ........... 31
      5.4.1 Adopted BB84 scheme .................... 32
5.4.2 Adopted Ekert scheme (Wigner’s inequality) .................. 33
5.4.3 Advantages of QKD based on Entanglement .................. 33
5.4.4 Outlook ........................................ 33

6 Quantum State Teleportation and Entanglement Swapping .......... 35
  6.1 Quantum State Teleportation Theory .......................... 35
  6.1.1 The Speed of Quantum State Teleportation .................. 37
  6.1.2 Quantum Nature of Quantum State Teleportation? ............ 37
  6.2 Entanglement Swapping .................................... 38

7 Entanglement Swapping in Experiment ............................ 41
  7.1 Interferometric Bell-state Analysis ........................... 41
  7.1.1 Implementation of the Bell-state Analyzer .................. 42
  7.2 The Entanglement Swapping Setup .............................. 43
  7.2.1 The Coincidence Logic .................................. 45
  7.2.2 The fs-Pulse UV-Laser system ............................. 47
  7.2.3 Adjustment and Performance of the Setup ................... 52
  7.2.4 Scans for Testing the System Alignment .................... 52
  7.3 Limits to the 4-fold Correlation Visibility .................... 54
  7.4 Experimental Results and Discussion ........................... 55
  7.4.1 Correlation Measurements for the swapped Entanglement .... 55
  7.4.2 The Timing-“Paradox” of Entanglement Swapping ............ 57
  7.4.3 Experimental Violation of Bell’s inequality .................. 58
  7.4.4 Some Deficiencies of this Teleportation Setup ............... 59
  7.4.5 Independence of the two Photon Pairs? ...................... 60
  7.4.6 What about the Classical Teleporter? ....................... 61

8 Towards More-Complete Teleportation with Switched Modulator ...... 63
  8.1 Implementation of the more-complete Bell-state Analyzer ........ 63
  8.2 Modulating the Receiving Photon ............................. 65
  8.3 The Programmable Coincidence Logic .......................... 67
  8.4 Progress of the Experiment .................................... 69

9 Concluding Outlook and Visions ................................... 71
  9.1 Entanglement-based Quantum Key Distribution .................. 71
  9.2 Entanglement Swapping and Quantum State Teleportation ........ 72

A Spontaneous Parametric Down-conversion .......................... 75
  A.1 Generation of polarization entangled photons with type-II SPDC in BBO 76
  A.2 Geometry of the down-conversion light ........................ 76
  A.3 Compensation of the walk-off effects in BBO .................... 78
  A.4 The state produced by down-conversion ........................ 80
    A.4.1 Visibility Reduction for SPDC from a fs-pulse Pump ....... 80

B The Fiber-based Quantum Channel ................................ 83
J  Curriculum Vitae 141
1 Abstract

This work describes experiments using entangled photons which demonstrate quantum key distribution and entanglement swapping, both being key parts of the new field called quantum communication.

Based on the famous Einstein-Podolksy-Rosen “paradox” [EPR35], the search for reality within or underneath the quantum world has troubled many minds over decades. Amongst the exciting findings in this quest are e.g. Bell’s theorem [Bel64], which shows contradictions between local realistic theories and quantum mechanics in describing quantum entanglement, or the notion of objective randomness, which accompanies the quantum measurement process. Quantum information exploits these issues for its fundamentally new communication and computation technologies, such as quantum cryptography, quantum teleportation or quantum computation, of which some were already shown in experiment. With today’s technology it is possible to perform experiments which at least demonstrate some of these ideas and concepts.

First the achievement of experimental quantum key distribution based on entangled photons over \(\approx 350 \text{ m}\) will be shown, and an image will be transmitted securely over this distance. In this variant of quantum key distribution the security rests on the incompatibility of local realism with quantum mechanics. Second, the realization of quantum teleportation and entanglement swapping, which is an important “workhorse” for quantum communication, will be described. The means for achieving high experimental fidelities will be developed. Consequently a test of Bell’s inequality for the entanglement swapped photons is performed, which shows a significant violation of the limit imposed by local realistic theories. This is the first experimental violation of Bell’s inequality for photons that never interacted. Apart from representing a step towards quantum communication applications, this result also demonstrates the quantum nonlocality of quantum teleportation. In a separate experiment the seemingly paradoxical space time ordering of the measurement events in the entanglement swapping experiment will be realized, i.e. that the entangling measurement is performed after the two to be entangled photons are registered. However the experimental results still show good agreement with the predictions of quantum mechanics. Finally the means for expanding the teleportation setup with a “More-Complete Bell-State Analyzer” and an electro-optic modulator for performing the unitary operation required on the receiver photon are presented.
Abstract
2 Introduction

My motivation for the experiments presented in the scope of this PhD-thesis is manifold and can be seen from quite different standpoints, which made this work gripping and intriguing. Let me explain:

**Quantum Reality** One the one hand, these experiments highlight the nature of quantum mechanics and are definitely interesting from a philosophical point of view. Or simpler, it is just that these experiments illustrate the basic ideas and the essential mind twisters such as superposition and entanglement in quantum systems in a rather clear way allowing even the enthusiastic quantum hobbyist (and a simple minded experimentalist like myself) to grasp. If one considers the correlation which occurs for two quantum entangled photons, then there is a discrepancy between the understanding these correlations with local realistic concepts and calculating the correlations with quantum mechanics. This difference of the two theories, known as Bell’s theorem, is already disturbing enough for standard intuition, but the situation becomes even tougher in the case of entanglement swapping, where finally entanglement between photons that never interacted is observed! So the work on such experiments does involve something magical and mystical, or as Christoph Simon put it: “Bell’s theorem really puts physics back to philosophy.”

**Future Applications of Quantum Information** Then, on the other hand, these experiments are within the new field of quantum information processing. Presently, of course, we are nowhere near realizing the visions of a “quantum information” society, but at least we can build model systems which allow to play around today with this technology of tomorrow (or the day after). The visions will become true if we can stretch the transmission of photons across the planet, for instance via Satellites, or when we are able to store entanglement for long times (days or even longer). Then we’ll be able to carry the particles around and at any time and place use it to perform quantum key distribution for secure communication, or quantum state teleportation for interconnecting quantum computers, etc.. The experiments I present here demonstrate fascinating quantum communication applications, which one day could be an ubiquitous technology. However, it is very exciting to be able to demonstrate quantum communication ideas for the first time.

**Fun** But just as important for me is the fun I have when setting up these experiments. I have always been a great handicraft enthusiast, starting in my early days with LEGO but soon extending my activities to bicycles, tree-huts, electric model trains...
and later to computers and electronics, before finally studying physics. So in our experiments, for me “the way is the target”\(^1\), and the actual goal of the experiments is only part of the game. I find it most enjoyable to design systems from scratch and always search for the simplest solution, which often also proves to be the best working (An example I’m quite proud of is the realization of a coincidence logic for correlated photons from two transistors and four resistors which replaced a set of NIM-modules). The only thing that can happen is, that I can easily get carried away in optimizing some details of an instrument or setup - so I must always keep my perfectionists tendencies under control. In my opinion, the experimental quantum physicist is nothing near to being a guru for practical esoterics, but more like a playful kid enjoying itself with LEGO.

For me, the work on these experiments which even is a combination of the above points, i.e. it is philosophical, has a potential application and is fun, is simply great, and I hope the reader will be able to feel this in the following description of my work.

I wish to note, that the work over all the years was certainly not as straight-lined as it might sound from the descriptions above. First I started on my PhD-program in Innsbruck, by assisting Gregor Weihs in the long-distance Bell experiment. Then, due to our transfer from Innsbruck to Vienna, many months were used up for organizing the packing and transfer of all the equipment in the old labs and arrange things in the new labs. Just after the experiments started to get running again in Vienna, I was called to the Austrian army for eight months, to complete the compulsory army service. Then I started to work on my actual thesis project, which was a long-distance teleportation experiment, which however did not quite realize, because I got involved with entanglement swapping and the work towards more-complete teleportation. However, the experiments I was able to perform are very interesting and I had a wonderful time in doing the work.

\(^1\)This is from the German saying "Der Weg ist das Ziel", as translated by the well renowned “Babel Fish Translation Service” on http://babelfish.altavista.com/tr.
3 The Basics of Qubits and Quantum Information

The new and exciting field of quantum communication is an important part of quantum information processing. This is because quantum communication offers new means of communication which have no resemblance in the classical world, and could one day be an ubiquitous technology. Furthermore, quantum communication is at present the experimentally most advanced aspect of quantum information processing, and first experiences using this technology can be performed. Quantum cryptography is already technically feasible and development of commercial systems is pursued at several institutions.

3.1 Entanglement

Strikingly, quantum information processing has its origins in the purely philosophically motivated questions concerning the nonlocality and completeness of quantum mechanics sparked by the work of Einstein, Podolsky and Rosen in 1935 [EPR35]. From thereon it took many years before John Bell in 1964 in his famous work [Bel64] showed a discrepancy between predictions for the correlations between entangled spin particles given by quantum mechanics and local realistic theories. The system of two spin-$\frac{1}{2}$ particles in the antisymmetric entangled state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$$

leave the individual particles with a completely undefined spin state, however defines their joint properties: i.e. the particles always have orthogonal quantum states without having individual states, no matter which measurement basis is chosen.

Up to now many experiments have been performed that demonstrate the violation of Bell’s inequality for entanglement for various types of particles: photons [CS78, AGR82, WJS+98, TBG+98], single ions [RKM+01], Rydberg atoms [HMN+97], single protons [LRM76], and even billions of Cs-Atoms [JKP01], just to name some examples, and many other systems may follow: e.g. Hg-Dimers [FWL95], electrons [BLS00], and soon maybe even kaons [BGH01]. The amount of theoretical and experimental work on entanglement is steadily growing, showing the relevance of this fundamental aspect in quantum mechanics.

In recent times even a range of applications of entanglement were developed, such as quantum cryptography, quantum state teleportation and quantum computation. Presently
it is still open, exactly where and to which extent quantum entanglement can enhance communication or computation procedures.

3.2 Bell’s inequality

Bell’s theorem states [Bel64], that the type of correlations given by entangled particles, which is predicted by quantum mechanics, can not be understood by assigning local hidden variables (sets of parameters the particles carry with them) which would determine their measurement results, i.e. the particles operate independently without any form of interaction between them. This is shown via an inequality for correlation measurements, which should be obeyed by systems which have a local realistic description. However, the correlations shown by entangled particles violate Bell’s inequality, as predicted by quantum mechanics as well as in experiments. It remains resolved, which of the assumptions in the derivation of Bell’s inequality must be discarded, locality or realism, or even both.

An experimentally very suitable version of Bell’s inequality is the CHSH-inequality, derived by Clauser, Horne, Shimony and Holt in 1969 [CHSH69]. It allows for experimental deficiencies such as the loss of particles or non-perfect state preparation. The CHSH-inequality has the following form:

\[ S = |E(a, b) + E(a', b')| + |E(a', b) - E(a', b')| \leq 2, \]  

where \( E(a, b) \) is the expectation value for the correlation measurement on particles 1 and 2, and \( a \) and \( b \) are the settings of particle’s 1 and 2 analyzer respectively. The quantum mechanical prediction of \( E(a, b) \) for photons in an polarization entangled state of the form shown in Equation 3.1 is \( E(a, b) = -\cos(a - b) \). For the settings \( a, a' = 0^\circ, 45^\circ \) and \( b, b' = 22.5^\circ, 67.5^\circ \) a maximal violation of Equation 3.2 is achieved, and \( S = 2\sqrt{2} \). Hence the quantum mechanical prediction of \( S \) clearly violates the limit given by local hidden variables.

A very comprehensible version of Bell’s inequality is Wigner’s version [Wig70]. This inequality will be used in the quantum key distribution experiment for checking the security of the quantum channel. The simple and intuitive derivation of Wigner’s inequality is given in Section 4.4.2.

3.3 The qubit

Motivated by the properties of spin-\( \frac{1}{2} \) particles the concept of the “qubit” was developed. A qubit can have two orthogonal states \( |0\rangle \) and \( |1\rangle \), which is analogous to the classical bit, the smallest unit of information, and has the values 0 or 1. The important difference of the qubit to the classical bit is that it can also have a state which is a superposition of the two basis states, in general:

\[ |Q\rangle = a|0\rangle + b|1\rangle \]  

Clearly the classical bit has no analogy to this superposition state. The physical realization of a qubit can be achieved by any two-state system, such as spins of electrons or nuclei,
polarization of photons, electronic states in atoms, etc. All these system have very different physical properties and dynamics which would make it difficult to detect and understand any "quantum information behaviour" of the system. Thus, based on qubits, theory can work with clean and easy systems using only simple mathematical tools, and bother about real implementations at a later time. This has opened the field of quantum information to experts from many other fields, e.g. mathematicians, cryptologists, computer scientists, who otherwise would certainly be overwhelmed by the vast amount of details of a physical system. The operations performed with single and multiple qubits and the associated algebra are described well in [BEZ00].

In terms of qubits, the entangled state for spins given in Equation (3.1) has the following form:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle).$$

(3.4)

### 3.3.1 Polarization of Photons as qubits

In all experiments presented in this work, qubits will be realized by the polarization of photons in the following way:

$$|0\rangle \rightarrow |H\rangle$$

(3.5)

$$|1\rangle \rightarrow |V\rangle$$

(3.6)

where $|H\rangle$ and $|V\rangle$ are photon states with horizontal and vertical polarization respectively, referenced to suitable local system for each photon, e.g. the plane of the optical table in the lab. Due to the linearity of quantum mechanics the general qubit-state has the form

$$a|0\rangle + b|1\rangle \rightarrow a|H\rangle + b|V\rangle,$$

(3.7)

Some distinct qubit states have a convenient representation and name in their corresponding polarization states, as shown in Table 3.1.

<table>
<thead>
<tr>
<th>Qubit State</th>
<th>Polarization State</th>
<th>Polarization Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>0\rangle$</td>
<td>$</td>
</tr>
<tr>
<td>$</td>
<td>1\rangle$</td>
<td>$</td>
</tr>
<tr>
<td>$\frac{1}{\sqrt{2}}(</td>
<td>0\rangle +</td>
<td>1\rangle)$</td>
</tr>
<tr>
<td>$\frac{1}{\sqrt{2}}(</td>
<td>0\rangle -</td>
<td>1\rangle)$</td>
</tr>
<tr>
<td>$\frac{1}{\sqrt{2}}(</td>
<td>0\rangle + i</td>
<td>1\rangle)$</td>
</tr>
<tr>
<td>$\frac{1}{\sqrt{2}}(</td>
<td>0\rangle - i</td>
<td>1\rangle)$</td>
</tr>
</tbody>
</table>

Table 3.1: A list of some qubit-states that correspond to a distinct polarization state of the photon. These states will be used throughout this work.
3 The Basics of Qubits and Quantum Information

3.3.2 Bloch sphere and Poincaré sphere

A very convenient representation of a qubit state is the Bloch sphere, see Figure 3.1. Any particular state $|Q\rangle$ is represented by a point on the surface of the sphere, which is addressed by the Bloch vector. The direction of the Bloch vector is defined by the complex amplitudes $a$ and $b$ of $|Q\rangle = a|0\rangle + b|1\rangle$. The norm of the vector is equal or less than one, and carries the purity of state. For a perfectly pure state, the norm will be one, and for a perfectly mixed state, the norm will be zero.

If the qubit states are expressed in the corresponding photon polarization states given in Table 3.1, the Poincaré sphere is obtained (see Figure 3.1). This is widely used for representing polarization in classical optics. All points on the equator of the Poincaré sphere represent linear polarization, the two poles circular polarization. The other polarization states are elliptical.

3.4 Bell-states

There are four distinct entangled states which form a basis in the Hilbert space of two qubits. These states are called Bell-states, and have the following form

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (3.8)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (3.9)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (3.10)$$
3.5 No-cloning theorem for qubits

\[ |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3.11} \]

Each of the Bell-states is a maximally entangled state and violates Bell’s inequality maximally.

**3.5 No-cloning theorem for qubits**

An important fact concerning qubits is that, provably, the exact quantum state of a single qubit can not be copied onto a different qubit while leaving the original qubit undisturbed. This is known as the no-cloning theorem, which was first shown up by Wooters and Zurek [WZ82]. The very obvious illustration of the no-cloning theorem is a simple copying device, which copies the state of a single qubit onto a separate blank qubit, and at the same time leaves the original qubit undisturbed. Let the machine perform the following operations:

\[ |0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \tag{3.12} \]
\[ |1\rangle|0\rangle \rightarrow |1\rangle|1\rangle \tag{3.13} \]

If the input qubit has a superposition state \( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \) then this machine will produce the following output due to the linearity of quantum mechanics:

\[ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{3.14} \]

an entangled state. However, the desired output of a working copying machine which should rather be:

\[ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{3.15} \]
\[ = \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \tag{3.16} \]

which is clearly different from expression (3.14). Therefore a general quantum cloning machine does not exist. But “approximate cloning” is possible, e.g. with the optimal procedure for general states given in [BH96]. A cloning device which has one input qubit in the state \( |\Psi\rangle \) which is transferred onto two identical output qubits, each in the mixed state \( \rho \) can achieve only a fidelity of about \( F = 0.82 \), where fidelity is defined as \( F = \langle \Psi | \rho | \Psi \rangle \).

Christoph Simon discovered in his PhD-thesis [Sim00, SWZ00] that optimal cloning can be realized using parametric down-conversion, which was recently demonstrated in the group of Bowmeester at Oxford (to be published soon).

But at the same time the no-cloning theorem is essential to quantum communication methods, as it provides the basis for the security of quantum cryptography, the necessity of quantum state teleportation for transferring quantum states between separate systems and also prohibits superluminal communication based on entangled systems [SBG01].
4 Quantum Key Distribution

4.1 Concept

The primary task of cryptography is to enable two parties (commonly called Alice and Bob) to mask confidential messages such that the transmitted data are illegible to any unauthorized third party (called Eve). Usually this is done using shared secret keys. However, in principle it is always possible to intercept classical key distribution unnoticedly. The recent development of quantum key distribution [BB84], also generally called quantum cryptography, can cover this major loophole of classical cryptography. It allows Alice and Bob to establish two completely secure keys by transmitting single quanta (qubits) along a quantum channel. The underlying principle of quantum key distribution is that nature prohibits to gain information on the state of a quantum system without disturbing it due to complementarity of certain observables of a system (or also via the no-cloning theorem, described in Section 3.5). Therefore, in appropriately designed protocols, no tapping of the qubits is possible without deceiving itself to Alice and Bob. These secure keys can be used in a One-Time-Pad protocol [Ver26], which makes the entire communication absolutely secure.

4.2 The Vernam-One-Time-Pad protocol

The encoding scheme developed by Vernam [Ver26] in 1926 is a very simple but effective method for highly secure cryptosystems. The idea is to use a secret key, of which both Alice and Bob hold a copy. The key must be “completely random”\(^1\) and have the same length as the transmitted message. If each bit of the secret key is used only once, then it is not possible to decipher the message by any statistical or numerical methods.

A simple implementation of the Vernam-One-Time-Pad is the bit-wise exclusive-or (XOR) operation of message and key. An example for encoding and decoding a short eight-bit message is given in Table 4.1.

The strength of the one-time-pad protocol is its simplicity. If an Eavesdropper tries to decrypt the message by guessing the key, her outcome will give any message without any

---

\(^1\)Complete randomness is a rather demanding requirement as a sequence of numbers can only be tested for its randomness at infinite lengths. Clearly, in practical systems this can not be accomplished and it must be assumed that the tested sample is a good representation of this infinite set. In this experiment a physical quantum random number generator was used, which is described in the PhD-thesis of Gregor Weihs [Wei99] and slightly more detail in [JWWZ00].
Table 4.1: A simple transmission of an eight-bit message from Alice to Bob via the one-time-pad protocol. The original message held by Alice is encoded by performing the exclusive-or (XOR) operation between the individual bits of the message and the key. The code is sent openly to Bob who decrypts the message by performing the very same XOR operation between the received code and his key. In this way Bob retrieves the original message. The required XOR operation has the following mapping of two input bits onto one output bit: 00 → 0, 01 → 1, 10 → 1, 11 → 0.

indication on which message is correct or wrong. Also each key must only be used once. If the same key were used twice for two separate transmissions, then the bit-wise XOR operation between the two encoded messages will give an overlay of the two messages, which may easily be untangled. However, the price to pay for the perfect security of the one-time-pad is that the key must be as long as the message, which leads to a large consumption of key material, and that key must only be used once. This coding scheme will be implemented later in a sample transmission performed in the quantum key distribution experiment described here.

Note, that the overall security of the one-time-pad rests completely on the key: A) the key must be perfectly random to avoid any statistical attacks, and B) the key must be transported to the participating parties. These two aspects are both hard to perform with classical means in a highly secure manner. This is because A) generating random signals or numbers is a very difficult task, and any deficiencies may allow for statistical attacks. For B), the transported keys can in principle be intercepted, copied, and sent on to the unsuspecting party, allowing the eavesdropper to listen to any communication between Alice and Bob which uses this key. It is these problems of key distribution that can be covered by implementing quantum key distribution, which use qubits for key generation and dissemination.

4.3 Quantum Key Distribution

In the following, only the two most popular schemes will be described, as these were implemented in the experiment described in this work. A good overview over several Quantum Key Distribution schemes can be found in [BBE92, BEZ00, GRTZ01]. All QKD protocols have a similar underlying procedure, which is shown in Figure 4.1.
4.3 Quantum Key Distribution

**Figure 4.1:** A schematic overview of quantum key distribution. The actual transmission of qubits generates the raw keys with a bit error rate $\epsilon$, e.g. [BB84, Eke91, Ben92]. The principal security of the quantum transmission is shown in [FGG+97, May98]. The successive classical communication via an error-free public channel is necessary for key sifting, error correction and privacy amplification [SRSF98, Lüt99, BBCM95, BS94] for obtaining the final secure key.

**Figure 4.2:** Schematic diagram of the BB84 protocol. Alice produces single photons which are polarized in one of four polarization states and sent to Bob. Bob has a two-channel polarization analyzer, which is randomly varied between $0^\circ$ and $45^\circ$ orientation. Bob detects the photons in one of the two outputs.

### 4.3.1 Single Qubits: BB84 scheme

The so called BB84 scheme was developed by Bennett and Brassard in 1984 [BB84]. The transmission of the key from Alice to Bob is based on single qubits, which carry one of four partly orthogonal states (Figure 4.2). For polarized photons these are the states: $|0^\circ\rangle$, $|90^\circ\rangle$, $|45^\circ\rangle$ and $|135^\circ\rangle$ (see Table 3.1). The photons are prepared in one of the four states at random by Alice, and sent to Bob. Bob analyzes the polarization of the photons with a two channel analyzer whose orientation he constantly and randomly varies between $0^\circ$ and $45^\circ$, and subsequently detects the photons in the two outputs of the analyzer. After a certain amount of qubits have been transmitted, Alice and Bob openly discuss which qubits actually arrived at Bob’s side. Then Bob tells Alice which measurement basis he chose for the received qubits. In return, Alice tells Bob when she had used the same basis, since for those cases Bobs measurement outcomes are correct. Alice and Bob use these cases to generate a key by assigning the $+$-polarization to a “1”, and the $-$-polarization to a “0”, which leaves them with identical sets of “1” and “0”, which is called the sifted key. The procedure of the BB84 protocol is illustrated in table 4.2.
Table 4.2: Illustration of the BB84 protocol. Alice sends photons prepared randomly in the $+$ or $-$ state within the $0^\circ$ or $45^\circ$ basis to Bob. He analyzes the photons with an analyzer set randomly at one of the two bases and detects the photons in the $+$ or $-$ output of the polarizer. For those cases where Alice and Bob used the same basis and the photons managed to reach Bob’s detector, a bit of the sifted key is generated.

The security of the sifted key is determined by estimating the quantum bit error rate of the raw key (QBER). This is performed either by openly comparing a random subset of the key and discarding these bits or during the classical error correction or the key which necessarily requires the exchange of some information of the keys. The eavesdropper Eve is not able to obtain any information about the transmitted qubits without introducing errors. The simplest strategy Eve can pursue is simply to “measure and resend” the photons. She measures the photons with a polarizer just like Bob has and send on a photon with the observed state to Bob. Since she can not know the basis of the photons she must guess, and this will introduce errors with 25 %. In more general terms the best Eve can do is limited by the optimal cloning procedure (see Section 3.5). So in principle, any observed errors will show up a potential security hazard. However, in a practical system, there will be inherent noise by the system itself, such as detector noise or transmission errors.

A limit on the maximally allowed bit error rate produced by Eve’s presence can be determined based on the coherent eavesdropping attack [FGG+97]. The coherent attack is not experimentally possible nowadays, however it is the best strategy known. In order to extract a secure key, the mutual information $I_{AB}$ between Alice and Bob must be at least larger than the mutual information $I_{EB}$ between Eve and Bob, i.e. $I_{AB} \geq I_{EB}$. Given a bit error rate $\epsilon$ for the sifted key, $I_{AB}$ is

$$I_{AB} = \ln_2 2 + \epsilon \ln_2 \epsilon + (1 - \epsilon) \ln_2 (1 - \epsilon)$$

$$= \frac{1}{2} \phi(1 - 2\epsilon), \quad (4.1)$$

where the expressions of $\ln_2$ are combined in the function $\phi$. For the coherent attack, $I_{EB}$ is found to take the value:

$$I_{EB} \leq \frac{1}{2} \phi(2\sqrt{\epsilon(1 - \epsilon)}). \quad (4.2)$$

In the limit of $I_{AB} = I_{EB}$ we find:

$$|1 - 2\epsilon| = 2\sqrt{\epsilon(1 - \epsilon)}. \quad (4.3)$$
4.3 Quantum Key Distribution

This leads to a limit for $\epsilon$ for a potentially safe quantum channel when

$$\epsilon < \frac{1}{2} - \frac{1}{2}\sqrt{2} \approx 0.146447.$$  \hspace{1cm} (4.4)

However, thorough theoretical considerations of practical quantum key distribution systems show \cite{BL99, SRSF98, Lüt99}, that the practical limit is rather $\epsilon \approx 0.105$. During error correction and privacy amplification a fraction of the key must be discarded with security margins, and the size of the final secure key will drop to 0 earlier than given by information theoretical estimations. This is because the information theoretical value can only be reached in the limit of ideal algorithms and infinite sets of bits.

4.3.2 Entangled Qubits: Ekert Scheme

A very elegant implementation of quantum key distribution based on entangled qubit states was developed by Ekert in 1991 \cite{Eke91}. This is a striking application of entanglement, which up to then was only thought to be of purely fundamental interest.

Alice and Bob both share entangled qubits, as shown in Figure 4.3. Alice and Bob each measure their qubit (or photon) with a polarization analyzer, which is randomly set to one out of three settings. In order to check if the qubits where manipulated in one or the other way during their dissemination to Alice and Bob, they perform a test of Bell’s-inequality (see Section 3.2) with some of these qubits. Only if the qubits show a significant amount of entanglement correlation, will a violation of Bell’s inequality be observed. Or in other words, Bell’s inequality can only be violated as long as only a certain amount of knowledge (e.g. by Eve) about the states of one or both of the qubits exists prior to their measurements performed by Alice and Bob. At the same time they can generate the quantum key with the measurements with parallel analyzers, since due to the perfect anticorrelation of the entangled state 3.1 they obtain perfectly opposite results. This is a very appealing feature of the Ekert scheme, since the key is actually produced only during the measurements done by Alice and Bob, and the outcomes are purely random. By definition of the entanglement, the individual photons do not even possess an actual state prior to their measurement.

A complete security proof for the Ekert scheme has not been performed yet. However, according to the present-day understanding of entanglement and Bell’s theorem, see Section 3.2, a violation of Bell’s inequality seems sufficient for limiting Eve’s mutual information with Bob’s key below a critical value. This was conjectured by Ekert in the original work describing the scheme \cite{Eke91}. Strikingly, C. Fuchs et al. \cite{FGG+97} have shown, that the quantum mechanical prediction of the Bell-parameter $S$, from Equation 3.2, expressed in terms of the error rate $\epsilon$ as

$$S = 2\sqrt{2}(1 - 2\epsilon),$$  \hspace{1cm} (4.5)

drops to the classical limit $S = 2$, where the violation of Bell’s inequality ceases, when $\epsilon$ satisfies Equation 4.4 derived for the BB84 scheme. Whether this equivalence is a pure coincidence or arrives from deeper implications of quantum information remains an open question.
Quantum Key Distribution

Figure 4.3: Schematic diagram of Ekert’s QKD scheme. Alice and Bob receive entangled qubits (photons) from a separate source. They both measure the photons with two-channel polarization analyzers with several settings, which they choose randomly. Alice chooses between $0^\circ$, $22.5^\circ$, $45^\circ$, and Bob between $22.5^\circ$, $45^\circ$, $67.5^\circ$. After a measurement run, they will find that several combinations of settings occurred, some of which allow a test of Bell’s inequality (Alice: $0^\circ$, $45^\circ$), Bob: $22.5^\circ$, $67.5^\circ$) and some which allow key extraction (Alice and Bob: $22.5^\circ$, $45^\circ$).

4.4 Quantum Key Distribution with Entangled Photons

A range of experiments have demonstrated the feasibility of quantum key distribution, including realizations using the polarization of photons [BBB+92, MBG93, FJ95, BHK+98] or the phase of photons in long interferometers [MT95, HLM+96, MHH+97]. These experiments have a common problem: the sources of the photons are attenuated laser pulses which have a non-vanishing probability to contain two or more photons, leaving such systems prone to the so called beam splitter attack. If more than one photon were produced at one instance, then the eavesdropper Eve can simply introduce a beam splitter into the path of the photons and split of some of the photons for gaining information on the quantum keys without showing up to Alice and Bob. Unfortunately, true single-photon sources are not available yet, however some promising approaches are being pursued, e.g. see [KMZW00, KBKY99].

Using photon pairs as produced by parametric down-conversion allows to approximate a conditional single photon source [GRA86, RTJ87] with a very low probability for generating two pairs simultaneously and a high bit rate [KMW+95]. Moreover, when utilizing entangled photon pairs one immediately profits from the inherent randomness of quantum mechanical measurements leading to purely random keys.

4.4.1 Adopted BB84 Scheme

A very elegant implementation of the BB84 scheme is to use polarization-entangled photon pairs, instead of the originally implemented polarized single photons. This is implemented very similar to the Ekert scheme described in Section 4.3.2 when Alice and Bob choose different settings of their analyzers for their measurements of the entangled photons. As opposed to the Ekert scheme where both Alice and Bob randomly vary their analyzers between three settings, in the adopted BB84 scheme they only vary their analyzers between
two states, namely $0^\circ$ and $45^\circ$. Due to the entanglement of the two photons, Alice’s and Bob’s polarization measurements will always give perfect anticorrelations if they have the same settings, no matter whether the analyzers are both at $0^\circ$ or at $45^\circ$ (see Section 3.1). A way to view this is to assume that if Alice’s measurement is earlier than Bob’s measurement and due to the entanglement it projects the photon traveling to Bob onto the orthogonal state of the one observed by Alice. So the photons traveling to Bob are, like in the BB84 scheme, polarized in one of the four polarizations $0^\circ$, $45^\circ$, $90^\circ$, $135^\circ$.

After a measurement run, where Alice and Bob independently collect photons for a certain time, they communicate over an open classical channel. By comparing a list of all detection times of photons registered by Alice and Bob they find out which detections came from corresponding photons. From these events they extract those cases, at which they both had used the same setting of the analyzers. Due to the mentioned perfect anticorrelations in these cases, Alice and Bob can build a string of bits (sifted key) by assigning a "0" to the +1 results and a "1" to the -1 result of the individual polarization measurements. When one of them inverts the bits, they finally obtain identical sets of bits, the raw key (or sifted key).

The use of entangled particles for quantum key distribution has a couple of practical advantages over the method of using faint laser pulses as the photon source. Through the coincidence measurements, an effective single photon source is realized, which is an important criterion for the security of a QKD system. This reduces the possibility of the so called beam splitter attack. Also, the inherent randomness of quantum entanglement dramatically helps in implementing perfectly random keys, also a vital ingredient for highly secure communication.

### 4.4.2 Adopted Ekert Scheme

As already described above, the Ekert scheme requires that Alice and Bob vary their analyzers randomly between three settings each since the CHSH inequality is used. An experimentally simpler system can be implemented with Wigner’s inequality [Wig70], which was presented in Section 3.2. When using Wigner’s inequality it turns out, that Alice and Bob only need two settings each, in order to perform the security check of the quantum channel and at the same time obtain the quantum key. Alice chooses between two polarization measurements along the axes $\chi$ and $\psi$ respectively, with the possible results $+1$ and $-1$, on photon $A$ and Bob between measurements along $\psi$ and $\omega$ on photon $B$. Polarization parallel to the analyzer axis corresponds to a $+1$ result, and polarization orthogonal to the analyzer axis corresponds to $-1$.

The derivation of Wigner’s inequality is quite easy, and is based on the assumption that the photons carry preassigned values determining the outcomes of the measurements $\chi, \psi, \omega$ and also perfect anticorrelations for measurements along parallel axes. If the photon pairs are randomly produced with variables denoting the outcomes for these three measurements for each of the two photons with a certain probability, e.g. $p(++,+,-,-,-)$, then the probability of obtaining $+1$ on both sides for a certain measurement, i.e. $p_{++}$,
can be determined by adding the two suitable probabilities:

\[ p_{++}(\chi; \omega) = p(\hat{\tau}, -; -; +, \hat{\tau}) + p(\hat{\tau}, -, -; +, \hat{\tau}); \]  
\[ \text{(4.6)} \]

where the \( \hat{\tau} \) indicates that the parameter is actually used for the particular measurement. Then the combination of \( p_{++}(\chi; \psi) \) and \( p_{++}(\psi; \omega) \) leads to

\[ p_{++}(\chi; \psi) + p_{++}(\psi; \omega) = p(\hat{\tau}, -; -; +, \hat{\tau}) + p(\hat{\tau}, -, -; +, \hat{\tau}) + p(\hat{\tau}, +, -; -, \hat{\tau}) + p(\hat{\tau}, +, -; -, \hat{\tau}) \geq p(\hat{\tau}, -; -; +, \hat{\tau}) + p(\hat{\tau}, -, -; +, \hat{\tau}) = p_{++}(\chi; \omega). \]  
\[ \text{(4.7)} \]

Rewriting the expression above leads to Wigner's inequality:

\[ p_{++}(\chi, \psi) + p_{++}(\psi, \omega) - p_{++}(\chi, \omega) \geq 0. \]  
\[ \text{(4.8)} \]

The quantum mechanical prediction \( p_{++}^{qm} \) for these probabilities at arbitrary analyzer settings \( \alpha \) (Alice) and \( \beta \) (Bob) measuring the \( \Psi^- \) state is

\[ p_{++}^{qm}(\alpha, \beta) = \frac{1}{2} \sin^2(\alpha - \beta). \]  
\[ \text{(4.9)} \]

The analyzer settings \( \chi = -30^\circ, \psi = 0^\circ, \) and \( \omega = 30^\circ \) lead to a maximum violation of Wigner's inequality (4.8):

\[ p_{++}^{qm}(-30^\circ, 0^\circ) + p_{++}^{qm}(0^\circ, 30^\circ) - p_{++}^{qm}(-30^\circ, 30^\circ) = \]
\[ = \frac{1}{8} + \frac{1}{8} - \frac{3}{8} = -\frac{1}{8} \geq 0. \]  
\[ \text{(4.10)} \]

As Wigner’s inequality is derived assuming perfect anticorrelations, which are only approximately realized in any practical situation, one should be cautious in applying it to test the security of a cryptography scheme. When the deviation from perfect anticorrelations is substantial, Wigner’s inequality has to be replaced by an adapted version, as suggested to us by Marek Zukowski.

In order to implement quantum key distribution, Alice and Bob each vary their analyzers randomly between two settings, Alice: \(-30^\circ, 0^\circ\) and Bob: \(0^\circ, 30^\circ\). Because Alice and Bob operate independently, four possible combinations of analyzer settings will occur, of which the three oblique settings allow a test of Wigner’s inequality and the remaining combination of parallel settings (Alice= \(0^\circ\) and Bob= \(0^\circ\)) allows the generation of keys via the perfect anticorrelations, where either Alice or Bob has to invert all bits of the key to obtain identical keys.

If the measured probabilities violate Wigner’s inequality, then the security of the quantum channel is ascertained, and the generated keys can readily be used for further processing.
5 Quantum Key Distribution in Experiment

5.1 The Hardware of the QKD System

This experiment was built up and performed at the University of Innsbruck, where our group was located before moving to the University of Vienna. The actual hardware used in the QKD experiment is identical to the system described in the PhD-thesis of Gregor Weihs [Wei99]. It will therefore only be sketched in rough terms. However, the necessary classical communication was developed to implement full QKD between the two independent users Alice and Bob, and will be described in detail.

An article describing this experiment was published in Physical Review Letters [JSW+00], see Section H.1.

5.1.1 The Optics

The experimental realization of the quantum key distribution system is sketched in Figure 5.1. The polarization entangled photon pairs with a wavelength of 702 nm are produced by type-II parametric down-conversion in BBO, pumped with an argon-ion laser working at a wavelength of 351 nm and a power of 350 mW, as described in Chapter A. The photons are each coupled into 500 m long optical single mode fibers and transmitted to Alice and Bob respectively, who are separated by 360 m. The fiber is specially selected with a non standard cutoff wavelength shorter than 700 nm. Measurements using down-conversion light traveling in the fiber (Section B.3) showed that even for lengths in excess of 1 km only very little loss of the degree of photon polarization occurs. Before each measurement, the polarization rotation introduced by the single mode fibers was compensated with so called “bat ears” (see Section B.2.3). Once adjusted, the polarization was stable for times on the scale of one hour.

Alice and Bob both have Wollaston polarizing beam splitters as polarization analyzers. The detection of parallel polarization (+1) is associated with the key bit 1 and the orthogonal detection (−1) with the key bit 0. Electro-optic modulators in front of the analyzers rapidly switch (rise time < 15 ns, minimum switching interval 100 ns) the axis of the analyzer between two desired orientations, controlled by quantum random signal generators. The quantum random signal generators are based on the quantum mechanical process of splitting a beam of photons and have a correlation time of less than 100 ns,
5 Quantum Key Distribution in Experiment

Figure 5.1: Setup of the qkd experiment based on entangled photons. The polarization entangled photons are produced by spontaneous parametric down-conversion and are transmitted via optical fibers to Alice and Bob, who are separated by 360 m. The two photons are analyzed, detected and registered independently.

and are described in the PhD-thesis of Gregor Weihs [Wei99] and slightly more detail in [JWWZ00].

5.1.2 Photon Registration and Coincidence Determination

The photons are detected by passively quenched silicon avalanche photo diodes (see Section C.2.1). Special time interval analyzers from Guide Technology Inc., USA, are used, which register all detection events as time tags taken in respect to a local time scale. This instrument has two completely independent channels, with a timing resolution of 0.1 ns and an accuracy of about 0.5 ns. The continuous event registration rate is about 100000 per second, and is limited by the data transfer rate from the time interval analyzer to the pc-memory. The dead time of each channel is 400 ns. The total observation time is unlimited and the absolute accuracy over long times is limited by the performance of the time bases. The start of a measurement is initiated through a pulse applied to a separated trigger input. In order to achieve a relative accuracy of Alice’s and Bob’s time bases to within a few nano seconds over a typical measurement time of one minute, two small rubidium oscillators, from Efratom Inc., Germany, were implemented. Details about various types of oscillators for generating two independent time scales are described in my diploma thesis [Jen97].

With this system, Alice and Bob register all detection events on their local personal computers as lists of time stamps together with the setting of the analyzers and the detection result. A measurement run is initiated by a pulse from a separate laser diode sent from the source to Alice and Bob via a second optical fiber. Only after a measurement run is completed, Alice and Bob compare their lists of detections to extract the coincidences and determine the quantum key. The maximal duration of a measurement is limited by the amount of memory in the personal computers (typically one minute).
5.1.3 Performance of the System

Overall our system has a measured total coincidence rate of $\sim 1700 \text{s}^{-1}$, and a singles rate of $\sim 35000 \text{s}^{-1}$. From this, one can estimate the overall detection efficiency of each photon path to be 5% and the pair production rate to be $7 \cdot 10^5 \text{s}^{-1}$. Our system is very immune against a beam splitter attack because the ratio of two-pair events is only $\sim 3 \cdot 10^{-3}$, where a two-pair event is the emission of two pairs within the coincidence window of 4 ns. The coincidence window in the experiment is limited by the time resolution of our detectors and electronics, but in principle it could be reduced to the coherence time of the photons, which is usually on the order of pico seconds.

The quality of correlation measurements for parallel analyzers showed a typical contrast of 50:1 up to 100:1. The variation of the contrast results mainly from the drifting bias birefringence of Alice’s and Bob’s modulators, which were only stable for a few minutes. Since it always took a few minutes of configuration before a measurement run was started, the observed contrast of the measured data is less than achieved during adjustment of the system.

5.2 Classical Communication of QKD

All classical communication between Alice and Bob for obtaining the quantum keys was performed via the standard local area network (LAN) of the University. The different implemented steps (as necessary for the QKD procedure, Figure 4.1) will be described.

5.2.1 Key Sifting

All detection events are registered locally by Alice and Bob as lists of time tags. Each time tag requiring 10 Byte of data overhead, for storing the time with a high resolution and encoding the detection channel and the setting of the modulator. During a measurement run of about one minute, each list consisted of several MBytes of data. The method for key sifting is sketched in Figure 5.2. Alice and Bob reveal their set of time tags to a separated station or to one another over the network via standard Windows file sharing. Note, that they only release the times and the modulator settings, not the actual outcomes of the measurements, since these must remain secret. This is performed by the control program Q-Cryptography.vi, see Figure 5.3, which is implemented in LabView, from National Instruments Inc., USA. First, it starts a program on Alice’s and Bob’s side using the communication features of LabView which operate with the TCP/IP protocol. This allows the control LabView routines running on any remote computer. The routine generates a new file from the full detection lists by stripping of the actual measurement results and putting these lists into folders which are opened for file sharing, and hence can be read from anywhere on the network. Then a C++ routine implemented in the control program compares all of Alice’s and Bob’s time tags in order to determine the detections that occurred within a coincidence time of a few ns and with the same orientation of the modulators. These events are kept by adding their indices in the original lists from Alice and Bob to new sets of indices. Once this has been accomplished, the extraction of the keys on Alice’s
5 Quantum Key Distribution in Experiment

Figure 5.2: A schematic view of the key sifting procedure. In order to find the coincidences and consequently build a key, Alice and Bob openly compare their detection times and analyzer settings. This comparison is performed with programs running on Alice’s and Bob’s computers which are connected via a local area network link.
5.2 Classical Communication of QKD

Figure 5.3: Screenshot from the LabView programs used for QKD. (left) Q-Cryptography.vi: this program is responsible for determining the detection events which occurred in the adjustable coincidence window of a few ns. (1) Specification of the detection data files. (2) Start button for determining the coincidences. (3) Specification of the host names of Alice’s and Bob’s computer, and start of the sub program Q-Key_Generation.vi for the quantum key generation. (4) Possibility to save the coincidence histogram and exit. (right) Q-Key_Generation.vi: this program extracts the corresponding keys, also it controls the security check and the classical error correction. (1) Button for inverting Alice’s key. (2) Security Check of the key by comparing every n-th bit of the key, and calculation of the bit error rate (BER). Based on this BER, the efficiency and residual BER of the error correction based on bit parities of blocks with the size n is plotted. (3) Button for calculating the bit parities of the small blocks of the key. The block size n must be specified first. (4) Start of the error correction based on the obtained parities. (5) Button for storing the final checked and error corrected key locally on Alice’s and Bob’s computers for further use.
and Bob’s side can be started. For this, the sub program Q-Key_Generation.vi, Figure 5.3, is started. This program remotely starts subroutines on Alice’s and Bob’s personal computer to which it hands the new index lists, allowing the routine to locally extract the measurement results sitting in the original list of detections at the corresponding indices. In this way, Alice and Bob have sets containing the measurement results from coincident detections taken with the same polarizer settings, i.e. +1 and −1, which they convert into strings of bits by identifying +1 “1” and −1 “0”. Finally, one of them is made to invert the key, which leaves Alice and Bob with their secret sifted key.

5.2.2 Security Check

The security of the quantum channel can be ascertained by checking that the rate of bit errors does not exceed a certain limit. This is because an eavesdropper cannot gain any information about the quantum channel without disturbing it. As was already discussed in Section 4.3.1, the bit error rate (BER) must be less than ∼ 14%. In practical systems, it might be tempting to also allow for an extra BER due to the experimentally induced errors. However, this would put the quantum cryptography system at risk, because the Eavesdroppers could replace the existing lossy and noisy quantum channel with an ideal channel (maybe via new technology which is only accessible to Eve), and use the extra margin of the BER for her own interests.

In the experiment described here, Alice and Bob perform the security check by openly comparing a certain fraction of the keys, which are consequently omitted from the key. The program Q-Key_Generation.vi which also generated the sifted key, compares bits taken at regular steps in the whole key, and thus calculates an estimate of the BER \( p \).

Typically, the step size is set to 10, i.e. every tenth bit of the sifted key is used in this way. Only if \( p < 0.14 \) will the program allow further processing of the key.

5.2.3 Simple Classical Error Correction

A simple and effective, yet inefficient method for a classical correction of errors in the keys, is to compare the bit parities for sub blocks of the keys. The bit parity simply shows if the number of ones in a set of bits is odd or even. Therefore by comparison of parities, only blocks with an odd numbers of bit errors can be detected.

Alice and Bob split their keys into blocks of the size \( n \) and calculate the corresponding parities, which they openly compare. Equal parities for corresponding blocks are assumed to indicate that the blocks are identical and they are kept for the final key. Different parities indicate that the blocks are not equal and these blocks are discarded. Since the parity already gives away some information about the key, one bit per block must be omitted in the final key, to make the information contained in the openly communicated parity bit useless. Assuming that the errors in the key appear independently, the block length \( n \) of the error correction can be optimized by a compromise between key losses and remaining bit errors. For a BER \( p \) the probability for \( k \) wrong bits in a block of \( n \) bits is given by the binomial distribution \( P_{n,k}(p) = \binom{n}{k} p^k (1-p)^{n-k} \). Neglecting terms for three or more errors and accounting for the loss of one bit per agreeing parity, this algorithm
5.3 Encoding Software

A program allowing to encode a real message with the key was programmed. In order to maintain the high security of the quantum keys, the one time pad protocol from Vernam must be used, see Section 4.2.

The program Nachricht Schlüsseln, see Figure 5.4, is implemented in Visual Basic from Microsoft Inc. The data path of both the message and the key can be specified. The program reads the message and the key data byte after byte, performs the bit-wise XOR operation, and writes the resulting bytes back into the message file at the same location. This scheme is completely symmetric, i.e. it works for both, the encoding as well as the decoding procedure.

\[ \eta(n) \approx (1 - P_{n,1}(p))(n - 1)/n, \]  

\[ p'(n) \approx (1 - P_{n,0}(p) - P_{n,1}(p))(2/n). \]

Based on the BER \( p \) determined in the security check, the program Q-Key_Generation.vi calculates \( \eta(n) \) and \( p'(n) \) for various \( n \), helping the user to choose \( n \) suitably.

5.4 Experimental Results and Discussion
5 Quantum Key Distribution in Experiment

Figure 5.5: The 49984 bit large keys generated by the BB84 scheme are used to securely transmit an image (a) of the “Venus von Willendorf” effigy. The image file has the Microsoft-Windows-BMP format with 60 × 90 pixel each with eight bit color information per pixel; i.e. 43200 bit of picture information. The file includes some header information and a color table, making the entire picture file 51840 bit. Only the picture information was encrypted, leaving the file header and the color table unchanged. Alice encrypts this image via bitwise XOR operation with her key and transmits the encrypted image (b) to Bob via the computer network. Bob decrypts the image with his key, resulting in (c) which shows only few errors due to the remaining bit errors in the keys. (The “Venus” von Willendorf was found in 1908 at Willendorf in Austria and presently resides in the Naturhistorisches Museum, Vienna. Carved from limestone and dated 24,000–22,000 BC, she represents an icon of prehistoric art.)

5.4.1 Adopted BB84 scheme

For the adopted BB84 scheme, Alice’s and Bob’s analyzers both switch randomly between 0° and 45° and key bits are generated for cases where Alice and Bob have parallel analyzers, which occur in half of the cases. In this way, a total of ~80000 bits of key was collected at a rate of 850 bits/second in several measurement runs. The observed quantum bit error rate is $p = 2.5\%$, which ensures the security of the quantum channel. This BER is still rather high from a standpoint of classical communication, and the key is subjected to classical error correction. With $p = 2.5\%$, the efficiency of Equation (5.1) $\eta(n)$ is maximized at $n = 8$ with $\eta(8) = 0.7284$, resulting in a residual BER of Equation (5.2) $p' = 0.40\%$. Hence, from ~80000 bits of raw key with a quantum bit error rate of 2.5%, Alice and Bob use 10% of the key for checking the security and the remaining 90% of the key to distill 49984 bits of error corrected key with a bit error rate of 0.4%. Finally, Alice transmits a 43200 bit large image to Bob via the One-Time-Pad protocol, utilizing a bitwise XOR combination of message and key data (Figure 5.5).
5.4 Experimental Results and Discussion

5.4.2 Adopted Ekert scheme (Wigner’s inequality)

In the experiment it was observed, that the left hand side of inequality (4.8) evaluated to \(-0.112 \pm 0.014\). The violation of this inequality is in good agreement with the prediction of quantum mechanics, which has the value \(-\frac{1}{8}\) and ensures the security of the key distribution. Hence the security of the quantum channel is shown, and the coincident detections obtained at the parallel settings \((0^\circ, 0^\circ)\), which occur in a quarter of all events, can be used as keys. In the experiment Alice and Bob established 2162 bits raw keys at a rate of 420 bits/second and observed a quantum bit error rate of 3.4 %.

5.4.3 Advantages of QKD based on Entanglement

One advantage of using entangled photons for implementing BB84 is that the individual results of the measurements on entangled photons are purely random and therefore the randomness of the final key is ascertained. However, great care must be taken with the switching of the analyzers between the two settings, since the security of the system is only given when Eve has no way to predict the setting of the analyzer. If she knew, then it would be easy for her to measure and resend the photons in the correct basis and have information on the key without being noticed. Therefore a carefully designed physical random generator must be implemented. In the QKD-experiment described in this thesis two physical quantum random number generators were implemented, which were described in the thesis of Gregor Weihs [Wei99] and in a separate publication [JWWZ00]. A further advantage of using entangled photons is that they represent a conditional single photon source, and the probability for having two photon pairs within the coincidence time-window (Section C.3) can be very low. In this QKD-experiment, the probability of having two photon pairs at the same time (i.e. within the coincidence window) was about \(10^{-3}\). This value is considerably lower than in most faint-laser-pulse experiments, where the probability for having two photons in one pulse is about \(5 \cdot 10^{-2}\).

However, the price to pay for these practical advantages is the high effort necessary to realize the source of entangled photons compared to the simple faint-laser-pulse sources.

5.4.4 Outlook

With this experiment, for the first time a full quantum cryptography based on entangled qubits system securely transmitted a message between two separated stations. The system described here is still a laboratory setup, but at the same time it represents almost an applicable system where most components are commercially available. Indeed, this system is already the starting point for the development of an industrial test system.

Further research will be necessary for establishing quantum key distribution over larger distances, e.g. via changing to other wavelengths of the photons or using free space or even satellite links. It seems very likely, that in the long run quantum key distribution will be a communication technology of tomorrow.
6 Quantum State Teleportation and Entanglement Swapping

Quantum state teleportation (QST), discovered by Bennett et al. in 1993 [BBC+, 93], strikingly underlines the peculiar features of the quantum world, since it allows the transfer of a quantum state from one system to another distant one. This system becomes the new original as it carries all information the original did and the state of the initial particle is erased, as necessitated by the quantum no-cloning theorem [BH96]. This is achieved via a combination of an entangled state and a classical message. This transfer of the quantum state from one particle to another is very fascinating because the quantum state of a single particle would be strongly disturbed by attempting to measure or copy it in order to implement the "teleportation". QST manages to transfer the quantum state without gaining any information about it whatsoever. That this is the case will be shown later by an experimental violation of Bell’s inequality for a teleported entangled particle (this procedure is known as entanglement swapping).

6.1 Quantum State Teleportation Theory

In the present work quantum state teleportation is implemented in terms of polarization states of photons, as described in Section 3.3.1, and hence the quantum channel is realized with polarization entanglement of photon pairs prepared in one of the four Bell states, which are

\[
|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{6.1}
\]

\[
|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{6.2}
\]

\[
|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{6.3}
\]

\[
|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{6.4}
\]

A schematic overview of the quantum state teleportation scheme is given in Figure 6.1.

Initially, the system is composed of the input photon 1 which is in a well defined but unknown input state \(|\Psi_{\text{in}}\rangle_1 = (\alpha|H\rangle_1 + \beta|V\rangle_1)\) and photons 2 and 3 which are in the Bell
state $|\Psi^-\rangle_{23}$ given in Equation (6.1). The total state can be written in the following way:

$$|\Psi_{\text{total}}\rangle = |\Psi_{\text{in}}\rangle_1 \otimes |\Psi^-\rangle_{23} = (\alpha|H\rangle_1 + \beta|V\rangle_1) \otimes \frac{1}{\sqrt{2}}(|H\rangle_2|V\rangle_3 - |V\rangle_2|H\rangle_3).$$  

(6.5)

Rearranging the terms of the above state and by expressing photon 1 and photon 2 in the basis of Bell states leads to:

$$|\Psi_{\text{total}}\rangle = \frac{1}{\sqrt{2}} \left[ (\alpha|H\rangle_3 - \beta|V\rangle_3)|\Psi^+\rangle_{12} - (\alpha|H\rangle_3 + \beta|V\rangle_3)|\Phi^-\rangle_{12} - (\alpha|V\rangle_3 + \beta|H\rangle_3)|\Phi^+\rangle_{12} + (\alpha|V\rangle_3 - \beta|H\rangle_3)|\Phi^-\rangle_{12} \right].$$  

(6.6)

To perform the QST, Alice subjects photons 1 and 2 to a measurement in a Bell-state analyzer\(^1\) (BSA). If, for example, she finds them in the state $|\Psi^-\rangle_{12}$, then photon 3 emerging on Bob’s side, will be in the state $-(\alpha|H\rangle_3 + \beta|V\rangle_3)$. This state is identical to the input state except for the negative global sign, which has no effect on the measurement results. Note, that if Alice observes any of the other Bell-states for photons 1 and 2, photon 3 will also be projected into a well defined state, which deviates from the original in the phase and/or basis states. As soon as Bob receives the classical information from Alice about her result of the BSA-measurement, he can apply a suitable unitary operation to photon 3 and transform its state into the original state. For example, if Alice observes $|\Phi^+\rangle_{12}$ in her BSA measurement, Bob has to swap the two basis states $|H\rangle \leftrightarrow |V\rangle$.

\(^1\)The Bell-state analyzer (BSA) is a device which can identify, in which of the four possible entangled Bell-states two particles are. If the two particles are independent, then naturally they have no correlation, and the BSA will give a random result.
6.1 Quantum State Teleportation Theory

Figure 6.2: A hypothetical classical teleporter. It will aim to somehow gain maximum information about the input state through some measurements. Also the classical device might even have the possibility to obtain some additional information on the state which will allow to optimize the measurement, e.g. the basis of the input. Anyhow, it will produce a new particle at the receiver end and prepare its state based on the gained knowledge about the input state. Ideally the output has the properties of the original. The information about the input state may also be stored or leak out of the device. Due to the theorems of quantum state estimation and no-cloning, the device will not be able to perfectly reproduce the input state at the output, unless it has access to the extra information on the input state.

6.1.1 The Speed of Quantum State Teleportation

This requirement of the classical signal transmission from Alice to Bob naturally limits the speed of "particle transfer" with QST to the vacuum speed of light. Although the actual quantum state of the receiving particle will be projected into a well defined state instantaneously during Alice's bell-state measurement, Bob can only replicate the initial particle after also obtaining the classical information from Alice allowing him to perform the unitary transformation. Since the classical information can only travel at the speed of light the overall speed of the teleportation is the speed of light. It is easy to see from Equation (6.6), that if Bob would not wait for the classical information to perform the unitary transformation, photon 3 will be in a perfectly random state.

However, there is at least one interesting application, where QST does have a time gain over a classical procedure, which is the instantaneous quantum computing with a probabilistic success [BPS+01].

6.1.2 Quantum Nature of Quantum State Teleportation?

Quantum State Teleportation involves some obvious “quantum features”. The nonlocality of entanglement and the measurement postulate let the state of the receiver particle at Bob’s side instantaneously correspond to the state of the input particle via Alice’s Bell-state measurement. Also the meaning of information in quantum physics is stressed, since in QST no information about the input state must be gained as a matter of principle.

A hypothetical classical teleporting machine as shown in Figure 6.2 might be able to show results similar to those of a proper QST device. But the classical machine would definitely not be able to reproduce a general input state perfectly, due to the no-cloning
6 Quantum State Teleportation and Entanglement Swapping

Note, that in any case there is at least some information about the teleported state within the classical teleporter, which in quantum physics necessarily limits the quality of the teleported state. In QST, no information about the teleported state is gained at all. A proof of the quantum nature of QST is possible by teleporting the most general possible state, which is that of a particle which is entangled with an other particle.

6.2 Entanglement Swapping

A definitive proof of the quantum nature of QST can be performed by teleporting not only an unknown state, but even an undefined state. This is the case for the individual partners of an entangled system, as only joint properties are defined, but no individual properties (Chapter 3). This procedure is also known as "Entanglement Swapping" [ZZHE93] because one starts with two pairs of entangled photons 0–1 and 2–3, subjects photons 1 and 2 to a Bell-state measurement by which photons 0 and 3 also become entangled. The resulting entanglement of photons 0 and 3 is best shown by performing a test of Bell’s inequality (see Section 3.2 and [Bel64, CHSH69]), because it can only be violated, if no substantial information about the state of the individual photons is known. Therefore, the violation of Bell’s inequality for the correlations between photons 0 and 3 confirms that the state of photon 1 remained undefined in a fundamental way and Alice and Bob could not have played any kinds of tricks to make the results look like successful teleportation.

The general scheme of entanglement swapping is given in Figure 6.3. A third party named Victor is introduced, who observes Alice’s and Bob’s independently measured results and can check whether the teleportation works as suggested by quantum theory.

Again expressed in polarized photons, the formalism of entanglement swapping runs as follows: Initially, the system is composed of two independent entangled states and can be written in the following way:

$$|\Psi_{total}\rangle = |\Psi^-\rangle_{01} \otimes |\Psi^-\rangle_{23}. \quad (6.7)$$

Including Equation (6.1) in (6.7) and rearranging the resulting terms by expressing photon 1 and photon 2 in the basis of Bell states leads to:

$$|\Psi_{total}\rangle = \frac{1}{2}[|\Psi^+\rangle_{03}|\Psi^+\rangle_{12} - |\Psi^-\rangle_{03}|\Psi^-\rangle_{12} - |\Phi^+\rangle_{03}|\Phi^+\rangle_{12} + |\Phi^-\rangle_{03}|\Phi^-\rangle_{12}]. \quad (6.8)$$

When Alice subjects photons 1 and 2 to a measurement in a Bell-state analyzer (BSA), and if she finds them in the state $|\Psi^-\rangle_{12}$, then photons 0 and 3 measured by Bob, will be in the entangled state $|\Psi^-\rangle_{03}$. If Alice observes any of the other Bell-states for photons 1 and 2, photons 0 and 3 will also be perfectly entangled correspondingly. In principle, Bob could transform all entangled states into $|\Psi^-\rangle_{03}$ by a local unitary transformation on one of his photons, as was shown in the dense coding experiment by Mattle et al. [MWKZ96]. However, photons 0 and 3 will already be perfectly entangled for any result of the BSA, and therefore it is not necessary to apply a unitary operation to the teleported photon 3 as in...
Figure 6.3: Entanglement swapping version of quantum teleportation. Two entangled pairs of photons 0–1 and 2–3 are produced in the sources I and II respectively. One photon from each pair is sent to Alice who subjects them to a Bell-state measurement, projecting them randomly into one of four possible entangled states. This procedure projects photons 0 and 3 into a corresponding entangled state. Alice records the outcome and hands it to Victor. Bob performs a polarization measurement on each photon, choosing freely the polarizer angle and recording the outcomes. He hands his results also to Victor, who sorts them into subsets according to Alice’s results, and checks each subset for a violation of Bell’s inequality. This will show whether photons 0 and 3 became entangled although they never interacted in the past. This procedure can be seen as teleportation either of the state of photon 1 to photon 3 or of the state of photon 2 to photon 0.

the standard teleportation protocol. But it is certainly necessary for Alice to communicate to Victor her Bell-state measurement result. This will enable him to sort Bob’s data into four subsets, each one representing the results for one of the four maximally entangled Bell-states [Zuk00b].

It is now up to an experiment on entanglement swapping for finding out if the criteria for the quantum nature of QST can be met with an actual physical realization of teleportation. Such an experiment will be presented in the next chapter.
7 Entanglement Swapping in Experiment

The experiment described here is based on the Innsbruck teleportation, set up by Bouwmeester et al. [BPM+97], where the teleportation of an unknown quantum state was demonstrated. In an experiment led by Kimble [FSB+98] teleportation was also performed with squeezed states of light, in a so called continuous variable teleportation experiment. However, the interpretation of these experiments is still subject to some discussion [BK98, BPD+98, BPWZ00, RS01]. A third experiment [BBDM+98], similar to remote state preparation [BDS+01], teleported a state classically known to Alice. Entanglement swapping was also shown in a previous experiment [PBWZ98], yet the low photon-pair visibility prevented a violation of Bell’s inequality for photons 0 and 3. The experiment described here is able for the first time to show a violation of Bell’s inequality for teleported entangled photons, and hence shows the quantum nature of quantum state teleportation.

This entanglement swapping experiment is based on polarization entangled photons. Since necessarily two photon pairs are required at one instant in time, i.e. within their coherence time which is typically 500 fs. Since no photon detectors with sufficient time resolution presently exist, the solution is to produce the photons by down-conversion (see Chapter A) which is pumped by pulses a UV-laser with a pulse width of about 200 fs [ZZW95]. However, first the most vital component of quantum state teleportation, the Bell-state analyzer, will be described.

7.1 Interferometric Bell-state Analysis

The Bell-state analyzer (BSA) is responsible for identifying for in which of the four possible entangled Bell-states two input particles are. There have been many proposals for the realization of a BSA for photons. One problem is, that the operation of the BSA necessitates a nonlinear coupling between the two particles, which is very difficult to achieve for photons. The most promising approaches are those with single atoms sitting in a cavity [NRO+99, THL+95, SEB99, VFT00, LI99, KKS01, RVG+97]. A phase shift of up to 16° for a single photon–photon interaction has been shown [THL+95]. Yet, presently these systems are technically highly demanding or not even suitable for single-photon operation. Note, that the ideal photon-photon BSA is equivalent to the general c-not-operation required for realizing quantum computers, which at date does not exist, because a BSA can likewise entangle or disentangle qubits just as the c-not-operation can.
7 Entanglement Swapping in Experiment

Figure 7.1: Configuration of the all-fiber Bell-state analyzer. The two photons are brought together via single-mode optical fibers, and then are detected with single photon detectors Dc and Dd. The $|\Psi^\rightarrow\rangle$-Bell-state is detected as a coincidence between the two detectors, as is explained in Chapter D. The adjustment of the polarization rotation of the fibers is performed by a polarization controller sitting in one arm. It is set such that a well defined polarization of the input beams arrive at the beam splitter in the same state. The components in the shaded box are only connected for adjustment, which is performed with a laser diode, running at 788 nm, the same wavelength as the down-conversion photons have. The laser light is externally split up, sent through polarizers, oriented at $\alpha$ and $\beta$ and then into the two input fibers a and b. The two beams interfere at the beam splitter and hence realize a Mach-Zhender interferometer. A phase modulator sitting in one input arm periodically (70 Hz) varies the phase of the interferometer. The intensity of the output beam d is measured with a standard silicon photo diode and viewed on an oscilloscope, allowing to observe the interference fringes.

However, it has been shown that by using linear optical elements it is possible to realize a non-perfect BSA, in the sense that its efficiency is always limited to maximally 50% [CL01]. This means, that the BSA can either identify only two out of the four possible Bell-states, or that it can identify all Bell-states with a loss ratio of 50%. The effect which can be exploited for this is the interference of two photons on a beam splitter. It was shown in theory and experiment in the diploma-thesis of Markus Oberparleiter [Obe97] and the PhD-thesis of Klaus Mattle [Mat97], that the statistics of two-photon interference on a normal 50:50 beam splitter allows the identification of the states $|\Psi^\rightarrow\rangle$ and $|\Psi^+\rangle$, as given in Chapter D.

7.1.1 Implementation of the Bell-state Analyzer

In all previous experiments, the BSA was implemented with free space beam splitter cubes. Good spatial mode overlap of the two input beams was realized by coupling the outputs into single mode fibers, which act as spatial mode filters. One practical draw back of using a free space configuration is that the input beams have to be coupled symmetrically into the two fiber couplers in the outputs.

A much more convenient way is to use a fiber beam splitter, where the input beams
7.2 The Entanglement Swapping Setup

are first put into fibers and then brought together. An all-fiber beam splitter is realized by the fusion of two optical single mode fibers in such a way, that any desired coupling ratio is achieved, i.e. 50:50 in this case. Fiber fusion couplers are a standard product from the telecommunication industry produced by Sifam Ltd. (UK), now part of Uniphase (Canada). The only disadvantage of using a fiber-based beam splitter, is that the polarization rotation induced in the fibers must be compensated (Section B.2). In this case, where two input beams interfere on the beam splitter, it is necessary that the polarizations of the two input beams are the same at the beam splitter. This is achieved with the help of an adjustment laser diode, which has a wavelength of 788 nm, the same as the actual input photons have, and a polarization controller in one arm. The configuration is shown in Figure 7.1. The fringes of the interference at the beam splitter are viewed on an oscilloscope, and by tuning the polarization controller can be set to a maximum or a minimum. The best way to find the optimal polarization adjustment is to choose orthogonal input polarizations, and to consequently adjust the interference to a minimum. The accuracy of the polarization setting is tested after adjustment, by rotating one of the polarizers until the fringes viewed on the oscilloscope are minimal. Then, the reading on the scale of the polarizer should be the same as was originally set for the alignment procedure. It was found that typically these two readings agree to within $\pm 0.5^\circ$, which is certainly sufficient for this experiment.

7.2 The Entanglement Swapping Setup

The setup of the entanglement swapping experiment is shown in Figure 7.2, and a photo of the setup is given in Figure 7.3. Two separate polarization entangled photon pairs are produced via type-II down conversion (described in detail in Chapter A). The BBO-crystal (barium borate) has 2 mm thickness and is pumped by UV laser pulses with a wavelength of 394 nm, a pulse width of $\approx 200$ fs, a repetition rate of 76 MHz, and an average power of 370 mW. The entangled photons had a wavelength of 788 nm. Through spectral filtering with a $\Delta \lambda_{\text{FWHM}} = 3.5$ nm for photons 0 and 3 and $\Delta \lambda_{\text{FWHM}} = 1$ nm (also 2 nm filters were used in first test measurements) for photons 1 and 2, the coherence time of the photons was made to exceed the pulse width of the UV-laser, making the two entangled photon pairs indistinguishable in time, a necessary criterion for interfering photons from independent down conversions [ZZW95]. The visibility limits of the interference of two photons on the beam splitter will be discussed in more detail in Section E.2.

All photons were collected in single-mode optical fibers for further analysis and detection. Single-mode fibers offer the high benefit that the photons remain in a perfectly defined spatial mode allowing high-fidelity interference. For performing the Bell-state analysis, photons 1 and 2 interfered at a fiber beam splitter, where one arm contained a polarization controller for compensating the polarization rotation introduced by the optical fibers. In order to optimize the temporal overlap between photon 1 and 2 in the beam splitter, the mirror which retroreflects the UV-laser into the down-conversion crystal was mounted on a translation stage, motorized by a DC-motor with position encoder (from Oriel, FR). The Photons 0 and 3 were sent to Bob’s two-channel polarizing beam split-
Figure 7.2: Setup of the entanglement swapping experiment. The components required for the entanglement swapping are contained in the boxes named Alice, Bob and Victor. The box named “fs-Pulse UV Laser” holds the components necessary for generating the UV-laser pulses as well as the instruments required for checking and optimizing the laser system.
7.2 The Entanglement Swapping Setup

Figure 7.3: The entanglement swapping experiment. The BBO down-conversion crystal sits in the center of the picture. The photons each are guided towards the couplers, which launch them into single mode fibers. The box mounted on the long post named “BSA” contains the fiber optic beam splitter. The black lines indicate the travel paths of the down-conversion photons, and the grey line indicates the location of the UV laser.

ters for analysis, and the required orientation of the analyzers was set with polarization controllers in each arm, where the polarizer of photon 0 is set to orientation $\phi_0$ and of photon 3 to $\phi_3$. All photons were detected with silicon avalanche photo diodes, with a detection efficiency of about 40%. The types used are the commercial SPCM devices (see Section C.1) from EG & G for D1 and D2 and the self designed actively quenched modules (see Section C.2.2) for detectors D0 and D3. Alice’s logic circuit detected coincidences between detectors D1 and D2. She passes the result as a classical signal to Victor, who sorts Bob’s detection events depending on Alice’s result. The implementation of the coincidence logic will be described below in Section 7.2.1.

7.2.1 The Coincidence Logic

This logic required by Victor is realized with 4-fold coincidence measurements, generated between the detection pulses from Alice’s two detectors, D1 and D2, in coincidence with the pulses from different combinations of Bob’s detectors behind the PBS. Expressed in Boolean logic, the four observed 4-fold rates are: $N_{++} = N(D0_+ \land D1 \land D2 \land D3_+)$, $N_{--} = N(D0_- \land D1 \land D2 \land D3_-)$, $N_{+-} = N(D0_+ \land D1 \land D2 \land D3_-)$ and $N_{-+} = N(D0_- \land D1 \land D2 \land D3_+)$, where $N(B)$ is the counted number of detection events that
Figure 7.4: The coincidence logic. Shown is only the connection scheme for the $N_{++} = N(D_{0+} \land D_{1} \land D_{2} \land D_{3+})$ 4-folds. The other three 4-folds are cabled likewise. The connections are realized by 50 Ω coaxial cable with LEMO-connectors for NIM connections, and BNC-connectors otherwise.

The logic is implemented in NIM modules (see Section G.4). The TTL (also described in Section G.4) detector pulses are inverted with high-bandwidth transformers (TMO-1-02 from Minicircuits Ltd., USA) and transformed to fast-NIM pulses with a discriminator (Type: 4608C from LeCroy, CH) with a pulse width of about 4 ns. The signals from the total of six detectors are combined on a 4-fold logic module (CD4020 form Perkin Elmer (Ortec), USA). This unit has four separate logic gates, which can be individually configured to realize various logical combinations of the inputs. Since the discriminator only delivers two output signals per input channel, a self built (designed and built by Andreas Mitterer at the Institute of Experimental Physics, University of Innsbruck) signal-multiplier is used which generates five separate NIM-signals from one input NIM-signal. In this way, the four 4-fold coincidences $N_{++}$, $N_{--}$, $N_{+-}$ and $N_{-+}$ are realized. Since the pulse width of each of the NIM-signals is about 4 ns, the coincidence window turns out to about ±2 ns, because a minimal pulse overlap of 2 ns of the pulses in the logic gate is required. Since the paths of the photons are not exactly equal before they hit the detectors, a time offset between the different detectors will result for simultaneously created photons. The temporal offset is compensated by sending the TTL pulses of the four detectors $D_{0+}$, $D_{0-}$, $D_{3+}$ and $D_{3-}$ through a 4-channel delay box (DB463, Perkin
Elmer (Ortec, USA) which offers a range of 0–63 ns delay per channel. The NIM-signals from detections of correlated photons on different detectors (e.g. \(D_{0+}\) and \(D_{1}\), etc.) were observed on two separate channels of a high speed digital oscilloscope (500 MHz). The two pulses are brought to overlap by adjusting the delay of the detector signal that uses the variable delay. The outputs of the logic gates deliver TTL-pulses, which are feed directly into a 9-channel counter card (PC-TIO from National Instruments Inc., USA) in a personal computer, which registers the events in a LabVIEW program. The extra channels of the counter were used for registering the single count rates of some of the detectors during the measurements, to check the performance of the system. One drawback of the PC-TIO counter card is, that it only has 16-bit counters. In order that the counters would not overrun, they were permanently started and stopped three times per second, and the counts of each run were added up. As it turned out, by this way, the counter effectively had a dead time of 10%, which is actually very much, considering the very low count rates of the 4-fold events (about 1 event in 100 s). This problem was solved only after finishing this experiment by using a 6602 counter card, also from National Instruments Inc., USA, which contains eight 32-bit counters.

For adjustment and alignment of the setup, the coincidence logic was configured such that the 2-fold coincidences of the correlated photon pairs are measured.

### 7.2.2 The fs-Pulse UV-Laser system

In experiments, such as the one described here, where two entangled photon pairs are required, it is necessary to pump the down-conversion with ultra short laser pulses with about 200 fs pulse width. It is a standard procedure these days to generate pulses of less than 100 fs with mode locking lasers in the near infrared. The photograph in Figure 7.5 shows the full fs-lasersystem. In this setup a commercial Ti:Sapphire mode locked laser, type Mira900aBasic, pumped by a green (532nm) solid state laser, Verdi 10W, both from Coherent Inc. USA, are used. With this system, laser pulses with an autocorrelation width of 150 fs at a wavelength of 789 nm are generated. The average power of the pulsed laser beam is 1.6 W, and the repetition rate is 76 MHz. Due to the very high energy densities occurring with the ultra short laser pulses, the frequency doubling using a nonlinear crystal is rather straight forward. The pulsed infrared beam is focused with a 4 cm lens onto the 1.5 mm thick LBO (lithium borate), which is cut for type-I second harmonic generation (SHG) of 789 nm → 394.5 nm. The typical SHG efficiency is 25%-30%, i.e. from an average IR (789 nm) power of 1.6 W a UV (394.5 nm) power of about 450 mW is generated. The UV light emerging from the crystal has an elliptical beam profile due to beam walk-off in the birefringent LBO crystal. This is corrected by collimating the UV beam with two crossed cylindrical lenses (UV grade silica glass), with a focusing length of 10 cm and 15 cm respectively. Then the laser beams are directed via three dichroic mirrors towards the down-conversion crystal. The dichroic mirrors are realized with dielectric layers, such that the second harmonic UV light is reflected, and the fundamental IR light is transmitted, in order to separate the UV from the IR laser light. Due to the imperfections of the mirrors also some UV will leak through the mirrors, which is used for measuring and adjusting the laser system.
Figure 7.5: The UV-fs-pulse laser system. The white lines indicate the location of the laser beams in the setup. At the rear is the Verdi laser which pumps the Mira Ti:Sa mode-lock laser, whose IR-pulse laser beam emerges from the front and is deflected with a mirror. Its focused with a lens onto the LBO crystal for second harmonic generation. The emerging UV-light is collimated with two crossed cylindrical lenses, which compensate the elliptical shape of the UV-light. The UV-beam is deflected by two dichroic mirrors with picomotor mounts, and is finally sent by a third dichroic mirror towards the down-conversion crystal, which sits to the right of the photographed section of the table (partly the UV-beam runs through pipes for higher stability of the air). The LaserCam CCD camera measures the spot sizes and position of the UV beams, and a laser spectrometer (the piece of white housing which can only just be seen on the right edge of the image) is placed behind the second dichroic mirror. The instrument at the lower center labeled “Micro” is an autocorrelator, able of measuring the pulse width of the IR pulses.
The first instrument used for checking the performance of the laser is a spectrometer, which sits behind the second dichroic mirror. It observes the spectra of both the IR and the UV light. Nominally, the laser system is adjusted such, that the Mira900a laser runs at a wavelength of $\lambda_{\text{Peak}} \approx 790$ nm with a width of $\Delta \lambda_{\text{FWHM}} \approx 8$ nm, and the UV laser light has a wavelength of $\lambda_{\text{Peak}} \approx 394.5$ nm and a width of $\Delta \lambda_{\text{FWHM}} \approx 2$ nm. Checking the spectrum is necessary, since the Ti:Sapphire laser is very easily detuned (e.g. optimization of the Laser, temperature instabilities), hence directly shifting the spectrum of the UV light. Also, even for a fixed IR wavelength, the UV spectrum can be shifted by about $\pm 2$ nm by tuning the phasematching of the LBO, accomplished by tilting it with respect to the laser beam.

The second instrument used for characterizing the laser system is a CCD detector (charge coupled device), which has a pixelized area of silicon detectors (640*480 pixel). The signal of the CCD is supplied as a standard RS-170 black and white video signal, with a refresh rate of 60 Hz. The type of camera used here is the 1/2"-LaserCam from Coherent Inc. The signal is digitized with a frame grabber card, type 4409 from National Instruments Inc., and evaluated on a personal computer running LabView. The CCD detector measures the UV laser which leaks through the third dichroic mirror, on its way to the down-conversion crystal, but also the light leaking through from the UV, which was retroflected through the down-conversion crystal and runs back exactly the same path. Therefore the laser beam is measured at two points which allows to perfectly determine the direction and position of the UV laser in respect to the down-conversion crystal. Of course only as long as none of the optics in the UV beam path after the second dichroic mirror is moved.

In order to always keep the UV laser at a fixed position, a software feedback loop was realized in LabView. The system permanently measures the position of the laser via a CCD-detector and with a simple algorithm adjusts the two first dichroic mirrors which are mounted on pico-motor actuated mirror mounts in order to keep the laser at its reference position. A block diagram of the active laser steering system is given in Figure 7.6. In this way, the photon pair count rates of the system can be kept stable for times longer than 24 h. This is highly important for performing long measurements, as necessitated by the low event rate achieved in the entanglement swapping experiment. Typical temporal variation of the count rate without and with the CCD feedback system deployed is shown in Figure 7.7.

Another important use of the CCD-detector system is that it allows to measure the profile of the UV laser beam. Experiences gained in our labs, and also from work performed by the group Harald Weinfurter in Munich [KOW01] showed, that the best pair count rate is achieved when the waist of the UV-laser is placed right at the down-conversion crystal and the size of the waist is rather small ($< 0.5$ mm diameter). Since in this experiment two down-conversion processes are required, the compromise is to put the waist of the laser at the UV-mirror for symmetry reasons. An extra mirror sitting on a flip-mount can be inserted into the UV-beam, such that the spot it generates on the CCD-detector corresponds directly to the spot of the beam at the retroflecting mirror. The size of this spot is minimized by adjusting the two cylindrical lenses, and the half-maximum area of the beam spot is about $1.6$ mm$^2$ (half maximum area), corresponding to a beam diameter
Figure 7.6: Schematic diagram of the CCD feedback loop for controlling the laser. The signal of the CCD detector is digitized with the frame grabber, resulting in an image with a resolution of 640×480 pixels and an intensity scale of 8 bit. Since both beam spots are on the detector at the same time, the program alternately cuts out the spot from the outgoing or the reflected beam. The position of the spots is calculated via the center-of-mass, which turned out to be better than using gaussian-fits applied to the profile. The deviation of the beams from the reference positions is used to steer the mirrors, where the deviation of the outgoing beam only steers the first mirror and the deviation of the reflected beam only steers the second mirror. This algorithm is certainly not optimal, yet its quite stable in converging once the individual gains of the two mirrors are suitably chosen. The mirrors are mounted in mirror mounts with pico-motor (from NewFocus, USA) actuated adjustment screws, which have an angular resolution of <1μrad.
Figure 7.7: Stability of the down-conversion rates. The curves show the typical stability of down-conversion count rates over time, with and without the active control of the laser beam position in operation. The 4-fold coincidence rate of the setup is calculated via the two measured 2-folds for photons 0 and 1, \( C_{01} \), and photons 2 and 3, \( C_{23} \) as given in Equation (7.2). The 4-fold rates shown in the diagram are normalized to allow better comparison.
of about 0.7 mm.

7.2.3 Adjustment and Performance of the Setup

After switching on the laser system, it must warm up for at least one hour. But often it is only stable after running for about 12 h. Therefore, the laser was usually left running for many days without interruption.

The registered events of photon pairs (2-folds) was about 2000 per second before the Bell-state analyzer (Alice) and the polarizing beam splitter (Bob). The 2-fold entanglement contrast was typically 30:1 to 35:1 in the 45° base, which corresponds to a visibility in the range of 0.935 to 0.944.

The expected number of 4-fold coincidences $C_{0123}$ for a particular measurement can be estimated in the following way:

$$C_{0123} = P_{01}P_{23}N_{\text{Laser pulse}}$$
$$= \frac{C_{01}}{f_{\text{Laser}}t_{01}} \frac{C_{23}}{f_{\text{Laser}}t_{23}}f_{\text{Laser}}t_{0123} = \frac{C_{01}C_{23}}{t_{01}t_{23}f_{\text{Laser}}},$$

where $P_{ij}$ is the probability for a 2-fold detection per laser pulse and $N_{\text{Laser pulse}}$ is the total number of laser pulses for one measurement time. In the second line the probabilities are expressed by the two measured 2-folds for photons 0 and 1, $C_{01}$, and photons 2 and 3, $C_{23}$, gathered in measurement times $t_{01}$ and $t_{23}$ respectively with the laser pulsing at the frequency $f_{\text{Laser}}$. Then in the duration of the measurement time $t_{0123}$ there will occur $C_{0123}$ 4-fold events. Given the values stated above, where $C_{01} = C_{23} = 2000$ counts in 1 second, and the laser pulse frequency of $f_{\text{Laser}} = 76$ MHz, Equation (7.2) gives a 4-fold probability of 0.0526 per second. However, in the actual entanglement swapping setup, each of the two 2-fold rates are reduced by a factor of $1/2$ due to the polarizing beam splitters on Bob’s side. A further reduction by $1/2$ is due to the beam splitter of the Bell-state analyzer, because the two entering photons will only take separate outputs for half the cases as long as no interference occurs. Therefore the result from Equation (7.2) is reduced by a factor of $1/8$, leading to a total 4-folds of 0.0065 in one second.

The compensation of the polarizations in the fibers for photons 0 and 3 was performed by placing polarizers in front of the couplers set at the desired orientation of the polarizers. Then by tuning the controllers and observing the single counts of the two outputs of the polarizers, the fiber was compensated such that all photons arrive in one output. In this way an polarization contrast for the single photons of better than 100:1 was achieved. The compensation of the fibers for photons 1 and 2 which lead to the beam splitter were compensated as described above in Section 7.1.1. The polarization alignment of all optical fibers performed before each measurement proved to be stable within 1° for 24 h.

7.2.4 Scans for Testing the System Alignment

A scan program was implemented in LabVIEW, which moved the position of the UV-mirror through a given position range in steps and at each step counted the detections for a certain measurement time. The longest time used was 16000 s.
7.2 The Entanglement Swapping Setup

Figure 7.8: Alignment test scans. Left diagram: shown is the interference of two independent photons 1 and 2 on the fiber beam splitter, both polarized at 45°. The given data are the 4-fold coincidences measured in 5300 s per point. Here, photons 0 and 3 serve as triggers for photons 1 and 2 entering the beam splitter. The minimum of the 4-folds occurs at the motor position where the photon overlap at the beam splitter is optimal. To indicate the form of the dip, a gaussian function is fitted to the data. The 4-folds outside of the interference region are random events. The dip has a visibility of $0.944 \pm 0.059$. Right diagram: this is entanglement swapping measured by placing two polarizers in the arms of photons 0 and 3. Since these two photons are projected into a $|\Psi^-\rangle$-state, a minimum of the 4-fold coincidences will occur when the overlap of the photons is optimal. The measurement of each point lasted for 6600 s, and a visibility of $0.813 \pm 0.103$ was observed.
Once the setup was running, many scan measurements were performed, in order to find the optimal position of the motorized UV mirror as well as to check and optimize the visibility of the interference occurring between photons 1 and 2 on the Bell-state analyzer. For these alignment measurements, the system was configured without polarizing beams splitters for photons 0 and 3, and two polarizers were introduced in front of the couplers of the photons. By placing the two polarizers into the paths of photons 1 and 2 before they meet on the beam splitter, a Hong-Ou-Mandel type experiment [HOM87] of interference for two independent photons is performed (a detailed analysis of this kind of experiment is given in the PhD-thesis of Klaus Mattle [Mat97]). In this experiment two photons with parallel polarization will always take the same output path of the beam splitter due to interference. In this case the two outer photons can be considered as triggers showing up that two photons entered the beam splitter in different inputs. A scan measurement of this interference is shown in the left diagram of Figure 7.8. The observed count rates have a minimum of 1 and a maximum of 32, which corresponds to an visibility\(^1\) of 0.944 ± 0.059 (see G.1 for the definition of the visibility). Before, many test scan for the interference of photon 1 and 2 were performed with the spectral filters for photons 1 and 2 at 2 nm FWHM-bandwidth, and typically a visibility of 0.835 ± 0.052 (maximum: 100, minimum: 9) was observed. This major difference in visibility between using 1 nm and 2 nm filters will be explained in the following section. However, in order to achieve the violation of Bell’s inequality for the teleportation of entanglement, the 1 nm filters had to be used. A list of the observed contrasts and visibilities for several different scans is given later in Table E.2.

An entanglement swapping test scan is performed by placing two polarizers into the arms of photons 0 and 3. With this Bell-state analyzer only \(|\Psi^-(03)|\Psi^-(12)\) term of Equation (6.8) will contribute and the 4-fold coincidences will be minimal when the two polarizers are parallel. This is observed in the data given in the right diagram of Figure 7.8, where a maximum of 29 and a minimum of 3 is observed. The estimated visibility is 0.813 ± 0.103. This value already indicates that the entanglement between photons 0 and 3 after the entanglement swapping will allow a violation of Bell’s inequality, which requires a visibility better than about 0.71.

### 7.3 Limits to the 4-fold Correlation Visibility

The visibility of the observed 4-fold interference, as described in the section above, is limited by a couple of effects. Some of the effects originate in limits of the photon-pair correlation (2-folds) and others are governed by the two photon interference at the beam splitter in the Bell-state analyzer. All of these effects but one are either quite obvious or described in previous theses [Mat97, Wei94]. However, the influence of the temporal walk off on the visibility on the two-photon interference was missed in the previous work, and it is important to see only by considering this contribution, can the actually observed

---

\(^1\) This visibility is only an estimate because of the low count rates and because the scan range is not completely outside the interference region.
visibility be understood. All the effects will be taken together in order to estimate the total visibility of the observed results, as described detail in Section E.

The estimation of the visibilities indicated, that by using filters for photons 1 and 2 with a FWHM-bandwidth of 1 nm, a visibility of 0.897 and 0.817 for the $0^\circ$-basis and the $45^\circ$-basis respectively can be achieved, which surpasses the visibility of 0.72 required for observing a violation of Bell’s inequality. These visibility estimations are matched by the results of several test scans. Since using such narrow filters drastically reduces the count rates, very long measurement times (15h - 20h) are necessary which puts hard requirements on the stability of the system. However, the system as described above, is now able to perform these tests.

### 7.4 Experimental Results and Discussion

#### 7.4.1 Correlation Measurements for the swapped Entanglement

In the experiment the four 4-fold count rates $N_{++}, N_{--}, N_{+-}$ and $N_{-+}$ for the correlation between photon 0 and photon 3 are observed. The expectation value of the correlation function is defined in the following way

$$E_{0,3}(\phi_0, \phi_3) = \frac{N_{++} - N_{--} - N_{+-} + N_{-+}}{N_{++} + N_{--} + N_{+-} + N_{-+}}. \quad (7.3)$$

Since the $N_{ij}$ are counts of Poissonian processes the statistical uncertainty is $\Delta N_{ij} = \sqrt{N_{ij}}$, and the statistical uncertainty of $E_{03}(\phi_0, \phi_3)$ can be determined via Gaussian error calculation. First a simplification is introduced by combining the two $N_{ij}$ with the same sign in Equation (7.3), because the uncertainty of the sum of two poissonian count values is transitive,

$$\Delta(N_{ij} + N_{kl}) = \sqrt{\sqrt{N_{ij}^2 + \sqrt{N_{kl}^2}}} = \sqrt{N_{ij} + N_{kl}}. \quad (7.4)$$

Then, analogous to the derivation given in Section G.1 of the statistics of the visibility, the uncertainty of the correlation coefficient is

$$\Delta E_{0,3}(\phi_0, \phi_3) = \frac{2\sqrt{(N_{++} + N_{--})^2(N_{+-} + N_{-+}) + (N_{++} + N_{--})(N_{+-} + N_{-+})^2}}{(N_{++} + N_{--} + N_{+-} + N_{-+})^2}. \quad (7.5)$$

As is customary the fidelity

$$F = \langle \Psi^- | \rho | \Psi^- \rangle \quad (7.6)$$

measures the quality of the observed state $\rho$ compared to the ideal quantum case $|\Psi^-\rangle$. Assuming that the observed state has the form

$$\rho = V|\Psi^-\rangle\langle\Psi^-| + (1 - V)\mathbf{1}, \quad (7.7)$$

where $V$ is the visibility of the state, which relates to the fidelity $F$ from Equation (7.6)as

$$F = \frac{3}{4} V + \frac{1}{4}. \quad (7.8)$$
Entanglement Swapping in Experiment

Figure 7.9: Observed entanglement fidelity obtained through correlation measurements between photons 0 and 3, which is a lower bound for the fidelity of the teleportation procedure. $\phi_0$, $\phi_3$ are the settings of the polarization analyzer for photon 0 and photon 3, and are set equal ($\phi_0 = \phi_3$). The minimum fidelity of 0.84 is well above the classical limit of $2/3$ and also above the limit of 0.79 necessary for violating Bell’s inequality. The fidelity is maximal for $\phi_0 = \phi_3 = 0^\circ, 90^\circ$ since this is the original basis in which the photon pairs are produced, as explained in Section E.1. Therefore the fidelity (or visibility) variation for the 2-fold correlations fully explains the variation of the shown fidelity. Thus the fidelity of the Bell-state analysis procedure is about 0.92, independent of the polarizations measured. The square dots represent the fidelity for the case that Alice’s and Bob’s events are space-like separated, thus no classical information transfer between Alice and Bob can influence the results. The circular dot is the fidelity for the case, that Alice’s detections are delayed by 50 ns with respect to Bob’s detections. This means, that Alice’s measurement projects photon 0 and 3 into an entangled state, at a time after they have already been registered.

Since the experimental correlation coefficient $E_{exp}$ is related to the ideal one $E_{QM}$ via $E_{exp} = V \cdot E_{QM}$ or with Equation (7.8) by $E_{exp} = (4F - 1)/3 \cdot E_{QM}$, $F$ can be estimated from measurements of the correlation coefficient $E_{exp}$. However, the state in Equation (7.6) assumes a rotationally invariant state, which is not quite the case in the experiment. Therefore, several measurements of $E(\phi_0, \phi_3)$ would be necessary to determine the full value of $F$.

A series of measurements were performed which show the very high fidelity for the correlation between photon 0 and 3 of at least $F = 0.85$, as can be seen in Figure 7.9. It seems rather natural, and this was concluded in private communication with Marek Zukowski, that already two measurements at perfectly non-orthogonal basis ($0^\circ, 45^\circ$) are sufficient to at least give lower bound on the fidelity of the system. This is also substantiated by the informational concept of entanglement developed by Caslav Brukner et al. [BZZ01]. Assuming that a two-qubit system can only carry two bits of information, then already two correlation measurements in independent bases will unequivocally define the entangled state. However, a complete theoretical analysis of the fidelity based on measured numbers is still missing.
7.4 Experimental Results and Discussion

Figure 7.10: Location of Alice’s and Bob’s detectors in respect with each other. The delay loops in front of Alice’s detectors were 10 m of fiber included for the delayed-choice experiment.

7.4.2 The Timing-“Paradox” of Entanglement Swapping

Interestingly, the quantum prediction for the observations of entanglement swapping does not depend on the relative space-time arrangement of Alice’s and Bob’s detection events. This leads to a seemingly paradoxical situation — as suggested by Peres [Per00] — when Alice’s Bell-state analysis is delayed long after Bob’s measurements. This seems paradoxical, because Alice’s measurement projects photons 0 and 3 into an entangled state after they have been measured! Nevertheless, quantum mechanics predicts the same correlations. Remarkably, Alice is even free to choose the kind of measurement she wants to perform on photons 1 and 2. Instead of a Bell-state measurement she could also measure the polarizations of these photons individually. Thus depending on Alice’s later measurement, Bob’s earlier results either indicate that photons 0 and 3 were entangled or photons 0 and 1 and photons 2 and 3. This means that the physical interpretation of his results depends on Alice’s later decision. However, the argument of A. Peres is that “...this paradox does not arise if the correctness of quantum mechanics is firmly believed.”

The dimensions of the experiment are sketched in Figure 7.10 and the travel time of all photons from the source to the detectors was equal within 2 ns. Alice’s detectors ($D_1, D_2$) and Bob’s detectors ($D_{0+}, D_{0-}, D_{3+}, D_{3-}$) where each located next to each other, but Alice and Bob were separated by about 2.5 m. This corresponding to a luminal signaling time of 8 ns between Alice and Bob. Since the time resolution of the detectors is < 1 ns, Alice’s and Bob’s detection events were space like separated for all measurements.
Entanglement Swapping in Experiment

The seemingly “paradoxical” delayed-choice experiment was performed by including two 10 m optical fiber delays for both outputs of the BSA. In this case photons 1 and 2 hit the detectors delayed by about 50 ns relative to Bob’s measurements, meaning that the entangling Bell-state measurement is performed long after photons 0 and 3 are registered. As shown in Figure 7.9, the observed fidelity of the entanglement of photon 0 and photon 3 matches the fidelity in the non-delayed case within experimental errors. Therefore, this result indicates that the time ordering of the detection events has no influence on the results.

The most important correlation coefficients and their corresponding fidelities are as follows:

<table>
<thead>
<tr>
<th>Measurement</th>
<th>$\phi_0 = \phi_3$</th>
<th>$E_{03}(\phi_0, \phi_3)$</th>
<th>Fidelity</th>
</tr>
</thead>
<tbody>
<tr>
<td>tomography45_451_00.dat (26.03.01)</td>
<td>45°</td>
<td>-0.785 ± 0.0364</td>
<td>0.839 ± 0.031</td>
</tr>
<tr>
<td>tomography00__001_00.dat (28.03.01)</td>
<td>0°</td>
<td>-0.896 ± 0.027</td>
<td>0.922 ± 0.023</td>
</tr>
<tr>
<td>delayedchoice45_451_00.dat (30.03.01)</td>
<td>45°</td>
<td>-0.800 ± 0.037</td>
<td>0.850 ± 0.032</td>
</tr>
</tbody>
</table>

The “tomography”-measurements measure the correlation for parallel analyzers, and the “delayedchoice”-measurement also included the delay of the Bell-state measurement. These results underline the high teleportation fidelities achieved with this setup.

7.4.3 Experimental Violation of Bell’s inequality

As described already in Section 3.2, the Clauser-Horne-Shimony-Holt (CHSH) inequality [CHSH69] is a variant of Bell’s Inequality, which overcomes the inherent limits of a lossy system using a fair sampling hypothesis. It requires four correlation measurements performed with different analyzer settings and has the form:

$$S = |E_{03}(\phi'_0, \phi'_3) - E_{03}(\phi'_0, \phi''_3)| + |E_{03}(\phi''_0, \phi'_3) + E_{03}(\phi''_0, \phi''_3)| \leq 2,$$  \hspace{1cm} (7.9)

$S$ being the “Bell parameter”, $E_{03}(\phi_0, \phi_3)$ being the correlation coefficient. The quantum mechanical prediction for photon pairs in a $\Psi^-$ state is $E_{QM}^{\Psi^-}(\phi_0, \phi_3) = -\cos(2(\phi_0 - \phi_3))$. The settings ($\phi'_0, \phi'_3, \phi''_0, \phi''_3$) = (0°, 22.5°, 45°, 67.5°) maximize $S$ to $S_{QM}^{\Psi^-} = 2\sqrt{2}$, which clearly violates the limit of 2 and leads to a contradiction between local realistic theories and quantum mechanics [Bel64].

The results of these four correlation measurements on photon 0 and 3 in the experiment are given in Table 7.1. Including the values into above inequality (7.9) leads to a value of the Bell-parameter $S = 2.421 \pm 0.091$, which clearly violates the classical limit of 2 by 4.6 standard deviations as measured by the statistical error. This degree of violation of 4.6 standard deviations means that the chance of obtaining a result that would not violate Bell’s inequality is about 1 in $10^{-10}$.

This is a clear violation of Bell’s inequality for photons that never “meet”, let alone interacted, meaning the local realistic theories can not describe this correlation, except for the so called detection loophole, which is usually surpassed with a fair-sampling hypothesis, which states that the actually measured photons represent a fair sample of all...
### 7.4 Experimental Results and Discussion

#### Table 7.1: Results of the four count rates and the correlation coefficients necessary for the experimental test of the CHSH version of Bell’s inequality. The differences in the correlation coefficients come from the higher correlation fidelity for analyzer settings closer to 0° and 90°, as explained in Section E.1. Each measurement is taken from separate scans, which consisted of four points, each lasting for 16000 s. The four data files are: bellmeasurement225\_456\_00.dat (22.03.01), bellmeasurement675\_456\_00.dat (23.03.01), bellmeasurement225\_007\_00.dat (24.03.01), bellmeasurement675\_006\_00.dat (25.03.01).

<table>
<thead>
<tr>
<th>$\phi_0$</th>
<th>$\phi_3$</th>
<th>$N_{++}$</th>
<th>$N_{--}$</th>
<th>$N_{+-}$</th>
<th>$N_{-+}$</th>
<th>$E_{03}(\phi_0, \phi_3)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>45°</td>
<td>22.5°</td>
<td>47</td>
<td>103</td>
<td>162</td>
<td>32</td>
<td>$-0.541 \pm 0.045$</td>
</tr>
<tr>
<td>45°</td>
<td>67.5°</td>
<td>27</td>
<td>116</td>
<td>121</td>
<td>37</td>
<td>$-0.575 \pm 0.047$</td>
</tr>
<tr>
<td>0°</td>
<td>22.5°</td>
<td>27</td>
<td>101</td>
<td>131</td>
<td>26</td>
<td>$-0.628 \pm 0.046$</td>
</tr>
<tr>
<td>0°</td>
<td>67.5°</td>
<td>122</td>
<td>16</td>
<td>33</td>
<td>132</td>
<td>$+0.677 \pm 0.042$</td>
</tr>
</tbody>
</table>

photons emitted by the source. So one might be prepared to accept that a source may somehow produce photons via an "elementary" process, which leads to the strong correlations of the quantum entanglement. But it seems, that things become much stranger now, as entanglement is observed between photons which never even met.

As a consequence, there is the feeling amongst people involved in quantum reality matters (e.g. D. Greenberger, A. Aspect, L. Vaidman, A. Zeilinger, etc.), that experiments such as the entanglement swapping presented here, allow to rule out further kinds of realistic models and might even lead to a new variant of Bell’s inequality. These ideas are currently being investigated.

#### 7.4.4 Some Deficiencies of this Teleportation Setup

The setup has two major deficiencies, which in the past lead to an ongoing debate [BK98, BPD98, RS01] about the quality of teleportation experiments with correlated photons produced by SPDC. The argued points are as follows:

**The teleportation efficiency is inherently limited to 25%.** The Bell-state analyzer described above, which is based on linear optics, is only able to detect one of the four Bell-states and therefore the efficiency of the teleportation is limited to 25%. However, this does not limit the fidelity of the teleportation. As explained by Bouwmeester et al. [BPWZ00], the teleportation efficiency measures the fraction of cases in which the procedure is successful and the fidelity characterizes the quality of the teleported state in the successful cases. For example, loss of a photon in this case leads outside the two-state Hilbert space used and thus reduces the efficiency and not the fidelity.

**The results are due to postselection of suitable parts of the full state.** The non-deterministic nature of the photon pair production implies an equal probability for producing two photon pairs in separate modes (one photon each in modes 0,
1, 2, 3) or two pairs in the same mode (two photons each in modes 0 and 1 or in modes 2 and 3). The latter can lead to coincidences in Alice’s detectors behind her beam splitter. We exclude these cases by only accepting events where Bob registers a photon each in mode 0 and mode 3. It was shown by Zukowski [Zuk00a], that despite these effects of the non-deterministic photon source experiments of our kind still constitute valid demonstrations of nonlocality in quantum teleportation.

### 7.4.5 Independence of the two Photon Pairs?

One might doubt the independence of the two initial entangled photon pairs 0-1 and 2–3, as is assumed in the quantum mechanical description of entanglement swapping, since the two pairs were produced by the same laser pulse in the same down-conversion crystal. For instance, the two photons which interfere in the BS could take on a phase or polarization coherence from the UV laser. It is to be noted, that the UV mirror was placed 13 cm behind the crystal, which greatly exceeds the pump pulse width of \( \sim 60 \mu m \). Furthermore it is important to note, that theory does not hint any kind of such correlation or coherence.

An argument against any “dependence” of the two photons is, that the 2-fold correlations of the two photon pairs measured separately are already able to violate Bell’s inequality at a high degree. At present, no four-photon state is conceivable, where two 2-photon subsystems are able to violate Bell’s inequality, and at the same time show entanglement between the two subsystems, as is shown in [SG01].

However, to shed some light on this issue, the relative phase drifts due to instabilities of the optical paths of photon 1 and 2 were measured with a Mach-Zehnder interference experiment. As was described in the adjustment procedure of the fiber beam splitter (Section 7.1.1), the beam of an adjustment laser was split up, fed into the optical fibers and recombined in the beam splitter. The interference of the two beams lead to intensity fluctuations in the outputs of the beam splitter due to the phase modulation of the piezo actuator placed in one of the input arms of the beamsplitter, which were detected with a silicon photo diode and observed on an oscilloscope. A computer program implemented in LabVIEW permanently measured the interferogram in time intervals of \( \tau_0 \), and kept track of the position of the fringe maximum and minimum. Consequently the relative drift of the phase between the two arms was recorded over many hours, see Figure 7.11(left).

The statistical analysis of the temporal phase variation was done using the Allan variance\(^2\) [All87, Jen97], which seems an appropriate measure. As opposed to the standard variance, the Allan variance is calculated as follows

\[
\sigma_y^2(n) = \frac{1}{2(M - 2n + 1)} \sum_{i=1}^{M-2n} (y_{i+n} - y_i)^2
\]

(7.10)

where \( \sigma_y^2(n) \) is the variance between the samples \( y \) with an difference in their index \( n \),

\(^2\)The Allan variance was developed for characterizing the frequency and time stability of high precision clocks. It was necessary, because the standard variance would not converge for measuring the characteristic drifts of clocks. The average over the difference of samples taken with a fixed spacing allows to estimate the stability over the time of this spacing. Therefore the Allan variance seems well suited for characterizing the statistics of the phase drift in an interferometer.
7.4 Experimental Results and Discussion

Figure 7.11: Drift of the relative path lengths of photons 1 and 2 before meeting in the Bell-state analyzer. (left:) Shows the accumulated phase during several hours, scaled in multiples of the wavelength of the laser, which was 788 nm. (right:) Given is the calculation of the root of the Allan variance ($\sigma_y(\tau)$) for different spacings $\tau = n\tau_0$ between two samples, again given in multiples of the wavelength. The straight line is an exponential function $f(\tau) = c\tau^{0.5}$, where $c$ is an amplitude constant, which represents the variation of $\sigma_y(\tau)$ with $\tau$ for the case of random walk noise.

and $M$ is the total number of samples. The calculated Allan variance of the phase drift for different spacings $\tau = n\tau_0$ is shown in Figure 7.11-right on a double-logarithmic scale, which allows to tell the statistical behaviour of the drifting motion. The motion is related to the $\tau$-dependence of the Allan variance in the following way: $\sigma_y^2(\tau) \propto \tau^\mu$, where $\mu = 1$ for random walk noise, $\mu = 0$ for flicker noise and $\mu = -1$ for white noise.

So according to the analysis, the phase approximately drifted in a random walk behavior, accumulated a 1σ statistical drift of one wavelength within 400 s, and had a maximum drift of 15 wavelengths during 10 h. In a single measurement which lasted 16000 seconds, any (hypothetical) phase relation between the two photons that interfered in the BSA would have been completely washed out. Therefore the contribution of such a phase relation to the outcome of the experiments can be ruled out, which is confom with present theory.

7.4.6 What about the Classical Teleporter?

A teleportation device which does not work as required by QST, e.g. the classical teleporter described in Section 6.1.2, would run into serious problems with the results obtained in this entanglement swapping experiment.
Firstly, since the correlations between the photons 0 and 3 which became entangled violated Bell’s inequality, the information gained in the teleportation scheme can only be small. This is necessitated by the Bell-theorem, which states, that only particles with fundamentally undefined individual properties can show a violation of the inequality. Since a classical teleporter would have to gain information about the individual properties of the teleported particle, the violation would be a difficult problem to solve.

Secondly, in the “quantum”-entanglement swapping, the ordering of the different measurements in space time is irrelevant. However, a classical teleporter (as described in Section 6.1.2) could at the best work in a single direction, i.e. from Alice to Bob, with the maximum signaling speed, i.e. the vacuum speed of light. Since Alice’s and Bob’s measurements were space-like separated, or even worse, in the “timing paradox”-experiment, Alice’s Bell-state measurement was even after Bob’s measurements, a device such as the classical teleporter would have perform really well on the timing trick.

Therefore the results observed in this entanglement swapping experiment definitely prof the quantum nature of teleportation.
Towards More-Complete Teleportation with Switched Modulator

In the experiments on quantum state teleportation described above only the simplest Bell-state analyzer was implemented, which is able to identify only one out of the four Bell-states. The advantage is that the optics is very simple, and also no active switching of the phase or the polarization on the receiving photon, as is necessary in the full teleportation protocol, is required. The enhancement of the entanglement swapping setup to “more-complete teleportation” as shown in Figure 8.1 will be described.

As already mentioned in Section 7.1, a Bell-state analyzer based on linear optical elements can only achieve a maximal efficiency of 50%. This means that a Bell-state analyzer able of detecting two of the four Bell-states is possible and already exhaustive. A Bell-state analyzer capable of detecting the two states is shown in Figure 8.1. The identification of the antisymmetric $|\Psi^-\rangle$-state is straightforward, as in this case the photons will take separate outputs and can only lead to a coincidence detection between one detector on each side. The symmetric $|\Psi^+\rangle$-state (also shown in Figure D.2) will let the photons both take the same output of the beam splitter, however they will still have orthogonal polarizations in the $HV$-basis, and therefore the two photons will take both outputs either in polarizer 1 or in polarizer 2 and lead to corresponding coincidence detections.

8.1 Implementation of the more-complete Bell-state Analyzer

The polarizing beam splitters are configured for fiber connections, thus allow easy combination with the existing fiber beam splitter. The polarization controllers are inline Polarite-controllers from General Photonics, USA, (see Figure B.2 on page 86). In principle, the adjustment of the polarization rotation in the fibers can be performed like in the case of the simpler BSA, which is done with an adjustment laser observing its interference at the beam splitter (see Section 7.1.1). There it was sufficient to adjust the fiber for the polarization which was actually analyzed for photons 0 and 3. However, in the more-complete BSA it is necessary to compensate the fibers before the beam-splitter for the full polarization space, i.e. for $HV$-basis as well as the $45^\circ$-basis, and to compensate the fibers from the beam splitter to the polarizers for the $HV$-basis. Since one does not have direct
Figure 8.1: Setup for the “more-complete” teleportation. The fiber beam splitter for the Bell-state analysis is extended with polarizing beam splitters in each of its arms, which also requires extra polarization controllers for compensating the polarization rotation of the fibers. There are two wave plates placed before one input of the BSA in order to perform a full compensation of any polarization rotation. The logic electronics compares all detection signals and extracts if a Bell-state occurred and which it was. This result is conveyed to the electro optic modulator, which performs the necessary phase shift on the polarization of receiving photon 3, depending on which Bell-state was measured.
access to the light within the fibers, a suitable procedure must be conceived which allows
to set the polarization controllers. For help in finding a correct procedure for all the fibers
and other components a simulation program was written in LabVIEW (Figure 8.2), which
allows to play around with different configurations and to test the alignment procedures.

As it turned out, a good combination is to use the fiber polarization controllers for align-
ing the 0°-polarization (HV-basis), and then independently align the 45°-polarization via
a quarter wave plate oriented at 45° and by rotating a half wave plate. This combination
effectively allows to adjust the phase between the 0° and 90° polarization. The adjustment
of the different controllers must be performed in a fixed sequence, as follows:

1. Align polarization controller 2 by minimizing the interference of the adjustment laser
   beam, polarized at 0° in input 1 and 90° in input 2.

2. Align polarization controllers 1 and 2’ for maximum interference contrast of their
two output signals, so they correspond to H and V polarization.

3. Rotate the half wave plate in front of input 2 by minimizing the interference of the
adjustment laser beam, polarized at 45° in input 1 and 135° in input 2.

8.2 Modulating the Receiving Photon

When the more-complete Bell-state procedure is used, it is necessary to actively perform
a phase modulation of receiving photon 3. This is best seen from the state of the system
after the projecting Bell-state measurement, which is as follows

$$|\Psi_{total}\rangle = \frac{1}{\sqrt{2}} \left[ (\alpha|H\rangle_3 - \beta|V\rangle_3)|\Psi^+\rangle_{12} - (\alpha|H\rangle_3 + \beta|V\rangle_3)|\Psi^-\rangle_{12} -
(\alpha|V\rangle_3 + \beta|H\rangle_3)|\Phi^+\rangle_{12} + (\alpha|V\rangle_3 - \beta|H\rangle_3)|\Phi^-\rangle_{12} \right],$$

(8.1)

the details of the teleportation procedure are described in Section 6.1. In the experiment
the two states $|\Psi^-\rangle_{12}$ and $|\Psi^+\rangle_{12}$ will be detected, and a Pockels cell will be used for
introducing conditional phase shift between the H and V polarization of photon 3. In the
case of $|\Psi^-\rangle_{12}$, the modulator is switched off and induces no phase change between H and
V polarization, and photon 3 directly carries state input state $\alpha|H\rangle + \beta|V\rangle).$ When the
$\Psi^+\rangle_{12}$ is detected, the modulator is activated to produce a phase difference of $\pi$ between
the H and V polarization, so that the state of photon 3 is transformed into the input
state. Hence the modulator must switch between a wave delay of 0 and $\lambda/2$ ($\lambda$ being the
wavelength of the photons).

The use of the fast electro optic modulator which operates on the entangled photon 3
requires a full polarization compensation of the transmission of photon 3, because the
orientation of the modulator must always be in the HV-basis, regardless of the direction at

---

1The Pockels cell consists of crystals (such as KDP, etc.) which vary their birefringence with an applied
electric field. The crystals have a natural optic axis perpendicular to the beam direction, and the delay
between the fast and the slow axis varies dependent on the modulation voltage.
**Figure 8.2:** Simulation of the polarization compensation in the fiber optic beam splitter. The polarization is represented in polar coordinates on the Poincare sphere (see Figure 3.1 on page 14). Any polarization rotating element, i.e. the fibers, the polarization controller and extra wave plates in the inputs of the beam splitter, are characterized by a rotation axis represented in polar coordinates and a rotation angle, and each element performs a rotation of the polarization state on the Poincare sphere (this is done for algorithmic reasons by transforming the polar coordinates internally to Cartesian coordinates, applying the rotation matrix and transforming back to polar coordinates). The rotation axes of the wave plates and the polarization controller are kept in the equatorial plane of the sphere, which corresponds to linear polarizations. Each input fiber of the beam splitter is tested with the two polarizations $A = 0^\circ$ and $B = 45^\circ$ respectively. When the fibers are fully compensated, both these polarizations must arrive parallel in respect with each other at the beam splitter after traveling through the two fibers, which is measured by the interference visibility.
which photon 3 is finally analyzed. It turns out, that the compensation of the birefringences in the fiber and the modulator for the full polarization space such that at the same time the $0^\circ$-polarization (HV-basis) and $45^\circ$-polarization are both aligned, can be performed independently. A simulation with a program similar to the one used for the Bell-state analyzer alignment (Figure 8.2) made this clear. The light signal used for the alignment can either be an adjustment laser or the down-conversion photon themselves, which is polarized before entering the fiber with a separate polarizer, and analyzed with a polarizer before and behind the modulator respectively.

1. The input polarization is set to $0^\circ$-polarization, and an auxiliary polarizer is placed in front of the modulator, also set at $0^\circ$-polarization (or $90^\circ$-polarization)\(^2\). The total transmitted signal is maximized (or minimized) via the polarization controller 3, hence compensating the fiber for the HV-basis.

2. The input polarization is set at $45^\circ$-polarization, and the polarizer behind the modulator is oriented at $45^\circ$-polarization (or $135^\circ$-polarization). The total transmitted signal is maximized (or minimized) by tuning the DC-bias of the modulator, hence compensating the polarization rotation of the fiber for the $45^\circ$-basis.

Note that in the experiment, photon 3 will have to be delayed sufficiently, such that the modulator can in time before photon 3 reaches it. The necessary delay must include the detection process in the Bell-state analyzer, the signal throughput time in the coincidence logic, the transmission time from Alice to Bob, and the switching delay of the actual modulator. These signal delays easily add up to 150 ns, which corresponds to a delay of photon 3 of about 30 m of optical fiber.

### 8.3 The Programmable Coincidence Logic

Since the more-complete Bell-state analyzer has four detectors which can fire in several possible combinations, a relatively complicated logic circuit is required (complicated at least in terms of fast NIM-logic). The realization in NIM-modules would be a large effort, as several 3-fold and 2-fold coincidences are necessary and also an adjustment mode must be foreseen, for determining the 2-fold coincidences. Summarizing, the requirements of the logic are:

- **High speed:** The detector pulses which have a few nano-seconds pulse width must be correlated. This requires at least the fastest TTL-logic family 74ACXX, or better the faster ECL-logic (TTL and ECL are defined in Section G.4).

- **Complicated logic:** The required logic is relatively complicated with several different levels of gates. This can lead to timing problems of the signals. Generally, wiring the signals on a printed circuit board for high speed logic is always difficult.

\(^2\)Usually, the alignment of a signal minimum yields better results than for the maximum. However, it is always to be checked that the signal is still present.
Towards More-Complete Teleportation with Switched Modulator

**Figure 8.3:** Block diagram of the programmable coincidence logic system based on a CPLD (configurable programmable logic device). This system was designed to be very general, so that it can be used in different types of experiments, only by appropriately programming the CPLD via the JTAG-link. The number of eight inputs and outputs was considered sufficient and is not the limit of pins of the device. The two select signals are slow inputs which can be used for switching the logic between different device configurations already programmed into the device, such as an adjustment mode and a measurement mode. All the signals are TTL levels.

Although the development of a logic circuit based on TTL or ECL is straight-forward, the difficulties of coping with high speed logic, and also the inflexibility of a discrete circuit led to use a programmable logic device instead. One disadvantage is however, that these programmable logic realize synchronous logic and therefore requires a clock signal. In the experiment this clock is generated from the 76 MHz pulse rate of the fs-laser system.

The device used here is the XC9536XL CPLD (configurable programmable logic device), from Xilinx Inc. USA, which operates at 3.3V and can work with clock frequencies as high as 200 MHz, which is well above the 76 MHz clock rate of the fs-laser system. This device contains about 4000 logic gates, which can all be configured and connected with an instruction file which is loaded into the CPLD via a parallel cable from a personal computer. Once the chip is programmed, it keeps the configuration. The CPLD can be reconfigured arbitrarily often (approx. 10000 times), which gives a high flexibility in this and future experiments, since any new logic can be implemented simply by downloading a new configuration into the chip via the JTAG-link. The desired logic function is programmed in VHDL (very high density hardware description language), which is similar to a normal programming language, and then compiled by a software package from Xilinx into a binary instruction file for the CPLD.

A very general and open hardware for the implementation of the CPLD was designed (see Figure 8.3), in order to allow use of this coincidence logic in several different experiments. It has eight inputs for detector signals, eight outputs giving the coincidence pulses which are counted externally, two static selector signal inputs, and a clock signal input.

As a first step towards more-complete teleportation, the logic was configured such that it is able to determine all coincidences of a static entanglement swapping experiment, i.e. the extension of the setup in Figure 7.2 with a more-complete Bell-state analyzer, but without the switched modulator. As can be seen from Equation (6.8), depending on the
result of the Bell-state, the measurement on photons 0 and 3 show the strong correlations for different but perfectly entangled states. The experiment will contain eight detectors, with two detectors for photons 0 and 3 each, called $D_{0+}$, $D_{0-}$ and $D_{3+}$ and $D_{3-}$, and the four detectors in the more-complete Bell-state analyzer, $D_{1+}$, $D_{1-}$, $D_{2+}$ and $D_{2-}$. The measurement-configuration of the logic measures all relevant 4-fold coincidences. Since there are four different combinations of the $D_0$ and $D_3$ detectors and two possible results of the Bell-state measurement ($\Psi^-_{12}$ or $\Psi^+_{12}$), eight relevant 4-fold coincidences must be observed. The adjustment-mode of the logic requires that all possible 2-fold events produced by the correlated photons must be measured, which are the 2-folds of $D_{0+}$, $D_{0-}$, $D_{3+}$ and $D_{3-}$ with the central detectors in the BSA. Also for adjustment the independent 2-fold rate between the detectors sitting in the two outputs of the beamsplitter are important. And finally, in a further mode of the logic, the single count rates of all eight detectors must be measured. The logic is switched between these three different configurations via digital signals applied to the “select signals”. The VHDL code files of this logic are given in appendix F.

First measurements in the entanglement swapping setup performed at the same time with the new programmable logic and with NIM-logic showed good agreement between the two systems. One difference is that due to the synchronous logic design in the CPLD the effective coincidence window (see Section C.3) is defined by the 13 ns period of the clock which is quite large compared to the ca. 4 ns coincidence window of the NIM-logic. Allthough this leads to higher background counts, the flexibility and simplicity of the programmable logic is invaluable for such experiments with correlations between many photons.

8.4 Progress of the Experiment

At the time of writing up this thesis the more complete teleportation experiment is under way. Most of the necessary components are already in the lab and tested, such as the fiber optic components for the BSA or the coincidence logic. The implementation of the modulator is still not resolved, since the originally planned device which was used in the QKD-experiment (Chapter 5) turned out to be faulty, and needs to be replaced. But I am sure that this experiment will be finished within the near future.
Towards More-Complete Teleportation with Switched Modulator
9 Concluding Outlook and Visions

The work presented in this thesis demonstrates fascinating applications from the field of quantum information, as well as the answer to fundamentally important questions of the nature of quantum physics. I will summarize the near-term outlook for future experiments as well as the long term perspective (which is rather speculative) leading to a vision of a quantum information world.

9.1 Entanglement-based Quantum Key Distribution

The advantages of entanglement-based quantum key distribution over the faint laser procedures are obvious and the experiment presented here demonstrates that it is feasible to realize such a system. Indeed, the system presented here is already the starting point for the development of an industrial test system, which is being pursued, among others, in our research group in a collaboration with an industrial partner.

Further research of entanglement-based quantum key distribution will aim at covering larger distances. This can be achieved via changing to longer wavelengths of the photons, enabling to use low-loss telecom optical fibers, or by changing to free-space photon transmission. The ultimate goal is to use satellite links, which will allow to establish quantum cryptography between stations sitting at virtually any location on the planet or in space. In the long run, it seems very likely that quantum key distribution will be part of tomorrows communication technology.

From a visionary standpoint, the advantages of entanglement-based quantum key distribution are overwhelming. The distance that can be covered by a single-qubit link is rather limited. With entanglement, in principle, by realizing so-called quantum repeaters (described below), it appears to be possible to cover any distance by combining many short links to one large one. Even more fascinating will be a future when entangled systems (e.g. qubits) may be stored over long times. Then it will be possible to transport a quantum memory carrying entangled systems around, and at any time and any location use these for quantum key distribution. Also it will be possible to implement quantum networks, where each qubit of the memory is entangled with a corresponding qubit kept at a central institution, and which by implementing entanglement swapping (see below) can be transformed into entanglement between any two parties willing to communicate securely.
9.2 Entanglement Swapping and Quantum State Teleportation

Quantum state teleportation and entanglement swapping are of great fundamental interest since it once more highlights the essential features of the quantum world. In the near future it is planned to perform an experiment extending the distance of teleportation to about 600 m from one side of the river Danube to the other. The quantum channel between Alice and Bob will be realized with an optical fiber laid in a tunnel under the river and the classical channel will be implemented with a microwave radio link above the river. Another planned experiment is to show teleportation and entanglement swapping with two truly independent photon pairs, by using two separate lasers for producing each of the down-conversion photon pairs.

However, entanglement swapping or quantum state teleportation also have a number of exciting applications in the new field of quantum communication and information processing, as listed below.

Communication between Quantum Computers: Should quantum computers ever exist, then quantum state teleportation will most certainly be used for interconnects between two devices, or even between different parts within one device. Most probably, quantum registers will be based on massive systems, e.g. atoms or ions, which will be localized in space. It will be necessary, that the transfer of the quantum state from one register to another is implemented by means of teleportation, since the actual qubits must not be moved and at the same time their states are not measured.

Quantum Repeaters: Quantum repeaters allow entanglement to be distributed over larger distances than it would be possible with a single link. Entanglement swapping is one key element of quantum repeaters, which were proposed by Briegel et al. [BDCZ98], as entanglement swapping leads to entanglement between two initially independent separated particles. The second ingredient required for quantum repeaters is the purification of entanglement [BEZ00, PSBZ01], where from an initial set of entangled pairs a subset of pairs is distilled with a higher quality of entanglement. A way of experimentally realizing purification was recently discovered by Jian-Wei Pan et al., a the experiment is currently pursued in our research group by himself and Sara Gasperoni.

Third Party Cryptography and Communication: Quantum state teleportation and entanglement swapping always has a sender station Alice sitting between the two communicating parties, and she must perform her measurements and reveal her results in order that the procedure works. However, Alice’s results do not allow any conclusions about the actually transmitted quantum states. This means, that Alice may act as a third party who decides if or if not two users (or more) communicate. Such schemes are interesting for certified communication between two parties.
Quantum Networks: A quantum network allowing to establish entanglement between two arbitrary users at any distance may be realized one day with the help of long-time quantum memories and entanglement swapping. A provider of quantum entanglement could provide users with a register of qubits which are each entangled with qubits sitting at a central location. If two users wish to have entangled particles for any kind of quantum communication, then the provider can “entangle” their memories by performing a series of Bell-state measurements necessary for entanglement swapping on the qubits sitting at the center. Once the entanglement is established, the users have completely secure means of communicating. These ideas of quantum networks are known as the “engineering of entanglement”, and are developed among others by the group of P. Knight from London [BVK98], and are summarized in [BEZ00].

Probabilistic Instantaneous Quantum Computing: Instantaneous quantum computing, developed by C. Brukner and A. Zeilinger [BPS+01], is at least one interesting application where QST implies a time gain over a classical procedure. It is realized by feeding an entangled state into the input of a quantum computer and let it perform the calculation. Note that the entangled state is actually an undefined state and therefore also the output of the computation will be undefined. However, as soon as the required input is known, it can be teleported onto the entangled state which was fed into the quantum computer. If, by chance, the Bell-state measurement gives the one single result which requires no unitary transformation, then immediately the output of the quantum computer will be projected into the result for the input, and the computation is performed instantaneously.

Linear Optics Quantum Computing: Just to throw around with some even more complicated terms, this interesting use of today technically feasible teleportation will be described. Note first, that with linear optical elements the Bell-state analyzer required for teleportation can only be realized with an efficiency of 1/2 (detecting two of the four Bell-states), which limits the efficiency of the teleportation. It has been shown by Milburne et al. [KLM01], that already the 1/2–efficient teleportation (i.e. more-complete teleportation) is sufficient for implementing a probabilistic c-not logic gate, the long-sought-for basic switching element comprising the heart of quantum computers.

The realization of all these visions still requires lots of imaginative research since most of the questions of how to realize these systems is open. It is clear, that the type of photon experiments presented in this work are certainly not suitable for actual applications of these ideas, but nevertheless they allow us to already see some of the visions work in the lab.
A Spontaneous Parametric Down-conversion

At present, the most efficient source of entangled photons is spontaneous parametric down conversion. The exploited effect is due to the \( \chi^{(2)} \) optical nonlinearity of certain media, such as KDP, LiIO\(_3\), KNbO\(_3\), LiNbO\(_3\) [TW01]. Recently new materials such as periodically poled lithium niobate (PPLN) have shown unprecedented effective nonlinearities [TdRT+01]. Nonlinear optical phenomena have long been used for wave mixing of light fields, such as frequency doubling or frequency summation/difference. Parametric down-conversion is the scheme in which a UV pump field is mixed with two IR fields, known as the signal and idler beam. For strong beams, all nonlinear phenomena can be understood by the classical theory of electro-magnetic waves. However, a quantum mechanical description of the interaction leads to nonclassical features at low light levels, such as the squeezing of phase quadratures of light or spontaneous photon pair production. The latter was first observed in 1970 [BW70] and has been used for a range of fundamental photon experiments by Ou and Mandel [OHM87, OM88]. Spontaneous parametric down-conversion (SPDC) allows to generate different kinds of entanglement such as energy-time entanglement, momentum or mode entanglement and polarization entanglement [TW01].

In a photon picture, down-conversion can be viewed as a decay of a pump photon into two photons under conservation of energy and momentum. Energy conservation requires that

\[
h\nu_{\text{pump}} = h\nu_{s-\text{beam}} + h\nu_{i-\text{beam}},
\]

where \( \nu \) is the frequency of the pump, s(ignal)-beam and i(dler)-beam wave respectively. And momentum conservation requires, that

\[
h\hat{k}_{\text{pump}} = h\hat{k}_{s-\text{beam}} + h\hat{k}_{i-\text{beam}},
\]

where \( \hat{k} \) is the momentum of pump, s- and i-beam photon, and \( |\hat{k}| = \frac{n2\pi}{\lambda} \) with the vacuum wavelength \( \lambda \) and the refractive index \( n \) of the media. These two conditions govern the wavelengths and the direction of the emerging photons from the “decay” of pump photons. Note, that due to dispersion of any transparent medium, \( n \) always increases with \( 1/\lambda \). Therefore the momentum conservation can only be fulfilled in birefringent crystals, where the differences in the refractive indices of the extraordinary and ordinary polarization mode are exploited. In the description based on wave theory this is called phase matching, see for example [DGN90, Yar89].
A. Spontaneous Parametric Down-conversion

Negative uniaxial crystal: $n_o > n_e$
Refractive Index for $\lambda = 0.40466 \ \mu m$ $n_o = 1.69267$, $n_e = 1.56796$
Refractive Index for $\lambda = 0.81890 \ \mu m$ $n_o = 1.66066$, $n_e = 1.54589$
Point group: 3m
Transparency range: 0.189 - 3.5 $\mu m$

Table A.1: Some optical properties of BBO [DGN90].

A.1 Generation of polarization entangled photons with type-II SPDC in BBO

The experiments described in this work are based on polarization entangled photons which are produced by so called type-II SPDC. Type-II means that the two emerging signal and idler photons have extraordinary polarization and ordinary polarization respectively. The crystal used is BBO ($\beta$-BaB$_2$O$_4$). It is cut in such a way, that the case of down-conversion with degenerate wavelengths, i.e. where $\lambda_{o-beam} = \lambda_{e-beam}$, is non-collinear. Some optical properties of BBO are given in Table A.1.

It turns out, that the two beams emerge from the down-conversion crystal on cones, see Figure A.1. The photon pairs found at the two intersection lines of the cones are polarization entangled when the individual photons carry no information whether they originate from the o-beam (horizontal polarization) or the e-beam (vertical polarization) cone, yet they will always have opposite polarization. To see entanglement in a practical system it is necessary to perform extra compensation of the dispersion produced by the birefringence in order to erase some timing information of the photons, as will be discussed in Section A.3. This type of source was developed in 1995 [KMW+95], and so far is the most effective source for polarization entanglement.

A.2 Geometry of the down-conversion light

In order to find the direction of the down-conversion for a certain set of $\lambda_{pump}$, $\lambda_{o-beam}$ and $\lambda_{e-beam}$, the orientation of the optic axis of the crystal with respect to the pump beam is critical. The phase-matching can be found by expressing applying polar-coordinates $\theta$ and $\varphi$ (see Figure A.2) and taking the dependence of the refractive index $n_e$ on $\theta$ on the e-beam into account (Equation 2.14 in [DGN90]). In his PhD-thesis, Gregor Weihs [Wei99] performed calculations with a Matlab program based on the crystal parameters and Equations (A.1) and (A.2) and determined the geometry of the emerging light depending on $\theta$. Interestingly, the phase matching itself is not affected by $\varphi$, however, the effective nonlinearity strongly depends on $\varphi$, hence a suitable value of $\varphi$ must be chosen. In the experimental setup the desired angle between the intersection lines of the cones is chosen to be 6° (full angle). It turns out, that at this particular angle the two cones intersect roughly at a right angle, which seems a good condition to go for. The cutting angles of the crystals necessary for achieving this geometry are given in Table A.2.
A.2 Geometry of the down-conversion light

**Figure A.1:** A schematic overview of type-II SPDC (taken from [Wei99]). The phase matching condition governs the “decay” of the photons such, that they emerge from the crystal on cones. In the degenerate case, i.e. when the two photons have the same wavelength, the intersection lines of the cones yield entangled photons. This is when the photons carry no information about whether they emerged with horizontal or vertical polarization, yet they will always have opposite polarization.

**Figure A.2:** Polar coordinate system for a describing the refractive properties of an uniaxial crystal. $\vec{K}$ is the light propagation direction, $Z$ is the optic axis, and $\theta$ and $\phi$ are the coordinate angles. The principal plane is defined by the $Z$-axis and by the wave vector $\vec{K}$. Light with polarization normal to the principal plane is called the ordinary beam ($o$-beam), and light with polarization parallel to the plane is called extraordinary beam ($e$-beam).

<table>
<thead>
<tr>
<th>Laser Type</th>
<th>$\lambda_{pump}$, $\lambda_o = \lambda_e$ [nm]</th>
<th>$\theta$ [°]</th>
<th>$\phi$ [°]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ar$^+$-ion</td>
<td>351.1 nm, 702.2 nm</td>
<td>50</td>
<td>30</td>
</tr>
<tr>
<td>Ti:SA, frequency doubled</td>
<td>394.4 nm, 788.8 nm</td>
<td>43.5</td>
<td>30</td>
</tr>
</tbody>
</table>

**Table A.2:** Cutting angles of the BBO crystal used for type-II SPDC with two types of laser systems. The Ar$^+$-ion system is a gas laser running in continuous wave mode. The Ti:SA laser is a frequency doubled mode lock laser, producing pulses with 100 - 200 fs pulse width.
More recently in his master-thesis, Guido Czeija [Cze01] has performed calculations on the geometry of the down-conversion light for the case of down-conversion produced by fs-laser-pulses. The difference to the CW case is, that the fs-pulses have a finite bandwidth (e.g. Gaussian-shaped laser pulses, centered at a wavelength of $\lambda = 394.4\text{ nm}$, with a width of $\Delta T_{2\sigma} = 100\text{ fs}$ have a corresponding spectral bandwidth of $\Delta \lambda_{2\sigma} = 3.3\text{ nm}$). If this is taken into account, then the calculation shows that each spectral component of the pump-beam produces a different distribution of down-conversion light, see the diagram in Figure A.3. The circle shown in the diagram corresponds to the region of down-conversion “seen” by a free-space-to-single-mode fiber coupling system.\footnote{The numerical aperture of the fiber coupler can be estimated by the following relation: $\sin (NA_F)f = \sin (NA_C)L$, where $NA_F = 0.11$ is the numerical aperture of the single mode fiber, $f = 11\text{ mm}$ is the focal length of the coupling lens, $L = 780\text{ mm}$ is the distance from the BBO crystal to the coupler. Then $NA_C = 0.00155$ or $NA_C = 0.089\text{°}$.}

Most noticeably, diagram A.3 shows that already a shift of the pump wavelength by $\pm 1\text{ nm}$ brings the components of one of the two cones far away from the region coupled into a single mode fiber. In conclusion this means, that the usable part of photon pairs produced by SPDC pumped with fs-pulses is limited to only a very narrow spectral component of the original pump power. This is in agreement with the experimental experience, that the relative rate of collected photon pairs is considerably less for the fs-pulse pump than for the CW pump (i.e. compared to the average pump power).

### A.3 Compensation of the walk-off effects in BBO

Due to the birefringence of BBO, transverse walk-off of the e-beam and longitudinal walk-off (=timing walk-off) between the e-beam and o-beam will occur, see Figure A.4. The transverse walk-off leads to a spatial shift of the cones, which makes the coupling of the photons into the optical fiber difficult and also leads to some distinguishability of the photons. The temporal walk-off leads to a distinguishability between the e-beam and o-beam, since in principle the relative timing would give information about whether an e-beam or an o-beam photon was observed. The temporal walk-off between the e-beam and o-beam for BBO is about 140 fs/mm at a wavelength of 702 nm (Ar$^+$-ion laser system, continuous wave), and about 200 fs/mm at a wavelength of 789 nm (Ti:SA laser system, frequency doubled fs-pulses).

Both walk-off effects actually can’t be compensated, but the introduced distinguishability can be washed out by the use of separate BBO crystals. The optic axis of these compensators is oriented in the same way as the down-conversion crystal, but are half the thickness of the down-conversion crystal. The polarization of the down-conversion is rotated by $90\text{°}$ (via a half wave plate) such that the e-beam and o-beam are exchanged. This reverses the walk-off effects by half, which consequently erases all temporal distinguishability and reduces the effect of the transverse walk-off of the e-beam and o-beam photons. A detailed description of the compensation is given in e.g. [Mat97, TW01]. A schematic drawing of the setup necessary for generating entangled photon pairs is given in Figure A.5.
A.3 Compensation of the walk-off effects in BBO

Figure A.3: A calculated distribution of down-conversion light at one intersection point of the down-conversion cones for a finite bandwidth pump. The calculation was performed in the diploma thesis of Guido Czejia [Cze01] with a matlab program. The pump beam spectrum is centered at a wavelength of $\lambda_p = 394.4$ nm. The calculation includes down-conversion in a wavelength band of $\lambda = 786 - 792$ nm. Also shown are the expected down-conversion signals for shifted spectral components of the pump, i.e. $\lambda_p + 1$ nm and $\lambda_p - 1$ nm. The circle corresponds to the down-conversion coupled into a single mode fiber by calculating the numerical aperture of the coupler system.

Figure A.4: Space-time diagram showing the temporal walk-off in the crystal. The down-conversion photons (e-beam and o-beam) emerging from point $z_0$ travel with different velocities due the birefringence. Note also, that both down-conversion-beams are faster then the pump-beam. This leads to relevant problems for down-conversion with fs-pump-pulses because it gives a broadening of the time distribution of the down-conversion.
Figure A.5: Top view of the down-conversion setup for producing polarization entangled photons.

A.4 The state produced by down-conversion

The ideal polarization entangled state which shall be produced by down-conversion has the form

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|H_1V_2\rangle - e^{i\varphi}|V_1H_2\rangle), \quad (A.3)$$

where $H$ and $V$ are horizontal and vertical polarization of photons 1 and 2 respectively and $\varphi$ is the phase between $H$ and $V$ polarization. The phase parameter $\varphi$ can be tuned to change the state $|\Psi\rangle$ between the $|\Psi^-\rangle$ or $|\Psi^+\rangle$ Bell-state, see Section 3.4.

The actual state produced by down-conversion contains much more details, since the phase-matching conditions, Equations (A.1, A.2), govern the photon pair production. In first approximation the general case can be described with finite bandwidths for the down-conversion photons and the pump-beam, and the finite thickness of the crystal:

$$|\Psi\rangle = k \int d\omega_p d\omega_e d\omega_o f_p(\omega_p)f_e(\omega_e)f_o(\omega_o)\delta(\omega_p - \omega_e - \omega_o)g(\Delta kD)$$

$$\left(a_{1V}^+(\omega_e)a_{2H}^+(\omega_o) - a_{1H}^+(\omega_o)a_{2V}^+(\omega_e)\right)|0\rangle \quad (A.4)$$

where the $d\omega$ are the frequencies of the pump-beam, $o$-beam and $e$-beam respectively with the spectral distribution functions $f_i(\omega)$, $g(\Delta kD)$ is the result of the integral over the crystal thickness $D$ with $g(x) = (e^{ix} - 1)/ix$ and $\Delta k = k_p - k_e - k_o$, and $a_{iJ}^+$ is the creation operator for a photon in spatial mode $i$ with polarization $J$ which acts on the vacuum $|0\rangle$. For zero spectral widths of the beams, the description of Equation (A.4) results in the ideal state of Equation (A.3).

A.4.1 Visibility Reduction for SPDC from a fs-pulse Pump

As was shown in [Mat97, Cze01, KR97] via numerical calculation, the achievable quality of entanglement for state (A.4), determined e.g. via a visibility measurement (see appendix G.1) in $|45^\circ\rangle$, is only perfect for zero spectral width of the pump beam, and for compensators with a thickness of $D/2$. For a finite spectral width of the pump-beam, the
The state produced by down-conversion

Figure A.6: Calculated visibility for the entanglement of photon pairs produced by SPDC in dependence of the spectral width of the pump-beam, taken from [Cze01]. The calculation assumed infinitely wide spectra for the down-conversion, perfect compensation (i.e. thickness of compensator crystals is exactly half the thickness of the down-conversion crystal) and a Gaussian spectral distribution of the pump beam.

Achievable visibility is below the ideal value. This case is relevant for down-conversion with fs-pump-pulses, as these have a finite spectral width.

Actually this dependence of the bandwidth of the pulse laser originates in the beam walk off between the pump photons (UV wavelength) and the down-conversion photons (IR wavelength), since the ultra-short pump pulses (about 200 fs wide) drift apart from the down-conversion pairs due to the dispersion in the media. BBO has the following inverse group velocities (calculated in [Mat97] with software supplied by the crystal producer Casix, China):

<table>
<thead>
<tr>
<th>Beam, Wavelength [nm]</th>
<th>Inverse Velocity 1/u [fs/mm]</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-beam (down-conversion), 789 nm</td>
<td>5413</td>
</tr>
<tr>
<td>o-beam (down-conversion), 789 nm</td>
<td>5612</td>
</tr>
<tr>
<td>e-beam (pump), 395 nm</td>
<td>5694</td>
</tr>
</tbody>
</table>

The walk off between the two down-conversion beams is corrected via the compensators, as explained above (Section A.3). However, the difference between the average of the two down-conversion beams (5513 fs/mm) and the pump beam (5694 fs/mm) leads to a distinguishability of the pairs dependent on their production location in the crystal, which inherently reduces the interference between these different pairs.

In the experiments described in this work, the FWHM spectral width of the fs-pulse-pump was $\approx 2.2$ nm, which leads to a maximum visibility of $\approx 0.98$. The results of the numerical calculation are shown in Figure A.6.
A Spontaneous Parametric Down-conversion
B The Fiber-based Quantum Channel

A vital component for realizing quantum communication schemes over “large” distances (“large” could mean: beyond the walls of a laboratory) is the ability to transmit the qubits, in our case photons, in a convenient way. The most suitable medium is an optical fiber, which can be installed like any other cable and works in a very stable way. For the transmission of photons only single-mode optical fibers can be used. Some of the effects of the fiber transmission on the photons will be discussed below.

B.1 Single-mode Optical Fiber

An optical fiber is made of a suitable transparent optical medium, such as glass, which is configured so that it has a core which is enclosed by a cladding. The core and the cladding have different refractive indices, such that light is confined to travel in the core by total reflection at the surface between the core and the coating. There are different types of configurations which can be categorized into multi-mode fibers, single-mode fibers and polarization-preserving fibers. An introduction over different fibers and the light propagation therein is given e.g. in [Hec89].

However, in the case of qubits represented by polarized photons, only single-mode fibers are suitable for transmitting the photons. In multi-mode fibers, the different propagation of several modes immediately leads to depolarization of the photons. Polarization-preserving fibers are single-mode and can preserve two distinct polarization directions, yet they are not suitable because they do not allow the transmission of a general polarization state, which occurs for the general state of a qubit.

B.1.1 The Essential Parameters

The most critical measure of a single-mode fiber is the cutoff wavelength $\lambda_{\text{cutoff}}$. This is the minimal wavelength at which the light can only propagate in a single mode. $\lambda_{\text{cutoff}}$ is defined by the diameter of the core. Another important parameter is the damping of the fiber due to absorption and other losses. This value is usually given in dB/km. A parameter interesting for coupling light in and out of fibers is the numerical aperture (NA) of a bare fiber, which is governed by the ratio of the core and coating refractive indices. Actual values of these parameters for fibers used in the experiments described in this work are given in Table B.1, and compared to a standard telecom fiber. Note the strong increase in the damping for shorter wavelengths.

The damping of the fiber specially selected for a cutoff of 690 nm is shown in Figure B.1.
### Table B.1: A list of the essential parameters for two single-mode optical fibers used for transmitting photonic qubits. The SMC1500 fiber is given for comparison only; note the large difference in the damping.

<table>
<thead>
<tr>
<th>Fiber</th>
<th>$\lambda_{\text{cutoff}}$ [nm]</th>
<th>Damping [dB/km] ( @ $\lambda$)</th>
<th>N.A.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specially selected fiber for 702 nm</td>
<td>?702 nm (?)</td>
<td>6 ( @ 702 nm)</td>
<td>0.11</td>
</tr>
<tr>
<td>SMC800 (standard product)</td>
<td>&lt; 780 nm</td>
<td>4 ( @ 800 nm)</td>
<td>0.14</td>
</tr>
<tr>
<td>SMC1500 (standard product)</td>
<td>&lt; 1500 nm</td>
<td>0.3 ( @ 1550 nm)</td>
<td>0.13</td>
</tr>
</tbody>
</table>

**Figure B.1:** Damping measurement for the specially selected fiber. The transmitted down-conversion photons have a wavelength of 788 nm and a spectral width of 3.5 nm FWHM. The remaining photons after a transmission of up to 1500 m are counted. An exponential decay function is fitted to the data, and shows an absorption length of 1200 $\pm$ 211 m, which corresponds to a damping of 3.6 $\pm$ 0.6 dB/km. The actual damping of the fiber is most likely even less because the fiber segments of each 500 m were connected with FC/PC connectors, which also induce losses.
B.2 Polarization Effects in Fiber Transmission

B.2.1 Transformation of the polarization

The unavoidable geometrical curvature of a laid-out optical fiber leads to stresses which induces slight birefringence in the glass. Generally, these birefringences are randomly distributed, and will hence produce an arbitrary transformation of the polarization of the photons. For suitable distances, where depolarization (see section below) does not occur, the induced polarization transformation remains unitary and hence can be fully compensated using polarization controllers (see Section B.2.3).

B.2.2 Temporal Drifts

The transformation will change over time, since the mechanical stress in the fiber varies because of temperature changes or mechanical changes. In a practical system, the fiber must be kept under constant mechanical and thermal conditions, in order to enhance the stability of the polarization transformation. Some test measurements show, that for a fiber of a few meters length which is taped onto an optical table, the stability of the polarization can better then 1° over a time of 24 h. A 500 m cable installed in the basement of a building shows drifts of the polarization in the range of 1° in 2 h.

B.2.3 Polarization Control in Single-Mode Fibers

The polarization is best viewed in terms of the Poincaré sphere (see [AB89] and Section 3.3.2). A unitary transformation, such as the effects of the fiber, will simply rotate the whole sphere by a certain angle around an axis. Clearly, in order to obtain a useful transmission of the qubits, this transformation has to be compensated.

In principle, this transformation could be corrected with polarization optics, such as wave plates. In terms of the Poincaré sphere, a wave plate is an element which has an axis sitting in the equator plane and will perform a rotation of the whole sphere around the axis by a certain fraction of $2\pi$, e.g. a half-wave plate performs a rotation of $2\pi/2$. The axis of the wave plate is adjusted by a simple rotation. So by combining several wave plates, any transformation of the sphere can be accomplished and the qubits are received in their correct state after the fiber transmission.

The best way to control the polarization transformation in a fiber is to use the effects of the actual fiber instead of external optics, by deliberately inducing birefringence in the fiber. There are three different types of in-fiber polarization controllers, which are shown in Figure B.2.

B.3 Depolarization of the photons in fibers

The single-mode fiber will also induce depolarizing effects on the transmitted photons, which unfortunately can not be compensated as easily as the polarization rotation caused by birefringence. I will only discuss the two most obvious effects.
B. The Fiber-based Quantum Channel

Figure B.2: Three different types of in-fiber polarization controllers. (a) The well-known “bat-ears” controller. Three fiber loops of a few cm in diameter are rotated with respect to each other. (b) The Polarite-controller. It implements a tunable wave plate via an actuator (e.g. screw), which presses the fiber and induces birefringence. The strength of the birefringence can be controlled by turning the screw in or out, and the axis of the birefringence is adjusted by rotating the screw mount. The screw can also be implemented by a piezo actuator. (c) A set of three to five piezo actuators induce birefringence with differently oriented axes. By only changing the birefringence via adjusting the piezo voltages any transformation can be achieved.

B.3.1 Polarization mode dispersion

Polarization mode dispersion (PMD) is the difference in the propagation velocity of two orthogonal polarization modes propagating in the fiber. It originates from the random birefringent segments of the fiber and shows statistics similar to that of random walk of particles [GPB+95, GRTZ01]. Therefore PMD is given in units of time per square root of the fiber length, and typical values of a modern telecom fibers are in the range of $0.1 - 0.5\text{ps/}\sqrt{\text{km}}$.

PMD leads to a depolarization of the light when the separation of the polarization modes is larger than the coherence time of the photons, see appendix G.3. For instance for down-conversion photons with $\Delta \lambda = 1.5 \text{ nm}$ (corresponds to $\Delta \lambda_{\text{FWM}} = 3.5 \text{ nm}$ ), the coherence time is $\tau_{\text{cohr}} = 220 \text{ fs}$. Therefore, even for the best fiber with a PMD of 100 fs/$\sqrt{\text{km}}$, one might run into problems of depolarization at a fiber length of $\approx 10 \text{ km}$.

A simple model for calculating the effect of PMD on the visibility (see appendix G.1) of polarization is to assume that the overlap of the two orthogonal polarization wavepackets reduces as a Gaussian function depending on the ratio $\tau_{\text{pmd}}/\tau_{\text{cohr}}$ in the form:

$$V = A e^{-\frac{\tau_{\text{pmd}}^2}{2\tau_{\text{cohr}}^2}},$$

where $A$ is an amplitude factor (allowing for a non-ideal initial polarization) and $\tau_{\text{pmd}} = \text{PMD} \ast \sqrt{L_{\text{fiber}}}$ depends on the PMD value and the length of the fiber.

The measured and calculated visibility of polarization for a fiber of up to 1.5 km length is shown in Figure B.3 for down-conversion photons traveling through a single-mode fiber. The photons were polarized before coupling into the fiber and analyzed after the fiber.
B.3 Depolarization of the photons in fibers

Figure B.3: Depolarization effect of the fiber. This graph shows the measurement of the visibility of the polarization of down-conversion photons after traveling through a single-mode fiber. The photons have a wavelength of 788 nm, and a spectral width of 3.5 nm FWHM. The given calculated visibility is based on the model of Equation (B.1) with a PMD value of 25 fs/$\sqrt{\text{km}}$ and a coherence time of the photons of $\tau_{\text{cohr}} = 0.219$ ps. The fiber was coiled up on drums in the lab.

The calculated polarization visibility has a value of about 25 fs/$\sqrt{\text{km}}$, which is much less than the value for telecom fibers which is at best 100 fs/$\sqrt{\text{km}}$, and can be ascribed to two effects: firstly that the actual spectral width of the photons was less than the assumed $\Delta\lambda_{\text{FWHM}} = 3.5$ nm or secondly, that the actual PMD of the fiber really is less than the assumed value for telecom wavelengths. Unfortunately at present it can not be said which effect dominated. The spectrum of the down-conversion photons is only defined via an interference filter placed in front of the fiber, and we do not have the means to actually measure the spectrum of the photons. The PMD value for single mode fibers at a wavelength of 788 nm is not specified, and could well be less than the assumed value. However, a producer for such fibers, Nufern Inc., Australia, does not specify the PMD value. Generally, not much is known about PMD at short wavelengths, as was pointed out by people at the Gisin group, University of Geneve, who usually work with fibers at the telecom wavelengths of 1.5 $\mu$m or 1.3 $\mu$m.

B.3.2 Chromatic Dispersion

Chromatic dispersion (CD) can also impose a problem on the transmission of photons with a finite bandwidth, as the different spectral components have different group velocities due to the dispersion relation of the medium. Depending on the fiber length and spectral width of the photons $\Delta\lambda$, CD could “stretch” the spectral components of the wave packet.
However, CD is only important for the timing of the photons, i.e. in an interferometer. The polarization of the photons is not lost.

For fused silica, such as a fiber, the slope of the refractive index centered at $\lambda = 800$ nm is $\delta n(800\text{nm}) \approx \frac{\Delta n}{\Delta \lambda} = 1.71 \cdot 10^{-5}$ $\frac{1}{\text{mm}}$. The temporal broadening of a wavepacket depending on $dn$ is $d\tau = \frac{L_{\text{fiber}}}{c} dn$ with $L_{\text{fiber}}$ being the length of the fiber and $c$ the vacuum speed of light. This expression can be used for an estimation of the effect of CD by expressing $dn \approx \delta n \Delta \lambda$ which leads to $\pm \Delta \tau_{cd} \approx \frac{L_{\text{fiber}}}{c} \delta n \Delta \lambda$. For photons with a spectral width of $\Delta \lambda = 1.5$ nm and a fiber length of 1000 m, the CD induced shift would be $\pm 85$ ps, and would therefore strongly broaden the wavepacket. However, CD is static and can be easily compensated externally e.g. by compensation prisms or chirped mirrors.
C Detecting Photons with APDs

The detection of the single-photons in our wavelength range is best performed in silicon avalanche photo diodes (APD) which are operated with a reverse bias voltage in excess of their break down voltage, called the Geiger-mode. Due to the high operating voltage of about 230 V the field in the isolating layer of the diode is so large, that already the presence of a single electron-hole pair produced by the photo absorption leads to a complete breakdown of the diode by triggering a strong avalanche which can easily be measured. Since the avalanche is self-sustaining, a quenching circuit must be implemented in order to stop the avalanche and reset the APD for the next detection event. Detailed information about APDs and also about the required electronics for single-photon counting operation can be found in [Jen97, BRR86, CGL'96, DDD'93]. This work will describe a newly developed detector system built to our own special needs.

C.1 Commercial Devices

The Si-APD CS30902S/CS30921S from Perkin-Elmer has been commercially available for many years and is very well suited for single photon counting. Originally this APD was developed for weak-light applications, but selected devices are suitable for single photon counting. The spectral response of this APD is shown in Figure C.1, and is typical for silicon photo detectors. The typical achievable efficiency of detecting a single photon with this APD is in the range of 40 %. When cooled to about -25 – -30°C, the detectors have a quite low dark count rate of 200 - 500 cps.

Since about 1997, Perkin Elmer - Optics, Canada, (formerly EG&G) builds complete detector modules, called single photon counting modules (SPCM). These are based on the more advanced Slik-APD [CGL'96] and contain the full detector electronics. However, our experiences with the SPCM modules were not very satisfying for two reasons. Firstly, the SPCM modules seem to have a rather short lifetime\(^1\) of typically two years. Also, the SPCMs seem to cease for no obvious reason during normal operation. This lifetime behaviour imposes a serious problem for the experiments, which naturally rely on a seamless operation of the detectors. Secondly, according to the specifications, the SPCM modules should achieve an efficiency of up to 70 %. However, by directly comparing counts

\(^{1}\)From our total sample of seven SPCMs, two ceased within their warranty (one year) and were repaired. One ceased after the warranty period and was also repaired. Two of the repaired modules ceased again after about one year. Presently, from the originally seven SPCM, only two are still in operation (four years). A rough estimate leads to an average lifetime of two years.
C Detecting Photons with APDs

Figure C.1: Spectral response of the CS30902S/CS30921S APD (taken from [Elm]). The spectrum is mainly defined by the absorption of light in silicon. The total efficiency of detecting a photon is given by the shown quantum efficiency multiplied with the break down probability. This is the probability that a photo electron results in an avalanche in the APD, and is as high as 0.8 when the APD is operated at a voltage 25 V above the break down voltage.
of down-conversion photons in a fiber (wavelength of 702 nm and 788 nm, single count rates of about 100 Kcps), we noticed only slight differences in the single count rates and no differences in the coincidence count rates of the SPCM modules and the self built detector modules based on the CS30921S APD, which have an efficiency of about 40%.

C.2 Self Designed Detector Systems

In the experiments presented in this work, two generations of self designed detector systems were used, each based on the APDs CS30921S/CS30902S. The earlier, and simpler, version implements so-called passive quenching of the APD (PQ-detector), and the later, and more advanced version, is based on active quenching of the avalanche in the APD (AQ-detector). Also, in the second detector version, the water cooling was replaced by air cooling and the detector electronics directly delivers TTL pulses, instead of the small APD pulses which required extra signal conditioning.

C.2.1 The PQ-Detector System

The passive quenching circuit is the simplest way to operate an APD in the Geiger mode for photon counting. A mere resistor $R_s$ is switched in series to the APD. The value of $R_s$ is chosen such, that when an avalanche break down of the APD occurs the maximal current is limited to a value of $\approx 50 \, \mu A$ (for this type of APD). Then the avalanche is no longer self sustaining and will stop, hence allowing the APD to reload to the bias voltage, which is in excess of the break down voltage, and wait for the next detection event. The typical efficiency for detecting a photon is in the range of 40%. Details about the break down and the ways to quench the avalanche can be found in [Jen97, CGL+96, DDD+93].

The PQ-detectors were built with two types of APDs, the CS30902S which has a detector window and an active area with a diameter of 0.5 mm ([Den93]), and the CS30921S, which is the same APD configured with a multi-mode fiber pigtail ([Rec96]). The PQ-detectors are used in the Zeilinger-group since about 1993 and have been well described in the theses stated above. Therefore, they will only be described very short terms. A small module contains the APD and the quenching resistor $R_s$, and uses Peltier cooling to bring the APD to a temperature of about -30 C. The released heat of the Peltier element is taken away via water cooling. A separate power supply generates the Peltier current as well as the bias voltage of about 230 V for operating the APD. The detection signals are delivered as a short pulse of $\approx 2 \, ns$ with 100 - 400 mV amplitude on 50 $\Omega$. These signals require extra amplification before and a discriminator, in order to turn into well defined pulses. This signal conditioning is usually realized with a VTC120A amplifier and a NIM-CFD545 discriminator both from Perkin Elmer, which produces standard NIM pulses (i.e. low: 0V, high: -1V on 50 $\Omega$).

Passive quenching is very elegant, however its drawback is that the reloading of the APD is defined also by $R_s$, and follows an exponential loading curve. This means, that after a detection event the voltage of the APD will increase “relatively” slowly, typically with a time constant $\tau = 1 \, \mu s$. The time constant is governed by the diode capacity.
C Detecting Photons with APDs

Figure C.2: Block diagram of the detector system. The system contains two APD channels. The photons are delivered to the APDs via a pigtailed multi mode fiber. The two APDs are in a housing for thermal insulation and are cooled to ≈ $-25\, ^\circ C$ via a two stage peltier element. The temperature is measured with a PT500 temperature sensor, and the peltier current is regulated by a temperature control unit from Wavelength-Electronics Inc., USA, which manages a temperature stability of better than 0.1 $^\circ C$. An active quenching circuit is responsible for actively resetting the detection avalanches in the APDs when operated in the photon counting mode, and for measuring the diode current when operated in the linear mode. The output signal for the photon detections are TTL-pulses, in the photon counting mode, and an analog linear signal in the linear mode. The control board generates several supply voltages required by the active quenching circuit, and also sets the operation mode of the APDs. Two power supplies deliver +12 V and −5 V to the control board and the temperature control unit.

and stray capacitances, and the value of $R_s$. Since the efficiency of the APD depends on the voltage, this loading characteristic will lead to an effective dead time of about 1 $\mu$s, which limits the maximal count rate. Typically, our PQ-detectors have a saturating count rate of about 400 kcps. Up to count rates of about 50 kcps, the dead time effect will not influence the efficiency. For higher count rates, a reduction of the effective efficiency must be accepted.

C.2.2 The AQ-Detector System

Due to our experience with the SPCMs, as described in Section C.1, the decision to implement a new and more advanced self built detector system as a replacement of the PQ-detectors was taken. A further advantage of the new AQ-system is, that a “linear” mode was implemented allowing to set the APD into a low-sensitivity linear mode where the diode can measure laser light, e.g. for adjustment procedures. The detector system delivers the photon detections as TTL-pulses (see Section G.4 for the definition of TTL) and the linear signal as an analog voltage signal.

Overview of the System

A block diagram of the different components in the detector are shown and described in Figure C.2. The view inside a completed detector device is shown in Figure C.3.
Most components of the AQ-system are standard and do not require any detailed description, apart from the active quenching circuit.

**The active quenching circuit**

The technically demanding part is the active quenching circuit, which shall be described in more detail. The active quenching circuit is responsible for stopping the strong avalanche in the APD after a photon detection. The circuit implemented is based on a concept described by Cova et al. [GCZS96], with some alterations like omitting the gating option and including the linear current measurement mode. The full circuit schematic is shown in Figure C.4.

The central device is D3, the APD. The cathode is connected to a positive bias voltage. The anode of the APD is connected via R20 and R1 to the relay switch K2. In the linear mode, K2 is open, and the photo current in the APD must flow into the current to voltage amplifier U1, which delivers a linear output signal. The bias voltage is about 30 V in this case. In the photon counting mode, the bias voltage is set to about 230 V, which is roughly 25 V above the break down voltage of the APD. In this mode, K2 is closed, and hence connects R1 to ground. The second relay switch, K1, enables the comparator IC1, which can detect a break down avalanche of the APD because the anode voltage will rapidly (within about 1 ns) rise to 25 V above ground. The comparator will notice a voltage increase on R1 and hence set its output to a logic high, in ECL logic standard (see Section G.4 for an explanation of the logic families). This logic state triggers the first monoflop, IC2, which produces the quench pulse of about 100 ns. This pulse, which has
Figure C.4: Full schematic diagram of the active quenching circuit. The function of the circuit is described in the text.
Figure C.5: Trace of the APD anode voltage for a full detection cycle. When the signal is near 0 V, the APD is armed. Due to a breakdown, the voltage increases. When the voltage has arrived at a certain value, the quench pulse is activated and the circuit pulls up the APD voltage with a higher rate and holds it. This allows for the avalanche in the APD to stop. After the quench pulse is over, the reset pulse rapidly pulls the APD voltage back to about 0 V, meaning that the APD is ready for the next detection event. The voltage scale is arbitrary, since the measurement had to be done with a probe only near the APD because the input capacitance would have disturbed the circuit too much. The maximum of the voltage pulse corresponds to about 28 V.

ECL logic levels is sent through the ECL/TTL converter IC4, to generate a TTL output pulse and a logically inverted TTL pulse (i.e. active low). This will switch off transistor Q1, in which course Q2 opens via R3. Then, due to the bootstrapping configuration with C1, Q2 switches the voltage of connector SV1-1, a DC voltage of +28V, via the high-speed schottky diode D1 to the APD. This quenches the APD because the effective voltage across the APD is now below the breakdown voltage. This state is held for the length of 100 - 150 ns, in order to free the APD from the charge carriers, which would lead to after-pulsing. When the quench pulse is over, it triggers monoflop 2, IC5, which generates the reset pulse, of about 10 ns length. The reset pulse is also transformed to a TTL signal via IC4, and switches on the two reset transistors Q3 and Q4. Q3 is responsible for reloading the APD voltage to the full extent, and Q4 resets the quench transistor Q2. After the reset pulse is over, the APD is fully ready for the next detection event. The signal trace of Figure C.5, taken with an oscilloscope, shows the quenching and the resetting process take place.

The main difficulty operating the active quench circuit is the handling of the switching
transistors Q1 - Q4\textsuperscript{2}. These transistors are ultra-fast MOSFETs, highly sensitive in operation, and are also sensitive to electrostatic discharge. Yet, once the circuit is set up on a well-designed printed circuit board, it works quite stable.

**Performance of the AQ Detectors**

Two measurements were performed to test the characteristics of the detector system. The first measurement, Figure C.6, shows the effectively counted photons depending on the input power, and allows to judge that the detector operates reasonably linear with counting rates about 1 million counts per second. This measurement was performed by detecting a laser beam, which was attenuated by two polarizers. The deviations from the linear curve are caused primarily by the dead time of the detector, which is roughly 150 ns, and by effects due to warming of the APD. At higher count rates the APD will experience warming due to the large number of current pulses. As the APD temperature rises, the breakdown voltage ($U_{br}$) of the APD will also increase and this leads to a reduction of the excess voltage over $U_{br}$ at which the APD is operated. The efficiency for detecting a photo electron in the APD strongly depends on this \cite{DDD+93} excess voltage, and therefore the

\textsuperscript{2}This particular type of transistor, the SD211, was originally produced by Vishay, USA. It has very special properties such as a high breakdown voltage (> 30V), low capacitance and ultra fast switching speeds (≈ 1 ns), which make it ideal for this circuit. Unfortunately the production of this type was stopped and seemingly no replacement type exists. However we were able to obtain quantities sufficient for realizing several detectors.
C.3 Coincidence Logic

Figure C.7: Relative timing accuracy of two AQ-detectors in respect to each other. The histogram shows time intervals between the detection pulses from two detectors observing down conversion photons which inherently have a temporal correlation better than 1 pico second. The gaussian fit to the histogram has a width of $\sigma_{DD} = \omega/2 = 0.33$ ns. Therefore, by assuming independent detectors the standard deviation for the timing accuracy is about $\sigma_{DD}/\sqrt{2} = 0.24$ ns. The measurement was performed with the time interval counter, type SR620, from Stanford Research Instruments, USA, which has a specified timing resolution of 25 ps, justifying to neglect the resolution of this instrument compared to that of the detectors.

total efficiency for detecting a photon is reduced.

A measurement concerning the timing accuracy of a detector was performed with correlated photons detected by two detectors. The two photons produced by down-conversion have a relative timing uncertainty of $\tau_{cohr}$ which is typically less than 1 ps, which makes them well suited for the timing measurement. The relative timing distribution of the two detectors in respect to each other is shown in Figure C.7. The distribution has a width of $\sigma_{DD} = 0.33$ ns, and by assuming independent detectors the resolution of a single detector can be estimated to be $\sigma_{D} = \sigma_{DD}/\sqrt{2} = 0.24$ ns. This standard deviation corresponds to FWHM-timing accuracy of 0.54 ns, which compares well with the best achieved FWHM-timing accuracy so far for the CS30921S APD of 0.46 ns, given by Lacaita in [LCG88].

C.3 Coincidence Logic

The experiments described in this work are based on the correlation of photons. In order to perform these experiments, it is necessary to implement suitable means for comparing the photon detection pulses in order to observe pair-photon events. In this work, overall three different types of coincidence electronics were used, whereof two are based on Boolean logic (NIM-logic, see Section 7.2.1 and programmable logic, see Section 8.3) for comparing the actual detectors pulses, and one is based on timing measurements of all detection events and later searching the coincidences through comparison of the stored
C Detecting Photons with APDs

time lists on a personal computer (see Section 5.1.2). The timing variant is technically very demanding, however it offers a very nice feature not possible with the Boolean logic, i.e. that all detection events are available for any kind of post processing, such as an adjustable coincidence window during the processing of the data, etc.. For example, the data sets obtained in the long-distance Bell experiment described in the thesis of Gregor Weihs [Wei99] were further analyzed in respect to local realistic models by a theory group in Argentina [HPS01] - a method of documenting a quantum optics experiment which offers previously unknown possibilities.

The most relevant parameter of all coincidence electronics is the coincidence window $\tau_{\text{coinc}}$. This is the time window, within which a coincidence circuit will count two detections as corresponding detections. In order to discriminate to photon detections of correlated photons from photon detections of independent photons, $\tau_{\text{coinc}}$ must be much smaller than the average time interval between two successive clicks of each detector. There will always be a certain amount of accidental coincidences, i.e. coincidence counts form independent photons leading to a background signal, which can be estimated in the following way. Given certain single counts $N_1, N_2$ obtained within a time $T$ for the two detectors, the accidental coincidences which will occur as a background in a photon pair measurement are

$$C_{\text{acc}} = \frac{N_1 N_2}{T^2} \tau_{\text{coinc}}.$$  \hspace{1cm} (C.1)

For example, if the two detectors have a single count rate of 100 kcps, and the coincidence logic has $\tau_{\text{coinc}} = 10$ ns, the amount of accidental coincidences will be 100 cps. This is still relatively low compared to the expected $\approx 10$ kcps of real coincidences. However, for very low efficiencies of the system, the detector dark counts will lead to a higher fraction of accidentals which can cover the real coincidences.
D The interferometric Bell-state Analyzer

The statistics of two-photon interference at a beam splitter, Figure D.1, is best calculated with the formalism of quantum electro dynamics, where $a^\dagger$ and $a$ are the creation and annihilation operators respectively of a photon in the mode $a$. Creation of one photon in mode $a$ comes about by the operation of the creation operator onto the vacuum state: $a^\dagger|0\rangle$. For each spatial mode, there are also two polarizations $H$ and $V$, e.g. the modes $a_H$, $a_V$, which must be treated separately. The transformation rules between the input modes $a$ and $b$ and the output modes $c$ and $d$ of a non-polarizing beam splitter have the following form:

\[
  \begin{align*}
    c &= iRa + Tb \\
    d &= Ta + iRb,
  \end{align*}
\]  

where $R$ and $T$ are the reflection and transmission coefficients, and $R^2 + T^2 = 1$. For a 50:50 beam splitter, $R = T = 1/\sqrt{2}$, which simplifies the above relations and allows to easily rewrite them as:

\[
  \begin{align*}
    a &= \frac{1}{\sqrt{2}}(-ic + d) \\
    b &= \frac{1}{\sqrt{2}}(c - id).
  \end{align*}
\]  

Figure D.1: Interferometric Bell-state analysis. The two photons interfere at the beam splitter, which allows the detection of two of the four Bell-states. The beam splitter is simply a device which reflects 50% of a light beam hitting its surface.
Figure D.2: Detecting Bell-states. The detection of the antisymmetric Bell-state $|\Psi^-\rangle$ is shown on the left. The two photons enter in modes $a$ and $b$ respectively, and are always found in different outputs, i.e. modes $c$ and $d$ of the beam splitter. If the two detectors in these output modes click, then this state was detected. In the case of one of the other three Bell-states, the two photons will be found in the same output mode. However, for the $|\Psi^+\rangle$ case, the two photons still have opposite polarization in the $H,V$-Basis. So extra polarizers are inserted in the outputs, as shown in the scheme on the right. If two detectors sitting in the two outputs of a polarizer click, then a $|\Psi^+\rangle$ is detected.

D.1 Detection of the antisymmetric Bell-state

Considering the two input photons to be in the only antisymmetric Bell-state $|\Psi_{-a,b}\rangle = 1/\sqrt{2}(a_H^+b_V^+ - a_V^+b_H^+)|0\rangle$, each term must be substituted by the beam splitter relations D.2, leading to

$$|\Psi^-_{c,d}\rangle = \frac{1}{2\sqrt{2}} \left( -ic_H^+d_H^+(c_V^+ - id_V^+) - (-ic_V^+ + d_V^+)(c_H^+ - id_H^+) \right) |0\rangle. \tag{D.3}$$

Expanding above equation leads to

$$|\Psi^-_{c,d}\rangle = \frac{1}{2\sqrt{2}} \left( -ic_H^+c_V^+ - c_H^+d_V^+ + d_H^+c_V^+ - id_H^+d_V^+ \right. \right.$$
$$+ ic_V^+c_H^+ + c_V^+d_H^+ - d_V^+c_H^+ + id_V^+d_H^+) |0\rangle$$
$$= \frac{1}{2\sqrt{2}} \left( -2c_H^+d_V^+ + 2c_V^+d_H^+ \right) |0\rangle = \frac{1}{\sqrt{2}} \left( -c_H^+d_V^+ + c_V^+d_H^+ \right) |0\rangle, \tag{D.4}$$

and only mixed terms of modes $c, d$ remain. This means, that an input state $|\Psi_{-a,b}\rangle$ will always lead to detection of the two photons in opposite outputs, see Figure D.2.
D.2 Detection of a symmetric Bell-state

The same calculation for the case that the two input photons are in one of the other three, symmetric Bell-states, e.g. \( |\Psi_{a,b}^+\rangle = \frac{1}{\sqrt{2}}(a_H^\dagger b_V^\dagger + a_V^\dagger b_H^\dagger)|0\rangle \) shows, that only terms remain where the two photons are in the same output modes \( c \) or \( d \). However, in the case of the \( |\Psi^+\rangle \), the two photons will still have opposite polarization in the \( H, V \) basis. So this case can be identified with polarizing beam splitters oriented at the \( H, V \) direction in the two outputs of the beam splitters. If a coincidence between the two outputs of a polarizing beam splitter occurs, then a \( |\Psi^+\rangle \)-state was present, as sketched in Figure D.2.

In principle, the \( |\Phi^+\rangle, |\Phi^-\rangle \)-states can be identified together, by including photon-number discriminating detectors in the outputs of the polarizers. For these two states, both photons have either \( H \) or \( V \) polarization and take the same output of the polarizer. So if a detector sees two photons in one output, a \( |\Phi^+\rangle \) or \( |\Phi^-\rangle \) was detected. This was demonstrated in the dense-coding experiment performed by Klaus Mattle et al. [MWKZ96].
D The interferometric Bell-state Analyzer
E Effects Limiting the 4-fold Correlation Visibility in the Entanglement Swapping

E.1 Limits of the 2-fold Correlation Visibility

Collection Deficiencies for SPDC The geometrical difficulties of collecting the photon pairs produced by the SPDC are manifold (see Chapter A) and clearly, the quality of the collection alignment of the photons will have an influence on the quality of the correlations. In practice, the visibility of the photon pair correlations is maximal for $\phi_0 = \phi_3 = 0^\circ, 90^\circ$ since this is the original basis in which the source produces the photon pairs ($|HV\rangle$ or $|VH\rangle$). This visibility is non perfect due to imperfections in the orientation of all the birefringent elements in the SPDC setup, i.e. the crystals and the half-wave plates. Moreover, for $\phi_0 = \phi_3 = 45^\circ$ (or circular polarization) the different production processes must even interfere ($|HV\rangle - |VH\rangle$) and the fidelity is reduced, since the collection alignment and beam walk in the crystals will make the two processes slightly distinguishable. Consequently, the correlation of the photon pairs will show a dependence of the actual orientation of the polarizers and will not be rotationally invariant, as it should be for the perfect $|\Psi^-\rangle$-entangled state.

Inherent Visibility Limit for Pulsed Down-conversion As explained in Section A.4, calculations performed by Klaus Mattle [Mat97] and more recently Guido Czeija [Cze01] show, that for photon pairs which are produced by spontaneous parametric down-conversion pumped with fs-UV-pulses which have a finite bandwidth, the achievable contrast of entanglement is inherently reduced. This will be most noticeable for measurements along the $45^\circ$ or the circular polarization basis, and will not show up for measurements in the $0^\circ$ basis, the basis in which the photons are originally produced. The origin of the effect is the temporal walk off between the pump (UV) and the down-conversion photons (IR), which is 180 fs/mm (explained in Section A.4.1).

The results of a numerical calculation of this effect is shown in Figure A.6. In this particular experiment, the pulsed UV-laser has a FWHM spectral width of $\approx 2.2$ nm which, according to the calculations, allow a maximum visibility of $\approx 0.98$ (in the $45^\circ$ basis). This effect adds to the above stated problems of collecting the photons.
In the experiment the photon-pair contrast was typically about 100:1 in the $0^\circ/90^\circ$ polarization basis (corresponding to a visibility of 0.980) and about 30:1 to 35:1 in the $45^\circ$ basis, corresponding to a visibility of 0.935 to 0.944 respectively, if the filters for photons 1 and 2 have a 1 nm FWHM bandwidth. If 2 nm filters are used, then the contrast at $45^\circ$ drops to about 20:1, which corresponds to a visibility of 0.904.

### E.2 Limits of the Two-Photon Interference at the Fiber Beam Splitter

**Non-symmetric Splitting-Ratio of the Fiber Beam Splitter** Ideally, the beam splitter in the BSA should have a splitting-ratio of 50:50. For a non symmetric splitting ratio the achievable visibility of the two-photon interference can be deduced by including the reflectivity $R$ and transmittivity $T$ in the calculation of the two-photon interference (see [Wei94]), leading to

$$V = \frac{2RT}{R^2 + T^2}. \quad (E.1)$$

The actually implemented device had a splitting ratio of about 45:55, which results in a visibility of 0.996.

**Polarization Alignment in the Fibers** The quality of the polarization alignment of the two input fibers of the beam splitters is also a relevant parameter. Including a polarization rotation of $\Delta \phi$ for one of the inputs in the calculation of the interference leads to a visibility $V = \cos(\Delta \phi)$. In this experiment the two inputs of the beam splitter were aligned better than $\Delta \phi = 3^\circ$ (as described above in Section 7.1.1). This would result in a visibility limit of 0.998.

**Difference in Center Wavelength of Photons 1 and 2** This effect is quite obvious, since a difference in the center wavelengths of photons 1 and 2 entering the beam splitter would leave them distinguishable. An expression is given by Gregor Weihs in his master thesis [Wei94], where the visibility depends on the spectrum of the two wave packets in the following way:

$$V = e^{-\frac{(\omega_{\text{diff}} \tau_{\text{cohr}})^2}{8}} \quad (E.2)$$

where $\omega_{\text{diff}}$ is the difference in angular frequency of the two input wave packets, and $\tau_{\text{cohr}}$ is their coherence time. A more practical expression can be found by expressing the coherence time $\tau_{\text{cohr}}$ by Equation (G.7) under consideration of Equation (G.6), and further by expressing $\omega_{\text{diff}}$ by the first order approximation $\omega_{\text{diff}} \approx \frac{2\pi}{\lambda_{\text{diff}}}$ (derived analogous to the derivation of the coherence time given in Section G.3) leading to

$$V \approx e^{-\frac{1}{2} \frac{1}{\ln(1/4)} \left( \frac{\Delta \lambda_{\text{diff}}}{\lambda_{\text{FWHM}}} \right)^2}, \quad (E.3)$$
where $\Delta \lambda_{\text{diff}}$ is the difference of the peak wavelengths of the wave packets and $\Delta \lambda_{\text{FWHM}}$ is their full-width-half-maximum width of the spectral distribution.

In the experiment $\Delta \lambda_{\text{FWHM}}$ is defined by the spectral filters for photons 1 and 2 and was 1 nm, and the accuracy of the filters was better than 0.25 nm. This results in a visibility of 0.977.

**Temporal fuzziness of the two down-conversion pairs** This effect was not taken into consideration in earlier work regarding interference of photons from different down-conversion processes. The temporal walk-off in BBO was already mentioned above, as it leads to an inherent visibility limit for pulsed down-conversion (see also Section A.4.1), yet it was overlooked so far in that it will also lead to a temporal fuzziness between the two down-conversion pairs. The simple numerical calculation shows that the influence of this effect is substantial, and can not be neglected.

Due to the dispersion in the BBO crystal, there will necessarily occur a walk-off between the UV-pump photons, propagating at with a group velocity of 5694 fs/mm, and the two down-conversion photons, propagating with 5413 fs/mm and 5612 fs/mm respectively. The difference in the speed of the two down-conversion photons is compensated via the compensator crystals. However, the difference between the speed of the pump photons and the average speed of the down-conversion photons, which is 180 fs/mm, remains. When photons 0 and 1 from independent down-conversion processes are brought together for interference, their wave packets will then have a temporal fuzziness due to this remaining speed difference between the pump and the down-conversion light. The extreme case would be that one pair was produced right at the beginning of the BBO and the second pair right at the end of the BBO. In this experiment, as the BBO was 2 mm thick, the two photon pairs are undefined by $\pm 360$ fs in respect to each other which is already relatively large compared to the coherence time of the two interfering photons of $\tau_{\text{cohr}} = 775$ fs and will therefore reduce the visibility.

Quantitative results were determined by numerical simulation of this effect in a short LabVIEW program. The interference is observed as the probability for having a photon in each of the outputs $c$ and $d$ of the beam splitter, and is assumed to be a Gaussian function which depends on the time delay $t$ and the offset $t_0$ between the two photons, compared to the coherence time of the photons $\tau_{\text{cohr}}$:

$$P_{c,d}(t - t_0) = 1 - e^{-\frac{(t - t_0)^2}{\tau_{\text{cohr}}^2}}.$$  \hspace{1cm} (E.4)

The program takes account of the walk-off in the crystal by varying the offset time $t_0$ between $\pm 2$ mm$\times 180$ fs/mm in a number of steps, and averaging over many different shifted probabilities $P_{c,d}(t - t_0)$, resulting in a final probability for the interference. The minimum of this function no longer reaches zero, and the estimated visibilities are (for 2 mm crystal, photon wavelength 788 nm):
E Effects Limiting the 4-fold Correlation Visibility in the Entanglement Swapping

<table>
<thead>
<tr>
<th>Effect</th>
<th>Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection of SPDC: 2-fold Correlation @ 0°</td>
<td>0.980</td>
</tr>
<tr>
<td>Collection of SPDC + Pulsed SPDC: 2-fold Correlation @ 45°</td>
<td>0.935</td>
</tr>
<tr>
<td>Non-symmetric Splitting-Ratio of the Fiber Beam Splitter</td>
<td>0.996</td>
</tr>
<tr>
<td>Polarization Alignment in the Fibers</td>
<td>0.998</td>
</tr>
<tr>
<td>Difference in Center Wavelength of Photons 1 and 2</td>
<td>0.977</td>
</tr>
<tr>
<td>Temporal Fuzziness of the two Pairs (1 nm Filter)</td>
<td>0.9618</td>
</tr>
<tr>
<td>Total: 0°:</td>
<td>0.897</td>
</tr>
<tr>
<td>Total: 45°:</td>
<td>0.817</td>
</tr>
</tbody>
</table>

Table E.1: Summary of the effects limiting the visibility of the 4-fold correlations in the entanglement swapping experiment. The first effect is noticed as a reduction of the 2-fold correlations and the lower effects occur at the Bell-state measurement with the fiber beam splitter. The details are given in Section E. The total visibilities are the products of all contributions, where the 2-fold correlations must be taken twice since two pairs are used in the setup.

<table>
<thead>
<tr>
<th>Filter Bandwidth $\Delta \lambda_{\text{FWHM}}$</th>
<th>Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 nm</td>
<td>0.9618</td>
</tr>
<tr>
<td>2 nm</td>
<td>0.8625</td>
</tr>
<tr>
<td>3 nm</td>
<td>0.7349</td>
</tr>
</tbody>
</table>

Above simulation results show the relevance of this effect. In this experiment, filters with a FWHM-Bandwidth of 1 nm were used, meaning that this effect contributes to a reduction of the visibility by a factor of 0.9618.

E.3 Comparison of the Visibility Limits with Measurements

The visibility reducing effects are summarized in Table E.1, together with their worst-case contribution and the overall visibility. The total visibility is calculated via the product of all contributing visibilities, where the 2-fold correlation visibility enters twice, because two pairs are used in the experiment.

A comparison of the visibility observed in several scans with the estimated visibilities in Table E.2 shows the good match of experiment and the model. However, it is not exactly clear, if all effects were considered or if the model is suitable.
### E.3 Comparison of the Visibility Limits with Measurements

<table>
<thead>
<tr>
<th>Scan Measurement</th>
<th>Type</th>
<th>Max/Min</th>
<th>Visibility</th>
<th>Est. Vis.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FWHM-bandwidth of filters = 2 nm</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fdip45deg3_00.dat (07.01.01)</td>
<td>a</td>
<td>24/2</td>
<td>0.846 ± 0.104</td>
<td>0.837</td>
</tr>
<tr>
<td>entswap_new1_00.dat (23.01.01)</td>
<td>b</td>
<td>25/8</td>
<td>0.515 ± 0.149</td>
<td>0.678</td>
</tr>
<tr>
<td>fdip45deg12_00.dat (25.01.01)</td>
<td>a</td>
<td>64/8</td>
<td>0.810 ± 0.070</td>
<td>0.837</td>
</tr>
<tr>
<td>fdip45deg13_00.dat (27.01.01)</td>
<td>a</td>
<td>100/9</td>
<td>0.835 ± 0.052</td>
<td>0.837</td>
</tr>
<tr>
<td><strong>FWHM-bandwidth of filters = 1 nm</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fdip45deg19_00.dat (30.01.01)</td>
<td>a</td>
<td>32/1</td>
<td>0.944 ± 0.059</td>
<td>0.934</td>
</tr>
<tr>
<td>entswap_new2_00.dat (31.01.01)</td>
<td>b</td>
<td>29/3</td>
<td>0.812 ± 0.103</td>
<td>0.817</td>
</tr>
<tr>
<td>entswap_new3_00.dat (01.02.01)</td>
<td>b</td>
<td>40/5</td>
<td>0.777 ± 0.093</td>
<td>0.817</td>
</tr>
<tr>
<td>tomography45_451_00.dat (26.03.01)</td>
<td>b</td>
<td>258/31</td>
<td>0.785 ± 0.036</td>
<td>0.817</td>
</tr>
<tr>
<td>tomography00_002_00.dat (28.03.01)</td>
<td>b’</td>
<td>227/18</td>
<td>0.883 ± 0.030</td>
<td>0.897</td>
</tr>
</tbody>
</table>

Table E.2: A small collection of scan measurements with the observed interference visibility in comparison to the estimated visibility. The scans of the type a are the bare interference of the two photons 1 and 2 at the beam splitter with polarizers at 45° placed in both of their arms. The type b measurements utilize entanglement swapping, since the correlation between photon 0 and 3 is observed with polarizers at 45° in their arms. The last two scans were taken in the final configuration of the setup where the polarizers are realized with polarizing beam splitters, and a much longer measurement time was used. The last measurement, type b’, was measured with both the polarizers oriented at 0°.
E Effects Limiting the 4-fold Correlation Visibility in the Entanglement Swapping
F VHDL Code of the Programmable Coincidence Logic

Below is the VHDL code for implementing the coincidence logic for a static entanglement swapping experiment with a more-complete Bell-state analyzer (see Section 8.3). This logic was implemented in a XC9536XL CPLD device from Xilinx, using the Foundation Express software from Xilinx.

F.1 Main Routine: telecoincall.vhd

This routine takes care of the inputs and outputs of the device, and also calls the required sub routines.

```vhdl
library IEEE; use IEEE.std_logic_1164.all;

entity telecoincall is
    port(
        dlong: in STD_LOGIC_VECTOR (0 to 7);
        clk: in STD_LOGIC;
        sel: in integer range 0 to 2;
        data: out STD_LOGIC_VECTOR (0 to 7)
    );
end telecoincall;

architecture coinc_arch of telecoincall is

component inplatch is
    port(
        d: in STD_LOGIC;
        clk: in STD_LOGIC;
        dd: out STD_LOGIC
    );
end component;
```
component compar is
    port (  
        d: in STD_LOGIC_VECTOR (0 to 7);  
        clk: in STD_LOGIC;  
        sel: in integer range 0 to 2;  
        data: out STD_LOGIC_VECTOR (0 to 7)  
    );
end component compar;

signal dt: STD_LOGIC_VECTOR (0 to 7);

begin

  l0: inplatch port map(dlong(0),clk,dt(0));
  l1: inplatch port map(dlong(1),clk,dt(1));
  l2: inplatch port map(dlong(2),clk,dt(2));
  l3: inplatch port map(dlong(3),clk,dt(3));
  l4: inplatch port map(dlong(4),clk,dt(4));
  l5: inplatch port map(dlong(5),clk,dt(5));
  l6: inplatch port map(dlong(6),clk,dt(6));
  l7: inplatch port map(dlong(7),clk,dt(7));

  c1: compar port map(dt,clk,sel,data);

end coinc_arch;

F.2 Sub Routine: inplatch.vhd

This sub routine transforms an input detection pulse which can be in the “high” state for times longer than one clock period to an internal variable, which is only “high” for the first clock period directly after the input pulse started. This is necessary, because the logic only compares the status of the inputs at a clock edge, which would lead to multiple counts for an input pulse which lasts for several clock edges.

library IEEE; use IEEE.std_logic_1164.all;

entity inplatch is
    port (  
        d: in STD_LOGIC;
    );
F.3 Sub Routine: compar.vhd

This subroutine performs the actual correlation of the detection pulses. Depending on the setting of the two select inputs, the routine checks for certain bit patterns on the eight detectors, and generates a pulse at the corresponding output.

library IEEE; use IEEE.std_logic_1164.all;

-- get all possible teleportation combinations for 8 detectors and 2 bell states

entity compar is
  port (
    d: in STD_LOGIC_VECTOR (0 to 7);
  );
end inplatch;

architecture inplatch_arch of inplatch is

signal temp: STD_LOGIC;

begin
  -- <<enter your statements here>>
  prcss_inplatch: process (clk)
  begin
    if (CLK = '1' and CLK'Event) then
      if (d='1' and temp='0') then
        dd <= '1';
        temp <= '1';
      elsif (d='1' and temp='1') then
        dd <= '0';
        temp <= '1';
      else
        dd <= '0';
        temp <= '0';
      end if;
    end if;
  end process;
end inplatch_arch;
F VHDL Code of the Programmable Coincidence Logic

    sel: in integer range 0 to 2;
    clk: in STD_LOGIC;
    data: out STD_LOGIC_VECTOR (0 to 7)
);

end compar;

architecture compar_arch of compar is

begin

    p1: process (clk)
    begin

        if (clk'event and clk='1') then
            -- input data structure: 8 Bits: (Bob0:) D0+, D0-, (BSA:) D1+, D1-, D2+, D2-,
            -- (Bob3:) D3+, D3-
            if sel=0 then
                -- determine all 8 4-fold coincidences
                -- output data meaning: bits 0-3: 0+ psi- 0+, 0+ psi- 0-, 0- psi- 0+, 0- psi- 0-
                -- bits 4-7: 0+ psi+ 0+, 0+ psi+ 0-, 0- psi+ 0+, 0- psi+ 0-

                if (d="10100110" or
                    d="10011010" or
                    d="10101010" or
                    d="10010110") then
                    data <= "10000000"; -- 0+ psi- 0+
                elsif (d="10100101" or
                         d="10011001" or
                         d="10101001" or
                         d="10010101") then
                    data <= "01000000"; -- 0+ psi- 0-
                elsif (d="01100110" or
                         d="01011010" or
                         d="01010110" or
                         d="01101010") then
                    data <= "00100000"; -- 0- psi- 0+
                elsif (d="01100101" or
                         d="01011001" or
                         d="01010101" or
                         d="01101001") then
                    data <= "00010000"; -- 0- psi- 0+ 
                else
                    data <= "00000000"; -- 0+ psi- 0-
                end if;
            end if;

        end if;

    end process;

end architecture;
data <= "00010000"; -- 0- psi- 0-

elsif (d="10110010" or
d="10001110") then
data <= "00001000"; -- 0+ psi+ 0+

elsif (d="10110001" or
d="10001101") then
data <= "00000100"; -- 0+ psi+ 0-

elsif (d="01110010" or
d="01001110") then
data <= "00000010"; -- 0- psi+ 0+

elsif (d="01110001" or
d="01001101") then
data <= "00000001"; -- 0- psi+ 0-

else
data <= "00000000";
end if;

elsif sel=1 then

-- determine several 2-folds for adjustment
-- outputs 0 to 4: 2-folds D0+^D1* D0+^D2*, D0-^D1* D0-^D2*, D3+^D1* D3+^D2*, D3-^D1* D3-^D2*, D1*^D2*

if (d="10100000" or
d="10010000" or
d="10001000" or
d="10000100") then
data <= "10000000"; -- 2-fold D0+^D1* or D0+^D2*

elsif (d="01100000" or
d="01010000" or
d="01001000" or
d="01000100") then
data <= "01000000"; -- 2-fold D0^-D1* or D0^-D2*

elsif (d="00100010" or
d="00010010" or
d="00001010" or
d="00000110") then
data <= "00100000"; -- 2-fold D3+^D1* or D3+^D2*

elseif (d="00100010" or
d="00010010" or
d="00001010" or
d="00000110") then
data <= "00100000"; -- 2-fold D3^-D1* or D3^-D2*
elsif (d="00100001" or 
d="00010001" or 
d="00001001" or 
d="00000101") then 
data <= "00010000";  -- 2-fold D3^D1* or D3^D2*
elsif (d="00101000" or 
d="00011000" or 
d="00100100" or 
d="00010100") then 
data <= "00001000";  -- 2-fold D1^D2*
else 
data <= "00000000";
end if;
elsif sel=2 then
  -- all signals mapped through for singles
  data <= d;
end if;
end if;
end process p1;
end compar_arch;
G Technical Terms

G.1 Visibility

The visibility is a well suited measure for the quality of interference, and is defined as:

\[ V = \frac{\text{Max} - \text{Min}}{\text{Max} + \text{Min}}, \tag{G.1} \]

where \( \text{Max} \) and \( \text{Min} \) are the maximal and minimal observed intensities respectively.

In the case that the observed values are count rates, also the calculation of the statistical error of \( V \) is relevant. Since photon detections are random their statistics obeys the poisson distribution, i.e. for a certain photon count number \( N \) the 1-\( \sigma \) standard deviation is \( \Delta N = \sqrt{N} \). From gaussian error calculation the standard deviation of \( V \) is given in general by

\[ \Delta V = \sqrt{\frac{\partial V}{\partial \text{Max}} \Delta \text{Max} + \frac{\partial V}{\partial \text{Min}} \Delta \text{Min}}. \tag{G.2} \]

Including the partial derivatives of \( V \) and the statistical uncertainty for \( \text{Max} \) and \( \text{Min} \) leads to the expression

\[ \Delta V = \sqrt{\left( \frac{2\text{Min}}{(\text{Max} + \text{Min})^2 \sqrt{\text{Max}}} \right)^2 + \left( \frac{-2\text{Max}}{(\text{Max} + \text{Min})^2 \sqrt{\text{Min}}} \right)^2}, \tag{G.3} \]

which is can be simplified to

\[ \Delta V = \frac{2}{(\text{Max} + \text{Min})^2} \sqrt{\text{Min}^2 \text{Max} + \text{Max}^2 \text{Min}}. \tag{G.4} \]

G.2 Gaussian \( \sigma \) and FWHM

The gaussian distribution is defined as

\[ g(x) = Ae^{-\frac{x^2}{2}} \tag{G.5} \]

with \( A \) the normalization, and \( \sigma \) the \( e^{-1/2} \) width of the distribution, or more conveniently \( \Delta x_{\text{Gauss}} = \sigma \). In many practical situations the full-width-half-maximum \( \Delta x_{\text{FWHM}} \) width is specified. This is the full width of the distribution at value which is half the maximum. The correspondence between the two widths can be calculated by setting \( g(x) = \frac{1}{2} \), which leads to

\[ \Delta x_{\text{Gauss}} = \frac{\Delta x_{\text{FWHM}}}{\sqrt{8 \ln 2}} \approx \Delta_{\text{FWHM}0.4247}. \tag{G.6} \]
G.3 Coherence Time

In vacuum, the dispersion relation has the simple form: \( c = \frac{\lambda \omega}{2\pi} \), where \( c \) is the vacuum speed of light, \( \lambda \) is the wavelength, and \( \omega \) the angular frequency of the wave. If the spectral distribution of a light signal is gaussian with a 1σ-width of \( \Delta \omega \), then the conjugated temporal distribution of the wave packet is also a gaussian, with a width: \( \Delta \omega \cdot \Delta \tau \geq 1 \). This \( \Delta \tau \) can be identified with the coherence time, or longitudinal coherence, of the associated wave packet. By expressing \( \Delta \omega \) by \( \Delta \lambda \) via the derivative of the dispersion relation given above, the coherence time has the form:

\[
\tau_{\text{cohr}} = \frac{\lambda^2}{2\pi c \Delta \lambda}.
\] (G.7)

Here \( \lambda \) is the central wavelength, \( \Delta \lambda \) is the 1σ width of the spectral distribution, \( c \) is the vacuum speed of light, and \( \tau_{\text{cohr}} \) is 1σ of a gaussian temporal coherence function. In practice, often the FWHM-values of the spectral distribution are known, but this value can easily be converted via Equation (G.6). For instance for down-conversion photons with \( \lambda = 788 \text{ nm} \) and \( \Delta \lambda = 1.5 \text{ nm} \) (corresponds to \( \Delta \lambda_{\text{FWHM}} = 3.5 \text{ nm} \)), the coherence time is \( \tau_{\text{cohr}} = 220 \text{ fs} \).

G.4 Standard Logic Signals: TTL, CMOS, ECL, NIM

These standards of logic families and signals which are commonly used in the photon correlation experiments described in this work are explained in short terms. Please consult the information available from the given manufacturers or dedicated literature, such as [TS99, HH89], for further details.

TTL - Transistor Transistor Logic

The TTL logic is a very common standard, and is based on bipolar transistors. The inputs and the outputs of the logic gates have a relatively high impedance. The standard logic levels of an input are: logic low, is in the range of 0 V – 0.8 V and the logic high is in the range of 2.0 V – 5.0 V. It is important to remember, that a TTL input internally is pulled to +5 V, meaning that if a high-signal is applied, no current will flow into the input (< 40µA), and if a low-signal is applied, up to 1.6 mA (!) flow from the input towards ground. Therefore, a standard TTL output, capable of driving ten gates (FAN-out of ten) can source +0.4 mA in the high-state and drain –16 mA in the low-state. Typically, if an instrument has a TTL output, it means it will have about 0 V in the low-state, and 2.5 – 5 V in the high state. The integrated circuits with gates realized in the TTL family usually have description code which has a 74 XXX, where 74 denotes the TTL and XXX the implemented logic circuit. The standard Low-Power-Schottky-TTL (74 LS XXX) can be used for clock frequencies of up to about 15 MHz. Higher switching rates of about 100 MHz and high power driving abilities is only achieved with the Advanced-CMOS-TTL famliy (74 AC XXX or 74 ACT XXX).
CMOS - Complementary Mosfet

The CMOS logic family is based on N-channel and P-channel MOSFET transistors. The CMOS inputs have high impedance, making the devices susceptible to noise as well as destruction via electro-static discharging. Standard CMOS has a large supply voltage range $V_B$, from 3 V to 18 V. The input range for the low-state input is $0 \text{ V to } 1/3V_B$ and the high-state input range is $2/3V_B$ to $V_B$. CMOS logic dissipates very little power when static, since energy is consumed during the transition of a gate between two logic states, meaning that the power consumption is frequency dependent. Standard CMOS logic integrated circuits are commonly available and are usually named 40XX or 45XX, where 40/45 indicate the CMOS family and the number XX denotes the logic function.

ECL - Emitter Coupled Logic

ECL logic was developed for extra rapid switching rates and short delay times. The operation frequencies of modern devices can are well above 1 GHz. This is achieved at the cost of high power consumption in the devices. The inputs are 75 kΩ to $-5.2 \text{ V}$, and the outputs are specified for driving 50 Ω referenced to $-2 \text{ V}$, and the outputs must be terminated so that the transistors are biased and the device can operate. The logic levels of ECL are about $-0.9 \text{ V}$ for the high-state and $-1.8 \text{ V}$ for the low-state. There are different generations of ECL standards, such as the 10K, the 100K, ECLinPS, etc. which differ in speed, tolerance requirements and also slightly in the logic levels. A further variant is so called PECL, which is nothing else than standard ECL used with shifted 0 V/+5 V supply voltages instead of the standard $-5.2 \text{ V}/0 \text{ V}$ supply. Details are best researched directly from the data sheets and application notes of the manufacturers, as from experience, the information in dedicated electronics books is very scarce.

NIM - Nuclear Instrument Module

The international NIM standard defines the implementation of nuclear instruments, most obviously that the modules operate in NIM-crates which supplies the electrical power. Several modules can be combined as required. NIM also defines different types of signals for interconnecting modules. Relevant in photon correlation experiments is the “NIM-Fast Negative Logic”. The rise and fall-times of this logic standard are about 1 ns, and all signals are terminated with 50 Ω, allowing the processing of photon detection pulses with high accuracy. The signals are defined in currents, but can easily be converted to voltages via the 50 Ω termination. Typically the output gives ±1 mA in the 0-state, and $-18 \text{ mA} (0.9 \text{ V in 50 } \Omega)$ in the 1-state.
## G.4.1 Summary of Standard Logic Levels

<table>
<thead>
<tr>
<th>Type</th>
<th>Output Levels (must deliver)</th>
<th>Input Levels (must accept)</th>
<th>Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL-0</td>
<td>0 to +0.4 V</td>
<td>0 to +0.8 V</td>
<td>Fairchild Semiconductor</td>
</tr>
<tr>
<td>TTL-1</td>
<td>+2.4 to +5 V</td>
<td>+2.0 to +5 V</td>
<td>ONSemiconductor (former Motorola)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Texas Instruments</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>STMicroelectronics</td>
</tr>
<tr>
<td>CMOS-0</td>
<td>0 V</td>
<td>0 to 1/3V_B</td>
<td>as for TTL; also Philips</td>
</tr>
<tr>
<td>CMOS-1</td>
<td>V_B</td>
<td>2/3V_B to V_B</td>
<td>Toshiba</td>
</tr>
<tr>
<td>ECL-0</td>
<td>−1.63 to −1.95 V</td>
<td>−1.48 to −1.95 V</td>
<td>ONSemiconductor (former Motorola)</td>
</tr>
<tr>
<td>ECL-1</td>
<td>−0.81 to −0.98 V</td>
<td>−0.81 to −1.13 V</td>
<td>Synergy</td>
</tr>
<tr>
<td>NIM-0</td>
<td>−1 to +1 mA</td>
<td>−4 to +20 mA</td>
<td>Perkin Elmer (Ortec)</td>
</tr>
<tr>
<td>NIM-1</td>
<td>−14 to −18 mA</td>
<td>−12 to −36 mA</td>
<td>LeCroy</td>
</tr>
</tbody>
</table>
H  Publications of the Author

Up to present, I have been involved in the work described in the following publications:


H.1 Published work of this Thesis

The work presented in this thesis was summarized in two publications, which are given in the following pages:
Quantum Cryptography with Entangled Photons

Thomas Jennewein,1 Christoph Simon,1 Gregor Weihs,1 Harald Weinfurter,2 and Anton Zeilinger1

1Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Wien, Austria
2Sektion Physik, Universität München, Schellingstrasse 4/III, D-80799 München, Germany

By realizing a quantum cryptography system based on polarization entangled photon pairs we establish highly secure keys, because a single photon source is approximated and the inherent randomness of quantum measurements is exploited. We implement a novel key distribution scheme using Wigner’s inequality to test the security of the quantum channel, and, alternatively, realize a variant of the BB84 protocol. Our system has two completely independent users separated by 360 m, and generates raw keys at rates of 400–800 bits/s with bit error rates around 3%.

PACS numbers: 03.67.Dd, 42.79.Sz, 89.80.+h

The primary task of cryptography is to enable two parties (commonly called Alice and Bob) to mask confidential messages, such that the transmitted data are illegible to any unauthorized third party (called Eve). Usually this is done using shared secret keys. However, in principle it is always possible to intercept classical key distribution unnoticedly. The recent development of quantum key distribution [1] can cover this major loophole of classical cryptography. It allows Alice and Bob to establish two completely secure keys by transmitting single quanta (qubits) along a quantum channel. The underlying principle of quantum key distribution is that nature prohibits gaining information on the state of a quantum system without disturbing it. Therefore, in appropriately designed schemes, no tapping of the qubits is possible without showing up to Alice and Bob. These secure keys can be used in a one-time-pad protocol [2], which makes the entire communication absolutely secure.

Two well-known concepts for quantum key distribution are the BB84 scheme and the Ekert scheme. The BB84 scheme [1] uses single photons transmitted from Alice to Bob, which are prepared at random in four partly orthogonal polarization states: 0°, 45°, 90°, and 135°. If Eve tries to extract information about the polarization of the photons she will inevitably introduce errors, which Alice and Bob can detect by comparing a random subset of the generated keys.

The Ekert scheme [3] is based on entangled pairs and uses Bell’s inequality [4] to establish security. Both Alice and Bob receive one particle out of an entangled pair. They perform measurements along at least three different directions on each side, where measurements along parallel axes are used for key generation and oblique angles are used for testing the inequality. In Ref. [3], Ekert pointed out that eavesdropping inevitably affects the entanglement between the two constituents of a pair and therefore reduces the degree of violation of Bell’s inequality. While we are not aware of a general proof that the violation of a Bell inequality implies the security of the system, this has been shown [5] for the BB84 protocol adapted to entangled pairs and the Clauser-Horne-Shimony-Holt (CHSH) inequality [6].

In any real cryptography system, the raw key generated by Alice and Bob contains errors, which have to be corrected by classical error correction [7] over a public channel. Furthermore, it has been shown that whenever Alice and Bob share a sufficiently secure key, they can enhance its security by privacy amplification techniques [8], which allow them to distill a key of a desired security level.

A range of experiments have demonstrated the feasibility of quantum key distribution, including realizations using the polarization of photons [9] or the phase of photons in long interferometers [10]. These experiments have a common problem: the sources of the photons are attenuated laser pulses which have a nonvanishing probability to contain two or more photons, leaving such systems prone to the so-called beam splitter attack [11].

Using photon pairs as produced by parametric down-conversion allows us to approximate a conditional single photon source [12] with a high bit rate [13], and yet a very low probability for generating two pairs simultaneously. Moreover, when utilizing entangled photon pairs one immediately profits from the inherent randomness of quantum mechanical observations leading to purely random keys.

Various experiments with entangled photon pairs have already demonstrated that entanglement can be preserved over distances as large as 10 km [14], yet none of these experiments was a full quantum cryptography system. We present in this paper a complete implementation of quantum cryptography with two users, separated and independent of each other in terms of Einstein locality and exploiting the features of entangled photon pairs for generating highly secure keys.

In the following, we will describe the variants of the Ekert scheme and of the BB84 scheme, both of which we implemented in our experiment, based on polarization entangled photon pairs in the singlet state

\[ |\Psi^-\rangle = \frac{1}{\sqrt{2}} (|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B). \]

where photon A is sent to Alice and photon B is sent to Bob, and H and V denote the horizontal and vertical linear polarization, respectively. This state shows perfect
anticorrelation for polarization measurements along parallel but arbitrary axes. However, the actual outcome of an individual measurement on each photon is inherently random. These perfect anticorrelations can be used for generating the keys, yet the security of the quantum channel remains to be ascertained by implementing a suitable procedure.

Our first scheme utilizes Wigner’s inequality [15] for establishing the security of the quantum channel, in analogy to the Ekert scheme which uses the CHSH inequality. Here Alice chooses between two polarization measurements along the axes Χ and Ψ, with the possible results +1 and −1, on photon A and Bob between measurements along Ψ and Ω on photon B. Polarization parallel to the analyzer axis corresponds to a +1 result, and polarization orthogonal to the analyzer axis corresponds to −1.

\[
p_{++}(-30°, 0°) + p_{++}(0°, 30°) - p_{-+}(-30°, 30°) = \frac{1}{8} + \frac{1}{8} - \frac{3}{8} = -\frac{1}{8} \neq 0.
\]

As Wigner’s inequality is derived assuming perfect anticorrelations, which are only approximately realized in any practical situation, one should be cautious in applying it to test the security of a cryptography scheme. When the deviation from perfect anticorrelations is substantial, Wigner’s inequality has to be replaced by an adapted version [16].

In order to implement quantum key distribution, Alice and Bob each vary their analyzers randomly between two settings, Alice: −30°, 0° and Bob: 0°, 30° (Fig. 1a). Because Alice and Bob operate independently, four possible combinations of analyzer settings will occur, of which the three oblique settings allow a test of Wigner’s inequality and the remaining combination of parallel settings (Alice = 0° and Bob = 0°) allows the generation of keys via the perfect anticorrelations, where either Alice or Bob has to invert all bits of the key to obtain identical keys.

If the measured probabilities violate Wigner’s inequality, then the security of the quantum channel is ascertained, and the generated keys can readily be used. This scheme is an improvement on the Ekert scheme which uses the CHSH inequality and requires three settings of Alice’s and Bob’s analyzers for testing the inequality and generating the keys. From the resulting nine combinations of settings, four are taken for testing the inequality, two are used for building the keys, and three are omitted completely. However, in our scheme each user needs only two analyzer settings and the detected photons are used more efficiently, thus allowing a significantly simplified experimental implementation of the quantum key distribution.

As a second quantum cryptography scheme we implemented a variant of the BB84 protocol with entangled photons, as proposed in Ref. [17]. In this case, Alice and Bob randomly vary their analysis directions between 0° and 45° (Fig. 1b). Alice and Bob observe perfect anticorrelations of their measurements whenever they happen to have parallel oriented polarizers, leading to bitwise complementary keys. Alice and Bob obtain identical keys if one of them inverts all bits of the key. Polarization entangled photon pairs offer a means to approximate a single photon situation. Whenever Alice makes a measurement on photon A, photon B is projected into the orthogonal state which is then analyzed by Bob, or vice versa. After collecting the keys, Alice and Bob authenticate their keys by openly comparing a small subset of their keys and evaluating the bit error rate.

The experimental realization of our quantum key distribution system is sketched in Fig. 2. Type-II parametric down-conversion in β-barium borate (BBO) [18], pumped with an argon-ion laser working at a wavelength of 351 nm and a power of 350 mW, leads to the production of polarization entangled photon pairs at a wavelength of 702 nm. The photons are each coupled into 500 m long optical fibers and transmitted to Alice and Bob, respectively, who are separated by 360 m.

Alice and Bob both have Wollaston polarizing beam splitters as polarization analyzers. We will associate a setting of parallel polarization (+1) with the key bit 1.
and orthogonal detection $(-1)$ with the key bit 0. Electro-optic modulators in front of the analyzers rapidly switch (rise time $<15$ ns, minimum switching interval 100 ns) the axis of the analyzer between two desired orientations, controlled by quantum random signal generators [19]. These quantum random signal generators are based on the quantum mechanical process of splitting a beam of photons and have a correlation time of less than 100 ns.

The photons are detected in silicon avalanche photo diodes [20]. Time interval analyzers on local personal computers register all detection events as time stamps together with the setting of the analyzers and the detection result. A measurement run is initiated by a pulse from a separate laser diode sent from the source to Alice and Bob via a second optical fiber. Only after a measurement run is completed, Alice and Bob compare their lists of detections to extract the coincidences. In order to record the detection events very accurately, the time bases in Alice’s and Bob’s time interval analyzers are controlled by two rubidium oscillators. The stability of each time base is better than 1 ns for 1 min. The maximal duration of a measurement is limited by the amount of memory in the personal computers (typically 1 min).

Overall our system has a measured total coincidence rate of $\sim 1700$ s$^{-1}$, and a singles rate of $\sim 35 000$ s$^{-1}$. From this, one can estimate the overall detection efficiency of each photon path to be 5% and the pair production rate to be $7 \times 10^5$ s$^{-1}$. Our system is very immune against a beam splitter attack because the ratio of two-pair events is only $3 \times 10^{-3}$, where a two-pair event is the emission of two pairs within the coincidence window of 4 ns. The coincidence window in our experiment is limited by the time resolution of our detectors and electronics, but in principle it could be reduced to the coherence time of the photons, which is usually of the order of picoseconds.

In realizing the quantum key distribution based on Wigner’s inequality, Alice’s analyzer switches randomly with equal frequency between $-30^\circ$ and $0^\circ$, and Bob’s analyzer between $0^\circ$ and $30^\circ$. After a measurement, Alice and Bob extract the coincidences for the combinations of settings of $(-30^\circ, 30^\circ)$, $(-30^\circ, 0^\circ)$ and $(0^\circ, 30^\circ)$, and calculate each probability. For example, the probability $p_{++,0^\circ,30^\circ}$ is calculated from the numbers of coincident events $C_{++, C_{+\pm}, C_{-\pm}, C_{-}}$ measured for this combination of settings by

$$p_{++,0^\circ,30^\circ} = \frac{C_{++}}{C_{++} + C_{+\pm} + C_{-\pm} + C_{-}}.$$  \hspace{1cm} (5)

We observed in our experiment that the left-hand side of inequality (2) evaluated to $0.112 \pm 0.014$. This violation of (2) is in good agreement with the prediction of quantum mechanics and ensures the security of the key distribution. Hence the coincident detections obtained at the parallel settings $\(0^\circ, 0^\circ\)$, which occur in a quarter of all events, can be used as keys. In the experiment Alice and Bob established 2162 bits raw keys at a rate of 420 bits/s [21], and observed a quantum bit error rate of 3.4%.

In our realization of the BB84 scheme, Alice’s and Bob’s analyzers both switch randomly between $0^\circ$ and $45^\circ$. After a measurement run, Alice and Bob extract the coincidences measured with parallel analyzers, $(0^\circ, 0^\circ)$ and $(45^\circ, 45^\circ)$, which occur in half of the cases, and generate the raw keys. Alice and Bob collected $\sim 80 000$ bits of key at a rate of 850 bits/s, and observed a quantum bit error rate of 2.5%, which ensures the security of the quantum channel.

For correcting the remaining errors while maintaining the secrecy of the key, various classical error correction and privacy amplification schemes have been developed [7]. We implemented a simple error reduction scheme requiring only little communication between Alice and Bob. Alice and Bob arrange their keys in blocks of $n$ bits and evaluate the bit parity of the blocks (a single bit indicating an odd or even number of ones in the block). The parities are compared in public, and the blocks with agreeing parities are kept after discarding one bit per block [22]. Since parity checks reveal only odd occurrences of bit errors, a fraction of errors remains. The optimal block length $n$ is determined by a compromise between key losses and remaining bit errors. For a bit error rate $p$ the probability for $k$ wrong bits in a block of $n$ bits is given by the binomial distribution $P_p(k) = \binom{n}{k} p^k (1-p)^{n-k}$.

Neglecting terms for three or more errors and accounting for the loss of one bit per agreeing parity, this algorithm has an efficiency $\eta(n) = [1 - P_p(1)](n - 1)/n$, defined as the ratio between the key sizes after parity check and before. Finally, under the same approximation as above, the remaining bit error rate $p'$ is $p' = [1 - P_p(0) - P_p(1)](2/n)$. Our key has a bit error rate $p = 2.5\%$, for which $\eta(n)$ is maximized at $n = 8$ with $\eta(8) = 0.7284$, resulting in $p' = 0.40\%$. Hence, from $\sim 80 000$ bits of raw key with a quantum bit error rate of 2.5%, Alice and Bob use 10% of the key for checking the security and the remaining 90% of the key to distill 49984 bits of error corrected key with a bit error rate of 0.4%. Finally, Alice transmits a 43 200 bit large image to Bob via the one-time-pad protocol, utilizing a bitwise XOR combination of message and key data (Fig. 3).
In this Letter we presented the first full implementation of entangled state quantum cryptography. All the equipment of the source and of Alice and Bob has proven to operate outside shielded lab environments with a very high reliability. While further practical and theoretical investigations are still necessary, we believe that this work demonstrates that entanglement based cryptography can be tomorrow’s technology.

This work was supported by the Austrian Science Foundation FWF (Projects No. S6502, No. S6504, and No. F1506), the Austrian Academy of Sciences, and the IST and TMR programs of the European Commission [Contracts No. IST-1999-10033 (QuComm) and No. ERBFMRXCT96-0087].

[2] In this classical cryptographic protocol the message is combined with a random key string of the same size as the message to form an encoded message which cannot be deciphered by any statistical methods. G. S. Vernam, J. Am. Inst. Electr. Eng. 55, 109 (1926).
[12] One photon of the pair can be used as a trigger for finding the other photon of the pair, provided that the probability of producing two pairs at a single time can be neglected. P. Grangier, G. Roger, and A. Aspect, Europhys. Lett. 1, 4 (1986); 1, 173 (1986); J. G. Rarity, P. R. Tapster, and E. Jakeman, Opt. Commun. 62, 201 (1987).
[13] Note also that in our case the beam splitter attack is less effective than for coherent pulses, because even when two pairs are produced simultaneously, Eve does not gain any information in those cases where Alice and Bob detect photons belonging to the same pair, because then the photon detected by Eve originates from a different pair and is completely uncorrelated to Alice’s and Bob’s photons.
[21] Note that it would be simple to bias the frequencies of analyzer combinations to increase the production rate of the keys.
[22] Removal of one bit erases the information about the blocks contained in the (public) parities.
[23] Windows-BMP format containing 60 × 90 pixels, 8 bit color information per pixel: 43200 bit of picture information. The file includes some header information and a color table, making the entire picture file 51840 bit. We encrypted only the picture information, leaving the file header and the color table unchanged.
[24] The “Venus” von Willendorf was found in 1908 at Willendorf in Austria and presently resides in the Naturhistorisches Museum, Vienna. Carved from limestone and dated 24 000–22 000 BC, she represents an icon of prehistoric art.
Experimental Nonlocality Proof of Quantum Teleportation and Entanglement Swapping

Thomas Jennewein, Gregor Weihs, Jian-Wei Pan, and Anton Zeilinger
Institut für Experimentalphysik, Universität Wien Boltzmanngasse 5, 1090 Wien, Austria
(Received 15 August 2001; published 18 December 2001)

Quantum teleportation strikingly underlines the peculiar features of the quantum world. We present an experimental proof of its quantum nature, teleporting an entangled photon with such high quality that the nonlocal quantum correlations with its original partner photon are preserved. This procedure is also known as entanglement swapping. The nonlocality is confirmed by observing a violation of Bell’s inequality by 4.5 standard deviations. Thus, by demonstrating quantum nonlocality for photons that never interacted, our results directly confirm the quantum nature of teleportation.

DOI: 10.1103/PhysRevLett.88.017903
PACS numbers: 03.67.Hk, 03.65.Ud, 42.50.Ct

Quantum state teleportation [1] allows the transfer of the quantum state from one system to another distant one. This system becomes the new original as it carries all information the original did and the state of the initial particle is erased, as necessitated by the quantum no-cloning theorem [2]. This is achieved via a combination of an entangled state and a classical message.

The most interesting case of quantum teleportation occurs when the teleported state itself is entangled. There the system to be teleported does not even enjoy its own state. This procedure is also known as “entanglement swapping” [3] because (Fig. 1) one starts with two pairs of entangled photons 0–1 and 2–3 and subjects photons 1 and 2 to a Bell-state measurement by which photons 0 and 3 also become entangled. As suggested by Peres [4] this even holds if the “entangling” Bell-state measurement is performed after photons 0 and 3 have already been registered. Entanglement swapping was shown [5] in a previous experiment, yet the low photon-pair visibility prevented a violation of a Bell’s inequality [6] for photons 0 and 3, which is a definitive test. This is the case, because if significant information about the state of the teleported photon 1 were gained in the teleportation procedure, the measurements on photons 0 and 3 would not violate Bell’s inequality. This fact is substantiated by the quantum no-cloning theorem [2]. Therefore, the violation of Bell’s inequality confirms that the state of photon 1 was even undefined in a fundamental way and Alice could not have played any kind of tricks to make the results look like successful teleportation. The experiment presented here provides now such a definitive proof of the quantum nature of teleportation.

In the present work quantum state teleportation is implemented in terms of polarization states of photons and hence relies on the entanglement of the polarization of photon pairs prepared in one of the four Bell states, e.g.,

$$|\psi_{01}\rangle = \frac{1}{\sqrt{2}} (|H\rangle_0 |V\rangle_1 - |V\rangle_0 |H\rangle_1).$$

(1)

A schematic overview of our quantum teleportation scheme is given in Fig. 1.

Initially, the system is composed of two independent entangled states and can be written in the following way:

$$|\psi_{\text{total}}\rangle = |\psi^-\rangle_0 \otimes |\psi^-\rangle_{23}.$$  

(2)

Including Eq. (1) in (2) and rearranging the resulting terms by expressing photon 1 and photon 2 in the basis of Bell states leads to

$$|\psi_{\text{total}}\rangle = \frac{1}{2} [(|\psi^+\rangle_0 |\psi^+\rangle_{12} - |\psi^-\rangle_0 |\psi^-\rangle_{12} - |\phi^+\rangle_0 |\phi^+\rangle_{12} + |\phi^-\rangle_0 |\phi^-\rangle_{12}].$$

(3)

Alice subjects photons 1 and 2 to a measurement in a Bell-state analyzer (BSA), and if she finds them in the state $|\psi^-\rangle_{12}$, then photons 0 and 3 measured by Bob will be in the entangled state $|\psi^-\rangle_{03}$. If Alice observes any of the other Bell states for photons 1 and 2, photons 0 and 3 will also be perfectly entangled correspondingly. We stress that photons 0 and 3 will be perfectly entangled for any result of the BSA, and therefore it is not necessary to apply a unitary operation to the teleported photon 3 as in the standard teleportation protocol. But it is certainly necessary for Alice to communicate to Victor her Bell-state measurement result. This enables him to sort Bob’s data into four subsets, each one representing the results for one of the four maximally entangled Bell states.

Therefore with suitable polarization measurements on photons 0 and 3, Victor will obtain a violation of Bell’s inequality and confirm successful quantum teleportation for each of the four subsets separately. In our experiment, Alice was restricted to identifying only the state $|\psi^-\rangle_{12}$ due to technical reasons. This reduction of the teleportation efficiency to 25% does not influence the fidelity. A large disturbance of the fidelity would perturb the teleported entanglement to such a degree that a violation of Bell’s inequality could no longer be achieved. As explained elsewhere [7] teleportation efficiency measures the fraction of cases in which the procedure is successful and the fidelity characterizes the quality of the teleported state in the successful cases. For example, loss of a photon in our case leads outside the two-state Hilbert space used and thus reduces the efficiency and not the fidelity.

It has been shown that using linear optical elements the efficiency of any BSA is limited to maximally 50% [8]. A configuration where photons 1 and 2 are brought to interference at a 50:50 beam splitter is able to identify two
FIG. 1. Entanglement swapping version of quantum teleportation. Two entangled pairs of photons 0–1 and 2–3 are produced in the sources I and II, respectively. One photon from each pair is sent to Alice who subjects them to a Bell-state measurement, projecting them randomly into one of four possible entangled states. Alice records the outcome and hands it to Victor. This procedure projects photons 0 and 3 into a corresponding entangled state. Bob performs a polarization measurement on each photon, choosing freely the polarizer angle and recording the outcomes. He hands his results also to Victor, who sorts them into subsets according to Alice’s results, and checks each subset for a violation of Bell’s inequality. This shows whether photons 0 and 3 became entangled although they never interacted in the past. This procedure can be seen as teleportation either of the state of photon 1 to photon 3 or of the state of photon 2 to photon 0. Interestingly, the quantum prediction for the observations does not depend on the relative space-time arrangement of Alice’s and Bob’s detection events.

Bell states exactly, and the remaining two only together (demonstrated in [9]). Particularly easy to identify is the $|\Psi^-\rangle$ state, as only in this case the two photons can be detected in separate outputs of the beam splitter.

The setup of our system is shown in Fig. 2. Two separate polarization entangled photon pairs are produced via type-II down-conversion in barium borate (BBO) [10] pumped by UV laser pulses at a wavelength of 394 nm, a pulse width of ~200 fs, a repetition rate of 76 MHz, and an average power of 370 mW. The entangled photons had a wavelength of 788 nm. Through spectral filtering with a $\Delta \lambda_{\text{WHM}} = 3.5$ nm for photons 0 and 3 and $\Delta \lambda_{\text{WHM}} = 1$ nm for photons 1 and 2, the coherence time of the photons was made to exceed the pulse width of the UV laser, making the two entangled photon pairs indistinguishable in time, a necessary criterion for interfering photons from independent down-conversions [11]. The registered event rate of photon pairs was about 2000 per sec before the Bell-state analyzer (Alice) and the polarizing beam splitter (Bob). The rate of obtaining a fourfold photon event for the teleportation was about 0.0065 per sec. Each single correlation measurement for one setting of the polarizers lasted 16 000 sec. The polarization alignment of the optical fibers performed before each measurement proved to be stable within 1° for 24 h.
The nondeterministic nature of the photon pair production implies an equal probability for producing two photon pairs in separate modes (one photon each in modes 0, 1, 2, 3) or two pairs in the same mode (two photons each in modes 0 and 1 or in modes 2 and 3). The latter cannot lead to coincidences in Alice’s detectors behind her beam splitter. We exclude these cases by accepting events only where Bob registers a photon each in mode 0 and mode 3. It was shown by Zukowski [12] that despite these effects of the nondeterministic photon source experiments of our kind still constitute valid demonstrations of nonlocality in quantum teleportation.

The entanglement of the teleported state was characterized by several correlation measurements between photons 0 and 3 to estimate the fidelity of the entanglement. As is customary the fidelity $F = \langle \Psi^- | \rho | \Psi^- \rangle$ measures the quality of the observed state $\rho$ compared to the ideal quantum case $| \Psi^- \rangle$. The experimental correlation coefficient $E_{\text{exp}}$ is related to the ideal one $E_{\text{QM}}$ via $E_{\text{exp}} = [(4F - 1)/3]E_{\text{QM}}$ [13]. The correlation coefficients are defined as $E = (N_{++} - N_{--} - N_{++} + N_{--})/2N_{ij}$, where $N_{ij}(\phi_0, \phi_3)$ are the coincidences between the $i$ channel of the polarizer of photon 0 set at angle $\phi_0$, and the $j$ channel of the polarizer of photon 3 set at angle $\phi_3$. The results (Fig. 3) show the high fidelity of the entangled teleportation.

The Clauser-Horne-Shimony-Holt (CHSH) inequality [14] is a variant of Bell’s inequality, which overcomes the inherent limits of a lossy system using a fair sampling hypothesis. It requires four correlation measurements performed with different analyzer settings. The CHSH inequality has the following form:

$$S = |E(\phi_0, \phi'_0) - E(\phi_0, \phi'_3)| + |E(\phi'_0, \phi'_1) + E(\phi'_0, \phi''_0)| \leq 2,$$

where $S$ is the “Bell parameter,” $E(\phi_0, \phi_3)$ is the correlation coefficient for polarization measurements where $\phi_0$ is the polarizer setting for photon 0, and $\phi_3$ is the setting for photon 3 [15]. The quantum mechanical prediction for photon pairs in a $\Psi^-$ state is $E_{\text{QM}}(\phi_0, \phi_3) = -\cos(2(\phi_0 - \phi_3))$. The settings $(\phi_0, \phi'_0, \phi''_0, \phi'_3) = (0^\circ, 22.5^\circ, 45^\circ, 67.5^\circ)$ maximize $S$ to $S_{\text{QM}} = 2\sqrt{2}$, which clearly violates the limit of 2 and leads to a contradiction between local realistic theories and quantum mechanics [6]. In our experiment, the four correlation coefficients between photons 0 and 3 gave the following results: $E(0^\circ, 22.5^\circ) = -0.628 \pm 0.046$, $E(0^\circ, 67.5^\circ) = +0.677 \pm 0.042$, $E(45^\circ, 22.5^\circ) = -0.541 \pm 0.045$, and $E(45^\circ, 67.5^\circ) = -0.575 \pm 0.047$. Hence, $S = 2.421 \pm 0.091$ which clearly violates the classical limit of 2 by 4.6 standard deviations as measured by the statistical error. The differences in the correlation coefficients come from the higher correlation fidelity for analyzer settings closer to $0^\circ$ and $90^\circ$, as explained in Fig. 3.

The travel time from the source to the detectors was equal within 2 ns for all photons. Both Alice’s and Bob’s detectors were located next to each other, but Alice and Bob were separated by about 2.5 m, corresponding to a luminal signaling time of 8 ns between them. Since the time resolution of the detectors is <1 ns, Alice’s and Bob’s detection events were spacelike separated for all measurements.

A seemingly paradoxical situation arises—as suggested by Peres [4]—when Alice’s Bell-state analysis is delayed long after Bob’s measurements. This seems paradoxical, because Alice’s measurement projects photons 0 and 3 into an entangled state after they have been measured. Nevertheless, quantum mechanics predicts the same correlations. Remarkably, Alice is even free to choose the kind of measurement she wants to perform on photons 1 and 2. Instead of a Bell-state measurement she could also measure the polarizations of these photons individually. Thus depending on Alice’s later measurement, Bob’s earlier results indicate either that photons 0 and 3 were entangled or photons 0 and 1 and photons 2 and 3. This means that the physical interpretation of his results depends on Alice’s later decision.

The entanglement of the teleported state was characterized by several correlation measurements between photons 0 and 3 to estimate the fidelity of the entanglement. As is customary the fidelity $F = \langle \Psi^- | \rho | \Psi^- \rangle$ measures the quality of the observed state $\rho$ compared to the ideal quantum case $| \Psi^- \rangle$. The experimental correlation coefficient $E_{\text{exp}}$ is related to the ideal one $E_{\text{QM}}$ via $E_{\text{exp}} = [(4F - 1)/3]E_{\text{QM}}$ [13]. The correlation coefficients are defined as $E = (N_{++} - N_{--} - N_{++} + N_{--})/2N_{ij}$, where $N_{ij}(\phi_0, \phi_3)$ are the coincidences between the $i$ channel of the polarizer of photon 0 set at angle $\phi_0$, and the $j$ channel of the polarizer of photon 3 set at angle $\phi_3$. The results (Fig. 3) show the high fidelity of the entangled teleportation.

The Clauser-Horne-Shimony-Holt (CHSH) inequality [14] is a variant of Bell’s inequality, which overcomes the inherent limits of a lossy system using a fair sampling hypothesis. It requires four correlation measurements performed with different analyzer settings. The CHSH inequality has the following form:

$$S = |E(\phi_0, \phi'_0) - E(\phi_0, \phi'_3)| + |E(\phi'_0, \phi'_1) + E(\phi'_0, \phi''_0)| \leq 2,$$

where $S$ is the “Bell parameter,” $E(\phi_0, \phi_3)$ is the correlation coefficient for polarization measurements where $\phi_0$ is the polarizer setting for photon 0, and $\phi_3$ is the setting for photon 3 [15]. The quantum mechanical prediction for photon pairs in a $\Psi^-$ state is $E_{\text{QM}}(\phi_0, \phi_3) = -\cos(2(\phi_0 - \phi_3))$. The settings $(\phi_0, \phi'_0, \phi''_0, \phi'_3) = (0^\circ, 22.5^\circ, 45^\circ, 67.5^\circ)$ maximize $S$ to $S_{\text{QM}} = 2\sqrt{2}$, which clearly violates the limit of 2 and leads to a contradiction between local realistic theories and quantum mechanics [6]. In our experiment, the four correlation coefficients between photons 0 and 3 gave the following results: $E(0^\circ, 22.5^\circ) = -0.628 \pm 0.046$, $E(0^\circ, 67.5^\circ) = +0.677 \pm 0.042$, $E(45^\circ, 22.5^\circ) = -0.541 \pm 0.045$, and $E(45^\circ, 67.5^\circ) = -0.575 \pm 0.047$. Hence, $S = 2.421 \pm 0.091$ which clearly violates the classical limit of 2 by 4.6 standard deviations as measured by the statistical error. The differences in the correlation coefficients come from the higher correlation fidelity for analyzer settings closer to $0^\circ$ and $90^\circ$, as explained in Fig. 3.

The travel time from the source to the detectors was equal within 2 ns for all photons. Both Alice’s and Bob’s detectors were located next to each other, but Alice and Bob were separated by about 2.5 m, corresponding to a luminal signaling time of 8 ns between them. Since the time resolution of the detectors is <1 ns, Alice’s and Bob’s detection events were spacelike separated for all measurements.

A seemingly paradoxical situation arises—as suggested by Peres [4]—when Alice’s Bell-state analysis is delayed long after Bob’s measurements. This seems paradoxical, because Alice’s measurement projects photons 0 and 3 into an entangled state after they have been measured. Nevertheless, quantum mechanics predicts the same correlations. Remarkably, Alice is even free to choose the kind of measurement she wants to perform on photons 1 and 2. Instead of a Bell-state measurement she could also measure the polarizations of these photons individually. Thus depending on Alice’s later measurement, Bob’s earlier results indicate either that photons 0 and 3 were entangled or photons 0 and 1 and photons 2 and 3. This means that the physical interpretation of his results depends on Alice’s later decision.
Such a delayed-choice experiment was performed by including two 10 m optical fiber delays for both outputs of the BSA. In this case photons 1 and 2 hit the detectors delayed by about 50 ns. As shown in Fig. 3, the observed fidelity of the entanglement of photon 0 and photon 3 matches the fidelity in the nondelayed case within experimental errors. Therefore, this result indicates that the time ordering of the detection events has no influence on the results and strengthens the argument of Peres [4]: This paradox does not arise if the correctness of quantum mechanics is firmly believed.

One might question the “independence” of photons 1 and 2 which interfere in the BSA, since all photons are produced by down-conversion from one and the same UV laser pulse, and the photons could take on a phase coherence from the UV laser. Note that the UV mirror was placed 13 cm behind the crystal, which greatly exceeds the pump pulse width of $\frac{1}{60}$ mm. We performed a Mach-Zehnder interference experiment of a laser on the BSA to measure the relative phase drifts due to instabilities of the optical paths. The statistical analysis of the temporal phase variation was done using the Allan variance [16], which we suggest as an appropriate measure. Accordingly, the phase drifted in a random walk behavior, accumulated a 1σ statistical drift of one wavelength within 400 s, and had a maximum drift of 15 wavelengths during 10 h. In a single measurement which lasted 16000 sec, any (hypothetical) phase relation between the two photons that interfered in the BSA would have been completely washed out. Therefore the contribution of such a phase relation to the outcome of the experiments can be ruled out.

Our work, besides definitely confirming the quantum nature of teleportation [17], is an important step for future quantum communication and quantum computation protocols. Entanglement swapping is the essential ingredient in quantum repeaters [18], where it can be used to establish entanglement between observers separated by larger distances as were possible using links with individual pairs only.

This work was supported by the Austrian Science Fund (FWF) and the “QuComm” IST-FET project of the European Commission.

[13] Evidently for a full characterization of $F$ one would have to perform many more measurements. Anyhow our observed values of $F$ give a reasonable estimate.
I’m very proud to mention that the publication on the quantum cryptography with entangled photons [JSW+00] has found great interest amongst the broad physics society as well the general public, also because it appeared at the same time with related experiments performed by the Geneva [TBZG00] and Los Alamos [NPW+00] groups, and was therefore reported in many specialist’s as well as general media. The media reports known to us are given in Table H.1.

Triggered by the impact of the QKD experiment, we were also invited to write a review article in a popular style on quantum cryptography and this experiment in particular for the “c’t” [JWZ01], one of the most popular computer magazines in Germany.

Table H.1: List of the media reports on the publication of the QKD experiment

<table>
<thead>
<tr>
<th>Media</th>
<th>WWW</th>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>American Institute of Physics, Physics News Update # 480</td>
<td><a href="http://www.aip.org">www.aip.org</a></td>
<td>24.04.2000</td>
<td>Exploiting Quantum “Spookiness” To Create Secret Codes</td>
</tr>
<tr>
<td>American Institute of Physics, News Release</td>
<td><a href="http://www.aip.org">www.aip.org</a></td>
<td>29.04.2000</td>
<td>You’d Have to Break the Laws of Physics to Break This Code</td>
</tr>
<tr>
<td>Nature Science Update</td>
<td><a href="http://www.nature.com">www.nature.com</a></td>
<td>03.05.2000</td>
<td>Top Secret</td>
</tr>
<tr>
<td>The New York Times</td>
<td><a href="http://www.nytimes.com">www.nytimes.com</a></td>
<td>03.05.2000</td>
<td>In The Quantum World, Keys to New Codes</td>
</tr>
<tr>
<td>Intelligence Newsletter</td>
<td><a href="http://www.intelligenceonline.com">www.intelligenceonline.com</a></td>
<td>04.05.2000</td>
<td>Cryptography-Progress in Quantum Technology</td>
</tr>
<tr>
<td>Süddeutsche Zeitung</td>
<td><a href="http://www.sueddeutsche.de">www.sueddeutsche.de</a></td>
<td>09.05.2000</td>
<td>Verschränkt und verschlüsselt</td>
</tr>
<tr>
<td>NRC Handelsblad, NL</td>
<td><a href="http://www.nrc.nl">www.nrc.nl</a></td>
<td>06.05.2000</td>
<td>Onkraakbare codes</td>
</tr>
<tr>
<td>Physics Today (Physics Update)</td>
<td><a href="http://www.aip.org">www.aip.org</a></td>
<td>06/2000</td>
<td>Quantum key distribution</td>
</tr>
<tr>
<td>Opto &amp; Laser Europe</td>
<td><a href="http://www.olemag.com">www.olemag.com</a></td>
<td>06/2000</td>
<td>R &amp; D: Optical encryption secures transmission of data</td>
</tr>
<tr>
<td>Physikalische Blätter</td>
<td><a href="http://www.wiley-vch.de">www.wiley-vch.de</a></td>
<td>06/2000</td>
<td>Geheime Schlüssel mit verschrankten Photonen</td>
</tr>
<tr>
<td>Weltwoche, Zurich</td>
<td><a href="http://www.weltwoche.ch">www.weltwoche.ch</a></td>
<td>06/2000</td>
<td></td>
</tr>
<tr>
<td>Science &amp; Vie</td>
<td><a href="http://www.science-et-vie.com/actu2.html">www.science-et-vie.com/actu2.html</a></td>
<td>07/2000</td>
<td>Discrétion absolue ... Entre voisins</td>
</tr>
<tr>
<td>Physics News in 2000 Supplement to APS News</td>
<td>01/2001</td>
<td>Quantum key distribution</td>
<td></td>
</tr>
</tbody>
</table>
Bibliography


[Elm] RCA Optoelectronics/Perkin Elmer. RCA datasheet: CS30901S/CS30921S silicon avalanche photo diode. 90


[Hec89] Eugene Hecht. *Optik*. Addison-Wesley (Deutschland) GmbH, 1989. 83


Bibliography


I Acknowledgements

I.1 Thank You

First I must thank Anton Zeilinger for supervising and supporting me over many years. It has been a special privilege for me to be in his group, as the work is led in a very open and motivating way, allowing me to include my personal ideas in the experiments. Every-day work can be stressfull at times, but the reward of working in the highly interesting and fascinating field more than compensates for this.

Special thanks also go to Gregor Weihs who has guided me through the work of this thesis. Also thanks to the theoreticians Christoph Simon, Caclav Brukner and Terry Rudolph for coping with my naive theory questions. Olaf Nairz is to be thanked for being a great office-mate and friend for all the years. Rupert Ursin and Markus Aspelmeyer are to be thanked for taking over the teleportation experiments now, and realizing the long distance teleportation experiment. I also thank Julia Petschinka for keeping up my moral, Alipasha Vaziri for the great conference journeys, Jian-Wei Pan for also keeping my work on track.

I must thank all the members of the team who have directly advised or helped me with the work, and all the rest of the people for comprising such a pleasant atmosphere that exists in that group.

Also I must thank my family who has supported me in many ways throughout my university career. It was very important to know and feel that my ambitions were backed during all this time.

I wish to thank all of those who know me and who have beard me over all the time.

I.2 Finance

I thank the Austrian state (=tax payers) as well as the European Commission for financially supporting this work via an university position and also via several research projects.
J Curriculum Vitae

Thomas Daniel Jennewein

Personal Data:
Born: 27. December 1971 in Sydney, Australia
Parents: Fritz und Ann Gulielma Jennewein

Chronology:
Dec. 1975: Migration from Sydney, Australia to Seefeld in Tirol, Austria
18. June 1991: Matura
13. October 1997: Diploma Examination: Magister der Naturwissenschaften
Oct. 1997– Jan. 1999: University assistant and PhD student at the Institute of Experimental Physics, University of Innsbruck
Feb. 1999: Migration from Innsbruck to Vienna together with the research group of Prof. Anton Zeilinger
Sept. 1999–Oct. 2000: Compulsory service with the Austrian army, based at the “Stellungskommission Wien”
Feb. 1999–Present: University assistant and PhD student at the Institute of Experimental Physics, University of Vienna, with Prof. Anton Zeilinger

Personal Interests apart from physics:
Making music (singing) and listening to music (concerts, opera)
Electronics
Paragliding, aeroplanes, flying in general