Experimental Investigation of Quantum Communication Protocols in Higher Dimensions

Diplomarbeit zur Erlangung des akademischen Grades
Magister der Naturwissenschaften

eingereicht von
Simon Gröblacher
Institut für Experimentalphysik
der Universität Wien

durchgeführt bei
O. Univ. Prof. Dr. Anton Zeilinger

November 2005

Gefördert vom **Fonds zur Förderung der wissenschaftlichen Forschung**, Projekt SFB F1506.

Contents

1. Introduction

The wish to protect information from unauthorized listeners has driven humans from early mankind to invent all sorts of cryptographic schemes and encryption algorithms. The modern computer age has made the security need as important and the difficulty of breaking classical algorithm based cryptography as easy as never. In the last decades of the 20th century S. Wiesner, H. Bennett, G. Brassard and A. Ekert [73, 12, 13, 32] proposed cryptography schemes which security relies on the laws of quantum mechanics. An intruder trying to listen in will always be detected. Because these schemes establish identical secret keys in two remote locations they have since become known under the term Quantum Key Distribution (QKD). QKD has been experimentally performed using all sorts of systems, applying various protocols, over distances of up to 120 km [41, 63, 61, 42]. These experiments are performed in the lab as well as in real-life environments, such as the nightly sky of a metropolitan city [55, 47]. Even a secure bank transfer has been performed [53] and commercial plug-and-play systems are already available, which underlines the need and usefulness of QKD systems.
All experiments performed so far were based on two-dimensional quantum systems (qubits). However, the usage of higher-dimensional systems offers advantages such as an increased allowance of noise in order to keep the key distribution secure and an increased information content of each system. In this thesis we will investigate higher-dimensional systems, in particular qutrits, encoded in the orbital angular momentum of photons. Two different types of QKD protocols are considered, namely the BB84 and the Ekert protocol. An approach using computer generated phase holograms to control the orbital angular momentum is discussed and numerical simulations are performed. Finally a quantum key distribution experiment is performed, where two separate keys are produced using a modified Ekert scheme.

2. Theoretical Aspects

2.1. Concepts of Quantum Information

The unit of information, the *bit*, is a concept that has become a part of everyday life. It is the fundamental unit of classical information. Almost all modern applications like computers, digital music, etc. work with bits of information. Such a bit can either have the value 0 or 1 and with a string of bits, like a byte (which is 8 bits), any information can be encoded. In quantum theory the basic unit of information is called a qubit (quantum bit). Any kind of two-level quantum system is a qubit. In contrast to the classical bit a qubit has no definite value but rather is a superposition of two values, i.e.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

where the $|\psi\rangle$, $|0\rangle$ and $|1\rangle$ are ket-vectors in a two-dimensional complex vector-space, Hilbert space $\mathcal{H}^2$. α and β are the respective complex amplitudes of $|0\rangle$ and $|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$. It is important to note, that in (2.1) $|0\rangle$ and $|1\rangle$ are orthogonal states, just like the two classical states of a bit 0 and 1 are mutually exclusive, i.e. their inner product[1] is $\langle 0|1\rangle = 0$. They span a complete orthonormal (they are normalized and orthogonal one to another) basis $\mathfrak{A}$ on the two-dimensional Hilbert space. The same state can be written in any different complete orthonormal basis. A state $|\psi\rangle$, that can be represented by a sum of basis vectors, like (2.1) is called a pure state. If such a description is not possible and the state is a statistical mixture of pure states, then it is called a mixed state.
A measurement on a quantum state is represented by an operator $\hat{A}$ on the same Hilbert space. Such an operator can be expanded by its eigenstates, e.g. $|0\rangle$ and $|1\rangle$. If a measurement is performed, the state is projected according to its amplitudes[2] α and β, e.g.

$$\hat{A}|\psi\rangle = |1\rangle\langle 1|\psi\rangle = \beta|1\rangle. \tag{2.2}$$

After a measurement has been performed the initial state remains in the projected state, with an updated amplitude (in the above case $\beta = 1$). Every measurement "disturbs"

[1] $\langle . | . \rangle$ is the inner product of a ket-vector $| . \rangle$ with a vector from its dual space, the bra-vector $\langle . |$ ($\langle . |^\dagger = | . \rangle$). It gives the overlap between the two vectors and is 0 if they are not overlapping, i.e. orthogonal, and 1 if they are equal.

[2] The absolute squares of the amplitudes α and β determine the probability of finding the system in state $|0\rangle$ or $|1\rangle$, respectively. In quantum theory this randomness is a fundamental feature of the theory.

the system and changes the amplitudes of the eigenstates, e.g. the measurement $\hat{B}$ in a different basis $\mathfrak{B}$, with $|\pm\rangle = \frac{1}{\sqrt{2}}\left[\,|0\rangle \pm |1\rangle\,\right] \in \mathfrak{B}$, would be:

$$\hat{B}|\psi\rangle = |+\rangle\langle+|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle. \tag{2.3}$$

Note, if $\alpha = \beta = \frac{1}{\sqrt{2}}$ the probability of measuring $|+\rangle$ is equal to 1. Further, $\mathfrak{A}$ and $\mathfrak{B}$ are said to be mutually conjugated[3], as the inner product of any of their basis vectors is $\langle 0|+\rangle = \frac{1}{\sqrt{2}}$.

The generalization of superposition to larger systems is entanglement [59]. Generally any quantum system with several degrees of freedom (e.g. multi-particles[4]) can be entangled. The best known example is a maximally entangled two particle system:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left[\,|0\rangle_1 \otimes |1\rangle_2 - |1\rangle_1 \otimes |0\rangle_2\,\right], \tag{2.4}$$

where the states with subscript 1 are system 1 and subscript 2 stands for system 2. The important difference to a non-entangled state is, that the states of two systems cannot be factorized. Hence, it is not possible to ascribe any state-vector to the individual systems, but only to the joint system — nothing can be said about one of the subsystems of a maximally entangled state, only about both jointly. Entanglement implies that the two systems, if measured, are always perfectly correlated, i.e. if system 1 is measured and projected on state $|0\rangle$, then system 2 is projected into state $|1\rangle$ and viceversa. In principle there is no limitations on the entanglement, i.e. two entangled systems can be arbitrarily spatially and temporarily separated. Entanglement has been demonstrated in many experiments and so far no deviations from quantum mechanical predictions have been observed [4, 71, 6]. State (2.4) is one of the so-called Bell states, which are defined as the four maximally entangled qubit states:

$$\begin{aligned}
|\psi^-\rangle &= \frac{1}{\sqrt{2}}\left[\,|0\rangle_1 \otimes |1\rangle_2 - |1\rangle_1 \otimes |0\rangle_2\,\right], \\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}\left[\,|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2\,\right], \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}\left[\,|0\rangle_1 \otimes |0\rangle_2 - |1\rangle_1 \otimes |1\rangle_2\,\right], \\
|\phi^+\rangle &= \frac{1}{\sqrt{2}}\left[\,|0\rangle_1 \otimes |0\rangle_2 + |1\rangle_1 \otimes |1\rangle_2\,\right].
\end{aligned} \tag{2.5}$$

[3] They are also called mutually unbiased bases (MUBs). For a general d-dimensional Hilbert space $\mathcal{H}^d$ the condition for MUB bases is $\langle\varphi_n|\psi_m\rangle = \frac{1}{\sqrt{d}}$.

[4] We will now talk about particles instead of system, without any loss of generality, as it is a more illustrative concept.

In contrast to the ideal Bell states there are non-maximally entangled Bell states, where the amplitudes are not uniform, i.e.

$$|\psi\rangle = \frac{1}{\sqrt{1+\gamma^2}} \left[|0\rangle_1 \otimes |1\rangle_2 + \gamma e^{i\varphi} |1\rangle_1 \otimes |0\rangle_2 \right]. \tag{2.6}$$

It is easy to see, that $\gamma = 1$ recovers the four Bell states and $\gamma = 0$ is a completely separable state and therefore not entangled.
Two measurements $\hat{A}$ and $\hat{B}$ are said to be non-commuting if their commutator does not vanish, i.e.

$$[\hat{A}, \hat{B}] = \hat{A} \cdot \hat{B} - \hat{B} \cdot \hat{A} \neq 0 \tag{2.7}$$

Any non-commuting measurements (or observables) cannot be measured simultaneously with arbitrary precision. For example, the observables momentum $\hat{P}$ and position $\hat{X}$ do not commute and therefore the momentum and the position of a particle can only be determined at the same time up to a lower bound, which is the so-called Heisenberg uncertainty principle, given by

$$\Delta\hat{P} \cdot \Delta\hat{X} \geq \frac{\hbar}{2}. \tag{2.8}$$

The uncertainty $\Delta\hat{A}$ of an observable $\hat{A}$ is defined as

$$\left(\Delta\hat{A}\right)^2 = \langle\hat{A}^2\rangle - \langle\hat{A}\rangle^2, \tag{2.9}$$

where $\langle\,.\,\rangle = \langle\psi|\,.\,|\psi\rangle$ is the operator mean for state $|\psi\rangle$. Here $\hbar$ is the Planck constant[5] h divided by 2π.

2.1.1. The No-Cloning Theorem

In 1982 W. K. Wootters and W. H. Zurek [75] pointed out, that an arbitrary quantum state, due to the linearity of quantum theory, could not be cloned. That means, that no perfect copy of a quantum state can be made, without destroying the original state. This stands in contrast to the classical intuition, where an arbitrary (and even unknown) state can be copied as many times as necessary. If $|\psi\rangle_i$ is the original state, $|\beta\rangle_c$ the blank state (like a blank sheet of paper, on which the copy will be made) and an operator $\hat{C}$ that is the quantum copy machine, then, making a copy of $|\psi\rangle_i$ means

$$\hat{C}\left(|\psi\rangle_i \otimes |\beta\rangle_c\right) = |\psi\rangle_i \otimes |\psi\rangle_c. \tag{2.10}$$

For the special cases, where $|\psi\rangle_i$ is in state (2.1), with amplitudes $\alpha = 1, \beta = 0$ and $\alpha = 0, \beta = 1$, the copy machine has to give the following results:

$$\begin{aligned} \hat{C}\left(|0\rangle_i \otimes |\beta\rangle_c\right) &= |0\rangle_i \otimes |0\rangle_c, \\ \hat{C}\left(|1\rangle_i \otimes |\beta\rangle_c\right) &= |1\rangle_i \otimes |1\rangle_c. \end{aligned} \tag{2.11}$$

[5] $h = 6.626 \cdot 10^{-34}$ J·s

If $|\psi\rangle_i$ now is a general superposition, where α and β are unknown, then a copy process yields

$$\begin{aligned}\hat{C}\left(|\psi\rangle_i \otimes |\beta\rangle_c\right) &= \hat{C}\left[(\alpha|0\rangle_i + \beta|1\rangle_i) \otimes |\beta\rangle_c\right] \\ &= \alpha|0\rangle_i \otimes |0\rangle_c + \beta|1\rangle_i \otimes |1\rangle_c, \end{aligned} \tag{2.12}$$

where we used (2.11). This result stands in contrast to the desired result of a perfect copy scheme:

$$\begin{aligned}\hat{C}\left(|\psi\rangle_i \otimes |\beta\rangle_c\right) &= |\psi\rangle_i \otimes |\psi\rangle_c \\ &= (\alpha|0\rangle_i + \beta|1\rangle_i) \otimes (\alpha|0\rangle_c + \beta|1\rangle_c) \\ &= \alpha^2|0\rangle_i \otimes |0\rangle_c + \alpha\beta|0\rangle_i \otimes |1\rangle_c + \beta\alpha|1\rangle_i \otimes |0\rangle_c + \beta^2|1\rangle_i \otimes |1\rangle_c. \end{aligned} \tag{2.13}$$

It is thus impossible to find a universal quantum copy machine $\hat{C}$, that makes a perfect copy of any arbitrary, unknown quantum state. However, imperfect copies are very well possible (for optimal cloning devices see [60, 72]). The no-cloning theorem is vital to the security of any quantum key distribution protocol, as will be shown in chapter 3.4.

2.2. Local Realism in Quantum Theory

In their famous 1935 *Gedankenexperiment* Einstein, Podolsky and Rosen (EPR) [31], based on the above concepts, argued that quantum theory could not give a complete description of physical reality. That is because the wave-function does not tell us with probability 1 the particle's position if we measure it. Einstein especially disliked this randomness as a basic principle of quantum mechanics and once said *"Gott würfelt nicht!"*[6]. In the following years a vivid discussion between Einstein, Bohr and many others arose. Some years later, attempts were made to "complete" quantum theory. People were looking for a deeper theory underlying quantum mechanics, which would explain the seemingly randomness by parameters in the new theory, which are not included in quantum theory (therefore they are normally called *hidden* parameters) and only appear as probability distributions [15, 16]. On the other hand various arguments were found trying to prove the EPR argument wrong [17, 69, 59]. Despite a lot of arguing neither side could objectively decide the dispute. Not until 1964, when John Bell discovered his famous Bell inequality [10]. Bell found an inequality that would be violated by quantum mechanical predictions for certain measurements, while satisfied by all local realistic theories that were mostly envisioned for a completion of quantum theory by EPR. Here locality is the impossibility of action between space-like separated regions, while realism in the words of EPR is "*If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity.*".

[6] "God does not play dice!"

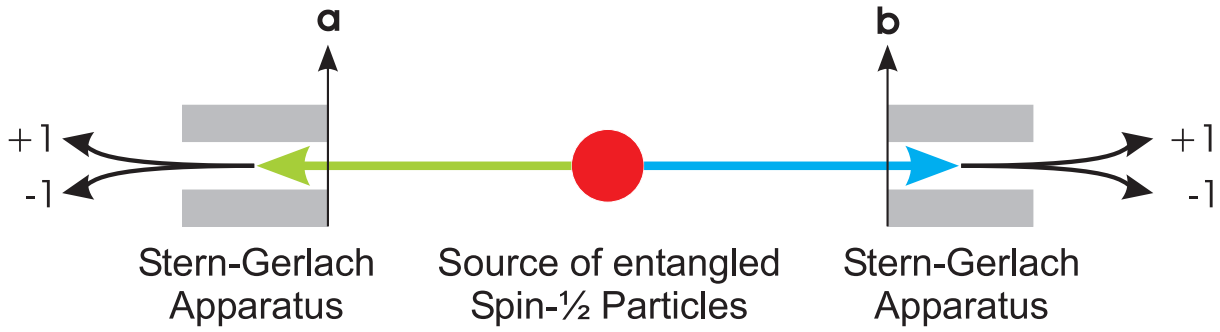


Figure 2.1.: *Schematic representation of a source used for testing a CHSH inequality. A pair of entangled spin-1/2 particles is emitted and their spins are measured in Stern-Gerlach apparatuses — inhomogeneous magnetic fields, in which particles with different spins are deflected in different directions. The measurement settings $\vec{a}_1, \vec{a}_2$ and $\vec{b}_1, \vec{b}_2$ are denoted as* ***a*** *and* ***b****, respectively. For spin-1/2 particles, the settings correspond to different orientations of the magnetic fields in the Stern-Gerlach apparatus. This case is in complete analogy to photons entangled in their polarization, where the analyzers are polarizers.*

In its more refined version of Clauser, Horne, Shimony and Holt (CHSH) [26] the derivation of the Bell inequality is as follows: a pair of entangled particles propagates towards two space-like separated labs, operated by observers A and B (throughout this thesis A will be a female observer, while B is male). Each of them can set her/his apparatus freely to one of two states, which are described by vectors $\vec{a}_1, \vec{a}_2$ and $\vec{b}_1, \vec{b}_2$, respectively for A and B. The results of these measurements are dichotomic, e.g. horizontal or vertical polarization for photons or spin up or down for spin-1/2 particles. To each result a unique value is assigned, being either $+1$ or -1.
In any local realistic theory describing the possible measurement outcomes for A and B and their correlations, realism implies that the dichotomic results obtained by A, $A(\vec{a}_k, \lambda) = \pm 1$, and B, $B(\vec{b}_l, \lambda) = \pm 1$, are defined prior to and independent of the measurement. Here λ is a set of hidden-variables, which can be any kind of number, function or operator. In addition, locality is the assumption that the results do not depend on parameters in a space-like separated region, i.e. each measurement is a function of the setting of the local measurement apparatus and the hidden-variables only.
The following algebraic identity holds for any dichotomic numbers (e.g. measurement results) [52, 76]:

$$A_1[B_1 + B_2] + A_2[B_1 - B_2] = \pm 2. \tag{2.14}$$

In an experiment the values of these four products cannot be directly compared as it is generally impossible to acquire them in a single run of an experiment. What can be experimentally tested is the average over the whole ensemble of emitted systems, i.e. the

average over several equally prepared experimental runs. The average of the product of measurement results, the correlation function, in a local hidden-variable theory is given by

$$E_{kl} = \int d\lambda \rho(\lambda) A(\vec{a}_k, \lambda) B(\vec{b}_l, \lambda), \tag{2.15}$$

where $\rho(\lambda)$ is the probability distribution of the hidden-variables. We can write the product of the outcomes under the integral because they are local and therefore separable, i.e. they only depend on the settings of the local measurement apparatus. Since identity (2.14) has to hold, a bound for all local realistic theories can be found:

$$S^{\text{Bell}} = E_{11} + E_{12} + E_{21} - E_{22} \leq 2. \tag{2.16}$$

This is the Clauser-Horne-Shimony-Holt inequality [26, 25], where S^{Bell} is the so-called Bell parameter.
The experimental correlation function E_{kl} is given by

$$\begin{aligned} E_{kl}^{\text{exp}} &= \langle A_k \cdot B_l \rangle = \sum A_k \cdot B_l \cdot P_{A_k B_l} = \\ &= (+1)(+1) \cdot P_{++} + (+1)(-1) \cdot P_{+-} + (-1)(+1) \cdot P_{-+} + (-1)(-1) \cdot P_{--} = \\ &= P_{++} + P_{--} - P_{+-} - P_{-+}, \end{aligned} \tag{2.17}$$

with $P_{A_k B_l}$ being the probability of obtaining the measurement results A_k and B_l. The quantum mechanical expectation value for particles with spin 1 (like photons) is

$$E_{kl}^{\text{QM}} = -\cos(a_k - b_l). \tag{2.18}$$

For the rotational invariant state (2.4) the experimental expectation values are $E_{kl}^{\text{exp}} = E_{kl}^{\text{QM}} \cdot V$, where V is the so called visibility, which is defined as

$$V = \frac{max - min}{max + min}, \tag{2.19}$$

where max are the perfectly correlated and min the measurements with no correlations at all. V is a measure for the perfect correlations, i.e. ideally for an entangled state all measurements are perfectly correlated but in a real-life experiment errors occur and therefore degrade the correlations. Due to $V < 1$ in any experimental setup, it is not possible to achieve maximal violation of inequality (2.16), which is predicted by quantum theory as $S_{max}^{\text{Bell}} = 2\sqrt{2}$ for $|\psi^-\rangle$. Consequently, no violation at all can be observed for $V < \frac{1}{\sqrt{2}} \approx 0.707$. Violations of this bound have been observed in all kinds of experiments [35, 36, 5, 4, 71, 57] and hence exclude the possibility of a local realistic extension of quantum theory.

2.3. Higher-dimensional Quantum Systems

Up to now we have only considered two-dimensional quantum systems. Qubits have the advantage that they are easy to realize in an experiment, like the polarization of photons or a two-level atom, and are mostly robust to external noise. Such low-dimensional systems have been widely used in all sorts of quantum applications, like quantum key distribution (QKD) (see Chapter 3), quantum teleportation [19], quantum computation [70] and many more. However, there are no fundamental reasons why these applications should only exploit qubits. At the moment it is only a matter of liability and simplicity why qubits are used in the vast majority of quantum experiments.
Higher-dimensional photonic quantum systems, i.e. systems with properties with more than two eigenstates, can be realized in many different ways, like bi-photons, higher-order parametric down-conversion and energy-time entanglement [49, 28, 68, 64]. They offer a variety of advantages and new possibilities in contrast to two-dimensional systems. E.g. the Byzantine agreement problem [33] and quantum coin tossing [50] are not feasible with qubit systems. In addition quantum computation complexity protocols become more efficient [20] and the security of QKD is increased.
The lowest higher-dimensional quantum systems are qutrits (trit for three-dimensional). The most general state of such a quantum system is

$$|\psi\rangle = a\, e^{i\phi_0}|0\rangle + b\, e^{i\phi_1}|1\rangle + c\, e^{i\phi_2}|2\rangle, \tag{2.20}$$

where the amplitudes, in analogy to (2.1), satisfy $|a|^2 + |b|^2 + |c|^2 = 1$. The general two particle qutrit state then is

$$|\psi\rangle = \alpha e^{i\varphi_0}|0\rangle \otimes |0\rangle + \beta e^{i\varphi_1}|1\rangle \otimes |1\rangle + \gamma e^{i\varphi_2}|2\rangle \otimes |2\rangle. \tag{2.21}$$

A simple, maximally entangled qutrit state can be obtained with $\alpha = \beta = \gamma = \frac{1}{\sqrt{3}}$ and $\varphi_0 = \varphi_1 = \varphi_2 = 0$. The generalization of the 4 qubit Bell-states (2.5) to qutrits gives

$$|\psi\rangle^{\text{Bell}} = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} e^{\frac{2\pi i}{3}kn}|k\rangle \otimes |k+m\rangle, \tag{2.22}$$

with $0 \leq m, n \leq 2$. Consequently there are nine qutrit Bell states. Such maximally entangled states also violate a Bell-type inequality and hence local realism. In the next section a three-dimensional Bell inequality will be briefly derived.

2.3.1. Three-dimensional Bell inequality

Similar to the derivation of inequality (2.16), Bell inequalities for two qutrits can be derived [27, 45]. Imagine therefore, observers A and B are sharing pairs of entangled particles. Each observer can perform two measurements, i.e. a_1,a_2 and b_1,b_2. In contrast to the CHSH inequality the possible outcomes are not dichotomic but can rather have

any integer value between 0 and $d-1$, where for our three-dimensional case $d=3$. Note that the assignment of values to the outcomes is an arbitrary choice. We will denote the probability for a measurement a_1 yielding the outcome j, a_2 outcome k, b_1 outcome l and b_2 outcome m as c_{jklm}, with $j,k,l,m = 0,\ldots,d-1$. For any local realistic theory there are d^4 such probabilities completely determining all possible outcomes. c_{jklm} has to be positive, i.e. $c_{jklm} \geq 0$, and normalized, $\sum_{jklm} c_{jklm} = 1$. Hence, the probabilities for the four combinations of joint measurements of A and B are

$$\begin{aligned} P(a_1 = j, b_1 = l) &= \sum_{km} c_{jklm}, \\ P(a_2 = k, b_1 = l) &= \sum_{jm} c_{jklm}, \\ P(a_1 = j, b_2 = m) &= \sum_{kl} c_{jklm}, \\ P(a_2 = k, b_2 = m) &= \sum_{jl} c_{jklm}. \end{aligned} \tag{2.23}$$

For the local variables $jklm$ we now introduce new variables, that we define as

$$\begin{aligned} r' &:= b_1 - a_1 = l - j, \\ s' &:= a_2 - b_1 = k - l, \\ t' &:= b_2 - a_2 = m - k, \\ u' &:= a_1 - b_2 = j - m. \end{aligned} \tag{2.24}$$

Note that in a local hidden variable theory, if we freely choose r', s' and t' then u' is fixed, since $r' + s' + t' + u' = 0$. This restriction can be used to find bounds on local realistic theories and hence Bell-type inequalities for arbitrary dimensions d. For our case of $d = 3$, the simplest such inequality is

$$\begin{aligned} S_3 = P(a_1 = b_1) + P(a_2 = b_1 - 1) + P(a_2 = b_2) + P(a_1 = b_2) - \\ -P(a_1 = b_1 - 1) - P(a_2 = b_1) - P(a_2 = b_2 - 1) - P(a_1 = b_2 + 1) \leq 2, \end{aligned} \tag{2.25}$$

with

$$P(a_a = b_b + \eta) = \sum_{\eta=1}^{3} P(a_a = \eta, b_b = (\eta + \kappa) \bmod 3) \tag{2.26}$$

being the probabilities that the outcomes of observers A and B measuring a_a and b_b differ by κ (modulo 3). For a detailed derivation see [27]. Note, that the local realistic bound for inequality (2.25) is the same as for the standard CHSH inequality (2.16) and

for qubits it is equivalent to the CHSH inequality. The maximal violation for the nine maximally entangled states (2.22) is $S_3^{\max} = 4/(6\sqrt{3} - 9) \approx 2.873$, which is slightly higher than the maximal violation for the qubit case. This inequality has already been tested experimentally and a clear violation of local realism has been found [68]. It is interesting to note, that in contrast to the standard CHSH inequality, certain non-maximally entangled qutrit states show a stronger violation of inequality (2.25) than any maximally entangled state. Namely, states of the form

$$|\psi\rangle^{\text{non-max}} = \frac{1}{\sqrt{n}} \left(|0\rangle \otimes |0\rangle + \gamma|1\rangle \otimes |1\rangle + |2\rangle \otimes |2\rangle\right), \tag{2.27}$$

with $\gamma = (\sqrt{11} - \sqrt{3})/2$ and $n = 2 + \gamma^2$, yield $S_3^{\text{non-max}} = 1 + \sqrt{11/3} \approx 2.915$ [1], which implies that this is not the optimal qutrit inequality.
The violation of a Bell-type inequality requires a certain visibility of the correlations (2.19), which for the CHSH is around 71 %. For the three-dimensional inequality presented above, the noise level can be somewhat higher, i.e. the correlations are more robust to noise. The minimal required visibility for a violation is $V = (6\sqrt{3} - 9)/2 \approx 0.696$ [27].

3. Quantum Key Distribution

3.1. Classical Cryptography

For many applications and reasons information has to be shared between two (or more) parties over more or less private channels and has to be kept secret from anyone else. Therefore the information has to be encrypted, such that the message, without knowing the decryption procedure, is useless.
In classical cryptography the simplest way is to take a message and replace each of the letters with a different sign. More advanced procedures use various numerical operations on the original message which are only known to legitimate partners. If two parties want to communicate in a secure way they have to share such a key to encrypt and decrypt messages. The security of the communication depends on the difficulty of breaking the key, i.e. how long it takes to compute at least part of the key. The best strategy is to use a totally random key, which, combined with the so called one-time-pad (or Vernam Cipher), ensures perfect security. The one-time-pad is a key that is used only once to encrypt a message and therefore is absolutely secure. As soon as it is used more often it is relatively easy to break the key. Thus the main problem in classical cryptography is the sharing of a secret key, which can be done by all sorts of means but ultimately always compromises the security of the scheme.
A different cryptographical approach is the so called public key cipher. Each party wanting to share a secret message announces an encrypter $\mathcal{E}$ (an encryption function) publicly. The particular feature of $\mathcal{E}$ is that its inverse function $\mathcal{D} = \mathcal{E}^{-1}$ (the decrypter) cannot be computed from $\mathcal{E}$ in polynomial time, i.e. it is extremely difficult to deduce $\mathcal{D}$ from $\mathcal{E}$. The second party who wants to share a secret message with the first now only has to take $\mathcal{E}$, encrypt the message and send it to the first party. One of the most widely used algorithms of this kind is the RSA [56] algorithm. The advantage of this scheme is that the two parties do not have to meet frequently as in the classical cryptography and further the parties can authenticate their messages (see [40] for a more detailed introduction to cryptography).
It is believed that breaking such a cipher is equivalent to the factorization of a large prime number, which is a very difficult task even for modern computers. But with the fast progress made in developing and building a quantum computer the factorization problems seem not unsolvable. Quantum computers are supposed to exponentially increase the factorization speed and therefore make it possible to break current cryptography schemes in a relatively short amount of time. If the fundamental and technological

difficulties of building a quantum computer are ever overcome, the time needed in order to break an encryption algorithm would decrease dramatically, as the necessary computing time would only be a polynomial function of the length of the key instead of an exponential. Therefore contemporary RSA cryptography would become useless and sensitive data would be available to anyone with access to a quantum computer.
The almost perfect cryptography scheme, even unbreakable with quantum computers, is a completely random one-time pad. The problem to produce such a key is the randomness, which is not a trivial issue as would naively be expected, and the distribution of the key between the two legitimate partners who want to exchange encrypted messages. In classical cryptography the key distribution is the part with the highest security risk. Quantum Cryptography (QC), or rather Quantum Key Distribution (QKD), is a scheme that allows the production of a secure key that can be used as a one-time pad. The basic ideas of the cryptography are the same as in classical cryptography only that QKD inherently provides a secure way of sharing a secret key and also solves the randomness problem. The security of QKD is based on fundamental laws of quantum mechanics and is therefore in principle secure. In this chapter the basic ideas of QKD will be presented. Different protocols and applications can be found in sections 3.2 and 3.3.
In the last decades of the 20th century S. Wiesner, H. Bennett, G. Brassard and A. Ekert [73, 12, 13, 32] proposed cryptography schemes where security relies on the fact that every measurement alters the system and therefore any unwanted measurement can be detected. Many different protocols were subsequently proposed, exploiting different additional features of quantum theory. The basic idea for all schemes is the same — two observers exchange a key by sending quantum particles to each other, which they then measure. Only the measurement projects them into a definite state (with a probability of up to unity, depending on the protocol) and results in the desired correlations. Any manipulation, i.e. the attempt of eavesdropping, results in errors and is therefore detectable. However different the various protocols are, they all provide a raw key, which has to be further processed. First the measurement bases have to be compared (this is the so called basis reconciliation), which leads to the sifted key. Additionally classical procedures are implemented to perform error correction and privacy amplification. In the following the two main schemes will be presented and some advantages and disadvantages will be discussed.

3.2. The BB84 Protocol

The BB84 Protocol was originally conceived by Charles Bennett and Gilles Brassard in 1984 [12]. In its original version an observer A sends single particles to an observer B. The particles are produced in four different states, two in each of two mutually conjugate bases. The states of the same basis are orthogonal to each other, e.g. for polarization states of photons the four states could be horizontal (H), vertical (V), $+45$ and -45 polarization. A randomly (and with equal probability) chooses between the states she

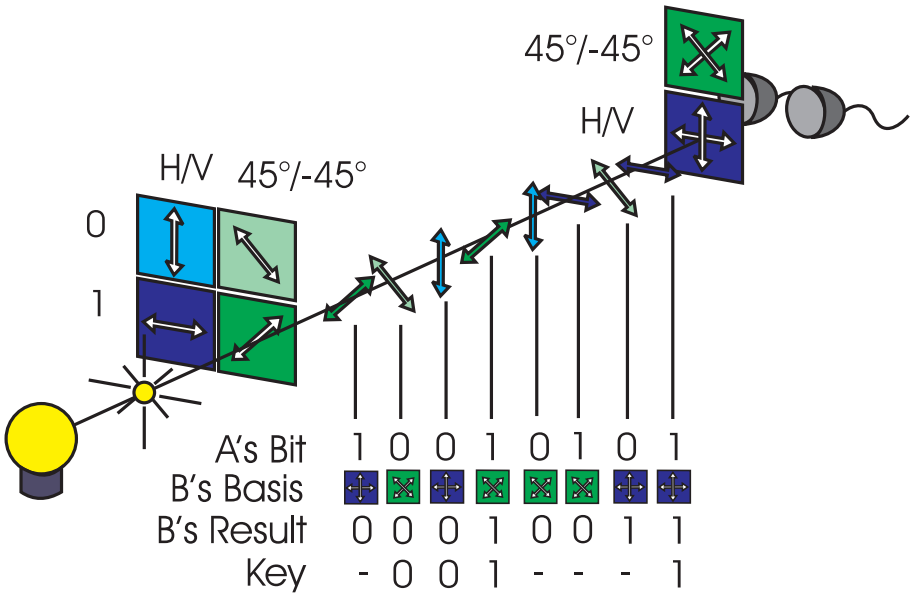


Figure 3.1.: The BB84 protocol with qubits encoded in the polarization states of photons. Observer A sends single photons to observer B. The choice of the polarization state, i.e. one of the four states ± 45 or H/V, she sends is completely random. If B then measures the photon in the right basis he gets outcomes perfectly correlated to A's preparation. However, if he chooses the wrong basis, the outcome result is random. (by Hannes R. Böhm)

sends to B. B measures the particles, switching between the two measurement bases at random. For B measuring in the same basis as the particle was sent, observer A knows the result of B's measurement. Therefore, both announce in which bases he/she measured (typically this is done after a few measurement runs or even after each run), which can be performed over a classical public channel, as it does not contain any information on the result itself. They compare the bases and hence know which of the results to keep. The results of the measurements in which B does not choose the preparation basis of the particle are completely random, as the bases are mutually conjugated. This is also the feature why an eavesdropper E (someone who is not authorized to but tries to gain some knowledge of the exchanged key) is not able to measure the particle before B receives it and to resend a copy (due to the obtained result) without introducing detectable errors. In that way, A and B produce a key, that is random (due to the randomness of the preparation of the initial states sent to B) and secure, as an intrusion can be easily detected by comparing a small set of the keys and checking whether they are, up to a maximal error rate, equal. In the BB84 protocol the error rate in the key is taken as a security prove. In addition, for the qubit case there is a one-to-one correspondence between the violation of the CHSH inequality, the mutual information and the maximally

allowed noise limit [40].
In practice it is difficult to produce real single particle states needed for the protocol (see 3.4), which is normally realized with faint laser pulses [11, 51, 22]. It is therefore convenient to take entangled states, where only the particles of the entangled pair and no third particle is correlated. E.g. one of the maximally entangled Bell states (2.5) is produced and one of the particles is distributed to observer A and the other to B. The two observers measure randomly in one of the two bases and if they measure in the same, they always have perfect (anti-) correlations, just as in the original BB84 protocol. Such variations of the original BB84 scheme have been experimentally demonstrated and thereto entanglement in many different degrees of freedom has been exploited, e.g. the polarization of photons and energy-time correlations of photons [53, 65].

3.3. The Ekert Protocol

In 1991 Artur Ekert proposed a novel QKD scheme based on entangled particles and a Bell inequality [32]. The observers A and B share an entangled pair of particles and perform measurements with at least three analyzer settings each. The settings which are the same for both are used for key production and the other are chosen such, that they violate a Bell's inequality. The inequality is only maximally violated if no eavesdropper tried to acquire some information on the QKD, as this would degrade the entanglement of the particles. Hence, this is used to test the security of the protocol.
For a pair of polarization entangled photons in state (2.4), where $|0\rangle$ is horizontal (H) polarization and $|1\rangle$ vertical (V), observer A randomly chooses between the polarizer settings $a_1 = 0$, $a_2 = \frac{\pi}{8}$ and $a_3 = \frac{\pi}{4}$, whereas B between $b_1 = \frac{\pi}{8}$, $b_2 = \frac{\pi}{4}$ and $b_3 = \frac{3\pi}{8}$ (see Fig. 3.2). If they measure the combinations $\{a_2, b_1\}$ or $\{a_3, b_2\}$ they obtain perfectly correlated results and hence produce a key. With the other combinations of settings they can look for a violation of the CHSH inequality and hence check for any unwanted intrusion in their QKD protocol.

3.4. Security of QKD

The simplest attack on a QKD protocol an eavesdropper E could make, is to measure B's particle and resend, in a state based on the measurement result, another particle to B. If E measures the particle in the same basis as A will (or prepared the state in), A and B cannot detect the intrusion. However, if E gets the basis wrong, she introduces detectable errors. For 75 % knowledge of the key she introduces a qubit error rate (QBER) of 25 %. Here two fundamental features of QKD guarantee the security of the protocol — the randomness of the measurement result (or equally the random state preparation of A), wherefore E has only a probability of $\frac{1}{2}$ to guess the right basis, and the no-cloning theorem. Latter ensures the impossibility of E perfectly copying the

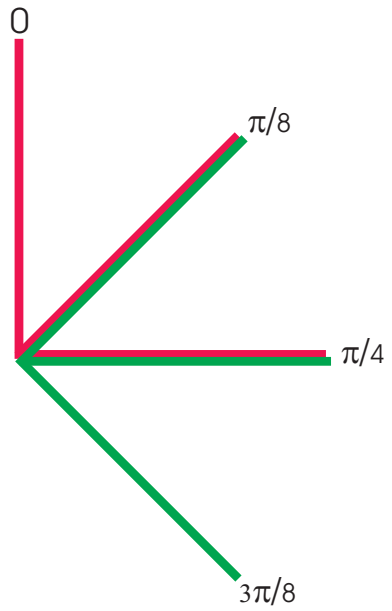


Figure 3.2.: *Polarizer settings for an entangled photon Ekert scheme. The red lines are the angles of the polarizer for observer A and the green for observer B. The overlapping settings are used for key production and the rest are to check the security of the protocol via the violation of the CHSH inequality.*

particle and resending the original to B and to measure the copy after B announces the basis of his measurement.
A different approach for E would be to imperfectly copy the state of the particle that is sent to B, wait until B reveals his measurement basis and only then measure her copy. For any qubit scheme this is the optimal way for E to gain at least some information on the key [37].
For any such attack, the protocol is still secure as long as the mutual information of A and B is greater than the mutual information of A and E (or B and E). The upper bound of the possible mutual information of an eavesdropper with one of the observers is proportional to the noise rate of the protocol, as E introduces more errors the more she interferes to gain information. Therefore an upper noise bound for a secure key distribution can be found (see Figure 3.3). For the qubit BB84 and the qubit Ekert scheme this bound is 14.64 % [37]. With modified protocols this upper limit can be slightly increased [21]. For these different schemes and different types of eavesdropping attacks, like a coherent attack, where E does not measure individual qubits but rather several coherently, the noise limit varies [24]. For a review on eavesdropping strategies and QKD in general see [40].

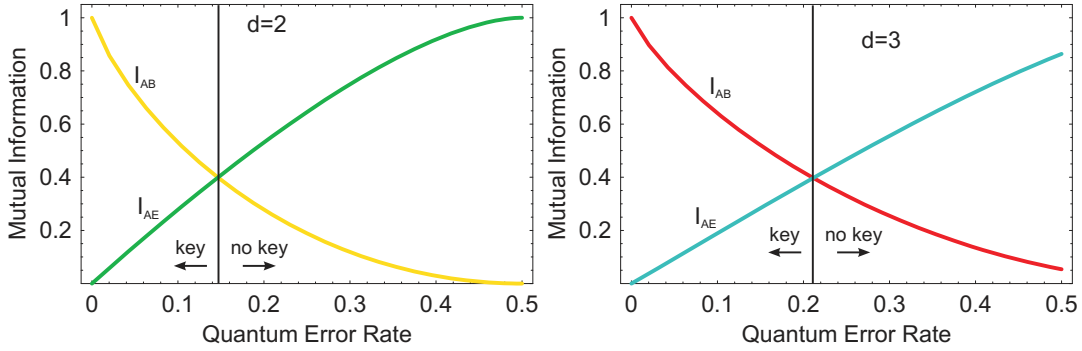


Figure 3.3.: *The left picture shows the normalized mutual information I_{AB} between observers A and B (yellow line) and I_{AE} for A and E (green line) as a function of the quantum error rate for a two bases qubit BB84 protocol. The point where the two curves intersect is the upper bound for the error rate for a secure protocol, which is around 0.1464. The right picture shows the same for a qutrit BB84 protocol, where the upper noise bound is 0.2113. Here I_{AB} is the red line, while I_{AE} is turquoise.*

3.5. QKD with Qutrits

Quantum key distribution has been proven to be a very useful and reliable technique of key generation for the encryption of sensitive data. As discussed previously in this chapter, there are various different protocols which all rely on similar features of quantum theory. Up to date all QKD schemes were based on qubits. However, higher-dimensional systems offer various advantages [18, 7], such as an increased level of tolerance to noise at a given level of security and a higher flux of information compared to the qubit cryptography schemes. It is easy to see, that each generated key contains more information than a key in a qubit scheme, as a higher alphabet is used. The information flux increases with the order of dimension of the system. For binary systems one needs 8 bits (1 byte) to encode the standard ASCII characters, whereas using trinary systems 5.048 trits are sufficient. Further, it was theoretically shown, that the qutrit QKD protocols allow for a higher noise rate and still be considered secure [24, 29]. E.g. the upper noise bound for a qutrit Ekert protocol in order to still ensure a secure key generation is approximately 22.47 %. For a three-dimensional BB84 protocol the noise can be as high as 21.13 % or even 22.67 % if the observers use a four bases protocol (see Table 3.1).

3.5.1. Three-dimensional BB84 and Ekert protocols

The extension of both, the BB84 and the Ekert qubit protocols to three-dimensional quantum systems is relatively simple. For the BB84 the only difference is, that the outcomes are no longer dichotomic but rather trichotomic. In its simplest form it still

d	$D_2^{BB84}[\%]$	$D_{d+1}^{BB84}[\%]$	$D^{Ekert}[\%]$
2	14.64	15.64	14.64
3	21.13	22.67	22.47
4	25	26.66	26.58
5	27.64	29.23	29.2
8	32.32	33.44	33.43

Table 3.1.: *Maximal error rates for different protocols and dimensions — D_2^{BB84} is the BB84 protocol with two mutually unbiased bases and D_{d+1}^{BB84} with $d+1$ MUBs. D^{Ekert} denotes the maximal allowed error rate for Ekert protocols in d dimensions. This clearly shows that the higher-dimensional the quantum key distribution scheme, the more secure it is.* [24, 30]

uses two mutually unbiased bases. As mentioned in the previous section, the security increases with the number of MUB bases, just like the noise resistance in the six-state protocol [21] is significantly higher than for the standard BB84 protocol. For the qutrit BB84 scheme up to four MUBs can be used.
With the Ekert protocol it is a little bit different, as there is no unique generalization of the CHSH inequality. Therefore, there are various possible Bell-type inequalities that can be exploited for the security survey. Nevertheless, several Ekert protocols for three-dimensional quantum systems have been proposed [18, 29]. One possibility is to use inequality (2.25). Two observers A and B switch between three settings, where a_1, a_2 (b_1, b_2) are the settings to maximally violate the Bell inequality and a_3 (b_3) is used for key production. A and B choose their settings independently and at random and also record their detections independently. After sufficiently many measurement runs A and B compare their settings. $\frac{1}{9}$ of the produced data can be used for the key, while $\frac{4}{9}$ of the data are for the violation of the Bell inequality and the remaining $\frac{4}{9}$ have to be discarded. After this basis reconciliation B sends his data for the Bell inequality check to A, who computes the value of S_3. In the case that $S_3 > 2$, the key is considered secure and any eavesdropping will not have gained useful information on the key.
Although qutrit quantum cryptography schemes are theoretically a relatively simple extension of the well established qubit protocols and even promise better performance and security, no experimental demonstration has been performed so far.

3.6. Mutually Unbiased Bases

The BB84 and the Ekert scheme, at least in their qubit versions, require different mutually unbiased bases. Mutually unbiased means, that the overlap of all eigenvectors of one basis with all eigenvectors of a second basis are 1 over the square root of the dimension

d of the basis, i.e.

$$\langle\varphi_n|\psi_m\rangle = \frac{1}{\sqrt{d}}. \tag{3.1}$$

Here $\varphi_n \in \mathfrak{A}$ and $\psi_m \in \mathfrak{B}$, with $0 \leq n, m \leq d-1$. In general, if d is the power of a prime number, there are exactly $d+1$ MUBs [74]. For qutrits the four possible MUB bases are

$$\text{Basis } \mathfrak{A} : |0\rangle, |1\rangle, |2\rangle \tag{3.2}$$

$$\begin{aligned}\text{Basis } \mathfrak{B} : & \frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |2\rangle\right) \\ & \frac{1}{\sqrt{3}}\left(|0\rangle + e^{i\frac{2\pi}{3}}|1\rangle + e^{-i\frac{2\pi}{3}}|2\rangle\right) \\ & \frac{1}{\sqrt{3}}\left(|0\rangle + e^{-i\frac{2\pi}{3}}|1\rangle + e^{i\frac{2\pi}{3}}|2\rangle\right)\end{aligned} \tag{3.3}$$

$$\begin{aligned}\text{Basis } \mathfrak{C} : & \frac{1}{\sqrt{3}}\left(e^{i\frac{2\pi}{3}}|0\rangle + |1\rangle + |2\rangle\right) \\ & \frac{1}{\sqrt{3}}\left(|0\rangle + e^{i\frac{2\pi}{3}}|1\rangle + |2\rangle\right) \\ & \frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + e^{i\frac{2\pi}{3}}|2\rangle\right)\end{aligned} \tag{3.4}$$

$$\begin{aligned}\text{Basis } \mathfrak{D} : & \frac{1}{\sqrt{3}}\left(e^{-i\frac{2\pi}{3}}|0\rangle + |1\rangle + |2\rangle\right) \\ & \frac{1}{\sqrt{3}}\left(|0\rangle + e^{-i\frac{2\pi}{3}}|1\rangle + |2\rangle\right) \\ & \frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + e^{-i\frac{2\pi}{3}}|2\rangle\right)\end{aligned} \tag{3.5}$$

It is easy to verify, that they are mutually conjugated and that each basis is orthonormal. In order to use the MUBs in a quantum protocol like QKD, one has to be able to transform between the bases. For two-dimensional systems these are simply states on the surface of the Poincaré sphere rotated by $\frac{\pi}{2}$, where the vectors of one basis enclose an angle of π. E.g. for the polarization of photons, the bases $\{|H\rangle, |V\rangle\}$, $\{|+\rangle, |-\rangle\}$ and

$\{|R\rangle, |L\rangle\}$ are mutually unbiased, where $|+\rangle, |-\rangle$ represent ± 45 polarization and $|R\rangle, |L\rangle$ right and left polarization, respectively. The transformation in the simplest case, is done with a polarizer. To make any general transformation two $\lambda/2$, one $\lambda/4$ waveplates and a polarizer suffice [44]. Due to the conservation of probabilities, such a transformation has to be unitary, i.e. any transformation operator $\hat{T}$ has to satisfy $\hat{T}^\dagger \hat{T} = \hat{T}\hat{T}^\dagger = \mathbb{1}$, where $\hat{T}^\dagger$ is the adjoint (complex conjugated and transposed) of $\hat{T}$ and $\mathbb{1}$ the unity element. Hence, in two-dimension the transformation is an element of the group $SU(2)$ and in general d-dimensions $\hat{T} \in SU(d)$. $SU(d)$ stands for the group of Special Unitary matrices in d-dimensions, where special means $\det \hat{T} = 1$. For the case of three dimensions, in which we are interested here to make the transformations for a QKD protocol, $\hat{T} \in SU(3)$. Given a density matrix[1] ρ, one can expand it into the unity matrix and the eight generators[2] λ_r of the $SU(3)$, i.e. any transformation $\hat{T} \in SU(3)$ is defined by $3 \cdot 3 - 1 = 8$ independent parameters n_r $(r = 1, \ldots, 8)$:

$$\hat{T} = \frac{1}{3}\left(\mathbb{1} + \sqrt{3}\, n_r \cdot \lambda_r\right). \tag{3.6}$$

The parameters n_r are vectors in a three-dimensional Hilbert space $\mathcal{H}^3$, therefore representing all possible pure qutrit states. The set of all n_r is the analogue of the Poincaré sphere in three dimensions, defining the seven-dimensional unit sphere $\mathcal{S}^7$. It is interesting to note, that mutually orthogonal states are not on opposite sides of the sphere but maximally enclose an angle of $\frac{2\pi}{3}$ [46]. Reck et al. proved that it is experimentally possible to realize any such unitary operation for arbitrary dimensions d [54].

[1] The density matrix of a state $|\psi\rangle$ is the product of $|\psi\rangle$ with its adjoint, i.e. $\rho = |\psi\rangle\langle\psi|$. If $|\psi\rangle$ is a pure state, ρ is hermitian, positive and projective, i.e. $\rho = \rho^\dagger = \rho^2 \geq 0$. For a mixed state $\rho^2 \neq \rho$.

[2] One of the standard representations of these generators are the Gell-Mann matrices [38], which obey the commutation relation $[\lambda_r, \lambda_s] = 2i f_{rst} \lambda_t$, where f_{rst} are completely antisymmetric structure constants.

4. Orbital Angular Momentum

The electromagnetic field and its quantization, the photon, possess both linear and angular momentum. While it is well-known that linear momentum is exchanged in the interaction of photons and matter, it was only in 1936 when Beth experimentally proved that the angular momentum exerted a torque on a birefringent plate [14]. In Beth's work he used (circularly) polarized photons, which is the spin part of the angular momentum. The other part is the orbital angular momentum (OAM), which is associated with the spatial distribution of the field. Both angular momenta are, in contrast to the linear momentum, quantized, where the spin component only exists in $\pm\hbar$ and the orbital component in multiples of $\hbar$. E.g. a right-handed polarized photon with momentum $+\hbar$ is transformed into a left-handed photon with momentum $-\hbar$ by passing a $\lambda/2$ waveplate and therefore $2\hbar$ of momentum are transferred from the photon to the waveplate. Allen et al. [2] showed theoretically that beams with a phase singularity possess OAM and that they are eigenmodes of the angular momentum operator[1] $\hat{L}_z$. It was later experimentally confirmed by He et al. [43] that orbital angular momentum can actually be associated with such modes.

4.1. Paraxial Waves

A paraxial wave's wavefront normals are paraxial rays, i.e. they are parallel to the propagation axis. Strictly speaking this is only true for plane waves. Nevertheless light is often described as a paraxial electromagnetic wave, what is a good approximation if it can be described as a plane wave with a slowly varying position dependent amplitude:

$$U(r) = A(r)e^{-ikz}, \tag{4.1}$$

where $r = \sqrt{x^2 + y^2 + z^2}$, k the wavenumber and z the position in the propagation direction. Such a paraxial wave is realized if the variation of $A(r)$ is small compared to the wavelength λ and therefore $U(r)$ locally resembles a plane wave. In most situations this description is sufficiently accurate for light waves. Any such paraxial wave has to

[1] In atomic physics the total angular field $\hat{J}$ is decomposed into two observables, i.e. $\hat{J} = \hat{L} + \hat{S}$. $\hat{S}$ is the spin component and $\hat{L}$ the orbital component. $\hat{L}_z$ therefore is the operator measuring the z component of the orbital angular momentum. However, it is not always clear, whether $\hat{L}$ and $\hat{S}$ are separate physical observables. For transversal modes of photons, this was shown by the work of Allen et al. .

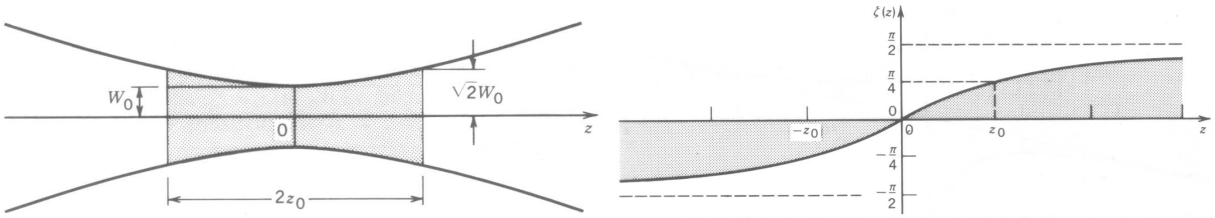


Figure 4.1.: *The left picture illustrates the Rayleigh length z_0, which is the distance where the beam waist is $\sqrt{2} \cdot W_0$. The right picture shows the Gouy phase $\zeta(z)$, being the phase retardation of the Gaussian beam relative to a uniform plane wave (images taken from [58]).*

satisfy the paraxial Helmholtz equation

$$\frac{\partial^2 U}{\partial x^2} + \frac{\partial^2 U}{\partial y^2} - i2k\frac{\partial U}{\partial z} = 0. \tag{4.2}$$

Probably the best known solution of this equation is the Gaussian beam

$$U(r) = \frac{A_1}{iz_0}\,\frac{W_0}{W(z)}\; e^{-\frac{\rho^2}{W^2(z)}}\; e^{-ikz - ik\frac{\rho^2}{2R(z)} + i\zeta(z)}, \tag{4.3}$$

where A_1 and z_0 are parameters determined by the boundary conditions, the latter being the so-called Rayleigh length — it is defined as the axial distance from the beam waist where the beam radius is increased by a factor of $\sqrt{2}$. Further, $\rho^2 = x^2 + y^2$ (the radial distance) and the other variables are beam parameters and are defined as functions of z_0 and the wavelength λ:

$$\begin{aligned} W(z) &= W_0\left[1 + \left(\frac{z}{z_0}\right)^2\right]^{\frac{1}{2}}, \\ R(z) &= z\left[1 + \left(\frac{z}{z_0}\right)^2\right], \\ \zeta(z) &= \tan^{-1}\frac{z}{z_0}, \\ W_0 &= \left(\frac{\lambda z_0}{\pi}\right)^{\frac{1}{2}}. \end{aligned} \tag{4.4}$$

$W(z)$ is the distance in axial direction in which the maximal intensity decreases by $\frac{1}{e^2}$ and is also called beam radius. Its minimum value is at $z = 0$ and is equal to W_0, the

so-called waist radius. $2W_0$ is also denominated as the spot size. Additionally, $R(z)$ is the radius of curvature of the wavefront. It is infinite at $z = 0$ (just like a plane wave) and reaches a minimum value of $2z_0$ at $z = z_0$. Finally, $\zeta(z)$ is the Gouy phase, a phase retardation relative to a uniform plane wave, which ranges from $-\frac{\pi}{2}$ to $+\frac{\pi}{2}$ between $z = -\infty$ and $z = +\infty$. Hence the total acquired phase retardation is π. The expression in the second exponent of (4.3) is the overall phase of the Gaussian beam $\varphi(\rho, z)$. On the beam axis the phase reduces to $\varphi(0, z) = kz - \zeta(z)$, where kz is the phase of a plane wave and $\zeta(z)$ the above described respective retardation.

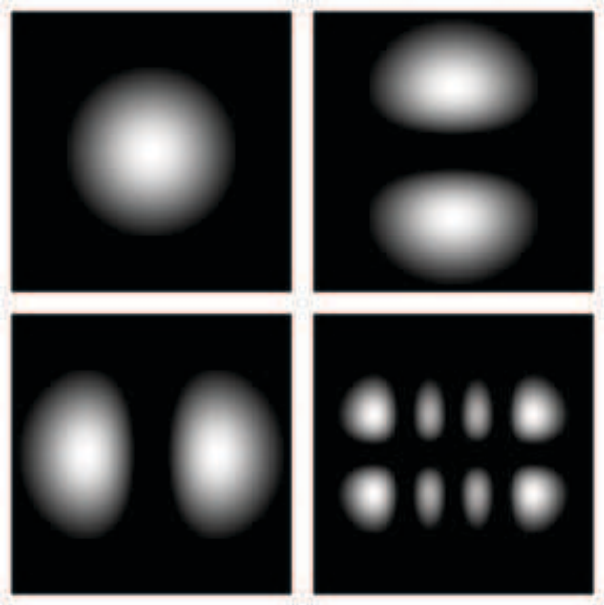


Figure 4.2.: *Hermite Gaussian modes have two indices m, n, where m is the number of vertical nodes, while n are the horizontal nodes. The upper left picture is the $HG_{0,0}$ mode, which is simply the Gaussian mode (and equivalently the $LG_{0,0}$ mode). The upper right is the $HG_{0,1}$, while the lower left and right are the $HG_{1,0}$ and $HG_{3,1}$ modes, respectively.*

In addition to the relatively simple and well-known Gaussian beam there are a number of other solutions of the paraxial Helmholtz equation (4.2). E.g. the transversal modes of a laser, which fulfill certain transverse boundary conditions, i.e. the electromagnetic field has to fall to zero in the direction of ρ. In their cartesian description, used for rectangular symmetrical situations, they are the Hermite-Gaussian modes (HG) (the intensity profiles of some HG modes are shown in Fig. 4.2) and in the cylindrically symmetric solutions they are called Laguerre-Gaussian modes (LG). Such transversal modes have a non-vanishing orbital angular momentum. In the following we will only

consider LG modes. An LG mode is defined as

$$U_{p,l}(\rho,\phi,z) = \sqrt{\frac{2p!}{\pi(p+|l|)!}}\frac{1}{W(z)}\left(\frac{\sqrt{2}\,r}{W(z)}\right)^{|l|} e^{\frac{-r^2}{W^2(z)}} e^{\frac{-ikr^2}{2R(z)}} e^{-i(2p+|l|+1)\zeta(z)} e^{-il\phi} L_p^{|l|}\left(\frac{2r^2}{W^2(z)}\right), \tag{4.5}$$

where $L_p^l(x)$ are the generalized Laguerre polynomials. Here the Gouy phase is

$$\zeta_{LG} = (2p+l+1)\cdot\zeta(z). \tag{4.6}$$

The Laguerre-Gaussian modes, which we will denote as $LG_{p,l}$ have two independent indices p and l, where $p+1$ represents the number of radial nodes, while the index l is the winding number, with $2\pi l$ describing the change in phase on a closed path around the propagation axis (4.3). This phase change is due to the term $e^{-il\phi}$ in Eq. (4.5) and results in a phase-singularity in the beam center, as there the change in phase becomes infinitely large. Hence, in contrast to the plane wave with plane wavefronts, the wavefronts are helical, which can be understand as the Poynting vector[2] spinning around the beam axis. The orbital angular momentum[3] of an LG mode is given by $l\cdot\hbar$ and l is sometimes called the topological charge of the singularity. A mode with indices $p = l = 0$ is a Gaussian mode and therefore has no orbital angular momentum. The LG modes form an orthogonal basis and hence span an infinite-dimensional Hilbert space. We will restrict our further discussion to modes with index $p = 0$. These $LG_{0,l}$ also span an infinite-dimensional Hilbert space and they are often called doughnut modes, due to their characteristic intensity profile (see Fig. 4.4).

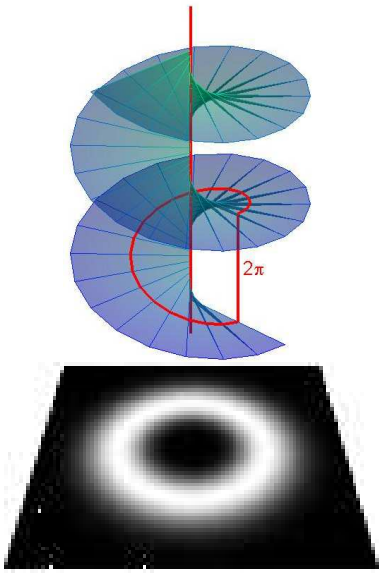


Figure 4.3.: *Sketch of the helix of an $LG_{0,x}$ mode. $2\pi l$ is the change in phase around a closed path. (by Martin Stütz)*

4.2. Generation of Laguerre-Gaussian Beams

LG modes are actual modes of a laser and are produced in almost any laser cavity. However, generally lasers are constructed such, that they suppress these modes and only emit a pure Gaussian beam.

[2]The Poynting vector is defined as $S = E \times H$, where E and H are the electric and magnetic field, respectively. For a plane wave it points in the propagation direction, as it has no orbital angular momentum.

[3]The orbital angular momentum is, as already mentioned above, the eigenvalue of the operator $\hat{L}_z = -i\hbar\frac{\partial}{\partial\phi}$.

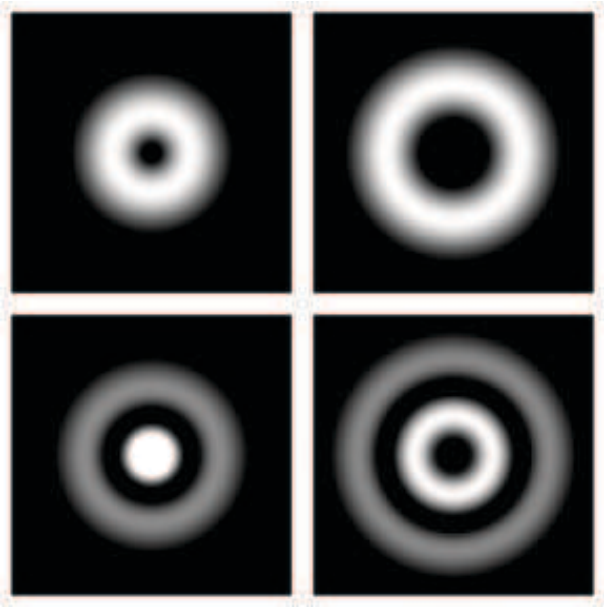


Figure 4.4.: *Numerically calculated Laguerre-Gaussian modes with different indices p and l. The upper left is an $LG_{0,1}$ mode and the upper right an $LG_{0,3}$ mode. Due to their characteristic intensity profile, these modes are called doughnut modes. $LG_{0,3}$ is a mode with a slightly bigger phase singularity compared to $LG_{0,1}$. In the lower pictures two radial nodes can be observed because of a non-vanishing index $p = 1$, where the left is an $LG_{1,0}$ and the right an $LG_{1,2}$ mode.*

In order to efficiently produce Laguerre-Gaussian beams several different approaches can be used — e.g. HG can be directly converted into LG modes. Therefor two cylindrical lenses have to be appropriately aligned such, that they introduce a Gouy phase on an incident HG mode, which converts the HG with indices m and n into an LG with $l = m - n$ and $p = min(m, n)$ [8]. However, producing the required HG modes with a commercial laser involves the same difficulties as directly producing LG modes.
A different approach would be to use spiral phase plates [66]. These are transparent plates with a spiral surface, which is one period of a helix, ended with a step discontinuity s. With $s = \frac{l\lambda}{n_1 - n_2}$, where λ is the wavelength, n_1, n_2 are the refractive indices of the plate and of the surrounding medium, respectively, the plate creates an azimuthal mode index l. The problem with the spiral plates is the accuracy of s, which for small λ is difficult to realize and any deviation is observed as a break in the doughnut intensity pattern.
Computer generated holograms probably provide the best way of producing an LG mode out of the Gaussian mode of a laser beam. The big advantage is, that basically any mode can be produced, without the need of complicated experimental setups. The desired holograms are simply calculated and put on a suitable medium.
In general a hologram is the recording of the interference pattern of the desired mode

with a suitable reference mode. The simplest reference field is the plane wave,

$$R = R_0 e^{ik_x x + ik_z z}, \tag{4.7}$$

where R_0 is the amplitude and k_x and k_z are the components of the wavevector in the respective direction. The interference pattern of (4.7) and (4.5) at $z = 0$ is given by

$$I(\rho, \phi) = |R_0 e^{ik_x x} + U_{p,l}(\rho, \phi)|^2, \tag{4.8}$$

which can be numerically calculated. The result of such a numerical calculation, for indices $p = 0$ and $l = 1$ is shown in Fig. 4.6. If such a hologram, which can be simply printed on a transparency or e.g. be etched onto a quartz plate, is illuminated with a gaussian beam (which is very close to a plane wave), the $LG_{0,1}$ mode is reproduced.

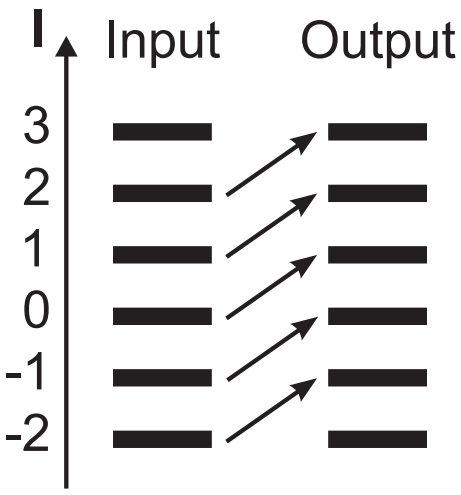


Figure 4.5.: *Scheme of the transformation of a computer generated phase hologram. An incident wave with index l is transformed into a wave with index $l + 1$. The process can be inverted and hence such a hologram can be seen as a realization of an approximate ladder operator.*

In the first diffraction order of such a hologram, a phase of $e^{i(l+\Delta l)\phi}$ is induced, which results in the desired $LG_{0,1}$ mode. One sees, that if the l in the original beam is non-zero, but for example $l = 2$, the resulting first order diffraction is an $LG_{0,3}$ mode. Additionally, the higher diffraction orders produce a correspondingly higher Δl, i.e. the second order diffraction induces a phase of $e^{i(l+2\Delta l)\phi}$ and so on. If the beam direction is inverted the transformation process of the hologram is also inverted and an $LG_{0,1}$ is transformed into an $LG_{0,0}$. Such a hologram can therefore be seen as the implementation of an approximate ladder operator, which increases (e.g. $+1$) or decreases (-1) the index l of an arbitrary incident mode (see Fig. 4.5).

In order to maximize the intensity of the first diffraction order, which is needed to reduce the loss in other orders and therefore increase the converted to incoming signal ratio, one can *blaze* the grating obtained in (4.8). For a detailed description of this technique and related issues on holograms see [3, 67]. In Fig. 4.6 the numerical result of such a calculation is shown.

If such a hologram is realized on reflective material, it is called a reflection hologram. Throughout this work we only use transmission holograms, albeit in chapter 7 we will briefly discuss a special kind of reflection hologram, which is envisioned for future applications. The most general transformation by a transmission hologram is described as

$$U_{out}(\rho, \phi) = T(\rho, \phi)\, U_{in}(\rho, \phi), \tag{4.9}$$

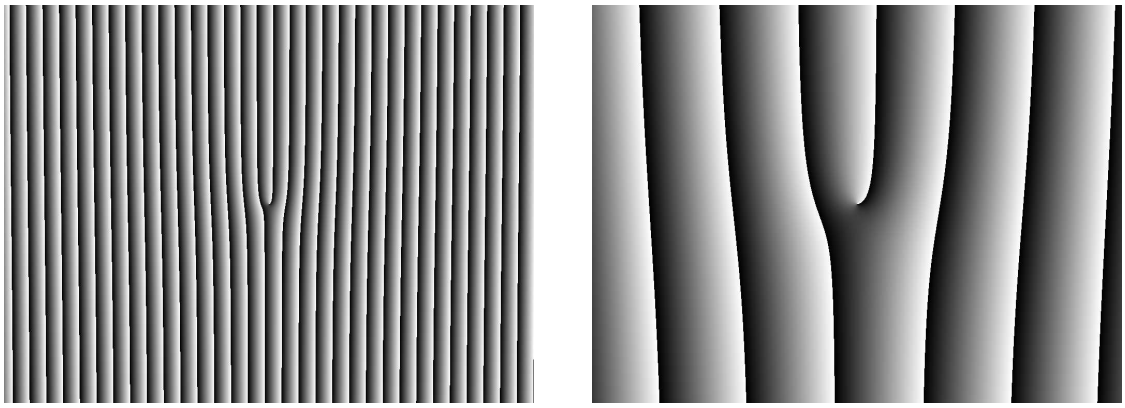


Figure 4.6.: *A computer generated phase hologram, which is the interference pattern of a plane wave with an $LG_{0,1}$ mode, i.e. $I(\rho,\phi) = |R_0 e^{ik_x x} + U_{p,l}(\rho,\phi)|^2$. The amplification on the right illustrates the singularity and the blazing of the grating.*

where U_{out} and U_{in} are the transformed and the original field, respectively. T is the transmission function describing the hologram, which in the above case for a blazed grating is

$$T(\rho,\phi) = e^{i\frac{\delta}{2\pi}(\Delta l\phi - \frac{2\pi}{\Lambda}\rho\cos\phi)\mathrm{mod}2\pi}, \tag{4.10}$$

where δ is the amplitude of the phase modulation, Λ the grating's periodicity and Δl the number of displacements. This transformation only holds if the incoming beam is centered on the hologram. E.g. a Gaussian beam is transformed into an $LG_{0,1}$ beam, with a central singularity in its intensity profile. However, if the hologram is slightly displaced from the beam center, a coherent[4] superposition of U_{out} and U_{in} is produced. Additionally, higher order modes, although with a very low ratio, are coherently superposed. The relative amplitudes of the different modes are given by

$$A_L^l(\rho_0,\phi_0) = \int_{-\infty}^{+\infty}\int_0^{2\pi} \rho\, d\rho\, d\phi \left(U_{P,L}(\rho,\phi,0)\, e^{-i\Delta l\frac{2\pi}{\Lambda}\rho\cos\phi}\right)^* T(\rho-\rho_0,\phi-\phi_0)U_{0,l}(\rho,\phi,0). \tag{4.11}$$

A_L^l is the amplitude of the $LG_{P,L}$ mode in the first diffraction order, where the original beam is a $LG_{0,l}$ and the hologram is displaced relative to the beam center by ρ_0, ϕ_0 (see Ref. [9]). The intensity distributions of the various modes as a function of the hologram position are shown in Fig. 4.7. This feature gives an easy way of producing all sorts of superpositions and we will discuss its application in a QKD protocol in the following section. However, for the same reason, the resulting modes are always superpositions (although arbitrarily small) of the desired index l with different indices p and hence the modes produced with holograms and spiral phase plates never are perfectly pure LG modes.

[4]Coherent means with a fixed phase relation.

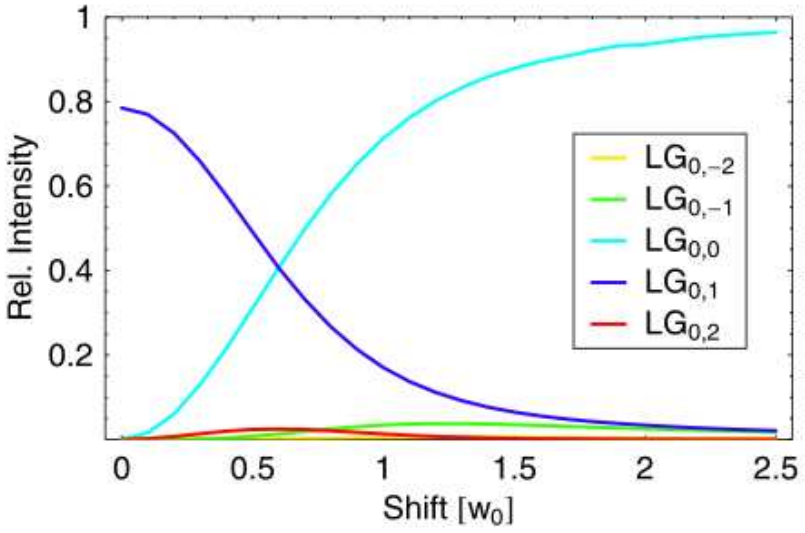


Figure 4.7.: *Relative intensity distribution of several LG modes as a function of the hologram displacement from the beam center in units of the waist radius. The hologram does a +1 transformation on an incident Gaussian mode. The maximal contribution of higher order modes is less than 3 %. (calculated by Gregor Weihs)*

Note that superpositions of *LG* modes can also be produced by splitting a Gaussian beam into two modes, transforming one with a hologram and recombining the two modes. This interferometric method can be scaled to arbitrary many modes and hence all sorts of superpositions can be produced. We will not further discuss this scheme but a short introduction can be found in [67].

4.3. Holograms and MUB Transformations

As mentioned in section 3.6, transformations between different MUB bases are required in order to realize a BB84-type QKD. The computer generated phase holograms described above can in principle be used to achieve such a transformation. If two consecutive holograms are chosen such, that one makes a $+1$ and the other a -1 transformation in the index l, then by displacing them appropriately it seems possible to make a MUB transformation. In this section we will first analytically discuss such transformations and then show the results of numerical calculations for a two-bases BB84 protocol. In order to find a suitable transformation, different criteria have to be fulfilled:

- The transformation matrix has to be unitary.
- The columns of the matrix have to be mutually orthogonal, which corresponds to the orthogonality of the basis vectors.

- As the MUB condition (3.1) has to be satisfied, the amplitudes of the matrix elements are supposed to be uniform.

In principle all criteria have to be exactly satisfied. As a first step we will analyze how well they can be satisfied by our approach.

4.3.1. An illustrative Approach

An ideal hologram only creates superpositions of the fundamental and the converted mode, without any higher order part, i.e. $|l\rangle \rightarrow a|l\rangle + b|l+1\rangle$ for the $+1$ operation and the respective for the -1, where $|l\rangle$ is an $LG_{0,l}$ and $|l+1\rangle$ an $LG_{0,l+1}$ mode. It is clear, that a real hologram always contains higher order modes because it would otherwise violate unitarity, but the higher order parts are negligibly small (at most around 3 % — see Fig. 4.7). Therefore it seems reasonable to assume an ideal hologram and show that a $+1/-1$ combination cannot, even in principle make a $SU(3)$ transformation. To demonstrate this, we will use a simple illustration:

	-3	-2	-1	0	+1	+2	+3
-1					$\frac{1}{\sqrt{3}}$		
0				$\frac{1}{\sqrt{3}}$			
+1			$\frac{1}{\sqrt{3}}$				

where the columns of the table represent an entangled state $|\Psi\rangle = \frac{1}{\sqrt{3}}(|-1+1\rangle + |00\rangle + |+1-1\rangle)$ of the original beam. The columns are the amplitudes of the modes of one particle and the rows represent the individual mode amplitudes of the other particle. Hence, performing a transformation on one means, the amplitudes of the rows are left unchanged, while the columns are actually transformed (or viceversa). A $+1$ transformation on one particle therefore yields the following:

	-3	-2	-1	0	+1	+2	+3
-1					$\frac{1}{\sqrt{3}}$		
0				$\frac{1}{\sqrt{3}}$			
+1			$\frac{1}{\sqrt{3}}$				

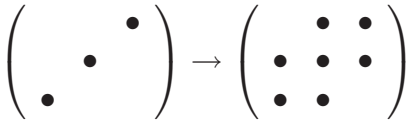
$\rightarrow$

	-3	-2	-1	0	+1	+2	+3
-1					$\frac{a}{\sqrt{3}}$	$\frac{b}{\sqrt{3}}$	
0				$\frac{a}{\sqrt{3}}$	$\frac{b}{\sqrt{3}}$		
+1			$\frac{a}{\sqrt{3}}$	$\frac{b}{\sqrt{3}}$			

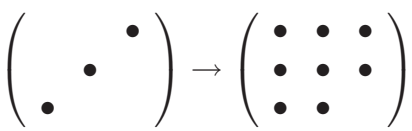
In a simplified matrix representation this looks like

$$\begin{pmatrix} & & \bullet \\ & \bullet & \\ \bullet & & \end{pmatrix} \rightarrow \begin{pmatrix} & & \bullet \\ & \bullet & \bullet \\ \bullet & \bullet & \end{pmatrix}$$

where the dots stand for non-vanishing amplitudes. A $+1/-1$ combination of two consecutive holograms would then result in



which clearly is not a suitable transformation between MUB bases, as some of the amplitudes are completely empty (or for non-ideal holograms close to zero). If one employs a -2 hologram ($|l\rangle \rightarrow d|l\rangle + e|l-1\rangle + f|l-2\rangle$), which simply is the interference pattern of a plane wave with an $LG_{0,2}$ mode, instead of the -1 hologram, the transformation looks like



Again, not all amplitudes are non-zero and hence only the combination of $+2$ with a -2 hologram can in principle achieve the desired transformation.

4.3.2. Three Holograms

The case with two 2-step holograms is intuitively included in the case with three consecutive holograms, e.g. a $+1/-2/+1$ combination. An approach with three hologram has the advantage of providing more degrees of freedom (remember, that for a general $SU(3)$ transformation, eight independent parameters are required). Subsequently we will try to solve this analytically and we will also show some numerical calculations.
We therefore start with $+1$ transformation hologram: $|l\rangle \rightarrow a|l\rangle + b|l+1\rangle$, followed by a -2: $|l\rangle \rightarrow c|l\rangle + d|l-1\rangle + e|l-2\rangle$ and finally another $+1$: $|l\rangle \rightarrow f|l\rangle + g|l+1\rangle$. In order to make the calculations simpler we choose $d = 0$. The first transformation yields

-3	-2	-1	0	+1	+2	+3
				a	b	
			a	b		
		a	b			

The second and third give

-3	-2	-1	0	+1	+2	+3
		ae	be	ac	bc	
	ae	be	ac	bc		
ae	be	ac	bc			

$\rightarrow$

-3	-2	-1	0	+1	+2	+3
		aef	aeg+bef	beg+acf	acg+bcf	bcg
	aef	aeg+bef	beg+acf	acg+bcf	bcg	
aef	aeg+bef	beg+acf	acg+bcf	bcg		

If, without loss of generality, we now set $a = c = f = 1$ and $b = \gamma_1 e^{i\varphi_1}$, $e = \gamma_3 e^{i\varphi_3}$, $g = \gamma_4 e^{i\varphi_4}$ and if we restrict ourselves to the desired subspace, we can rewrite the list in matrix form

$$\mathrm{T} = \begin{pmatrix} \gamma_3 e^{i\varphi_3} & \gamma_1\gamma_3 e^{i(\varphi_1+\varphi_3)} + \gamma_3\gamma_4 e^{i(\varphi_3+\varphi_4)} & \gamma_1\gamma_3\gamma_4 e^{i(\varphi_1+\varphi_3+\varphi_4)} + 1 \\ \gamma_1\gamma_3 e^{i(\varphi_1+\varphi_3)} + \gamma_3\gamma_4 e^{i(\varphi_3+\varphi_4)} & \gamma_1\gamma_3\gamma_4 e^{i(\varphi_1+\varphi_3+\varphi_4)} + 1 & \gamma_1 e^{i\varphi_1} + \gamma_4 e^{i\varphi_4} \\ \gamma_1\gamma_3\gamma_4 e^{i(\varphi_1+\varphi_3+\varphi_4)} + 1 & \gamma_1 e^{i\varphi_1} + \gamma_4 e^{i\varphi_4} & \gamma_1\gamma_4 e^{i(\varphi_1+\varphi_4)} \end{pmatrix}$$

As all entries have to have uniform amplitudes but can still have an arbitrary phase, we get

$$\gamma_3 = \gamma_1\gamma_4, \tag{4.12}$$

$$\gamma_3^2 e^{i(\varphi_1+\varphi_3+\varphi_4)} + 1 = \gamma_3 e^{i\varphi_x}, \tag{4.13}$$

$$\gamma_1 e^{i\varphi_1} + \gamma_4 e^{i\varphi_4} = \gamma_3 e^{i\varphi_y}, \tag{4.14}$$

$$\gamma_1\gamma_3 e^{i(\varphi_1+\varphi_3)} + \gamma_3\gamma_4 e^{i(\varphi_3+\varphi_4)} = \gamma_3 e^{i\varphi_z}, \tag{4.15}$$

where we introduced the new phases $\varphi_x, \varphi_y, \varphi_z$. By rearranging (4.15) to $(\gamma_1 e^{i\varphi_1} + \gamma_4 e^{i\varphi_4})e^{i\varphi_3} = e^{i\varphi_z}$ and substituting it into (4.14) we arrive at

$$\gamma_3 e^{i(\varphi_3+\varphi y)} = e^{i\varphi_z} \tag{4.16}$$

and thus obtain $\gamma_3 = 1 = \gamma_1\gamma_4$. From (4.13) we now get $\varphi_1 + \varphi_3 + \varphi_4 = \pm\frac{2\pi}{3}$. The orthogonality condition gives three further constraints, which leaves us with five equations for five unknown variables. It was however not possible to solve these equations by hand and even with *Mathematica* no useful result could be obtained. It leaves the open question, whether such a transformation matrix can be found at all. Not to mention, that the case where $d \neq 0$ is somewhat more complicated. We were not able to show if this problem is solvable at all.
Consequently it seems not possible to realize a qutrit BB84 protocol with two or three consecutive holograms. It is however likely that some other schemes, like the interferometric method, can actually perform the needed transformations.

4.3.3. A numerical Approach

With Wolfram's *Mathematica* we calculate the amplitudes (4.11) for different combinations of holograms. The first approach is two holograms, where one does a $+1$ and the other a -1 transformation. The horizontal and vertical positions with respect to the beam center of both holograms are individually changed, with a maximal displacement of ± 1.5 and a step size of 0.1 (in arbitrary units). The respective amplitudes for the desired qutrit subspace, i.e. $LG_{0,-1}$, $LG_{0,0}$ and $LG_{0,1}$, are calculated for every combination

of the 31^4 relative positions. This data is then used to find the transformation that best suites the three criterions from section 4.3.1.
Other combinations of holograms are also evaluated. E.g. a $+1/-2/+1$ combination is simulated with maximal displacements of ± 1 and a step size of 0.1, which is a total number of 21^6 combinations. Finally we even tried 4 holograms but the exponentially increasing number of combinations and the hence very high demand on computational power made it more and more difficult. On top of that the quality of the results with more holograms did not increase the way we expected. The program for simulating three holograms is shown in Appendix A.1.
Some calculated matrices T_i for the three hologram case are shown here. The entries are rounded off to the third decimal places and the matrices are checked for uniformity (by taking the square of the matrix and comparing the entries) and orthogonality.

$$T_1 = \begin{pmatrix} 0.589 + 0\,i & 0 + 0\,i & 0 + 0\,i \\ 0 + 0\,i & 0.785 + 0\,i & 0 + 0\,i \\ 0 + 0\,i & 0 + 0\,i & 0.589 + 0\,i \end{pmatrix},$$

which is clearly orthogonal but nothing close to uniform.

$$T_2 = \begin{pmatrix} -0.131 + 0.111\,i & 0 - 0.245\,i & -0.024 - 0.019\,i \\ -0.190 + 0.183\,i & -0.004 + 0.120\,i & 0.093 - 0.125\,i \\ -0.086 + 0.123\,i & 0.010 + 0.080\,i & -0.151 + 0.261\,i \end{pmatrix}$$

The column vectors of T_2 are almost orthogonal, i.e. the inner products are 0.005, 0.009 and 0.010, but again, the uniformity is not provided.

$$T_3 = \begin{pmatrix} -0.196 + 0.097\,i & -0.062 - 0.010\,i & -0.121 + 0.006\,i \\ -0.117 + 0.036\,i & -0.179 + 0.115\,i & 0.077 + 0.038\,i \\ -0.077 + 0.026\,i & -0.010 + 0.044\,i & -0.181 + 0.140\,i \end{pmatrix}$$

Here the orthogonality is not entirely satisfied, as the inner products are 0.034, 0.017 and 0.033, the matrix is not uniform and additionally the amplitudes are very small. Unfortunately, we could not find any suitable transformation that complied with uniformity and orthogonality satisfactory. It remains unclear, whether such a transformation can be realized with this scheme after all.

5. Experimental Realization of Photonic Qutrits

For the realization of QKD with photons entangled in their orbital angular momentum, various different experimental tools are needed. In the previous chapters, the physical background of the experimental components and the setup itself have been discussed. In the following we will introduce and explain the components employed for the creation of entangled photons, the basis transformation, the detection process and the key generation scheme.

5.1. The Source

Certain crystals are non-linear media as electromagnetic fields E_i couple quadratically (or in even higher orders) to the induced polarization field P_i in the crystals, i.e.

$$P_i = \chi^{(1)}_{ij} E_i + \chi^{(2)}_{ijk} E_j E_k + \chi^{(3)}_{ijkl} \dots \tag{5.1}$$

Such a quadratic dependency is sometimes called three-wave mixing, as an incident field is coupled to two outgoing fields. If an intense laser shines on such a $\chi^{(2)}$-non-linear crystal, an incident pump photon may decay into two outgoing photons. This effect is called spontaneous parametric down-conversion (SPDC) and is used to produce pairs of entangled photons. Here, the energy and the momentum of the pump photon p are conserved and therefore two conditions have to hold:

$$\vec{k}_p = \vec{k}_s + \vec{k}_i, \tag{5.2}$$

$$\omega_p = \omega_s + \omega_i, \tag{5.3}$$

where signal s and idler i denote the outgoing fields. $\vec{k}$ are the wavevectors inside the crystal and ω the frequencies, i.e. the energies, of the photons. Note that $\vec{k}_s$, $\vec{k}_i$ and ω_s, ω_i are in principle arbitrary but have to satisfy the above conservation laws. A BBO ($\beta - BaB_2O_4$) crystal, is an optical negative medium, i.e. $n_o > n_e$, where n_o is the refraction index for the ordinary field and n_e the refraction index for the extraordinary field. For the momentum conservation, two different phase matching conditions exist, which are normally denoted as type-I and type-II. In type-I phase matching

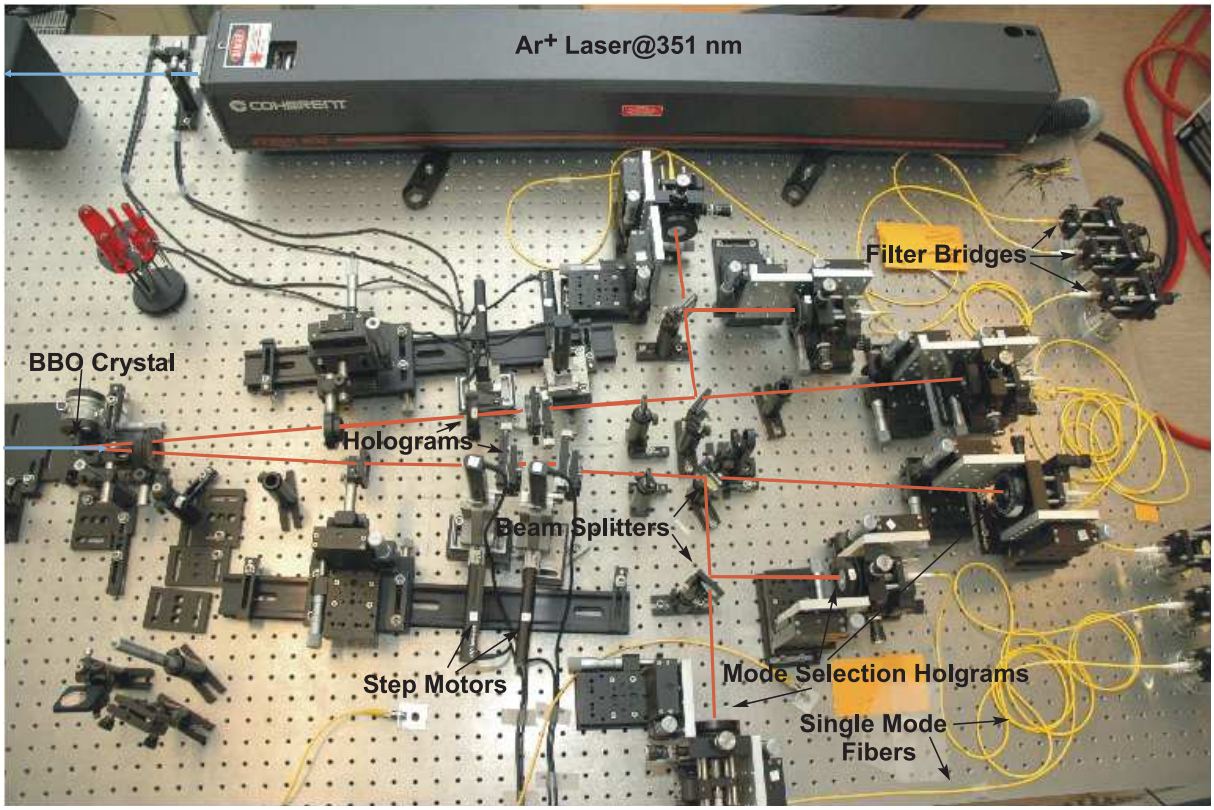


Figure 5.1.: *Photograph of the experimental setup for the violation of a three-dimensional Bell inequality and a qutrit quantum key distribution scheme. The source is an Ar^+ laser pumping a BBO crystal at a wavelength of* 351 *nm and an optical power of approximately* 95 *mW. Two phase holograms in each down-conversion arm, mounted on computer-controlled step motors, are used for transforming the incoming maximally entangled qutrit state. Probabilistic mode analyzers, consisting of beam splitters, mode selection holograms and single mode fibers, allow the differentiation between the three orthogonal modes $LG_{0,-1}$, $LG_{0,0}$ and $LG_{0,1}$. Finally, separate filter bridges, in which interference filters are mounted, ensure that only the energy degenerate photons from the parametric down-conversion are detected.*

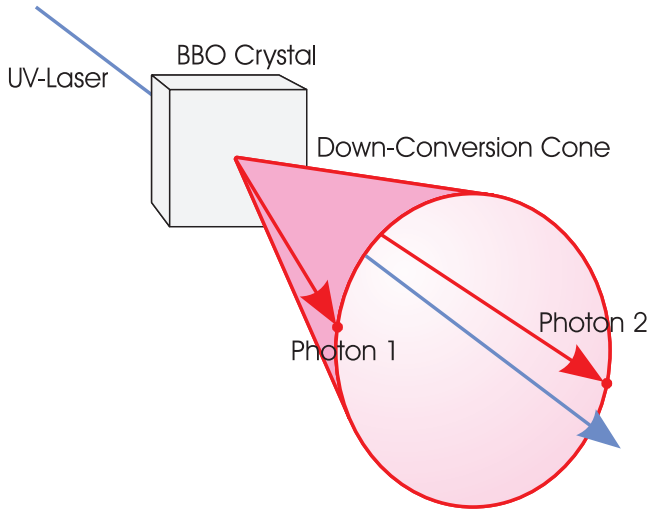


Figure 5.3.: *Type-I spontaneous parametric down-conversion. The photons have equal polarization and for the energy degenerate case the down-converted photons are emitted on opposite sides of a single cone. In this process the total orbital angular momentum of the pump photon is conserved and therefore an entangled orbital angular momentum state can be produced.*

the signal and idler modes have the same polarization and photons with equal wavelength are emitted on opposite sides of the same emission cone. Typically an ordinary pump field couples to an extraordinary signal and idler field and viceversa, i.e. $\vec{k}_p^o = \vec{k}_s^e + \vec{k}_i^e$. Type-II phase matching couples an extraordinary pump mode to one ordinary and one extraordinary mode ($\vec{k}_p^e = \vec{k}_s^o + \vec{k}_i^e$). The down-converted photons not only are in orthogonal polarization states, but also are emitted on two distinct cones.

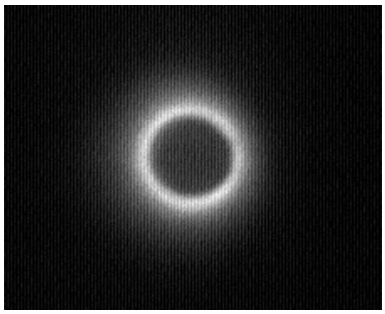


Figure 5.2.: *Photograph of the type-I down-conversion process, observed with a CCD camera through a low-pass filter with a cutoff at* 800 *nm.*

It was experimentally [48, 23] shown and later theoretically [34] confirmed, that the orbital angular momentum of photons is conserved in the process of parametric down-conversion in the collinear regime. If the pump beam creating pairs of entangled photons has a Gaussian profile it is thus possible to obtain the maximally entangled state

$$\psi = \alpha|0\rangle|0\rangle + \beta|1\rangle|2\rangle + \gamma|2\rangle|1\rangle, \tag{5.4}$$

with $\alpha = \beta = \gamma = \frac{1}{\sqrt{3}}$. Here $|1\rangle$ is the $LG_{0,1}$ mode, $|2\rangle$ the $LG_{0,-1}$ mode and $|0\rangle$ the Gaussian mode $LG_{0,0}$.
For our source of entangled photons we pump a 1.5 mm thick BBO with a vertically polarized Ar^+ laser at a wavelength of 351 nm (Coherent Innova 300) and an optical output power of 95 mW. Before the laser actually hits the

BBO, its spectrum is cleaned from fluorescent light of the gas discharge in the laser-tube with a 60° prism. To increase the intensity of the pair production, the laser is then focused into the BBO crystal with a 600 mm UV-lens. In order to get an entangled state, the photons of each pair produced have to be indistinguishable. Therefore, we use a BBO with type-I phase matching as it produces polarization degenerated photons. Furthermore, the wavelengths of signal and idler have to be equal and hence $\frac{\omega_p}{2} = \omega_s + \omega_i$. But as mentioned above, in principle the photons can have any wavelength satisfying (5.3). For this reason, we have to filter out all the pairs with unequal wavelengths and only detect the ones with $\lambda = 702$ nm. This is done by introducing interference filters, which will be explained in section 5.3.

5.2. Basis Transformation

For the basis transformation and the mode detection (see section 5.3) computer generated holograms are used. As already discussed in chapter 2.3 such holograms can generate superpositions of LG modes. In order to make transformations needed for the violation of inequality (2.25) it has been experimentally demonstrated [68], that two consecutive holograms, one being a $+1$ and the other a -1, are sufficient. The holograms we use were made by Prof. Bernhard Kley's group at the Institut für angewandte Physik der Friedrich-Schiller Universität in Jena, Germany [67]. They are transmissive phase gratings, with a single dislocation each. The numerically calculated structure was patterned via electron-beam lithography and etched onto $10 \times 10 \times 2$ mm quartz plates. The final active holographic size is 3×3 mm. The periodicity of the grating is 30 μm and approximately 80 % of the intensity are diffracted into the first diffraction order, due to the blazing of the grating. To optimize the holograms for a wavelength of 702 nm, they were coated with an anti-reflex layer for the near IR.

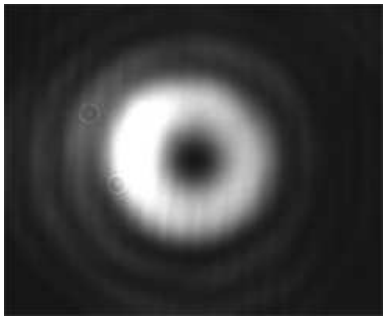


Figure 5.4.: *Intensity profile of a 702 nm laser diode after passing two consecutive holograms, where one makes a $+1$ transformation and the other none. The image was taken with a CCD camera.*

The generation of superpositions of various LG modes requires the possibility of horizontally dislocating the holograms from the beam center of the down-converted photons. Therefore they are individually mounted on step motors (Newport), which are connected to motion controllers, that can be addressed via a *LabView* program. The exact scheme will be explained in section 5.4.

5.3. Detection

It is further necessary to distinguish the orbital angular momentum states of each individual photon. This is not as simple as it at first seems but with a hologram and a single-mode fiber one can build probabilistic mode detectors. As fibers have small core diameters, they only support certain wavelengths to propagate. The reason is, the higher the wavelength λ, the bigger the spatial size of the mode. The core radius a of the single-mode fibers (a fiber that only supports one spatial mode) we use can be calculated as follows:

$$a = F \cdot \frac{\lambda_{\text{cutoff}}}{2\pi \cdot \text{NA}} = 1.59 - 1.91\ \mu m, \tag{5.5}$$

where $\lambda_{\text{cutoff}} = 500 - 600$ nm is the cutoff wavelength, $F = 2.405$ is called the fiber parameter and NA $= 0.12$ the numerical aperture of the fiber. In the case of LG modes, only the Gaussian mode $LG_{0,0}$ has substantial overlap with the fiber mode and therefore is the only mode that propagates in the fiber — neither the $LG_{0,1}$ nor the $LG_{0,-1}$ do. If a $+1$ hologram is placed in front of a single-mode fiber coupler, then only an $LG_{0,-1}$ mode can be coupled into the fiber, as it is transformed into a Gaussian mode (see Fig.5.5). The same can be done with a -1 hologram for detecting an $LG_{0,1}$ mode. By employing a $2:1$ and a $1:1$ beam splitter into the down-conversion arms (hence equally splitting them into three parts) and using the above described mode detection scheme, with a $+1$, a -1 and a hologram that does not do any transformation at all, one can build a probabilistic mode analyzer for the $LG_{0,-1}$, the $LG_{0,0}$ and the $LG_{0,1}$ mode, with $\frac{1}{3}$ probability of success. This probabilistic nature of the analyzers is equivalent to a reduced detection efficiency but otherwise leads to no additional security loopholes.

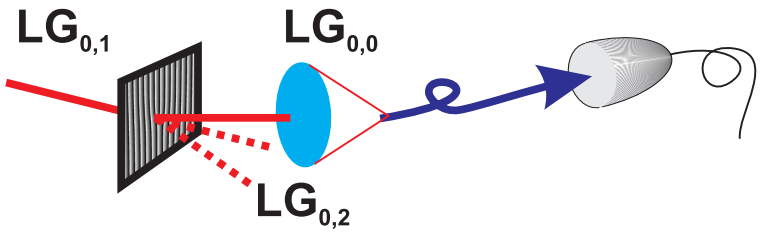


Figure 5.5.: *Analyzing scheme of an $LG_{0,1}$ mode. The incoming mode is transformed into an $LG_{0,0}$ and coupled into a single mode fiber. As only the Gaussian mode propagates in the single mode fiber, this scheme serves as a mode analyzer — with a different setting of the hologram the other modes can be unmistakeably discriminated. The dotted lines show other diffraction orders, which have a low relative intensity due to the blazing of the hologram.*

To obtain the maximally entangled state (5.4), only photons from the energy degenerate SPDC events have to be detected. Therefore, after the mode selection, we built filter bridges that consist of two couplers and an interference filter. An interference filter

relies on the interference of multiple reflected beams. Dielectric material, half a desired wavelength thick, is sandwiched between two high reflectance layers with a different refractive index, hence forming a cavity. An incident light beam is reflected several times from the layers and if these reflections are in phase they constructively interfere and pass through the reflection layer. If, on the other hand, they are out of phase, they destructively interfere and the transmission is reduced to near zero. It is clear, that beams with a wavelength twice the thickness of the dielectric material will be in phase, while others will not. By putting several cavities on top of each other, the transmission of unwanted wavelengths can be made arbitrarily small. Our interference filters have a central wavelength of 702 nm and a bandwidth of ±1 nm.
Six silicon avalanche photo diodes are used as detectors, which are operated at a voltage of 230 V. A single photon hitting the active area of the diode produces a current of secondary electrons and is finally converted into a TTL pulse[1]. To keep the dark count rate of the detector low, which is due to thermal electrons in the diode, it is cooled with a Peltier element and kept at around −25 °C.
As the detectors have different internal delays the outgoing TTL pulses are passed via coaxial cables to a delay box, where they are balanced, and then finally counted in a logic unit. To find the photons from one entangled pair, the respective arrival times have to be compared and if they are within 3 ns, they are counted as coincidences and hence as one pair. The logic unit for the violation of inequality (2.25) consists of such a coincidence counter, where all six signals are counted and the nine possible coincidence count rates are displayed on a computer.

5.4. Experimental QKD Setup

For the quantum key distribution it is necessary to find the settings of the transformation holograms, for which inequality (2.25) is maximally violated. Only then can the two observers A and B produce the secure key by independently and randomly switching between their respective settings.
In order to find the optimal settings for the violation of the Bell inequality the two holograms of A and the two holograms of B are iteratively displaced and the six single and all nine coincidence count rates are recorded. This data is later analyzed to find the settings with a maximal violation of the inequality. The Bell parameter S_3 from the measured count rates is calculated as

$$S_3 = \sum_{k=1}^{4} E_k, \tag{5.6}$$

where the $k = 1, \ldots, 4$ are the four different combinations of hologram settings and the

[1] A TTL pulse is a standard pulse, with a length of 150 ns and an amplitude of 5 V.

E_k's are obtained from explicitly writing out Eq. (2.25):

$$E_1 = \frac{N_{00} + N_{11} + N_{22} - N_{02} - N_{10} - N_{21}}{\sum_{ij} N_{ij}},$$

$$E_2 = \frac{N_{10} + N_{21} + N_{02} - N_{00} - N_{11} - N_{22}}{\sum_{ij} N_{ij}},$$

$$E_3 = \frac{N_{00} + N_{11} + N_{22} - N_{02} - N_{10} - N_{21}}{\sum_{ij} N_{ij}},$$

$$E_4 = \frac{N_{00} + N_{11} + N_{22} - N_{20} - N_{01} - N_{12}}{\sum_{ij} N_{ij}}, \tag{5.7}$$

with N_{ij} $(i, j = 0, 1, 2)$ being the coincidence count rates between observer A measuring an $LG_{0,i}$ and observer B an $LG_{0,j}$ mode for the respective hologram settings k.
To switch between the hologram settings the step motors doing the displacements are computer controlled via a GPIB interface. Therefore a *LabView* program used by A. Vaziri in [67] was adapted and the measurements could be fully automatically run. Typically such a measurement run lasted two days, depending on the number of steps taken with each hologram.

Figure 5.6.: *One of the two logic units, built by dotfast consulting.*

With the optimal settings a_1, a_2 and b_1, b_2 (note that in our case these are combinations of hologram settings) of the transformation holograms at hand, the QKD scheme can be performed. The settings for the key production we choose as $a_3 = b_3 = 0.8$ mm, which means that all four holograms are set to 0.8 mm, as there almost no transformation of the incoming mode is performed and the beam spot is completely on the holograms.
In contrast to the measurement of the Bell inequality, the communication partners A and B now have to be absolutely independent of each other. In principle A and B could be hundreds of kilometers apart and are supposed to be completely separated observers. Therefore we use two distinct computers and logic units (Fig. 5.6). The only way they identify their coincidences is with the help of sync signals — if they detect both, the signal from the other side and a local detection — one entry, 0, 1 or 2 depending on the result of the local detectors, is stored locally in a computer file (see Fig. 5.7). Furthermore, the current settings of the transformation holograms are also written to the data file. The positions of the holograms are computer controlled and the data from the logic units are passed to the computers via USB connections. A *LabView* program (see Appendices A.3 and A.4) automated the random choice of settings, the associated motor alignments, the synchronization of the measurements

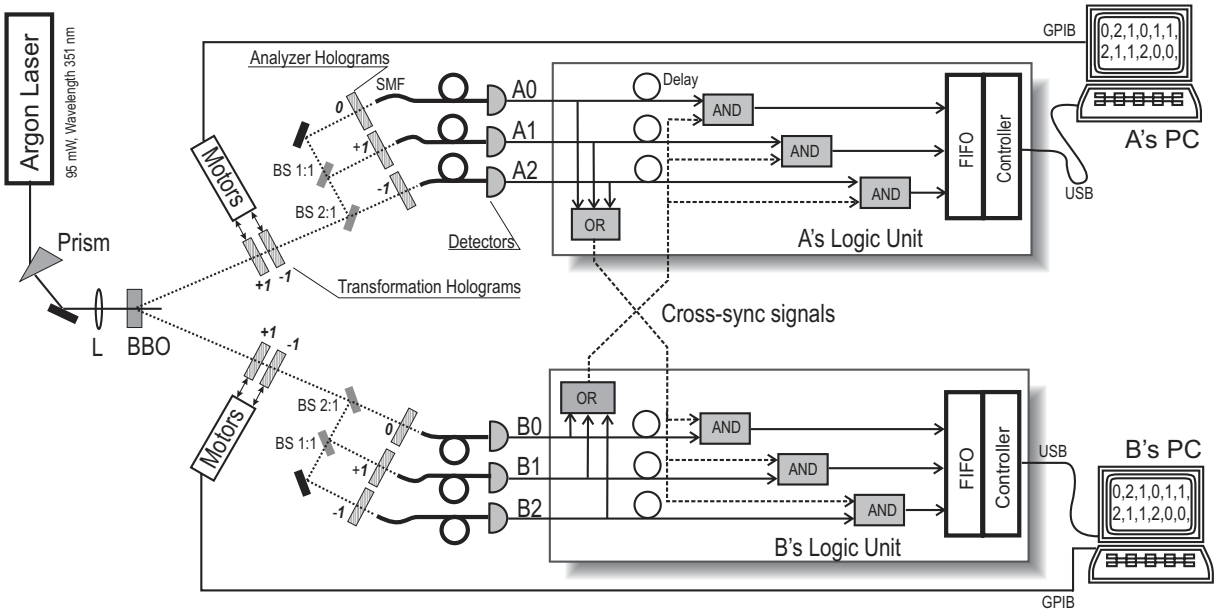


Figure 5.7.: *Illustration of the experimental setup for the QKD with qutrits. The detection signals from the entangled photons are processed in two separate logic units, where the coincidences are only registered via cross-sync signals. Depending on the local measurement result, a value being either* 0, 1 *or* 2 *is passed to the logics first-in first-out buffer (FIFO) and read out by a computer.*

and the readout of the logics FIFO's[2]. The program also synchronized the beginning of writing the measured data to a file.
After a few runs of the quantum key distribution procedure, the two partners A and B have to extract their key and check for the violation of the Bell inequality. A pictogram in Fig. 5.8 shows the scheme of the two parties to retrieve the keys and verify the violation of the inequality.

[2]FIFO is the abbreviation for *first in first out* and is a storage buffer of the detection events for the logical unit. If needed, this buffer can be read out by a computer.

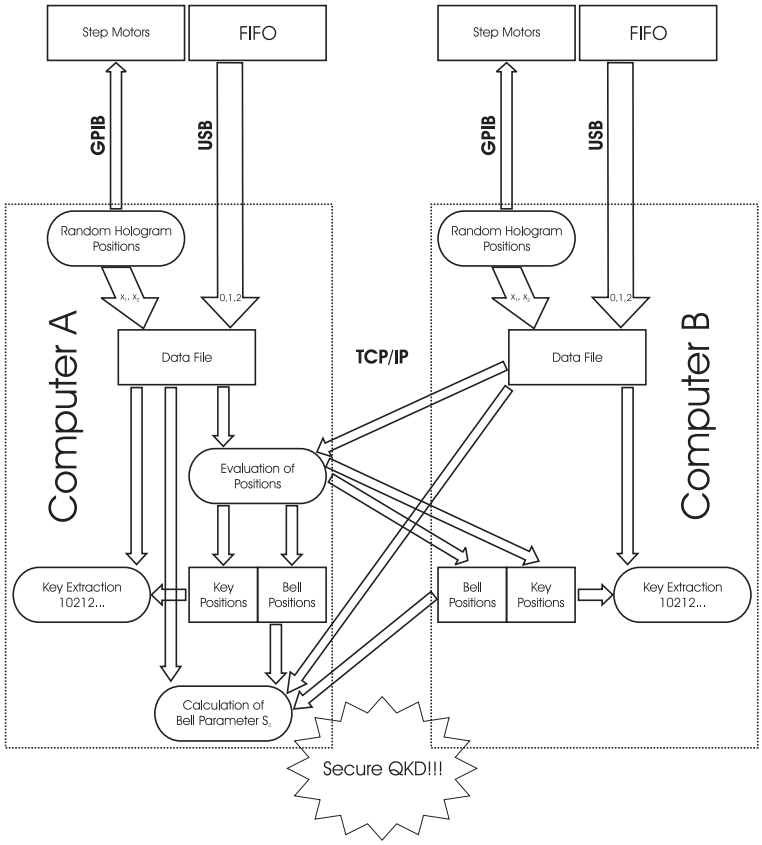


Figure 5.8.: *Scheme of the procedure of A and B extracting a secure key. Both parties write their measurement results from the quantum key distribution to files on their computer. Then observer B publicly announces his list of measurement positions, and A compares them to hers. She will distinguish between suitable combinations for the test of the Bell inequality, positions with perfect correlations for the key and the completely incompatible cases and also announce the results publicly. This basis reconciliation can be performed over any classical public channel. Both know now from which data to extract their key and additionally B broadcasts the data, which is intended for the Bell inequality, on a public channel, and A computes the value of the Bell parameter S_3. If the inequality is violated she will announce, that their quantum key distribution was successful.*

6. Experimental Results

6.1. Violation of the Bell inequality

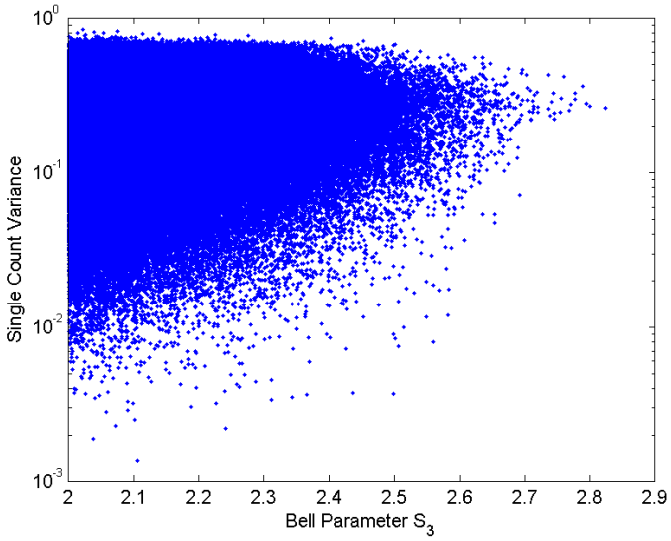


Figure 6.1.: *All violations of the three-dimensional Bell inequality (2.25) for every* 7^{th} *possible combination. The plot shows a total of* 382 415 S_3 *values greater than* 2*, against the maximal variation of the sum of the single counts compared to their mean value.*

The experimentally produced state for the violation of the Bell inequality in order to find the settings for the QKD was almost maximally entangled, with coefficients in (2.21) $\alpha = 0.642$, $\beta = 0.546$ and $\gamma = 0.539$ and the phases $\varphi_0 = \varphi_1 = \varphi_2 = 0$. To find the maximal violation each of the transformation holograms was displaced by ± 1.2 mm from the beam center in 16 equal steps. For every of the 83 521 (17^4) combinations of settings the count rates were integrated over 5 s and written to a file. After analyzing the data a maximal value for S_3 of 2.825 ± 0.052 was found, which is a violation by approximately 16 standard deviations. The errors were calculated assuming a Poissonian distribution of the count rates and therefore taking their square root as the errors. The respective settings in mm from the beam center were 1.05, 0.75 (hologram 1), 1.2, 0.3 (hologram 2) for A and 0.45, 1.05 (hologram 3), 0.15, 0.0 (hologram 4) for B's side. The typical single

S_3	σ	ΔSC	SC_1	SC_2	SC_3	SC_4	SC_5	SC_6
2.825	0.052	22.8 %	88 719	68 137	59 133	112 966	59 580	70 612
			68 265	41 609	32 801	112 706	59 797	70 797
			66 810	48 566	35 132	63 965	53 818	139 382
			88 912	77 645	59 007	64 557	54 902	140 040
2.586	0.056	0.5 %	54 245	119 508	43 071	60 003	131 572	76 864
			67 994	56 311	90 113	60 229	131 729	76 899
			66 412	56 716	90 243	101 692	83 682	84 070
			51 979	118 738	43 589	101 343	84 168	83 625
2.418	0.049	8.9 %	68 277	85 744	103 933	54 413	147 584	77 146
			43 420	104 149	72 637	54 295	148 144	76 990
			41 397	108 276	72 572	106 906	82 317	98 428
			66 511	90 921	102 713	105 133	82 942	97 993

S_3	ΔC	CC_1	CC_2	CC_3	CC_4	CC_5	CC_6	CC_7	CC_8	CC_9	H1 [mm]	H2 [mm]	H3 [mm]	H4 [mm]
2.825	120.5 %	520	51	149	63	415	23	121	114	793	+1.05	+1.2	+0.75	+0.3
		7	249	64	25	13	82	519	54	84	+1.05	+1.2	+1.05	±0.0
		122	129	87	18	178	74	108	37	2067	+0.75	+0.3	+1.05	±0.0
		388	30	228	51	789	421	16	49	2255	+0.75	+0.3	+0.75	+0.3
2.586	52.7 %	286	6	28	12	1362	72	26	236	230	−0.15	−0.6	+0.15	−0.3
		34	780	83	12	78	42	114	197	42	−0.15	−0.6	−1.05	−0.6
		589	75	146	40	288	32	14	101	87	−0.6	−0.75	−1.05	−0.6
		289	64	79	117	560	81	18	20	338	−0.6	−0.75	+0.15	−0.3
2.418	8.3 %	33	1122	57	0	302	18	231	351	90	±0.0	−0.75	+0.75	+0.6
		85	438	132	15	1112	70	132	229	56	±0.0	−0.75	−0.15	−0.45
		774	18	22	76	679	107	6	24	382	−0.6	−0.6	−0.15	−0.45
		892	9	81	28	648	5	4	72	389	−0.6	−0.6	+0.75	+0.6

Table 6.1.: *Experimental data for three exemplary Bell parameters S_3, violating the Bell inequality by several standard deviations, and the respective variation of the single and coincidence count rates ΔSC and ΔC, respectively. The individual single counts per 5 s SC_i for all six detectors are shown and in addition the nine coincidence count rates CC_j. The first S_3 value shows a large variation of the sum of SC_i, ΔSC, and of the sum of CC_j, ΔC, whereas the third is the lowest in both jointly. The Bell parameters are computed from the CC_j's according to formula (5.6). Finally, the positions of the transformation holograms for the respective values of S_3, in mm from the beam center, are shown.*

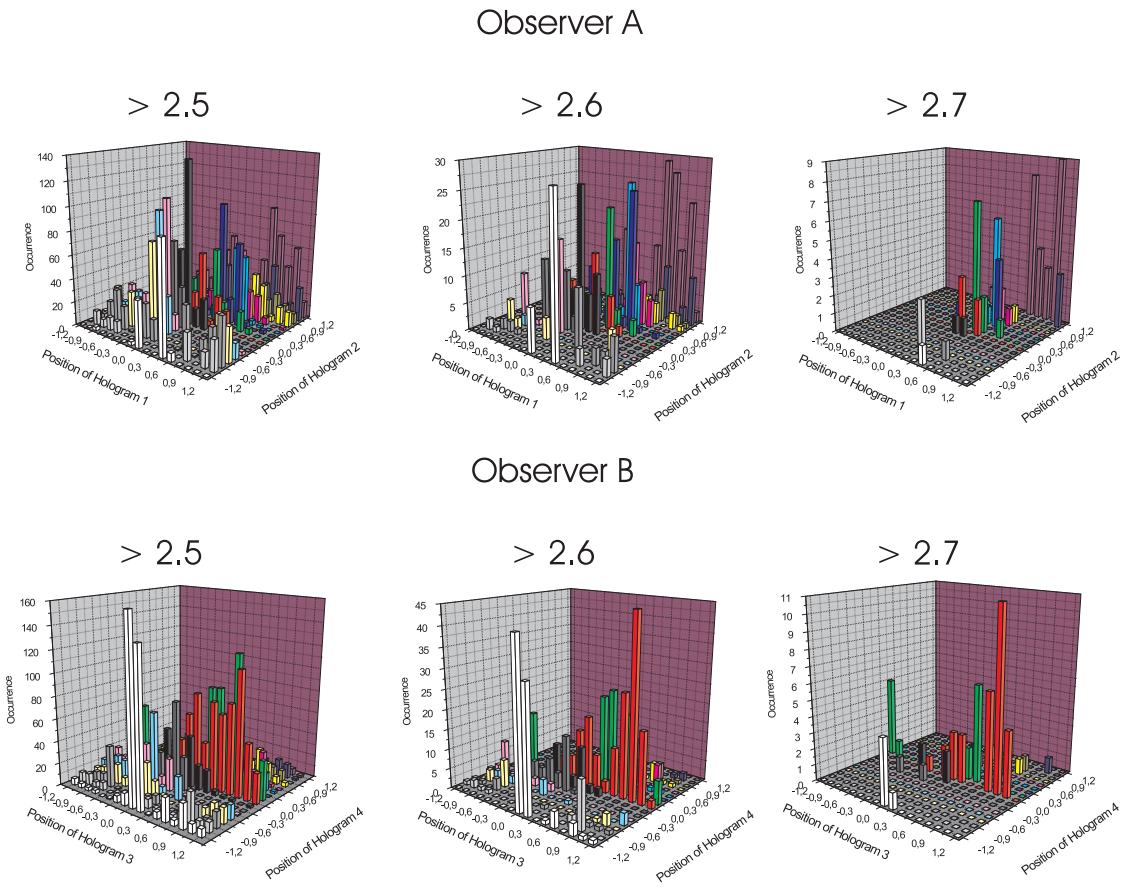


Figure 6.2.: *These plots show the occurrence of the transformation hologram positions for different values of S_3. For both observers A and B, a certain convergence of the positions to small areas for higher S_3 values can be observed. The colors are a guide for the eye only.*

count rates were around 19 000 s^{-1} and the coincidences of the perfect correlations about 250 s^{-1} (see Fig. 6.1 and Table 6.1), with a background of about 7.4 %, i.e. the total coincidence counts in the unwanted channels. In addition we have checked the variation of the sum of the single and coincidence count rates for the different hologram positions, which should ideally be zero. Therefore, the sum of the counts for the four different settings was taken and the minimal was subtracted from the maximal value and divided by the mean. For the settings of maximal violation they were approximately 22.8 % and 120.5 %, respectively. In terms of these variances the settings for the maximal violation were not optimal, which might be due to a relatively high background of modes with a non-zero index p and imperfections in the alignment of the transformation holograms. In Table 6.1 some violations of (2.25) with a smaller variance of the single and coincidence

count rates and the corresponding hologram positions are shown. Figure 6.1 is a plot of all evaluated Bell parameters $S_3 > 2$, with their respective single count variances. As the data file was too large to make every possible combination of S_3, only every seventh combination was calculated. Nevertheless a total of 382 415 violations of the inequality were found. At the moment a calculation of all possible S_3 values is running on the University of Vienna's *Schrödinger* cluster, which is a computer cluster with 240 Intel Pentium 840 'Prescott' 64 Bit CPU's. With a single Intel P4 processor it would take several months to finish the calculations. The program for analyzing the violation was written in *Matlab* and can be found in Appendix A.2.

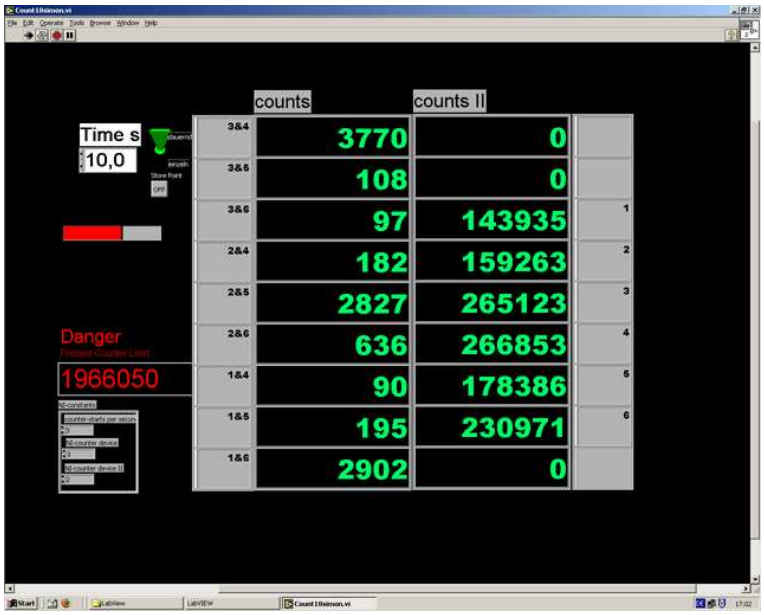


Figure 6.3.: *Typical count rates per* 10 *s for the experimental violation of the Bell inequality and the experimental qutrit quantum key distribution. The left column shows the coincidences, where the three perfect correlated count rates are easily distinguished from the rest. In the right column are the single counts of the six detectors.*

6.2. Key Generation

In the first realization of our qutrit QKD scheme each measurement lasted 1 s and the step motors needed an additional 5 s to align. After approximately 15 minutes of key distribution, the data was analyzed according to the pictogram shown in Fig. 5.8. The analysis of the recorded data yielded a Bell parameter $S_3 = 2.688 \pm 0.171$, which represents a clear violation of local realism and ascertained the successful completion of the protocol. We extracted keys of a length of 150 trits for A and B separately (the keys

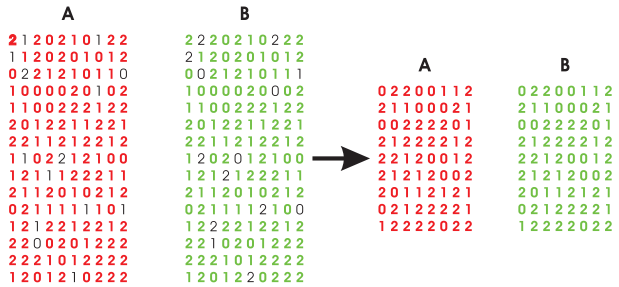


Figure 6.4.: *On the left are the sifted keys obtained by observers A and B via three-dimensional quantum key distribution. The bold (colored) numbers are the correct trits while the plain numbers are errors. The ratio of correct key to total key is* 90.7 %*, i.e. from a total key of* 150 *trits,* 136 *entries were the same for A and B. The security of this key is ascertained by the violation of the Bell inequality (2.25), with $S_3 = 2.688 \pm 0.171$. On the right are the keys after error correction, which is done by checking the parity of blocks of three trits. Due to the correction, the keys are reduced to a length of* 72 *trits.*

are shown in Fig. 6.4). Out of the 150 trits 14 were errors, which corresponds to a QTER (Quantum Trit Error Rate) of 9.3 %. This demonstrates the successful key distribution, since the error rate is well below the maximal allowed noise ratio and additionally Bell's inequality (2.25) is violated.

Although we generated two keys, with a small QTER, we encountered several problems with our experimental setup. The most difficult to overcome was the synchronization of the measurements of observers A and B. Despite using the same software on both computers, we had to deal with a chitter of a few FIFO entries. A further problem was that apparently one of the two logics dropped FIFO entries from time to time, which resulted in displacements of the detection events. It was impossible to correct for both problems and we only managed to reduce them to a minimum with a tricky adaption of the software. If one of the problems occurred, it inevitably induced errors and thus artificially worsened our QKD protocol. To obtain the final keys with a relatively small error rate, various attempts of QKD had to be made. For future applications, the logics could be replaced with time tagging cards, which give each measurement result a unique time stamp, and hence the above mentioned problems could be completely eliminated.

In order to illustrate the quality of our generated keys and a possible application of QKD, a small message will be encoded with the key produced on A's side, and subsequently decoded with B's key. Therefore, we encode the alphabet into strings of three trits using the conversion table 6.2.

A text message can then be encoded into a string of 0, 1 and 2. This row of numbers is encrypted by taking the key of observer A and adding to each trit of the message a trit of the key, modulo 3. The encrypted text is now completely random to anyone trying to read it, like an eavesdropper E. Only observer B can reverse the encryption using his

Character	Code	Character	Code	Character	Code
A	000	**J**	100	**S**	200
B	001	**K**	101	**T**	201
C	002	**L**	102	**U**	202
D	010	**M**	110	**V**	210
E	011	**N**	111	**W**	211
F	012	**O**	112	**X**	212
G	020	**P**	120	**Y**	220
H	021	**Q**	121	**Z**	221
I	022	**R**	122	␣	222

Table 6.2.: *To each letter in the alphabet we assign a unique string of three trits. Interestingly three trits suffice to represent all characters of the Latin alphabet plus one additional character.*

key and obtains, ideally, the exact message that A originally wrote. This procedure is shown in Table 6.3 for a short message.

Original Text	**T**	**H**	**E**	␣	**R**	**E**	**S**	**U**	**L**	**T**	␣	**I**	**S**	␣	**F**	**O**	**R**	**T**	**Y**	␣	**T**	**W**	**O**
Original Code	201	021	011	222	122	011	200	202	102	201	222	022	200	222	012	112	122	201	220	222	201	211	112
Key A	022	001	122	110	002	100	222	201	212	222	122	212	001	221	212	002	201	121	210	212	222	122	222
Cipher	220	022	100	002	121	111	122	100	011	120	011	201	201	110	221	111	020	022	100	101	120	000	001
E's Text	**Y**	**I**	**J**	**C**	**Q**	**N**	**R**	**J**	**E**	**P**	**E**	**T**	**T**	**M**	**Z**	**N**	**G**	**I**	**J**	**K**	**P**	**A**	**B**
Cipher	220	022	100	002	121	111	122	100	011	120	011	201	201	110	221	111	020	022	100	101	120	000	001
Key B	022	001	122	110	002	100	222	201	212	222	122	212	001	221	212	002	201	121	210	212	222	122	222
Decrypted Code	201	021	011	222	122	011	200	202	102	201	222	022	200	222	012	112	122	201	220	222	201	211	112
Decrypted Text	**T**	**H**	**E**	␣	**R**	**E**	**S**	**U**	**L**	**T**	␣	**I**	**S**	␣	**F**	**O**	**R**	**T**	**Y**	␣	**T**	**W**	**O**

Table 6.3.: *Encryption and decryption of a short, important message sent between the two partners A and B using the error corrected key obtained via the three-dimensional quantum key distribution. An eavesdropper trying to intercept the message only gets random characters and hence cannot obtain any information on the original text, whereas observer B uses his key to decipher the original message.*

7. Conclusion and Outlook

In this thesis we described the first experimental qutrit quantum key distribution. Two completely independent parties A and B produce keys, while violating a three-dimensional Bell inequality by more than 4 standard deviations. The sifted keys had an error rate of approximately 10 %. The effective key rate we achieved is rather low, but this will change in the near future with the implementation of a different basis transformation such as by a spatial light modulator, which allows transformation rates of a few Hz (for an extensive introduction to spatial light modulators and their possible application in OAM based quantum key distribution see [62]). In addition, with a biased choice of the positions of the transformation holograms, the key production rate could be increased.

A further challenge is the distortion-free transmission of OAM encoded photons over large distances. The possibilities of free-space and fiber links are still under investigation, since atmospheric turbulences and mode crosstalk in fibers have to be overcome. Gibson et al. already demonstrated a free-space link of photons with OAM over a distance of 15 m [39]. Additionally, encoding higher dimensions into other degrees of freedom, such as time bins [64], might also be considered. For cryptographic schemes based on single qutrits, similar to the BB84 scheme, transformations between mutually unbiased bases (MUBs) are required. Further investigations of such transformations with our holographic scheme are under investigation and ultimately with an interferometric approach arbitrary $SU(3)$ transformations could be possible to achieve. In contrast to the polarization degree of freedom, in principle there is no limitation on the dimension of the two photon entanglement and therefore an extension of the qutrit to a more general qudit case also seems feasible.

The work presented in this thesis is intended to be published in a scientific journal. At the moment it is still in the internal review process but will be submitted soon. Additionally, a second publication on non-local realistic (in the sense EPR discussed local realism) theories is about to be submitted to a journal. In this paper a bound on a certain class of non-local hidden-variable theories is derived and shown to be at variance with quantum theory and experimental evidence.

A. Computer Programs

A.1. Numerical Simulations with three Holograms

Overlap integral definition / numeric definition

```
atanspec[x_, y_] = If[x == 0.0 && y == 0.0, 0, ArcTan[x, y]] (* zur Vermeidung von Warnmeldungen *)
```

```
overlap[li_, lo_, m_, x0_, y0_, x_, y_] =
  2 / (π √(Abs[li]! Abs[lo]!)) (2 (x^2 + y^2))^((Abs[li]+Abs[lo])/2) e^(-2 (x^2+y^2)+i ((li-lo) atanspec[x,y]+m atanspec[x-x0,y-y0]))
```

```
overlapnum =
 Compile[{{li, _Integer}, {lo, _Integer}, {m, _Integer}, {x0, _Real}, {y0, _Real}, {x, _Real}, {y, _Real}},
  2 / (π √(Abs[li]! Abs[lo]!)) If[li + lo == 0, 1, (2 (x^2 + y^2))^((Abs[li]+Abs[lo])/2)] e^(-2 (x^2+y^2)+i ((li-lo) atanspec[x,y]+m atanspec[x-x0,y-y0]))]
```

■ **Zusätzliche Definitionen**

```
Off[NIntegrate::slwcon]
```

```
overlapint[li_, lo_, m_, x0_, y0_] :=
 NIntegrate[overlapnum[li, lo, m, x0, y0, x, y], {x, -3, 3}, {y, -3, 3}, AccuracyGoal → 3, PrecisionGoal → 3]
```

Matrixkonstruktion - Versuch einer MUB Trafo

Berechnung der Matrixelemente der Multiplikation der zwei HologrammMatrizen und Ausgabe von U und U'U=1 Überprüfung. Weiters werden die momentanen Positionen auch ins File geschrieben.

```
(* Berechnung und Ausgabe von U=f2*f1 (mat1),
 U' U (mat2) und der Orthogonalität der einzelnen Basisvektoren (mat3) *)

mat1 = {α, β, γ, ϵ, ζ, η, ϑ, κ, λ, iAl, jAl, kAl};
mat2 = {Abs[α α1 + β β1 + γ γ1], Abs[α ϵ1 + β ζ1 + γ η1],
   Abs[α ϑ1 + β κ1 + γ λ1], Abs[ϵ α1 + ζ β1 + η γ1], Abs[ϵ ϵ1 + ζ ζ1 + η η1], Abs[ϵ ϑ1 + ζ κ1 + η λ1],
   Abs[ϑ α1 + κ β1 + λ γ1], Abs[ϑ ϵ1 + κ ζ1 + λ η1], Abs[ϑ ϑ1 + κ κ1 + λ λ1], iAl, jAl, kAl};
mat3 = {Abs[α1 β + ϵ1 ζ + ϑ1 κ], Abs[β1 γ + ζ1 η + κ1 λ], Abs[γ1 α + η1 ϵ + λ1 ϑ], iAl, jAl, kAl};

(* Berechnung aller Koeffizienten und ablegen selbiger in Listen *)

z = 10 (* 10* +/- Grenze für Verschiebung der Hologramme *)
zA = (2 z + 1) ^2 (* Anzahl der Iterationen in den For-Schleifen - +1, weil Liste bei [[1]] beginnt *)


a = Flatten[Table[overlapint[-1, -1, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];
b = Flatten[Table[overlapint[-1, 0, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];
c = Flatten[Table[overlapint[-1, 1, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];
d = Flatten[Table[overlapint[0, 0, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];
e = Flatten[Table[overlapint[0, 1, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];
f = Flatten[Table[overlapint[0, 2, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];
g = Flatten[Table[overlapint[1, 1, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];
h = Flatten[Table[overlapint[1, 2, 1, (x1 / 10), (y1 / 10)], {x1, -z, z}, {y1, -z, z}]];


i = Flatten[Table[overlapint[-1, -3, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
j = Flatten[Table[overlapint[-1, -2, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
k = Flatten[Table[overlapint[-1, -1, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
l = Flatten[Table[overlapint[0, -2, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
u = Flatten[Table[overlapint[0, -1, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
n = Flatten[Table[overlapint[0, 0, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
o = Flatten[Table[overlapint[1, -1, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
p = Flatten[Table[overlapint[1, 0, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
q = Flatten[Table[overlapint[1, 1, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
r = Flatten[Table[overlapint[2, 0, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];
s = Flatten[Table[overlapint[2, 1, -2, (x2 / 10), (y2 / 10)], {x2, -z, z}, {y2, -z, z}]];


t = Flatten[Table[overlapint[-3, -1, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
v = Flatten[Table[overlapint[-2, -1, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
w = Flatten[Table[overlapint[-2, 0, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
a1 = Flatten[Table[overlapint[-1, -1, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
b1 = Flatten[Table[overlapint[-1, 0, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
c1 = Flatten[Table[overlapint[-1, 1, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
d1 = Flatten[Table[overlapint[0, 0, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
e1 = Flatten[Table[overlapint[0, 1, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];
g1 = Flatten[Table[overlapint[1, 1, 1, (x3 / 10), (y3 / 10)], {x3, -z, z}, {y3, -z, z}]];


(* Matrixelemente der 3 x3 Matrix f3*f2*f1 und c.c. *)

α = Flatten[Table[a[[iA]] i[[jA]] t[[kA]] + v[[kA]] (a[[iA]] j[[jA]] + b[[iA]] l[[jA]]) +
     a1[[kA]] (a[[iA]] k[[jA]] + b[[iA]] u[[jA]] + o[[jA]] c[[iA]]), {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
α1 = Conjugate[α];
β = Flatten[Table[v[[kA]] d[[iA]] l[[jA]] + a1[[kA]] (d[[iA]] u[[jA]] + e[[iA]] o[[jA]]),
    {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
β1 = Conjugate[β];
γ = Flatten[Table[a1[[kA]] g[[iA]] o[[jA]], {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
γ1 = Conjugate[γ];
ϵ = Flatten[
   Table[w[[kA]] (a[[iA]] j[[jA]] + b[[iA]] l[[jA]]) + b1[[kA]] (a[[iA]] k[[jA]] + b[[iA]] u[[jA]] + o[[jA]] c[[iA]]) +
     d1[[kA]] (b[[iA]] n[[jA]] + c[[iA]] p[[jA]]), {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
ϵ1 = Conjugate[ϵ];
ζ = Flatten[Table[w[[kA]] d[[iA]] l[[jA]] + b1[[kA]] (d[[iA]] u[[jA]] + e[[iA]] o[[jA]]) +
     d1[[kA]] (d[[iA]] n[[jA]] + e[[iA]] p[[jA]] + f[[iA]] r[[jA]]), {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
ζ1 = Conjugate[ζ];
η = Flatten[Table[b1[[kA]] g[[iA]] o[[jA]] + d1[[kA]] (g[[iA]] p[[jA]] + h[[iA]] r[[jA]]),
    {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
η1 = Conjugate[η];
```

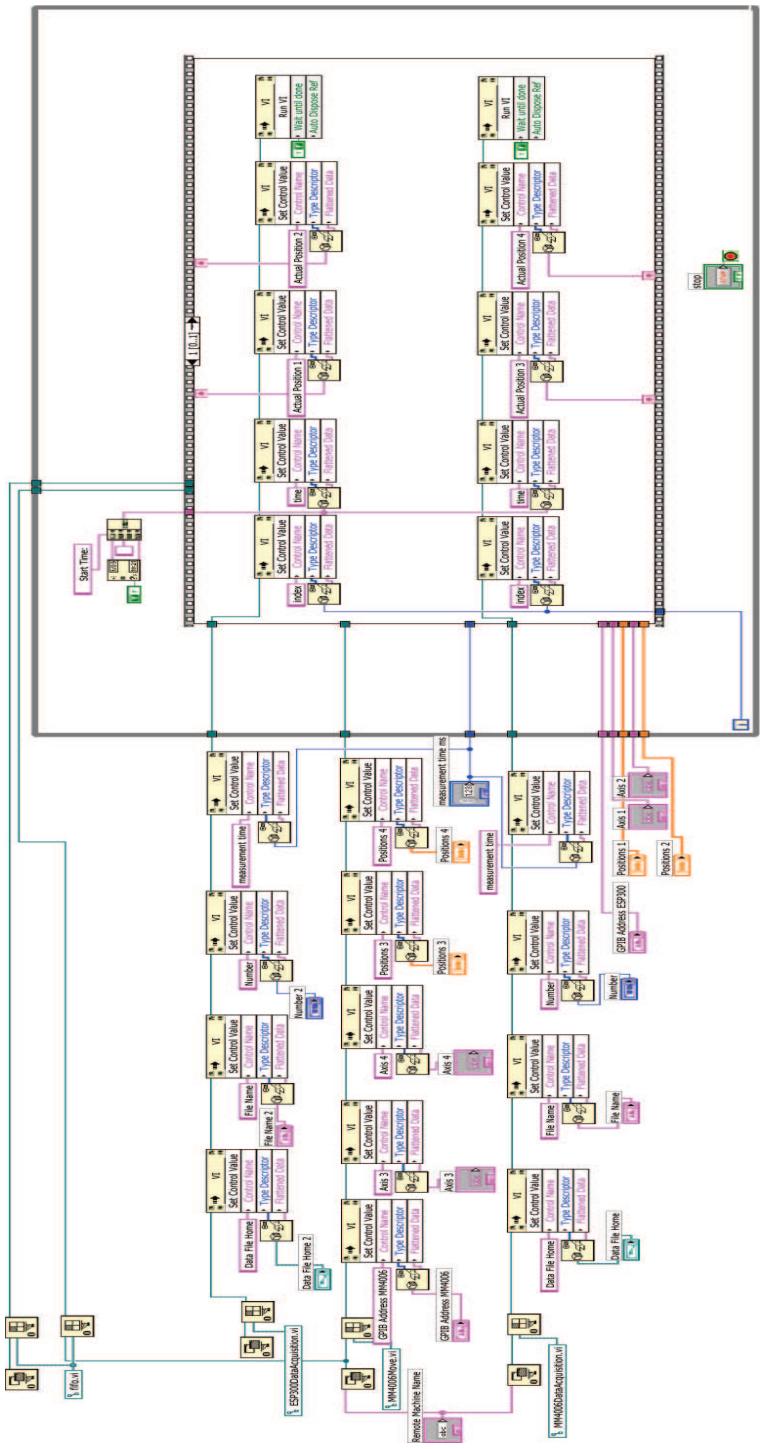
```
θ = Flatten[
   Table[c1[[kA]] (a[[iA]] k[[jA]] + b[[iA]] u[[jA]] + o[[jA]] c[[iA]]) + e1[[kA]] (b[[iA]] n[[jA]] + c[[iA]] p[[jA]]) +
     g1[[kA]] c[[iA]] q[[jA]], {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
θ1 = Conjugate[θ];
κ = Flatten[
   Table[c1[[kA]] (d[[iA]] u[[jA]] + e[[iA]] o[[jA]]) + e1[[kA]] (d[[iA]] n[[jA]] + e[[iA]] p[[jA]] + f[[iA]] r[[jA]]) +
     g1[[kA]] (e[[iA]] q[[jA]] + f[[iA]] s[[jA]]), {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
κ1 = Conjugate[κ];
λ = Flatten[Table[c1[[kA]] g[[iA]] o[[jA]] + e1[[kA]] (g[[iA]] p[[jA]] + h[[iA]] r[[jA]]) +
     g1[[kA]] (g[[iA]] q[[jA]] + h[[iA]] s[[jA]]), {iA, 1, zA, 1}, {jA, 1, zA, 1}, {kA, 1, zA, 1}]];
λ1 = Conjugate[λ];


(* Ausgabe der Zähler in Listen *)
For[σ = 1, σ ≤ zA, σ = σ + 1, ξ[σ] = Table[σ, {μ, 1, zA^2, 1}]];
iAl = Flatten[Array[ξ, zA]];

For[σ = 1, σ ≤ zA, σ = σ + 1, ψ[σ] = Table[σ, {μ, 1, zA, 1}]];
For[σ = 1, σ ≤ zA, σ = σ + 1, ρ[σ] = Flatten[Array[ψ, zA]]];
jAl = Flatten[Array[ρ, zA]];

For[σ = 1, σ ≤ zA, σ = σ + 1, χ[σ] = Table[μ, {μ, 1, zA, 1}]];
For[σ = 1, σ ≤ zA, σ = σ + 1, τ[σ] = Flatten[Array[χ, zA]]];
kAl = Flatten[Array[τ, zA]];


Export["h:\\matrix.mat", mat1]
Export["h:\\unitarity.mat", mat2]
Export["h:\\orthogonality.mat", mat3]
```

A.2. Calculation of S_3

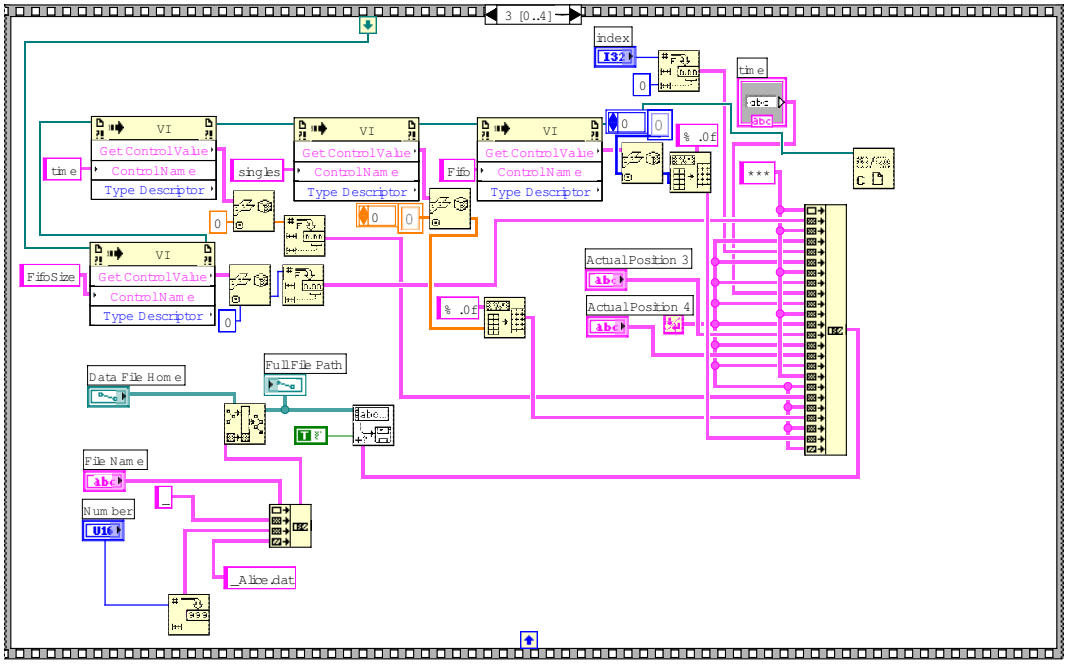
```
%check for Violation of 3-dimensional Bell inequality & check the variances
%of single and coincidence count rates

clear all

tic

count=0;
zeit=0;

load runNEU_1.dat -ascii
Data1=runNEU_1;


base2=17^2;
base3=17^3;
prozent=0;
prozent_vorher=0;
prozent_scale=100/(length(Data1)*length(Data1));

% Schreiben einer Tabelle mit allen Werten für die Berechnung des S Wertes (xx1(a) = xx3(a))
for a=1:1:length(Data1)
    xx1(a) = (Data1(a,5)+Data1(a,13)+Data1(a,9)-Data1(a,6)-Data1(a,11)-Data1(a,10))/sum(Data1(a,5:13));
    xx2(a) = (Data1(a,11)+Data1(a,10)+Data1(a,6)-Data1(a,5)-Data1(a,13)-Data1(a,9))/sum(Data1(a,5:13));
    xx4(a) = (Data1(a,5)+Data1(a,13)+Data1(a,9)-Data1(a,8)-Data1(a,7)-Data1(a,12))/sum(Data1(a,5:13));
end

% Tabelle mit Fehlerfortpflanzung
for b=1:1:length(Data1)
    sx1(b) = (Data1(b,5)+Data1(b,13)+Data1(b,9)+Data1(b,6)+Data1(b,11)...
        +Data1(b,10))/((sum(Data1(b,5:13)))^2);
    sx2(b) = ((Data1(b,5)+Data1(b,13)+Data1(b,9)-Data1(b,6)-Data1(b,11)...
        -Data1(b,10))^2)*(sum(Data1(b,5:13)))/(sum(Data1(b,5:13))^4);
    sx3(b) = (Data1(b,11)+Data1(b,10)+Data1(b,6)+Data1(b,5)+Data1(b,13)...
        +Data1(b,9))/((sum(Data1(b,5:13)))^2);
    sx4(b) = ((Data1(b,11)+Data1(b,10)+Data1(b,6)-Data1(b,5)-Data1(b,13)...
        -Data1(b,9))^2)*(sum(Data1(b,5:13)))/(sum(Data1(b,5:13))^4);
    sx5(b) = (Data1(b,5)+Data1(b,13)+Data1(b,9)+Data1(b,6)+Data1(b,11)...
        +Data1(b,10))/((sum(Data1(b,5:13)))^2);
    sx6(b) = ((Data1(b,5)+Data1(b,13)+Data1(b,9)-Data1(b,6)-Data1(b,11)...
        -Data1(b,10))^2)*(sum(Data1(b,5:13)))/(sum(Data1(b,5:13))^4);
    sx7(b) = (Data1(b,5)+Data1(b,13)+Data1(b,9)+Data1(b,8)+Data1(b,7)...
        +Data1(b,12))/((sum(Data1(b,5:13)))^2);
    sx8(b) = ((Data1(b,5)+Data1(b,13)+Data1(b,9)-Data1(b,8)-Data1(b,7)...
        -Data1(b,12))^2)*(sum(Data1(b,5:13)))/(sum(Data1(b,5:13))^4);
end

for ii=0:7:(length(Data1)-1)
    for jj=ii+1:7:(length(Data1)-1)
        zeit=zeit+1;

        s1=mod(ii,17); s2=floor(ii/17);
        t1=mod(s2,17); t2=floor(s2/17);
        u1=mod(t2,17); u2=floor(t2/17);
        v1=mod(u2,17); v2=floor(u2/17);

        w1=mod(jj,17); w2=floor(jj/17);
        x1=mod(w2,17); x2=floor(w2/17);
        y1=mod(x2,17); y2=floor(x2/17);
        z1=mod(y2,17); z2=floor(y2/17);
```

```
        k=v1*base3+u1*base2+x1*17+w1+1;
        l=z1*base3+y1*base2+t1*17+s1+1;
        i=ii+1;
        j=jj+1;

        %Berechnung des S Wertes
        x = xx1(i)+xx2(k)+xx1(j)+xx4(l);

        %Berechnung der Varianz der Single & CC counts
        singles=[sum(Data1(i,16:21)) sum(Data1(j,16:21)) sum(Data1(k,16:21)) sum(Data1(l,16:21))];
        vars=(max(singles)-min(singles))/mean(singles);

        cc=[sum(Data1(i,5:13)) sum(Data1(j,5:13)) sum(Data1(k,5:13)) sum(Data1(l,5:13))];
        varc=(max(cc)-min(cc))/mean(cc);

        if ((x>2)&(vars<0.1)&(varc<0.1))

        prozent=ii*jj*prozent_scale;

        if prozent-prozent_vorher > 0.01
            prozent
            prozent_vorher=prozent;
        end

        %Fehlerfortpflanzung
        sigmax = sqrt(sx1(i)+sx2(i)+sx3(k)+sx4(k)+sx5(j)+sx6(j)+sx7(l)+sx8(l));

        count=count+1;

        %Ausgabe
        Bell3D(count,:)=[i j k l x sigmax vars varc];

        end
        clear x
    end
end


save Bell3D_withCC_13.dat -ascii Bell3D
semilogy  (Bell3D(:,5),Bell3D(:,7),'b.')
semilogy  (Bell3D(:,5),Bell3D(:,8),'r.')

toc
```

A.3. LabView Program for Synchronized Measurements



A.4. LabView Program for Data Acquisition



B. Acknowledgements

Only the help and support of many people made this thesis an "element of reality" — without them it would have been much more difficult, even impossible and certainly not as much fun as it finally was. Therefore, I would like to thank:

Prof. Anton Zeilinger, who eventually made this work possible. I am deeply grateful for the opportunity of working in his group, along with outstanding physicists doing excellent and interesting research.

My supervisor Thomas Jennewein, for the idea of the thesis, for his time, the encouragement and all the help with small and big problems.

Markus Aspelmeyer for being my clandestine advisor, giving me lots of insights, making physics the fun it is and for the extra activities, which not always involved too much physics after all.

Gregor Weihs, who always had time, no matter what, to answer even the stupidest questions, thus giving me the feeling of being welcome and helping me with better understanding my work.

I could and should thank many more people directly involved in my thesis but I leave it with a general thank to all members of the Zeilinger group, who made the work easy by providing an excellent working atmosphere, with plenty of interesting discussions and free time activities. Additionally I would like to thank Jay Lawrence, Tomasz Paterek and Paulo H. S. Ribeiro.

Besides the people on the physics side of my life, I would like to thank all my friends for their patience and for understanding me and my priorities. Especially Leonie, Ingo and my brother Daniel, who definitely had the biggest burden to carry. I am also grateful to all my parents and brothers and sisters — real, half, step and Brazilian — for their love and support. Without whom I would not be where I finally ended up.

C. Curriculum Vitae

Simon Gröblacher
Glockengasse 14/6
A-1020 Wien

Birthday: November 21st, 1980
e-mail: simon.groeblacher@univie.ac.at

Educational History

10/2004 – 12/2005	Diploma Thesis with Prof. Anton Zeilinger: „Experimental Investigation of Quantum Communication Protocols in Higher Dimensions“
01/2004 – 09/2004	Studies at the Universidade Federal do Rio de Janeiro, RJ, Brazil, in the quantum optics group of Prof. Paulo H. S. Ribeiro
08/2003 – 09/2003	„Investigation of the efficiency of the Skim-Programs at BELLE“ for the Institute of High Energy Physics of the Austrian Academy of Sciences at the BELLE-Experiment, KEK, Tsukuba, Ibaraki, Japan
10/2001 –	Physics studies at the University of Vienna
10/2000 –	Astronomy studies at the University of Vienna Portuguese & Spanish studies at the University of Vienna
10/1999 – 09/2000	Philosophy and Pedagogic studies at the University of Vienna
06/1999	Matura at the Bundesrealgymnasium Krems a. d. Donau with honors
07/1997 – 06/1998	Exchange year at the Colégio Sagrado Coração de Jesus, Ijuí, Rio Grande do Sul, Brazil, with AFS (American Field Service)
09/1991 – 05/1999	Bundesrealgymnasium Krems a. d. Donau
09/1987 – 06/1991	Volksschule Krems Lerchenfeld

Personal History

04/2005 –	System administrator at the Institut für Experimentalphysik
10/2004 –	Photographer for Vienna Online
02/2001 – 09/2001	European Voluntary Service, Project: „Märjamaa Cultural House“, Raplamaa, Estonia
06/2001	Leader of the Project „Uusaja Workcamp“, Hiiumaa, Estonia
07/1998 – 07/2002	Volunteer for AFS Austria

Qualifications

Languages:	German:	mother tongue
	Portuguese:	fluent, written and spoken
	English:	fluent, written and spoken
	Spanish:	good knowledge
	French:	average knowledge
	Estonian:	basic knowledge

Bibliography

[1] A. Acín, T. Durt, N. Gisin and J. I. Latorre, *Quantum non-locality in two three-level systems*, Phys. Rev. A, **65** (2002), p. 052325. 13

[2] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw and J. P. Woerdman, *Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes*, Phys. Rev. A, **45** (1992), pp. 8185–8189. 23

[3] J. Arlt, *Applications of Laguerre-Gaussian beams and Bessel beams to both nonlinear optics and atom optics*, PhD Thesis, School of Physics and Astronomy, University of St Andrews, 1999. 28

[4] A. Aspect, J. Dalibard and G. Roger, *Experimental Test of Bell's Inequalities Using Time-Varying Analyzers*, Phys. Rev. Lett., **49** (1982), pp. 1804–1807. 6, 10

[5] A. Aspect, P. Grangier and G. Roger, *Experimental Tests of Realistic Local Theories via Bell's Theorem*, Phys. Rev. Lett., **47** (1981), pp. 460–463. 10

[6] M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther and A. Zeilinger, *Long-Distance Free-Space Distribution of Quantum Entanglement*, Science, **301** (2003), pp. 621–623. 6

[7] H. Bechmann-Pasquinucci and A. Peres, *Quantum Cryptography with 3-State Systems*, Phys. Rev. Lett., **85** (2000), pp. 3313–3316. 19

[8] M. W. Beijersbergen, L. Allen, H. E. L. O. van der Veen and J. P. Woerdman, *Astigmatic laser mode converters and transfer of orbital angular momentum*, Opt. Commun., **96** (1993), pp. 123–132. 27

[9] M. W. Beijersbergen, R. P. C. Coerwinkel, M. Kristensen and J. P. Woerdman, *Helical-wavefront laser beams produced with a spiral phaseplate*, Opt. Commun., **112** (1994), pp. 321–327. 29

[10] J. S. Bell, *On the Einstein Podolsky Rosen Paradox*, Physics, **1** (1964), pp. 195–200. 8

[11] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, *Experimental quantum cryptography*, Journal of Cryptology, **5** (1992), pp. 3–28. 17

[12] C. H. Bennett and G. Brassard, *Quantum cryptography: Public Key Distribution and coin-tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (1984), pp. 175–179. 4, 15

[13] C. H. Bennett and G. Brassard, *Quantum public key distribution system*, IBM Tech. Discl. Bull., **28** (1985), pp. 3153–3163. 4, 15

[14] R. A. Beth, *Mechanical Detection and Measurement of the Angular Momentum of Light*, Phys. Rev., **50** (1936), pp. 115–125. 23

[15] D. Bohm, *A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I*, Phys. Rev., **85** (1952), pp. 166–179. 8

[16] D. Bohm, *A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. II*, Phys. Rev., **85** (1952), pp. 180–193. 8

[17] N. Bohr, *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?*, Phys. Rev., **48** (1935), pp. 696–702. 8

[18] M. Bourennane, A. Karlsson and G. Björk, *Quantum key distribution using multilevel encoding*, Phys. Rev. A, **64** (2001), p. 012306. 19, 20

[19] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, *Experimental quantum teleportation*, Nature, **390** (1997), pp. 575–579. 11

[20] Č. Brukner, M. Żukowski and A. Zeilinger, *Quantum Communication Complexity Protocol with Two Entangled Qutrits*, Phys. Rev. Lett., **89** (2002), p. 197901. 11

[21] D. Bruss, *Optimal Eavesdropping in Quantum Cryptography with Six States*, Phys. Rev. Lett., **81** (1998), pp. 3018–3021. 18, 20

[22] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson and C. M. Simmons, *Practical Free-Space Quantum Key Distribution over 1 km*, Phys. Rev. Lett., **81** (1998), pp. 3283–3286. 17

[23] D. P. Caetano, M. P. Almeida, P. H. S. Ribeiro, J. A. O. Huguenin, B. C. dos Santos and A. Z. Khoury, *Conservation of orbital angular momentum in stimulated down-conversion*, Phys. Rev. A, **66** (2002), p. 041801(R). 37

[24] N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, *Security of Quantum Key Distribution Using d-level Systems*, Phys. Rev. Lett., **88** (2002), p. 127902. 18, 19, 20

[25] J. F. Clauser and M. A. Horne, *Experimental consequences of objective local theories*, Phys. Rev. D, **10** (1974), pp. 526–535. 10

[26] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Phys. Rev. Lett., **23** (1969), pp. 880–884. 9, 10

[27] D. Collins, N. Gisin, N. Linden, S. Massar and S. Popescu, *Bell Inequalities for Arbitrarily High-Dimensional Systems*, Phys. Rev. Lett., **88** (2002), p. 040404. 11, 12, 13

[28] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden and N. Gisin, *Tailoring photonic entanglement in high-dimensional Hilbert spaces*, Phys. Rev. A, **69** (2004), p. 050304. 11

[29] T. Durt, N. J. Cerf, N. Gisin and M. Żukowski, *Security of quantum key distribution with entangled qutrits*, Phys. Rev. A, **67** (2003), p. 012311. 19, 20

[30] T. Durt, D. Kaszlikowski, J.-L. Chen and L. C. Kwek, *Security of quantum key distributions with entangled qudits*, Phys. Rev. A, **69** (2004), p. 032313. 20

[31] A. Einstein, B. Podolsky and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Phys. Ref., **47** (1935), pp. 777–780. 8

[32] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett., **67** (1991), pp. 661–663. 4, 15, 17

[33] M. Fitzi, N. Gisin and U. Maurer, *Quantum Solution to the Byzantine Agreement Problem*, Phys. Rev. Lett., **87** (2001), p. 217901. 11

[34] S. Franke-Arnold, S. M. Barnett, M. J. Padgett and L. Allen, *Two-photon entanglement of orbital angular momentum states*, Phys. Rev. A, **65** (2002), p. 033823. 37

[35] S. J. Freedman and J. F. Clauser, *Experimental Test of Local Hidden-Variable Theories*, Phys. Rev. Lett., **28** (1972), pp. 938–941. 10

[36] E. S. Fry and R. C. Thompson, *Experimental Test of Local Hidden-Variable Theories*, Phys. Rev. Lett., **37** (1976), pp. 465–468. 10

[37] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu and A. Peres, *Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy*, Phys. Rev. A, **56** (1997), pp. 1163–1172. 18

[38] M. Gell-Mann and Y. Neeman, *The Eightfold Way*, W. A. Benjamin, New York, 1964. 22

[39] G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett and S. Franke-Arnold, *Free-space information transfer using light beams carrying orbital angular momentum*, Optics Express, **12** (2004), pp. 5448–5456. 50

[40] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Quantum Cryptography*, Rev. Mod. Phys., **74** (2002), pp. 145–195. 14, 17, 18

[41] C. Gobby, Z. L. Yuan and A. J. Shields, *Quantum key distribution over 122 km of standard telecom fiber*, Appl. Phys. Lett., **84** (2004), pp. 3762–3764. 4

[42] C. Gobby, Z. L. Yuan and A. J. Shields, *Unconditionally secure quantum key distribution over 50 km of standard telecom fibre*, Electron. Lett., **40** (2004), pp. 1603–1605. 4

[43] H. He, M. E. J. Friese, N. R. Heckenberg and H. Rubinsztein-Dunlop, *Direct Observation of Transfer of Angular Momentum to Absorptive Particles from a Laser Beam with a Phase Singularity*, Phys. Rev. Lett., **75** (1995), pp. 826–829. 23

[44] T. Jennewein, *Quantum Communication and Teleportation Experiments using Entangled Photon Pairs*, PhD Thesis, Universität Wien, 2002. 22

[45] D. Kaszlikowski, L. C. Kwek, J.-L. Chen, M. Żukowski and C. H. Oh, *Clauser-Horne inequality for three-state systems*, Phys. Rev. A, **65** (2002), p. 032118. 11

[46] A. B. Klimov, L. L. Sánchez-Soto, H. de Guise and G. Björk, *Quantum phases of a qutrit*, J. Phys. A: Math. Gen., **37** (2004), pp. 4097–4106. 22

[47] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity, *Quantum cryptography: A step towards global key distribution*, Nature, **419** (2002), p. 450. 4

[48] A. Mair, A. Vaziri, G. Weihs and A. Zeilinger, *Entanglement of the orbital angular momentum states of photons*, Nature, **412** (2001), pp. 313–316. 37

[49] G. A. Maslennikov, A. A. Zhukov, M. V. Chekhova and S. P. Kulik, *Practical realization of a quantum cryptography protocol exploiting polarization encoding in qutrits*, J. Opt. B: Quantum Semiclass. Opt., **5** (2003), pp. S530–S534. 11

[50] G. Molina-Terriza, A. Vaziri, R. Ursin and A. Zeilinger, *Experimental Quantum Coin Tossing*, Phys. Rev. Lett., **94** (2005), p. 040501. 11

[51] A. Muller, J. Breguet and N. Gisin, *Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km*, Europhys. Lett., **23** (1993), p. 383. 17

[52] A. Peres, *Quantum Theory: Concepts and Methods*, Kluwer Academic Publishers, 1998. 9

[53] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein and A. Zeilinger, *Practical quantum key distribution with polarization entangled photons*, Optics Express, **12** (2004), pp. 3865–3871. 4, 17

[54] M. Reck, A. Zeilinger, H. J. Bernstein and P. Bertani, *Experimental realization of any discrete unitary operator*, Phys. Rev. Lett., **73** (1994), pp. 58–61. 22

[55] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter and A. Zeilinger, *Distributing entanglement and single photons through an intra-city, free-space quantum channel*, Optics Express, **13** (2005), pp. 202–209. 4

[56] R. L. Rivest, A. Shamir and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21, **2** (1978), pp. 120–126. 14

[57] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe and D. J. Wineland, *Experimental violation of a Bell's inequality with efficient detection*, Nature, **409** (2001), p. 791. 10

[58] B. E. A. Saleh and M. C. Teich, *Fundamental of Photonics*, John Wiley & Sons, Inc., New York, 1991. 24

[59] E. Schrödinger, *Die gegenwärtige Situation in der Quantenmechanik*, Die Naturwissenschaften, **48** (1935), pp. 808–849. 6, 8

[60] C. Simon, G. Weihs and A. Zeilinger, *Optimal Quantum Cloning via Stimulated Emission*, Phys. Rev. Lett., **84** (2000), pp. 2993–2996. 8

[61] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, *Quantum key distribution over 67 km with a plug & play system*, New J. Phys., **4** (2002), pp. 41.1–41.8. 4

[62] M. Stütz, *Aktive Hologramme zur Qutrit-Manipulation*, Masters Thesis, Universität Wien, 2006. 50

[63] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue and Y. Yamamoto, *Differential phase shift quantum key distribution experiment over 105 km fibre*, New J. Phys., **7** (2005), p. 232. 4

[64] R. T. Thew, A. Acín, H. Zbinden and N. Gisin, *Bell-Type Test of Energy-Time Entangled Qutrits*, Phys. Rev. Lett., **93** (2004), p. 010503. 11, 50

[65] W. Tittel, J. Brendel, H. Zbinden and N. Gisin, *Quantum Cryptography Using Entangled Photons in Energy-Time Bell States*, Phys. Rev. Lett., **84** (2000), pp. 4737–4740. 17

[66] G. A. Turnbull, D. A. Robertson, G. M. Smith, L. Allen and M. Padgett, *The generation of free-space Laguerre-Gaussian modes at millimetre-wave frequencies by use of a spiral phaseplate*, Opt. Comm., **127** (1996), pp. 183–188. 27

[67] A. Vaziri, *Experimente mit Singulären Quantenzuständen Höherdimensional Verschränkter Photonen*, PhD Thesis, Universität Wien, 2003. 28, 30, 38, 41

[68] A. Vaziri, G. Weihs and A. Zeilinger, *Experimental Two-Photon, Three-Dimensional Entanglement for Quantum Communication*, Phys. Rev. Lett., **89** (2002), p. 240401. 11, 13, 38

[69] J. von Neumann, *Mathematische Grundlagen der Quantentheorie*, Springer, 1931. 8

[70] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger, *Experimental one-way quantum computing*, Nature, **434** (2005), pp. 169–176. 11

[71] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter and A. Zeilinger, *Violation of Bell's Inequality under Strict Einstein Locality Conditions*, Phys. Rev. Lett., **81** (1998), pp. 5039–5043. 6, 10

[72] R. F. Werner, *Optimal cloning of pure states*, Phys. Rev. A, **58** (1998), pp. 1827–1832. 8

[73] S. Wiesner, *Conjugate coding*, SIGACT News, **15** (1983), pp. 78–88. 4, 15

[74] W. K. Wootters and B. D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. Phys., **191** (1989), pp. 363–381. 21

[75] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature, **299** (1982), pp. 802–803. 7

[76] M. Żukowski and Č. Brukner, *Bell's Theorem for General* N*-Qubit States*, Phys. Rev. Lett., **88** (2002), p. 210401. 9