universität wien

MASTERARBEIT

Titel der Masterarbeit

Efficient Characterization of Multi-Qubit States and their Application to Demonstrate Measurement Only Blind Quantum Computing

Verfasserin

Marie-Christine Röhsner, BSc

angestrebter akademischer Grad

Master of Science (MSc)

Wien, 2014

Studienkennzahl lt. Studienblatt:	A 066 876
Studienrichtung lt. Studienblatt:	Masterstudium Physik
Betreuer:	Assoz. Prof. Dr. Philip Walther

Contents

Abstract

Multi-qubit quantum states are the basic resource for future quantum computation and quantum communication. For the reliable realization of these applications the experimental generation of the desired multi-qubit state has to be certified. This thesis presents the implementation of a new method to characterize multi-qubit stabilizer states which are of particular interest for quantum computing schemes. It is based on the concept of Identity Products (IDs) and relies on just N+1 measurement settings for a N-qubit state. We characterized an experimentally generated four-qubit linear cluster state, as well as a three- and a four-qubit GHZ state and compared our results to other methods for partial and full state characterization. Furthermore, the implementation of a possible application for the characterized states, measurement only blind quantum computing, is shown. This new blind quantum computing protocol enables a quasi-classical client Alice, only able to perform single-qubit measurements, to delegate a quantum computation to an untrusted provider without leaking any of her information to him. Moreover, she can verify the preparation of the correct resource state. We show an especially elegant verification protocol for quantum computer resources by using a four-qubit linear cluster state.

Zusammenfassung

Quantenzustände, welche aus mehrerern Qubits bestehen, sind die grundlegende Ressource für zukünftige Quanten-Computer und Quanten-Kommunikation. Um die verlässliche Realisierung dieser Anwendungen zu ermöglichen, muss die experimentelle Herstellung des gewünschten Multi-Qubit Zustands sichergestellt werden. Diese Arbeit stellt die Implementierung einer neuen Methode zur Charakterisierung von Multi-Qubit Stabilizer-Zuständen vor. Sie basiert auf dem Konzept der Identity Products (IDs) und

benötigt nur N+1 Messeinstellungen für einen N-Qubit-Zustand. Wir charakterisierten einen experimentell erzeugten vier-Qubit linearen Cluster-Zustand, sowie einen drei- und einen vier-Qubit GHZ-Zustand und verglichen unsere Resultate mit anderen Methoden zur teilweisen und vollständigen Zustands-Charakterisierung. Außerdem wird die Implementierung einer möglichen Anwendung für die charakterisierten Zustände gezeigt, das sogenannte "measurement only blind quantum computing". Dieses neue Protokoll erlaubt einer quasi-klassischen Auftraggeberin Alice, welche nur die Möglichkeit hat, einzelne Qubits zu messen, eine Quanten-Berechnung an einen nicht vertrauenswürdigen Anbieter zu delegieren ohne, dass er einen Teil ihrer Informationen erhalten kann. Des Weiteren kann sie überprüfen, ob der richtige Zustand als Ressource erzeugt wurde. Unsere Implementierung basiert auf dem vier-Qubit linearen Cluster-Zustand, für welchen wir ein besonders starkes Überprüfungsprotokoll demonstrieren.

Acknowledgments

First of all I would like to thank my parents who are always there for me and made this thesis (and all my studies) possible. Also I want to thank my supervisor Assoz. Prof. Dr. Philip Walther for the opportunity to work in his amazing group as well as for all his help and encouragements. Without Chiara Greganti, patiently explaining me our setup and everything else I needed to know to work with her during this last year and Stefanie Barz who kept pushing and encouraging me, I would have been utterly lost. It was a lot of fun to work with everyone in the group and I'm thankful for many physics and even more non-physics related discussions as well as the regular cooking sessions which I greatly enjoyed. Special thanks go to everyone who proofread (parts of) my thesis: Jonas Zeuner, Emma Dowd, Chiara Greganti and my amazing father Georg Röhsner.

Finally I would like to thank my whole family and friends for their support. Especially my friends Lisa, Veronika, Elli, Paula, Babsi, Tobias, Julien, Michael, Dominik, Matthias, Max, Viktor, Gregor and all the others for always cheering me up and for telling me that what I do is cool, Peter for always being there, and last but not least my three brothers.

Introduction

„Will we have a quantum computer soon? And can we use it to play Mario Kart?“ My brothers have repeatedly asked me these and similar questions. Unfortunately, I do not have a good answer as I do not know when the first powerful quantum computers will be available to the general public (or what for this general public will use them). But I do know that there are still some major challenges to be mastered before this goal can be achieved.

One of these challenges is certainly the preparation of multi-qubit states with a high number of qubits as a resource for future powerful quantum computers. To allow for reliable computations it is necessary to certify if a generated physical state is actually equal or close to the desired theoretical state. The required number of measurement settings for some common methods to characterize states scales exponentially with the number of qubits [1, 2, 3, 4]. Thus, they are unfeasible even for comparably low qubit numbers.

This problem is approached in the first part of the thesis where I will describe a new method scaling linearly with the number of qubits, that can be used to efficiently characterize important properties of multi-qubit stabilizer states [5]. Those states are the basic resource for many applications in quantum computing and communication [5, 6, 7].

Another challenge and a possible application for the characterized states is the protection of data privacy in quantum computing. Even today complex computations are often delegated to distant providers, which is known as cloud computing. Recently, newspapers are full of reports about security incidents in this context. Should powerful quantum computers be available in such manner Alice, a (quasi-classical) client, might want to use the quantum resources of Bob, the operator of a powerful quantum computer, even

though she does not trust him. Blind quantum computing (BQC) first introduced in 2009 [8] allows Alice to delegate her computation to Bob without leaking any of her information to him. Additionally, even without a quantum computer on her side, she can verify if Bob is honest and provides her with the correct results or resources for her computation [9, 10]. A new protocol was proposed by Morimae [11] which increases the security and simplifies the BQC for Alice as it only requires her to perform single-qubit measurements. It is therefore referred to as „measurement only blind quantum computation“. The first proof-of-principle demonstration of this protocol focusing on its verification is described in the second part of this work.

The rest of this thesis is organized as follows: In Section 1 the basic theoretical concepts, e. g. qubits, entanglement and nonlocality, will be explained.

A discussion of the implementation and manipulation of photonic qubits is given in Section 2. Here, also our setup to generate different highly entangled three- and four-qubit states is described together with a brief alignment tutorial.

Section 3 introduces the new method to efficiently characterize multi-qubit stabilizer states. It presents the theory of Identity Products (IDs) and how they can be used for experimental tests of nonlocality, finding a lower bound on quantum state fidelity and discriminating entanglement. The experimental implementation is reported and the collected data is analyzed.

Finally Section 4 starts with a short introduction to quantum computing, followed by a description of the protocol for measurement only blind quantum computing and its verification. Our experimental proof-of-principle demonstration is explained together with a discussion of our results at the end of the chapter.

1 Basic Principles

Non-classical phenomena, like entanglement and nonlocality, form the basis of the experiments presented in the following sections. These fundamental concepts will be introduced here starting with the smallest unit of quantum information the qubit, followed by descriptions of multi-qubit states and entanglement. Additionally, quantum state fidelity and entanglement witnesses, which are used to experimentally certify the preparation of a quantum state and the desired entanglement are presented. In the last part of the chapter nonlocality and the Greenberger Horne Zeilinger (GHZ) theorem which are of special importance to the experiment in Section 3 will be explained.

1.1 The Qubit

Information processing in classical computers is based on the bit. A bit can take on two different states „0“ and „1“. Quantum information processing on the other hand is based on the quantum bit or qubit. It can occupy the states $|0\rangle$ and $|1\rangle$ but also any linear combination of those.

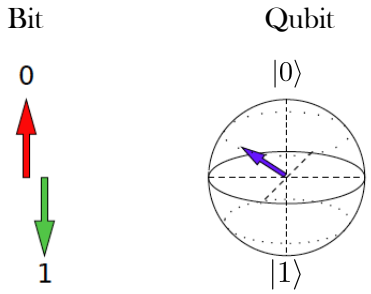


Figure 1: Comparison of a classical bit which can take two values and a qubit that can occupy any linear combination the states $|0\rangle$ and $|1\rangle$.

Therefore, a general qubit can be written as

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.1}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. This is known as state vector representation and states that can be described in this form are called pure states. However, a quantum system can also be in a statistical ensemble of different state vectors, in which case they are called mixed states. They cannot be described by a state vector but by a density matrix. The density matrix of a pure state $|\Psi\rangle$ is given by

$$\rho = |\Psi\rangle\,\langle\Psi|\,, \tag{1.2}$$

whereas the density matrix of a mixed state is of the form

$$\rho = \sum_i p_i\,|\Psi_i\rangle\,\langle\Psi_i|\ . \tag{1.3}$$

where p_i are the relative populations of the states $|\Psi_i\rangle$ and $\sum_i p_i = 1$ [12].

1.1.1 The Bloch Sphere

All possible qubit states can be represented on a sphere, the Bloch sphere [13]. To see this we rewrite the state of a general qubit in a form that automatically incorporates the normalization relation $|\alpha|^2 + |\beta|^2 = 1$ as follows:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle\,. \tag{1.4}$$

It can be seen that θ and ϕ fully define a point on the three-dimensional unit sphere so every pure single-qubit state can be represented as a point on this sphere which is known as the Bloch sphere representation. Mixed states correspond to points within the sphere. Any unitary operation on a single qubit can be represented as rotation of the state vector $|\Psi\rangle$ on the Bloch sphere. The states on the equator of the sphere represent equal

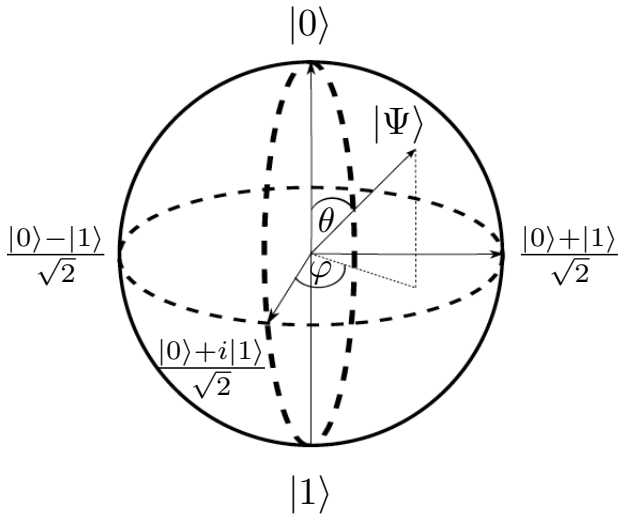


Figure 2: Illustration of the Bloch sphere. Any pure state of a qubit can be represented as a point on the surface of this sphere. Mixed states lie within the sphere.

superpositions of $|0\rangle$ and $|1\rangle$. Of particular importance are the eigenstates of the Pauli X and Y operators. The matrix representations of the Pauli operators in the computational basis ($\{|0\rangle, |1\rangle\}$) are given by

$$\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.5}$$

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1.6}$$

$$\sigma_Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}. \tag{1.7}$$

The corresponding eigenstates and eigenvalues λ are shown in Table 1.

	$\lambda = +1$	$\lambda = -1$
σ_Z	$\|0\rangle$	$\|1\rangle$
σ_X	$\|+\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|-\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
σ_Y	$\|R\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + i\,\|1\rangle)$	$\|L\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - i\,\|1\rangle)$

Table 1: Eigenstates of the Pauli operators.

1.2 Multi-Qubit States and Entanglement

Until now we have restricted our discussion to single qubits. The size of the Hilbert space, needed to describe a system, grows exponentially with the number of qubits; for N qubits the Hilbert space has the dimension $d = 2^N$. Therefore, multi-qubit systems are far more complex and also exhibit new, interesting phenomena like entanglement.

Starting from the single-qubit description we might try to construct a multi-qubit state by taking the tensor product of N single-qubit pure states

$$|\Phi_N\rangle = \frac{1}{\sqrt{N}}(|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes |\Psi_3\rangle \otimes \ldots \otimes |\Psi_N\rangle) \ . \tag{1.8}$$

States which can be written as tensor products of pure states are called *separable states* or *product states*. But there also exist states which cannot be written in form of equation (1.8) in any basis; these states are called entangled.

Especially important and widely used in experiments (e. g. tests of the Bell inequality, see Section 1.5) are maximally entangles states. A two-qubit state is maximally entangled if the reduced density matrix of each qubit is a multiple of the identity operator [14]. Among those states the only maximally entangled states (up to local unitary (LU) transformations) are the Bell-states given by

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{1.9}$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \ . \tag{1.10}$$

Here $|0\rangle \otimes |0\rangle$ is denoted $|00\rangle$ for improved readability. For three qubits there are two LU inequivalent classes of maximally entangled states [15] represented by the Greenberger-Horne-Zeilinger (GHZ) state [16] and the W state [17]. The GHZ state is given by

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{1.11}$$

and the W state is given by

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle). \tag{1.12}$$

For pure four-qubit states there are nine classes of entanglement under stochastic local quantum operations assisted by classical communication (SLOCC) [18]. But one particular kind of four-qubit states will be central to the rest of this work. These states, known as cluster states, will be introduced in the next section.

1.2.1 Cluster States

Cluster states, introduced in 2001 by Briegel and Raussendorf [19] are an especially interesting class of states because they form a universal resource for measurement-based quantum computing (see Section 4.1.2)[6]. Every cluster state corresponds to a graph on

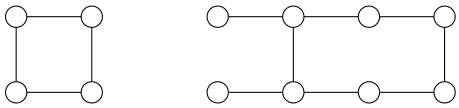


Figure 3: Two examples for graphs corresponding to different cluster states.

a two dimensional square lattice[1] (e. g. Figure 3). Given a graph the cluster state can be defined by assuming that every vertex in the graph corresponds to a qubit initially in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and applying a $C - Phase$ gate on every two qubits connected with a line in the graph [20]. The matrix representation of the C-Phase gate in the computational basis is given by

$$U_{C-Phase} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{1.13}$$

[1] If this requirement is dropped the corresponding state belongs to the more general class of graph states.

Alternatively, a cluster state can be defined (again starting form a given graph) as the joint eigenstate with all positive eigenvalues of operators of the form

$$A_i = \sigma_X(i) \prod_{j \in N(i)} \sigma_Z(j) \tag{1.14}$$

where $\sigma_X(i)$ and $\sigma_Z(j)$ are Pauli-matrices applied the qubit on vertex i (j) and $N(i)$ is the neighborhood of a vertex i given by all other vertices that are connected to it with a line in the graph.

Finally it should be mentioned that cluster states (and graph states) are a subset of the more general stabilizer states. A state $|\Psi\rangle$ is stabilized by an operator O_i if $O_i|\Psi\rangle = |\Psi\rangle$. The stabilizer states are the set of states V_S that are stabilized by S (the stabilizer group) which is a subgroup of the n-qubit Pauli group G_n.[2] If the elements of S commute, and $-I$ is not an element of S, V_S is a non-trivial vector-space [5, 21].

1.3 Entanglement Witnesses

Given the much higher complexity of multi-qubit states compared to single-qubit states it is in general non trivial to determine whether a state (experimentally prepared or given as a density matrix) is entangled. Thus it is useful to have a directly measurable observable that can be used to detect entanglement. Entanglement witnesses fulfill those requirements and therefore provide an important tool for experiments. An observable $\mathcal{W}$ is defined to be an entanglement witness if

$$Tr(\mathcal{W}\rho_s) \geq 0 \qquad \text{for all separable states } \rho_s, \tag{1.15}$$

$$Tr(\mathcal{W}\rho_e) < 0 \qquad \text{for at least one entangled } \rho_e. \tag{1.16}$$

When $Tr(\mathcal{W}\rho) < 0$ for a given state, then one knows with certainty that this state is entangled [15]. In two-qubit systems, only one type of entanglement witness exists; however, in higher-dimensional cases there are different types of witnesses to detect the

[2] The n-qubit Pauli group G_n is given by all n-fold tensor products of the Pauli matrices and the identity matrix and multiplicative factors of ± 1 and $\pm i$ so e. g. $G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$.

different classes of entanglement [15].

1.4 Fidelity

In the experimental generation of quantum states, a desired state cannot be achieved with infinite precision. In order to quantify how „close“ the produced quantum state is to the ideal one, we introduce a measure called fidelity [22]. The fidelity $\mathcal{F}$ is a measure of the distance between two states. For a pure state $|\Psi\rangle$ and a second state characterized by ρ the fidelity is defined as

$$\mathcal{F} = \langle\Psi|\,\rho\,|\Psi\rangle \tag{1.17}$$

which is the overlap between $|\Psi\rangle\langle\Psi|$ and ρ. Given a density matrix (which might have been reconstructed form experimental data) this can be used to calculate the overlap with the ideal state. For two mixed states ρ and σ, the fidelity is defined as

$$\mathcal{F} = Tr(\sqrt{\rho}\sigma\sqrt{\rho})\ . \tag{1.18}$$

1.5 Entanglementand Nonlocality

Entanglement, first addressed by Einstein, Podolsky and Rosen (EPR) in 1935 [23], refers to the notion that quantum mechanical objects can exhibit correlations that cannot be explained by assigning local hidden variables to each object. Einstein, Podolsky and Rosen showed that if one assumes locality[3] and realism[4], the quantum mechanical description of reality cannot be complete. According to them, local hidden variables should exist that determine the outcomes of measurements on quantum mechanical systems. But in 1964 John Bell showed that there are cases in which any local hidden variable theory (LHVT) will predict different results than quantum mechanics (QM) [24]. He derived a inequality with which it became possible to test the predictions of QM against those of LHVTs. The test is based on a two-party system of entangled particles

[3] Actions in one place cannot influence measurement outcomes in another place instantaneously.
[4] Any observable must have a pre-existing value for any given measurement.

and two separated observers performing measurements. Since the original inequality was based on perfect correlations between the two parties it could not be tested under realistic laboratory conditions which suffer from imperfections like particle loss. In 1969 the inequality was adapted by Clauser, Holt, Shimony and Horne (CHSH) [25] and became testable in laboratories. The experiment was based on a source that emits two entangled particles that are sent to two separated observers referred to as Alice and Bob. Each of them can perform measurements on those particles along two different directions each: $\vec{a}, \vec{a'}$ (for Alice) and $\vec{b}, \vec{b'}$ (for Bob). The inequality in the CHSH-formulation reads as follows

$$S = |E(\vec{a}, \vec{b}) + E(\vec{a'}, \vec{b}) + E(\vec{a}, \vec{b'}) - E(\vec{a'}, \vec{b'})| \leq 2 \tag{1.19}$$

where $E(\vec{a}, \vec{b})$ is the expectation value of the product of the measurement outcomes along $\vec{a}$ and $\vec{b}$. This inequality has to hold for any LHVT but QM predicts a maximum outcome of $S = 2\sqrt{2}$. A violation of the classical bound was reached for the first time by Freedman and Clauser in 1972 [26]. This first test and a variety of tests ever since have confirmed the predictions of quantum mechanics instead of local hidden variable theories. Therefore, we see that some correlations described by quantum mechanics and found in nature cannot be explained by local hidden variables and this phenomenon is known as nonlocality.[5] It will be the basis of many of the ideas presented in this thesis.

1.5.1 The GHZ Theorem

All tests of nonlocality based on the (CHSH) Bell inequality are based on a contradiction of a statistical nature – the contradiction between the statistical predictions given by quantum mechanics versus the LHVT. In 1989, Greenberger, Horne, and Zeilinger (GHZ) showed that there exist experiments using three or more particles for which quantum mechanics and LHVT predict different deterministic outcomes [16]. As it is based on deterministic predictions it is considered to allow for a stronger contradiction between QM and LHVTs. The original argument was based on four spin-1/2 particles but it is

[5] To be more precise this could be called nonlocal realism instead of nonlocality since both assumptions (locality and realism) are needed for LHVTs. For simplicity it will only be referred to as nonlocality (in accordance with e.g. [27]).

sufficient to consider just three. (Note that here I do not use the original representation but one similar to that used by Mermin in [28], for it gives the result using a formalism more convenient for the applications we will consider.)

Let us start with the now well-known Greenberger-Horne-Zeilinger-state (GHZ state):

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{1.20}$$

It is the joint eigenstate of the operators $\sigma_Y \otimes \sigma_Y \otimes \sigma_X$ (YYX), $\sigma_Y \otimes \sigma_X \otimes \sigma_Y$ (YXY) and $\sigma_X \otimes \sigma_Y \otimes \sigma_Y$ (XYY) with the eigenvalue -1 and $\sigma_X \otimes \sigma_X \otimes \sigma_X$ (XXX) with the eigenvalue $+1$. In the following, I shorten these expressions by writing X (Y,Z) instead of $\sigma_{X(Y,Z)}$ and omit all tensor product signs. To reproduce the predictions of QM with a LHVT we assign local hidden variables λ_X, λ_Y to the single-qubit operators. The possible values of λ_X andλ_Y are the possible outcomes of X and Y measurements, or ± 1. For a LHVT to be consistent with the predictions of QM, the following should hold:

$$-1 = (\lambda_{X1}\lambda_{Y2}\lambda_{Y3})(\lambda_{Y1}\lambda_{X2}\lambda_{Y3})(\lambda_{Y1}\lambda_{Y2}\lambda_{X3}) = \lambda_{Y1}^2\lambda_{Y2}^2\lambda_{Y3}^2\lambda_{X1}\lambda_{X2}\lambda_{X3} = \lambda_{X1}\lambda_{X2}\lambda_{X3} = +1 \tag{1.21}$$

Clearly, this is invalid; thus, LHVT cannot reproduce the predictions of QM. This contradiction enables us to realize a test of nonlocality in just one measurement. In particular, if we know that the outcomes of the YYX, YXY and XYY measurements are -1, we only need to realize an XXX measurement; then, an outcome $+1$ agrees with LHVT, whereas a result of -1 agrees with QM. This is also known as a one-shot-distinction [29] since it in principle does not rely on statistics or inequalities. Real experiments are of course never ideal, noiseless or errorless, so any experimental test of the GHZ theorem will still rely on statistics.

2 Photonic Systems for Generating Multi-Qubit States

In this thesis I will describe the implementation of two different theoretical concepts, efficiently characterizing multi-qubit stabilizer states and measurement only blind quantum computing. Both implementations are based on photonic systems and are realized using the same setup. In this section the basic building blocks of our experiments are explained followed by an introduction of our setup and its alignment.

2.1 Photonic Qubits

The most elementary resource in any quantum information processing experiment is the qubit. Qubits have been realized in many different ways, among them are trapped ions [30, 31], solid state systems [32, 33] and superconductors [34, 35, 36]. For our experiments the polarization of photons is used to implement the qubits. This photonic implementation has many advantages among them the mobility of the photons which can be transported in fibers or free space and their long coherence times. Additionally, single-qubit rotations are easy to realize which will be described in the following section.

2.1.1 Basic Linear Optical Elements

A first important step in the manipulation of photons is to perform single-qubit gates or rotations of a state on the Bloch sphere. The action of any single-qubit gate on the state of a qubit can be described by a unitary 2×2 matrix. Here the matrix representation of the linear optical elements used in our experiment will be given in the computational

basis where horizontally polarized photons encode the state $|0\rangle$ and vertically polarized photons correspond to the state $|1\rangle$ which can be written as:

$$|0\rangle \equiv |H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{2.1}$$

$$|1\rangle \equiv |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.2}$$

Half-Wave Plates (HWP)

Wave plates are optical elements made from uniaxial birefringent crystals that induce a relative phase shift between the polarization component aligned with the ordinary and the extraordinary axis of the crystal. A half-wave plate (HWP) introduces a phase shift of π between these two components. Rotating the wave plate in the plane perpendicular to the direction of the incoming light determines the influence of the wave plates on the polarization components as this corresponds to a change in basis. The effect of a half-wave plate can in matrix representation be written as

$$U_{HWP}(\theta) = e^{i\frac{\pi}{2}} \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix} \tag{2.3}$$

where θ is the angle between the optical axis and the horizontal plane [37].

Quarter-Wave Plates (QWP)

Quarter-wave plates (QWP) are optical elements similar to half-wave plates but they create a phaseshift of $\pi/2$ (instead of π) between the polarization component aligned with the ordinary and the one aligned with the extraordinary axis of the crystal. In matrix representation the effect of a quarter-wave plate can be written as

$$U_{QWP}(\theta) = \frac{1}{\sqrt{2}} \begin{pmatrix} (1+i)\cos(2\theta) & i\sin(2\theta) \\ i\sin(2\theta) & (1-i)\cos(2\theta) \end{pmatrix} \tag{2.4}$$

here θ is again the angle between the optical axis and the horizontal plane [37].

Beamsplitters (BS)

Beamsplitters are optical elements with two inputs and two outputs. Incoming light will either get reflected or transmitted with a probability depending on the reflectivity value of the beamsplitter. Most commonly used are symmetric or 50:50 beamsplitters. For one input they create an equal superposition between the output paths so they act like a Hadamard gate in the spatial degree of freedom. Beamsplitters can also be used to interfere two input modes in which case e. g. the Hong-Ou-Mandel effect [38] can be observed.

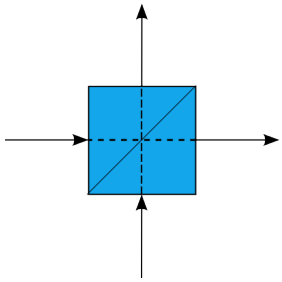


Figure 4: Schematic of a beamsplitter.

Polarizing Beamsplitters (PBS)

A polarizing beamsplitter (PBS) is a special kind of beamsplitter with the characteristic that it transmits light that is horizontally polarized and reflects light that is vertically polarized. Therefore, they can be used to convert qubits encoded in polarization into qubits encoded in the path degree of freedom (one path is assigned the state $|0\rangle$, the other one the state $|1\rangle$).

2.2 Nonlinear Optical Crystals

The source of light in our experiment is a pulsed laser which emits coherent light. For our experiment though we need single photons (to encode our qubits). To reach this goal we have to manipulate our light using two main second order processes. First we change

the wavelength of our laser light. This is referred to as second harmonic generation (SHG) and it enables us to perform spontaneous parametric down conversion (SPDC) as a second process. Both of these can be realized using nonlinear optical crystals. The term "nonlinear" refers to the fact that those crystals have responses to light that depend non-linearly on the strength of the optical field.

To describe this more precisely we recall how in linear materials the polarization $\vec{P}$ depends on the electrical field $\vec{E}$:

$$\vec{P} = \epsilon_0 \chi^{(1)} \vec{E} \tag{2.5}$$

where $\chi^{(1)}$ is the linear susceptibility and ϵ_0 is the permittivity of free space. For nonlinear materials this relation no longer holds and the expression for the i^{th} component of the polarization can be generalized like

$$P_i = \epsilon_0 [\chi^{(1)}_{ij} E_j + \chi^{(2)}_{ijk} E_j E_k + \chi^{(3)}_{ijkl} E_j E_k E_l + ...] \tag{2.6}$$

where the $\chi^{(n)}$ are the nonlinear susceptibilities. If a given crystal does not have a center of symmetry it is called non-centrosymmetric. Those are the materials that can have a non-vanishing $\chi^{(2)}$ and will be the materials of interest in this section [39].

2.2.1 Second Harmonic Generation (SHG)

An example for an effect occurring in a crystal with $\chi^{(2)} \neq 0$ is SHG, also known as up-conversion. In this process two photons with the frequency $\omega_1 = \omega_2$ are absorbed[6] and a third photon with the frequency $\omega_0 = \omega_1 + \omega_2$ is emitted. Obviously this can only happen if energy and momentum are conserved which corresponds to

$$\vec{k_0} = \vec{k_1} + \vec{k_2} \tag{2.7}$$

$$\omega_0 = \omega_1 + \omega_2. \tag{2.8}$$

[6]There is also a more general case where $\omega_1 \neq \omega_2$ which is called sum frequency generation.

These are referred to as phase matching conditions and can only be fulfilled by the right choice of polarization for the three photons. The crystals typically used in this kind of experiments exhibit birefringence due to the fact that they have a principal axis of symmetry and therefore (for each frequency) there are two refractive indexes: the ordinary $n_o(\omega)$ and the extraordinary $n_e(\omega, \theta)$ where θ is the angle between the direction of propagation and the principal axis of the crystal. Two kinds of phase matching can satisfy those conditions[7]:

Type I phase matching can be achieved if the incoming beams have parallel polarization and propagate as ordinary rays in the crystal. Then the third beam will have the orthogonal polarization and propagate as extraordinary beam. In this case the photons satisfy the following relations

$$k_1 = k_2 = \frac{\omega_1 n_o(\omega_1)}{c} \tag{2.9}$$

$$k_0 = \frac{\omega_0 n_e(\omega_0, \theta_0)}{c} \tag{2.10}$$

where θ_0 is the angle between the direction of the output beam and the optical axis.

In **type II** phase matching the incoming beams have orthogonal polarization. In this case the output beam is also propagating as an extraordinary ray and fulfills the relations

$$k_1 = \frac{\omega_1 n_o(\omega_1)}{c} \tag{2.11}$$

$$k_2 = \frac{\omega_2 n_e(\omega_2, \theta_2)}{c} \tag{2.12}$$

$$k_0 = \frac{\omega_0 n_e(\omega_0, \theta_0)}{c}. \tag{2.13}$$

If a configuration is chosen where the k-vectors of all three beams are parallel this is called a collinear configuration [39].

[7]Here the case of *negative* crystals i.e.$n_e < n_o$ is described. For positive crystals ($n_e > n_o$) the role of ordinary and extraordinary rays are reversed.

2.2.2 Spontaneous Parametric Down-Conversion (SPDC)

As SHG is described by a unitary evolution the inverse process is also possible. This means a high frequency photon can be absorbed and two photons of lower energy (given the name signal and idler) can be emitted in the crystal. This process is known as spontaneous parametric down conversion (SPDC). In this context *parametric* means that the optical medium is unchanged by the process. Down conversion can happen in materials with a non-vanishing $\chi^{(2)}$. A schematic drawing of the process is shown in Figure 5. In our experiment we used SPDC with type-II phase matching in a non-collinear

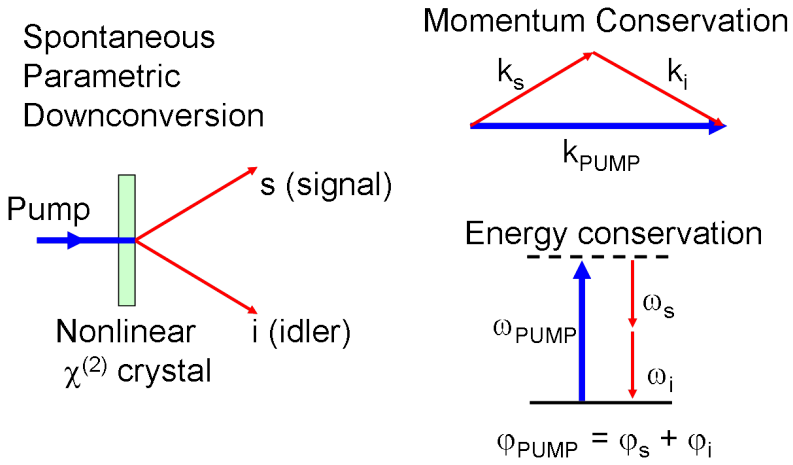


Figure 5: Schematic of the SPDC process. For historical reasons the two down-converted photons are called *signal* and *idler*. Figure taken from [40].

configuration (so signal and idler photon are emitted under an angle with respect to the pump beam) in a nonlinear crystal called BBO (β-barium borate, BaB_2O_4). Our experimental scheme is based on interference and therefore (as SPDC is a spontaneous process) we have to limit the interaction time of our input laser beam with the crystal in a way that the coherence time of the photons is longer than the uncertainty in the creation time of the photons [41]. This is achieved by using a pulsed laser. Additionally, this pulsed laser has the advantage of providing high energy densities which is essential since the probability of photons being down-converted for this kind of SPDC is typically around 10^{-12} [42].

To fulfill the (type II) phase matching conditions the photons have to be orthogonally

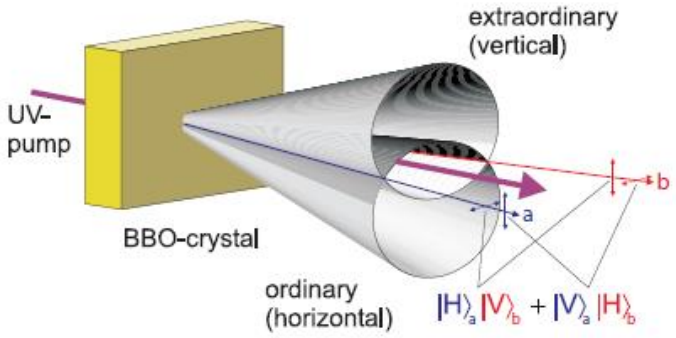


Figure 6: Photons are emitted from the BBO-crystal along two cones. The intersection of those cones defines two spatial modes a and b in which the polarization of the photons is undefined. Photons from this state will be (after proper compensation of walkoff and phase) in a maximally entangled Bell-state. Figure taken from [41].

polarized and are emitted in cones from the crystal (see Figure 6). The two spatial modes a and b are defined by the intersection of the two cones. In those modes the polarization of a single photon is undefined. However photons with different polarizations are affected differently by the BBO since it is a birefringent crystal. This leads to walk-off effects which have to be compensated to make the photons indistinguishable.[8] Turning the polarization of the photons by 90° using a HWP (and therefore from ordinary to extraordinary and vice versa) and letting them pass through a BBO of half the length of the down-conversion crystal compensates the average walk-off. This is illustrated in Figure 7.

If we now use birefringent elements to set the phase between the horizontally and vertically polarized photons to 0 or π the photon pairs are emitted in a maximally entangled Bell state.

We have seen that the down-converted photons are always emitted in pairs but in general more than one pair per pulse can be created. Using the formalism of second

[8]Note that also pairs with $\omega_s \neq \omega_i$ are produced (as they also can fulfill the phase matching conditions). For our experiments we need the photons to be indistinguishable therefore we select only the pairs of equal wavelength using bandwidth filters.

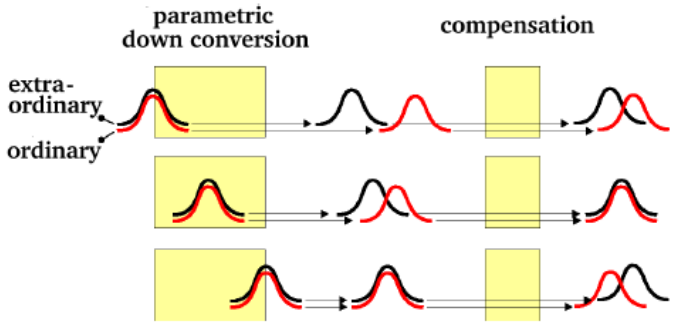


Figure 7: Due to birefringence in the down-conversion crystal the ordinary and extraordinary photons move at different velocities. To make the photons indistinguishable this walk-off effect has to be compensated. This is done using a second BBO of half the length. Between the crystals the polarization of the photons is turned from ordinary to extraordinary and vice versa. In this way they experience the opposite walk-off in the second crystal. Since the pairs might have been created in any part of the first crystal on average the time delay between the photons is compensated. Figure taken from [41].

quantization the interaction of a laser pulse with the crystal can be described as follows:

$$K e^{-i\alpha(a_V^\dagger b_H^\dagger + a_H^\dagger b_V^\dagger)} |0\rangle \tag{2.14}$$

Here $|0\rangle$ denotes the vacuum state, K is a normalization constant, α is proportional to the pulse amplitude and $a_V^\dagger$ is the creation operator of a vertically polarized photon in mode a (analogous for horizontal polarization H and mode b) [43]. This can be expanded as

$$K[1 - i\alpha(a_V^\dagger b_H^\dagger + a_H^\dagger b_V^\dagger) - \frac{\alpha^2}{2}(a_V^\dagger b_H^\dagger + a_H^\dagger b_V^\dagger)^2 + \ldots] |0\rangle . \tag{2.15}$$

So with a probability proportional to α^2 a single pair of photons is emitted in modes a and b in the state

$$|\Psi_{SP}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_a |V\rangle_b + |H\rangle_a |V\rangle_b) \tag{2.16}$$

but with a probability proportional to α^4 two pairs are emitted (which is called a double pair emission). The two pairs are emitted in the state

$$|\Psi_{DP}\rangle = \frac{1}{\sqrt{3}}(|2H\rangle_a |2V\rangle_b + |2H\rangle_a |2V\rangle_b + |H\rangle_a |V\rangle_a |H\rangle_b |V\rangle_b). \tag{2.17}$$

Note that the three terms in this sum appear with equal amplitude since the creation operator acts like $a^\dagger |n\rangle = \sqrt{n+1}\,|n+1\rangle$ meaning $(a_H^\dagger)^2 |0\rangle = \sqrt{2}\,|2H\rangle_a$. Of course with a probability proportional to α^6 three pairs are emitted and so on. In our experiment we will use the single and double pair emissions to align the setup and create our states. This will be described in more detail in the following section.

2.3 The Setup

In this section a specific case of photonic system, is presented. It was used for both experiments described in this thesis and has been used by our group in several experiments in the past due its compactness and high stability [44, 45, 46, 47].

The Setup is based on two parallel interferometers that can be used to generate two different entangled four-qubit states, the linear cluster and the GHZ state. I will first give a general description and then briefly explain how to align the different components.

For our experiments we used a *Coherent* 10 W 532 nm solid state laser (Verdi-V10) to pump a *Coherent* Mira 900, a mode-locked Ti:sapphire laser that generates ultra-short laser pulses (200 fs) at a central wavelength of 789 nm. The mode-locked averaged output power of the Mira is currently up to 1.85 W at a repetition rate of 76 MHz. A lens (f=40 mm) focuses the beam on a 2 mm LBO (lithium triborate, LiB_3O_5) crystal, cut for type-I collinear second-harmonic generation (SHG). After filtering out the remaining infrared light using dichroic mirrors we obtain 394.5 nm UV-light with a cw-averaged power of up to 820 W. Distortions of the beam-shape due to the birefringence of the LBO are corrected using two cylindrical lenses (f_1=100 mm, placed 11.8 cm after the LBO and f_2=110 mm, placed 19 cm after the LBO) mounted perpendicular to each other.

The pulsed UV-beam passes through a 2 mm BBO (β-barium borate, BaB_2O_4) crystal where pairs of entangled photons with a wavelength of 789 nm are produced via SPDC. The infrared photons are emitted under an angle of 3° with respect to the UV beam. The

pairs produced in this first passing of the beam will be called forward pairs. The beam is reflected on a mirror and passes through the BBO again, therefore entangled photons pairs are produced in the opposite direction as well, which will be called backward pairs. Walk-off effects that occur due to the birefringence in the BBO are compensated using a HWP and a 1mm BBO in each path. From the SPDC-crystal the pairs will be emitted in the state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_a |V\rangle_b + e^{i\varphi} |V\rangle_a |H\rangle_b) \tag{2.18}$$

where φ can be adjusted by tilting the compensation BBOs. Two additional HWPs, one in the path of the forward and the other in the path of the backward pair can be adjusted so that the photons can be emitted in any of the four Bell-states.

The photons are emitted into four different paths (a_1, a_2, b_1, b_2) which are pairwise overlapped on two PBSs. Afterwards the photons pass through 3 nm bandwidth filters which select the pairs of equal wavelength from the SPDC. They are coupled into single-mode fibers and led to the detection stage of the experiment where each of the four outputs is analyzed using a QWP and a HWP followed by a PBS which enables us to analyze the polarization of the incoming photons in any basis. After the PBSs the photons are detected by Silicon Avalanche Photo Diodes (Si-APD) with an efficiency of approximately 40%. The detector signals are post-processed in a coincidence logic. To generate the desired states we post select the data and only consider four-fold coincidences between the four outputs of the setup. Using this configuration we can achieve a typical four-fold coincidence rate of 0.33 Hz.

2.3.1 Alignment

Here I will to give a brief introduction in how to align the setup. My focus will be on those procedures that correspond to the fine alignment, which is the most critical and important part. The rough pre-alignment was already implemented and I refer to [41] for a well detailed alignment tutorial.

Following the path of the light in the setup I will start at the very beginning: the Verdi V-10. In principle this is a turn-key system that does not need a lot of attention.

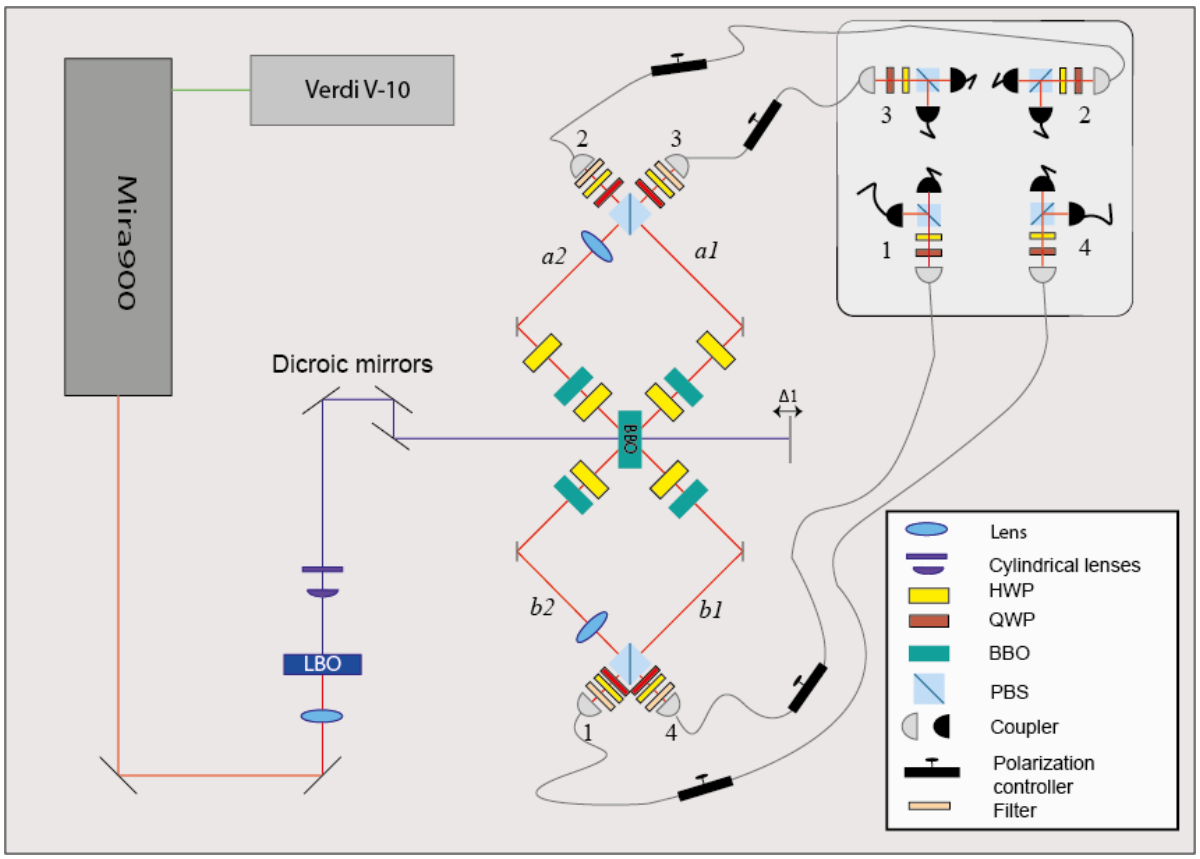


Figure 8: Detailed scheme of the setup used for the experiment.

But two things should be monitored from time to time: first check if the chillers (needed for the Verdi V-10 and the Mira900) are working properly and contain enough water. Second keep track if the diode current (which can be read from the display on the Verdi power supply) is stable over time. If this current should increase significantly (5-10% - currently it is stable at approximately 19 A) this would be a sign that the diodes are no longer working correctly which might lead (among other problems) to instabilities in the output power of the Verdi, consequently in the output beam of the Mira and then in the whole experiment. In this case a *Coherent* technician should be contacted.

The next step is the *Mira*900. From time to time it can be necessary to slightly realign the Mira to increase the output power, improve mode-locking (this might get unstable over time due to back-reflections into the Mira or temperature changes in the laboratory) or correct a slightly changed beam-path.

Figure 9: Part of the *Mira*900 without cover. The screws marked in blue should be used for aligning the *Mira* cavity. Marked in red is the screw that changes the wavelength of the emitted laser light which should be checked regularly.

If the Mira is mode-locked and the output power is satisfying, the next step is to align the LBO together with the lens focusing into it. The lens can be tilted in two directions and the LBO can be translated (using translation stages) along three axes and additionally it can be tilted in two directions. To align this part it is very useful if the rest of the setup is already pre-aligned well enough so that two-fold coincidences can be detected. All of those degrees of freedom should be used to maximize the coincident counts (provided that there are some of them already) or otherwise the power of the UV beam. Notice that the position of maximum power does not necessarily coincide with the position resulting the highest coincidence rates[9] but usually these two settings do not differ very much. It can be useful to alternate between maximizing the power and increasing the coincidence rates. When the LBO is aligned there might be a strong back-reflection of the blue beam visible in the LBO. If possible, this should be avoided since it seems to destabilize the setup and the Mira. We fixed this problem by adding an additional pinhole between LBO and cylindrical lenses. This cuts off a part of the

[9] As the coincidence rate is not only influenced by the power of the UV beam directed at it but also by the focusing and the beam shape at the position of the BBO.

beam and therefore decreases the power but can increase some of the coincidence rates significantly and can reduce oscillations in the count rates.

To align the cylindrical lenses one should again try to maximize the coincidence rates but it is important to be careful. Especially when translating the lens along the axis perpendicular to the beam and the cylinder axis coincidence-counts can easily be lost.

Aligning the parts within the main part of the setup (the part shown in Figure 10) is mostly specific to the state we want to generate, but a few more steps are common to all states. The first one is of course to improve the coupling into the single-mode fibers if possible. This should be repeated regularly, especially, if there is a possibility that the path of the beam has changed, as in the case of problems with the lasers. To improve the coupling of the backward pair also two lenses placed directly before the PBSs can be used. They are also useful to decouple one path if this is necessary to balance the different coincidence rates. It is important as well to check the polarization compensation in the fibers. In the single mode fibers the polarization of the incoming light is rotated due to (stress induced) birefringence in the fiber. Therefore, this (randomly occurring) effect has

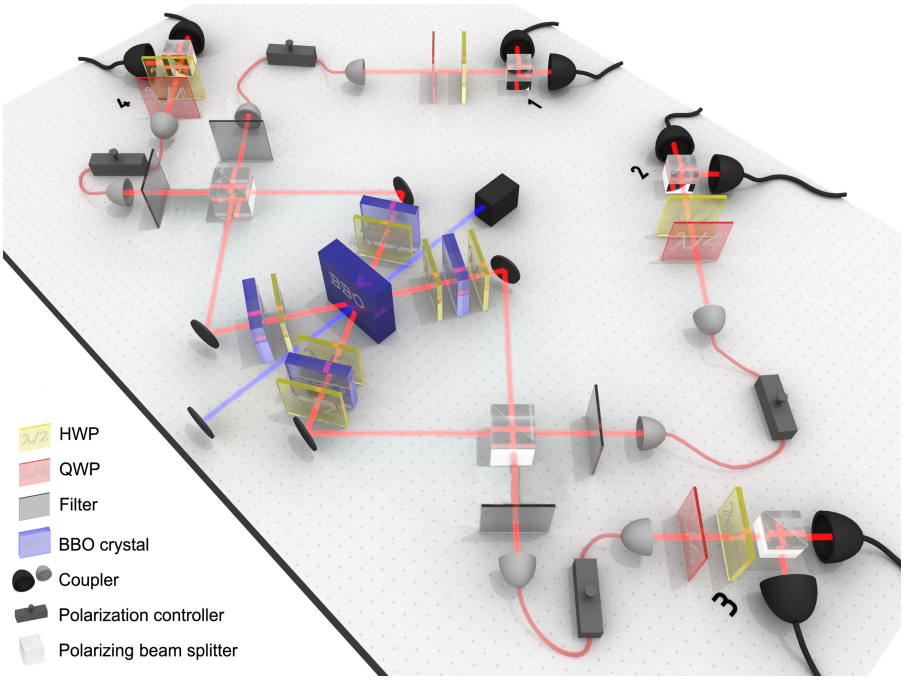


Figure 10: Main part of the setup used for our experiment.

to be compensated if we want to reliably analyze the polarization of the photons. This is realized by applying extra stress to the fiber in a controlled way, using polarization controllers consisting of a rotatable screw squeezing the fiber. In order to check and set the proper polarization we insert additional polarizers in front of the couplers. As the polarization is defined by the two angles θ and φ in the Bloch sphere the transmission in two orthogonal bases has to be checked to verify that any rotation of the polarization can be compensated. First we used polarizers only transmitting horizontally-polarized light and compensate rotations by rotating and turning the screw (stressing the fiber) until a maximum of horizontally and a minimum of vertically polarized light reaches the detector. Then, the polarizers are set to transmit only $|+\rangle$ polarized light and wave plates on the detection stage are set to analyze the photons in the +/− basis. In front of each coupler a QWP (oriented at 45°) succeeded by a HWP is placed and this HWP should be turned to minimize the transmission of $|-\rangle$ while maximizing $|+\rangle$ polarized light. In this way the test of polarization compensation in the two different bases should be alternated until the polarization transmission in both bases is sufficiently aligned.

In recent runs of the experiment it was noticed that the polarization compensation (particularly in mode 1) seems to be less stable than in the past. This might be caused due to the old fibers, less stable mounts, couplers or fiber connectors or instabilities in the temperature. Therefore, the polarization compensation should be checked before every measurement to ensure reliable polarization analysis.

Aligning for the four-qubit linear cluster state

In our experiment we generate the state

$$|C_{lin}\rangle = \frac{1}{2}(|HHHH\rangle + |HHVV\rangle + |VVHH\rangle - |VVVV\rangle) \tag{2.19}$$

which is equivalent under local unitary operations to the linear cluster state (3.17). To create this we set the HWPs in mode $a1$ and $a2$ such that the photons are emitted in a

$|\Phi^{\pm}\rangle$ state. To set the phase φ in the emitted state

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_a |H\rangle_b \pm e^{i\varphi} |V\rangle_a |V\rangle_b) \tag{2.20}$$

the compensation BBOs are tilted such that a $|\Phi^{-}\rangle$ state is emitted into the forward and a $|\Phi^{+}\rangle$ state is emitted into the backward direction. To set the right phase in one of the directions the respective other path (forward or backward) is blocked and polarizers in +/− basis are inserted so that the correlations of the state can be verified in an orthogonal basis. To set e. g. a Φ^{+} state which in the +/− basis can be written as $|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)$ we need to adapt the tilting of the compensation BBO until a minimum in $|+\rangle|-\rangle$ or $|-\rangle|+\rangle$ and a maximum in $|+\rangle|+\rangle$ ($|-\rangle|-\rangle$) is observed.

If we now consider the case that the $|\Phi^{+}\rangle$ and the $|\Phi^{-}\rangle$ are overlapped at the two PBSs, the generated state looks like

$$|\Psi_{FB}^{total}\rangle = \frac{1}{2}(|V\rangle_1 |V\rangle_2 + |H\rangle_3 |H\rangle_4)(|H\rangle_1 |H\rangle_2 - |V\rangle_3 |V\rangle_4). \tag{2.21}$$

Only two terms lead to exactly one photon in each output and therefore cause a four-fold coincidence so after post-selection the state is given by

$$|\Psi_{FB}\rangle = \frac{1}{2}(|H\rangle_1 |H\rangle_2 |H\rangle_3 |H\rangle_4 - |V\rangle_1 |V\rangle_2 |V\rangle_3 |V\rangle_4). \tag{2.22}$$

However it is equally likely that two entangled pairs are emitted in just one of the directions which can also lead to four-fold coincidences. If there are two pairs emitted in forward direction it leads to the state

$$|\Psi_{FF}^{total}\rangle = \frac{1}{2}(|H\rangle_1 |H\rangle_2 - |V\rangle_3 |V\rangle_4)(|H\rangle_1 |H\rangle_2 - |V\rangle_3 |V\rangle_4) \tag{2.23}$$

of which only the term

$$|\Psi_{FF}\rangle = -|H\rangle_1 |H\rangle_2 |V\rangle_3 |V\rangle_4 \tag{2.24}$$

leads to four-fold coincidences.

From the double emissions in the backwards direction we get

$$|\Psi_{BB}^{total}\rangle = \frac{1}{2}(|V\rangle_1|V\rangle_2 + |H\rangle_3|H\rangle_4)(|V\rangle_1|V\rangle_2 + |H\rangle_3|H\rangle_4) \tag{2.25}$$

with the only term leading to four-fold coincidences being

$$|\Psi_{BB}\rangle = |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 . \tag{2.26}$$

If we now consider the ratio between the emission probabilities of a photon pair in the forward and backward mode and $\Delta\phi$ the relative phase between photons emitted in forward and backward direction, the state we get (after post selecting on four-fold coincidences) is given by

$$\begin{aligned} |\Psi_{all}\rangle \;=\; & \frac{1}{2}(re^{i\Delta\phi}|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 - |H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 \\ & + r^2e^{2i\Delta\phi}|V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 - re^{i\Delta\phi}|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4). \end{aligned} \tag{2.27}$$

In $|\Psi_{all}\rangle$ the term $-|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$ still has the opposite sign compared to the linear cluster state. This can be changed using the HWP in mode a_1. Turning the wave plate by an angle θ turns the state to $-cos(2\theta)|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$. Therefore, $\theta > \frac{\pi}{8}$ results in a sign flip. This also turns the Bell state $|\Psi^-\rangle_{a1b1} = \frac{1}{\sqrt{2}}(|H\rangle_{a1}|V\rangle_{b1} - |V\rangle_{a1}|H\rangle_{b1}$ to $\cos(\theta)|\Psi^-\rangle_{a1b1} + \sin(\theta)|\Psi^+\rangle_{a1b1}$. Fortunately this does not lead to any new four-fold coincidence terms after the PBS. Therefore, turning the wave plate changes the state to

$$\begin{aligned} |\Psi_{final}\rangle \;=\; & \frac{1}{2}(r\cos(\theta)e^{i\Delta\phi}|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 + \cos(2\theta)|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 \\ & + r^2e^{2i\Delta\phi}|V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 - r\cos(\theta)e^{i\Delta\phi}|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4). \end{aligned} \tag{2.28}$$

To equalize the amplitudes of the different terms we choose $r = \frac{1}{\sqrt{3}}$ and $\theta \approx 27.5°$ (this might be slightly varied to equalize the four-fold coincidence rates).[10] In the alignment one should take care that, before turning the wave plate, the two-fold coincidences caused

[10]Note that $\theta \approx 27.5°$ has to be added to the rotation of 45° which was applied to set the $|\Phi\rangle$ state.

by forwards pairs are three-times as high as the coincidences from the backwards pair (typically $6000\,\mathrm{s}^{-1}$–$7500\,\mathrm{s}^{-1}$ and $2000\,\mathrm{s}^{-1}$–$2500\,\mathrm{s}^{-1}$).

Additional birefringent effects in the setup (e. g. in the PBS) cause an unwanted extra phase shift in this state. This can be compensated by setting the forwards pair to a $|\Phi^+\rangle$ which will be turned by the phase shift to an effective $|\Phi^-\rangle$.[11]

After setting the proper ratio and checking phase of the Bell-state emitted in the forward and backward direction there is one thing left to be done before turning the HWP (remember that a rotation of θ corresponds to a HWP-setting of $\frac{\theta}{2}$) and starting the measurement: The phase between the forwards and the backwards pairs $\Delta\phi$ has to be set to a multiple of 2π.[12]

For this task we consider the case where only a single pair per pulse is emitted from the BBO which is in the state

$$|\Phi_{SP}\rangle = \frac{1}{2}(|H\rangle_{a1}|H\rangle_{b1} - |V\rangle_{a1}|V\rangle_{b1}) + e^{i\Delta\phi}(|H\rangle_{a2}|H\rangle_{b2} + |V\rangle_{a2}|V\rangle_{b2}). \tag{2.29}$$

This state is entangled in path and polarization. If we analyze this in the +/− basis[13] the state after the PBS can be written as

$$\begin{aligned} |\Phi_{SP}\rangle \;=\; & \frac{1}{4}[(1+e^{i\Delta\phi})(|+\rangle_1|+\rangle_2 + |-\rangle_1|-\rangle_2 + |+\rangle_3|-\rangle_4 + |-\rangle_3|+\rangle_4) && (2.30)\\ & +(1-e^{i\Delta\phi})(|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2 + |+\rangle_3|+\rangle_4 + |-\rangle_3|-\rangle_4)]. && (2.31) \end{aligned}$$

Using a piezo positioning system (with a resolution of 25 nm) we can vary the phase $\Delta\phi$. Scanning the position of the mirror $\Delta 1$ enables us to see fringes[14] in the coincidence rates as shown in Figure 11.

[11] Alternatively additional birefringent elements can be added e. g. before the couplers 3 and 4.

[12] This can also be done after turning the HWP but if errors occur it is easier to identify and correct them before turning the HWP.

[13] To change the basis in which the photons are analyzed in the detection box we used the Labview vi *main_base_rotation.vi*.

[14] For this purpose we use the *Labview vi main_piezo_scan_stefanie.vi*. It is important to stop all other labview vi's (e. g. the counter *main_counter_4photon_single_vs_Ccs.vi*) first because otherwise the scan might not work. Also the Plexiglas plate that covers the setup should be in place during this step because otherwise the setup is not stable enough to observe the fringes.

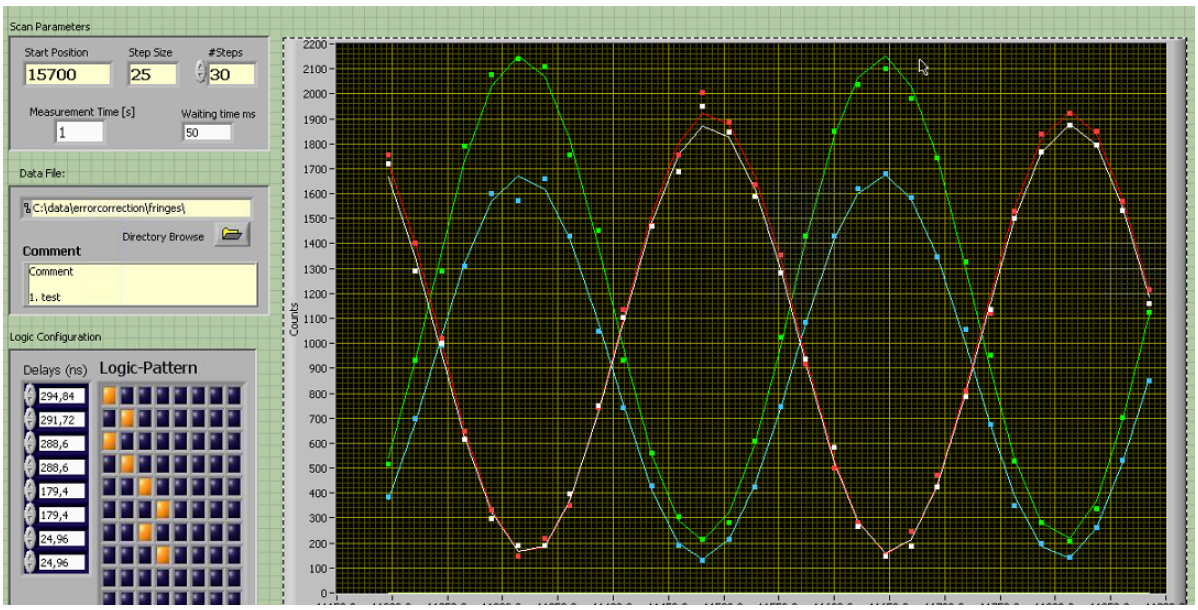


Figure 11: Examplary result of scanning the piezo position. As final position for the piezo a maximum of the white ($|+\rangle_1 |+\rangle_2$) curve should be chosen.

The curves belonging to coincidences rates of $|+\rangle_1 |+\rangle_2$ ($|-\rangle_1 |-\rangle_2$) and the ones corresponding to $|+\rangle_3 |+\rangle_4$ ($|-\rangle_3 |-\rangle_4$) should be anti-correlated. If this is not the case additional phase shifts need to be inserted. Small shifts might also be compensated using the tilting of the compensation BBOs but it is important to be careful not to lose the correct phase in the Bell-states. To set the phase $\Delta\phi$ to a multiple of 2π we fix the mirror in a position where we observe a maximum of $|+\rangle_1 |+\rangle_2$.

After concluding the alignment (i.e. if the ratio is correct, all phases are set and the HWP is turned to the correct position) a measurement can be started.[15]

To analyze the state we are generating with the newly aligned setup we can do a overcomplete state tomography (see Section 2.3.1). As the wave plates we use for polarization analysis are motorized the necessary measurements can be done fully automated and controlled by a PC. Since the measurements for a full tomography usually run for many hours the phase $\Delta\phi$ can be automatically readjusted at regular intervals.

[15]For the measurement we used the vi *main_master_vi.vi*.

Aligning for the four-qubit GHZ state

To generate a four-qubit GHZ state using our setup the alignment obviously differs in some points from the alignment for the cluster state. One of the main differences is that we turn the HWP in mode a_2 so that the backwards pair is emitted in a $|\Psi^+\rangle$ state. The forwards pair is emitted in a $|\Phi^+\rangle$ state. In this way the only four-fold coincidences are produced by double pair emissions in one direction. Two pairs emitted in the backwards direction lead to the state

$$|\Psi_{BB}^{total}\rangle = \frac{1}{2}(|H\rangle_1|V\rangle_3 + |V\rangle_4|H\rangle_2)(|H\rangle_1|V\rangle_3 + |V\rangle_4|H\rangle_2) \tag{2.32}$$

So the only term causing four-fold coincidences is

$$|\Psi_{BB}\rangle = |H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 \tag{2.33}$$

A double pair emission in the forwards path leads to the state

$$|\Psi_{FF}^{total}\rangle = \frac{1}{2}(|H\rangle_3|H\rangle_4 + |V\rangle_1|V\rangle_2)(|H\rangle_3|H\rangle_4 + |V\rangle_1|V\rangle_2) \tag{2.34}$$

after post-selecting the only relevant term is given by

$$|\Psi_{FF}\rangle = |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 \tag{2.35}$$

Coherently overlapping those terms and adding two HWP in the modes 3 and 4 leads to the state

$$|\Psi_{GHZ}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 + e^{i\Delta\phi}|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4) \tag{2.36}$$

Note that in this case we want to have equal two-fold coincidences rates from both forwards and backwards pairs (in this experiment we had typical rates of $2700s^{-1}$). To compensate for unwanted phase shifts (due to birefringence in some of the elements e. g. the PBS) we set the forwards pair to a $|\Phi^-\rangle$ instead of a $|\Phi^+\rangle$. Still the phase between

forwards and backwards pairs has to be set using the piezo system. In this case the visibility of the fringes is lower since only one photon of each pair can interfere in the PBSs (in the case of the cluster state both photons of a pair met and could interfere). Nevertheless we can set the Piezo to a maximum of $|+\rangle_1 |+\rangle_3$ which leads to the correct phase in the output state. Note that we are now looking at different coincidence rates and we observe the correct phase if the curves are correlated.[16]

State Analysis using State Tomography

As mentioned above over-complete state tomography [1, 2] can be used to reconstruct the density matrix of the states we generated in our experiment. This requires in general 3^N measurement settings, so 81 for our four qubits. Those 81 measurement settings are all possible combinations of measuring the qubits in Z,X and Y basis. For each setting the detected coincidences for all 16 combinations of outputs are collected. From this data the density matrix can be reconstructed using the maximum likelihood approximation [1]. In principle it would be sufficient to collect only a subset of this data (e. g. all combinations of $\{|0\rangle, |1\rangle, |+\rangle, |R\rangle\}$) but since we always collect data from both outputs of the PBS with our system to analyze polarization we can use all combinations of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |R\rangle, |L\rangle\}$ (over-complete data) which reduces the error. The error is calculated using a Monte Carlo simulation of the analysis of the state tomography in which Poissonian noise is added to the count statistics in each run [2].

[16] The other coincidences we looked at were $|+\rangle_2 |+\rangle_4$,$|-\rangle_1 |-\rangle_2$,$|-\rangle_3 |-\rangle_4$.

3 Efficiently Characterizing Multi-Qubit Stabilizer States

Multi-qubit states are an essential resource for the next generations of experiments in quantum information as well as for future quantum computing and communication. In particular N-qubit stabilizer states are a well-proved resource for one-way quantum computation and quantum information processing [6, 7, 5]. The full characterization of such systems raises significant challenges as the extraction of state properties typically scales exponentially with the number of qubits. Here a new method for characterizing stabilizer states, that scales linearly with the number of qubits, is presented. It is compared to different other special purpose methods (among them also another linearly scaling method) that are tailored for estimating e. g. only the quantum state fidelity.

3.1 Theoretical Background

The theoretical concepts presented here were mainly developed by Mordecai Waegell and discussed in great detail in [48, 27]. I will give here a short introduction to the concepts behind the experimental work presented later on. Starting with the concepts of Identity Products it will be shown how to construct tests of the GHZ theorem and a Bell-like inequality based on those structures. Finally, the derived Bell-like parameter will be used to get fidelity bounds for an experimentally produced state and to test whether quantum entanglement has been generated experimentally.

3.1.1 Identity Products (IDs)

Identity Products (IDs) were first introduced by M. Waegell and P. Aravind in 2012 [49] and are in detail described in [27] and [48]. They are fundamental non-classical structures strongly related to N-qubit entanglement and are defined as sets of mutually commuting observables with the additional property that their overall product is $\pm\mathbb{I}$ (identity in the space of all N qubits). Throughout this work IDs will be written as tables in which every row is one observable and each column corresponds to a single qubit. An example is given in Table 2.

X	X	X
Y	X	Y
X	Y	Y
Y	Y	X

Table 2: ID made from four three-qubit observables. The rows (XXX,YXY,YYX) show the three-qubit observables (yellow ellipse) and each column corresponds to one qubit (red ellipse). Tensor product signs between the columns are omitted for better readability. In each column every single-qubit observable appears twice (as highlighted by the different colors in the first column).

IDs will be the fundamental structures behind many of the applications and ideas shown in this work later on so in the following some useful definitions concerning important properties of IDs are given:

- **Positivity/Negativity**: Since the product of all observables of an ID has to be either $+\mathbb{I}$ or $-\mathbb{I}$ one can define two types of IDs: **positive** IDs (with an overall product of $+\mathbb{I}$) and **negative** IDs (with an overall product of $-\mathbb{I}$).

- **Single-Qubit-Product (SQP)**: The product of all single-qubit observables in one column (corresponding to one qubit) of an ID might also be referred to as **Single-Qubit-Product (SQP)**.

- **even and odd SQPs**: In **even** SQPs every single-qubit observable appears an

even number of times and analogously in **odd** SQPs every single-qubit observable appears an odd number of times.

- **IDM$^{\mathbf{N}}_{\mathbf{O}}$**: An ID is given a name that characterizes some of its central properties. This name has the structure

$$ID\mathbf{M}^{\mathbf{N}}_{\mathbf{O}} \tag{3.1}$$

where **M** is the number of observables (rows) in the ID, **N** is the number of qubits (columns) and **O** is the number of odd Single Qubit Products (SQPs) in the ID. Therefore, the example in Table 2 is an $ID4^3_0$.

- **partial and whole IDs**: IDs with $O > 0$ will be called **partial** IDs whereas IDs without odd SQPs (ID_0s) will be called **whole** IDs.

- **entangled IDs**: An ID is maximally entangled if it is not possible to simultaneously tensor-factorize its observables O_i into two or more smaller IDs. This ensures that the joint eigenbasis of the M observables that form the ID is maximally entangled over all N qubits.[17]

- **critical IDs**: An entangled ID is critical if one cannot get a smaller ID by deleting observables and/or qubits from the ID. This definition guarantees that a critical ID is a minimal or irreducible non-classical structure. The maximal number of observables in a critical ID is $M = N + 1$

- **unique or representative IDs**: For the applications presented in this thesis we are interested in the different possible kinds of IDs. It should be noticed that certain modifications will not change the relevant properties of an ID. Therefore, not every ID has to be considered individually. A **representative** or **unique** ID stands for the whole class of IDs which can be obtained by all possible permutations of the observables in an ID and the qubit order as well as rotations or reflections of each qubits coordinate system.

[17] For a proof of this statement see the appendix of [27].

- **complete IDs**: The maximum number of observables M in a critical ID is M=N+1. This case is called a **complete ID**. The set of observables in a complete ID fully define, a maximally entangled (eigen-)basis. Furthermore by taking the products of those observables it is possible to generate the whole stabilizer group [5] of that basis.

3.1.2 Constructing GHZ Tests from IDs

As described in Section 1.5 the GHZ theorem allows us to violate local-realistic models, originally in the three-qubit case but it can easily be generalized for N-qubits. The purpose of this section is to show how a N-qubit GHZ theorem and experimental tests of such can be constructed using IDs [27].

Any whole negative ID can be used to construct a GHZ proof which can be seen as follows: The wholeness of the ID guarantees that every single Pauli-observable (Z_q,X_q,Y_q) appears an even number of times in the ID. Therefore, any LHVT will predict that if we measure all the observables in the ID the product of the measurement outcomes will be `+1`. On the other hand the negativity of the ID tells us that the product of all N-qubit observables in the ID is $-\mathbb{I}$. Consequently, quantum mechanics will predict an outcome of `-1` for the product of all measurement outcomes.

We can use this contradiction between the predictions of quantum mechanics and local hidden variable theories to test a N-party GHZ theorem. For the ideal case we need a source that repeatedly produces a joint eigenstate of the ID and N space-like separated detectors that randomly measure the operators Z_q,X_q,Y_q and I_q. After that the sets of measurements, where the observables from the ID were measured, are selected and the others are discarded. Then the product of the measurement outcomes is calculated and compared to the predictions of quantum mechanics and LHVTs. If the result is found to be `-1` (in an ideal measurement) N-party nonlocality is shown [27].

In a realistic experimental setup there are of course some imperfections to be dealt with. First the eigenstate will not be produced with perfect fidelity which leads to measured expectation values with an absolute value smaller than `1`. Second it is very hard to

realize space-like separation of the detectors especially as N increases, meaning this will probably not be possible in an actual experiment. In our realization also the requirement of randomly chosen experimental setting had to be dropped. But nevertheless we were able to perform a proof-of-principle demonstration of a N-party GHZ test (see Section 3.2).

As we have seen, the only requirements an ID has to meet to construct a GHZ theorem, are to be whole and negative. However there is one more subtle distinction between two possible kinds of constructed GHZ tests that should be mentioned here:

- GHZ tests based on non-critical IDs:
  As mentioned above it is not necessary for an ID to be critical to allow us to construct a GHZ test. In this case it is sufficient that the used eigenstate of the ID is a maximally entangled N-qubit state (like in [50]) . But in this case there also exist other eigenstates in which only a subset of η qubits is maximally entangled $(3 \leq \eta < N)$ and with which it is still possible to demonstrate the GHZ theorem. In this case some of the qubits (that are not part of the maximally entangled state) can simply be ignored. This can happen because an ID that is non-critical always belongs to several different stabilizer groups corresponding to different kinds of entanglement. This situation still allows to test the GHZ theorem but the same measurements would also allow to demonstrate $\eta-$party nonlocality if a different eigenstate would be prepared.

- GHZ tests based on critical IDs:
  In this case only N-party nonlocality can be shown and it can only be shown using an eigenstate of the ID where all N qubits are maximally entangled. This kind of GHZ tests have been called *strongly genuine N-partite two-level GHZ paradoxes* in [27]. This must not be confused with what is often called *genuine N-partite nonlocality* e. g. in [15]. The kind of local hidden variable theories we can exclude using the IDs method assumes that the probability distribution for each qubit is

independent of all others:

$$\langle A_i B_j C_k ... \rangle = \int d\lambda p(\lambda) \mathfrak{A}_\lambda(A_i) \mathfrak{B}_\lambda(B_j) \mathfrak{C}_\lambda(C_k) ... \tag{3.2}$$

To ensure *genuine N-partite nonlocality* one has to exclude also hybrid theories in which the measurement result might be explained by a subset of parties having a joint probability distribution. Which e. g. in the three partite case would look like this

$$\begin{aligned} \langle A_i B_j C_k \rangle \quad &= p_1 \int d\lambda p(\lambda) \mathfrak{A}_\lambda(A_i) \mathfrak{D}_\lambda(B_j C_k) + p_2 \int d\lambda p'(\lambda) \mathfrak{B}_\lambda(B_j) \mathfrak{E}_\lambda(A_i C_k) \\ &\quad + p_3 \int d\lambda p''(\lambda) \mathfrak{C}_\lambda(C_k) \mathfrak{F}_\lambda(A_i B_j) \end{aligned} \tag{3.3}$$

with $p_1 + p_2 + p_3 = 1$ [15].

This can be done using the Svetlichny inequality [51] which requires more measurements than our method.

Bell-like Inequalities for ID GHZ Tests

In real experiments the fidelity of prepared states is limited, therefore to implement the above derived test of the GHZ theorem it is helpful to have a Bell-like inequality. This kind of inequality can directly be constructed from the ID we used for the GHZ test. Starting from a given whole negative IDM^N composed of M observables O_i with a joint eigenstate and corresponding eigenvalues λ_i $(i = 1, ..., M)$ we define the operator α

$$\alpha = \sum_i \lambda_i O_i = \sum_{i|\lambda=+1} O_i - \sum_{i|\lambda_i=-1} O_i \ . \tag{3.4}$$

According to quantum mechanics the expectation value of this operator is $\langle \alpha \rangle_{QM} = M$. But for any local hidden variable theory the following inequality must hold

$$\langle \alpha \rangle_{LHVT} \leq M - 2 \tag{3.5}$$

which we will call the *ID-Bell inequality* [52]. It can be proofed as follows:

We know that due to the wholeness of the ID each single-qubit Pauli observable (Z_q, X_q, Y_q) has to appear an even number of time in the ID. In any LHVT, the eigenvalues of those observables must belong to a noncontextual[18] value assignment. Therefore, also the total number η of observables, that are assigned the eigenvalue `-1`, must be even. This constraint enables us to obtain an upper bound on the expectation value $\langle\alpha\rangle_{LHVT}$ in any LHVT.

If we try to construct a LHVT that fulfills the prediction of quantum mechanics, every term in α must be positive overall so the expectation value adds up to M. This means that each term O_i in the left sum must contain an even number of single-qubit Pauli observables assigned the value `-1`, and each term in the right sum must contain an odd number of them. Now we enumerate the different configurations that can realize this constraint: Say that there are n terms in the left summation which contain two single-qubit observables assigned a `-1`, m terms that each contain four `-1`s, l terms with six and so on. Likewise there are r terms in the right summation that each contain a single `-1`, s terms that each contain three `-1`s, t terms with five and so on. Because the ID is negative the overall number of terms in the right summation $\gamma = r + s + t + \ldots$ always has to be odd.

Using these definitions, we can now write for η the total number of observables that are assigned the value `-1`

$$\eta = (2n + 4m + 6l + \ldots) + (r + 3s + 5t + \ldots) = (2n + 4m + 6l + \ldots) + (2s + 4t + \ldots) + \gamma. \quad (3.6)$$

Looking at the right side of the equation one can easily see that all the numbers in the parentheses are even. But because the ID is negative γ has to be odd and therefore η must be odd too (so M, the maximum value for $\langle\alpha\rangle$ cannot be reached).

This means that it is impossible for a LHVT to agree with the quantum mechanical predictions. Since the ID is whole η has to be even and this causes at least one term in

[18] This means that the values have to be context-independent, so they must not depend on the measurements performed on other parts of the system.

α to be negative. This yields an upper bound for any LHVT:

$$\langle \alpha \rangle_{LHVT} \leq M - 2 \tag{3.7}$$

which is finally the ID-Bell inequality given above [52].

3.1.3 Fidelity Bounds using IDs

Certifying the generation of the right kind of entanglement is a crucial step in any quantum information experiment. In particular before performing a quantum computation it should be possible to verify if the right kind of resource state has been prepared. Therefore, it is an important task to measure or estimate the fidelity of a generated state. As the general description of multi-qubit states becomes rapidly more complex and the size of the Hilbert space increases exponentially with the number of qubits a major question is how the number of measurement settings increases as the size of the state grows. It seems obvious that methods scaling exponentially in the system size will become impractical even for comparatively low qubit numbers.

One of the advantages of the above derived ID-Bell inequalities is that it can be violated even if we are not able to produce the eigenstate of the ID with perfect fidelity which makes it testable in a real experiment. Even more remarkable is the fact that if we experimentally determine the ID-Bell parameter $\langle \alpha \rangle_{exp}$ we can use it to calculate a lower bound for the fidelity of the generated state with respect to the ideal eigenstate of the ID which will be called $|\kappa_0\rangle$. To show how this can be done it is helpful to first consider the (idealized) case where the state we produced is a pure state $|\Psi\rangle$ which is not exactly equal to the state $|\kappa_0\rangle$ but can be expressed in the eigenbasis of our ID:

$$|\psi\rangle = a\,|\kappa_0\rangle + \sum_i b_i\,|\kappa_i\rangle\,, \tag{3.8}$$

where $|a|^2 + \sum_i |b_i|^2 = 1$. It is possible to use the measured value $\langle \alpha \rangle_{exp}$ to put a lower

bound on the amplitude a of our target state $|\kappa_0\rangle$. To see this consider

$$\langle\alpha\rangle = |a|^2 |\langle\kappa_0|\alpha|\kappa_0\rangle + \sum_i |b_i|^2 \langle\kappa_i|\alpha|\kappa_i\rangle . \tag{3.9}$$

Then we allow for the presence of noise and use the relations $\langle\kappa_0|\alpha|\kappa_0\rangle = M$ and $\langle\kappa_i|\alpha|\kappa_i\rangle \leq M-4$. This holds because other eigenstates of the ID must have different eigenvalues than $|\kappa_0\rangle$ but the product of the eigenvalues of the observables of the ID is fixed. Therefore, we get at least two terms in (3.4) with a negative sign and this leads to the maximum value of $M-4$. All together this gives

$$|\alpha\rangle \leq M|a|^2 + (M-4)\sum |b_i|^2 = 4|a|^2 + M - 4 \ , \tag{3.10}$$

which we can rewrite as

$$|a|^2 \geq (\langle\alpha\rangle - M + 4)/4 \ . \tag{3.11}$$

So $\langle\alpha\rangle_{exp}$ is an experimental lower bound on the amplitude of $|\kappa_0\rangle$ within the state $|\psi\rangle$. It should be mentioned that convex combinations of these specific pure states (excluding $|\kappa_0\rangle$) and/or noise models cannot increase $\langle\alpha\rangle$, so the Bell inequality holds for mixed states as well [52].

This derivation can now be generalized to the (more realistic) case where a mixed state was experimentally prepared. One can write for a general convex combination of m different pure states and noise:

$$\rho = c_0 I + \sum_{j=1}^{m} c_j |\psi_j\rangle\langle\psi_j| , \tag{3.12}$$

with $\sum c_j = 1$. As a next step we can expand each $|\psi_j\rangle$ as in Equation3.8, and following analogous arguments one obtains:

$$\langle\alpha\rangle \leq \sum_{j=1}^{m} c_j(4|a_j|^2 + 1). \tag{3.13}$$

Since in an experiment we have no access to the coefficients c_j, we must allow the constant

term to take its maximum value, and so we obtain

$$\langle |a|^2 \rangle \geq (\langle \alpha \rangle - M + 4)/4 \tag{3.14}$$

where $\langle |a|^2 \rangle \equiv \sum c_j |a_j|^2$ is the weighted average amplitude of $|\kappa_0\rangle$ among the pure states that make up ρ (for the amplitude a_0 of the ideal state $|\kappa_0\rangle$ in the noise component we assume $|a_0|^2 = 0$). So we are able to place a lower bound on the average amplitude of $|\kappa_0\rangle$ within a mixed state ρ. This is an important achievement since we can now use $\langle |a|^2 \rangle$ as a direct measure of the fidelity of the generated state:

$$\mathcal{F}_{\min} = \langle |a|^2 \rangle \geq (\langle \alpha \rangle - M + 4)/4 \ . \tag{3.15}$$

A further question one could ask is what has to be the minimum fidelity of the prepared state with which we can still violate the ID-Bell inequality?

This can be answered by simply setting $\langle \alpha \rangle$ to the maximum for a LHVT $\langle \alpha \rangle = M - 2$ and inverting Equation 3.15 by which we obtain

$$\langle a|^2 \rangle_{nl} > 1/2 \ . \tag{3.16}$$

If we can prepare the state $|\kappa_0\rangle$ with a fidelity greater than 1/2, we will be able to demonstrate N-qubit nonlocality.

Until now we have shown that an ID can be used to construct an ID-Bell inequality which allows us to find a lower bound on the fidelity of an experimentally generated state. It should be mentioned that this derivation does also hold for IDs that are not whole and negative and therefore can not be used for tests of the GHZ theorem. For any graph state we can find an ID that has this graph state as a joint eigenstate and use this ID (even if it is positive, partial or non critical) to find a lower bound of the fidelity [52].

Another important point already mentioned in the beginning of this section is the scaling of the method. With the ID approach it becomes possible to certify the preparation of a specific quantum state with a maximum of N+1 measurement settings which are

necessary to determine $\langle\alpha\rangle_{exp}$.

This is an enormous speedup compared to e. g. over-complete quantum state tomography (QST) [1, 2] which has been used by our group in past experiments and requires 3^N measurement settings for N qubits. There exist two other methods that should be mentioned here, using incomplete data (i.e that do not reconstruct the density matrix), which allow to estimate the state fidelity. The first approach ([3, 4]) uses the stabilizer group (SG) [5] and is based on the measurement of 2^N observables. It still scales exponentially even if it uses less resources than QST. Additionally, this approach tends to overestimate the state fidelity in the presence of noise, which might jeopardize the actual applicability of the characterized state.

The second method I want to mention is the estimation of fidelity using the generators of the stabilizer group ($GoSG$) of a given state [53, 54]. It requires the measurement of only N operators (precisely the generators) so it scales linearly in N, similar to the ID approach but under realistic experimental conditions shows lower values than the ID-method. In Section 3.2.4 an analytical comparison of the two methods is shown. Additionally it should be emphasized that the ID method provides a more detailed analysis since it is designed to capture all at once different quantum features of a prepared state.

3.1.4 Entanglement Discrimination using IDs

The fidelity of an experimentally generated state is never ideal. The ID-Bell inequality can help identifying the generated kind of entanglement.

To demonstrate this let us consider as an example the four-qubit linear cluster state given by

$$|C'_{lin}\rangle = (|+00+\rangle + |+01-\rangle + |-10+\rangle - |-11-\rangle)/2 \ . \tag{3.17}$$

In our experiment we generate a state which is equivalent to this state under local unitary operations

$$|C_{lin}\rangle = (|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)/2 \ . \tag{3.18}$$

This is the joint eigenstate of the ID given in Table 3. Using this whole negative

Z	Z	I	I
Z	I	X	X
I	Z	Y	Y
Y	X	X	Y
Y	X	Y	X

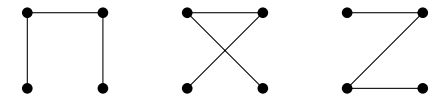
Table 3: Example of a $\mathrm{ID}4_0^5$ which has the four-qubit linear cluster state as a joint eigenstate.

ID we can construct a ID-Bell inequality and it turns out that other pure quantum states will never lead to a value of $\langle\alpha\rangle > 3$ which is in this case also the maximum value achievable by LHVTs. This upper bounds have been obtained by constructing $\langle\alpha\rangle$ for a general four-qubit pure state $|\psi\rangle$ using numerical maximization techniques. By grouping the states depending on how their qubits are entangled this analysis could be carried out. Starting with a particular kind of entanglement it is possible to explore the whole entanglement class using only local unitary (LU) operations which significantly reduces the number of free parameters one needs to consider. The result of this maximization for the given ID is shown in Figure 4[52].

State Type	$\langle\alpha\rangle_{max}$	State Type	$\langle\alpha\rangle_{max}$
$\|\psi_1\rangle\|\psi_2\rangle\|\psi_3\rangle\|\psi_4\rangle$	2	$\|\psi_3\rangle\|GHZ_{124}\rangle$	3
$\|\psi_1\rangle\|\psi_2\rangle\|\Phi_{34}\rangle$	3	$\|\psi_4\rangle\|GHZ_{123}\rangle$	3
$\|\psi_1\rangle\|\psi_3\rangle\|\Phi_{24}\rangle$	2	$\|\psi_1\rangle\|W_{234}\rangle$	2.6667
$\|\psi_1\rangle\|\psi_4\rangle\|\Phi_{23}\rangle$	2	$\|\psi_2\rangle\|W_{134}\rangle$	2.6667
$\|\psi_2\rangle\|\psi_3\rangle\|\Phi_{14}\rangle$	2	$\|\psi_3\rangle\|W_{124}\rangle$	2.3610
$\|\psi_2\rangle\|\psi_4\rangle\|\Phi_{13}\rangle$	2	$\|\psi_4\rangle\|W_{123}\rangle$	2.3610
$\|\psi_3\rangle\|\psi_4\rangle\|\Phi_{12}\rangle$	2	$\|GHZ_{1234}\rangle$	3
$\|\Phi_{12}\rangle\|\Phi_{34}\rangle$	3	$\|W_{1234}\rangle$	3
$\|\Phi_{13}\rangle\|\Phi_{24}\rangle$	1	$\|C_{\text{⧖}}\rangle$	3
$\|\Phi_{14}\rangle\|\Phi_{23}\rangle$	1	$\|C_{\text{⌟}}\rangle$	3
$\|\psi_1\rangle\|GHZ_{234}\rangle$	3	$\|C_{lin}\rangle$	**5**
$\|\psi_2\rangle\|GHZ_{134}\rangle$	3		

Table 4: Full results of the maximization of $\langle\alpha\rangle$ over local unitary operations for different states. Here $|\psi_1\rangle|\psi_2\rangle|\psi_3\rangle|\psi_4\rangle$ is a fully separable state, $|\Phi\rangle$ is a 2 qubit Bell-state, $|C_{\text{⧖}}\rangle$ (*shear* cluster) and $|C_{\text{⌟}}\rangle$ (Z cluster) are reached by exchanging the order of qubits in the linear cluster state $|C_{lin}\rangle$.

One can clearly see that states belonging to different entanglement classes like the four-qubit GHZ state $|\mathrm{GHZ}_4\rangle = (|0000\rangle + |1111\rangle)/\sqrt{2}$ or the four-qubit W state $|W_4\rangle = (|1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle)/2$ cannot exceed the LHVT-bound of $\langle\alpha\rangle = 3$. But since the linear cluster state is not entirely symmetric under the exchange of qubits we also need to consider the *shear*-cluster $|C_{\bowtie}\rangle = (|0000\rangle + |0101\rangle + |1010\rangle - |1111\rangle)/2$ and the Z-cluster $|C_{\sqsubset}\rangle = (|0000\rangle + |0110\rangle + |1001\rangle - |1111\rangle)/2$ which are reached by exchanging the order of the qubits in $|C_{lin}\rangle$. The graphs corresponding to those cluster states are given in Figure 12.



(a) $|C_{lin}\rangle$ (b) $|C_{\bowtie}\rangle$ (c) $|C_{\sqsubset}\rangle$

Figure 12: Graphs corresponding to the linear cluster $|C'_{lin}\rangle$, the shear cluster $|C_{\bowtie}\rangle$ and the Z cluster $|C_{\sqsubset}\rangle$.

The states given here are the only Pauli states for four qubits, but actually there are an infinite number of entanglement classes for four and more qubits that are inequivalent to one another under local unitary transformations. Using this method we cannot consider all of them. At present no good approach to solve this general problem is known [52].

We have seen that a violation of the inequality allows us to certify four-party entanglement. Additionally it allows us to rule out the four-qubit GHZ and W states, as well as all other cluster states: Unfortunately to rule out other maximally entangled four-qubit states a more comprehensive calculation would be necessary.

Taken together, this shows that the inequality $\langle\alpha\rangle \leq 3$ can only be violated by a four-party nonlocal theory. Within the four-qubit Pauli group this can only be done by one specific cluster state $|C_{lin}\rangle$ - or states that include it as a part of a superposition or mixed state.

With regard to the experimental states created within our setup (see Section 3.2) this analysis has also been done for the three-qubit GHZ state for which a whole negative critical ID exists which is shown in Figure 13.

$$\begin{array}{ccc} X & X & X \\ Y & X & Y \\ X & Y & Y \\ Y & Y & X \end{array}$$

Figure 13: $\mathrm{ID}4_0^3$ corresponding to the three-qubit GHZ state.

The results of the maximization for the ID-Bell parameter $\langle\alpha\rangle$ corresponding to this ID are given in Table 5.

State Type	$\langle\alpha\rangle_{max}$
$\|\psi_1\rangle\|\psi_2\rangle\|\psi_3\rangle$	$\sqrt{2}$
$\|\psi_i\rangle\|\Phi_{jk}\rangle$	2
$\|W_3\rangle$	3
$\|\mathrm{GHZ}_3\rangle$	4

Table 5: Results of the maximization over local unitaries for $\langle\alpha\rangle$ constructed from the $\mathrm{ID}4_0^3$ given in Figure 13.

In this case the W state can violate the ID-Bell inequality but not reach the maximum value $\langle\alpha\rangle = 4$ given for the GHZ state.

For the four-qubit GHZ state no whole negative ID exists and therefore no GHZ argument and corresponding ID-Bell inequality can be constructed. Nevertheless IDs that have the GHZ state as a joint eigenstate, like the one given in Figure 14, can be used in practice to derive a lower bound on the fidelity of an experimentally generated quantum state.

$$\begin{array}{cccc} Z & I & Z & I \\ Z & Z & I & I \\ I & Z & I & Z \\ X & Y & X & Y \\ X & Y & Y & X \end{array}$$

Figure 14: $\mathrm{ID}5_2^4$ which has four-qubit GHZ state as a joint eigenstate. As it is not a whole negative ID it cannot be used to derive a test of the GHZ theorem. Nevertheless it can be used to find a lower bound on the fidelity.

3.2 Experimental Realization

To demonstrate the efficiency and practicability of the above described ID-Bell inequality and its applications we experimentally generated different multi-qubit entangled states using a photonic setup. The qubits were encoded in the polarization of photons which were generated using a „railway-crossing configuration“ based on a double SPDC process, bulk optics and motorized tomographic elements which allowed for reliable measurements over a long time [44, 45, 46, 47].

Especially useful to demonstrate the versatility of our method was the four-qubit linear cluster state which is the eigenstate of a critical whole negative ID. This enabled us to construct a test of the GHZ theorem, violate an ID-Bell inequality and find a lower bound on the fidelity of the experimentally generated state using only five measurement settings. We compared this result with estimations of the fidelity using over-complete quantum state tomography (QST)[1, 2], an approach which uses the stabilizer group (SG) of the state [3, 4] and a method relying on the generators of the stabilizer group (GOSG)[53, 54]. Additionally, using the process of entanglement discrimination, we could test which kind of entanglement was generated in our experiment.

Projecting one of the qubits in the four-qubit linear cluster state we created a state equivalent under LU operations to a three-qubit GHZ state. Since for this state a critical whole negative ID exists as well we could exploit the full possibilities of the ID approach.

Finally, we generated four-qubit GHZ state for which it is not possible to construct a whole negative ID but we demonstrated that, using a partial positive ID, a lower bound on the fidelity can be found. Also in this case we compare our method to other approaches for the estimation of the state fidelity.

3.2.1 The four-qubit Cluster State

As described in Section 2 we experimentally generated the state $|C_{lin}\rangle$ (which is equivalent under LU operations to the linear cluster state)

$$|C_{lin}\rangle = \frac{1}{2}(|HHHH\rangle + |HHVV\rangle + |VVHH\rangle - |VVVV\rangle) \ . \tag{3.19}$$

This is the eigenstate of a whole negative critical ID and therefore we could characterize it using our ID method.

Testing the GHZ Theorem

The state $|C_{lin}\rangle$ is the joint eigenstate of the critical whole negative $\mathrm{ID}4_0^5$ given in Table 6. It can easily be seen that every single-qubit observable appears an even number of

Z	Z	I	I
Z	I	X	X
I	Z	Y	Y
Y	X	X	Y
Y	X	Y	X

Table 6: Critical whole negative $\mathrm{ID}4_0^5$ to which the four-qubit linear cluster state is a joint eigenstate.

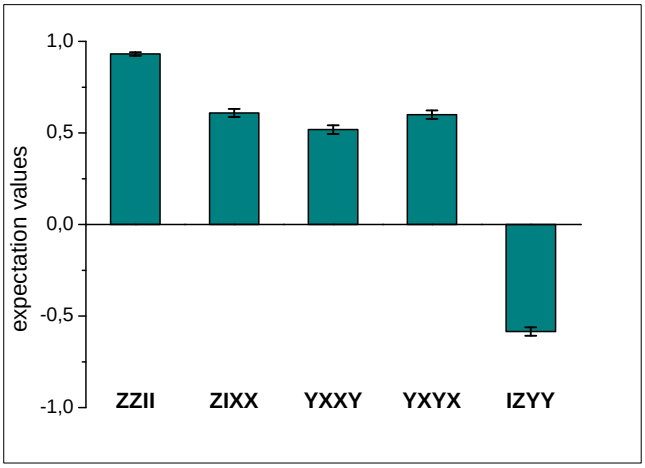
times in the ID, but since it is a negative ID the overall product of the observables is $-\mathbb{I}$. Therefore, as described in Section 3.1.2, we can use it to test the GHZ theorem. If our measurement results agree with the predictions of LHVTs, the product of all five measurement outcomes should be +1, if they agree with QM, the product should be −1. Due to experimental imperfection we can not reach ideal values (± 1) but we can tell if the product is positive or negative and by how many standard deviations. The measured expectation values of the observables in the ID are shown in Figure 15 .

The product of all measured observables is $P = -0.103 \pm 0.008$ which is negative by more than 12 standard deviations. This result is clearly in favor of QM, meaning that we proved four-qubit nonlocality.

Another way of demonstrating nonlocality using our results is the ID-Bell inequality which in the four-qubit case is given by

$$\langle \alpha \rangle_{LHVT} \leq 3 \ . \tag{3.20}$$

Using the results of our measurement we find $\langle \alpha \rangle_{\mathbf{exp}} = \mathbf{3.24 \pm 0.05}$ which corresponds to a violation of 4.8 standard deviations and therefore again clearly demonstrates four-party nonlocality.



observable	expectation value
ZZII	0.93 ± 0.01
ZIXX	0.61 ± 0.02
YXXY	0.52 ± 0.02
YXYX	0.60 ± 0.02
IZYY	-0.59 ± 0.02
Product	$\mathbf{-0.103 \pm 0.008}$
$\langle\alpha\rangle_{\mathbf{exp}}$	$\mathbf{3.24 \pm 0.05}$

Figure 15: Measured expectation values for $ID5_0^4$. Due to the reduced fidelity (0.629±0.007 according to QST) and experimental imperfections the ideal values of ±1 cannot be reached but the results can be used to clearly demonstrate four-qubit nonlocality. The acquisition time for each setting was 4800s. The error bars were derived from Poissonian statistics and thus correspond to a lower limit.

Entanglement Discrimination

We can also use the measured ID-Bell parameter to analyze which class of entanglement has been created in our experiment. As described in Section 3.1.4 the only state that can violate the ID-Bell inequality based on the ID shown in Table 6 is the four-qubit linear cluster state. The maximum values for other four-qubit entangled states are shown in Table 7. The measured ID-Bell parameter of $\langle\alpha\rangle_{\mathbf{exp}} = \mathbf{3.24 \pm 0.05}$ clearly can not be explained by any of the four-qubit states in Table 7 but $|C_{lin}\rangle$. The states shown in Table 7 and 4 include all Pauli states for four qubits. As there exists an infinite number of LU inequivalent entanglement classes for four qubits a much more comprehensive calculation would be required to obtain a bound for a general four-qubit state. In any case, given that the Bell state is the only class of two-qubit states, and the GHZ and W states are the only classes for three qubits, our entanglement discrimination allows us to fully certify four-party entanglement. Additionally, we can rule out some other

State Type	$\langle\alpha\rangle_{max}$
$\|W_4\rangle$	3
$\|\mathrm{GHZ}_4\rangle$	3
$\|C_{\text{⧖}}\rangle$	3
$\|C_{\text{⌐}}\rangle$	3
$\|C_{lin}\rangle$	**5**

Table 7: Results of the maximization of $\langle\alpha\rangle$ over all possible local unitary operations for different four-qubit entangled states. $|C_{\text{⧖}}\rangle=(|0000\rangle+|0101\rangle+|1010\rangle-|1111\rangle)/2$ and $|C_{\text{⌐}}\rangle=(|0000\rangle+|0110\rangle+|1001\rangle-|1111\rangle)/2$ are reached by exchanging the order of qubits in the linear cluster state. The full table, also including states where not all four qubits are entangled is shown in Table 4.

maximally entangled four-qubit states. Although, there are no general numerical results for $N \geq 4$, we conjecture that the violation of the ID-Bell inequality can happen only with the specific stabilizer state (up to LU transformations) which is the joint eigenstate of the ID - or states that include it as a part of a superposition or mixed state [52].

Fidelity Bound

We can also use the measured parameter to find a lower bound on the fidelity using the formula derived in Equation 3.1.3 which, in the four-qubit case, is given by

$$\mathcal{F} \geq \frac{\langle\alpha\rangle - 1}{4} \ . \tag{3.21}$$

Inserting our measured ID-Bell parameter $\langle\alpha\rangle_{exp} = 3.24 \pm 0.05$ we find $\mathcal{F}_{\mathrm{ID}} \geq \mathbf{0.56 \pm 0.01}$.

In fact there are eight equivalent critical whole negative IDs for the state we generated and all of them can be used for our approach. They are presented in Figure 16 together with the lower bounds on the fidelity that we can extract from the measurement of those observables which are in the range from 0.51 ± 0.01 to 0.56 ± 0.01 . Now one might ask how this result compares to other methods estimating the fidelity. We compared our approach to three other methods: Reconstructing the density matrix using over-complete quantum state tomography (QST) [1, 2], using the stabilizer group (SG) of the state [3, 4] and calculating a lower bound on the state fidelity based on the generators of the

$$\begin{matrix} Z & Z & I & I \\ Z & I & X & X \\ I & Z & Y & Y \\ Y & X & X & Y \\ Y & X & Y & X \end{matrix}$$

(a)
$F_{min} = 0.56 \pm 0.01$

$$\begin{matrix} Z & Z & I & I \\ Z & I & Y & Y \\ I & Z & X & X \\ Y & X & X & Y \\ Y & X & Y & X \end{matrix}$$

(b)
$F_{min} = 0.56 \pm 0.01$

$$\begin{matrix} Z & Z & I & I \\ Z & I & X & X \\ I & Z & Y & Y \\ X & Y & X & Y \\ X & Y & Y & X \end{matrix}$$

(c)
$F_{min} = 0.53 \pm 0.01$

$$\begin{matrix} Z & Z & I & I \\ I & Z & X & X \\ Z & I & Y & Y \\ X & Y & X & Y \\ X & Y & Y & X \end{matrix}$$

(d)
$F_{min} = 0.53 \pm 0.01$

$$\begin{matrix} I & I & Z & Z \\ Y & Y & I & Z \\ X & X & Z & I \\ Y & X & X & Y \\ X & Y & X & Y \end{matrix}$$

(e)
$F_{min} = 0.52 \pm 0.01$

$$\begin{matrix} I & I & Z & Z \\ Y & Y & Z & I \\ X & X & I & Z \\ Y & X & X & Y \\ X & Y & X & Y \end{matrix}$$

(f)
$F_{min} = 0.51 \pm 0.01$

$$\begin{matrix} I & I & Z & Z \\ Y & Y & I & Z \\ X & X & Z & I \\ Y & X & X & X \\ X & Y & Y & X \end{matrix}$$

(g)
$F_{min} = 0.55 \pm 0.01$

$$\begin{matrix} I & I & Z & Z \\ Y & Y & Z & I \\ X & X & I & Z \\ Y & X & Y & X \\ X & Y & Y & X \end{matrix}$$

(h)
$F_{min} = 0.54 \pm 0.01$

Figure 16: All eight equivalent $\mathrm{ID}5_0^4$ whose joint eigenstate is $|C_{lin}\rangle$ and the corresponding lower bounds on the state fidelity.

stabilizer group (GoSG) [53, 54].

First, using QST ($3^4 = 81$ measurement settings), we reconstructed the density matrix of the generated state (see Figure 17). From this density matrix we could directly calculate the fidelity $\mathcal{F}_{\mathrm{QST}} = \mathbf{0.629 \pm 0.007}$.

Next we used the SG approach to estimate the fidelity: This is done by taking the average of the measured expectation values of all stabilizers of the state ($2^4 = 16$). Here we find $\mathcal{F}_{\mathrm{SG}} = \mathbf{0.657 \pm 0.006}$. All results of the stabilizer measurements are summed up in Table 8.

Using only a subset of those measurements namely the ($N = 4$) generators of the stabilizer group (GOSG), we can calculate a lower bound on the fidelity using the

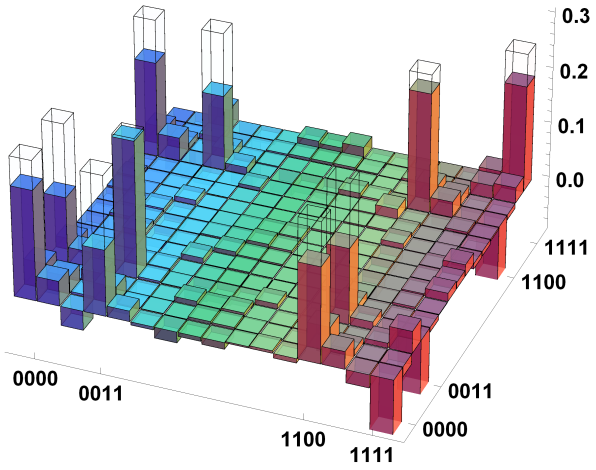


Figure 17: Reconstructed density matrix (real part) of the four-qubit linear cluster state ($\mathcal{F}_{\mathrm{QST}} = 0.629 \pm 0.007$). The black frames show the theoretical prediction for $|C_{lin}\rangle$. For each measurement the acquisition time per setting was 600s. The imaginary part of the reconstructed density matrix is not shown since its components are below 0.05.

following formula introduced in [53, 54]:

$$\mathcal{F}_{\mathrm{GOSG}} = \frac{\sum_{n=1}^{N} |a_n| - N + 2}{2} \tag{3.22}$$

where a_n are the measurement outcomes for the generators g_i ($i = 1, ...4$) of the stabilizer group. In our case this leads to a lower bound on the fidelity of $\mathcal{F}_{\mathrm{GOSG}} = \mathbf{0.48 \pm 0.02}$. A comparison of the fidelities of all generated states calculated with the four different methods can be found at the end of this chapter in Section 3.2.4 .

3.2.2 The three-qubit GHZ State

Projecting the second qubit of the four-qubit cluster state onto the state $|-\rangle$ generates the state

$$|\mathrm{GHZ}_3'\rangle = \frac{1}{\sqrt{2}}(|-00\rangle + |+11\rangle) \tag{3.23}$$

which is equivalent to the three-qubit GHZ state after applying a Hadamard gate and a σ_X gate on the first qubit. The data is extracted from the tomography measurements

Observable	Expectation value
ZZII	0.93 ± 0.01
IIZZ	0.78 ± 0.02
ZIXX	0.61 ± 0.02
IZXX	0.59 ± 0.02
IZYY	-0.58 ± 0.02
ZIYY	-0.58 ± 0.02
XXZI	0.66 ± 0.02
XXIZ	0.62 ± 0.02
YYIZ	-0.65 ± 0.02
YYZI	-0.65 ± 0.02
XYXY	0.47 ± 0.02
XYYX	0.52 ± 0.02
YXXY	0.52 ± 0.02
YXYX	0.60 ± 0.02
ZZZZ	0.75 ± 0.02
IIII	1 ± 0.03

Table 8: Measured expectation values for all operators in the stabilizer group of $|C_{lin}\rangle$.

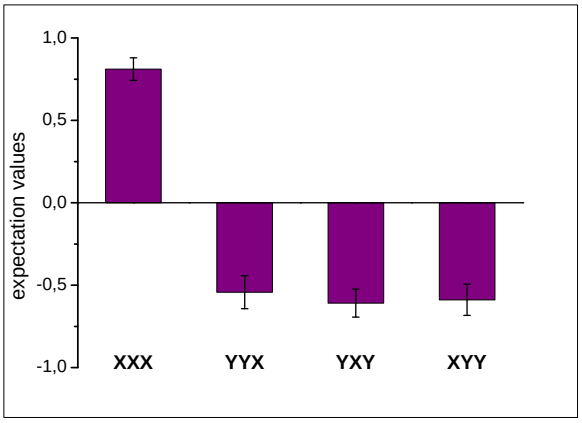
of the cluster state. For the three-qubit GHZ state we can construct a critical whole negative ID which is given in Table 9 which means we can again tap the full potential of our method.

X	X	X
Y	X	Y
X	Y	Y
Y	Y	X

Table 9: The critical whole negative $\mathrm{ID}4_0^3$ corresponding to the three-qubit GHZ state.

Testing the GHZ Theorem

We used the $\mathrm{ID}4_0^3$ for a test of the GHZ theorem and three-qubit nonlocality. The measured expectation values of the observables in the ID are shown in Figure 18 . From this results we can calculate the product of the observables (again QM predicts an outcome of `-1` and LHVT an outcome of `+1`) which is $\mathbf{P = -0.16 \pm 0.05}$. This is negative by more than 3 standard deviations and therefore shows three-qubit nonlocality. This



observable	expectation value
XXX	0.81 ± 0.07
YYX	-0.54 ± 0.10
YXY	-0.61 ± 0.09
XYY	-0.59 ± 0.09
Product	$\mathbf{-0.16 \pm 0.05}$
$\langle\alpha\rangle$	$\mathbf{2.6 \pm 0.2}$

Figure 18: Measured expectation values of the three-qubit GHZ state. The data is extracted from the tomographic measurements of the four-qubit cluster state, therefore the acquisition time for each measurement setting was 600s.The error bars were derived from Poissonian statistics and thus correspond to a lower limit.

can also be shown using the ID-Bell inequality which in the three-qubit case can be written as

$$\langle\alpha\rangle_{LHVT} \leq 2 \tag{3.24}$$

which is clearly violated by our measurement results $\langle\boldsymbol{\alpha}\rangle = \mathbf{2.6 \pm 0.2}$ (by 3 standard deviations) and nonlocality is again demonstrated.

Entanglement Discrimination

Also in the three-qubit case our ID-Bell parameter $\langle\boldsymbol{\alpha}\rangle = \mathbf{2.6 \pm 0.2}$ could be used for entanglement discrimination. As shown in Table 10 our measured value was high enough to exclude any state that is not three-party entangled but not the W state. To exclude this as well, a higher fidelity ($\mathcal{F}_{\mathrm{ID}} > 0.75$) would have been necessary. In this case due to experimental imperfections and the limited fidelity of the cluster state this was not possible.

State Type	$\langle\alpha\rangle_{max}$
$\|\psi_1\rangle\|\psi_2\rangle\|\psi_3\rangle$	$\sqrt{2}$
$\|\psi_i\rangle\|\Phi_{jk}\rangle$	2
$\|W_3\rangle$	3
$\|\mathrm{GHZ}_3\rangle$	4

Table 10: Discrimination values for the three-qubit GHZ state. Here $|\psi_i\rangle|\Phi_{jk}\rangle$ is a product of a Bell state and single-qubit state, $\{i, j, k\}$ can be any permutation of $\{1, 2, 3\}$).

Fidelity Bound

Again using the ID-Bell parameter we determined a lower bound on the fidelity of the experimentally generated state. Using the formula for the three-qubit ($N = 3, M = 4$) case

$$\mathcal{F} \geq \frac{\langle\alpha\rangle_{exp}}{4} \tag{3.25}$$

and our measured parameter $\langle\alpha\rangle = 2.6 \pm 0.2$ we find the lower bound $\mathcal{F}_{\mathrm{ID}} = \mathbf{0.67 \pm 0.05}$.

To compare this result we reconstructed the density matrix using QST, the result of which is shown in Figure 19. The corresponding fidelity is $\mathcal{F}_{\mathrm{QST}} = \mathbf{0.69 \pm 0.02}$. Additionally, we used the SG and the GoSG method to calculate the fidelity resulting in $\mathcal{F}_{\mathrm{SG}} = \mathbf{0.71 \pm 0.02}$ and $\mathcal{F}_{\mathrm{GOSG}} = \mathbf{0.65 \pm 0.06}$. The full measurement results of the corresponding operators are shown in Table 11.

stabilizer	expectation value
Z Z I	0.61 ± 0.09
I Z Z	0.88 ± 0.05
Z I Z	-0.64 ± 0.09
XXX	0.81 ± 0.07
YYX	-0.54 ± 0.10
YXY	-0.61 ± 0.06
XYY	-0.59 ± 0.09
I I I	1.00 ± 0.12

Table 11: Measured expectation values for all observables in the stabilizer group of the three-qubit GHZ state.

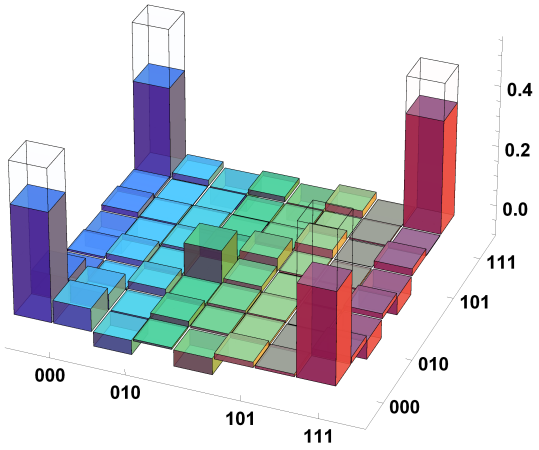


Figure 19: Reconstructed density matrix (real part) of the three-qubit GHZ state ($\mathcal{F}_{\mathrm{QST}} = 0.672 \pm 0.015$) . The imaginary part has components below 0.07 and is not shown. The data is extractd from the tomography measurements of the four-qubit cluster state where one of the qubits is projected on the state $|-\rangle$ and after appling a Hadamard and a σ_X operation this corresponds to the three-qubit GHZ state. The black frames show the theoretically predicted matrix for an ideal three-qubit GHZ state.

3.2.3 The four-qubit GHZ State

The four-qubit GHZ state is an example for a graph state for which no whole negative ID exists. But as for any graph state there is a set of IDs which has this graph state as a joint eigenstate [27]. Therefore, we can still use our ID approach, if not to test the GHZ theorem, at least to find a lower bound on the fidelity of the experimentally generated state. We chose to use the partial positive ID given in Table 12 to test our approach.[19]

$$\begin{array}{cccc} Z & I & Z & I \\ Z & Z & I & I \\ I & Z & I & Z \\ X & Y & X & Y \\ X & Y & Y & X \end{array}$$

Table 12: A partial positive ID5^4_2. It cannot be used to test the GHZ theorem but we could use it to find a lower bound on the fidelity of our experimentally generated four-qubit GHZ state.

[19] Actually there are 196 equivalent IDs we could use for this task and one is free to choose the best suited for a given experimental setting (e. g. if some measurement are more troubling than others).

observable	expectation value
ZIZI	0.90 ± 0.02
ZZII	0.87 ± 0.02
IZIZ	0.90 ± 0.02
XYXY	-0.56 ± 0.03
XYYX	-0.60 ± 0.03
$\langle\alpha\rangle$	$\mathbf{3.84 \pm 0.05}$

Table 13: Measured expectation values for the $\mathrm{ID}4_2^5$ which has the four-qubit GHZ state as joint eigenstate.The aquisition time for each measurement setting was 4800s.

Measuring all observables in the $\mathrm{ID}4_2^5$ (the measured expectation values are given in Table 13) we found a lower bound on the fidelity of $\mathcal{F}_{\mathrm{ID}} = \mathbf{0.71 \pm 0.01}$. Using the SG approach (measurement results in Table 14) we found a fidelity of $\mathcal{F}_{\mathrm{SG}} = \mathbf{0.712 \pm 0.006}$ and using the GoSG gives a lower bound on the fidelity of $\mathcal{F}_{\mathrm{GOSG}} = \mathbf{0.57 \pm 0.02}$. We also reconstructed the density matrix using QST. The result of the reconstruction is shown in Figure 20. This allowed us to calculate the fidelity of the generated state $\mathcal{F}_{\mathrm{QST}} = \mathbf{0.701 \pm 0.008}$.

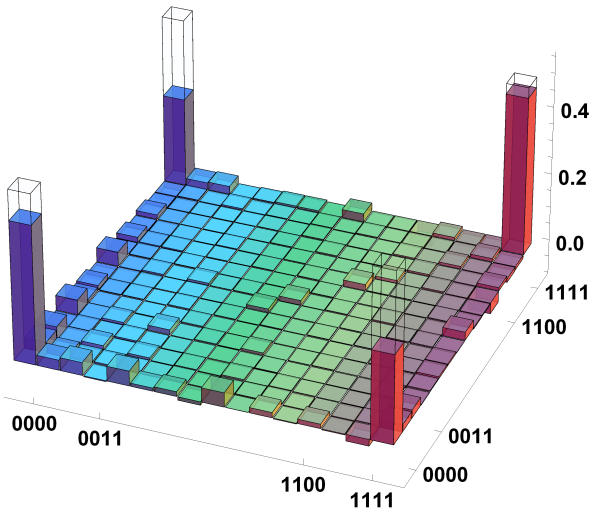


Figure 20: Reconstructed density matrix (real part) of the experimentally generated four-qubit GHZ state ($\mathcal{F}_{\mathrm{QST}} = 0.701 \pm 0.008$). The black frames show the theoretically predicted matrix for an ideal GHZ state. The aquisition time for each measurement setting was 600 s. The imaginary part of the reconstructed density matrix is not shown since its components are below 0.03.

stabilizer	expectation value
ZZII	0.87 ± 0.02
IIZZ	0.88 ± 0.02
ZIZI	0.90 ± 0.02
IZIZ	0.90 ± 0.02
ZIIZ	0.85 ± 0.02
IZZI	0.85 ± 0.02
ZZZZ	0.85 ± 0.02
XXXX	0.54 ± 0.03
YYYY	0.56 ± 0.03
XXYY	-0.51 ± 0.03
XYXY	-0.56 ± 0.03
XYYX	-0.60 ± 0.03
YXXY	-0.48 ± 0.03
YXYX	-0.51 ± 0.03
YYXX	-0.53 ± 0.03
IIII	1 ± 0.03

Table 14: Measured expectation values for the observables in the stabilizer group of the four-qubit GHZ state.The aquisition time for each measurement setting was 4800s.

3.2.4 Comparison of Different Fidelity Methods

As described above we generated three different states for which we calculated the fidelity (or a lower bound) using four different methods. The results are shown in Figure 21 and will be compared in this section. Within the error bars (one standard deviation) the lower bound given by our ID approach is always in agreement with the QST results whereas the SG method gives a higher fidelity in the case of the cluster state and the three-qubit GHZ state. The SG approach is based on the assumption that the generated state is actually a graph state and apparently tends to overestimate the state fidelity for states with noise. The GOSG method gives a lower bound of the fidelity but in two of our three cases ($|C_{lin}\rangle$ and $|\mathrm{GHZ}_4\rangle$) the bound is significantly lower than the other three results. For the state $|C_{lin}\rangle$ the result is even under the 0.5 limit therefore this method does not suffice to certify that this state can violate a Bell-type inequality. The ID method seems to give (at least in most cases) a tighter bound. We have performed a general comparison

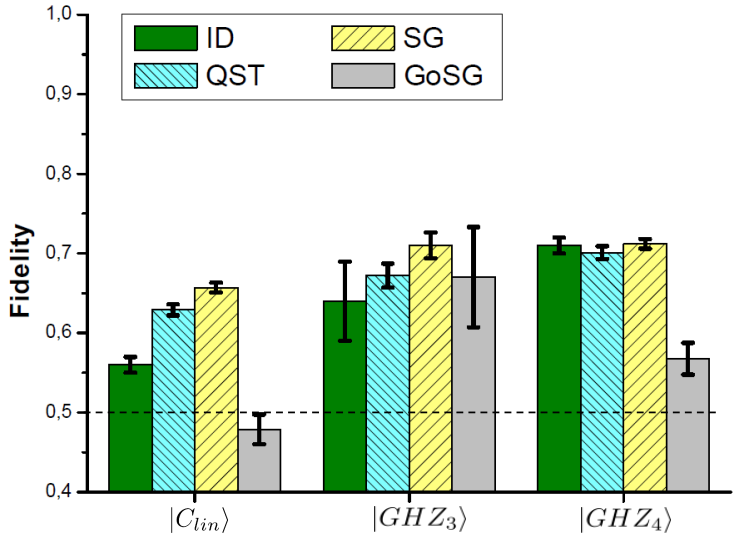


Figure 21: Comparison of the fidelities obtained with the different methods. For the four-qubit linear cluster, four-qubit GHZ state and three-qubit GHZ state the fidelities are calculated using over-complete quantum state tomography, QST, (dark grey bar) and the stabilizer group approach, SG, (light grey bar). Those methods scale exponentially with the number of qubits while IDs (yellow bar) whereas the fidelities calculated based on the generators of the stabilizer group, GoSG, (green bar) scale linearly with the number of qubits.The error bars were derived from Poissonian statistics and thus correspond to a lower limit.

of the ID and the GoSG method to test this assumption. In Reference [53] a general equation for a lower bound on the fidelity given any set of N generators is provided:

$$F_g = (\sum_n a_n - N + 2)/2 \ , \tag{3.26}$$

while the ID method gives a lower bound of

$$F_{ID} = (\sum_m a_m - M + 4)/4 \ , \tag{3.27}$$

where $a_i = \langle A_i \rangle$ are the experimentally obtained expectation values of the observables A_i. From every set of N independent generators an IDM^N (with $M = N + 1$) can be

constructed by adding one more observable A_M to the set:

$$A_M = \lambda_M \prod_n A_n \ , \tag{3.28}$$

where λ_M is equal to the sign of the resulting ID, such that $0 \leq a_i \leq 1$. Combining all of this we can construct a quantitative comparison of the two bounds for the same set of N generators and the additional M^{th} observable necessary for the ID method

$$F_{ID} - F_g = (\sum_m a_m - M + 4)/4 - (\sum_n a_n - N + 2)/2 = [(a_M - 1) + (N - \sum_n a_n)]/4 \ . \tag{3.29}$$

Clearly, the difference vanishes if both methods give perfect fidelity. However, in the case that the measurements are imperfect, $0 \leq a_M < 1$ and $0 \leq N - \sum_n a_n < N$ the two methods can give different values. If we let all of the a_m take the same average value $a_0 < 1$, this reduces to

$$F_{ID} - F_g = (N-1)(1-a_0)/4 > 0 \ , \tag{3.30}$$

which shows that the ID bound is usually better. Of course in practice this will depend on the specific values of the a_m, and indeed in the theoretical extreme case that $a_M = 0$ and $a_n = 1$, we get $F_{ID} = 0.75$ and $F_g = 1$, and the GoSG bound is actually higher. In general the GoSG method gives a better bound when

$$\sum_n a_n > a_M + N - 1 \ . \tag{3.31}$$

As it is arbitrary which of the observables A_m is chosen as A_M we can examine all M choices, and take the best of the $M+1$ different bounds obtained from the measured set a_m. F_{ID} is better for the case that the average error of all measurements is comparable, as this is usually the case in realistic experiments. The comparison is still applicable even in the case that the M operators used for the ID approach do not contain the N generators used to calculate $\mathcal{F}_{\mathrm{GoSG}}$. Assuming that all of the a_m and all of the a_n in Equation (3.29) take the same average value a_0, the ID bound still gives a better result [52].

4 Experimental Demonstration of Measurement Only Blind Quantum Computing

In today's increasingly technologized world the computational demands are often met by delegating computational tasks to a distant provider also called „the cloud“. It seems quite likely that the first major quantum computers will be realized in a cloud-like fashion too, because high requirements have to be met to operate such systems. The protection of data privacy in such cloud computations is a highly relevant topic. It has been shown that the privacy of the client delegating a computation to a server can be fully maintained using blind quantum computation (BQC) [8, 55], which allows a client to use the full quantum computational power of a server while neither the input, nor the program, nor the output is known to the server. The client's quantum resources are limited to the preparation of single qubits and their transmission to the quantum server.

Recently a new protocol of BQC has been proposed [11, 10]. This scheme does not require a client to prepare any quantum states but only to measure single-qubit states in the basis defined by the computation. Therefore, the client, which will be called Alice, needs even less quantum resources than in the first protocol. Additionally, the client Alice can, again without using any quantum computer, test if her provider, Bob, has prepared the correct resource state for her computation, i.e. if the results can be trusted. Furthermore this protocol has the advantage of a simple and more fundamental security proof based on the no-signaling principle. In this section I start with a brief introduction into quantum computing before presenting the new protocol. In explaining this new

protocol I will focus on the verification of Bob's honesty by Alice using a four-qubit linear cluster state. This state is especially suitable for this kind of verification. We have for the first time implemented the verification protocol using a photonic setup to create the cluster state. A more comprehensive demonstration of this protocol, including the blind implementation of a universal set of gates, is currently being implemented so I will give a brief outlook at the end of this section.

4.1 Quantum Computing

What are the differences between quantum and classical computations? On a fundamental level classical computations are based on *bits*, whereas quantum computing is based on the qubit which cannot just take the values 0 and 1 but any superposition of those. This can be a huge advantage since it means that e. g. a function can be evaluated for two inputs at once which is used for example in the Deutsch-algorithm [56]. Perhaps one of the most striking examples one can give to demonstrate the advantage of quantum systems is to consider a general system of n qubits. The basis states of such a system are of the form

$$|\Psi\rangle = c_1 |00\ldots00\rangle + c_2 |00\ldots01\rangle + c_3 |000\ldots10\rangle + \ldots + c_{2^n} |11\ldots11\rangle \tag{4.1}$$

so a general state is described by 2^n complex amplitudes. If we would try to store this state on a classical computer even for comparably small numbers like $n = 500$ the number of amplitudes we would need to store is larger than the estimated number of atoms in the universe [21]! But quantum computers do not only offer a faster solution to some problems they also can use resources like entanglement or protocols like teleportation [57] which no classical computer has access to.

To come back to the analogy between classical and quantum computers, we know that classical computers are built from electrical circuits where wires connect gates. Following this form it is possible to describe quantum computation in the circuit model using quantum wires and single- or multi-qubit gates.

4.1.1 The Circuit Model

There are different ways to construct a model for quantum computing but the most widely used is the quantum circuit model [58]. It is the generalization of the classical model of circuit computation which is based on boolean logic.

Quantum circuits are built from a few main elements. An example showing some of those elements can be found in Figure 22 .

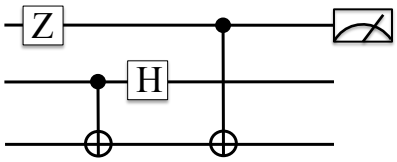


Figure 22: Example of a circuit showing some basic elements. It is composed of three wires (corresponding to qubits), a Z gate, two C-NOT gates, a Hadamard gate and a single-qubit measurement. The single elements are explained in the main text.

The horizontal lines are the wires of the circuit and each line represents one qubit. They can pass through single-qubit gates which are represented as squares that are usually labeled with a single letter (see Figure 23).

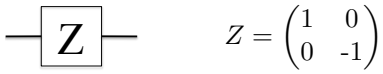


Figure 23: Example of a single-qubit gate: the symbol representing the σ_Z-gate in the circuit and the matrix representation of the gate in the computational basis.

Another important example besides the Pauli-operators (denoted by squares with the letters Z,X,Y) is the Hadamard gate.

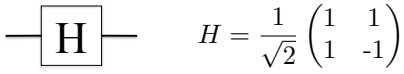


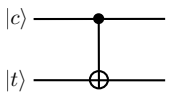
Figure 24: Symbol and matrix representation of the Hadamard gate in the computational basis.

This gate transforms e. g. the state $|0\rangle$ into $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1)\rangle$. Another commonly used set of single-qubit gates are the rotations by an angle θ around the Z,X and Y axis denoted by $Z(\theta) = e^{-i\theta Z}$, $X(\theta) = e^{-i\theta X}$, and $Y(\theta) = e^{-i\theta Y}$.

Besides the single-qubit gates one needs to consider also the possibility that one qubit is changed depending on the state of another qubit. One of the most common two-qubit gates is the controlled-NOT or *CNOT* gate. It has two inputs: the control $|c\rangle$ and the target $|t\rangle$ qubit on which it acts as shown in the following table

c_{in}	t_{in}	c_{out}	t_{out}
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

In the circuit representation it is given as shown in Figure 25



$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Figure 25: Symbol and matrix representation of the CNOT gate in the computational basis. The upper qubit is the control qubit, the lower qubit is the target qubit.

A second important two-qubit gate is the Controlled-Phase gate also known as controlled-Z gate which is represented as

$$C - Phase = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Figure 26: Symbol and matrix representation of the C-Phase gate in the computational basis.

Arbitrary single-qubit gates together with a two-qubit entangling gate like the CNOT (or the C-Phase) gate form an universal set which means that any n-qubit gate can be realized using only combinations of these gates [59]. Finally the result of the computation can be read out by measuring in the computational basis resulting in a string of classical

bits. In the circuit picture measurements are symbolized by symbols like the one shown in Figure27.

Figure 27: Example for a symbol representing a measurement in the circuit.

4.1.2 Measurement-Based Quantum Computing

Measurement-based Quantum Computing (MBQC), introduced in 2001 by Raussendorf and Briegel [6], is an alternative model of quantum computing. It provides a conceptually different way to perform quantum computing as it is not based on building a fixed circuit for a given computation but on performing adaptive single-qubit measurements on a highly entangled resource state. Only those measurements determine the computation that is performed.

The resources for this kind of computation are cluster states[20] introduced in Section 1.2.1. The preparation of this cluster states is followed by a sequence of adaptive single-qubit measurements on individual qubits of the cluster. This sequence of measurements determines the computation that is realized. In general this sequence of measurements will not be entirely predefined but some measurements will depend on the outcomes of earlier measurements which is known as feed forward of the classical measurement results [20].

There can be two different types of outcome of such measurement-based quantum computations: On the one hand the output can be a quantum state, namely one or more qubits that remain after the necessary measurements were performed and that now contain the desired information. On the other hand we might define a set of readout measurements on the remaining qubits and in this case the outcome of the computation is a string of classical bits [20].

To demonstrate this concept let us consider how measurement-based quantum computation can simulate computations in the circuit model [20, 62]. To perform universal

[20] Also other states have been proposed for MBQC that will not be considered here [60, 61].

computations we need to be able to realize single-qubit rotations and a two qubit entangling gate (like the CNOT). This is possible based on the single-qubit teleportation [57]. The circuit corresponding to this is shown in Figure 28a .

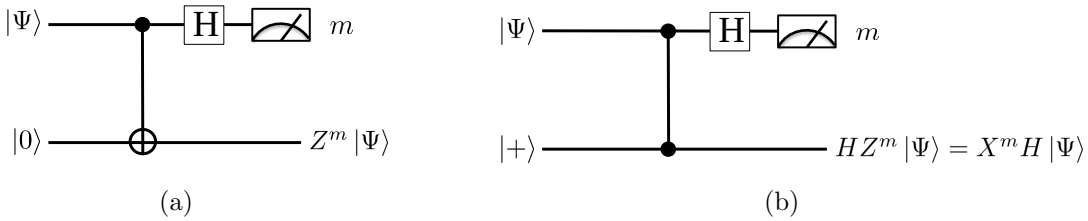


Figure 28

Here m is the outcome of the single-qubit measurement in the computational basis. If $m = 0$ the input state has successfully been transferred, if $m = 1$ a Pauli-Z operation has to be performed to restore the correct input state. This is an important step: Depending of the outcome of the single-qubit measurement we might have to perform a Pauli-operation on the output state.

The C-NOT gate is equivalent to applying two Hadamard gates on the target qubit and in between one C-Phase gate as shown in Figure 28b . There the first Hadamard is included in the initial state of the ancilla qubit. It is useful to mention some relations at this point:

$$ZX = -XZ \tag{4.2}$$

$$X = HZH \tag{4.3}$$

Also remember that any single-qubit rotation of θ can be decomposed as

$$R(\theta) = Z(\gamma)X(\beta)Z(\alpha) = Z(\gamma)HZ(\beta)HZ(\alpha) \ . \tag{4.4}$$

So let us now consider a simple rotation around the z-axis in our circuit:

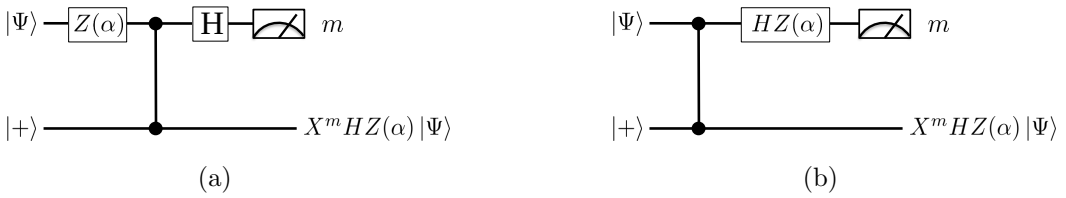


Figure 29

On the one hand this can be seen as replacing $|\Psi\rangle$ by $Z(\alpha)|\Psi\rangle$. On the other hand the $Z(\alpha)$ rotation commutes with the C-Phase gate (since they are both diagonal in the computational basis) so both circuits in Figure 29 are equivalent. But we can easily reinterpret the circuit in Figure 29b as having an entangled input state (the C-phase gate acts on $|\Psi\rangle$ and $|+\rangle$ which entangles them[21]) and absorbing the action of $HZ(\alpha)$ in the measurement basis (so the first qubit is no longer measured in the computational basis but in a basis depending on α). Remarkably this means that by changing the measurement basis we change the output of the circuit. Up to a Pauli-operation (depending on the outcome of the measurement) we have now performed the operation $HZ(\alpha)$ on our input state. To perform an arbitrary single-qubit operation we can use the circuit shown in Figure 30:

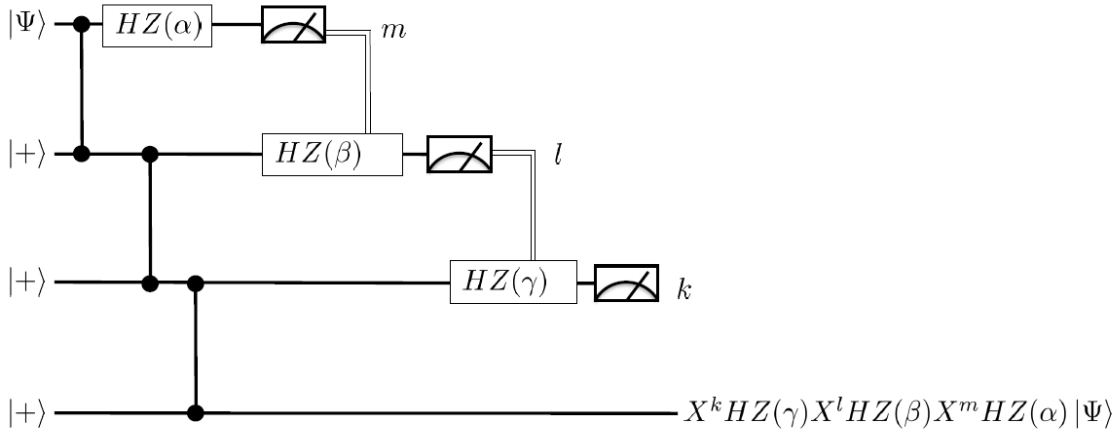


Figure 30

In that circuit the double lines represent the classical communication of the measurement

[21]Note that if our input state is equal to $|+\rangle$ this is exactly the definition of a two-qubit cluster state.

outcomes m, l, k (0 or 1). Adapting the sign of the rotation angle according to the previous measurement outcome allows us to commute all unwanted Pauli X gates to the left since $Z(\pm\beta)X^m = X^m Z((-)^m\beta)$ and $HX^m = Z^m H$ so the output state becomes

$$|\Psi_{out}\rangle = X^k Z^l X^m HZ((-1)^l\gamma)HZ((-1)^m)\beta)H(Z(\alpha))\,|\Psi_{in}\rangle \tag{4.5}$$

and the final circuit looks like

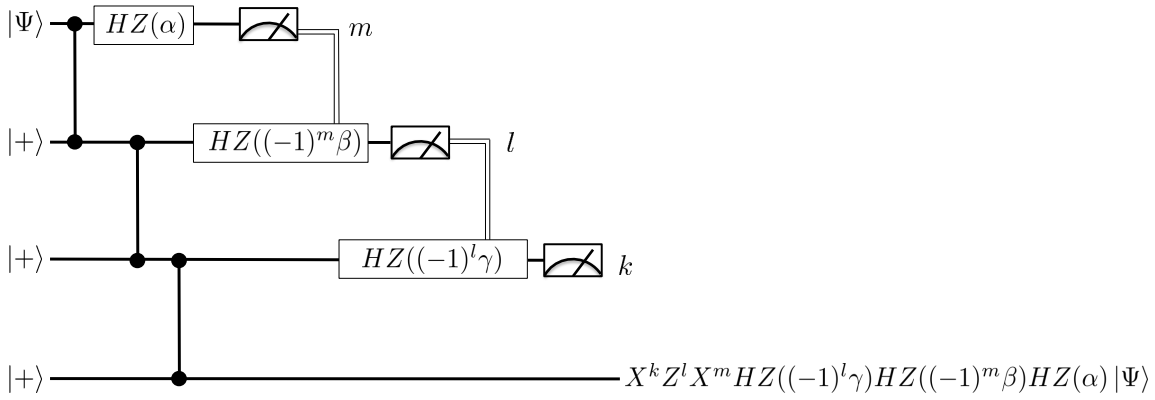


Figure 31

This means that by performing single-qubit measurements on an entangled resource state one can perform an arbitrary single-qubit rotation up to some operators that can in principle be absorbed in the measurement basis of an output measurement. If we are able to perform arbitrary single-qubit rotations we can also start our computation with the input state $|+\rangle$ and encode the specific input using the appropriate measurements. In the cluster state picture this computation corresponds to single-qubit measurements (as given in the circuit in Figure 31) on a liner cluster state as shown in Figure 32.

Due to the measurements involved in this kind of computations the process is no longer unitary. The feed forward routine dictates a clearly defined time pattern for the measurements, hence the name one-way quantum computing.

By using cluster states based on two dimensional graphs it is also possible to implement two-qubit gates. Among them the C-NOT gate which can be realized using the four-qubit

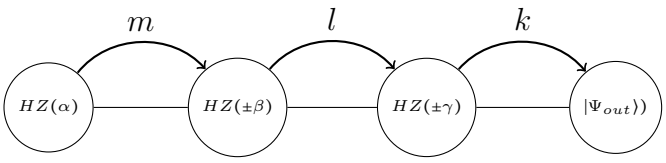


Figure 32: Any output state $|\Psi_{out}\rangle)$ can be generated by measuring the single qubits in appropriate bases. The outcomes of prior measurements (m, l, k) need to be considered in the following measurements to generate the right state.

star graph state[22] shown in Figure 33 [63]. In fact, if the underlying cluster state is large

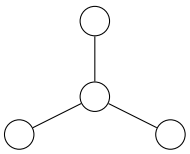


Figure 33: Graph corresponding to the four-qubit star graph state.

enough any quantum computation can be implemented.

Furthermore if a general cluster state is given we can shape it using measurements in the $\{|0\rangle, |1\rangle\}$ basis. Those measurements disentangle qubits from the cluster deleting all edges connected to their corresponding vertex in the graph.

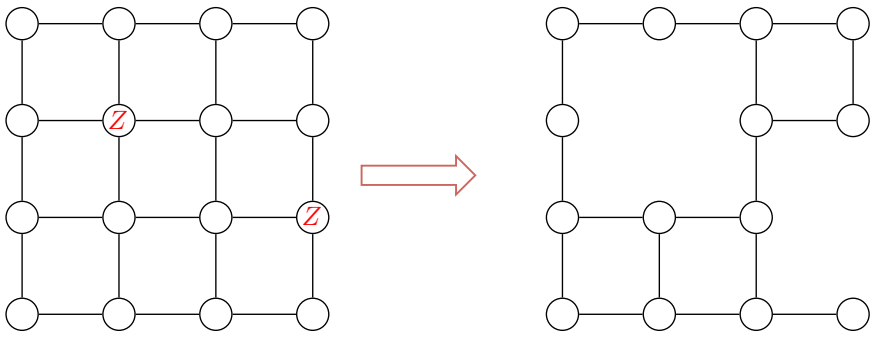


Figure 34: Shaping a cluster using measurements in the computational basis.

[22] Since cluster states are defined as being based on a two dimensional square lattice this is not a cluster but a graph state (graph states can be based on arbitrary lattices). The C-NOT can also be performed using cluster states but this is a particularly simple realization since it only relies on a four-qubit state.

4.1.3 Blind Quantum Computing

In contrast to classical computing[23], quantum computing can provide the security that a server can perform tasks for a client without having access to any information about the input, the computation or the output. This can be realized based on MBQC and became known as blind quantum computing (BQC). It was proposed originally in [8] and I will briefly summarize it here before describing the alternate protocol implemented in our experiment [11].

As the performed computation is defined by the angles of the single-qubit measurements these angles have to be hidden from the server to keep the clients information secret. To realize this BQC blind cluster states are required as a resource. The generation of the blind cluster states and the blind computation can be performed according to the following protocol where a client Alice (without a quantum computer) delegates a computation to an untrusted provider Bob (who operates a quantum server):

1. To generate a blind cluster state Alice has to prepare single qubits in the state $|\theta_j\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle)$. The angle θ_j is chosen randomly from $\{0, \pi/4, \ldots, 7\pi/4\}$.

2. She then sends the states to Bob who entangles them using C-Phase gates, building a blind cluster state.

3. Alice chooses the measurement bases for her computation $|\pm\delta_j\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\delta_j}|1\rangle)$. As measuring the blind cluster in this basis has the affect of applying a rotation $R(-\delta_j + \theta_j)$ followed by a Hadamard on the input state, δ_j is chosen as $\delta_j = \phi_j + \theta_j + \pi r_j$ where ϕ_j is the actual measurement angle necessary to perform the desired computation and r_j is randomly chosen from $\{0, 1\}$ and is used to hide the measurement outcome.

4. Alice uses classical communication to transmit the measurement bases $|\pm_{\delta_j}\rangle$ to Bob. He measures the qubit in those bases and sends the outcome to Alice.

[23] In the classical case there exists a protocol enabling date processing on encrypted data but this is only computationally secure [64] . This means that the security relies on assumptions about the limited computational power of the opponent.

5. Alice deciphers the output by flipping bit j if $r_j = 1$ or doing nothing if $r_j = 0$

In this way Alice can use the quantum computational power of Bob without leaking any of her information to him which means that the input, the computation and the output are entirely hidden from him [8, 55].

4.2 Measurement Only Blind Quantum Computing

A new protocol for BQC, the „measurement only blind quantum computing“, was proposed by Morimae and Fujii in 2013 [11]. It has several advantages compared to the original protocol described in the previous section. On the one hand it requires less resources to perform single-qubit measurements than to prepare single-qubit quantum states. On the other hand, in the original protocol Alice has to trust her device so she knows e. g. that only one qubit in the desired state is sent.[24] In this new protocol this assumption is no longer necessary, we assume that Bob has a sufficiently large, fully functional quantum computer and Alice is equipped to do single-qubit measurements in any basis necessary for the computation she wants to perform. Another advantage is that, contrary to the original protocol, Alice does not need a random number generator. As it is still a hard task to generate truly random numbers this simplifies the requirements for Alice. The protocol runs as follows:

1. Fist Bob prepares his highly entangled resource state for measurement-based quantum computation (a cluster state).

2. Bob sends one of his qubits from the cluster state to Alice.

3. When Alice receives the qubit she measures it in the basis determined by the computation she wants to run. Note that if Bob encodes the single-qubit state into a many-qubit state even a threshold detector is sufficient for Alice (so she does not have to detect single qubits).

[24] Alice might have bought her device from a company secretly under the control of Bob which emits instead of $|intended\ state\rangle$ a state like $|intended\ state\rangle \otimes |Alice's\ secret\rangle$. So she would have to verify her device which is considered very difficult due to her limited technological resources.

4. Steps (2.) and (3.) are repeated until the computation is complete

So if Bob is honest, at the end of the protocol, Alice gets the correct result of her computation. But even if Bob is malicious he cannot learn anything about Alice's computation since Alice does not send any signal to Bob. Therefore, the security of the protocol is guaranteed by the no signaling principle[25] and is therefore even more fundamental than quantum mechanics[26] [65]. This can easily be seen by considering that Alice has two options: a) Measuring the qubits she receives and therefore performing the desired computation, leaving Bob's system (after her computation) in the state ρ_1 or b) discarding all of the qubits leaving Bob's system in the state ρ_2. Of course, since Alice did not send any signal, $\rho_1 = \rho_2$ (otherwise this could be used to send a message from Alice to Bob). But ρ_2 obviously does not contain any information about Alice's input, output, or routine, so it is impossible for ρ_1 to contain any of Alice's secret information.

This also means that the security of this protocol is device independent: Alice does not have to trust her device to ensure that Bob cannot learn anything about her secret. At this point it should be mentioned that it is always assumed that there is no unwanted information leakage from Alice's laboratory (it is e. g. not bugged) which is a standard assumption also in quantum key distribution [11].

Until now we have seen how the protocol fulfills two important requirements for blind quantum computations: The correctness and blindness. If a protocol satisfies correctness it can be used to perform the correct computation, given that Bob is honest. The attribute of blindness certifies that, whatever Bob does, it is not possible for him to learn anything about Alice's secret (except for some unavoidable information leakage e. g. an upper bound on the size of the input). Another important requirement is the verification, which will be explained in the next section.

[25] No signaling means that if Alice and Bob are separated but share a (classical, quantum or even super quantum state) a measurement Alice performs on her state this will not transmit any information to Bob.

[26] There is a theory that predicts stronger-than-quantum correlations but does not violate no-signaling.

Verification

A protocol allows for verification if Alice can verify whether Bob is performing the right computation respectively providing her with the correct resource even though she has no quantum technology comparable to Bob's quantum computer. It has been shown, and experimentally demonstrated that this is possible in the original BQC protocol described above [9, 66].

In a recent paper it was shown that this is also possible for measurement only blind quantum computing [10] using „trap" qubits which Alice can remotely prepare in Bob's laboratory. When Bob and Alice agree to do a quantum computation Bob sends the qubits of his original resource state one-by-one to Alice. Alice then measures the received qubits which changes the state in Bob's laboratory. She measures until she remotely creates the N-qubit state which is composed form three $N/3$-qubit parts

$$|\Psi_{Trap}\rangle = \sigma_q |\Psi_P\rangle = \sigma_q P(|R\rangle \otimes |+\rangle^{\otimes N/3} \otimes |0\rangle^{\otimes N/3}) \ , \tag{4.6}$$

here σ_q denotes the Pauli operators that can occur as a byproduct of the measurement-based quantum computation (as described in Section 4.1.2 depending on the output of the previous measurements additional Pauli operations might be needed to generate the desired output state). The state $|R\rangle$ is a $N/3$-qubit universal resource state which will be used for the actual computation while the qubits in $|+\rangle$ and $|0\rangle$ are used as traps to test Bob's honesty. P is a N-qubit permutation (which Alice hides from Bob) that keeps the order of the qubits in $|R\rangle$.

As we assume that there is no communication channel that goes from Alice to Bob, Bob cannot know anything about P. Otherwise this would violate the no-signaling principle.

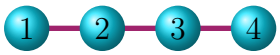
Bob now sends the qubits from $|\Psi_{Trap}\rangle$ one-by-one to Alice: Before she measures the qubits she applies the proper correcting operations $\sigma_q^\dagger$ to the state[27] in order to compensate any unwanted Pauli operations. If the qubit she received belongs to $|R\rangle$ she uses it to perform her quantum computation. The other qubits are used as traps. She

[27] Since she receives and measures the qubits one-by one she applies on qubit j the operator $\sigma_q^\dagger|_j$ so the restriction of $\sigma_q^\dagger$ to qubit j.

measures the qubits which are supposed to be in the $|+\rangle$ and $|0\rangle$ state (if Bob prepared the right state) in the X and Z basis. If she obtains any „minus“ result (she finds the qubit in a $|-\rangle$ or $|1\rangle$ state) she knows that Bob did not prepare the correct state and stops the protocol. If none of the traps gives a wrong result she trusts the outcome of her quantum computation [10].

Demonstrating the Verification using a Linear Cluster State

In our experiment we performed a proof-of-principle experimental demonstration of the protocol based on the four-qubit linear cluster state $|C'_{lin}\rangle$:



$$|C'_{lin}\rangle = \tfrac{1}{2}\left(|0+0+\rangle + |0-1-\rangle + |1-0+\rangle + |1+1-\rangle\right) .$$

This state can be experimentally generated[28] using the well-tested photonic setup described in Section 2.3 . Additionally, it allows for an especially strong verification. In the general protocol the probability that Alice is fooled by Bob (regardless of the traps) is exponentially small. However, in the realization using the four-qubit linear cluster state this probability is equal to zero [67]. This can be seen as follows:

1. Bob, the mistrusted provider of the quantum computational resource state prepares a four-qubit linear cluster state. He sends the qubits of the state one-by-one to Alice.

2. Alice chooses to perform one of three options:

   a) The $(1,3)$ test: Alice measures qubits 1 and 3 in the Z basis and qubits 2 and 4 in the X basis. Qubits 2 and 4 will become trap qubits.

   b) The $(2,4)$ test: Alice measures qubits 2 and 4 in the Z basis and qubits 1 and 3 in the X basis. The qubits 1 and 3 will be turned into traps.

[28] The state that is generated corresponds to the linear cluster state up to LU which have to be considered in the analysis of the data.

c) Alice uses the cluster state as a resource state for her measurement-based quantum computation.

The trap qubits allow Alice to test if Bob prepared the right state. If the qubits he sent to her were prepared in a four-qubit linear cluster state, Alice will find the expected states shown in Table 15 and 16 with a probability equal to 1. If she finds any unexpected result she knows Bob prepared a different state and aborts the protocol. Let us see if

Measured Outcome (1,3)		Expected State (2,4)	
0	0	+	+
0	1	-	-
1	0	-	+
1	1	+	-

Table 15: List of expected states in qubits 2 and 4 depending on the measured outcomes in qubits 1 and 3 enabling Alice to perform a (1,3) test.

Measured Outcome (2,4)		Expected State (1,3)	
0	0	+	+
0	1	+	-
1	0	-	-
1	1	-	+

Table 16: List of expected states in qubits 1 and 3 depending on the measured outcomes in qubits 2 and 4 enabling Alice to perform a (2,4) test.

there is a way that Bob can prepare any other state than the linear cluster state without being detected by Alice:

To pass Alice's (1,3) test, he has to prepare the state

$$|\Psi\rangle \equiv \frac{1}{2}\Big(|0+0+\rangle\,|a_1\rangle + e^{i\theta_2}\,|0-1-\rangle\,|a_2\rangle + e^{i\theta_3}\,|1-0+\rangle\,|a_3\rangle + e^{i\theta 4}\,|1+1-\rangle\,|a_4\rangle \Big)\,, \qquad (4.7)$$

where $\{|a_j\rangle\}$ are the states of Bob's ancilla qubits (which are normalized $|\langle a_j|a_j\rangle|^2 = 1$, but do not have to be mutually orthogonal). But Bob does not know which of her options Alice will choose so his state at the same time has to pass the (2,4) test. If Alice performs the (2,4) test and gets the result $(0,0)$ on qubits 2 and 4 the state after the measurement

becomes

$$|\Psi'\rangle \equiv \frac{1}{2}\Big(|0\rangle_1 |0\rangle_3 |a_1\rangle + e^{i\theta_2} |0\rangle_1 |1\rangle_3 |a_2\rangle + e^{i\theta_3} |1\rangle_1 |0\rangle_3 |a_3\rangle + e^{i\theta 4} |1\rangle_1 |1\rangle_3 |a_4\rangle \Big) . \tag{4.8}$$

As shown in Table 16 this state must be equal to, $|+\rangle_1 |+\rangle_3 |b\rangle$ for a state $|b\rangle$ in order to pass the (2,4) test. Therefore, the reduced density operator of $|\Psi'\rangle$ for Bob's ancilla

$$\rho = \frac{1}{4} \sum_{j=1}^{4} |a_j\rangle\langle a_j| \tag{4.9}$$

must have rank 1, which leads to $|a_j\rangle = |a_k\rangle$ (up to a phase factor). Now the state is

$$\frac{1}{2}\Big(|0\rangle_1 |0\rangle_3 + e^{i\theta'_2} |0\rangle_1 |1\rangle_3 + e^{i\theta'_3} |1\rangle_1 |0\rangle_3 + e^{i\theta 4'} |1\rangle_1 |1\rangle_3 \Big) |a_1\rangle . \tag{4.10}$$

Next, in order for this state to be $|+\rangle_1|+\rangle_3|b\rangle$, we need to have $\theta'_j = 0$ for all $j = 2, 3, 4$. And combining this we see that the original state has to be

$$|\Psi\rangle \equiv \frac{1}{2}\Big(|0+0+\rangle + |0-1-\rangle + |1-0+\rangle + |1+1-\rangle \Big) |a_1\rangle \tag{4.11}$$

which means that Alice's qubits have to be prepared in the linear cluster state. The experimental demonstration of this verification protocol will be described in the next section.

4.3 Experimental Realization

To realize the verification protocol we experimentally prepared the state $|C_{lin}\rangle$ equivalent to the four-qubit linear cluster state up to the local unitary (LU) operation $H_1 \otimes I_2 \otimes I_3 \otimes H_4$, as described in the Sections 2.3 and 3.2.1. This state is given by

$$|C_{lin}\rangle = (|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle)/2 \tag{4.12}$$

and was generated with a fidelity of $\mathcal{F}_{\mathrm{QST}} = 0.676 \pm 0.007$ (under LU operations).[29]

Bob's laboratory is realized via the photonic set-up described in Section 1.1 based on two interferometers with polarizing beamsplitters (PBSs) which entangle the four photons and create the state $|C_{lin}\rangle$. Through four single mode fibers this is connected to the detection stage, corresponding to Alice's laboratory where the polarization of the incoming photons is analyzed using four HWPs, four QWPs, four PBSs and eight single photon counting detectors (APDs) in order to speed up the data acquisition.[30]

In Alice's part the qubits are measured according to the protocol in the order that Bob sent them to perform a (1,3) or a (2,4) test. If Alice should find an unexpected result she aborts the protocol which means that the second trap qubit is only analyzed if we found the expected outcome in the first trap. For all possible outcome combinations we obtained the expected result when measuring the trap qubits with probabilities between 0.68 ± 0.07 and 1.00 ± 0.19. The full results are shown in Tables 17 and 18. Due to experimental imperfections causing the reduced fidelity of the generated linear cluster state the trap qubits are not always found to be in the expected states. Nevertheless, considering realistic laboratory conditions we find our results in agreement with the theory. Therefore, following the procedure of both tests, Alice successfully verified the four-qubit resource, which Bob has prepared for her BQC.

Outcomes (1,3)	Expected State q2	Fidelity	Expected State q4	Fidelity
00	$\|+\rangle$	0.85 ± 0.06	$\|+\rangle$	0.97 ± 0.03
01	$\|-\rangle$	0.74 ± 0.07	$\|-\rangle$	1.00 ± 0.19
10	$\|-\rangle$	0.85 ± 0.06	$\|+\rangle$	0.90 ± 0.06
11	$\|+\rangle$	0.79 ± 0.06	$\|-\rangle$	0.90 ± 0.05

Table 17: Probabilities of finding the the traps (qubit 2 and qubit 4) in the expected after performing a (1,3) test.

[29] The density matrix reconstructed using over-complete state tomography is shown in Figure 17 in Section 3.2.1.

[30] In principle if would be sufficient for her to have only one set elements to analyze the incoming photons but in this configuration we significantly speed-up the measurement process.

Outcomes (2,4)	Expected State q1	Probability	Expected State q3	Probability
00	$\|+\rangle$	0.95 ± 0.03	$\|+\rangle$	0.80 ± 0.05
01	$\|+\rangle$	0.98 ± 0.02	$\|-\rangle$	0.68 ± 0.07
10	$\|-\rangle$	0.98 ± 0.02	$\|-\rangle$	0.92 ± 0.04
11	$\|-\rangle$	0.94 ± 0.04	$\|+\rangle$	0.85 ± 0.06

Table 18: Probabilities of finding the the traps (qubit 1 and qubit 3) in the expected state after performing a (2,4) test.

4.4 Discussion

Concluding, the proof-of-principle experiment with a four-qubit linear graph state showed the capability of Alice to test the resource state prepared by Bob. The measurement only BQC was found to be feasible and practical with Bob's and Alice's laboratories being realized based on photonic qubits.

It should be emphasized that in our implementation Alice's part was equipped with four HWPs, four QWPs, four PBSs and eight APDs analyzing the photons sent from Bob in four single mode fibers, but in principle only one fiber and corresponding analysis would be sufficient to implement the protocol. The only additional requirement in Bobs part would be a time-delay multiplexer (as the one used in [68]). In this case the quantum power required for Alice is restricted to a detector device able to distinguish single-qubit states (if Bob encodes the single-qubit states into many-qubit states even a threshold detector is sufficient and not even a detector able to detect single qubits is necessary). This constitutes a step further to the realistic use of quantum computing by a general public, as soon as powerful and working quantum computers are available.

Besides the verification of the resource state, the four-qubit linear cluster state Bob sends to Alice can of course be used to perform a quantum computation as has been demonstrated in [45]. Additionally we used our setup to generate a four-qubit GHZ state (see Section 2.3.1) which is equivalent under LU operations to the star graph state. It can be used to realize an universal set of gates. We plan to realize a C-NOT gate as well as a Hadamard and a T-gate [63] in the near future. This would allow us to exploit the full possibilities of this state in the context of this new BQC protocol.

Conclusion

This thesis presents the experimental realization of two novel protocols in quantum information processing. On the one hand the ID-Bell inequality enables the efficient characterization of various important properties of multi-qubit stabilizer states. On the other hand we have implemented for the first time measurement only blind quantum computing which simplifies the technological challenges even further for a client by requiring only the capability to perform single qubit measurements.

Our experiment might lay the path for state characterization in future scenarios using more qubits. For stabilizer states this can be efficiently achieved using the ID method described in Section 3.1 which relies on only N+1 measurement settings for N qubits. We experimentally generated a four-qubit linear cluster state, a three-qubit GHZ state and a four-qubit GHZ state to demonstrate the applicability of this new method. For the first two states we could show three- and four-qubit nonlocality as well as discriminate the entanglement class and find a lower bound on the fidelity of the generated states. For the special case of a four-qubit GHZ state, a stabilizer state for which the full power of our method cannot be exploited, still a lower bound on the fidelity could be found using just 5 measurement settings. The comparison with other methods to estimate the fidelity shows that in all cases the ID method agrees with the results from QST, whereas the SG methods seems to overestimate the fidelity for noisy states and under realistic conditions the GoSG method gives a less tight lower bound than our method.

After the characterization of our experimentally generated states, Section 4 describes our implementation of a new protocol for BQC, measurement only blind quantum computing [11]. This new protocol requires Alice only to perform single-qubit measurements and is therefore less demanding on her side than the original protocol [8]. We could implement

a verification protocol [10] based on the four-qubit linear cluster state which allows Alice to test if Bob prepared the correct quantum state for her computation. We found that the preparation of trap qubits is possible, even though experimental imperfections reduce the overlap between the produced trap qubits and the ideal states. In the near future we also plan to implement a universal set of gates in this blind manner based on a four-qubit star graph state.

Bibliography

[1] D.F.V. James, P.G. Kwiat, W.J. Munro, and A.G. White. Measurement of qubits. *Phys. Rev. A*, 64(5):52312, 2001.

[2] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White. Demonstration of a simple entangling optical gate and its use in bell-state analysis. *Phys. Rev. Lett.*, 95(21):210504, 11 2005.

[3] G. Tóth and O. Gühne. Entanglement detection in the stabilizer formalism. *Phys. Rev. A*, 72:022340, Aug 2005.

[4] N. Kiesel, C. Schmid, U. Weber, G. Tóth, O. Gühne, R. Ursin, and H. Weinfurter. Experimental analysis of a four-qubit photon cluster state. *Phys. Rev. Lett.*, 95:210502, 2005.

[5] D. Gottesman. *Stabilizer codes and quantum error correction.* PhD thesis, Caltech, 1997.

[6] R. Raussendorf and H.J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, 2001.

[7] H.-J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. Measurement-based quantum computation. *Nature Phys.*, 5(1):19–26, 2009.

[8] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Proceedings of the 50th Annual Symposium on Foundations of Computer Science*, pages 517–526, 2009.

[9] J.F. Fitzsimons and E. Kashefi. Unconditionally verifiable blind computation. *arXiv:1203.5217*, 2012.

[10] T. Morimae. Verification for measurement-only blind quantum computing. *Phys. Rev. A*, 89:060302, Jun 2014.

[11] T. Morimae and K. Fujii. Blind quantum computation protocol in which alice only makes measurements. *Phys. Rev. A*, 87(5):050301, 2013.

[12] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley, 2003.

[13] F. Bloch. Nuclear induction. *Phys. Rev.*, 70:460–474, Oct 1946.

[14] N. Chandra and R. Ghosh. *Quantum Entanglement in Electron Optics: Generation, Characterization, and Applications*. Springer Series on Atomic, Optical, and Plasma Physics. Springer, 2013.

[15] O. Gühne and G. Tóth. Entanglement detection. *Physics Reports*, 474(1-6):1 – 75, 2009.

[16] D. M. Greenberger, M. A. Horne, and A. Zeilinger. *Going beyond Bell's Theorem*, pages 73–76. Kluwer, Dordrecht, 1989.

[17] W. Duer, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62:62314–62325, 2000.

[18] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, 65:052112, 2002.

[19] H. J. Briegel and R. Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86:910–913, 2001.

[20] M.A. Nielsen. Cluster-state quantum computation. *Rep. Math. Phys.*, 57(1):147–161, 2006.

[21] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[22] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41(12):2315–2323, 1994.

[23] A. Einstein, B. Podolski, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, 5 1935.

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

[25] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 10 1969.

[26] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28(14):938–941, 4 1972.

[27] M. Waegell. Primitive nonclassical structures of the N-qubit Pauli group. *Physical Review A*, 89(1):012321, January 2014.

[28] N. David Mermin. What's wrong with these elements of reality? *Print edition*, 43(6):9–11, 1990.

[29] S.-Y. Hao, Y. Xia, J. Song, and N. B. An. One-step generation of multiatom Greenberger-Horne-Zeilinger states in separate cavities via adiabatic passage. *Journal of the Optical Society of America B Optical Physics*, 30:468, February 2013.

[30] Huai-Xin Lu, Lian-Zhen Cao, Jia-Qiang Zhao, Ying-De Li, and Xiao-Qin Wang. Extreme violation of local realism with a hyper-entangled four-photon-eight-qubit greenberger-horne-zelinger state. *Sci. Rep.*, 4:4476, 2014.

[31] R. Ozeri. The trapped-ion qubit tool box. *Contemporary Physics*, 52:531–550, November 2011.

[32] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. Blok, L. Robledo, T. Taminiau, M. Markham, D. Twitchen, L. Childress, et al. Heralded entanglement between solid-state qubits separated by three metres. *Nature*, 497(7447):86–90, 2013.

[33] C. G. Yale, B. B. Buckley, D. J. Christle, G. Burkard, F. J. Heremans, L. C. Bassett, and D. D. Awschalom. All-optical control of a solid-state spin using coherent dark states. *Proceedings of the National Academy of Sciences*, 110(19):7595–7600, 2013.

[34] M. H. Devoret, A. Wallraff, and J. M. Martinis. Superconducting Qubits: A Short Review. *arXiv:cond-mat/0411174*, 2004.

[35] M. H. Devoret and R. J. Schoelkopf. Superconducting circuits for quantum information: An outlook. *Science*, 339(6124):1169–1174, 2013.

[36] D. Riste, M. Dukalski, C. A. Watson, G. de Lange, M. J. Tiggelman, Ya. M. Blanter, K. W. Lehnert, R. N. Schouten, and L. DiCarlo. Deterministic entanglement of superconducting qubits by parity measurement and feedback. *Nature*, 502:350–354, 2013.

[37] N.K. Langford. *Encoding, manipulating and measuring quantum information in optics.* PhD thesis, University of Queensland, 2007.

[38] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59(18):2044–2046, 11 1987.

[39] J. C. Garrison and R. Y. Chiao. *Quantum optics / J.C. Garrison and R.Y. Chiao.* Oxford University Press Oxford ; New York, 2008.

[40] Wikipedia. Spontaneous parametric down-conversion — wikipedia, the free encyclopedia, 2014. [Online; accessed 29-July-2014].

[41] R. Prevedel. *Experimental all-optical one-way quantum computing.* PhD thesis, University of Vienna, 2008.

[42] A. Ling, A. Lamas-Linares, and C. Kurtsiefer. Absolute emission rates of spontaneous parametric down-conversion into single transverse gaussian modes. *Phys. Rev. A*, 77(4):043834, 2008.

[43] H. Weinfurter and M. Żukowski. Four-photon entanglement from down-conversion. *Phys. Rev. A*, 64(1):010102, 2001.

[44] P. Walther and A. Zeilinger. Experimental realization of a photonic bell-state analyzer. *Phys. Rev. A*, 72(1):10302, 2005.

[45] P. Walther, KJ Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, 2005.

[46] R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein, and A. Zeilinger. High-speed linear optics quantum computing using active feed-forward. *Nature*, 445(7123):65–69, 2007.

[47] S. Barz, R. Vasconcelos, C. Greganti, M. Zwerger, W. Duer, H.J Briegel, and P. Walther. Demonstrating an element of measurement-based quantum error correction. *arXiv. 1308.5209*, 2014.

[48] M. Waegell. *Nonclassical Structures within the N-qubit Pauli Group.* PhD thesis, Worcester Polytechnic Institute, 2013.

[49] M. Waegell and P. K. Aravind. Proofs of the kochen-specker theorem based on a system of three qubits. *Journal of Physics A: Mathematical and Theoretical*, 45(40):405301, 2012.

[50] P. Walther, M. Aspelmeyer, K. J. Resch, and A. Zeilinger. Experimental violation of a cluster state bell inequality. *Phys. Rev. Lett.*, 95:020403, Jul 2005.

[51] G. Svetlichny. Distinguishing three-body from two-body nonseparability by a bell-type inequality. *Phys. Rev. D*, 35:3066–3069, May 1987.

[52] C. Greganti, M. C. Roehsner, S. Barz, M. Waegell, and P. Walther. Practical and efficient experimental characterization of multi-qubit stabilizer states. *in preperation.*

[53] H. Wunderlich and M. B. Plenio. Quantitative verification of entanglement and fidelities from incomplete measurement data. *Journal of Modern Optics*, 56(18-19):2100–2105, 2009.

[54] H. Wunderlich, G. Vallone, P. Mataloni, and M. B. Plenio. Optimal verification of entanglement in a photonic cluster state experiment. *New Journal of Physics*, 13(3):033033, 2011.

[55] S. Barz, E. Kashefi, A. Broadbent, J.F. Fitzsimons, A. Zeilinger, and P. Walther. Demonstration of blind quantum computing. *Science*, 335(6066):303–308, 2012.

[56] D. Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. R. Soc. A*, 400(1818):97–117, 1985.

[57] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, 3 1993.

[58] D. Deutsch. Quantum computational networks. *Proc. R. Soc. A*, 425(1868):73–90, 1989.

[59] J.L. Brylinski and R. Brylinski. Universal quantum gates. *arXiv:quant-ph/0108062*, 2002.

[60] T. Wei, I. Affleck, and R. Raussendorf. Two-dimensional affleck-kennedy-lieb-tasaki state on the honeycomb lattice is a universal resource for quantum computation. *Phys. Rev. A*, 86:032328, 2012.

[61] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia. Measurement-based quantum computation beyond the one-way model. *Phys. Rev. A*, 76(5):052315, 11 2007.

[62] P. Kok. Five lectures on optical quantum computing. *arXiv:0705.4193 [quant-ph]*, 2007.

[63] B. A. Bell, M. S. Tame, A. S. Clark, R. W. Nock, W. J. Wadsworth, and J. G. Rarity. Experimental characterization of universal one-way quantum computing. *New Journal of Physics*, 15(5):053030, 2013.

[64] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Theory of Computing*, pages 169–178. ACM, 2009.

[65] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[66] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther. Experimental verification of quantum computation. *Nature Physics*, 9:727–731, 2013.

[67] C. Greganti, M. C. Roehsner, S. Barz, T. Morimae, and P. Walther. Experimental demonstration of measurement only blind quantum computing. *in preperation.*

[68] M. J. Collins, C. Xiong, I. H. Rey, T. D. Vo, J. He, S. Shahnia, C. Reardon, T. F. Krauss, M. J. Steel, A. S. Clark, and B. J. Eggleton. Integrated spatial multiplexing of heralded single-photon sources. *Nat Commun*, 4, 10 2013.

Curriculum Vitae

Marie-Christine Röhsner, BSc

marie-christine.roehsner@univie.ac.at

Education:

Since 01.10.2012:	Master studies in physics, University of Vienna
01.10.2009-02.07.2012:	Bachelor studies in physics, University of Vienna, graduated with distinction
19.6.2009:	Matura (school leaving exam) with distinction
2005-2009:	Sir-Karl-Popperschule („Schulversuch für Hochbegabte Schüler/innen“ am Wiedner Gymnasium)

Employment:

01.07.-31.07.2013:	Internship at the Institute of High Energy Physics (HEPHY), Austrian Academy of Sciences
01.03.-31-07.2012:	„Studienassistentin“(study assistant) at the Faculty of Physics, University of Vienna

Scholarships:

2009/10, 2010/11, 2011/12, 2012/13	Leistungsstipendium, University of Vienna