universität wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

Quantum photonics for classically-accessible blind quantum computing

verfasst von / submitted by

Sophie-Elisabeth Lerchbaumer, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2021 / Vienna, 2021

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 876
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Physik
Betreut von / Supervisor:	Univ.-Prof. Dipl-Ing. Dr. Philip Walther

ABSTRACT

Ever since light was first recognised as discrete particles called *photons* and the development of quantum mechanics resulted out of that, it has kept the world of research busy. Combined with the rapid growth of computer science, finding always more and more complex problems to solve, and the increasing desire for more security and privacy in the age of internet, it was soon recognised that the tools needed to solve these problems could be found in superposition, interference and entanglement of quantum mechanics. With this, the field of quantum computing was born.

These new computers are neither particularly easy to handle nor to maintain. For this reason, the most probable future scenario will be a small number of quantum servers around the world which will be accessible via classical computers by everyone. In this sense, we are dedicated to the implementation of a proof-of-principal experiment that allows to access a quantum computer via a classical client while hiding input, output as well as the calculations performed for the client from the server.

This form of quantum computing is based on highly entangled states consisting of several qubits. In our implementation we use a non-deterministic single-photon source based on spontaneous parametric down conversion to generate our qubits. Unfortunately, the state generation is limited due to the fact that the number of generated entangled photon pairs scales with the pump intensity, which simultaneously leads to an increase of multi pair emission with rising pump power. For this reason we switch to a new technique of photon generation, based on quantum dots. In this context a polarisation suppression setup has also been realised, which will improve future quantum computing schemes based on these new sources.

ZUSAMMENFASSUNG

Seitdem erstmals erkannt wurde dass Licht aus diskreten Teilchen, sogenannte *Photonen*, besteht und sich daraus die Quantenmechanik entwickelte, hält diese die Welt der Forschung auf Trapp. Kombiniert mit dem rasanten Wachstum der Informatik, die immer mehr und komplexere Probleme zu lösen hatte, und dem zunehmenden Wunsch nach mehr Sicherheit und Privatsphäre im Zeitalter des Internets, erkannte man bald, dass die Werkzeuge zur Lösung dieser Probleme in der Überlagerung, Interferenz und Verschränkung der Quantenmechanik zu finden waren. Dies war die Geburtsstunde der Quantencomputer.

Diese neuen Computer sind weder besonders einfach zu handhaben noch zu warten. Aus diesem Grund liegt es nahe, dass es zukünftig eine kleine Anzahl an Quantenservern über die ganze Welt verteilt geben wird, welche über alltägliche klassische Computer für jeden zugänglich sein werden. In diesem Sinne widmen wir uns der Implementierung eines Proof-of-prinzipal Experiments, das es erlaubt, über einen klassischen Client auf einen Quantencomputer zuzugreifen und dabei die Eingabe, die Ausgabe sowie die für den Klienten durchgeführten Berechnungen vor dem Server zu verbergen.

Diese Form des Quantencomputers basiert auf hoch verschränkten Zuständen, die aus mehreren Qubits bestehen. In unserer Implementierung verwenden wir eine nicht-deterministische Ein-Photonen-Quelle, die auf spontaner parametrischer Fluoreszenz basiert, um die Qubits zu erzeugen. Unsere Cluster-Generierung ist jedoch dadurch begrenzt dass die Anzahl der erzeugten verschränkten Photonenpaare mit der Pumpintensität skaliert, was gleichzeitig zu einer Zunahme der Multipaar-Emission mit steigender Pumpleistung führt. Aus diesem Grund wechseln wir zu einer neuen Technik der Photonenerzeugung, basierend auf Quantenpunkten. In diesem Zusammenhang wurde auch ein Aufbau zur Polarisationsunterdrückung realisiert, der zukünftige Quantencomputing-Schemata, die auf diesen neuen Quellen basieren, deutlich verbessern wird.

ACKNOWLEDGEMENTS

Over the last year I had the great opportunity to work in the research group of Univ.-Prof. Dipl.-Ing. Dr. Philip Walther and collect an unbelievable amount of experience in many different areas, working on an already running experiment, designing and building my own optical setups and planning as well as building a new laboratory. Therefore, I want to thank first of all Michal, for letting me be part of all the projects and having enough trust in me, to let me work on the experiment as well as give me the opportunity to try things out on my own. Without you, this amazing experience wouldn't have been possible.

Also a big thank goes to Philip, for letting me join the group, and Lee who took me under his wings during several weeks of my master project.

My time here would have been not even half as enjoyable, if it wasn't for my amazing colleagues, which never stingied with helping out and discussing upcoming challenges. Therefor a huge thanks to Michal, Juan, Mat, Michele, Peter S., Philipp, Valeria, Marie-Christine, Peter N., Stefan and particularly Beate. A special thanks goes therefore also to my 3rd floor lab companions with which we drowned the Cryo-noise in even louder music and who never got annoyed by me hiding behind curtains, making strange sounds, constantly humming or singing.

Even with such an amazing professional environment, all that wouldn't have been possible if it wasn't for my family and friends always supporting me in any situation.

Danke Mom, Dad, Beate, Igi, Peter und Lena! You always knew how to calm me down, push me forward or give me a different point of view if needed.

Mom und Dad, danke dass Ihr mir Alles
ermöglicht und immer hinter mir steht!

CONTENTS

1 | INTRODUCTION

Over the last 120 years Planck discovered that electromagnetic radiation is emitted only in discrete energy bundles called quanta, Einstein solved the mystery around the photoelectric effect by describing light as particles called photons and the theory of quantum mechanics was developed by Heisenberg, Schrödinger and Dirac, to name only the most popular [1].
Next to this evolution of quantum mechanics another field started to develop even faster. Although it already existed in Babylonian times around 1750 B.C., computer science was revisited 1936 by Turing and his *Turing machine* [2]. Not long afterwards, the invention of the transistor in 1947 started a new age of computer science, evolving so fast that Moore came 1965 to the conclusion that computational power will roughly double every two years for constant cost [3]. Ever since, with the miniaturization of transistors, computers have become smaller, faster and more powerful while taking over our everyday life [4].

The fast growth of computational power will face limitations as transistors have reached already a size of 1 nm [5] and won't become much smaller without entering a regime where quantum physical effects can't be neglected any longer. As Feynman realized 1982 [6], one can take advantage of these quantum effects and use them to process information and simulate quantum systems, whose constellation would be too complex to be computed by classical computers. Computational machines based on quantum mechanical effects are today called quantum computers and they can predominate classical computers in specific tasks. This was shown for the first time with the Deutsch-Josza algorithm [7], followed by Shor's algorithm [8] and Grover's algorithm [9] only to name a few of them [10].

Quantum computers don't rely on classical bits like their counter parts, representing either the value 0 or 1, but on quantum mechanical two-level systems called qubits that can exist also in any coherent superposition of 0 and 1. Which two level quantum system will win the race of being used to implement future quantum computer isn't decided jet. Until today quantum computers have been implemented on the base of atoms [11, 12], ions [13], superconducting systems [14, 15], solid-state- systems [16] and photons [17–19]. Using quantum mechanical superposition, interference and entanglement result not only in computational speedup in specific tasks, but also in new and safer data protection opportunities [20–24].

Over the last year, we have focused on the implementation of a photonic quantum computer that processes information in the form of measurements and presents security advantages. We decided to implement qubits by using photons as they do not decohere due to their lack of interaction with their environment and with one another. Additional, photons can easily be sent from one place to another through free space or fibers and single qubits can easily be manipulated by waveplates, if the qubits are polarization encoded, as it is the case in our experiment.
Unlike the blind quantum computer architectures implemented so far [18], our implemented

protocol allows a complete classical client following the server-client structure [25]. This is an important aspect, as near future quantum computers won't be easy to handle machines for everyone's living room, but rather shared quantum servers around the world, that external people with classical computers will access.

For our implementation, single photons are generated by spontaneous parametric down conversion (SPDC) single photon sources, which are the most common used single photon sources providing entangled photons pairs [26]. We have chosen this source, because measurement based quantum computing (MBQC) architectures require highly-entangled multi-particle resource states [20, 22, 23, 27, 28] and SPDC sources provide already polarization entangled photon pairs with a high repetition rate [26, 29]. By using SPDC sources, we need fewer probabilistic tasks to generate the needed resource state, compared to the case with non-entangled single photon sources.
On the other hand, the SPDC process is a spontaneous effect occurring with a probability that is dependent on the pump power [30]. Rising the pump power will not only increase the single photon pair generation, but also the multi photon emission. In order to prevent such multi photon events, the probability of generating a single photon pair per pump pulse is kept typically under 0.1 [31], which makes the source non-deterministic. Since future quantum computers will have to solve more complicated tasks and therefore require more complex resource states, we will switch to single photon sources based on quantum dots, that can generate single photons and polarization entangled photon pairs on demand [30, 32–34]. For future experiments including these new sources, I build a setup, that separates pump photons from single photons emitted by the quantum dot on the bases of their different polarization. This polarization suppression setup, combined with the quantum dot single photon sources will improve future MBQC protocol implementations.

In the first chapter I give an introduction to the theory of quantum computing, which starts with the basic concepts of quantum mechanics, leading to the different structures of quantum computing before closing with the theoretical explanation of the targeted protocol. Following up in the next chapter, the experimental implementation of the building blocks for the desired quantum computer are given together with the underlying theory and required technology. In the end of this chapter the results of the experiment so far are noted.
As it wasn't possible to finish the experiment during the last year, an outlook explains the further steps in the implementation. An additional experimental proposal for quantum-dot based sources is also provided. Finally, this thesis ends with a short conclusion, summarizing the discussed topics.

2 THEORY OF QUANTUM COMPUTING

2.1 BASIC CONCEPTS OF QUANTUM COMPUTING

In this section, the main building blocks of quantum computers are presented together with an introduction to the concept of quantum computing itself. Finally the implemented protocol is explained in more detail. The processing of a quantum computer relies on the usage of quantum effects, which are described using the mathematical framework of quantum mechanic. So before rushing into the theory of quantum computing, let us have a short reminder of the concepts of quantum mechanics based on [4, 10, 20, 35–37].

Quantum States

Any *isolated* physical system is described by a complex vector space with an inner product (Hilber space). In this *state space* the system is fully specified by a unit vector $|\psi\rangle$ known as *state vector* of the system. A special property of quantum mechanics is that if one takes two or more possible states $|\psi_n\rangle$, any complex linear combination of these states is also a possible state of the system. This is called *superposition*.

$$|\psi\rangle = \sum_n a_n |\psi_n\rangle \qquad a_n \in \mathbb{C} \tag{2.1}$$

If these vectors are orthonormal, which means that they are normalized and orthogonal ($\langle\psi_i|\,\psi_j\rangle = \delta_{i,j}$), then $\sum_n |a_n|^2 = 1$.
The time evolution of these states in a *closed* system is described by unitary transformations. So if $|\psi\rangle$ describes the system at t_1 and $|\psi'\rangle$ at t_2, then they are related to each other by a unitary operator U.

$$|\psi'\rangle = U\,|\psi\rangle \tag{2.2}$$

Another way of describing a state is given by the *density operator* ρ. With it, one has the opportunity to differentiate between fully specified states, also known as *pure states*, and *mixed states*. For the latter ones, information is missing and only the probability p_n to find the system in a specific state $|\psi_n\rangle$ is known. The density matrix is positive, Hermitian, normalized and defined in the following way.

$$\rho = \sum_n p_n\,|\psi_n\rangle\,\langle\psi_n| \qquad \text{with} \qquad \sum_n p_n = 1 \tag{2.3}$$

It simplifies for pure states to

$$\rho = |\psi\rangle\,\langle\psi| \tag{2.4}$$

Since $\mathrm{Tr}(\rho^2) = 1$ holds for all pure states, all the others are defined to be mixed. How pure a given state ρ is can therefore be determined by the purity $\mathcal{P}$ and the closer $\mathcal{P}$ gets to 1, the purer the state [10].

$$\mathcal{P} = \mathrm{Tr}(\rho^2) \tag{2.5}$$

Additionally, the density matrix can be used to characterize a state prepared in the laboratory, and the elements of the matrix are measured via quantum state tomography. Afterwards one can determine how much the generated state differs from the desired one by measuring the closeness of the prepared and desired state via the Fidelity $\mathcal{F}$. It gives the probability that a system prepared in state ρ will pass a test that determines if the given system is in the expected state σ [10].

$$\mathcal{F} = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2 \tag{2.6}$$

Quantum entanglement

It gets even more interesting if not only one, but two quantum systems a and b are taken into account. Assuming these systems to be seperable and in the pure states $|\phi\rangle_a$ and $|\xi\rangle_b$, one can write the pure state of the product Hilbert space as

$$|\psi\rangle = |\phi\rangle_a \otimes |\xi\rangle_b \tag{2.7}$$

On such separable states one can perform unitary transformations on all of the states, or only one of them without influencing the others. Aside from that, there also exists the opportunity for correlations between states, which is referred to as *Entanglement*. If two or more states can't be written as a product state given in (2.7), they are entangled. It follows, that all correlated pure states are entangled, but this doesn't hold for mixed states. Latter ones are considered to be entangled only if they can't be written as

$$\rho = \rho_a \otimes \rho_b \tag{2.8}$$

The most famous entangled states are the *maximally entangled two-qubit Bell* states. If one of the qubits in such a state is measured, the measurement result of the second qubit is predefined due to their entanglement.

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle \pm |1\rangle|1\rangle\right) \tag{2.9}$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle \pm |1\rangle|0\rangle\right) \tag{2.10}$$

The correlations between the entangled states have no limitation in distance and made Einstein, Podolsky and Rosen question the completeness of quantum mechanic, also known as *EPR paradox* [38]. Building on their paradox, it was experimentally proven many times that quantum states are in fact non-local [39–41]. A common way to determine entanglement is given by the use of entanglement witnesses $\mathcal{W}$. Not every witness fits for every entangled

state, so the challenge lies in finding the entanglement witness suitable for the state of the system. If such a witness is found for an entangled state σ, then $\mathrm{Tr}(\mathcal{W}\sigma) < 0$ [42]. This is done by measuring the mean value of the witness operator $\langle \mathcal{W} \rangle = \mathrm{Tr}(\mathcal{W}\sigma)$.

Quantum Measurements

General, quantum measurements are given by a complete collection of Hermitian *measurement operators*. In this thesis we refer as measurements to *von Neumann measurements* with measurement operators M.

$$M = \sum_m a_m P_m \tag{2.11}$$

Here a_m is an eigenvalue of the observable, which gives a possible outcome of the measurement and P_m describes the corresponding orthogonal projectors.

If the operator M acts on a state $|\psi\rangle$, then the outcome will be one of the eigenvalues of the operator and the state is irreversibly projected onto the corresponding eigenvector. This phenomenon is also known as 'collapse of the wave-function'. Immediately repeating the measurement with the same operator will give the same result and no additional information about the original state $|\psi\rangle$. Gaining further information of the original state would mean to measure with an observable A with different eigenvectors than the already used one M. This also means that this two observables are not commuting $[M, A] \neq 0$ so that due to Heisenberg's uncertainty principle the outcome of the second measurement will be completely random and wouldn't tell anything more about the original state [4].

2.1.1 The Qubit

Classical computations are based on physical *bits*, which are systems that have two distinct states 0 and 1. Similar to the classical computations, one uses quantum systems with two distinct, meaning orthogonal, states, as basic pieces of information. They are called quantum bits or *qubits* for short and the states in the computational basis of such a qubit are labeled in the braket notation as $|0\rangle$ and $|1\rangle$.

In difference to its classical counterpart, the qubit can, according to the superposition principle (2.1), be prepared in any linear combination of the two distinguishable states $|0\rangle$ and $|1\rangle$.

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.12}$$

Therefore α and β are complex numbers that have to fulfil the normalization condition $|\alpha|^2 + |\beta|^2 = 1$, and the computational basis states can be written in the vector notation as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.13}$$

A common way to illustrate a qubit is to picture it as a point on the surface of the *Bloch sphere* (see figure 2.1). It is a sphere of radius one, where each point on the surface corresponds to a different pure state and opposite points are pairs of mutually orthogonal states. A qubit

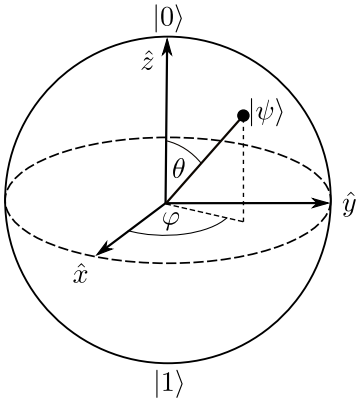


Figure 2.1: Bloch Sphere. Illustration of a qubit on the Bloch Sphere with its free parameters θ, ϕ and the norm $|\cdot|^2$. If the state is pure, it has norm 1 and lies on the surface of the sphere. Otherwise it is mixed.

can then in general be represented by a point on the Bloch sphere with the spherical polar coordinates θ and ϕ, as visualized in figure 2.1.

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.14}$$

Despite the fact that there exist infinitely many points on the Bloch sphere, a measurement in the computational basis will only give the outcome $|0\rangle$ with probability $|\alpha|^2$ or $|1\rangle$ with probability $|\beta|^2$ and no further information about the values α and β. This is also reflected in the fact that one can only get one bit of information out of a single qubit [4]. However, during the time the qubit isn't observed, all this information, that cannot be directly extracted, cause experimentally verifiable consequences. This is what builds the heart of quantum computing and quantum information.

2.1.2 Quantum logic gates

Essential components of a classical computer are the memory, to store information, and the processor, which performs calculation by applying binary logic gates on bits. For a quantum computer the information bit is represented by qubits and the information is processed depending on the type of quantum computer architecture that is used. There are two different types of quantum computer architectures. One is the *circuit based quantum computing*, where processing is realized by letting qubits pass as many quantum logic gates as needed to perform the desired calculation and measuring the transformed qubits in the end to get the final result. The second type is called *measurement based quantum computing* (MBQC), which relies on highly entangled multi qubit states, were information processing is performed by measuring qubits of the given resource state in different measurement bases.

Since a bit in classical computing can only have the value 0 or 1, there exist only two possible actions for classical single-bit gates. Either the identity or the flip gate, also known as NOT gate. In the case of two-bit classical gates, two input bits are combined to a single output bit. Most commonly known two-bit gates are the AND and OR gate, as well as their complementary, NAND and NOR. The last two gates form individual a universal set of gates [10]. As in classical computation, also in the quantum case there exists a universal set of

different quantum logic gates with which any desired computational task can be performed. In other words, with such a set, we are able to implement any unitary. In quantum computing we need therefore a sequence of single-qubit gates and one type of two-qubit gate [36]. But compared to classical computation, single-qubit logic gates will not only change between 0 and 1, but will be rotated on the Blochsphere. Also for the two-qubit gates, the input states are not combined to a single output, but both input states remain, and change according to the performance of the gate. This results out of the unitarity of quantum mechanics.

SINGLE-QUBIT GATES Using the vector notation of a qubit, given in section 2.1.1, a single qubit gate can be written as a 2×2 unitary matrix. The fact that it has to be unitary implies that every quantum logic gate is *reversible* and follows from the condition that the norm of a given state must be preserved during the computation [36]. For single qubit operations, the most important gates are the Pauli matrices, which perform a transformation equivalent to a π rotation on the Bloch sphere along the corresponding axis.

$$\begin{aligned} \sigma_0 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{2.15}$$

Three additional major gates are the *Hadamard* gate H, which transformes the computational states into a superposition of each other

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.16}$$

the *Phase*-gate S, that adds a phase of $\pi/2$ at the computational basis state $|1\rangle$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{2.17}$$

and the $\pi/8$-gate (or T-gate), that also applies a phase on $|1\rangle$ of the value $\pi/4$.

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \tag{2.18}$$

In general not all of these gates are needed to perform computation. For example a general rotation around an arbitrary axis of the Bloch sphere can be written as a decomposition of Pauli gates [4]. In fact the set of gates that is needed to perform any one qubit gate can be reduced down to the H and the $\pi/8$ gate. These two gates are universal and an effectual long series of these gates can perform any desired one-qubit transformation [4].

One more gate, that is frequently used in MBQC is the rotation around the z- or x-axis in an amount of an arbitrary angle α.

$$R_z(\alpha) = e^{-i\alpha\sigma_z/2} \qquad R_x(\alpha) = e^{-i\alpha\sigma_x/2} \tag{2.19}$$

With this relation one can write the decomposition of an arbitrary rotation δ on the Bloch sphere with the *Euler angles* α, β and γ [20, 43].

$$R(\delta) = R_z(\alpha)R_x(\beta)R_z(\gamma) \tag{2.20}$$

MULTI-QUBIT GATES To have a universal set of gates, we are missing multi-qubit gates that let qubits interact. Particular useful are the *controlled* unitary operators that take two qubits as an input and are represented as 4×4 matrices in the matrix notation. The first qubit in the notation is defined to be the *control* qubit, dependent on which the second qubit, named *target*, is transformed.

Common two-qubit gates are the controlled-NOT gate (CNOT) and the controlled-phase gate (CZ or C*Phase*). If the control qubit is in state $|0\rangle$, the gate leaves everything unchanged. But if the state is $|1\rangle$, the gate performs a transformation on the target qubit. For the CNOT gate, the target state would be flipped, corresponding to an X operation and the CZ gate would add a phase of -1 to the target qubit, if the target is in state $|1\rangle$.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{2.21}$$

These two gates are the most important two-qubit gates in quantum information and quantum computing. Together with the H and the $\pi/8$ gate, the CNOT forms a universal set of gates, with which any unitary operation can be approximated with any desired accuracy [4, 10, 36]. So if it is possible to physically implement these three gates, then it is possible to physically realize any type of computation.

These gates are especially important, as they are crucial to generate entanglement between qubits. As an example take two horizontally polarized photons, where the first one passes a Hadamard gate while the second one is flipped. Afterwards they interfere in a CNOT gate, where the first photon is taken as control qubit, a $|\psi^+\rangle$ Bell-state is generated.

$$|H,H\rangle_{a,b} \xrightarrow{H_a,\sigma_{x,b}} \frac{1}{\sqrt{2}}\left(|H,V\rangle_{a,b} + |V,V\rangle_{a,b}\right) \xrightarrow{CNOT_{a,b}} \frac{1}{\sqrt{2}}\left(|H,V\rangle_{a,b} + |V,H\rangle_{a,b}\right) \tag{2.22}$$

But implementing these gates with linear optics, as it is the case for our experiment, holds a challenge in itself, because it is not possible to perform deterministic two-qubit gates, as the CNOT or the CZ gate, with linear optics in the dual-rail or polarization encoding [44, 45]. This is a consequence of the fact that photons do not interact with each other or their environment.

Transformation performed with linear optics are described by *Bogoliubov transformations* of creation operators represented by $\hat{a}^\dagger$ or $\hat{b}^\dagger$. And as an example we have a look at the example given in (2.22).

$$\hat{a}_H^\dagger \hat{b}_H^\dagger \quad \rightarrow \quad \left(\sum_{k=H,V} \alpha_k \hat{a}_k^\dagger + \beta_k \hat{b}_k^\dagger\right)\left(\sum_{k=H,V} \gamma_k \hat{a}_k^\dagger + \delta_k \hat{b}_k^\dagger\right) \tag{2.23}$$

$$\neq \quad \hat{a}_H^\dagger \hat{b}_V^\dagger + \hat{a}_V^\dagger \hat{b}_H^\dagger \tag{2.24}$$

For any choice of α_k, β_k, γ_k and δ_k it is impossible to make the right-hand side in both lines of the equation above equal. In the equation, the first line represents the Bogoliubov transformation performed by linear optics, whereas the second line gives a maximally entangled state. This shows that it is not possible to deterministically generate maximal polarization entanglement given only single photons and linear optics [44].

In order to achieve the needed 'interaction' between photons in two-qubit gates, one can take advantage of the fact that photons follow bosonic statistics and fulfil the bosonic commutator relation $[\hat{a}_j, \hat{a}_i^\dagger] = \delta_{ji}$. Therefor, it is possible to built probabilistic two-qubit gates based on second-order interference, which will be explained in more detail in section 3.1.

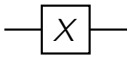
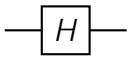
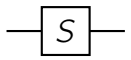
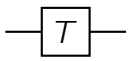
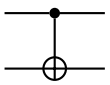
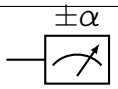
2.1.3 Circuits

Up to now we have all the building blocks to perform any desired computation, but the more complex the protocols become, the more single and two-qubit gates have to be combined. It can get hard to follow the performed transformations in the matrix notation or even in the Dirac notation. Therefore it is useful to connect gates similar to the Boolean gates used in digital electronics and built quantum circuits [36]. In this diagrammatic representation, all qubits are visualized as horizontal lines that pass through single qubit gates, which are represented by small boxes (see table 2.1). If two qubits pass together a two qubit gate, then they are connected by a vertical line. The symbols for the main quantum gates introduced in the previous section are given in table (2.1).

2.2 MEASUREMENT BASED QUANTUM COMPUTING

In circuit based quantum computing, qubits are passed through quantum logic gates in order to process information. Therefore entanglement that is needed for the computation ins generated during the processing procedure itself. Coming back to the fact that our experiment is based on photons and therefore includes probabilistic two-qubit gates, the wish arises to overcome these non-deterministic elements in the circuit. One idea was given by Gottesman and Chuang 1999 [46], where the probabilistic tasks are performed offline and teleported into the circuit only, if the gate was performed successfully. Unfortunately also this teleportation trick relies on Bell measurements, which are impossible to perform in a deterministic way with linear optics [45]. Knill, Laflamme and Milburn (KLM) came 2001 up with a protocol that allows efficient quantum computation based only on the use of beam splitters, phase shifters, single photon sources and photo-detectors [47]. They have their own variant of Bell measurement,

Table 2.1: This table includes the symbols of the most important gates used in quantum computing represented in the circuit notation. For the Pauli matrices only the Pauli-X is listed representative for all of them. The last entry shows the symbol for a measurement in the basis $|\pm\alpha\rangle$ as defined in equation (2.29). If no measurement basis is given, the measurement is performed in the computational basis.

Gate	Circuit Symbol
Pauli-X	
Hadamar	
Phase gate	
$\pi/8$	
CNOT	
CZ	
Measurement	

that includes an arbitrary small error scaling with the number of used ancilla photons. But to get the error smaller than the fault-tolerant threshold, a tremendous resource is needed. The KLM protocol was improved many times and lead to quantum computing schemes called *measurement-based quantum computing* (MBQC). In comparison to the circuit based protocols, MBQC uses sequences of adaptive measurements to implement different computations [20, 22, 23, 27, 28]. The advantage of these schemes is, that the qubits don't have to pass through probabilistic multi-qubit gates during the calculation process. The probabilistic tasks are outsourced into the state preparation.

There are two different types of MBQC. One is *teleportation-based* quantum computing [28] and the other one is called *one-way* quantum computing [22, 27]. Teleportation based quantum computing relies on Bell-pairs and two qubit measurements based on the *Gottesman-Chuang theorem* [46]. Since the focus of this thesis is more on the one-way computation architecture, the teleportation scheme won't be discussed in more detail here. However, it was shown that the two types of MBQC are anyway equivalent [48].

Processing of information in the one-way quantum computing scheme is based only on single-qubit measurements [22, 23, 27]. Since these measurements can't create entanglement, this has to be provided as a resource, which is given by highly-entangled multi-particle states.

2.2.1 Graph states

As mentioned, the recourse for MBQC has to be a highly-entangled multi-particle state. To visualize this type of state it can be useful to represent it by a mathematical graph $G = (V, E)$. In the graph the vertices V symbolize the physical qubits and the edges E refer to CZ gates applied between those. The states needed for one-way quantum computing are those, where the underlying graphs have the form of d-dimensional lattices also known as cluster states [25, 49]. An example of such a two-dimensional lattice state is given in figure 2.3. Such a state is generated by preparing all qubits that will be part of the cluster in an initial state of $|+\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle)$ and afterwards entangling them according to the edges in the graph by applying CZ gates on the qubits that have to be entangled with each other. Assuming that

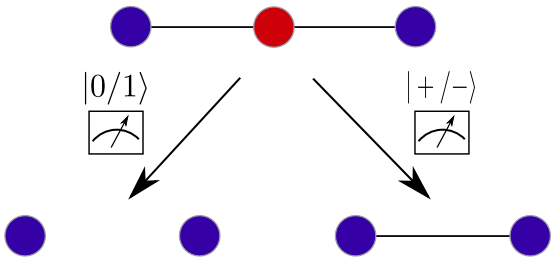


Figure 2.2: Measuring the red qubit will remove the qubit itself and in case of a measurement in the computational basis $|0/1\rangle$ also the entanglement between the neighboring qubits. Instead, for the diagonal basis $|+/-\rangle$ the entanglement between the nearest neighbors of the measured qubit will remain.

we already have such a lattice state and want to change the structure afterwards, then we can apply measurements in the Z-basis $|H/V\rangle$ on a vertex a, which will delete the measured qubit from the cluster and break all the edges with which it was connected to its nearest neighbors $\mathcal{N}_a$. Instead, applying a measurement in the the X-basis $|+/-\rangle$ will also delete the qubit from the graph, but preserve the entanglement between the nearest neighbors (see figure 2.2) [22, 23, 27].

Finally characterizing the generated cluster can be done by state tomography, using 3^n measurements where n is the number of qubits in the cluster [42]. Instead, one can take advantage of the fact that graph states can be written down in the stabilizer formalism [50, 51]. It states that for every vertex a a stabilizer S_a can be defined

$$S_a \coloneqq \sigma_x^{(a)} \prod_{b \in \mathcal{N}_a} \sigma_z^{(b)} \tag{2.25}$$

Each stabilizer S_a has a unique graph state $|G\rangle$ as eigenstate, fulfilling the eigenstate equation (2.26) with an eigenvalue of $+1$.

$$S_a |G\rangle = |G\rangle \tag{2.26}$$

In this way a cluster state can be fully characterized by the stabilizer operators of the vertices.

LOCAL COMPLEMENTATION For the ability to perform different circuits, one needs access to diverse graph states. This is because dissimilar graph states perform different circuits [18, 19]. Luckily there exists a way to transform graph states into each other when they are equivalent under *local Clifford unitaries* (LCs) [51–54].

Local Clifford unitaries are part of a class of transformations, that map the Pauli operators onto themselves under conjugation, and performed on a cluster they perform a transformation called *local complementation*. Applying such a transformation on a vertex a, the edges connected directly to a remain, while all the existing edges between the nearest neighbors of a are removed and the edges that were missing between the neighbors before are added [52]. An example of such an LC transformation is pictured in figure 2.3. Two graph states $|G\rangle$ and $|G'\rangle$ are LC-equivalent if and only if, the two graphs G and G' are transformable into each other by applying a sequence of local complementations. The LC operator U_a^{LC} that causes an LC transformation on a vertex a is given by [52–54]

$$U_a^{LC}(G) = \sqrt{-i\sigma_x^{(a)}} \prod_{b \in \mathcal{N}_a} \sqrt{i\sigma_z^{(b)}} \tag{2.27}$$

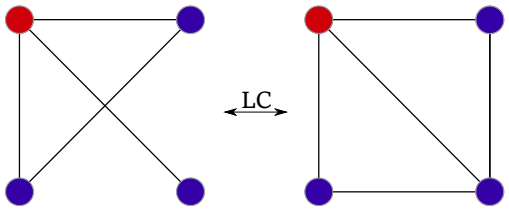


Figure 2.3: Local complementation. A local complementation applied on the red vertex of the graph removes all edges between the nearest neighbors of a ($\mathcal{N}_a$) and adds the ones that were missing before. The connections between the red vertex and $\mathcal{N}_a$ remain unchanged.

where the square root of the Pauli operators can also be written using exponentials.

$$\sqrt{-i\sigma_x} = \exp\left(-i\frac{\pi}{4}\sigma_x\right) \qquad \sqrt{i\sigma_z} = \exp\left(i\frac{\pi}{4}\sigma_z\right) \tag{2.28}$$

This is known as the *LC rule* [53, 54]. Applying this rule consecutively on any graph allows to generate the complete orbit of this graph state under local unitary operations within the Clifford group [54]. Experimentally this opens the opportunity to have access to a much larger variety of graph states, and with that, the chance to implement a larger amount of different quantum circuits.

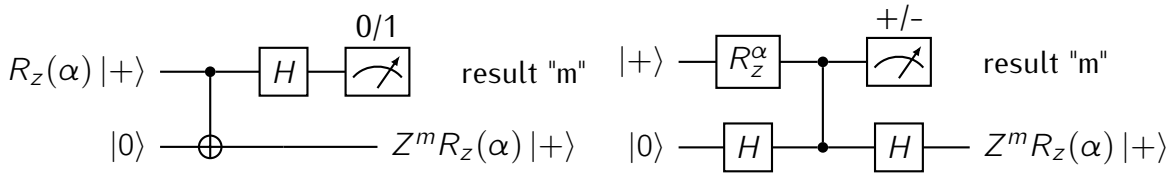
2.2.2 One-way quantum computing

For the computation in the one-way computation model, the resources are given by two dimensional lattice graph states (as an example see figure 2.3), and single-qubit measurements in combination with feed-forward realize the processing of the information. A computation is seen as performed in the correct way if all the measurements give the result 0. This is referred to as the *positive branch* and all circuits are outlined in a way that the desired result is given in the case of a positive branch. However, if that is not the case, because projective measurements are inherently random in quantum mechanic, and a result in between is given by 1, a feed-forward mechanism has to correct the appearing error by applying Pauli corrections on the effected qubits or adapting future measurement angles. If it is possible to make each branch of the calculation equal to the positive branch after each measurement, by applying local corrections and if that is possible independent of the measurement angle, then the calculation is called to be *uniformly*, *strongly* and *stepwise deterministic* [25, 55].

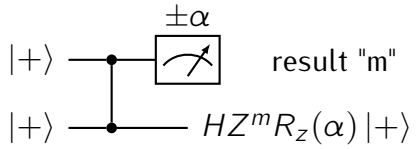
Different graph states allow individual computations. The idea is to build a complete two dimensional lattice graph state and remove all the vertices that should not be part of the calculation with measurements in the computational- or x-basis. This disconnects the qubit from the cluster and breaks all their connections to other vertices. In that way the wanted cluster can be formed [22, 23, 27]. Then, the horizontal entanglement connections are used to perform one-qubit gates while the vertical ones open the opportunity to perform two-qubit gates [27]. Therefore the qubits are measured in the basis $|\pm\alpha\rangle$ which applies a rotation of $R_z(\alpha)$ (see equation (2.19)) on an encoded qubit in the graph state up to a Hadamard gate.

$$|\pm\alpha\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle \pm e^{-i\alpha}|1\rangle\right) \tag{2.29}$$

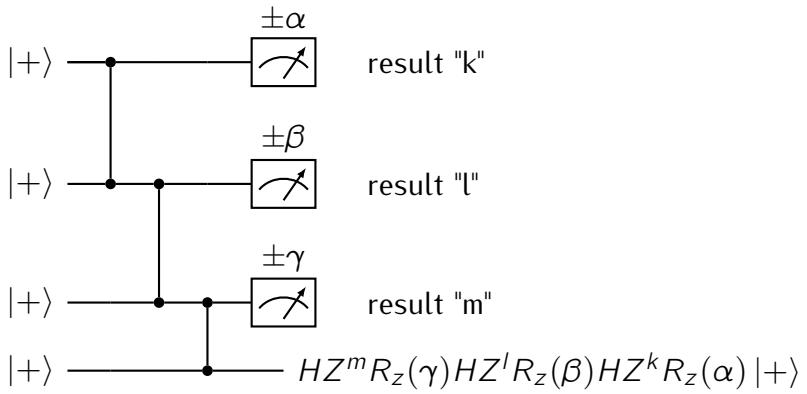
Let us have a closer look at a teleportation circuit. There, information of an unknown qubit $R_z(\alpha)\,|+\rangle$ is teleported (up to a pauli correction) onto a second qubit initially prepared in state $|0\rangle$. As the preparation of the unknown qubit can also be performed inside the circuit and a CNOT gate is equivalent to a CZ gate up to Hadamard gates ($\mathrm{CNOT} = (\mathbb{1} \otimes H)\mathrm{CZ}(\mathbb{1} \otimes H)$) the following two teleportation circuits are equivalent [20].



Here Z and later also X represent Pauli matrices. Be aware that in these circuits each horizontal line represents a physical quibt. There are also circuits were every line represents a logical qubit. Since the rotation around the z-axis commutes with the CZ gate ($[R_z, \mathrm{CZ}] = 0$), it can be implemented after the gate and be 'absorbed' in the measurement. In the same way the preparation of the second qubit can include the Hadamard gate, which simplifies the given circuit to this equivalent implementation.



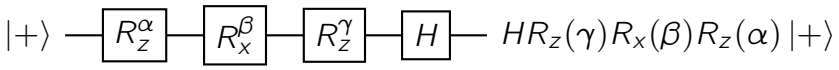
With this a rotation around the z-axis is performable. For any arbitrary rotation $R(\delta)$ in the Bloch sphere, rotations around the x- and the z-axis are needed (see equation (2.20)). This can be implemented by a four qubit linear cluster state [19]. Following circuit corresponds exactly to such a rotation.



Since the x and z rotations can be transformed into each other ($XR_z(\alpha) = R_z(-\alpha)X$, $HZ = XH$ and $HR_z(\alpha)H = R_x(\alpha)$) we can rewrite the output state as

$$X^l Z^m X^k H R_z\left((-1)^l\gamma\right) R_x\left((-1)^k\beta\right) R_z(\alpha)\,|+\rangle$$

It is common to write circuits down assuming the positive branche and visualizing in each horizontal line the evolution of a logical qubit. Translating that to the circuit from above gives us the following circuit.



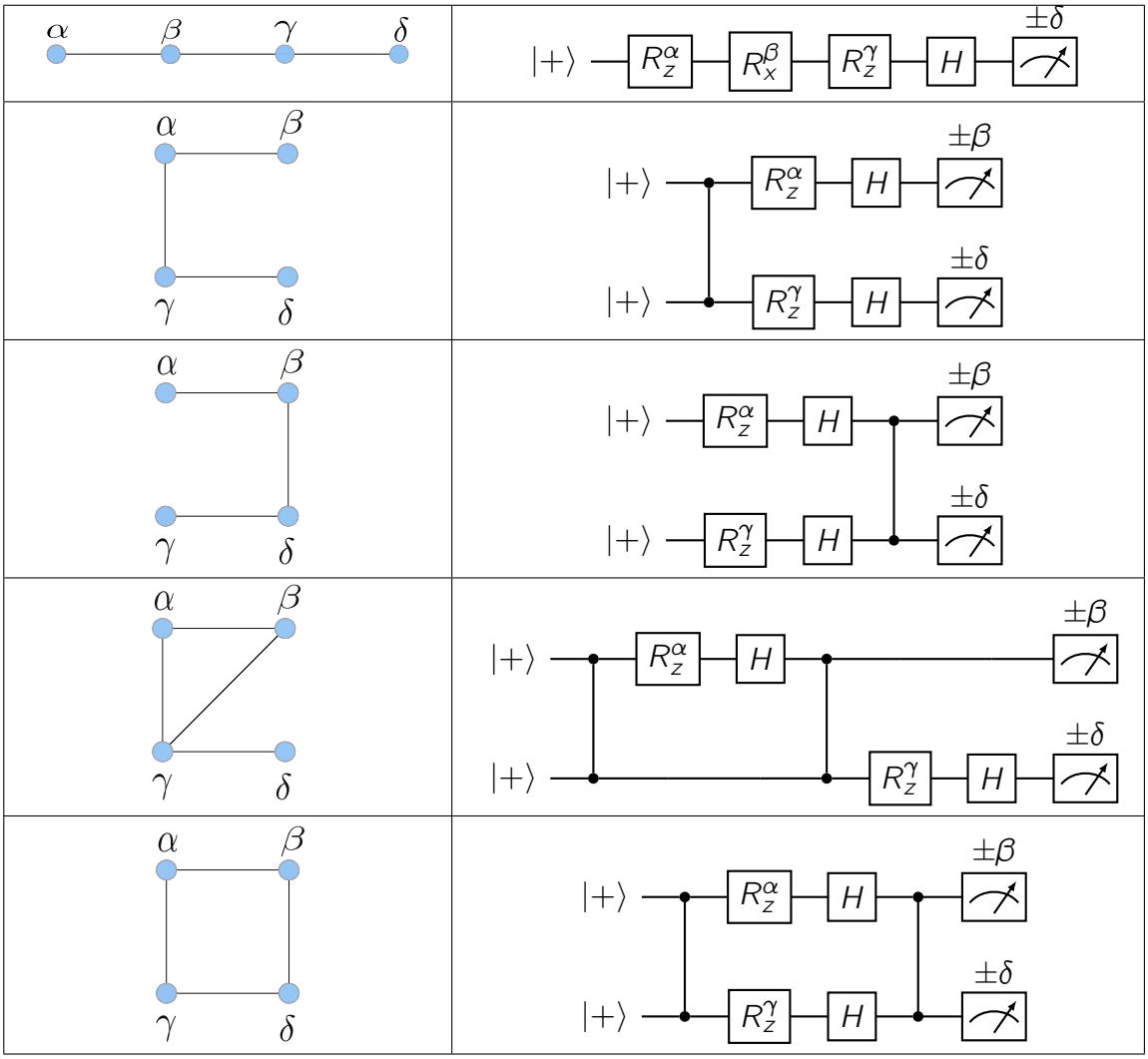


Table 2.2.: This table includes different four qubit cluster states and the according circuit one can perform with them as given in [18, 19]. Over the vertices in the graph states, the measurement angles are noted.

All computations performed with a linear cluster can still be efficiently simulated with a classical computer [56]. In order to have a universal quantum computer two-qubit gates are also needed, which are implemented by the vertical lines in a cluster. As we have seen in section 2.2.1, by only using LC operations, a cluster can be reshaped into other clusters that can perform different quantum circuits. Some examples of such LC transformations are given in table A.2 in the appendix and in table 2.2 some additional examples of different cluster graph states with the circuits on can perform with them are noted in [18, 19].

BLIND QUANTUM COMPUTING Quantum computers based on measurements need feed forward procedures to correct runtime errors and therefore they offer benefits in speedups as well as advantages in privacy and security compared to their classical counterparts. This will become very important in the future, since current realizations of quantum computers rely on ions [13], photons [18, 19], superconducting- [14, 15], atomic- [11, 12] or solid-state-

systems [16], which need an immense effort to be built and continuously run. This leads to the assumption, that the most probable scenarios for future quantum computers will be a handful of powerful quantum servers existing around the world, which will be accessible for external clients. In order to ensure the privacy of the clients, the server should have no information about the input or the output, or even the calculation of the tasks itself that he has to perform. This can be achieved by a concept based on one-way quantum computing called *blind quantum computing* (BQC) [21, 24].

Starting with hiding the computation from the server, the structure of the graph state, on which the calculation is performed, should not reveal any information about the circuit that will be processed. Since different graph state structures enable different circuits (see table 2.2), the given cluster state should provide the opportunity to perform any task. In other words, it has to be uniform [18]. By applying random rotations θ_j to the initial qubits, and therefore preparing random qubits $|\theta_j\rangle$, the input information can be hidden.

$$|\theta_j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{-i\theta_j}|1\rangle\right)$$

Measurements on these random qubits $|\theta_j\rangle$ in the basis $|\pm\delta_i\rangle$ (see equation (2.29)) then cause a rotation of $R_z(\pm\delta_i + \theta_j)$ followed by a H on the encoded input state $|+\rangle$. The hiding of input and output information is achieved by the fact that the measurement angle sent to the server δ_i includes three different parameters.

$$\delta_j \ = \phi_j + \theta_j + \pi r_j \tag{2.30}$$

The real measurement angle that should be applied to the encoded qubit $|+\rangle$ is given by ϕ_j and θ_j compensates the initial random rotation and any upcoming Pauli errors caused by measurement outcomes. Finally, the random variable $r_j \in \{0, 1\}$ adds a π shift to the measurement angle, which causes a flip of the measurement outcome and can be easily redone, if r_j is known.

If θ_j is unknown, no information about ϕ_j can be extracted. After every measurement, the server sends the outcome to the client who flips the outcome depending on r_j and calculates the next measurement angle that it again sends to the server. In this way, the input as well as the output and the performed circuit are hidden from the server and the privacy of the client is kept.

Since, the random rotations shouldn't be known by the server, the qubits have to be prepared by the client itself and afterwards transmitted to the server, where they are entangled by the server and information processing is performed similar to the one-way quantum computing scheme by measuring qubit after qubit in the measurement basis that the server receives each round from the client. Performing this protocol requires a semi-quantum client, able to prepare randomly rotated qubits, that is connected to the server via a quantum as well as a classical channel. But access to future quantum servers should be possible for everyone by only using our everyday classical computers and shouldn't presume a running laboratory, which is impossible in this protocol.

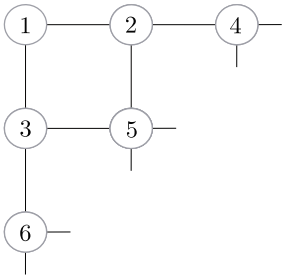


Figure 2.4: Two dimensional lattice graph. In the vertices the numbers refer to the measurment order of the qubits. For the *Flow Ambiguity* protocol we refer always to this measurement order.

2.3 FLOW AMBIGUITY

Until now, blind MBQC was based on semi-quantum clients or classical clients in combination with two non-communicating entangled quantum servers [24]. Making the quantum server accessible for everyone and offering security with the BQC protocol necessitates, that every household that wants to have access to the server will need a laboratory at home and a quantum channel to the server. Since this is not possible with the technical and infrastructural standards of today, a new protocol was invented, called *Flow Ambiguity* [25]. It still provides security by hiding the input, output and computation from the server but simultaneously allows fully classical clients. Instead of hiding the input in qubit preparation and the performed computation in a universal cluster, this protocol secures this information by hiding the Pauli matrices that have to be applied during the feed-forward procedure in MBQC to compensate randomly appearing errors caused by measurement outcomes. Performed computations are hidden because different adaptions strategies correspond to different computations [25].

GENERAL NOTATION The computations are based on the MBQC scheme with a N-qubit cluster state $|G\rangle$ as resource, that can be visualized using a graph $G = (V, E)$ (see section 2.2.1). For the qubits that are meant to hold the input information for the circuit and the qubits that carry the final output information of the calculation, we define two sets of qubits $\{I, O\}$ on the graph G. I referes to the input and O to the output set. This procedure defines an *open graph* $G(I, O)$ with $I, O \subseteq V$ and the complement of this sets are given by I^c and O^c. In general these two sets can overlap and since we will only work with MBQC that implements unitary embeddings $|I| = |O| \leq N$. Also denoted by $P(I^c)$ is the power of all the subsets of the elements in I^c and by $\mathrm{Odd}(K)$ the *odd neighborhood* of a set of vertices $K \subseteq V$ is defined.

$$\mathrm{Odd}(K) := \{i : |\mathcal{N}_i \cap K| = 1 \mod 2\} \tag{2.31}$$

In our experiment we will only measure in the (X, Y) plane of the Bloch sphere and the measurement on qubit j is therefore noted as $M_j^{\alpha_j} = \{|\pm\alpha\rangle \langle\pm\alpha|\}$ with $|\pm\alpha\rangle$ defined as in equation (2.29). Furthermore, the description of the resource state, the measurement order and the correction of any errors is summarized in the term *measurement pattern*.

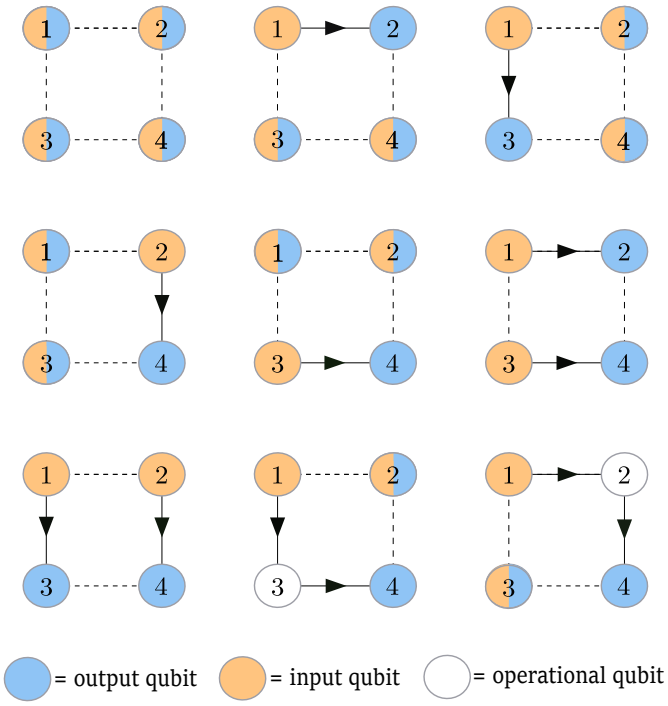


Figure 2.5: Visualisation of the nine possible open graphs $G(I, O)$ for the four qubit Box state given the measurement order according to figure 2.4. The arrows indicate the flow direction of the quantum information. Note also that the input and output sets can overlap.

2.3.1 G-flow

Since, measurements in quantum mechanics are inherently random, errors that occur if a measurement outcome is given by $b_i = 1$, have to be corrected, so that the computation follows the desired positive branch. If that is possible the pattern is known to be uniformly, strongly and stepwise deterministic [55]. In the following we will use *deterministic* to indicate all three attributes.

The strategy that determines how a MBQC measurement pattern can be made deterministic, is given by the *generalized quantum-information flow*, in short *g-flow* [55].

Given a fixed measurement pattern $\prec$ and an open graph $G(I, O)$, a pattern can be made deterministic with a g-flow $(g, \prec)$ that determines in which direction the information flows during the MBQC procedure [55]. In other words, the g-flow determines which qubits will be influenced by which previous measurement outcomes, given a measurement order and input/output set of qubits. Experimentally, this defines the set of Pauli corrections needed to correct upcoming errors caused by previous measurement outcomes. Which measurements will be influenced by an outcome of a measurement on qubit i is given by the *successor function* $g(i)$ that has to fulfil the following conditions.

(G1): if $j \in g(i)$ and $j \neq i$ then $j \succ i$

(G2): if $j \not\succ i$ and $j \neq i$ then $j \notin \mathrm{Odd}(g(i))$

(G3): $i \notin g(i)$ and $i \in \mathrm{Odd}(g(i))$

(G4): if $k \in \mathcal{N}_i \cup \mathcal{N}_j$ and if $k \in g(i)$ then $k \notin g(j)$

The first condition (G1) tells us that if the measurement on qubit j has to be corrected depending on the outcome of i, then measurement i has to be performed before measurement

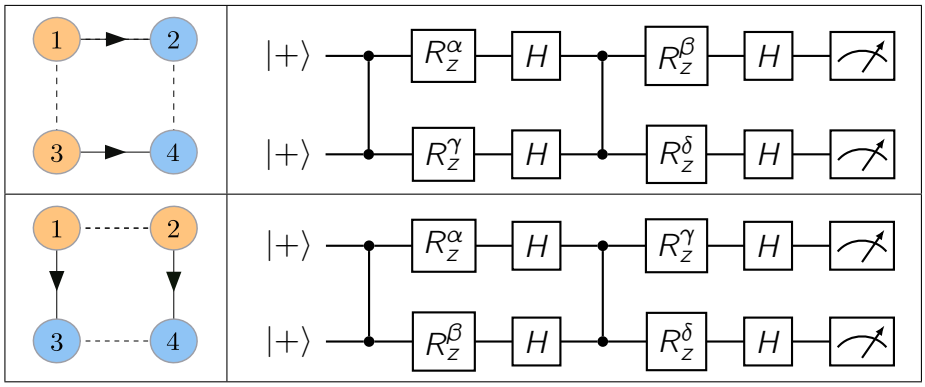


Table 2.3: Example of two different circuits that could be performed on one and the same cluster state. The parameter that makes the difference is the choice of the g-flow that determines the information flow during the processing.

j. Condition (G2) states, that if j is measured before i, but is part of its correction set, then it has to have an even number of connections to i. In that way an even number of Pauli corrections will be applied on j which equals an identity operation and won't change anything. Because also the measurement can't be corrected by its own outcome, i is not part of its own correction set, but has an odd number of connections to $g(i)$ so that the needed corrections are actually performed. This is stated by condition (G3). Last but not least, condition (G4) is not strictly required by *g-flow* but will make the counting of possible open graphs $G(I, O)$ that fulfil the *g-flow* easier.

For the causal order of measurements that is given in figure 2.4 (which will be the fixed order of measurements from now on) the *g-flow* conditions allow only a flow of information from a qubit to stay at the same position, move to the right or to the bottom, but not both at the same time. Additionally, condition (G4) doesn't allow information paths to cross. For the four qubit Box state combined with our fixed measurement order, there are nine possible flows that are visualized in figure 2.5. Since different open graphs with associated g-flows correspond to different quantum computations on the same cluster state, this can be used to provide blindness in MBQC protocols. As an example two different flows are given in table 2.3 together with the circuits they implement.

2.3.2 Classically-driven blind quantum computing

Starting from the situation that the client 'Alice' and all the connections to the quantum server 'Bob' are completely classical, it follows that all inputs and outputs of the quantum computer have to be classical as well. Hence, Alice specifies her computation completely by a classical description $\Delta_{\mathcal{A}}$.

$$\Delta_{\mathcal{A}} = \{\rho_I, U_A, \mathcal{M}\} \tag{2.32}$$

It includes the n-qubit input state ρ_I, the unitary transformation U_A that maps the input state on the output state $\rho_O = U_A \rho_I U_A^\dagger$ and the measurement set $\mathcal{M}$ that extracts the classical information out of the output state ρ_O. This implies that the input state ρ_I of the quantum computation has to be fully describable in a classically way. A possible task that Alice could perform would be the sampling of a probability distribution $\{p_i\}$ of the joint measurement

outcomes given by $\Delta_{\mathcal{A}}$. The blind operation that is performed by the protocol is then given by the map τ.

$$\vec{p} = \{p_i\} = \tau(\Delta_{\mathcal{A}}) := \mathcal{M}(U_A \rho_I U_A^\dagger) \tag{2.33}$$

THE PROTOCOL Alice chooses a graph state $|G\rangle$ and forwards it to Bob, who generates the resource state for the protocol. Additionally, she chooses a g-flow that is represented by a string $\vec{f}$ which includes the *flow control bits* and corresponds to an open graph $G(I, O)$ together with her measurement angles $\vec{\alpha}$ that correspond to the positive branch of the computation she wants to perform. Therefore her quantum circuit is fully specified by $(|G\rangle, \vec{\alpha}, \vec{f})$ and the MBQC pattern is given by

$$\Delta_{\mathcal{A}}^{\mathcal{M}} = (G, \vec{\alpha}, \vec{f}) \tag{2.34}$$

Since Alice may not trust Bob, she hides the measurement outcomes $\vec{b}$ by randomly adding a π shift to the measurement angle every time an entry of a uniformly random generated N-bit string $\vec{r}$ ($r_i \in [0, 1]$) has the value 1. This causes a random flip of the outcomes measured by Bob $\vec{b'}$.

Depending on the outcome b_i, Alice has to update further measurement angles $\vec{\alpha}'$ that she sends to Bob. This adaptations of the measurement angles for qubit j on the previous measurement outcomes $j-1$ (denoted by $\vec{b}_{<j}$) are included in *dependency sets* $\vec{s^x}$ and $\vec{s^z}$. They determine the σ_x and σ_z corrections associated with the measurement angle of each qubit α_j and depend on the measurement outcomes $\vec{b_{<j}}$ as well as the flow bits $\vec{f}$. These sets are uniquely defined for an open graph $G(I, O)$. In order to minimize Bob's knowledge about $\vec{\alpha}$, the domain of $\vec{\alpha}$ is chosen in such a way that the domain of all valid $\vec{\alpha'}$ is the same.

$$\mathcal{A} = \{(-1)^x \theta + z\pi | \theta \in \mathcal{A}, x \in \mathbb{Z}_2, z \in \mathbb{Z}_2\} \tag{2.35}$$

During the interactive part Alice calculates α'_i (see equation (2.37)) at each step i and sends it to Bob. Since for the first measurement there exist no previous measurement outcomes, we choose $s_1^x = s_1^y = 0$ without loss of generality. Bob then measures and sends the outcome b'_i back to Alice, who encodes the result by

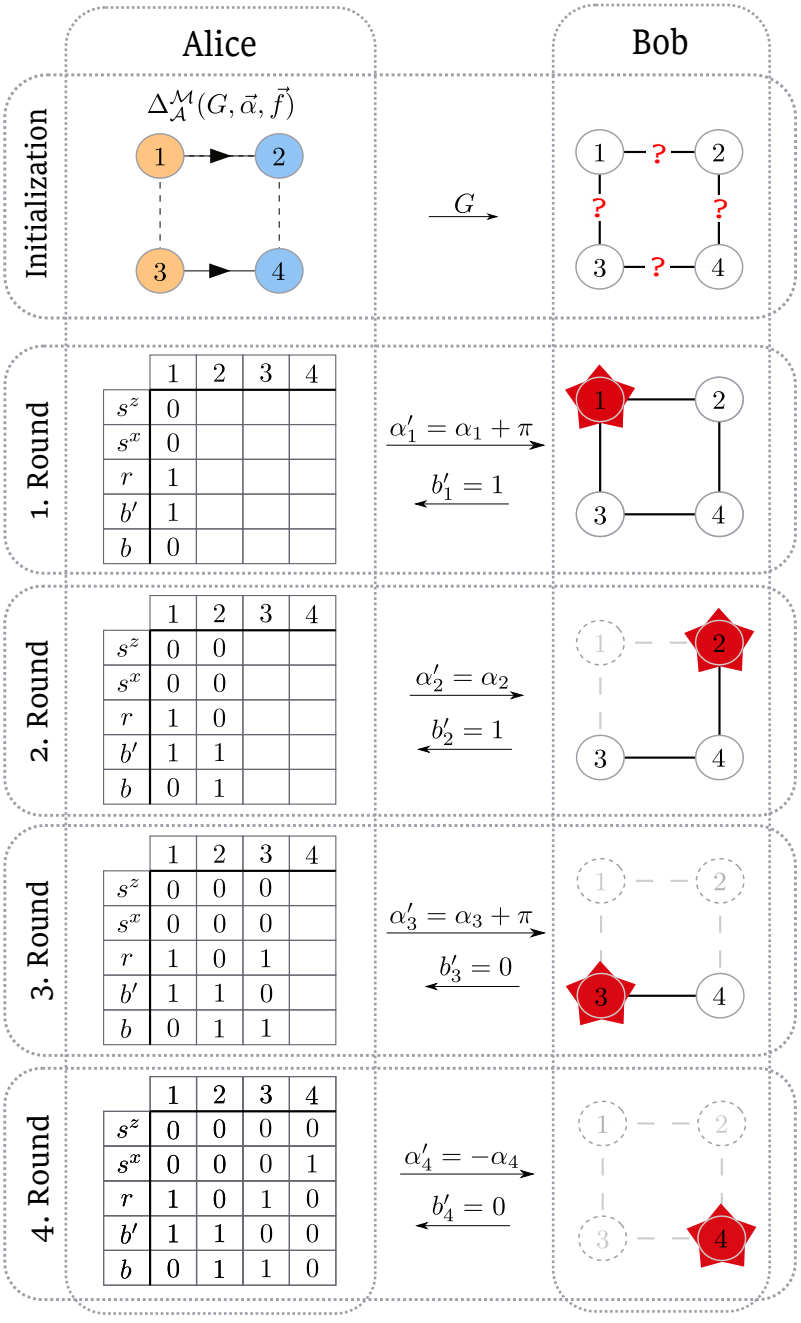
$$\vec{b} = \vec{b'} \oplus \vec{r} \mod 2 \tag{2.36}$$

After that, she updates the dependency sets $\vec{s^x}$ and $\vec{s^y}$ and calculates the future measurement angles α'_j.

$$\vec{\alpha'} = (-1)^{\vec{s^x}} \vec{\alpha} + (\vec{s^z} + \vec{r})\pi \mod 2\pi \tag{2.37}$$

The adapted new measurement angle for the next quibt is again communicated to Bob and the routine starts again. This back and forth is repeated until all the qubits in the cluster state are measured.

Each time that Alice receives a measurement result of a qubit from the output set O, she saves it in a *result* vector $\vec{p_B^C}$. If Bob is honest then $\vec{p_B^C} = \vec{p^C}$, which represents the classical



	1	2	3	4
s^z	0			
s^x	0			
r	1			
b'	1			
b	0			

	1	2	3	4
s^z	0	0		
s^x	0	0		
r	1	0		
b'	1	1		
b	0	1		

	1	2	3	4
s^z	0	0	0	
s^x	0	0	0	
r	1	0	1	
b'	1	1	0	
b	0	1	1	

	1	2	3	4
s^z	0	0	0	0
s^x	0	0	0	1
r	1	0	1	0
b'	1	1	0	0
b	0	1	1	0

Figure 2.6: Visualisation of an example run of the *Flow Ambiguity* protocol. In the beginning, Alice chooses the graph G, a g-flow $\vec{f}$ for the desired computation and the corresponding measurement angles $\vec{\alpha}$. Only the desired state is shared with Bob. Information proceeding is performed in the following way. Alice calculates dependency sets $\vec{s^x}$ and $\vec{s^z}$ dependent on previous measurement outcomes and $\vec{f}$. Additionally generates a random number r_i. With this values she determines α'_i via equation (2.37), that she afterwards communicates to Bob. He performs the measurement at the given angle and returns the outcome b'_i back to Alice. By using $b_i = b'_i \oplus r_i \bmod 2$ she calculates the real outcome according to α_i. After this, the steps repeat themselves until all the qubits are measured. In the end Bob only has access to $(|G\rangle, \vec{\alpha'}, \vec{b'})$ and he can always find an $\vec{\alpha}$ for any possible g-flow $\vec{f}$ according to the information that he has recorded. This ambiguity in possible flows is what hinders Bob of knowing the computation Alice has performed.

result of the computation up to classical post-processing. The final result is then calculated by $\vec{p} = \vec{p^C} \otimes \vec{s_O^Z}$, where the post-processing given by σ_z corrections applied on the output qubits is represented by $\vec{s_O^Z}$.

The protocol is summarized in table 2.4 and was directly taken from [25]. Also an example run of the protocol is given in figure 2.6 for better understanding.

2.3.3 Blindness Analysis

Let us assume a cheating Bob, that can follow any strategy allowed by the laws of physics and has access to unlimited computational power. How much information would he gain about the performed computation in one run of the protocol? Since he has no access to the uniformly random variable $\vec{r}$ he has no knowledge about the real output $\vec{b}$. Let us say he knows equation (2.37), the measurement angles $\vec{\alpha}$ are nevertheless unfamiliar to him because he is missing the information of the random bit flip $\vec{r}$ and the the flow control bits $\vec{f}$. Hence also the input is hidden.

Finally the computation itself. The first intuition would be that he knows the performed quantum circuit, since he knows the graph state $|G\rangle$ together with the measurement order. But even with that information he is missing the choice of open graph $G(I, O)$ with the corresponding g-flow, that defines the performed computation. In fact, different choices of g-flow result in different quantum circuits and this flow ambiguity is what hides the input information and the performed computational task from Bob. To summarize, in the end Bob only knows the set $(|G\rangle, \vec{\alpha'}, \vec{b'})$.

To fully describe the performed computation $\Delta_{\mathcal{A}}^{\mathcal{M}}$, Bob would need n_a bits to describe the chosen angles and n_f bits to determine the used flow, makes in total $n_a + n_f$ bits [25]. After one round he knows only $(|G\rangle, \vec{\alpha'}, \vec{b'})$, which equals in the best case for Bob n_a bits. Therefore, the number of hidden bits from Bob is given by n_f. This is enough to hinder Bob from knowing the computation that is performed by Alice.

A minimal choice of angles which can not be simulated in a classical way (via the Gottesmann-Knill theorem [57]) is given by the following set.

$$\mathcal{A} = \left\{ \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4} \right\} \tag{2.38}$$

For this special situation that we will also use in our experiment, Bob gets at most two bits of information during each measurement he applies on a qubit. So in total he has access to $2N$ bits, where N is the number of measured qubits. For our implementation with a four photon cluster state that would be then in total 8 bits of information.

PROTOCOL PARAMETERS:

- A graph G with an implicit total ordering of vertices
- A set of angles $\mathcal{A}$ satisfying equation (2.35).

ALICE'S INPUT:

- A target computation $\Delta_{\mathcal{A}}$ implemented using MBQC as

$$\Delta_{\mathcal{A}}^{\mathcal{M}} = \{G, \vec{\alpha}, \vec{f}\} \tag{2.39}$$

representing a measurement pattern on G compatible with the total ordering of measurements implicit in G, which describes a unitary embedding U_A. The set $\vec{\alpha}$ represents a sequence of N measurement angles over the graph G, with each angle chosen from a set $\mathcal{A}$, which is also taken to be a parameter of the protocol and is known to both parties. The g-flow construction fully determines the input state ρ_I, through the location of the input and output qubit sets on the graph (I and O, respectively) and the dependency sets $(s^x; s^z)$

STEPS OF THE PROTOCOL:

1. **State preparation**
   (a) Bob prepares the graph state $|G\rangle$
2. **Measurements**
   For $i = 1, ..., N$, repeat the following:
   (a) Alice picks a binary digit $r_i \in \mathbb{Z}_2$ uniformly at random.
   Then, using r_i, s^x, s^z and the function in equation (2.37), she computes the angle α'_i

$$\vec{\alpha'} = (-1)^{\vec{s^x}}\vec{\alpha} + (\vec{s^z} + \vec{r})\pi \mod 2\pi$$

   and transmits α'_i to Bob.

   (b) Bob measures the ith qubit in the basis $\{|\pm\alpha'_i\rangle\}$ and transmits to Alice the measurement outcome $b'_i \in \mathbb{Z}_2$.

   (c) Alice records $b_i = b'_i \oplus r_i \mod 2$ in $\vec{b}$ and then updates the dependency sets $(\vec{s^x}; \vec{s^z})$. If $i \in O$, then she also records b_i in $\vec{p}_B^C$.
3. **Post-processing of the output**
   (a) Alice implements the final round of corrections to the output string by calculating $\vec{p} = \vec{p}_B^C \otimes \vec{s}_O^Z$, with $\vec{s}_O^Z$ the set of σ_z corrections on the output at the end of the protocol.

Table 2.4.: Short summery of the classically-driven blind quantum computation protocol as given in [25].

3 EXPERIMENTAL REALIZATION

During the last year we were working on the implementation of a classically-driven measurement based blind quantum computer (CDBQC) relying on photons as qubits. The underlying protocol of this CDBQC was first described 2017 by Mantri *et. all.* [25]. It consists of a single-photon source, the resource state preparation as well as a setup to implement measurements in the bases given by the classical client. A basic sketch of the implemented protocol is given in figure 3.1.

To improve the performance of such a protocol and MBQC setups in general, we are preparing to replace our Poisson distributed spontaneous parametric down conversion single-photon source by a almost deterministic one, based on QDs. Therefore I already built a polarization suppression setup that separates photons of the pump beam from single photons generated by the QD single-photon source in a resonant pumping scheme based on their polarization. In combination with the new sources, this separation setup will improve future MBQC protocols and applications in quantum information and quantum cryptography immensely.

3.1 PHOTONS FOR QUANTUM COMPUTING

According to DiVicenzo in 2000 [58], a system for universal quantum computing needs to fulfil five requirements. First of all, it has to be scalable with well characterized qubits and we should be able to initialise and controlled them. Additionally, the qubits should exhibit a long coherence time, stretching way over the gate operation time, so that the needed gates can be performed. For the universality of the computation, a universal set of quantum gates is needed. This is given by single-qubit rotations and either a CNOT or CZ gate. Finally the last requirement asks for a qubit-specific measurement capability for read out.

A good candidate for quantum computing, fulfilling all the requirements, are photons. They are elementary particles without mass that carry an energy of $E = \hbar\omega$, where ω refers to the angular frequency and $\hbar$ to Planck's constant. They are the quanta of the electromagnetic field and fully specified by their polarisation, frequency and orbital angular momentum. A

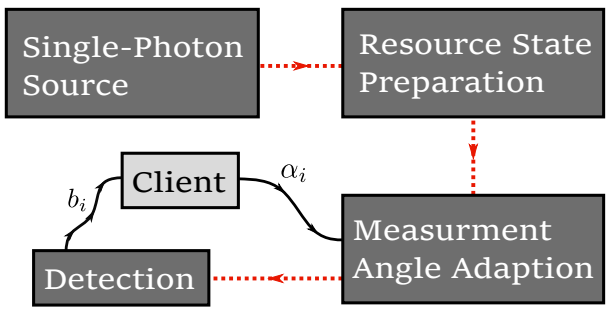


Figure 3.1: Sketch of the implemented CDBQC protocol. Single-photon pairs are generated by SPDC sources and sent to the resource state preparation that consists out of a CZ gate and unitary operations. For the protocol performance a classical client sends measurement angles α_i to the quantum computer, which adapts these angles and measures the qubits after each other. Each measurement result i is sent to the client.

specialty of photons is their hardly present decoherence, due to their lack of interaction with each other or their environment. But this advantage comes with a challenge, since computations rely on single- and two-qubit gates. In later ones the photons have to interact with each other. In order to achieve this with photons, optical nonlinearities are needed [59]. A solution for that was found in the photon based KLM scheme [47], where they use linear optics and introduce nonlinearities in form of measurements. Still, their architecture is non-deterministic, but they were able to increase the success probability by using ancilla photons. But reaching the level where the error gets smaller than the fault-tolerant threshold would require a huge number of ancilla photons. Instead of decreasing the probabilistic tasks, the MBQC scheme moves them out of the computational task into the state preparation. Further development of MBQC resulted in protocols offering more security and blindness [18].

QUANTUM STATES OF LIGHT AND THEIR EVOLUTION In the second quantization of the electromagnetic field, light is represented by a Hamiltonian $\hat{H}$ that describes an ensemble of harmonic oscillators, which represent the different modes of the electromagnetic field.

$$\hat{H} = \sum_k \hat{H}_k \qquad \text{with} \qquad \hat{H}_k = \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right) \tag{3.1}$$

In these equations ω_k denotes to the angular frequency of a photon in mode k and $\hat{a}_k$ and $\hat{a}_k^\dagger$ are the annihilation and creation operators respectively. A mode of a photon can describe anything from spatial modes to spectral modes over polarisation to time modes. It is also useful to define so-called quadrature operators $\hat{X} = 1/2 \left(\hat{a} + \hat{a}^\dagger \right)$ and $\hat{Y} = 1/2i \left(\hat{a} - \hat{a}^\dagger \right)$ that are associated with field amplitudes oscillating out of phase with each other by 90°. They are not commuting and fulfil the uncertainty relation $\Delta\hat{X}\Delta\hat{Y} \geq 1/4$. Since photons are bosons, many of them can be simultaneously in the same state, where they are *indistinguishable*. In difference to fermions, they have an integer spin and follow Bose-Einstein statistics.

$$[\hat{a}_k, \hat{a}_l] = [\hat{a}_k^\dagger, \hat{a}_l^\dagger] = 0 \qquad\qquad [\hat{a}_k, \hat{a}_l^\dagger] = \delta_{kl} \tag{3.2}$$

Not all states of quantum light are the same. Light that is emitted by a laser for example is approximated by coherent light, which is an eigenstate of the annihilation operator, $\hat{a}_k |\alpha\rangle_l = \alpha |\alpha\rangle_k$, where α is a complex number that represents the *displacement*. It has a minimal uncertainty of $1/4$ where both quadratures operators have the same fluctuation of $1/2$. As the coherent state has a higher resemblance to the dynamics of classical harmonic oscillators, it is often also called classical light [1]. In comparison, there also exist squeezed states, where the minimal uncertainty is also given by $1/4$, but one of the quadrature fluctuation is below the vacuum noise level of $1/2$. Both the coherent and the squeezed states have undefined photon numbers. The only states with a well defined photon number are the Fock states $|n\rangle_k$ which represents single photons, where n gives the number of photons in mode k. Fock states fulfil following relations

$$\hat{a}_k^\dagger |n\rangle_k = \sqrt{n+1}\,|n+1\rangle\,, \qquad \hat{a}_k |n\rangle_k = \sqrt{n}\,|n-1\rangle\,, \qquad \hat{N}_k = \hat{a}_k^\dagger \hat{a}_k \tag{3.3}$$

in which $\hat{N}_k$ represents the number operator that gives the number of photons in mode k.

Dynamics of light that doesn't interact with any matter, is defined by *Bogoliubov transformations*, which are linear transformations of the mode operators. In the case of Gaussian unitaries, it can be described by a Hamiltonian of the form

$$\hat{H} = \underbrace{\sum_{k=1}^{m} \alpha_k \hat{a}_k^\dagger + h.c.}_{\text{Displacement}} + \underbrace{\sum_{k,l=1}^{m} \eta_{kl} \hat{a}_k^\dagger \hat{a}_l^\dagger + h.c.}_{\text{Squeezing}} + \underbrace{\sum_{k\geq l=1}^{m} \mu_{kl} \hat{a}_k^\dagger \hat{a}_l + h.c.}_{\text{Linear optics}} \tag{3.4}$$

were $h.c.$ gives the hermitian conjugate. The first two terms describe an evolution that displaces or squeezes the electromagnetic field in the given mode, while the third term, denoted by H_3 describes transformations caused by linear optics that make most parts of our experiment. For this linear optic evolution's we denote a unitary map $\mathcal{U} = \exp(-i\hat{H}_3 t)$ that alters the operators for all modes $\hat{\mathbf{a}}^\dagger = \left(\hat{a}_1^\dagger, ..., \hat{a}_m^\dagger\right)$ and is given in the Heisenberg picture by the unitary $m \times m$ matrix $U = \exp(-i\mu t)$ for which μ is the Hermitian matrix given in the third term of equation (3.4) with the matrix elements μ_{kl}.

$$\hat{\mathbf{a}}^\dagger \to \mathcal{U}\hat{\mathbf{a}}^\dagger\mathcal{U}^\dagger = U^\intercal \hat{\mathbf{a}}^\dagger \tag{3.5}$$

The unitary property of the evolution matrices is due to the fact that the energy is preserved during the linear optic processes. When we have a look at a transformation from a single photon prepared in mode i, then the probability of detecting this photon after the transformation in mode j is given by $\left|U_{ji}\right|^2$. For further understanding have a look in the appendix.

Building any linear transformation only needs two main operations. *Phase shifters* $U_{PS}(\phi)$, that applies a phase of ϕ on the second mode and *beam-splitters* (BS) $U_{BS}(\eta)$ with a reflectivity given by η.

$$U_{PS}(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \qquad U_{BS}(\eta) = \begin{pmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{pmatrix} \tag{3.6}$$

Since linear optic unitary transformations map coherent states onto other coherent states with amplitudes $\mathcal{U}|\alpha\rangle = |U\alpha\rangle$, the output amplitude in mode j, if light was initiated in mode i is given similar to the single-photon case with a rescaling factor of $\left|U_{ji}\right|^2$ [60]. Therefore a classical coherent state behaves in the same way as a single-photon state in a linear optical setup. This is not true for more than one photon, because we have to take second-order interference effects into account. [1, 60]

INTERFERENCE A simple case, were quantum interference can be observed is given already with a 50/50 BS, described by the matrix $U_{50/50} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, which is equivalent to the representation of a BS given in equation (3.6). Let us assume that photons are entering the BS from different input ports. For classical, not interfering light, each photon has a 50% probability of being reflected or transmitted, resulting in four possible scenarios for the photons to leave the BS. Those are visualized in figure 3.2. Either both reflected or both transmitted, so that they leave in different ports, or one is reflected while the other one is transmitted, letting them leave in the same port. The measurement after the BS is based on

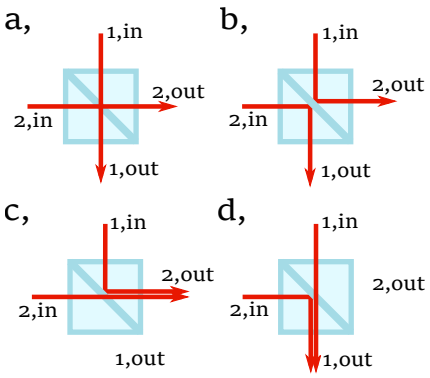


Figure 3.2: Four possible cases for two distinguishable photons leaving a 50/50 beam splitter while entering from two different input ports. Either both leave from different ports **a,** and **b,** or they leave in the same port **c,** and **d,**. In the case of indistiguishable photons, the uper two cases interfere destructively and the photons will always leave the BS in the same port.

coincidence clicks (CCs) between two detectors, where each of them is placed in one output arm of the BS. A CCs event is detected if both the detectors recognise a photon during a previous defined time interval called *coincidence window*. For the non-interacting classical particles, CCs are measured in half of the cases.

For the quantum scenario, two single photons enter the same BS again from two different ports represented by $\hat{a}_1^\dagger |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\hat{b}_2^\dagger |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Written down in a mathematical way it is given as following

$$U_{50/50}\hat{a}_{1,in}^\dagger \hat{b}_{2,in}^\dagger |0\rangle = \frac{1}{2}\left(\hat{a}_{1,out}^\dagger + \hat{a}_{2,out}^\dagger\right)\left(\hat{b}_{1,out}^\dagger - \hat{b}_{2,out}^\dagger\right)|0\rangle \tag{3.7}$$

$$= \frac{1}{2}\left(\hat{a}_{1,out}^\dagger \hat{b}_{1,out}^\dagger - \hat{a}_{1,out}^\dagger \hat{b}_{2,out}^\dagger + \hat{a}_{2,out}^\dagger \hat{b}_{1,out}^\dagger - \hat{a}_{2,out}^\dagger \hat{b}_{2,out}^\dagger\right)|0\rangle \tag{3.8}$$

where $|0\rangle$ represents the vaccum state.

For the case of indistinguishable photons, the two terms in the middle of equation (3.2), interfere destructively. This results in the phenomenon, that the photons will always leave the BS together in the same port. The state after the BS is therefore given in the Fock basis by

$$\frac{1}{\sqrt{2}}\left(|2\rangle|0\rangle - |0\rangle|2\rangle\right) \tag{3.9}$$

where the numbering of the vectors is omitted and the first vector always refers to the first spatial mode. This is called *photon bunching* and was first described by Hong, Ou and Mandel 1987 [61] which also gave the name *HOM effect*. For the effect to occur, the photons have to arrive at the BS at the same time, otherwise they would be distinguishable in time. To achieve that in an experimental setup we have to be able to tune the relative delay between the photons. For the photons that are not overlapping in time, CCs will be measured similar to the classical situation. Getting closer to the zero delay point, CCs decrease until they drop (in an ideal case) to zero, where the photons are truly indistinguishable. Continuing the delay scan will let the CCs rise again. The appearing decrease and increase in CCs depending on the delay is called *HOM-dip* (see figure 3.13).

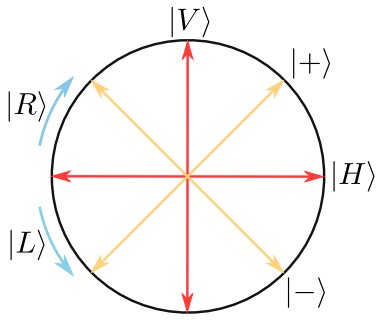


Figure 3.3: Visualization of the electric field vector of vertical $|V\rangle$, horizontal $|H\rangle$, diagonal $|+\rangle$ and anti-diagonal $|-\rangle$ linear polarized light. Additional also right $|R\rangle$ and left $|L\rangle$ circular light is given.

PHOTONS AS QUBITS That photons are good candidates for realizing qubits was already discussed in the beginning of this chapter. But there are many possible ways of encoding them. Encoding can be based on the path, the time or as in our experiment on the polarization. Polarization describes the direction of the electric field of an electromagnetic wave [36] and was chosen as our encoding method due to low decoherence and the easy control of the qubits, since it is very easy to implement single qubit gates in this encoding. If it points constantly in one direction, it is called *linear*. For the case that the polarization rotates while the wave is propagating and draws a circle during one cycle of the wave it is called *circuarly polarized*. If the circle is drawn clockwise/anticlockwise for an observer that looks towards the light source, it is referred to as *right circular*/*left circular* ($|R\rangle$/$|L\rangle$). Is the drawing an ellipse or the polarization is random, it is called elliptical polarized or unpolarized, respectively.

Polarization encoding is realized by using horizontal $|H\rangle$ and vertical linear polarized light $|V\rangle$ as computational basis states $|0\rangle$ and $|1\rangle$. Similarly to the Bloch-sphere, a polarization encoded qubit is presented by a point on the *Poincare sphere*, where the z-axis points towards the computational basis $|H\rangle$ and $|V\rangle$, the x-axis towards the diagonal basis $|+/-\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ and the y-axis towards the circular states $|R/L\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i\,|L\rangle)$.

PHOTONIC GATES For polarization encoded qubits, single-qubit gates are realized by waveplates. These are made out of birefringe material for which the refractive index is dependent on the polarization and propagation direction of the passing photons. Inside the material light splits up into two components that travel, dependent on the refractive index, with different speed and recombine while leaving the material. The phase added between the two components of the wave varies due to the thickness of the material. For a *half-wave plate* (HWP) plate the phase added between the polarization components equals π or half a wavelength, therefore, linear polarization will be rotated to another linear polarization. If a phase equal $\pi/2$ or an odd number of quarter-wavelengths is added one speaks of a *quater-wave plate* (QWP). It can transform linearly polarized waves into circularly polarized waves and vice-versa. The matrix representation of these wave-plates is given by

$$U_{HWP} = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix} \tag{3.10}$$

$$U_{QWP} = \begin{pmatrix} \cos(\theta)^2 + i\sin(\theta)^2 & (1-i)\cos(\theta)\sin(\theta) \\ (1-i)\cos(\theta)\sin(\theta) & \sin(\theta)^2 + i\cos(\theta)^2 \end{pmatrix} \tag{3.11}$$

Basis	θ_{QWP}	θ_{HWP}
$\|H/V\rangle$	0°	0°
$\|+/-\rangle$	45°	22.5°
$\|R/L\rangle$	0°	22.5°

Table 3.1.: Setting for the QWP angle θ_{QWP} and the HWP angle θ_{HWP} to perform measurements in the different polarization bases.

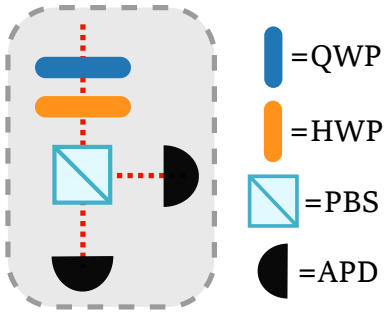


Figure 3.4.: Setup of polarization analyzing detection stage consisting out of a PBS and an APD in each output path. A QWP combined with a HWP opens the possibility to switch between the measurement bases between $|H/V\rangle$, $|+/-\rangle$ and $|R/L\rangle$.

where θ defines the angle between the horizontal axis and the fast axis of the wave plate [62]. Any arbitrary rotation can be performed by the sequence QWP-HWP-QWP [43], which results in a universal single-qubit gate set for polarization encoded qubits.

Multi-photon gates need photons to interact with each other in order to work and there have been many different approaches to realize such gates [44]. The CZ gate in our experiment is based on polarization-dependent beam-splitters (PDBSs) and second-order interference between indistinguishable photons similar to the HOM-experiment and was implemented already 2005 by Kiesel *et.al.* [63]. This specific gate will be explained in more detail in the implementation.

DETECTION So far we focused on characteristics of photons as well as how they are manipulated if they are used as polarization encoded qubits. But in the end of each protocol the qubits have to be read out, which happens by measuring them. There are many ways to detect photons, but in our experiment we detect single photons by using avalanche photodiodes (APDs). In those, each photon generates a charge by a photoelectric effect that acquires sufficient energy in the large electric field of a junction region in the APD to generate new carriers by impact ionization, which results in a cascade of moving carriers [62]. In this way single photons are generating a current, large enough to be readily detected by the electronics in the device. This kind of detection tells if a photon was detected or not, but gives no further information of any other property. Polarization measurements can be achieved by adding a polarizing beam splitter (PBS), that transmits horizontally polarized photons while it reflects vertically polarized photons. Measurements in the polarization bases $|H/V\rangle$, $|+/-\rangle$ and $|R/L\rangle$, can be realized by combining a QWP and a HWP together with a PBS and placing an APD in each of the optical paths after the PBS. The polarization analyzing setup is given in figure 3.4. The QWP and HWP are set for the different bases in such a way that they the state to be measured to $|H\rangle$. The angle settings for the bases $|H/V\rangle$, $|+/-\rangle$ and $|R/L\rangle$ are written down in table 3.1. See the appendix for a short explanatory example.

In order to identify the density matrix of a system, several measurements on a set of identically prepared states have to be performed. This procedure builds the basis of *quantum state tomography* [64]. Thereby the *Stokes parameter* of the photons are determined by performing measurements in different polarization bases. The number of measurements grows with 3^n, where n is the number of qubits in the to be measured state [42].

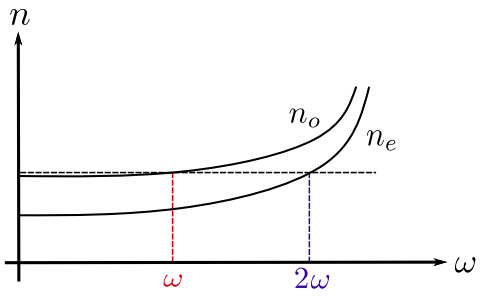


Figure 3.5: Frequency dependent refractive index of a negative uniaxial crystal were $n_e < n_o$. For a positive uniaxial crystal the extraordinary index would be greater than the ordinary. Additionally, the phase matching situation for a second harmonic generation process with the phase matching condition $n_e(2\omega) = n_o(\omega)$ is given. The picture was taken from [65].

3.2 SINGLE-PHOTON SOURCES

An ideal single-photon source, as described in [30], should provide pulses of light as efficiently as possible, where the pulses should contain only one photon each. All these single photons should be indistinguishable and in a pure quantum state. The *single-photon purity* can be characterized by using the second-order correlation function $g^{(2)}$, that measures coincidences after the generated pulses pass a 50/50 BS. Laser light has a value of $g^{(2)}(0) = 1$ whereas an ideal single-photon would exhibit $g^{(2)}(0) = 0$. *Indistinguishability* can be verified by HOM interference on a 50/50 BS combined with an unbalanzed Mach–Zehnder interferometer. An additional important property to characterize single-photon sources is given by the *brightness*, that gives the probability that a pump pulse contains photons and not only vacuum components $|0\rangle$. For an ideal single-photon source the brightness would be given by $B = 1$ as the visibility of the HOM-dip $\mathcal{V}_{HOM} = 1$.

For many quantum cryptography, quantum key distribution and quantum computing protocols, as well as in this experiment, a spontaneous parametric down-conversion (SPDC) single-photon source is used to provide entangled single-photon pairs [26].

3.2.1 Spontaneous parametric down-conversion

In an SPDC source an input pump field in a nonlinear crystal stimulates the vacuum field of two other electromagnetic fields called *signal* and *idler* [26, 29]. During the process a pump photon is spontaneously down-converted into two photons. In comparison to optical parametric generators (OPG) or optical parametric oscillators (OPO), the pump power is fare below the OPO threshold, so that single photons are generated. On the other hand, the pump power is so low that the probability, that a photon is down converted is very small, which makes the source probabilistic.

During the process the three photons have to conserve energy $\omega_p = \omega_s + \omega_i$ as well as momentum $\vec{k}_p = \vec{k}_s + \vec{k}_i$. Energy conservation can always be achieved, but the momentum conservation demands more effort to be fulfilled, since the wave vector $\vec{k} = \frac{2\pi\vec{n}}{\lambda}$ does not only depend on the wavelength λ but also on the refractive index of the medium $\vec{n}$, which is given by the orientation of the medium, the polarization, the wavelength and the propagation direction of the electromagnetic wave. If the momentum conservation is satisfied the polarization and the electric field are in phase (phase matched) and energy flows from the pump field to the vacuum field of signal and idler [26, 65].

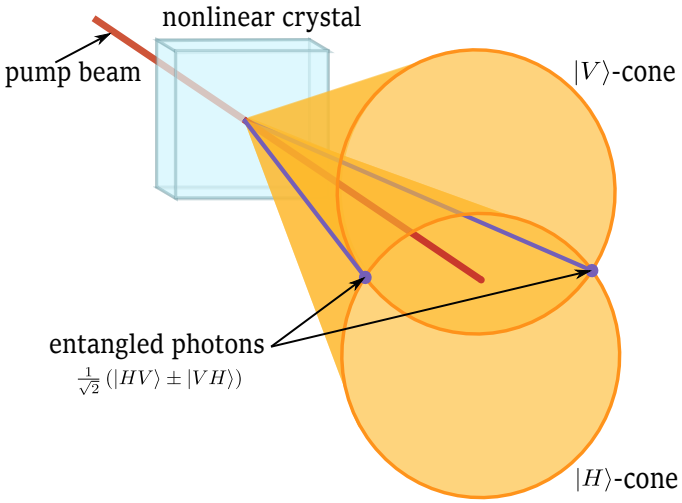


Figure 3.6: For a non-collinear type-II phase matched crystal the SPDC source emits two photons with orthogonal polarization along two distinct cones. Collecting single photons from the intersection points of the cones gives polarization entangled photons, due to the missing information that tells which collected photon comes from which cone. Momentum conservation ensures that for each collected photon in one overlapping point there is also the other generated photon from the other cone collected in the other intersection point.

Phase matching can be achieved by using birefringent materials, where $\vec{n}$ also depends on the polarisation and direction of propagation of an electromagnetic field passing through the medium. For birefringent materials there exist refractive indices n_x, n_y, n_z along the principal axis, were at least two of the refractive indices are different. An unpolarized plane wave traveling through the medium along one of the principal planes, for example along the the z-axis, will experience two refractive indices n_x and n_y. In uniaxial material, there exist a single direction, called optical axis, in which unpolarized light doesn't experience birefringe. As an example, let us assume this optical axis is along the z-axis with $n_z = n_o$, then this would mean that for this direction $n_x = n_y = n_e$. *Ordinary waves* (o-waves) waves, that are polarized perpendicular to the plane spanned by $\vec{k}$ and the optical axes, will experience an ordinary refractive index n_o, that is independent of the propagation direction of the o-wave. Instead, *extraordinary waves* (e-waves), that have electric field vectors in the plane containing the k-vector and the optical axes, will experience $n_e(\theta)$, depending on the angle θ between the optical axis and $\vec{k}$. These properties of birefringent media can be used to achieving phase matching. To see that we rewrite the momentum conservation in terms of refractive indices.

$$n_1\omega_1 = n_2\omega_2 + n_3\omega_3 \tag{3.12}$$

Then different combinations of polarisation are used to let $\vec{k}_p$ shrink while $\vec{k}_s$ and $\vec{k}_i$ are stretched, which is realized by choosing the polarization of the pump beam in the direction of the lower refractive index [26, 65]. This depends then on whether the nonlinear crystal is positive ($n_e > n_o$) or negative ($n_e < n_o$) uniaxial. Two different types of phase matching for birefringent materials are possible. Type-I, where the generated photons have the same polarization perpendicular to the polarization of the pump photon, and type-II, for which the signal and idler have perpendicular polarization.

Type-I:	o	$\longrightarrow$	$e+e$			positive uniaxial
	e	$\longrightarrow$	$o+o$			negative uniaxial
Type-II:	o	$\longrightarrow$	$o+e$	or	$e+o$	positive uniaxial
	e	$\longrightarrow$	$e+o$	or	$o+e$	negative uniaxial

Birefringent phase matching can be achieved by controlling the orientation of the nonlinear crystal relative to the propagation direction of the pump light so that θ is set in such a way that the phase matching condition (3.12) is fulfilled [65]. For second-harmonic generation, which is the inverse process of SPDC, the phase-matching condition would be given by $n_e(2\omega) = n_o(\omega)$ and phase matching can be realized as shown in firgure 3.5.
Similar to that, also phase matching for a negative uniaxial crystal type-II and an SPDC process generating two photons with the same wavelength $\omega_2 = \omega_3$ and $\omega_1 = 2\omega_2$, as it will be the case in our experiment, will be achieved by fulfilling the phase matching condition:

$$2n_e(2\omega_2, \theta) = n_e(\omega_2) + n_o(\omega_2) \tag{3.13}$$

For the type-II phase matching, signal and idler fields are generated along two different cones, one for the e-wave and one for the o-wave. According to the momentum conservation the photons are always emitted into complementary directions. Collecting single photons at the overlapping points of the two cones gives no information from which cone the collected photons are coming from (see figure 3.6). Due to momentum conservation, for each collected photon in one overlapping point the second generated photon from the other cone is collected in the other overlapping point. Therefor, collecting photons at the overlapping points gives $|\psi^{\pm}\rangle$ Bell states.

$$\frac{1}{\sqrt{2}} \left(|HV\rangle \pm |VH\rangle \right) \tag{3.14}$$

The probability of generating single-photon pairs scales in the low pump power regime, linear with the pump power P, while it scales for n-photon emission with P^n. Therefore, increasing the pump power boosts the probability of multi-photon generation, which leads to a growth of the second-order-correlation function $g^{(2)}(0)$ and a decrease of the HOM-dip visibility $\mathcal{V}_{HOM}$ [30]. In order to prevent such multi photon events, the probability of generating a single-photon pair per pump pulse is kept typically under 0.1 [31].

3.2.2 Quantum Dots

Instead of the nondeterministic SPDC sources discussed above, one can use quantum dots (QDs) as nearly deterministic single-photon sources, where each excitation will generate one photon on demand. This can be achieved with $g^{(2)}(0) < 0.01$, high efficiency and photon indistinguishablity of up to 97% [30, 33].

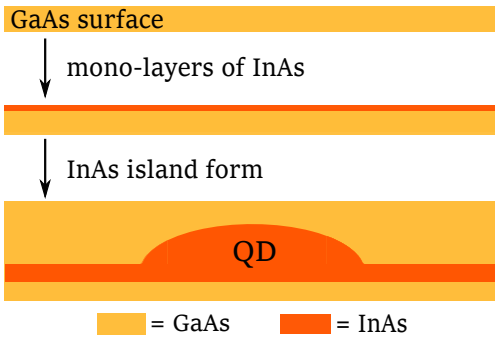


Figure 3.7.: Sketch of a self-assembling epitaxy growth process of a QD. On a GaAs surface, mono-layers of InAS are placed layer by layer. Because of the lattice-constant mismatch between GaAs and InAs, after some layers the strain energy in the InAs layer become so big that small islands form. This islands give the actual QD.

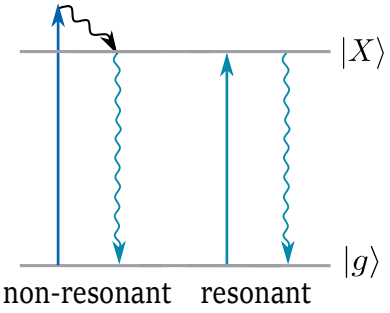


Figure 3.8.: Resonant and non-resonant pumping schemes for exciting a quantum dot to its exiton state.

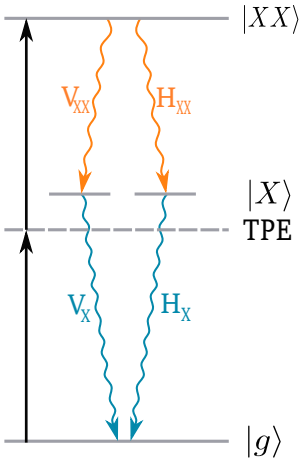


Figure 3.9.: Energy levels of a QD with the visualization of TPE over a virtual level to excite the QD into the biexiton state $|XX\rangle$. From there two different decay processes are possible over different exiton states $|X\rangle$, generating the polarization entangled state $\frac{1}{\sqrt{2}}(|H_{XX}H_X\rangle + |V_{XX}V_X\rangle)$.

Quantum dots are small nano-structures that can be approximated theoretical by potential wells that have discrete energy levels for electrons and holes due to strong quantum confinement. Many different processes can be used to generate such QDs, but we focus now on self-assembled epitaxial QDs to get an idea of how these QDs can be grown. A small sketch of this growth process is given in figure 3.7. Self-assembled epitaxial growth uses two semiconductor materials with a small lattice-constant mismatch as given for example for InAs and GaAs. Placing atomic mono-layers of InAs on a GaAs surface, forms a planar layer (wetting layer) after 1.7 mono-layers. By continuously adding InAs layers, the strain energy grows, which results in InAs forming small islands to minimize the total energy. These small islands give the actual QDs. Single photons are created by exciting an electron of a QD into an excited state, from which it decays back to its ground state by emitting a single photon. The advantage compared to SPDC sources is that the brightness of QDs is largely independent of single-photon purity, since each excitation provides only one decay process.

Single photons can be generated on demand by driving only one transition. It is possible not only to excite exciton states $|X\rangle$, with one electron and one hole, but also biexciton state $|XX\rangle$ consisting of two electrons and two holes. Combining that with Pauli exclusions results in a manifold of ground states so that there are different possible decays from $|XX\rangle$ to the ground state $|g\rangle$ over different exiton states $|X\rangle$ (see figure 3.9). Due to strong Coulomb interaction between the carriers the wavelength of the two cascades $|XX\rangle \rightarrow |X\rangle$ and $|X\rangle \rightarrow |g\rangle$ differ by a couple of nano-meters. This small shift in the wavelengths allows one transition to be filtered out and therefore have a single-photon source. Collecting all photons of the transition from $|XX\rangle$ to $|g\rangle$ over one of two bright $|X\rangle$ states offers the opportunity of generating polarization entangled photon pairs [32, 33] or even hyperentanglement [34].

Excitation to a higher energy level can be realized by different pumping schemes. If the QD is exited non-resonantly with higher frequency, which for example pumps the GaAs bulk or the wetting layer, the carriers diffuse through carrier collisions and phonon emissions to the exciton state. From there it decays back to the ground state by emitting a photon in a different wavelength than the pump photons. Therefore, the excitation beam can be easily separated from the generated single-photons due to their different frequencies. See figure 3.8. Same procedure can be done for the biexiton state. Higher indistinguishability can be obtained by direct resonant pumping of the $|X\rangle$ or resonant pumping via two-photon excitation (TPE) processes to the $|XX\rangle$ state. Since the three wavelengths differ for the TPE pumping scheme,

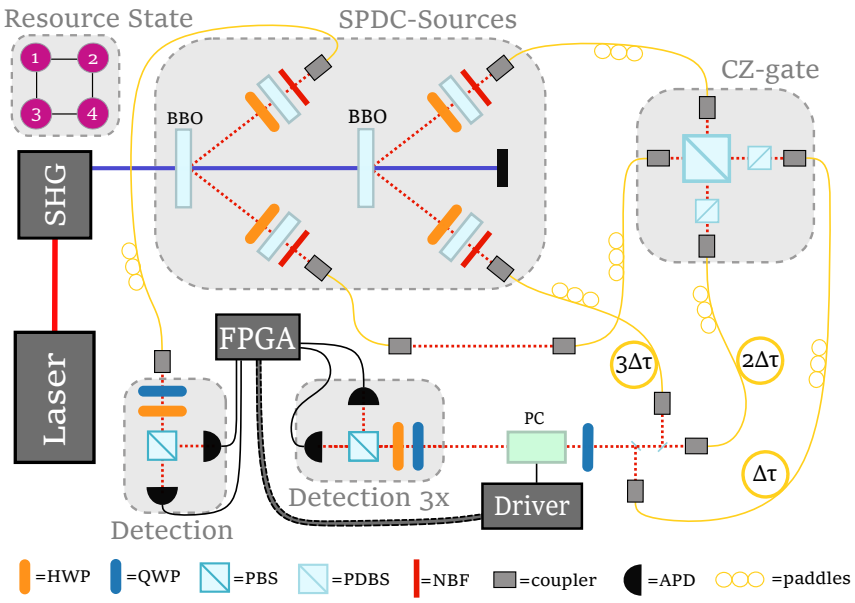


Figure 3.10.: Flow Ambiguity Implementation: Two SPDC sources generate entangled photon pairs which are then used to create a four-photon cluster state (resource state) using a CZ gate. After that the protocol is performed by measuring the qubits of the resource state based on a feed forward procedure that includes a FPGA and an ultra-fast PC. They adapt future measurement angles depending on previous measurement results by calculations that are defined by the protocol. Since the qubits are measured after each other, later measured photons have to be delayed in fiber loops by given delays $\Delta\tau$.

the generated photons can be separated from each other and the pump laser by narrow band filters (NBFs).

This is not possible for the resonant pumping scheme of an exciton state, because the photons of the pump beam and the generated photons are indistinguishable in frequency. Still there exists the opportunity to separate them by their polarisation. Therefore the collection system operates in a dark-field mode, where the excitation and detection polarization states are orthogonal to each other, which is called *polarization suppression* [66]

3.3 IMPLEMENTATION AND RESULTS

In the following sections the setup of the Flow Ambiguity protocol, as well as the single optical elements it consists of are discussed in more detail. Finally a polarisation suppression implementation and its performance are described at the end of this chapter.

3.3.1 Flow Ambiguity

Our experimental implementation of the *Flow Ambiguity* protocol is based on polarization encoded photons and a schematic sketch is given in figure 3.10.
Photons are transmitted from one part of the setup to another partially through fibers, which

cause losses, dispersion as well as changes in polarization [62]. Dispersion can, in our implementation, be neglected as we made sure that before photon interference the interfering photons pass the same amount of fiber. Changes in polarization is compensated by paddles that act as QWP-HWP-QWP sequence. In these, the fiber forms loops that cause birefringent and turning the paddles rotates the optical axes. With this configuration the unitary transformation caused by the fiber can be compensated by adding the inverse transformation with the paddles.

STATE PREPARATION is performed by two SPDC sources generating $|\psi^-\rangle$ Bell-states, which are transformed on their way to the CZ gate, described in section 3.3.3, via paddles to $|\phi^+\rangle$ states. In the gate the interfering photons are transformed into the cluster state

$$|\psi_c\rangle = \frac{1}{2}\left(|HHHH\rangle + |HHVV\rangle + |VVHH\rangle - |VVVV\rangle\right) \tag{3.15}$$

which will be further transformed by Hadamard gates and a SWAP gate into the Box resource state [19] shown in figure 3.10.

$$|Box\rangle = \frac{1}{2}\left(|H+H+\rangle + |H-V-\rangle + |V-H-\rangle + |V+V+\rangle\right) \tag{3.16}$$

$$= SWAP_{2,3}H_1H_2H_3H_4\,|\psi\rangle \tag{3.17}$$

PROTOCOL EXECUTION is implemented by measuring all the qubits after each other relying on a feed forward procedure. Therefore every time a single photon is detected the measurement result is passed to *field-programmable gate array* (FPGA) representing the classical client, which calculates the next measurement angle based on the *Flow Ambuguity* protocol described in section 2.3 and sends it back to the server, where the measurement basis is adjusted.

During the calculation time of the FPGA and the setting of the measurement angle, the photons that haven't been measured until then have to be delayed. This is done by injecting them into fiber loops, whose length is matched with the requested delay time $\Delta\tau$, that is dependent on the calculation time of the FPGA, the data exchange between the server and the client as well as the time needed for the measurement angle update. As the probability that a photon is absorbed in a fiber grows exponentially with the length of the fiber [62], the feed forward procedure as well as the measurement angle change has to be implemented as fast as possible. For the angle rotation we therefore resort to an electro-optic medium, were the refractive index of a non-centrosymmetric materials is linearly dependent on an applied electric field, called a *Pockels cell* (PC) [62]. This PC is used in our implementation as a fast switching HWP that can operate at a repetition rate of 1MHz.

3.3.2 Single-Photon Sources

In our setup the sources are based on 2mm thick type-II phase matched birefringe β-Barium Borate (BBO) crystals, generating entangled photons at a wavelength of 789 nm while pumped at a wavelength of 394,5 nm. This pump beam is generated by a tuneable pulsed *Chameleon Ti:Sapphire* laser from *Coherent*, operating at 789nm with a repetition rate of 80

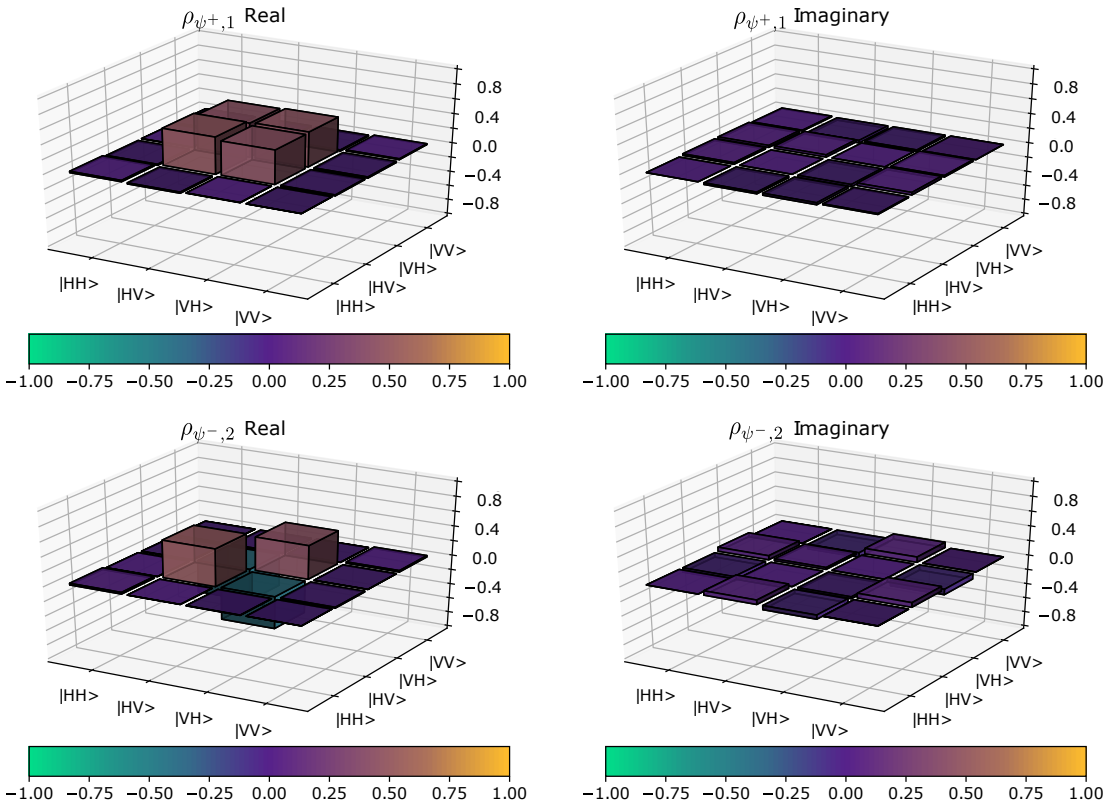


Figure 3.11.: Real and imaginary part of the density matrices representing the states possible to generate by the sources. By tilting the compensation BBOs it was possible to generate either a $|\psi^+\rangle$ or a $|\psi^-\rangle$ state. In this measurement we were able to achieve a $|\psi^+\rangle$ state with a fidelity of $\mathcal{F}_{\psi^+,1} = 0.945 \pm 0.031$ at the first source and at the second source we generated a $|\psi^-\rangle$ state with a fidelity of $\mathcal{F}_{-,2} = 0.920 \pm 0.024$.

MHz and a pulse length of 150 fs, that pumps a BBO crystal in a second harmonic generation (SHG) system from *Coherent*. In the SHG crystal the inverse process of SPDC causes the transformation of two 789nm photons to combine together into one photon with half the wavelength of the original ones, generating the pump beam for the SPDC source at 394,5 nm. The beam diameter of the pump beam is controlled on the way to the crystals by a set of lenses not included in the figure of the setup given in 3.10.

Since the SPDC process in the (main) crystal happens spontaneously at a random position and the o-wave and e-wave experience different refractive indices, there is a walk-off between the generated photons. Compensation of this is achieved by placing a HWP, that flips the polarization in each arm, followed by a compensation BBO half the thickness of the main crystal. In the compensation crystal the photons experience just the opposite refractive index of the one in the main crystal, so that in average, the temporal and transverse walk-off cancels out [26]. A 3 nm-bandwith spectral narrow-band-filter (NBF) and coupling the photons into single mode fibers (SMFs) ensures polarization entangled photons with high spectral and spatial purity.

To generate the four-photon resource cluster state, the two SPDC sources are placed behind each other, pumped by the same beam. They generate $|\psi^-\rangle$ Bell-states, which are

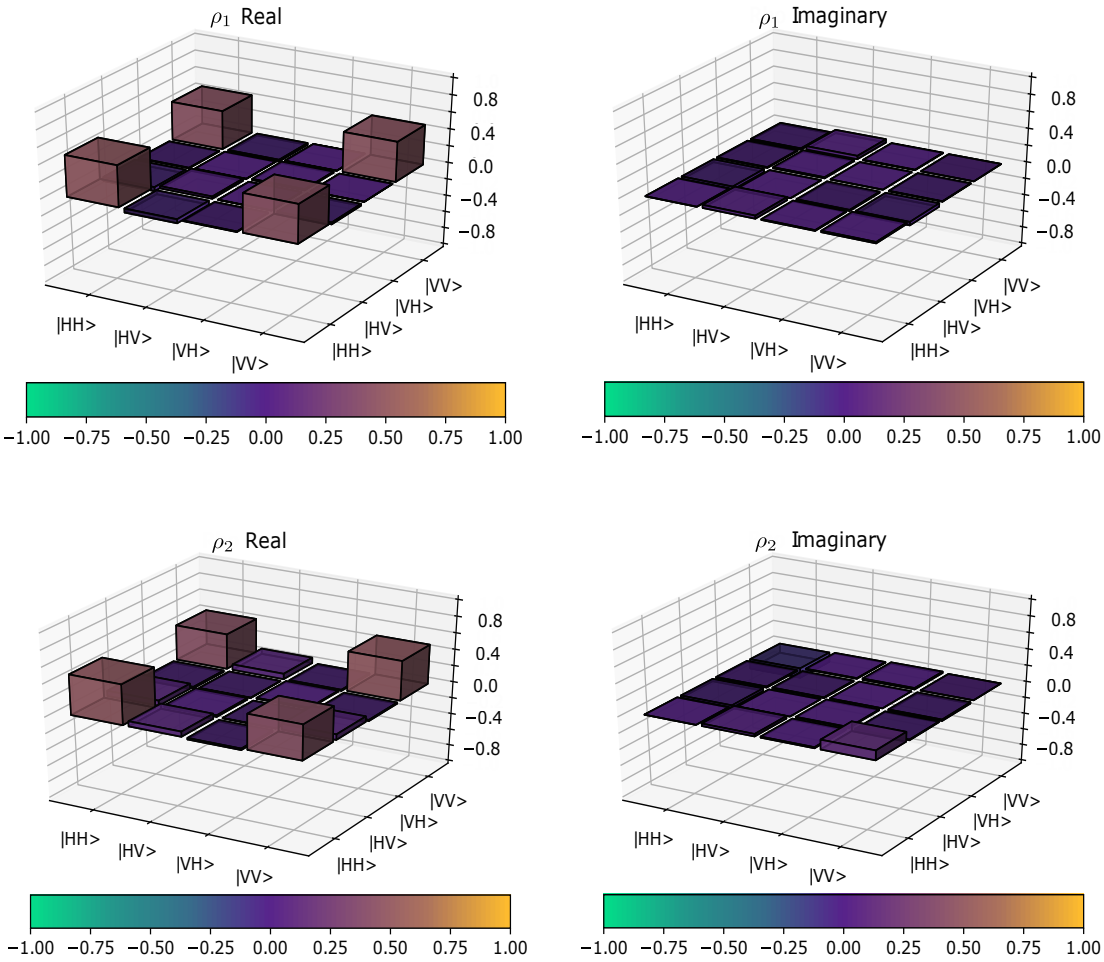


Figure 3.12.: Real and imaginary part of the density matrices representing the state generated by the two sources arriving at the CZ gate. They equal $|\phi^+\rangle$ states with a fidelity of $\mathcal{F}_1 = 0.949 \pm 0.023$ and $\mathcal{F}_2 = 0.952 \pm 0.037$ respectively.

transformed in the fibers before the CZ gate via paddles so that at the gate the states are given by $|\phi^+\rangle$. State tomography was performed two times. In the beginning to see which states the sources generate in principle and a second time to see which states leave the CZ gate. The first one was performed by leading the generated photon of each source after the couplers directly to the detection stage. With the SPDC sources we were able to generate $|\psi^+\rangle$ or $|\psi^-\rangle$ Bell-states, depending on the tilting of the compensation BBOs. As an example, we once generated a $|\psi^+\rangle$ state with the first source and a $|\psi^-\rangle$ state with the second with fidelities $\mathcal{F}_{\psi^+,1} = 0.945 \pm 0.031$ and $\mathcal{F}, \in_{\psi^-} = 0.920 \pm 0.024$. Corresponding density matrices are illustrated in figure 3.11.

Tomography of the states leaving the gate was performed for each source separately. Therefore, one source was blocked during the measurement for the other source. Photons that are not meant to go to the gate, were directly guided to the detection stage while the other half pass the gate before they were guided to the polarization analyzer. Only the photons that were transmitted at the main cube in the gate were taken into account for the measurement. The density matrix of the state was determined by measuring CCs in a time window of 1 ns

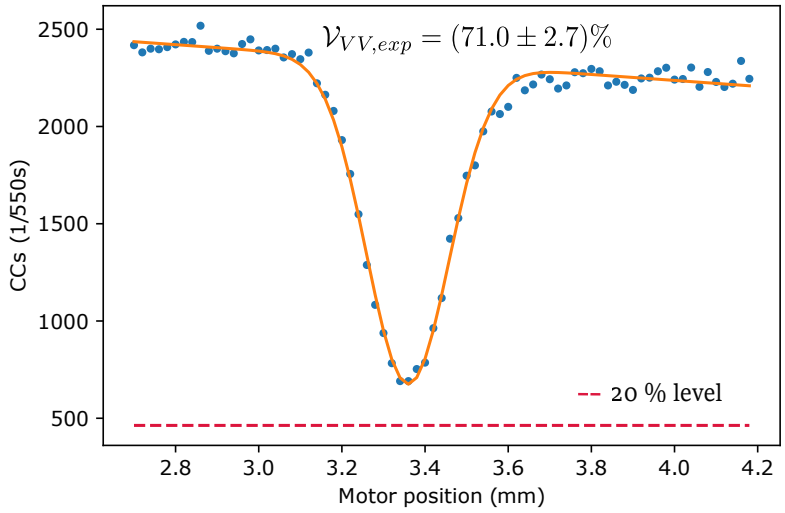


Figure 3.13: Four-photon HOM-dip with vertically polarized photons at the PDBS with transmission $T_H = 1$ and $T_V = 1/3$. The red line symbolizes the theoretical depth of the dip at 20%. The interference takes place between two photons from different sources resulting experimentally in a maximal visibility of $\mathcal{V}_{VV,exp} = (71.0 \pm 2.7)\%$.

and in 16 different bases given in table A.1 in the appendix. State tomography showed that the states at the gate resemble two $|\phi^+\rangle$ states with a fidelity of $\mathcal{F}_1 = 0.949 \pm 0.023$ for the first and $\mathcal{F}_2 = 0.952 \pm 0.037$ for the second source, which are visualized in figure 3.12.

3.3.3 Photonic CZ-gate

Entanglement between the two photon pairs is created using a CZ gate (see matrix in 2.21) that causes the characteristic phase shift based on second-order interference between indistinguishable photons at a polarization dependent beam splitter (PDBS) as pictured in figure 3.10 [63]. The gate is performed successfully for coincidence events between the output arms. For the PDBS used in our gate, horizontal light is fully transmitted ($T_H = 1$) and vertical light is transmitted with a probability of ($T_V = 1/3$) and reflected with a probability of ($R_V = 2/3$). Two compensation PDBSs, each placed in one output arm of the main PDBS, balance the unequal transformation in a way that for any input state, the output amplitudes for coincidence events are balanced. Therefore the compensation PDBSs have full transmission for vertically polarized light ($T_{C,V} = 1$) and one third for horizontal light ($T_{C,H} = 1/3$). Destructive, second order interference at the main cube happens only for the $|VV\rangle$ therm, which represents the case of two vertical polarized photons entering the cube at different ports. For all the other cases the photons are either distinguishable ($|HV\rangle$ and $|VH\rangle$) or the transmission is unity ($|HH\rangle$). The transformation for two vertically polarized photons entering the gate is given as following

$$\hat{a}^\dagger_{1,V}\hat{b}^\dagger_{2,V} \xrightarrow{\text{gate}} \left(\sqrt{\frac{1}{3}}\hat{a}^\dagger_{1,V} + i\sqrt{\frac{2}{3}}\hat{a}^\dagger_{2,V}\right)\left(\sqrt{\frac{1}{3}}\hat{b}^\dagger_{2,V} + i\sqrt{\frac{2}{3}}\hat{b}^\dagger_{1,V}\right) \tag{3.18}$$

$$= \frac{1}{3}\hat{a}^\dagger_{1,V}\hat{b}^\dagger_{2,V} + i\frac{\sqrt{2}}{3}\hat{a}^\dagger_{1,V}\hat{b}^\dagger_{1,V} + i\frac{\sqrt{2}}{3}\hat{a}^\dagger_{2,V}\hat{b}^\dagger_{2,V} - \frac{2}{3}\hat{a}^\dagger_{2,V}\hat{b}^\dagger_{1,V} \tag{3.19}$$

Measurement Basis
$\|HHHH\rangle$
$\|HH{+}{+}\rangle$
$\|HHRR\rangle$
$\|{+}{+}HH\rangle$
$\|RRHH\rangle$
$\|{+}R{+}R\rangle$
$\|{+}RR{+}\rangle$
$\|R{+}{+}R\rangle$
$\|R{+}R{+}\rangle$

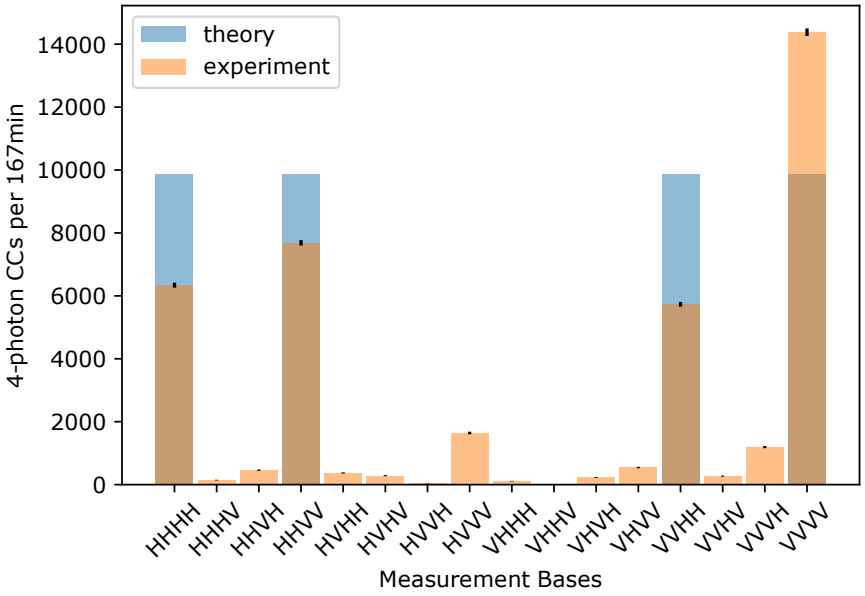


Figure 3.14.: Measurement bases for stabilizer CCs measurements together with a histogram of four photon CCs in a 2 ns time window, detected during 167 minutes of measurement in the $|H/V\rangle$-basis. Distinguishable vertical photons are responsible for the excess counts in the $VVVV$ therm. As comparison the theoretical values are also given.

For distinguishable vertically polarized photons the probability of detecting CCs after the gate is 5/9 whereas for the indistinguishable case it is 1/9, resulting in a theoretical HOM-dip visibility $\mathcal{V} = \frac{c_\infty - c_0}{c_\infty}$ for vertical photons of $\mathcal{V}_{VV} = 80\%$, where c_∞ gives the CCs count rate at huge delays of the incoming photons and c_0 represents the same only at zero delay. Paying attention to CCs events only, the CZ gate adds a phase shift if both input photons are vertically polarized $|VV\rangle \rightarrow -\frac{1}{3}|VV\rangle$.

The spatial and temporal difference between our two sources have to be taken into account for the photons of the different sources to overlap in the CZ gate. For them to interfere, they have to be indistinguishable. Therefore they pass the same amount of fiber and the fiber based optical path of the photons coming from the first source is extended by a free space part, as long as the spatial difference between the sources to ensure maximal indistinguishability and temporal overlap. With that, a maximal four photon HOM-dip visibility of $\mathcal{V}_{VV,exp} = (71.0 \pm 2.7)\%$ was achieved as can be seen in figure 3.13. Comparing this with the theoretical visibility of 80% results in an overlap quality of $\mathcal{Q} = \mathcal{V}_{exp}/\mathcal{V}_{th} = 0.888 \pm 0.034$. This tells us that less that 12% of the detected photons are distinguishable and therefore not interfering. This could be caused by a combination of multi-photon emissions, slight misalignment of the NBF in each photon path, a slightly different splitting ratio for the vertically polarized photons at the main PDBS in the CZ gate due to rotations of the cube and by spatially not overlapping photons in the main cube.

3.3.4 Cluster state Analysis

Our setup provided cluster state generation with a frequency around 10 Hz. The generated four-photon cluster state is not characterized with state tomography, as it would need 81

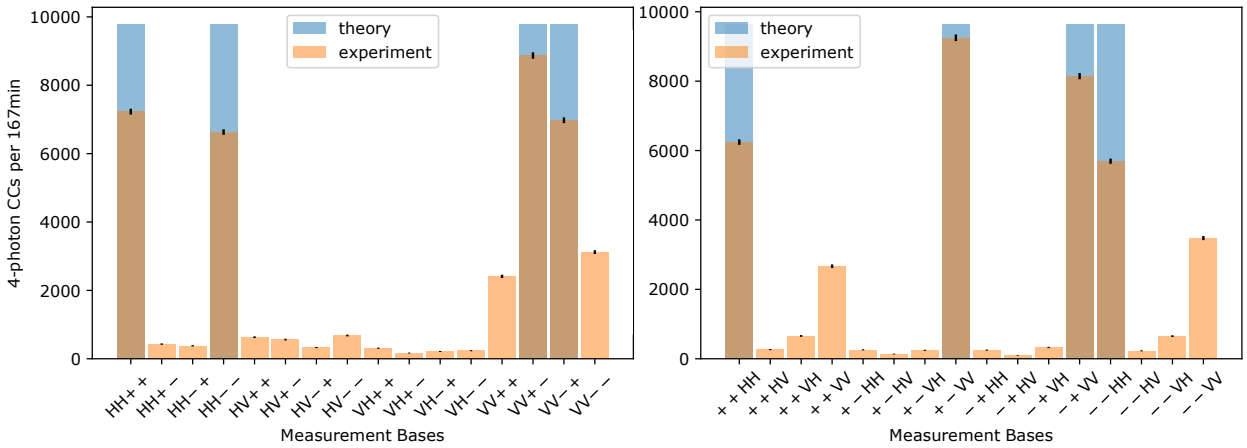


Figure 3.15.: Four photon CCs in a CCs window of 2 ns are detected during 167 minutes of measurement together with the theoretical values. The first/last two of the four photons are measured in the $|+/-\rangle$-bases in the right/left histogram, while the others are still measured in $|H/V\rangle$. An amount of 12% vertical photons are distinguishable and cause higher values of the $\sigma_x\sigma_x VV$ and $VV\sigma_x\sigma_x$ therms.

measurement settings [42, 67]. Instead we used the fact that the cluster is a graph state, which is defines by its stabilizers. Measuring the average expectation value of the stabilizer operators determines the fidelity of our cluster state and was performed similarly to [67]. Additionally, graph states offer the opportunity of designing an entanglement witness, testing four-partite entanglement with the stabilizer formalism. The entanglement witness for our state $|\psi_c\rangle$ in equation (3.15) is given by

$$\mathcal{W}_{\psi_c} := 3 \cdot \mathbb{1}^{\otimes 4} - \frac{1}{2}\left(\sigma_z\sigma_z\mathbb{1}\mathbb{1} + \mathbb{1}^{\otimes 4}\right)\left(\mathbb{1}\sigma_z\sigma_x\sigma_x + \mathbb{1}^{\otimes 4}\right) \tag{3.20}$$

$$- \frac{1}{2}\left(\sigma_x\sigma_x\sigma_z\mathbb{1} + \mathbb{1}^{\otimes 4}\right)\left(\mathbb{1}\mathbb{1}\sigma_z\sigma_z + \mathbb{1}^{\otimes 4}\right) \tag{3.21}$$

with a theoretical value of $\mathrm{Tr}(\mathcal{W}_{\psi_c}\rho_{th}) = -1$ for the theoretical density matrix ρ_{th} of state $|\psi_c\rangle$ [67–69]. Therefore, polarization analysis as pictured in 3.10 is performed and all possible combinations of four-photon CCs in a time window of 2 ns in nine different bases given in figure 3.14 are measured each over 167 minutes. The resulting expectation values of the stabilizers are noted in table 3.2. By taking the average of the expectation values, one gets the fidelity of the measured state, which in our case was $\mathcal{F}_{exp} = 0.6600 \pm 0.0010$. In figure 3.14 and 3.15 the experimental CCs of the generated cluster measured in three different bases, are visualized together with the theoretical values.

Due to the HOM-dip visibility of $\mathcal{V}_{VV,exp,cluster} = 0.677 \pm 0.034$ for this cluster measurement (see figure A.1 in the appendix), we know that a little bit more than 15% of our vertical polarized photons are distinguishable and therefore not interacting. This results in additional polarization noise as well as higher values of the $VVVV$ term in figure 3.14 and an increase of the values $\sigma_x\sigma_x VV$ and $VV\sigma_x\sigma_x$ in figure 3.15. To prove that the system is in a coherent superposition, we measured in the computational bases and additionally also took CCs for the cases where the first or last two photons are measured in the x-basis while the others stay in the computational basis. Results of this cluster analysis are given in the histograms shown in figure 3.14 and 3.15. Measurements in the basis $|HH++\rangle$ and $|++HH\rangle$ were

Stabilizer operators	Expectation value	Stabilizer operators	Expectation value
$\sigma_z \otimes \sigma_z \otimes \mathbb{1} \otimes \mathbb{1}$	0.8370 ± 0.0028	$\sigma_x \otimes \sigma_x \otimes \mathbb{1} \otimes \sigma_z$	0.6003 ± 0.0041
$\mathbb{1} \otimes \mathbb{1} \otimes \sigma_z \otimes \sigma_z$	0.8673 ± 0.0025	$\sigma_y \otimes \sigma_y \otimes \mathbb{1} \otimes \sigma_z$	-0.6006 ± 0.0041
$\sigma_z \otimes \mathbb{1} \otimes \sigma_x \otimes \sigma_x$	0.6034 ± 0.0041	$\sigma_y \otimes \sigma_y \otimes \sigma_z \otimes \mathbb{1}$	-0.5778 ± 0.0042
$\mathbb{1} \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x$	0.5902 ± 0.0041	$\sigma_x \otimes \sigma_y \otimes \sigma_x \otimes \sigma_y$	0.5975 ± 0.0042
$\mathbb{1} \otimes \sigma_z \otimes \sigma_y \otimes \sigma_y$	-0.5866 ± 0.0042	$\sigma_x \otimes \sigma_y \otimes \sigma_y \otimes \sigma_x$	0.5906 ± 0.0042
$\sigma_z \otimes \mathbb{1} \otimes \sigma_y \otimes \sigma_y$	-0.6076 ± 0.0041	$\sigma_y \otimes \sigma_x \otimes \sigma_x \otimes \sigma_y$	0.5869 ± 0.0042
$\sigma_x \otimes \sigma_x \otimes \sigma_z \otimes \mathbb{1}$	0.5754 ± 0.0042	$\sigma_y \otimes \sigma_x \otimes \sigma_y \otimes \sigma_x$	0.5783 ± 0.0043
$\sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z$	0.7601 ± 0.0033	$\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}$	1.0000 ± 0.0051
$\mathcal{F}_{exp} = 0.6600 \pm 0.0010$			
$\mathrm{Tr}(\mathcal{W}_\psi \rho_{exp}) = -0.037 \pm 0.012$			

Table 3.2.: Expectation values of the stabilizer measurements performed on the generated cluster after the CZ gate. The resulting fidelity $\mathcal{F}_{exp}$ is given together with the result of the witness measurement, where the corresponding operator is given in equation (3.21). Measurements were performed by detecting CCs events in a CCs time window of 2 ns for the given bases over 176 minutes.

sufficient to prove four photon entanglement based on the stabilizer witness $\mathcal{W}_{\psi_c}$ given in equation (3.21). For our generated cluster state the witness measurement resulted in a value of $\mathrm{Tr}(\mathcal{W}_{\psi_c}\rho_{exp}) = -0.037 \pm 0.012$ and therefore proves genuine four-photon entanglement. Still this could be improved, so that the amplitudes in the superposition of the four states are better balanced when measured in the different bases. Until now, this is not the case, due to 12% of indistinguishable photons that are not interfering in the CZ gate. Errors of the measured quantities are caused by Poissonian counting statistics of the detection events.

3.3.5 Pockel Cell

Our PC is made of Kaliumtitanylphosphat (KTP) from *EKSMA*, that provides a transmission of over 98% at 790 nm. To compensate the spatial walk off and reduce the applied voltage by half, a double KTP crystal was chosen. It acts as a HWP at an applied voltage of 2.9 kV and can be operated at a repetition rate of 1MHz.

During the protocol the angles of three photons have to be adapted which is implemented in our setup by using only a QWP, a single PC and renaming the logic of the detectors. This offers the opportunity of implementing four different measurement angles given in (2.38). The first angle is given by the original naming of the detectors and the PC off. Second and third are implemented by renaming the logic or turning the PC on and the fourth angle is given for the case when the PC is turned on and the detectors are renamed as well.

Since letting all three photons pass the PC the same way would decrease entropy, they pass through the PC in different spatial modes. Therefore the beam paths are aligned parallel to each other in a triangle formation shown in figure 3.16 a,. It is crucial that the PC and the photon paths are aligned in such a way that the beams don't overlap and all three photons experience the same rotation of their polarization. With a set of lenses that are not shown in the drawing of the setup, the diameters of the beams were decreased, so that they can pass together the PC without overlapping each other. Therefore, the beam diameter and the distances between the three different beam paths were measured with laser light and a

WinCamD from *DataRay*. The diameters d_1, d_2 and d_3 of the three beams as well as the difference between the first and the second $\overline{12}$, the second and third $\overline{23}$ and last but not least the first and third $\overline{13}$, were measured to be given as following.

$$\begin{aligned} d_1 &= (219 \pm 3)\mu\text{m} & \overline{12} &= (749.52 \pm 0.71)\mu\text{m} \\ d_1 &= (237 \pm 3)\mu\text{m} & \overline{23} &= (713.81 \pm 0.71)\mu\text{m} \\ d_1 &= (261 \pm 3)\mu\text{m} & \overline{13} &= (1047.53 \pm 0.71)\mu\text{m} \end{aligned}$$

For the PC characterization and alignment we used again laser light and added two PBS and a HWP to the setup as shown in figure 3.16 b. The PBS before the PC makes sure that only initial $|H\rangle$ photons are part of the characterization. After that, these photons pass the PC and the HWP, which is rotated in 5° steps. A PBS filters the polarization before a photo diode. For each HWP position, the intensity was measured for the PC switched on and off with a photodiode and read out via an oscilloscope. The phase between the two intensity functions defines the angle at which the PC is set and the KTP crystal was aligned in such a way that it acts as a HWP at an angle of $\theta = 22.5°$ and applies the transformation $|H\rangle \rightarrow |+\rangle$ to photons in all three different beam paths. The measured intensity functions are given in figure 3.16 and result in a transformation equal a HWP set at the angles given below. The errors are given by the smallest possible step size of the PCB motor in which the HWP was mounted.

$$\theta_1 = (22.569 \pm 0.125)° \tag{3.22}$$
$$\theta_2 = (22.581 \pm 0.125)° \tag{3.23}$$
$$\theta_3 = (22.597 \pm 0.125)°. \tag{3.24}$$

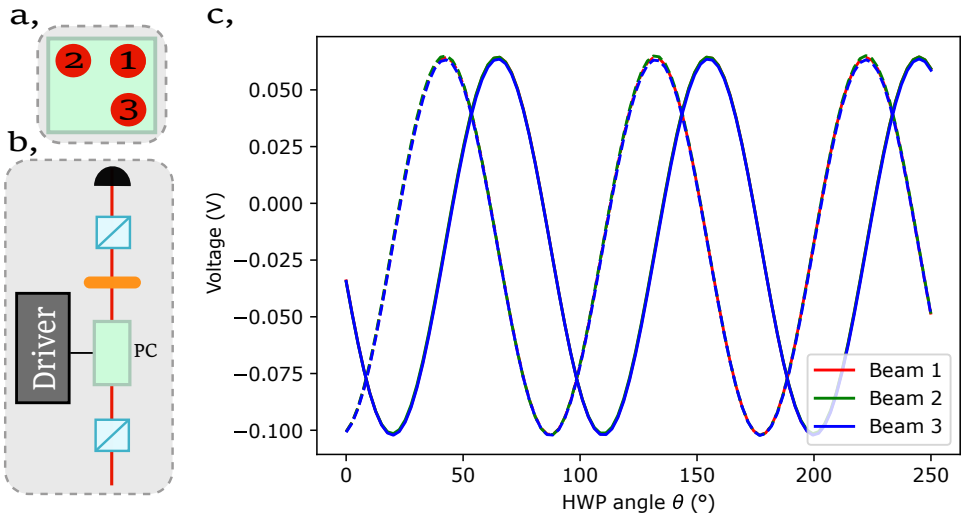


Figure 3.16.: a, A cut through the 3 beams passing the PC, perpendicular to the propagation direction. **b,** Setup for the PC characterization which resukts are visualized in **c,** For clearer understanding only the fitting functions of the intensity measurements are plotted, where the dashed lines represent the case where the PC is turned off. The transformation equals a HWP at an angle of $\theta = (22.582 \pm 0.125)°$ and is the same for all beams. The error results from the smallest possible step size of the PCB motor on which the HWP was mounted.

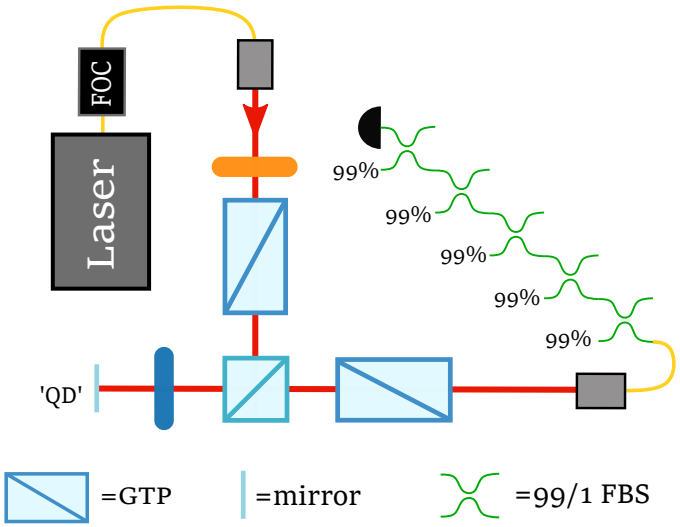


Figure 3.17: Polarization suppression: A HWP and a GTP are used as power regulation define the pump beam to be polarized vertically. The QWP compensates upcoming elliptic polarization and the PBS reflects the pump beam on the 'QD' (presented in this setup by a mirror) and separates on the way back the pump photons from photons generated by the 'QD'. A second GTP acts as a second polarization filter. Five/one FBS decrease the coupled signal for the case for unsupressed/supressed laser light. To avoid laser fluctuations caused by back reflected light, a fiber based optical circulator (FOC) was added after the laser.

3.4 POLARIZATION SUPPRESSION

Polarisation suppression (PS) relies on operating a collection system in a dark-field mode that is defined by polarization. Therefore, the detection polarization state is orthogonal to the excitation polarization state which is implemented in our setup by a PBS, two Glan-Taylor polarizer (GTP), a HWP and a QWP. The HWP and one GTP are used as power control and provide a linearly polarized pump beam, in our case vertically polarized laser light. The back-reflected laser light is suppressed in transmission by the PBS and another GTP, which only transmits horizontal polarized photons. The QWP manages the polarization between the PBS and the QD. It defines the back-reflected laser light intensity in the detection path, which depends periodically on the QWP angle with a period of $\pi/4$. To align the detection path, the QWP is set on an angle $\theta_{PS} + \pi/4$, where the laser light is optimally transmitted to the detection. θ_{PS} indicates the QWP angle of optimal laser filtering. Additional the QWP can compensate for possible elliptic parts in the polarization. The corresponding setup is shown in figure 3.17.

Our future single-photon sources will be based on semiconductor InAs/GaAs QDs emitting photons around 1550 nm, that will be grown by the group of Peter Michler at the *Institut für Halbleiteroptik und Funktionelle Grenzflächen* from the university of Stuttgart. Therefore, our setup was pumped with laser light at a wavelength of 1550 nm. Since laser reflections back into the laser have caused problems in the stability of laser performance, an isolator in form of a fiber based optical circulator (FOC) was placed after the laser output. To provide as much stability as possible the whole setup was build in a cage system and due to the lack of a usable QD sample or cryostat, the suppression was tested with a mirror instead of a sample and without any microscopic elements.

To determine the magnitude of suppression of the setup, given by the *optical density* $OD = \log(1/T)$ where T is the transmission, we measured single-photon counts once with the PS on and once with the PS off as shown in figure 3.18 a. Both times the photons

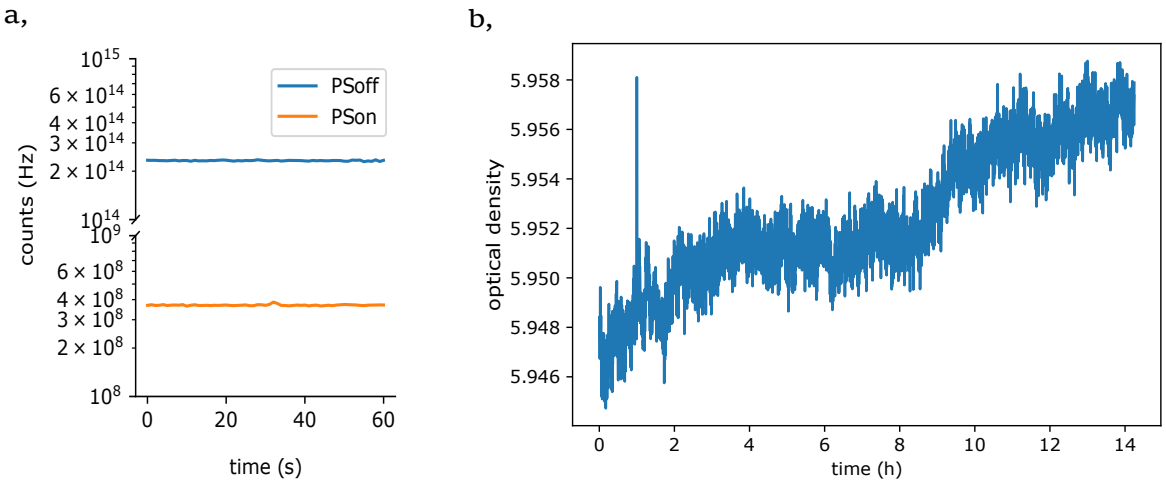


Figure 3.18.: a, PS on and off: Measurement of single photons after the PS setup shown in figure 3.17. Once the measurement was done with the PS on and once with the QWP at 45° to let as much light as possible pass. A suppression of almost six magnitudes was achieved. **b, Stability:** The pump laser was suppressed in the beginning of the measurement and afterwards the setup was left alone by itself over 14 hours. The average optical density during the stability measurement was $OD = 5.95 \pm 0.12$.

were detected by an InGaAs/InP APD from the company *IDQuantique*, so that they can be directly compared with each other. Due to the fact that the signal for the measurement with unsuppressed laser light would have been way too high for the APD, the photons were first sent through a cascade of five fiber based beam splitters (FBSs) with a splitting ratio of 99 to 1, where we always took the 1% transmission path. For the situation with suppressed laser light, a single FBS was also needed to decrease the signal. A suppression of the laser light of almost six magnitudes was achieved when comparing the PS on and PS off as can be seen in figure 3.18. Leaving the setup running on its own over more than 14 hours, left the suppression almost unchanged at an optical density of $OD = 5.95 \pm 0.12$ as can be seen in figure 3.18 b.

4 OUTLOOK

During this thesis we worked on the implementation of a classically-driven blind MBQC protocol based on a four-photon box cluster state, where single photons were generated by type-II SPDC sources. So far we were able to build up all single optical parts needed for the implementation of this protocol. Starting at the source and the CZ gate for cluster state generation, continuing with the PC for adaptive measurement angles and finishing with the detection stage.

The generated cluster state shows the needed four-photon entanglement with the four-partite entanglement witness and also measurements in different bases demonstrating that our cluster is in a coherent superposition of four different states. The unbalanced amplitudes of the four states in the superposition of our cluster result out of fidelity of the cluster state could result of sub-optimal fidelities of 12% distinguishable photons in the CZ gate.

In order to run the protocol, the next steps of the experiment will be to add the delay lines in the form of fiber spools and to program the FPGA.

For the polarisation suppression setup, it would be convenient to fix the whole setup directly at the optical table, to enable even more stability. Also the suppression of the laser light can be increased when running the system in a dark-field microscope mode.

4.1 PROPOSAL

Since the brightness of an SPDC source is related to the single photon purity, its performance is limited. Because of that we are preparing to change to QD single-photon sources, which hold the promise to be deterministic sources. These new sources will open new possibilities in optical quantum computing as well as quantum cryptography protocols. And for these new sources a setup to suppress the pump beam in the single photon collection path by almost six magnitudes was built. This will be needed for characterizations of the source while it is pumped resonantly.

However, so fare QDs emitting entangled photon pairs haven't been used to generate the full set of four-photon cluster states [70]. In this part of the thesis I want to give an experimental proposal, realizing exactly the just mentioned task. According setup to that is given in figure 4.1.

Therefore a semiconductor QD will be used to generate polarization entangled photons. Via TPE it will be lifted to the biexiton states $|XX\rangle$ from where it will decay back to the ground state, emitting the Bell-state $|\phi^{\pm}\rangle$ as pictured in figure 3.9. The exiton and biexiton photons will be separated by narrow-band filters (NBFs) and coupled into single-mode fibers. A fiber beam splitter (FBS) directs them either along a direct or delayed path (see figure 4.1). These two paths are necessary, because the QD emits only one entangled photon pair at a time and to generate a four photon cluster state, two of these entangled pairs are needed. So

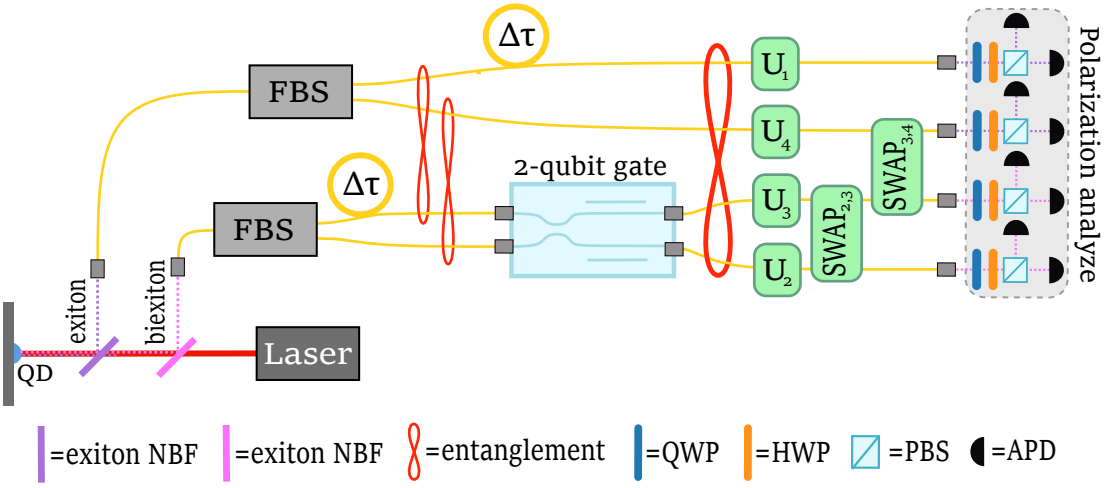


Figure 4.1.: A GaAs QD will excitet via TPE into a biexiton state from were it decays and emits an entangled photon pairs in the state $|\psi^{\pm}\rangle$. By narrow band filters (NBF) the exiton and biexiton photons are separated and the first generated paire is delayed so that it can overlap on a two-qubit gate with the second Bell pair generated afterwards. With the two possible two-qubit gates, the possible unitary operations U_i in each photon path and a SWAP gate between the two photons that interact at the gate ($SWAP_{2,3}$), any of the desired four qubit cluster states given in figure 4.2 can be realized.

one pair will be delayed in a way that it overlaps with the later generated second pair. Two photons, one from each entangled pair, will interfere in a two-qubit gate. This is similar to the implementation of the *Flow Ambiguity* implementation in section 3.3.1, but this time the gate will be realized via integrated optics on a chip. It will be possible to choose between a CZ-gate or a PBS. When the photons arrive at the gate, both pairs will be in the state $|\phi^{+}\rangle$. If only CCs between the four polarization analysing detection stages are taken into account, the generated four qubit cluster state is either the $|\psi_c\rangle$ or the Greenberger-Horne-Zeilinger state ($|GHZ\rangle$) dependent on if the two-qubit gate was a CZ-gate or a PBS. For the $|GHZ\rangle$ state generation see [71].

$$|\psi_c\rangle = \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle\right) \tag{4.1}$$

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|0000\rangle + |1111\rangle\right) \tag{4.2}$$

The qubits are as before polarization encoded so that $|0\rangle = |H\rangle$ and $|1\rangle = |V\rangle$. To have the opportunity of performing all possible circuits based on four qubit cluster states, we are going to generate the full set of four-qubit graph states (see figure 4.2). This is realized by unitary operations in each photon path and a SWAP-gate between the photons that were interacting in the two-qubit gate. Polarization analysis is in the end performed by a QWP and a HWP followed by an APD in each path behind a PBS. The proposed setup is pictured in figure 4.1. Our source will be a strain-tunable GaAs produced by the group of Univ.-Prof. Dr. Armando Rastelli from the *JKU Linz*.

As we have seen in section 2.2.1 it is possible to transform graph states into each other by local complementations. In table A.2 in the appendix, the full set of four qubit graph states

with their quantum state is given together with the transformations needed to generate the states with either the state $|\psi_c\rangle$ or $|GHZ\rangle$.

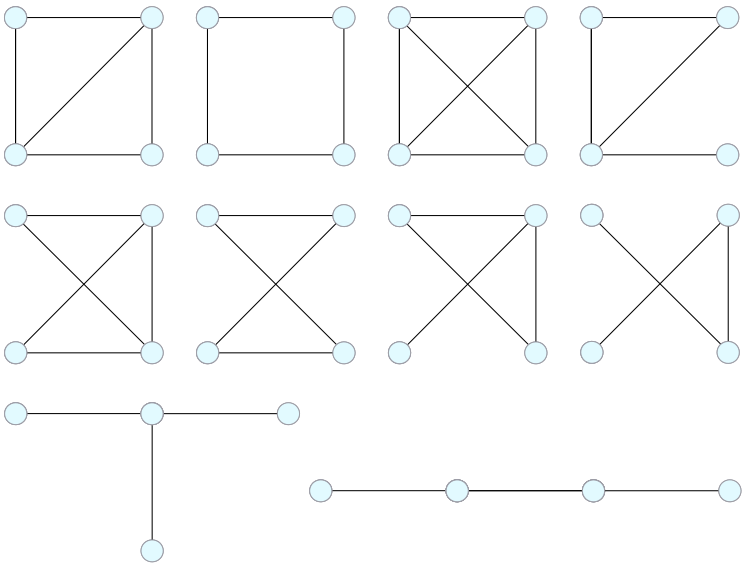


Figure 4.2.: Full set of four qubit cluster states.

5 | CONCLUSION

During the last year we worked on a classically-driven photonic blind measurement based quantum computer, to show that apart from the already existing theory it could also be implemented experimentally. This ambitious goal was not achieved within the time-frame of this master thesis due to delays in the delivery of essential experimental equipment, such as the delay fiber loops and the programming of the FPGA. However, security in computing already plays a crucial role in everyday life and as classical computational power reaches its limits and quantum hardware starts to be ready for the global market, the protocol we were working on can play a significant role in the near future.

This is given by the fact that the most realistic scenario for the first quantum computers will be several commercial usable quantum servers around the world, externally accessible. Since, our infrastructure is completely classical and will stay like this in the near future, the classical access to these quantum servers will be necessary. Such an architecture is supported by the *Flow Ambiguity* protocol. Already existing fiber networks obviously lead to the conclusion that photons will be the perfect candidates for realizing qubits.

In our implementation qubits are realized using polarization encoded photons, generated by SPDC sources. The resource cluster state is created by letting photons interfere in a two-qubit CZ-gate. Information processing will be performed in a feed forward structure, were for each measurement, a classical client calculates the measurement angle depending on previous outcomes.

Due to the fact that our experiment is a proof-of-principle experiment of the protocol, it relies on the simplest universal four-qubit resource state for MBQC given by the box cluster state. By generating the resource state for our protocol, we already reached the limits of our SPDC source. Future commercial usable quantum computers, based on the Flow Ambiguity protocol, will have to calculate a larger amount of different and even more complex tasks. In order to be able to perform these calculations, more complex resource states, including more qubits, will be needed. It is therefore necessary that we change to a more promising photon source, given by quantum dots. These sources can provide the necessary brightens and single photon purity and will offer new opportunities in quantum computing and quantum cryptography protocols. A first setup, that separate pump photons from single photons emitted by the QDs, was build and an experimental proposal using this new sources was introduced.

The combination of new sources together with the quantum computer structure of our experiment bring us a step closer to photonic quantum computers, accessible online for everyone while providing security and privacy. It is still a long way until then, with many barriers on the road, but remembering how fast our world has changed in the last decades and keeping in mind that also our personal everyday computers were developed from the first computers, which were room filling and run by a team of scientists, gives hope that in some years from now, quantum technology will be accessible for everyone.

BIBLIOGRAPHY

[1] Peter Knight Chris Gerry. *Introductory Quantum Optics*. Cambridge University Pr., Oct. 1, 2004. 320 pp. ISBN: 052152735X.

[2] A. M. Turing. "On Computable Numbers, with an Application to the Entscheidungsproblem". In: *Proceedings of the London Mathematical Society* s2-42.1 (1937), pp. 230–265. DOI: 10.1112/plms/s2-42.1.230.

[3] Gordon E. Moore. "Cramming more components onto integrated circuits, Reprinted from Electronics, volume 38, number 8, April 19, 1965, pp.114 ff." In: *IEEE Solid-State Circuits Society Newsletter* 11.3 (Sept. 2006), pp. 33–35. DOI: 10.1109/n-ssc.2006.4785860.

[4] Isaac L. Chuang Michael A. Nielsen. *Quantum computation and quantum information*. 10th Anniversary edition published 2010. Cambridge University Press, 2010. ISBN: 9781107002173.

[5] S. B. Desai et al. "MoS2 transistors with 1-nanometer gate lengths". In: *Science* 354.6308 (Oct. 2016), pp. 99–102. DOI: 10.1126/science.aah4698.

[6] Richard P. Feynman. "Simulating physics with computers". In: *International Journal of Theoretical Physics* 21.6-7 (June 1982), pp. 467–488. DOI: 10.1007/bf02650179.

[7] David Deutsch and Richard Jozsa. "Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (Dec. 1992), pp. 553–558. DOI: 10.1098/rspa.1992.0167.

[8] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (Oct. 1997), pp. 1484–1509. DOI: 10.1137/s0097539795293172.

[9] Lov K. Grover. "A fast quantum mechanical algorithm for database search". In: *arXiv* (1996).

[10] Stephen Barnett. *Quantum Information*. eng. Vol. 16. Oxford Master Series in Physics. Oxford: Oxford University Press, Incorporated, 2009. ISBN: 9780198527626.

[11] S. Debnath et al. "Demonstration of a small programmable quantum computer with atomic qubits". In: *Nature* 536.7614 (Aug. 2016), pp. 63–66. DOI: 10.1038/nature18648.

[12] T. Wilk et al. "Single-Atom Single-Photon Quantum Interface". In: *Science* 317.5837 (July 2007), pp. 488–490. DOI: 10.1126/science.1143835.

[13] R. Blatt and C. F. Roos. "Quantum simulations with trapped ions". In: *Nature Physics* 8.4 (Apr. 2012), pp. 277–284. DOI: 10.1038/nphys2252.

[14] L. DiCarlo et al. "Demonstration of two-qubit algorithms with a superconducting quantum processor". In: *Nature* 460.7252 (June 2009), pp. 240–244. DOI: 10.1038/nature08121.

[15] Frank Arute et al. "Quantum supremacy using a programmable superconducting processor". In: *Nature* 574.7779 (Oct. 2019), pp. 505–510. DOI: 10.1038/s41586-019-1666-5.

[16] I. Fushman et al. "Controlled Phase Shifts with a Single Quantum Dot". In: *Science* 320.5877 (May 2008), pp. 769–772. DOI: 10.1126/science.1154643.

[17] Han-Sen Zhong et al. "Quantum computational advantage using photons". In: *Science* 370.6523 (2020), pp. 1460–1463. ISSN: 0036-8075. DOI: 10.1126/science.abe8770.

[18] S. Barz et al. "Demonstration of Blind Quantum Computing". In: *Science* 335.6066 (Jan. 2012), pp. 303–308. DOI: 10.1126/science.1214707.

[19] P. Walther et al. "Experimental one-way quantum computing". In: *Nature* 434.7030 (Mar. 2005), pp. 169–176. DOI: 10.1038/nature03347.

[20] Stefanie Barz. "Quantum computing with photons: introduction to the circuit model, the one-way quantum computer, and the fundamental principles of photonic experiments". In: *Journal of Physics B: Atomic, Molecular and Optical Physics* 48.8 (Mar. 2015), p. 083001. DOI: 10.1088/0953-4075/48/8/083001.

[21] Joseph F. Fitzsimons and Elham Kashefi. "Unconditionally verifiable blind quantum computation". In: *Physical Review A* 96.1 (July 2017). DOI: 10.1103/physreva.96.012303.

[22] Robert Raussendorf, Daniel E. Browne, and Hans J. Briegel. "Measurement-based quantum computation on cluster states". In: *Physical Review A* 68.2 (Aug. 2003). DOI: 10.1103/physreva.68.022312.

[23] H. J. Briegel et al. "Measurement-based quantum computation". In: *Nature Physics* 5.1 (Jan. 2009), pp. 19–26. DOI: 10.1038/nphys1157.

[24] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. "Universal Blind Quantum Computation". In: *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, Oct. 2009. DOI: 10.1109/focs.2009.36.

[25] Atul Mantri et al. "Flow Ambiguity: A Path Towards Classically Driven Blind Quantum Computation". In: *Physical Review X* 7.3 (July 2017). DOI: 10.1103/physrevx.7.031004.

[26] Joseph W. Haus Peter E. Powers. *Fundamentals of Nonlinear Optics*. Taylor Francis Inc, Apr. 6, 2017. 480 pp. ISBN: 1498736831.

[27] Robert Raussendorf and Hans J. Briegel. "A One-Way Quantum Computer". In: *Physical Review Letters* 86.22 (May 2001), pp. 5188–5191. DOI: 10.1103/physrevlett.86.5188.

[28] Charles H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Physical Review Letters* 70.13 (Mar. 1993), pp. 1895–1899. DOI: 10.1103/physrevlett.70.1895.

[29] Paul G. Kwiat et al. "New High-Intensity Source of Polarization-Entangled Photon Pairs". In: *Physical Review Letters* 75.24 (Dec. 1995), pp. 4337–4341. DOI: 10.1103/physrevlett.75.4337.

[30] Pascale Senellart, Glenn Solomon, and Andrew White. "High-performance semiconductor quantum-dot single-photon sources". In: *Nature Nanotechnology* 12.11 (Nov. 2017), pp. 1026–1039. DOI: 10.1038/nnano.2017.218.

[31] Xi-Lin Wang et al. "Experimental Ten-Photon Entanglement". In: *Physical Review Letters* 117.21 (Nov. 2016). DOI: 10.1103/physrevlett.117.210502.

[32] N. Akopian et al. "Entangled Photon Pairs from Semiconductor Quantum Dots". In: *Physical Review Letters* 96.13 (Apr. 2006). DOI: 10.1103/physrevlett.96.130501.

[33] M. Müller et al. "On-demand generation of indistinguishable polarization-entangled photon pairs". In: *Nature Photonics* 8.3 (Feb. 2014), pp. 224–228. DOI: 10.1038/nphoton.2013.377.

[34] Maximilian Prilmüller et al. "Hyperentanglement of Photons Emitted by a Quantum Dot". In: *Physical Review Letters* 121.11 (Sept. 2018). DOI: 10.1103/physrevlett.121.110503.

[35] Jonas Malte Zeuner. "Complex Multiphoton Processing Using Integrated Circuits". PhD thesis. Universität Wien, 2018.

[36] Mark Fox. *Quantum Optics*. Oxford Unniversal Press, 2006. ISBN: 9780198566731.

[37] Joy A. Thomas Thomas M. Cover. *Elements of Information Theory*. 2nd ed. John Wiley Sons, 2006. ISBN: 13 978-0-471-24195-9.

[38] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Physical Review* 47.10 (May 1935), pp. 777–780. DOI: 10.1103/physrev.47.777.

[39] Bernhard Wittmann et al. "Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering". In: *New Journal of Physics* 14.5 (May 2012), p. 053030. DOI: 10.1088/1367-2630/14/5/053030.

[40] B. Hensen et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". In: *Nature* 526.7575 (Oct. 2015), pp. 682–686. DOI: 10.1038/nature15759.

[41] Marissa Giustina et al. "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons". In: *Physical Review Letters* 115.25 (Dec. 2015). DOI: 10.1103/physrevlett.115.250401.

[42] Nicolai Friis et al. "Entanglement certification from theory to experiment". In: *Nature Reviews Physics* 1.1 (Dec. 2018), pp. 72–87. DOI: 10.1038/s42254-018-0003-5.

[43] Nathan K. Langford. "Encoding, Manipulating and Measuring Quantum Information in Optics". PhD thesis. University of Queensland, 2007.

[44] Pieter Kok et al. "Linear optical quantum computing with photonic qubits". In: *Reviews of Modern Physics* 79.1 (Jan. 2007), pp. 135–174. DOI: 10.1103/revmodphys.79.135.

[45] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen. "Bell measurements for teleportation". In: *Physical Review A* 59.5 (May 1999), pp. 3295–3300. DOI: 10.1103/physreva.59.3295.

[46] Daniel Gottesman and Isaac L. Chuang. "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". In: *Nature* 402.6760 (Nov. 1999), pp. 390–393. DOI: 10.1038/46503.

[47] E. Knill, R. Laflamme, and G. J. Milburn. "A scheme for efficient quantum computation with linear optics". In: *Nature* 409.6816 (Jan. 2001), pp. 46–52. DOI: 10.1038/35051009.

[48] F. Verstraete and J. I. Cirac. "Valence-bond states for quantum computation". In: *Physical Review A* 70.6 (Dec. 2004). DOI: 10.1103/physreva.70.060302.

[49] Hans J. Briegel and Robert Raussendorf. "Persistent Entanglement in Arrays of Interacting Particles". In: *Physical Review Letters* 86.5 (Jan. 2001), pp. 910–913. DOI: 10.1103/physrevlett.86.910.

[50] Daniel Gottesman. "Stabilizer Codes and Quantum Error Correction". PhD thesis. California Institud of Technology, Pasadenia, California, 1997.

[51] Marc Hein et al. "Entanglement in Graph States and its Applications". In: *arXiv* (2006).

[52] Ilan Tzitrin. "Local equivalence of complete bipartite and repeater graph states". In: *Physical Review A* 98.3 (Sept. 2018). DOI: 10.1103/physreva.98.032305.

[53] M. Hein, J. Eisert, and H. J. Briegel. "Multiparty entanglement in graph states". In: *Physical Review A* 69.6 (June 2004). DOI: 10.1103/physreva.69.062311.

[54] Maarten Van den Nest, Jeroen Dehaene, and Bart De Moor. "Graphical description of the action of local Clifford transformations on graph states". In: *Physical Review A* 69.2 (Feb. 2004). DOI: 10.1103/physreva.69.022316.

[55] Daniel E Browne et al. "Generalized flow and determinism in measurement-based quantum computation". In: *New Journal of Physics* 9.8 (Aug. 2007), pp. 250–250. DOI: 10.1088/1367-2630/9/8/250.

[56] Michael A. Nielsen. "Cluster-state quantum computation". In: *Reports on Mathematical Physics* 57.1 (Feb. 2006), pp. 147–161. DOI: 10.1016/s0034-4877(06)80014-5.

[57] Daniel Gottesman. "The Heisenberg Representation of Quantum Computers". In: *Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, eds. S. P. Corney, R. Delbourgo, and P. D. Jarvis, pp. 32-43 (Cambridge, MA, International Press, 1999)* (July 1, 1998).

[58] David P. DiVincenzo. "The Physical Implementation of Quantum Computation". In: *Fortschr. Phys.* 48.9-11 (Sept. 2000), pp. 771–783. DOI: 10.1002/1521-3978(200009)48:9/11<771::aid-prop771>3.0.co;2-e.

[59] T. D. Ladd et al. "Quantum computers". In: *Nature* 464.7285 (Mar. 2010), pp. 45–53. DOI: 10.1038/nature08812.

[60] Stefano Paesani. "Large-Scale Integrated Quantum Photonics: Development and Applications". PhD thesis. Universtity of Bristol, School of Physics, Apr. 2019.

[61] L. Mandel C. K. Hong Z. Y. Ou. "Measurement of subpicosecond time intervals between two photons by interference". In: *Physical Review Letters* 59.18 (Nov. 1987), pp. 2044–2046. DOI: 10.1103/physrevlett.59.2044.

[62] Malvin Carl Teich Bahaa E. A. Saleh. *Fundamentals of photonics*. Hoboken, NJ: Wiley, 2019. ISBN: 9781119506898.

[63] Nikolai Kiesel et al. "Linear Optics Controlled-Phase Gate Made Simple". In: *Physical Review Letters* 95.21 (Nov. 2005). DOI: 10.1103/physrevlett.95.210505.

[64] Daniel F. V. James et al. "Measurement of qubits". In: *Physical Review A* 64.5 (Oct. 2001). DOI: 10.1103/physreva.64.052312.

[65] Boyd Robert W. *Nonlinear Optics.* Vol. 3rd ed. Academic Press, 2008. ISBN: 9780123694706.

[66] Andreas V. Kuhlmann et al. "A dark-field microscope for background-free detection of resonance fluorescence from single semiconductor quantum dots operating in a set-and-forget mode". In: *Review of Scientific Instruments* 84.7 (July 2013), p. 073905. DOI: 10.1063/1.4813879.

[67] Nikolai Kiesel et al. "Experimental Analysis of a Four-Qubit Photon Cluster State". In: *Physical Review Letters* 95.21 (Nov. 2005). DOI: 10.1103/physrevlett.95.210502.

[68] Géza Tóth and Otfried Gühne. "Detecting Genuine Multipartite Entanglement with Two Local Measurements". In: *Physical Review Letters* 94.6 (Feb. 2005). DOI: 10.1103/physrevlett.94.060501.

[69] Mohamed Bourennane et al. "Experimental Detection of Multipartite Entanglement using Witness Operators". In: *Physical Review Letters* 92.8 (Feb. 2004). DOI: 10.1103/physrevlett.92.087902.

[70] Jin-Peng Li et al. "Multiphoton Graph States from a Solid-State Single-Photon Source". In: *ACS Photonics* 7.7 (June 2020), pp. 1603–1610. DOI: 10.1021/acsphotonics.0c00192.

[71] Jian-Wei Pan et al. "Experimental Demonstration of Four-Photon Entanglement and High-Fidelity Teleportation". In: *Physical Review Letters* 86.20 (May 2001), pp. 4435–4438. DOI: 10.1103/physrevlett.86.4435.

[72] C Schmid et al. "The entanglement of the four-photon cluster state". In: *New Journal of Physics* 9.7 (July 2007), pp. 236–236. DOI: 10.1088/1367-2630/9/7/236.

[73] Mojtaba Jafarpour and Leila Assadi. "Multipartite entanglement in four-qubit graph states". In: *The European Physical Journal D* 70.3 (Mar. 2016). DOI: 10.1140/epjd/e2016-60555-5.

A | APPENDIX

A.1 A EVOLUTION OF QUANTUM STATES

In section 3.1 the evolution of quantum states was discussed. When we have a look at a transformation from a single photon prepared in mode i, than the probability of detecting this photon after the transformation in mode j is given by $\left|U_{ji}\right|^2$, which results from following calculation.

$$p(j|i) = \left|\langle \mathbf{0}|\, \hat{a}_j \left(\mathcal{U}\hat{a}_i^\dagger \mathcal{U}^\dagger\right)|\mathbf{0}\rangle\right|^2 = \left|\langle \mathbf{0}|\, \hat{a}_j \sum_k U_{ki}\hat{a}_k^\dagger\, |\mathbf{0}\rangle\right|^2 = \left|U_{ji}\right|^2 \tag{A.1}$$

A.2 EXPERIMENTAL DETAILS

DETECTION STAGE WAVEPLATE SETTING A combination of QWP, HWP, PBS and an APD in the transmission as well as the reflection path of the PBS allow measurements in different polarization bases. The angle setting for the horizontal, diagonal and circular bases are given in table 3.1. To understand that in a better way lets think that through. As an example for the $|+/-\rangle$-bases, the QWP is set at 45° so that it hasn't any effect on an incoming $|+\rangle$ or $|-\rangle$ state. The HWP at 22.5° maps the state $|+/-\rangle$ state to $|H/V\rangle$. In the transmission/reflection path of the PBS the APD measures only horizontal/vertical photons that were, before arriving at the HWP and QWP sequence, in the state $|+\rangle/|-\rangle$.

In the same way the setting for 16 different CCs measurements, for the two-qubit state tomography, were realized by setting only 9 different bases and considering different paths after the PBS as noted in table A.1.

HOM-DIP MEASUREMENT FOR CLUSTER STATE ANALYZE The HOM-dip measurement for the cluster state analysis given in 3.3.4 resulted in a visibility of $\mathcal{V} = (67.7 \pm 3.4)\%$ and shows that a little bit more than 15% of the vertical photons in the PDBS are distinguishable.

A.3 FULL SET OF FOUR-QUBIT CLUSTER STATES

As discussed in section 4.1, we want to generate the full set of four-qubit cluster states given in figure 4.2, by two $|\phi^+\rangle$ states passing either a CZ-gate or a PBS, followed by unitary transformations in each photon path and a SWAP gate between the two photons that

Basis 1	Basis 2	QWP_1	HWP_1	QWP_2	HWP_2	Path 1	Path 2
$\|H\rangle$	$\|H\rangle$	0°	0°	0°	0°	T	T
$\|H\rangle$	$\|V\rangle$	0°	0°	0°	0°	T	R
$\|V\rangle$	$\|V\rangle$	0°	0°	0°	0°	R	R
$\|V\rangle$	$\|H\rangle$	0°	0°	0°	0°	R	T
$\|R\rangle$	$\|H\rangle$	0°	22.5°	0°	0°	T	T
$\|R\rangle$	$\|V\rangle$	0°	22.5°	0°	0°	T	R
$\|+\rangle$	$\|V\rangle$	45°	22.5°	0°	0°	T	R
$\|+\rangle$	$\|H\rangle$	45°	22.5°	0°	0°	T	T
$\|+\rangle$	$\|R\rangle$	45°	22.5°	0°	22.5°	T	T
$\|+\rangle$	$\|+\rangle$	45°	22.5°	45°	22.5°	T	T
$\|R\rangle$	$\|+\rangle$	0°	22.5°	45°	22.5°	T	T
$\|H\rangle$	$\|+\rangle$	0°	0°	45°	22.5°	T	T
$\|V\rangle$	$\|+\rangle$	0°	0°	45°	22.5°	R	T
$\|V\rangle$	$\|L\rangle$	0°	0°	0°	22.5°	R	R
$\|H\rangle$	$\|L\rangle$	0°	0°	0°	22.5°	T	R
$\|R\rangle$	$\|L\rangle$	0°	22.5°	0°	22.5°	R	R

Table A.1.: Measurement basis with corresponding waveplate angles. The last two columns define which patch after the PBS is taken into account for the CCs measurement.

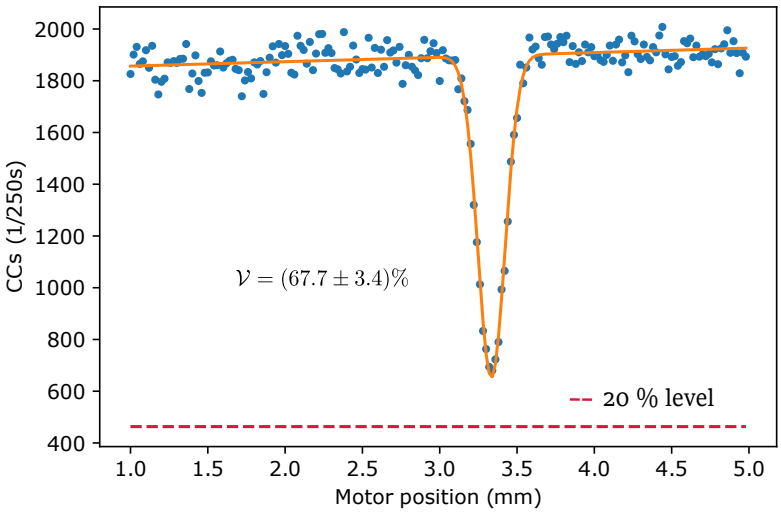
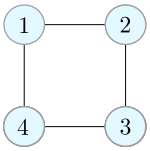
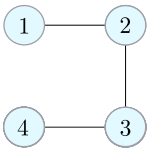
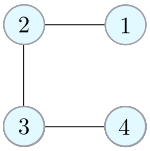
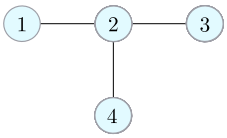
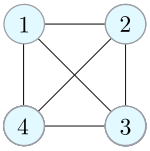
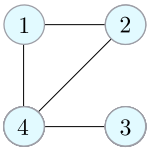


Figure A.1: Four-photon HOM-dip measurement of vertically polarized photons at the PDBS in the photonic CZ-gate for the cluster state analysis. The red line symbolizes the theoretical depth of the dip at 20%. The interference takes place between two photons from different sources resulting experimentally in a visibility of $\mathcal{V} = (67.7 \pm 3.4)\%$.

interact in the two-qubit gate as picture in figure 4.1. In tables A.2 the graph states together with their quantum states as well as their LC transformations needed to transform the state after the two-qubit gate into the wanted state. This time the numbering of the qubits doesn't represent the measurement order but label of the qubits since we us the notation $|0\rangle_1 |+\rangle_2 |1\rangle_3 |-\rangle_4 = |0+1-\rangle$.

Graph-state	Cluster-state	Local Complementation
	$\|Box\rangle = \|0+0+\rangle +$ $\|0-1-\rangle +$ $\|1-0-\rangle +$ $\|1+1+\rangle$	$SWAP_{2,3} H_1 H_2 H_3 H_4 \|\psi\rangle$ [19]
	$\|+0+0\rangle +$ $\|+0-1\rangle +$ $\|-1-0\rangle +$ $\|-1+1\rangle$	$H_1 H_2 \|\psi\rangle$ [72]
	$\|+0+0\rangle +$ $\|+0-1\rangle +$ $\|-1-0\rangle +$ $\|-1+1\rangle$	$H_1 H_2 \|\psi\rangle$ [72]
	$\|+0++\rangle +$ $\|-1--\rangle$	$H_1 H_3 H_4 \|GHZ\rangle$
	$\|+0+0\rangle +$ $\|+0-1\rangle +$ $\|-1-0\rangle +$ $\|-1+1\rangle$	$H_1 H_2 \|\psi\rangle$ [72]
	$\|0+00\rangle +$ $\|0-01\rangle +$ $\|0-10\rangle -$ $\|0+11\rangle +$ $\|1-00\rangle -$ $\|1+01\rangle -$ $\|1+10\rangle -$ $\|1-11\rangle$	$\sqrt{\sigma_{z,4}}^\dagger \sqrt{\sigma_{z,3}}^\dagger \sqrt{\sigma_{x,2}} \sqrt{\sigma_{z,1}}^\dagger$ $H_1 H_3 H_4 \|GHZ\rangle$ [73]
	$\|+00+\rangle +$ $\|-01-\rangle +$ $\|-10+\rangle -$ $\|+11-\rangle$	$\sqrt{\sigma_{z,1}} \sqrt{\sigma_{x,2}}^\dagger \sqrt{\sigma_{z,3}} H_1 H_4 \|\psi\rangle$ [18]

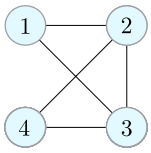
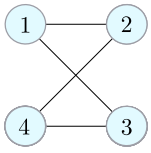
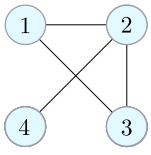
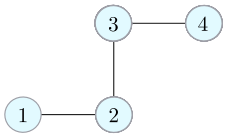
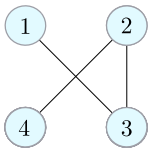
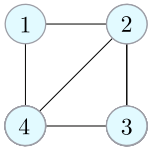
	$\|+0+0\rangle +$ $\|-0-1\rangle +$ $\|-1-0\rangle -$ $\|+1+1\rangle$	$\sqrt{\sigma_{x,1}}\sqrt{\sigma_{z,2}}^{\dagger}\sqrt{\sigma_{z,4}}^{\dagger}\|Box\rangle$ [51]
	$\|0+0+\rangle +$ $\|0-1-\rangle +$ $\|1-0-\rangle +$ $\|1+1+\rangle$	$SWAP_{2,3}H_1H_2H_3H_4\|\psi\rangle$ [19]
	$\|+0+0\rangle +$ $\|-0+1\rangle +$ $\|-1-0\rangle -$ $\|+1-1\rangle$	$\sqrt{\sigma_{z,1}}^{\dagger}\sqrt{\sigma_{x,2}}\sqrt{\sigma_{z,3}}^{\dagger}\sqrt{\sigma_{z,4}}^{\dagger}$ $SWAP_{3,4}\sqrt{\sigma_{x,1}}\sqrt{\sigma_{z,2}}^{\dagger}\sqrt{\sigma_{z,4}}^{\dagger}\|Box\rangle$ [51, 73]
	$\|+0+0\rangle +$ $\|+0-1\rangle +$ $\|-1-0\rangle +$ $\|-1+1\rangle$	$H_1H_2\|\psi\rangle$ [72]
	$\|+0+0\rangle +$ $\|+0-1\rangle +$ $\|-1-0\rangle +$ $\|-1+1\rangle$	$H_1H_2\|\psi\rangle$ [72]
	$\|+00+\rangle +$ $\|-01-\rangle +$ $\|-10-\rangle -$ $\|+11+\rangle$	$SWAP_{3,4}\sqrt{\sigma_{x,1}}\sqrt{\sigma_{z,2}}^{\dagger}\sqrt{\sigma_{z,4}}^{\dagger}\|Box\rangle$ [51, 73]

Table A.2.: Summary of the full set of four-qubit graph states, together with their quantum states and the needed transformations to generate them from the two possible states after the two qubit gate given by $|\psi\rangle$ and $|GHZ\rangle$ in equation (4.1) and (4.2).