



universität
wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

**„SPDC sources and their application in
quantum information including one-time
programs and flow ambiguity“**

verfasst von / submitted by

Stefan Zeppetzauer, BSc

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

Master of Science (MSc)

Wien, 2020 / Vienna, 2020

Studienkennzahl lt. Studienblatt /
degree programme code as it appears on
the student record sheet:

A 066 876

Studienrichtung lt. Studienblatt /
degree programme as it appears on
the student record sheet:

Masterstudium Physik UG2002

Betreut von / Supervisor:

Univ.-Prof. Dipl.-Ing. Dr. Philip Walther

Zusammenfassung

Die Erzeugung von Photonen mit maßgeschneiderten Eigenschaften ist von größter Bedeutung in der experimentellen Quantenoptik. Fast alle verwendeten Photonenquellen basieren heutzutage auf spontaner Fluoreszenz, durch die ein Photon in einem nichtlinearen Kristall spontan in zwei Photonen zerfällt. Mithilfe dieses Effektes lassen sich sowohl Einzelphotonenquellen als auch Quellen zur Erzeugung von verschränkten Photonenpaaren verwirklichen. In dieser Arbeit werden die Eigenschaften von verschiedenen, auf Fluoreszenz basierender, Photonenquellen beschrieben, sowie ihre Anwendung in zwei ausgewählten quantenoptischen Experimenten. Das erste Experiment stellt eine Anwendung der sogenannten blinden Quantendatenverarbeitung dar, in der ein Anwender ohne quantenmechanische Ressourcen eine Berechnung auf einen Server auslagert, der über große Quantenkapazitäten verfügt. Das Besondere dabei ist, dass der Server die Berechnung zwar ausführt, dabei aber keine Details über die Berechnung selbst erfährt. Er ist der Eingabe, der Durchführung und der Ausgabe gegenüber 'blind'. Das zweite Experiment beschäftigt sich mit Einmalprogrammen, die nach einmaliger Verwendung unbrauchbar und nicht kopiert werden können. Durch Eigenschaften der Quantenmechanik ist es möglich, diese Art von Programmen zu verwirklichen ohne die physische Zerstörung von Hardware. Abschließend werden die Vorteile einer gebrauchsfertigen Photonenquelle besprochen, die durch ihre einfache Handhabung ideal für quantenoptische Experimente in einem Laborpraktikum geeignet ist.

Abstract

The generation of photons with tailor-made properties is of paramount importance in experimental quantum optics. Almost all sources for photons nowadays are based on spontaneous fluorescence where a photon spontaneously decays into two photons in a nonlinear crystal. Using this effect single-photon sources as well as sources for the generation of entangled pairs of photons can be realized. This thesis describes the properties of different photon sources based on fluorescence and their application in two selected quantum optical experiments. The first experiment represents an application of so-called blind quantum computing, in which a client without quantum resources outsources a computation to a server providing large quantum capacities. While the server carries out the computation, it is oblivious to the details of the computation itself. The server is 'blind' to the input, the computation and the output. The second experiment deals with one-time programs that become unusable after a one evaluation and cannot be copied. Due to the properties of quantum mechanics, it is possible to implement this type of program without physically destroying hardware. Furthermore, the advantages of a plug-and-play photon source are discussed which, due to its simple handling, is ideally suited for quantum optical experiments in a laboratory course.

Contents

1	Introduction	1
2	Quantum optics	7
2.1	Basic Concepts of Quantum Mechanics	7
2.1.1	Single-qubit states	7
2.1.2	No-cloning theorem	9
2.1.3	Bloch sphere	10
2.1.4	Polarization qubits	11
2.1.5	Two-qubit states	12
2.1.6	Bell inequality	14
2.2	Spontaneous Parametric Down-Conversion Photon Sources	17
2.2.1	Laser sources	17
2.2.2	Second-order coherence function	21
2.2.3	Spontaneous parametric down-conversion	24
2.2.4	Quasi phase-matching	35
2.2.5	Application: single-photon source	39
2.2.6	Application: Entangled photon pair source	40
2.3	Linear optical components	40
2.3.1	Beam splitters	41
2.3.2	Polarizing beam splitters	44
2.3.3	Linear absorbing polarizer	44
2.3.4	Waveplates	46
2.4	Single-photon detectors	51
2.4.1	Single-photon avalanche diodes	52
2.4.2	Superconducting nanowires	53
3	Blind quantum computing with a classical client	57
3.1	Quantum Information Theory	58
3.2	Measurement-based quantum computing	62
3.3	Classically Driven Blind Quantum Computing	69
3.4	Experimental setup	74
4	Commodity-based one-time programs	81
4.1	Oblivious Transfer and One-time Programs	81

4.2	One-time programs using quantum entanglement	83
4.3	Experimental setup	91
4.4	Application: One-time digital signature	91
5	SPDC source in a lab course	95
5.1	Qutools Entanglement Demonstrator	95
5.2	Quantum state tomography	96
5.2.1	Single-qubit tomography	98
5.2.2	Multi-qubit tomography	100
5.2.3	Maximum likelihood estimation	101
5.2.4	Fidelity and purity	102
5.3	Hong-Ou-Mandel interference	102
6	Conclusion	109
	Bibliography	113

Introduction

Quantum theory has revolutionized our understanding of Nature. Counterintuitive properties such as the superposition of physical systems and the apparent instantaneous communication of correlated quantum systems were explored in the 1930s in famous thought experiments including Schrödinger's cat [1] and the Einstein-Podolsky-Rosen paradox [2]. Experiments realizing the superposition of electrons in 1961 [3, 4] and the demonstration of entanglement in 1967 [5, 6] established quantum theory as a theory of how Nature behaves on a fundamental level. Additionally, technological breakthroughs such as the invention of the laser [7] and the transistor [8] were made possible by employing the laws of quantum theory. In the following years, the principles of quantum theory were tested with increasingly sophisticated experiments and existing technologies benefited from advances in quantum research, which in turn lead to further improved experiments. Soon, physicists began to wonder whether principles of quantum theory could be used to implement fundamentally new technologies and concepts not possible with merely classical physics. First ideas for quantum algorithms and quantum cryptography protocols [9–12] showed the potential of using quantum objects and their properties as resources. In information theory, it has been suggested that quantum algorithms may result in significant speedups compared to classical algorithms, for example for the factoring of large numbers [13], the search in unordered lists [14] or the simulation of quantum systems [15].

One of the main challenges to realize these quantum algorithms the isolation of the quantum system from unwanted environmental influences. On the other hand, this susceptibility to disturbances also allows the reliable detection of malicious third parties in cryptographic protocols. For example, the Ekert91 protocol [16] employs the nonclassical threshold given by the Bell inequality to test for the security of a quantum channel. A main advantage in quantum cryptography is that the security is not guaranteed by technological means but rather by the laws of nature themselves. Quantum theory enables protocols that are secure even in the face of an adversary with unlimited resources - quantum or otherwise. In this type of quantum cryptography protocol, known as quantum key distribution (QKD), the scenario assumes two friendly parties, usually named Alice and Bob, who want to securely exchange information, for example an access key or a private message. They combine their knowledge and resources to keep a malicious eavesdropper, known

as Eve, from intercepting the transmitted information. Depending on the premise, Eve has more or less options to gain access to the information without Alice and Bob noticing, however, Alice and Bob can always find a way to guarantee a secure communication.

The protocols discussed in this thesis deal with the premise of Alice and Bob not trusting each other nor any intermediary. Each party is potentially malicious and might try to cheat during the protocol to gain an advantage. Nevertheless, they both rely on a joint resource to accomplish a certain task. Therefore, they work together but at the same time try to exchange only the bare minimum of information necessary for the completion of the task. This is a common scenario in our every-day lives: we need banks to manage our money and give us access to it when we need it. We store data on the servers of companies and expect them to keep it private. If we need to conduct computations that are too computationally intensive for a personal computer, we have to delegate the computation to a more powerful computer not under our purview. In all of these cases, we rely on the discretion of the supplier of the resource. We have to trust the bank to not steal our money, we trust the server company to not leak our data and we trust the computation provider not to steal the results of our computation. We rely on them, knowing that bank accounts can get hacked and private data gets stolen regularly. In most of these cases, the failure in security lies at the end of one of the active parties. Every time we exchange access keys or rules about how to construct a security measure, there is a chance that a malicious party at the other end takes the information to gain knowledge about our data or program. In a classical world, we would have to accept and live with these insecurities forever. However, employing the laws of quantum theory opens up possibilities to exchange messages with or use the resources of a non-trustworthy party without leaking essential information.

Quantum theory enables us to let someone run our program without providing access to the program itself. If we want to implement a secret quantum computation but do not have one ourselves, we can delegate the computation to a quantum server without ever telling the server what he is actually computing [17]. Here, we discuss implementations of both of these premises. The first application is realized using one-time programs, which are functions that allow for one input by a user but cannot be used a second time [18, 19]. All the while, the structure of the program is hidden from the user. This is primarily possible due to a fundamental property of quantum theory: the measurement outcome of a quantum state in a superposition of the measurement basis cannot be predicted with certainty [20, 21]. The second application has gained traction since the first quantum cloud processors have been opened to private users [22–24]. Blind quantum computing is a premise that allows a user to implement a computation on a quantum computer without the server knowing the computation conducted [18]. This feature, which sounds

impossible at first, is again enabled employing the inherently random outcome of the measurement of a quantum state. While quantum technology is still in its infancy, vast improvements in the implementations have been made in the last few years. This is possible due to the improvement of existing and the development of new technologies, a large part of which addresses the performance of the physical system used to encode the basic unit of information in quantum computing, the qubit.

While qubits encoded in the electronic spin [25–27], in the nuclear spin [28–30] or in the degrees of freedom of Josephson junctions [31, 32] are becoming more and more feasible, photonic qubits remain one of the top contenders in quantum information and quantum cryptography. Linear optical components such as waveplates and beam splitters allow the manipulation of photons to a high precision, and detection systems based on semiconductors or superconducting wires can detect single photons with high probability [33]. On the other hand, the generation of photons leaves room for improvements in various regards.

Today, the vast majority of quantum optical experiments rely on a process called spontaneous parametric down-conversion (SPDC) where a single incident photon is split in two daughter photons of lower frequency [34]. SPDC sources can be used to create single photon states [35] (making use of a special technique) and entangled photon pairs [36] used as basic resource in countless experiments. Since the Knill-Laflamme-Milburn (KLM) scheme turned photonic qubits into viable candidates for universal quantum computing [37], much attention has been given to the improvement of SPDC sources. While current SPDC sources offer a wide wavelength range, high photon count rates and high versatility despite requiring low resources and low maintenance, more and more research is focused on the development of alternatives. Technologies such as quantum dots [38–40] and NV centers [41] are potential candidates for natural single-photon source but, apart from requiring careful and resource-intensive preparation, they still need improvements in order to take over the primary role of single-photon sources. While these sources gradually take over state-of-the-art research labs, many applications continue to be based on the tried- and true technology of SPDC in the foreseeable future. All the experiments discussed in this thesis are based on such sources, and while they all rely on the same process for the generation of photons, each source is built differently, providing different advantages and properties.

The goal of this thesis is to give an overview of the applicability of SPDC sources in different quantum technology protocols as well as an example for their use for educational purposes. It will be shown that while having inherent drawbacks, SPDC sources are still extremely powerful and versatile sources of photons for a wide variety of applications. As a first example of the main topic of this thesis, Figure 1.1 depicts a possible architecture of an SPDC source. The heart of the source is a nonlinear BBO-crystal pumped by a continuous-wave laser at 780nm. For each

pump photon entering the crystal, there is a small chance that spontaneous down-conversion occurs, splitting the pump photon into two photons of half the frequency, referred to as signal and idler photons. In this example, the generated photons are orthogonally polarized and exit the crystal in overlapping emission cones. After emission from the BBO crystal, the photons traverse a half-wave plate which switches the polarization state and are then spatially separated by two prism mirrors. In the path of each photon, a second BBO-crystal of half the length of the main crystal is placed. In combination with the aforementioned waveplate, the crystals cancel out dispersive effects caused by the birefringent nature of the BBO that would reduce the coherence of the photons. Additionally, frequency filters are placed in each path to further increase the quality of the entanglement and block residual pump light. Finally, signal and idler photon are collected into a single-mode fibers which act as spatial filters and guide the photons to the subsequent parts of the experiment. In any case, after the desired operations have been implemented, the final properties of the photons are measured which, for photons, corresponds to the absorption in a single-photon detector. Apart from the source technology, the overarching premise of this thesis is the mistrust between the two communicating parties, Alice and Bob, as discussed above. Using SPDC sources, optical components and single-photon detectors, the two can implement various protocols together without ever having to resolve their trust issues.

The thesis is structured as follows: In **Chapter 2**, the fundamentals of quantum optics are introduced, starting with single-qubit states, a graphical representation and the polarization degree of freedom to encode quantum information in photons. Subsequently, the creation, manipulation and detection of photonic qubits in a laboratory will be described, including the main topic of this thesis, SPDC. **Chapter 3** deals with qubits as information carrier in quantum information theory. Measurement-based quantum computing (MBQC) [42] is introduced, along with one of its main applications, blind quantum computing (BQC) [18]. Based on this, the theory and experimental implementation of a new protocol of blind quantum computing is discussed, dealing with the interaction between a classical client and a universal quantum server. This protocol, known as classically-driven blind quantum computing (CDBQC) [43], retains partial blindness for the server while shifting the required quantum resources away from the client. The second protocol of this thesis is described in **Chapter 4**: Quantum theory provides advantages to one-time programs, functions that can be evaluated for only one input. The protocol is split into two communication phases, one wholly quantum and the other entirely classical. Finally, in **Chapter 5** a new kind of plug-and play SPDC source is used to implement some of the most fundamental experiments in quantum optics. Here, two examples are given, namely the reconstruction of the density matrix for a given quantum state and the generation of indistinguishable photons and the verification

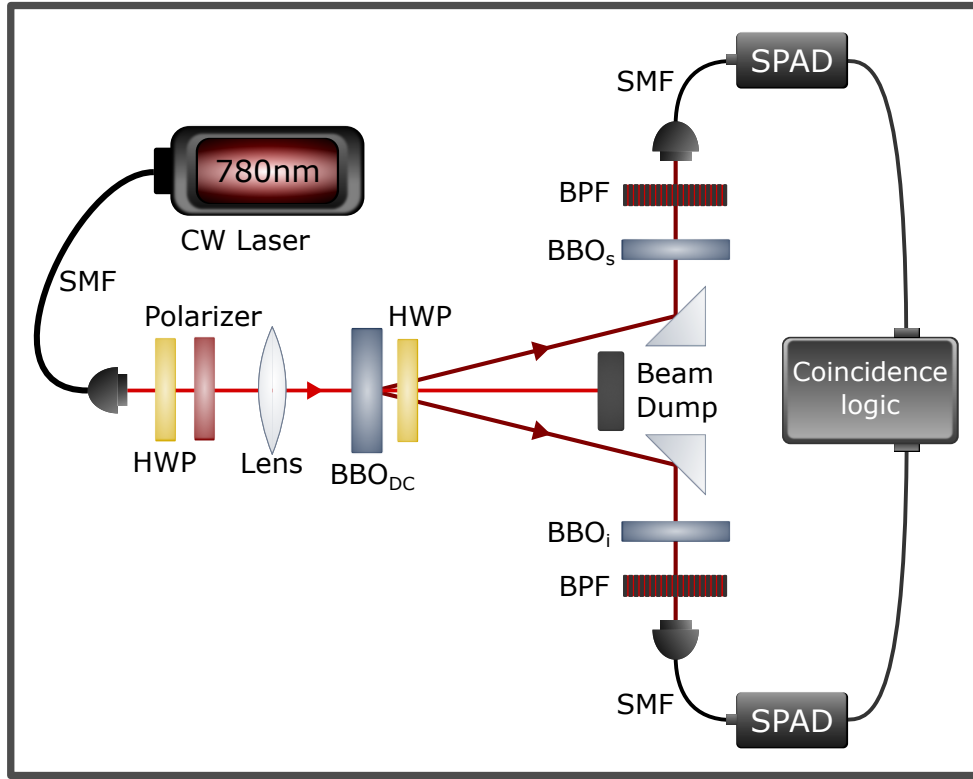


Fig. 1.1: Example for an SPDC source design: a pump beam emitted by a continuous-wave laser at 780nm is coupled to a single-mode fiber (SMF). The power of the pump beam is tuned using a half-wave plate (HWP) in combination with a linear polarizer. A convex lens focusses the laser beam to the center of a nonlinear beta barium borate crystal (BBO_{DC}) where pump photons are spontaneously split in pairs of daughter photons via SPDC. The generated photons are orthogonally polarized and emitted in overlapping cones. Photons collected from the intersection points denoted by the red arrows show non-classical correlations. Prism mirrors are used to spatially separate photons from the two intersection points. Due to birefringent effects in the crystal, a half-wave plate after the BBO is used to exchange the polarization of the daughter photons. In combination with BBO_s and BBO_i which are half the thickness of BBO_{DC} , these effects can be compensated to a high degree. Bandpass filters (BPF) are used to filter scattered pump light and to spectrally post-select the generated photons. Both photons are coupled into SMFs which are connected to single-photon avalanche diodes (SPAD). Coincidence events in both detectors are noted in the coincidence logic (e.g. a field programmable gate array (FPGA)). The source can be used as a heralded single-photon source or a source for entangled photon pairs. To analyze the polarization properties of the generated state, additional polarizers have to be placed in front of the SMFs.

via Hong-Ou-Mandel interference. The thesis is concluded with a comparison of the most important properties of the different SPDC sources introduced.

Quantum optics

In this Chapter, basic concepts of quantum mechanics applied to light are introduced. Quantum optics emerged as its own field in the 1950s, following research into coherence of light [44] and the invention of the laser [7]. The improvement of lasers, optical components and detectors in the following decades allowed for more and more sophisticated experiments using quantum states of light. Many remarkable results were achieved in experimental quantum optics in the 1990s and the early 2000s, including the realization of quantum teleportation [45], entanglement swapping [46] and two-qubit logic gates [47–49]. Today, quantum optics is a diverse field of research including fundamental research as well as the investigation of quantum technologies. The comparably simple manipulation of photonic qubits allows for the implementation of a large amount of proposals using a handful of types of components for the most parts. In the following, we start by introducing single-qubit states, including their general properties and their graphical representation on the Bloch sphere. We then briefly discuss polarization-qubits since all qubits employed in this thesis are of this type. Related, we define states of multiple qubits and introduce the concept of entanglement including tests of entanglement in the form of Bell inequalities. The final part of the Chapter discusses the creation, manipulation and detection of single- and two-qubit states, in theory as well as in an experiment. This includes the basic working principles of lasers, nonlinear optics and SPDC, the properties of linear optical components and the detectors used to measure single photons.

2.1 Basic Concepts of Quantum Mechanics

2.1.1 Single-qubit states

In quantum mechanics, a physical system is completely described by a state Ψ represented by a ray in a separable Hilbert space \mathcal{H} . Using Dirac's ket notation, a ray is defined by $\{e^{i\phi}|\Psi\rangle \mid \phi \in \mathbb{R}\}$, i.e. the equivalence class of vectors differing by multiplication with a complex scalar $e^{i\phi}$. Choosing a representative of the class, denoted by $|\Psi\rangle$ and with unit norm $\langle\Psi|\Psi\rangle = 1$, states can be represented by

normalized vectors and overall (global) phases $e^{i\phi}$ are of no physical significance for $|e^{i\phi}| = 1$. A quantum system evolves unitarily in time, described by

$$|\Psi(t)\rangle = \hat{U}(t) |\Psi(t=0)\rangle \quad (2.1)$$

where $\hat{U}(t)$ is a unitary operator, i.e. a bounded linear map $\hat{U} : \mathcal{H}^d \rightarrow \mathcal{H}^d$ in d dimensions satisfying $\hat{U}(t)^\dagger \hat{U}(t) = \hat{U}(t) \hat{U}(t)^\dagger = \mathbb{1}$. Every state of a finite d -dimensional quantum system can be decomposed into a linear superposition of a set of vectors $\{\phi_i\}$ spanning \mathcal{H} , giving

$$|\Psi\rangle := \sum_{i=1}^d \lambda_i |\phi_i\rangle \quad (2.2)$$

where λ_i are complex amplitudes normalized to $\sum_{i=0}^d |\lambda_i|^2 = 1$. The probability to measure and find the system in state $|i\rangle$ is then given by $|\lambda_i|^2$ using equation 2.2. Note that if the elements of $\{\phi_i\}$ spanning \mathcal{H} are linearly independent, they form a basis for the space. Properties of the state that can (in principle) be measured are called observables and realized by Hermitian operators $\hat{A}^\dagger = \hat{A}$ for \hat{A} bounded. Hermitian operators in a Hilbert space \mathcal{H} have a spectral representation in \mathcal{H} , i.e. their eigenstates form a complete orthonormal basis. The observable can therefore be represented as

$$\hat{A} = \sum_{m=1}^d \lambda_m M_m \quad (2.3)$$

where λ_m are the eigenvalues of \hat{A} and M_m are the corresponding orthogonal projection operators onto the space of eigenvectors with eigenvalue λ_m . Projective operators are orthogonal and Hermitian and can be expressed as

$$\hat{M}_m = |m\rangle \langle m| \quad (2.4)$$

where $\{m\}$ is the orthonormal basis of eigenstates of \hat{A} . When applying \hat{M}_m to $|\Psi\rangle$ the measurement result m occurs with a probability p given by the square absolute value of the overlap

$$p(m) = \langle \Psi | \hat{M}_m | \Psi \rangle \quad (2.5)$$

To conclude, an observable gives information about the probability distribution of the measurement outcomes, a projector gives the outcome of a single measurement of the corresponding observable. In the following we will specifically deal with state vectors describing two-level systems, i.e. qubits

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2.6)$$

for $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$, and therefore focus our discussion on these states. The measurement operators which span a complete orthonormal basis of observables in two-dimensional Hilbert space are the (unitary Hermitian) Pauli operators¹

$$\hat{\sigma}_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{\sigma}_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{\sigma}_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (2.7)$$

with eigenstates

$$\begin{aligned} |\Psi_{x+}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & |\Psi_{x-}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ |\Psi_{y+}\rangle &= |+_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) & |\Psi_{y-}\rangle &= |-_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \\ |\Psi_{z+}\rangle &= |0\rangle & |\Psi_{z-}\rangle &= |1\rangle \end{aligned} \quad (2.8)$$

where the subscripts $A\pm$ denote the eigenvalue ± 1 , respectively. Having established the fundamental rules of how to describe the states, time evolution and measurement of a quantum system, we can already state one of the most fundamental rules of quantum theory:

2.1.2 No-cloning theorem

The no-cloning theorem [50] is one of the most important properties of quantum theory, in particular for the following protocols. It states that arbitrary quantum states cannot be perfectly copied. Suppose there exists a unitary operator $\hat{U}_c(t)$ that acts on a qubit $|\Psi\rangle_1$ and a qubit in an initial state $|i\rangle_2$ such that $|\Psi\rangle_1 |i\rangle_2 \xrightarrow{\hat{U}_c(t)} |\Psi\rangle_1 |\Psi\rangle_2$. However, due to the linearity of quantum mechanics

$$\begin{aligned} \hat{U}_c(t) |\Psi\rangle_1 |i\rangle_2 &= \alpha \hat{U}_c(t) |0\rangle_1 |i\rangle_2 + \beta \hat{U}_c(t) |1\rangle_1 |i\rangle_2 \\ &= \alpha |0\rangle_1 |0\rangle_2 + \beta |1\rangle_1 |1\rangle_2 \end{aligned} \quad (2.9)$$

which is an entangled state and different from $|\Psi\rangle_1 |\Psi\rangle_2$ except for $|i\rangle = |\Psi\rangle$ or $|i\rangle \perp |\Psi\rangle$. Therefore, cloning an arbitrary unknown quantum state is not possible. While this makes error correction in quantum computing impossible with classical schemes (where bits are copied to reduce the error rate), the no-cloning theorem is the fundamental principle preventing eavesdroppers from copying transmitted quantum information. Moreover, the no-cloning theorem is essential for the uncertainty principle and prevents superluminal communication with entangled states.

¹while in most of quantum mechanics, the notation $\hat{\sigma}$ is common for the Pauli matrices, in quantum information theory the Pauli matrices correspond to single-qubit gates denoted as X, Y, Z

2.1.3 Bloch sphere

An important geometric tool for the graphical representation of qubit state vectors is the Bloch sphere depicted in Figure 2.1a. The two-dimensional Hilbert space \mathcal{H}^2 and the Bloch sphere have a one-to-one correspondence meaning every element of \mathcal{H}^2 can be represented by a point on the sphere: Qubits are points on the surface of the unit sphere, their position can be determined by the polar coordinates θ and ϕ

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \quad (2.10)$$

where $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$. This representation of the qubit state vector in spherical polar coordinates is called the Bloch vector. Orthogonal elements of \mathcal{H}^2 are represented by antipodal points on the sphere, e.g. the eigenstates of the Pauli operators which are located at the poles of the sphere. Applying a Pauli operator $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ to a single-qubit state rotates the state by π about the x, y, z -axis, respectively and up to a global phase. To restore the original state, $\hat{\sigma}_x$ needs to be applied two more times making the Bloch sphere 4π -symmetric which is significant if the phase is relative between two qubits. In general, every single-qubit unitary corresponds to a rotation $\hat{R}_{\hat{n}}(\theta)$ around an axis $\hat{n} = (n_x, n_y, n_z)$ on the Bloch sphere. Furthermore, $\hat{R}_{\hat{n}}(\theta)$ can be decomposed into a linear combination of the Pauli operators and the identity in terms of

$$\begin{aligned} \hat{R}_{\hat{n}}(\theta) &= \exp\left(-\frac{i\theta\hat{n} \cdot \sigma}{2}\right) \\ &= \cos\left(\frac{\theta}{2}\right)\mathbb{1} - i\sin\left(\frac{\theta}{2}\right)(n_x\hat{\sigma}_x + n_y\hat{\sigma}_y + n_z\hat{\sigma}_z) \end{aligned} \quad (2.11)$$

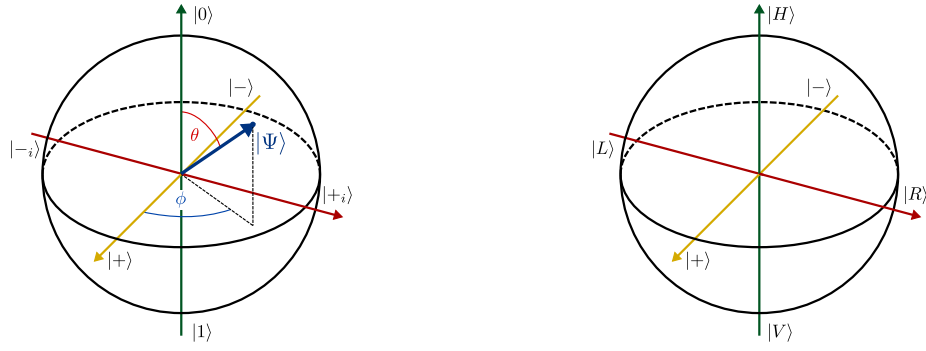
where $\sigma = (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)^\top$ [51]. Therefore, an arbitrary single-qubit state can be continuously rotated into any other single-qubit state by applying a unitary single-qubit operator. Using $e^{\theta\hat{A}} = \cos(\theta)\mathbb{1} + \sin(\theta)\hat{A}$ for $\hat{A}^2 = \mathbb{1}$, we can express rotations about the x -, y -, and z -axis in terms of rotation matrices

$$\hat{R}_x(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -i\sin\left(\frac{\theta}{2}\right) \\ -i\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}, \quad \hat{R}_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}, \quad \hat{R}_z(\theta) = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \quad (2.12)$$

Since $\hat{R}_{\hat{n}}(\theta)$ can rotate any single-qubit state into any other single-qubit state up to a global phase, we can define an arbitrary single-qubit unitary operator as

$$\hat{U} = \exp(i\gamma)\hat{R}_{\hat{n}}(\theta) \quad (2.13)$$

for angles γ and θ . From this operator, all single-qubit unitaries used in this thesis can be directly derived by choosing appropriate unit vectors \hat{n} and angles. Furthermore,



(a) Bloch sphere

(b) Poincaré sphere

Fig. 2.1: (a) **Bloch sphere to represent single-qubit states.** The sphere is spanned by the eigenstates of the Pauli matrices, antipodal states are mutually orthogonal. Qubit states can be written in the Bloch sphere representation as $|\Psi\rangle = \cos \theta/2 |0\rangle + e^{i\phi} \sin \theta/2 |1\rangle$ where $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$. (b) **Poincaré sphere to represent single polarization-qubit states.** The states representing for linear, diagonal and circular polarization are located at the poles. Apart from the notation and the name, the representation of a qubit state on the Poincaré sphere is identical to the representation on the Bloch sphere which is why the names are often used synonymously.

we denote measurement operators that project a state on the eigenstates of the Pauli operators, located on the x -, y - or z -axis of the Bloch sphere, by

$$\begin{aligned}\hat{\sigma}_x : \hat{M}_{\pm \hat{n}_x} &= |\pm\rangle \langle \pm| \\ \hat{\sigma}_y : \hat{M}_{\pm \hat{n}_y} &= |+_i\rangle \langle -_i| \\ \hat{\sigma}_z : \hat{M}_{\pm \hat{n}_z} &= |0/1\rangle \langle 0/1|\end{aligned}\tag{2.14}$$

Depending on the type of qubit, different methods have to be applied to implement unitary operations and measurements. Since in this thesis, the same type of photonic qubits are used for all experiments, we are going to introduce their most important properties in the following.

2.1.4 Polarization qubits

In general, various physical two-level systems can be used to encode qubits (atoms [52, 53], electrons [54, 55], Josephson junctions [31, 32]), some more suitable for specific tasks than others. Here, qubits encoded in the polarization degree of freedom of photons will be used for all applications. While photons offer several degrees of freedom that can be used to encode quantum information (frequency, orbital angular momentum, arrival time), polarization-encoding is especially useful since single-qubit unitary operators can be implemented using standard optical elements

such as wave plates, beam splitters and polarizers. Due to the particle-wave duality, we can assign a polarization state to a photon according to the oscillation of the electromagnetic field. In analogy to classical optics, the polarization can be linear, diagonal or circular. We assign polarization states to corresponding computational qubit states defined in 2.8 to get

$$\begin{aligned} |H\rangle &\equiv |0\rangle & |V\rangle &\equiv |1\rangle \\ |D\rangle &\equiv |+\rangle & |A\rangle &\equiv |-\rangle \\ |R\rangle &\equiv |+_i\rangle & |L\rangle &\equiv |-_i\rangle \end{aligned} \tag{2.15}$$

where A (D) denote the (anti-) diagonal and R (L) the right- (left-) handed polarization states. We can therefore treat polarization-qubits as eigenstates of the Pauli operators as described before. Furthermore, this tells us that these polarization states are enough to form a complete basis in two-dimensional complex Hilbert space giving a full representation of any polarization state possible.

In experiments, polarization qubits are remarkably convenient in contrast to many other qubits for several reasons: as mentioned, they can be manipulated using classical polarization manipulation technology that has been explored and refined for centuries. Secondly, photons as having neither charge nor mass only couple weakly to the environment making it possible to transmit them through air with limited loss of coherence or absorption (satellite QKD). Qubits such as atoms or superconducting qubits have to be isolated in vacuum chambers resulting in expensive and sophisticated setups. At last, for selected wavelength regimes, highly efficient single-photon detectors make the detection of photons comparably convenient. As for all things, these advantages come with drawbacks: one of the most prevalent drawbacks of photonic qubits is the complicated creation of entangled states and nonlinear gates for quantum computing. Photons do not interact directly up to first order since they are electrically neutral and second-order interactions only occur at high energies through the creation and annihilation of virtual particle-antiparticle pairs [56]. Since these energies are not easily accessible in an optical laboratory, experimentalists have to resort to different means such as nonlinear crystals and probabilistic gates. Despite these problems, photons are still the most versatile, robust and easiest-to-set up system for the implementation of qubits.

2.1.5 Two-qubit states

The states discussed up until now describe a single two-level system. When describing composite systems made up of several individual subsystems, for example systems

consisting of several qubits, the multi-partite state for two qubits 1 and 2 can be expressed as

$$|\Psi\rangle_{12} := \alpha |0\rangle_1 |0\rangle_2 + \beta |0\rangle_1 |1\rangle_2 + \gamma |1\rangle_1 |0\rangle_2 + \delta |1\rangle_1 |1\rangle_2 \quad (2.16)$$

in a bipartite Hilbert space $\mathcal{H}_{12} = \mathcal{H}_1 \otimes \mathcal{H}_2$ where $\{00, 01, 10, 11\}$ is the computational two-qubit basis, $\{\alpha, \beta, \gamma, \delta\}$ are complex amplitudes and \otimes is the tensor product. If a bipartite state can be written as a tensor product of the individual subsystems 1 and 2 as

$$|\Psi\rangle_{12} = |\Psi\rangle_1 \otimes |\Psi\rangle_2 \quad (2.17)$$

the state is called separable. However, since the Hilbert space is linear, it also contains superpositions of states such as $|00\rangle + |11\rangle$. These states can't be decomposed into a tensor product of their subsystems, i.e. $|\Psi_{ab}\rangle \neq |\Psi_a\rangle \otimes |\Psi_b\rangle$. These states are called nonlocal or entangled and give rise to quantum phenomena that cannot be described using classical theories². For the applications discussed here, we are most interested in the four pure maximally entangled two-qubit states known as the Bell states:

$$\begin{aligned} |\Psi^\pm\rangle &:= \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle) \\ |\Phi^\pm\rangle &:= \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle) \end{aligned} \quad (2.18)$$

which, amongst other properties, form an orthonormal basis for the four-dimensional Hilbert space. The singlet state $|\Psi^-\rangle$ (spin quantum number 0) is of significant importance since it is isotropic with respect to rotations around an angle θ , i.e. it looks the same in any basis rotated by θ respective to $|0\rangle$. This makes the $|\Psi^-\rangle$ oftentimes the go-to state for experiments, especially since Bell states can be transformed into any other Bell state by local unitary transformations.

Projective operators acting on two-qubit states are generated from single-qubit operators $\hat{M}_{m_{12}} = \hat{M}_{m_1} \otimes \hat{M}_{m_2}$ and applied in the same way such that $p(m) = {}_{12}\langle\Psi|\hat{M}_{m_{12}}|\Psi\rangle_{12}$. Single-party measurements are equivalent to applying the projection operator on the bipartite state: $|\Psi\rangle_{m_2} = (\hat{M}_{m_1} \otimes \mathbb{1})|\Psi\rangle_{12}$ where $|\Psi\rangle_2$ is the reduced output state. If $|\Psi\rangle_{12}$ was an entangled state, local measurement of one subsystem immediately collapses the remaining subsystem into a well-defined local quantum state independent of the distance between the parties holding the qubits 1 and 2. These correlations hold not only in the basis the state was prepared in (which would be explainable with classical probability theory) but in any basis such as the $\{+, -\}$ basis. In this case the qubit gets projected onto either the state $+$ or $-$ with a probability of 50%. Which state it is, however, is probabilistic and only decided in the instant of the projection. Nevertheless, as soon as Alice measures

²For the most part from now on, we are going to suppress the indices describing the individual subspaces 1 and 2 for better readability)



Fig. 2.2: Schematics for a Bell-type experiment. A source located in the center distributes particles to Alice on the left and Bob on the right. Both parties are equipped with a suitable detector which can be set to measure one of two properties \hat{A}, \hat{A}' and \hat{B}, \hat{B}' of the particle. Alice and Bob can freely choose their setting but are not allowed to communicate. Every time the detector measures, it gives out a binary output ± 1 depicted by the two light bulbs at the side of the detector. After the experiment, Alice and Bob compare their results and compute the correlation parameter C . If the measured particles are at most classically correlated, $|\langle C \rangle|_{\text{Cl}} = 2$. If the source emits maximally entangled particles, $|\langle C \rangle|_{\text{QT}} = 2\sqrt{2}$, violating the classical bound.

+, Bob will always measure – independent of distance, and vice versa. This seemingly instantaneous communication between two separated parts of an entangled state are perhaps the most peculiar feature of quantum theory and gave rise to the well-known EPR paradox in 1935 [2]. In essence, if quantum theory is to be considered complete, it cannot be both realistic and local. Realistic in the sense that the properties of the constituent parts of the system are in some sense deterministic to measurement and local in the sense that manipulation of a subsystem at place A should not instantaneously influence the properties of subsystem B at a spacelike separated location. Since both assumptions are very intuitive and dropping them would mean to break with two very fundamental properties of reality, a solution was to assume that quantum theory is incomplete and there exist local hidden variables, properties of the system not accessible by a quantum treatment. This would render quantum theory incomplete and keep the assumptions of local realism intact.

2.1.6 Bell inequality

In 1964, John S. Bell formulated an inequality that assigns an upper bound to correlations and should be obeyed by all local realistic theories [20]. In Bell's original paper, perfect anticorrelation is assumed for the measurement outcomes. Since this is impossible to realize experimentally, a more general version of Bell's inequality is used for experiments, introduced in 1969 by Clauser, Horne, Shimony and Holt [57]: In the scenario, two parties, Alice and Bob, share a bipartite state distributed by a source. Each party can choose to measure one of two observables we denote by \hat{A}, \hat{A}' for Alice and \hat{B}, \hat{B}' for Bob. The observables can take the values $\{\pm 1\}$ and are assumed to be functions of some hidden variable. Alice and Bob are not allowed to communicate which can be guaranteed by spacelike separation. From the possible outputs of the observables, we can see that either $\hat{A} + \hat{A}' = 0$ and

therefore $\hat{A} - \hat{A}' = \pm 2$ or else $\hat{A} - \hat{A}' = 0$ and $\hat{A} + \hat{A}' = \pm 2$. Using this, we can define the correlation parameter

$$C := (\hat{A} + \hat{A}')\hat{B} + (\hat{A} - \hat{A}')\hat{B}' = \pm 2 \quad (2.19)$$

The assumption for local hidden variables (LHV) is implicit in this definition since we assume that $\{\pm 1\}$ can be assigned to all four observables even though it is impossible to measure both \hat{A}, \hat{A}' and \hat{B}, \hat{B}' . Taking a series of measurements, the absolute of the expectation value of C is bounded by

$$|\langle C \rangle|_{\text{Cl}} = |\langle \hat{A}\hat{B} \rangle + \langle \hat{A}'\hat{B} \rangle + \langle \hat{A}\hat{B}' \rangle - \langle \hat{A}'\hat{B}' \rangle| \leq 2 \quad (2.20)$$

since $|\langle C \rangle| \leq \langle |C| \rangle_{\text{Cl}} = 2$. It was first shown in 1972 that this bound can be violated if Alice and Bob share an entangled state, for example a Bell state [6]. For a long time, it was not clear if this violation is inherent in quantum theory or if it is merely a product of flaws in the experimental design. For example, the detection loophole addresses the problem arising from imperfect detectors: Since only a subsample of all emitted pairs is detected, the whole sample might result in random outcomes while the quantum correlations detected are the result of LHV combined with specific detector settings. If the measuring parties are not spacelike separated, the detector on one side might communicate with the other detector, somehow influencing the results. This is known as the communication loophole. In the years following the first experimental demonstration, numerous experiments were designed and conducted to close these and other loopholes. Eventually, three groups reported loophole-free Bell tests all violating Bell's inequality in 2015, showing that quantum theory cannot be described by LHV theories [58–60]. It is important to understand that, while quantum entanglement allows for stronger correlations than expected in LHV theories, it does not allow for faster-than-light communication since Alice has no way to know the random measurement outcome on Bob's side and therefore no way to transmit this information to Bob. This becomes apparent in the fact that, would Alice and Bob reconstruct the their part of the state on their side they would get a maximally mixed state. The condition of no faster-than light communication is called 'no-signalling' and is implicit in the formulations of Bell's inequalities in the sense that Alice's measurement settings does not influence Bob's settings and vice versa. Using correlations obtained from measurements on entangled states, there exists a maximum violation of Bell's inequality, known as Tsirelson's bound and given by

$$|\langle C \rangle|_{\text{QT}} \leq 2\sqrt{2} \quad (2.21)$$

Approximate equality can be achieved by using maximally entangled states and specific measurement angles. Remarkably, Tsirelson's bound is not the algebraic upper bound of 2.20, which is given by $|\langle C \rangle|_{\text{Alg}} = 4^3$. This discrepancy has inspired

³Note that $|\langle C \rangle|$ is discontinuous from $2\sqrt{2}$ to exactly 4

researchers to look for more generalized probability theories that include quantum theory as a special case while still obeying no-signalling (see, for example PR-boxes in [61–63]).

CHSH Game

In the context of quantum information theory, the CHSH inequality and Tsirelson's bound is often introduced via an alternative approach called the CHSH game. Here, a referee distributes two input bits $\{0, 1\}$ and sends one to Alice and the other one to Bob. After receiving their bits, Alice and Bob both produce an output bit and send it back to the referee who compares the results. If a certain condition is fulfilled, Alice and Bob win the game, otherwise, they lose. The CHSH inequality can then be expressed in terms of the winning probabilities for the different configurations of the game and is given by

$$\langle p \rangle_{\text{Cl}} \leq \frac{3}{4} = 0.75 \quad (2.22)$$

This is the classical upper bound of the CHSH inequality introduced above. Again, it can be shown that if Alice and Bob receive one part of an entangled state, the classical winning probability can be surpassed. Specifically, the winning probability when using entanglement results to

$$\langle p \rangle_{\text{QT}} \leq \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.853 \quad (2.23)$$

The upper bound of 0.853 is simply Tsirelson's bound in the context of the CHSH game. The advantages that can be gained by employing quantum entanglement are diverse and powerful. For this reason, entangled quantum states have become fundamental resources in the development of quantum technologies. It is used to teleport information from qubit to qubit in measurement-based quantum computing or shared between parties to enable universally secure communication in QKD. The CHSH inequality, as a fundamentally valid proof of non-classicality, is commonly employed to verify the presence of entanglement or to detect eavesdroppers in a private channel.

For the applications discussed in the following sections, photonic qubits will be the constituents of the entangled states. While entanglement between photons is robust, the practical creation of entanglement is one of the main challenges in today's experimental quantum optics, especially if one wants to create higher-dimensional entangled states such as the three-photon GHZ state. In the following section, we will describe SPDC, one of the best-developed techniques to create polarization entanglement in the lab, followed by a description of some of the most important optical components to apply unitary operations to photonic qubits. Following that,

we will conclude with the implementation of measurements on single- and multi-qubit systems.

2.2 Spontaneous Parametric Down-Conversion Photon Sources

2.2.1 Laser sources

For many applications in classical as well as quantum optics including SPDC, a basic necessity are sources of spatially and temporally coherent light. Spatial coherence means that two points of the wave can interfere with each other while temporal coherence means that a wave can interfere with itself in different points in time. When the first laser (light amplification by stimulated emission of radiation) was built in 1960 [7], it was regarded as a curiosity with no apparent applications. Nowadays, since for many effects in (quantum) optics interference of wave(-functions) is a prerequisite necessary for many secondary effects (e.g. nonlinear effects and multiphoton interference), lasers are one of the fundamental building blocks of any photonic experiment. Apart from providing the light source from which the photonic states are created, lasers are crucial for manipulation and readout of photonic systems. Here, we are going to give a basic overview of the working principle of laser diodes and optical amplifiers which, in combination, make up the basic source used in the following experiments to create continuous highly monochromatic, coherent light.

Laser diodes

In almost all modern solid-state laser sources, the light pumping the gain material is provided by a laser diode. They consist of two semiconductor crystals stacked on top of each other but separated by a narrow slit, one crystal with an excess of electrons, called n-type, and one with a deficit of electrons (or a surplus of holes), called p-type. The area between the semiconductors is referred to as p-n-junction. A schematic of a laser diode is reported in Figure 2.3. When the diode is polarized in forward direction, the electrons flow towards the holes and vice versa. In order to recombine at the p-n-junction the electron has to lose some energy, since the hole is in a lower energy state, resulting in the emission of a photon. In addition to a positive net radiative decay, to turn the diode into a laser diode, a feedback or resonator mechanism has to be provided to keep the photons in the junction. Fortunately, the semiconductors have a high refractive index relative to the air in the slit resulting in total reflection similar to a waveguide. The semiconductor

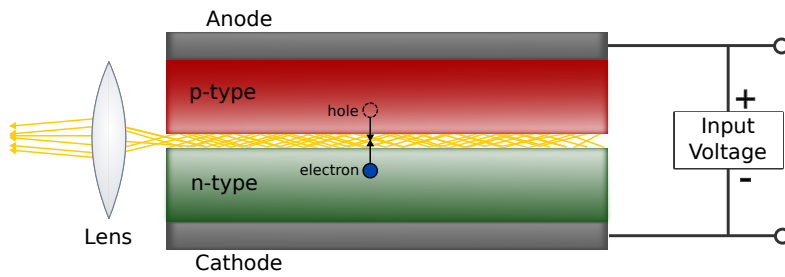


Fig. 2.3: Schematics of a laser diode. A p-type semiconductor is brought close to an n-type semiconductor, leaving a thin open slit called the p-n-junction. A voltage is applied, generating a current in forward direction. At the p-n-junction, which acts as the active area in the diode, electron-hole-recombination leads to the emission of identical photons. Due to the high refractive index of the semiconductors, photons are reflected from the boundaries. While the right junction output is highly reflective, the left output is only partially reflective and is therefore the laser output coupler. Since the outgoing radiation is typically divergent, a lens is necessary for collimation.

crystals act as the gain material as well as the optical resonator simultaneously. If the area between the crystals is dimensioned appropriately, i.e. the separation of the frequency modes is larger than the spectral width, only one mode is amplified and the diode produces and amplifies coherent single-mode photons. Since the slit is rather narrow, the photons are emitted in a large divergence angle and results in a wedge-shape opposed to a Gaussian shape. Therefore, collimation optics to shape the beam have to be implemented. Using appropriate semiconductors and dimensions of the p-n-junction, laser diodes can produce light in a wavelength range from the ultraviolet to the infrared. For example, a laser diode made of GaN and InGaN produces light at 405nm while diodes made of InGaAsP emit light in the telecom band [64].

Today, laser diodes are the most commonly used types of lasers. Among other features, they are small, efficiently⁴ produce light in a wide wavelength range and can be pumped and modulated easily using the external current source or optically. On the other hand, since the transition in the laser diode is between energy bands opposed to discrete electronic energy levels in other types of lasers, the light produced by laser diodes is of high bandwidth and low coherence. Also, while laser diodes can produce pumped light up to femtosecond pulses, the power output is limited by the intrinsic heating of the semiconductors.

Therefore, if one of these mentioned properties or other special light properties are required, as is the case for many applications in quantum optics, the laser diodes can provide the pump light in a gain material of a different type. This is the case

⁴in terms of pumping-to-light conversion

in the laser sources used in the Chapters 3.2 and 3.3, while the laser pumping the SPDC-crystal in Chapter 5 is a laser diode.

Cavity laser basics

When electrons are confined in a potential, for example the atomic potential of a nucleus, the electronic energy levels are quantized and the energy states E_n are the eigenvalues of the Hamiltonian \hat{H} in the time-independent Schrödinger equation $\hat{H} |\Psi_n\rangle = E_n |\Psi_n\rangle$. The probability to find fermions in a certain energy state E_n is given by the Fermi-Dirac distribution. However, since the energy of the contributing optical transition relevant for the lasing process is usually far higher than the Fermi energy, i.e. $E \gg E_F$, the probability distribution can be approximated by a Boltzmann distribution $P(E_n) \propto \exp(-E_n/k_B T)$ [64]. In equilibrium $P(E_n) > P(E_{n+1})$ but for non-equilibrium conditions a distribution according to $P(E_{n+1}) > P(E_n)$ can be achieved. This is called occupation inversion and a necessary condition for lasing. When an electromagnetic mode containing a photon interacts with an atom, chances are that the photon is absorbed by the atom inducing a transition to a higher energy level of the atom. For absorption to occur the energy of the photon has to be equal to the transition energy of the atom, i.e. $h\nu = E_2 - E_1$. After some time, depending on the cross section of the transition, the atom will spontaneously emit a photon of approximately the same energy into the electromagnetic mode, transitioning back to the ground state. Light created by spontaneous emission is the kind of light we typically see around us in everyday life, such as thermal emitters or LEDs. Since the emission occurs spontaneously and independent of the photon number in the electromagnetic mode, their amplitudes and phases are not correlated, therefore incoherent in time and position.

In order to create coherent light, the emission of photons by atoms contained in an active medium, has to be stimulated. This can be achieved by letting atoms already in an excited state E_2 interact with an electromagnetic mode containing photons of energy $E_2 - E_1$ where E_1 is again the ground state. Speaking heuristically, bosonic particles such as photons prefer to be close to each other than apart, therefore the photons in the mode stimulate the excited atoms to emit identical photons which are of the same frequency and strongly correlated in phase (meaning a long coherence length). To make sure that the light is amplified, the emission of photons has to exceed the absorption, which means more atoms have to be in an excited state than in the ground state, i.e. the aforementioned population inversion. For this reason, the active medium containing the atoms/molecules has to be pumped by an external source, either electrically in the case of gas lasers (via DC current) or optically by laser diodes or a flash lamp. In order to ensure population inversion and subsequent stimulated emission, all lasers are based on the same fundamental layout sketched

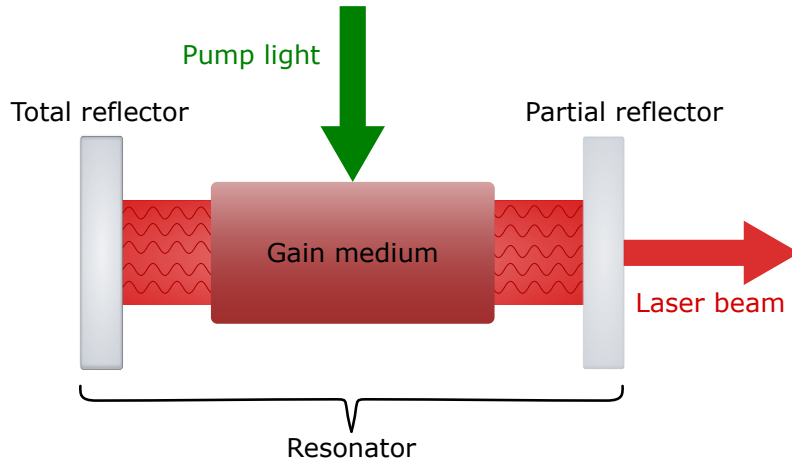


Fig. 2.4: Schematics of a typical cavity laser in cw operation. A gain medium, e.g. a crystal or a gas, is placed in the center of a cavity, or resonator, comprised by at least two mirrors. The gain medium is excited by an external source of energy to achieve population inversion in the medium. Light emitted by the gain medium is coherently amplified via reflection at the mirrors. A fraction of the total radiation is continuously transmitted through the partially reflective mirror and makes up the laser beam. Note the mirrors in real cavities are typically curved since flat mirrors are highly sensitive to small deviations from parallel alignment.

in 2.4: an optical resonator consisting of two adjacent mirrors, i.e. a cavity, and an optical amplifier, i.e. the active medium in between. An external source pumps the active medium creating population inversion between the ground and an excited state. After turning on the pump, the atoms absorb photons and spontaneously emit them again after some time. The emitted photons are recoupled into the cavity and lead to stimulated emission of more photons. The design (e.g. the length) of the cavity only allows for certain electromagnetic modes, specifically, if no other elements are included, Gaussian modes (TEM_{00}). To extract some of the light of the cavity to use is, one of the cavity mirrors has to be partially transmittent (typically around 99% reflectance).

Together with the active medium, the resonator acts as a frequency selection mechanism effectively creating light of a certain frequency and phase. As long as the resonator is optically stable and the emission exceeds the absorption, the signal gets enhanced and the laser is above threshold necessary for lasing. A measure for optical stabilization of the resonator is given by the resonator parameter $g_n = 1 - \frac{d}{R_n}$ relating the radius of the mirrors $R_{1,2}$ to the length d of the cavity, that ensures that the beam is reflected onto itself after reflection if $0 \leq g_1 g_2 \leq 1$. The modes allowed in the resonator are characterized by the finesse

$$\mathcal{F} = \frac{\Delta\nu}{\nu_0}$$

where $\Delta\nu$ is the full width half maximum of the resonator modes, defined by the linewidth of spectral lines of the emitting atoms, and $\nu_0 = \frac{c}{2L}$ is the free spectral range, i.e. the spectral distance between the modes. At every moment, a part of the light in the cavity mode is transmitted through the output coupler leading to a continuous output of coherent, approximately monochromatic and collimated wave trains. If the laser is emitting continuously it is running in continuous-wave (CW) operation, in contrast to pulsed lasers where the light is concentrated in evenly spaced, short pulses. The coherence properties of the wave trains emitted by the laser can be characterized by the coherence time τ_c , which is inversely proportional to the linewidth of the emitting atoms in the active media

$$\tau_c \propto \frac{1}{\Delta\nu} \quad (2.24)$$

and the coherence length $l_c = c\tau_c$ which quantifies how long and how far the light of a laser continues to interfere. Typical values for the coherence lengths and times of lasers are in the range of $0.3\mu\text{s} - 300\mu\text{s}$ corresponding to $100\text{m} - 100\text{km}$ compared to the coherence length of a mercury lamp which is about 3mm .

In the quantum optics framework, the output state of a laser above threshold is described by a coherent state which is the eigenstate of the annihilation operator $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$ where α is a complex number related to the average photon number by $|\alpha|^2$. The coherent state can be expressed as

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

in terms of the number state $|n\rangle = (a^\dagger)^n |0\rangle$. Coherent states have a Poissonian distribution and are the states that most resemble classical states since many properties are the same as in classical optics. However, one should keep in mind that coherent states, as all states of light, are inherently quantum in nature.

The output of a laser consists of many photons, either in bunches in the case of pulsed lasers or in a continuous stream. To distinguish laser (coherent) light from other quantum states of light, we will look at an important measure in the following section.

2.2.2 Second-order coherence function

For the characterization of coherence properties of different states of light, quantum coherence functions of n -th order are a useful tool, quantifying spatial and temporal correlations between quantized electric field operators \hat{E} at different places and times. While the first-order coherence function developed by Glauber in the 1960s

[44] can be used to determine (among other things) the coherence length of a state of light, it cannot be used to distinguish among states of light of the same spectral distributions but different photon number distributions (e.g. a photon number state $|n\rangle$ and the coherent state $|\alpha\rangle$). For this purpose, the second order coherence function comes into play, which can be given in the normalized form for temporal coherence (and fixed detector positions) as

$$g^{(2)}(\tau) = \frac{\langle \hat{E}^{(-)}(t) \hat{E}^{(-)}(t+\tau) \hat{E}^{(+)}(t+\tau) \hat{E}^{(+)}(t) \rangle}{\langle \hat{E}^{(-)}(t) \hat{E}^{(+)}(t) \rangle \langle \hat{E}^{(-)}(t+\tau) \hat{E}^{(+)}(t+\tau) \rangle}$$

which can be interpreted as the probability of a detection event after time τ after a first event. When assuming a single-mode quantized plane wave of the form $\hat{E}^{(+)} = iK\hat{a}e^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)}$ and $\hat{E}^{(-)} = -iK\hat{a}^\dagger e^{-i(\mathbf{k}\cdot\mathbf{r}-\omega t)}$ where \mathbf{k} is the wave vector, \mathbf{r} is the spatial position, ω is the angular frequency and K is a normalization factor, the coherence function simplifies to

$$g^{(2)}(\tau) = \frac{\langle \hat{a}^\dagger(0) \hat{a}^\dagger(\tau) \hat{a}(\tau) \hat{a}(0) \rangle}{\langle \hat{a}^\dagger(0) \hat{a}(0) \rangle^2} = 1 + \frac{\langle (\Delta\hat{n})^2 \rangle - \langle \hat{n} \rangle}{\langle \hat{n} \rangle^2}$$

where $\hat{n} = \hat{a}^\dagger \hat{a}$ is the photon number operator. Calculating the $g^{(2)}(\tau)$ for some of the most important states of light, as it is shown in Figure 2.5, gives the following results:

- **single-mode thermal states** $|\beta\rangle$: $g^{(2)}(0) = 2$ which means that there is a higher probability for coincidence events as $\tau = 0$. This effect is called photon bunching and comes from the fact that photons, as bosonic particles, tend to arrive in bunches.
- **coherent states** $|\alpha\rangle$: $g^{(2)}(\tau) = 1$ for all τ . This means that the photon detection events appear completely uncorrelated in point of view of the detector
- **number states** $|n\rangle$: $g^{(2)}(0) = 1 - \frac{1}{n}$ for $n \geq 1$ which is a behaviour called photon antibunching. The probability to detect coincidences is lower than for uncorrelated states or states that show bunching. An ideal single-photon source has $g^{(2)}(\tau) = 0$ meaning one single photons arriving at the detector in equal time steps.

In experiments, the most straight-forward way to measure the $g^{(2)}(\tau)$ of a source is by using the setup employed by Hanbury, Brown and Twiss in an attempt to determine the angular size of stars [65]: a 50 : 50 beam splitter is placed in the beam of photons to divide the beam, followed by a photodetector in both output arms that are connected by a coincidence count logic. The coincidence count rate

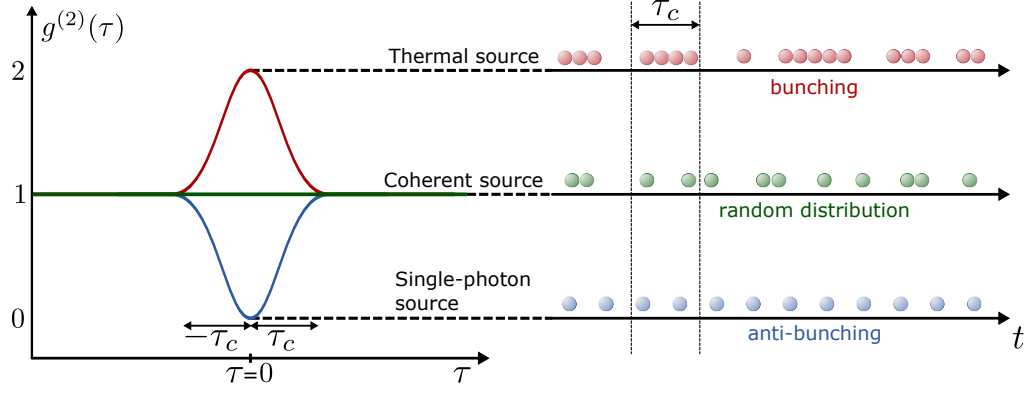


Fig. 2.5: Bunching statistics for different photon sources. On the left, the second-order coherence function $g^{(2)}(\tau)$ is plotted around $\tau = 0$. The width of the red and blue curve is twice the coherence time of the source τ_c . On the right, the bunching behavior of photons emitted by a certain source is depicted. Photons emitted by a thermal source, depicted by the red curve, show bunching which corresponds to $g^{(2)}(0) = 2$. A coherent source, e.g. a laser, emits photons in a random distribution, resulting in $g^{(2)}(0) = 1$. Ideal single-photon sources emit single photons in equal time-bins, a behaviour called anti-bunching and corresponding to $g^{(2)}(0) = 0$. By simply attenuating the light source, the photon statistics does not change.

is proportional to $g^{(2)}(\tau)$ for small integration times, i.e. the time delay τ is much smaller than the average time between two events. Antibunching is a highly non-classical behavior shown first in 1977 by Kimble et al. [66]. It cannot be recreated using 'classical' light sources such as lamps and can only be approximated using coherent sources. The latter case could be achieved by attenuating a laser source to create a coherent state with $|\alpha|^2 = \langle n \rangle \ll 1$ where the major contribution to the state is the vacuum state $|0\rangle$, i.e. no photon and a small contribution is $|1\rangle$, i.e. one photon. The disadvantages of this method are that, firstly, it is very inefficient since most of the time no photon is detected and secondly, since this is still a coherent state, it contains higher-order contributions i.e. multi-photon states. Nevertheless, attenuated lasers are used in experiments, for example in quantum cryptography [67].

The most commonly used single-photon sources used today are based on spontaneous parametric down-conversion (SPDC). SPDC occurs in nonlinear media where a single-photon is converted in two photons of lower frequency. In the following Chapter we will look at the nonlinear effect in certain crystals that makes down-conversion possible. After that, we will describe the use of down-conversion sources in experimental quantum optics.

2.2.3 Spontaneous parametric down-conversion

Every source discussed in this thesis is based on spontaneous parametric down-conversion, a nonlinear effect theoretically predicted in 1961 [68] and experimentally discovered by three independent groups in 1967 [69–71]. The groups observed output radiation at a parametric amplifier without an input beam and referred to it as parametric noise. The nature of this output radiation, specifically that it is comprised of a flux of photon pairs created in an extremely narrow time window, was explored in the following years [72, 73]. In order to describe the properties of SPDC, it is necessary to introduce a few concepts of classical nonlinear optics: When light propagates through an ordinary, dielectric medium, the response of the polarization of the material $\mathbf{P}(t)$ to the electric field strength $\mathbf{E}(t)$ is linear, i.e.

$$\mathbf{P}(t) = \epsilon_0 \chi^{(1)} \mathbf{E}(t) \quad (2.25)$$

where ϵ_0 is the vacuum permittivity and $\chi^{(1)}$ is the electric susceptibility to first order [74]. The polarization of a material describes the charge displacement of atomic dipoles due to external electromagnetic fields. Two of the consequences of this linear response are that first, the absorptive and refractive index of the material is independent of the intensity of the light and secondly, two light waves propagate through the medium without influencing each other.

However, when light of high intensity (for example emitted by a laser), propagates through a nonlinear material, these principles do not hold anymore: the refractive index becomes dependent on the intensity $n = n(I)$ ⁵ and therefore propagating waves influence the propagation of other waves. Higher-order terms in the polarization expansion need to be taken into account, hence 2.25 turns into:

$$\begin{aligned} P(t) &= \epsilon_0 \left(\chi^{(1)} E(t) + \chi^{(2)} E^2(t) + \chi^{(3)} E^3(t) + \dots \right) \\ &:= P_L + P_{NL} \end{aligned} \quad (2.26)$$

where we defined the nonlinear polarization terms

$$P_{NL} := \epsilon_0 \chi^{(2)} E^2(t) + \epsilon_0 \chi^{(3)} E^3(t) + \dots \quad (2.27)$$

and used scalar notation for simplification⁶ Each of these terms describes numerous nonlinear effects depending on the frequencies of the generating waves. Since

⁵The dependency of the refractive index on the intensity stems from the relation $n^2 = 1 + \chi$. When higher-order terms of χ have an effect due to higher intensities, the refractive index is affected by the intensities as well

⁶When all spatial dimensions are required, the polarization as seen before, is a vector and the susceptibility of the material is a tensor, e.g. d_{ijk} for second-order nonlinearities

the magnitude of the electric susceptibility decreases with higher-order, higher and higher field strengths are necessary to see noticeable higher-order effects. For example, the second-order coefficient $\chi^{(2)}$ is of order 10^{-12}m/V which makes it much weaker than first-order effects, $\chi^{(1)}$ being at the order of unity for solids. The nonlinear term of second order

$$P^{(2)}(t) = \epsilon_0 \chi^{(2)} E^2(t) \quad (2.28)$$

can be expressed in terms of the frequencies $P^{(2)}(t) = \sum_n P(\omega_n) e^{-i\omega_n t}$. The processes described by the second-order nonlinearity include generation of a wave at frequency $\omega_3 = \omega_1 \pm \omega_2$ from two waves at frequencies ω_1 and ω_2 . For example, the process $\omega_3 = \omega_1 + \omega_2 = 2\omega_1$ is known as second harmonic generation (SHG) and is commonly used in optical labs, creating frequencies not naturally available from lasers, or in spectroscopy. Second harmonic generation and other nonlinear effects can only occur if the in- and outgoing wave vector components are equal, i.e. in a scalar fashion

$$k_1 + k_2 = k_3 = \frac{n_3 \omega_3}{c} = \frac{n_1 \omega_1}{c} + \frac{n_2 \omega_2}{c} \quad (2.29)$$

This condition cannot be fulfilled in normally dispersive materials since $n_1(\omega_1) < n_2(\omega_2) < n_3(\omega_3)$ for $\omega_1 < \omega_2 < \omega_3$. Therefore, nonlinear effects such as SHG and SPDC can only occur in birefringent (anisotropic) materials where the refractive index is different depending on the input polarization and propagation direction. For example, in uniaxial crystals, the refractive index depends on the direction of propagation relative to the optical axis of the crystal. Light propagating parallel to the optical axis experiences the so-called ordinary refractive index n_o regardless of its polarization. For rays propagating in any other direction but with a polarization perpendicular to that of the ordinary ray, the polarization direction will be partly in the direction of the optical axis. This extraordinary ray will be governed by a different, direction-dependent refractive index. The refractive index of an extraordinary wave entering the material is therefore split in two components, given by

$$\frac{1}{n^2(\theta, \omega)} = \frac{\cos^2(\theta)}{n_o^2(\omega)} + \frac{\sin^2(\theta)}{n_e^2(\omega)} \quad (2.30)$$

where $0^\circ \leq \theta \leq 90^\circ$ is the angle between the propagation direction of the wave and the optical axis. We can therefore tune this angle accordingly, for example $n_e(\omega_3) = n_o(\omega_1 = \omega_2)$ the requirement for nonlinear effects can be achieved.

The reversal of SHG or of sum frequency generation (SFG) in the case $\omega_1 \neq \omega_2$ as in general in 2.29, is called parametric down-conversion, where one pump beam 2ω is converted in two output beams of either different frequencies (non-degenerate) or same (half) frequency (degenerate). In classical optics, a similar process is used to amplify a weak wave of frequency ω_1 by inferring it with a strong pump wave

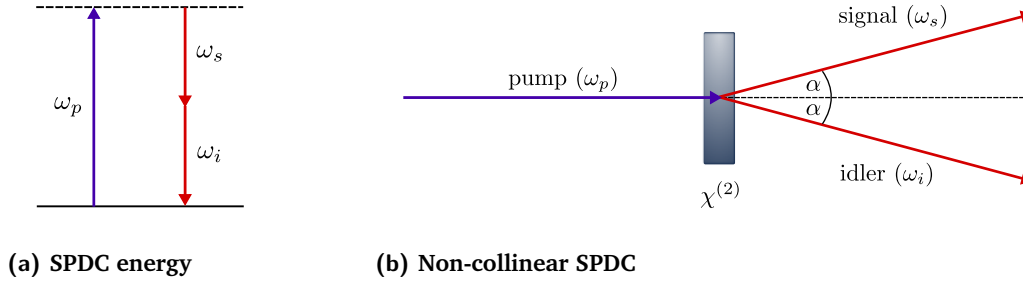


Fig. 2.6: (a) **Energy diagram of SPDC.** The vacuum state, denoted by the solid line, can be excited to a virtual higher energy state, denoted by the dashed line, by a pump photon of frequency ω_p . The pump photon is destroyed in the process. In certain materials, the excited state can decay by releasing two daughter photons of frequency ω_s and ω_i obeying $\omega_s + \omega_i = \omega_p$. (b) **Non-collinear SPDC in a nonlinear crystal.** An incident pump photon is split in two daughter photons named signal and idler. The down-conversion rate in the crystal is characterized by the coefficient of second order $\chi^{(2)}$. In non-collinear downconversion, the signal and idler photon are emitted in an angle α relative to the pump beam.

at $\omega_3 \equiv \omega_p$. Besides the 'signal' at $\omega_1 \equiv \omega_s$, a second weak beam called 'idler' is generated at $\omega_2 \equiv \omega_i$. It can be shown, however, that, without a second input beam, no amplification of the signal and no generation of the idler can take place classically [34, 75]. Describing the process as a quantum process, the vacuum is occupied by the vacuum state $|0\rangle$ in the number basis. In a nonlinear crystal, there exists a small probability that a pump photon excites the vacuum state to a virtual higher-energy state which, as it decays, generates two photons of lower energy (see figure 2.6a). Since this process is based on the spontaneous fluctuation of the vacuum, it is known as spontaneous PDC or SPDC.

The properties of the photons involved in the SPDC process obey conservation of energy- and momentum, in this context known as phase-matching conditions:

$$\begin{aligned}\hbar\omega_p &= \hbar\omega_s + \hbar\omega_i \\ \hbar\mathbf{k}_p &= \hbar\mathbf{k}_s + \hbar\mathbf{k}_i\end{aligned}\tag{2.31}$$

where \mathbf{k} are the respective wave vectors of pump, signal and idler photons. In practice, the phase-matching conditions can never be perfectly fulfilled⁷, giving rise to a phase-mismatch Δk . The mismatch has to be included in the momentum conservation which then reads as

$$\mathbf{k}_p = \mathbf{k}_s + \mathbf{k}_i + \Delta\mathbf{k}\tag{2.32}$$

⁷due to deviations in the wavelength of the pump beam, the angle between pump beam and the crystal or material imperfections

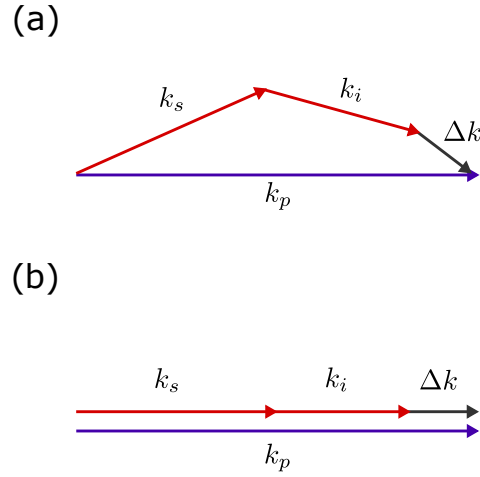


Fig. 2.7: (a) **Non-collinear phase-matching:** The pump photon with wave vector \mathbf{k}_p is split in the signal photon with wave vector \mathbf{k}_s and idler photon \mathbf{k}_i , both emitted in an angle relative to \mathbf{k}_p . Due to experimental imperfections, a phase-mismatch $\Delta\mathbf{k}$ is present, leading to fluctuations in the down-conversion rate. (b) **Collinear phase-matching:** The signal and idler photons propagate in the same direction as the pump photon. Again, due to experimental factors, a phase-mismatch $\Delta\mathbf{k}$ is present. Both types of phase-matching obey the condition $\mathbf{k}_p = \mathbf{k}_s + \mathbf{k}_i + \Delta\mathbf{k}$

and is graphically depicted in figure 2.7. $\Delta\mathbf{k}$ leads to a reduced generated power as well as to fluctuations in the down-conversion rate, which is why it should be reduced as much as possible. While the phase-mismatch cannot be fully avoided in birefringent phase-matching, it can be minimized by careful alignment of pump beam and nonlinear crystal. Furthermore, in Chapter 2.2.4, a type of phase-matching will be introduced to counter the phase-mismatch, leading to down-conversion rates higher than possible here (however, still lower than perfect phase-matching). To discuss the quantum properties of SPDC, we are going to derive the output quantum state generated in SPDC processes following [76–78]: The quantized Hamiltonian for SPDC consisting of the free electromagnetic field Hamiltonian \hat{H}_{em} and an interaction term \hat{H}_I [79] can be written as:

$$\hat{H}_{\text{SPDC}} = \hat{H}_{\text{em}} + \hat{H}_I = \sum_{i=0}^2 \left(\hat{n}_i + \frac{1}{2} \right) + \hbar g \left(\hat{a}_0 \hat{a}_1^\dagger \hat{a}_2^\dagger + \hat{a}_0^\dagger \hat{a}_1 \hat{a}_2 \right) \quad (2.33)$$

where $g \propto \chi^{(2)}$ is the coupling constant of the interaction. The two terms in the interaction part describe SPDC and SFG, respectively. Since the state of the pump is usually a coherent state emitted by a laser and remains a coherent state after some photons get down-converted, we assume that the SPDC process doesn't deplete the pump beam of photons, i.e. $\langle \hat{n}_1(t) \rangle, \langle \hat{n}_2(t) \rangle \ll |\alpha|^2$. This approximation is justified by the fact that the SPDC efficiency is typically of the order of 10^{-7} . We therefore assume the pump field to be a classical, i.e. $\hat{a}_0 \sim E e^{-i\omega_0 t}$ [78]. Furthermore,

we label mode 1 (2) as signal (idler) mode s (i), without loss of generality. The interaction part of \hat{H}_{SPDC} can then be written as

$$\hat{H}_I = i\eta\hbar \left(\hat{a}_s^\dagger \hat{a}_i^\dagger + h.c. \right) \quad (2.34)$$

where we absorbed the classical field and the coupling constant in the parameter η . Starting from the initial state $|\Psi(0)\rangle$, we can describe the output state $|\Psi(t)\rangle = \hat{U} |\Psi(0)\rangle$ using

$$\hat{U} = \exp(-i\hat{H}_I t/\hbar) = \exp\left(\xi \left(\hat{a}_s^\dagger \hat{a}_i^\dagger + h.c. \right)\right) \quad (2.35)$$

where $\xi = \eta t$ is a parameter that depends on the nonlinearity, the interaction time t and the strength of the pump beam. This operator generates the well-known two-mode squeezed state which, in the high gain regime $|\xi| \gg 1$ corresponds to parametric amplification. Here, we are interested in the low gain regime of $|\xi| \ll 1$, and assume spontaneous PDC, i.e. the initial state is in the vacuum $|\Psi(0)\rangle = |0\rangle_s |0\rangle_i$. The (unnormalized) output state then results to

$$\begin{aligned} |\Psi(t)\rangle &= \exp(\xi \hat{a}_s^\dagger \hat{a}_i^\dagger + h.c.) |0\rangle_s |0\rangle_i \\ &\approx \exp(\xi \hat{a}_s^\dagger \hat{a}_i^\dagger) |0\rangle_s |0\rangle_i \\ &= \sum_{j=0}^{\infty} \frac{\xi^j}{j!} \left(\hat{a}_s^\dagger \right)^j \left(\hat{a}_i^\dagger \right)^j |0\rangle_s |0\rangle_i \\ &= |0\rangle_s |0\rangle_i + \xi |1\rangle_s |1\rangle_i + \xi^2 |2\rangle_s |2\rangle_i + \dots \end{aligned} \quad (2.36)$$

where we approximate the second line using normal ordering of the operators [78]. The probability to randomly convert pump photons into daughter photons is given by $|\xi|^2$ for one pair, $|\xi|^4$ for two pairs, and so on. For small ξ , we can drop higher order terms such as ξ^2 and get

$$|\Psi(t)\rangle \approx |0\rangle_s |0\rangle_i + \xi |1\rangle_s |1\rangle_i \quad (2.37)$$

which is the superposition of the vacuum and a two-photon state. Since the vacuum state $|0\rangle$ cannot be registered in detectors, we can post-select the $|1\rangle |1\rangle$ -term by using two detectors and counting the coincidences. Increasing the pump power increases the down-conversion rate ξ , however, it also leads to a higher probability of multi-pair emissions. Since most detectors used in experiments cannot distinguish between different number states, a detected coincidence might originate from a multi-pair emission. If the $|1\rangle_s |1\rangle_i$ is the desired state, higher-order emissions decrease the quality of the state, acting as a source of noise. This is one of the main limiting factors of SPDC sources. Therefore, it is important to find a balance between acceptable noise and high down-conversion rate in experiments. The output radiation can originate from any coupled field mode that fulfill the phase-matching conditions 2.31. Therefore, multiple modes may contribute to the parametric process which

in turn generates entanglement between the modes. The entanglement generated depends on different experimental factors and the type of phase-matching in the crystal. For example, since the SPDC process has a wide spectrum, the two generated photons are typically entangled in the wavelength (frequency), fulfilling

$$\frac{1}{\lambda_p} = \frac{1}{\lambda_s} + \frac{1}{\lambda_i} \quad (2.38)$$

If the wavelengths of signal and idler are close, i.e. $\lambda_s \approx \lambda_i \approx 2\lambda_p$, the daughter photons are called degenerate. This property is required if the goal is to create indistinguishable photon pairs. Since there is still ambiguity in the wavelengths, typically bandwidth filters with a bandwidth of a few nanometers are used to spectrally post-select the photons. If the wavelength of the photons can be clearly distinguished, i.e. $\lambda_s \neq \lambda_i$, the process is called non-degenerate. In certain crystals, the photons can be separated by a few hundred nanometers, making it easy to spatially separate the photons. In this thesis, while we exploit spatial and spectral entanglements, we mostly focus our discussion on the polarization degree of freedom since we use polarization-qubits in every experiment discussed.

In this regard, we distinguish two types of phase-matching: in type-I phase-matching, a pump photon generates daughter photons that have the same polarization. The photons are emitted at diametrical points of a cone centered around the pump beam, where the opening angle depends on the pump wavelength and orientation of the optical axis of the crystal with respect to the pump beam. The generated photons are entangled in the frequency, temporal and spatial mode but not in polarization. By collecting photons from opposing points of the cone, type-I phase-matching can be used to generate highly indistinguishable photon pairs of the form in equation 2.37, used for example for a heralded single-photon source. In type-II phase-matching, the daughter photons generated have orthogonal polarization. Since the refractive index in the birefringent material depends on the polarization, the signal and idler photon are shifted relative to each other and leave the crystal in two overlapping cones. When collecting photons from the overlapping points of the cones, we cannot distinguish one photon from another (see 2.8). The state is entangled in the paths (s and i) and polarization (H and V) degrees of freedom. We can write the output state of type-II SPDC by

$$\begin{aligned} |\Psi\rangle &\propto \sum_{n=0}^{\infty} \xi^n \left[\sum_{m=0}^n (-1)^m |n-m\rangle_{Hs} |m\rangle_{Vs} |m\rangle_{Hi} |n-m\rangle_{Vi} \right] \\ &= |0\rangle_s |0\rangle_i + \xi |1\rangle_{Hs} |0\rangle_{Vs} |0\rangle_{Hi} |1\rangle_{Vi} - \xi |0\rangle_{Hs} |1\rangle_{Vs} |1\rangle_{Hi} |0\rangle_{Vi} + \dots \end{aligned} \quad (2.39)$$

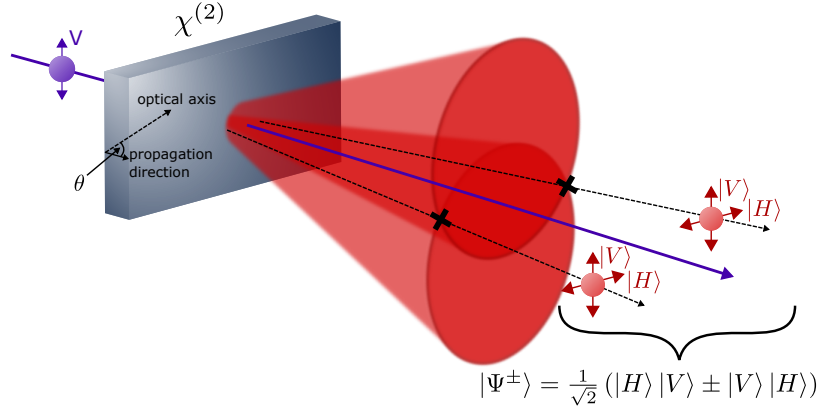


Fig. 2.8: Type-II SPDC. A pump photon in the state $|V\rangle$ is extraordinarily polarized with respect to the optical axis of the nonlinear crystal $\chi^{(2)}$. The angle between the pump propagation direction and the optical axis is denoted by θ . If down-conversion occurs, photons of mutually orthogonal polarization are emitted in the form of two overlapping cones. At the intersection points of the cones, entanglement between the photons is generated resulting in the state $|\Psi^\pm\rangle$.

Post-selection on one photon in each spatial mode, defining $|1\rangle_{Hs/i} |0\rangle_{Vs/i} \equiv |H\rangle_{s/i}$ and $|1\rangle_{Vs/i} |0\rangle_{Hs/i} \equiv |V\rangle_{s/i}$ and normalization yields the maximally entangled singlet state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|H\rangle_s |V\rangle_i - |V\rangle_s |H\rangle_i) \quad (2.40)$$

Type-II SPDC sources are typically used for entanglement experiments, since polarization-entangled pairs can be easily generated from the down-conversion process. Furthermore, the $|\Psi^-\rangle$ can be transformed in any other Bell state via local transformations. However, while photons generated by type-I phase-matching are in a product state in the polarization degree of freedom, two identical type-I crystals with their optical axis crossed can be combined to create the entangled $|\Phi^+\rangle$ state. For example, entanglement generated from type-I phase-matching will be used for the source in Chapter 5, where we will describe the experimental scheme in more detail. Note that while equations 2.37 and 2.40 describe the quantum state generated by SPDC, they do not give information about the spectral properties of the state and the influence of phase-matching on the output. A detailed discussion on these properties can be found for example in [78].

For the derivation of the SPDC quantum state, we used the arbitrary labels signal and idler to distinguish between the two daughter photons. While in type-I, both signal and idler photon are in the same polarization state and in type-II, they are orthogonally polarized, we can further distinguish the types by referring to

the ordinary and extraordinary polarization in Chapter 2.2.3. Depending on the polarization of the pump photon with respect to the optical axis of the crystal, we can then define the following phase-matching types:

- **type-I:**
 - type-I a: $o \rightarrow e + e$
 - type-I b: $e \rightarrow o + o$
- **type-II:**
 - type-II a: $o \rightarrow o + e$
 - type-II b: $e \rightarrow o + e$

where o means ordinary polarization (perpendicular to the optical axis) and e means extraordinary polarization (in parts parallel to the optical axis). As discussed before, in a birefringent material, the refractive index differs for ordinary and extraordinary polarization. In type-II phase-matching, this leads to a different group velocity of the signal and the idler photon resulting in a longitudinal offset and leading to polarization-temporal correlations. Additionally, the differing refractive index causes a transversal offset between the o-cone and the e-cone and, in turn to correlation between the spatial and the polarization mode. Since both effects reduce the indistinguishability, to produce polarization-entangled states via type-II down-conversion, one has to account for effects caused by the birefringence of the nonlinear crystal, known as walk-off effects:

Walk-off

In order to generate polarization-entangled states, the photons have to be indistinguishable in the remaining degrees of freedom. This is usually not the case after propagation in a nonlinear crystal since the birefringence induces a spatial and a temporal walk-off between the o- and the e-beam. The temporal and spatial walk-off are sketched in Figure 2.9 and 2.10, respectively.

- **Longitudinal/temporal walk-off** originates from the different group velocities $v_g = c/n_g$ of the ordinary and the extraordinary beam in the crystal where n_g is the refractive group index. Therefore, the beams leave the crystals at

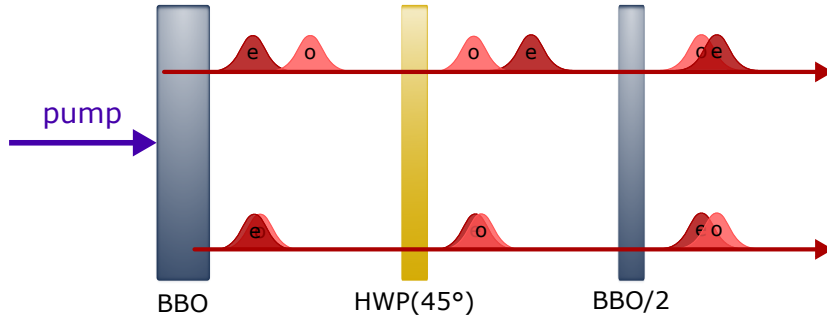


Fig. 2.9: Longitudinal walk-off compensation for SPDC in a BBO crystal. In type-II SPDC, the group velocity in the nonlinear crystal is smaller for e-polarized light. Depending on the point of down-conversion, the wave packets of the photons are shifted relative to each other when exiting the crystal reducing the entanglement quality. To compensate this effect, first a half-wave plate rotated by 45° is placed in the way of the wave packets, swapping the polarization. Next, a nonlinear crystal of half the thickness of the main crystal induces a temporal walk-off on the swapped wave packets, effectively shifting them together and increasing the overlap. If the down-conversion takes place close to the exit of the crystal as depicted in the lower case, the walk-off compensation may reduce the overlap. However, since the majority of the down-conversion events happen close to the center of the crystal on average, the walk-off compensation overall increases the entanglement quality.

different times dependent on the point of creation in the crystal. The time delay is given by

$$\Delta t = |(n_o - n_e)L/c| \quad (2.41)$$

where L is the length of the crystal. If Δt exceeds the coherence time $\tau_c = \sqrt{2 \ln 2} \lambda^2 / (\pi \Delta \lambda) c$ of the photons, the walk-off has to be compensated to avoid correlations between the time of arrival and the photon polarization.

- **Transversal/spatial walk-off** is caused by the dependence of n_e on the angle between the propagating wave and the optical axis. The wave-vector \mathbf{k} is not parallel to the direction of the energy flow of the wave as in the case of the ordinary beam but separated by a walk-off angle ρ given by

$$\tan(\rho) = -\frac{1}{n_e} \frac{dn_e}{d\theta} \quad (2.42)$$

The temporal and the spatial walk-off are usually compensated by identical crystals half the length of the SPDC-crystal that are placed in the signal (e/o) and the idler (o/e) beam and rotated by 180° .

This is achieved by rotating the signal and idler beam by 90° using a half-wave plate and placing two crystals of the same type but half the length and rotated by 180° in each arm with respect to the optical axis. With ordinary and extraordinary beams

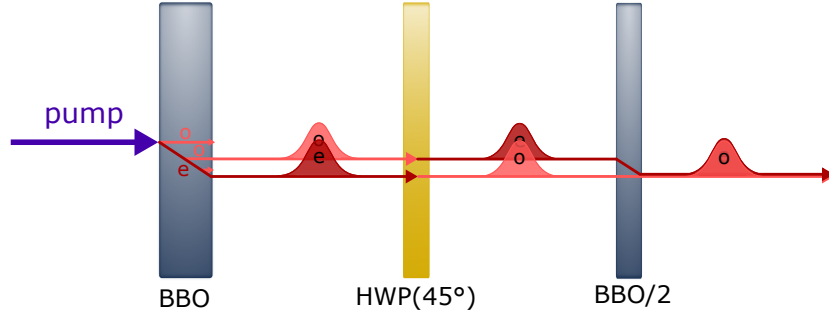


Fig. 2.10: Transversal walk-off compensation for SPDC in a BBO. Due to the birefringence of the nonlinear material, the e-polarized wave packet gets refracted and transversally offset relative to the o-polarized wave packet. After exiting the crystal, the transversal walk-off increases the distinguishability, therefore reducing the quality of entanglement. Placing a half-wave plate at 45° exchanges the o-polarized with the e-polarized wave packet. A nonlinear crystal of half the thickness of the main crystal induces a walk-off on the formerly o-polarized wave packet, shifting the wave packets back together. As for the temporal walk-off compensation, assuming that most of the down-conversion takes place close to the crystal center, the overlap and the entanglement quality is overall increased.

exchanged, the compensation crystals compensate the walk-off induced by the main crystal.

Two of the first nonlinear crystals used for SPDC were KDP and BBO. Since BBOs are still the most widely used crystals including two of the three experiments discussed in this thesis, we will take a closer look at its properties and its uses.

BBO

Beta-barium borite is a uniaxial negative crystal, i.e. $n_f < n_s$ ('f' denotes the fast, 's' the slow axis of the crystal) $n_e < n_o$ transparent in the range 190 – 3000nm [80]. When the pump beam enters the BBO crystal at an angle θ with respect to the optical axis the refractive index for the extraordinary beam depends on the angle. In a BBO, phase-matching can only be achieved for an incoming beam of extraordinary polarization. The down-conversion processes possible in a BBO are depicted in figure 2.11.

In type-II down-conversion, the signal and idler beam exit the BBO in the form of two cones of orthogonal polarization that fulfill the phase-matching conditions. One of the cones contains photons in the ordinary polarization mode, the other cone in the extraordinary polarization, e.g. $e(V) \rightarrow e(V) + o(H)$. Tilting the crystal changes the size of the cones and allows for the ordinary and the extraordinary beam to overlap. At the cross sections of the two cones, horizontally and vertically polarized photons overlap. This can be used to create polarization-entangled states of the

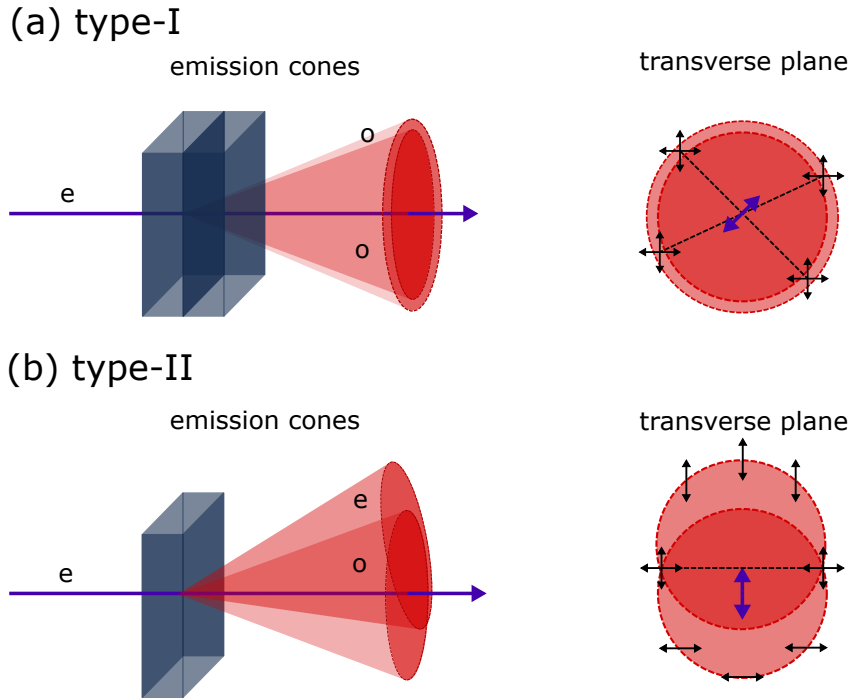


Fig. 2.11: (a) **Type-I SPDC.** Emission cones: Two nonlinear crystals with crossed optical axes are stacked together. The pump beam is polarized diagonally. On average, half of the incident light is e-polarized relative to the optical axis of the first crystal and the other half relative to the second crystal. If down-conversion takes place at the intersection between the two crystals, the polarization of the generated photons cannot be determined with certainty, creating a superposition of o-polarization with respect to the first or the second crystal. Since both photons are o-polarized, the emission cones are both centered around the pump beam, the size determined by the point of down-conversion in the crystals. To the right, a projection of the transverse plane shows the diagonally polarized pump beam in the center and photons of ambiguous polarization at the overlap of the cones. Photons at opposite points of the cones are polarization-entangled. (b) **Type-II SPDC.** Emission cones: The e-polarized pump beam generates one o-polarized and one e-polarized photon in the nonlinear crystal. After exiting of the crystal the e-polarized emission cone is spatially offset relative to the o-polarized cone due to the birefringence. The cut in the transverse plane to the right depicts the pump beam centered in the o-polarized cone and above, the e-polarized cone. Photons at the intersection points of the cones are ambiguous in polarization, giving rise to entanglement.

form $\frac{1}{\sqrt{2}} (|H\rangle |V\rangle + e^{i\phi} |V\rangle |H\rangle)$ (where ϕ is a relative phase) as long as the spatial and temporal walk-off are compensated, usually by placing a half-wave plate and a compensation BBO in the signal and idler arms as described above.

Unfortunately, while the compensation of walk-off effects allow for high coherence between the emitted photons, both type-I and type-II sources based on SPDC in a nonlinear crystal suffer from multiple disadvantages additional to the low efficiency and the linear scaling with pump power. Firstly, since η is proportional to the pump field strength and the (usually small) second-order susceptibility, which shows that the proportion of photons that are created in the signal and idler mode is small and most of the times signal and idler will remain in the vacuum mode, no down-conversion taking place. It also implies that the intensity of SPDC scales linearly with the pump intensity $I_p = |E_p|^2$ whereas classical effects such as SHG scale quadratically. In the equations 2.37 and 2.40 we dropped higher order terms containing multi-pair emissions of the form $|n\rangle |n\rangle$. These terms become relevant when the pump field strength contained in η is increased.

Secondly, in both configurations, entangled photon pairs are emitted non-collinearly. In type-I, the entangled photons are located at opposite points in the cones, in type-II sources entangled photons are in the intersection lines of the cones. Spatially selecting the entangled photon pairs using single-mode fibers, effectively discards the majority of the emitted photons and leads to inherently small count rates.

Thirdly, reducing the phase mismatch Δk in experiments requires careful alignment and cannot be completely disposed of due to dispersion and the finite crystal length L . If $\Delta k \neq 0$, it results in position-dependent phases $\Delta \mathbf{k} \cdot \mathbf{r}$ in the medium, leading to destructive interference between the pump and the daughter fields and therefore to lower returns and periodic fluctuations in the output intensity.

While the efficiency of SPDC sources is inherently limited by its very nature, the development of new source designs allows to maximize the spatial collection of photons and minimize the effect of the phase-mismatch. We next consider SPDC sources collinearly ($\alpha_{s,i} = \alpha_p = 0$) emitting frequency-degenerate ($\lambda_s \neq \lambda_i$) photon pairs. Furthermore, the efficiency is increased by introducing another type of phase-matching known as quasi-phase-matching.

2.2.4 Quasi phase-matching

Certain nonlinear materials can be modified to make the nonlinearity of the material position-dependent. Specifically, the sign of the effective nonlinear coefficient d_{eff} is periodically reversed, turning the material in a nonlinear grating with periodicity

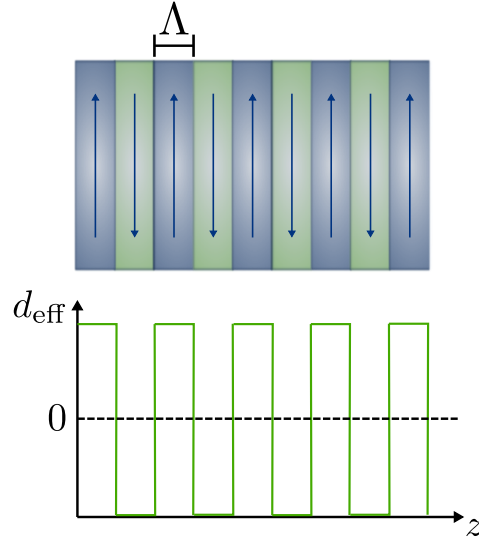


Fig. 2.12: Periodical poling of a nonlinear crystal. The effective nonlinearity of the material d_{eff} which depends on the direction of the optical axis (indicated with the arrows) changes its sign every grating period Λ along the direction z .

Λ . This technique can be used to reset the phase mismatch periodically, therefore increasing the efficiency of nonlinear processes such as SPDC. We define the phase-mismatch of m -th order by

$$\Delta k_m \equiv \Delta k - m \frac{2\pi}{\Lambda} \quad (2.43)$$

where m is a positive or negative integer. Therefore, from the definition the phase-mismatch

$$\Delta k = k_p - k_s - k_i \quad (2.44)$$

we get the quasi-phase-matching condition

$$\Delta k_m = 2\pi \left(\frac{n_p}{\lambda_p} - \frac{n_s}{\lambda_s} - \frac{n_i}{\lambda_i} - \frac{m}{\Lambda} \right) = 0 \quad (2.45)$$

Therefore, choosing the poling periodicity as

$$\Lambda = m \frac{2\pi}{\Delta k} \quad (2.46)$$

we can achieve phase-matching. In essence, instead of tuning the incidence angle in the crystal as in type-I and type-II, a crystal with an appropriate poling periodicity is constructed for quasi-phase-matching. The periodic poling of the nonlinearity is usually achieved by thermal or ferro-electric flipping of the electric polarization. Since Λ is highly temperature-dependent, usually the temperature of the crystal has to be tuned to achieve optimal periodicity.

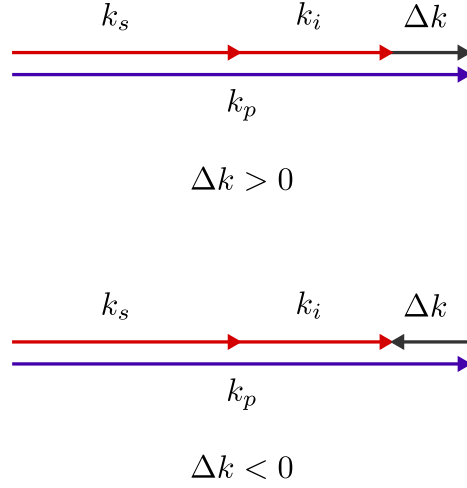


Fig. 2.13: Positive and negative phase mismatch vectors Δk in a nonlinear crystal. The momentum phase-matching condition in this case is given by $k_p = k_s + k_i + \Delta k$. By periodically poling the crystal an appropriate quasi phase-matching order m can be chosen to cancel the positive, the negative or both phase-mismatch vectors.

Some of the most used periodically poled crystals for SPDC are potassium titanyl phosphate (KTP) and lithium niobate (LN) (referred to as ppKTP and ppLN, respectively). Employing crystals suitable for quasi-phasematching can increase the efficiency of down-conversion by a factor proportional to the square of the number of periods in the structure [64]. A number of different architectures for SPDC sources based on QPM in periodically-poled nonlinear crystals have been developed in the last two decades. Among the most common designs are double-crystal single-pass sources in a Mach-Zehnder interferometer, where a pp crystal is placed in each arm and the output is combined afterwards, and single-crystal double-pass configurations where a pp crystal is placed in a Sagnac loop pumped from both sides. Both of these designs require sophisticated alignment, negating one of the advantages of typical QPM sources.

Fortunately, attempts are made to design QPM sources that are both easy to align and more efficient than sources based on birefringent phase-matching. For the experiment in 4.2, we use a source introduced in [81] where entangled photon pairs are generated by overlapping two SPDC processes in a single crystal during a single pass. As in every QPM source, the phase-mismatch can be reset by periodical poling every period $\Lambda = m2\pi/\Delta k$. In general, Δk can be positive or negative, resulting in the two cases depicted in figure 2.13. To counteract the phase-mismatch, the QPM order m has to be chosen positive or negative accordingly. The output state of the source can then be written as the sum of two terms

$$|\Psi\rangle_{\text{out}} := \alpha |\Psi_+\rangle + \beta |\Psi_-\rangle \quad (2.47)$$

where $|\Psi_{\pm}\rangle$ correspond to SPDC processes achieved by compensating $\pm\Delta k$. While in most setups, only one of the terms is phase-matched, it is possible to configure the crystal such that both SPDC processes contribute to the output state. Two pairs of photons with wavelengths

$$\begin{aligned} \lambda_{s+}, \quad \lambda_{i+} \\ \lambda_{s-}, \quad \lambda_{i-} \end{aligned} \quad (2.48)$$

are then emitted collinearly with respect to the pump beam. Here, the down-conversion is of type-II and we denote the signal photons as horizontally and the idler photon as vertically polarized. The pump and the crystal can be set up such that two wavelengths with different polarizations are overlapped and cannot be told apart, i.e.

$$\begin{aligned} \lambda_{H+} &= \lambda_{V-} \\ \lambda_{V+} &= \lambda_{H-} \end{aligned} \quad (2.49)$$

Since then there is no information if the pair originated from $|\Psi_{+}\rangle$ or $|\Psi_{-}\rangle$, the total output state is entangled in polarization and wavelength and is given by

$$\begin{aligned} |\Psi\rangle_{out} &= \alpha \hat{a}_{HB}^{\dagger} \hat{a}_{VR}^{\dagger} |0\rangle + \beta \hat{a}_{HR}^{\dagger} \hat{a}_{VB}^{\dagger} |0\rangle \\ &= \alpha |H\rangle |V\rangle \otimes |B\rangle |R\rangle + \beta |H\rangle |V\rangle \otimes |R\rangle |B\rangle \end{aligned} \quad (2.50)$$

where B denotes the short and R the long wavelength. The output state can be spatially separated in modes 1 and 2 by either using a PBS, reducing the state to a wavelength-entangled state or a dichroic mirror, creating a polarization-entangled state

$$|\Psi\rangle = (\alpha |H\rangle_1 |V\rangle_2 + \beta |V\rangle_1 |H\rangle_2) \otimes |B\rangle_1 |R\rangle_2 \quad (2.51)$$

as it is done in the experiment here. In general, the superimposed SPDC processes have a different spectral width as well as unequal amplitudes. To avoid spectral distinguishability and equalize the amplitudes, a narrowband filter is placed in the brighter arm. The resulting polarization-entangled state is then of the approximate form

$$|\Psi\rangle \approx \frac{1}{\sqrt{2}} \left(|H\rangle_1 |V\rangle_2 + e^{i\phi} |V\rangle_1 |H\rangle_2 \right) \quad (2.52)$$

The phase ϕ can be set using calcite crystals, which at the same time can be tuned to cancel the temporal walk-off induced in the crystal due to dispersion. If the phase is set appropriately, the final state is the Bell state $|\Psi^{-}\rangle$.

The two main applications for SPDC in this thesis are the creation of single photons and the creation of polarization-entangled photon pairs.

2.2.5 Application: single-photon source

Parametric down-conversion simultaneously generates two photons, signal and idler, spontaneously. Since the process is probabilistic, the photons tend to bunch and measuring the second-order coherence function of either the signal or the idler arm gives the statistical properties of a thermal source, i.e. $g^{(2)}(0) = 2$. Since the photons are always created in pairs at the same time, the detection of a photon in the idler mode implies the presence of a photon in the signal mode. This property of SPDC can be exploited to create an artificial single-photon source by using one photon as a herald for the second photon [35]. The heralded photon then shows the statistics of a single-photon source.

To test this, the idler photon is detected by a SPAD and the time t_i is tagged. The signal photon is guided to a Hanbury-Brown-Twiss interferometer consisting of a 50 : 50-beam splitter and SPADs in both outputs. The setup can be used to measure the autocorrelation function of the signal photons heralded by the idler photon. In the case of antibunching, at most one signal photon should then be detected in the interval $t_i + \tau^8$, i.e. low coincidences in the HBT interferometer. To quantify the degree of antibunching, the coherence function conditioned on the detection of an idler photon, can be expressed in the form

$$g_h^{(2)}(t_{s1}, t_{s2} | t_i) = \frac{P_{ssi}(t_{s1}, t_{s2}, t_i) R(0)}{P_{si}(t_{s1} - t_i) P_{si}(t_{s2} - t_i)} \quad (2.53)$$

where P_{ssi} is the trifold coincidence rate and $R(0)$ is the rate of pair-generation [82]. In the special case of $g_c^{(2)}(t_i, t_i + \tau | t_i) = g_c^{(2)}(0, \tau, 0)$, antibunching results in $g_c^{(2)}(0, \tau, 0) \approx 0$ which is one of the most important criteria for single-photon sources. Recently, $g^{(2)c}$ -values of approximately 0.07 using a ppKTP crystal [82] and 0.088 for an on-chip source [83] have been reported. Note that $g_c^{(2)}$ can be reduced by reducing the power of the pump laser, however, at the expense of the count rate. Unfortunately, the quality of these types of sources is intrinsically limited by the non-zero probability of multi-pair emission. Specifically, increasing the pump intensity to achieve higher brightness leads to more multi-pair emissions which in turn reduces the antibunching properties and the $g_c^{(2)}$ function. Compared to SPDC single-photon sources, 'true' single-photon sources such as quantum dots, ions and NV centers offer higher single-photon rates while retaining a large $g_c^{(2)}$ factor and high indistinguishability.

For example, the heralded SPDC source introduced in [84], based on QPM in a ppKTP, yields a down-conversion probability of 0.05 when pumped with a pulsed laser of 80MHz repetition rate at 100mW, which results in a single-photon rate of 4MHz and

⁸this interval depends on the specific experiment and the detectors used, but is typically in the regime of ns and chosen far shorter than the coherence time of the photon pair

a $g_c^{(2)}$ function of $0.02 - 0.05$. A quantum dot source such as [85], on the other hand, provides down-conversion rates as high as 0.3 at a repetition rate of 80MHz, giving a single-photon rate of 24MHz and a $g_c^{(2)}$ function of < 0.02 . Additionally, when spatial encoding is desired, the rate for higher photon numbers sharply decreases for the SPDC source due to the dependence on the down-conversion probability. The 5-photon rate is around 1Hz for the SPDC source while the quantum dot source still yields a rate of 9.5kHz.

For these reasons, real single-photon sources are slowly replacing SPDC single-photon sources in applications where high-quality single-photons are crucial. In many other applications, however, single-photon sources based on SPDC are still the option to go for based on their simplicity and versatility, in contrast to the above mentioned sources which require complicated and expensive setups to function properly and are still in the early stages of development.

2.2.6 Application: Entangled photon pair source

The second application is the creation of polarization-entangled photon pairs [36]. The setup of the source is the same as for a heralded single-photon source, however, the coherence of the photons has to be maintained during manipulation and until detection in a particular polarization basis. To ensure a high quality of entanglement (i.e. visibility and fidelity), filtering and walk-off compensation is especially important. Ideally, the state generated is one of the Bell states, the particular state determined by the type of phase-matching. As mentioned in 2.1.5, any Bell state can be transformed in any other Bell state by means of local operations, i.e. placing a phase shifter and a half-waveplate in one of the arms to control the relative phase and the polarization state of one photon, respectively.

2.3 Linear optical components

The evolution of quantum states after their creation and before their measurement is described by applying unitary operators to the state as described in Chapter 2.1.1. In a quantum optical experiment, unitary operators are implemented by linear optical components. In contrast to nonlinear elements discussed in the previous chapter, linear components leave the number of photons invariant, conserving the inner product. Of course, there are no real elements that perfectly apply the corresponding unitary due to unwanted effects including the nonzero reflectance of phase retarders, transmittance of mirrors and absorption in fibers. Fortunately, the deviations from unitarity are small enough in many cases that the operations can be assumed unitary in the following applications. Some of the unitary operators that will be introduced

in this chapter can be conveniently represented with a matrix in the Jones formalism known from classical optics. Other operators, however, have to be adapted to account for the quantum nature of the incoming states, since the outgoing state differs from the expected state in a classical treatment.

To describe the effect of multiple unitaries acting on the state successively, e.g. \hat{U}_1 first and \hat{U}_2 afterwards, the matrices are applied on a polarization state $|\Psi\rangle$ as $\hat{U}_2\hat{U}_1|\Psi\rangle$ consistent with ordinary matrix multiplication being read from right to left. We will focus on two types of components: one for controlling the spatial evolution of photons which includes the splitting and recombination of beams and one for manipulating the polarization degree of freedom, i.e. phase retarders and polarizers. Of course, these components are not generally exclusive, as can be seen in the example of polarizing beam splitters whose spatial transformation depends on the polarization mode.

2.3.1 Beam splitters

A beam splitter divides incoming light in two parts by transmitting one part and reflecting the other. In many cases, a beam splitter is made of a glass substrate coated with a dielectric material or a metal. However, also prisms or fads can induce a beam splitting operation. In classical optics, the action of a beam splitter is characterized by how much of the amplitude of the incoming light is transmitted (t) and how much is reflected (r). More technical, an incoming normalized amplitude A_1 is split in two outgoing amplitudes $A_2 = rA_1$ and $A_3 = tA_1$ such that the sum of intensities gives

$$|A_1|^2 = |A_2|^2 + |A_3|^2 = 1$$

in the case of an ideal, lossless beam splitter. This requires $|r|^2 + |t|^2 = 1$ for the reflectance and the transmittance. To describe the operation of a beam splitter for quantum input states, we quantize the classical amplitudes by assigning corresponding operators, i.e. $A_i \rightarrow \hat{a}_i$. \hat{a} and the adjoint \hat{a}^\dagger are the bosonic annihilation and creation operators defined as

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle$$

where $|n\rangle$ is a state occupied by n identical bosons, obeying the commutation relations $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$ and $[\hat{a}_i, \hat{a}_j] = [\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0$ (i.e. ladder operators acting on different Hilbert spaces commute). In the quantum mechanical description of the beam splitter, unitarity requires that the classically empty second input port of the beam splitter is occupied by a quantized vacuum field \hat{b} . Therefore, we update

the beam splitter transformation to include the vacuum field giving $\hat{c} = t\hat{a} + r\hat{b}$ and $\hat{d} = r\hat{a} + t\hat{b}$ (see Figure 2.14). This relation can be written in terms of a transformation matrix as

$$\begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} = \begin{pmatrix} t & r \\ r & t \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}$$

Expressing the complex transmittance t and the reflectance r in polar coordinates as $t = t_r e^{i\phi_t}$ and $r = r_r e^{i\phi_r}$ where $\{t_r, r_r\}$ are real numbers and $\{\phi_t, \phi_r\}$ are the phase shifts of the transmitted and reflected beams, respectively. For 50 : 50 beam splitters, as will be used in the following applications, $r_r = t_r = \frac{1}{\sqrt{2}}$. If the beam splitter is based on a dielectric layer, the transmitted and reflected beam differ by a phase factor of $\pm\pi/2$, i.e. $\phi_t/r = \phi_r/t \pm \pi/2$. We assume a $\pi/2$ shift for the reflected beam and set $\phi_t = 0$, since global phases are not observable, to get the transformations

$$\begin{aligned} \hat{c} &= \frac{1}{\sqrt{2}} (\hat{a} + i\hat{b}) \\ \hat{d} &= \frac{1}{\sqrt{2}} (i\hat{a} + \hat{b}) \end{aligned} \quad (2.54)$$

which corresponds to

$$\begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix}$$

We now apply the transformations in 2.54 to the three cases relevant in the following chapters, starting with light closest to 'classical' light, namely coherent light usually emitted by lasers⁹. As noted before, coherent light is an infinite sum of number states $|\alpha\rangle \propto \sum_{n=0}^{\infty} |n\rangle$. Applying the beam splitter transformation as defined above to an input of coherent light in one mode and the vacuum in the second mode gives

$$|0\rangle_a |\alpha\rangle_b \rightarrow \exp \left\{ \frac{\alpha}{\sqrt{2}} (i\hat{c}^\dagger + \hat{d}^\dagger) - \frac{\alpha^*}{\sqrt{2}} (-i\hat{c} + \hat{d}) \right\} |0\rangle_c |0\rangle_d = \left| \frac{i\alpha}{\sqrt{2}} \right\rangle_c \left| \frac{\alpha}{\sqrt{2}} \right\rangle_d \quad (2.55)$$

meaning a coherent state gets split in equal parts giving coherent states in both output modes. The i in mode 2 represents the phase shift of $\pi/2$ in the reflected mode. This result is not surprising, as one would also classically expect laser light to be present in both output modes of a beam splitter when illuminated. Next, we discuss the case of a single photon in one input mode of the beam splitter and the vacuum mode in the second, i.e. $\hat{a}^\dagger |0\rangle_a |0\rangle_b = |1\rangle_a |0\rangle_b$, induces the transformation

$$|1\rangle_a |0\rangle_b \rightarrow \frac{1}{\sqrt{2}} (\hat{c}^\dagger + i\hat{d}^\dagger) |0\rangle_c |0\rangle_d = \frac{1}{\sqrt{2}} (|1\rangle_c |0\rangle_d + i|0\rangle_c |1\rangle_d) \quad (2.56)$$

using 2.54.

This case was shown by Grangier in 1986 [86] and it was one of the first experiments showing the particle nature of light. Note that the output state is a pure

⁹Note that in general, most natural light sources can be made coherent by appropriate filtering

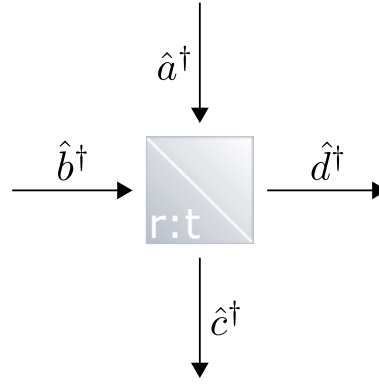


Fig. 2.14: Quantum mechanical description of a beam splitter. The transmittance is denoted by t , the reflectance by r . The input modes of the beam splitter are either occupied by a photon generated by \hat{a}^\dagger or \hat{b}^\dagger , or remain in the vacuum mode $|0\rangle$. Mode-mixing in the beam splitter results in the two output modes \hat{c}^\dagger and \hat{d}^\dagger , related to the input modes as defined in 2.54. If the input consists of either one photon or two distinguishable photons, they are transmitted with probability r and transmitted with probability t . If two indistinguishable photons are going through the beam splitter coming from the two different input modes, interference results in both photons always exiting the beam splitter in the same output mode.

bipartite entangled state. Detecting the photon in one path immediately collapses the remaining path in the state of no photon. However, this particular entanglement is of limited direct use since there is still only one single photon carrying information. Especially local operations such as bit flips cannot be implemented directly since they would have to add or remove a photon from a spatial mode and therefore require some form of nonlinearity. For this reason, the spatially entangled state is oftentimes translated to polarization which makes manipulation much easier. One tool to transform polarization qubits to spatial qubits and vice versa is a polarizing beam splitter which we are going to describe in the next Chapter. For now, let us discuss the final case of input states relevant for us, which are two single photons each of them occupying one input mode, i.e. $|1\rangle_0 |1\rangle_1$. We again apply the beam splitter transformation U_{BS} :

$$|1\rangle_a |1\rangle_b \rightarrow \frac{1}{2} (\hat{c}^\dagger + i\hat{d}^\dagger) (i\hat{c}^\dagger + \hat{d}^\dagger) |0\rangle_a |0\rangle_b = \frac{1}{\sqrt{2}} (|2\rangle_c |0\rangle_d + |0\rangle_c |2\rangle_d) \quad (2.57)$$

In this case, a curious effect emerges: The output state contains both photons either in mode c or in mode d but there is no contribution of one photon being in either mode, i.e. $|1\rangle_c |1\rangle_d$. This effect was first shown in 1987 and is known as Hong-Ou-Mandel effect after the discoverers of the same name [87]. The reason of the photons being either both in port c or in port d is a direct result of interference between indistinguishable particles of bosonic nature. We will further discuss Hong-Ou-Mandel interference in Chapter 5.9.

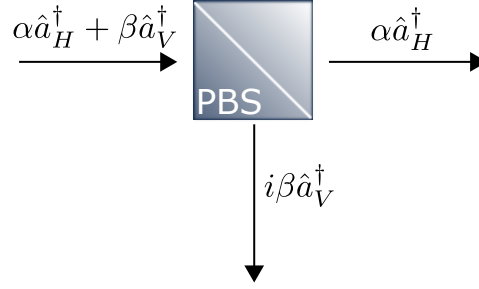


Fig. 2.15: Quantum mechanical description of a polarizing beam splitter. The input state $\alpha \hat{a}_H^\dagger + \beta \hat{a}_V^\dagger$ is split in the orthogonally polarized terms. The horizontal part with amplitude α is transmitted while the vertical part with amplitude β is reflected and is phase-shifted by i .

2.3.2 Polarizing beam splitters

Polarizing beam splitters spatially separate ordinary and extraordinary polarization components of incident light. A typical cubic PBS consists of two anisotropic (uniaxial) triangular prisms glued together and are designed to transmit horizontally and reflect vertically polarized light. The degree of separation depends on the design of the beam splitter, here we use Glan-Thomson beam splitters that reflect vertically polarized light by a 90° angle, offering a large spatial separation. They are one of the most commonly used optical components in polarization optics since they offer a convenient way to translate polarization into spatial modes enabling full tomography of the polarization state of light when photodetectors are placed in both output modes [88]. Note that while light in the state $|H\rangle$ gets fully transmitted and light in $|V\rangle$ gets reflected, a polarizing beam splitter acts as 50 : 50 beam splitter for incident light in diagonal or circular polarization states.

A special case of polarizing beam splitters are partially-polarizing or polarization-dependent beam splitters where the transmission and reflection coefficients are based on the incident polarization. Such unbalanced beam splitters are necessary for the implementation of nonlinear quantum gates, for example the CPhase (CZ) gate in section 3.3 or for state estimation protocols.

2.3.3 Linear absorbing polarizer

A linear absorbing polarizer is a filter that transmits light polarized in the direction of its transmission axis and absorbs the orthogonally polarized component. In this sense a linear polarizer acts similarly to a polarizing beam splitter separating light based on polarization. Contrary to polarizing beam splitters, where both orthogonal

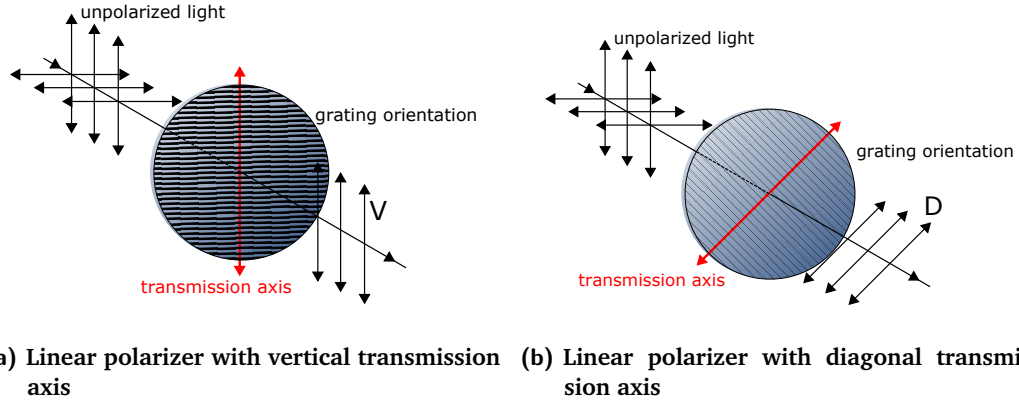


Fig. 2.16: Illustration of a linear polarizer. The polarizer consists of a stretched grating that interacts with the incident light. The component of light parallel to the grating is absorbed while the component orthogonal to the grating is transmitted. If the incident light is a photon, the polarizer acts in the same way. Arbitrary polarization states get projected onto a linear polarization state determined by the orientation of the transmission axis. (a) shows the polarizer with a vertically oriented transmission axis, therefore transmitting only vertically (V) polarized light. In (b), the polarizer is rotated to 45° , only transmitting diagonally (D) polarized light.

polarization states are preserved and can be further processed, a linear polarizer absorbs the light polarized orthogonally to the transmission axis, destroying the quantum state.

Linear absorptive polarizers are used to prepare or probe the polarization state of light in optical experiments since they can be rotated to transmit arbitrary linear polarization states. Depending on the wavelength the filter consists of a heated and stretched polaroid foil (for the visible spectrum) or stretched wires (for infrared) are used. Light polarized in the direction of the wires is absorbed due to interaction with the dipole moment of the material while orthogonal light is transmitted. The transformation matrix is given by

$$\begin{aligned}\hat{M}_H &= |H\rangle \langle H| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \hat{M}_V &= |V\rangle \langle V| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\ \hat{M}_D &= |+\rangle \langle +| = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} & \hat{M}_A &= |-\rangle \langle -| = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\end{aligned}\quad (2.58)$$

for a polarizer transmitting horizontal light \hat{M}_H , vertical light \hat{M}_V or diagonally polarized light \hat{M}_D and \hat{M}_A . As can be noted immediately, these transformations are not unitary and correspond to a projection operator $\hat{M}_m = |m\rangle \langle m|$ into a linear polarization state. Since the orthogonal polarization is absorbed, it is not possible to access a complete polarization basis simultaneously as is the case when using a polarizing beam splitter and two detectors.

2.3.4 Waveplates

A waveplate is a type of polarization retarder implemented in form of a birefringent material such as cristalline quartz that has slightly different indices of refraction in the direction parallel and orthogonal to the optical axis of the material. Therefore, the velocity of light in the material depends on the direction of polarization, leading to a relative phase shift between two differently polarized components of the incident light. Specifically, the phase of incoming light orthogonal to the optical axis of the waveplate (called slow axis) is delayed by a phase factor ϕ whereas light polarized parallel to the optical axis (fast axis) is unaffected. The effect of a waveplate acting on a polarization state is described by the operator

$$U_{WP} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\Gamma} \end{pmatrix} \quad (2.59)$$

where we set the fast axis in x-direction and the slow axis in y-direction without loss of generality. The phase shift Γ is related to the thickness of the waveplate d relative to the wavelength λ by

$$\Gamma = \frac{2\pi d(n_s - n_f)}{\lambda} \quad (2.60)$$

where n_s is the refractive index along the slow and n_f is the refractive index along the fast axis. For example, using cristalline quartz, the thickness for a half waveplate for telecom wavelength is around $88\mu\text{m}$. Apart from the desired retardance for a specific wavelength that determines the thickness of the waveplate, two other criteria for consideration are the reflectance which is minimized by coating the waveplate with an anti-reflection coating, and the dependance of the retardance on the angle between the angle of incidence and the surface of the waveplate. The latter criteria comes from the fact that the surfaces of the waveplate are not perfectly parallel as would be the ideal case. If the angle of incident differs from 0° with respect to the surface, the refraction in the material leads to an offset in the outgoing beams that is especially noticeable when the waveplate is rotated. Therefore, ensuring a high degree of parallelism is an important factor for the performance of waveplates.

A waveplate that shifts the phase by exactly Γ without excess is called zero-order plate. They offer a high stability over a broad wavelength range (bandwidth) and temperature stability. However, due to the required thickness, the fabrication and handling can be delicate. For that reason, in many cases multi-order waveplates are used where the retardance is the required phase shift is $\Gamma + n2\pi$ with $n = 0, 1, 2, \dots$. This makes the waveplate thicker and therefore easier to produce. For the designated wavelength λ , multi-order waveplates offer the same performance as zero-order waveplates, however, their bandwidth is comparably smaller and they are more temperature-sensitive (since the refractive index changes with temperature). A

compromise of zero-order retardance and the more robust design of multi-order waveplates are effective zero-order waveplates where two waveplates with a slightly different thickness are glued together such that the fast axes of the first waveplate is orthogonal to the fast axis of the second waveplate, therefore almost cancelling the phase shift, effectively reducing it to the effect of a zero-order plate. These waveplates also offer a broad wavelength range and are not as sensitive to the angle of incident compared to multi-order waveplates. If the incident light is in the linear polarization states $|H\rangle$ or $|V\rangle$, that is to say parallel or orthogonal compared to the optical axis, the waveplate doesn't change the state, only adding a global phase to $|V\rangle$. However, diagonally or circularly polarized light gets transformed into different states depending on Γ . The most commonly used waveplates sketched in Figure 2.17 are half- and quarter-waveplates:

Half-waveplate

A half-waveplate (HWP) induces a phase shift of $\Gamma = \pi$ for light propagating parallel to the slow axis. Diagonal and circular polarization states are rotated by 90 deg, e.g. $|+\rangle$ into $|-\rangle$ and $|R\rangle$ into $|L\rangle$. Equivalently, the waveplate may be rotated by an angle θ relative to the x-axis using $WP' = R(\theta)WPR(-\theta)$ which results in the following transformation matrix:

$$\hat{U}_{\text{HWP}} = e^{i\frac{\pi}{2}} \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \quad (2.61)$$

Quarter-waveplate

A quarter-waveplate (QWP) shifts the polarization along the slow axis by a quarter wavelength or $\Gamma = \pi/2$. The transformation is given by

$$\hat{U}_{\text{QWP}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 + i \cos 2\theta & i \sin 2\theta \\ i \sin 2\theta & 1 - i \cos 2\theta \end{pmatrix} \quad (2.62)$$

For example, linearly polarized light is transformed into a circular polarization, e.g. $|+\rangle$ into $|R\rangle$ and $|-\rangle$ into $|L\rangle$. On the Poincaré sphere (see Figure 2.1b), the effect of rotating a waveplate by an angle θ relative to the input state can be depicted as a rotation of the state by an angle of 2θ as seen directly in the components of the matrix in the relations 2.61 and 2.62.

Quarter- and half-waveplates are among the most important elements in quantum optics since they are used to implement single-qubit unitary operators defined in 2.13.

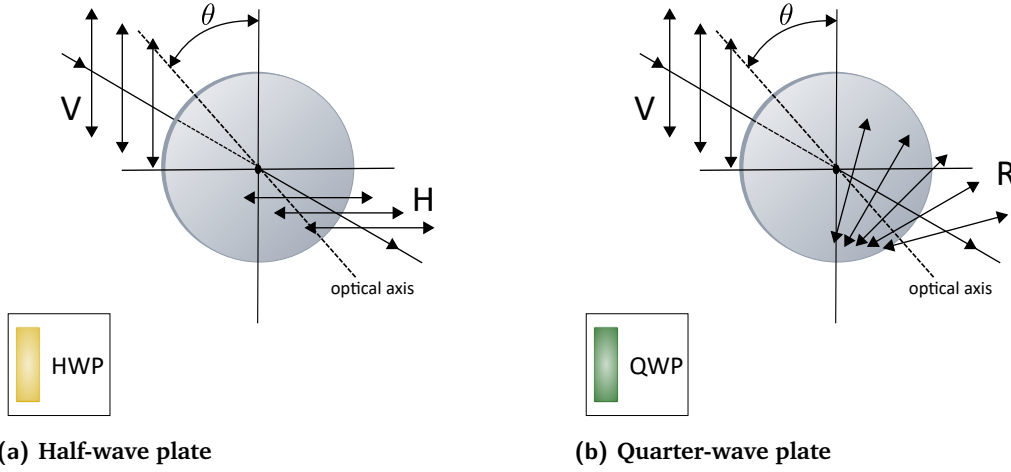


Fig. 2.17: (a) A half-wave plate with an optical axis rotated by $\theta = 45^\circ$. The half-wave plate can be used to rotate the polarization of light. Here, incident light of vertical polarization gets rotated by 2θ to horizontal polarization. The symbol on the lower left is the depiction of a half-wave plate in the following setup schemes. (b) A quarter-wave plate rotated by $\theta = 45^\circ$. It has half the thickness of a half-wave plate and transforms incident light of linear (or diagonal) polarization to circular polarization and vice versa. Here, incident light of vertical polarization gets transformed to right-handed circular polarization. The symbol in the lower left will be used to symbolize quarter-wave plates in the following experimental setups.

Specifically, we can decompose this unitary into a combination of three waveplates to induce arbitrary rotations on the Bloch sphere

$$\hat{U} = \hat{U}_{\text{QWP}}(\gamma) \hat{U}_{\text{HWP}}(\beta) \hat{U}_{\text{QWP}}(\alpha) \quad (2.63)$$

for angles α, β and γ . In table 2.1, the most important single-qubit unitary operations are listed together with the required settings of the waveplates (up to global phases). To analyze arbitrary polarization states, the state is usually rotated to the H/V -basis and split in orthogonal spatial modes using a PBS. For this transformation, a QWP followed by a HWP are sufficient [90]:

$$\hat{U}_{H/V} = \hat{U}_{\text{HWP}}(\beta) \hat{U}_{\text{QWP}}(\alpha) \quad (2.64)$$

The standard bases for polarization-qubits and the required waveplate setting to transform them to the H/V -basis are given in table 2.2. Mechanical waveplates that are rotated physically, are among of the most used optical elements to manipulate and analyze the polarization state of light, since they are available in a wide variety of specifications and comparably cheap. In applications that require fast, active polarization manipulation, however, optical elements that rotate the polarization state without having to be rotated physically offer a distinct advantage.

Single-qubit gate	Symbol	Waveplate setting
Identity	\mathbb{I}	QWP(0)HWP(0)QWP(0)
Pauli-X	X	HWP($\frac{\pi}{4}$)
Pauli-y	Y	QWP($\frac{\pi}{4}$)HWP(0)
Pauli-Z	Z	HWP(0)
Hadamard	H	HWP($\frac{\pi}{8}$)
X-rotation	$R_X(\theta)$	QWP($\frac{\pi}{2}$)HWP($-\frac{\theta}{4}$)QWP($\frac{\pi}{2}$)
Y-rotation	$R_Y(\theta)$	QWP($\frac{\pi}{2} + \frac{\theta}{2}$)HWP($\frac{\theta}{4}$)QWP($\frac{\pi}{2}$)
Z-rotation	$R_Z(\theta)$	QWP($\frac{\pi}{4}$)HWP($-\frac{\pi}{4} - \frac{\theta}{4}$)QWP($\frac{\pi}{4}$)

Tab. 2.1: Waveplate settings for the most common single-qubit unitaries. The angle θ described the rotation on the Bloch sphere, while the angles of the waveplates correspond to the physical rotation angles relative to the incident polarization. Note that any gate might also induce a global phase. Source: [89]

Input \rightarrow	QWP	HWP	\rightarrow Output
H/V	0°	0°	H/V
D/A	45°	22.5°	H/V
R/L	45°	45°	H/V

Tab. 2.2: Waveplate settings for the analysis of the standard polarization states. A quarter- and a half-waveplate are sufficient to transform arbitrary input polarizations to the H/V -basis. Source: [89]

If the goal is to rotate a linear polarization state to a different polarization, faster polarization retarders with a response time in the kHz regime, can be implemented by utilizing the response of special materials to the application of a magnetic or an electric field: For example, specific glasses rotate the polarization of a propagating wave proportional to an externally applied magnetic field, an effect known as Faraday effect [91]. In so-called nematic liquid crystals, stretched molecules are uniformly oriented and randomly distributed creating an anisotropy. Applying an electric field to this type of liquid leads to a realignment of the molecules inducing a phase shift between polarization components of propagating light, effectively creating a polarization retarder. One advantage of using polarization retarders that are proportional to an external field is that the retardance can be varied by tuning the applied field. This allows for arbitrarily tuneable waveplates where the phase shift usually grows linearly with the thickness of the rotator as well as the magnetic flux in case of a Faraday rotator and the degree of twist in a liquid crystal retarder (LCR).

In Chapter 3.2, the polarization of photons separated by around $1\mu\text{s}$ is manipulated using a device called Pockels cell. It consists of a nonlinear electro-optical crystal that induces a polarization-dependent retardance on light when an electrical voltage is applied. The Pockels effect [92] describes the change of the refractive index linearly with the electrical field strength E , i.e. $\Delta n \propto E$ and is also called linear electro-optical effect. An important figure of merit is the half-wave voltage $U_{\lambda/2}$, at which the Pockels cell acts as a half-wave plate. While the voltage that has to be applied is of the magnitude of kV for most materials, a Pockels cell offers switching times of around 1MHz, way beyond the switching times reachable with any mechanically rotated waveplates.

For the first experiment introduced in Chapter 4.2 liquid crystal retarders are used to control the polarization state of single-qubit states offering a switching speed in the kHz regime. A variable liquid crystal retarder is constructed by filling a solution of liquid crystals in a cell surrounded by quartz glass in front and back and a conductive material on top and bottom. The molecules have a stretched form and can be seen as local uniaxial crystals where the optical axis is parallel to the long axis of the molecules. With no voltage applied, the molecules are aligned in direction of the light propagation, inducing a maximal delay for all incident light. When an AC voltage is applied, the liquid crystals begin to align in direction of the electric field, therefore changing the birefringence of the material and inducing a relative phase shift to light polarized diagonally with respect to the optical axis, effectively rotating the polarization state.

When transmitting light through an optical fiber, polarization of the input state is usually scrambled due to thermal, vibrational or mechanical noise causing leakage between arbitrary polarization modes. The original polarization state is usually re-

stored using a combination of a quarter-, a half-, and another quarter-waveplate since this combination offers full control of the polarization state (a specific ingoing state can be transformed in an arbitrary outgoing state). Often times this type of polarization control is implemented directly in-fiber, where waveplates are implemented in form of fiber-stretchers. The mechanical stress induces a direction-dependent change in the refractive index, effectively acting as a phase retarder. However, since the fast and slow axis of a fiber stretcher are not as clearly distinguished as in a bulk waveplate, fiber stretchers are usually not used for exact manipulation and analyzing but for restoring a specific known state.

2.4 Single-photon detectors

The last crucial part of any (quantum-) optical setup is the readout and analysis of the information carrier used, in this case photons. Photonic detectors are all based on absorption of the photons, hence destroying the quantum state. An ideal photodetector fulfills, among others, the following properties: every single incident photon should induce a detection event in the detector, described as 'click'. This property is quantified by the detection efficiency

$$\eta = \frac{n_{\text{detection}}}{n_{\text{incident}}} \quad (2.65)$$

which is 1 for an ideal detector. Not every registered click is caused by a photon incident from the experimental setup, however, since thermal photons (generated via lattice vibrations) can cause clicks even if there are no photons impinging on the active area of the detector. These photon counts are referred to as dark count rate and is 0 in the case of an ideal detector (i.e. the detector is in the ground state). After the detection of a photon, the detector should be able to immediately detect a possible next incident photon, a feature defined by the dead-time τ_d of the detector, $\tau_d = 0$ in the ideal case. In every single-photon detector available, the absorption of a photon is translated into an electrical signal fed to a counting electronics. The time between the detection event of the photon and the translation to the electrical signal can vary, a property named jitter Δt , which is 0 for an ideal detector. In this sense, the jitter is a measure of the uncertainty in the arrival time of the detected photon. Finally, an ideal detector should be able to distinguish the number of photons impinging on it at the same time, a property called photon-number resolution. Detectors that do not possess this feature simply distinguish between photon and no photon but do not give information about the number of photons per event.

Naturally, real detectors differ from these ideal properties, but high detection efficiencies, a low dark count rate, short dead-times, and a short jitter can be achieved

in most commercial detectors available today. However, while there are techniques being developed to improve photon-number resolution [93–96], the detectors used in the experiments described here do not offer the distinction between different numbers of photons. In the following we are going to give an overview about the most important features of the types of detectors used in the experiments in the subsequent chapters.

2.4.1 Single-photon avalanche diodes

Single-photon avalanche diodes (SPAD) consist of a p-n-junction operated in reverse bias at a voltage above the breakdown voltage. A sketch of a SPAD is reported in Figure 2.18. When a photon hits the active area of the detector, an electron is transitioned from the valence to the conduction band creating an electron-hole pair in a process called impact ionization. The electron-hole pair sets off an avalanche of carriers that increases exponentially and results in a measurable current in the milli Ampere regime. This mode of operation is named Geiger mode, in contrast to an avalanche photodiode where the current response is linear to the intensity of the light, when the bias voltage is below the breakdown voltage. In order to stop the avalanche current and reset the detector for the detection of the next photon, the diode is quenched, i.e. the voltage is lowered to or below the breakdown voltage. Finally, the voltage is raised again to restore the detector to the original state, ready for a detection. The time the quenching takes is the dead-time of the detector and depends on the specific layout and material. A scheme of the working principle of a SPAD is reported in 2.19. Typical dead times of SPADs are in the range of μs to ns with a jitter in the ps regime [97]. The specific semiconductor used depends on the wavelength of interest: Silicon is used for the visible to near infrared range offering efficiencies up to 85%. For longer wavelengths, the efficiency typically decreases since the photons carry less energy. InGaAs detectors, which are used for detection in the infrared, have typical efficiencies around 20%. Increasing the bias voltage would increase the efficiency, however, due to the enhanced sensitivity, the dark count rate is increased as well. In order to reduce dark counts due to thermal photons, InGaAs detectors are typically cooled to around $200 - 250\text{K}$ which also decreases the breakdown voltage making the detector more sensitive. Impurities and defects in the crystal lattice can also lead to afterpulsing, an effect where one photon results in two current pulses, i.e. two clicks. In general, SPADs offer the possibility to detect single photons in a wide spectral range, while requiring relatively low power to operate. The efficiency, however, strongly depends on the wavelength the SPAD is constructed for.

For the detection of photons in the telecom, where the performance of SPADs is far below the efficiency reached in the visible regime, an alternative type of detector

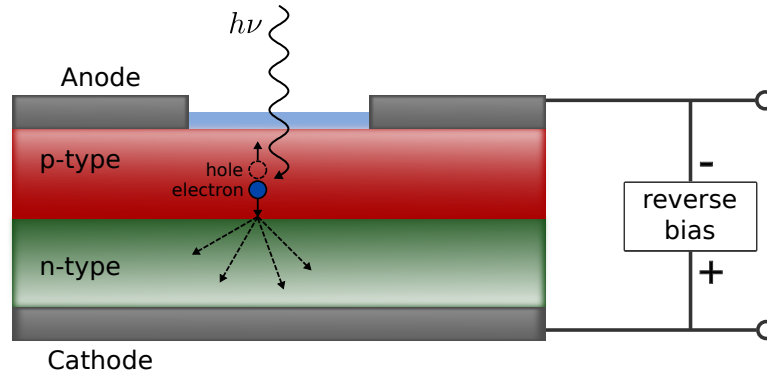


Fig. 2.18: Schematics of an SPAD. A p-type semiconductor layer is connected to an n-type semiconductor layer. A reverse bias voltage above the breakdown voltage is applied to the diode. When a photon impinges on the active area, it is absorbed by an electron in the p-type layer, creating an electron-hole pair. Due to the strong bias voltage, the electron triggers an electron avalanche when entering the n-type layer, increasing the current in the diode to a detectable magnitude.

that relies on a thermal effect and offers better properties in almost all mentioned categories is used.

2.4.2 Superconducting nanowires

Superconducting nanowire single-photon detectors (SNSPDs) are narrow, thin wires that are cooled to a temperature where the material gets superconducting (below 4K). They are biased with a current barely below the critical current density above which the resistance gets back to normal. The working principle of a SNSPD is sketched in Figure 2.20 and briefly described in the following. The absorption of a photon leads to a localized heating breaking the superconductivity at the spot of incidence. The current flows around the normal area which increases the current above the critical density resulting in the normal resistance across the whole width of the wire. This yields a voltage spike that can be detected and fed to a counting electronics. The nanowire cools off and as soon superconductivity is restored, the nanowire is ready for the next detection event. The cooling time, which is the dead-time in this case is below 100ps which is much faster than in the case of SPADs. Dark counts are naturally lower since the nanowires are cryogenically cooled and are dominated by background photons that leak into the optical fibers (if not properly shielded). Since a single nanowire only covers a tiny area, nanowires are usually put in a meandering arrangement to increase the active area. To further increase the detection efficiency, the nanowires can also be placed in a cavity that reflects photons not absorbed. SNSPDs made of NbN are highly efficient in the infrared regime and regularly reach detection efficiencies around 90% [98]. In addition to their efficiency, the low dark count rate and the short dead-time, there is no chance

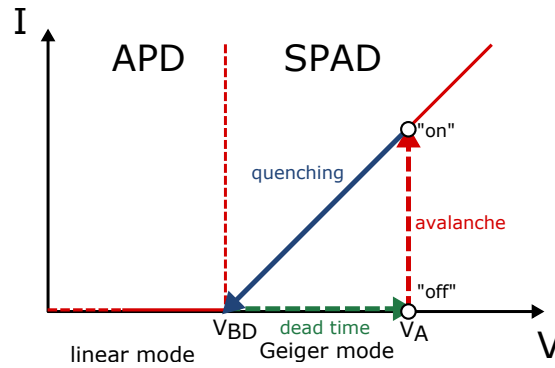


Fig. 2.19: Work cycle of an avalanche photodiode run in Geiger mode. Before a detection event, the diode is in the off state. In this state, the voltage is set to V_A , far above the breakdown voltage V_{BD} . When a photon is absorbed, an electron avalanche is triggered, leading to a current spike and setting the photodiode in the state "on". After detection, the photodiode is quenched by lowering the voltage to about V_{BD} to stop the current. The voltage is increased back to V_A to reset the photodiode for the next detection event. The time it takes the photodiode to go back to the off state after the detection of a photon is the deadtime.

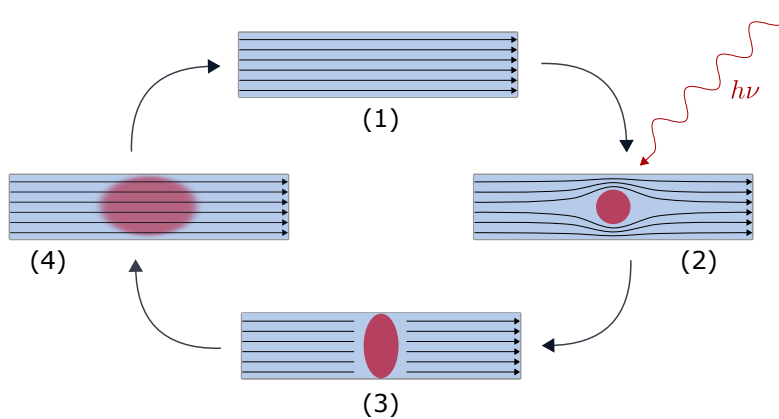


Fig. 2.20: Working principle of a SNSPD. (1) Superconduction is enabled by cooling the nanowire below a critical temperature. Current can then flow through the nanowire without resistance. (2) An incident photon with energy $h\nu$ creates a hot spot on the nanowire when absorbed. The temperature is higher than the critical temperature, breaking superconductivity at the spot of absorption. The current flow circumvents the spot, increasing the current density. (3) Due to the high current density at the sides of the nanowire, superconductivity is broken across the whole width of the nanowire. The resulting voltage spike can be detected. (4) Dissipation of the heat leads to a reduction of the temperature, eventually restoring the superconducting state and resetting the nanowire.

of afterpulsing due to the effect being thermal and not relying on charge carrier avalanches.

On the other hand, SNSPDs are far more complex to manufacture and to maintain than SPADs since they need to be cooled to cryogenic temperatures. Therefore, they are used in applications where efficient photon detection is crucial. In this thesis, the experiment described in Chapter 4.2 employs SNSPDs for the detection of telecom-wavelength photons, however, the experiment could in principle also be conducted with SPADs.

Blind quantum computing with a classical client

Since personal quantum computers are a long road ahead, increasing focus lies in the idea of a quantum server, or a quantum cloud. A client, Alice, with limited or no quantum capabilities provides an input and directions for the computation to a server, Bob, who has access to a universal quantum computer. After completion of the computation, the output is sent back to Alice. For some reason, Alice doesn't trust Bob and therefore wants to keep the details of the computation private, i.e. the input (if the input is quantum), the intended computation (if the encryption is not fully homomorphic [99]) and the output. Bob wants to help Alice but cannot (or does not want to) give Alice his device. Fortunately, quantum theory offers ways for Alice to use Bob's quantum computer without revealing information about the computation to him. Scenarios where Bob conducts a quantum computations without knowing the details are known as blind quantum computing.

The idea was first considered by Childs in 2001 [18] and developed further in the following years. In 2009, Broadbent et al published a paper describing several protocols for universal blind quantum computing able to detect a cheating server and measures for fault-tolerance [17]. The protocols make use of a special graph state called Brickwork state that allows universal computations with measurements being restricted to the xy-plane (measurements in the z-direction would reveal information to the server) [100]. The protocols described assume a client with different quantum capabilities [101]: Alice might be able to prepare the input in the form of single qubits; she might be able to conduct the final measurements and apply the final round of corrections; or she might be completely classical. While the last scenario seems to be the most desirable, it requires two space-like separated quantum servers sharing entangled states. Naturally, this improves the complexity of the implementation and reduces the applicability, at least short-term.

Numerous follow-up papers are assuming a client with the ability to prepare single-photon states (e.g. [102]). While we do not go into details of the protocol, in short Alice sends a sufficient number of qubits to Bob who entangles to create the graph state. Alice then provides the measurement angles to Bob who returns the measurement result to Alice for her to send the next angle. Alice uses random numbers to hide the real measurement angles from Bob. She might also plant 'trap'

of which she knows the measurement result to detect a dishonest Bob. After the last qubit is measured, the protocol is concluded. The protocol requires a quantum channel only in the first step to provide Bob with the physical qubits and can afterwards be discarded since the subsequent information exchanged is classical. However, as might have become clear in the Chapters describing photon sources, the creation of single-photon states in an arbitrary basis is still a task of considerable effort for the typical client. Therefore, BQC-protocols that assume a completely classical client are of special interest for short-term quantum computing solutions.

In this Chapter, we start by describing basic concepts of quantum information theory and information processing in terms of the unitary gate framework. We are then going to introduce measurement-based quantum computing (MBQC), the framework on which blind quantum computing protocols are based on. In the following part, we are going to describe the main protocol of this Chapter, classically-driven blind quantum computing, starting with the theory following the original paper [43], and concluding with the properties of the planned experimental implementation.

3.1 Quantum Information Theory

In Chapter 2.1.1, we introduced general single-qubit states $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ as a fundamental entity in quantum theory. Here, we use qubits as the fundamental building block for information encoding and manipulation. In contrast to classical bits, which can take binary values, qubits can take infinitely many values quantified by the probability amplitudes α and β . Since the 1980s, it is strongly believed that computers based on qubits can outperform classical computers in various tasks. Well-known applications include the simulation of quantum systems [15], the determination if a function is constant or balanced [11], the factorization of large numbers in prime factors [103] or the search of an entry in a database [14].

As in all applications described in this thesis, we use the polarization-degree of freedom to encode quantum information in photonic qubits or, more specifically, polarization-qubits. While photonic qubits are resilient against environmental decoherence and single-qubit gates can be easily realized using linear optical components, they barely interact with each other. Since universal quantum computing requires interaction between qubits, photonic qubits were for a long time ruled out as candidates for quantum computing. However, in 2001, Knill, Laflamme and Milburn showed that universal quantum computing is indeed possible with photons using linear optical components and a non-linearity in the detection process [37]. The KLM scheme is a measurement-based scheme and closely related to the one-way quantum computing scheme used for the BQC protocol discussed later. Before

focusing on measurement-based quantum computing, we are going to introduce some basic principles of quantum computing utilizing the unitary gate scheme [104]. One or more input states are transformed by the action of quantum equivalents of classical logic gates. After the desired gates have been applied, the quantum information contained in the transformed output state is readout by measurements in the computational basis $\{|0\rangle, |1\rangle\}$. Quantum logic gates are realized via unitary transformations that coherently evolve the quantum states in time. As in classical information theory, circuit diagrams can be used to graphically depict the evolution of a quantum state and the applied unitaries:

$$|\Psi\rangle \longrightarrow \boxed{U} \longrightarrow U|\Psi\rangle \quad (3.1)$$

However, while there is only one non-trivial single-bit gate for classical bits (the NOT gate), there are infinitely many possible quantum logic gates corresponding to infinitely many possible unitary operators. Some of the most important single-qubit gates are defined in table 3.1. Note that in this chapter, although all single- and two-qubit gates introduced are unitary operators, they are written without the hat to improve the readability.

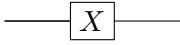
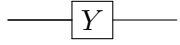
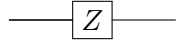
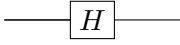
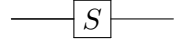
The Pauli-X gate is the quantum equivalent of the classical NOT gate inducing a bit flip and is equivalent, as the Pauli-Y and the Pauli-Z gate, to the corresponding Pauli operators introduced in 2.7. The Hadamard gate transforms states from the computational in the diagonal basis and vice versa. Finally, the phase gate $R(\theta)$ is most commonly given for two specific phases defining

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \quad (3.2)$$

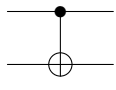
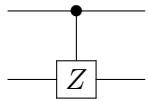
S-gate adds a phase of $\pi/2$ and the T-gate a phase of $\pi/4$ to $|1\rangle$. Both the S- and the T-gate are instances of the rotation operator $R_{\hat{n}}(\theta)$ defined in 2.11 with $\hat{n} = n_z$. As mentioned in the Chapter introduction, a control two-qubit gate is required in addition to single-qubit gates in order to ensure universality. These gates take two qubits as input and perform an operation that is conditioned on the state of one the qubits:

$$\begin{array}{c} |\Psi\rangle_1 \\ |\Psi\rangle_2 \end{array} \longrightarrow \boxed{U} \longrightarrow \text{CU } |\Psi\rangle_1 |\Psi\rangle_2 \quad (3.3)$$

The qubits are labeled control and target qubit. Depending on the state of the control qubit, the target is either left invariant or a unitary operation is performed. Two potential two-qubit gates are defined in the following table:

Single-qubit gates		
Pauli- X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	
Pauli- Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	
Pauli- Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	
Hadamard H	$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$	
Phase gate $R(\theta)$	$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$	

Tab. 3.1: Essential single-qubit gates for quantum computation. The gates correspond to unitary operators and can be expressed in form of a matrix. The circuit representation of the gates is depicted in the right column

Two-qubit gates		
CNOT/CX	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	
CPHASE/CZ	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$	

Tab. 3.2: Essential two-qubit gates for quantum computing. The controlled-NOT gate CNOT and the controlled-phase gate CPhase take two qubits as input and perform a conditional transformation on one qubit (target) depending on the state of the second qubit (control). In the circuit representation in the right column, the top channel is the control qubit, while the bottom channel is the target qubit displayed with the respective conditional operation.

The CX gate is a conditioned bit flip changing $|0\rangle \rightarrow |1\rangle$ and $|0\rangle \rightarrow |1\rangle$ if the control bit is in $|1\rangle$. The CZ gate adds a conditional phase to the target if both the control and the target bit are in state $|1\rangle$. An important property of both of these control gates is their ability to generate entanglement. A Hadamard gate in combination with a CX gate gives out one of the four Bell states depending on the input qubits. For the purposes discussed in the following Chapter, however, the CZ is the more suitable candidate: applied on a two-qubit state it induces the transformation

$$\text{CZ} |i\rangle |j\rangle = (-1)^{ij} |i\rangle |j\rangle \quad (3.4)$$

i.e. an input state $|1\rangle |1\rangle$ acquires a phase shift of π . Note that the CZ gate is symmetric with respect to labeling of control and target qubit ($i \leftrightarrow j$).

Using single-qubit gates and one control gate, a universal set of gates can be constructed such that all possible n-qubit operations on a quantum computer can be approximated by a finite sequence of gates of that set¹. A common universal gate set is $\{\text{CX}, S, T\}$. While entanglement-generating gates are necessary for a universal gate set, they are not alone sufficient to ensure an advantage compared to classical algorithms in terms of efficiency [106]. This requirement is met by the inclusion of the T-gate which results in algorithms that cannot be simulated efficiently classically (i.e. the simulation requires exponential time).

Up until now, we used the unitary circuit model of quantum computing to introduce the different types of quantum logic gates. The computations is implemented by the application of unitary gates on qubits, in effect coherently evolving the system in time. To readout the results of the computation at the end, the quantum states are measured which collapses the quantum state, converts the quantum into classical information and concludes the circuit. There are, however, numerous models for quantum computing which can prove more suitable than the circuit model for specific applications, such as the adiabatic model [107][108], boson sampling [109] or the topological model. For blind quantum computing introduced in Chapter 3 and the experimental application, the most suitable mode is, however, one-way quantum computing, a universal, measurement-based model for quantum computing.

¹since there are (uncountably) infinite possible unitary quantum gates, an exact reconstruction of an arbitrary unitary is not possible using a finite set of gates. We can, however, simulate an arbitrary unitary using a finite sequence of certain gates resulting in a bounded error. Additionally, it has been proven that the number of gates required for the simulation grows logarithmically, i.e. the simulation using a universal gate set is feasible [105]

3.2 Measurement-based quantum computing

In contrast to the unitary circuit model, measurement-based quantum computing is based on encoding the computation in adaptive sequential measurements. While they are conceptually different, they are computationally equivalent and quantum gates encoded in an MBQC scheme can also be depicted in terms of a circuit. The main driving factors behind MBQC are implementations of instantaneous quantum poly-time machines related to the research of the advantage of quantum computers, and, important in this thesis, blind quantum computing. In any case, the fundamental principle of information processing in MBQC models is the encoding of unitary transformations through quantum teleportation induced by measurements.

In principle, measurement-based quantum computing can be divided in two schemes which both rely on quantum teleportation: the Knill-Laflamme-Milburn (KLM) scheme which is based on Bell pairs and two-qubit measurements including ancilla qubits, and the one-way computing scheme (1WQC) introduced by Raussendorf and Briegel, which relies on highly entangled cluster states and single-qubit measurements [42, 110]. Both models are equivalent and based on the same fundamental principles [111]. However, since the one-way model is more suitable for blind quantum computing, we are going to restrict our discussion to this model from now on and furthermore use the term MBQC to refer to one-way quantum computing exclusively as is the case in most publications.

One-way quantum computing schemes start with the generation of a resource state, a highly entangled multi-qubit state, and proceed with the computation via measurement of single-qubits of the state in a suitable basis. The resource state is consumed in this process and since measured qubits can't be recovered, one-way computing is irreversible or, 'one way'.

The general resource state used is an undirected graph $G=(V,E)^2$ [112], an n -dimensional set of vertices (qubits) connected by edges (entanglement between vertices) (figure 3.1). A graph state $|G\rangle$ is defined as

$$|G\rangle = \prod_{a,b \in E} CZ^{(a,b)} |+\rangle^{\otimes n} \quad (3.5)$$

where CZ is applied to pairs of vertices (a,b) . In short, to generate the resource state is created from an input $|+\rangle^{\otimes n}$ by applying a CZ-gate to each pair of connected vertices [113]. Since CZ-gates commute, the order in which the gates are applied is not important. While graph state may refer to arbitrary topologies, the graph state defined here is special case in the form of a regular n -dimensional lattice and is

²i.e. a pair of sets V and $E \subset V \times V$ where for each $e \in E$ and $u, v \in V$, $e(u, v) = e(v, u)$

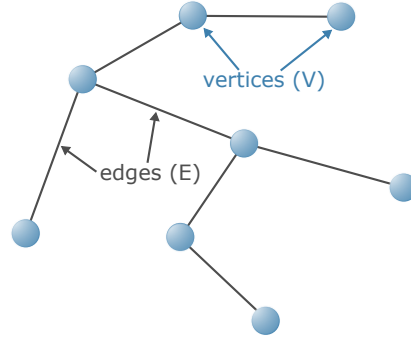


Fig. 3.1: Example of an open graph. The vertices V are partially connected by edges E .

called cluster state. Every horizontal line of physical qubits connected via CZ-gates corresponds to one logical qubit. Vertical lines depict entanglement between physical qubits in different horizontal lines.

An alternative and useful definition for the graph state is the description in terms of the stabilizer language which in turn is defined as follows: An operator \hat{A} stabilizes a state $|\Psi\rangle$ if and only if

$$\hat{A}|\Psi\rangle = |\Psi\rangle \quad (3.6)$$

i.e. the state is an eigenstate of $|\hat{A}\rangle$ corresponding to the eigenvalue $+1$ or is left invariant by the action of \hat{A} . A subspace S is stabilized by \hat{A} if $\forall |\Psi\rangle \in S$, equation 3.6 holds. Furthermore, if a subspace or state is stabilized by a set of operators $\{\hat{A}_1, \hat{A}_2, \dots, \hat{A}_n\}$, that subspace or state is uniquely determined. The stabilizer formalism is used to describe operators that fulfill equation 3.6 and are additionally elements of the Pauli group, i.e. tensor products of the identity and Pauli operators. For certain states, a set of such operators can be found to uniquely determine the state, e.g. the Bell states, codes for error correction and, of course, the graph state. In this way, the graph state 3.5 is defined by

$$\hat{K}_i := \hat{X}_i \left(\prod_{j \in N_G(i)} \hat{Z}_j \right) \quad (3.7)$$

as $\hat{K}_i |G\rangle = |G\rangle$. In words, for each qubit $i \in V$, there exists a stabilizer \hat{K}_i that consist of a Pauli X-gate applied to i and a Pauli Z-gate applied to all qubits j in the neighborhood N_G of i in the graph. The generating set of stabilizing operators can be used to describe the unitary evolution of a state $|\Psi\rangle \rightarrow \hat{U}|\Psi\rangle$ by updating the operators $\hat{A}_i \rightarrow \hat{U}^\dagger \hat{A}_i \hat{U}$ accordingly. This way of describing the evolution of a state is especially helpful in MBQC where measurement outcomes influence subsequent measurements. Since certain operations such as Pauli gates map stabilizer states to stabilizer states, it can be used to track and find the most efficient way to handle

the effect of measurements. Finding the stabilizers for a specific cluster state also uniquely identifies its structure, making it a tool to find the graphical depiction of the state. After the graph state is prepared using $|+\rangle$ input states and applying the entangling CZ-operator, the resource is ready for the computation:

As mentioned, the computation process in MBQC is encoded in single-qubit measurements on the cluster state. The state or, more precisely, the entanglement between the resource qubits, is consumed during the process. As in the circuit model, an appropriate universal set of gates can be constructed for MBQC. We define the gate set in terms of unitary operators and include a Hadamard-rotated phase gate

$$J(\theta) := HR(\theta)_z = \begin{pmatrix} 1 & e^{i\theta} \\ 1 & e^{-i\theta} \end{pmatrix} \quad (3.8)$$

where H and $R(\theta)$ are both defined in 3.1 (and $J(0) = H$). Since any single-qubit unitary can be decomposed in a series of rotations $\hat{U} = J(\theta_0)J(\theta_1)J(\theta_2)J(\theta_3)$, combining $J(\theta)$ and the required two-qubit gate CZ, we arrive at the universal gate set $\{CZ, J(\theta)\} \forall \theta$ for MBQC.

While the CZ gates are applied in the preparation of the state, single-qubit gates, i.e. rotations on the Bloch sphere are encoded in the measurement bases. The bases used are

$$\begin{aligned} M_j &:= \{|0\rangle, |1\rangle\} \\ M_j^\theta &:= \{|+\theta\rangle, |-\theta\rangle\} \end{aligned} \quad (3.9)$$

where the states of M_j^θ are defined as

$$\begin{aligned} |+\theta\rangle &:= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \\ |-\theta\rangle &:= \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta}|1\rangle) \end{aligned} \quad (3.10)$$

with $\theta \in [0, 2\pi]$. Measuring qubit j in the computational basis M_j , disentangles it from the rest of the graph state and corresponds to the Z -axis on the Bloch sphere. If the outcome of the measurement is 1, a Z correction gate has to be applied to the former neighbors of the qubit. Measurements in the computational basis are required for the creation of specific cluster states as will be shown later. The basis where the computation is carried out is the M_j^θ -basis covering the xy-plane of the Bloch sphere: measuring a qubit in this basis is equivalent to a rotation $J(-\theta)$ on an entangled qubit in the cluster state up to X or Z gates when the outcome is 1. These correction gates are necessary due to the inherent randomness of quantum measurements. Since the outcome for a measurement on qubit j is $s = 0, 1$, following measurement angles have to be adapted in the case of $s = 1$ in order to make the computation

Finally, measuring the first qubit in the $|\pm_\theta\rangle$ -basis results in the outcome s_1 and the final state

$$|\Psi\rangle_{\text{out}} = X_2^{s_1} J(-\theta)_2 |\Psi\rangle_2 \quad (3.14)$$

i.e. $|\Psi\rangle$ was teleported to the second qubit including the $J_z(-\theta)$ -gate and an X-correction if $s_1 = 1$. Since this teleportation scheme can be concatenated, arbitrary single-qubit gates can be implemented while correction gates are applied depending on the measurement outcome of the last qubit.

To implement a general single-qubit gate, 4 qubits in a linear cluster state are sufficient. Employing the teleportation scheme, i.e. measuring qubits 1 – 3 successively in the corresponding basis gives the measurement results s_1, s_2, s_3 and results in the output state

$$|\Psi\rangle_{\text{out}} = X_4^{s_3} J(-\theta_3)_4 X_4^{s_2} J(-\theta_2)_4 X_4^{s_1} J(-\theta_1)_4 |\Psi\rangle_4 \quad (3.15)$$

If desired, the Pauli corrections can be commuted through the rotations to give a result of the form of 3.13. As can be seen, the order of measurements is fixed since the Pauli corrections and the measurement angles depend on the outcomes s_i . One-dimensional cluster states are enough to implement single-qubit rotations which can be simulated classically [106].

For universal quantum computing, two-qubit gates are required which, in MBQC, are implemented using 2D cluster states: these states contain vertical lines corresponding to the entanglement of logical qubits. A natural two-qubit gate to implement is the CZ-gate as it is already used for the generation of the resource state. It can be implemented in form of the cluster state in figure 3.3, called horseshoe cluster. Two single-qubit teleportations are applied and $J(0) = H$ (since single-qubit rotations can be shifted in the preparation phase for $|\Psi\rangle \otimes |\phi\rangle$), results in

$$\begin{aligned} |\Psi'\rangle_3 &= X_3^{s_1} H |\Psi\rangle_3 \\ |\phi'\rangle_4 &= X_4^{s_2} H |\phi\rangle_4 \end{aligned} \quad (3.16)$$

for qubits 3 and 4.. The remaining qubits are then entangled by applying a CZ-gate

$$\begin{aligned} |\Psi\rangle_{\text{out}} &= \text{CZ}_{34} |\Psi'\rangle_3 |\phi'\rangle_4 \\ &= (X_3^{s_1} Z_3^{s_2} \otimes X_4^{s_2} Z_4^{s_1}) \text{CZ}_{34} (H_3 |\Psi\rangle_3 H_4 |\phi\rangle_4) \end{aligned} \quad (3.17)$$

using $\text{CZ}(X_1 \otimes \mathbb{1}) = (X_1 \otimes Z_2) \text{CZ}_{12}$ to commute CZ through the correction gates. The result is the CZ-gate applied to H-evolved states $|\Psi\rangle |\phi\rangle$ up to single-qubit X- and Z-corrections. Hence, two-qubit cluster states are universal resources for a given computation size as long as the vertical length scales faster than logarithmically with

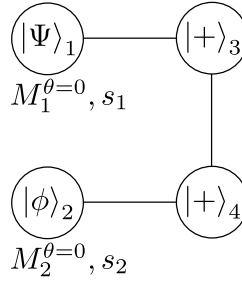


Fig. 3.3: Horseshoe cluster state. This type of cluster state implements two single-qubit teleportations and entanglement creation on the outcome states. Measuring qubits $|\Psi\rangle_1$ and $|\phi\rangle_2$ in the $M^{\theta=0}$ -basis teleports the qubits to $|+\rangle_3$ and $|+\rangle_4$, respectively, along with a Hadamard gate. Applying a CZ next entangles the teleported qubits up to the Hadamard gates and correction gates depending on the measurement outcomes s_1 and s_2 .

the length of the cluster. The specific structure of the cluster state depends on the computation. In general, if a unitary \hat{U} should be implemented,

In order to create the desired state, a large resource state is prepared and qubits j not needed for the computation are disconnected from the state using measurements in the M_j -basis, i.e. the computational basis. In case of $s_j = 1$, a Z-correction has to be added to the neighboring qubits $N(j)$. This does not change the bases required for subsequent measurements and can be taken care of by flipping the measurement results for neighboring qubits. For measurements in the M_j^θ -basis, the following angles have to be adapted if $s = 1$ to account for X-corrections. Therefore, after the preparation of the cluster state, the task left during computation is the tracking of Z-corrections and X-corrections and the appropriate adaption of the measurement angles. Using the stabilizer formalism, it is possible to identify gates to apply Z-corrections, or products of gates that result in a Z-gate, anachronically, i.e. corrections that have to be applied on a measured qubit are implemented by acting on other (unmeasured) qubits afterwards.

This is a powerful feature of the one-way model: Assume a qubit i and a neighbor $j \notin I$ (where I is the set of input vertices). If the measurement on qubit i gives $s_i = 1$, a Z-correction applied on i would be required (which is not possible after the measurement). Using the stabilizer condition, we see

$$Z_i |G(\Psi)\rangle = Z_i K_{j=N(i)} |G(\Psi)\rangle = \mathbb{1} \otimes X_j \otimes_{k \in N(j) \neq i} |G(\Psi)\rangle \quad (3.18)$$

i.e. applying $X_j \otimes_{k \in N(j) \neq i}$ on a system of qubits not yet measured has the same effect as applying Z_i . As we know, correction gates can be encoded by modifying subsequent measurement angles: X-correction are applied by $M_i^{\theta_i} Z_i = M_i^{\theta_i + \pi}$ and Z-corrections by $M_i^{\theta_i} X_i = M_i^{-\theta_i}$. The longer the computations, i.e. the larger the cluster state, the more important it is to keep track of the order of measurements

and corrections which accumulate to retain a deterministic computation. The order of measurements combined with the required correction is defined by the causal flow, that assigns to each non-output vertex measured a non-input vertex for the corrections.

A more general correction strategy can be created employing the generalized flow (gflow) [115]: with each non-output vertex a set of non-input vertices is associated for corrections (instead of a single vertex). This has several advantages including a reduction in the computational depth and correction strategies for open graphs that do not have a causal flow. Since the gflow is a fundamental building block for the blind quantum computing protocol described in Chapter 3.3, let us give a more formal definition for measurements in the xy-plane: (g, \prec) is a gflow of (G, I, O) where $g : V(G) \setminus O \rightarrow P(V(G) \setminus I \setminus \{\emptyset\})$ and \prec is a strict partial order over $V(G)$, iff for all $i \in O$

(G1) if $j \in g(i)$ then $i \prec j$

(G2) if $j \in \text{Odd}(g(i))$ then $j = i$ or $i \prec j$

(G3) $i \in \text{Odd}(g(i))$

where we introduced the odd neighborhood, $\text{Odd}(K) := \{u | |N(u) \cap K| = 1\} \pmod{2}$. The restriction of the correction set to the odd neighborhood of $g(i)$, i.e. the set of vertices having an odd number of neighbors in $g(i)$ ensures that there exist correction gates or products of corrections result in a correction gate when employing the stabilizer formalism. Concurrently, there are only even connections to the past of the measured vertex making sure that correction gates referring to the past are canceled³. If $g(i)$ contains only one element and all measurements are conducted in the xy-plane, the gflow reduces to the causal flow.

Using the definition of the gflow, a scheme for the adaption of measurement angles can be developed to account for X - and Z -corrections from previous measurements. X -corrections from $s_x = s_{g^{-1}(i)}$ and Z -corrections from all qubits $s_z = \sum_{j: i \in N_G(g(j)) | j \neq i} s_j$ can be included in the adapted measurement angle ϕ' which, after measurement of qubit i , is given by

$$\alpha'_i = (-1)^{s_x} \alpha_i + \pi s_z \quad (3.19)$$

where g^{-1} refers to the past of i . In words, for qubits in the past of i , add an X -correction and a Z -correction for all qubits $j \neq i$ such that their gflow $g(j)$ is

³ $X^2 = Y^2 = Z^2 = \mathbb{1}$

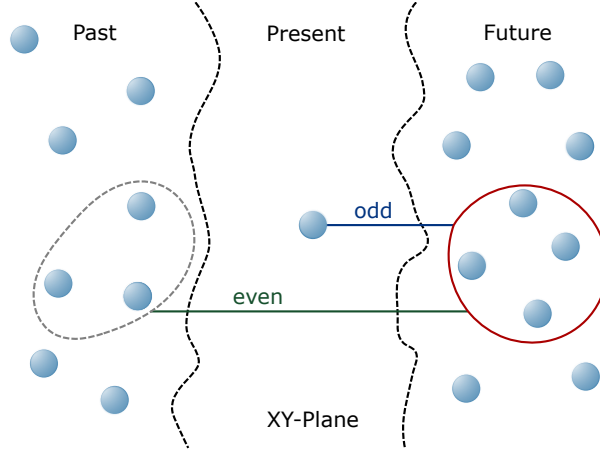


Fig. 3.4: Example for the gflow of a vertex in the present. The circled vertices in the future are connected to the present by an odd number of edges and to the past by an even number of edges. This ensures that all correction gates from the past cancel in the future and correction gates from the present remain.

a neighbor of i . It is important to note that, given an open graph and a fixed total measurement order, different gflows can be constructed in order to implement various deterministic computations. This ambiguity in the gflow can be used to hide parts of the computation from the system conducting the measurements and is the basic idea of the protocol for blind quantum computing introduced in the following Chapter. Before, we are going to introduce the fundamental principles of BQC and explain why MBQC is the natural model of choice.

3.3 Classically Driven Blind Quantum Computing

In 2017, Mantri et al. proposed a scheme exploring the possibilities of classically-driven blind quantum computing (CD-BQC) between a client and a server [43]. Using the ambiguity in information flow during a computation on a cluster state, the client is able to hide essential information from the server. More specifically, the information obtained by the server is bounded below what would be necessary to unambiguously identify the computation. In the following, we are going to introduce the basic principles of the scheme named flow ambiguity and how partial blindness on the server's side is ensured. The computation conducted by the client, Alice, is described by

$$\Delta = \{G_{n,m}, \alpha, g\} \quad (3.20)$$

where $G_{n,m} = (I, O)$ denotes a square-lattice graph state with $N = n \times m$ vertices, α the set of measurement angles and g is the gflow defining how to adapt the measurement angles. For a fixed graph, there exist multiple possible gflow patterns, consistent with the same total measurement order, implementing different computations. Hiding the gflow of the resource state from the server effectively

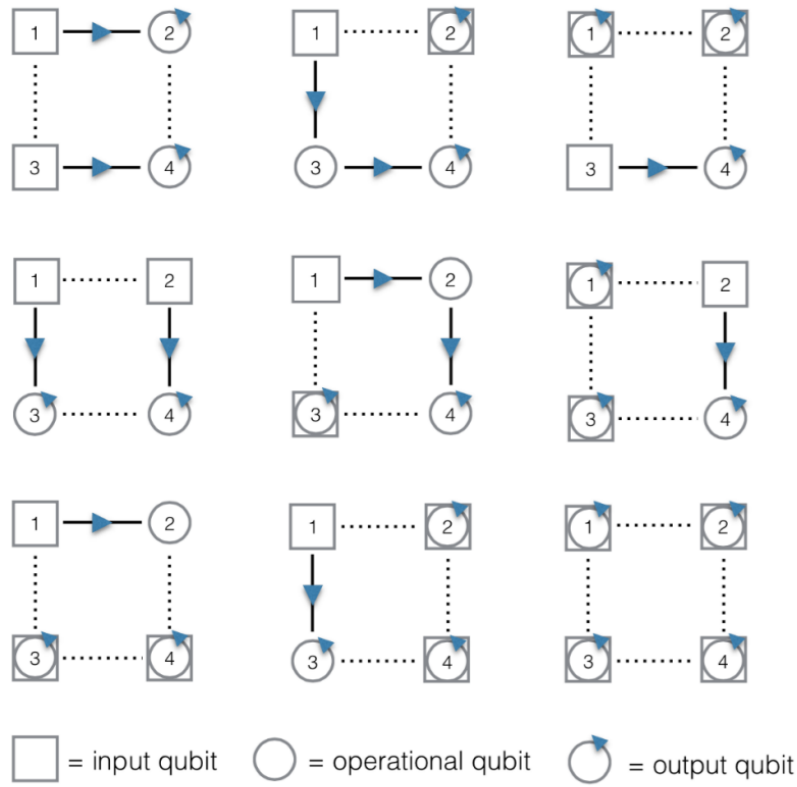


Fig. 3.5: All 9 possible gflows for the two-dimensional box cluster state. The dashed lines denote entanglement between the qubits, solid arrows denote the gflow. By choosing a specific gflow along with appropriate in- and output qubits allows to encode different computations while retaining the same total measurement pattern from 1 to 4. Source: [43]

hides the specific protocol implemented from the server. For example, figure 3.5 lists the possible gflows for a 2×2 square cluster, called a box cluster state. While the order of measurement is constant, the number and distribution of input, output and operational qubits changes, hence corresponding to the implementation different computations. The CD-BQC protocol is, as the protocol described above, interactive in the sense that Alice and Bob have to exchange (classical) information after each measurement on Bob's side.

At the start of the protocol, Alice picks a string of measurement angles $\alpha = (\alpha_1, \dots, \alpha_N)$ and generates a uniformly random bit string $\mathbf{r} = (r_1, \dots, r_N) \in \{0, 1\}$. Depending on the computation, Alice chooses a suitable gflow out of a string $\mathbf{g} = (g_1, \dots, g_M)$ where M is the number of possible gflows for a given graph. The interactive part of the protocol is conducted in N rounds (measurements) and works as follows: Alice sends the dimension $n \times m$ of the graph state to Bob for him to prepare $|G\rangle$ by entangling qubits via the CZ-gate. When the state is ready, measurements take place in rounds $i = 1, \dots, N$. In each round i , Bob sends the result to Alice who chooses a random bit r_i and, updates the measurement angle α_i necessary for the computation and,

together with the measurement outcome $b'_{<i}$, constructs a modified measurement angle α'_i she sends to Bob. α'_i depends on α_i in the following way:

$$\alpha'_i = (-1)^{s^x} \alpha_i + (r_i + s^z)\pi \quad \text{mod } 2\pi \quad (3.21)$$

where s^x and s^z are the corrections that have to be applied according to the gflow. Equation θ'_i is the corrected measurement angle defined in equation 3.19 up to the random bit r that is used to hide the real angle. Bob proceeds to perform a measurement of the i -th qubit in the xy-plane in the $M_i^{\theta'}$ -basis and transmits the outcome b'_i to Alice. She extracts the real outcome according to $b_i = b'_i \oplus r_i$, records the results in a bit string b and updates the correction set $\{s^x, s^z\}$. Note that if Bob is dishonest, b_i is not necessary equal to b'_i .

If qubit i is an output qubit ($\in O$), she registers bit b_i in the output string p_B^C . Alice and Bob repeat the procedure for all qubits in the graph in the given total measurement order. At the end of the protocol p_B^C contains the result of the computation up to final corrections. The (classical) corrections on the output string is conducted by Alice by calculating $p = p^C \oplus s_O^Z$ where p^C is the output string extracted from b and s_O^Z are the final Z-corrections on the output qubits. A graphical overview of the protocol is depicted in figure 3.6. In the end, if both Alice and Bob followed the protocol, Alice is in possession of the classical output string p corresponding to the desired probability distribution that follows from the measurements on Bob's side. Bob has information about the randomized measurement angles $\alpha' = (\alpha'_1, \dots, \alpha'_N)$ and the measurement outcomes $b' = (b'_1, \dots, b'_N)$. While Alice's secret consists of the real angles α and the information about the gflow g_i , the question is to what degree Bob can determine Alice's computation on average using the information he possesses, i.e. Bob's blindness. A full analysis of the blindness is beyond the scope of this thesis, however, we are going to give an overview of the general idea. The complete analysis is described in [43].

For this purpose, we define the real measurement angle variable A (whereas α denotes the measurement angles in a particular instance), the modified measurement angle A' , the gflow variable G and the outcome variables B and B' . Furthermore, we introduce the conditional entropy

$$H(A, F|B', A') = H(A, G) - I(B', A'; A, G) \quad (3.22)$$

where $H(A, G) = H(A) + H(G) := \log_2(N_A) + \log_2(N_G)$ and N_A, N_G denote the number of possible choices for the measurement angle variable and the gflow variable. The conditional entropy described how much information is unknown about A, G considering B', A' is known. It is equal to the difference between the information missing about A, G (which Alice has), and the mutual information

Classically Driven Blind Quantum Computation

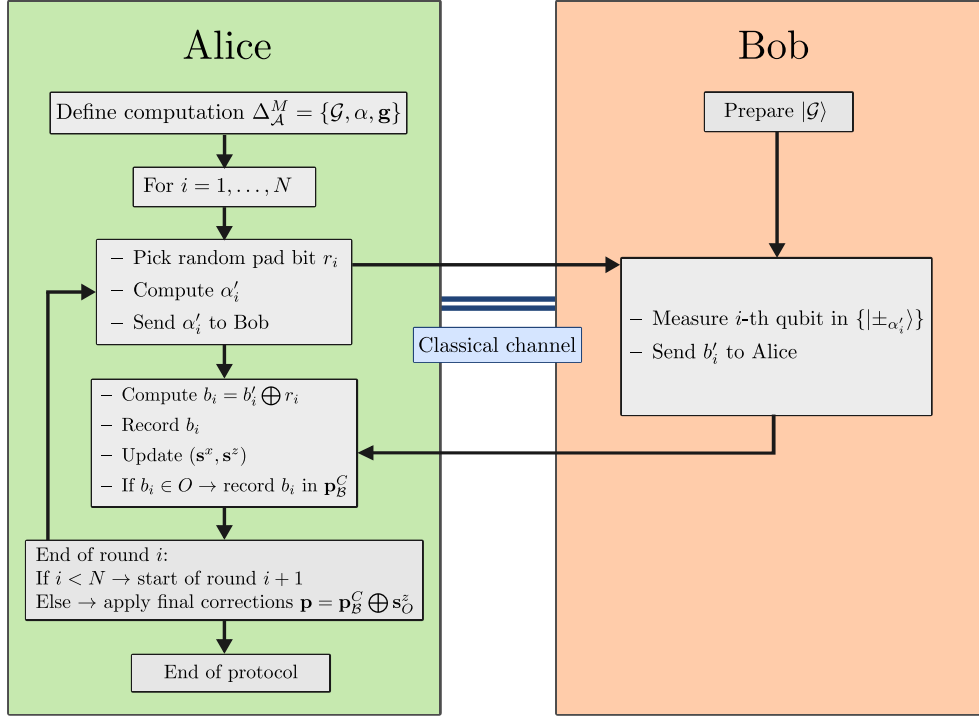


Fig. 3.6: CDBQC protocol. Classical client Alice defines a computation by a graph state \mathcal{G} , measurement angles α and the possible gflows \mathbf{g} . The computation is implemented in N measurement rounds. For each round, Alice picks a pad bit r_i and computes the randomized measurement angle α'_i which she sends to Bob using a classical channel. The quantum server Bob prepares a two-dimensional graph state $|\mathcal{G}\rangle$ and a fixed total order of measurements. Bob measures qubit i in the angle α'_i as instructed by Alice and sends back the result b'_i . Alice computes and records the real output b_i using the pad bit r_i and updates the sets of correction gates \mathbf{s}^x and \mathbf{s}^z if necessary. If the output bit is part of the computation output, she records b_i in the output string \mathbf{p}_G^C . If $i < N$, Alice continues with round $i + 1$, using a new pad bit and the correction gates to compute the new measurement angle. After the last round $i = N$, Alice applies the last set of corrections to her output string, concluding the protocol.

I quantifying how much Bob can discern about A, G knowing B', A' (the more dependent the quantities, the higher I). For a random variable X and the number of possible outcomes N_X , $n_X = \log_2 N_X$ bits are required to enumerate them. This gives a natural bound for the entropy for a variable, $H(X) \leq n_X$. In our case, to fully describe Δ_A^M , $n_A + n_G$ bits are needed. Therefore, the entropy about A, G results to $H(A, G) = n_A + n_G$ if A, G are uniformly random.

In a single run of the protocol, it can be shown (employing techniques from information theory) that the mutual information is bound: $I(B', A'; A, G) \leq H(A')$. Using that $H(A') \leq n_A$ and the definition 3.22, we get $H(A, G|B', A') \geq n_G$. If we only had one possible choice of measurement angle for each qubit, $n_A = 0$. However, this is not allowed by the Gottesmann-Knill theorem. A minimal set of angles not simulable classically is given by the set

$$\alpha = \left\{ \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}, \frac{7\pi}{4} \right\} \quad (3.23)$$

In this case, for each θ_i , and since $n_{\theta_i} = \log_2 4 = 2$ we get $n_A = 2N$. Therefore $H(A') = n_A$ ($n_A = n_{A'}$). Per qubit measured, Bob can gain 2 bits of information at most. We can apply these relations to the case of cluster states $G(I, O)_{n,m}$ and a number of gflows that, in addition to the standard properties, obey

$$(G4) \text{ if } k \in N(i)N(j) \text{ and if } k \in g(i), \text{ then } k \notin g(j) \quad (3.24)$$

to simplify the counting of flows. The length of the string of possible gflows is given by $M = n_G = \log_2 N_G$. A lower bound for M is given by counting the possible number of flows that obey (G1)-(G4). Therefore

$$N_F \geq \#G(I, O)_{n,m} \quad (3.25)$$

where $\#G(I, O)_{n,m}$ is the number of ways an open graph can be constructed such that G1-G4 are satisfied. To find $\#G(I, O)_{n,m}$ for a given dimension N , the open graphs are cut through edges in a specific way (details in [43]) and, it can be shown that $\#G(I, O)_{n,m}$ grows exponentially with the number of graph dimensions assuming $m = \text{poly}(n)$ (for universality) and $N = n \times m$. Hence,

$$n_F \geq \log_2 \#G(I, O)_{n,m} \approx 1.388N \quad (3.26)$$

which results in a conditional entropy

$$H(A, F|B', A') \geq 1.388N \quad (3.27)$$

This tells us that the number of bits to determine the computation is $n_A + n_G \approx 3.388N$. But Bob only gets $2N$ bits of information as established before. Therefore,

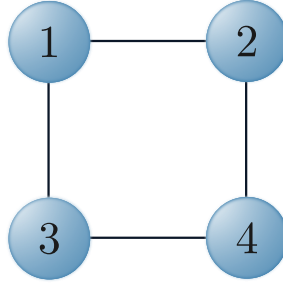


Fig. 3.7: Box cluster state used in the CDBQC protocol. The numbers denote the total measurement pattern which is the same in every computation.

Bob cannot unambiguously distinguish between the possible computations for the given graph state. It can furthermore be shown that Bob can guess Alice’s computation with $p < 1/2^{1.388N}$. This result shows that partial blindness can be ensured assuming a fully classical client in a single run of the protocol.

While this investigation of flow ambiguity provides a bound for the information leaked to Bob, question about security in a stricter sense, the verifiability of the protocol and the possibility to hide a universal set of computations after transmission of the measurement angle, are not answered yet. It is, in general, an open question if completely blind quantum computing with classical clients is possible at all [116–118]. In any case, flow ambiguity is an approach to give access to quantum resources to a classical client without handing over every detail of the computation to the server. Therefore, it is interesting to test the applicability in an experiment.

3.4 Experimental setup

For the experimental implementation, a box cluster state $|\Psi\rangle_{\square}$ as shown in figure 3.7 is chosen as the resource state. It is a 2×2 square lattice and the lowest-dimensional cluster state that has a fundamentally different entanglement structure compared to two- and three-qubit states [119].

A box cluster state can be prepared from a linear four-qubit cluster state by means of local transformations while the linear cluster is usually generated by entangling two Bell pairs. This brings us back to the unifying theme of this thesis: the creation of entangled photon pairs by means of SPDC. A laser generates pulses with a duration of 150fs, a repetition rate of 80MHz repetition rate and 500mW average power at 789nm [120]. The pulses are frequency-doubled via second harmonic generation to pump two identical 2mm type-II BBO crystals set up in line. With a low probability, photons in each pulse decay in a down-conversion event in neither, one or both of the crystal. Here, only the latter case is of use, producing two Bell pairs in the

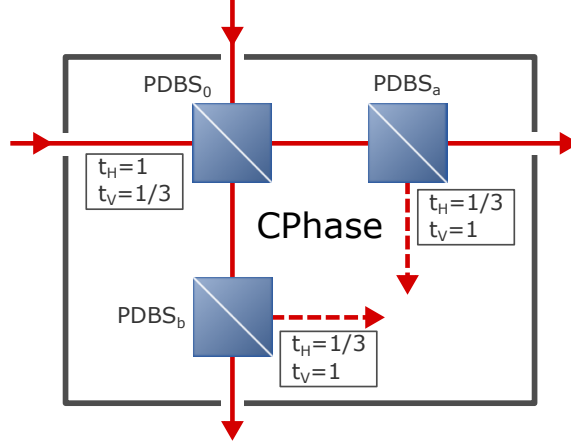


Fig. 3.8: Probabilistic CPhase gate based on PDBSs. Incident photons on PDBS₀ are transmitted and reflected bases on their polarization state. Reflected photons gain a phase of i , resulting in a conditional phase of -1 in the case of reflection for two vertically polarized photons. To equalize the amplitudes, PDBS_a and PDBS_b with reversed transmittance and reflectance relative to PDBS₀ are placed in the output modes.

$|\Psi^\pm\rangle$ -state. A half-wave plate in one arm of each emitted photon pair is used to rotate each state to $|\Psi^+\rangle$, which in total results in a product state of two Bell pairs of the form

$$|\Phi^+\rangle_{12} |\Phi^+\rangle_{34} = \frac{1}{2} (|H\rangle_1 |H\rangle_2 |H\rangle_3 |H\rangle_4 + |H\rangle_1 |H\rangle_2 |V\rangle_3 |V\rangle_4 + |V\rangle_1 |V\rangle_2 |H\rangle_3 |H\rangle_4 + |V\rangle_1 |V\rangle_2 |V\rangle_3 |V\rangle_4) \quad (3.28)$$

To transform this state into the box cluster state, a CPhase gate has to be applied to qubits 2 and 3, introducing a π -phase shift to $|VV\rangle_{23}$. The CPhase gate used in this experiment is based on two-photon interference at a polarization-dependent beam splitter (PDBS) [49] and is pictured in figure 3.8. In a PDBS, the transmission and the reflectance depend on the polarization state of the incoming photon. The transmission and reflectance for horizontal (vertical) polarization are denoted by t_H (t_V) and r_H (r_V), respectively. For a $|VV\rangle$ -polarized state in input modes a and b , $t_V = 1/3$, $t_H = 1$ and therefore $r_V = 2/3$ and $r_H = 0$. The amplitude for a coincidence event after the PDBS then results to

$$(t_V^a \cdot t_V^b) + (ir_V^a \cdot ir_V^b) = \sqrt{\frac{1}{3}} \sqrt{\frac{1}{3}} - \sqrt{\frac{2}{3}} \sqrt{\frac{2}{3}} = -\frac{1}{3} \quad (3.29)$$

where i is the phase shift for the reflected part. No interference occurs for terms containing H since $t_H = 1$. In order to equalize the amplitudes of all output terms, two more PDBS with exchanged transmission and reflectance amplitudes, i.e. $t_V = 1$ and $t_H = 1/3$, have to be inserted in both output modes in order to attenuate the H terms. This leads to a total coincidence probability of $1/3 \cdot 1/3 = 1/9$ after

the second PDBS. Hence, the gate acts as an entangling phase-gate with a success probability $p_{success} \approx 0.11$. When conditioned on the detection on coincidences, the gate transforms the input state from above to

$$\begin{aligned} CZ_{23} |\Phi^+\rangle_{12} |\Phi^+\rangle_{34} = & \frac{1}{2} (|H\rangle_1 |H\rangle_2 |H\rangle_3 |H\rangle_4 + |H\rangle_1 |H\rangle_2 |V\rangle_3 |V\rangle_4 \\ & + |V\rangle_1 |V\rangle_2 |H\rangle_3 |H\rangle_4 - |V\rangle_1 |V\rangle_2 |V\rangle_3 |V\rangle_4) \end{aligned} \quad (3.30)$$

This state corresponds to the 4-qubit linear cluster state $|\Psi\rangle_{lin}$. As described above, cluster states can be transformed in different cluster states including two-dimensional states, by means of single-qubit (Clifford) gates. For example, the horseshoe cluster state can be generated from $|\Psi\rangle_{lin}$ by applying. The desired box cluster is created by Hadamard gates $H_1 \otimes H_2 \otimes H_3 \otimes H_4$ to $|\Psi\rangle_{lin}$, resulting in

$$\begin{aligned} |\Psi_{\square}\rangle = & \frac{1}{2} (|0\rangle_1 |+\rangle_2 |0\rangle_3 |+\rangle_4 + |1\rangle_1 |+\rangle_2 |1\rangle_3 |+\rangle_4 \\ & + |0\rangle_1 |-\rangle_2 |1\rangle_3 |-\rangle_4 + |1\rangle_1 |-\rangle_2 |0\rangle_3 |-\rangle_4) \end{aligned} \quad (3.31)$$

Note that while the Hadamard gates could be implemented using half-wave plates at 22.5° , it is more convenient to absorb the gate in the measurement basis as described in Chapter 3.2. In the final step, swapping or simply relabeling of qubits 2 and 3 results in the desired box cluster state and concludes the preparation of the resource state.

Using the box cluster state, the main part of the protocol can be started: A primary set of measurement angles α is chosen by the client according to the desired computation. During the experiment, the active post-processing of the results and modification of the measurement angles is realized by a field-programmable gate array (FPGA). Since no correction gates have to be applied to the first photon to be measured, i.e. $\alpha_1 = \alpha'_1$, it is directly guided to a polarization analysis setup consisting of a PBS and two Si single-photon detectors, simultaneously heralding the arrival of the three other photons. For the polarization rotation that has to be applied to photons 2 – 4, a novel approach is implemented:

To minimize resources on the server's side, all three photons are guided through a single Pockels cell in narrow spatial modes. The Pockels cell is connected to the FPGA and acts as a half-wave plate when a high voltage is applied. A crucial advantage of a Pockels cell compared to mechanical wave-plates is the high switching speed of 1MHz. Since the measurements are conducted successively and the angles have to be adapted, photons 3 and 4 have to be delayed delayed in an optical fiber it is of high importance to keep decoherence effects to a minimum. The minimal set of angles required for universality as introduced in equation 3.23, i.e.

$$\alpha_1 = \frac{\pi}{4}, \quad \alpha_2 = \frac{3\pi}{4}, \quad \alpha_3 = \frac{5\pi}{4}, \quad \alpha_4 = \frac{7\pi}{4} \quad (3.32)$$

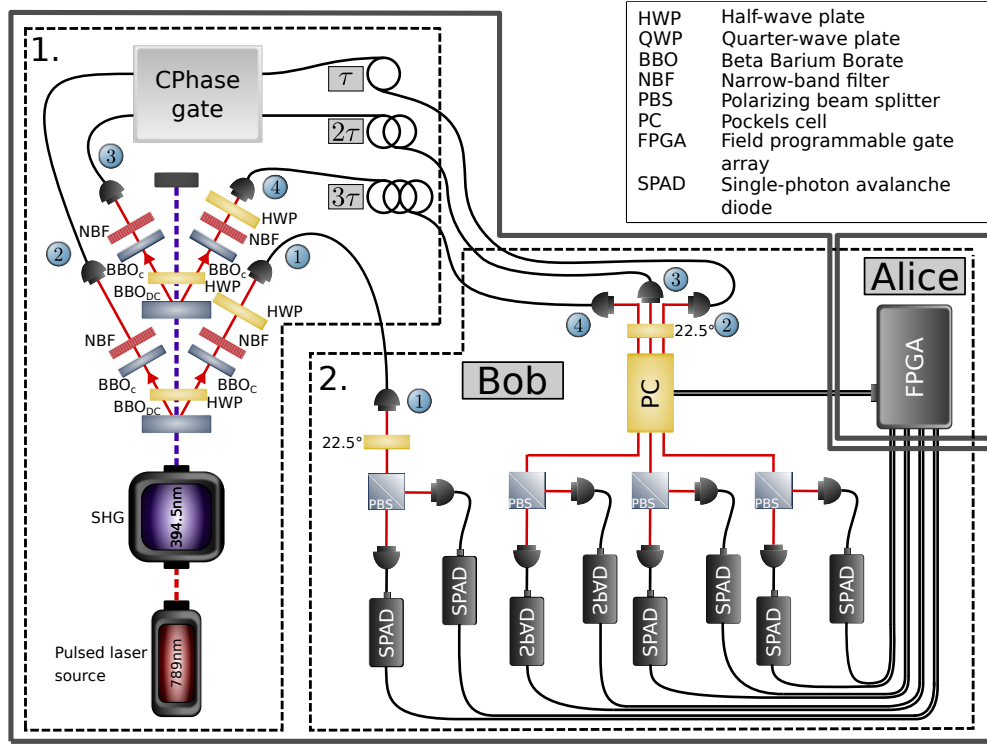


Fig. 3.9: Schematics for the experimental implementation of the CDBQC protocol. On the server side (Bob), a pulsed laser beam at 794nm is converted to 394.5nm in a nonlinear crystal via second harmonic generation SHG. The emitted beam pumps two type-II BBO crystals (BBO_{DC}) to generate two $|\Psi^-\rangle$ states. Half-wave plates and compensation BBOs (BBO_{C}) are placed in each signal and idler arm to compensate the usual walk-off effects. Narrowband filters are used for spectral post-selection to improve the quality of the states. The resource box cluster state is generated by fusing the Bells states. This is achieved by entangling qubits 2 and 3 via application of the CPhase gate and subsequent swapping of the labels. Qubit 1 is measured in the M^α -basis, heralding the three subsequent qubits. To ensure the right measurement order, qubits 2, 3 and 4 are delayed by appropriate times τ , 2τ and 3τ . The measurement basis is set by a half-wave plate followed by a Pockels cell which can be turned 'on' or 'off' depending on the required angle. A PBS followed by silicon SPDADs in every output are used to analyze the polarization of the qubits. The measurement results are transmitted to the client (Alice) who registers the outcomes and sets the measurement basis for the next qubit according to the computation, the random flip and the previous outcome. After measurement of the last qubits, Alice applies the last round of post-processing to get the final result of the computation.

is accessed using the combination of a half-wave plate and the Pockels cell. The angles are accessed by rotating the $|+\rangle$ -state about the Z-axis, i.e. a rotation

$$R_z(\alpha_i) = \begin{pmatrix} e^{-i\alpha_i/2} & 0 \\ 0 & e^{i\alpha_i/2} \end{pmatrix} \quad (3.33)$$

A half-wave plate at 22.5° applies a rotation of $\pi/4$ on an incident photon, realizing the first required angle α_1 . When the Pockels cell is turned on, the additional rotation of $\pi/2$ results in the second angle $\alpha_2 = 3\pi/4$. Realizing that $\alpha_3 = \alpha_1 + \pi$ and $\alpha_4 = \alpha_2 + \pi$ allows to rotate to these measurement bases in the post-processing by simply measuring α_1 and α_3 and flipping the result (π -flip). Hence, all required measurement bases can be accessed using only a HWP and a Pockels cell. Since every photon is passing through the same Pockels cell, it is crucial to ensure that the polarization rotation is applied identically for each photon. If the action of the Pockels cell varies depending on the spatial position of the photon in the cell, information about the gflow leaks to the server which reduces the conditional entropy. After setting the desired measurement angle, the polarization state of the photons is measured using the same analysis setup as for photon 1. The measurement result is transmitted to the FPGA which records the result, updates the measurement angle accordingly and feeds an on/off instruction to the Pockels cell. After the fourth photon is measured, classical post-processing as described in Chapter 3.2 results in the output string, concluding the protocol.

In follow-up experiments, higher-dimensional cluster states could be implemented to allow for more complex computations. More qubits also allows for the inclusion of trap qubits to expose a corrupt server. Due to spatial constraints, the number of photons propagating through the same Pockels cell is limited, especially if spatial invariance has to be ensured. However, using one Pockels cell for three photons already drastically reduces the amount of optical components required. Blind quantum computing driven by classical users allows us to take the next step towards a quantum-enhanced future. Server providers are able to offer the advantages of quantum computing and simultaneously guarantee discretion. Users that want to delegate delicate computations to the quantum cloud do not have to trust the server provider to uphold secrecy but have fundamental laws of nature on their side. In this sense, blind quantum computing is quantum in two ways: it combines the speedup of quantum algorithms and the enhanced security making use of entanglement and the inherent randomness of measurements. While the advantages of quantum mechanics are straight-forward in quantum computing, a different yet intriguing approach is to use principles of quantum mechanics to improve the security of classical protocols. In the next Chapter, we are going to introduce a scheme that combines classical computing algorithms with the security provided by quantum theory. While the

scheme itself has been well-known for a long time, the implementation is only possible by making use of security only quantum theory can provide.

Commodity-based one-time programs

Self-destructing hardware has been a common trope in movies and TV shows for years¹. Usually, the agent receives secret information in form of a letter or a video tape. After the letter is read or the tape is played, they miraculously burst into flames or self-destruct in some other way. Therefore, the information cannot fall into the hands of a malicious third party and is safe with the agent. For enhanced security, the agent might have to provide an input to access the secret message such as a key or a password. We can then describe the problem in more general terms: a function f is provided that takes an input x and gives an output $f(x)$ to the agent. The agent is only able get one output and cannot reuse or copy the function.

In reality, the construction of self-destructive hardware is much less trivial. It is hard to guarantee that an adversary is not able to disable the mechanism, especially if instead of a letter or a video tape one translates the concept of one-time hardware to more modern means, i.e. a chip or a computer. If we shift the requirement of one-time usage from the hard- to the software, malicious use can in general not be avoided: classical software can always be copied in a way, therefore rendering a destructive mechanism useless.

In this Chapter, we are going to introduce the theory and implementation of quantum-enhanced one-time programs. The goal is to allow an unconditionally secure implementation of classical programs that can be evaluated once and only once.

4.1 Oblivious Transfer and One-time Programs

One-time programs are closely related to a fundamental cryptographic primitive known as oblivious transfer (OT) where a sender, Alice, transmits information to a receiver, Bob, without knowing what pieces of information are accessed by Bob. While the basic concept of OT was first described by Wiesner in the context of conjugate coding [9], it only became known (and gained attention) as OT in 1981 in a paper by Rabin [121]. Alice sends a message $a \in \{0, 1\}$ to a receiver, Bob, who

¹see e.g. Inspector Gadget or Mission Impossible

receives the message with a probability of 50%. If the message is transmitted, Bob learns m with a probability of 100%, if it is not transmitted, he learns nothing about m which is why this type of OT is known as all-or-nothing OT. Alice remains oblivious if Bob received the message during the whole protocol. Soon after, one-out-of-two oblivious transfer was developed by Even [122].

Here, Alice prepares two bits a_0 and a_1 and Bob chooses an input bit $b \in \{0, 1\}$. Bob then receives the output bit a_b without learning about Alice's other bit. Alice, on the other hand, does not know Bob's input bit and therefore can only guess which output he received. If these requirements are met, i.e. both parties do not obtain more information than they are supposed to, the protocol is said to be fully secure. It was furthermore shown that both types of OT protocols can be built from the other one, they are therefore computationally equivalent [123]. Classical OT protocols can be broken by quantum algorithms and can therefore not be constructed in an information theoretically secure way. However, even in the quantum case, no-go theorems show that perfect and information theoretically secure OT protocols cannot be realized without assuming further constraints [124–126]. Therefore, these no-go theorems have to be circumvented to implement quantum OT (QOT) protocols, for example by assuming that the adversary does not have access to a large reliable quantum memory (noisy-storage model) [127]. Using OT, two parties can implement classical non-interactive secure two-party computations, where a sender and a receiver evaluate a publicly known function without interaction [128, 129].

One-time programs are a special case of non-interactive two-party communication introduced in 2008 by Goldwasser, Rothblum and Kalai [130]: a function f can be evaluated for one input x by a receiver. No adversary (receiver or third-party) should be able to learn anything about $f(x')$ for $x \neq x'$ beyond what can be inferred from the input-output pair $(x, f(x))$. As mentioned, however, classical software can always be copied, therefore one-time programs have to rely on additional assumptions such as interaction between the parties as in OT or hypothetical hardware, e.g. one-time memories [131]. To improve the security of one-time programs, an idea is to employ the properties of quantum theory: As is well-known, in contrast to classical information, quantum information cannot be copied. The no-cloning theorem states that arbitrary quantum states cannot be cloned due to the linearity of unitary time evolution [50, 132]. Furthermore, measurements are irreversible, changing the quantum state in the process [133]. These properties allow for many classically impossible protocols such as QKD or quantum money [9]. However, as shown in 2013 by Broadbent et al. secure deterministic one-time programs are not possible even using quantum states (apart from some trivial functions) [19]. Hence, again additional assumptions have to be made for the adversary or the transmission channel to realize quantum one-time programs.

4.2 One-time programs using quantum entanglement

A related implementation of OTPs discussed here was introduced in [134] in 2018. Instead of placing limitations on the adversary's quantum capabilities, the protocol circumvents the no-go theorems by allowing for a bounded probability of error to the computation results, i.e. in the success rate of Bob obtaining the desired output $f(x)$ is $< 100\%$. It can be shown that the implementation of probabilistic OTPs allows for an advantage in security compared to classical implementations, without assuming further restrictions.

The premise of probabilistic OTPs is the delegation of a classical software from a software provider or sender, Alice, to a receiver or user, Bob. As in blind quantum computing, Alice and Bob do not fully trust each other and want do not want to leak non-essential information to the other party. Alice sends an encoded version of the software f to Bob without leaking information about the gate structure to him. Bob then provides an input x to the software on his side and receives the output $f(x)$ after which the software cannot be used again. After executing the program, Bob has knowledge about an input-output pair $(x, f(x))$ and is not be able to obtain a second output $f(x')$ for $x' \neq x$. Alice, on the other hand, has no way of finding out x and $f(x)$ since the protocol is one-way and neither specific inputs nor outputs get transferred back to her. To build the function f , Alice chooses Boolean logic gates with k inputs and 1 output, making up the gate set $\mathcal{G}^{(k)}$. All $\mathcal{G}^{(k)}$ -gates can be built from $\mathcal{G}^{(1)}$ - and $\mathcal{G}^{(2)}$ -gates, i.e. 1-input-1-output and 2-input-1-output gates. Arbitrary $\mathcal{G}^{(2)}$ -gates are constructed from a fixed and public circuit in order for Bob to process the information. This circuit, taking three $\mathcal{G}^{(1)}$ -gates as input and consisting of two $\mathcal{G}^{(2)}$ -gates (AND, OR) and one $\mathcal{G}^{(3)}$ -gate (PARITY), is depicted in figure 4.1. In total, there are four possible $\mathcal{G}^{(1)}$ -gates defined in table 4.1.

The states are constructed after fixing measurement bases on Bob's side corresponding to inputs 0 and 1. To keep Bob from learning about the measurement outcomes in the input basis *not* chosen, the measurement operators are chosen from the set of anticommuting operators for the given dimension of the Hilbert space. In the case of qubits, this is the set of Pauli matrices σ fulfilling $\{\hat{\sigma}_i, \hat{\sigma}_j\} = 2\delta_{ij}\mathbb{1}$ where δ_{ij} is the Kronecker-Delta. For the binary inputs $i \in \{0, 1\}$, we choose measurements along $\hat{\sigma}_z$ for input $x = 0$ and $\hat{\sigma}_x$ for input $x = 1$ resulting in the measurement operators $M_0 \equiv M_Z = \{|0\rangle, |1\rangle\}$ and $M_1 \equiv M_X = \{|+\rangle, |-\rangle\}$. This choice confines the measurements to the xz-plane of the Bloch sphere reducing hardware requirements in the experiment. In the xz-plane, the states to maximize the success rate for each input are depicted in figure 4.2. We can construct these states by rotating the

$\mathcal{G}^{(1)}$	input	output
\mathcal{G}_0	0	0
	1	0
\mathcal{G}_1	0	1
	1	1
\mathcal{G}_{id}	0	0
	1	1
\mathcal{G}_{not}	0	1
	1	0

Tab. 4.1: Truth tables for classical $\mathcal{G}^{(1)}$ gates. The middle column shows the two possible input bits while the right column shows the output bits depending on the gate and input

computational basis states $|0\rangle$ and $|1\rangle$ by $\pi/4$ and $3\pi/4$ around the Y-axis, e.g. \mathcal{G}_0 is encoded by

$$\begin{aligned}
\hat{R}_y(\pi/4) |0\rangle &= \cos(\pi/8) |0\rangle + \sin(\pi/8) |1\rangle \\
&= \frac{\sqrt{2+\sqrt{2}}}{2} |0\rangle + \frac{\sqrt{2-\sqrt{2}}}{2} |1\rangle \\
&= \frac{1}{\sqrt{2}} (|0\rangle + |+\rangle) \equiv |\Psi\rangle_0
\end{aligned} \tag{4.1}$$

where $\hat{R}_y(\theta)$ is the rotation operator defined in 2.11. Overall, the four states comprising the $\mathcal{G}^{(1)}$ set are

$$\begin{aligned}
\mathcal{G}_0 &\rightarrow |\Psi\rangle_0 \equiv \frac{1}{\sqrt{2+\sqrt{2}}} (|0\rangle + |+\rangle) \\
\mathcal{G}_1 &\rightarrow |\Psi\rangle_1 \equiv \frac{1}{\sqrt{2+\sqrt{2}}} (|1\rangle - |-\rangle) \\
\mathcal{G}_{\text{id}} &\rightarrow |\Psi\rangle_{\text{id}} \equiv \frac{1}{\sqrt{2+\sqrt{2}}} (|0\rangle + |-\rangle) \\
\mathcal{G}_{\text{not}} &\rightarrow |\Psi\rangle_{\text{not}} \equiv \frac{1}{\sqrt{2+\sqrt{2}}} (|1\rangle + |+\rangle)
\end{aligned} \tag{4.2}$$

which result in the output given by the respective truth table with a probability of

$$p_{\text{succ}} = \left| \left(1 + \frac{1}{\sqrt{2}} \right) \frac{1}{\sqrt{2+\sqrt{2}}} \right|^2 \approx 85.36\% \tag{4.3}$$

and the wrong output with a probability

$$p_{\text{fail}} = \left| \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2 + \sqrt{2}}} \right|^2 \approx 14.64\% \quad (4.4)$$

The overall success probability p_{succ} is optimal and equivalent to the best winning strategy in the CHSH introduced in Chapter 2.1.6. We cannot construct states to improve the success probability for one basis without reducing the success for the other basis (input) in turn. The output of the gates is encoded in the measurement outcomes in either basis. Outcome $b' = 0$ (1) is assigned to projection on the positive (negative) eigenvalue of the corresponding Pauli matrix $\hat{\sigma}_x$ or $\hat{\sigma}_z$. Therefore, after measurement, Bob is with a probability of p_{succ} in possession of the input-output pair $(x, f(x))$.

While $\mathcal{G}^{(2)}$ -gates can be constructed using a fixed circuit as described above, this method gets complicated for $\mathcal{G}^{(k)}$ -gates with $k > 2$. A more appealing way is to directly implement $\mathcal{G}^{(k)}$ gate-OTPs maximizing the success probability by using the scheme to construct $\mathcal{G}^{(1)}$ gate-OTPs as a subroutine: The binary inputs to the gates are mapped to measurement sets $\{\hat{M}_i\}$ where each measurement is composed of separable single-qubit measurements in the xz-plane, i.e.

$$\hat{M}_i = \bigotimes_{j=1}^{2^k-1} \hat{\sigma}_{ij} \quad \forall i \quad (4.5)$$

where $\hat{\sigma}_{ij} \in \{\hat{\sigma}_x, \hat{\sigma}_z\}$. Gate-OTPs for k inputs can then be described by the mixed state

$$\begin{aligned} \hat{\rho}_G &= \frac{1}{\text{Tr}(\mathbb{1})} \left(\mathbb{1} + \frac{1}{\sqrt{2^k}} \sum_{i=1}^{2^k} (-1)^{G(i)} M_i \right) \\ &= \sum_i \frac{1}{2^k} \hat{\rho}_i \\ &= \sum_i \frac{1}{2^k} \left(\sum_{j=1}^{2^k-1} \tilde{G}_{ij} \right) \end{aligned} \quad (4.6)$$

where $G(i)$ is the output of the gate G for input i and $\hat{\rho}_i$ is a set of pure states. Since each \tilde{G}_{ij} is a $\mathcal{G}^{(1)}$ gate-OTP, arbitrary $\mathcal{G}^{(k)}$ gate-OTPs can be constructed using only $\mathcal{G}^{(1)}$ states. In contrast to $\mathcal{G}^{(1)}$ gate-OTPs, there exists a whole subspace of encoding gates for higher-order gates. For example, using three linearly polarized photons, there exist four combinations of $\mathcal{G}^{(1)}$ states to encode each possible $\mathcal{G}^{(2)}$ gate which can be found in the supplementary information of [134]. Therefore, by randomly selecting from the set of possible states, the state received by Bob is equal to the mixed state ρ_G under all measurements. In the original implementation,

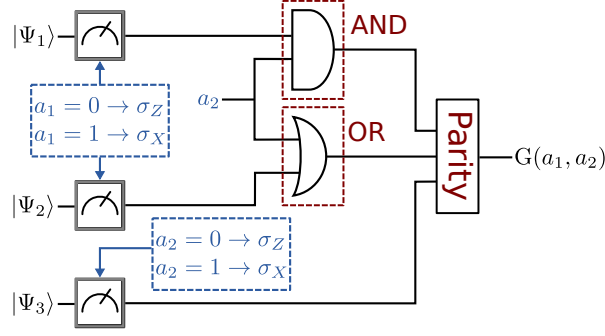


Fig. 4.1: Construction of an arbitrary $\mathcal{G}^{(2)}$ gate from three hidden $\mathcal{G}^{(1)}$ gates. Bob sets the measurement basis for qubits $|\Psi_1\rangle$, $|\Psi_2\rangle$ and $|\Psi_3\rangle$ according to his inputs a_1 and a_2 . For each $\mathcal{G}^{(2)}$ gate, Alice can choose one out of four equivalent combinations of $\mathcal{G}^{(1)}$ gates, keeping the truth table of the gate hidden from Bob. Recreated with modified notation from [134]

Alice encodes all possible $\mathcal{G}^{(1)}$ gates in certain remotely prepared single-qubit states using a heralded single-photon source based on SPDC and liquid crystal retarders. The states are sent to Bob who sets his input using fast polarization retarders as well. While several applications were shown including one-time digital signatures, the applicability of the encoding scheme is limited due to several factors. These include the limited gate rate due to the dependence on the switching rate of the active elements on both Alice's and Bob's side and the requirement of a quantum channel for the whole protocol.

To sort out these issues, reduce the hardware requirements and improve real-world applicability, a follow-up experiment was proposed and realized recently [135]. One of the most crucial improvements compared to the implementation in [134] is the separation of the quantum information exchange and the evaluation part. For the encoding of the one-time program, Alice and Bob create a cryptographic commodity using a single-qubit remote state preparation scheme. In contrast to the original implementation, only passive polarization elements are used, reducing the hardware requirements on both Alice's and Bob's side. When enough gates are encoded and transmitted, the quantum communication can be stopped since the evaluation part can be conducted via a classical channel at any time after the encoding. Furthermore, it requires only a classical channel between Alice and Bob, further reducing the technical complexity.

The scheme works as follows: Instead of preparing and sending single-qubit gate states in a fixed order, Alice shares an entangled state with Bob and employs remote state preparation to transmit a random list of \mathcal{G}_1 gates to Bob. Specifically, Alice generates a two-qubit singlet state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$, keeps qubit 1 and sends qubit 2 to Bob. The four \mathcal{G}_1 gates are then prepared by Alice by projecting her part of the state randomly uniformly in two spatial modes a and b and applying

the rotation operator $\hat{R}_y(\pi/4)$ to one mode and $\hat{R}_y(3\pi/4)$ to the other mode. This results in the states

$$\begin{aligned} |\Psi\rangle_{12}^a &= \hat{R}_y(\pi/4) |\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}} [|\Psi_0\rangle_1 |1\rangle_2 - |\Psi_1\rangle_1 |0\rangle_2] \\ |\Psi\rangle_{12}^b &= \hat{R}_y(3\pi/4) |\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}} [|\Psi_{\text{not}}\rangle_1 |1\rangle_2 - |\Psi_{\text{id}}\rangle_1 |0\rangle_2] \end{aligned} \quad (4.7)$$

each making up 50% of the total amplitude on Alice's side. Alice then sends the states on a PBS and detects in one of the two output modes, remotely preparing one of the four gate states for Bob's side. For example, state $|\Psi\rangle_{12}^a$ can be rewritten in the computational basis for Alice's qubit

$$\begin{aligned} |\Psi\rangle_{12}^a &= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2+\sqrt{2}}} [(|0\rangle + |+\rangle)_1 |1\rangle_2 - (|1\rangle - |-\rangle)_1 |0\rangle_2] \\ &= \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2+\sqrt{2}}} [|0\rangle_1 (|1\rangle - |-\rangle)_2 - |1\rangle_1 (|0\rangle + |+\rangle)_2] \\ &= \frac{1}{\sqrt{2}} [|0\rangle_1 |\Psi_1\rangle_2 - |1\rangle_1 |\Psi_0\rangle_2] \end{aligned} \quad (4.8)$$

Measurement in the computational basis \hat{M}_z then projects Bob's qubit on the state Ψ_0 or Ψ_1 . Equivalently, state $|\Psi\rangle_b$ can be rewritten to

$$|\Psi\rangle_{12}^b = \frac{1}{\sqrt{2}} [|0\rangle_1 |\Psi_{\text{id}}\rangle_2 - |1\rangle_1 |\Psi_{\text{not}}\rangle_2] \quad (4.9)$$

where the measurement on Alice's side results in the probabilistic implementation of the gates \mathcal{G}_{not} or \mathcal{G}_{id} . Alice can identify the gate sent to Bob from the measurement result on her side, i.e. if she measures $|\Psi\rangle_0$, the state sent to Bob is $|\Psi\rangle_1$. Bob also splits his part of the entangled in two spatial modes and then measures one mode in the basis \hat{M}_z and the other mode in \hat{M}_x . Again, Bob encodes the binary input in the measurement bases, i.e. $a(\hat{M}_z) = 0$ and $a(\hat{M}_x) = 1$ and assigns the projection on the eigenstates of the Pauli matrices positive eigenvalue $+1$ to the binary outcome $b' = 0$ and the negative eigenvalue -1 to the outcome $b' = 1$.

Both parties record the measurement outcomes as well as the time of detection on their side and create a table they keep hidden from the other party. Alice's table consists of the gates she sent, i.e. a string of gates $\mathcal{G} = (G_1, G_2, \dots, G_L) \in \mathcal{G}^{(1)}$ for L total gates. Bob's table consists of the input string $\mathbf{a} = (a_1, \dots, a_L) \in \{0, 1\}$ and the measurement outputs $\mathbf{b}' = (b'_1, \dots, b'_L) \in \{0, 1\}$. Note that the total number of gates L to be prepared is significantly higher than the number required for a loss-free and deterministic implementation due to the losses and the probabilistic nature of the evaluation part of the protocol. By noting their measurement results, Alice and Bob create a shared table, a cryptographic commodity for the evaluation of the

OTPs. The protocol is loss-tolerant since all measurements not corresponding to a coincidence event between Alice and Bob are discarded from the shared table. After creating a sufficiently large table, the quantum communication is stopped and all subsequent communication is conducted via classical communication. When Bob wants to evaluate the OTP, he establishes a classical channel with Alice. Using their shared table, they implement the computation by evaluating each necessary gate. The protocol requires two-way communication and works as follows for each gate:

Alice starts by choosing the gate G_i in the logic circuit comprising the program. To make sure that Bob can't gain information about the program by delaying his measurement, Alice creates a random bit r that acts as one-time pad for each gate-OTP. If $r = 0$ Alice looks for the desired gate in her table, if $r = 1$ she instead looks for the negation of the gate (e.g. $\mathcal{G}_{id} \rightarrow \mathcal{G}_{not}$). She then tells the line number to Bob who looks up the line in his table. Bob has to choose the right input to process the information, which means if the input on the line Alice tells him matches the required input, they proceed. Otherwise he tells Alice to repeat the process and they both discard the line in the table. Bob doesn't learn anything about the gate in that case because he doesn't know the pad value. If the input is right, he tells Alice who in turn submits the pad value r . Bob applies the one-time pad to his output result b'_i and gets the real result $b_i = b'_i \oplus r$. They both delete the line from the table and repeat the whole process until the final output is acquired. A graphical summary of the classical communication part is depicted in figure 4.3. The run time of the classical part scales linearly with the complexity of the function and the latency between the parties. After L rounds, the computation is finished, concluding the protocol.

Splitting the transmission and the evaluation part of the protocol also increases the complexity for Eve, an eavesdropper who wants to acquire information about either the gates or the output of the program: she needs to be present in both the quantum as well as the classical part of the protocol. If she is only there in the quantum channel, she doesn't know the value of the one-time pad and which lines are used. Furthermore, Alice and Bob can check for an eavesdropper in the quantum channel using the protocol developed by Ekert [16]. They randomly select a sample from the shared table before starting the evaluation and test for non-classical correlations between their measurement results. In an ideal case, a value of $2\sqrt{2}$ can be achieved using a CHSH inequality. If the correlation value falls below a certain threshold, Alice and Bob conclude that the channel is corrupted and discard the table. In the classical evaluation part, an eavesdropper gains nothing since no information about the gates or the output is transmitted. In conclusion, the commodity-based probabilistic OTP protocol allows for the secure delegation of classical circuits.

Part I: Creation of shared table

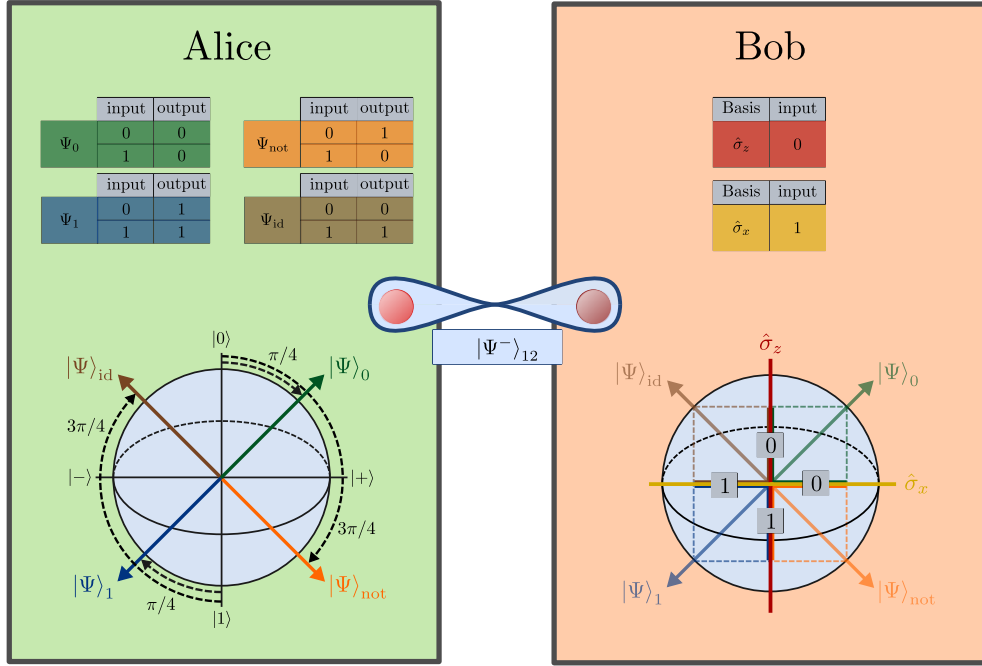


Fig. 4.2: Quantum part of the OTP protocol. Alice encodes the four $\mathcal{G}^{(1)}$ gates in four polarization-qubit states depicted on the top left including the corresponding truth tables. To prepare the gates, Alice shares an entangled state with Bob over a quantum channel. Rotating her part of the state by $\pi/4$ and $3\pi/4$ and measuring prepares the gate states $|\Psi\rangle_0/|\Psi\rangle_1$ and $|\Psi\rangle_{not}/|\Psi\rangle_{id}$, respectively. Subsequent measurement in the computational basis projects the negation of the prepared gate to Bob's qubit. Alice prepares her part of the shared table by recording the measurement outcomes. The input to the computation is chosen by Bob and encoded in the measurement basis. Measurements in the computational basis, corresponding to measurements in \hat{M}_z , define input '0' while measurements in the diagonal basis, corresponding to \hat{M}_x , define input '1'. Bob creates his part of the shared table by recording the input (measurement basis) and the output (measurement outcome). After the table has reached the required length, Alice and Bob terminate the quantum channel, concluding the quantum part of the protocol.

Part II: Evaluation of OTP

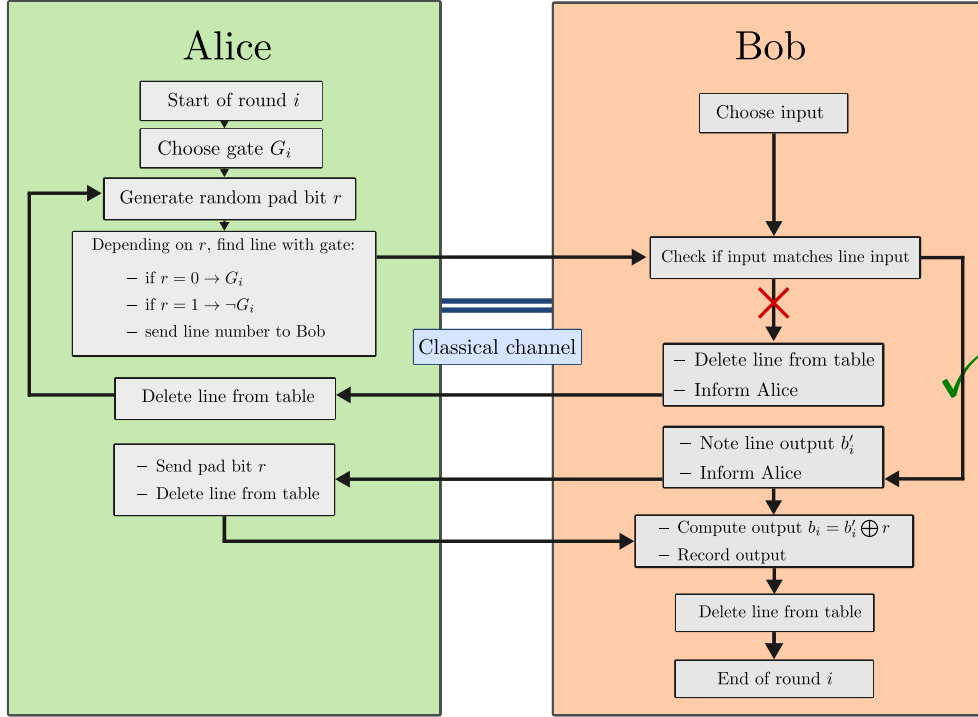


Fig. 4.3: Classical part of the OTP protocol. To evaluate the OTP, Alice and Bob need the shared table created in Part I of the protocol and communication via a classical channel. Each round i starts by Alice choosing the $G_i^{(1)}$ and Bob choosing the input. Alice also generates a random pad bit $r \in \{0, 1\}$ to one-time pad the computation. If $r = 0$, she then finds a line with the corresponding gate and sends the line number to Bob. If $r = 1$, she finds a line with the negation $\neg G_i^{(1)}$ of the gate and sends this line number instead. Bob checks if the recorded input on the line matches the required input. If no, he deletes the line from the table and informs Alice who does the same. Alice then goes back to the pad bit generation and they start over. If the input on the line in Bob's table matches his input, he records the output b'_i of the line and informs Alice. Alice sends the value of pad bit r to Bob and deletes the line from the table. Bob uses the value of the pad bit to calculate the real output $b_i = b'_i \oplus r$ which he records. He proceeds to delete the line from the table, ending round i of the protocol.

4.3 Experimental setup

In broad terms, the setup consists of three main parts: the SPDC source that produces the Bell state and two measurement setups, one on Alice's and one on Bob's site. The measurement stages are connected by a fiber that constitutes the quantum channel. The SPDC source used in the setup is of the design described in Chapter 2.2.4 on page 31 and was introduced in [81].

A continuous-wave laser at 515nm pumps a ppKTP of 30mm length and heated to around 65°C to achieve the desired wavelengths for the downconverted photons. In the crystal two down-conversion processes are phase-matched simultaneously to create non-degenerate photon pairs at 785nm and 1498nm. Both processes are superimposed creating the entangled state $1/\sqrt{2}(|HV\rangle \otimes |BR\rangle + e^{i\phi} |VH\rangle \otimes |BR\rangle)$ and separated by wavelength using a dichroic mirror. In the long-wavelength arm, a calcite crystal is placed to compensate the temporal walk-off caused by dispersion in the crystal and the relative phase ϕ is set using a LCR to produce the desired Bell state $|\Psi^-\rangle$. A tuneable narrowband filter is set in the long-wavelength path to ensure spectral indistinguishability.

The red photon at 785nm is sent to Alice's preparation stage that is fully built of in-fiber components and consists of a 50:50 beam splitter, followed by fiber paddles (acting as polarization retarders) and a PBS in each path and, in total, four silicon avalanche photodiodes with a quantum efficiency of around 60%. The 50 : 50 beam splitter randomizes the gate choice, whereas the half-wave plates are set to $\pi/16$ and $3\pi/16$ to rotate the state to one of the four $\mathcal{G}^{(1)}$ gate-OTPs. After detection in one of the four SPADs, Alice knows which gate has been sent to Bob due to the anticorrelation of the $|\Psi^-\rangle$ state by checking the states derived in 4.8. The telecom-wavelength photon is coupled to a telecom fiber and transmitted to Bob in a different building approximately 650m far away. On Bob's side, a similar setup is prepared to measure the received photons in the appropriate basis. A 50 : 50 beam splitter randomly chooses one of two measurement bases (input encoding), whereas in one of the paths a half-wave plate at $\pi/8$ is used to rotate the state to the $\hat{\sigma}_x$ basis. The PBSs then project the state onto the respective basis and four superconducting nanowire detectors with a detection efficiency of approximately 40% are used to detect the photons.

4.4 Application: One-time digital signature

The application realized using the described setup is the signing of a message using a one-time digital signature. Suppose Alice needs to grant Bob the power to sign a

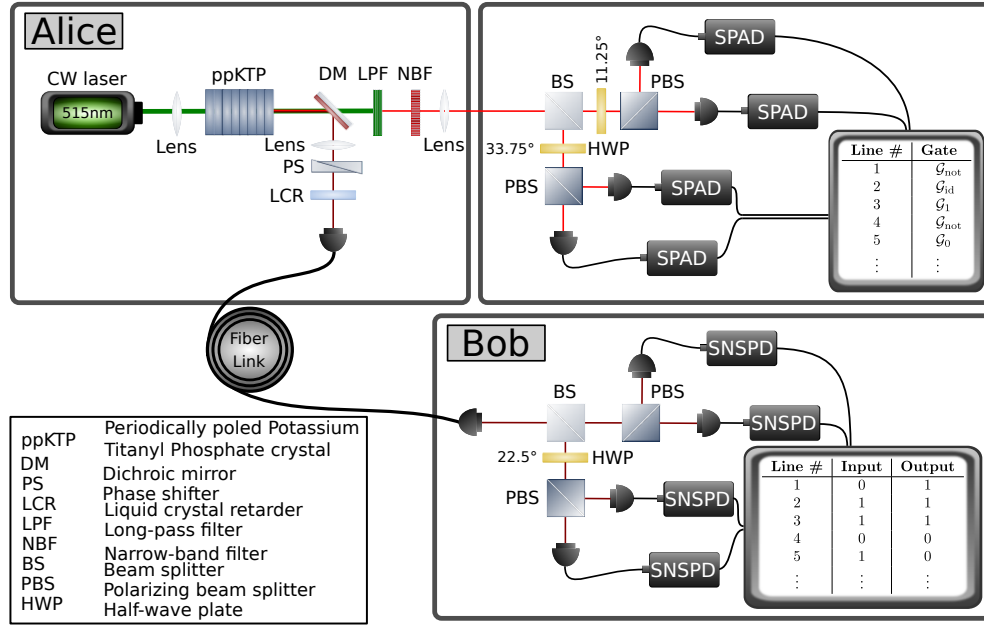


Fig. 4.4: Experimental setup for the passive OTP protocol. The setup is divided in the server part (Alice) for preparing the entangled states and encoding the $\mathcal{G}^{(1)}$ gates, and the client part (Bob) for measuring the shared part of the state and provide the input. The required $|\Psi^-\rangle$ -state is generated by a single-pass single-crystal type-II SPDC source: A continuous-wave laser emits a pump beam at 515nm, fiber paddles are used to control the polarization. The laser beam pumps a type-II quasi phase-matched ppKTP crystal where two SPDC processes are overlapped to generate pairs of non-degenerate signal and idler photons at around 785nm and 1498nm. A long-pass filter is used to remove the pump light and a dichroic mirror (DM) splits the signal and idler photons based on their wavelength. The short-wavelength photons are sent to Alice while the long-wavelength photons are transmitted to Bob over a telecom fiber link, constituting the quantum channel. To improve spectral indistinguishability, a tuneable narrow-band filter is placed in Alice's arm. Following the filter, a 50 : 50 beam splitter (BS) randomizes the gate preparation process. In the first output, a half-wave plate at 11.25° rotates the photons to the states $|\Psi\rangle_0$ and $|\Psi\rangle_1$. In the second output, a half-wave plate at 37.75° rotates the photons to the states $|\Psi\rangle_{\text{not}}$ and $|\Psi\rangle_{\text{id}}$. The states are then identified by projective measurements using polarizing beam splitters and silicon single-photon avalanche diodes (Si-SPAD). Alice uses the measurement result to identify the $\mathcal{G}^{(1)}$ gates projected on Bob's qubit by the measurement. On Bob's side a 50 : 50 BS is used to randomize the measurement bases. For input '0', Bob's qubit is measured in the computational basis, for input '1', the qubit is measured in the diagonal basis by rotation of the polarization by 22.5° using a HWP. For the detection of the telecom-wavelength photons, Bob employs PBSs and superconducting nanowire single-photon detectors (SNSPD). Bob can identify the measurement basis and the output by noting which detector clicked and records the results. Employing this scheme, Alice and Bob create the shared table to be used in the second, classical part of the protocol.

document in her name, for example a contract. However, Alice doesn't trust Bob and fears that Bob might misuse the signature to sign more than one document. Using a digital signature scheme, Alice can't be sure that Bob will not abuse the power she grants him. There is no information theoretically secure way to ensure that the signature is only used once. Using the quantum advantage for one-time programs, however, a one-time digital signature can be realized.

Alice initiates the protocol by generating a private key and encoding the encryption with that key using $\mathcal{G}^{(1)}$ gate-OTPs. For every bit of hash of the message that Bob wants to encrypt, Alice sends N gate-OTPs to Bob who hashes the message to make sure that the input to the protocol is always of the same length m . After using bit after bit of his hashed message as input to the sent gates, Bob receives the signature as output. Since he receives N gates per OTP, the total signature length amounts to $L = m \cdot N$. Note that to maintain the security of the protocol, the N OTPs per hash bit all have to be encoded individually using a different private key. To verify the signature, Bob sends the signature back to Alice combined with the signed message. Alice certifies the validity of the message by applying decryption with the key to the signature and comparing it with the hash of the plain text. For a valid signature, each bit string has to be correct in at least τ of N positions where τ is a threshold set by Alice giving the number of correctly evaluated bits to make her accept. Each gate-OTP has an inherent success probability of $P_{\text{succ}} \approx 0.85$. The overall success rate can be increased, however, by using more than one gate-OTP per bit of hash. Specifically, requiring at least $\tau \cdot N$ correct evaluations allows for the overall success probability to approach 1 asymptotically by increasing N .

We can compare the success probabilities of an honest Bob, who signs one and only one message with Alice's keys, and a cheating Bob, who tries to sign two messages. To give a bound for successful cheating, we assume the worst case where the hashes of Bob's messages differ by only one bit, and the ideal individual gate-OTP success probability of $P_{\text{succ}} \approx 0.85$. For Bob to cheat successfully, he then has to sign one line of the hash for both possible inputs, reducing the overall rate of correct outputs. Alice has to choose her threshold accordingly to maximize the difference $\Delta\tau$ of success probability between an honest and a dishonest Bob. It can be shown that choosing τ between 0.75 and 0.85 the probability of signing one message approaches one while the probability for signing two messages goes to zero for increasing N in an ideal implementation (supplementary material of [134]). For a real implementation, the optimal τ is chosen to maximize $\Delta\tau$ for a given number N of gate-OTPs per hash bit.

For example, if $N = 1000$ $\mathcal{G}^{(1)}$ gate-OTPs are encoded per bit of hash, setting $\tau = 0.776$ gives a success probability of $P_{\text{hon}} = 99.87\%$ for an honest and $P_{\text{dishon}} = 0.11\%$ for a dishonest receiver, which corresponds to a threshold difference $\tau_{\text{honest}} -$

$\tau_{\text{dishonest}} = 0.9976$ [135]. If the message is hashed using the SHA2-224 [136] algorithm which encrypts the message in a bit string of length $m = 224$, this results to $L = 224000$ total gates per program. Fortunately, to verify the signature, the gates do not have to be evaluated in a specific order which would require N rounds of classical communication. Instead, they can be simultaneous evaluation of gates reduces the necessary rounds of communication by $\log_2(L)$. For the given example, this results in 18 rounds of communication on average.

In conclusion, probabilistic one-time programs allow for the secure distribution and evaluation of functions without revealing the structure of the function itself. The one-timeness is ensured by the laws of nature and not by specific hardware. Compared to the original implementation, the new protocol reduces the requirements for sender and receiver by various factors. The encoding part through a quantum channel at telecom-wavelength is completely separated from the evaluation part which only requires classical communication. Furthermore, all active polarization switching parts have been replaced by passive elements, minimizing the input required by Alice and Bob during the preparation of the shared table. In the future, the remaining bulky parts, namely the source and the detectors can be replaced by smaller versions. In the end, both Alice's preparation setup and Bob's measurement setup could fit into portable boxes to be distributed to business or even private clients.

SPDC source in a lab course

Apart from research, SPDC sources are common sources in quantum optical lab courses due to their versatility, reliability and relative simplicity. However, since typical bulk sources consist of many individual components which have to be set up and aligned, the construction of a source can take up a lot of time of the course, leaving less time for actual experiments. This drawback can be overcome by using a source where all the components are prealigned and placed on a breadboard at fixed positions in order to maintain the alignment. One such example is the QuED by qutools. It consists of a laser diode pumping a BBO crystal, appropriate walk-off compensation crystals as well optical components to spatially and spectrally filter the emitted photons and couple them to optical fibers. The laser and the crystals are prealigned and covered by a box during operation, leaving only the coupling components open for adjustments. This design makes the source almost plug-and-play, since realignment is relatively straightforward. In this chapter, we describe the type of source used in the quED, followed by two basic experiments suitable for introductory lab courses in quantum optics.

5.1 Qutools Entanglement Demonstrator

The main part of the quED is a type-I SPDC source based on a laser diode at 405nm pumping a 2mm long BBO crystal (see figure 5.2). As described in Chapter 2.2.3, type-I phase-matching in a BBO generates a pair of o-polarized photons from an e-polarized pump photon probabilistically. Here, the phase-matching results in non-collinear emission of degenerate biphoton product states at $810 \pm 10\text{nm}$ after filtering. While type-II phase-matching directly allows for the extraction of entangled pairs from the cone intersection points, a more sophisticated technique has to be employed to create entanglement from type-I SPDC: two identical BBO crystals are set in line such that their optical axes are orthogonal to each other. An incoming photon of H (V) polarization is then downconverted into a pair of VV (HH) photons in the first or second crystal. Pumping the crystal with D- or A-polarized light creates ambiguity in the origin of the emitted photon pairs, with an approximately equal probability of downconversion occurring in either the first or the second crystal. Since the downconversion processes are coherent with respect to each other, the process results in the entangled state $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)$ being contained in the

emission cones. While the relative sign of the generated state depends on the input ($|A\rangle$ or $|D\rangle$) the remaining $|\Phi\rangle$ state can be generated by rotating a half-wave plate inserted in the pump beam by 45° . Using an additional waveplate in one of the arms of the down-converted photons, the state can be rotated to the Bell states $|\Psi^\pm\rangle$.

As in any SPDC process, the propagation of the photons through the nonlinear crystal induces temporal and spatial walk-off between the photon pairs. These effects increase the distinguishability of the photons and, in turn, reduce the coherence and the purity of the entangled state. The impact of the spatial walk-off, which depends on the length of the nonlinear crystal, can be reduced by spatial filtering of the down-converted pairs using single-mode fibers. The temporal walk-off results from the group velocity mismatch between the pump photon and the downconverted photons and leads to advanced propagation of photon pairs originating from the first crystal with respect to photons from the second crystal. To counteract, a BBO crystal is inserted in the pump beam before the downconversion crystals delaying one polarization component of the pump beam and effectively pre-compensating the walk-off. Since the downconversion is non-degenerate due to the spectrally broad laser diode, the wavelength-dependent dispersion between the pairs leads to different cone sizes after emission of the second crystal. A second BBO crystal after the DC crystals is inserted in the path of the downconverted photons to compensate this walk-off by recombining the cones. The pre- and post-compensation in combination with the spatial filtering applied here leads to entangled states of high fidelity and purity, even using a laser diode and without spectral filtering of the downconverted photons. In the case of the quED, all down-conversion components are covered by a box during operation, as depicted in 5.1. A longpass filter placed on the exit aperture of the box blocks the residual pump light. Two mirrors reflect photons from opposite points of the cones (i.e. entangled pairs) to single-mode fiber couplers which are preceded by additional longpass filters. The downconverted photons are coupled into single-mode fibers which guide them to Si-SPAD detectors contained in a control box. Between the mirrors and the fiber couplers, waveplates and polarizers can be inserted to transform the two-photon state and to project to specific linear polarization states, respectively. By inserting additional quarter-wave plates, the emitted quantum state can be fully characterized and compared to the theoretically expected state via quantum state tomography.

5.2 Quantum state tomography

In previous sections, we described the states of quantum systems using complex wave vectors. This formalism is sufficient for pure states, however, states generated in a lab are always mixed, i.e. an incoherent superposition of pure states. Since it is

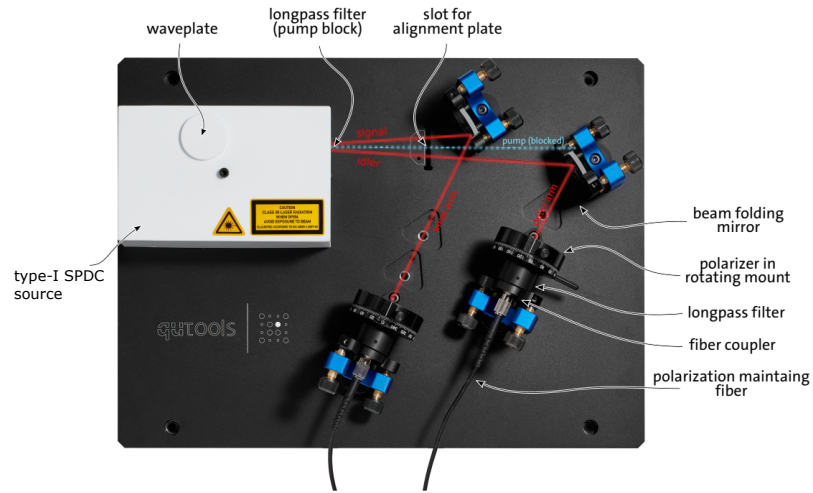


Fig. 5.1: Qutools Entanglement Demonstrator. The white box contains the type-I SPDC source. A longpass filter at the exit port of the box filters out the pump light, leaving mostly signal and idler photons at $810 \pm 10\text{nm}$. The photons are coupled to polarization-maintaining fibers using a mirror and a fiber coupler in each arm. Polarizers in front of the couplers are needed to violate a CHSH inequality and to analyze the generated biphoton state. Additional longpass filters mounted on the fiber couplers block residual pump light as well as scattered light from the environment. Source: [137]

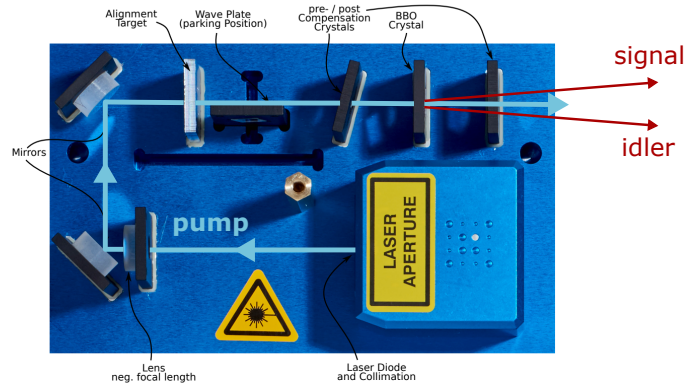


Fig. 5.2: Qutools Entanglement Demonstrator SPDC source. A laser diode emits the pump beam centered at 410nm . The beam is collimated by a telescope in the diode and a lens with negative focal length. The down-conversion process takes place in two wedged BBO crystals with crossed optical axes. Pre- and post-compensation is necessary due to the properties of the laser diode and the temporal offset of the downconverted wave packets. The waveplate, here in the parking position i.e. not inserted in the pump beam, is placed in the pump beam to induce down-conversion in both crystals, generating the entangled state $|\Phi^\pm\rangle$. The waveplate can be rotated by 180° to change the phase of the Bell state from $|\Phi^+\rangle$ to $|\Phi^-\rangle$. During operation, the source is covered by a white box. Source: [137]

important for many experiments to know the real mixed quantum state created, it is convenient to introduce density operator $\hat{\rho}$, defined as

$$\hat{\rho} := \sum_{i=0}^n p_i |\psi_i\rangle \langle \psi_i| \quad (5.1)$$

where $|\psi_i\rangle$ denotes a set of pure states $\{|\psi_i\rangle\}$ and $\sum p_i = 1$. For pure states all except one p_i are 0 and the expression simplifies to $\hat{\rho} = |\psi\rangle \langle \psi|$. The density operator fulfills the following properties:

(i) Hermiticity: $\hat{\rho} = \hat{\rho}^\dagger$

(ii) Trace unity: $\text{Tr}\{\hat{\rho}\} = 1$

(iii) Positivity: $\langle \psi | \hat{\rho} | \psi \rangle \geq 0 \quad \forall |\psi\rangle$

and additionally idempotency: $\hat{\rho}^2 = \hat{\rho}$ for pure states, while $\text{Tr}\{\rho^2\} < 1$ for mixed states. The second and third properties stem from the normalization of probabilities and the non-physicality of negative probabilities, respectively.

To derive the density matrix for a specific polarization-qubit state, the contribution of every polarization has to be accounted for. In practice, this means that measurements have to be conducted in a complete set of mutually unbiased bases, for example $\{H, V\}, \{A, D\}, \{R, L\}$ for polarization qubits.

5.2.1 Single-qubit tomography

In the most basic case, i.e. a single-photon state, the state vector can be visualized on the Bloch sphere where the three orthogonal bases correspond to the set of Pauli matrices $\{\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3\}$ and the origin is at $\hat{\sigma}_0/2 \equiv \mathbb{1}/2$. The density operator for the state can then be written as a linear combination of the Pauli matrices, i.e.

$$\hat{\rho} = \frac{1}{2} \sum_{i=0}^3 S_i \hat{\sigma}_i \quad (5.2)$$

The coefficients S are called Stokes parameters originally introduced in classical optics as a measure for the electric field amplitudes [138]. They are defined as $S_i := \text{Tr}\{\hat{\sigma}_i \hat{\rho}\}$ and obey

$$0 \leq \sum_{i=1}^3 S_i^2 \leq 1 \quad (5.3)$$

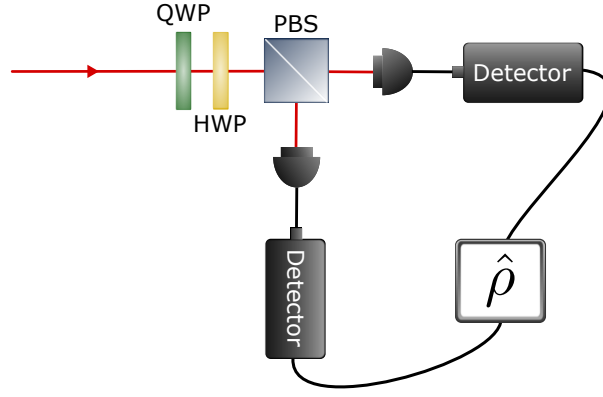


Fig. 5.3: Experimental setup for a single-qubit state tomography. A quarter- and a half-wave plate rotate arbitrary incident polarization states to a linear polarization. The state is then analyzed via projective measurements using a polarizing beam splitter (PBS) and some type of single-photon detectors. By measuring in all mutually unbiased bases, i.e. $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$, the density matrix of the polarization-qubit can be determined up to experimental accuracy.

and $S_0 = 1$ due to normalization. The upper bound of 5.3 describes pure states located on the surface of the Bloch sphere. Mixed states lie below the surface ($0 < S^2 < 1$) and the maximally mixed state is located at the center of the sphere ($S^2 = 0$). The Stokes parameters can be expressed in terms of measurement probabilities and therefore be obtained experimentally via projective measurements :

$$\begin{aligned}
 S_0 &= p_{|H\rangle} + p_{|V\rangle} \\
 S_1 &= p_{|D\rangle} - p_{|A\rangle} \\
 S_2 &= p_{|R\rangle} - p_{|L\rangle} \\
 S_3 &= p_{|H\rangle} - p_{|V\rangle}
 \end{aligned} \tag{5.4}$$

where P are measurement probabilities normalized in terms of an arbitrary orthogonal basis $\{|\psi\rangle, |\psi^\perp\rangle\}$ as $p_{|\psi\rangle} + p_{|\psi^\perp\rangle} = 1$. The density operator describing the measured state can then be derived from equation 5.2 resulting in a 2×2 matrix for a single-qubit state.

An analyzer setup as depicted in figure 5.3 consisting of a QWP, a HWP, a PBS and one or two photodetectors is sufficient to fully probe the two-dimensional Hilbert state of a single-photon qubit. If the HWP and the PBS are exchanged with a linear polarizer or if only one detector is available, merely one of two basis states can be measured at once and the necessary analyzer settings double for a complete set of measurements.

5.2.2 Multi-qubit tomography

When dealing with multi-qubit states, the definitions and properties of the density matrix as described above still hold. While there is no visualization for multi-qubit Bloch spheres, the density operator for n -qubit states in terms of the Stokes parameters can be generalized as

$$\hat{\rho} = \frac{1}{2^n} \sum_{i_1, i_2, \dots, i_n=0}^3 S_{i_1, i_2, \dots, i_n} \hat{\sigma}_{i_1} \otimes \hat{\sigma}_{i_2} \otimes \dots \otimes \hat{\sigma}_{i_n} \quad (5.5)$$

where $S_{0,0,\dots,0} = 1$ due to normalization [139]. Taking this into account, there are $4^n - 1$ real parameters that have to be determined corresponding to 2^n basis states. Restricting the discussion to two-qubit states ($n=2$) labeled by i_1, i_2 , the Stokes parameters can again be expressed in terms of measurement outcomes as

$$S_{i_1, i_2} = \left(p_{|\Psi_{i_1}\rangle} - p_{|\Psi_{i_1}^\perp\rangle} \right) \otimes \left(p_{|\Psi_{i_2}\rangle} - p_{|\Psi_{i_2}^\perp\rangle} \right), \quad i_1, i_2 \neq 0 \quad (5.6)$$

allowing the determination of each two-qubit Stokes parameter by four local measurement settings. In other words, every combination of $\{H, V, D, R\}$ has to be measured (taking into account the completeness relation $\{|\Psi\rangle, |\Psi^\perp\rangle\}$ as $P_{|\Psi\rangle} + P_{|\Psi^\perp\rangle} = 1$) in order to determine every Stokes parameter. The number of analyzer setting is determined by the amount of available detectors, either one or two for each outcome. The primary advantage of having four detectors in total is that one analyzer setting can access the complete basis simultaneously [90]. Therefore, enough information to determine a Stokes parameter can be obtained with one analyzer configuration. Since certain Stokes parameters can be calculated with the same measurements, the number of required settings reduces to 9 from 16 in the one-detector case, where in each case one of the measurement settings is required to determine the normalization.

The quED consists of a polarizer that absorbs $|\Psi^\perp\rangle$ ($|\Psi\rangle$) and transmitting $|\Psi\rangle$ ($|\Psi^\perp\rangle$) and only one detector, therefore requiring at least 16 measurement settings. A schematic of the quED setup for tomography measurements is depicted in figure 5.4. The state emitted by the quED source is one of the Bell states $|\Phi^+\rangle$ and $|\Phi^-\rangle$ depending on the position of the wave-plate in the pump beam. A quarter-wave plate in each arm is used to probe circular polarization components after which the polarizers project the state on a linear polarization. Longpass filters in front of the fiber couplers block residual pump light as well as short-wavelength stray light. The quED control unit containing two Silicon SPADs is used to tune the pump laser and track the coincidence counts for the various measurement settings.

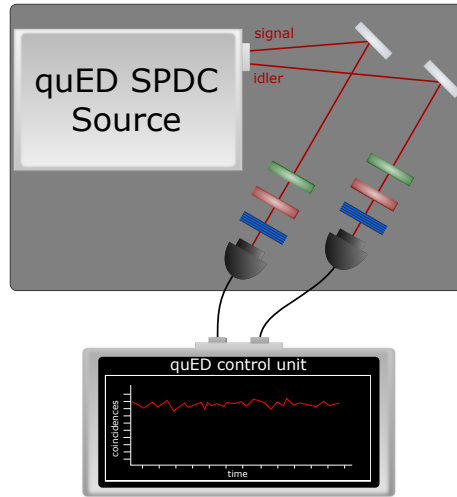


Fig. 5.4: quED two-qubit state tomography setup. A half-wave plate is added in signal and idler arm to the quED setup from 5.1. The linear polarizers act as a combination of a half-wave plate and a PBS, transmitting only one linear polarization state at a time (the drawback to using a half-wave plate and a PBS followed by 2 detectors is that more measurement settings are required). The following longpass filters removes residual pump light and stray light. In the quED control unit, the silicon-based SPADs to detect the incident photons are housed along with the required electronics to analyze the state (shown in the picture are the coincidence rates between signal and idler arm).

5.2.3 Maximum likelihood estimation

Due to experimental noise, the finite number of measurements and imperfect optical components, measurements suffer from statistical and systematic errors. This can result in an unphysical density matrix. In particular, the positivity property may not be fulfilled due to one or more of the eigenvalues being negative. The probability to encounter negative eigenvalues grows linearly with the dimension of the state and is therefore especially apparent when dealing with large systems. If the density operator yields unphysical eigenvalues, various methods can be employed to recover a physical density matrix from the measured parameters. A common numerical method is the maximum likelihood estimation (MLE) which assumes errors in the measurement results and gives out the physical density matrix that is closest to the measured data [140, 141].

In general, a maximum likelihood method algorithm generates a density matrix that is Hermitian, positive and therefore physical. A likelihood function quantifies the fit between the density matrix and the experimental data. The likelihood is then optimized via numerical methods, e.g. Monte Carlo, to result in the most probable physical density matrix. Implementing the MLE algorithm on one's own usually goes beyond the complexity and the temporal boundaries of an introductory lab course. Fortunately, ready-to-use code packages exist either for several popular programming

languages [142], as well as in the form of an online tomography interface which includes a graphical output for the density matrix [143].

5.2.4 Fidelity and purity

After a physical density matrix is retrieved, several helpful measures for the quality of the quantum state can be derived: For example, the fidelity

$$\mathcal{F}(\hat{\rho}_{th}, \hat{\rho}_{exp}) := \left(\text{Tr} \left\{ \sqrt{\sqrt{\hat{\rho}_{th}} \hat{\rho}_{exp} \sqrt{\hat{\rho}_{th}}} \right\} \right) \quad (5.7)$$

quantifies the overlap between the experimentally obtained state $\hat{\rho}_{exp}$ and the theoretically expected state $\hat{\rho}_{th}$. $0 \leq \mathcal{F} \leq 1$ where $\mathcal{F} = 1$ if the states are identical, i.e. $\hat{\rho}_{exp} = \hat{\rho}_{th}$. Using the quED, $\mathcal{F} > 0.88$ can be achieved using the standard alignment procedure [137]. From the fidelity, measures for the degree of entanglement of mixed states¹, can be directly recovered [144, 145]. The purity is a measure to quantify how mixed the obtained state is and is given by

$$\gamma := \text{Tr}\{\hat{\rho}^2\}, \quad 1/d \leq \gamma \leq 1 \quad (5.8)$$

where d is the dimension of the Hilbert space. The upper and lower bound for γ represent a pure and the completely mixed state, respectively, following directly from the properties of $\hat{\rho}$. Using the quED, all four Bell states can be prepared and characterized by conducting a quantum state tomography [146]. Single-qubit states can be created by heralding one of the two photons of each pair and rotating the remaining photon using a half- or a quarter-wave plate [35].

5.3 Hong-Ou-Mandel interference

When two identical photons (i.e. same polarization, frequency, phase,...) enter a beam splitter via both input modes, both photons will be detected in the same output mode. The number of coincidence events between detectors placed in the output ports vanishes in an ideal setup. This effect is known as Hong-Ou-Mandel (HOM) interference and was first shown in 1987 by the authors of the same name [87]. In contrast to many other quantum effects, HOM interference can be shown through a relatively minimal equipment, which makes it a suitable experiment for an undergraduate lab course [147]. Apart from a source generating identical photons, the required components are a beam splitter where the downconverted photons are combined and a variable delay line for either the signal or the idler arm to overlap the time of incidence at the beam splitter. We define the two-photon input state

¹e.g. the tangle and the concurrence

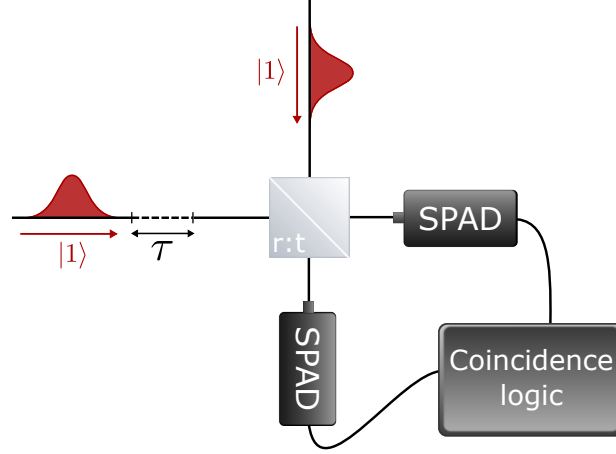


Fig. 5.5: Experimental setup to measure Hong-Ou-Mandel interference. Two single-photon states are interfered at a 50:50 beam splitter, i.e. $t = r = 1/\sqrt{2}$. If the photons are indistinguishable, interference leads to both photons always exiting the beam splitter in the same output mode. SPADs in each mode used to detect the photons are connected to a coincidence logic. If interference occurs, the coincidence count should reach a minimum. To adjust the arrival time at the detectors and visualize the coincidence 'dip', a delay τ is added to one of the two input modes.

before arriving at the beam splitter in the Fock (number) basis

$$|\Psi_{\text{in}}\rangle_{ab} = \hat{a}^\dagger \hat{b}^\dagger |0\rangle_a |0\rangle_b \quad (5.9)$$

where \hat{a}^\dagger and \hat{b}^\dagger are the bosonic creation operators acting on the two-photon vacuum state in the input modes a and b . We introduce the indices j and k to label properties of the photons such as polarization, frequency, time of arrival, spectral and transverse spatial mode. Note that in the previous description of a beam splitter in Chapter 2.3.1 we assumed the photons to be identical, i.e. indistinguishable and therefore suppressed these indices. The transformation induced by an ideal beam splitter of transmission t and reflectance r is described by a unitary matrix \hat{U}_{BS} which acts in the following way on the creation operators if we make no assumptions about the distinguishability:

$$\begin{aligned} \hat{a}^\dagger &\xrightarrow{\hat{U}_{\text{BS}}} t\hat{c}^\dagger + ir\hat{d}^\dagger \\ \hat{b}^\dagger &\xrightarrow{\hat{U}_{\text{BS}}} ir\hat{c}^\dagger + t\hat{d}^\dagger \end{aligned} \quad (5.10)$$

where \hat{c}^\dagger and \hat{d}^\dagger describe the creation of a photon in the output mode c and d , respectively. Applying \hat{U}_{BS} to the incident two-photon state then results in the output state

$$|\Psi_{\text{out}}\rangle_{cd} = \hat{U}_{\text{BS}} |\Psi_{\text{in}}\rangle_{ab} = \left(itr\hat{c}_j^\dagger \hat{c}_k^\dagger + t^2 \hat{c}_j^\dagger \hat{d}_k^\dagger - r^2 \hat{c}_k^\dagger \hat{d}_j^\dagger + itr\hat{d}_j^\dagger \hat{d}_k^\dagger \right) |0\rangle_c |0\rangle_d \quad (5.11)$$

using equation 5.9 and 5.10 and $[\hat{c}^\dagger, \hat{d}^\dagger] = 0$ in the third term. Assuming a 50 : 50 beam splitter, i.e. $t = r = 1/\sqrt{2}$, $|\Psi_{\text{out}}\rangle_{cd}$ reduces to

$$|\Psi_{\text{out}}\rangle_{cd} = \frac{1}{2} \left(i\hat{c}_j^\dagger \hat{c}_k^\dagger + \hat{c}_j^\dagger \hat{d}_k^\dagger - \hat{c}_k^\dagger \hat{d}_j^\dagger + i\hat{d}_j^\dagger \hat{d}_k^\dagger \right) |0\rangle_c |0\rangle_d \quad (5.12)$$

The four terms on the right hand side correspond to the possible outcomes after undergoing the beam splitter transformation, as depicted in figure 5.6. In half of the possible outcomes, where either both photons are transmitted or reflected, the detectors in both output modes click, indicating a coincidence event. The remaining terms correspond to both photons exiting the beam splitter in output c or d and both arriving at the same detector.

Remarkably, two of these possible outcomes only occur for distinguishable photons. If the incident photons are indistinguishable, two terms cancel out and HOM interference can be observed: The properties of photons relevant for the distinguishability are included in the subscripts i, j of the creation operators. If $i \neq j$, the photons are distinguishable which is the case e.g. for orthogonal polarization where $j = H$ and $k = V$. The output state $|\Psi_{\text{out}}\rangle_{cd}$ is then given by

$$\begin{aligned} |\Psi_{\text{out}}\rangle_{cd} &= \frac{1}{2} \left(i\hat{c}_H^\dagger \hat{c}_V^\dagger + \hat{c}_H^\dagger \hat{d}_V^\dagger - \hat{c}_V^\dagger \hat{d}_H^\dagger + i\hat{d}_H^\dagger \hat{d}_V^\dagger \right) |0\rangle_c |0\rangle_d \\ &= \frac{1}{2} (i|1; H\rangle_c |1; V\rangle_c |0\rangle_d + |1; H\rangle_c |1; V\rangle_d - |1; V\rangle_c |1; H\rangle_d + i|0\rangle_c |1; H\rangle_d |1; V\rangle_d) \end{aligned} \quad (5.13)$$

where we explicitly wrote both the number state and the polarization state of the photons in the output modes. As above, two terms correspond to both photons in the same output mode and two terms to one photon in both mode c and d , resulting in a click at both detectors with probability $p_{\text{coinc}} = 1/2$. If the photons are in the same polarization state and assuming the other properties to be equal as well, $i = j$. The photons are indistinguishable resulting in the state

$$\begin{aligned} |\Psi_{\text{out}}\rangle_{cd} &= \frac{1}{2} \left(i\hat{c}_j^\dagger \hat{c}_j^\dagger + \hat{c}_j^\dagger \hat{d}_j^\dagger - \hat{c}_j^\dagger \hat{d}_j^\dagger + i\hat{d}_j^\dagger \hat{d}_j^\dagger \right) |0\rangle_c |0\rangle_d \\ &= \frac{i}{\sqrt{2}} \left(\frac{(\hat{c}_j^\dagger)^2}{\sqrt{2}} + \frac{(\hat{d}_j^\dagger)^2}{\sqrt{2}} \right) |0\rangle_c |0\rangle_d = \frac{i}{\sqrt{2}} (|2\rangle_c |0\rangle_d + |0\rangle_c |2\rangle_d) \end{aligned} \quad (5.14)$$

We can see that the terms where both output modes are occupied cancel out (destructively interfere) resulting in bunching of the photons and $p_{\text{coinc}} = 0$. The photons leave the beam splitter in pairs (randomly) in one of two outputs with probability $1/2$. Note that this destructive interference is not interference between two single

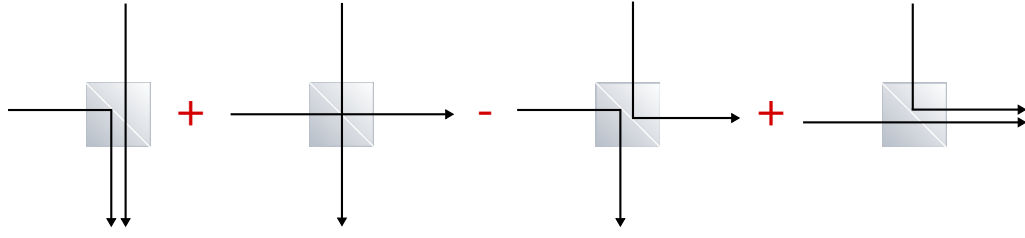


Fig. 5.6: Schematics of Hong-Ou-Mandel interference in a 50:50 beam splitter. Indistinguishable single photons from each input mode interfere in a beam splitter. The total output state results from adding all contributing amplitudes. Due to the minus sign in front of the third term, the contributions of one photon in each output mode cancel out, leaving only the contributions with both photons in one output mode, i.e. a two-photon number state.

photons but a two-photon interference effect arising from the two-photon probability amplitude in equation 5.14.

HOM interference can be visualized in experiments by the so-called HOM dip, referring to the decrease in coincidence counts when the photons approach temporal indistinguishability. Using entangled photon pairs generated by type-I SPDC and compensating the walk-off effects, we assume that the polarization, the frequency and the transverse spatial mode are identical for both the signal and the idler photon. To detect the HOM dip, some sort of time delay has to be inserted in one of the input (or output) ports of the beam splitter in order to overlap the wave packages as depicted in figure 5.7. The more the wave packages overlap, the higher the indistinguishability, resulting in a reduction of the coincidence counts or a deepening of the HOM dip. The coincidence counts can then be plotted against the time delay τ between the signal and idler arm, resulting in the graphical representation of the HOM dip. The deepness of the dip depends on the experimental setup, i.e. the experimentally achieved indistinguishability and can be quantified in terms of the HOM visibility given by

$$V_{\text{HOM}} := \text{Tr}\{\hat{\rho}_a \hat{\rho}_b\} = 1 - \frac{p_{\text{coinc}}(\tau \rightarrow 0)}{p_{\text{coinc}}(\tau \rightarrow \infty)} \quad (5.15)$$

If the photons are entangled or if they are separable but have the same density matrix $\hat{\rho}_a = \hat{\rho}_b$, the visibility is equivalent to the purity γ of the state

$$V_{\text{HOM}} \equiv \gamma \quad (5.16)$$

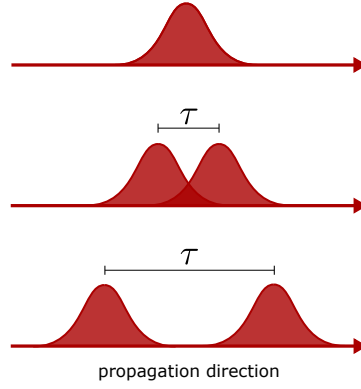


Fig. 5.7: Temporal overlap between two wave packages. The wave packages are assumed to be indistinguishable in all other degrees of freedom. In the case at the top, the wave packages are fully overlapped and interfere, i.e. they are fully coherent and would show ideal contrast in an interference pattern or perfect visibility in a HOM dip experiment. In the middle case, the wave packages are partially overlapped, quantified by the temporal shift τ , leading to reduced coherence. They still interfere since $\tau < \tau_c$ (where τ_c is the coherence time) but the contrast in an interference pattern and the depth of the HOM dip is reduced. In the bottom case, the wave packages do not overlap, i.e. $\tau > \tau_c$. Coherence is lost and no interference can be observed.

The width of the dip at full width half maximum (FWHM) is the coherence time of the two-photon state related to the coherence length by

$$\text{FWHM} \equiv \tau_c = l_c/c \quad (5.17)$$

while the form of the dip depends on the spectral distribution of the photons which itself depends on the nonlinear profile of the crystal used for SPDC [148]. For example, a BBO has the nonlinear profile of a top-hat function, which results in a spectral profile of the generated photons that is proportional to the sinc of a linear function and results in the coincidence probability

$$p_{\text{coinc}}^{\text{sinc}} = \frac{1}{2} - \frac{1}{4\sigma}((\sigma - \tau)\text{sgn}(\sigma - \tau) + (\sigma + \tau)\text{sgn}(\sigma + \tau) - 2\tau\text{sgn}(\tau)) \quad (5.18)$$

where σ is the standard deviation related to the full width at half maximum via $\text{FWHM} = 2\sqrt{2\ln 2}\sigma$. Spectral filtering after the SPDC source and before the beam splitter might change the function to a profile proportional to a Gaussian function which gives

$$p_{\text{coinc}}^{\text{Gauss}} = \frac{1}{2} - \frac{1}{2}e^{-2\sigma^2\tau^2} \quad (5.19)$$

Both functions are plotted in figure 5.8.

For the quED setup, a HOM effect upgrade can be purchased that consists of an in-fiber 50 : 50 beam splitter and a translation state in one arm that is used to tune

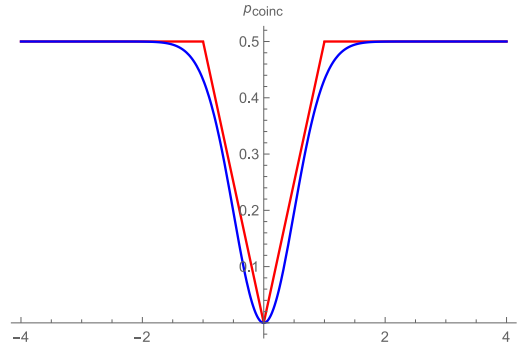


Fig. 5.8: Plot of the Hong-Ou-Mandel dip. Equation 5.19 (5.18) is depicted in blue (red). The width of the wave packages σ is set to 1. Tuning the temporal overlap between the wave packages τ changes the depth of the dip. In the case of perfect indistinguishability (including $\tau = 0$) and zero dark counts, the coincidence rate p_{coinc} drops to zero.

the time delay. The coincidence counts can be displayed on the detector console and tuning the delay will then result in the appearance of the HOM dip if the rest of the setup is appropriately aligned. A schematic depiction of the quED setup used to visualize the HOM-dip is given in figure 5.9. The experiment can be conducted in a relatively short amount of time and a lab course report may include calculation of the visibility and the purity of the generated state.

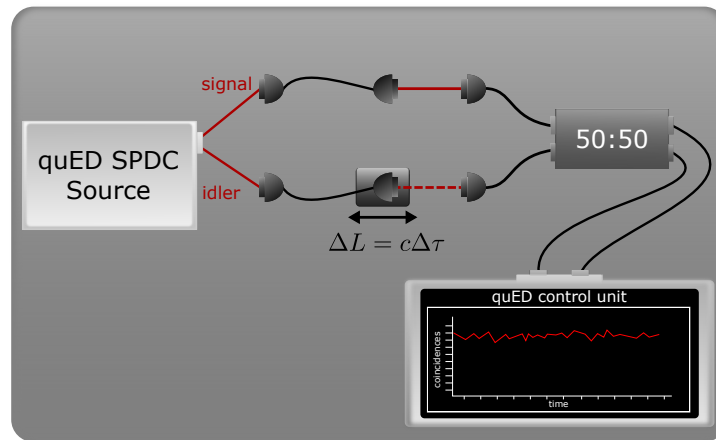


Fig. 5.9: quED setup to study Hong-Ou-Mandel interference between signal and idler photons. Both photons are coupled to a fiber which leads to an in-fiber 50:50 beam splitter. To tune the arrival time, one fiber coupler is mounted on a translation stage which can be moved by $\Delta L = c\Delta\tau$. The beam splitter is connected to the detectors in the quED control unit, where the coincidence count is directly displayed. The HOM-dip becomes visible by tuning the translation stage, overlapping the signal and idler wave packages.

To summarize, HOM interference is a quantum effect that shows the degree of indistinguishability of two particles, in this case photons. There is no classical equivalent

since the effect emerges from a fundamental property of bosons, namely bunching. Indistinguishability is a requirement for high degrees of entanglement, therefore HOM interference is a common measure for the quality of a source supposed to generate identical or entangled photon pairs. Furthermore, due to the relative simplicity of the setup, HOM interference is also a suitable experiment for undergraduate lab courses.

Conclusion

Over the course of the last few chapters, we laid out three experimental applications that rely on SPDC sources. The first experiment is an implementation of blind quantum computing that is driven by a completely classical client. Measurement-based quantum computing, which is the underlying framework for blind quantum computing, is based on measurements on a highly entangled resource state, in this case a box cluster state consisting of four physical qubits. The state is generated by pumping two type-II BBO crystals to create two Bell pairs at 800nm and fuse the pairs using a probabilistic CZ gate. While down-conversion rates provided by SPDC sources are inherently low, count rates of around 10Hz can be achieved at 500mW for the box cluster resource state after fusing.

The second experiment enables the realization of universally secure one-time programs by encoding classical gates in qubits. Sharing a Bell state allows the remote preparation of the gates via measurement on the server's part without compromising the type of gate sent to the client. The source used to generate the Bell state is based on a special type of quasi-phase-matching in a periodically-poled crystal. A solid-state laser at 515nm pumps a ppKTP specifically tuned to allow for two SPDC processes to take place simultaneously. Overlapping the processes allows for the generation a Bell state made up of highly nondegenerate photons at 785nm and 1498nm. Transmitting the long-wavelength photon to the client and the short-wavelength photon for the state preparation allows for long transmission channels to the client and at the same time, keeps the resource requirements as low as possible on the server's side.

In the last chapter, we discuss the application of a plug-and-play type-I SPDC source in undergraduate lab courses. The source is based on a laser diode at 405nm pumping two wedged type-I BBO crystals generating either pairs of indistinguishable photons or a Bell state depending on the pump polarization. Due to the design of the source, the time required for the alignment is vastly reduced, leaving more time to investigate the basics quantum optics such as quantum state tomography and Hong-Ou-Mandel interference.

In Table 6.1, some of the most important properties of the sources described are compared. The sources summarized, while based on the same fundamental process,

Experiment	Crystal	Phase-matching	λ_p	$\lambda_{s,i}$	Direction
CDBQC	BBO	type-II	394.5nm	degenerate	non-collinear
OTPs	ppKTP	QPM	515nm	non-degenerate	collinear
Lab course	BBO	type-I	400nm	non-degenerate	non-collinear

Tab. 6.1: A summary of the SPDC sources employed in this thesis. 'CDBQC' refers to the classically-driven blind quantum computing protocol, 'OTPs' to the one-time programs using entanglement, and 'lab course' to the quED entanglement demonstrator used for laboratory course experiments. The pump wavelength (λ_p) is given as well as the properties of the down-converted photons in terms of wavelength ($\lambda_{s,i}$) (degenerate/non-degenerate) and (emission) direction (collinear/non-collinear).

are all employing different types of phase-matching, generate different states with different rates, in a wide range of degenerate and non-degenerate wavelengths. The extensive variability is one of the main advantages of SPDC sources. While the sources and the corresponding setups discussed are different in their properties and application, there are overarching themes apart from the down-conversion process. Excluding the lab course experiments, both protocols discussed assume interaction between non-trusting parties. For short and midterm implementations of quantum computing, the classically-driven blind quantum computing protocol offers a possibility for users restricted to classical capabilities to be able to use a quantum server without having to fear compromization of the details of the computation. In the future, the fidelity of the resource state can be improved by using more efficient entanglement sources and by implementing entanglement gates based on nonlinear materials to achieve higher entanglement rates. This would also enable the extension of the resource state to larger and possibly universal cluster states, while keeping the hardware requirements reasonable.

For the evaluation of classical gates, quantum principles allow the preparation and evaluation of one-time programs. In the protocol introduced, a focus already lies in the applicability of the protocol by preparing the gates using only passive in-fiber elements and a one-way quantum channel, and requiring simply a classical channel for the evaluation. Further improvements can be made by increasing the mobility of the quantum part of the protocol. For example, the bulk source used in the protocol is designed to be eventually integrated in a chip, substantially reducing the size of the server's setup. On the client's side, using smaller but less-efficient telecom-wavelength detectors would allow to confine the whole setup to a small box.

All in all, the improvement of the protocols discussed is mainly dependent on the development of the non-linear components. Though SPDC sources can be used for diverse applications and are comparably easy to set up, they are fundamentally bound by their spontaneous working principle and the increasing chance of multi-

pair emissions for higher pump powers. Both effects can reduce the fidelity of the generated states as well as the security in cryptographic protocols. Therefore, the development of deterministic and efficient single-photon sources is the required next big step in the field of quantum technologies. However, since candidates for single-photon sources are still in their infancy and require expensive components to set up, SPDC sources will continue to play a crucial role in quantum optical setups in the coming years.

Bibliography

- [1]Erwin Schrödinger. „Die gegenwärtige Situation in der Quantenmechanik“. In: *Naturwissenschaften* 23.50 (1935), pp. 844–849 (cit. on p. 1).
- [2]Albert Einstein, Boris Podolsky, and Nathan Rosen. „Can quantum-mechanical description of physical reality be considered complete?“ In: *Physical review* 47.10 (1935), p. 777 (cit. on pp. 1, 14).
- [3]Claus Jönsson. „Elektroneninterferenzen an mehreren künstlich hergestellten Feinspalten“. In: *Zeitschrift für Physik* 161.4 (1961), pp. 454–474 (cit. on p. 1).
- [4]Claus Jönsson. „Electron diffraction at multiple slits“. In: *American Journal of Physics* 42.1 (1974), pp. 4–11 (cit. on p. 1).
- [5]Carl A Kocher and Eugene D Commins. „Polarization correlation of photons emitted in an atomic cascade“. In: *Physical Review Letters* 18.15 (1967), p. 575 (cit. on p. 1).
- [6]Stuart J Freedman and John F Clauser. „Experimental test of local hidden-variable theories“. In: *Physical Review Letters* 28.14 (1972), p. 938 (cit. on pp. 1, 15).
- [7]Theodore H Maiman. „Stimulated optical radiation in ruby“. In: *Nature* 187.4736 (1960), pp. 493–494 (cit. on pp. 1, 7, 17).
- [8]Michael Riordan, Lillian Hoddeson, and Conyers Herring. „The invention of the transistor“. In: *More Things in Heaven and Earth*. Springer, 1999, pp. 563–578 (cit. on p. 1).
- [9]Stephen Wiesner. „Conjugate coding“. In: *ACM Sigact News* 15.1 (1983), pp. 78–88 (cit. on pp. 1, 81, 82).
- [10]Charles H. Bennett and Gilles Brassard. „Quantum cryptography: Public key distribution and coin tossing“. In: *Theoretical Computer Science* 560 (2014), pp. 7–11 (cit. on p. 1).
- [11]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 (1992), pp. 553–558 (cit. on pp. 1, 58).
- [12]Ethan Bernstein and Umesh Vazirani. „Quantum complexity theory“. In: *SIAM Journal on computing* 26.5 (1997), pp. 1411–1473 (cit. on p. 1).
- [13]Peter W Shor. „Algorithms for quantum computation: discrete logarithms and factoring“. In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134 (cit. on p. 1).

- [14]Lov K Grover. „A fast quantum mechanical algorithm for database search“. In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996, pp. 212–219 (cit. on pp. 1, 58).
- [15]Richard P Feynman. „Simulating physics with computers“. In: *Int. J. Theor. Phys* 21.6/7 (1982) (cit. on pp. 1, 58).
- [16]Artur K Ekert. „Quantum cryptography based on Bell’s theorem“. In: *Physical review letters* 67.6 (1991), p. 661 (cit. on pp. 1, 88).
- [17]Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. „Universal blind quantum computation“. In: *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE. 2009, pp. 517–526 (cit. on pp. 2, 57).
- [18]Andrew M. Childs. „Secure assisted quantum computation“. In: *Quantum Information and Computation* 5, 456 (2005) (initial version appeared online in 2001) (cit. on pp. 2, 4, 57).
- [19]Anne Broadbent, Gus Gutoski, and Douglas Stebila. „Quantum one-time programs“. In: *Annual Cryptology Conference*. Springer. 2013, pp. 344–360 (cit. on pp. 2, 82).
- [20]John S Bell. „On the einstein podolsky rosen paradox“. In: *Physics Physique Fizika* 1.3 (1964), p. 195 (cit. on pp. 2, 14).
- [21]Simon Kochen and Ernst P Specker. „The problem of hidden variables in quantum mechanics“. In: *The logico-algebraic approach to quantum mechanics*. Springer, 1975, pp. 293–328 (cit. on p. 2).
- [22]IBM Quantum Experience. <https://www.ibm.com/quantum-computing>. Accessed on 11th August 2020 (cit. on p. 2).
- [23]Quantum in my Cloud. <http://www.bristol.ac.uk/physics/research/quantum/engagement/qcloud>. Accessed on 11th August 2020 (cit. on p. 2).
- [24]Qutech Quantum Inspire. <https://www.quantum-inspire.com>. Accessed on 11th August 2020 (cit. on p. 2).
- [25]M Veldhorst, JCC Hwang, CH Yang, et al. „An addressable quantum dot qubit with fault-tolerant control-fidelity“. In: *Nature nanotechnology* 9.12 (2014), p. 981 (cit. on p. 3).
- [26]TF Watson, SGJ Philips, Erika Kawakami, et al. „A programmable two-qubit quantum processor in silicon“. In: *Nature* 555.7698 (2018), pp. 633–637 (cit. on p. 3).
- [27]J Yoneda, K Takeda, A Noiri, et al. „Quantum non-demolition readout of an electron spin in silicon“. In: *Nature communications* 11.1 (2020), pp. 1–7 (cit. on p. 3).
- [28]Bruce E Kane. „A silicon-based nuclear spin quantum computer“. In: *Nature* 393.6681 (1998), pp. 133–137 (cit. on p. 3).
- [29]Juha T Muhonen, Juan P Dehollain, Arne Laucht, et al. „Storing quantum information for 30 seconds in a nanoelectronic device“. In: *Nature nanotechnology* 9.12 (2014), p. 986 (cit. on p. 3).
- [30]Lieven MK Vandersypen and Isaac L Chuang. „NMR techniques for quantum control and computation“. In: *Reviews of modern physics* 76.4 (2005), p. 1037 (cit. on p. 3).

- [31]Y Nakamura, CD Chen, and Jaw Shen Tsai. „Spectroscopy of energy-level splitting between two macroscopic quantum states of charge coherently superposed by Josephson coupling“. In: *Physical review letters* 79.12 (1997), p. 2328 (cit. on pp. 3, 11).
- [32]M. H. Devoret, A. Wallraff, and J. M. Martinis. *Superconducting Qubits: A Short Review*. 2004. arXiv: cond-mat/0411174 [cond-mat.mes-hall] (cit. on pp. 3, 11).
- [33]Chandra M Natarajan, Michael G Tanner, and Robert H Hadfield. „Superconducting nanowire single-photon detectors: physics and applications“. In: *Superconductor science and technology* 25.6 (2012), p. 063001 (cit. on p. 3).
- [34]Christophe Couteau. „Spontaneous parametric down-conversion“. In: *Contemporary Physics* 59.3 (2018), pp. 291–304 (cit. on pp. 3, 26).
- [35]CK Hong and Leonard Mandel. „Experimental realization of a localized one-photon state“. In: *Physical Review Letters* 56.1 (1986), p. 58 (cit. on pp. 3, 39, 102).
- [36]Paul G Kwiat, Klaus Mattle, Harald Weinfurter, et al. „New high-intensity source of polarization-entangled photon pairs“. In: *Physical Review Letters* 75.24 (1995), p. 4337 (cit. on pp. 3, 40).
- [37]Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. „A scheme for efficient quantum computation with linear optics“. In: *Nature* 409.6816 (2001), pp. 46–52 (cit. on pp. 3, 58).
- [38]P Michler, A Kiraz, C Becher, et al. „A quantum dot single-photon turnstile device“. In: *Science* 290.5500 (2000), pp. 2282–2285 (cit. on p. 3).
- [39]E Moreau, I Robert, JM Gérard, et al. „Single-mode solid-state single photon source based on isolated quantum dots in pillar microcavities“. In: *Applied Physics Letters* 79.18 (2001), pp. 2865–2867 (cit. on p. 3).
- [40]A Kress, F Hofbauer, N Reinelt, et al. „Manipulation of the spontaneous emission dynamics of quantum dots in two-dimensional photonic crystals“. In: *Physical Review B* 71.24 (2005), p. 241304 (cit. on p. 3).
- [41]Christian Kurtsiefer, Sonja Mayer, Patrick Zarda, and Harald Weinfurter. „Stable solid-state source of single photons“. In: *Physical review letters* 85.2 (2000), p. 290 (cit. on p. 3).
- [42]Robert Raussendorf and Hans J Briegel. „A one-way quantum computer“. In: *Physical Review Letters* 86.22 (2001), p. 5188 (cit. on pp. 4, 62).
- [43]Atul Mantri, Tommaso F Demarie, Nicolas C Menicucci, and Joseph F Fitzsimons. „Flow ambiguity: A path towards classically driven blind quantum computation“. In: *Physical Review X* 7.3 (2017), p. 031004 (cit. on pp. 4, 58, 69–71, 73).
- [44]Roy J Glauber. „The quantum theory of optical coherence“. In: *Physical Review* 130.6 (1963), p. 2529 (cit. on pp. 7, 22).
- [45]Danilo Boschi, Salvatore Branca, Francesco De Martini, Lucien Hardy, and Sandu Popescu. „Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels“. In: *Physical Review Letters* 80.6 (1998), p. 1121 (cit. on p. 7).
- [46]Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. „Experimental entanglement swapping: entangling photons that never interacted“. In: *Physical Review Letters* 80.18 (1998), p. 3891 (cit. on p. 7).

- [47]TB Pittman, MJ Fitch, BC Jacobs, and JD Franson. „Experimental controlled-NOT logic gate for single photons in the coincidence basis“. In: *Physical Review A* 68.3 (2003), p. 032316 (cit. on p. 7).
- [48]Jeremy L O’Brien, Geoffrey J Pryde, Andrew G White, Timothy C Ralph, and David Branning. „Demonstration of an all-optical quantum controlled-NOT gate“. In: *Nature* 426.6964 (2003), pp. 264–267 (cit. on p. 7).
- [49]Nikolai Kiesel, Christian Schmid, Ulrich Weber, Rupert Ursin, and Harald Weinfurter. „Linear Optics Controlled-Phase Gate Made Simple“. In: *Physical Review Letters* 95.21 (2005) (cit. on pp. 7, 75).
- [50]William K Wootters and Wojciech H Zurek. „A single quantum cannot be cloned“. In: *Nature* 299.5886 (1982), pp. 802–803 (cit. on pp. 9, 82).
- [51]Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information*. 2002 (cit. on p. 10).
- [52]Immanuel Bloch. „Quantum coherence and entanglement with ultracold atoms in optical lattices“. In: *Nature* 453.7198 (2008), pp. 1016–1022 (cit. on p. 11).
- [53]Mark Saffman, Thad G Walker, and Klaus Mølmer. „Quantum information with Rydberg atoms“. In: *Reviews of modern physics* 82.3 (2010), p. 2313 (cit. on p. 11).
- [54]Daniel Loss and David P DiVincenzo. „Quantum computation with quantum dots“. In: *Physical Review A* 57.1 (1998), p. 120 (cit. on p. 11).
- [55]Thaddeus D Ladd and Malcolm S Carroll. „Silicon qubits“. In: *Encyclopedia of Modern Optics* (2018), pp. 467–477 (cit. on p. 11).
- [56]David d’Enterria and Gustavo G da Silveira. „Observing light-by-light scattering at the Large Hadron Collider“. In: *Physical review letters* 111.8 (2013), p. 080405 (cit. on p. 12).
- [57]John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. „Proposed experiment to test local hidden-variable theories“. In: *Physical review letters* 23.15 (1969), p. 880 (cit. on p. 14).
- [58]Bas Hensen, Hannes Bernien, Anais E Dréau, et al. „Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres“. In: *Nature* 526.7575 (2015), pp. 682–686 (cit. on p. 15).
- [59]Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, et al. „Significant-loophole-free test of Bell’s theorem with entangled photons“. In: *Physical review letters* 115.25 (2015), p. 250401 (cit. on p. 15).
- [60]Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, et al. „Strong loophole-free test of local realism“. In: *Physical review letters* 115.25 (2015), p. 250402 (cit. on p. 15).
- [61]Sandu Popescu and Daniel Rohrlich. „Quantum nonlocality as an axiom“. In: *Foundations of Physics* 24.3 (1994), pp. 379–385 (cit. on p. 16).
- [62]Leonid A Khalfin and Boris S Tsirelson. „Quantum and quasi-classical analogs of Bell inequalities“. In: *Symposium on the foundations of modern physics*. Vol. 85. Singapore: World Scientific. 1985, p. 441 (cit. on p. 16).

- [63]Peter Rastall. „Locality, Bell’s theorem, and quantum mechanics“. In: *Foundations of physics* 15.9 (1985), pp. 963–972 (cit. on p. 16).
- [64]Bahaa EA Saleh and Malvin Carl Teich. *Fundamentals of photonics*. John Wiley & sons, 2019 (cit. on pp. 18, 19, 37).
- [65]R Hanbury Brown and Richard Q Twiss. „A test of a new type of stellar interferometer on Sirius“. In: *Nature* 178.4541 (1956), pp. 1046–1048 (cit. on p. 22).
- [66]H Jeff Kimble, Mario Dagenais, and Leonard Mandel. „Photon antibunching in resonance fluorescence“. In: *Physical Review Letters* 39.11 (1977), p. 691 (cit. on p. 23).
- [67]Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, et al. „Advances in quantum cryptography“. In: *arXiv preprint arXiv:1906.01645* (2019) (cit. on p. 23).
- [68]WH Louisell, A Yariv, and AE Siegman. „Quantum fluctuations and noise in parametric processes. I.“ In: *Physical Review* 124.6 (1961), p. 1646 (cit. on p. 24).
- [69]Douglas Magde and Herbert Mahr. „Study in ammonium dihydrogen phosphate of spontaneous parametric interaction tunable from 4400 to 16 000 Å“. In: *Physical Review Letters* 18.21 (1967), p. 905 (cit. on p. 24).
- [70]SA Akhmanov, VA Fadeev, RV Khokhlov, and ON Chunaev. „Pis’ ma Zh. Eksp. Teor. Fiz., 6 1967, 575“. In: *JETP Lett* 6 (1967), p. 85 (cit. on p. 24).
- [71]SE Harris, MK Oshman, and RL Byer. „Observation of tunable optical parametric fluorescence“. In: *Physical Review Letters* 18.18 (1967), p. 732 (cit. on p. 24).
- [72]B Ya Zel’Dovich and DN Klyshko. „Field statistics in parametric luminescence“. In: *ZhETF Pisma Redaktsiiu* 9 (1969), p. 69 (cit. on p. 24).
- [73]David C Burnham and Donald L Weinberg. „Observation of simultaneity in parametric production of optical photon pairs“. In: *Physical Review Letters* 25.2 (1970), p. 84 (cit. on p. 24).
- [74]Robert W Boyd. *Nonlinear optics*. Academic press, 2019 (cit. on p. 24).
- [75]JM Manley and HE Rowe. „Some general properties of nonlinear elements-Part I. General energy relations“. In: *Proceedings of the IRE* 44.7 (1956), pp. 904–913 (cit. on p. 26).
- [76]Peter Shadbolt. *Complexity and Control in Quantum Photonics*. Springer, 2015 (cit. on p. 27).
- [77]Jonathan CF Matthews. *Multi-photon Quantum Information Science and Technology in Integrated Optics [electronic Resource]*. Springer. (cit. on p. 27).
- [78]Zhe-Yu Jeff Ou. *Multi-photon quantum interference*. Vol. 43. Springer, 2007 (cit. on pp. 27, 28, 30).
- [79]Leonard Mandel and Emil Wolf. *Optical coherence and quantum optics*. Cambridge university press, 1995 (cit. on p. 27).
- [80]Bob D Guenther and Duncan Steel. *Encyclopedia of modern optics*. Academic Press, 2018 (cit. on p. 33).
- [81]Fabian Laudenbach, Sebastian Kalista, Michael Hentschel, Philip Walther, and Hannes Hübel. „A novel single-crystal & single-pass source for polarisation-and colour-entangled photon pairs“. In: *Scientific reports* 7.1 (2017), pp. 1–9 (cit. on pp. 37, 91).

- [82]E Bocquillon, C Couteau, M Razavi, R Laflamme, and G Weihs. „Coherence measures for heralded single-photon sources“. In: *Physical Review A* 79.3 (2009), p. 035801 (cit. on p. 39).
- [83]Xiang Guo, Chang-ling Zou, Carsten Schuck, et al. „Parametric down-conversion photon-pair source on a nanophotonic chip“. In: *Light: Science & Applications* 6.5 (2017), e16249–e16249 (cit. on p. 39).
- [84]Francesco Graffitti, Peter Barrow, Massimiliano Proietti, Dmytro Kundys, and Alessandro Fedrizzi. „Independent high-purity photons created in domain-engineered crystals“. In: *Optica* 5.5 (2018), pp. 514–517 (cit. on p. 39).
- [85]*How to compare efficiencies of different single photon sources - Table, page 5*. <http://quandela.com/download/white-paper>. Accessed on 11th August 2020 (cit. on p. 40).
- [86]Philippe Grangier, Gerard Roger, and Alain Aspect. „Experimental evidence for a photon anticorrelation effect on a beam splitter: a new light on single-photon interferences“. In: *EPL (Europhysics Letters)* 1.4 (1986), p. 173 (cit. on p. 42).
- [87]Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. „Measurement of subpicosecond time intervals between two photons by interference“. In: *Physical review letters* 59.18 (1987), p. 2044 (cit. on pp. 43, 102).
- [88]G Mauro D’Ariano, Matteo GA Paris, and Massimiliano F Sacchi. „Quantum tomography“. In: *Advances in Imaging and Electron Physics* 128 (2003), pp. 206–309 (cit. on p. 44).
- [89]Yannick Ole Lipp. „Experimental realization of an interferometric quantum circuit to increase the computational depth“. PhD thesis. uniwien, 2011 (cit. on p. 49).
- [90]Joseph B Altepeter, Evan R Jeffrey, and Paul G Kwiat. „Photonic state tomography“. In: *Advances in Atomic, Molecular, and Optical Physics* 52 (2005), pp. 105–159 (cit. on pp. 48, 100).
- [91]M. Faraday, T. Martin, and Royal Institution of Great Britain. *Faraday’s Diary*. Faraday’s Diary Bd. 4. Bell, 1932 (cit. on p. 50).
- [92]Friedrich Pockels. *Über den Einfluss des elektrostatischen Feldes auf das optische Verhalten piezoelektrischer Krystalle*. Vol. 39. Dieterichsche Verlags-Buchhandlung, 1894 (cit. on p. 50).
- [93]Clinton Cahall, Kathryn L Nicolich, Nurul T Islam, et al. „Multi-photon detection using a conventional superconducting nanowire single-photon detector“. In: *Optica* 4.12 (2017), pp. 1534–1535 (cit. on p. 52).
- [94]Aleksander Divochiy, Francesco Marsili, David Bitauld, et al. „Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths“. In: *Nature Photonics* 2.5 (2008), pp. 302–306 (cit. on p. 52).
- [95]Saeedeh Jahanmirinejad and Andrea Fiore. „Proposal for a superconducting photon number resolving detector with large dynamic range“. In: *Optics express* 20.5 (2012), pp. 5017–5028 (cit. on p. 52).
- [96]Francesco Mattioli, Zili Zhou, Alessandro Gaggero, et al. „Photon-counting and analog operation of a 24-pixel photon number resolving detector based on superconducting nanowires“. In: *Optics express* 24.8 (2016), pp. 9067–9076 (cit. on p. 52).

- [97]Matthew D Eisaman, Jingyun Fan, Alan Migdall, and Sergey V Polyakov. „Invited review article: Single-photon sources and detectors“. In: *Review of scientific instruments* 82.7 (2011), p. 071101 (cit. on p. 52).
- [98]Lixing You. „Superconducting Nanowire Single-Photon Detectors for Quantum Information“. In: *arXiv preprint arXiv:2006.00411* (2020) (cit. on p. 53).
- [99]Urmila Mahadev. „Classical homomorphic encryption for quantum circuits“. In: *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2018, pp. 332–338 (cit. on p. 57).
- [100]Atul Mantri, Tommaso F Demarie, and Joseph F Fitzsimons. „Universality of quantum computation with cluster states and (X, Y)-plane measurements“. In: *Scientific reports* 7 (2017), p. 42861 (cit. on p. 57).
- [101]Joseph F Fitzsimons. „Private quantum computation: an introduction to blind quantum computing and related protocols“. In: *npj Quantum Information* 3.1 (2017), pp. 1–11 (cit. on p. 57).
- [102]Chiara Greganti, Marie-Christine Roehsner, Stefanie Barz, Tomoyuki Morimae, and Philip Walther. „Demonstration of measurement-only blind quantum computing“. In: *New Journal of Physics* 18.1 (2016), p. 013020 (cit. on p. 57).
- [103]Peter W Shor. „Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer“. In: *SIAM review* 41.2 (1999), pp. 303–332 (cit. on p. 58).
- [104]David Elieser Deutsch. „Quantum computational networks“. In: *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 425.1868 (1989), pp. 73–90 (cit. on p. 59).
- [105]Christopher M. Dawson and Michael A. Nielsen. *The Solovay-Kitaev algorithm*. 2005. arXiv: quant-ph/0505030 [quant-ph] (cit. on p. 61).
- [106]Daniel Gottesman. *The Heisenberg Representation of Quantum Computers*. 1998. arXiv: quant-ph/9807006 [quant-ph] (cit. on pp. 61, 66).
- [107]Dorit Aharonov, Wim van Dam, Julia Kempe, et al. *Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation*. 2004. arXiv: quant-ph/0405098 [quant-ph] (cit. on p. 61).
- [108]Andris Ambainis and Oded Regev. *An Elementary Proof of the Quantum Adiabatic Theorem*. 2004. arXiv: quant-ph/0411152 [quant-ph] (cit. on p. 61).
- [109]Scott Aaronson and Alex Arkhipov. „The computational complexity of linear optics“. In: *Proceedings of the forty-third annual ACM symposium on Theory of computing*. 2011, pp. 333–342 (cit. on p. 61).
- [110]Robert Raussendorf. „Measurement-based quantum computation with cluster states“. In: *International Journal of Quantum Information* 7.06 (2009), pp. 1053–1203 (cit. on p. 62).
- [111]Frank Verstraete and J Ignacio Cirac. „Valence-bond states for quantum computation“. In: *Physical Review A* 70.6 (2004), p. 060302 (cit. on p. 62).
- [112]Marc Hein, Jens Eisert, and Hans J Briegel. „Multiparty entanglement in graph states“. In: *Physical Review A* 69.6 (2004), p. 062311 (cit. on p. 62).

- [113]Dave Bacon, Miguel Martin-Delgado, and Martin Roetteler. *Theory of quantum computation, communication, and cryptography*. 2011 (cit. on p. 62).
- [114]Robert Raussendorf and Hans J. Briegel. *Quantum computing via measurements only*. 2000. arXiv: quant-ph/0010033 [quant-ph] (cit. on p. 65).
- [115]Daniel E Browne, Elham Kashefi, Mehdi Mhalla, and Simon Perdrix. „Generalized flow and determinism in measurement-based quantum computation“. In: *New Journal of Physics* 9.8 (2007), p. 250 (cit. on p. 68).
- [116]Tomoyuki Morimae and Takeshi Koshiba. „Impossibility Of Perfectly-Secure Ono-Round Delegated Quantum Computing for classical client“. In: *Quantum Inf. Comput.* 19 (2019), pp. 214–221 (cit. on p. 74).
- [117]Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. „On the implausibility of classical client blind quantum computing“. In: *ArXiv abs/1704.08482* (2017) (cit. on p. 74).
- [118]Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. *On the possibility of classical client blind quantum computing*. 2018. arXiv: 1802.08759 [cs.CR] (cit. on p. 74).
- [119]Philip Walther, Kevin J Resch, Terry Rudolph, et al. „Experimental one-way quantum computing“. In: *Nature* 434.7030 (2005), pp. 169–176 (cit. on p. 74).
- [120]Jonas Zeuner, Aditya N Sharma, Max Tillmann, et al. „Integrated-optics heralded controlled-NOT gate for polarization-encoded qubits“. In: *npj Quantum Information* 4.1 (2018), pp. 1–7 (cit. on p. 74).
- [121]Michael O Rabin. „How To Exchange Secrets with Oblivious Transfer.“ In: *IACR Cryptology ePrint Archive* 2005 (2005), p. 187 (cit. on p. 81).
- [122]Shimon Even, Oded Goldreich, and Abraham Lempel. „A randomized protocol for signing contracts“. In: *Communications of the ACM* 28.6 (1985), pp. 637–647 (cit. on p. 82).
- [123]Claude Crépeau. „Equivalence between two flavours of oblivious transfers“. In: *Conference on the Theory and Application of Cryptographic Techniques*. Springer. 1987, pp. 350–354 (cit. on p. 82).
- [124]Hoi-Kwong Lo. „Insecurity of quantum secure computations“. In: *Physical Review A* 56.2 (1997), p. 1154 (cit. on p. 82).
- [125]Hoi-Kwong Lo and Hoi Fung Chau. „Is quantum bit commitment really possible?“ In: *Physical Review Letters* 78.17 (1997), p. 3410 (cit. on p. 82).
- [126]Dominic Mayers. „Unconditionally secure quantum bit commitment is impossible“. In: *Physical review letters* 78.17 (1997), p. 3414 (cit. on p. 82).
- [127]Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. „Cryptography from noisy storage“. In: *Physical Review Letters* 100.22 (2008), p. 220502 (cit. on p. 82).
- [128]Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. „Efficient non-interactive secure computation“. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2011, pp. 406–425 (cit. on p. 82).

- [129]Vipul Goyal, Yuval Ishai, Amit Sahai, Ramarathnam Venkatesan, and Akshay Wadia. „Founding cryptography on tamper-proof hardware tokens“. In: *Theory of Cryptography Conference*. Springer. 2010, pp. 308–326 (cit. on p. 82).
- [130]Shafi Goldwasser, Yael Tauman Kalai, and Guy N Rothblum. „One-time programs“. In: *Annual International Cryptology Conference*. Springer. 2008, pp. 39–56 (cit. on p. 82).
- [131]Mihir Bellare, Viet Tung Hoang, and Phillip Rogaway. „Adaptively secure garbling with applications to one-time programs and secure outsourcing“. In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2012, pp. 134–153 (cit. on p. 82).
- [132]DGBJ Dieks. „Communication by EPR devices“. In: *Physics Letters A* 92.6 (1982), pp. 271–272 (cit. on p. 82).
- [133]John Neumann. *Mathematical foundations of quantum mechanics*. Princeton university press, 1955 (cit. on p. 82).
- [134]Marie-Christine Roehsner, Joshua A Kettlewell, Tiago B Batalhão, Joseph F Fitzsimons, and Philip Walther. „Quantum advantage for probabilistic one-time programs“. In: *Nature communications* 9.1 (2018), pp. 1–8 (cit. on pp. 83, 85, 86, 93).
- [135]Joseph Fitzsimons Marie-Christine Roehsner Joshua A. Kettlewell and Philip Walther. „Probabilistic one-time programs using quantum entanglement“. In: *Manuscript in preparation* (2020) (cit. on pp. 86, 94).
- [136]Morris J Dworkin. *SHA-3 standard: Permutation-based hash and extendable-output functions*. Tech. rep. 2015 (cit. on p. 94).
- [137]qutools *quED: A Science Kit for Quantum Physics*. <https://www.qutools.com/qued>. Accessed on 11th August 2020 (cit. on pp. 97, 102).
- [138]George Gabriel Stokes. „On the composition and resolution of streams of polarized light from different sources“. In: *Transactions of the Cambridge Philosophical Society* 9 (1851), p. 399 (cit. on p. 98).
- [139]Daniel FV James, Paul G Kwiat, William J Munro, and Andrew G White. „On the measurement of qubits“. In: *Asymptotic Theory of Quantum Statistical Inference: Selected Papers*. World Scientific, 2005, pp. 509–538 (cit. on p. 100).
- [140]Z. Hradil. „Quantum-state estimation“. In: *Phys. Rev. A* 55 (3 1997), R1561–R1564 (cit. on p. 101).
- [141]Daniel F. V. James, Paul G. Kwiat, William J. Munro, and Andrew G. White. „Measurement of qubits“. In: *Phys. Rev. A* 64 (5 2001), p. 052312 (cit. on p. 101).
- [142]Kwiat Quantum Information Group. *Github: Quantum State Tomography*. <https://github.com/KwiatQIM/Quantum-Tomography>. Accessed on 11th August 2020 (cit. on p. 102).
- [143]Kwiat Quantum Information Group. *Guide to Quantum State Tomography*. <http://research.physics.illinois.edu/QI/Photonics/Tomography>. Accessed on 11th August 2020 (cit. on p. 102).
- [144]Valerie Coffman, Joydip Kundu, and William K Wootters. „Distributed entanglement“. In: *Physical Review A* 61.5 (2000), p. 052306 (cit. on p. 102).

- [145]William K Wootters. „Entanglement of formation of an arbitrary state of two qubits“. In: *Physical Review Letters* 80.10 (1998), p. 2245 (cit. on p. 102).
- [146]Andrew G White, Daniel FV James, Philippe H Eberhard, and Paul G Kwiat. „Nonmaximally entangled states: production, characterization, and utilization“. In: *Physical review letters* 83.16 (1999), p. 3103 (cit. on p. 102).
- [147]Jorge Carvioto-Lagos, Gustavo Armendariz, Victor Velázquez, et al. „The Hong–Ou–Mandel interferometer in the undergraduate laboratory“. In: *European journal of physics* 33.6 (2012), p. 1843 (cit. on p. 102).
- [148]Agata M. Brańczyk. *Hong-Ou-Mandel Interference*. 2017. arXiv: 1711.00080 [quant-ph] (cit. on p. 106).