



universität
wien

MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

**„Nonlinear Behavior of Entangled Photon Emission
and its impact on Quantum Communication
Protocols“**

verfasst von / submitted by

Ulrich Galander 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:

UA 066 876

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

Masterstudium Physik UG2002

Betreut von / Supervisor:

emer. o. Univ.-Prof. Dr. Dr. h.c. Dr. h.c. Anton Zeilinger

Acknowledgment

This thesis would not be finished without a few people. Hence, I want to say thank you to

- Prof. Anton Zeilinger and Dr. Rupert Ursin for letting me work in this extraordinary field of physics and welcoming me in such a friendly way in their group.
- The Quapitalist Sebastian N. for answering me all my questions, even the dumbest ones, and Domenico and Lukas A. for the funny time in the lab.
- Lukas B, Sebastian E. and Kristian for showing me that free-space is more awesome than fiber.
- Johnny, Dominik, Johannes, Matthias, Sören, Julius and of course Thomas for always taking time when I had questions.
- Robert for accompanying me from the first lecture in my master studies until the end.

And of course I want to thank my family for supporting me in every possible way.

Abstract

In order to implement a first international quantum key distribution (QKD) link between two cities using deployed telecom glass fibers, we built up and characterized with a visibility measurement a polarization entangled photon source in Sagnac configuration. We achieved a visibility in H/V: 99.09% and in D/A: 97.87%. Further we built up and characterized two free-space detection modules, which will be used at the endpoints of the QKD link to analyze the polarization of the incoming photons.

Afterwards we investigated how the visibility and the quantum bit error rate (QBER) scaled with the mean photon pair number μ in a regime where $\mu < 0.1$ and found a linear behaviour for both of them. In the end we calculated the keyrates for different channel losses and compared them with a new developed model. In our investigated regime ($\mu < 0.1$) the experimental data and the simulation were in good accordance to each other.

Abstract

Im Zuge des Aufbaus eines Quantenschlüsselnetzwerks zwischen zwei Städten, das bereits verlegte Telekom-Glasfasern benutzt, wurde eine Quelle für polarisationsverschränkte Photonen gebaut und charakterisiert. Die Charakterisierung geschah mit einer Kontrast Messung. Wir erreichten einen Kontrast in der H/V-Basis von 99.09% und in der D/A-Basis von 97.87%. Weiters wurden zwei Freistrahlempfangsmodule für die beiden Endpunkte des Quantenschlüsselnetzwerkes gebaut und analysiert.

Danach untersuchten wir die Abhängigkeit des Kontrastes und der Quanten-Bit-Error-Rate von der durchschnittlichen Photonen Paar Zahl μ und fanden einen linearen Zusammenhang im Bereich für $\mu < 0.1$. Zum Schluss berechneten wir die Schlüsselrate für verschiedene Verluste entlang der Kanäle, verglichen unsere Daten mit einem neu entwickelten Model und fanden eine gute Übereinstimmung im Bereich $\mu < 0.1$.

1	Introduction	4
2	Theoretical Background	6
2.1	Quantization of the Electromagnetic Field	6
2.2	Quantum State	8
2.3	Quantum Bit (Qubit)	9
2.4	Entanglement	9
2.5	Spontaneous Parametric Down Conversion	11
2.6	QKD	13
2.6.1	BBM92	13
2.6.2	Quantum Bit Error Rate (QBER)	14
2.6.3	Keyrate	14
2.7	Single Counts, Jitter, Coincidence Counts and Visibility	15
2.8	Detection Module for Polarization Entangled Photons	16
3	Sources for Polarization-Entangled Photons	18
3.1	Beta Barium Borate (BBO) Source	18
3.2	Crossed-Crystal Configuration	19
3.3	Folded Sandwich Configuration	21
3.4	Sagnac Loop	22
3.4.1	Generation of Entanglement with a Sagnac Interferometer	22
3.4.2	Source	24
3.4.3	Alignment Procedure	27
3.4.4	Dense Wavelength Division Multiplexing	31
3.4.5	Setting a Bell State	34
3.4.6	Results	35

CONTENTS

4	Polarization Analysis of Single Photons	39
4.1	Detection Module for Polarization Entangled Photons	39
4.1.1	Alignment Procedure	40
4.2	Superconduction Nanowire Single Photon Detectors (SNSPD)	43
4.3	Time Tagging Module (TTM)	45
4.3.1	Jitter	46
4.3.2	Correlation Measurement	47
5	Quantum Key Distribution using a CW-Laser	50
5.1	General Considerations	50
5.2	Asymmetric Noisy Link	51
5.3	Symmetric Link	54
6	Conclusion and Outlook	60
	List of Figures	61
	List of Tables	62
	Bibliography	63
A	No-cloning Theorem	68
B	Jones Formalismus	69
C	Gaussian Optics	70
D	Accidental Coincidence Counts	72

CHAPTER 1

INTRODUCTION

Quantum Key Distribution (QKD) has its origin in 1984, when Charles H. Bennett and Gilles Brassard showed how to use the polarization of single photons to securely transfer information from A to B [1], historically called Alice (A) and Bob (B). Their protocol (BB84) is now a prime example in introductory lectures on quantum information.

A few years later, in 1991, Artur Ekert published a QKD protocol which utilized entangled states in order to generate a secret key, and its security relies on the Clauser-Horne-Shimony-Holt (CHSH) inequality [2], a variation of the famous Bell inequality [3]. One year later Charles Bennett developed a protocol for QKD where non-orthogonal states [4] are used. The protocol is nowadays known as BBM92 and will be the one that we use in this thesis. These three protocols have one main thing in common: They guarantee security based on the no-cloning theorem¹, a quantum mechanical statement and therefore based on universal physical laws, whereas common cryptography (e.g. RSA-based-cryptosystems) relies on the computational hardness of certain mathematical operations². The latter seemed secure for *classical*³ computers anyway. However, this is not the case for a quantum computer anymore, due to Peter Shor. He developed an algorithm which, if ran on a quantum computer, is way more efficient than a *classical* computer to overcome this computational hardness [5].

Although quantum computers seemed far away, Google recently published an article claiming *quantum supremacy* [6], as they created a 53 qubit quantum computer.

This strengthens the reasons for research in QKD. Pioneering work has already been done in which free-space links, optical fiber links and also satellite-to-ground links were

¹See appendix A

²For example the factorisation of prime numbers

³With *classical* we mean any one of various supercomputers worldwide

used. [7, 8, 9] is only a small subset of the enormous amount of publications regarding this subject.

In order to establish a quantum network connecting several European cities, the project QUAPITAL⁴ (Quantum Photonic Intercity TrAnsmision Lattice) was started. QUAPITAL uses existing glass-fibers between those cities to generate a first quantum-internet utilizing QKD, which is working 24/7. The first link we want to establish is between the Austrian city St. Poelten and the capital of Slovakia, Bratislava.

In figure 1.1 we see an overview of the situation. The entangled photon source will be located in Vienna. The signal is then distributed from there on a symmetric link through glass-fiber. The most challenging parts of the project are overcoming the dispersion of the signal and the loss (roughly 25 dB between St. Poelten and Vienna). But there will still pass a lot of time until the project reaches the point when first measurements between these two cities can be done.

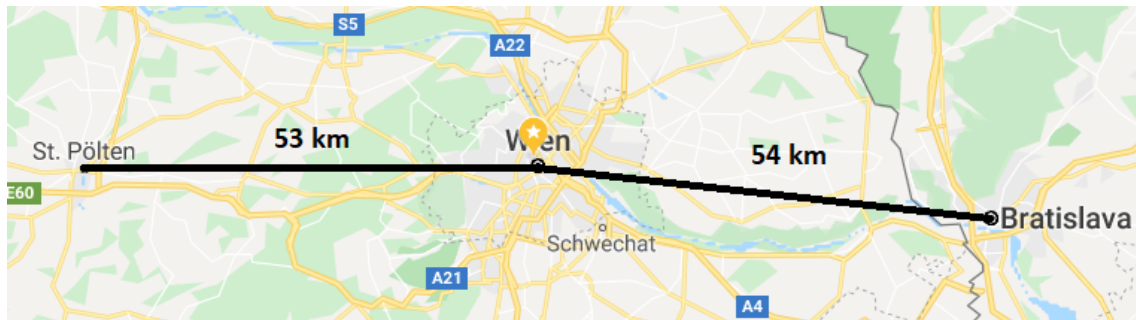


Figure 1.1: The first QUAPITAL link between St. Poelten and Bratislava. Figure taken from <https://www.google.at/maps>

But at this time, the entangled photon source is ready and fully functional. So we could test a QKD model developed for a source which works with a continuous wave (cw) laser [10]. Until now, the standard keyrate model, developed by Xiongfeng Ma [11], has only considered pulsed laser sources.

Now I would say, let the journey begin...

⁴<https://quapital.eu>

CHAPTER 2

THEORETICAL BACKGROUND

This section serves to define briefly the very basic ideas of the theoretical background which is needed for this thesis. For a more detailed explanation of the concepts, there is incredibly much excellent literature available, online as well as printed. A small subset of my personal favourites are [12, 13, 14].

2.1 Quantization of the Electromagnetic Field

The electric ($\vec{E}(\vec{x}, t)$) and magnetic ($\vec{B}(\vec{x}, t)$) field calculated from the Maxwell equations, see e.g. [15], emerges from a more fundamental entity, the so-called photon field $\vec{A}$, as follows:

$$\vec{E} = -\frac{1}{c} \frac{\partial \vec{A}}{\partial t}, \quad \vec{B} = \nabla \times \vec{A}, \quad (2.1)$$

where $\vec{A}$ satisfies the Coulomb gauge ($\nabla \cdot \vec{A} = 0$) and also the wave equation¹

$$\square \vec{A} = 0 \quad (2.2)$$

We can interpret $\vec{A}$ as the wave function of a photon which travels through space with a certain energy and momentum.

The most basic classical solution, up to a constant of (2.2), is

$$\vec{A}(\vec{x}, t) \sim \sum_{\vec{k}, \lambda} \left[e^{i(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)} \vec{b}_{\vec{k}, \lambda} + e^{-i(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)} \vec{b}_{\vec{k}, \lambda}^* \right], \quad (2.3)$$

where $\omega_{\vec{k}} = |\vec{k}|c$, $\vec{b}_{\vec{k}}$ is the polarization vector orthogonal to $\vec{k}$ and $\vec{b}_{\vec{k}}^*$ its complex conjugate.

¹ $\square := (\Delta - \frac{1}{c^2} \frac{\partial^2}{\partial t^2}) = 0$, where Δ is the Laplace operator

Now we can define the polarization of the field by writing $\vec{b}_{\vec{k}}$ as a linear combination of normalized real vectors $\vec{\epsilon}_{\vec{k},1}$, $\vec{\epsilon}_{\vec{k},2}$ which form together with $\vec{k}$ an orthonormal system, as seen in figure 2.1.

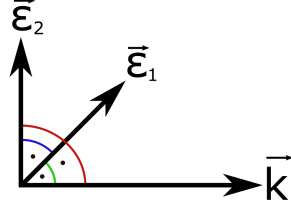


Figure 2.1: The polarization vector $\vec{b}_{\vec{k}}$ is set according to this orthonormal vectors, where $\vec{k}$ represents the wave vector of the field.

Linear Polarization

By writing the polarization vector as

$$\vec{b}_{\vec{k}} = b_{\vec{k},1}\vec{\epsilon}_{\vec{k},1} + b_{\vec{k},2}\vec{\epsilon}_{\vec{k},2}, \quad \vec{b}_{\vec{k}} = \vec{b}_{\vec{k}}^* \quad (2.4)$$

equation (2.3) reduces to

$$\vec{A}(\vec{x}, t) \sim \sum_{\vec{k}} \cos(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t) (b_{\vec{k},1}\vec{\epsilon}_{\vec{k},1} + b_{\vec{k},2}\vec{\epsilon}_{\vec{k},2}). \quad (2.5)$$

Here one can see that both polarization vectors oscillate with the same phase. If $b_{\vec{k},1} = 0$, we call the field vertically polarized, and if $b_{\vec{k},2} = 0$, we call it horizontally polarized.

Circular Polarization

Now if we define another two orthogonal vectors in the complex plane

$$\vec{\epsilon}_{\vec{k},\pm} = \frac{1}{\sqrt{2}}(\vec{\epsilon}_{\vec{k},1} \pm i\vec{\epsilon}_{\vec{k},2}), \quad (2.6)$$

equation (2.3) can be rewritten in the following way:

$$\begin{aligned} \vec{A}(\vec{x}, t) \sim \sum_{\vec{k}} 2b_{\vec{k}+} \left[\frac{1}{\sqrt{2}}(\cos(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)\vec{\epsilon}_{\vec{k},1} + \sin(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)\vec{\epsilon}_{\vec{k},2}) \right] \\ + 2b_{\vec{k}-} \left[\frac{1}{\sqrt{2}}(\cos(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)\vec{\epsilon}_{\vec{k},1} - \sin(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)\vec{\epsilon}_{\vec{k},2}) \right]. \end{aligned} \quad (2.7)$$

By definition, the first term corresponds to right-handed circular, the bottom term to left-handed circular polarization.

Usually, to obtain an expression of a quantized version of $\vec{A}$, one starts by considering the field in a box of finite volume $V = L^3$ and writing down the classical Hamiltonian $\mathcal{H}$ of the field. It can then be shown that $\mathcal{H}$ has the form of a Hamiltonian of a harmonic oscillator. The quantization of a harmonic oscillator is well known in quantum mechanics and it is then straightforward to apply the same quantization procedure, with the annihilation and creation operators, to the case of the photon field $\vec{A}$. At the end one takes the limit of $V \rightarrow \infty$. For a rigorous derivation of a quantized photon field see for example [14].

In the end, the quantized $\vec{A}$ field has the form:

$$\hat{\vec{A}}(\vec{x}, t) = \sum_{\vec{k}, \lambda} \sqrt{\frac{\hbar}{2\omega_{\vec{k}}\epsilon_0 V}} \left[e^{i(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)} \hat{a}_{\vec{k}, \lambda} \vec{b}_{\vec{k}, \lambda} + e^{-i(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)} \hat{a}_{\vec{k}, \lambda}^\dagger \vec{b}_{\vec{k}, \lambda}^* \right]. \quad (2.8)$$

$\hbar$ is the reduced Planck constant, and $\hat{a}_{\vec{k}, \lambda}^\dagger$, $\hat{a}_{\vec{k}, \lambda}$ are the annihilation and creation operators, satisfying $[\hat{a}_{\vec{k}, \lambda}^\dagger, \hat{a}_{\vec{k}', \lambda'}^\dagger] = 0 = [\hat{a}_{\vec{k}, \lambda}, \hat{a}_{\vec{k}', \lambda'}]$ and $[\hat{a}_{\vec{k}, \lambda}, \hat{a}_{\vec{k}', \lambda'}^\dagger] = \delta_{\vec{k}, \vec{k}'} \delta_{\lambda, \lambda'}$. From (2.1) one can then obtain the quantized electromagnetic field

$$\hat{\vec{E}}(\vec{x}, t) = i \sum_{\vec{k}, \lambda} \sqrt{\frac{\hbar\omega_{\vec{k}}}{2\epsilon_0 V}} \left[e^{i(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)} \hat{a}_{\vec{k}, \lambda} \vec{b}_{\vec{k}, \lambda} - e^{-i(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)} \hat{a}_{\vec{k}, \lambda}^\dagger \vec{b}_{\vec{k}, \lambda}^* \right]. \quad (2.9)$$

(2.9) can be written in a simpler form by splitting up the individual terms in positive and negative frequency parts

$$\hat{\vec{E}}(\vec{x}, t) = i \sum_{\vec{k}, \lambda} \hat{\vec{E}}^+(\vec{x}, t) + \hat{\vec{E}}^-(\vec{x}, t), \quad (2.10)$$

where the following holds:

$$\hat{\vec{E}}^+(\vec{x}, t) = i \sum_{\vec{k}, \lambda} \sqrt{\frac{\hbar\omega_{\vec{k}}}{2\epsilon_0 V}} e^{i(\vec{k} \cdot \vec{x} - \omega_{\vec{k}} t)} \hat{a}_{\vec{k}, \lambda} \vec{b}_{\vec{k}, \lambda} \quad (2.11)$$

and

$$\hat{\vec{E}}^-(\vec{x}, t) = [\hat{\vec{E}}^+(\vec{x}, t)]^\dagger. \quad (2.12)$$

2.2 Quantum State

A quantum state $|\psi\rangle$, often referred to as wave function, is an element of a complex vector space $\mathcal{H}$, i.e.

$$|\psi\rangle \in \mathcal{H} \quad (2.13)$$

This vector space $\mathcal{H}$ is also called a Hilbert space. $|\psi\rangle$ can be written as an expansion of an orthonormal basis $\{|\phi_n\rangle\}$ of $\mathcal{H}$ as:

$$|\psi\rangle = \sum_n c_n |\phi_n\rangle, \quad (2.14)$$

where $c_n = \langle\phi_n|\psi\rangle$ are complex amplitudes with $\sum_n |c_n|^2 = 1$. A quantum measurement is represented by a Hermitian operator $\hat{A} = \hat{A}^\dagger$. It is known that for each Hermitian operator there is a complete orthonormal basis $\{|\psi_n\rangle\}$ of $\mathcal{H}$ made of eigenvectors of $\hat{A}$:

$$\hat{A} |\psi_n\rangle = a_n |\psi_n\rangle \quad (2.15)$$

The eigenvalues of this operator are the possible outcomes of a measurement of observable $\hat{A}$.

2.3 Quantum Bit (Qubit)

What we call in classical information theory a bit, has a quantum mechanical analogue. The so called 'quantum bit' or qubit. The most general form on how to express a qubit is as follows:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (2.16)$$

where $|0\rangle, |1\rangle$ is the so-called computational basis. Note that due to normalization $|\alpha|^2 + |\beta|^2 = 1$ holds. A qubit can be any two-level system, for example the ground and excited state of an atom. However, in the outline of this thesis we are looking at two-level systems which are formed by the (linear) polarization states of photons. So we can assign the computational basis in the following way:

$$|0\rangle \equiv |H\rangle, \quad |1\rangle \equiv |V\rangle, \quad (2.17)$$

where $|H\rangle$ refers to horizontally and $|V\rangle$ to vertically polarized photon states, respectively.

For completeness, the computational basis can also be written in terms of diagonal $|D\rangle$ and anti-diagonal $|A\rangle$ or right-handed circular $|R\rangle$ and left-handed circular $|L\rangle$ polarization states.

2.4 Entanglement

Entanglement is one of the puzzling properties of quantum theory.

Although the following treatment can be generalized to any dimension, let us for the sake of simplicity restrict ourselves to two qubit systems **A** and **B**. Each system is described by a Hilbert space $\mathcal{H}_A^2$, $\mathcal{H}_B^2$ respectively. Now let us consider one state of each system:

$$|\phi\rangle_A \in \mathcal{H}_A^2, \quad |\phi\rangle_B \in \mathcal{H}_B^2 \quad (2.18)$$

Via the tensor product of the two sub-spaces one can describe the composite system **AB** as follows:

$$\mathcal{H}_{AB}^4 = \mathcal{H}_A^2 \otimes \mathcal{H}_B^2 \quad (2.19)$$

If we can *not* write the state of the combined system **AB** as a product state of the two individual states, then we call it an entangled state. On the other hand, if it is possible to write it down in that way, we call it a product state.

Entangled state	Product state
$ \phi\rangle_{AB} \neq \phi\rangle_A \otimes \phi\rangle_B$	$ \phi\rangle_{AB} = \phi\rangle_A \otimes \phi\rangle_B$

Table 2.1: Difference between a product state and an entangled state for a two-qubit system.

For two-qubit systems, the Bell states below are of great importance:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B) \quad (2.20)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A |H\rangle_B - |V\rangle_A |V\rangle_B) \quad (2.21)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A |V\rangle_B + |V\rangle_A |H\rangle_B) \quad (2.22)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A |V\rangle_B - |V\rangle_A |H\rangle_B). \quad (2.23)$$

In this representation they describe two entangled photons polarized in the H/V basis. Equation (2.20)-(2.23) can be written in the D/A basis as well as the R/L basis. However, in these forms they may exhibit different correlation than in the H/V basis. Except for the $|\Psi^-\rangle$ state. It has the same form in all polarization bases, i.e. it is rotational invariant.

With just one part of a Bell state, we do not have any information about the total system. Only if we possess the full state, i.e. the full Bell state, we have complete

knowledge of the system. This can be used for several applications, like quantum key distribution (QKD), super dense coding [16] or quantum teleportation [17].

2.5 Spontaneous Parametric Down Conversion

To the present date the most convenient method to produce polarization entangled photons has been by utilizing spontaneous parametric down-conversion (SPDC). This process describes the interaction of a strong pump laser with a non-linear material [18]. Non-linear means that the electric susceptibility χ of the material can be Taylor expand, so that for the polarisation $\vec{P}$ and the electric field E the following holds:

$$\vec{P} = \epsilon_0(\chi^{(1)}E + \chi^{(2)}E^2 + \mathcal{O}(3)), \quad (2.24)$$

where ϵ_0 is the electric permittivity, $\chi^{(2)}$ is a rank 3 tensor and called the second order non-linear susceptibility.

On the scale of individual photons, SPDC can be described as the interaction of a pump photon with a non-linear material. The pump photon gets down-converted into two lower energy photons, namely the signal and idler photons, which exhibit a correlation in their polarization degree of freedom. Later we will exploit these correlations to generate an entangled state.

In general, one can distinguish three different kinds of a SPDC process:

- type-0: pump, signal and idler photons have the same polarization, e.g. $|H\rangle_p \rightarrow |H\rangle_s |H\rangle_i$
- type-I: signal and idler photons have the same polarization, but orthogonal to the pump photon's polarization, e.g. $|H\rangle_p \rightarrow |V\rangle_s |V\rangle_i$
- type-II: the polarization of signal and idler photons is orthogonal to each other, e.g. $|H\rangle_p \rightarrow |H\rangle_s |V\rangle_i$

Like in every physical process, energy and momentum conservation have to be complied. Energy conservation is given by:

$$\omega_p = \omega_s + \omega_i, \quad (2.25)$$

where p, s and i stand for pump, signal and idler, respectively. And momentum conservation is given by:

$$\vec{k}_p = \vec{k}_s + \vec{k}_i \quad (2.26)$$

In the case of a collinear phase matched crystal, where pump, signal and idler photons propagate in the same direction, equation (2.26) is reduced to the following scalar

equation

$$\omega_p n(\omega_p) = \omega_s n(\omega_s) + \omega_i n(\omega_i), \quad (2.27)$$

where we used $|\vec{k}| = \frac{n(\omega)\omega}{c}$ and $n(\omega)$ as the refractive index of the material. Both the equations (2.25) and (2.27) have to be fulfilled so that down conversion happens inside the crystal. However, due to the frequency-dependent refractive index, this is hardly ever the case.

The equation (2.26) is called the phase-matching condition, and in order to implement this condition, one can fabricate crystals so that $d_{eff} = \frac{\chi^{(2)}}{4}$, with $\chi^{(2)}$ as the second-order non-linear susceptibility, switches sign after a period² of Λ . This so-called "quasi-phase-matching"³ yields an extended version of (2.26),

$$\Delta\vec{k} = \vec{k}_p - \vec{k}_s - \vec{k}_i - \frac{2\pi}{\Lambda} = 0, \quad (2.28)$$

which we will need later on.

Now, in order to get an expression of the SPDC-state, one starts with the Hamiltonian [20]

$$\hat{H}_I = \epsilon_0 \int dV \chi^{(2)} \vec{E}_p \vec{E}_s^- \vec{E}_i^- + h.c. , \quad (2.29)$$

with the quantized electric fields described in 2.1 and $h.c.$ denoting the Hermitian conjugate. It is important to mention that $\vec{E}_p$ is assumed to be the field of a classical continuous wave (cw) laser. The most general solution of the Schrödinger equation for a time-dependent Hamiltonian is given by

$$|\psi\rangle_{SPDC} = e^{-\frac{i}{\hbar} \int_{t_0}^t dt' \hat{H}_I(t')} |0\rangle \quad (2.30)$$

By neglecting higher-order terms, which correspond to multi-photon states, we end up with an expression for a 2-photon SPDC-state [20, 21]

$$|\psi\rangle_{SPDC} \approx |0\rangle - \frac{i}{\hbar} \int_{t_0}^t dt' \hat{H}_I(t') |0\rangle \quad (2.31)$$

One solution of (2.31) is [20]

$$|\psi\rangle_{SPDC} \approx L \int d\Omega \operatorname{sinc}\left(\frac{\Delta\vec{k}L}{2}\right) a_s^\dagger(\Omega) a_i^\dagger(-\Omega) |0\rangle \quad (2.32)$$

where $\Delta\vec{k}$ is given in (2.28). Since the maximum value of a sinc-function is at zero, we

²This is what we call periodical poling

³For a comprehensive analysis of phase-matching in general see [19]

conclude that it is preferable to achieve $\Delta \vec{k} = 0$. Therefore we use periodically poled crystals, because with the additional factor of Λ in equation (2.28) it is easier to achieve $\Delta \vec{k} = 0$ if the poling period Λ is chosen appropriately.

2.6 QKD

One way to securely distribute a message between Alice and Bob is by using a random bit string, a so-called one-time-pad (OTP), with which they can encrypt and decrypt their message. The advantage of the OTP is that it is completely secure, but therefore the OTP has to be at least the same length as the message Alice and Bob want to encrypt. Like the name suggests, the OTP can only be used once and for each additional message Alice and Bob want to encrypt they need a new OTP. With quantum key distribution (QKD) two parties can generate a secret key, which they can use as a one-time-pad.

In this section we give an overview of the BBM92 QKD protocol [4], which utilizes non-orthogonal states to generate a secret key. Afterwards we will focus on two parameters which are relevant for QKD, namely the quantum bit error rate (QBER) and how to calculate keyrates.

2.6.1 BBM92

Roughly speaking, the BBM92 protocol is a mixture of the BB84 protocol [1] and the Ekert protocol [22] in the sense that we measure only in two bases like in the BB84 protocol but use entangled states like in the Ekert protocol. In the BBM92 protocol an entangled photon source produces a $|\Phi^+\rangle$ state, which is then distributed between Alice and Bob. Both Alice and Bob can randomly choose between two non-orthogonal measurement bases, in our case between H/V and D/A, to measure their part of the above mentioned Bell state. Since $|\Phi^+\rangle$ is rotational invariant between these two bases, i.e.

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s |H\rangle_i + |V\rangle_s |V\rangle_i) = \frac{1}{\sqrt{2}}(|D\rangle_s |D\rangle_i + |A\rangle_s |A\rangle_i), \quad (2.33)$$

Alice and Bob observe perfect correlations if they measure in the same basis. However, if the measurement basis Alice chose is different from the one Bob chose, the result will be uncorrelated.

Now consider a stream of $|\Phi^+\rangle$ states distributed between them. Alice as well as Bob choose their measurement basis randomly. In order to extract a secret key, they then communicate their chosen measurement basis, but not the specific outcome, over a public channel. After that, Alice and Bob discard every measurement where they have chose different measurement bases. In the next step they assign to their measurement outcome $|H\rangle$ or $|D\rangle$ the bit value 1, and to $|V\rangle$ or $|A\rangle$ the bit value 0. The resulting bit

string is called *sifted key*. However, a possible eavesdropper and technical imperfections lead to slightly different versions of the key Alice and Bob possess. In order to correct the erroneous bits, a classical error correction protocol has to be realized on the sifted key. The last step, known as privacy amplification, serves to erase information which a possible eavesdropper has about the sifted key. However, Alice and Bob have to sacrifice a part of the generated key. After all these steps, Alice and Bob share a random secret key which they can use as a one-time-pad.

2.6.2 Quantum Bit Error Rate (QBER)

As mentioned above, a possible eavesdropper or technical imperfections cause errors in the resulted sifted key. This error is called quantum bit error rate (QBER). We need to know the QBER to estimate how much information a possible eavesdropper could have about the key and therefore how much of our sifted key we have to sacrifice in the privacy amplification process.

The QBER is defined as [23]

$$QBER = \frac{\text{Number of wrong bits}}{\text{Total number of bits}} \quad (2.34)$$

This can be split up into two different contributions

$$QBER = QBER_{opt} + QBER_{acc} \quad (2.35)$$

It can be shown that the measurable QBER, depending on the fringe visibility $\mathcal{V}$ (2.40), is given by

$$QBER = \frac{1 - \mathcal{V}}{2} \quad (2.36)$$

$QBER_{opt}$ is the error which occurs due to optical imperfections of the system, i.e. the extinction ratio (4.1) of the used PBSs. $QBER_{acc}$ has its origin in the coincidence counts (CC) which do not originate from the true entangled photons. This can be for example CC from a noise count with one part of an entangled pair, from multi-pair emission from the source or from two noise counts.

2.6.3 Keyrate

The key generation rate R , a lower bound for the final key (assuming the limit of an infinite key) after a QKD process, including error correction and privacy amplification, is given by [11]:

$$R \geq \frac{1}{2} \{Q_\lambda [1 - H_2(QBER)(1 + f)]\} \quad (2.37)$$

Q_λ is the sum of all measured coincidences, f is the bi-directional error correction efficiency, which, simply put, is the average number of bits one needs to correct one erroneous bit. In our case, $f = 1.1$ and $H_2(x)$ is the binary entropy function

$$H_2(x) = -x \log_2(x) - (1-x) \log_2(1-x) \quad (2.38)$$

The factor $\frac{1}{2}$ in front of (2.37) can be explained by the fact that half of the time Alice and Bob measure in different bases and therefore they have to discard these results from the very first [24]. Equation (2.37) shows that for $f = 1.1$, QBER of $\sim 10\%$ is too much to gain any secure key at all.

2.7 Single Counts, Jitter, Coincidence Counts and Visibility

Alice as well as Bob measure their receiving photons (signal or idler) locally. Their measurement rate, given in counts per second (counts/s), are so-called single counts. However, in order to verify that signal and idler photons originated from the same pump photon, we correlate the single counts on Alice's side with the single counts on Bob's side to gain coincidence counts CC. A coincidence count, commonly called coincidence, is defined as a click on the detector on Alice's side and a click on the detector on Bob's side, which happens within a given time interval τ_{CC} (typical values are between 200 ps up to 1 ns) called coincidence window and with a fixed delay due to different fiber lengths. Unfortunately, detectors have a so-called jitter τ_{jitter} . τ_{jitter} is an uncertainty in the time T the detector needs to convert an incoming photon into a measurable electric signal. Therefore it is necessary to choose τ_{CC} appropriately. We will go into more detail in section 4.3.1.

The fringe visibility or simple visibility $\mathcal{V}$ is a common measure of the quality of the entangled state the source produces. The visibility is given by

$$\mathcal{V} = \frac{CC_{Max} - CC_{Min}}{CC_{Max} + CC_{Min}}, \quad (2.39)$$

where CC_{Max} are the maximum coincidence counts, namely these coincidences we are measuring. CC_{Min} , on the other hand, has three contributions, where the most significant part comes from accidental coincidences CC_{acc} . But this will be discussed later in chapter 5.

For a $|\Phi^+\rangle$ or $|\Phi^-\rangle$ state the visibility is given by:

$$\mathcal{V} = \frac{CC_{ii} + CC_{jj} - CC_{ij} - CC_{ji}}{CC_{ii} + CC_{jj} + CC_{ij} + CC_{ji}}, \quad (2.40)$$

where CC_{ij} is the number of coincidences when Alice measures i and Bob measures j . In the H/V basis i corresponds to H and j to V , whereas in the D/A basis $i = D$ and $j = A$.

2.8 Detection Module for Polarization Entangled Photons

To measure linearly polarized photons, we use a so-called detection module depicted in figure 2.2. The photons travel through a single mode fiber (SMF) to a fiber coupler, where they get collimated. At a beam splitter (BS), which is *not* polarization dependent, with a splitting ratio of 50:50, the photons get randomly transmitted or reflected. Hence, the BS works as a passive random basis choice for a QKD setup.

Transmitted Arm of the 50:50 BS, i.e. H/V Basis Measurement

In the transmitted arm of the 50:50 BS, the photons enter a polarizing beam splitter, (PBS) which distinguishes the polarization states of the photons. A horizontally polarized photon gets transmitted to detector 1, whereas a vertically polarized photon gets reflected to detector 2. Diagonal or anti-diagonally polarized photons have a probability of $1/2$ to get either transmitted or reflected.

Reflected Arm of the 50:50 BS, i.e. D/A Basis Measurement

The reflected photons first pass a half wave plate (HWP) oriented at 22.5° with respect to the optical axis. The HWP induces the following transformation to the polarization of the incident photons (omitting global phases):

$$\begin{aligned} |D\rangle &\rightarrow |H\rangle, & |H\rangle &\rightarrow |D\rangle \\ |A\rangle &\rightarrow |V\rangle, & |V\rangle &\rightarrow |A\rangle \end{aligned}$$

After the HWP they also have to pass a PBS, where again horizontally polarized photons are transmitted to detector 3 and vertically polarized photons are reflected and led to detector 4. Therefore in the reflected arm of the 50:50 BS, a diagonally polarized photon is turned into $|H\rangle$ and transmitted into detector 3 and an anti-diagonally polarized photon is reflected into detector 4, whereas a horizontally or vertically polarized photon has a chance of $1/2$ to get either to detector 3 or detector 4.

The transformation and the HWP together with the PBS measuring in the D/A basis can be achieved in another way too. For that, one has to remove the HWP and physically rotate the PBS around 45° with respect to the optical axis. This changes the reference frame of the PBS in such a way that it now transmits diagonal polarized photons and

reflects anti-diagonal polarized ones. This was actually performed by Matthias Fink in [25].

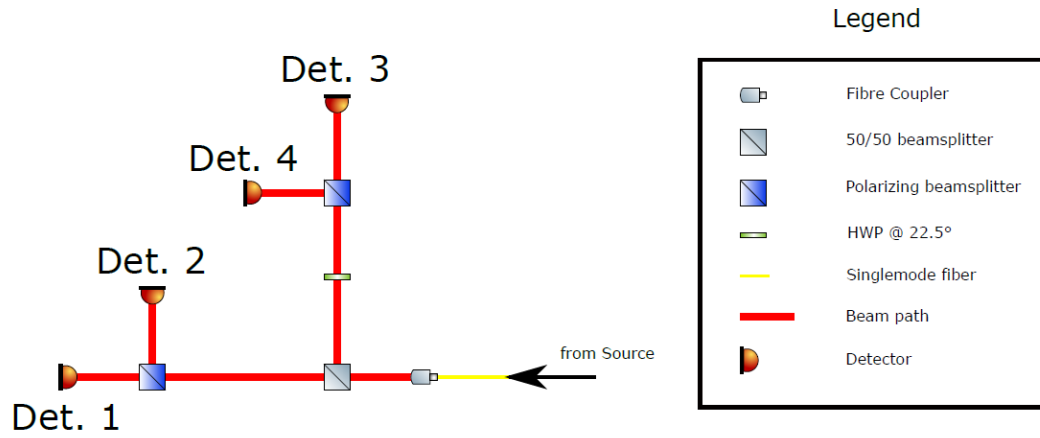


Figure 2.2: Sketch of a detection module to detect linear polarized photons. For a further explanation we refer to the main text.

CHAPTER 3

SOURCES FOR POLARIZATION-ENTANGLED PHOTONS

In the following chapter, we will introduce different sources for polarization-entangled photon pairs. All of them exhibit their own advantages and drawbacks, which make them usable for different applications. After that, we will discuss the so-called 'Sagnac'-source, which is used in this experiment, in more detail. This type has the big advantage of being able to yield a high brightness, which is necessary for the upcoming experiments, where we will use the source we built here.

3.1 Beta Barium Borate (BBO) Source

The first publication of a polarization-entangled photon pair source using a beta barium borate (BBO) crystal was by Kwiat et al. in [26]. The crystal was manufactured for type-II phase matching. Therefore the emitted signal and idler photon were polarized orthogonally to each other and emitted in two cones. At the intersections of these two cones one can describe the state by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A |V\rangle_B + e^{i\alpha} |V\rangle_A |H\rangle_B). \quad (3.1)$$

The phase α is due to the BBOs birefringence and can be set by additional birefringence phase shifters, as Kwiat et al. pointed out in [26]. The four Bell states (2.20)-(2.23) can then be fixed by placing a half wave plate (HWP) and a quarter wave plate (QWP) in one arm to change the polarization from vertical to horizontal and vice versa [26].

The used setup of Kwiat et al. [26] is shown in figure 3.1. The crystal was pumped by a 150 mW strong laser, which had an operation wavelength of 351.1 nm. Signal and idler beam were spatially separated and each led through an additional BBO crystal (C1 and

C2 in figure 3.1) to compensate for transversal (the extraordinary beam gets a transverse shift relative to the ordinary beam) and longitudinal (arises because of different group velocities of the two beams inside the BBO) walk-off effects. With HWP1 and QWP1 one can set the desired Bell state. With this source Kwiat et al. reached a visibility of 97.8 % and achieved a violation of the CHSH inequality by more than 100 standard deviations [26].

Although for this time (1995) the source was a great achievement, in comparison to today's sources ($CC \approx 8000s^{-1}$) the coincidence count rates in [26] ($CC \approx 50s^{-1}$) were much lower. This is easy to see, since the entangled state only exists at the intersection of the cones. Nevertheless, due to this unpretentious setup, this type of source is often used in lab courses on universities to demonstrate the principles of experimental quantum optics.

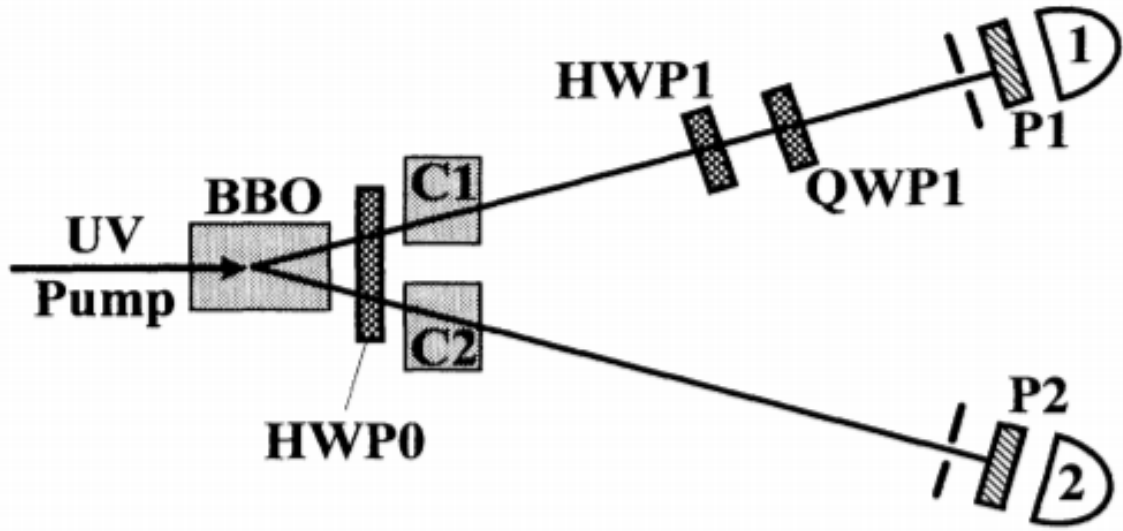


Figure 3.1: Setup of an type II source with a BBO crystal. Picture taken from [26].

3.2 Crossed-Crystal Configuration

Four years after the publication of his BBO source [26], Paul Kwiat set up a source again. Together with his colleagues at the Los Alamos National Laboratory, he constructed a novel source for polarization entangled photons, where two nonlinear crystals were placed right behind each other. The researchers used again BBO crystals in a type-I SPDC process and achieved a, for the time (1999), high brightness source (10 000 CC/s at 150 mW pump power), which was able to violate Bell's inequality in 160 s up to $246\text{-}\sigma$ [27]. Since then, various other authors have published articles about polarization entangled photon sources, like Scheidl et al. in [28] or Steinlechner et al. in [18].

In Steinlechner's paper [18] the crossed-crystal configuration for a source improved for applications in free space was used. By utilizing two 20 mm periodically poled potassium titanyl phosphate (ppKTP) crystals with a collinear type-0 phase matching, they detected 16 000 CC/s with a pump power of 25 μ W, and the generated state had a fidelity $F = \langle \Phi^+ | \rho | \Phi^+ \rangle$ of (0.983 ± 0.005) [18].

How the entangled state is produced is shown in figure 3.2. The two crystals are placed one after another, but the second crystal is turned by 90° with respect to the first one, as seen in figure 3.2. Non-linear crystals are fabricated so that the down-conversion only happens if one pumps the crystal with a specific polarization. Now we assume that the pump photon is $|D\rangle_p = \frac{1}{\sqrt{2}}(|H\rangle_p + |V\rangle_p)$ polarized. This in mind, we see that the horizontal polarized part of the pump-photon can get down-converted only in the first crystal according to

$$|H\rangle_p \rightarrow e^{i\alpha} |H\rangle_s |H\rangle_i,$$

whereas the vertically polarized part of the pump photon only can get down-converted in the second crystal like this:

$$|V\rangle_p \rightarrow e^{i\beta} |V\rangle_s |V\rangle_i$$

Since it cannot be known which of these two options actually happens the state after the two crystals is a superposition of these two alternatives (omitting a global phase):

$$|D\rangle_p \rightarrow |H\rangle_s |H\rangle_i + e^{i(\beta-\alpha)} |V\rangle_s |V\rangle_i,$$

up to some normalization factor. A possible "which-crystal" information that results in a reduced visibility can be compensated with a Yttrium Vanadate (YVO_4) crystal [18]. For a more detailed description see [18, 20].

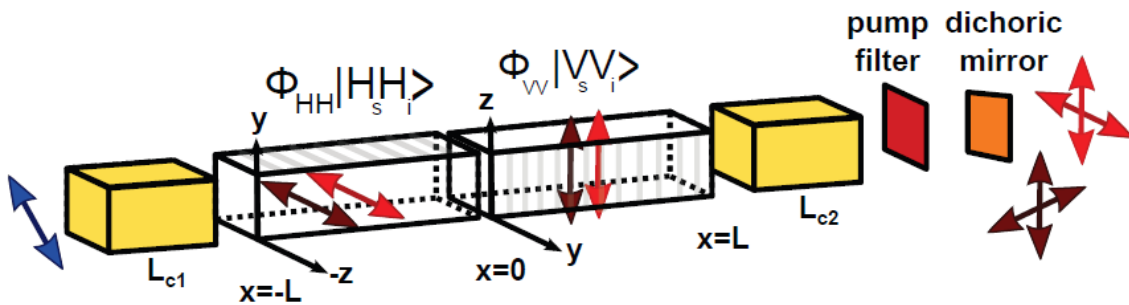


Figure 3.2: Sketch of the generation of an entangled state with a crossed crystal configuration. For description we refer to the main text. Picture taken from [20].

3.3 Folded Sandwich Configuration

Another type of source, first experimentally implemented in 2003 by Marco Barbieri et al. [29], later by Juan Hodelin et al. [30] and Fabian Steinlechner et al. [31], exploits a mirror so that the pump beam passes through the crystal twice, but in different directions. Since both Barbieri and Hodelin used a BBO crystal for their setup, we will stick in the further discussion to Steinlechner's publication [31], which described a type-0 periodically poled KTiOPO₄ (ppKTP) crystal.

Steinlechner pumped a 11.48 mm ppKTP with a laser diode operating at 405 nm. The down-converted signal and idler photons had non-degenerated wavelengths of 784 nm and 839 nm, respectively. With their setup they achieved 11 800 CC/s with 10.4 μ W pump power on the crystal facet. The measured Bell state fidelity without accidental coincidence correction $F = \langle \Phi^+ | \rho | \Phi^+ \rangle$ was (0.992 ± 0.003) [31].

Figure 3.3 shows the working principle of this source type. The following discussion is based on [31]. Furthermore we omit a global phase. However, due to the pass through the non-linear crystal a relative phase between signal and idler photons appears which can not be neglected.

Let us consider that the crystal is placed in such a way that it has to be pumped with vertically polarized light. Since we are dealing with a type-0 crystal, the SPDC state after the first pass through the crystal reads:

$$|V\rangle_p \rightarrow |V\rangle_s |V\rangle_i$$

The SPDC photons as well as the pump photons have to pass a special waveplate (SWP in figure 3.3) which acts as a HWP for the pump photons and as a QWP for signal and idler photons, respectively. After that, the photons are reflected at mirror M1 (see figure 3.3), which works for the wavelength of the pump photon as well as for the SPDC photons, and pass the non-linear crystal a second time.

So let us have a look at what is happening if we consider a perfect waveplate with the abilities mentioned above. If the SPDC happens in the first pass through the crystal we have the following successive events:

$$\begin{aligned} |V\rangle_p &\xrightarrow{\text{crystal}} |V\rangle_s |V\rangle_i \xrightarrow{\text{SWP}} |L\rangle_s |L\rangle_i \xrightarrow{\text{mirror}} |R\rangle_s |R\rangle_i \xrightarrow{\text{SWP}} |H\rangle_s |H\rangle_i \\ &\xrightarrow{\text{crystal}} |H\rangle_s |H\rangle_i. \end{aligned}$$

In the case where the SPDC happens in the second pass through the crystal, the following order holds:

$$|V\rangle_p \xrightarrow{\text{crystal}} |V\rangle_p \xrightarrow{\text{SWP}} |H\rangle_p \xrightarrow{\text{mirror}} |H\rangle_p \xrightarrow{\text{SWP}} |V\rangle_p \xrightarrow{\text{crystal}} |V\rangle_s |V\rangle_i.$$

The relevant matrices in Jones formalism are given in appendix B.

Since we do not know in which pass the SPDC happens, we end up with the following entangled Bell state:

$$|\Phi\rangle = \frac{1}{\sqrt{2}}(|V\rangle_s |V\rangle_i) + e^{i\alpha} |H\rangle_s |H\rangle_i.$$

The phase α , like in 3.2, is again due to the pass through the crystal and has to be compensated. With a dichroic mirror DM1 in figure 3.3 the SPDC is then separated from the pump beam. Afterwards signal and idler photons are separated from each other by DM2.

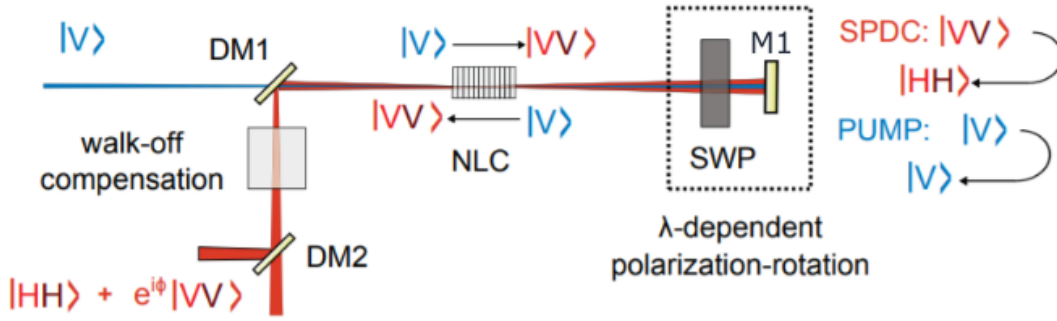


Figure 3.3: Schematic working principle of the folded sandwich configuration for polarization entangled photons. As one can see, the type-0 crystal gets pumped twice due to the reflection at mirror M1. By this double pass through the non-linear crystal, one can generate an entangled state. A dichroic mirror DM1 separates the SPDC from the pump photons and DM2 separates signal and idler photon from each other. Figure taken from [31].

3.4 Sagnac Loop

The first demonstration of a polarization entangled photon source using a Sagnac interferometer was demonstrated by Shi in [32], where they used a type-I phase matched BBO crystal. Later Kim et al. [33] and Fedrizzi et al. [34] enhanced this configuration.

3.4.1 Generation of Entanglement with a Sagnac Interferometer

In order to generate a Bell state with a Sagnac interferometer, one has to assume a superposition of the clock and counter-clockwise propagating SPDC photons at the PBS after one round trip.

Let us analyse the two propagation directions in detail.

Counter-Clockwise Propagation

If the pump photon is horizontally polarized $|H\rangle_p$ like in figure 3.4 (a), the photon is transmitted through the dual wavelength PBS (dPBS). If down-conversion happens in

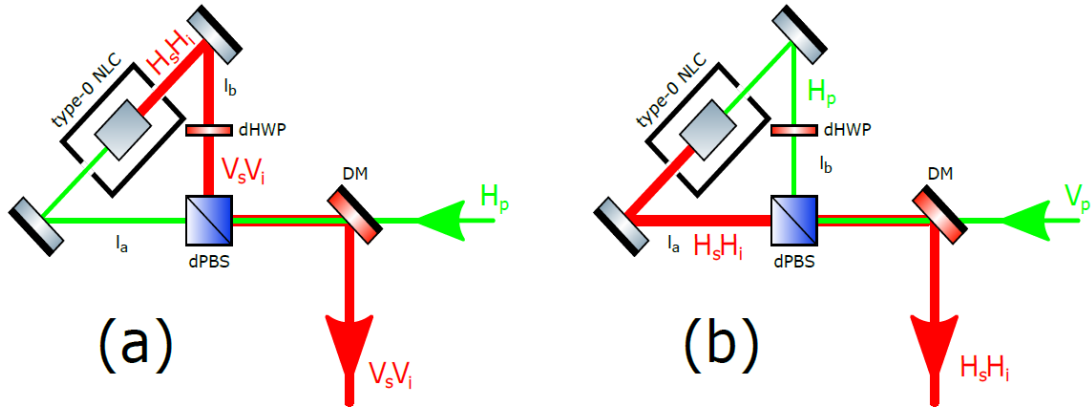


Figure 3.4: Sagnac-loop for producing polarization entangled photons. (a) Pump beam is horizontally polarized, (b) Pump beam is vertically polarized. In order to produce a polarization entangled state, the pump beam is polarized as a superposition $|H\rangle_p + e^{i\alpha}|V\rangle_p$ so that both scenarios are realised.

the type-0 non-linear crystal (NLC), the pump photon transforms to signal and idler photons $|H\rangle_s |H\rangle_i$. After traversing the dual wavelength HWP@45° (dHWP), they change polarization to $|V\rangle_s |V\rangle_i$ and are reflected by the dPBS. Hence, after the dPBS the state $|H\rangle_p$ has made the following transformation [33]

$$|H\rangle_p \rightarrow e^{i[k_p l_a + (k_s + k_i)l_b + \theta_s + \theta_i]} \eta_H E_H |V\rangle_s |V\rangle_i. \quad (3.2)$$

$l_{a,b}$ are the distances from the dPBS to the crystal, $\theta_{s,i}$ is the additional phase of signal and idler photon for crossing the dHWP, η_H is the generation efficiency and E_H is the horizontal component of the electric field of the pump [35].

Clockwise Propagation

For a vertically polarized photon $|V\rangle_p$ an analogous procedure holds. The pump photon gets reflected at the dPBS first, then changes the polarization to $|H\rangle_p$ by crossing the dHWP@45° (of course it picks up a phase too). If down-conversion happens, the state after the non-linear crystal is $\sim |H\rangle_s |H\rangle_i$ and it is transmitted through the dPBS. So the state undergoes the following transition:

$$|V\rangle_p \rightarrow e^{i[\phi_p + k_p l_b + (k_s + k_i)l_a + \theta_p]} \eta_V E_V |H\rangle_s |H\rangle_i. \quad (3.3)$$

If we now choose the pump photon to be diagonally polarized, we have to assume a superposition of (3.2) and (3.3) in the output port of the dPBS. Therefore we can write the state as

$$|\Psi\rangle \propto |H\rangle_s |H\rangle_i + e^{i\delta} \gamma |V\rangle_s |V\rangle_i, \quad (3.4)$$

where we have used the fact that in free space it holds true that $k_p = k_s + k_i$ and the phase given by $\delta = \phi_p + \theta_p - \theta_i - \theta_s$. $\gamma = \frac{\eta_V E_V}{\eta_H E_H}$ can be set to 1 by changing the input pump ratio E_V/E_H and δ can be adjusted by the pump phase ϕ_p [33]. After that a dichroic mirror (DM) separates the state $|\Psi\rangle$ from the pump and $|\Psi\rangle$ is led to the dense wavelength division multiplexers (DWDMs).

3.4.2 Source

Source parameters

The most important parameter for designing a source is the so-called focus parameter

$$\xi = \frac{L}{2z_R}. \quad (3.5)$$

z_R is the Rayleigh range¹ of a Gaussian beam and L is the length of the crystal. The cases $\xi < 1$ correspond to weak focusing into the non-linear crystal, whereas $\xi > 1$ corresponds to strong focusing. Although strong focusing into the crystal leads to a high brightness (will be explained below in the text), the heralding (conditional probability that a detected photon on Alice's detector has a partner SPDC photon which got detected on Bob's detector, the heralding is calculated as the ratio between coincidence clicks and single clicks) becomes worse [20].

So in order to calculate the focus parameters, we set $\xi = 1$. Therefore we were able to determine z_R by rearranging equation (3.5). With Gaussian ray optics and the ABCD-matrix² formalism we calculated the needed focal lengths of the lenses for the source. The computed parameters are shown schematically in figure 3.5.

Another important parameter is the so-called brightness or pair-rate B . It is the amount of generated entangled pairs per mW pump power in the non-linear crystal [31]. The brightness is connected to the coincidences from entangled photon pairs in the following way

$$CC_{pairs} = B\eta_A\eta_B, \quad (3.6)$$

where $\eta_{A,B}$ is the transmittance³ in Alice and Bob's arm, respectively. Furthermore, the single counts from photons on Alice and Bob's side can be expressed as

$$S_{A,0} = B\eta_A, \quad S_{B,0} = B\eta_B \quad (3.7)$$

with the pair-rate B . Unfortunately, we only have access to the measured coincidences ($CC_{Max} = CC_{pairs} + \frac{1}{2}CC_{acc}$). However, since we are dealing with a dark count rate

¹Gaussian optics in appendix C

²See Appendix C

³The transmittance depends on the coupling efficiency and performance of the optical elements

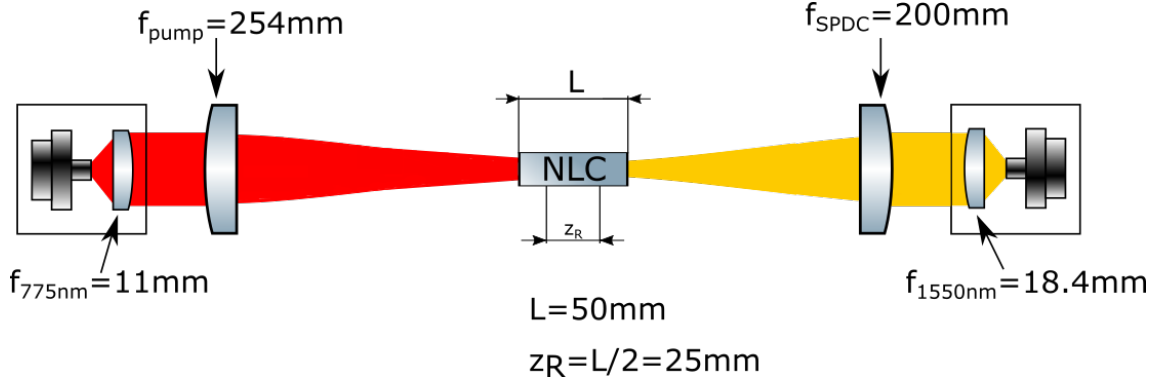


Figure 3.5: Here we see schematically how the source is built up with the relevant parameters. The fiber coupler with $f_{775 \text{ nm}}$ collimates the pump beam (indicated by red). Afterwards f_{pump} focuses inside the non-linear crystal. The resulting SPDC (yellow beam) is collimated with f_{SPDC} and coupled into a SMF with $f_{1550 \text{ nm}}$.

of ~ 350 Hz and low pump powers of the non-linear crystal, we can neglect CC_{acc} . Therefore the transmittance η_A and η_B are given by

$$\eta_A = \frac{CC_{\text{Max}}}{S_{B,0}} \quad (3.8)$$

$$\eta_B = \frac{CC_{\text{Max}}}{S_{A,0}}, \quad (3.9)$$

which gives an easy expression for the transmittance in Alice and Bob's channels. Later in section 5.2, we will come back to this, but also consider dark counts.

Closely connected to the brightness is the mean photon pair number per coincidence window μ :

$$\mu = B\tau_{CC} \quad (3.10)$$

Laser

We used a continuous wave (cw) laser from Optromix, with an operation wavelength of 775 nm. The laser emission was produced by second harmonic generation (SHG). Therefore additional short-pass filters were used to filter out the undesired low energy photons.

Setup

The setup in our laboratory is depicted in figure 3.6, with the beam propagation direction following the arrows in the figure. The pump beam with central wavelength of 775.06 nm is coupled out of a single-mode fiber (SMF) mounted to a Schäfter+Kirchhoff collimator with a focal length of $f = 11$ mm. (2) is a PBS coated for 775 nm, which transmits

only horizontally polarized photons. Together with (3), a HWP@ 22.5° (manufactured for 775 nm), we can set the state of the pump photons to $|D\rangle$. The mirror (4) is for directing the beam. (5) are posts for pinholes to align the pump beam. The lens (6) has a focal length of $f_{pump} = 254$ mm, is coated for 775 nm, and focuses the pump beam inside a 50 mm periodically poled lithium niobate (ppLN) type-0 non-linear crystal with a poling period $\Lambda = 19.36$ μm (12). The crystal inside the oven is depicted in figure 3.7. The Sagnac loop itself begins with a dual wavelength polarizing beam splitter (dPBS) (10). The dPBs works for the pump beam wavelength (775 nm) as well as for the SPDC wavelength (1550 nm). The same holds for the HWPs ((9a) and (9b)). The dichroic mirror (DM) (9) reflects 98.5% of the SPDC photons if it is mounted as in figure 3.6. The lens (13) is coated for 1550 nm and collimates the down-converted beam. It has a focal length of $f_{SPDC} = 200$ mm. With mirror (14) (coated for 1550 nm) and coupler (15) the SPDC is directed into a SMF with a fiber collimator from Schäfter+Kirchhoff ($f = 18.4$ mm). The ppLN crystal is held at constant temperature (operating temperature $T = 47.9^\circ C$) with an oven from Covesion Ltd. and their controller OC2 which comes with a PC control GUI. It has a specified thermal stability of $\pm 0.01^\circ$.

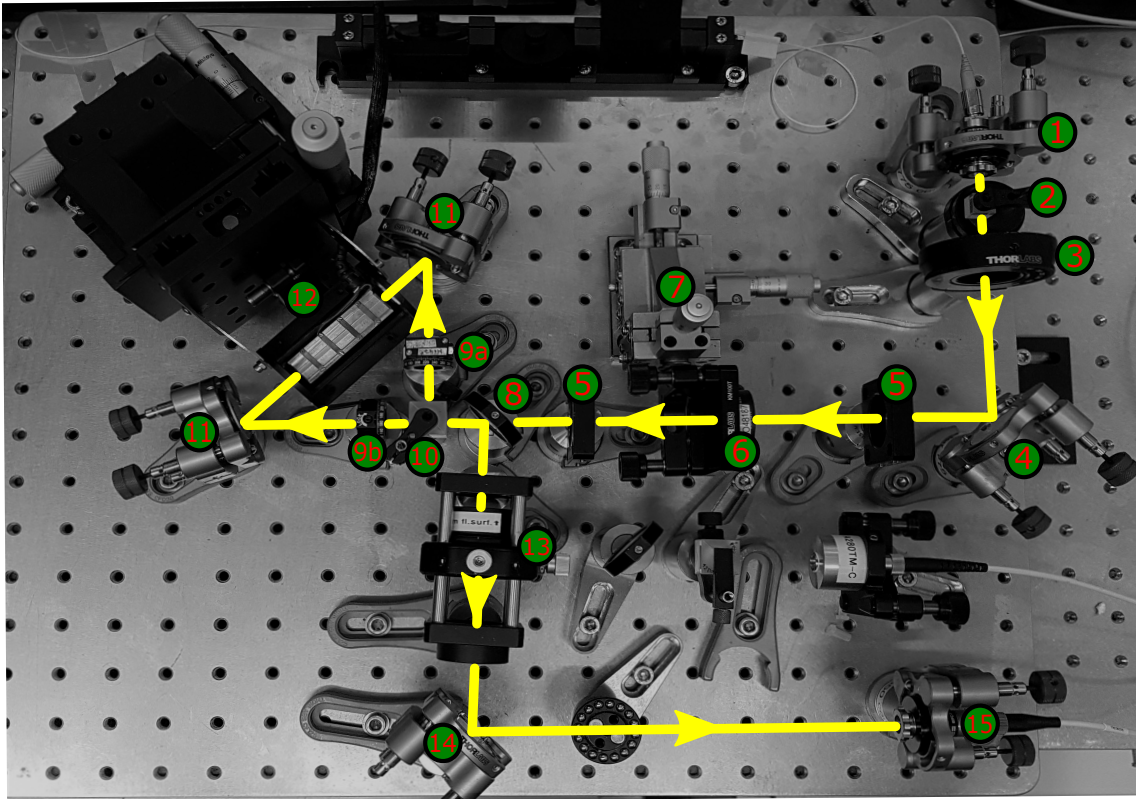


Figure 3.6: The pump beam enters the source at (1). With a PBS (2) and a HWP (3) we set the desired diagonal polarization state for the loop. (6) focuses the beam right in the center of the crystal, which is depicted here within the oven (12). With a dual wavelength PBS (dPBS) (10) we split up the beam, so that we have a clock-wise and a counter-clockwise propagating beam. The counter-clockwise propagating beam changes polarization due to the dHWP (9a). In this way the non-linear crystal is pumped from the clock- and counterclockwise direction with horizontal polarization. (9b) compensates the fact that the crystal is not mounted perfectly parallel to the dPBS but slightly rotated around the beam propagation axis. The SPDC is then separated from the pump beam by a dichroic mirror (DM) (8). The lens (13) collimates the SPDC. With mirror (14) and the fiber collimator mounted on coupler (15) the SPDC is coupled into a SMF, which leads it further to the DWDMs.

3.4.3 Alignment Procedure

The crucial part in aligning the Sagnac source is the loop. Only if the clockwise and counter-clockwise propagating beam are perfectly spatially overlapping, after a roundtrip in the loop, at the dPBS, they interfere with each other and therefore produce an entangled state. In order to do so, Fabian Steinlechner developed a scheme in the

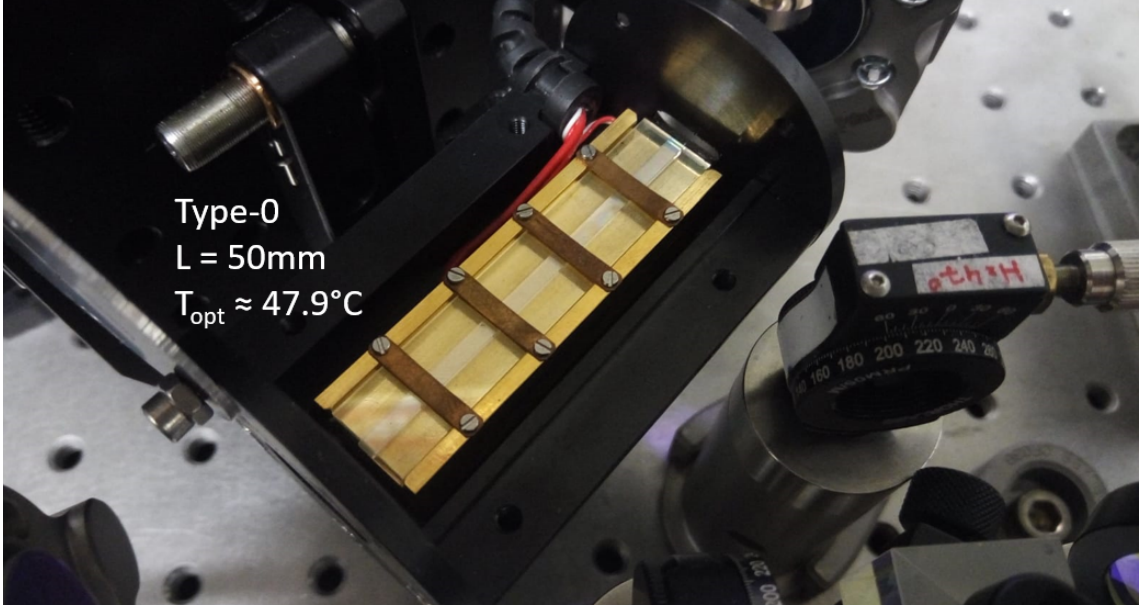


Figure 3.7: The type-0 collinear ppLN non-linear crystal which is used for the source. It is 50 mm long and the phase-matching condition is met at a temperature of $\sim 47.9^\circ\text{C}$. By now (Feb. 2020) this is the longest non-linear crystal ever used in this research group.

European Space Agency (ESA) funded Space EPS project which facilitated this procedure enormously. Sebastian Neumann, one of his former students, describes this scheme exhaustively in his master thesis [36], so that we will restrict ourselves to the basic functional principle.

Isolator Stage

The isolator stage has two functions in our setup. First, the stage helps us to align the Sagnac-loop, which will be explained in detail below. Second, it prevents that the beam which comes back from the loop enters the laser and creates a cavity, which causes power fluctuations.

A sketch of the isolator stage is shown in figure 3.8, where the most important device is the isolator. A beam coming from the laser is first coupled into a SMF and coiled through a polarization controller (PC) to set the polarization. It then enters the isolator stage through a collimator, which collimates the beam. The isolator itself consists of PBS1, a Faraday rotator (FR) and PBS2 which is rotated by 45° with respect to PBS1 (see figure 3.8). The rotated PBS has the effect that now diagonally polarized light is transmitted and anti-diagonally polarized light is reflected.

With the PC one can set the polarization of the beam to $|H\rangle$ so that maximal power is transmitted through PBS1. The FR then rotates the plane of polarization around 45° (regardless of the direction from where the beam comes from) to $|D\rangle$. The beam then gets fully transmitted through the rotated PBS2. Hence, the state after the isolator is

diagonally polarized. Since the pump beam was produced via second harmonic generation (SHG⁴), we placed three shortpass filters after the isolator to filter out the residual 1550 nm light. Afterwards the beam gets coupled into a SMF and is led through a PC to coupler (1) in figure 3.6. According to the analysis in [36], the pump beam returns to the isolator stage, after a round trip in the Sagnac loop of the source, with the same polarization as it left it, in our case diagonally polarized. Therefore the beam gets fully transmitted through PBS2 and the FR rotates the polarization to $|V\rangle$. In the end, PBS1 reflects the pump beam and its power can be measured.

In a perfect world, the power of the reflected light from PBS1 after a round trip in the loop would be the same as the initial power we were sending into the loop in the first place. However, since nothing is perfect, we only can maximize the output of the reflected light from PBS1 to about 50%. This gives us in the end a feedback of how well aligned the loop is.

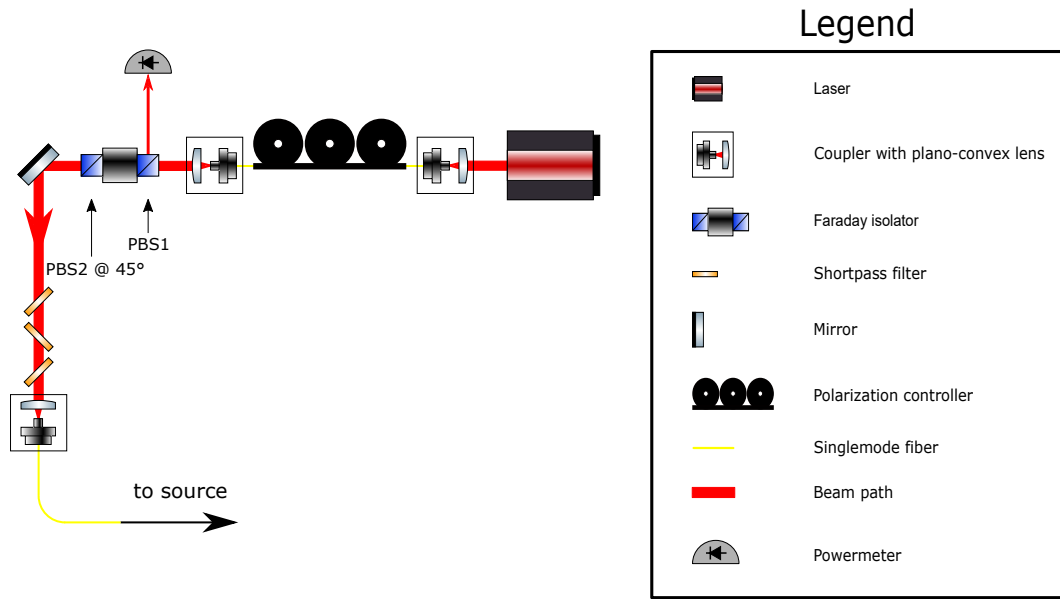


Figure 3.8: Sketch of the isolator stage for aligning the Sagnac loop. Note that PBS2 is rotated by 45° around the beam propagation axis with respect to PBS1.

⁴Two photons of lower energy convert to a high energy photon: $\omega_{1550} + \omega_{1550} \rightarrow \omega_{775}$, this process is the reverse process of down-conversion and much more efficient than it. This process is often called up-conversion.

Alignment of the Source

First we arranged all the components roughly on the breadboard as shown in figure 3.6. Here it is important to note that we placed the loop dPBS (10) and the PBS (2) in such a way that the beam hit them perpendicularly. This was done by back reflection as follows: We started by connecting an alignment laser with an wavelength of 650 nm to the SMF which connects coupler (1) to the isolator stage. Since the dPBS has an anti-reflection (AR) coating only for the wavelengths of 775 nm and 1550 nm, the dPBS reflects the 650 nm beam back. We used this fact to set the dPBS (10) right. This was done by punching a hole of the size of a needle into a sheet of paper and hold it directly in front of coupler (1). Due to the back-reflection from the dPBS we saw a spot on the paper which could be moved by arranging the dPBS (10). By adjusting the dPBS so that the back-reflection propagates back through the hole we made sure that the beam hits the dPBS roughly perpendicularly to the surface. In an analogous procedure we set the PBS (2).

It is also vital to mention that the DM (8) was set in such a manner that it showed the highest percentage of reflection for 1550 nm (98.5 %). This was in our case not at an 45° angle with respect to the incoming beam, but at roughly 50° .

In a first step we just wanted to align the loop with the pump beam. This was done initially without the crystal (12) and the pump beam lens (6). Therefore we first aligned the pump beam so that it hits the dPBS perpendicularly. In order to do so, we placed a $350\ \mu\text{m}$ and a $375\ \mu\text{m}$ pinhole in the designated posts (5) and maximized the output through both of them by tipping and tilting the coupler (1) and the mirror (4) only. Once this was done, we removed the pinholes and set the polarization of the pump beam with HWP (3) to diagonal, so that both directions of the loop were pumped equally. Then we poked a hole of the size of a needle in a piece of paper and placed it in front of (1) so that the pump beam went through the hole. What we were able to observe on the paper were two spots from the clockwise and counter-clockwise propagation of the pump beam in the loop. We walked the mirrors (11) until these two spots overlapped at the hole in the paper. Afterwards we removed the paper and we already observed an output at the isolator stage as discussed above in 3.4.3. Iteratively we first maximized the output at the isolator with the mirrors (11) and then changed the focus on coupler (1). By doing this, we improved the output at the isolator further until we reached a maximum.

Next we put the lens (6) into its place. Inserting the lens caused a beam displacement. However, with the translation stage (7) we were able to readjust the beam in such a way that we again observed an output at the isolator.

Now it was time to place the oven with the crystal (12) inside the loop. First we

made sure that the beam went straight through the crystal rather than being reflected inside the brass mounting of the crystal. Then we repeated the same procedure as before. First we tried to couple back to the isolator stage to see an output at the isolator and then we tried to maximize this output by alternatively utilizing all degrees of freedom at the mirrors (11), the lens (6) and the translation stage (7).

Once we reached a maximum at the isolator and could not improve it further we changed our alignment strategy. Because from now on we shone diagonally polarized 1550 nm laser light from coupler (15) back into the source. The reason for that was, that from now on we utilized second harmonic generation (SHG) to align the loop from the other direction. With coupler (15) and mirror (14) only, we were able to align the loop from the back so that we could measure the SHG light of 775 nm after the Sagnac loop with a powermeter. If the clock- and counter-clockwise propagated SHG light is perfectly overlapping inside the loop, the state after the dPBS is diagonal due to the interference of the $|H\rangle$ and $|V\rangle$ beams. In order to check this hypothesis, we placed a polarizer, set to $|D\rangle$ ($|A\rangle$), in the SHG beam path after the loop and we measured a maximum (minimum) with the powermeter. The ratio of these two values is therefore a measure of how good the loop is aligned. We were able to improve this ratio with the loop mirrors (11). In the end we reached a ratio of $\sim 1:100$.

We then removed the polarizer and coupled the up-converted light into coupler (1), where we used only coupler (15), mirror (14) and lens (13). Since the up-converted light has the same polarization as the light from the pump beam, we again aimed to maximize the output at PBS1 at the isolator.

Let us summarize the proceeding. First we aligned the loop without crystal and pump lens by measuring the returned light reflected by the isolator. After that we placed the lens and the crystal into the right position and did the same again. Subsequently, we made use of SHG as we shone light backwards through the loop to generate 775 nm light and then coupled this back to the isolator and measured the output.

3.4.4 Dense Wavelength Division Multiplexing

In telecommunication networks, different wavelengths are used to transport independent signals of information through glass-fibers from point A to B [37, 38]. To combine, and later separate, each signal, one uses wavelength division multiplexers (WDM). In principle there are two different WDM systems which differ by the spacing between the wavelengths, also called channels:

- Coarse WDM with a channel spacing of 20 nm
- Dense WDM with a channel spacing of 0.8 nm

However, in telecommunication WDMs are defined in the frequency domain. Dense WDMs (DWDM) operate on 73 different channels on an optical frequency grid between 190.1 THz to 197.3 THz with a 100 GHz spacing between each channel. These values are normed by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T). Due to these definitions from the ITU-T we produced our SPDC spectrum centered at 1550.12 nm. Therefore we had to pump the non-linear crystal with a wavelength of 775.06 nm, see section 2.5.

The multiplexing inside the used DWDMs is achieved with dielectric thin-film filters. A thin-film filter has many alternating dielectric layers of high and low refractive indices with quarter- or half-wavelength thickness [38]. This arrangement of different layers exploits thin-film interference. Therefore it is possible to manufacture a device which is highly transmittive in a small wavelength range.

The source we built produces a degenerate wavelength SPDC-spectrum, where signal and idler photon propagate collinearly. In order to spatially separate them, we used DWDMs (see figure 3.10) with a 100 GHz grid, which corresponds to a channel spacing in the wavelength domain of 0.8 nm. With this narrow spectrum of 0.8 nm after the DWDMs, we reduced detrimental dispersion effects.

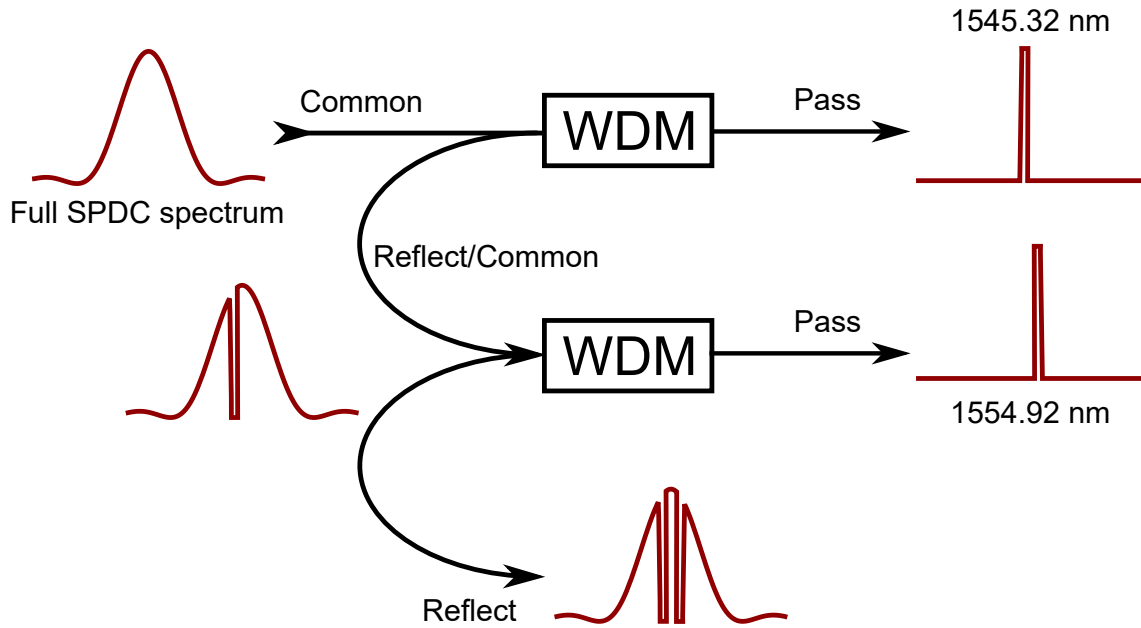


Figure 3.9: SPDC spectrum before and after two DWDMs. Here we see how two narrow bands are cut out from the full spectrum symmetrically from the center wavelength of 1550.12 nm.

We connected two DWDMs as shown in figure 3.9. The DWDMs are chosen so that they cut out two spectral slices symmetrically around the SPDC peak of 1550.12 nm, in

our case 1545.32 nm and 1554.92 nm. So they still fulfill energy conservation

$$\omega_{775.06nm} = \omega_{1545.32nm} + \omega_{1554.92nm}. \quad (3.11)$$

Through the COMMON port the whole SPDC spectrum enters the first DWDM, where a spectral slice centered at 1545.32 nm gets cut out. This slice is led via the PASS port to the receiver module on Alice's side. The rest of the spectrum is reflected and guided to the second DWDM, which cuts out a slice at 1554.92 nm and leads it then to the receiver module at Bob's side. The whole process is seen in figure 3.9. The spectrum after the second reflection is not used anymore, but in principle one could again use two symmetrical DWDMs around 1550.12 nm to split up the spectrum further.

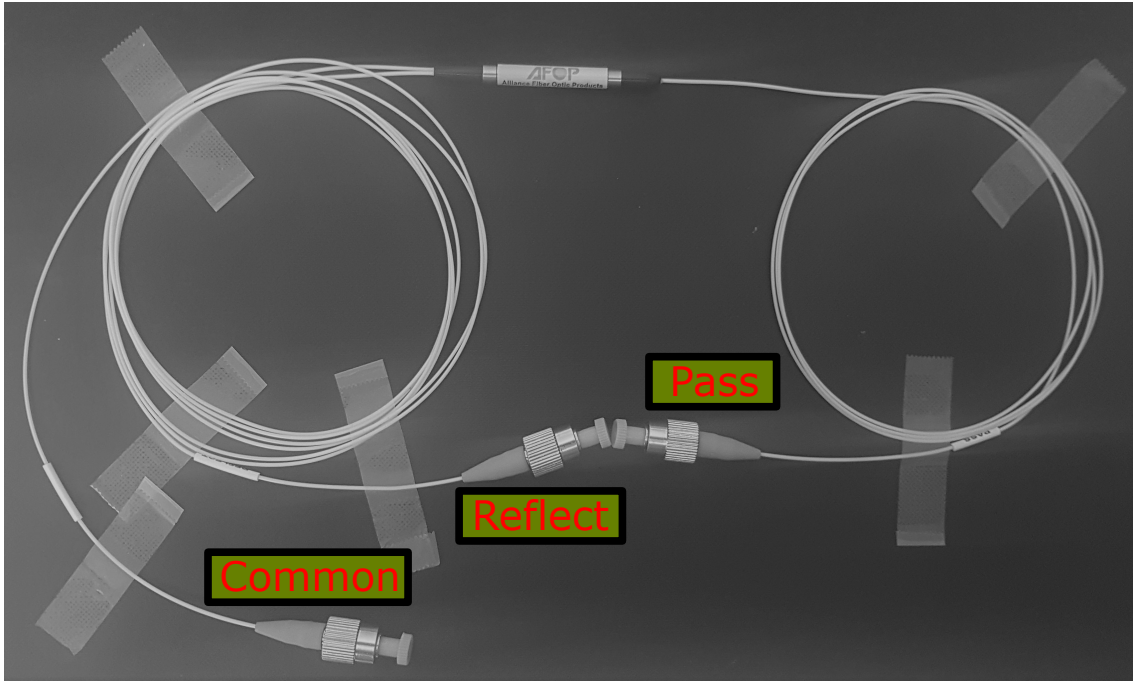


Figure 3.10: One of the used DWDMs. The common-port acts as the input, whereas the pass-port guides the filtered spectrum of the SPDC. The rest of the spectrum is reflected into the reflect-port. The actual DWDM is realised as a multi-layer dielectric thin-film filter.

Figure 3.11 shows the transmission profile of the DWDMs we used. For the graphs we first measured the power output of a laser which has a tunable wavelength range between 1520 nm up to 1570 nm. Afterwards we connected this laser to the COMMON port of the DWDM and the PASS port of the DWDM to a powermeter. As we changed

the wavelength, we measured the power output and normalized it with the initial output before.

3.11a depicts the profile for the 1545.32 nm DWDM (channel 40 of the frequency grid from ITU-T). It exhibits $\sim 85\%$ transmission with a full width at half maximum (FWHM) of ~ 0.62 nm. **3.11b** (DWDM for 1554.92 nm, channel 28 of the frequency grid from ITU-T) shows a slightly higher transmittivity ($\sim 90\%$) at a FWHM of ~ 0.61 nm. Both DWDMs have a smaller channel spacing than the expected 0.8 nm.

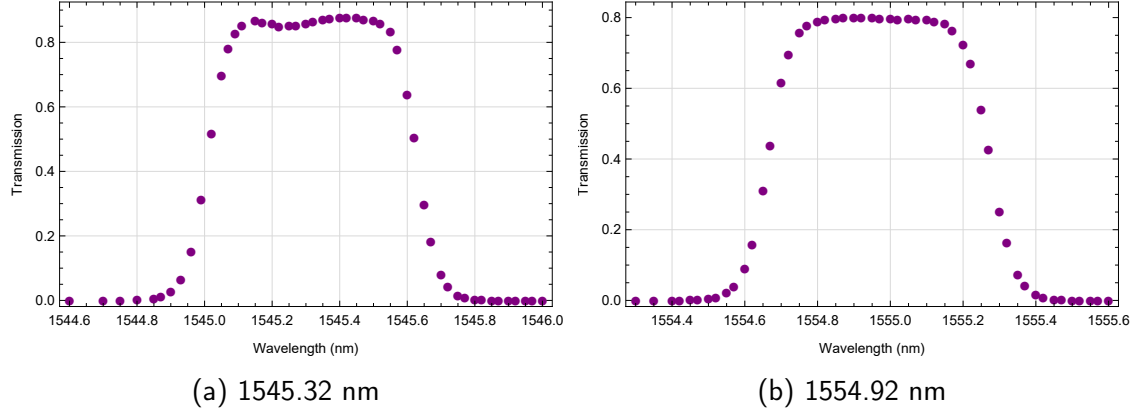


Figure 3.11: Measured transmission profiles of the used DWDMs. One can see the bandwidth where they are transmissive. (a) FWHM ~ 0.62 nm, (b) FWHM ~ 0.61 nm.

3.4.5 Setting a Bell State

If we assume that the non-linear crystal is pumped equally from both sides in the Sagnac-loop, we can set $\gamma = 1$ in (3.4). This leaves us with an unknown phase δ , which can be adjusted with HWP ③ in figure 3.6. We can for example pump the crystal with $|H\rangle_p - |V\rangle_p$, where we chose $\delta = \pi$. On the other hand we can choose $\delta = 0$ and pump the crystal with $|H\rangle_p + |V\rangle_p$.

The following treatment shows that we can set any Bell state by applying a unitary transformation $\hat{U}$ without loss of generality on the idler photon only.

$$\hat{D} = \mathbb{I}_{2 \times 2, s} \otimes \hat{U}_i \rightarrow \frac{1}{\sqrt{2}} (|H\rangle_s \hat{U}_i |H\rangle_i + e^{i\delta} |V\rangle_s \hat{U}_i |V\rangle_i), \quad (3.12)$$

where $\mathbb{I}_{2 \times 2, s}$ is the two dimensional unity matrix. The unitary $\hat{U}_i$ is a rotation on the Poincaré sphere, and can be written as follows

$$\hat{U}_i = e^{-i\vec{\alpha} \cdot \vec{\sigma}/2} = \cos\left(\frac{|\vec{\alpha}|}{2}\right) \mathbb{I}_{2 \times 2} - i \sin\left(\frac{|\vec{\alpha}|}{2}\right) \vec{n} \cdot \vec{\sigma}, \quad (3.13)$$

where $\vec{\alpha} \in \mathbb{R}^3$ and $|\vec{\alpha}|$ is the angle of the rotation and $\vec{n} = \frac{\vec{\alpha}}{|\vec{\alpha}|}$ is the rotation axis. $\vec{\alpha} \cdot \vec{\sigma} = \alpha_1 \sigma_1 + \alpha_2 \sigma_2 + \alpha_3 \sigma_3$ indicates a symbolic scalar product of $\vec{\alpha}$ with the Pauli

matrices⁵ $\sigma_{1,2,3}$.

Let us discuss for simplicity the case where we rotate around an angle $|\vec{\alpha}| = \pi$, so $\hat{U}_i$ reduces to $\hat{U}_i = -i\vec{n} \cdot \vec{\sigma}$, around the three axes which correspond to H/V, D/A and R/L on the Poincaré sphere.

H/V axis

In order to rotate around the H/V axis, $\vec{n}$ is given by $\vec{n} = (1, 0, 0)$ and therefore $\hat{U}_i = -i\sigma_1$. Inserting $\hat{U}_i$ into equation (3.12), we arrive at the following state

$$\hat{D} = \mathbb{I}_{2x2,s} \otimes -i\sigma_1 \rightarrow \frac{e^{-i3\pi/2}}{\sqrt{2}}(|H\rangle_s |V\rangle_i + e^{i\delta} |V\rangle_s |H\rangle_i). \quad (3.14)$$

We see that we can set (up to a global phase) either $|\Psi^+\rangle$ or $|\Psi^-\rangle$ by setting the phase δ .

D/A axis

In this case we rotate around the D/A axis. $\vec{n}$ is now given by $\vec{n} = (0, 1, 0)$ and $\hat{U}_i = -i\sigma_2$. Inserting $\hat{U}_i$ into (3.12) results in the state

$$\hat{D} = \mathbb{I}_{2x2} \otimes -i\sigma_2 \rightarrow \frac{1}{\sqrt{2}}(|H\rangle_s |V\rangle_i - e^{i\delta} |V\rangle_s |H\rangle_i). \quad (3.15)$$

By setting the phase δ we can set the state to $|\Psi^+\rangle$ or $|\Psi^-\rangle$.

R/L axis

Here we rotate around the R/L axis. The rotation axis is $\vec{n} = (0, 0, 1)$ and $\hat{U}_i = -i\sigma_3$. In the end we obtain the following state

$$\hat{D} = \mathbb{I}_{2x2} \otimes -i\sigma_3 \rightarrow \frac{e^{-i3\pi/2}}{\sqrt{2}}(|H\rangle_s |H\rangle_i - e^{i\delta} |V\rangle_s |V\rangle_i) \quad (3.16)$$

and again by setting the phase δ we obtain either $|\Phi^+\rangle$ or $|\Phi^-\rangle$, up to a global phase.

3.4.6 Results

To verify the quality of the polarization-entangled state which the Sagnac source produces we performed a visibility measurement.

5

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

But before the measurement, we had to compensate the transformation the fiber induced to the state from the source. This was done with a polarization controller (PC) on the fiber of the idler photon. Because the polarization of light inside a fiber is highly dependent on mechanical pressure on the fiber, we can use a PC to squeeze and stress the fiber and manipulate the polarization in that way. Therefore we can use a PC to set any polarization state on the Poincaré sphere. So we see that the PC acts as the unitary $\hat{U}$ from section 3.4.5.

Figure 3.13 shows a visibility measurement between the H/V basis and the D/A basis. The measurement configuration is depicted in figure 3.12. On Bob's side we placed a motorized HWP and incremented its angle in 3° steps, integrating over ten seconds for each data point. The probability to detect a coincidence count now depends on the angle of the HWP and is given by [39]:

$$|\langle \Phi^+ | \mathbb{I}_{2 \times 2} \otimes HWP_B(\theta) | H \rangle_A | H \rangle_B|^2 = \frac{1}{2} \cos^2(\theta) \quad (3.17)$$

$$|\langle \Phi^+ | \mathbb{I}_{2 \times 2} \otimes HWP_B(\theta) | H \rangle_A | V \rangle_B|^2 = \frac{1}{2} \sin^2(\theta) \quad (3.18)$$

$$|\langle \Phi^+ | \mathbb{I}_{2 \times 2} \otimes HWP_B(\theta) | V \rangle_A | H \rangle_B|^2 = \frac{1}{2} \sin^2(\theta) \quad (3.19)$$

$$|\langle \Phi^+ | \mathbb{I}_{2 \times 2} \otimes HWP_B(\theta) | V \rangle_A | V \rangle_B|^2 = \frac{1}{2} \cos^2(\theta) \quad (3.20)$$

We obtained a visibility in the D/A basis of

$$\mathcal{V}_{D/A} = (97.87 \pm 0.17)\% \quad (3.21)$$

and in the H/V basis of

$$\mathcal{V}_{H/V} = (99.09 \pm 0.12)\%, \quad (3.22)$$

where we did not correct for accidental counts. The different count rates are due to different coupling efficiencies into SMF and the slightly different detector efficiencies.

Using Gaussian error propagation and assuming Poissonian photon statistics, one can derive the following formula for the error of the visibility $\mathcal{V}$

$$\Delta \mathcal{V} = \frac{2}{(R_{ii} + R_{jj} + R_{ij} + R_{ji})^2} \times \sqrt{(R_{ij} + R_{ji})^2 (\Delta R_{ii}^2 + \Delta R_{jj}^2) + (R_{ii} + R_{jj})^2 (\Delta R_{ij}^2 + \Delta R_{ji}^2)} \quad (3.23)$$

The solid lines in figure (3.13) were fitted according to the equations (3.17)-(3.20).

If we use the entanglement witness⁶

$$\mathcal{W} = \frac{1}{4}(1 - \mathcal{V}_{H/V} - \mathcal{V}_{D/A} - \mathcal{V}_{R/L}) \quad (3.24)$$

from [40, 41] and assuming the worst case, where $\mathcal{V}_{R/L} = 0$, since we have not measured it, we get the following value of $\mathcal{W}$

$$\mathcal{W} = -0.2424 \pm 0.0005, \quad (3.25)$$

which shows clearly a negative value. So with $\mathcal{W}$ we double checked that the produced state from the source is indeed entangled, even if we only measure in two bases.

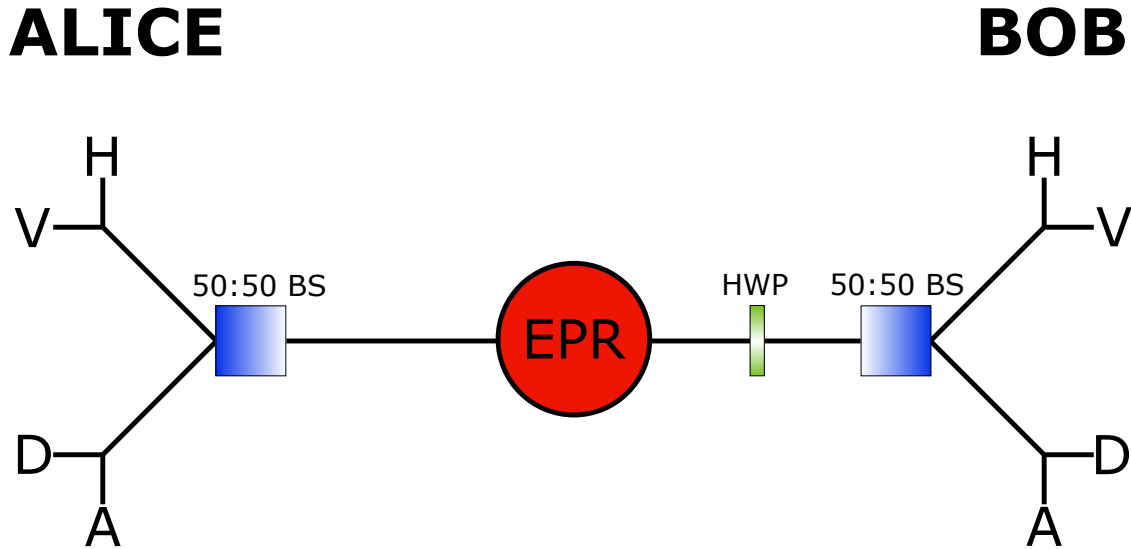


Figure 3.12: Measurement configuration for a visibility measurement. EPR is an abbreviation for Einstein-Podolsky-Rosen and is simply the entangled photon source. Both Alice and Bob can measure in two different bases H/V and D/A.

⁶An entanglement witness is a constructed Hermitian operator, which guarantees entanglement if $\text{Tr}[\mathcal{W}\rho] < 0$ for a given quantum state ρ , see [40]

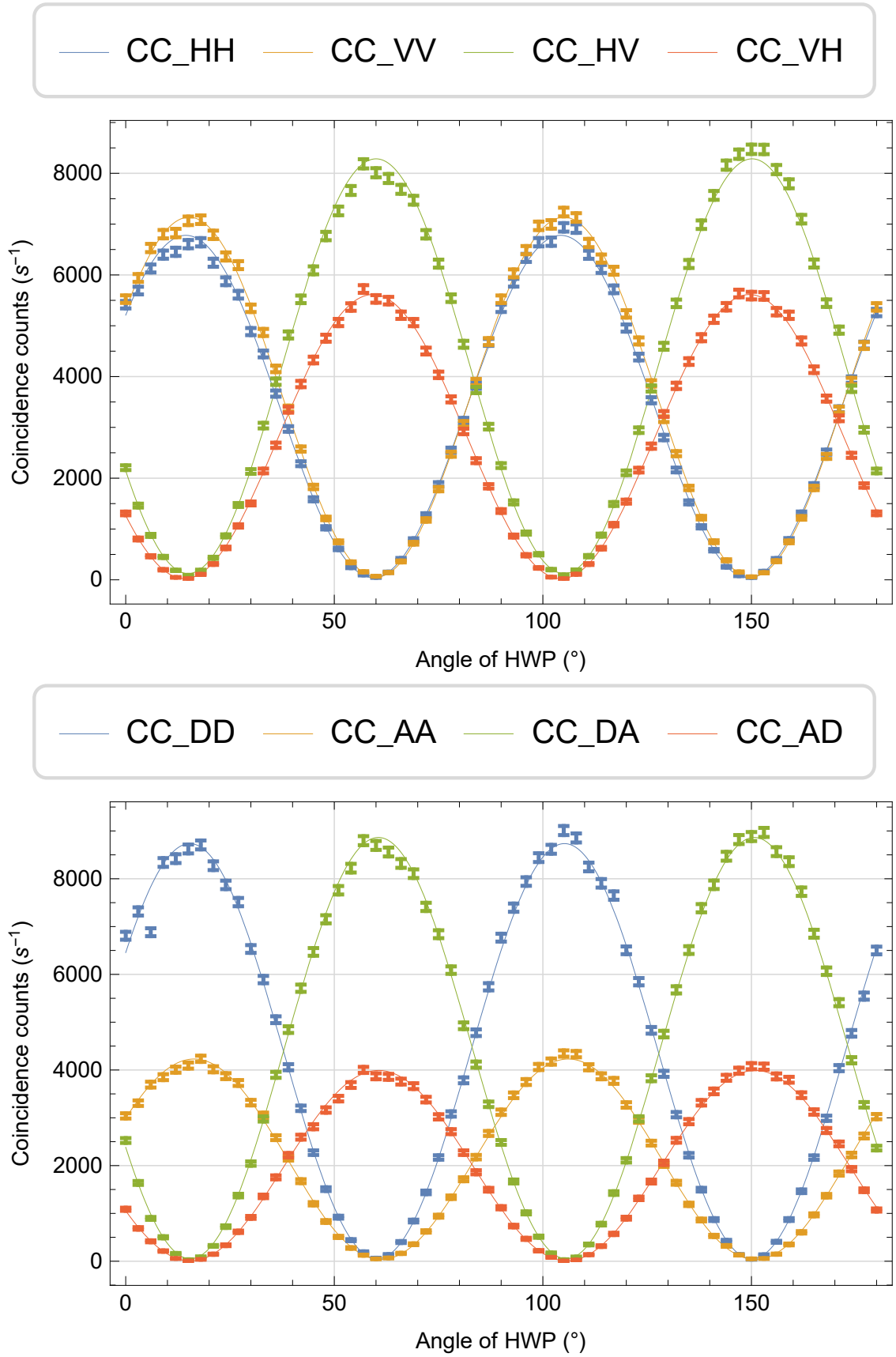


Figure 3.13: Visibility in $H/V = 99.09\%$ and $D/A = 97.87\%$. The angle of the HWP was incremented in 3° steps and we integrated over ten seconds for each data point. The solid lines are fitted curves to the data points.

CHAPTER 4

POLARIZATION ANALYSIS OF SINGLE PHOTONS

Until now we only discussed how to produce a polarization-entangled state with a Sagnac source. However, to investigate the properties of our entangled state produced, we have to perform a measurement on that state. Hence, this chapter serves as an introduction on how we can measure single photons.

First we discuss the detection module¹ from section 2.8 in more detail. Such a detection module allows us to distinguish between two mutually unbiased bases, which is necessary for an entanglement based QKD protocol. Each of these modules has four channels, which lead the photons to our superconducting nanowire single photon detectors (SNSPD), which produce an electric signal with a certain probability each time a photon hits the detector. After that we investigate the so-called time tagging module (TTM). A TTM assigns each detection event on the SNSPDs a precise time stamp. With these stamps we are able to correlate different channels with each other.

4.1 Detection Module for Polarization Entangled Photons

The working principle of a detection module was already discussed in section 2.8. With the detection modules we built, we were able to measure the polarization of an incoming photon in the two linear polarization bases H/V and D/A. One of the two detection modules is depicted in figure 4.1. All the optical elements were manufactured in such a manner that they work around our operating wavelength of 1550 nm.

¹In lab-slang often called Bob module, although Alice also needs one for a QKD protocol. This comes from the fact that in early prepare-and-send QKD protocols, Alice was always the sender and Bob the receiver.

4.1.1 Alignment Procedure

The alignment was done with a laser operating with a wavelength of 1550 nm and an output of 10 mW, which we from now on call telecom laser. We started to place all the required components on the breadboard. We payed attention to the fact that we could place one additional optical element between coupler ① and BS ② as well as after each PBS ③. We made sure that the laser beam propagates parallel to the long side of the breadboard and hits every element roughly in the center. In this way we checked that all the elements are on the same height. Since the HWP did not need to be aligned in a special way, we removed it during the alignment procedure and placed it back to the right position in the end. This caused no troubles regarding beam displacement.

Alignment of the 50:50 BS

The 50:50 BS ② in figure 4.1 was aligned with the back reflection procedure we discussed for aligning the dPBS at the Sagnac source in section 3.4.3.

Alignment of the two PBS

The alignment of the two PBS ③ is done in the same way.

The telecom laser we used to align the receiver module enters the module via a SMF, which is coiled through a PC to set the polarization state of the photons. The SMF is connected to a fiber collimator with an aspheric lens and a fixed focus of $f = 8.17$ mm mounted at coupler ①. In order to align PBS ③ we placed a reference PBS between the 50:50 BS ② and the fixed PBS ③. In the reflected arm of the reference PBS we placed a powermeter sensor for 1550 nm and minimized the power output by moving the paddles of the PC. As soon as we reached a minimum, we knew that the light-beam which came into the receiver module was horizontally polarized with respect to the reference PBS. Now we placed the sensor of the powermeter in the reflected arm of the fixed PBS ③. By adjusting PBS ③ we were able to minimize the output at the reflected arm further. After we reached a minimum, we concluded that the PBS was aligned in the right way and we removed the reference PBS.

Single Mode Fiber coupling

The last alignment step was to couple the four beams after the PBSs ③ into the SMFs, which are connected to fiber collimators with a focal length of $f = 8$ mm, mounted at couplers ⑥. Therefore we shone with a telecom test laser from coupler ① into the receiver module and with a hand-sized alignment laser (wavelength $\lambda = 690$ nm) from coupler ⑥ back into the module. When we placed a laser viewing card at some point between coupler ① and coupler ⑥ we saw two spots, one from the telecom laser and one from the alignment laser. By walking the beam with mirror ⑤ and coupler ⑥ we

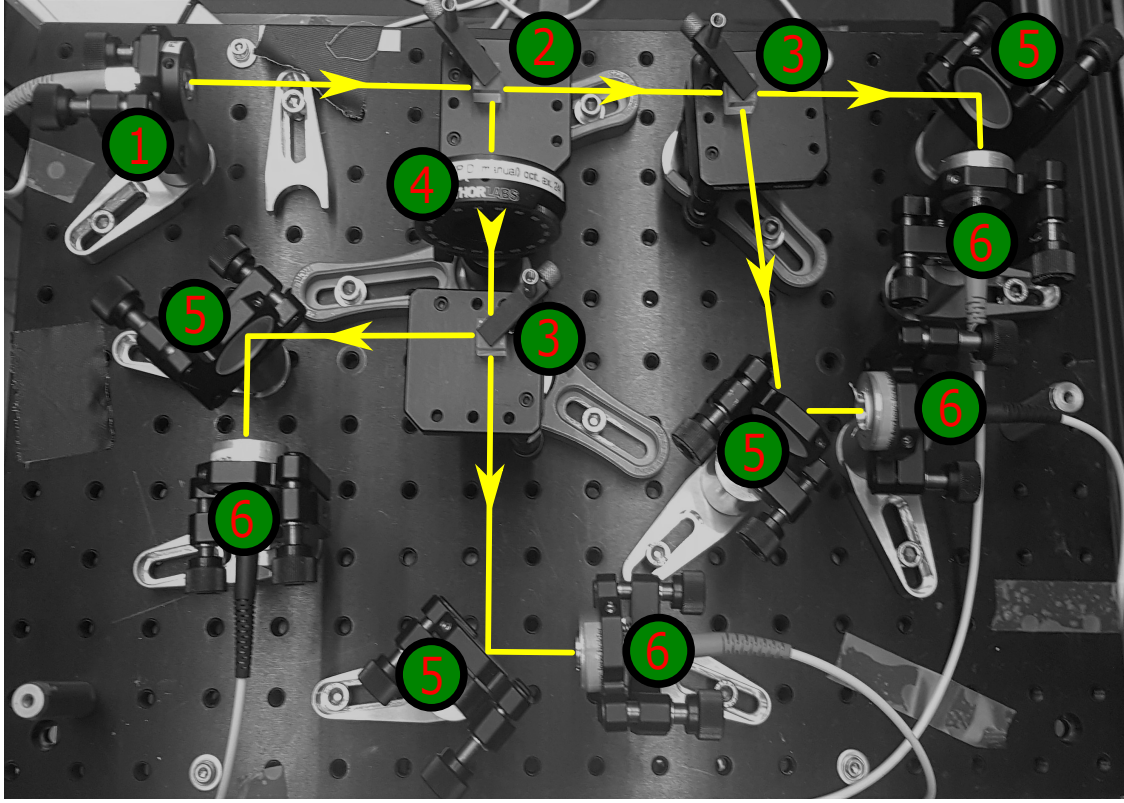


Figure 4.1: A free-space receiver module, built from scratch which was used for the experiments in this thesis. The signal/idler photon enters the detection-module through a SMF, which is connected to a fiber collimator, at coupler (1). A 50:50 BS (2) acts as a passive random basis choice. (3) are a PBS. Depending on the photon's polarization, the photon is either transmitted or reflected. As it can be seen, the best position for the PBS is slightly tilted. This is because in this position, the PBS shows the highest extinction ratio. HWP (4) is rotated by 22.5° around the optical axis, to rotate the polarization of the photons so that the basis of the reflected arm of the 50:50 BS is unbiased with respect to the basis of the transmitted arm. With the mirrors (5) we can couple the photons into the SMF, which is connected to a fiber collimator mounted on coupler (6).

were able to make these two spots overlap over the whole distance. When we reached this point, we exchanged the alignment laser with a powermeter sensor and measured the output power, because after this rough alignment a low signal was already visible. In an iterative procedure we alternated between a focus change of the fiber collimator at coupler (6) and a beam walking process with mirror (5) and coupler (6) in order to reach a maximum output value compared to the input value right in front of coupler (6). Due to the used FC/PC fiber which was connected to the powermeter, the beam got reflected back from the sensor into the fiber, which caused a fluctuation of the measured output power. This resulted in an uncertainty in the coupling efficiency, as seen in table

4.1.

After that we put the HWP back in its place.

Table 4.1 shows the measured data from the two detection modules. The most important value here is the extinction ratio R_x . It was measured as follows:

We set the polarization state of the incoming beam from the telecom laser to $|H\rangle$ by minimizing the output power at the reflected arm ($|V\rangle$ -arm) of the PBS ③ as low as possible. After that we measured the output at the transmitted arm ($|H\rangle$ -arm) between PBS ③ and mirror ⑤. The extinction ratio is then given by

$$R_x = \frac{\text{Power of maximized reflected arm}}{\text{Power of minimized transmitted arm}} \quad (4.1)$$

And it simply says that one out of R_x photon passes through the wrong port of the PBS ③. This gives us a number on how good the PBS distinguishes between polarization states. The extinction ratio contributes directly to the overall $QBER$ of a quantum key distribution protocol (see section 5.3).

Another important parameter is the coupling efficiency. It is defined as the ratio between the power output after the SMF connected to coupler ⑥ and the power right before coupler ⑥.

Alice		
	Trans. Arm	Ref. Arm
50:50 BS	42 %	46 %
	Coupling efficiency	
$ H\rangle$	78% - 86%	
$ V\rangle$	76% - 85%	
$ D\rangle$	76% - 88%	
$ A\rangle$	77% - 82%	
	Extinction ratio	
$ H\rangle$	1:45	
$ V\rangle$	1:4750	
$ D\rangle$	1:183	
$ A\rangle$	1:3100	

Bob		
	Trans. Arm	Ref. Arm
50:50 BS	45 %	40 %
	Coupling efficiency	
$ H\rangle$	75% - 79%	
$ V\rangle$	78% - 85%	
$ D\rangle$	79% - 84%	
$ A\rangle$	76% - 80%	
	Extinction ratio	
$ H\rangle$	1:1800	
$ V\rangle$	1:3500	
$ D\rangle$	1:3300	
$ A\rangle$	1:6000	

Table 4.1: Specification data measured for two receiver modules using a telecom laser with a power output of 10 mW. The range in the coupling efficiency is due to fluctuations of the power output, caused by the used FC/PC fiber.

4.2 Superconduction Nanowire Single Photon Detectors (SNSPD)

The requirements for a single photon detector are very high. We want a high detection efficiency η_{det} , meaning a photon which impings the detector gets detected with a probability η_{det} , a low dark count rate (intrinsic counts at the detector which originate from thermal photons), at best no dead-time (time the detector needs to recover after it detected a photon, in the dead-time the detector will not register a photon), a low timing-jitter and a wide operating range in terms of wavelength.

Single photon avalanche photodiodes (SPADs) are used commonly in today's optics laboratories. There are two semiconducting materials that are frequently used: Silicon (Si) and indium gallium arsenide (InGaAs).

Silicon SPADs do not have the desired sensitivity for 1550 nm since photons with a wavelength of 1550 nm have not enough energy to excite electrons above the bandgap of Si (1.1eV) [42], so they are not suitable for our needs. The alternative is a InGaAs SPAD where e.g. IDQ offers with the ID230 a InGaAs SPAD for a wavelength detection range between 900 nm - 1700 nm, a detection efficiency $\eta_{det} = 10\%$ and a dark count rate of < 50 Hz. [43].

To detect quantum mechanical effects in more depth, a new kind of detector was developed which uses superconductive nanowires to detect single photons. SNSPDs were first demonstrated in 2001 by Gol'tsman et al. in [44]. Since then, the detection efficiency has increased further. Commercially available setups already have an efficiency of $\sim 80\%$. The highest reported efficiencies so far are 93% [45] and 95% [46].

A comprehensive table of different single-photon detectors and their performance is given in [47].

Our SNSPD setup from Single Quantum exhibits a detection efficiency of roughly $\eta_{det} \sim 80\%$ and a maximum dark count rate of ~ 350 Hz. They have a dead time of ~ 30 ns and a short timing-jitter of ~ 22 ps. However, SNSPDs have a huge disadvantage. The nanowire inside the SNSPDs is enclosed by a vacuum of $\sim 10^{-6}$ mbar. Therefore a vacuum pump is needed, also the nanowire is only superconducting if it is cooled down to a temperature of ~ 2.6 K. Hence, we need a cryogenic system too.

The key component of a SNSPD is the already mentioned nanowire, depicted in figure 4.2a. The wire has a radius of $5 \mu\text{m}$. Common materials for the nanowire are NbN and NbTiN [48]. The spiraling geometry exhibits a reduced polarization dependency for the detection efficiency [48]. Each input channel of the cryostat of the SNSPD (see figure 4.2b, the yellow fibers connected to the cryostat) has its own nanowire.

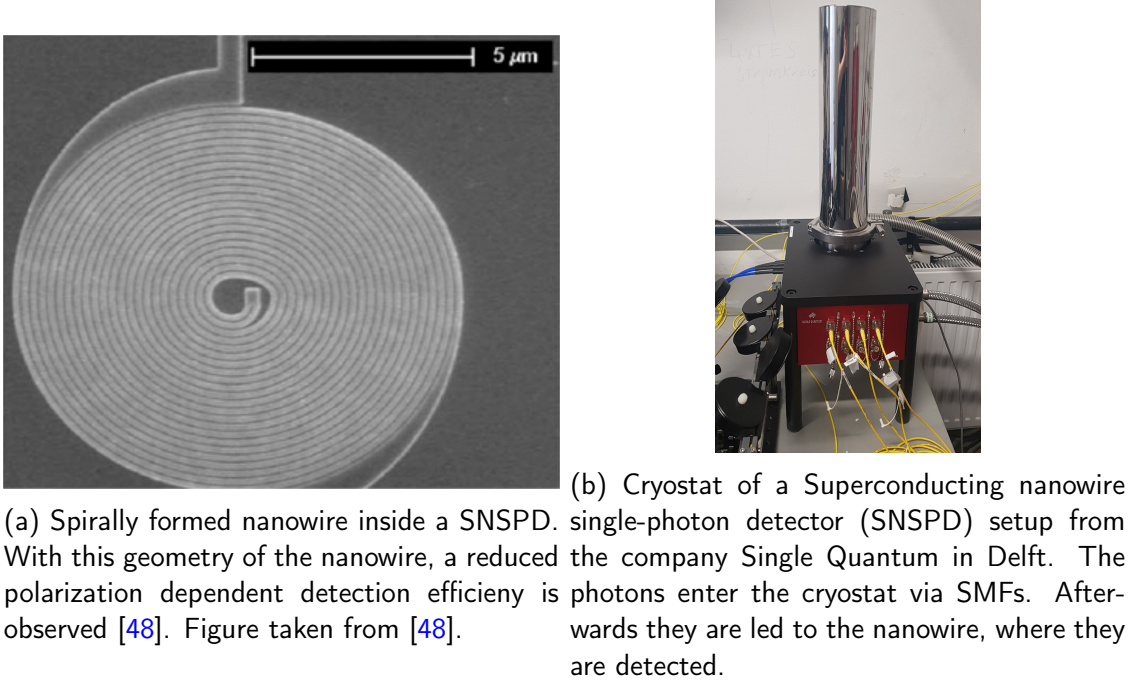


Figure 4.2: The nanowire (a) inside a cryostat (b) of a SNSPD setup.

Operation Process

The operational principle of a SNSPD can be described in a cyclic process as shown in figure 4.3, where the following is based on [49]:

- (i) If the nanowire is below a critical temperature T_C and the bias current below a critical current I_C , the nanowire is superconducting².
- (ii) If now a photon hits the nanowire, it has enough energy to break apart hundreds of Cooper pairs³ at the impact place. This is then called a hot spot.
- (iii) At such a hot spot, the resistance is much higher. This leads the current to flow around the hot-spot where it is "squeezed" and the current density raises above I_C .
- (iv) This results in a complete breakdown of the superconductivity through the whole wire. Subsequently, this produces a measurable voltage pulse.
- (v) Due to the sudden resistance, the nanowire heats up more strongly and the resistive region grows to the point where no current flows anymore. After this point is reached, the resistance fades, so that the wire becomes superconducting again.

²Superconducting means that for specific materials there is no electrical resistance below a certain temperature

³Due to superconductivity, electrons connect pairwise with each other, which is called Cooper pair.

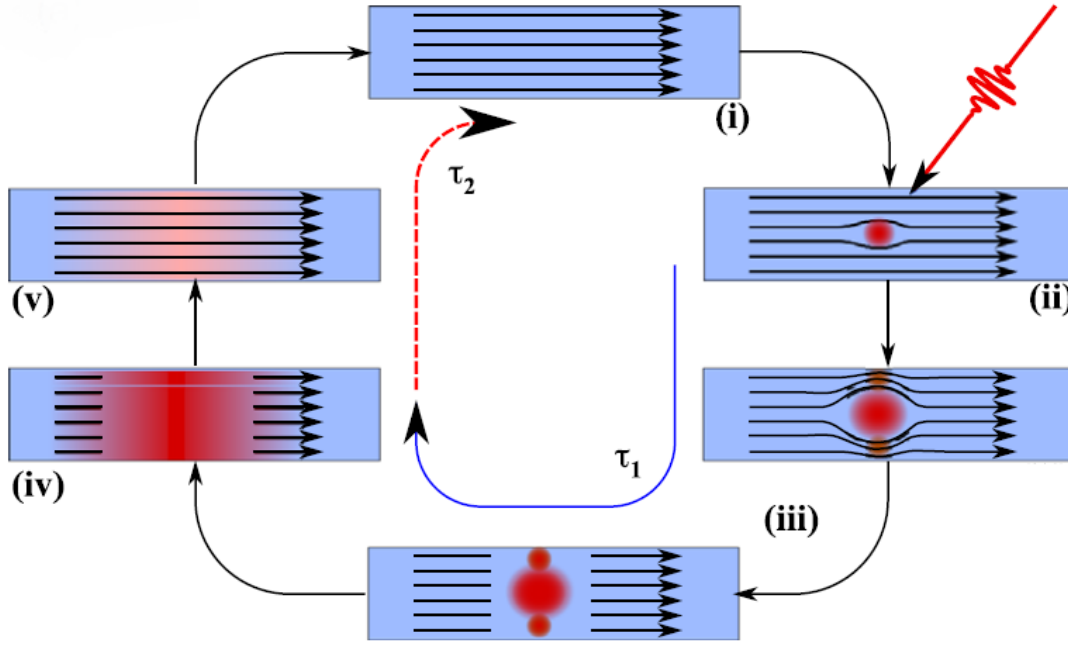


Figure 4.3: The cyclic operation process of a SNSPD to detect single photons. For the description we refer to the main text. Picture modified and taken from [49].

Figure 4.4 shows the detection setup with the two cryostats, containing the superconducting nanowires, from the company Single Quantum together with the two detection modules and the polarization controllers to maximize the count rate, since the detection efficiency of the SNSPDs is polarization dependent.

4.3 Time Tagging Module (TTM)

The last part in our detection system is the time tagging module depicted in figure 4.5. It simply stores for each click on the SNSPD a data block of 16 bytes (called tag) which specifies the channel where it clicked and a time stamp when it clicked. Our TTM from Swabian instruments model *TimeTaggerUltra* has 8 input channels and is capable of streaming 65 M tags per second via USB 3.0 to a computer. It exhibits a timing jitter τ_{TTM} of $\tau_{TTM} \approx 11$ ps. It can also be locked to an external clock with a frequency of 10 MHz.

We use the time stamps from the TTM to correlate different channels with each other. Since the paths from the source to the nanowires have in general different lengths and also the electronics in the SNSPDs and TTM operate with different speeds, the channels show a time delay between them, which has to be corrected in order to gain a

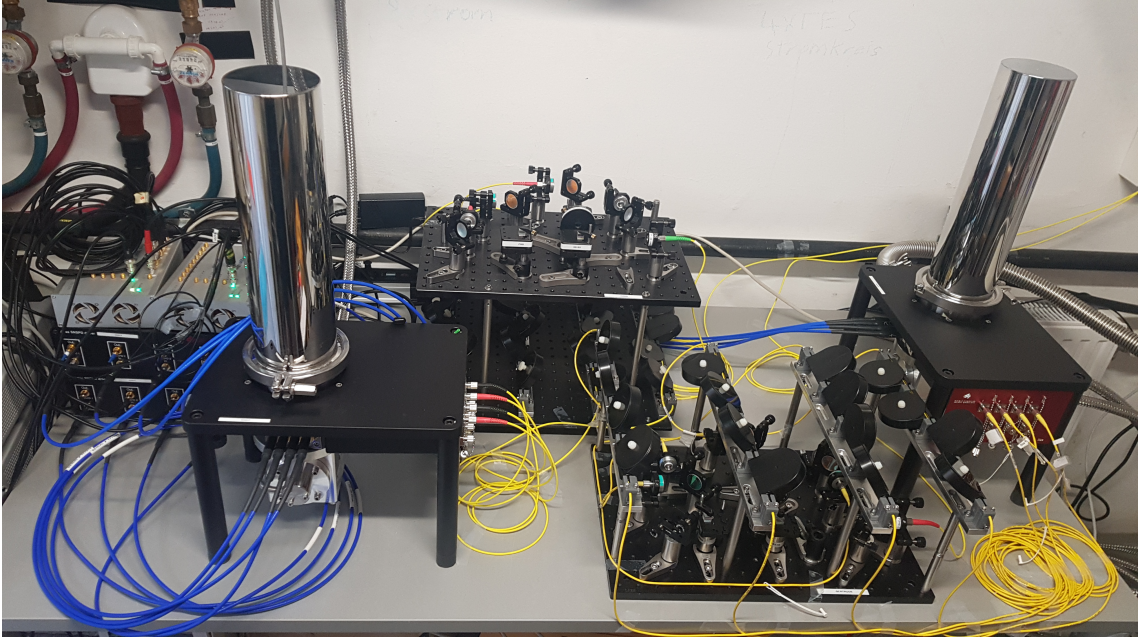


Figure 4.4: The setup of the detection part of the whole system with the two SNSPDs, one for Alice's side and one for Bob's side, the receiver modules, the time-tagging unit and the polarization controllers.

correlation histogram. If this is not done, we see so-called accidental coincidences

$$CC_{acc} = S_A \cdot S_B \cdot \tau_{CC}, \quad (4.2)$$

where $S_{A,B}$ are the single counts at Alice and Bob's side, respectively. Equation (4.2) represents the random coincidence counts which arise due to the width of the coincidence window τ_{CC} . For a derivation of (4.2) see appendix D. In the end CC_{acc} leads to a reduced visibility since these "accidental" coincidences are not correlated and have nothing in common with the original signal.

4.3.1 Jitter

In section 2.7 we explained what a jitter is in principle. The jitter of the whole QKD setup is a convolution of the jitter due to the two SNSPDs and the TTM.

It would be desirable to set the coincidence window in such a way that not too many noise counts could jitter into our coincidence window τ_{CC} and not too many of the correlated photons could jitter out of τ_{CC} and we lose part of our signal.

Let us consider two extreme cases:

$$\tau_{CC} \gg \tau_{jitter}$$

Here the coincidence window is much larger than the jitter. This leads to a reduced visibility since now there are much more noise counts inside τ_{CC} . Therefore the probability for an accidental coincidence is much higher.

$$\tau_{CC} \ll \tau_{jitter}$$

When τ_{CC} is much shorter than τ_{jitter} we lose correlated photons, because they simply jitter out of the coincidence window. This reduces the overall number of coincidences, which is not desirable since this leads in the end to a reduced keyrate.

A rule of thumb to set the coincidence window τ_{CC} is to choose it big enough that only the correlation peak fits inside (see figure 4.6).

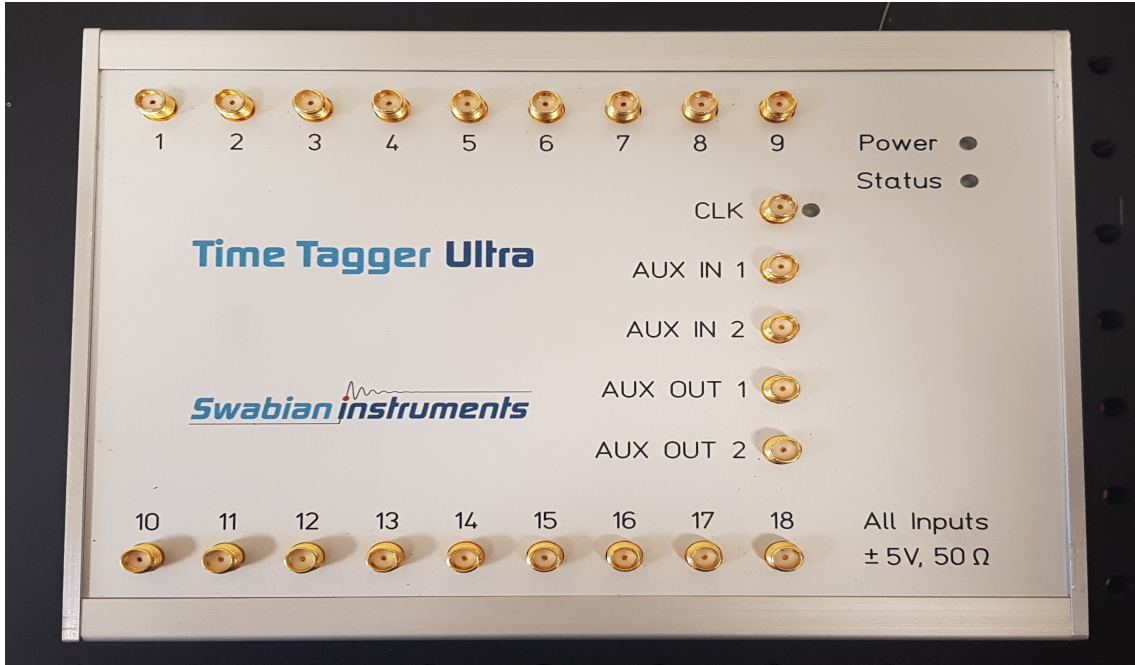


Figure 4.5: Time Tagger Ultra from Swabian Instruments

4.3.2 Correlation Measurement

Signal- and idler-photon exhibits a high temporal correlation which can be measured with the non-normalized cross correlation function [50]

$$G_{si}^2(t_1, t_2) = \left\langle \hat{E}_s^-(t_1) \hat{E}_i^-(t_2) \hat{E}_i^+(t_2) \hat{E}_s^+(t_1) \right\rangle. \quad (4.3)$$

$\langle \dots \rangle$ is defined as a time-average [14]

$$\langle f(t) \rangle = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T dt f(t) \quad (4.4)$$

This strong temporal correlation allows us to measure a correlation histogram as shown in figure 4.6. As mentioned above in 4.3, we had to add a time delay to one side of the time stamps from the TTM in order to gain such a histogram. The delay is caused by different fiber lengths and by the used electronics.

Figure 4.6 shows a histogram, where we correlated one channel at Alice's side and one channel at Bob's side. With an integration time of one second, we obtained a full width at half maximum (FWHM) through a Gaussian fit (solid orange line)

$$\text{FWHM} = 87.7 \text{ ps}$$

with a standard deviation of

$$\sigma = 37.3 \text{ ps.}$$

By performing this measurement, we used a second TTM in addition to the two SNSPDs and the first TTM. All those devices contribute to the overall jitter of the measurement setup. This jitter has as consequence that the actual $G_{s,i}^{(2)}$ function (typically in the order of a few fs to hundreds of fs) between signal and idler photon is broadened to 37.3 ps. Therefore the correlation histogram in figure 4.6 is actually a measure of the jitter of the setup.

A good estimate of the jitter of the whole setup is given by the following formula:

$$\tau_{\text{setup}} = \sqrt{2\tau_{\text{SNSPD}}^2 + 2\tau_{\text{TTM}}^2} \quad (4.5)$$

τ_{SNSPD} is the jitter of the SNSPDs. τ_{TTM} is the jitter of one TTM. The additional factor of 2 is a result of the fact that Alice as well as Bob use a SNSPD and a TTM. Using the jitter values of the SNSPDs $\tau_{\text{SNSPD}} \approx 22 \text{ ps}$ from section 4.2, together with $\tau_{\text{TTM}} \approx 11 \text{ ps}$ from 4.3, we get:

$$\tau_{\text{setup}} = \sqrt{2(22\text{ps})^2 + 2(11\text{ps})^2} \approx 38.6 \text{ ps} \quad (4.6)$$

This is in good agreement with the measured value of 37.3 ps.

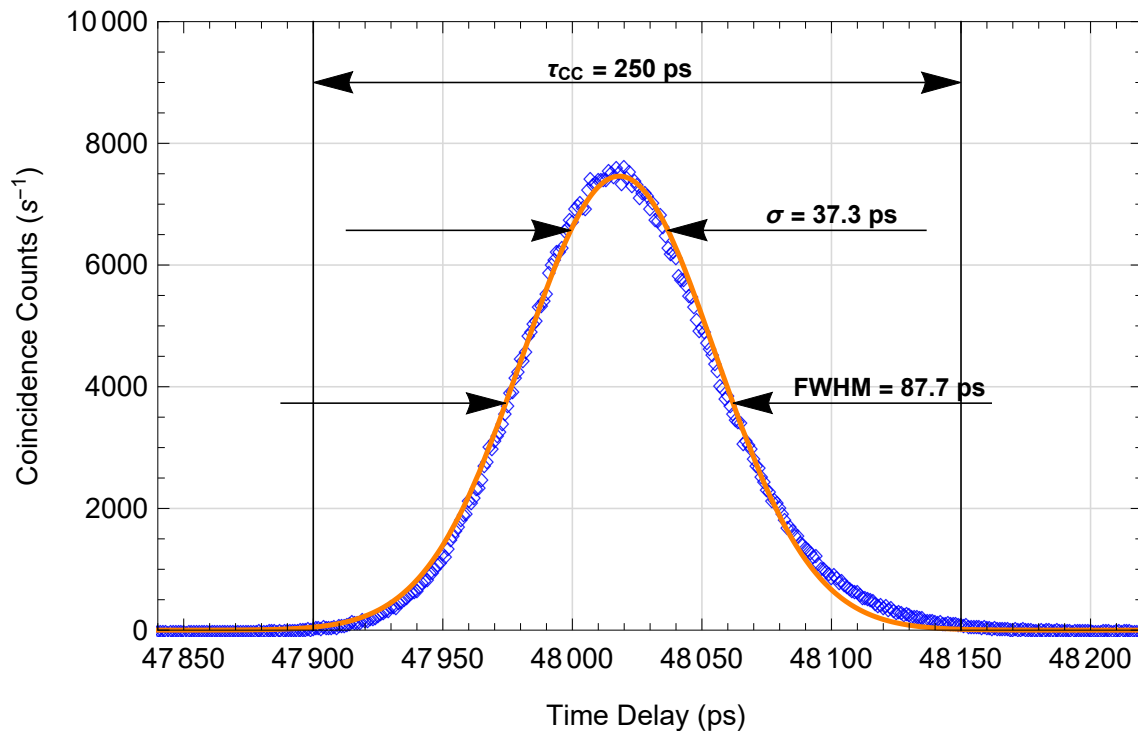


Figure 4.6: Here we see a typical histogram of a correlation peak between two channels of the SNSPD. The solid line is a Gaussian fit with a FWHM of 87.7 ps and a standard deviation of $\sigma = 37.3$ ps. The integration time was 1s. A good choice for the coincidence window is $\tau_{CC} = 250$ ps.

CHAPTER 5

QUANTUM KEY DISTRIBUTION USING A CW-LASER

In this chapter we discuss two possible scenarios for a QKD scheme. First, the entangled photon source is placed at Alice's side, where she measures her part of the entangled photons locally, whereas Bob's part of the entangled state travels to him through a lossy link. In addition Bob has some issues with stray light at the detector. In the second scenario the source is placed between Alice and Bob and both have to deal with the same loss.

We investigate both scenarios in a regime, where for the mean photon pair number μ holds: $\mu < 0.1$. This results in a linear behaviour of the *QBER* and the visibility $\mathcal{V}$.

5.1 General Considerations

As already mentioned in section 4.3, accidental coincidences (CC_{acc}) have the effect that they reduce the visibility $\mathcal{V}$ (2.40) of our entangled state. Let us now look how this works exactly. First of all we define $S_{A,B}$ as the sum of all clicks in the two measurement bases (H/V, D/A) on Alice and Bob's detectors, respectively, as follows:

$$S_A = B\eta_A + \Delta_A \quad (5.1)$$

$$S_B = B\eta_B + \Delta_B \quad (5.2)$$

$B\eta_A$ and $B\eta_B$ are the clicks which originate from the Sagnac source, i.e. clicks which came from entangled photons, see equation (3.7). Δ_A, Δ_B are clicks which either originate from intrinsic dark counts of the detector or from stray light.

The total amount of coincidences we are measuring (CC_{Max}) can be split up as follows:

$$CC_{Max} = CC_{pairs} + \frac{1}{2}CC_{acc} \quad (5.3)$$

CC_{pairs} are the coincidences from entangled pairs, see equation (3.6). CC_{acc} are accidental coincidences. The factor $\frac{1}{2}$ is due to the fact that also two dark counts can give a correct correlation by chance. CC_{acc} is defined in equation (4.2). Hence, we can write for CC_{acc} :

$$CC_{acc} = B^2\eta_A\eta_B\tau_{CC} + B\eta_A\tau_{CC}\Delta_B + B\eta_B\tau_{CC}\Delta_A + \tau_{CC}\Delta_B\Delta_A \quad (5.4)$$

The first term corresponds to accidentals due to multi-photon emission of the source, the second and third term corresponds to accidental coincidences from dark counts Δ_A (Δ_B) with a photon from the source. The last term, $\tau_{CC}\Delta_B\Delta_A$, describes accidentals which arise only due to dark counts Δ_A and Δ_B .

The minimum coincidences CC_{Min} has three contributions:

$$CC_{Min} = \frac{1}{2}CC_{acc} + B\eta_A\eta_B e_{opt}(1 - e_{opt})2 + B\eta_A\eta_B e_{opt}^2(1 - e_{opt})^2 \quad (5.5)$$

CC_{acc} has been discussed above. The second term, $B\eta_A\eta_B e_{opt}(1 - e_{opt})2$, corresponds to the coincidence counts which come from technical imperfections of the optical elements. e_{opt} is the probability that a photon gets assigned the wrong bit value. This corresponds for example to the extinction ratio (4.1), where it is always possible that e.g. a horizontally polarized photon is reflected instead of transmitted through a PBS. Therefore $B\eta_A\eta_B e_{opt}(1 - e_{opt})2$ describes a coincidence count from an entangled pair, where one part of the pair was accidentally led into the wrong port of the PBS. Hence, it caused an error. Third: This term describes the probability that on Alice's side and on Bob's side a photon passes through the wrong port of the PBS, which would correspond to a correct correlation, but was induced by two errors. However, the third contribution is very unlikely to happen and can in general be neglected. Hence, we write for CC_{Min} :

$$CC_{Min} = \frac{1}{2}CC_{acc} + B\eta_A\eta_B e_{opt}(1 - e_{opt})2 \quad (5.6)$$

Table 5.1 shows some values of the above discussed quantities from our setup. These were taken from the symmetric loss scenario (see section 5.3) with a pump power of the non-linear crystal of ~1.3 mW. Note that only CC_{Max} and CC_{Min} are experimentally accessible and the rest has to be backcalculated using the formulas discussed above and in section 3.4.2.

5.2 Asymmetric Noisy Link

In the further discussion we want to show qualitatively how the visibility $\mathcal{V}$ depends on the loss and on accidental coincidences. In this case only the first term in (5.6) is

$CC_{Max} [s^{-1}]$	$CC_{Min} [s^{-1}]$	$CC_{acc} [s^{-1}]$	η_A	η_B	$B [s^{-1}]$	e_{opt}
~8300	~63	~16	~0.044	~0.032	~ $5.66 \cdot 10^6$	~0.004
~2200	~26	~5	~0.023	~0.017	~ $5.8 \cdot 10^6$	~0.005
~730	~10	~1	~0.013	~0.009	~ $5.6 \cdot 10^6$	~0.007

Table 5.1: Here we see typical values of the above discussed quantities from our setup. These values are taken from the symmetric loss scenario, which is going to be described in section 5.3, with a pump power of the NLC of ~1.3 mW.

relevant, so we neglect for convenience the second one and come back to it in section 5.3.

By using the definition of the visibility $\mathcal{V}$ (see equation (2.39)), we can write $\mathcal{V}$ depending on the transmission loss η_A and η_B as follows:

$$\begin{aligned} \mathcal{V}(\eta_A, \eta_B) &\propto \frac{CC_{pairs}}{CC_{pairs} + CC_{acc}} \\ &= \frac{B}{B + B^2\tau_{CC} + B\tau_{CC}\Delta_B/\eta_B + B\tau_{CC}\Delta_A/\eta_A + \tau_{CC}\Delta_B\Delta_A/(\eta_A\eta_B)}, \end{aligned} \quad (5.7)$$

where we used equation (3.6) at the last equality sign.

In a scenario where the Sagnac source is located at Alice side, she measures her photon of the entangled state locally. Hence, the transmission probability η_A is a constant and only η_B varies.

Since we were interested in how the visibility $\mathcal{V}$ changes due to accidental coincidences, we introduced stray light at Bob's detectors. This means the dark counts on Bob's side were much higher than Alice's dark counts, $\Delta_B \gg \Delta_A$. But this implies that $B\tau_{CC}\Delta_B \gg B\tau_{CC}\Delta_A$. So we can rewrite equation (5.7) in the following form

$$\mathcal{V}(\eta_B) \approx \frac{B}{B + B^2\tau_{CC} + B\tau_{CC}\Delta_B/\eta_B + \tau_{CC}\Delta_B\Delta_A/(\eta_A\eta_B)} \quad (5.8)$$

Here we see how the visibility is reduced, due to accidental coincidences from noise counts, for different losses at Bobs side. Only the terms with dark counts Δ_B and Δ_A are dependent on the transmission probability η_B . Hence, if we increase the dark counts and decrease η_B ¹, the visibility $\mathcal{V}$ decreases overall. Therefore, the further away Bob is, the lower the transmission η_B will be, and the lower the visibility $\mathcal{V}$ is. This is clearly the case in figure 5.1.

In order to simulate this behaviour in the laboratory, we had to generate artificial noise directly at the receiver module, because the dark count rate of the SNSPDs were very low (~ 350 Hz). This noise was introduced at Bob's receiver module via a red

¹This means a higher loss at Bobs side

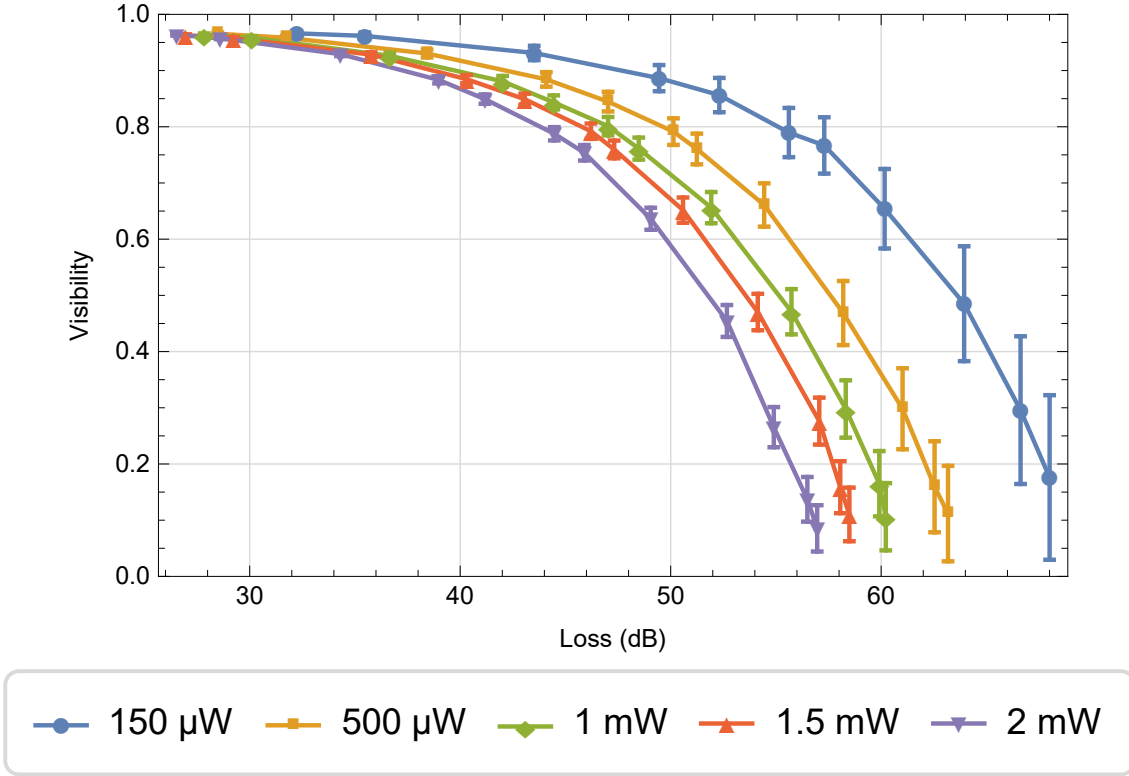


Figure 5.1: Here we see how an asymmetric noisy link on Bob's side affects the visibility for different pump powers. We observe that the visibility decreases as derived in equation (5.8). The error bars were calculated with equation 3.23. The lines are connecting just the data points to highlight the behaviour.

light emitting diode (LED) at the unused 50:50 BS port. According to the observed correlation peaks, we chose a coincidence window of $\tau_{CC} = 300$ ps, in the same way as we did in figure 4.6. The loss was simulated via neutral density (ND) filters. With (3.9) we calculated the transmittance η_B . After that we converted η_B to decibel (dB), a typical unit in telecommunication, by

$$Loss(dB) = 10 \cdot \log_{10}(\eta) \quad (5.9)$$

The power with which the non-linear crystal was pumped was measured before the loop in the source. Due to the really bad laser we had at our disposal, we could pump the crystal with a maximum power of 2 mW. This was still enough to produce roughly $CC_{Max} \sim 40000s^{-1}$.

From the measured visibility in figure 5.1 we calculated the expected keyrate with equation (2.37). What we observe in figure 5.2 is the typical "waterfall" behaviour,

a fast decrease of the keyrate at a certain loss. This is again due to the accidental coincidences CC_{acc} discussed above. For higher pump powers we see the drop earlier.

The error bars are omitted in figure (5.2) like it is usual in standard scientific articles regarding this topic in quantum communication.

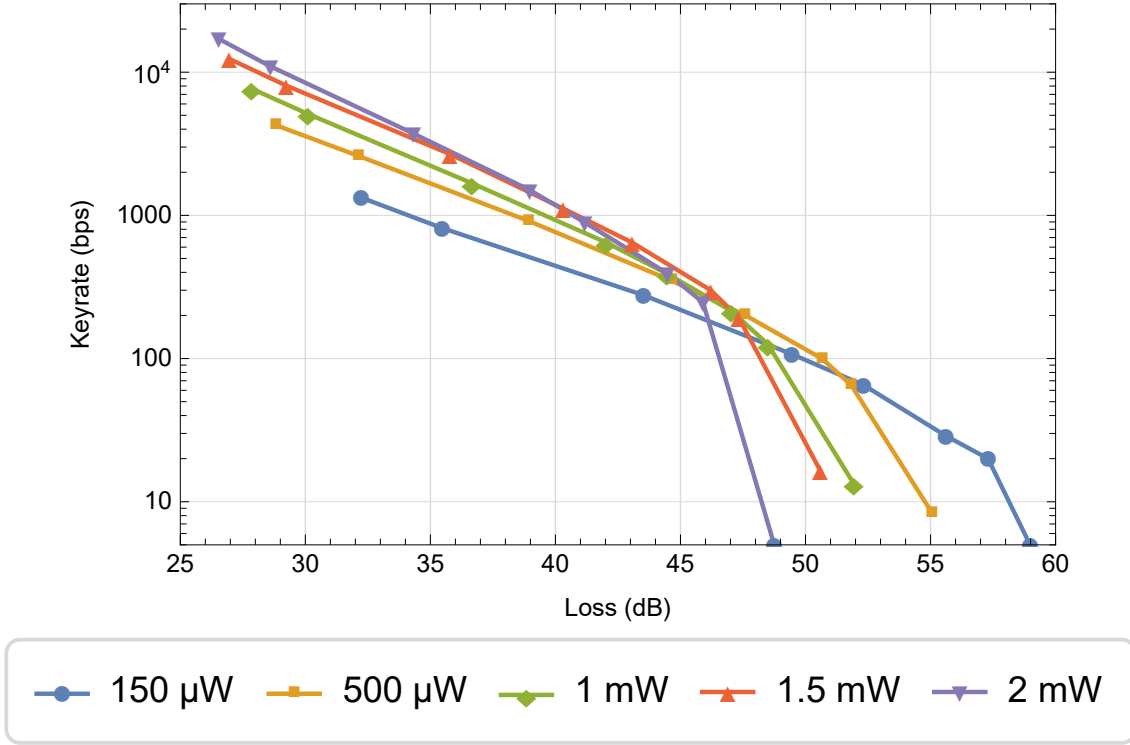


Figure 5.2: Keyrate depending on the link-loss. As we see here, a low pump power can be used to withstand a higher loss, although the keyrate is worse compared to a high pump power. The lines are connecting just the data points to highlight the behaviour.

5.3 Symmetric Link

In the following we consider an entangled photon QKD scheme with the source in between Alice and Bob. This configuration is completely different from the setups in 5.2, because now nobody measures directly at the source. This configuration is even then secure, when the source is in possession of a possible eavesdropper.

For choosing the coincidence window, we again observed first the correlation peaks. Therefore we came to the conclusion that $\tau_{CC} = 350$ ps is an appropriate value. We introduced loss again, but this time symmetrically for Alice and Bob by misplacing the SPDC coupler in the source (see figure 3.6, (15)). Now we are interested in how the pump power of the non-linear crystal effects the key generation in general without

artificial dark counts. Therefore we removed the red LED and dealt with a QKD-link without additional noise, which mimics the case of a real fiber-based quantum channel.

QBER

An alternative way of writing equation (2.34) for the *QBER* is given below

$$QBER = \frac{CC_{Min}}{CC_{Max} + CC_{Min}}, \quad (5.10)$$

where CC_{Min} , CC_{Max} are the minimum and maximum coincidence counts defined above. However, now we take e_{opt} into account, but still neglect terms $\propto e_{opt}^2$. This is reasonable since e_{opt} corresponds to the extinction ration R_x of the PBSs (see equation (4.1)). But in our case we achieved partially $R_x > 1 : 2000$. So it is safe to say that e_{opt}^2 is negligible. Therefore we can rewrite equation (5.10) as follows:

$$QBER \approx \frac{\frac{1}{2}CC_{acc} + 2B\eta_A\eta_B e_{opt}}{CC_{pairs} + CC_{acc} + 2B\eta_A\eta_B e_{opt}}. \quad (5.11)$$

Now a reasonable assumption is that the accidental coincidences are much lower than CC_{pairs} , $CC_{pairs} \gg CC_{acc}$ and also the following holds: $B\eta_A\eta_B \gg B\eta_A\eta_B e_{opt}$. Moreover, the dark count rate of the SNSPDs are $\approx 350s^{-1}$, so in equation (5.1)-(5.2) we can set $\Delta_{A,B} \approx 0$. It follows that the only dominant part in the denominator of equation (5.11) is $CC_{pairs} = \eta_A\eta_B B$, which leads to the following expression:

$$QBER \approx \frac{\frac{1}{2}CC_{acc} + 2B\eta_A\eta_B e_{opt}}{B\eta_A\eta_B}. \quad (5.12)$$

With μ defined in (3.10) as the mean photon pair number, we can simplify this further to

$$(5.12) \stackrel{(4.2)}{=} \frac{\frac{1}{2}S_A S_B \tau_{CC}}{\eta_A \eta_B B} + 2e_{opt} \stackrel{(3.7)}{=} \frac{1}{2}B\tau_{CC} + 2e_{opt} \stackrel{(3.10)}{=} \frac{\mu}{2} + 2e_{opt}. \quad (5.13)$$

Let us analyse equation (5.13) a bit further. e_{opt} is constant for a given QKD system because of unavoidable imperfections in the used elements. μ , on the other hand, can be changed easily by tuning the pump power of the crystal and the coincidence window. However, we only tuned the pump power because by increasing τ_{CC} we would have increased the probability for accidental counts caused by dark counts rather than by accidentals due to multi-photon emission. So mathematically speaking, (5.13) is a linear, strictly monotonously increasing function where e_{opt} is the intersection with the y-axis (see figure 5.3).

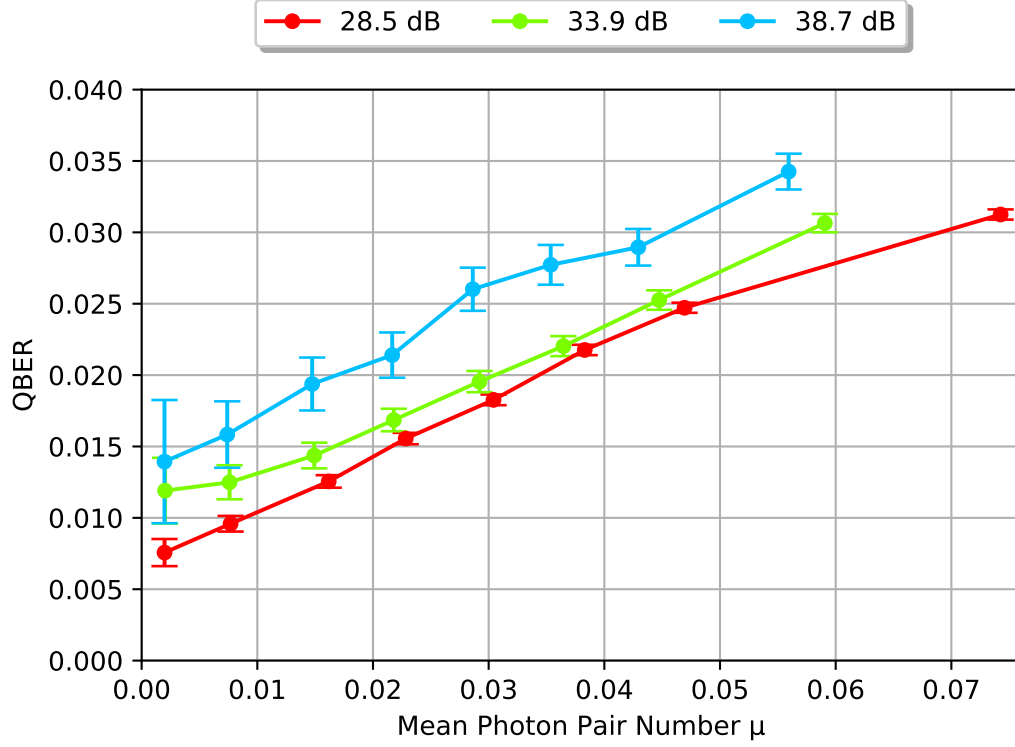


Figure 5.3: Here we see that the quantum bit error rate scales approximately linear with the mean photon pair number $\mu < 0.1$. Coincidence window $\tau_{CC} = 350$ ps.

Visibility

Now in order to investigate the whole QKD model further we come back to equation 2.36.

If we insert (5.13) into (2.36) we arrive at the following expression for the visibility $\mathcal{V}$:

$$\mathcal{V}(\mu) \approx 1 - 4e_{opt} - \mu \quad (5.14)$$

As in the case above, this is a linear function too. The first term $(1 - 4e_{opt})$ corresponds to the probability that both photons of an entangled pair are assigned the correct bit value² (Reminder: e_{opt} is the probability that a photon is assigned the wrong bit value due to polarization limitations). The second term in equation (5.14) describes how the visibility decreases with increasing μ due to multi-photon emission of the source. Note the similarity of equation (5.14) with the one derived in [51]. This work came theoretically up with the same functional behaviour as we did.

Figure 5.3 and 5.4 show exactly the behaviour derived above for the quantum bit error rate $QBER$ and the visibility $\mathcal{V}$. They are linearly increasing ($QBER$) and decreasing ($\mathcal{V}$) as the mean photon pair number μ is growing.

²Note that we neglected terms $\propto e_{opt}^2$

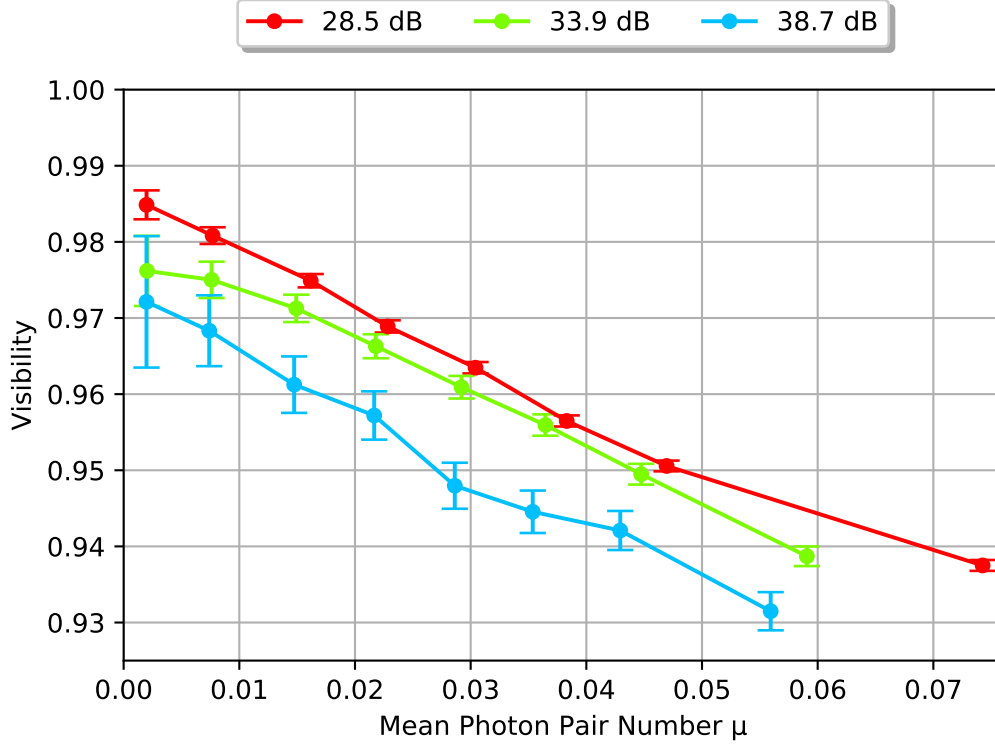


Figure 5.4: Visibility depending on the mean photon number μ . The decrease of the visibility can be explained by equation (5.14). We chose a coincidence window of $\tau_{CC} = 350$ ps.

In figure 5.5 we plot equations (5.13) and (5.14) for the 38.7 dB quantum link, because it represents the Vienna-Bratislava link. We see a good matching of our measured points with the simulation. From that we extracted an optical error $e_{opt} = 0.006$, which corresponds to a combined extinction ratio of the four PBS in the detection modules of roughly 1:150.

It should be mentioned that equations (5.13) and (5.14) show the dependence for the case when the mean photon pair number is in the regime $\mu \ll 1$. This is the reason that the theoretical model in figure (5.5) is not perfect for larger μ , but describes the situation well for small μ .

Keyrate

An extension of the QBER model by Ma et al. [11] was developed by Liu et al. [10]. Using this model, we see that the keyrate in dependence on μ describes our measured values very well, as it can be seen in figure 5.6. We note that the model by Liu et al. [10] is still under development and for a detailed treatment we refer to the article [10].

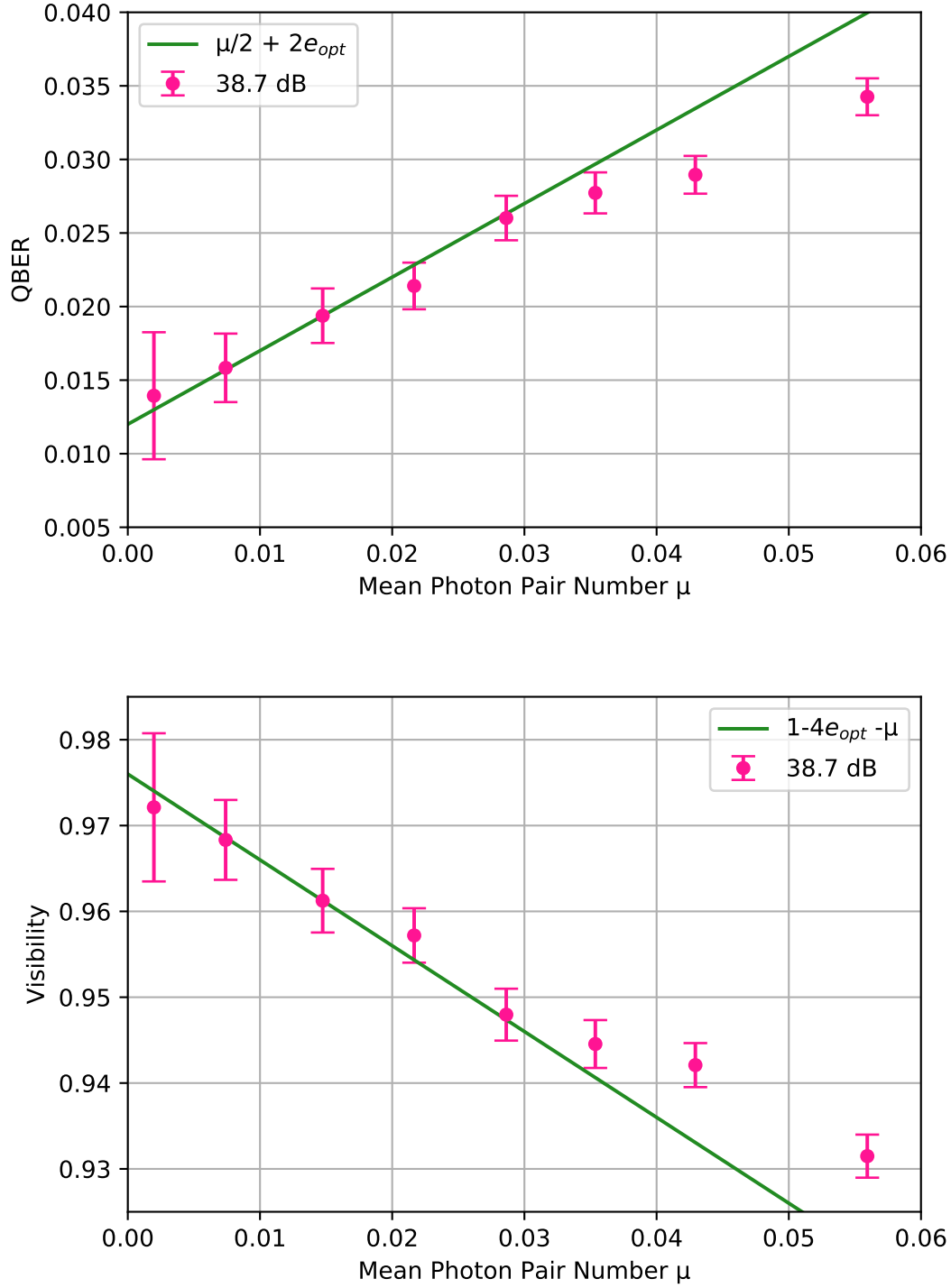


Figure 5.5: Here we see the measured $QBER$ and visibility $\mathcal{V}$ together with equations (5.13) and (5.14) for that one measurement. The optical error we chose here is $e_{opt} = 0.006$. We point out that equations (5.13) and (5.14) are first order approximations for the case when $\mu \ll 0.1$. This is the reason why the simulation does not fit our data points perfectly.

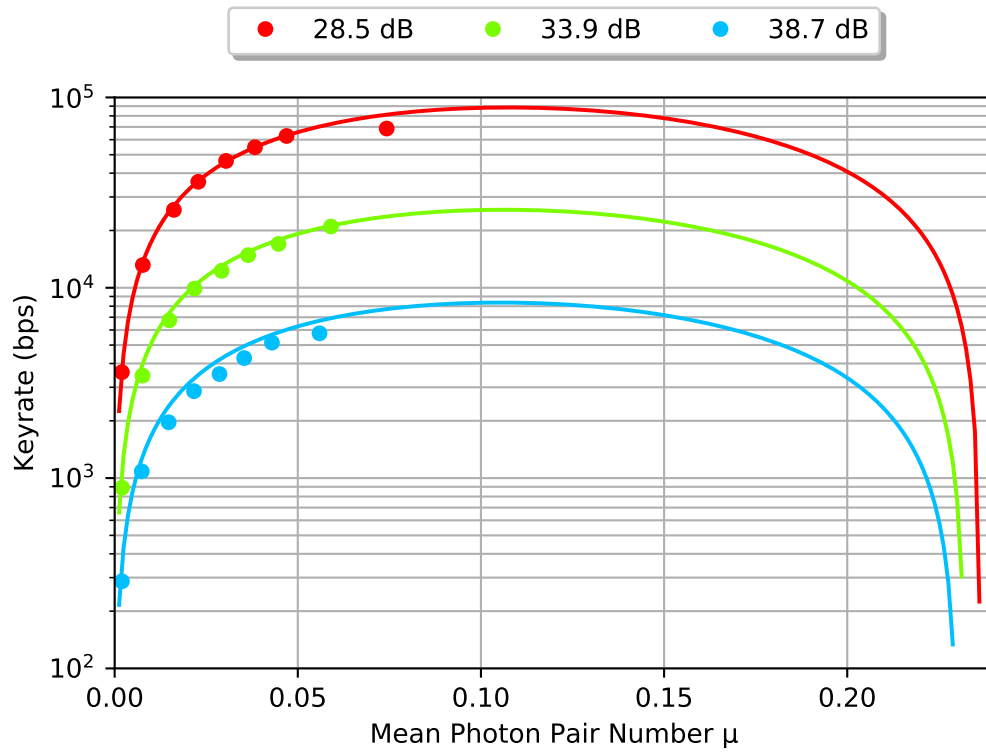


Figure 5.6: This figure shows the keyrate for different mean photon numbers μ . The solid lines show the theoretical model [10] by Liu et al. The measured data points are in nice accordance to the theoretical model for a regime where μ is smaller than 0.074. We could not achieve a higher μ due to the laser we had at that time.

CHAPTER 6

CONCLUSION AND OUTLOOK

In this thesis we constructed and characterised the most relevant parts for a deployed fiber-based quantum key distribution setup for the project QUAPITAL, namely the entangled photon source and the detection system.

We first constructed both detection modules, discussed in chapter 4, from scratch, and characterized them by the extinction ratio of the PBSs and their coupling efficiencies. Unfortunately, due to their shipping to different locations, we had to realign them several times, but this took a maximum of two hours each time. Hence, the extinction ratio may have changed over time. Both modules were used in several measurements, not only for the scope of this thesis. But the main purpose of them in future will be to operate as measurement devices in St. Pölten and Bratislava, respectively.

The Sagnac type of source was built from scratch too. Since the source is a lot more complex in comparison to a detection module, the alignment took several hours. With a visibility of $\sim 98\%$ (D/A) and $\sim 99\%$ (H/V) we achieved a high fringe visibility.

The keyrate model [10], which extends the old model by Ma [11] with an analysis of continuous wave QKD, was verified in a low power regime (up to ≈ 40 mW). That was owed to bad luck in the choice of laser company. However, after some troubles we are now in possession of a high power laser (up to ≈ 1 W). With this instrument, we should be able to check the model for the full range of the mean photon pair number μ as seen in figure 5.6.

After this, we are in the position to continue with the main experiment¹. The next step will be to install a glass fiber from the IQOQI-Vienna to a Telecom network hub and from there to the two endpoints in St. Pölten and Bratislava. Then nothing should hold us back from first measurements (except maybe dispersion).

¹Probably without me, since my time with this project has an expiration date...

LIST OF FIGURES

1.1	QUAPITAL endpoints	5
2.1	Orthonormal system used to set the polarization of the field	7
2.2	Sketch of a detection Module	17
3.1	Beta Barium Borate source	19
3.2	Crossed Crystal configuration	20
3.3	Folded Sandwich configuration	22
3.4	Sagnac-loop directions	23
3.5	Sketch of important parameters of the Sagnac source	25
3.6	Picture of Sagnac source	27
3.7	Type-0 collinear ppLN non-linear crystal	28
3.8	Isolator stage	29
3.9	SPDC spectra after DWDM	32
3.10	Dense Wavelength Division Multiplexer	33
3.11	Transmission profile of the DWDMs	34
3.12	Measurement configuration for visibility	37
3.13	Visibility in H/V and D/A basis	38
4.1	Picture of receiver-module	41
4.2	Nanowire and Cryostat	44
4.3	Detection Setup	45
4.4	Detection Setup	46
4.5	Time tagging module	47
4.6	Histogram of a correlation peak	49
5.1	Visibility vs. Loss for different laser pump powers	53
5.2	Keyrate vs. Loss for different laser pump powers	54

5.3	Qber for different mean photon numbers μ . Coincidence window: 350 ps	56
5.4	Visibility for different mean photon numbers μ . Coincidence window: 350 ps	57
5.5	Qber and Visibility with Fit-function	58
5.6	Keyrate for different mean photon numbers μ . Coincidence window: 350 ps	59

LIST OF TABLES

2.1	Difference between a product state and an entangled state for a two-qubit system.	10
4.1	Alignment data of the two Receiver-modules	42
5.1	Typical values for CC_{Max} , CC_{Min}	52

BIBLIOGRAPHY

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing.," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, 2014.
- [2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct 1969.
- [3] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964.
- [4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical review letters*, vol. 68, no. 21, p. 3121, 1992.
- [5] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.
- [6] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.
- [7] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, *et al.*, "Entanglement-based quantum communication over 144 km," *Nature physics*, vol. 3, no. 7, p. 481, 2007.
- [8] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Phys. Rev. Lett.*, vol. 84, pp. 4729–4732, May 2000.

- [9] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan 2018.
- [10] B. Liu, S. Neumann, R. Ursin, and T. Scheidl, "Modeling quantum key distribution with continuous-wave entangled photon sources." Article in preparation (2020).
- [11] X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," *Phys. Rev. A*, vol. 76, p. 012307, Jul 2007.
- [12] D. J. Griffiths and D. F. Schroeter, *Introduction to Quantum Mechanics*. Cambridge University Press, 3 ed., 2018.
- [13] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics*. Wiley, 1991.
- [14] C. Gerry and P. Knight, *Introductory Quantum Optics*. Cambridge University Press, 2004.
- [15] M. Krenn, *Quantum experiments with spatial modes of photons in large real and Hilbert spaces*. Phd thesis, Universität Wien, Fakultät für Physik, 2017.
- [16] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on einstein-podolsky-rosen states," *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, Nov 1992.
- [17] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993.
- [18] F. Steinlechner, P. Trojek, M. Jofre, H. Weier, D. Perez, T. Jennewein, R. Ursin, J. Rarity, M. W. Mitchell, J. P. Torres, H. Weinfurter, and V. Pruneri, "A high-brightness source of polarization-entangled photons optimized for applications in free space," *Opt. Express*, vol. 20, pp. 9640–9649, Apr 2012.
- [19] P. E. Powers and J. W. Haus, *Fundamentals of Nonlinear Optics*. CRC Press, 2 ed., 2017.
- [20] F. Steinlechner, *Sources of photonic entanglement for applications in space*. tesi doctoral, UPC, Institut de Ciències Fotòniques, 2015.
- [21] Y.-H. Kim, "Measurement of one-photon and two-photon wave packets in spontaneous parametric downconversion," *J. Opt. Soc. Am. B*, vol. 20, pp. 1959–1966, Sep 2003.

- [22] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical review letters*, vol. 67, no. 6, p. 661, 1991.
- [23] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002.
- [24] X. Ma, *Quantum cryptography: theory and practice*. Ph.d. thesis, University of Toronto, 2008.
- [25] M. Fink, "A receiver for optical free space quantum communication," Master's thesis, Technische Universität Wien, Fakultät für Physik , Atominstitut , E141, 12 2014. <http://katalog.ub.tuwien.ac.at/AC12155915>.
- [26] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, Dec 1995.
- [27] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultra-bright source of polarization-entangled photons," *Physical Review A*, vol. 60, no. 2, p. R773, 1999.
- [28] T. Scheidl, F. Tiefenbacher, R. Prevedel, F. Steinlechner, R. Ursin, and A. Zeilinger, "Crossed-crystal scheme for femtosecond-pulsed entangled photon generation in periodically poled potassium titanyl phosphate," *Phys. Rev. A*, vol. 89, p. 042324, Apr 2014.
- [29] M. Barbieri, F. De Martini, G. Di Nepi, P. Mataloni, G. M. D'Ariano, and C. Macchiavello, "Detection of entanglement with polarized photons: Experimental realization of an entanglement witness," *Phys. Rev. Lett.*, vol. 91, p. 227901, Nov 2003.
- [30] J. F. Hodelin, G. Khoury, and D. Bouwmeester, "Optimal generation of pulsed entangled photon pairs," *Phys. Rev. A*, vol. 74, p. 013802, Jul 2006.
- [31] F. Steinlechner, S. Ramelow, M. Jofre, M. Gilaberte, T. Jennewein, J. P. Torres, M. W. Mitchell, and V. Pruneri, "Phase-stable source of polarization-entangled photons in a linear double-pass configuration," *Opt. Express*, vol. 21, pp. 11943–11951, May 2013.
- [32] B.-S. Shi and A. Tomita, "Generation of a pulsed polarization entangled photon pair using a sagnac interferometer," *Physical Review A*, vol. 69, no. 1, p. 013803, 2004.
- [33] T. Kim, M. Fiorentino, and F. N. Wong, "Phase-stable source of polarization-entangled photons using a polarization sagnac interferometer," *Physical Review A*, vol. 73, no. 1, p. 012316, 2006.

- [34] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, "A wavelength-tunable fiber-coupled source of narrowband entangled photons," *Opt. Express*, vol. 15, pp. 15377–15386, Nov 2007.
- [35] L. M. Procopio Peña, *Single-photon experiments and characterization of superconducting nanowire single-photon detectors*. dissertation, Universität Wien, 2016.
- [36] S. P. Neumann, "Towards narrow-band photon pair sources for continuous-wave entanglement swapping," Master's thesis, Universität Wien, Universität Wien, Fakultät für Physik, 2016.
- [37] G. E. Keiser, "A review of wdm technology and applications," *Optical Fiber Technology*, vol. 5, no. 1, pp. 3–39, 1999.
- [38] H. Ishio, J. Minowa, and K. Nosu, "Review and status of wavelength-division-multiplexing technology and its application," *Journal of Lightwave Technology*, vol. 2, no. 4, pp. 448–463, 1984.
- [39] K. Hjorth, "Using photon entanglement as a fundamental resource in experimental physics," Master's thesis, Norwegian University of Science and Technology, Faculty of Natural Sciences, Department of Physics, 2019.
- [40] O. Gühne and G. Tóth, "Entanglement detection," *Physics Reports*, vol. 474, no. 1–6, pp. 1–75, 2009.
- [41] T. Herbst, T. Scheidl, M. Fink, J. Handsteiner, B. Wittmann, R. Ursin, and A. Zeilinger, "Teleportation of entanglement over 143 km," *Proceedings of the National Academy of Sciences*, vol. 112, no. 46, pp. 14202–14205, 2015.
- [42] W. Slys, M. Wegrzecki, J. Bar, P. Grabiec, M. Gorska, E. Reiger, S. Dorenbos, V. Zwiller, I. Milostnaya, and O. Minaeva, "Fiber-coupled nbn superconducting single-photon detectors for quantum correlation measurements," *Proceedings of SPIE, 2007 vol. 6583*, 10 2019.
- [43] "Infrared single-photon counter." <https://www.photonicsolutions.co.uk/upfiles/id230-specs.pdf>, 2014. Data Sheet.
- [44] G. Gol'Tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," *Applied physics letters*, vol. 79, no. 6, pp. 705–707, 2001.
- [45] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, *et al.*, "Detecting single infrared photons with 93% system efficiency," *Nature Photonics*, vol. 7, no. 3, p. 210, 2013.

- [46] A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," *Opt. Express*, vol. 16, pp. 3032–3040, Mar 2008.
- [47] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature photonics*, vol. 3, no. 12, p. 696, 2009.
- [48] S. Dorenbos, E. Reiger, N. Akopian, U. Perinetti, V. Zwiller, T. Zijlstra, and T. Klapwijk, "Superconducting single photon detectors with minimized polarization dependence," *Applied Physics Letters*, vol. 93, no. 16, p. 161102, 2008.
- [49] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," *Superconductor science and technology*, vol. 25, no. 6, p. 063001, 2012.
- [50] A. Valencia, G. Scarcelli, and Y. Shih, "Distant clock synchronization using entangled photon pairs," *Applied Physics Letters*, vol. 85, no. 13, pp. 2655–2657, 2004.
- [51] O. Kuzucu and F. N. Wong, "Pulsed sagnac source of narrow-band polarization-entangled photons," *Physical Review A*, vol. 77, no. 3, p. 032314, 2008.
- [52] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, p. 802, 1982.

APPENDIX A

NO-CLONING THEOREM

Due to the No-cloning theorem [52], it is not possible to copy an arbitrary quantum state. Therefore it is not possible for an eavesdropper to e.g. catch a photon from a QKD measurement, copy it and then send it on to the actual receiver without him noticing.

Here we present a simple proof of this theorem. Let us consider two arbitrary states $|\phi\rangle$ and $|\psi\rangle$, as well as $|c\rangle$, which will get 'overwritten' in the cloning process.

So let us consider we have a transformation that works on $|\phi\rangle$ and $|\psi\rangle$ in the following way

$$|\phi\rangle |c\rangle \rightarrow |\phi\rangle |\phi\rangle \quad (\text{A.1})$$

$$|\psi\rangle |c\rangle \rightarrow |\psi\rangle |\phi\rangle . \quad (\text{A.2})$$

This must also hold for a linear combination of these two states $|\xi\rangle = \alpha |\phi\rangle + \beta |\psi\rangle$

$$|\xi\rangle |c\rangle \rightarrow \alpha |\phi\rangle |\phi\rangle + \beta |\psi\rangle |\psi\rangle \quad (\text{A.3})$$

where we assumed that the transformation acts linearly on $|\xi\rangle$ [12]. But actually we wanted this transformation

$$|\xi\rangle |c\rangle \rightarrow |\xi\rangle |\xi\rangle = \alpha^2 |\phi\rangle |\phi\rangle + \beta^2 |\psi\rangle |\psi\rangle + \alpha\beta |\phi\rangle |\psi\rangle + \beta\alpha |\psi\rangle |\phi\rangle , \quad (\text{A.4})$$

which is not the same as above. This shows that such a transformation can exist for individual states, but it will fail in general.

APPENDIX B

JONES FORMALISMUS

In the Jones formalism, optical elements like a HWP, QWP or polarizers are represented by 2x2 matrices.

A QWP for example can be written as:

$$QWP = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \quad (\text{B.1})$$

And a HWP is given in the following form:

$$HWP = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (\text{B.2})$$

If the WP is rotated with respect to the optic axis around θ , the resulting operation on a given state is given by:

$$R(-\theta) \cdot WP \cdot R(\theta) \cdot |\phi\rangle, \quad (\text{B.3})$$

where $R(\theta)$ is the following rotation matrix

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} \quad (\text{B.4})$$

APPENDIX C

GAUSSIAN OPTICS

An Ansatz for a paraxial wave can be written as

$$U(\vec{x}) = A(\vec{x})e^{-ikz} \quad (\text{C.1})$$

with the assumptions: $\frac{\partial A}{\partial z} \ll kA$ and $\frac{\partial^2 A}{\partial z^2} \ll k\frac{\partial A}{\partial z}$, the paraxial wave equation reads

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} - 2ik\frac{\partial}{\partial z}\right)A(\vec{x}) = 0 \quad (\text{C.2})$$

Now we draw up some definitions:

$$z \rightarrow z - \zeta \equiv q(z) \quad \text{q-parameter} \quad (\text{C.3})$$

If we set $\zeta = -iz_0$, the following holds:

$$\frac{1}{q(z)} = \frac{1}{z + iz_0} = \frac{z}{z^2 + z_0^2} - i\frac{z_0}{z^2 + z_0^2} =: \frac{1}{R(z)} + i\frac{\lambda}{\pi\omega^2(z)}, \quad (\text{C.4})$$

where $R(z)$ is the curvatur of the wavefront

$$R(z) = z \left(1 + \frac{z_R^2}{z^2}\right) \quad (\text{C.5})$$

$\omega(z)$ is the beam waist at distance z

$$\omega(z) = \omega_0 \sqrt{1 + \frac{z}{z_R}} \quad (\text{C.6})$$

and ω_0 is the beam waist at the focus point. The Rayleigh range is defined as $z_R = \frac{\pi\omega_0^2}{\lambda}$. The wave is then given by

$$E(\vec{x}) = \frac{N\omega_0}{iz\omega(z)} \exp\left(-\frac{x^2 + y^2}{\omega^2(z)}\right) \exp\left(ikz + ik\frac{x^2 + y^2}{2R(z)} - i\xi(z)\right) \quad (\text{C.7})$$

with the Gouy phase $\xi(z) = \tan^{-1}(\frac{z}{z_R})$. For a more detailed discussion, see [15]

The smart thing about the q-parameter is that it holds the information about the beam waist and the curvature of the beam.

Any paraxial approximated optical system can be represented by a 2x2 matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad (\text{C.8})$$

So in order to determine how the q-parameter changes through a system, the following holds

$$q_2 = \frac{Aq_1 + B}{Cq_1 + D} \quad (\text{C.9})$$

With this knowledge, we were able to calculate the needed lenses for the Sagnac source in the following way.

1. Setting ξ in (3.5) for our purpose (L is given from the crystal), we calculated the Rayleigh range z_R inside the crystal. Therefore we knew ω_0 .
2. Now, by using the ABCD-law for the pump-lens and then for the collimation lens into the SMF, we were able to calculate the best matching focal lengths.
3. Repeat the same for the SPDC

The ABCD matrix for a thin lens with focal length f is given by

$$\begin{pmatrix} 1 & 0 \\ -\frac{1}{f} & 1 \end{pmatrix} \quad (\text{C.10})$$

And for a beam travelling a distance d

$$\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \quad (\text{C.11})$$

A beam entering a medium with refractive index n_2 coming from a medium with refractive index n_1 can be described by the following matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & \frac{n_1}{n_2} \end{pmatrix} \quad (\text{C.12})$$

APPENDIX D

ACCIDENTAL COINCIDENCE COUNTS

Here we derive the formula for the accidental coincidence counts given by equation (4.2).

The probabilities to detect n photons are governed by the Poissonian distribution

$$P(\mu) = e^{-\mu} \frac{\mu^n}{n!}, \quad (\text{D.1})$$

where μ is the mean photon number.

The mean photon number in a given time interval τ_{CC} on Alice's side is given by

$$\mu = S_A \tau_{CC}, \quad (\text{D.2})$$

where S_A is the total number of photons at Alice's. The probability to detect at least one photon ($n > 0$) is given by

$$P_{1,A}(\mu) = \sum_{n=1}^{\infty} e^{-S_A \tau_{CC}} \frac{(S_A \tau_{CC})^n}{n!} = 1 - e^{-S_A \tau_{CC}} \quad (\text{D.3})$$

The same holds for Bob. Hence, we can exchange S_A with S_B in the above equations. Now, to detect at least one photon on Alice's side and one photon on Bob's side per time interval τ_{CC} , we can multiply these two probabilities and divide by τ_{CC}

$$P_{1,A}(\mu) P_{1,B}(\mu) \frac{1}{\tau_{CC}} = (1 - e^{-S_A \tau_{CC}})(1 - e^{-S_B \tau_{CC}}) \frac{1}{\tau_{CC}} = S_A S_B \tau_{CC}, \quad (\text{D.4})$$

where we used $S_A \tau_{CC} \ll 1$ and $S_B \tau_{CC} \ll 1$ at the last equality sign. Therefore we were able to Taylor expand the exponential functions around zero to first order and neglect all higher order terms.

