LUDWIG-MAXIMILIAN-UNIVERSITY MUNICH
DEPARTMENT OF PHYSICS

MASTER'S THESIS

Peter Freiwang

Towards Hand-held Quantum Key Distribution

Supervised by
Prof. Dr. Harald WEINFURTER

26.01.2017

LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN
FAKULTÄT FÜR PHYSIK

MASTERARBEIT
Peter Freiwang

Entwicklungen für Quantenschlüsselverteilung mit tragbaren Komponenten

Betreut durch
Prof. Dr. Harald WEINFURTER

26.01.2017

Abstract

Quantum Key Distribution (QKD) is an unconditionally secure method, based on quantum mechanical laws, to generate a shared secret key between two parties further usable for encrypted communication. Besides reaching longer distances for QKD, also short range applications exist, however, at this point the integration into conventional communication platforms plays a major role. Within this work, an existing freespace QKD setup with an operating distance about 0.5 m, consisting of a novel miniaturised sender module and a tracking receiver was characterised. The size of the sender optics of only $35 \times 20 \times 8\,\mathrm{mm}^3$ allows for the integration into mobile devices and, in combination with a tracking receiver, a key exchange in hand-held operation becomes possible. The system implements the BB84 protocol using weak coherent laser pulses ($\mu \approx 0.1$) from four vertical-cavity surface-emitting lasers (VCSELs) at 850 nm. An improved method for the quantum state tomography (QST) to determine the output states of the sender module and the complete characterisation of the receiver allowed the demonstration of a key exchange where the sender was firstly stationary and then held by the user. Here, secure key rates on the order of a few 100 kBit/s in stationary and a few 10 kBit/s in hand-held operation at quantum bit error ratios (QBERs) of less than 2% were achieved.

Zusammenfassung

Die Quantenschlüsselverteilung (QKD) ist eine Methode, frei von mathematischen Annahmen, für die Generierung eines geheimen Kryptographie-Schlüssels zwischen zwei Parteien, welcher dann für die Verschlüsselung der Kommunikation verwendet werden kann. Hauptsächlich wird versucht QKD auf größeren Distanzen zu realisieren, jedoch gibt es auch Anwendungen für kurze Distanzen, wobei hier die Möglichkeit der Integration in kommerzielle Kommunikationssysteme sehr wichtig ist. Im Rahmen dieser Arbeit wurde ein bestehender Freistrahl-QKD Testaufbau mit einem Arbeitsabstand von ca. 0.5 m, zusammengesetzt aus einem miniaturisierten Sender-Modul und einem Empfänger, welcher über die Möglichkeit eines dynamischen Strahlführungssystems (Tracking) verfügt, charakterisiert. Die Abmessung der Sender-Optik von nur $35 \times 20 \times 8\,\mathrm{mm}^3$, erlaubt die Integrierung in mobile Endgeräte. In Verbindung mit dem Tracking-Empfänger ist ein Schlüsselaustausch möglich, bei dem das Sender-Modul in der Hand gehalten wird. Das Testsystem verwendet das BB84-Protokoll mit abgeschwächten Laser-Pulsen ($\mu \approx 0.1$). Als Lichtquelle dienen oberflächenemittierende Halbleiterlaser (VCSELs) bei einer Wellenlänge von 850 nm. Eine verbesserte Methode zur Bestimmung der Polarisationszustände des Sender-Moduls (QST) und eine vollständige Charakterisierung des Empfängers ermöglichten einen Schlüsselaustausch, wobei das Sender-Modul zuerst fest vor dem Empfänger montiert war und anschließend in der Hand des Anwenders gehalten wurde. Hierbei wurden für ersteren Fall eine sichere Schlüsselrate von einigen 100 kBit/s und für zweiteren Fall einigen 10 kBit/s bei einer Fehlerrate (QBER) von unter 2%, erreicht.

Contents

1. Introduction

Quantum key distribution (QKD) [1–3] uses the quantum mechanical properties of light in order to provide an unconditionally secure method for exchanging a secret key between two authenticated parties. Sharing a secret key is the basis for the highly secure symmetrical cryptography schemes (e.g. Advanced Encryption Standard (AES) [4]), where the same key is used for encryption and decryption. However, attacks on the key exchange process, which often is the weakest link for these systems, can break the security relatively easy. QKD closes this security gap. If QKD is combined with the so called One-Time-Pad (OTP) [5], where the original message is encrypted with a random key of the same length as the message, even absolute security can be reached theoretically. In other words, an eavesdropper[1] is not able to decrypt the message even if equipped with unlimited computational power and only being restricted by the fundamental laws of physics.

In order to avoid a direct exchange of a secret key over insecure channels, so called asymmetrical cryptography methods (e.g. RSA [6]), where different keys are used for encryption and decryption, were proposed. Their security is based on mathematical assumptions like the difficulty of the factorisation of large numbers and assumptions on the limited computational power of the attacker. However, the Shor algorithm [7] running on a quantum computer can break the key. Furthermore, even if the attacker does not have a quantum computer, there is still no proof that there does not exist an effective classical algorithm for the given problems. This argument is still valid if an attacker has a quantum computer as there exists no proof that a quantum computer can not break the security of post-quantum cryptography algorithms[2], as well.

As we live in the digital age, a big part of our daily communication like private and business correspondence, bank transfers and more takes place over the internet and must be protected against eavesdropping and manipulation. Besides security holes which affect our personal communication, the much more far-reaching problem is concerning the national and international affairs including internal security, diplomacy and military affairs. The most recent example was the 2016 presidential election in the USA, which was overshadowed by hacker attacks [8]. QKD will be an important part for enabling a secure communication when, undoubtedly, someday our current cryptography system will collapse leading to unpredictable consequences on a global scale.

Stephan Wiesner gave the first impulse to use quantum effects for the secure exchange of information around 1970, published 1983 [9], with the idea of quantum

[1] A third party with access to the communication channel, however, no access to the devices of the communicating parties.

[2] Classical cryptographic algorithms, which are supposed to be as complex as also a quantum computer is not able to break the security within a practicable amount of time.

money. The first protocol for QKD was proposed by Charles H. Bennett and Gilles Brassard in 1984 [10], where four states of linearly polarised photons in two conjugate bases are used for encoding the qubits. Various families of QKD protocols have been developed over the years in order to improve the performance of QKD systems in the context of reaching longer distances, increasing extractable secret key rates, closing security loopholes, merging with commercial telecom components and more. From the first experimental demonstration of QKD in 1992 [11], it took around ten years until the first commercial QKD products were available from several companies which offer QKD systems[3]. In order to extend QKD networks, which were already demonstrated in Vienna (Austria) [12], Geneva (Switzerland) [13] and Tokio (Japan) [14], to a larger scale, it is important to bridge long distances (current records: fiber based QKD: 404 km [15], freespace link: 144 km [16, 17]). The big goal here is to realise a QKD network based on satellites. A first step in this direction was the realisation of a link between an airplane and a ground station in 2013, where also successfully a key was exchanged [18]. A first simulation of a satellite-earth link feasible for QKD was established in 2015 [19]. In 2016, a satellite by a Chinese research project has been launched in order to perform quantum experiments including QKD [20]. Besides that, also miniaturised satellites [21, 22] are used in order to win the race [23] for first satellite-earth key exchange.

On the other side there is also a need for secure communication over small distances, e.g. for contactless payment, network access or other critical processes. For this reason, a sender based on micro optics was designed and built with the size of only $35 \times 20 \times 8\,\mathrm{mm}^3$ implementing the BB84 protocol with attenuated laser pulses [24, 25]. The small size of the micro optics allows for its integration into mobile devices like smartphones or tablets. For applications considered above a key exchange where the sender is held by the user should be enabled. To achieve this, a stationary receiver consisting of a polarisation analysis unit was extended by a beam tracking and controlling system [26].

This Master's thesis deals with the characterisation and modification of this QKD setup in order to increase the general performance of the system. The characterisation methods for sender and receiver were improved in precision and stability. Furthermore, modifications on the system were made, where the overall error as well as the functionality could be improved. This allowed for a key exchange in a hand-held scenario.

This work is organised as follows: Chapter 2 deals with the concepts of cryptography including classical cryptography schemes and an introduction to QKD. The experimental part is divided into three chapters, which describe the characterisation and modifications of the sender unit Alice (Chapter 3), the receiver Bob (Chapter 4) and the results of the key exchange achieved at the very end of this work (Chapter 5). Respectively the first part of the chapters concerning the sender and the receiver explains the general idea and the design of the devices and also shows the state of the experiment at the beginning of this work.

[3] MagiQ Technologies (New York, USA), ID Quantique (Geneva, Switzerland), QuintessenceLabs (Deaking, Australia), SeQureNet (Paris, France)

2. Concepts of Cryptography

This chapter gives an overview of cryptography and starts with the methods of classical cryptography schemes. The major task here is to share a secret key between the communicating parties. Quantum key distribution (QKD) is an unconditionally secure method to achieve this and is presented in the second section.

2.1. Classical cryptography

In the following, the basic principles and terminology of classical cryptography are presented. Furthermore symmetrical and asymmetrical encryption systems are discussed.

2.1.1. Basic principle

Suppose two parties, usually called Alice and Bob, want to exchange a secure message. If Alice sends the message in the original or plain text form, a simple attack at the communication link enables an eavesdropper, conventionally called Eve, to read the message. Depending on Eve's strategy, Alice and Bob may not even notice that their communication was eavesdropped upon. At this point, cryptography, which can be seen as the art of converting a message such that it is unintelligible to any unauthorised party [1], becomes important. Besides providing confidentiality, additional factors are assigned to the field of cryptography, which are ensuring integrity, techniques for exchanging secret keys, protocols for authenticating users, nonrepudiation and more [27, 28].

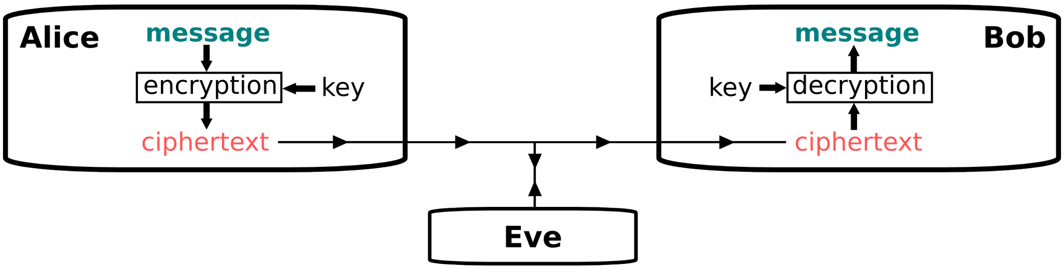


Figure 2.1.: **Simplified model for an encrypted communication**
Alice holds a message, which is encrypted and sent to Bob where the original message can be decrypted. The eavesdropper (Eve) can only intercept the ciphertext.

Figure 2.1 illustrates the basic procedure of an encrypted communication between Alice and Bob. Alice's message in plain text form is encrypted into a ciphertext and sent to Bob. At Bob's side, the received ciphertext is decrypted back into the plain text form. The encryption and decryption methods, which are used in modern cryptography are based on the Kerckhoffs' principle, i.e., the method is known publicly and the security of the whole process relies only on the key itself. Thereby, an algorithm together with a key is used for encryption and decryption. A party, which receives the ciphertext and holds the right key is able to reconstruct the message. A perfectly secure ciphertext is impossible to decrypt without the key. There exist basically two cryptography models, which are discussed in the following: The symmetrical and the asymmetrical setting.

2.1.2. Symmetrical encryption

A cryptography method is called symmetric, if an identical key for encryption and decryption is used.

In modern cryptography, the most commonly used symmetrical system is the Advanced Encryption Standard (AES) [4]. AES belongs to the block ciphers, where blocks of the message (maximal block size: 128 bit) are substituted and permuted with a random key, in several rounds. Independently from the block size, the key size n is 128, 192 or 256 bit [28]. The number of possible combinations P, which has to be tested during a brute force attack is 2^n (For $n = 128$, $P \sim 10^{38}$). Even a brute force attack with a modern super computer (e.g. the SuperMUC, Munich, $\sim 10^{15}$ FLOPS) would take on the order of $10^{38}/10^{15} = 10^{23}$ seconds $\approx 10^{16}$ years to go through all possible combinations. So far, only the cipher of so called reduced round variants of AES show a ponderable reduced security, which could be exploited by an attacker [28]. However, only the fact that still no attack is found, which can efficiently break the AES, does not imply that no methods exist.

In contrast to AES, the so called one-time-pad (OTP) [5] provides unconditional security, if it is correctly implemented. For this purpose, a random key with the same length as the message is needed. Furthermore, it is not allowed to use the key more than once. By applying a XOR operation onto every character of the message with a character of the key, a completely random ciphertext can be created. Even if all combinations could be tested by brute force, an attacker can not identify the original message. The encrypted message simply contains no information [29]. Despite the theoretical security of the OTP, it is only rarely used as it becomes impractical for longer messages.

The security of a symmetrical cryptography method decisively depends on the confidentiality of the key, which has to be exchanged between the communicating parties. As many attacks aim at the communication link, especially the key distribution becomes a crucial point here.

2.1.3. Asymmetrical encryption

If different keys are used for encryption and decryption of a message, the cryptography method is called asymmetrical. For example, for the widely used public key method, the communicating parties basically have to go through the following steps:

- Bob generates two keys: the public and the private key. The public key is sent to Alice over an insecure channel whereas the private key has to be held secretly.
- Alice encrypts the message by the usage of the public key and sends the ciphertext to Bob.

- Bob decrypts the ciphertext by the usage of the private key.

The most prominent asymmetrical cryptography method is the RSA scheme [6]. Its security is based on the difficulty of the factorisation of large numbers (here the public key), with known classical methods.

At the moment, the General Number Field Sieve (GNFS) is the fastest known algorithm for factorisation. Using the GNFS, the complexity of the problem scales superpolynomial with the length of the number. Even for modern super computers, ludicrous long running times would be needed, in order to factorise a RSA key with typically 2000 digits.

However, it is still not proven that there exists no effective classical factorisation algorithms. Furthermore, the security of RSA could be broken by running the Shor algorithm [7] on a quantum computer. In this case the factorisation problem scales polynomially, which would lead to drastically reduced computational times for attackers as compared to the currently known classical algorithms.

The advantage of asymmetrical cryptography methods is that no secret key has to be exchanged between Alice and Bob. However, the cryptography procedure takes much longer (approximately by a factor of 10^3) as compared to symmetrical ones. For this reason, so called hybrid cryptography systems are used commonly. Here, in a first step, the asymmetrical scheme serves for the generation of a shared secret key, which is used in the next step for a symmetrical encryption and decryption of the message.

2.2. Quantum key distribution (QKD)

The previous section showed that only the so called one-time-pad (OTP) can enable absolute security, given that it is correctly implemented, which becomes impractical for longer messages. The modern symmetrical schemes provide a strong security, however, a secret key has to be shared by the communicating parties. If an attacker obtains the key, the security is completely broken as the encryption algorithms are public. Attacks often aim at the communication link, where the key usually is exchanged. In 1984, Charles H. Bennett and Gilles Brassard presented a novel key exchange method, where the security is only based on quantum mechanical laws. The so called BB84 protocol [10] was the first step into the field of Quantum Key Distribution (QKD). QKD provides an unconditional security for generating and distributing a random key plus the possibility to detect the presence of an eavesdropper, however, it is often erroneously denoted as cryptography method per se.

In this section, the basic principle of QKD is explained and the procedure and security aspects of common QKD protocols are presented. A short section explains the last steps of every QKD protocol: The error correction and the privacy amplification. Finally, some of the possible attacks as well as so called side channels are discussed.

2.2.1. QKD - Basic principle

For the implementation of QKD, the communication link between two authenticated parties is extended by a so called quantum channel over which a key is exchanged (see Figure 2.2).

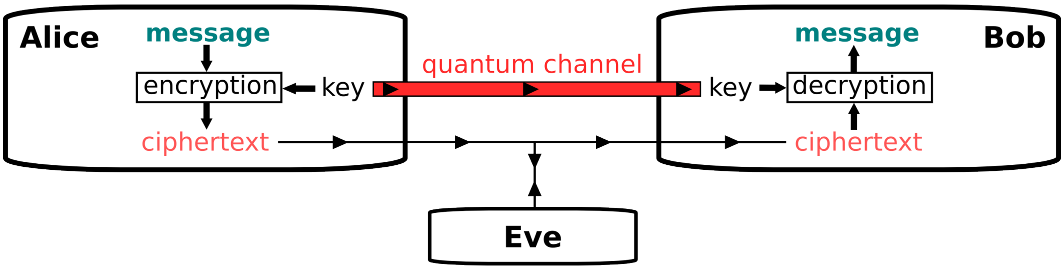


Figure 2.2.: **Simplified model of QKD for encrypted communication**
Besides the insecure classical channel between Alice and Bob, there is also a quantum channel, which is used for the key exchange.

The cryptography process itself is in principle untouched and still classical (see Section 2.1). The idea behind QKD is that an eavesdropper can be detected by Alice and Bob due to disturbances of the quantum channel, which occur if Eve performs measurements on the exchanged quantum states. This is still the case, even in the presence of a very powerful eavesdropper, which is only limited by the laws of quantum mechanics. QKD can not prevent an attack, however, under certain conditions, QKD may still allow a secure key exchange even in the presence of an eavesdropper. This is possible as the amount of information accessible to Eve can be estimated by Alice and Bob. During a so called privacy amplification step, Eve's knowledge about the key can be shrunk to zero by reducing the size of the key. If no key can be generated during the privacy amplification, the exchanged signals are discarded and a new key has to be sent.

2.2.2. Quantum mechanical foundations

In the beginning of this section, the qubit, as counterpart to the classical bit as well as quantum mechanical measurements are explained. Furthermore, the no-cloning theorem, which is a cornerstone for the security of QKD, is presented.

2.2.2.1. Qubits and measurements

The smallest information unit, in the classical information theory, is called bit. It can be in one of two possible states. Such states can be for example two different voltage levels U_0 and U_1, where U_0 corresponds to the bit value 0 and U_1 to the bit value 1. Of course there exist voltage levels somewhere in between U_0 and U_1, which requires to define a voltage range for U_0 and U_1. If a certain voltage level does not lie in the range of one of the two levels, it is not possible to assign a bit value.

The quantum mechanical equivalent to the classical bit is the so called quantum bit (qubit). A qubit requires a quantum mechanical two state system, for instance an atom with two possible energy states, a spin-1/2 particle (spin up and spin down) or the polarisation degree of freedom of a photon. Any quantum state $|\Psi\rangle$ out of such a two state system can can be described by a superposition of two arbitrary, however, linearly independent basis vectors $|\Psi_0\rangle$ and $|\Psi_1\rangle$ of the corresponding two-dimensional Hilbert space:

$$|\Psi\rangle = \alpha\,|\Psi_0\rangle + \beta\,|\Psi_1\rangle \qquad (2.1)$$

where α and β are complex probability amplitudes, which fulfil the normalisation condition: $|\alpha^2|+|\beta^2|=1$. Within this work we consider only the qubits encoded in the polarisation degree of freedom of photons. For this reason, the notation in the following refers to polarisation states.

For a two-dimensional Hilbert space, there exist three complimentary sets of basis vectors B_X, B_Y and B_Z [30], which are eigenstates to the operators σ_Z, σ_X and σ_Y respectively (see Table 2.1).

Basis	Basis states	Description
B_X	$\lvert H\rangle$	Horizontally polarized ↔
	$\lvert V\rangle$	Vertically polarized ↕
B_Y	$\lvert P\rangle=\frac{1}{\sqrt{2}}(\lvert H\rangle+\lvert V\rangle)$	Diagonally polarized ⤢
	$\lvert M\rangle=\frac{1}{\sqrt{2}}(\lvert H\rangle-\lvert V\rangle)$	Anti-diagonally polarized ⤡
B_Z	$\lvert R\rangle=\frac{1}{\sqrt{2}}(\lvert H\rangle+i\lvert V\rangle)$	Right-circularly polarized ↻
	$\lvert L\rangle=\frac{1}{\sqrt{2}}(\lvert H\rangle-i\lvert V\rangle)$	Left-circularly polarized ↺

Table 2.1.: The basis states of B_X, B_Y, B_Z and their physical meaning.

Suppose, a photon is vertically polarised, which corresponds to the quantum state $|V\rangle$. A measurement of the polarisation state is performed in the basis $B_X=\{|H\rangle,|V\rangle\}$. The probabilities to measure a vertically or horizontally polarised photon then are given by:

$$P(V)=|\langle V|V\rangle|^2=1 \tag{2.2a}$$

$$P(H)=|\langle H|V\rangle|^2=0 \tag{2.2b}$$

Both measurements are performed on eigenstates of the measurement basis and the measurement outcome is definite. If the same measurement is performed in one of the two conjugated bases, here B_Y or B_Z, the measurement results are completely undetermined. Exemplary calculations for a given state $|V\rangle$, which is measured in B_Y yields:

$$P(P)=|\langle P|V\rangle|^2=|\frac{1}{\sqrt{2}}(\langle H|+\langle V|)|V\rangle|^2=\frac{1}{2} \tag{2.3a}$$

$$P(M)=|\langle M|V\rangle|^2=|\frac{1}{\sqrt{2}}(\langle H|-\langle V|)|V\rangle|^2=\frac{1}{2} \tag{2.3b}$$

Note that after the last two measurements, the quantum states are either $|P\rangle$ or $|M\rangle$. If now a measurement is performed in B_X, the outcome is also uncorrelated, despite the fact that the original states were eigenstates of B_X.

2.2.2.2. No-cloning theorem

Essential for the security of QKD is that an attacker cannot clone, i.e., build an exact copy of an unknown quantum state, which is proven by the No-cloning theorem. More precisely, there exists no unitary operator U such that:

$$U|\Psi\rangle \otimes |0\rangle = |\Psi\rangle \otimes |\Psi\rangle \tag{2.4}$$

where $|\Psi\rangle$ is an arbitrary and $|0\rangle$ a blank quantum state. A possible proof of the theorem uses the linearity of quantum mechanics and was first done by W. K. Wootters and W. H. Zurek in 1982 [31].

2.2.3. QKD protocols

In the following, a short overview of the three families of QKD protocols is given. Within this project, the well known BB84 protocol is implemented experimentally. For this reason, the procedure of the BB84 protocol as well as security aspects are presented. The decoy state method, which can be seen as a protocol extension, solves problems caused by the usage of attenuated lasers instead of real single photon sources and is shown in the third part of this section.

2.2.3.1. Three families of QKD protocols

There exist a huge number of different QKD protocols[1] and they can be divided into three families [2]: Discrete-variable coding (DVC), continuous-variable coding (CVC) and distributed-phase-reference (DPR) coding. The main difference lies in their detection method. While DVC and DPR are photon counting methods, for CVC, the light-field quadratures are analysed.

The first protocol for QKD was the so called BB84 protocol, proposed by Charles H. Bennett and Gilles Brassard in 1984 [10]. It belongs to the family of DVC protocols, where in general every key character is related to a single qubit. DVC protocols are still the most popular ones, as BB84-like protocols (e.g. SARG04 [32], Six-state protocol [33]) are comparatively easy to implement with attenuated lasers. Here, different degrees of freedoms (DOF) of photons are used for encoding, basically depending whether the QKD system is designed with optical fibres (DOF: time coding, frequency coding and others) or a free-space link (DOF: polarisation). There also exists protocols, which use entangled states [34]. By implementing these protocols, the distance may further be increased (>200 km), as higher channel losses can be tolerated [3].

For DPR protocols [35], the information is encoded in the phase between photon pulses. The signal is analysed at Bob's side by a Mach-Zehnder interferometer and two single photon detectors. So far, these protocols only have been demonstrated for distances below 100 km [3].

[1] As this section should just give a small overview, only the first publication, which touched the respective topic is cited. For further information see the reviews [1–3].

By implementing CVC protocols [36], the light-field quadratures become modulated by Alice and analysed by Bob, using homodyne or heterodyne detection methods. The great advantage of CVC protocols is that they do not require single photon detectors and can be realised with standard telecom components promising higher speed [3].

2.2.3.2. BB84 protocol - Procedure and security aspects

In the BB84 protocol, Alice sends a random sequence of quantum states, which are encoded in a certain DOF of single photons, originally the polarisation, via a quantum channel to Bob. The single photons have to be indistinguishable in all other DOFs. Beside the quantum channel, there exists a public classical channel for the post processing. Generally, both channels have to be authenticated. Alice and Bob agree on the two complementary bases $B_X = \{|H\rangle, |V\rangle\}$ and $B_Y = \{|P\rangle, |M\rangle\}$ for linear polarised light and declare the bit values 0 and 1 to the four polarisation states ($|H\rangle$ and $|P\rangle$: bit value 1, $|V\rangle$ and $|M\rangle$: bit value 0). Note that the assignment of the bit values must be chosen such, that the non-orthogonal states have the same bit value. With this preferences, the procedure of the protocol can start:

- Alice chooses randomly one of the four polarisation states and consecutively sends the photons over the quantum channel to Bob.
- Bob chooses randomly one of the two bases and measures the polarisation of the incoming photons.

  So far the communication between Alice and Bob only happened over the quantum channel and both parties then hold a sequence of N bits called the raw key. Note that the raw key of Alice is not the same as Bob's.
- Alice and Bob communicate over the classical channel which bases they have chosen and discard the bits where the bases are different. This process is called sifting and leads to the sifted key of length $\approx N/2$.

For a deeper analysis regarding the security of the BB84 protocol, the so called quantum bit error ratio (QBER), which is the ratio of the number of false bits to the total number of bits in the sifted key, has to be determined. Here, Alice and Bob simply analyse a small part of the sifted key, where they compare their bit values. By performing an error correction and the privacy amplification (see Section 2.2.4), the so called secret key can be distilled from the sifted key. A theoretical limit for the achievable secure key rate $R_{sec-max}$ after the privacy amplification step is given by [37]:

$$R_{sec-max} = R_{sifted} \times \mathrm{MAX}[1 - 2H_2(E), 0] \tag{2.5}$$

where R_{sifted} is the shifted key rate and $H_2(E)$ the Shannon entropy as a function of the QBER $\equiv E$, which denotes the upper bound of information an attacker may have:

$$H_2(E) = -E\log_2(E) - (1-E)\log_2(1-E) \tag{2.6}$$

Solving equation 2.5 yields that for a QBER $\geq 11\%$, $R_{sec-max} = 0$.

So far it is assumed that Alice holds a real single photon source. The experimental implementation of single photon sources within QKD experiments has already been shown [38–40]. However, the technical effort there is very high, compared to the attenuation of lasers down to the single photon regime. Laser sources exhibit a Poissonian statistics for which the probability for a n-photon pulse as a function of the mean photon number per pulse μ can be calculated:

$$P_\mu(n) = \frac{\mu^n}{n!} \mathrm{e}^{-\mu} \tag{2.7}$$

Even for $\mu \ll 1$ there exists a certain probability for pulses to contain more than one photon. The photons in one pulse carry the same information (polarisation), which allows for the powerful photon number splitting (PNS) attack. Here, Eve blocks all pulses, which contain only one photon and stores respectively one photon of the multi photon pulses for later analysis (see Section 2.2.5).

Gottesman et al. [37] analysed this problem an found a new upper bound for a secret key rate $R_{sec-GLLP}$:

$$R_{sec-GLLP} = R_{sift} \times \mathrm{MAX}\Big[(1-\Delta) - f(E)H_2(E) - (1-\Delta)H_2(\frac{E}{1-\Delta}), 0\Big] \tag{2.8}$$

where $f(E)$ denotes a correction factor (effectiveness of the error correction) and Δ is the number of tagged bits. Tagged bits could be used by Eve, as they carry the information of which basis was used for encoding. The Δ-parameter is defined as the probability of an multi photon pulse divided by the probability for a detection event at Bob's side:

$$\Delta = \frac{P_\mu(n > 1)}{\eta P_\mu(n > 0)} \tag{2.9}$$

where η denotes the overall transmission, which is given by:

$$\eta = T_{Bob}\eta_D \tag{2.10}$$

where T_{Bob} is the product of the receiver and channel transmission (see Section 4.3.4) and η_D the efficiency of the detector.

2.2.3.3. Decoy state method

In the previous Section 2.2.3.2, a solution proposed by Gottesman et al. [37] against the PNS attack (see Section 2.2.5) was shown, however, for a real QKD implementation this can lead to a strongly reduced secret key rate. Based on an idea of W.-Y. Hwang and H.-K. Lo, the decoy state method emerged [41–43], which points at the problems caused by the usage of weak laser pulses instead of real single photon sources, too. In the following, the idea of the decoy method as well as the model, which is used to calculate the secret key rate [37, 44], is presented [2].

The idea of the decoy state method is to set not only one intensity per pulse μ. During the key exchange, also decoy states with a mean photon number $\nu < \mu$ are sent by Alice. Eve does not know which of the pulses are signal or decoy states and is forced to treat them similarly when she performs a PNS attack. Here is the crucial point: Eve changes the photon number statistics differently for pulses with intensities ν and μ. But she can not do better since coherent states $|\nu\rangle$ and $|\mu\rangle$ are not orthogonal.

[2] The content of this section is closely related to a work by T. Schmitt-Manderbach [45].

After the key exchange, Alice announces, which of the pulses were signal or decoy states. An attack can be detected by simply evaluating the photon number statistics of the two groups.

In order to estimate the secret bit fraction of the exchanged key, Ma et al. [44] merges the work of Gottesman et al. [37] with the idea of the decoy state method. To do this, a model, which includes source, channel and detector is defined. The formulas concerning the channel and detector, however, are slightly modificated here, as originally proposed in [46]. This is because our project is a short range ($\sim 0.5\,\mathrm{m}$) free space application. The attenuation of air is negligible for 850 nm on this length scale. The following points show the components of the model.

• The transmittance of an i-photon state η_i:

$$\eta_i = 1 - (1-\eta)^i \tag{2.11}$$

where i stands for the number of photons in the pulse and η is the overall transmission (Equ. 2.10).

• The *Yield* Y_i of an i-photon state:

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \cong Y_0 + \eta_i \tag{2.12}$$

which denotes the probability of a detection event at the receiver in the case when an i-photon pulse is sent by the transmitter. Here, Y_0 is the background rate, including the dark counts of the detector as well as environmental influences (stray light, beacon laser).

• The *Gain* Q_μ of pulses with a mean photon number μ:

$$Q_\mu = \sum_{i=0}^{\infty} Q_i = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{2.13}$$

which is the sum over the products of the probability, that Alice sends a i-photon pulse with the probability of an detection event at Bob's side.

Finally, Ma et al. [44] worked out a formula for the secret key rate, when the decoy state method is used:

$$R_{sec-decoy} \geq q\Big[Q_1(1 - H_2(E_1)) - Q_\mu f(E_\mu)H_2(E_\mu)\Big] \tag{2.14}$$

where E_μ and E_1 are the QBERs of the signal and single photon pulses respectively and H_2 denotes the Shannon entropy (Equ. 2.6). Q_1 is the *gain* of a single photon event (Equ. 2.13). The factor q is dependent on which protocol is experimentally implemented. In the case of the BB84 protocol, $q = \frac{1}{2} \times f_{rep} \times p_\mu$, where f_{rep} is the repetition rate of the pulses and p_μ denotes the probability to send pulse with a mean photon number of μ. Note, that only the signal states (mean photon number μ) contributes to the secret key, which also implies that Q_1 is only related to this class of pulses.

At this point, also an intuitive explanation of equation 2.14 should be given. The secret key rate is given by subtracting two factors from the gain of the single photon signals Q_1. First, the amount of Eve's information on the single photon pulses, which is indicated by the QBER on these signals $(-Q_1 H_2(E_1))$. Second, the factor $-Q_\mu f(E_\mu)H_2(E_\mu)$, which is the information revealed due to the privacy amplification.

However, the needed quantities Q_1 and E_1, in order to calculate the secret key rate (Equ. 2.14), can not be determined from the data. This would not be possible even if Bob could count the number of photons in each received pulse, as it is not clear, if photons got lost during the transmission. To overcome this problem, Ma et al. [44] calculated worst case expressions Q_1^L and E_1^U, which can be determined from the data and thus be used to find a lower bound for the secret key rate.

$$Q_1^L = \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu - \nu^2}\left(Q_\nu \mathrm{e}^{\nu} - Q_\mu \mathrm{e}^{\mu}\frac{\nu^2}{\mu^2} - \frac{\mu^2-\nu^2}{\mu^2}Y_0\right) \leq Q_1 \tag{2.15}$$

$$e_1^U = \frac{E_\mu Q_\mu - \frac{1}{2}Y_0 \mathrm{e}^{-\mu}}{Q_1^L} \geq e_1 \tag{2.16}$$

Note that the last expression is only valid for the so called vacuum+weak decoy protocol, which uses two decoy intensities ($\nu_0 = 0$ and $\nu_1 = \nu < \mu$).

Compared with the GLLP results [37], where the secret key rate $R_{sec-GLLP}$ (Equ. 2.8) for QKD systems, which uses weak laser pulses, goes with $\mathrm{e}^{-2\eta}$, $R_{sec-decoy}$ is proportional to $\mathrm{e}^{-\eta}$. By implementing the decoy state method, the η-dependency is similar to the usage of a true single photon source, which can increases the extractable secret key rate drastically, especially in the case of high losses in the channel.

2.2.4. Error correction and privacy amplification

The last steps to extract the secret key out of the sifted key are the error correction and the privacy amplification. However both steps can only be made if the measured QBER is below 11%, as this is the theoretical limit at which the secret key rate $R_{sec-max} > 0$ (see Section 2.2.3.2).

The former mentioned step serves for discarding uncorrelated bits which can come for example due to dark counts of the detectors. It can be realised by error correction algorithms like Cascade [47], Winnow [48] or the low-density parity-check [49].

The amount of information which an eavesdropper may have can be deleted by the so called privacy amplification. This is realised by compressing steps where universal hash functions are used [50].

2.2.5. Attacks and side-channels

The most obvious eavesdropping strategy is the so called intercept and resend attack. Here, Eve behaves in principle like Bob and measures the intercepted photons in one of the two bases B_X or B_Y. As Eve may also performs a so called quantum non-demolition (QND) measurement, she is able to resend the same photon to Bob. Eve becomes unnoticed if she measures in the same basis as Alice sends the photon. However, if Eve measures in the conjugated basis, she modifies the quantum state such that in half of the cases Bob gets a wrong bit as the measurement results are uncorrelated after Eve's measurement (see Section 2.2.2.1). In total, Eve introduces a QBER of 25%, which is a clear sign for Alice and Bob that their communication has been eavesdropped upon. The intercept and resend attack belongs to the so called individual attacks. Here, Eve performs measurements on the exchanged signals between Alice and Bob before the classical communication.

An other, however, much more powerful attack is the so called photon number splitting (PNS) attack [51–53]. For practical reasons, attenuated lasers are often used as light source instead of real single photon sources. Lasers underlie the Poissonian statistics (Equ. 2.7) and even for small mean photon numbers per pulse $\mu \ll 1$, multi photon pulses appear. Again, Eve's capabilities are only limited by the laws of quantum mechanics, which allow her to split and store respectively one photon of the multi photon pulses, whereas she blocks every single photon pulse. This attack can be used as long as $P_\mu(n > 1) > \eta P_\mu(n = 1)$, where η is the overall transmission. As Eve knows the chosen basis of Alice and Bob, she can perform the same measurements. By doing so, she will obtain the same key as Alice and Bob without introducing any error. In Section 2.2.3, the PNS attack as well as possible control measures were already discussed.

In general, there is a gap between the theoretical security of QKD and the real systems leading to so called side-channels, which an eavesdropper may exploit. The first example for side-channels are other DOFs of the signal photons, which may contain the same information as the DOF chosen for encoding. If Eve performs a QND measurement, where the original DOF is untouched, Eve introduces no error. Many successful attacks were shown, often aiming at the device imperfections on the receiver side, which can be for example the detection efficiency mismatch (e.g. [54]), the spatial mode side channel [55], the detector dead time [56], the detector-blinding attack [57] and others [1–3]. A strategy in order to close a known side-channel is to apply the suitable control measurement, for example realised by adding different kinds of optical filters, time filtering or spatial mode filtering.

3. Sender unit “Alice”

In the first part of this chapter, the design of the sender unit Alice, which was done by G. Mélen in a former work [24, 25] is presented. The methods for setting and determining the mean photon number of Alice as well as the temporal pulse shape are shown in the second part. Moreover, the quantum state tomography (QST), for analysing the polarisation output states of Alice, is discussed, followed by the modifications on Alice, which were done during this work. The last part deals with the results of the QST for uncompensated and compensated output states of Alice.

3.1. Experimental setup - Design of the sender

The goal of this project, regarding the sender unit, is to build the optical part, for generation and preparation of optical pulses, as small as possible, in order to facilitate the integration into mobile devices.

For the experimental implementation of the BB84 protocol, four linear polarisation states $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$ are needed (see Section 2.2.3.2). This can be realised either by switching between four light sources, which emit the desired polarisation state (intrinsically polarised or in combination with a polariser filter), or by using one light source and an active polarisation switching device (e.g. an electro-optic modulator (EOM)). The former mentioned method fits better to the concept of this project referring the integration of the optical components. Furthermore, in order to reach reasonable key rates, the modulation speed must be at least on the order of some MHz. This could be realised by using an EOM, however, not for small device dimensions in combination with high extinction ratios of the polarisation states, yet. For practical reasons, weak laser pulses instead of single photon sources are used.

3.1.1. Micro optics

Figure 3.1 shows the micro optical setup of Alice. The first component is an array of four vertical-cavity surface-emitting laser diodes (VCSELs) at 850 nm with a pitch of 250 μm. An array of micro-lenses is focusing the laser beams onto the inputs of a waveguide chip. The waveguide chip, incorporating three directional couplers, serves for the spatial overlap of the four laser modes. A wire-grid-polariser (WGP) array is placed between the lenses and the waveguide chip in order to set the BB84 polarisation states. A bright visible laser at 680 nm is overlapped with the signal beam by using a dichroic beam splitter and serves for beam tracking and clock synchronisation. In order to collimate the divergent mode emerging from the waveguide chip, a small aspheric lens is glued on the dichroic beam splitter. All components were assembled on a micro optical bench with the help of a 6-axis stage and vacuum tweezers and fixed with an UV-curing glue. In the following, the components are considered in more detail.

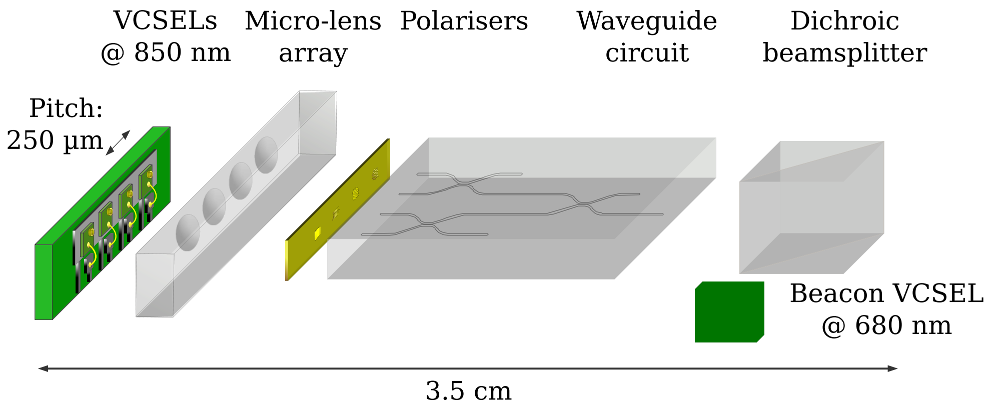


Figure 3.1.: **Overview of the micro optical setup**
The components of the micro optics are an array of VCSELs, micro-lenses and wire-grid polarisers followed by a waveguide chip. Additionally, a beacon laser is overlapped with the signal beam by a dichroic beam splitter. Not shown are the collimation lens, which is glued on the dichroic beam splitter and the beam blocker after the waveguide circuit. Taken from [25].

VCSEL array

Vertical-cavity surface-emitting laser diodes (VCSELs) are semiconductor lasers [58] produced by modern nano-fabrication methods. The cavity is built from so called distributed Bragg reflectors, which consist of many alternating layers of AlAs and GaAs, where the thickness of the single layers is one-quarter of the final emission wavelength, which is defined by the length of the cavity. The active area, which is embedded within the cavity, employs an InGaAs-GaAs quantum well. In most cases, the injection of the electric current is achieved by ohmic contacts on the top epitaxial layer and the back side of the substrate. VCSELs can be highly modulated and provide single mode operation.

For this Alice module, a 12-channel single-mode array at a wavelength of 850 nm is used. Four neighbouring diodes (pitch = 250 μm) of this array are electrically connected and can be driven with a modulation speed up to 28 GHz. The polarisation behavior in continuous-wave (CW) and pulsed regime differs strongly. In CW mode, they show a stable degree of polarisation (DOP) above 90% over the complete current range. In pulsed mode, with a pulse duration below 100 ps, the DOP is one order of magnitude lower as compared to the CW mode. This allows a subsequent setting of any linear polarisation by an array of integrated polarisers.

Polariser array

The polariser array used here consists of four wire-grid polarisers (WGPs) [24, 25, 59]. The working principle of a WGP is based on its different behavior towards the polarisation type of the incoming light field. If the polarisation direction is perpendicular to the stripes (TM, also called π or p polarisation), the coupling to surface plasmon polaritons and waveguiding effects through the slits, can lead to a so called extraordinary optical transmission (EOT) [59]. If the light field is polarised parallel to the grid (TE, also called σ or s polarised), it is mostly reflected. The penetrating light field in this case shows an exponential decay within the slits if the wavelength is above a critical value $\lambda_c \approx 2w$, where w is the slit width [24].

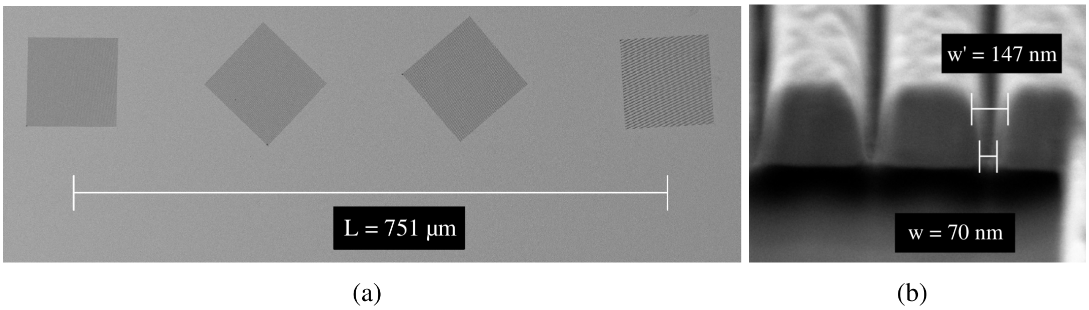


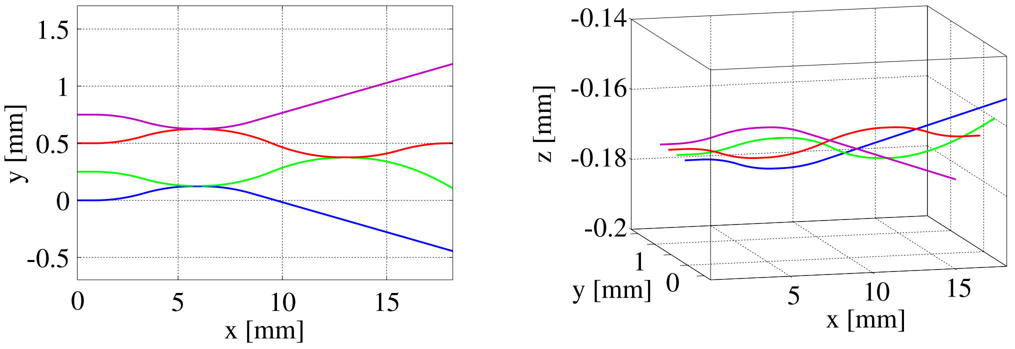
Figure 3.2.: **Wire-grid polariser array**
(a) The array consists of 4 wire-grid polarisers (WGPs) with a size of 120 μm × 120 μm each. They are separated by a distance of 250 μm. The WGPs have relative angles to each other, which should compensate for birefringence effects of the waveguides. (b) The slit width range is 70 nm - 147 nm with a period of 500 nm. Both pictures were made using a scanning electron microscope. Taken from [24].

Figure 3.2 shows the WGP array as it is used. The top material is a 265 nm thick gold layer, which is deposited by physical vapour deposition onto a glass substrate. The gratings are made via focused ion beam milling. The optimal grating parameters are found by Finite-Difference Time-Domain simulations. The achieved extinction ratio for the four WGPs is well above 1:1000.

Waveguide circuit

In order to guarantee the spatial indistinguishability of the QKD signal pulses, a waveguide circuit combines the four separated spatial modes of the four light sources into one single output. The waveguide circuit is produced by femtosecond laser writing in the group of Dr. R. Osellame at the Politecnico di Milano in Italy. This technique allows to produce single-mode waveguides with almost arbitrary geometry. By bringing two waveguides close together (in the order of a few micrometer) to allow for evanescent coupling one can produce a so called directional coupler, whose ratio is defined by the interaction length L (in the order of some hundred micrometers) [60].

Figure 3.3 shows the design of the waveguide circuit for Alice from top and perspective view. In order to reduce the polarisation dependence of the couplers, a 3D structure of the embedded waveguides is realised. The 3D structure was nevertheless believed to add small path-dependent phases. This contribution was compensated by a slight rotation of the input states prepared by the WGPs (see Figure 3.2). Three directional couplers, with a splitting ratio of 50/50, combine the four paths. One quarter of the incoming intensity at each input, is guided to the main output (see Figure 3.3, red waveguide). The propagation loss along the path is approximately 0.5 dB/cm. The waveguides exhibit a small birefringence of $\Delta n = 7 \times 10^{-5}$.



(a) Top view

(b) Perspective view

Figure 3.3.: **Waveguide circuit**
The four inputs on the left side belong to four waveguides, which are written into a glass substrate. In so called interaction zones, evanescent coupling of the light field from one waveguide into an other takes place. By employing a 3D structure, an almost polarisation independent splitting of the incoming light is achieved, where respectively one quarter of the intensity of every input is guided to the main output (red). Taken from [25].

3.1.2. Driving electronics

In order to achieve very short laser pulses (<100 ps), which is needed to drive the VCSELs in a mode where the DOP is small, a very fast driving electronics is required. The main part of the driving electronics is a circuit consisting of a dual-channel delay chip, a high-speed AND-gate and the laser driver (see Figure 3.4). The dual-channel delay chip shifts the two incoming clock signals by the delay values $d1$ and $d2$. The delayed clock signals C_{d1} and C_{d2}, are logically combined at an AND-gate as C_{d1} & $\overline{C_{d2}}$, yielding a pulse with a length of a fraction of a cycle. The intensity of the pulses is set by the levels for the bias current i_b and the modulation current i_m at the laser driver. The values i_b, m_b, $d1$ and $d2$ used for the Alice control software can be converted in SI-units for current I_{SI}[mA] and delay time d_{SI}[ps] via:

$$I_{SI} = 0.1 + \mathrm{i} \times 0.047 \text{ [mA]} \tag{3.1a}$$
$$d_{SI} = \mathrm{d} \times 5 \text{ [ps]} \tag{3.1b}$$

In order to enable a separate control of the VCSELs, four of these circuits and an additional laser driver for the beacon laser are integrated on a single printed board. A field programmable gate array (FPGA), serves for the control of the pulse parameter and is connected to a PC via USB. The repetition rate is set by a 100 MHz clock.

3.2. Temporal pulse shape and mean photon number

For every experimental implementation of QKD, the mean photon number per pulse μ of the transmitter has to be determined, as it is an important security parameter for

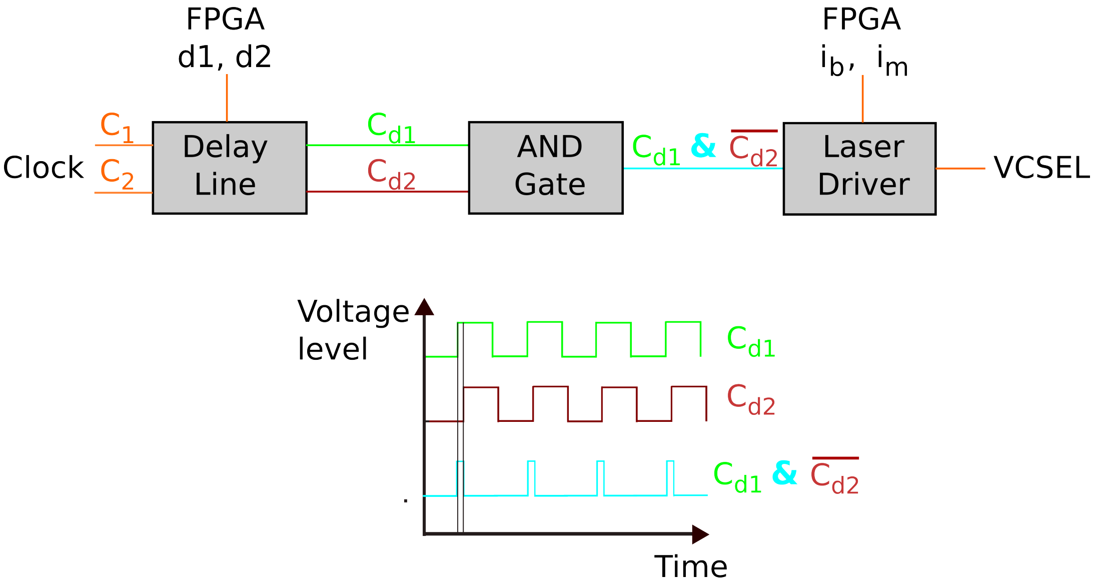


Figure 3.4.: **Driving electronics**
The main part of the driving electronics consists of a dual-channel delay chip, a high speed AND-gate and the laser driver, where the settings for the delay values (d1, d2) and currents (i_b, i_m) come from a FPGA. Adapted from [24].

the key exchange (see Section 2.2.3). Here, in order to determine μ at the output of the Alice module, the receiver APDs are used because the detection efficiency and the receiver transmission are known (see Section 4.3.4). However, before μ can be measured, the appropriate settings of the laser driver electronics, which guarantee the maximal temporal overlap of the pulses, have to be found. For this purpose, an additional fast APD is required, because the timing jitter of the receiver APDs is to high ($\sim$ 100 ps) in order to get a sufficient resolution of the pulses (FWHM $\approx$ 100 ps). The pulse duration has to be such short in order to allow a subsequently setting the polarisation of the lasers (see Section 3.1.1). The determination of μ by using only the additional APD is not possible, because of the unknown coupling efficiency.

The temporal pulse shape can be monitored by a single APD connected to an oscilloscope (Lecroy, 4 GHz). The 100 MHz clock signal from Alice serves as trigger. The resulting photon arrival times are plotted in a histogram for all four channels.

Figure 3.5 shows the pulse shape of the four channels before performing a key exchange (see Section 5). The corresponding settings for the driving electronics have to be found in several iteration steps, where the starting point is the weakest channel, here channel 1 due to ageing of the laser diode. Because of this, also the achievable μ is limited as well as the optimal alignment of the pulse shape.

In addition to the pulse shape the count rates also need to be equal, which is primary defined by their modulation level. Note that the interference filter (IF) in front of the single APD can affect the count rates differently because of a slight difference in the wavelength of the different channels.

For the final step of setting and determining μ, the receiver APDs are used. Here, only small changes of the modulation level are necessary. The expression to determine

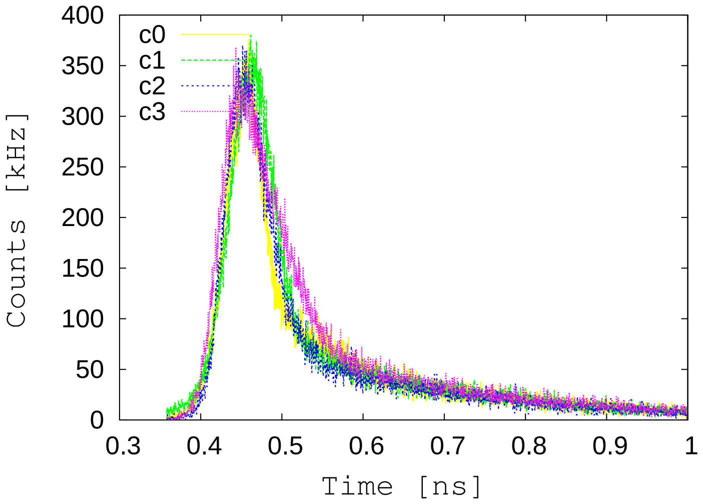


Figure 3.5.: **Temporal pulse shape of the four channels**
The four channels show a high temporal overlap. The pulse duration is 100 ps (FWHM).

μ (only valid for small μ due to the Poissonian distribution) is given by:

$$\mu = \frac{1}{\eta_{det} T_{Bob} f_{rep}} \sum_i (R_i c_i \eta_i^{rel} - R_i^{dc}) \tag{3.2}$$

where the factor in front of the sum contains the average efficiency of the detectors η_{det} (PerkinElmer DTS SPCM-AQ4C, 38%), the transmission of the receiver T_{Bob} (see Section 4.3.4, 41,3%) and the repetition frequency of the pulses f_{rep} (here $f_{rep} =$ 100 MHz). Furthermore, the sum of the four detector count rates R_i is taken ($i =$ H, V, P, M). Here, some additional factors have to be taken into account: The factor η_i^{rel}, which denotes the relative detection efficiencies of the four detectors (see Section 4.3.2) and the dark count rate R_i^{dc}. Finally, the non-linearity factor c_i of the respective detectors, which appears due to their dead time t_{dt} (here $t_{dt} = 50\,\text{ns}$), in which no further incoming photon can be detected, is calculated as:

$$c_i = \frac{1}{1 - t_{dt} R_i} \tag{3.3}$$

3.3. Quantum state tomography (QST)

In order to determine the polarisation states, which are prepared by Alice, a quantum state tomography (QST) of the four outputs is made. In the first part of this section, the general method of a QST is presented, followed by a discussion about the methods of the QST as it was performed previously. Finally, an improved procedure for the QST is shown and the measurement error is estimated.

3.3.1. Method and experimental realisation

The quantum mechanical state of a qubit, which is encoded in the polarisation degree of freedom of light, can be completely described by a Stokes vector (see Section A).

As the BB84 protocol is a discrete variable protocol, every character of the raw key is related to a single photon (if perfectly implemented). However, it is not possible to determine the Stokes components of a single photon as one has to measure the optical power after the six basis projections ($P_{H/V}$, $P_{R/L}$ and $P_{P/M}$) within one measurement. For the experimental implementation of a QST, this can be overcome by running the sender module in a mode, where one of the four polarisation states is sent continuously, i.e., many identical states are generated, while the measurement setup sets the needed projections and measures the respective optical power.

A free space silicon avalanche photo diode (APD) capable of detecting single photons with an efficiency of 10% (PDM series from MPD, size of active area: 50 μm, resolution: 30 ps) serves as detector. Because the number of photons per unit of time N is directly proportional to the optical power of a laser beam, the usage of an APD for single photon counting is justified. The choice of a single photon detector is motivated by the opportunity to analyse the sender in the operation mode of the QKD scenario, where the mean photon number per pulse μ is on the order of 0.05 to 0.5 (depending on different protocol parameter, see Section 2.2.3 and 5). Moreover, the usage of a standard optical power meter is not possible, because the reachable optical power of Alice in highest CW mode is on the order of some nW or less. There are basically three reasons why the optical power of Alice is so low and also differs for the channel pairs 0(V)/1(M) and 2(P)/3(H). Firstly, for the assembly of the micro optics, the light of the VCSEL's has to be coupled simultaneously into the four waveguides leading to slightly varying coupling efficiencies. Secondly, the VCSELs have a DOP of above 90% in CW mode (see Sections 3.1.1). In particular for channel 0, this leads to a strong extinction of the output polarisation. Last, channel 1 is occasionally not working correctly due to ageing, which can not be repaired without a complete disassembling of the micro optics.

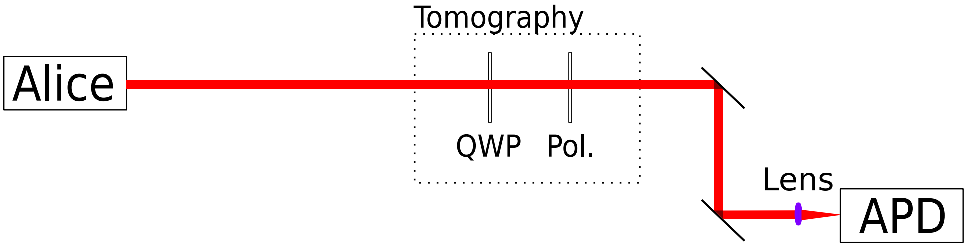


Figure 3.6.: **Scheme of the experimental setup for the QST with a single APD**
The setting of the projections are made by a quarter wave plate (QWP) and a linear polariser. The photons are detected by an avalanche photo diode (APD).

Figure 3.6 shows the schematic of the experimental setup for performing the QST. The tomography part consists of a quarter wave plate (QWP) and a linear polariser. The two components serve for the setting of the needed projections, in order to determine the Stokes components. After the linear polariser there are two mirrors for coupling into the APD. A lens is mounted in front of the APD in order to focus the incoming beam onto the active area of the APD. As shown in the next Sections 3.3.2 and 3.3.3, it is necessary to guarantee a precise and also fast setting of the angles of the tomography components. Therefore, the wave plates and the polariser are mounted in motorised rotation stages (DRTM series from OWIS, resolution: 4800 steps/90°), which are controlled via a computer. For performing a QST, one has to run a script, which basically performs the following actions:

- A channel of the sender module is activated (pulsed QKD scenario settings).
- The step motors set the projections (H $\rightarrow$ V $\rightarrow$ R $\rightarrow$ L $\rightarrow$ P $\rightarrow$ M) one after another (see Table 3.1).
- When the step motors reach the wanted positions, the count rate of the APD is recorded (integration time = 1 s) and stored into a file.
- After all projections are made for one channel, this channel is disabled and the next channel is activated.

The script stops when each of the four channels of the sender module have been analysed. In the last step of the QST, an additional script reads the file and displays the Stokes components (Equ. A.1) of the measured channels. The QBER for the four channels can be directly calculated from the Stokes components S_1, S_2 and S_3 with [26]:

$$\mathrm{QBER}_{H/V} = \frac{1 \mp S_1}{2},\ \mathrm{QBER}_{P/M} = \frac{1 \mp S_2}{2},\ \mathrm{QBER}_{R/L} = \frac{1 \mp S_3}{2} \tag{3.4}$$

Table 3.1 shows the angles of the polariser and the QWP, which are used here, in order to set the six basis projections. The order of the projections is chosen such that a minimal number of motor activity is required.

Projection	H	V	R	L	P	M
QWP	0°	0°	0°	0°	+45°	+45°
Polariser	0°	90°	+45°	-45°	+45°	-45°

Table 3.1.: **Settings for the QST angles**
The angles for the different projections are sent to the motorised rotation stages. In order to rotate the stage by a relative angle of 90°, the motor has to make 4800 steps.

3.3.2. Discussion of the previously performed QST

The first QST of the Alice module [24, 26] after the assembly of the micro optics showed a high average QBER of 8.53% for the polarisation states (see Table 3.2). The four channels, especially channel 2, have a strong circular component, which can

Channel	0 (V)	1 (M)	2 (P)	3 (H)
S_1	-0.869	-0.198	-0.468	0.920
S_2	-0.362	-0.841	0.688	0.174
S_3	0.226	0.462	-0.516	-0.281
DOP	0.968	0.980	0.979	0.978
QBER	6.55%	7.95%	15.60%	4.00%

Table 3.2.: **Former QST results of Alice module**
Results of the QST after assembling the micro optics of the Alice module [24, 26]. The average QBER is 8.53%.

not be explained by the birefringence of the waveguide and the beam splitter only.

There are several reasons for these results, which can be either assigned to intrinsic properties of the sender module (see Section 3.4) or also to the method of the QST at that time. However, it is hard to distinguish, which effects contribute at which time due to varying conditions, e.g. the change of the beam block position behind the waveguide chip, which causes a varying coupling of stray light or light from other channels into the QST APD (see Section 3.4.1), or the exchange of waveplates for the QST. Nevertheless there are some critical points in the former realisation of the QST, which affect the measurement outcome as well as the reproducibility:

- Some steps of the QST procedure were executed manually, e.g. the activating and disabling of the four channels between the projection measurements. This leads to varying cycle times, which could affect the reproducibility. Furthermore, a completely automatised procedure script facilitates a long-term QST, where a large number of complete QST cycles can be made. This would give the possibility to detect instabilities or drifts of the polarisation states (see Section 3.4.2).
- For setting the six projections, the tomography components need to be rotated. However, this leads to a displacement of the transmitted beam due to small tilts of the components relative to the rotation axis. Due to the small size of the active area of the used APD (50 μm), the coupling into the APD varies, depending on the position of the polariser and the QWP, which can lead to inconsistent measurements of the Stokes components. To overcome this, one has to ensure the maximal coupling for every position before the execution of the QST procedure (see Section 3.3.3).
- The former QST sequence measures the six projections one after another. The integration time per projection was 10 s. A complete QST cycle required 4 min plus the time for the manually switch of the channels. The laser intensity of the Alice module can vary up to 10% within minutes (Figure 3.7). This leads to inconsistent results, especially, when the intensity varies between the measurement within a basis pair. A solution to overcome this are alternating short-term measurements of the single projections (see Section 3.3.3).

3.3.3. Improvements of the QST procedure

As discussed in the previous section, the previously used QST procedure had some critical flaws, which affect the measurement outcomes and the reproducibility. In the following, the effects on the QST due to the displacement of the beam caused by the rotation of the step motors as well as a solution to overcome this problem are shown. Furthermore, a new QST sequence, which is less sensitive to fluctuating intensity, and additionally enables a long-term QST, is presented.

Beam displacement during QST

During the QST, the QWP and the linear polariser are rotated in order to set the six projections H, V, P, M, R and L. The alignment of the QWP and polariser is performed such that the incoming beam overlaps with the beam which is reflected at the optical components. This ensures that the facets of the components are orthogonal to the incoming beam. However, the components can not always be mounted such that the rotational axis is not tilted. This leads to a displacement of the incoming beam depending on the angle of rotation. As the size of the active area of the used APD is very small (50 μm), also the tolerance to the beam displacement is small. Empirically, in the case of ideal focusing and coupling, the size of the tolerance region was found to be approximately twice the diameter of the beam size at the place of the active area of the APD. Therefore, even small deviations of the beam can lead to six different coupling efficiencies. In the worst case, the coupling can drop to zero. Note that for analysing the measurement data, the value for the coupling efficiency does not need to be known, but is supposed to be constant. In the end, this can lead to inconsistent or even not physical results (DOP > 1) as well as not reproducible results in particular when the setup has changed (realignment or the change of components). Checking the coupling manually for every projection setting would not be practical. Nevertheless, by taking attention of the following points, the setup can be arranged in a way that the displacement of the beam does not affect the QST results:

- It is necessary to arrange the components of the setup very close to each other, in order to keep the absolute deviation of the beam small.
- The alignment of the motorised rotation stages is done best while they are continuously rotating. Then a position can be found, where the beam reflection is moving circularly around the incoming beam. In this position, the relative deviation of the beam is the same for every rotation angle. Furthermore, the arrangement of the setup, is better reproducible.
- Before a QST and at every point, the coupling has to be checked for each setting individually. One starts at the first setting and checks whether it is possible to reach a higher coupling by tilting the mirrors. Here, it is essential, that the initial position of the mirrors is restored after every check of the coupling. Only if it’s not possible to increase the coupling at one of the six settings, a constant coupling efficiency can be assumed. If there are projections, where the coupling can be improved, a realignment of the setup is necessary. Of course, this method assumes an ideal coupling before the start of the test.

New QST procedure

As discussed in Section 3.3.2, the former QST procedure has to be improved in order to get correct and reproducible results. Additionally, the QST procedure should run completely automatised to get stable cycle times and the possibility of a long-term QST. Whereas the last point is basically only an extension of the existing QST procedure, the problem of the fluctuating laser intensities requires a different approach for it.

Figure 3.7 shows the measured optical light power of channel 2 running in CW mode over a measurement time of 50 min. Power fluctuations up to 10% around the mean value are detected, which were also occupied for the other channels and in pulsed mode too. However, for the analysis of the measurement data, a constant laser intensity is assumed. This problem affects the QST in the same way as the deviation of the laser beam (see Section 3.3.3). Basically, it can be overcome by measuring a reference intensity, using a second APD and an additional beam splitter

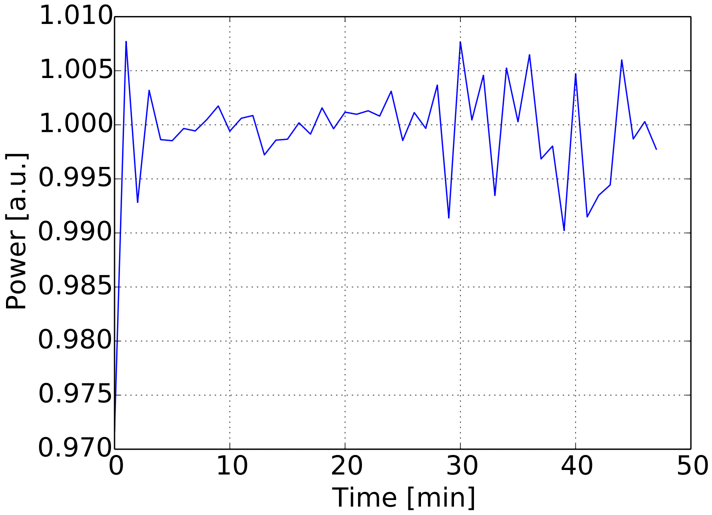


Figure 3.7.: **Optical power fluctuations of the Alice module**
The optical light power as a function of time for channel 2 running in CW mode ($i_b = 20$) for a measurement time of 50 min. After the laser diode is turned on, the optical light power increases within the first minutes and shows then a instability up to 10%.

(BS), which is placed between the sender and the tomography components. The BS must be characterised in order to determine the additional phase shift caused by the birefringence and the polarisation dependence. However, due to the low detection efficiency of 10% of the used APD for the QST, an additional attenuation of the beam would lead to very low count rates, with the consequence of a higher uncertainty. Of course, the problem of the lower statistics can be overcome by increasing the measurement time. However, a complete QST cycle should take only some minutes to be able to analyse possible short-term changes of the polarisation states. Especially this argument justifies a new QST procedure. Besides that, the new QST procedure does not require an extension of the existing setup (see Figure 3.6). It looks as follows:

- A channel of the sender module is activated (pulsed QKD scenario settings).
- The count rates for the first projection pair H/V are recorded. For this, H and V are set alternately. When the corresponding step motor reaches the wanted position, the count rate of the APD (integration time: 1 s) is stored into a file. Note, that for analysing a projection pair, only one motor has to rotate.
- After five cycles of alternation, the procedure is repeated for the remaining projection pairs R/L and P/M.
- After all projections are made for one channel, this channel is disabled and the next channel is activated.

The new analysis script implements a linear approximation for the drift of the optical laser power. To do this, the mean values of the next neighbouring projections are calculated. The run time for one complete QST cycle (all four channels) takes approximately 2 minutes. Note that here the hysteresis of the step motors is also taken into account by using the same direction of the rotation to the measuring position. An additional timing script serves for a continuous repetition of the QST sequence. This enables a long-term QST by which possible drifts of the polarisation states can be detected (see Section 3.4.2).

3.3.4. QST error estimation

In order to estimate the error of the QST, a test tomography of a polarising filter, which is placed between Alice and the tomography components is performed for the projections H, V, P, and M (see Table 3.3).

	H	V	P	M
S_1	0.9994(5)	-0.9999(4)	0.025(4)	-0.022(3)
S_2	-0.026(4)	0.016(5)	0.9992(5)	-0.9992(5)
S_3	0.006(6)	-0.013(6)	-0.004(7)	0.006(7)
DOP	0.9994(4)	1.0001(3)	0.9995(4)	0.9995(4)

Table 3.3.: **Results for a test QST of a polarising filter**
The Stokes components S_1, S_2 and S_3 as well as the DOP for the projections H, V, P and M. The values in parenthesis denotes the measurement error of the last given digit.

By assuming a Poisson-distributed error, the uncertainty of the measurement can be estimated by the root of the total count rate. The measurement results confirm a excellent reconstruction of the settled projections. From the Stokes components follows that the average angle difference to the setted angles (0°, -45°, +45°, 90°) is below 1.5° in laboratory frame, which is approximately the precision by which the angle of the polarising filter can be adjusted by hand.

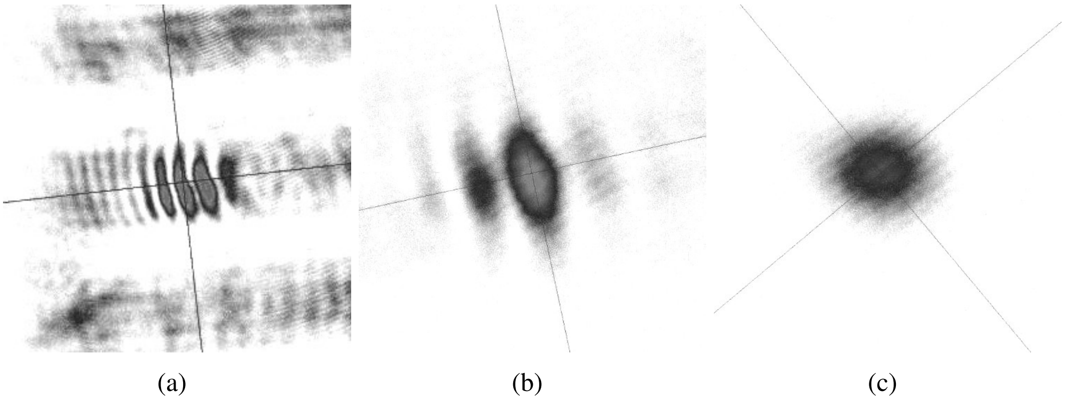
3.4. Modifications of Alice

The first results of the QST of the Alice output states after the assembly (see Section 3.3.2) showed an unexpected huge discrepancy to ideal the BB84 states. Furthermore, there was a large scatter of the results between different measurements. This can be caused either by intrinsic properties of the sender or by a failure of the characterisation method. A clear separation, however, is not always possible as both effects can appear at the same time within one measurement. For example, if the polarisation states show a certain instability, this could be wrongly interpreted as a problem of the measuring method and vice versa.

In the following, modifications of the Alice module, which were done during this work, are shown. The first part describes the insertion of an additional beam block into the micro optics for minimizing the stray-light in the main output of the waveguide circuit. Secondly, based on the results of the new characterisation methods (see Section 3.3.3), the stability of the output states could be improved.

3.4.1. Additional beam block after waveguide chip

The waveguide chip has four entrance and output facets, respectively. Whereas all four inputs are needed, only one output of the waveguide chip serves as signal output (see Figure 3.3, red waveguide), which makes it necessary to block the three remaining outputs. Furthermore the amount of stray-light (light which is not coupled into a waveguide and penetrates the glass substrate of the waveguide circuit) has to be minimised, too. Therefore, a blocker (Kodak filter foil, both sides painted with a Edding33 pen, slit width $\approx 200\,\mu$m) was positioned directly after the waveguide chip [26], in order to block the stray-light and the three outputs, which are not needed.


(a)

(b)

(c)

Figure 3.8.: **Transversal mode of Alice**
(a) The transversal mode at a distance of 20 cm behind Alice without an additional beam block. The mode shows a strong modulation caused by stray-light (dark bars) (b) Distance: 60 cm, without additional beam block. The mode is still modulated, despite less stray-light at a larger distance. (c) Distance: 60 cm, with additional beam block. The transversal mode shows no modulation.

To investigate the profile of the Alice main output beam, a CCD camera and a Laptop with an according camera software, which also offers a live picture mode is used. Figure 3.8 (a) shows the strongly modulated transversal mode at a distance of 20 cm behind Alice, mostly caused by the stray light, which can be clearly seen as dark bars. At a distance of 60 cm behind Alice, almost no stray light could be seen by the camera as the stray light is strongly divergent, however, the mode was still modulated (see Figure 3.8 (b)).

A first test investigating whether the modulation is depending on an additional light block was performed by using a sharp knife, which was mounted on a 3-axis stage. The test confirmed the assumption that the existing beam block does not remove all of the unwanted light as a position for the knife could be found directly behind the waveguide, where the modulation vanishes (see Figure 3.8 (c)).

At the very end of this work it was found, that the fixation of the first beam block was not optimal, which lead to a displacement some weeks or month after the assembly of the Alice module. This was not clear at that time where the problem of the modulated mode was analysed. This leads to a solution where an additional beam block was positioned directly behind the existing one. As all measurements presented in this work were performed in the configuration with an additional blocker, the procedure of inserting it is shortly explained in the following.

With the help of a tweezer mounted on a 3-axis stage, a small metal sheet (thickness = $100\,\mu$m) was placed directly after the existing beam block. A two component glue (2K-Stabilit Express, Patex) served for the fixation. The glue used for the assembly

(OP-67-LS, Dymax) of Alice is not suitable because it requires UV-curing, and an additional exposure of the micro optics could lead to stress effects due to post curing of the existing bonds. Some glue was applied at the bottom of the beam block and also at the ground plate of the micro optical bench. By monitoring the transversal mode, using the live picture mode of the camera, the ideal position of the beam block could be found, when the mode picture showed no modulation and also no diffraction effects (see Fig. 3.8 (c)). The tweezer fixed the metal blocker until the glue was completely cured, which took 20-30 minutes. The additional blocker also leads to an improvement of the four output states, which is discussed in Section 3.6.

3.4.2. Polarisation stability of the output states

At a certain point during this work, not reproducible results of QST measurements lead to the assumption, that the polarisation states of the Alice module were not stable. As the QST methods are well understood and controlled (see Section 3.3), their contribution to the error is small. For this reason, a long-term QST (receiver APDs (see Section 4.4)) was performed in order to observe the signal states of Alice.

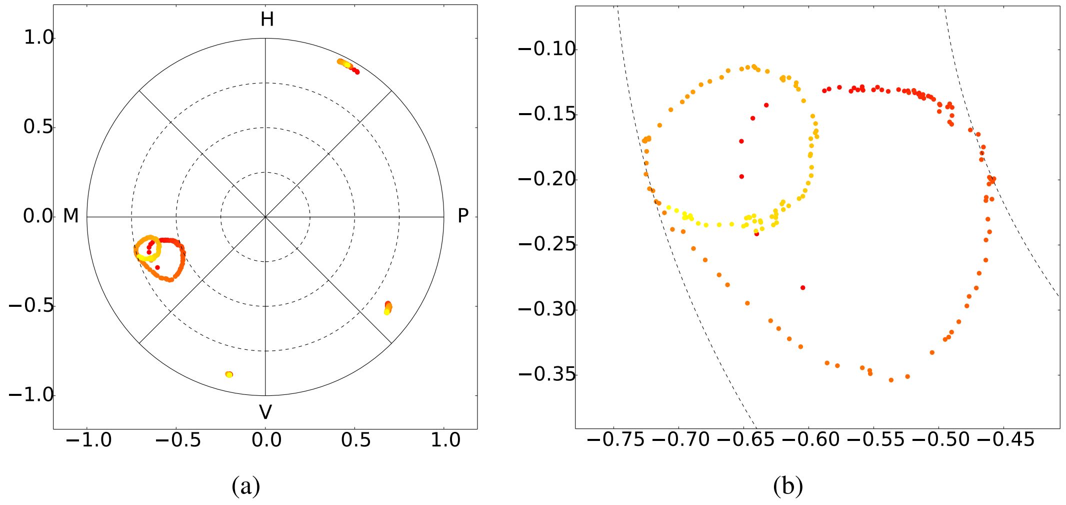


Figure 3.9.: **Long-term QST**
(a) Projection of the four measured signal states of the Alice module onto the equatorial plane of the Poincaré sphere. The overall measurement time is 10 h. The sequence for one data point takes approximately 2 min. The timeline goes from the red to the yellow points. (b) Zoom showing the evolution of the P-state.

Figure 3.9 shows the projection of the measured output states onto the equatorial plane of the Poincaré sphere for a long-term QST over 10 h. A single QST sequence took approximately two minutes and was continuously repeated. The timeline goes from the red points to the yellow ones. The first data point was taken directly after the Alice module was switched on. It can be clearly seen, that especially two states (H, M) show a strong and continuous drift. Concerning the P-state, the drift within the first 15 min after Alice is turned on, is faster compared to the following time period. However, fast drifts occur during the whole measurement time and there are no periods where the polarisation is stable for a longer time.

A possible reason for this effect might be the temperature dependence of the Alice module. To investigate this, a thermistor was placed close to the waveguide circuit, as this component is critical for the polarisation of the output states and its temperature dependence was not analysed, yet. Additionally, various types of ventilation scenarios of Alice (fans on/off, mask openings of the casing) were tried. It was found, that the temperature near the optical bench is constant (resolution 1 K) over time, independently of the type of ventilation. The QST measurements for the various ventilation scenarios also show a drift, especially for the P-state despite the temperature appears stable within 1 K.

So far, the QST method using the receiver detectors, was applied (see Section 4.4). However, with this method, only an incomplete QST can be perfomed with no information about the degree of polarisation (DOP). For this reason, an additional long-term QST was performed, by using the single APD method (3.3.3). It was found, that besides the drift of the polarisation states, the DOP of the drifting channels was lower than the DOP of the stable ones (∼90% vs. ∼99%). This can be explained by electrical crosstalk. During the QST only one channel should be activated, however, the decreased DOP indicates one or more incoherent light sources, which are emitting during the QST. A first test, where the driving electronics was exchanged, confirmed this suspicion. A long-term QST over several hours showed stable polarisation states at a DOP of approximately 99% for all channels after the exchange of the driving electronics.

The observed instability, however, is still not fully understood and further analysis is required. Especially, the fact that only two polarisation states show a drift, when the old driving electronics is used, is difficult to explain. A temperature dependence of the waveguide circuit should affect all channels as the waveguides are embedded in the same glass substrate, which could not be observed. Nevertheless, for the next version of the Alice module, the temperature dependence of the waveguide circuit has to be analysed with a higher resolution and possibly a temperature stabilisation of the critical components has to be implemented.

3.5. Compensation of output states

As shown in Section A, any unitary transformation can be realised by three wave plates, which are aligned in a row (QWP, QWP, HWP). This can be used in order to compensate for phase shifts, which occur due to the birefringence of optical components. In the case of Alice, two components behind the polariser array are birefringent and hence influencing the initial polarisation states. The waveguide chip induces a global phase close to 3π and the dichroic beam splitter a global phase of $-\pi/5$ [26]. Besides the global phase, the separated waveguide paths can show a certain polarisation, and therefore state dependency, which is expected to be small due to the 3D structure of the wave guides [25]. Furthermore, a compensation step can aim at any device imperfections for example caused by miscalculations for optical components, manufacturing errors and others, in order to improve the performance of the QKD device.

The compensation of the polarisation states can be described with the Mueller calculus (see Section A) and looks as follows:

$$\begin{aligned} S_F^i &= M_{comp}(\alpha, \beta, \gamma) S_I^i \\ &= M_{\frac{\lambda}{2}}(\gamma) M_{\frac{\lambda}{4}}(\beta) M_{\frac{\lambda}{4}}(\alpha) S_I^i \end{aligned} \tag{3.5}$$

where S_F^i and S_I^i are the four (i = channel 0 - 3) final and initial states of Alice respectively and M denotes the Mueller matrices of the wave plates, which are functions of the three Euler angles α, β and γ. In order to perform a compensation of the initial states, angles have to be found for which the average QBER of S_F^i is minimal. This is realised here by a Python script, which searches for a global minimum of equation 3.5. Note that the resulting compensation angles are a compromise for all four states as only one transformation is possible for all states at the same time. Therefore, especially relative angles of the four output states to each other can be a problem if they are too large.

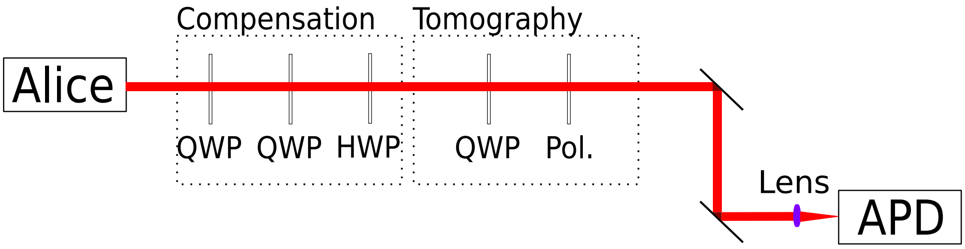


Figure 3.10.: **Experimental setup for the compensation of polarisation states** Three wave plates (1 × HWP and 2 × QWP) are aligned in a row in order to perform a unitary transformation. The calculated angles for compensation of the output state of Alice can be tested by performing a QST (see Section 3.6).

Figure 3.10 shows the setup for testing the calculated angles. The tomography setup (see Section 3.6) is extended by the three wave plates, which are also mounted in motorised rotation stages in order to enable a precise setting of the compensation angles. Due to the usage of high quality wave plates (B. Halle, quartz zero order) with extinction ratios of 1:5000 between crossed polarisers with higher extinction ratio, the error is negligible.

3.6. Results QST and compensation

In the following, the results of the QST (improved procedure, see Section 3.3.3) of the uncompensated and compensated output states after the modifications of Alice (see Section 3.4) are presented. The control parameter of Alice (repetition rate of the pulses, modulation, laser bias) during the QST are similar to the ones under key exchange conditions.

Table 3.4 [1] shows the QST measurement results of the four uncompensated output states of Alice. By comparing with the former results (see Section 3.3.2), the QBER could be improved from 8.53% to 3.21%.

Figure 3.11 shows the polarisation states visualised on the Poincaré sphere. All

[1] Data from: 2016-05-24, reproduced on the following day.

	ch 0 (V)	ch 1 (M)	ch 2 (P)	ch 3 (H)
S_{I1}	-0.9090(6)	-0.358(1)	0.091(1)	0.9460(5)
S_{I2}	0.284(1)	-0.9156(4)	0.9730(3)	-0.291(1)
S_{I3}	-0.295(1)	0.085(1)	-0.066(1)	0.070(1)
DOP	0.9968(7)	0.9867(6)	0.9795(3)	0.9922(6)
QBER	4.55(3)%	4.22(2)%	1.35(1)%	2.70(2)%

Table 3.4.: **QST Alice output states - uncompensated**
The Stokes components S_{I1}, S_{I2} and S_{I3}, the DOP and the QBER of the four uncompensated output states of Alice. The average QBER is 3.21±0.01%.

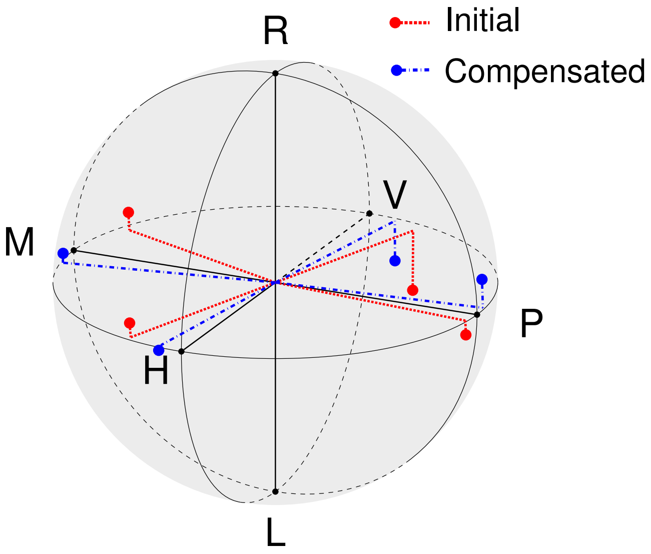


Figure 3.11.: **The output states of Alice**
The four polarisation states, which are generated by the Alice sender module. Red: uncompensated, Blue: compensated The corresponding Stokes components are given in Table 3.4 and 3.5, respectively.

four states are slightly rotated in the equatorial plane and the channel 0 (V) shows a comparatively strong circular component.

The average QBER of 3.21% would allow a key exchange, however, a smaller QBER would increase the achievable secret key rate for QKD (see Section 2.2.3). For this reason, a compensation of the output states (see Section 3.5) is tested. Calculations have shown that the measured states (see Table 3.4) can be compensated either by the usage of three wave plates (2 × QWP, 1 × HWP) or only two wave plates (2 × QWP) without a difference in the resulting average QBER, wherefore the second mentioned is chosen for the test.

Table 3.5 shows the results for the calculated Stokes components (S_{F_c}) as well as the measured ones (S_{F_m}) for the four channels of Alice by performing a compensation. The settings for the waveplate angles are (fast axis horizontal): $\alpha = 72.68°$, $\beta = 169.62°$, $\gamma = 0°$ (no HWP used). The calculated average QBER is 1.04%, however, the measured one is slightly higher at 1.48±0.01%. The discrepancy between measured and calculated results is comparatively small, however, not within the cal-

	ch 0 (V)	ch 1 (M)	ch 2 (P)	ch 3 (H)
S_{F1_c}	-0.992	-0.114	-0.147	0.978
S_{F2_c}	0.073	-0.980	0.967	-0.051
S_{F3_c}	-0.068	0.029	0.051	-0.158
QBER	0.40%	1.00%	1.65%	1.1%
S_{F1_m}	-0.9876(2)	-0.167(1)	-0.092(1)	0.9876(2)
S_{F2_m}	0.122(1)	-0.9709(3)	0.9570(3)	-0.122(1)
S_{F3_m}	-0.196(1)	0.044(1)	-0.132(1)	-0.020(1)
DOP	0.9952(7)	0.9867(6)	0.9704(3)	0.9953(2)
QBER	1.71(1)%	1.45(1)%	2.15(2)%	0.62(1)%

Table 3.5.: **QST Alice output states - compensated**
The Stokes components S_{F1}, S_{IF2} and S_{F3}, and the QBER of the four compensated output states of Alice - calculated (c) and measured (m). The measured average QBER is 1.48±0.01%.

culated error margin. Most probable the reason therefore are miscalculated compensation angles or still a failure in the QST procedure.

The performed compensation is visualised in Figure 3.11. Except for channel 2 (P), the compensated states are all closer to the ideal BB84 states as uncompensated. Despite the small gap between the calculated and the measured states, the compensated states with an average QBER of 1.48±0.01% enables promising possibilities for the further QKD experiment.

4. Receiver “Bob”

In the first part of this chapter, the receiver, which was designed in a former work by T. Vogl [26, 61, 62], is presented. The second section deals with the improvements of the receiver, which were done during this work. Furthermore, the methods and results of the characterisation measurements are presented. The receiver allows to perform a QST of polarisation states, which is explained in the fourth section. Finally, the compensation of signal states for QKD performed by the receiver is discussed.

4.1. Experimental setup - Design of the receiver

The purpose of the receiver unit is to facilitate the detection and analysis of weak laser pulses, sent by the transmitter, for a freespace QKD application (operating distance about 0.5 m), in the case where the transmitter is held by the user. The main part of the receiver is a polarisation analysis unit (PAU). In order to achieve a user-friendly operation, the receiver is complemented by a beam tracking and basis alignment system. Here, the misalignment due to the motion of the hand during the key exchange is compensated by measuring the direction of the beacon beam emitted by the sender. The synchronisation of the transmitter and receiver clocks is achieved by modulating the beacon beam. Figure 4.1 shows the complete receiver setup, which is explained in detail in the following.

4.1.1. Polarisation analysis unit

The polarisation analysis unit, which serves for the detection and analysis of the QKD signals is an arrangement of a 50/50 beam splitter (BS), two polarising beam splitters (PBSs), one half wave plate (HWP) and four fibre coupled avalanche photo diodes (APDs, PerkinElmer DTS SPCM-AQ4C), as shown in Figure 4.1. The 50/50 BS serves for a passive random choice of the measurement basis. A reflection of an incoming photon at the BS corresponds to a measurement in the H/V basis. The PBS in this path is oriented such, that horizontally polarised light is transmitted and vertically polarised light is reflected. In the ideal case, a horizontally polarised photon causes a click in detector 1 with a probability of 100% whereas the probability, to get a click of detector 3, is zero. In the case of a P or M polarised photon, both detectors in this path click with equal probability. If the incoming light is transmitted at the 50/50 BS, it passes a HWP. The angle of the optical axis of the HWP to the vertical axis is 22.5°, which leads to a rotation of linear polarised light in the horizontal plane of the Poincaré sphere of 90° (45° in laboratory frame). In other words, the reference frame in this path is rotated, which corresponds to a measurement in the P/M basis. The detection in this path works the same way as just explained for the H/V path.

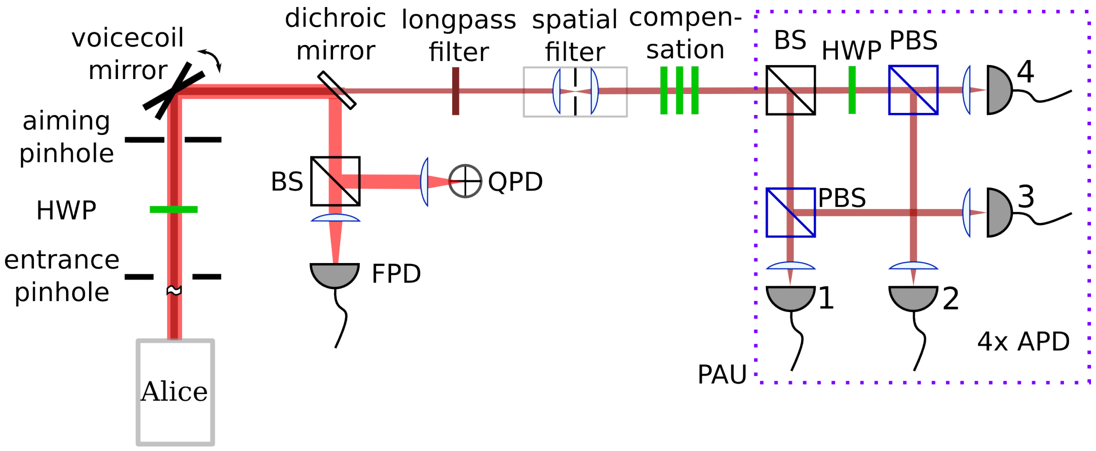


Figure 4.1.: **Receiver setup “Bob”**
A widely open iris defines the entrance area. During the hand-held operation one has to aim at the second pinhole. A HWP allows for alignment of the reference frames. A voicecoil mirror and a quadrant photo diode (QPD) serve for beam tracking and controlling. A dichroic mirror separates the signal from the beacon beam. For synchronisation, a fast photo diode (FPD) detects the modulated beacon beam. A longpass filter reduces the background radiation. A possible spatial mode side channel is closed by a spatial filter. Three wave plates (2×QWP, 1×HWP) in a row serves for the compensation of the polarisation states. The parts from the first beam splitter (BS) up to the four avalanche photo diodes (APDs) build the polarisation analysis unit (PAU). Adapted from [26].

4.1.2. Beam tracking and basis alignment

The security of a free space implementation can be compromised by the so called spatial mode side channel, exploiting the spatial mode dependency of the detection efficiencies [55]. To overcome this problem, an angle restriction of the incoming beam has to be made using a spatial filter, realised by a pinhole (diameter = 30 μm), which is placed between two lenses (f = 11 mm). The resulting acceptance range of the receiver is only ±0.08°. The coupling into receiver would drop drastically in a hand-held scenario, due to the movement of the users hand, without an efficient beam tracking and control system. This is realised by using a quadrant photo diode (QPD) and an electrically controllable voicecoil mirror. The beacon beam of the Alice module is separated from the signal beam by a dichroic mirror in front of the spatial mode filter and is focused onto the QPD. Under the initial conditions, the focus point lies in between the four active areas of the QPD and the respectively detected intensities are equal. In this case, the voicecoil mirror is at its zero position and the signal beam is optimally coupled through the spatial mode filter. A tilt of the incident beam leads to a shift in the intensity distribution at the QPD, from which the control parameters of the voicecoil mirror are calculated. The voicecoil mirror can compensate for the beam tilting by a range of ±3°. The coupling efficiency in a hand-held scenario (time duration from a few seconds up to approximately one minute) with enabled beam tracking can reach values above 30% relative to the case when the sender is stationary [62].

In a first version of the system, the user had to aim through two pinholes, which requires to observe two points simultaneously in order to couple into the receiver. In the improved version, which is used in this work, the user still aims through two pinholes, however, the first one is widely open and an additional audio feedback over the PC speakers, representing the actual coupling efficiency, is given (implemented by Jannik Luhn [63]). Here, the closer to the optimal position, the higher the tone pitch of the feedback. Compared to the first version, the coupling efficiency is approximately the same, however, the later one is more comfortable for the user who only has to observe the second pinhole. Other ways of giving a feedback to the user would also be possible, e.g. optical or sensory.

A second problem, which the user is confronted with, is the angle mismatch of the reference frames, due to a rotation of the hand during the key exchange. It has been shown, that by the implementation of the reference frame independent (RFI) QKD protocol [64–66], no further correction for the basis alignment has to be made. The states, which are used there for the key generation, are in the rotationally invariant circular basis. For the standard BB84 protocol, which is implemented in this project, the secret key fraction drops to zero, in the case of a mismatch between the reference frames close to ±45°. This can be overcome by either giving somehow a feedback to the user, as it is already realised for the beam tracking, or the receiver automatically aligns the reference frames. The later one is implemented here, by the usage of a half wave plate (HWP), which is mounted in a motorised rotation stage directly behind the entrance pinhole. The motion sensor of a standard mobile phone, which is placed on top of Alice, is read out and the data are sent via WLAN to the receiver. The respective motor positions, in order to align the reference frames, are calculated and transferred to the motor control unit with a refresh rate of 10 Hz.

4.2. Improvements of the receiver

The following section describes the modifications which were done on the receiver setup within this work. The beam tracking as well as the spatial filter had to be readjusted and in order to increase the performance of the PAU, both PBS were exchanged.

4.2.1. Readjustment of beam tracking and spatial filter

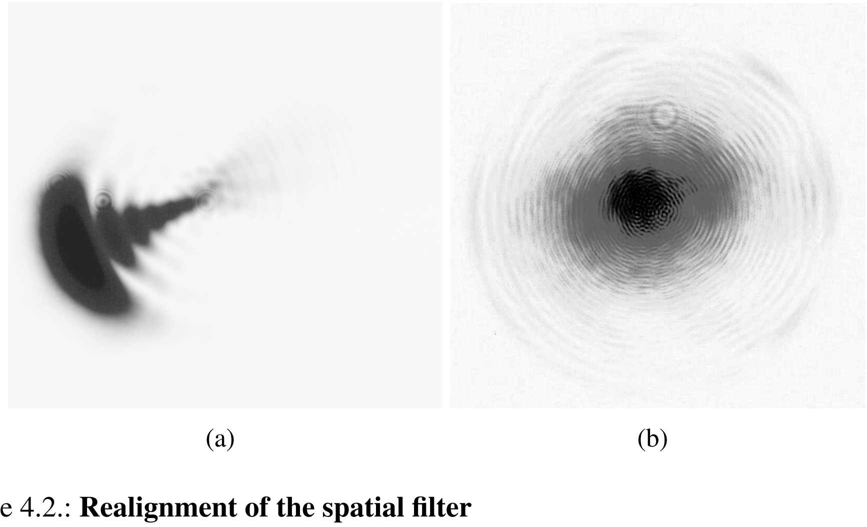
Tests of the beam tracking and controlling showed a coupling efficiency in the handheld case of approximately 17%, which is two times lower compared to former performance measurements [62].

A first approach to increase the coupling efficiency consisted in optimising the motor control parameter of the voicecoil mirror. They were empirically determined, however, for the optimisation procedure, a collimated laser beam was used. As the beacon beam of the Alice module is slightly divergent, the control parameter might have to be redetermined. However, it turned out, that no better control parameter could be found, even when using Alice for the optimisation procedure.

In a next step, the QPD has been readjusted. Here, a feature of the voicecoil mirror control software is used, which enables a stepwise scan of the voicecoil mirror axes (range adjustable). During the scan, the respective intensities of the QPD are recorded. By executing the scanning function, an absolute chaotic behaviour for the four detection levels of the respective active areas of the QPD could be observed. This indicates that the lens in front of the QPD is not in the right distance and/or that the beacon beam is not perpendicular to the plane of the lens. After both parameters have been controlled and corrected, the scanning function showed the expected behaviour [62].

A further problem, which was found during this work, was the misalignment of the spatial filter. A picture of the Alice mode after the spatial filter shows conspicuous lens effects (see Figure 4.2 (a)), which indicate that the pinhole between the two lenses of the spatial filter is not in the right position. This leads to a decreased acceptance range and also to a generally reduced transmission through the spatial filter and requires a realignment, where the following steps have to be made:

- A collimated laser beam has to be aimed centrally and perpendicularly onto the first lens.
- The transmitted power has to be maximised iteratively, by optimising the horizontal and vertical position of the pinhole as well as the distance between the first lens and the pinhole.
- The position for the second lens has to be set, where the transmitted beam is approximately collimated.
- The optimal positions of the first lens and pinhole has to be found by the usage of a camera. When a maximum of the transition is reached (powermeter), the mode has to be circularly symmetric (see Fig 4.2 (b)). Otherwise, the spatial filter would have a narrower acceptance range.
- A position for the second lens has to be set, such that the output beam is collimated.



(a) (b)

Figure 4.2.: **Realignment of the spatial filter**
The transversal mode profile (a) before the realignment of the spatial filter and (b) after. For both pictures, the Alice module in CW mode was used. The distance between the spatial filter and the camera was approximately 5 cm.

4.2.2. Exchange of the PBS at the PAU - Realignment

The characterisation of the PAU, in its original state, showed low extinction ratios of the used PBSs. After both PBSs have been changed, higher extinction ratios were achieved. The measurement data before and after the exchange of the PBS are shown in Figure 4.3.2. The average QBER induced by the PAU could be improved from 1.23% to 0.58%.

After exchanging the PBS, the coupling into the fibres of the APDs had to be reestablished. Despite the fact that the used optical fibre couplers only have two degrees of freedom (DOFs) for adjustment, an optimal coupling into the optical fibre couplers as well as a high overlap of the four detection paths still can be achieved. For this, light is coupled backwards into the fibre from the APDs side and aimed onto a 50/50 BS placed approximately 30 cm behind the PAU. A CCD camera in both paths, detecting the light propagating backwards from the BS, allows for monitoring the four modes. The goal is to achieve an overlap of the modes at both camera positions. Additionally, the four fiber couplers were adjusted to have similar divergence angles. This guarantees that the beams overlap at all positions. The adjustment procedure is as follows:

- The path where the light is transmitted at the PBS and the BS of the PAU is the reference path (see Figure 4.1, fiber coupler 4), as here the beam can only be controlled by the two DOFs of the fibre coupler. An appropriate criterion is that the light passes centrally through the pinhole in front of the PAU.
- The second path to adjust is, where the light is reflected at the BS and transmitted at the PBS (see Figure 4.1, fiber coupler 1). Here, besides the fibre coupler, additionally the tilt of the BS can be used as DOF, in order to achieve the overlap with the reference path.
- Then the two remaining path, where the light is respectively reflected at one of the PBSs (see Figure 4.1, fiber coupler 2 and 3), can be overlapped. Here also the additional tilting DOF of the PBSs can be used to achieve this, without affecting the paths, which are already adjusted.

4.3. Characterisation of the receiver

The following section is about the characterisation of the complete receiver unit. It starts with a discussion of the previously used characterisation methods. The next two parts show the methods and results from the characterisation of the PAU and the optical path after the improvements (see Section 4.2) were made. Finally, the method for determining the transmission through the receiver is presented.

4.3.1. Discussion of previously used characterisation methods

The former characterisation of the receiver, which was done by T. Vogl [26], was repeated in order to get a better understanding of the whole receiver setup. Some critical points are discussed in the following:

- The previous characterisation were made with one of the four receiver APDs and two wave plates (1 × QWP, 1 × HWP) of the receiver compensation. By the usage of these components a QST can be performed similar to the QST shown in Section 3.3.1. The major argument against this method is the missing possibility to distinguish the polarisation effects of the optical path and the PAU. Therefore the optical path and the PAU should be characterised separately. Furthermore, if Alice is used as laser source, this method is very sensitive to laser intensity fluctuations, which basically leads to similar problems as discussed in Section 3.3.2.

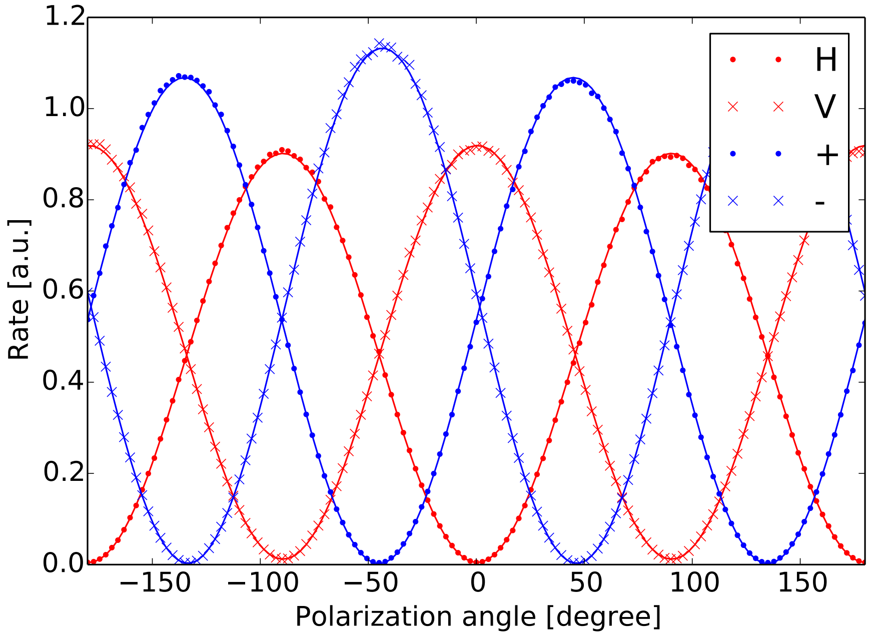
- Concerning the characterisation of the optical path, more than six polarisation states should be sent through the receiver in order to analyse the polarisation changes. This facilitates the fit of the Mueller matrix, which was not done yet.
- The calculated compensation angles should be tested before performing QKD. A separate characterisation enables this, without changing the setup. As shown in section 4.4, with the knowledge of the relative detection efficiencies of the PAU as well as the inverse Mueller matrix of the optical path, a partial tomography can be performed.
- The transmission T_{Bob} of the receiver was measured by using an additional alignment laser source with a collimated beam. Characterisation measurements have shown, that the output beam of Alice is slightly divergent. Coupling light from the alignment laser or from the Alice module through the spatial filter gives different values for the transmission (alignment laser $\approx 92\%$, Alice module $\approx 60\%$). To overcome this problem, the transmission has to be determined by using the Alice module as light source (see Section 4.3.4).
- As it turned out, during the preceding determination of the receiver transmission, the interference filter was not inserted. The measured transmission of the used filter is $\approx 60\%$ at the wavelength range of the Alice module, which leads to an additional channel attenuation. For the determination of the receiver transmission in this work, the same configuration of the receiver is used as later for QKD.

4.3.2. Detection characteristics of the PAU

One method for characterising the PAU, is to measure the count rates, which are detected by the four APDs of the PAU for different linear polarisations. The approach is described in the PhD-thesis of T. Schmitt-Manderbach [45].

The setup consists of a polarising filter and a half wave plate, which are positioned in front of the PAU. As light source serves the Alice module in CW mode. The combination of a linear polariser and a wave plate enables a rotation of the polarisation axis without a change of the optical light power. The wave plate is mounted in a motorised rotation stages to ensure fast and precise rotation settings. For one measurement point, the count rates of the four APDs are recorded simultaneously and the step size between two measurement points is 1.41 degrees (75 steps). The complete measurement for the 256 wave plate settings with an integration time of 0.5 seconds takes about 2 minutes, spanning four full periods on the equatorial plane of the Poincaré sphere.

From previous experiments it is known, that the optical output power of the Alice



Detector:	H	V	+	-	Average
Extinction ratio PBS:	1/200	1/76	1/545	1/406	1/307
	(1/40)	(1/60)	(1/100)	(1/67)	(1/60)
QBER (%):	1.31	0.49	0.33	0.17	0.58
	(1.83)	(0.64)	(1.59)	(0.86)	(1.23)
η^{rel}:	0.90	0.91	1.07	1.13	/
	(0.89)	(0.91)	(1.09)	(1.10)	/

Figure 4.3.: **Characterisation of the PAU**
The count rates of the four receiver APDs as a function of the rotation angle of the incident light. From the fits to the data points the values for the extinction ratios of the PBS, the QBER, and the relative detection efficiencies η^{rel} can be extracted. The values in parenthesis show the performance before both PBS were changed (see Section 4.2).

module varies up to 10% in CW mode on the time scale of minutes (see Figure 3.7). This problem can be circumvented by using an additional APD (MPD, PDB series) for a reference measurement during the characterisation measurement. As described in [45] the contribution of every detector to the QBER can be calculated, here exemplary for the $|H\rangle$ polarisation state, by:

$$\mathrm{QBER}_{|H\rangle} = \frac{R_V(|H\rangle)}{R_V(|H\rangle)+R_H(|H\rangle)} \tag{4.1}$$

where R_V and R_H are the count rates of the V and H detector respectively. A measurement of the initial configuration of the PAU, showed very low extinction ratios of the used PBS (see Figure 4.3, values in parenthesis), which would introduce an average QBER of 1.23%. By changing both PBS (see Section 4.2), the performance of the PAU could be improved such that the final configuration introduces an average QBER of only 0.58%.

In principle, it is possible to reach a better performance by tilting the PBS to the position with the highest extinction ratios. However, the given PAU is constructed such, that these DOFs of the PBS and the BS are used for achieving an optimal coupling of the light into the fibre couplers and the overlap of the four detection paths (see Section 4.2).

4.3.3. Polarisation rotation by the optical components

Along the optical path between the first entrance pinhole and the PAU, the incoming light passes several optical components (mirrors, dichroic mirror, band pass filter, lenses), which leads to a rotation of the incoming polarisation states. All used components show no or just a small polarisation dependent loss [26], therefore, the rotation of the states is described in good approximation by a unitary Mueller matrix.

In order to determine the Mueller matrix of the optical components along the optical path, the polarisation states before and after the transmission through the receiver have to be determined. This can be realised by a preparation setup in front of the receiver and a QST setup directly before the PAU. The preparation as well as the QST setup consist of a linear polariser and a QWP, which are mounted in motorised rotation stages (DRTM series from OWIS). The combination of polariser and QWP (in beam direction) allows to prepare an arbitrary polarisation state and the reverse order, analogously, allows to measure any polarisation state (see Figure 3.10). Basically, the QST method is the same as for analysing the sender unit (see Section 3.3.1). However, because of the lack of available space in front of the PAU, a power meter (PM series from Thorlabs) is used as detector instead of an APD. This requires the usage of a stronger laser source at 850 nm, as the maximally achievable laser power of the Alice module is only on the order of some nW, which is on the very low end of the dynamic range of the power meter.

The first step of the measurement procedure is to set a randomly chosen polarisation state, which is then analysed by performing a QST (see Section 3.3.3). An additional script serves for a repetition of the two steps for fifty further randomly chosen states. The usage of fifty randomly chosen polarisation states allows a good scan over the whole Poincaré sphere and facilitates the fit of the Mueller matrix due to an adequate number of measurement points. The unitary matrix M_{Bob} is found to be[1]:

$$M_{Bob} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.979 & 0.193 & 0.072 \\ 0 & 0.205 & -0.893 & -0.402 \\ 0 & -0.013 & 0.408 & -0.913 \end{pmatrix} \tag{4.2}$$

To check the quality of the fit, the absolute angle between the measured and the calculated Stokes vector for each of the 50 input states are calculated. That this deviation is smaller than 3° (mean value: 1.6°, standard deviation: 0.7°) in Stokes space for all fifty data points. The main reason for the deviations is the small polarisation dependent loss of some optical components along the path leading to a non-unitary

[1] Within this work, the Mueller matrix have been determined several times, because components along the path have been changed. M_{Bob} (Equ. 4.2) is the latest one (2016-10-05).

Mueller matrix. Further errors also occur due to the reading accuracy of the power meter as well as the preparation and tomography procedure.

4.3.4. Transmission of the receiver

As already discussed in section 4.3.1, the determination of the receiver transmission had to be repeated as the previously used interference filter (transmission $\approx 60\%$, strongly dependent on the angle of incidence), was replaced by a longpass filter (FELH0800 from Thorlabs), which shows nearly no attenuation of light in the IR regime and a cut-on wavelength of 800 nm. Furthermore, the spatial filter as well as the PAU were realigned.

In order to determine the attenuation in the receiver, the optical power of the beam before and after the transmission through the receiver, has to be measured. Note that this project is designed as a QKD application with a short-range free space link about 0.5 m. The attenuation of light at 850 nm in air for this length scale is negligible, thus the attenuation caused by the receiver and the channel do not have to be measured separately.

As discussed in Section 4.3.1 the Alice module has to be used as light source for determining the attenuation. As the maximally achievable laser power of the Alice module is only in the order of some nW, the receiver APDs are used as detectors. Furthermore, this also allows a very fast measurement procedure, because the count rate of the four detectors (and therefore also of the four PAU paths) can be read out simultaneously. The optical light power before passing the receiver should also be measured with one of the receiver APDs. However, as the APDs are fibre coupled, this light first has to be coupled into a multi mode fibre. This can be achieved by an additional mirror, which is mounted on a flip mount adapter directly in front of the voicecoil mirror.

To determine the fraction of light, which is coupled into the additional fiber (C_{AF}), an additional APD or alternatively a CCD camera can be used. The later one is easier to implement in the existing setup. In order to avoid unwanted light, a pinhole is placed in front of the fibre coupler. The procedure, to determine (C_{AF}), is the following:

- A background picture is taken (laser beam blocked).
- A picture of the Alice mode (CW, i_b = 30 (see Section 3.1.2), channel 2 and channel 3) is taken directly before the coupler.
- The camera is removed and then placed at the fiber output.
- Because the position of the camera has changed, a second background picture has to be taken (laser beam blocked).
- A picture of the fiber output mode is taken.

As the camera position has to be changed between the steps, it is advantageous to mark the positions of the camera, where the mode size for both cases is equal. In this position, the size of the selected area (camera software tool), which should be chosen as small as possible in order to avoid a high background, has not to be changed. The whole procedure takes about 30 s and is repeated several times. Finally, the background picture is subtracted from the picture with the laser beam. By comparing the sum of the pixel intensities of the pictures before and after the fiber, C_{AF} is found to be 83,3%. The exposure time as well as the laser power need to be chosen such that the camera is not saturated.

The procedure for the receiver transmission measurement per se, is as follows:

- The flip mirror in front of the voicecoil mirror is put into the position, where the light is guided into the additional coupler.
- The output of the fiber is connected to one of the APDs.
- Recording of the corresponding APD count rate for 10 s with an integration time of 1 s.
- The mirror is flipped into the position, where the light can pass the receiver.
- At the entrance of the APDs, the additional fiber is replaced with the fiber of the PAU.
- Recording of the four APD count rates for 10 s with an integration time of 1 s.

The procedure is repeated for the four laser sources (ch 0 to ch 3) of Alice (see Table 4.1). Note that for the determination of the transmission values for the single channels, the relative detection efficiencies (see Section 4.3.2) as well as dark counts have to be taken into account. The average transmission was found to be 41.3%, however, the respective values for the four laser diodes of Alice (ch 0 to ch 3) slightly differs. The reason for this behaviour is assumed to be in a slightly polarisation dependent reflection coefficient of several components along the path as well as a slightly different coupling of the four different modes from the Alice module.

ch 0	ch 1	ch 2	ch 3
42,5%	39,5%	43,8%	39,6%

Table 4.1.: **Results of the receiver transmission**
The transmission of the receiver for the four channels of the Alice module. The average value for T_{Bob} is 41.3%

4.4. QST using the receiver APDs

As shown in Section 3.3.1, for a complete QST, six projections (H, V, R, L, P, M) have to be measured in order to be able to determine the Stokes vector (Equ. A.1) of the polarisation states sent by Alice. The polarisation analysis unit (PAU) (see Section 4.1.1) of the receiver enables a simultaneous measurement of the four linear projections as it is designed for measuring the projections H, V, P and M. Basically, this is sufficient to calculate the Stokes vector of the polarisation states, but only if the degree of polarisation (DOP) is known and constant. In this case, the absolute value of the circular component S_3 can be simply calculated. However, by using this method, its sign is unknown. This can be overcome by comparing the results with the QST, where a single APD is used. By performing a QST with the receiver APDs, the complete receiver setup (see Figure 4.1) has to be characterised. In other words, the Mueller matrix of the optical path between the first entrance pinhole and the PAU has to be determined (see Section 4.3.3). Moreover the relative detection efficiencies of the four detectors need to be known (see Section 4.3.2). The procedure for a QST using the receiver APDs is as follows:

- A channel of the sender module is activated (pulsed QKD scenario settings)
- The count rates of the four APDs are recorded simultaneously over a time of 10 s with an integration time of 1 s.
- The analysed channel is disabled and the next channel is activated.

The cycle time is below one minute. An analysis script calculates the Stokes vectors of the four channels. For this, the aforementioned factors such as DOP, signs and relative detection efficiencies have to be taken into account. In addition, the determined Stokes vectors have to be transformed by multiplying with the inverse Muller matrix of the optical path. The advantages of this QST method are very fast cycle times and that a QST can be executed without changing the setup. This allows to test the calculated compensation angles before the key exchange. However, to use only this method for analysing the output states of Alice is not sufficient as no complete QST, i.e., the measurement of all Stokes components, is performed.

4.5. Compensation scenario

The knowledge of the Mueller matrix of the receiver system M_{Bob} (see Section 4.3.4) by which the rotational changes of the input polarisation states along the optical path can be determined allows to perform a compensation of the polarisation states with wave plates as shown in Section 3.5. Furthermore the compensation angles can be tested as a partial tomography is possible using the receiver components (see Section 4.4).

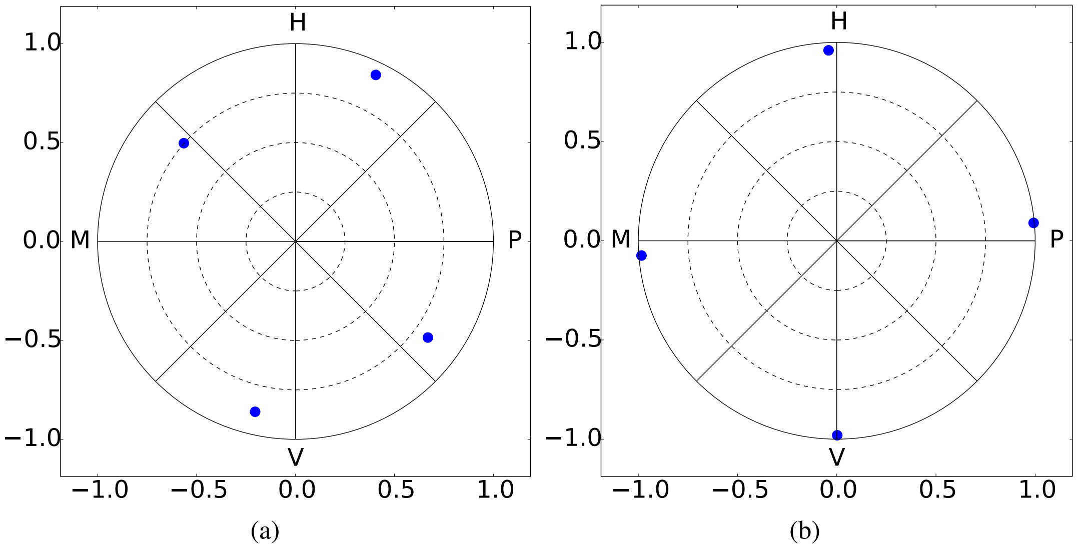
In order to calculate the compensation angles, the average QBER of the final Stokes vectors S_F^i (Equ. 3.4) has to be minimised for the following expression:

$$\begin{aligned} S_F^i &= M_{comp}(\alpha, \beta, \gamma) M_{Bob} S_I^i \\ &= M_{\frac{\lambda}{2}}(\gamma) M_{\frac{\lambda}{4}}(\beta) M_{\frac{\lambda}{4}}(\alpha) M_{Bob} S_I^i \end{aligned} \tag{4.3}$$

where S_I^i and S_F^i are the initial and final Stokes vectors of the four channels of Alice (i = channel 0 - 3) and M denotes the Mueller matrices of the wave plates and Bob respectively.

Figure 4.4 shows the results for a partial QST of uncompensated and compensated Alice output states for typical (QKD) electronics driving parameter. The compensation angles were: $\alpha = 42.41°$, $\beta = -71.42°$, $\gamma = 85.16°$. The predicted average QBER = 0.02%.

Without a compensation of the polarisation states, a key exchange would not even be possible as the measured average QBER$_I$ = 11.85±0.01%, which is above the threshold of 11% (see Section 2.2.3.2), where a secret key can be generated. This is caused both by the intrinsic QBER of the Alice module and the rotation of the polarisation states due to the transmission through the receiver. However, by testing the calculated compensation angles, an average QBER$_F$ of 1.04±0.01% was measured, which indicates an almost optimal setting of the compensation. The reason for the



	ch 0 (V)	ch 1 (M)	ch 2 (P)	ch 3 (H)
S_{I1}	-0.8613(3)	-0.4848(5)	0.4918(4)	0.8455(2)
S_{I2}	-0.1977(5)	0.6703(4)	-0.5498(4)	0.3997(4)
S_{I3}	0.4680(6)	0.5619(6)	0.6759(4)	0.3540(7)
QBER$_I$	7.72(1)%	6.93(1)%	16.24(2)%	16.49(2)%
S_{F1}	-0.9805(1)	-0.0745(6)	-0.0901(5)	0.9602(1)
S_{F2}	0.0016(5)	-0.9841(1)	0.9921(1)	-0.040(4)
S_{F3}	0.1967(5)	0.1611(6)	0.0868(5)	0.2765(4)
QBER$_F$	0.97(1)%	0.79(1)%	0.39(1)%	1.99(1)%

Figure 4.4.: **Alice output states detected by Bob - uncomp/comp**
The measured (a) uncompensated and (b) compensated Stokes components of the four output states of Alice after transmission through Bob, projected on the equatorial plane of the Poincaré sphere. The average QBER$_I$ = 11.85±0.01% and QBER$_F$ = 1.04±0.01%.

difference to the predicted QBER is hard to find but most probably caused by still a slight instability of the Alice output states.

Supposed the transmitter would show a very low intrinsic QBER, also a compensation of just the receiver setup could be made. Here a M_{comp} (Equ. 4.3) has to be calculated, which corresponds to the inverse of the Mueller matrix of the receiver M_{Bob}, however, this is not proven experimentally, yet.

5. Static and hand-held QKD

Finally, we can report about a successful key exchange which was achieved at the very end of this work. The data set[1] shown in this chapter was produced in cooperation with Jannik Luhn [63], who also made the evaluation of the key data. In the following, an overview of the general interplay of Alice and Bob, the preliminaries for the key exchange and the QKD results for the static and hand-held case are presented.

5.1. Interplay between sender and receiver

In this section, the key generation, recording and storage, the synchronisation of the clocks of Alice and Bob and the communication over the classical channel for post processing, are discussed.

Key generation, recording and storage

For every QKD scenario, a random key has to be generated at the transmitter side. We use the cryptographically strong pseudo random number generator from Java to generate a key of the length of 131 056 bits, which is currently the maximum possible key length that can be stored on the FPGA of the driving electronics of Alice. During the key exchange, the key is repeated continuously which is of course not allowed in a real QKD scenario, however, sufficient for demonstration and will be improved in a future version of the driving electronics. At the receiver side, the APDs are connected to a time to digital converter (TDC). By executing a read-out software, the time-stamp and channel number of every detected signal is written onto the harddisc of a computer.

Clock synchronisation

In order to synchronise the clocks of transmitter and receiver, the beacon beam is modulated with 50 MHz and detected at the receiver side by a fast photo diode (FPD) (see Section 4.1). The signal of the FPD is converted by a clock recovery electronics into a 100 kHz signal which then is detected by a TDC. In our case this is sufficient to find the correlation between the sent key and the received signals during the post processing. In order to exactly assign the pulses, however, the repeated key blocks have to be numbered, which is not implemented, yet. This could be realised by integrating block numbers into the beacon modulation or also by a header in the key signal including the block number before every key block [67].

[1] Measurement performed: 2016-11-21

Classical channel and post processing

The classical communication where Alice and Bob compare their chosen basis as well as the post processing is only partially performed here. For analysing the received signals, a Python script searches for correlations with the sent key, which is of course not the correct post processing procedure, however, it is the most straightforward way of determining all performance parameter of the QKD system.

5.2. Preliminaries for the key exchange

Directly before the key exchange the following preliminaries have to be considered: Setting/measuring the temporal pulse shape and the mean photon number (see Section 3.2), a full QST of the Alice output states (see Section 3.3) and setting/testing of the compensation angles (see Section 4.5).

After the key exchange, it was found that again a problem with the beam block position in Alice's micro optics has happened, resulting in more stray light emitted by Alice. This led to slightly noise results of the QST (decreased DOPs) as the used method is very sensitive for stray light (average QBER measured: 5.02%). The average QBER after compensation ($\alpha = 152.05°$, $\beta = 137.52°$, $\gamma = 54.90°$), was predicted to be 1.88%, however, by testing the compensation angles, an average QBER of 1.21% was measured. The contradiction between predicted and measured QBER, however, can be explained. The compensation angles have been tested by the QST method using the receiver APDs, which is less sensitive for stray light as the full QST using a single APD. The test of the compensation angles confirmed that they work despite the failure of the QST.

Regarding the key exchange, the stray light emitted by Alice can be ignored as it is filtered at the spatial filter of the receiver.

5.3. Results of the key exchange

The first key exchange realised with our QKD system was performed with a stationary Alice module (distance to the receiver entrance pinhole $\approx$ 15 cm) over a running time of 29.83 s (see Figure 5.2). For two further rounds the sender was held in the hand (two different persons, here distance to the receiver $\approx$ 20 cm) over a running time of 10 s and 21.5 s respectively (see Figure 5.3 and 5.4).

The received data were evaluated for two models of privacy amplification - GLLP (see Section 2.2.3.2) and the decoy state method (see Section 2.2.3.3). For our system, the implementation of the decoy state protocol is not done yet, however, it would be possible with minor changes by driving two VCSELs simultaneously in order to generate decoy pulses [68]. Nevertheless, the key data can be evaluated by using the decoy scheme. For this reason, μ was maximised (limited by one channel, see Section 3.2), which leads to a reduced achievable key rate for GLLP as the set μ was to high (see Figure 5.1, hand-held key exchange of user X (see Figure 5.3): $\mu_{optimal}$ for GLLP: 0.04, μ_{set}: 0.078). Furthermore, a signal to noise ratio (SNR) filter was used in the evaluation process. Here, the received key is devided in blocks. Only this blocks, where the transmission is above a certain threshold, contributes to the secret key. The optimal values for block size and threshold are found by maximising the

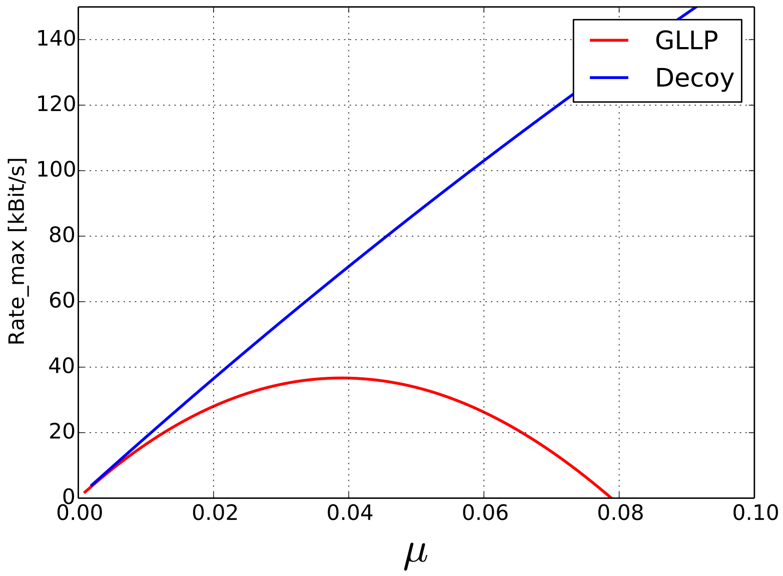


Figure 5.1.: **Achievable key rate for GLLP and Decoy**
The maximally achievable key rate R_{max} as a function of the mean photon number μ for the post-processing performed with GLLP (red) or decoy parameter (blue) (see Sections 2.2.3.2 and 2.2.3.3). Here, evaluated for the hand-held key exchange of user X (see Figure 5.3).

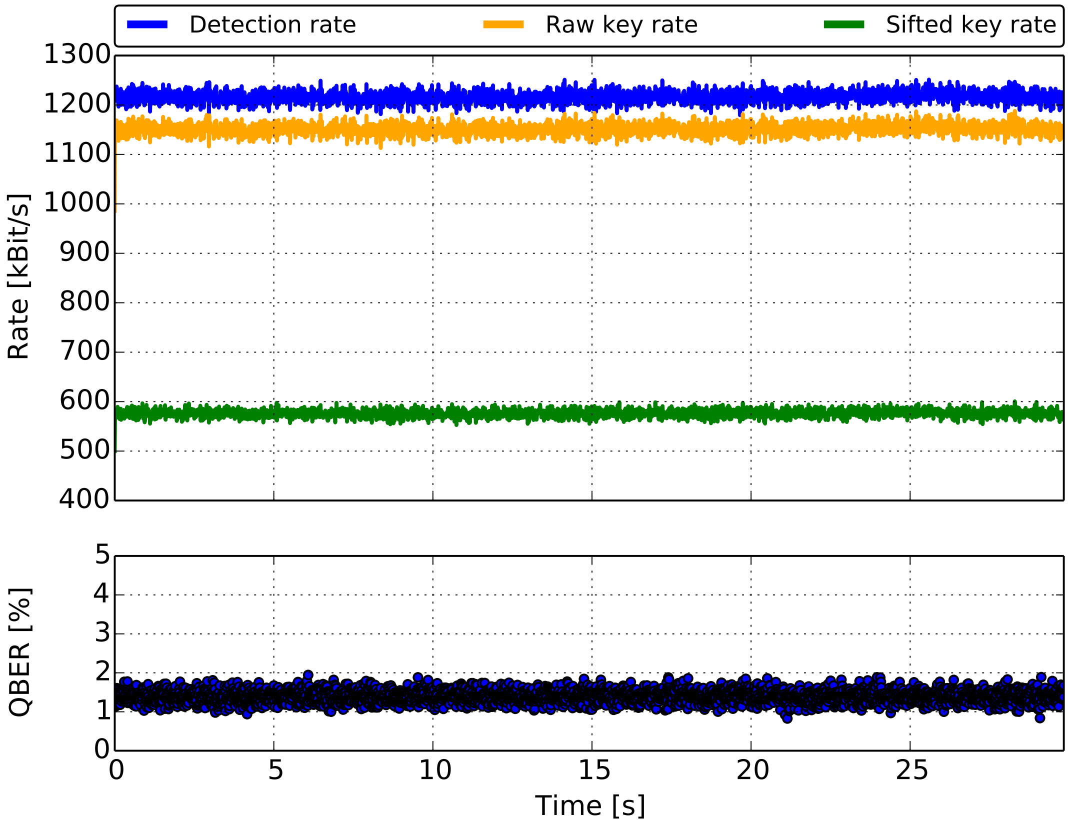
secret key rate for every data set individually.

Generally, the raw bit rate is lower than the detection rate as the short optical pulses allows for time filtering with a detection window of approximately 1.5 ns, which is individually optimised and set for every data set, too.

In the case of the static key exchange no SNR filter is needed as no fluctuations appear. Furthermore, the detection rate is found to be very stable over the measurement time. Nevertheless, longer key exchange times in the order of minutes should be tested for future data sets. The low QBER of 1.4% and the good transmission of 38.84% allows a secret key rate of 391.24 kBit/s for decoy.

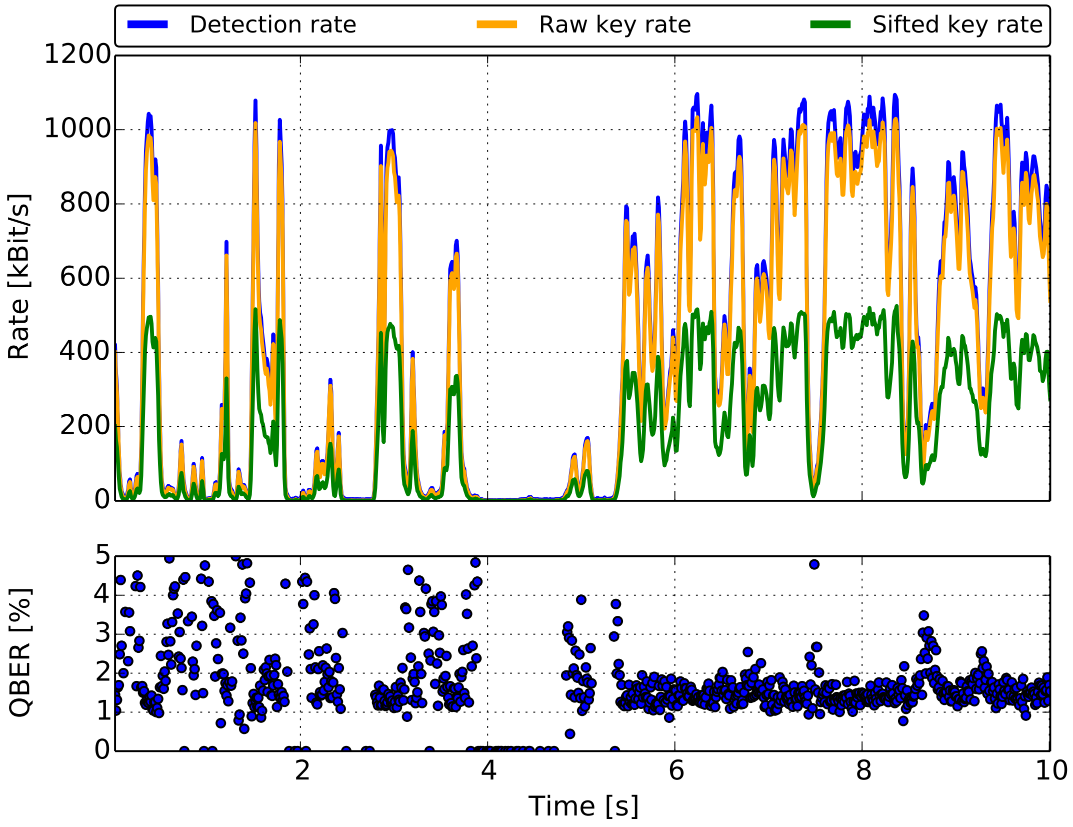
For both hand-held runs secret key rates for decoy of 137.17 kBit/s and 73.64 kBit/s respectively, were achieved. Especially the key exchange performed by user X confirmed that the beam tracking works. By applying the SNR filter to the hand-held runs it is even possible to extract a secret key fraction for GLLP despite not optimal settings.

Concluding a good performance of our QKD system was shown, however, a strong factor for the hand-held scenario is also the user itself respectively its steady hand.



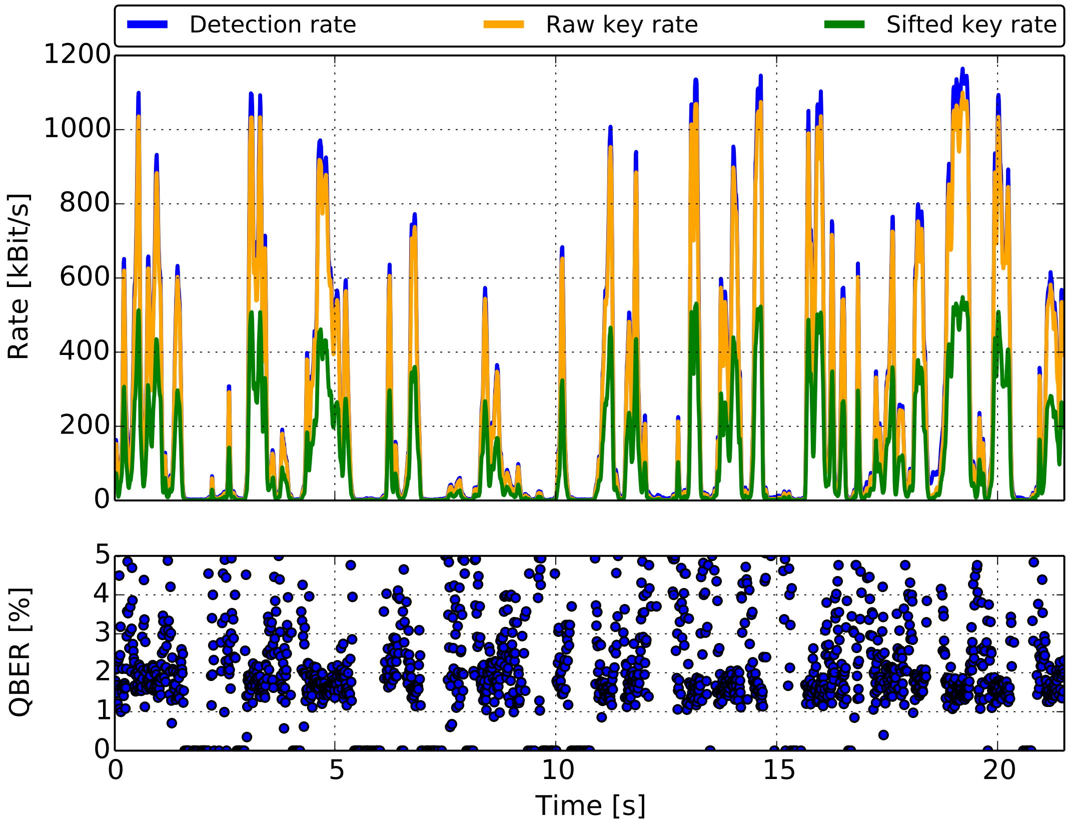
	No SNRF	GLLP	Decoy
Time [s]	/	29.83	
μ [$\frac{\text{photons}}{\text{pulse}}$]	/	0.078	
Transmission [%]	/	38.84	
QBER [%]	/	1.40	
Detection rate [kBit/s]	/	1216.23	
Raw key rate [kBit/s]	/	1151.11	
Sifted key rate [kBit/s]	/	576.00	
Secret key rate GLLP [kBit/s]	/	293.69	/
Secret key rate Decoy [kBit/s]	/	/	391.24

Figure 5.2.: **Key exchange – static**
Detection rate, raw key rate and sifted key rate over a measurement time of 29.83 s. The QBER is determined for an evaluation block size of 10 ms.



	No SNRF	GLLP + SNRF	Decoy + SNRF
Time [s]	10		
μ [$\frac{\text{photons}}{\text{pulse}}$]	0.078		
SNRF Threshold [%]	/	25.03	3.10
Transmission [%]	12.68	7.60	12.44
Hand-held efficiency [%]	30.71	18.40	30.12
QBER [%]	1.49	1.39	1.46
Detection rate [kBit/s]	399.46	237.96	391.18
Raw key rate [kBit/s]	376.12	224.66	369.41
Sifted key rate [kBit/s]	188.73	112.75	185.39
Secret key rate GLLP [kBit/s]	0.0	41.78	/
Secret key rate Decoy [kBit/s]	127.11	/	137.17

Figure 5.3.: **Key exchange – Hand-held user X**
Detection rate, raw key rate and sifted key rate over a measurement time of 10 s. The QBER is determined for an evaluation block size of 10 ms.



	No SNRF	GLLP + SNRF	Decoy + SNRF
Time [s]	21.5		
μ [$\frac{\text{photons}}{\text{pulse}}$]	0.078		
SNRF Threshold [%]	/	22.97	2.64
Transmission [%]	7.34	3.27	7.05
Hand-held efficiency [%]	17.77	7.92	17.07
QBER [%]	1.84	1.57	1.70
Detection rate [kBit/s]	233.10	102.51	221.69
Raw key rate [kBit/s]	217.46	96.85	209.00
Sifted key rate [kBit/s]	106.70	47.57	102.56
Secret key rate GLLP [kBit/s]	0.0	14.90	/
Secret key rate Decoy [kBit/s]	68.15	/	73.64

Figure 5.4.: **Key exchange – Hand-held user Y**
Detection rate, raw key rate and sifted key rate over a measurement time of 21.5 s. The QBER is determined for an evaluation block size of 10 ms.

6. Conclusion and Outlook

Within this work, an existing QKD system, consisting of a miniaturised sender and a tracking receiver, was characterised. Furthermore, modifications were made at both sides which then allowed for a key exchange in static and hand-held case.

The stability and the precision of the characterisation methods of the sender were improved. Here, the uncertainty induced by the beam displacement due to the rotation of the QST components during the QST sequence was removed. Furthermore, a QST sequence which is less sensitive against the fluctuations of the optical light power of Alice was developed. Based on the results of the improved characterisation methods, problems of the sender module regarding the emission of stray-light and the stability of the output states were identified and solved. A compensation was performed, which corrected for the rotation of the output states due to birefringence of optical components and further imperfections of the sender module. By these means, the source intrinsic QBER of the sender was reduced from 3.21% to 1.48%.

At the receiver side, the polarisation rotation caused by the optical components along the optical path was analysed by determining the corresponding Mueller matrix. Moreover, a new method for determining the receiver transmission, which is a critical parameter for evaluating the secure key rate, was developed. The QBER of the the receiver was reduced from 1.24% to 0.58% by exchanging both PBS of the PAU. Based on the knowledge of the Mueller matrix and the relative detection efficiencies, a partial QST of the sender could be performed using the receiver APDs. This allowed for testing the calculated compensation angles, which showed promising results (compensated QBER of 1.04%).

A key exchange was made for a stationary sender module reaching a secret key rate of 391.24 kBit/s over a measurement time of 29.83 s at an average QBER of 1.40%. Two further runs were made by different users in hand-held operation reaching secret key rates of 73.64 kBit/s (21.5 s, QBER: 1.70%) and 137.17 kBit/s (10 s, QBER: 1.46%) respectively, showing the capability of the system to perform a realistic key exchange.

There are several goals of future improvements: The software of the driving electronics has to be extended by the option to enable the usage of decoy states. To assign the sent bits with the received ones, also the synchronisation apparatus has to be modified allowing for sending and receiving key block numbers. Regarding the micro optics, the temperature dependency of the waveguide output states has to be analysed. Altogether these developments may allow the realisation of a compact secure QKD device for real-life applications.

A. Appendix

Stokes formalism and Mueller calculus

In order to describe the polarisation state of light, the Stokes formalism [60] can be used. The normalised Stokes vector is defined as

$$\vec{S}_N = \begin{pmatrix} 1 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1 \\ \frac{P_H - P_V}{P_H + P_V} \\ \frac{P_P - P_M}{P_P + P_M} \\ \frac{P_R - P_L}{P_R + P_L} \end{pmatrix} \tag{A.1}$$

where P_i denotes the power of polarised light, after the projection onto the six polarisation basis states $|i\rangle$ (see Table 2.1). In order to calculate the degree of polarisation (DOP), the sum of the squared (normalised) Stokes components has to be taken:

$$\mathrm{DOP} = \sqrt{S_1^2 + S_2^2 + S_3^2} \tag{A.2}$$

Any polarisation state can be visualised on the so called Poincaré sphere. By expressing the polarisation states as Stokes vector, the projections onto the three axes of the Poincaré sphere are automatically known, as it is denoted by the Stokes components S_{N1}, S_{N2} and S_{N3} (Equ. A.1).

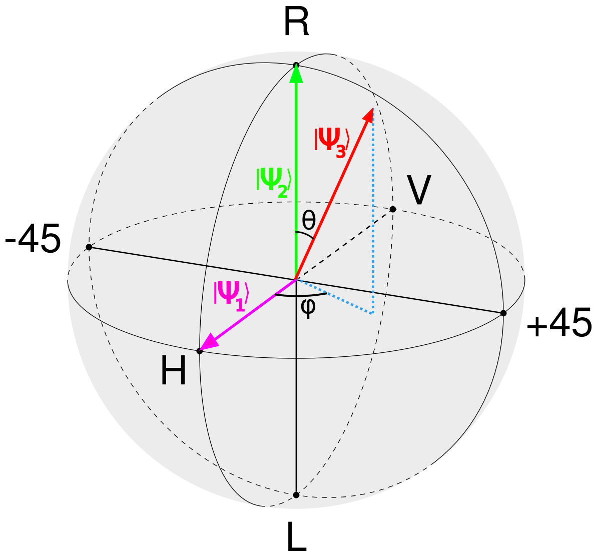


Figure A.1.: **Poincaré sphere**
The quantum states $|\Psi_1\rangle$ and $|\Psi_2\rangle$ denote the basis states $|H\rangle$ and $|R\rangle$, respectively. $|\Psi_3\rangle$ is a superposition, expressed by equation A.4.

Figure A.1 shows three examples for polarisation states, visualised onto the Poincaré sphere. The corresponding Stokes vectors are:

$$\vec{S}_{|\Psi_1\rangle} = \begin{pmatrix}1\\1\\0\\0\end{pmatrix},\ \vec{S}_{|\Psi_2\rangle} = \begin{pmatrix}1\\0\\0\\1\end{pmatrix},\ \vec{S}_{|\Psi_3\rangle} = \begin{pmatrix}1\\0.25\\0.4\\0.775\end{pmatrix} \tag{A.3}$$

where $|\Psi_1\rangle = |H\rangle$ and $|\Psi_2\rangle = |R\rangle$. The quantum state $|\Psi_3\rangle$ can be expressed by a superposition of basis states, here exemplary from B_Z:

$$|\Psi_3\rangle = \cos\left(\frac{\Theta}{2}\right)|L\rangle + e^{i\phi}\sin\left(\frac{\Theta}{2}\right)|R\rangle \tag{A.4}$$

The Mueller calculus [69] can be used in order to calculate the influence of optical components onto a known polarisation state:

$$\vec{S}_i = M\vec{S}_f \tag{A.5}$$

where $\vec{S}_i$ and $\vec{S}_f$ are the Stokes vectors of the initial and final polarization states respectively and M is the 4 x 4 Mueller matrix.

The Mueller matrix for a linear polariser is given by:

$$M_{pol} = \frac{1}{2}\begin{pmatrix} 1 & \mathrm{c}(2\theta) & \mathrm{s}(2\theta) & 0 \\ \mathrm{c}(2\theta) & \mathrm{c}^2(2\theta) & \mathrm{s}(2\theta)\mathrm{c}(2\theta) & 0 \\ \mathrm{s}(2\theta) & \mathrm{s}(2\theta)\mathrm{c}(2\theta) & \mathrm{s}^2(2\theta) & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{A.6}$$

where sin() ≡ s(), cos() ≡ c() and θ is the angle between the horizontal axis of the system and the polariser axis.

Retarders are described by:

$$M_\lambda = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathrm{c}^2(2\theta)+\mathrm{c}(\delta)\mathrm{s}^2(2\theta) & \mathrm{c}(2\theta)\mathrm{s}(2\theta)-\mathrm{c}(2\theta)\mathrm{c}(\delta)\mathrm{s}(2\theta) & \mathrm{s}(2\theta)\mathrm{s}(\delta) \\ 0 & \mathrm{c}(2\theta)\mathrm{s}(2\theta)-\mathrm{c}(2\theta)\mathrm{c}(\delta)\mathrm{s}(2\theta) & \mathrm{c}(\delta)\mathrm{c}^2(2\theta)+\mathrm{s}^2(2\theta) & -\mathrm{c}(2\theta)\mathrm{s}(\delta) \\ 0 & -\mathrm{s}(2\theta)\mathrm{s}(\delta) & \mathrm{c}s(2\theta)\mathrm{s}(\delta) & \mathrm{c}(\delta) \end{pmatrix} \tag{A.7}$$

where δ denotes the phase difference between fast and slow axis and θ is the angle between the horizontal axis of the system and the fast axis of the retarder.

Tab A.1 shows a list of frequently used Mueller matrices for typical settings of polarising filters and retarders.

By the combination of three retarders, any unitary transformation can be done:

$$M_U(\alpha,\beta,\gamma) = M_{\frac{\lambda}{2}}(\gamma)M_{\frac{\lambda}{4}}(\beta)M_{\frac{\lambda}{4}}(\alpha) \tag{A.8}$$

where α, β and γ are the three Euler angles in the (z, x', z") standard notation.

Polariser	Transmission			
	Horizontal	Vertical	+45 °	-45 °
	$\frac{1}{2}\begin{pmatrix}1 & 1 & 0 & 0\\ 1 & 1 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$	$\frac{1}{2}\begin{pmatrix}1 & -1 & 0 & 0\\ -1 & 1 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$	$\frac{1}{2}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 1 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$	$\frac{1}{2}\begin{pmatrix}1 & 0 & -1 & 0\\ 0 & 0 & 0 & 0\\ -1 & 0 & 1 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}$
Retarder	(Fast axis: vertical) $\frac{\lambda}{2}$	(Fast axis: horizontal) $\frac{\lambda}{4}$	(Fast axis: vertical) $\frac{\lambda}{4}$	
	$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & -1\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & -1 & 0\end{pmatrix}$	$\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\end{pmatrix}$	

Table A.1.: Mueller matrices of frequently used optical components in several configurations.

Bibliography

[1] N. Gisin, G. Ribordy, W. Tittel und H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, **74**:145–195, Mar 2002. doi: 10.1103/RevModPhys.74.145. URL http://link.aps.org/doi/10.1103/RevModPhys.74.145.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus und M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, **81**:1301–1350, Sep 2009. doi: 10.1103/RevModPhys.81.1301. URL http://link.aps.org/doi/10.1103/RevModPhys.81.1301.

[3] H.-K. Lo, M. Curty und K. Tamaki. Secure quantum key distribution. *Nature Photonics*, **8**:595–604, 2014. doi: 10.1038/nphoton.2014.149.

[4] NIST. Announcing the advanced encryption standard. *Federal Information Processing Standards Publication*, **197**, 2001.

[5] S. Vernam. Secret signaling system. *UNITED STATES PATENT*, **US 1310719 A**, 1919.

[6] R. L. Rivest, A. Shamir und L. Adleman. Cryptographic communications system and method. *UNITED STATES PATENT*, **US 4405829 A**, 1983.

[7] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, **41**(2):303–332, 1999.

[8] Grizzly steppe - russian malicious cyber activity. URL http://web.archive.org/web/20080207010024/http://www.808multimedia.com/winnt/kernel.htm. Accessed: 2017-01-15.

[9] S. Wiesner. Conjugate coding. *SIGACT News*, **15**(1):78–88, January 1983. ISSN 0163-5700. doi: 10.1145/1008908.1008920. URL http://doi.acm.org/10.1145/1008908.1008920.

[10] C. H. Bennett und G. Brassard. Quantum cryptography : Public key distribution and coin tossing. *International Conference on Computer System and Signal Processing, IEEE,*, pages 175–179, 1984. URL http://ci.nii.ac.jp/naid/20001457561/en/.

[11] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail und J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, **5**(1):3–28, 1992. ISSN 1432–1378. doi: 10.1007/BF00191318. URL http://dx.doi.org/10.1007/BF00191318.

[12] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden und A. Zeilinger. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, **11**(7):075001, 2009. URL `http://stacks.iop.org/1367-2630/11/i=7/a=075001`.

[13] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta und H. Zbinden. Long-term performance of the swissquantum quantum key distribution network in a field environment. *New Journal of Physics*, **13**(12):123001, 2011. URL `http://stacks.iop.org/1367-2630/13/i=12/a=123001`.

[14] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev und A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, **19**(11):10387–10409, May 2011. doi: 10.1364/OE.19.010387. URL `http://www.opticsexpress.org/abstract.cfm?URI=oe-19-11-10387`.

[15] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang und J.-W. Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, **117**:190501, Nov 2016. doi: 10.1103/PhysRevLett.117.190501. URL `http://link.aps.org/doi/10.1103/PhysRevLett.117.190501`.

[16] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter und A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, **3**:481–486, 2007. doi: 10.1038/nphys629.

[17] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger

und H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, **98**:010504, Jan 2007. doi: 10.1103/PhysRevLett.98.010504. URL `http://link.aps.org/doi/10.1103/PhysRevLett.98.010504`.

[18] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick und H. Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, **7**:382–386, 2013. doi: 10.1038/nphoton.2013.46.

[19] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco und P. Villoresi. Experimental satellite quantum communications. *Phys. Rev. Lett.*, **115**:040502, Jul 2015. doi: 10.1103/PhysRevLett.115.040502. URL `http://link.aps.org/doi/10.1103/PhysRevLett.115.040502`.

[20] E. Gibney. Chinese satellite is one giant step for the quantum internet. *Nature*, **535**:478–479, 2016. doi: 10.1038/535478a.

[21] M. Swartwout. The first one hundred cubesats: A statistical look. *Journal of Small Satellites*, **2**(2):213–233, 2013.

[22] R. Bedington, X. Bai, E. Truong-Cao, Y. C. Tan, K. Durak, A. VillarÂ Zafra, J. A. Grieve, D. K. Oi und A. Ling. Nanosatellite experiments to enable future space-based qkd missions. *EPJ Quantum Technology*, **3**(1):12, 2016. doi: 10.1140/epjqt/s40507-016-0051-7. URL `http://dx.doi.org/10.1140/epjqt/s40507-016-0051-7`.

[23] T. Jennewein und B. Higgins. The quantum space race. *Physics World*, **26**(03): 52, 2013. URL `http://stacks.iop.org/2058-7058/26/i=03/a=37`.

[24] G. Mélen. Integrated quantum key distribution sender unit for hand-held platforms. Dissertation, Ludwig-Maximilians-University Munich, 2016.

[25] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame und H. Weinfurter. Design and evaluation of a handheld quantum key distribution sender module. *IEEE Journal of Selected Topics in Quantum Electronics*, **21**(3):131–137, May 2015. ISSN 1077-260X. doi: 10.1109/JSTQE.2014.2364131.

[26] T. Vogl. Mobile free space quantum key distribution for short distance secure communication. Master's thesis, Ludwig-Maximilians-University Munich, 2016.

[27] B. Schneier. *Applied Cryptography*. Wiley, 1996.

[28] J. Katz und Y. Lindell. *Introduction to Modern Cryptography*. CRC Press, 2015.

[29] C. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, **28**:656–715, 1949.

[30] W. K. Wootters und B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, **191**(2):363 – 381, 1989. doi: http://dx.doi.org/10.1016/0003-4916(89)90322-9. URL `http://www.sciencedirect.com/science/article/pii/0003491689903229`.

[31] W. K. Wootters und W. H. Zurek. A single quantum cannot be cloned. *Nature*, **299**(5886):802–803, oct 1982. URL `http://dx.doi.org/10.1038/299802a0`.

[32] A. Acín, N. Gisin und V. Scarani. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A*, **69**:012309, Jan 2004. doi: 10.1103/PhysRevA.69.012309. URL `http://link.aps.org/doi/10.1103/PhysRevA.69.012309`.

[33] H. Bechmann-Pasquinucci und N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, **59**:4238–4248, Jun 1999. doi: 10.1103/PhysRevA.59.4238. URL `http://link.aps.org/doi/10.1103/PhysRevA.59.4238`.

[34] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, **67**:661–663, Aug 1991. doi: 10.1103/PhysRevLett.67.661. URL `http://link.aps.org/doi/10.1103/PhysRevLett.67.661`.

[35] K. Inoue, E. Waks und Y. Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, **89**:037902, Jun 2002. doi: 10.1103/PhysRevLett.89.037902. URL `http://link.aps.org/doi/10.1103/PhysRevLett.89.037902`.

[36] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf und P. Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, **421**:238–241, 2003.

[37] D. Gottesman, H. K. Lo, N. Lutkenhaus und J. Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136, 2004. doi: 10.1109/ISIT.2004.1365172.

[38] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat und P. Grangier. Single photon quantum cryptography. *Phys. Rev. Lett.*, **89**:187901, Oct 2002. doi: 10.1103/PhysRevLett.89.187901. URL `http://link.aps.org/doi/10.1103/PhysRevLett.89.187901`.

[39] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat und P. Grangier. Experimental open-air quantum key distribution with a single-photon source. *New Journal of Physics*, **6**(1):92, 2004. URL `http://stacks.iop.org/1367-2630/6/i=1/a=092`.

[40] T. Heindel, C. Kessler, M. Rau, C. Schneider, M. Fuerst, F. Hargart, W. Schulz, M. Eichfelder, R. Rossbach, S. Nauerth, M. Lermer, H. Weier, M. Jetter,

M. Kamp, S. Reitzenstein, S. Hoefling, P. Michler, H. Weinfurter und A. Forchel. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New Journal of Physics*, **14**(8):083001, 2012. URL http://stacks.iop.org/1367-2630/14/i=8/a=083001.

[41] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, **91**:057901, Aug 2003. doi: 10.1103/PhysRevLett.91.057901. URL http://link.aps.org/doi/10.1103/PhysRevLett.91.057901.

[42] H.-K. Lo, X. Ma und K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, **94**:230504, Jun 2005. doi: 10.1103/PhysRevLett.94.230504. URL http://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

[43] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, **94**:230503, Jun 2005. doi: 10.1103/PhysRevLett.94.230503. URL http://link.aps.org/doi/10.1103/PhysRevLett.94.230503.

[44] X. Ma, B. Qi, Y. Zhao und H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, **72**:012326, Jul 2005. doi: 10.1103/PhysRevA.72.012326. URL http://link.aps.org/doi/10.1103/PhysRevA.72.012326.

[45] T. Schmitt-Manderbach. Long distance free-space quantum key distribution. Dissertation, Ludwig-Maximilians-University Munich, 2007.

[46] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, **61**:052304, Apr 2000. doi: 10.1103/PhysRevA.61.052304. URL http://link.aps.org/doi/10.1103/PhysRevA.61.052304.

[47] G. Brassard und L. Salvail. *Secret-Key Reconciliation by Public Discussion*, pages 410–423. Springer Berlin Heidelberg, Berlin, Heidelberg, 1994. ISBN 978-3-540-48285-7. doi: 10.1007/3-540-48285-7_35. URL http://dx.doi.org/10.1007/3-540-48285-7_35.

[48] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue und C. G. Peterson. Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A*, **67**:052303, May 2003. doi: 10.1103/PhysRevA.67.052303. URL http://link.aps.org/doi/10.1103/PhysRevA.67.052303.

[49] R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory*, **8**(1):21–28, January 1962. ISSN 0096-1000. doi: 10.1109/TIT.1962.1057683.

[50] C. H. Bennett, G. Brassard, C. Crepeau und U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, **41**(6):1915–1923, Nov 1995. ISSN 0018-9448. doi: 10.1109/18.476316.

[51] B. Huttner, N. Imoto, N. Gisin und T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, **51**:1863–1869, Mar 1995. doi: 10.1103/PhysRevA.51.1863. URL `http://link.aps.org/doi/10.1103/PhysRevA.51.1863`.

[52] M. Dušek, O. Haderka und M. Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Optics Communications*, **169**:103–108, 1999. doi: http://dx.doi.org/10.1016/S0030-4018(99)00419-8. URL `http://www.sciencedirect.com/science/article/pii/S0030401899004198`.

[53] G. Brassard, N. Lütkenhaus, T. Mor und B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, **85**:1330–1333, Aug 2000. doi: 10.1103/PhysRevLett.85.1330. URL `http://link.aps.org/doi/10.1103/PhysRevLett.85.1330`.

[54] V. Makarov, A. Anisimov und J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, **74**:022313, Aug 2006. doi: 10.1103/PhysRevA.74.022313. URL `http://link.aps.org/doi/10.1103/PhysRevA.74.022313`.

[55] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth und H. Weinfurter. Spatial mode side channels in free-space qkd implementations. *IEEE Journal of Selected Topics in Quantum Electronics*, **21**(3):187–191, May 2015. ISSN 1077-260X. doi: 10.1109/JSTQE.2014.2372008.

[56] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth und H. Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics*, **13**(7):073024, 2011. URL `http://stacks.iop.org/1367-2630/13/i=7/a=073024`.

[57] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar und V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, **4**:686–689, 2010.

[58] R. Michalzik. *VCSELs: Fundamentals, Technology and Applications of Vertical Cavity Surface Emitting Lasers*. Springer, 2013.

[59] G. Mélen, W. Rosenfeld und H. Weinfurter. Impact of the slit geometry on the performance of wire-grid polarisers. *Opt. Express*, **23**(25):32171–32178, Dec 2015. doi: 10.1364/OE.23.032171. URL `http://www.opticsexpress.org/abstract.cfm?URI=oe-23-25-32171`.

[60] B. E. A. Sahleh und M. C. Teich. *Fundamentals of Photonics*. Wiley, 2007.

[61] T. Vogl. Security of a free space qkd-receiver module with angle-dependent detection efficiency mismatch. Bachelor's thesis, Ludwig-Maximilians-University Munich, 2014.

[62] T. Vogl. Construction of an electronically-driven mirror system for qkd. Internship report, Ludwig-Maximilians-University Munich, 2015.

[63] J. Luhn. Master's thesis, Ludwig-Maximilians-University Munich, 2017.

[64] A. Laing, V. Scarani, J. G. Rarity und J. L. O'Brien. Reference-frame-independent quantum key distribution. *Phys. Rev. A*, **82**:012304, Jul 2010. doi: 10.1103/PhysRevA.82.012304. URL `http://link.aps.org/doi/10.1103/PhysRevA.82.012304`.

[65] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'Brien und A. O. Niskanen. Demonstration of free-space reference frame independent quantum key distribution. *New Journal of Physics*, **15**(7):073001, 2013. URL `http://stacks.iop.org/1367-2630/15/i=7/a=073001`.

[66] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, D. O'Brien und D. Bitauld. Motion-compensated hand-held quantum key distribution system. *arxiv*, **quant-ph-1608.07465**, 2016.

[67] H. Weier. European quantum key distribution network. Dissertation, Ludwig-Maximilians-University Munich, 2011.

[68] J. W. Harrington, J. M. Ettinger, R. J. Hughes und J. E. Nordholt. Enhancing practical security of quantum key distribution with a few decoy states. *arxiv*, **quant-ph-0503002**, 2005.

[69] H. Mueller. Memorandum on the polarization optics of the photoelastic shutter. *Tech. rep1943*, 1943.

Acknowledgement

Am Ende dieser Arbeit möchte ich mich bei einigen Menschen bedanken.

Prof. Dr. Harald Weinfurter, für die Möglichkeit in seiner Gruppe eine Masterarbeit gemacht haben zu dürfen. Ich danke Dir für Deine Betreuung, Deine Geduld und für Deine immer angenehme Umgangsweise. Ich freue mich schon sehr auf das nächste Projekt.

Dr. Wenjamin Rosenfeld und Dr. Gwenaelle Mélen, für Ihre Betreuung und hilfreichen Diskussionen. Auch Ihr hattet wirklich immer ein offenes Ohr für meine Probleme. Ihr habt mir jederzeit weitergeholfen und viel Energie in dieses Projekt gesteckt. Ihr seid Vorbilder für mich.

Jannik Luhn, für die tolle Zusammenarbeit. Ich bin unglaublich froh, Dich als Masterkollegen gehabt zu haben und weiterhin mit Dir in einem Team sein zu dürfen.

Allen XQPs und besonders Martin Zeitlmair für ihre Hilfsbereitschaft, sowie Clemens Sonnleitner für seinen prüfenden Blick auf diese Arbeit. Ich schätze das kollegiale und freundschaftliche Klima in unserer Gruppe sehr.

Meinen Eltern und Großeltern für Ihre Unterstützung und Ihr Vertrauen in mich.

Meiner Freundin Maria, dass Du mein Halt im Leben bist.

Declaration

Hiermit erkläre ich, die vorliegende Arbeit selbständig verfasst zu haben und keine anderen als die in der Arbeit angegebenen Quellen und Hilfsmittel benutzt zu haben.

München, der 26.01.2017

Peter Freiwang