DEPARTMENT OF PHYSICS
LUDWIG-MAXIMILIAN-UNIVERSITY OF MUNICH

Master's Thesis

Mobile Free Space Quantum Key Distribution for short distance secure communication

Tobias Vogl

January 21, 2016

Supervised by Prof. Dr. Harald Weinfurter and Gwenaelle Mélen

DEPARTMENT FÜR PHYSIK
LUDWIG-MAXIMILLIANS-UNIVERSTITÄT MÜNCHEN

Masterarbeit

Mobile Freiraum Quanten Schlüssel Verteilung für sichere Kommunikation über kurze Distanzen

Tobias Vogl

January 21, 2016

Betreut durch Prof. Dr. Harald Weinfurter und Gwenaelle Mélen

Contents

1 Introduction

Worldwide communication is one of the most important achievements of the 20^{th} and especially of the 21^{st} century. The safe transfer of information plays an important role and is ensured by cryptography. The field of applications ranges from private e-mails over the exchange of banking information to the transmission of national secrets. Especially through the development of the internet cryptography gained in importance. But in the last years security loopholes in classical cryptography have been frequently discovered. In 2013 the "NSA-Scandal"[1] showed that the topic of a safe encryption method is more actual than ever.

Modern cryptographic systems rely on unproven assumptions like the difficulty of factorising large numbers, the difficulty of solving the discrete logarithm problem and assumptions on a limit to available computational power. A famous example is the widespread RSA algorithm, a public-key method with a public key for encrypting and a private key for decrypting. The private key can be calculated from the public key by solving the factorisation problem, but currently no efficient classical algorithm for this is known. But this might change over night. However, alternatively a quantum computer with enough qubits can factorise large numbers and extract discrete logarithms efficiently and thus break RSA or Diffie-Hellman key exchange, even if based on elliptic curves[2]. Public-key systems are frequently used because there is no need to transmit an initial secret key between sender and receiver of a message. For the distribution of secure keys no proven secure classical possibility exists, unless sender and receiver meet and exchange a key, for example on a hard drive, but this is hardly likely practical for everyday applications. Until today, the only provable secure encryption method is the so-called One Time Pad, but this method requires an initial secret key exchange as well.

For the first time in the long history of cryptography, a possibility for provably secure key exchanging was developed: Quantum Key Distribution (QKD)[3], which security relies only on fundamental laws of quantum mechanics and not on mathematical assumptions. As long as the laws of quantum mechanics hold, QKD will be a safe procedure, independent of available algorithms or skills of a potential eavesdropper. A possible attack on the key transmission will always be detected and the information of the eavesdropper can be estimated from analysis of the key distillation and reduced to zero with classical post-processing. The theory of QKD is already quite advanced, the first proof-of-principle experiments[4] soon where followed by implementations of QKD which in turn resulted in first commercial products[5]. Currently implementation loopholes have to be made impossible and for a wide usage the operating distances must be improved. First networks have been launched for example in Vienna[6] and Tokyo[7] among others, while the future vision would be a network on a global scale. However, in the cryptography and security community Quantum Key Distribution plays only a minor role as precisely those implementation loopholes gave rise to the assumption that QKD can never be better than conventional, quantum-resistant cryptography, also known as post-quantum cryptography. But this is a very naive assumption! On the one hand QKD allows backward and forward security which can never be reached by any classical cryptographic system. The eavesdropping must take place at the time, when the key is exchanged.

For classical data this condition relaxes as one can simply monitor and store the complete internet traffic. This is exactly what the National Security Agency of the USA (NSA) does, storing ciphertexts now and decrypting later. For this purpose the NSA built a huge data centre in Utah, USA with an estimated capacity between $3 \cdot 10^{18} - 10^{24}\, bytes$[8][9]. On the other hand it is not proven, that a quantum computer cannot break the security of post-quantum cryptography, for example classical lattice-based cryptography. Hence post-quantum cryptography is just another bet on the unknown as RSA was almost 40 years ago. However fact is, that someday the current public-key cryptography will collapse. Whether it will be replaced by Quantum Key Distribution or post-quantum cryptography is yet unknown, maybe also by both. But the transition must start now, as it took more than a decade to change from DES to AES and these are two very similar algorithms[10]. Even the NSA's Information Assurance Directorate stated recently, that they

> *"will initiate a transition to quantum resistant algorithms in the not too distant future"*[11].

While most research on quantum cryptography is targeting long-distance applications, QKD offers a huge potential on short ranges as well: One could think of a small handheld device, possibly integrated into a smart phone, which transmits credit card information without contact to an ATM or to the reading device at a checkout counter. Or even more advanced, such a small device could serve as a quantum network interface for a worldwide quantum internet. The idea is to miniaturise the transmitter while keeping all bulky optical components on the receiver's side.

In this Master's Thesis an integrated compact micro-optics based sending unit for free space operation on short ranges is developed and finally tested. It is believed that this implementation could open new possibilities for commercial applications towards secure daily-life authentication. The sender, with dimensions as small as $35 \times 20 \times 8\, mm^3$, implements the well-known BB84 protocol and can be controlled at least partially by a smart phone via an Android App classically communicating with the receiver's computer over Wi-Fi. An additional beacon laser allows both synchronisation with the clock of the receiver and efficient beam tracking and controlling for continuous operation.

This work starts with the theoretical basics for conventional and quantum cryptography and reviews the Stokes formalism, which is used to describe polarisation. Next, the state of the experiment at the start of this work is described with a small outlook of the remaining tasks, followed by a detailed presentation of the experiment itself. This part is divided into two parts: The first part describes the development of the sender and receiver while the second part presents first QKD tests and results. After further analysis of the results, taking finite key effects into account and evaluating also the SARG04 protocol, an outlook is given with possible improvements and next steps. Finally a conclusion summarises the experiment so far. Most of the theoretical background has been acquired with [12], [13], [14] and other standard quantum mechanics and optics books. It might not always be extra marked as a citation.

2 Theoretical Essentials

2.1 Conventional Cryptography

Cryptography is the art of safely storing information and transmitting messages between two parties impossible to read for any unauthorised third party. In the following the focus is on the transmission of secret messages. Such a secret message is encrypted by a cryptographic algorithm. This algorithm provides a cipher (the encrypted message) which can be transferred through an authenticated channel. It does not matter whether this message is intercepted and read by any eavesdropper as long as the cipher remains unchanged during the transmission, which can be ensured by using a Hash-algorithm (changing the cipher will change its Hash-value). To read the message the receiver has to apply another cryptographic algorithm to decrypt the cipher. In some cases this can be the same algorithm as for encrypting.

2.1.1 Symmetric encryptions

In modern cryptography all algorithms can be classified in two different categories: Asymmetric and symmetric encryptions. In a symmetric encryption the same key is used for encrypting and decrypting as well. Two famous examples are the Advanced Encryption Standard (AES)[15] or the One Time Pad (OTP)[16] which is the only information theoretically secure encryption. As the OTP is important later it will be explained in detail.

If two parties, usually called Alice and Bob, want to communicate and Alice wants to send for example the message *LMUXQP*, then Alice starts by converting the text to binary code, in the next step Alice and Bob perform a secret key exchange (with a key length as long as the message length) and finally Alice applies the XOR operation to the plain text and the key, that means bitwise sum modulo 2 (see table 2.1). The resulting bit string or cipher is then transferred to Bob and as Bob also has the key he can simply apply the XOR operation to the cipher and the key again and will restore the initial plain text (see table 2.2) as a simple proof shows:

$$x \oplus y \oplus y = x \oplus 2y = x \qquad \forall\ x, y \tag{2.1}$$

where x is the message, y the key and $\oplus$ denotes the direct sum, that means bitwise sum modulo 2. If the key is only used once and perfectly random, then the cipher is also perfectly random. Hence it does not contain any information about the message, which makes the OTP perfectly secure. Due to the requirement of the key length usually AES is used which has key lengths between $128\,bit$ and $256\,bit$.

AES is considered to be ultra-secure as well[17] and recommended by the NSA to protect top secret information[11]. The problem with all symmetric encryptions is, that they require a prior secret key exchange. For this purpose usually asymmetric encryptions are used.

message	L	M	U	X	Q	P
binary	01001100	01001101	01010101	01011000	01010001	01010000
key	11011111	00111110	10110100	10100101	10011010	00110111
XOR	10010011	01110011	11100001	11111101	11001011	01100111

Table 2.1: Alice's side. Message XOR key gives the cipher.

cipher	10010011	01110011	11100001	11111101	11001011	01100111
key	11011111	00111110	10110100	10100101	10011010	00110111
XOR	01001100	01001101	01010101	01011000	01010001	01010000
message	L	M	U	X	Q	P

Table 2.2: Bob's side. Cipher XOR key restores the initial message.

2.1.2 Asymmetric encryptions

In contrast, an asymmetric encryption uses two different keys: one public key for encrypting and one private key for decrypting. The future receiver of a message can broadcast his public key so that the sender can encrypt the message with this key. Then the sender can broadcast the resulting cipher which can only be decrypted by the receiver since he is the only one who has the private key. These encryptions are based on one-way functions, which are functions, where it is easy to compute the image for any given input value, but hard for a random image to compute the input value. Easy in this manner means, that the algorithm is in the computational complexity class P meaning that the effort (for example computational time) scales polynomially with the size of the problem. On the contrary hard means, that the algorithm is in the complexity class NP or NP-complete meaning that the effort scales exponentially with the size of the problem. In cryptography the characteristic magnitude or size of the problem is usually the key N with length n. Given two numbers of $\mathcal{O}(N)$, the effort for multiplication of these numbers scales with $\mathcal{O}(N^2)$. Taking only dominating terms into account the factorisation complexity for any integer N in L-notation[18] is given by

$$L_N\left[u,v\right] = exp\left\{v\cdot\left(log\left(N\right)\right)^u\left(log\left(log\left(N\right)\right)\right)^{1-u}\right\} \tag{2.2}$$

The two limiting cases are exponential ($u = 1$) and polynomial ($u = 0$), while the intermediate region $0 < u < 1$ is sub-exponential or super-polynomial. Note that it

requires n bits to express N, that means N is of the order $\mathcal{O}(2^n)$. This problem is exploited in the famous RSA encryption[19], which can be broken by factorising the public key. For factorisation the Number Field Sieve (NFS) can be used which has complexity $L_N\left[1/3, \sqrt[3]{64/9}\right]$, that means it is super-polynomial and for typical RSA key lengths of $2048\,bit$ even super computers would need times of the order of the age of the universe to factorise the RSA modulus and thus break the encryption. Although the NFS is the best known classical algorithm for factorisation it has not been proven that there does not exist any better classical algorithm.
Even though this might hold in a classical world, however, a quantum computer can run Shor's algorithm[20] which has complexity $L_N\left[0, 3\right]$, that means a reasonable quantum computer would need only a few days to crack long RSA keys. For a comparison between the NFS and Shor's algorithm see figure 2.1. Note that the quantum computer can also solve the discrete logarithm problem efficiently and thus break the security of Elliptic Curve Cryptography and ElGamal, as well as Diffie-Hellman key exchange (even if based on elliptic curves) that means basically of every public key encryption used today[2]. In the not-too-far future different key exchange procedures are required to guarantee secure communication. One possibility is Quantum Key Distribution (QKD) as explained in the next sections. For the sake of completeness it shall be mentioned that there exists also post-quantum cryptography (PCQ), which aims to develop quantum-resistant public key encryptions. A famous example is lattice-based cryptography. However, post-quantum cryptography is only believed to be quantum-resistant, there does not exist any proof that a quantum computer (or even a classical computer) could not break the security of PCQ.

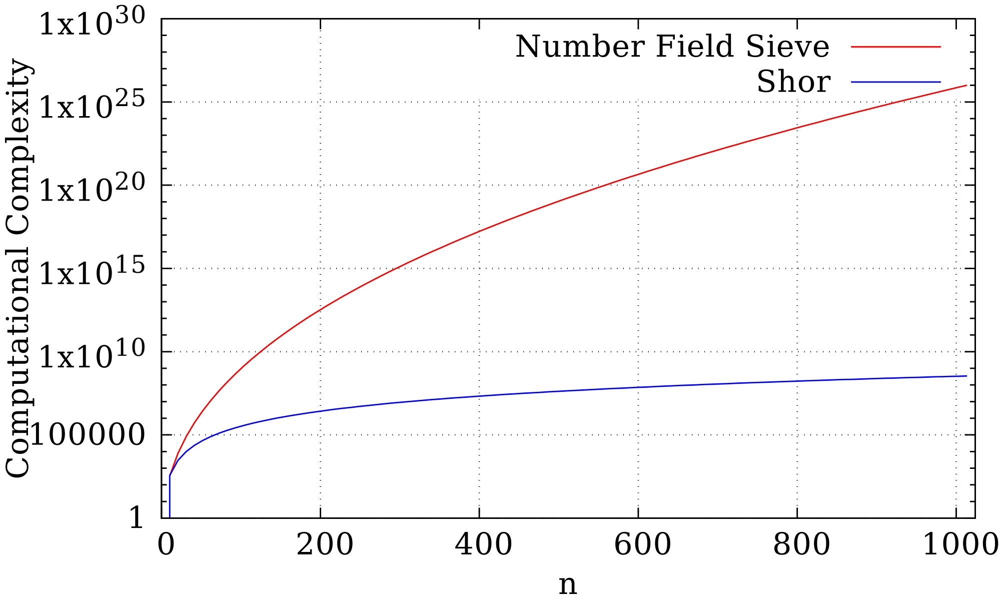


Figure 2.1: Computational complexity of the NFS and Shor's algorithm for a n-bit number.

2.2 Quantum Mechanical Fundamentals

2.2.1 States, Operators and Measurements

In quantum information in general it is common to work with two-state systems following classical computing with a bit as basic information unit. A classical bit can be 0 or 1 expressed usually through low voltage or high voltage in modern computers. In quantum information one introduces a **qubit** (or quantum bit) as a new basic information unit. Analogous to classical computing one defines the **computational basis** with its basis states $|0\rangle$ or $|1\rangle$ in Dirac's bra-ket notation. The huge advantage of quantum information is, that the system can be in state $|0\rangle$, $|1\rangle$ or any linear superposition of both. Thus a general state becomes

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.3}$$

The coefficients α and β are in general complex probability amplitudes and fulfil the normalisation condition

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.4}$$

The corresponding column vectors (see figure 2.2) of these basis states can be written as:

$$|0\rangle \mathrel{\widehat{=}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{and}\, |1\rangle \mathrel{\widehat{=}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.5}$$

If this basis is rotated by an angle of 45° one gets another set of basis states: $\left|\bar{0}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ and $\left|\bar{1}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$. Because $|0\rangle$ and $|1\rangle$ are eigenvectors of the Pauli matrix Z and $\left|\bar{0}\right\rangle$ and $\left|\bar{1}\right\rangle$ are eigenvectors of the Pauli matrix X one usually

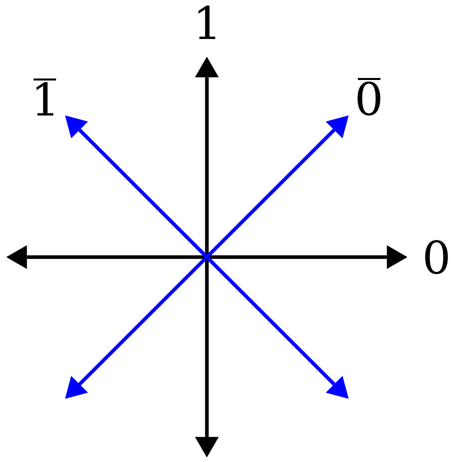


Figure 2.2: The eigenstates of Z (black) and X (blue) in vector representation.

calls these bases Z and X basis respectively.

In general a qubit is a vector in Hilbert space with dimension $d \leq \infty$. The Hilbert space of a N-qubit system has dimension $d = 2^N$, that means for a single qubit $d = 2$.
An operator **Q** in quantum mechanics is a linear map in Hilbert space. For a d-dimensional Hilbert space operators are $d \times d$ complex matrices fulfilling the eigenvalue equation:

$$\boldsymbol{Q}\left|\psi_i\right\rangle = q_i \left|\psi_i\right\rangle \tag{2.6}$$

$\left|\psi_i\right\rangle$ are called eigenstates of $\boldsymbol{Q}$ and q_i the corresponding (in general complex) eigenvalues. Note that there also exist operators without eigenstates (for example in quantum mechanics the creation operator $\hat{\mathrm{a}}^\dagger$). An important class of operators are self-adjoint operators, because they represent observables. Eigenstates of a self-adjoint operator are orthonormal or at least can be orthogonalised and normalised (the latter case only if d is finite), so eigenstates fulfil $\left\langle \psi_i \,\middle|\, \psi_j \right\rangle = \delta_{ij}$ and form a basis of the Hilbert space. The eigenvalues of the operator are the possible results for a measurement. After a measurement the system will be in an eigenstate of the operator.

The probability of measuring state $|\psi\rangle$ when the system is in state $|\phi\rangle$ is given by

$$P\left(|\psi\rangle\right) = |\left\langle \psi \,\middle|\, \phi \right\rangle|^2 \tag{2.7}$$

This means for the computational basis the following: Consider the system is in state $|\psi\rangle$. The probabilities for measuring $|0\rangle$ or $|1\rangle$ in the Z basis (analogous relations follow for $\left|\bar{0}\right\rangle$ or $\left|\bar{1}\right\rangle$ in the X basis) are:

$$P\left(|0\rangle\right) = |\left\langle 0 \,\middle|\, 0 \right\rangle|^2 = 1 \qquad P\left(|1\rangle\right) = |\left\langle 1 \,\middle|\, 0 \right\rangle|^2 = 0 \qquad \text{if } |\psi\rangle = |0\rangle \tag{2.8}$$

$$P\left(|0\rangle\right) = |\left\langle 0 \,\middle|\, 1 \right\rangle|^2 = 0 \qquad P\left(|1\rangle\right) = |\left\langle 1 \,\middle|\, 1 \right\rangle|^2 = 1 \qquad \text{if } |\psi\rangle = |1\rangle \tag{2.9}$$

Measuring in the X basis while the system is in an eigenstate of Z (analogous relations follow for measuring in the Z basis while the system is in an eigenstate of X) will give the following results:

$$P\left(\left|\bar{0}\right\rangle\right) = |\left\langle \bar{0} \,\middle|\, 0 \right\rangle|^2 = \frac{1}{2} \qquad P\left(\left|\bar{1}\right\rangle\right) = |\left\langle \bar{1} \,\middle|\, 0 \right\rangle|^2 = \frac{1}{2} \qquad \text{if } |\psi\rangle = |0\rangle \tag{2.10}$$

$$P\left(\left|\bar{0}\right\rangle\right) = |\left\langle \bar{0} \,\middle|\, 1 \right\rangle|^2 = \frac{1}{2} \qquad P\left(\left|\bar{1}\right\rangle\right) = |\left\langle \bar{1} \,\middle|\, 1 \right\rangle|^2 = \frac{1}{2} \qquad \text{if } |\psi\rangle = |1\rangle \tag{2.11}$$

In other words: performing a measurement on a system in a basis when the system is not in an eigenstate of this basis will give complete random results with equal probability, namely one half.

An alternative explanation for this result is the Heisenberg uncertainty principle:

$$\langle(\Delta A)^2\rangle\langle(\Delta B)^2\rangle \geq \frac{1}{4}|\langle[A,B]\rangle|^2 \tag{2.12}$$

and the fact that X and Z do not commute, that means [X,Z] $\neq 0$. Bases with maximum uncertainty for eigenstates of other bases are called **mutually conjugated bases**. For long times the Heisenberg uncertainty was seen as a generic limit in quantum physics, but as it turns out this can be exploited in quantum information processing.

2.2.2 No-cloning Theorem

Another fundamental element of quantum mechanics (employed for quantum cryptography) is the No-cloning theorem. It states that no unknown quantum state can be perfectly copied. An intuitive proof works as follows:
Assume cloning of a quantum state would be possible. Then there exists a copying machine with the unitary operator $\boldsymbol{F}$, that

$$\boldsymbol{F}\,|O\rangle\,|X\rangle = |O\rangle\,|O\rangle \tag{2.13}$$

where $|O\rangle$ is the state to be copied and $|X\rangle$ an empty object (like a blank paper in a real photocopier). The outcome are two versions of $|O\rangle$. Copying $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ will give

$$\boldsymbol{F}\,|\psi\rangle\,|X\rangle = \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle \neq \alpha^2\,|0\rangle\,|0\rangle + \alpha\beta\,|0\rangle\,|1\rangle + \beta\alpha\,|1\rangle\,|0\rangle + \beta^2\,|1\rangle\,|1\rangle = |\psi\rangle\,|\psi\rangle \tag{2.14}$$

Hence it is not possible to clone any unknown quantum state. Note that most proofs of the No-cloning theorem use the unitary condition and not the linearity of quantum mechanics.

2.3 Quantum Key Distribution

Quantum Key Distribution (QKD)[3] can, as the name states, only perform a key exchange, so conventional cryptography is still required. As shown in the previous section the key exchange for the symmetric encryption will be a problem in the presence of a quantum computer, so that a quantum-safe key exchange is required. QKD together with AES or OTP forms quantum cryptography, which can guarantee secure communication by physical laws. The security of QKD is based on two basic principles of quantum mechanics: The No-cloning theorem and the Heisenberg-uncertainty (see previous sections). As long as quantum mechanics holds, QKD will in principle be secure and of course it is believed that quantum mechanics will also hold in the future.

2.3.1 The BB84 Protocol

The BB84 protocol was the first scheme for Quantum Key Distribution developed by Charles Bennett and Gilles Brassard in 1984[21] (originally published in 1983[22]). For the protocol four different states in two conjugated bases are required: $|0\rangle$, $|1\rangle$, $\left|\bar{0}\right\rangle$ and $\left|\bar{1}\right\rangle$. As one usually wants to communicate over long distances, photons are basically the only feasible information carrier. Following the initial proposal in the BB84 protocol this work uses linear polarisation as degree of freedom of the photons for encoding the states with the following assignment: $|H\rangle = |0\rangle$, $|V\rangle = |1\rangle$, $|P\rangle = \left|\bar{0}\right\rangle$ and $|M\rangle = \left|\bar{1}\right\rangle$. Note that for example phase[23] or frequency[24] are feasible degrees of freedoms as well. For the protocol single photon states are assumed where the polarisation of each single photon can be chosen individually. In all other degrees of freedom the photons are indistinguishable.
For example Alice can send $|0\rangle$ and if Bob measures along Z he will always get $|0\rangle$. If he measures along X he will get $\left|\bar{0}\right\rangle$ and $\left|\bar{1}\right\rangle$ with equal probability. If there is an eavesdropper (Eve) present, then she could launch a naive intercept-and-resend-attack. Due to the No-cloning theorem she cannot produce copies of the photon, that means she guesses Alice's basis choice, measures the photon and according to the measurement outcome Eve has to re-prepare the state and forward it to Bob. Then the following situation can happen: Alice sends $|0\rangle$, Eve measures along X (on average in 50 % of the cases Eve will make the wrong basis choice) and then forwards $\left|\bar{0}\right\rangle$ or $\left|\bar{1}\right\rangle$. If Bob then measures along Z he will get $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$ for each state, as the system was now in an eigenstate of X. But the probability for measuring $|1\rangle$ when Alice sends $|0\rangle$ is zero without the presence of an eavesdropper. So overall this eavesdropping strategy introduces an average error of 25 % which is also called the **Quantum Bit Error Ratio** or **QBER**. Note that there exist more sophisticated attacks (coherent and individual) which can reduce the introduced error ratio to 11 %[3]. Nevertheless the QBER can always be used to find an upper bound of Eve's suspected information.

For exchanging a secret key Alice and Bob perform the following steps (see also table 2.3):

1. Alice and Bob agree that each state corresponds to a certain bit value, for example $|0\rangle$ and $\left|\bar{0}\right\rangle$ correspond to logical bit 0 while $|1\rangle$ and $\left|\bar{1}\right\rangle$ correspond to logical bit 1.

2. Alice prepares randomly one of the four states in one of the two bases and sends this state through a quantum channel to Bob.

3. Bob chooses randomly a basis in which he will measure the qubit from Alice.
→ If he chooses the same basis as Alice he will get an unambiguous result.
→ If he chooses the conjugated (other) basis he will get a totally random result.

4. Alice and Bob repeat the second and third step until they have a list of bit pairs (basis bit and bit value).

5. Then Bob announces publicly in an authenticated classical channel when he received a qubit and in which basis he performed his measurement.

6. Alice deletes all events when Bob did not receive any qubit and confirms whenever her basis bit was the same as Bob's basis bit, all other events are also deleted.

7. Bob also deletes all events, whenever his basis bit was not equal to Alice's basis bit.

Alice's basis	X	X	X	Z	Z	X	Z	X	X	X
Alice's bit	0	1	1	0	1	0	1	0	0	1
Bob's basis	Z	X	Z	Z	Z	X	X	X	X	Z
Bob's result	0	1	1	0	1	0	0	0	0	0
sifted key		1		0	1	1		0	0	

Table 2.3: An example of a key exchange according to the BB84 protocol. Always when Alice and Bob make the same basis choice they generate a new bit for the key. The exchanged key in this example is 101100.

The classical post-processing is called **key sifting**. The authentication is performed via a previously shared secret key. For example if Alice and Bob have an initial secret 256 *bit*-key they can hash their classical communication and encrypt the hash-value with this pre-shared key. Therefore QKD is sometimes also called secret key expansion. It does not matter whether the public channel is being eavesdropped, as long as it is authenticated (to prevent the Man-in-the-middle attack).
In principle Alice and Bob now should have two equal lists. They can check whether there was an eavesdropper by randomly comparing bit values and estimating the QBER. In practice they will use an efficient **error correcting algorithm** for this, but the principle stays the same. Depending on the error ratio they will also apply other classical algorithms which will be explained in the next section.

2.3.2 Realistic Devices

In theory Quantum Key Distribution as described above is perfectly secure. Unfortunately realistic implementations differ from the theoretic description of the devices. Still, a secure key exchange is possible even with practical devices, but one has to understand the differences to the theoretic description very well.

Single Photon Source

It is very important that single photon states are used. Otherwise Eve could block all single photon pulses and always keep one photon from a multi photon state and store this photon in an optical quantum memory letting all the other photons pass to Bob. After the basis announcement Eve could then measure the stored photons in the now publicly known correct basis and thus gaining full information without introducing any noise to the key. This is known as the so-called Photon Number Splitting (PNS) attack or memory attack.

As there is no practical single photon source available yet one can make recourse to weak coherent laser pulses. Weak in this manner means a mean photon number below one. A laser emits coherent states, so the number of photons in a laser pulse is Poisson-distributed:

$$P_\mu(n) = \frac{\mu^n}{n!} e^{-\mu} \tag{2.15}$$

P is the probability of having n photons in one pulse while μ denotes the average number of photons per pulse. Note that $P_\mu(1) \neq 0$ also implicates $P_\mu(2) \neq 0$. If μ is chosen sufficiently small then $P_\mu(1) = \mu e^{-\mu} \approx \mu$ and $P_\mu(2) = \frac{\mu^2}{2} e^{-\mu} \approx \frac{\mu^2}{2}$, so $P_\mu(2)$ (and of course $P_\mu(n > 2)$) are negligibly small. In this scenario a lot of pulses contain no photon at all and looking at $\frac{P_\mu(1)}{P_\mu(2)} = \frac{2}{\mu}$ shows that in those pulses with photons the fraction of more than one photon is large. Lowering the average number of photons per pulse seems to solve this problem, but one consequence is a low key rate due to even more empty pulses.

An expedient to use a reasonable mean photon number (on the order of 10^{-1}) is the Decoy State Protocol (DSP)[25]. This additional protocol uses the idea of QKD: To send non-orthogonal, not perfectly distinguishable states in the photon number basis to detect a PNS attack. A decoy state is a state with different intensity ($\mu_{decoy} \neq \mu_{state}$ and $|\langle \mu_{decoy} \,|\, \mu_{state} \rangle|^2 \neq 0$). Note that $|\langle \mu_{decoy} \,|\, \mu_{state} \rangle|^2 \neq 0$ implies that a decoy state cannot be distinguished perfectly from a signal state. An alternative to the normal DSP is the decoy detector method, where detectors with varying detection efficiencies are used[26]. In detail the protocol works as follows:

1. Alice sends states as in BB84 protocol, randomly a signal state (normal faint laser pulse) or a decoy state.
2. Bob measures as in BB84 protocol.
3. After transmission during the public discussion Alice announces which state a signal state was and which state a decoy state.
4. Hence Alice and Bob can estimate from the detection probability the transmission probability for signal and decoy states.
5. Finally they compute a lower bound for the transmission of single photons.

When Eve tries a photon number splitting attack she *a priori* cannot know whether the state was a signal state with more than one photon or a decoy state. So if Eve resends one out of two photons and blocks all single photon states the statistic of the pulses changes and therefore the attack will be detected. The multi photon states will reach Bob with a higher probability than single photon states, that means the transmission for decoy and signal states will be different. Note that in practice one normally uses a mixture of different intensities (vacuum state, decoy state, signal state) with different weights. It is also possible to use $\mu_{decoy} < \mu_{signal}$ which is in practice often the case to get higher key rates[27]. With the decoy protocol higher mean photon numbers are possible. In this work the decoy protocol was not implemented, so the used mean photon number was below the in principle possible one. Future improvements could thus improve key rate. Decoy states can also be implemented by turning on two lasers at the same time[28].

Side Channels and other Attacks

One has also to be very careful that the photons are indistinguishable in all degrees of freedom except for polarisation (or the specific degree of freedom in which the key is encoded). Otherwise so-called side channels are opened for Eve. Measuring in another degree of freedom does in principle not change the polarisation (that means the measurement operator commutes with the polarisation measurement operator) and if the states are distinguishable in this degree of freedom Eve gets full information about the key and can re-prepare the correct states and forward them to Bob and thus this eavesdropping attempt stays unrecognised. Examples are spatial, temporal or spectral side channels.

There is also the possibility for eavesdropping strategies, where not the photons themselves are attacked, but information about the key is obtained from the devices itself. Eve can route light into the transmitter or receiver and analyse the back-reflected light, to read out which laser just flashed or which detector clicked[3] or to launch a detector blinding attack[29][30]. These attacks can be classified as Trojan horse attacks. Analysing the light emitted by the receiver caused by light from the detectors during breakdown is also a possibility[31] as well as exploiting detection efficiency mismatches[32][33][34]. Once one knows about these side channels or attacks one can always apply an appropriate counter measure, for example interference filters, neutral density filters and optical isolators to reduce the amount of additional incoming and outgoing light into the devices as well as filtering (e.g. temporally and spatially). Ultimately with the damage threshold of the used components together with filters and isolators one can compute an upper bound for the leaked information and reduce this amount with privacy amplification to zero[35]. Hence at least these kinds of trojan horse attacks can be ruled out.

There is also the possibility of unconditional security with realistic devices, called Device Independent QKD (DIQKD)[36] (see also the next section), where one uses entangled photons and the security is based on the violation of Bell's inequality, which is of course device independent. Although there have already been experimental demonstrations of measurement DIQKD[37], in practical scenarios this is yet infeasible. Linear photonic Bell-state measurements work only probabilistically, highly efficient single photon detectors and for long distances quantum repeaters with quantum memories would be required.

Natural Error Rate

In a practical scenario Alice and Bob will always measure a non-zero QBER even without the presence of an eavesdropper. The main reasons are imperfect polarisation preparations at Alice's side, polarisation rotations in birefringent quantum channels (e.g. glass fibres), imperfect polarisation analysis and dark count events in the detectors at Bob's side. As one can never distinguish between a natural error and an error introduced due to the presence of an eavesdropper one has to assign every error due to the presence of an eavesdropper. As already mentioned there exist efficient error correcting algorithms (like CASCADE[38], Winnow[39] or LPDC[40]) capable of correcting an error at a certain QBER. Which error correcting algorithm one has to apply depends on the QBER since these algorithms are differently efficient at different QBERs.

The suspected information leakage to an eavesdropper can be reduced to zero via **privacy amplification**. The principle of privacy amplification is the following: Assuming that Eve knows one of $2\,bit$, but it is unknown which, then Alice and Bob can replace both bits through the XOR value of these bits. Of course Eve knows now that both bits have the same value, so one has to be discarded. In this case all information of Eve is erased. Of course this works only if the mutual information of Alice and Bob is larger than the mutual information of Alice and Eve and the mutual information of Bob and Eve.

In practice Alice and Bob will use a matrix approach. If the key length is n bit long and Eve knows about $k < n$ bit, then the key has to be shortened by $m = n - k$. For shortening the initial key K^i in a binary vector representation, it is multiplied by a m×n Matrix with binary entries, such that for each element of the final key K^f_k the following relation holds:

$$K^f_k = \left(\sum_{j=0}^{N} M_{k,j} K^i_j \right) \bmod 2 \tag{2.16}$$

The last modulo 2 operation ensures to get a binary key. As matrix a Töplitz-matrix $M = T$ defined as

$$T_{i,j} = T_{i+1,j+1} \qquad \forall\ i \in \{1, ..., m\} \, \text{and} \ j \in \{1, ..., n\} \tag{2.17}$$

is usually used. The advantage is less memory requirements and faster matrix multiplication.

Both privacy amplification and error correction will shorten the key and will only work if QBER $<$ 11 % (for more details see also section 2.3.4).

2.3.3 Other Protocols

The BB84 protocol is now more than 30 years old. During these years a large variety of different protocols have been developed. One distinguishes between two categories of protocols: prepare-and-measure protocols (as BB84) and entanglement-based protocols. For the sake of completeness a few other protocols shall be introduced briefly.

The 3-State protocol

There is also a BB84-related protocol called the 3-State protocol[41] which is the BB84 protocol with only three of the four states, for example $|H\rangle$, $|V\rangle$ and $|M\rangle$. Then the key is encoded in the Z basis, while the state in the X basis is only sent for the security check. Usually this protocol is used when in a BB84 transmitter one of the four laser sources is out of operation (or equivalently one detector in the receiver) or in frequency-based QKD systems[42] where the three states can be prepared easily.
As shown in sections 3.3.6 and 3.4.3 one of the four states in this experiment has a high QBER which results in a high average QBER and thus in a low secret key rate. The state with the high QBER can be left out in the 3-State protocol and thus using this protocol could result in a higher secret key rate, because the QBER is now lower. As it was not clear until the final experiment whether the 3-State protocol or the BB84 protocol yields a higher key rate this protocol is introduced here as well. In section 3.4.3 it is shown that the BB84 protocol leads indeed to a higher secret key rate than the 3-State protocol, so for the final experiment the BB84 protocol has been used, but as some measurements intermediately indicated (wrongly) a higher secret key rate for the 3-State protocol sometimes measurements only for three states have been performed. The security proof for this protocol differs from the proofs for BB84 and in general this protocol will have a lower key rate than BB84 with equal QBER. For more details about the secret key rates in both protocols see section 2.3.4.

Six-state

The Six-state protocol[43] is an easy modification of the standard BB84 protocol. The only difference is, instead of using four states in two different bases it uses six states in three different bases. The bases have to be pairwise conjugated with each other. The advantage is, that an eavesdropper causes a QBER of 33 % instead of 25 % (with a normal intercept-and-resend attack) and is therefore easier to detect. The disadvantage is, that the sifted key ratio lowers to 33 % instead of 50 %, because Bob chooses only in 33 % of all detections the same basis as Alice chose. The lower key ratio is the reason why the Six-state protocol is typically not commonly used. With polarisation encoding circular polarisation serves as a third mutually conjugated basis.

Eckert91

An entanglement based protocol is the E91 protocol proposed by Arthur Ekert in 1991[44]. Alice and Bob share a pair of entangled states. Alice measures each received photon in a basis from the set Z_0, $Z_{22.5}$, Z_{45} while Bob measures each received photon in a basis from the set Z_0, $Z_{22.5}$, $Z_{-22.5}$ (Z_ϕ is the Z basis rotated by ϕ). Since the state is entangled they will get perfect correlation, if they measure in the same basis, otherwise they will get a random result. The same is true if they measure in any other polarisation basis. The key is encoded in Z_0 basis and the results at Alice and Bob in the other three bases have to violate a Bell inequality. An eavesdropping attack will determine local hidden variables and hence the Bell inequality would not be violated any longer. In principle the source of the entangled pairs could be under control of Eve, as long as the Bell inequality is violated, Eve cannot have any information about the results of Alice and Bob. As already mentioned this leads to DIQKD.

BBM92

The BBM92 protocol, named after Charles Bennett, Gilles Brassard and N. David Mermin proposed in 1992[45], is also an entanglement based protocol. This protocol is similar to the standard BB84, but again like in E91 protocol instead of sending a state to Bob, Alice and Bob share an entangled state. The difference between E91 and BBM92 is the security test: In BBM92 an eavesdropper is detected by the estimation of the QBER similar to the detection of the eavesdropper in the BB84 protocol.

This is of course not a complete list of protocols. Other famous classes of protocols are continuous variable QKD (CVQKD) protocols[46] and round robin differential phase shift (RRDPS) protocols[47] among others.

2.3.4 Calculation of the Key Rate

For calculating the key rate of a practical implementation of a QKD system one has to model all components: source, channel and detectors.

As already described in section 2.3.2 for a **weak coherent source** the photon number in each pulse is Poisson-distributed (equation 2.15) with a mean photon number μ.

The **channel** is described by the transmittance τ which is limited by the absorption in the channel.

On the **detector** (or receiver) side one has to multiply the transmittance with a factor t_{Bob} taking into account all optical losses in the receiver (for example at mirrors, lenses, wave plates, filters, glass fibre couplers) and with the quantum efficiency η of the single photon detectors. For a handheld scenario one has to multiply this transmittance also with a coupling efficiency due to handheld operation

g so that the total transmittance τ_{tot} is given by

$$\tau_{tot} = \tau \cdot t_{Bob} \cdot \eta \cdot g \tag{2.18}$$

Assuming a threshold detector, that means the detector can distinguish between a vacuum state and a non-vacuum state, but cannot count the number of photons in a pulse (although this is not forbidden by the laws of quantum mechanics and recently has been demonstrated[48], but this is not practical yet), then the transmittance of an n-photon state is given by

$$\tau_n = 1 - (1 - \tau_{tot})^n \qquad \forall\, n \in \mathbb{N}_0 \tag{2.19}$$

Remember that the number of photons in each pulse is Poisson-distributed, so each pulse can contain n photons. Note that the equation above assumes independence of the photons which is a reasonable assumption, as photons do not directly interact without light-matter interaction. With that one can define the **yield** Y_n of an n-photon state which is the probability for Bob detecting an event with the condition that Alice has sent an n-photon state:

$$Y_n = Y_0 + \tau_n - Y_0 \cdot \tau_n \approx Y_0 + \tau_n \tag{2.20}$$

where Y_0 is the yield of the dark counts. The approximation assumes $Y_0, \tau_n \ll 1$, which is in most experiments very well-justified. The probability, that Alice transmits a particular state and that this state is detected by Bob is called the **gain** Q_n of that particular state:

$$Q_n = Y_n \cdot P_\mu(n) \tag{2.21}$$

where $P_\mu(n)$ is the Poisson distribution (see equation 2.15). The total gain is then simply the sum over all states n:

$$Q_\mu = \sum_{n=0}^{\infty} Q_n = 1 + Y_0 - e^{-\tau_{tot}\mu} \tag{2.22}$$

The last equality follows analytically from a few lines of calculation.
Finally the QBER E in general is defined as

$$E = \frac{\text{number of false bit}}{\text{number of all bit}} \tag{2.23}$$

For the 3-State protocol, where the key is encoded only in one basis and the state in the conjugated basis is sent only for the security check, one distinguishes between the error ratio in the Z basis (that means of $|H\rangle$ and $|V\rangle$) and the error ratio in the X basis (that means the error of $|M\rangle$). These error ratios are called α and e_b respectively (in analogy to the security proof of the 3-State protocol[41]). The phase error ratio e_p can be upper-bounded:

$$e_p \leq \alpha + 2e_b + 2\sqrt{e_b\alpha} \tag{2.24}$$

The derivation for this inequality can be found in [41]. A special case is $e_b = \alpha$ which implicates that

$$e_p \leq 5e_b \tag{2.25}$$

Note that for the normal BB84 protocol $e_p = e_b$ which shows the superiority of the BB84 protocol over the 3-State protocol, as the error ratio used for privacy amplification is five times lower, which is not intuitive at first glance. The vivid explanation is the following: Assume Alice sends randomly $|H\rangle$, $|V\rangle$ or $|M\rangle$. If Eve makes a normal intercept-and-resend-attack and randomly measures in the Z and X basis she will guess the basis wrongly on average in half of the cases. If she chose the X basis and measures $|P\rangle$ she does not know the sent state, but she knows that her basis choice was wrong as she measured a state orthogonal to $|M\rangle$ and she can simply block this pulse (that means not resending anything). In a normal BB84 protocol this information can never be obtained. Thus the introduced error in the key will be smaller and therefore one needs more privacy amplification in the 3-State protocol compared to the BB84 protocol. However, this argument is not sufficient to explain the five times higher amount of privacy amplification.
Finally one can find a lower bound for the secret bit per sent bit:

$$R \geq \max\left\{\frac{1}{2}\left[-Q_\mu f\left(e_b\right)h_2\left(e_b\right) + Q_1\left(1 - h_2\left(e_p^1\right)\right)\right], 0\right\} \tag{2.26}$$

where the factor of $\frac{1}{2}$ is due to a symmetric basis choice, $f\left(e_b\right)$ is the efficiency of the error correcting algorithm capable correcting a code at an error ratio of e_b and $h_2\left(p\right)$ denotes the binary Shannon entropy function:

$$h_2\left(p\right) = -p\log_2\left(p\right) - \left(1-p\right)\log_2\left(1-p\right) \tag{2.27}$$

and e_p^1 is the phase error ratio on the single photon states (as one has to assume that all errors originate in the worst case from single photon states):

$$e_p^1 \leq e_p \cdot \frac{Q_\mu}{Q_1} \tag{2.28}$$

The secret key rate R_{secret} is then given by R times the sent bit per second, that means the laser repetition frequency f_{laser}:

$$R_{secret} \geq \max\left\{\frac{1}{2}\cdot f_{laser}\left[-Q_\mu f\left(e_b\right)h_2\left(e_b\right) + Q_1\left(1 - h_2\left(e_p^1\right)\right)\right], 0\right\} \tag{2.29}$$

For evaluating the secret key rate from a measured sifted key rate it is more convenient to rewrite equation 2.29 with $Q_1/Q_\mu = (1-\Delta)$:

$$R_{secret} \geq \max\left\{\frac{1}{2}\cdot f_{laser} Q_\mu \left[-f\left(e_b\right) h_2\left(e_b\right) + (1-\Delta)\left(1 - h_2\left(\frac{e_p}{1-\Delta}\right)\right)\right], 0\right\} = \tag{2.30}$$

$$= \max\left\{\frac{1}{2}\cdot f_{laser} Q_\mu \left[1 - f\left(e_b\right) h_2\left(e_b\right) - \Delta - (1-\Delta) h_2\left(\frac{e_p}{1-\Delta}\right)\right], 0\right\} = \tag{2.31}$$

$$= \max\left\{R_{sifted}\left[1 - f\left(e_b\right) h_2\left(e_b\right) - \Delta - (1-\Delta) h_2\left(\frac{e_p}{1-\Delta}\right)\right], 0\right\} \tag{2.32}$$

The parameter Δ is the probability for a multi photon pulse divided by the probability that an emitted photon is detected:

$$\Delta = \frac{P_\mu\left(n>1\right)}{\tau_{tot} P_\mu\left(n>0\right)} \tag{2.33}$$

This parameter has to be subtracted from the sifted key, as in equation 2.32 the overall gain adds positive to the key and not only the gain of the single photon states as in equation 2.29. This has to be taken into account because one has to allow Eve launching a PNS attack on each multi photon state. The probability that an emitted photon is detected enters into the equation since a PNS attack only affects the security if Bob detects something. Note that the parameter Δ already sets a lower bound on the transmission or an upper bound on the average mean photon number per pulse for a given τ_{tot} as it requires

$$\Delta < 1 \Rightarrow \frac{P_\mu\left(n>1\right)}{P_\mu\left(n>0\right)} = 1 - \frac{\mu}{e^\mu - 1} < \tau_{tot} \tag{2.34}$$

otherwise the secret key rate will always be zero. Sometimes the parameter Δ is also called the fraction of *tagged bits*. Note that with the DSP a better bound on Δ can be found. The sifted key rate can also be approximated:

$$R_{sifted} = \frac{1}{2} f_{laser} P_{\mu\tau_{tot}}\left(n \neq 0\right) = \tag{2.35}$$

$$= \frac{1}{2} f_{laser}\left(1 - e^{-\mu\tau_{tot}}\right) \approx \tag{2.36}$$

$$\approx \frac{1}{2} f_{laser} \mu\tau_{tot} \tag{2.37}$$

where the approximation $e^{-x} \approx 1 - x$ if $x \ll 1$ has been used.

In general all parameters for equation 2.32 are obtained from the experiment. To estimate the transmission for the parameter Δ one can use the raw detection rate

R_{raw}:

$$\tau_{tot} \approx \frac{R_{raw}}{f_{laser}\mu} \tag{2.38}$$

which follows directly from equation 2.37 and

$$R_{sifted} = \frac{1}{2} R_{raw} \tag{2.39}$$

Hence the transmission and thus the parameter Δ varies with the raw detection rate.
Note that in a perfect scenario (BB84, protocol, error correction efficiency $f(E) = 1$, known as the Shannon limit[49], single photon source $P(n > 1) = 0 \Rightarrow \Delta = 0$) equation 2.32 simplifies to

$$R_{secret} \geq \max\left\{R_{sifted}\left[1 - 2h_2(E)\right], 0\right\} \tag{2.40}$$

Solving this equation for $R_{secret} = 0$ gives the well-known error bound of 11.0 %.

2.4 Quantum State Tomography

For calculating the source-intrinsic QBER the states emitted from the transmitter unit have to be characterised and if necessary corrected. Responsible for the source-intrinsic QBER is mainly wrong polarisation preparation or polarisation rotations in the transmitter. For describing polarisation and polarisation changes one can utilise the Stokes formalism and Mueller calculus. Initially developed for classical light waves the formalism can directly be adopted to quantum light (or to the single photon level) as the light intensity I is proportional to the photon number n:

$$I \propto n \tag{2.41}$$

Hence for **quantum state tomography** it is sufficient to average over a large number of photons (it is impossible to measure the complete unknown polarisation state of a single photon). The following formalism can be directly applied.

2.4.1 Stokes parameter

The **Stokes parameter** is a set of four variables which fully describe the polarisation of a state. It is defined as

$$\vec{S} = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} I_H + I_V \\ I_H - I_V \\ I_P - I_M \\ I_R - I_L \end{pmatrix} \tag{2.42}$$

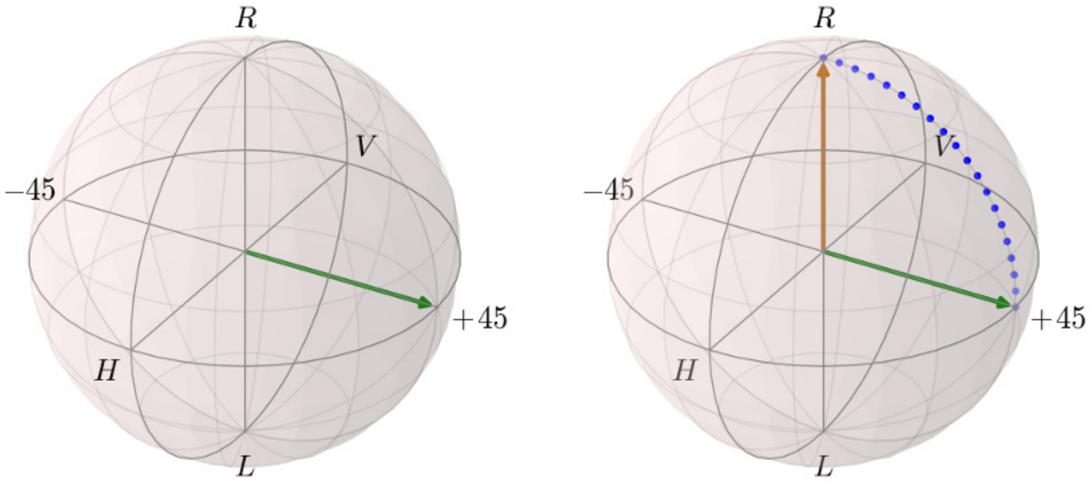
with I_H, I_V, I_P, I_M, I_R and I_L being the intensities of the projections onto the six polarisation basis states. Note that $I_H + I_V = I_P + I_M = I_R + I_L$. Often it is convenient to work with a normalised Stokes vector:

$$\vec{S}_N = \frac{1}{S_0}\begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1 \\ \frac{I_H - I_V}{I_H + I_V} \\ \frac{I_P - I_M}{I_P + I_M} \\ \frac{I_R - I_L}{I_R + I_L} \end{pmatrix} \tag{2.43}$$

Note that sometimes the Stokes vector is also defined via the polarisation ellipse and not via the projections. The **degree of polarisation** Π (DOP) is then given by

$$\Pi = \frac{\sqrt{S_1^2 + S_2^2 + S_3^3}}{S_0} \tag{2.44}$$

In the normalised version S_0 is equal to unity. The Stokes vector can easily be visualised on the **Poincaré sphere** (see figure 2.3 (a)): The components $-1 \leq S_1, S_2, S_3 \leq 1$ are the three Cartesian coordinates. Π is then the length of the vector. Fully-polarised light ($\Pi = 1$) lies on the sphere, while partially-polarised light ($\Pi < 1$) lies within the sphere. The origin describes unpolarised light ($\Pi = 0$).



(a) Visualisation of the state $|P\rangle = (0,1,0)^T$.

(b) Visualisation of the rotation from the state $|P\rangle = (0,1,0)^T$ to $|R\rangle = (0,0,1)^T$ via a quarter wave plate with the fast-axis being vertical.

Figure 2.3: Poincaré sphere with different states and rotations.

2.4.2 Mueller calculus

A polarisation rotation on the Poincaré sphere (see figure 2.3 (b)) can be described with a 4 × 4 Mueller matrix M. The Stokes vector changes according to

$$\vec{S}_{out} = M\vec{S}_{in} \tag{2.45}$$

Every optical component has a corresponding matrix representation. In this work several matrices are used which shall be introduced in the following. The matrix for a rotated quarter and half wave plate (angle α between fast-axis and H in both cases) have the following matrix representations respectively:

$$M_{\frac{\lambda}{4}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\alpha) & \sin(2\alpha)\cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha)\cos(2\alpha) & \sin^2(2\alpha) & \cos(2\alpha) \\ 0 & \sin(2\alpha) & -\cos(2\alpha) & 0 \end{pmatrix} \tag{2.46}$$

$$M_{\frac{\lambda}{2}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\alpha) - \sin^2(2\alpha) & 2\sin(2\alpha)\cos(2\alpha) & 0 \\ 0 & 2\sin(2\alpha)\cos(2\alpha) & \sin^2(2\alpha) - \cos^2(2\alpha) & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{2.47}$$

A general phase difference δ between H and V is introduced by the following matrix:

$$M_{\delta} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos(\delta) & -\sin(\delta) \\ 0 & 0 & \sin(\delta) & \cos(\delta) \end{pmatrix} \tag{2.48}$$

The most general arbitrary polarisation rotation on the Poincaré sphere can be performed with the three Euler angles α, β, γ for a (z, x', z")-rotation:

$$M_{Euler} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathrm{c}_\alpha\mathrm{c}_\gamma - \mathrm{s}_\alpha\mathrm{c}_\beta\mathrm{s}_\alpha & \mathrm{s}_\alpha\mathrm{c}_\gamma + \mathrm{c}_\alpha\mathrm{c}_\beta\mathrm{c}_\gamma & \mathrm{s}_\beta\mathrm{c}_\gamma \\ 0 & -\mathrm{c}_\alpha\mathrm{c}_\gamma - \mathrm{s}_\alpha\mathrm{c}_\beta\mathrm{c}_\gamma & -\mathrm{s}_\alpha\mathrm{c}_\gamma + \mathrm{c}_\alpha\mathrm{c}_\beta\mathrm{c}_\gamma & \mathrm{s}_\beta\mathrm{c}_\gamma \\ 0 & \mathrm{s}_\alpha\mathrm{s}_\beta & -\mathrm{c}_\alpha\mathrm{s}_\beta & \mathrm{c}_\beta \end{pmatrix} \tag{2.49}$$

where for the sake of clarity the following definitions have been introduced:

$$s_i = \sin(i) \qquad \text{for i} = \alpha, \beta, \gamma \tag{2.50}$$

$$c_i = \cos(i) \qquad \text{for i} = \alpha, \beta, \gamma \tag{2.51}$$

Any unitary transformation $U(\alpha, \beta, \gamma)$ can be decomposed into wave plate rotations, which is in general easier accessible as it consists only of standard optics:

$$U(\alpha, \beta, \gamma) = M_{\frac{\lambda}{2}}(\gamma)\, M_{\frac{\lambda}{4}}(\beta)\, M_{\frac{\lambda}{4}}(\alpha) \tag{2.52}$$

Note that this decomposition in wave plates is not unique.
A polarisation independent loss can be described by

$$M_{loss} = \begin{pmatrix} t & 0 & 0 & 0 \\ 0 & t & 0 & 0 \\ 0 & 0 & t & 0 \\ 0 & 0 & 0 & t \end{pmatrix} \tag{2.53}$$

with $0 \leq t \leq 1$ being the transmittance through the optical component. For light passing successively through different components the corresponding matrices can simply be multiplied. Note that matrix multiplication is associative, but in general not commutative!

2.4.3 QBER in the Stokes formalism

One advantage of this formalism is that the QBER of a state can directly be calculated from the normalised Stokes parameter. As the intensity is proportional to the photon number (equation 2.41), the probabilities of measuring H or V are given by

$$P(H) = \frac{I_H}{I_H + I_V} \tag{2.54}$$

$$P(V) = \frac{I_V}{I_H + I_V} \tag{2.55}$$

With

$$S_1 = P(H) - P(V) \tag{2.56}$$

$$1 = P(H) + P(V) \tag{2.57}$$

it follows that

$$P(H) = \frac{1 + S_1}{2} \tag{2.58}$$

$$P(V) = \frac{1 - S_1}{2} \tag{2.59}$$

Analogous relations follow for $P(P)$ and $P(M)$:

$$P(P) = \frac{1 + S_2}{2} \tag{2.60}$$

$$P(M) = \frac{1 - S_2}{2} \tag{2.61}$$

With the assumption that state i was sent with Stokes vector $\vec{S^{(i)}}$ where $i = H, V, P, M$ it follows that the QBERs E_i are given by

$$E_H = \frac{1 - S_1^{(H)}}{2} \tag{2.62}$$

$$E_V = \frac{1 + S_1^{(V)}}{2} \tag{2.63}$$

$$E_P = \frac{1 - S_2^{(P)}}{2} \tag{2.64}$$

$$E_M = \frac{1 + S_2^{(M)}}{2} \tag{2.65}$$

2.4.4 Jones formalism

In addition to the Stokes formalism and Mueller calculus there also exists the Jones calculus. The difference is, that the Jones calculus can only describe fully-polarised light, apart from that both formalisms give the same result. As the Jones vector is needed in section 5.1 the connection to the Stokes formalism shall be introduced briefly.

The electric field of a plane wave propagating in z-direction is given by

$$\vec{E} = \begin{pmatrix} E_x(t) \\ E_y(t) \\ 0 \end{pmatrix} = \begin{pmatrix} E_{0x}e^{i\phi_x} \\ E_{0y}e^{i\phi_y} \\ 0 \end{pmatrix} e^{i(kz-\omega t)} \tag{2.66}$$

The Jones vector is then simply the complex two-state vector

$$\vec{J} = \begin{pmatrix} E_{0x} \\ E_{0y}e^{i(\phi_y - \phi_x)} \end{pmatrix} \tag{2.67}$$

Note that only relative phases $\Delta = \phi_y - \phi_x$ have to be taken into account as global phases are not accessible in an experiment. It shall be mentioned that the Stokes vector can also be defined via the electric field as a real four state vector, which is equal to the definitions made in the previous sections. The following relations connect the Stokes and the Jones vector:

$$1 = E_{0x}^2 + E_{0y}^2 \tag{2.68}$$

$$S_1 = E_{0x}^2 - E_{0y}^2 \tag{2.69}$$

$$S_2 = 2E_{0x}E_{0y}\cos(\Delta) \tag{2.70}$$

$$S_3 = 2E_{0x}E_{0y}\sin(\Delta) \tag{2.71}$$

so that the components for the Jones vector are given by

$$E_{0x} = \sqrt{\frac{1 + S_1}{2}} \tag{2.72}$$

$$E_{0y} = \sqrt{\frac{1 - S_1}{2}} \tag{2.73}$$

$$\Delta = \tan^{-1}\left(\frac{S_3}{S_2}\right) \tag{2.74}$$

3 Experimental Part I: Setup

In this chapter the experiment shall be presented. First, the idea of the experiment is described followed by a report on the state of the experiment at the beginning of this thesis. Then the development, fabrication and characterisation of the transmitter and receiver is presented in detail. The final tests and results will be shown in the next chapter.

3.1 Idea of the Experiment

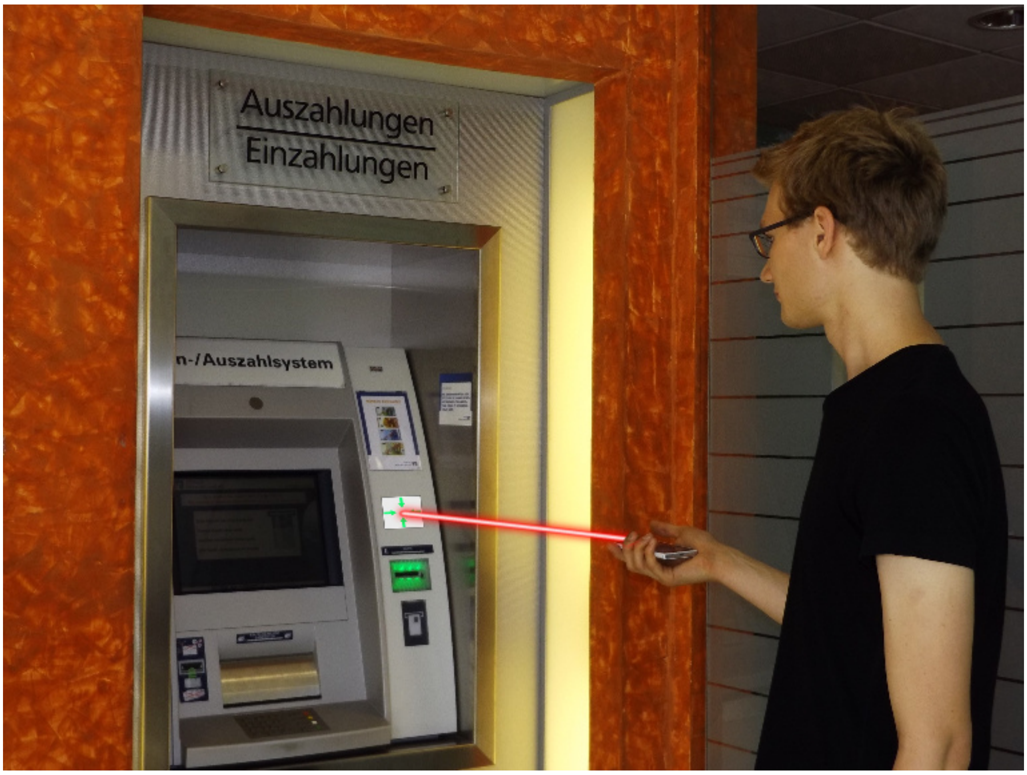


Figure 3.1: A practical scenario: A user authenticates his smart phone to an ATM.

As described in section 2.3 QKD can guarantee unconditional security. Most research is targeting long-range applications, such as long-distance communication or networks. The vision would be a complete quantum internet via fibre networks connected through satellite relay stations. But there also exists a large variety of

short-distance applications, for example for the mobile usage or as a quantum network interface.
This work focuses on a practical scenario where a user owns an integrated mobile device with which he can exchange on-demand a secure key with an authenticated receiver. A possible example is a user transmitting his credit card information secured by QKD to an ATM (see figure 3.1). For this a miniaturised sender unit is required while all bulky optical and expensive components must be kept at the receiver side. In the ideal case the sender is integrated into existing technology (for example into a smart phone).

3.1.1 Design of the Transmitter

Implementing the BB84 protocol (or the 3-State protocol) the transmitter needs to provide the four (three respectively) differently polarised basis states. This can be achieved by either manipulating the polarisation of a single laser (with an electro-optical modulator) or using differently polarised lasers which are spatially overlapped. In this implementation the latter approach has been used which is in general the easier way.

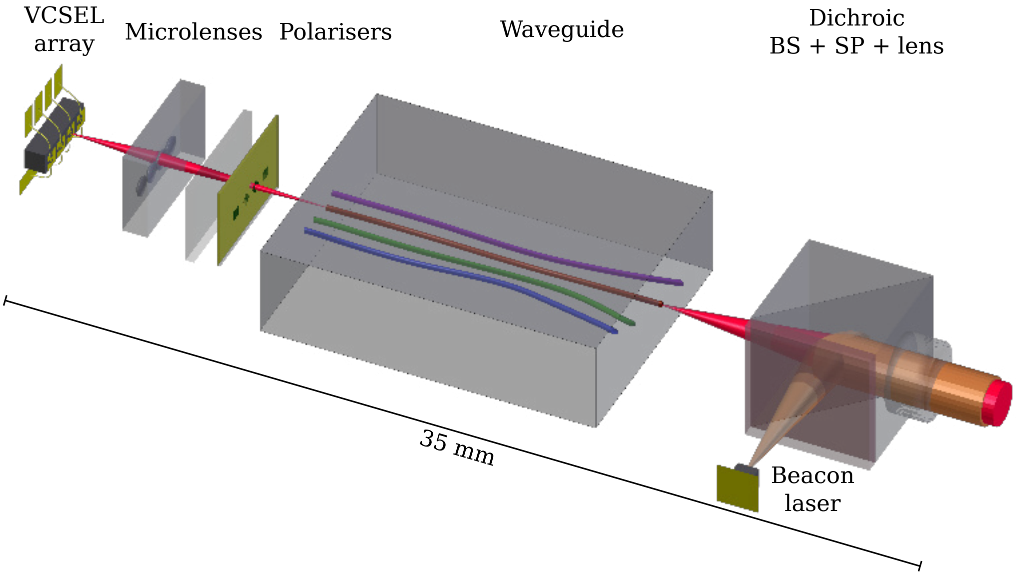


Figure 3.2: Experimental design of the transmitter. BS: beam splitter, SP: short-pass filter. The single components are not to scale. Total size approximately: $35 \times 10 \times 3\,mm^3$.

The different states are generated by an array of vertical-cavity surface-emitting lasers (VCSELs) at an operating wavelength of $850\,nm$ (see figure 3.2). Via an array of microlenses the different laser beams are focused through a micro-polariser array onto four different input ports of a waveguide chip array which spatially overlaps the four beams using 50:50 beam splitters (BS) combining the light into a single main output. Of course, as regular beam splitters this structure also has four output ports. These ports must, except for the main output, be blocked. An additional bright visible beacon laser is overlapped at a dichroic beam splitter (DBS) with the signal photons allowing both efficient beam tracking and controlling as well as pulse synchronisation. The beacon laser is spectrally filtered by a shortpass filter to suppress noise at the operating wavelength of the VCSELs. Finally, after the DBS both beams are collimated with an outcoupling lens. All components are arranged on a micro-optical bench. The module can, in principle, be controlled by an Android-App.

3.1.2 Quantum and Classical Channel

For a handheld scenario with integrated mobile devices free space is a natural choice as a quantum channel as no fibre connection is required. As already mentioned the signal photons have a wavelength of 850 *nm*. This has two reasons: On the one hand air has a transmission window around 850 *nm* (see figure 3.3). On the other hand for light at at 850 *nm* there are good single photon detectors with high quantum efficiencies commercially available. For the classical channel some kind of wireless communication must be used (otherwise one looses the advantage of the free space

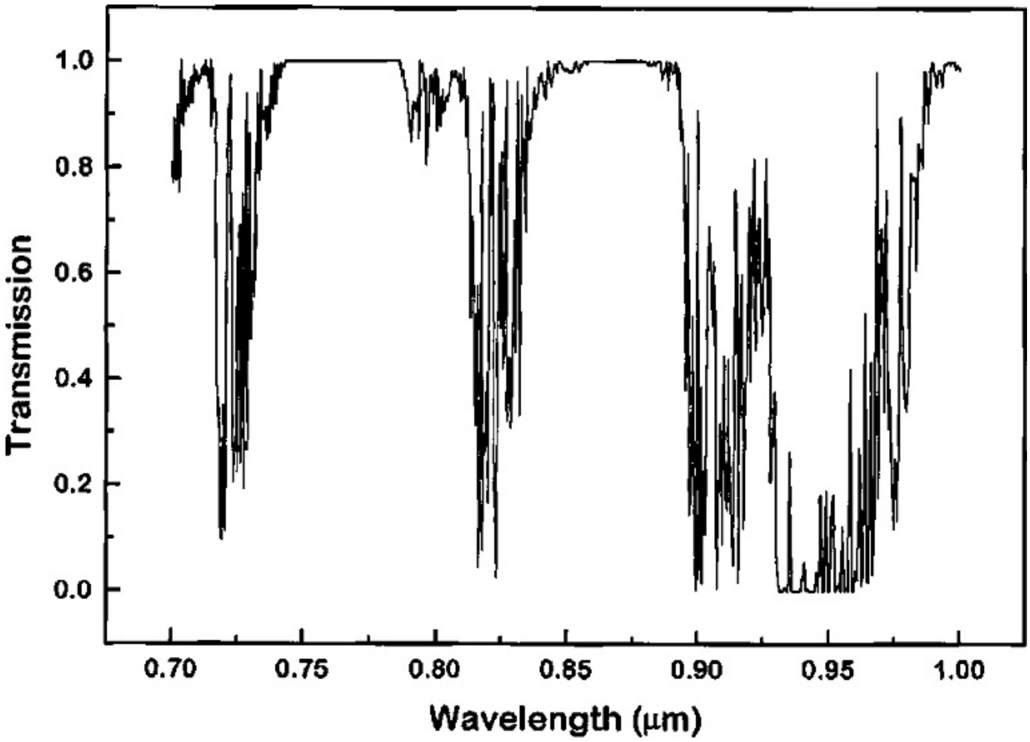


Figure 3.3: Transmission of optical and near infra-red (NIR) light in free space as calculated using the LOWTRAN code for earth-to-space transmission at the elevation and location of Los Alamos, USA. Taken from [3].

quantum channel), so in this case using Wi-Fi as a classical channel is an appropriate choice. One more advantage is that modern Wi-Fi networks can reach data rates up to 600 $Mbit/s$ (IEEE 802.11n)[50].

3.1.3 Design of the Receiver

The main part of the receiver is a standard BB84 polarisation analysis unit (see figure 3.4): A 50:50 beam splitter makes a passive basis choice ensuring true randomness in Bob's basis choice. In one arm of the beam splitter another polarising beam splitter (PBS) transmits H-polarised light while reflecting V-polarised light and thus this PBS allows to measure in the Z basis. The photons are then detected by two fibre-coupled avalanche photodiodes (APDs) in each arm of the PBS. In the other arm of the BS a half wave plate (with an angle of 22.5° between H and the fast-axis) rotates the polarisation by 45°. Thus this wave plate performs a basis transformation Z ⇔ X. In quantum information this is known as the Hadamard-transformation. Therefore another PBS and two fibre-coupled APDs detect P- and M-polarised light.

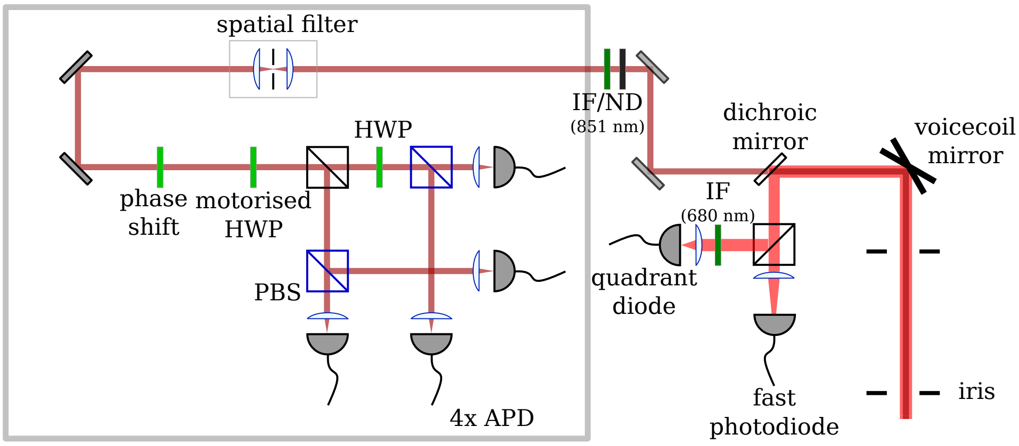


Figure 3.4: Experimental design of the receiver. IF: interference filter. ND: neutral density filter. HWP: half wave plate. PBS: polarising beam splitter. APD: avalanche photodiode.

In principle this is already sufficient for the BB84 protocol, but for a practical implementation one needs some additional features, such as a beam tracking and controlling system[51] and a dynamic basis alignment to allow user-friendly operation, clock and pulse synchronisation with the transmitter, spatial filtering to prevent spatial mode side channels[34] and a phase shift to compensate for polarisation rotations.

It shall be mentioned, that the polarisation rotation of phase shift and of the motorised HWP do not commute. Therefore the order of both transformations must be exchanged, which was in the experiments not the case!

3.2 State of the Experiment

In this section the state of the experiment at the time of the beginning of this work shall be presented briefly. There will also be a list of the remaining main tasks which are addressed in this work. Note that this thesis is based on [33], [34], [51] and [52]. It shall be further mentioned that the work described in section 3.2.1 as well as the design of the polarisers was done by Gwenaelle Mélen (see also reference [53]). The fabrication and characterisation of the polarisers (section 3.3.2), as well as the assembly of the micro-optics (section 3.3.5) and parts of the characterisation of the complete module (section 3.3.6) was done in cooperation with Gwenaelle Mélen (some additional details might be found in reference [53]).

3.2.1 State of the Transmitter

VCSELs

In this experiment an array of 12 single-mode (Laguerre-Gaussian intensity profile) VCSELs from VI Systems (Model V25A-850C12SM) with a high modulation speed of 28 $Gbit/s$ is used as a laser source, of which only four of the VCSELs are active. The advantage of using one array instead of four single VCSELs is on the one hand of course that such an array has far less space requirements, as these VCSELs can be packed very closely (in this array they have a spacing of 250 μm). On the other hand the hope is that the emission properties of the VCSELs from a single array are maximally equal for all of them.

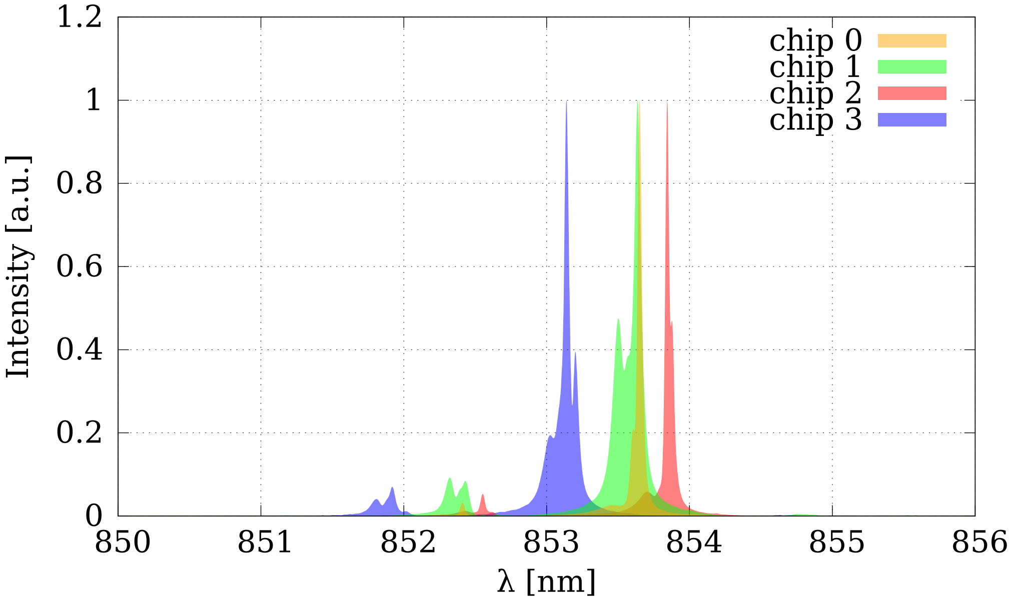


Figure 3.5: Normalised spectrum using a Fourier Transform Infra-Red spectrometer (FTIR).

It turned out that the polarisation of a pulse depends on its length[52]. Operated in CW-mode, the VCSELs are polarised along H with a degree of polarisation $\Pi = 90\,\%$. In contrast, if operated in pulsed mode Π decreases as the pulse length decreases. For an optimal pulse length of $46\,ps$ the DOP is only $\Pi = 5\,\%$. For the final shape of the pulses see section 3.3.6.
If one measures the spectrum with a high resolution one sees a difference in the spectrum of the VCSELs and thus this opens a spectral side channel (see figure 3.5). Note that the spectral difference between channel 2 and channel 3 is only $0.71\,nm$. As proposed in [52] one could overcome this by individual thermal tuning of the spectrum exploiting the thermal shift of the VCSELs ($\Delta\lambda = 0.06\,nm \cdot K^{-1}$) or by using MEMS-tunable VCSELs (exploiting a micro-electro-mechanical effect for tuning the cavity length and thus the wavelength). The feasibility of these possibilities is calculated theoretically in section 6.1.

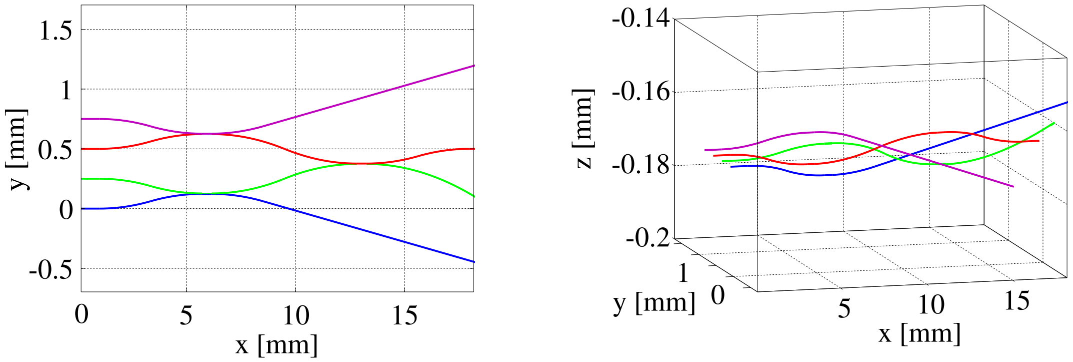
Driving Electronics

The driving electronics is PCB-based (Printed Circuit Board) and basically already completely designed (some minor changes have to be added, such as adding a laser driver for the beacon laser). The laser drivers slow the modulation speed of the VCSELs down to 4 GHz while the delay lines (with which the temporal shape of the pulses can be tuned) slow the modulation speed down to $100\,MHz$ (although they are capable of 3 GHz) which is then the final repetition rate of the module. Going to higher data rates in principle is possible, but using a smart phone for controlling the module the hardware resources limit the communication rates to $14.808\,Mbit/s$[54] and the maximal detection rates are limited by the read-out electronics and the dead time of the APDs even further to $4\,Mbit/s$.

Waveguide

The spatial overlapping of the pulses takes place in a femtosecond-pulsed laser-written waveguide[52] fabricated by Dr. Osellame's group at the Politecnico di Milano. If a femtosecond-pulsed laser is focused onto a glass substrate one can change the refractive index and by moving the focus (or the substrate) one can write waveguides (see figure 3.6). The goal is to have a compact waveguiding structure combining four input beams to a single output. It has to provide stability and indistinguishability (of the output pulses). The latter one is important because it must be impossible to determine the input port by measuring the spatial mode of the output. Figure 3.7 shows that the used waveguide fulfils these requirements.
The waveguide has a small stress induced birefringence of $\Delta n = 7 \cdot 10^{-5}$ and a path attenuation $L = 0.5\,dB \cdot cm^{-1}$. One can compensate for the birefringence effects by determining the Mueller matrix of the waveguide and sending rotated states into the waveguide such that the polarisation is rotated such that one gets the desired states (namely H, V, P and M) which was done in [52]. Still, the waveguide makes a phase of $\approx \frac{\pi}{6}$ which can only be compensated with a birefringent material. For

this a phase compensation will be added in the receiver.



(a) Top view of the circuit.

(b) Main view of the circuit.

Figure 3.6: Waveguide design. Taken from [52].

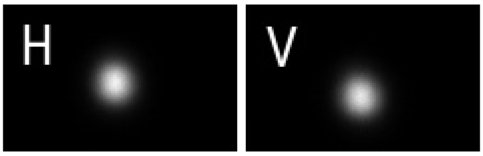


Figure 3.7: Spatial modes of the main output at different polarisations.

3.2.2 Remaining Tasks I

The major remaining tasks for the transmitter module are:

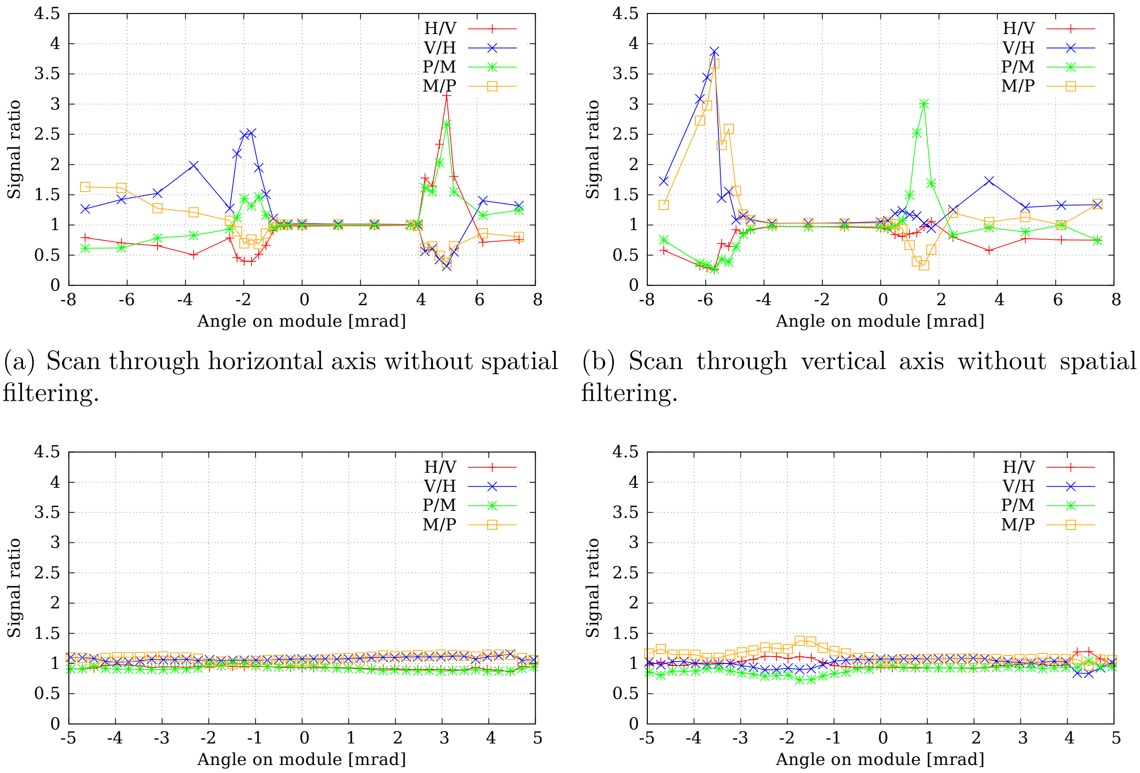
- Measuring temperature behaviour of the driving electronics simulating the situation of a mobile module.
- Fabrication and characterisation of a new polariser array.
- Feasible choice and characterisation of a beacon laser and a dichroic beam splitter.
- Assembly of the complete unit.
- Characterisation of the complete unit.
- Development of software for operating the unit.

Each of these tasks (among others) will be addressed in the next section, after describing the state of the receiver.

3.2.3 State of the Receiver

Spatial Mode Side Channels

As shown in [34] free space implementations can suffer especially of spatial mode side channels meaning that the detection efficiency at the receiver can depend on the spatial mode of the incoming light. In this experiment (and usually in the BB84 protocol) four different detectors are used to analyse the four different states. Due to imperfect spatial mode matching of the detectors the detection efficiency strongly depends on the incoming angle of the light towards the receiver. In the experiment the incident angle of the input beam was varied on the horizontal and vertical axis. As can be seen in figure 3.8 (a) and (b) the detection efficiencies in a range of $\approx 3\,mrad$ are almost equal (the ratios are close to one), while beyond this region, especially directly at the borders of this range, there are large discrepancies in the detection efficiency. Eve can exploit this by routing the light through different angles towards the receiver and thus she can force Bob to measure the same result as she had. Therefore she can predict the measurement outcome with a certain probability and hence she gains information about the key.



(a) Scan through horizontal axis without spatial filtering.

(b) Scan through vertical axis without spatial filtering.

(c) Scan through vertical axis with spatial filtering.

(d) Scan through vertical axis with spatial filtering.

Figure 3.8: Ratio of the detector signals for different angles on both axes with and without spatial filtering. Taken from [33].

As the detection efficiency mismatch is very small in the center region it is a natural counter measure to restrict the incident angles to this region by applying a spatial filter (see figure 3.9). The spatial filter used in this experiment has cut-off angles at $\alpha = \pm 1.36\,mrad$ that means all larger angles are blocked. The experiment has been repeated with the spatial filter in the experimental setup. The results (see figure 3.8 (c) and (d)) show a much better detection efficiency match. However, the signal ratios are also with the spatial filter not unity. In this case (and any other type of detection efficiency mismatch) an additional amount of privacy amplification is required and calculated in [34]. It is expected that the remaining mismatch can be further reduced by better aligning the four fibre-couplers. With the current setup (with fixed couplers) this is not possible.

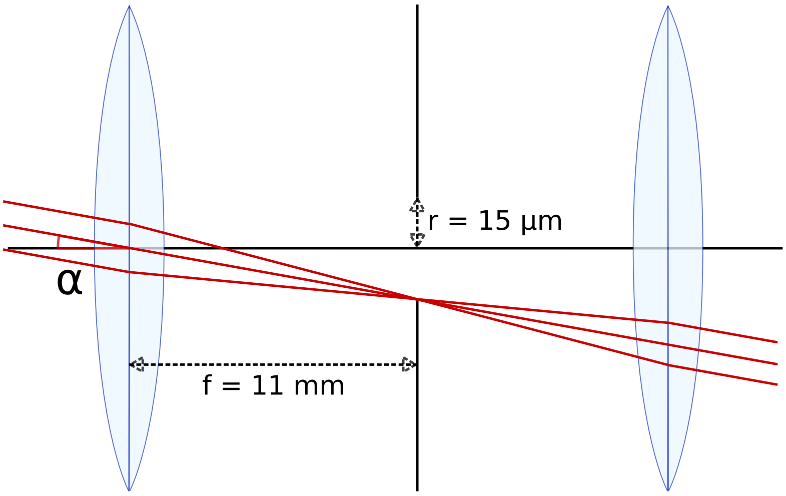


Figure 3.9: Spatial filter: A lens with $f = 11\,mm$ focuses through a narrow pinhole with a diameter of $30\,\mu m$. Afterwards another lens re-collimates the beam.

Beam Tracking and Controlling

Beam tracking and controlling is necessary since the spatial filter restricts the incoming light to angles $|\alpha_{in}| < 1.36\,mrad$ which corresponds at a distance of $1\,m$ to a tiny window with a diameter of $2.72\,mm$ and this is clearly not feasible for any practical scenario, as a study showed in [34]. Therefore a user will not be able to couple much light into the receiver due to shaking. For the beam tracking the beacon laser (which is overlapped with the NIR-VCSELs) is separated from the infra-red light by a dichroic beam splitter: The dichroic mirror transmits NIR-light which is guided to the polarisation analysis unit while reflecting optical light (cut-off-wavelength is at $757\,nm$). The red light is further split by a 50:50 beam splitter and one part is guided to an angle-resolving detector (namely a quadrant diode) which tracks the incident angle and sends an error signal to a voicecoil mirror (an electronically-driven mirror) which in turn compensates for incoming angles

$-52.4\,mrad < \alpha_{in} < 52.4\,mrad$. The average coupling efficiency due to handheld operation defined with the average intensities in the handheld and static case as $g = \frac{I_{handheld}}{I_{static}}$ can be as high as $g = 0.338$ (see figure 3.10). This control only has to be reconfigured to the new wavelengths (as it was operated at $650\,nm$ initially). The details of the mirror control are presented in [51]. Other tests showed that 24.2 % always get lost at the first two pinholes (which limit the incident angle to the range the voicecoil mirror is capable of correcting, see figure 3.4), so that the upper limit for the coupling efficiency due to handheld operation is $g \leq 0.758$.

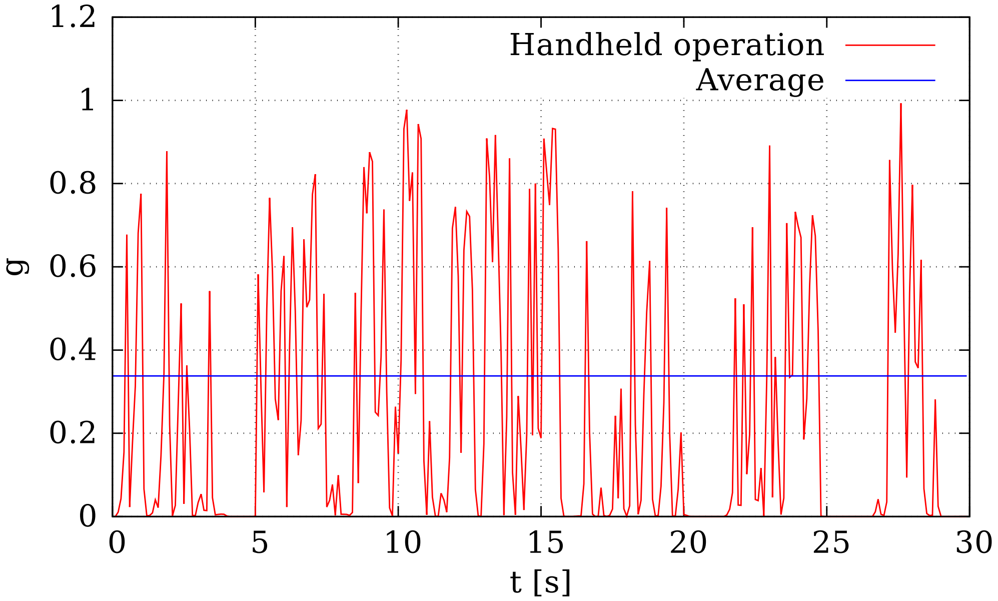


Figure 3.10: Coupling efficiency g to the APDs due to handheld operation over $30\,s$ (red) and average (blue). Other optical losses have not been taken into account.

3.2.4 Remaining Tasks II

The major remaining tasks for the receiver module are:

- Development of a clock recovery and pulse synchronisation.
- Design an active basis alignment.
- Implementation of APDs (and determination of the dark count rate, maybe also under daylight conditions and development of a readout software).

Each of these tasks (among others) will be addressed in the next sections. Finally the complete experiment, that means a key exchange, shall be performed which is described in chapter 4.

3.3 The Transmitter: Alice Module

3.3.1 Development of the driving Electronics

First tests of the driving electronics showed that the main circuit board heats up a lot during operational time. Especially tests in an aluminium box (simulating the situation of the final module) showed that the temperature of the fast delay lines (with which the pulses can be tuned) reach $> 90°C$ after $4 - 6\,min$ and at these temperatures these chips do not work properly anymore as they are only specified up to temperatures of $80°C$. As a result the pulses start to drift which will be a problem when the detection events are gated. Passive cooling elements helped only partially as temperatures $> 90°C$ were reached after $8 - 10\,min$ in that case. To overcome this problem active cooling or better thermal conduction inside the circuit board is thinkable. The second approach is the more desired option as it allows a more compact module without active cooler fans.
To get the heat away from the chips reflow soldering has been used. Advantages of this method are on the one hand fast and clean soldering and on the other hand better heat conduction from the chips to the board. In this case there is also a lot of solder under the chips, so that the heat conducting area is much larger compared to manual soldering, where it is impossible to have solder directly under the chips. To get the heat further out of the board thermal vias have been added. For the reflow method solder paste is attached to the contact pads on the board (using a mask) and then all components (capacitors, resistances and chips) are placed on the appropriate places. Finally the entire assembly must be subjected to a special temperature profile in a reflow oven (any oven where the temperature can be controlled works). This profile includes a ramp-to-soak-phase, a preheat-phase, a ramp-to-peak-phase, a reflow-phase and a final cooling-phase. For the used solder paste (AIM Solder NC254) the temperature profile should have the following reflow profile:

phase	ramp to	preheat	to peak	time above	cool down
temperature	$150°C$	$150 - 175°C$	$245°C$	$217°C$	$20°C$
short profile	$\leq 75\,s$	$30 - 60\,s$	$45 - 75\,s$	$30 - 60\,s$	$45 \pm 15\,s$
long profile	$\leq 90\,s$	$60 - 90\,s$	$45 - 75\,s$	$60 - 90\,s$	$45 \pm 15\,s$

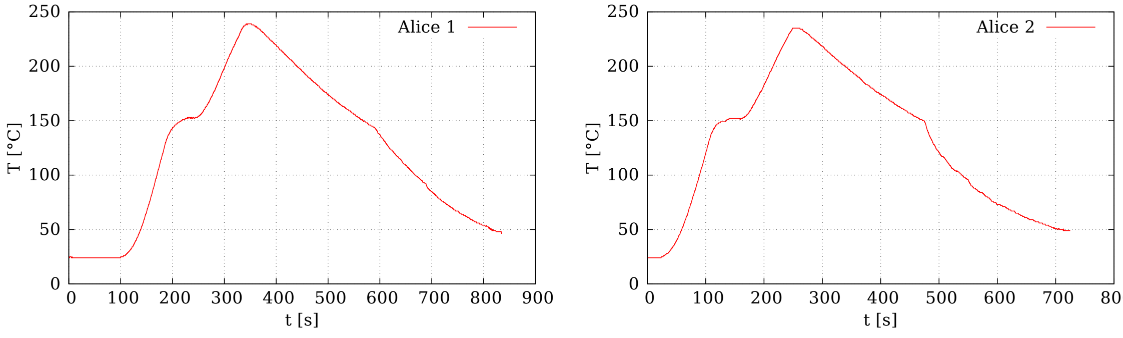
Table 3.1: The recommended reflow profile for NC254. The rate of rise should be maximal $2°C/s$ while the maximal cool down rate should not exceed $-4°C/s$. The short profile is for low density boards and the long profile for high density boards.

In this experiment a standard pizza oven has been used. The following guide will give such a temperature profile (long profile, see also figure 3.11):

- Set oven to $230°C$ upper/lower heat.
- Turn oven off at $T = 125°C$ for $20 - 30\,s$.

- Turn oven on for $3 - 5\,s$, then again off.
- If the temperature starts to fall off (usually after $10 - 30\,s$) heat to peak temperature.
- Turn oven off at $T = 230°C$.
- Open oven at $T = 150°C$.

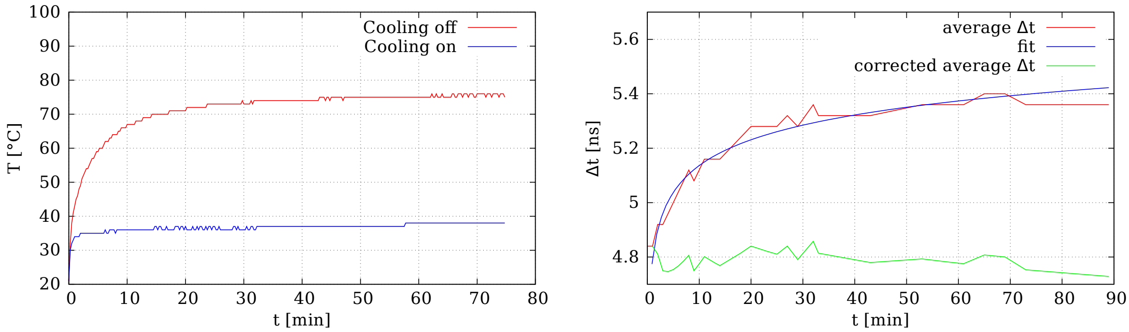
Following this guide the temperature profile should look like in figure 3.11 (two Alice boards have been soldered). Note that with this method only one side of the board can be soldered, all components on the other side must still be soldered manually.



(a) Reflow profile for Alice 1.

(b) Reflow profile for Alice 2.

Figure 3.11: Thermal profiles for both soldered Alice boards. In the final module Alice board 1 is used.



(a) Temperature inside the Alice module on delay line on channel 2 with and without cooling.

(b) Centre peak position of received pulses as a function of time (red), fit (blue) and corrected centre peak position (green). Data taken before active coolers have been installed.

Figure 3.12: Temperature behaviour of the Alice module: Temperature as a function of time with and without cooling (a) and shift of the pulses (b).

The resulting measured temperatures in the final box are also measured (see figure 3.12 (a)). As the temperatures reach $70°C$ after $14\,min$ on chip (thermistor on delay chip 2, inside the chip the temperature is even higher) it is better to stabilise the temperature even more with active cooler fans above and below the PCB. With this improvement the temperature maintained below $40°C$ even after $70\,min$ (see figure 3.12 (a)). Another measurement without cooler fans showed that the centre peak position of the received pulses shift in time (see figure 3.12 (b)) due to the rising temperature. The problem is, that the detections will be gated in a narrow time window to suppress dark count events, hence the pulses will drift out of this detection window. The initial idea was to correct the time window time-dependent with a fit through the data. The corrected peak centre position is given by $fit(t) - fit(1)$ and

$$fit(t) = 7.47 - \frac{2.68}{t^{0.06}} \tag{3.1}$$

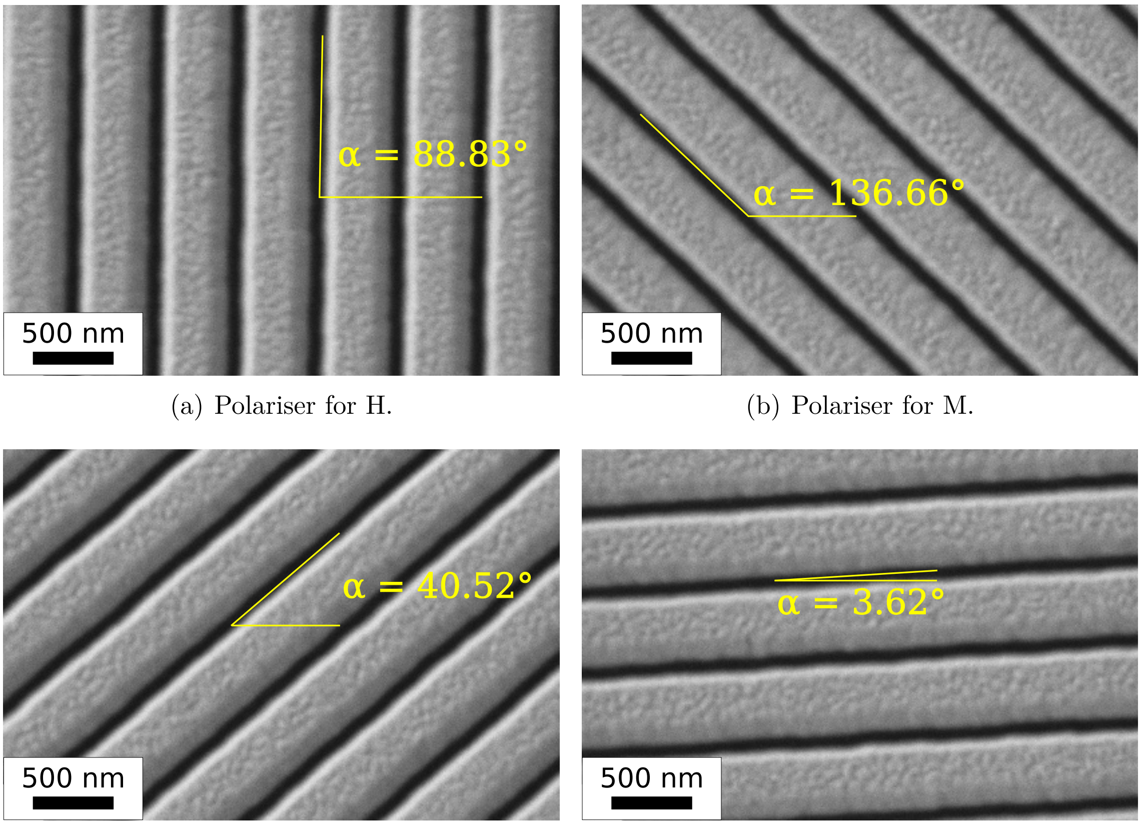
However, the active cooler fans are capable of stabilising the temperature such that after less than $30\,s$ the peak centre position is constant (see also section 4.4.2).

3.3.2 Fabrication of the Polariser Array

In the next step a new polariser array (designed by Gwenaelle Mélen, see also [53]) must be fabricated. For the polarisation state preparation a technique was adopted which was used for long times in microwave engineering: A polariser for microwaves is just a sub-wavelength wire-grid. If this wire-grid is scaled down to optical wavelengths one gets a polariser for optical and infra-red light. Such small slit widths can be achieved using Focused Ion Beam milling (FIB)[55] or etching techniques[56]. For this implementation the first option has been chosen. One general advantage of these techniques is that one can fabricate an array of four polarisers with the required spacing ($250\,\mu m$) which is easier to align than rotating polarised laser diodes or assemble different micro-polarisers.

polariser	channel 0	channel 1	channel 2	channel 3
α	3.62°	40.52°	136.66°	88.83°
β	−86.38°	−49.48°	46.66°	−1.17°
β'	85.21°	48.31°	−47.83°	0.00°
γ'	87.71°	40.89°	−42.91	0.00°
$\gamma' - \beta'$	2.50°	−7.42°	4.92	0.00°

Table 3.2: The angles of reverse (α) and forward ($\beta = \alpha - 90°$) direction of the polarisers as measured in figure 3.13. Note that ±180° will give the same polarisation direction. Additionally shown are the relative angles between the polarisers and the polariser for H for the fabricated polariser (β') and theoretically calculated optimal polarisers (γ') in [52]. The beam propagation direction has been equalised.



(a) Polariser for H.

(b) Polariser for M.

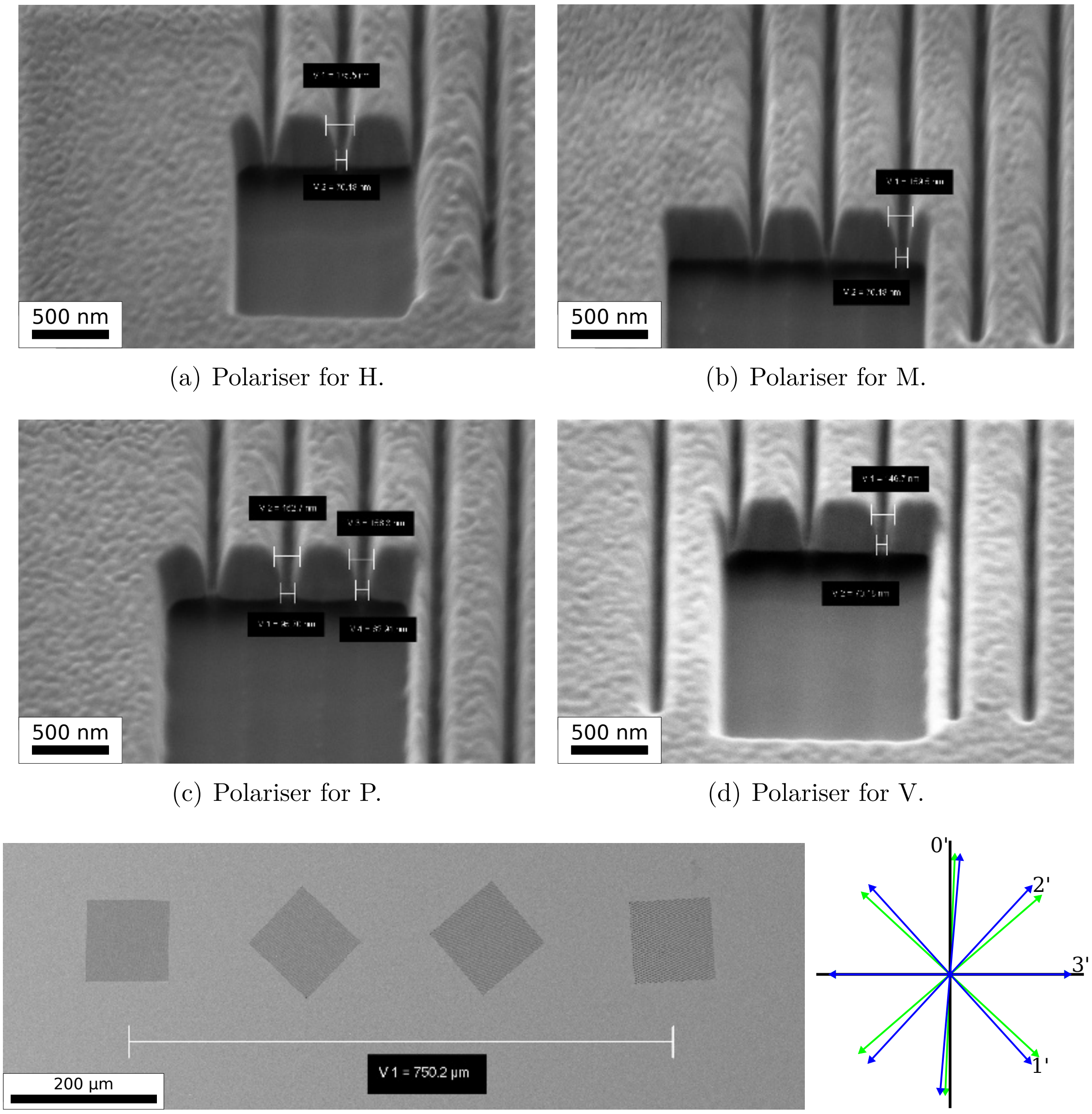
(c) Polariser for P.

(d) Polariser for V.

Figure 3.13: The four different polarisers with angles α. Note that the polarisation forward direction is $\beta = \alpha - 90°$ and the beam propagation direction is out of the paper plane.

The basis for the polarisers is a 265 nm thick gold foil vacuum-deposited onto a glass substrate. Each polariser has a total area of $120 \times 120\,\mu m^2$ which is about three times the beam diameter, which is chosen to prevent diffraction effects. The slit width is 150 nm while the slits have a spatial period of 500 nm. The polarisers feature a transmission of 9 %.

The measured angles (see figure 3.13) of the polarisers are shown in table 3.2. These angles can be compared to the theoretically calculated optimal input angles for the waveguide[52]. The waveguide rotates the polarisation and consequently these optimal input angles have been calculated such that the polarisation is rotated that the output states are precisely the desired states. As the horizontal axis in figure 3.13 has been chosen arbitrarily one has to take only relative angles into account. For this comparison both polarisers, the fabricated and the theoretical for H are aligned parallel. As can be seen in table 3.2 and figure 3.14 (f) the difference between the theoretical and fabricated angles of the polarisers is large for channel 1 and channel 2. It is noteworthy that the relative angle between channel 1 and channel 2 is wrong by 12.34° which is close to 10° which is one of the rough rotation steps of the gold foil in the FIB (also finer steps are possible and have been made). One possible explanation is that here was simply one step missed. How this results in an error in the final polarisation is calculated in section 3.3.6. A close-up image of the polarisers is shown in figure 3.14 together with an overview of the complete array. The measured average slit width is $\approx 150\,nm$.



(a) Polariser for H.

(b) Polariser for M.

(c) Polariser for P.

(d) Polariser for V.

(e) Complete array.

(f) Angles of the four polariser forward directions, theoretical (green) and as fabricated (blue).

Figure 3.14: (a)-(d): The different polarisers (close-up images). (e) Overview of the complete array. (f) Alignment of the polariser forward direction.

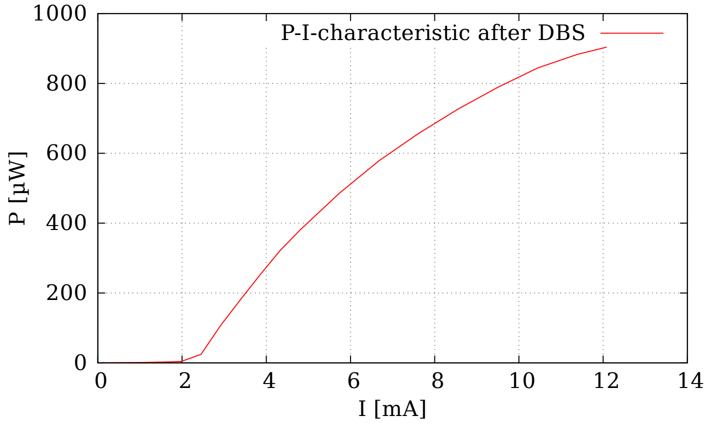
The polarisers show an extremely good performance, the high extinction ratios (see table 3.13) result in an average QBER of $E = 0.07\,\%$ originating from the polarisers (but not including the wrong relative angles).

polariser	channel 0	channel 1	channel 2	channel 3
extinction ratio	1:1150	1:1200	1:1620	1:1800
E [%]	0.09	0.08	0.06	0.05

Table 3.3: Extinction ratios of the four polarisers and the resulting QBERs E.

3.3.3 Beacon Laser

In the next step the beacon laser must be characterised. As already mentioned the infra-red signal photons must be overlapped with a bright visible beacon laser. As beacon laser a red multi-mode VCSEL from Vixar Inc. emitting at $680\,nm$ (Model 680M-0000-X002) is used and then overlapped with the infra-red beam using a dichroid beam splitter. Together with the outcoupling lens after the dichroic beam splitter the beacon laser is collimated. The advantage of this VCSEL is its availability as bare die which allows to bond the VCSEL in a feasible chip carrier ready for the assembly on the micro-optical bench. A measurement of the output power is shown in figure 3.15.



(a) Plot of the P-I-characteristic of the beacon laser as it is emitted by the module.

I [mA]	P [µW]	I [mA]	P [µW]
0	0.001	4.80	735
0.57	0.998	5.74	940
1.04	2.335	6.68	1120
1.51	4.33	7.62	1271
1.98	7.68	8.56	1406
2.45	47.2	9.50	1526
2.92	208.3	10.44	1632
3.39	351.1	11.83	1708
3.86	489	12.09	1749
4.33	623		

(b) Table of the P-I-characteristic after the beam splitter.

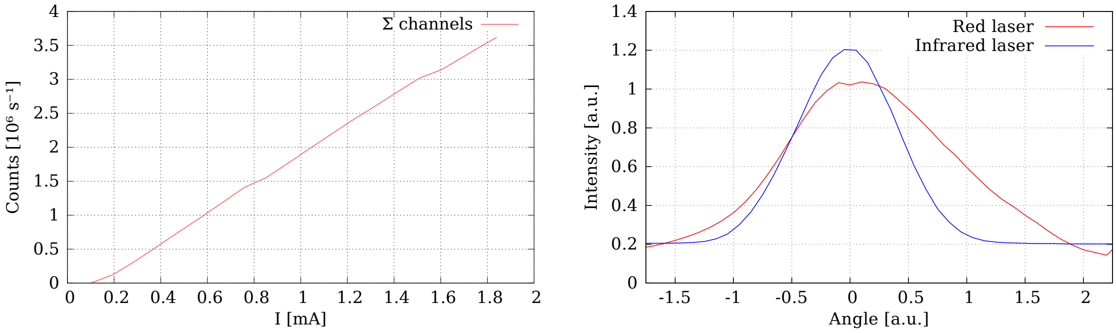
Figure 3.15: P-I-characteristic of the beacon laser.

The beacon laser can not only be used for beam tracking. The clocks at Alice's and Bob's side will drift making it impossible to assign the sent to the received pulses. To get to synchronously running clocks at both sides the beacon laser has to be modulated with a rectangularly shaped signal with a frequency of $100\,MHz$. As the beacon is modulated with the same clock as the signal VCSELs the modulation of the beacon also transmits the modulation of the signal VCSELs which can then be recovered by a fast photodiode in the receiver. For the details of the complete clock recovery and pulse synchronisation see section 3.4.1.

As it turned out during the first key exchange experiments there was a lot of background if only the beacon laser was running. Already at moderate beacon output powers ($P_{out} < 7\,\mu W$, below lasing threshold) the total background count rate (sum over all four channels) exceeded $4 \cdot 10^6\, s^{-1}$ which is the maximal count rate of the APDs (see figure 3.16 (a)). Additional narrow interference filters could not suppress this noise which means the background is really at $850\,nm$. Blocking the path to the infra-red VCSELs did not change anything either indicating that the additional noise can in principle only originate from two different sources:

1. It could be that the beacon pumps fluorescence in the UV glue used to mount the outcoupling lens to the dichroic beam splitter, in one of the dichroic beam splitters or at an interference filter.

2. It could be that the beacon emits around $850\,nm$.



(a) Background count rate at different beacon currents detected by the APDs of the receiver.

(b) Intensity of the noise after the spatial filter with varying angle of incidence (red) and for a comparison perfectly collimated light (blue). The FWHM is a measure for the degree of collimation.

Figure 3.16: Background count rates and collimation measurement.

A measurement (see figure 3.16 (b)) showed that this background is collimated, indicating that this is probably no fluorescence effect in the components which is in general isotropic and thus not much light should pass through the spatial filter. Also a shortpass filter (SP) placed directly after the module did not help, that means the background light must originate from the module itself. Still it could have the first reason mentioned above, but after the collimation measurement this is very unlikely. Anyway, fluorescence effects inside the module could not be overcome. The spectrum of the background is shown in figure 3.17 recorded with a single photon spectrometer

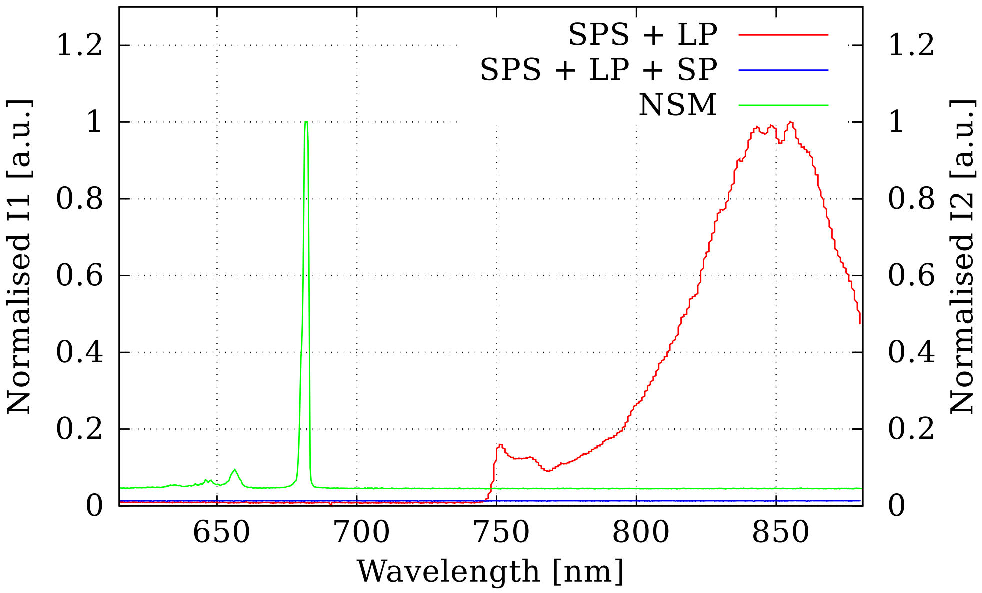


Figure 3.17: SPS + LP: Spectrum with single photon spectrometer and longpass filter (red). SPS + LP + SP: Spectrum with single photon spectrometer and longpass filter and shortpass filter in the module (blue). NSM: Normal spectrum with much higher intensity $I2 \gg I1$ (green).

and an ultrasteep longpass filter (LP) with the edge at $750\,nm$ in the beam (Semrock 750US). To suppress this background a shortpass filter ($3 \times 3 \times 0.1\,mm^3$, two-sided coating KP700-S customised by bk Interferenzoptik) has been added in the beacon beam before the dichroic beam splitter (directly glued to the beam splitter). The shortpass filter has a cut-off wavelength at $701\,nm$ and transmittances $T_{680} = 0.83$ and $T_{850} < 10^{-4}$. As the spectrum with the filter in the module shows, there is no background left in the near infra-red. Thus, as expected, the background is emitted by the beacon laser itself. Probable explanations could be recombination of electron-hole-pairs in the semiconductor material as typically used semiconductor materials have energy band gaps around $1.49\,eV$ (for GaAs) at room temperature ($850\,nm$ corresponds to $1.46\,eV$). This suspicion is substantiated as the background is already present below the laser threshold, which indicates spontaneous emission. Additionally shown in figure 3.17 is a spectrum without any filters measured with a normal fibre-coupled spectrometer. Note that the intensity $I2$ of the line at $680\,nm$ is much higher than the intensity $I1$ of the background. Both intensities have been normalised individually to unity.

3.3.4 Dichroic Beam Splitter

After the waveguide the infra-red beam has to be spatially overlapped with the red beacon laser. For this a micro-beam splitter is required. In the ideal case this is a dichroic beam splitter, because then one does not loose any infra-red photons for the key exchange at the beam combination. In principle of course a standard-sized beam splitter would work as well, but then the total size of the module increases making the unit harder to integrate into other scenarios. Non-polarising cube beam splitters are available with edge lengths $\geq 5\,mm$. The desired edge length for this experiment is $3\,mm$ which is the diameter of the collimating lens. Non-polarising dichroic cube beam splitters at these dimensions can be specially designed and produced, but at very low quantities those are very expensive. As it turned out optical pick-up systems in DVD drives use dichroic beam splitters to combine laser light at $790\,nm$ (wavelength for CD) with laser light at $650\,nm$ (wavelength for DVD). The cut-off-wavelength is usually between $710\,nm$ and $740\,nm$ which makes it perfectly suited also for combining $680\,nm$ and $850\,nm$, the design-wavelengths in this experiment. The only constraint is that the DBS must not be polarising, but a unitary rotation does not matter, as it can always be corrected by the inverse transformation in the receiver. From the available DVD drives five different beam splitters have been dismounted and characterised with the following setup in figure 3.18:

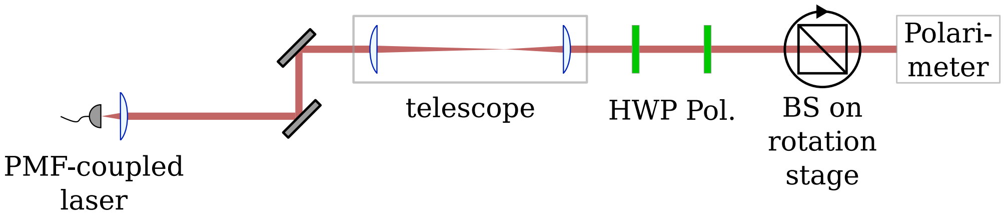
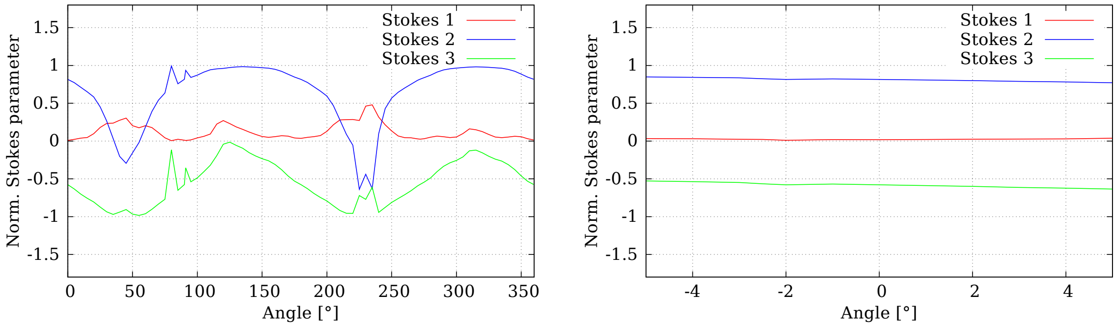


Figure 3.18: Setup for the characterisation of the beam splitters. PMF: polarisation-maintaining fibre. HWP: half wave plate. Pol: polariser. BS: beam splitter.

A polarisation-maintaining-fibre-coupled laser at $850\,nm$ is used as light source. The diameter of the beam is narrowed with a telescope that it is smaller than the edge length of the smallest beam splitter. With two lenses ($f_1 = 75\,mm$ and $f_2 = 35\,mm$ at a distance of $110\,mm$) the beam diameter is reduced according to

$$d' = d\frac{f_2}{f_1} \tag{3.2}$$

where d' and d are the beam diameters after and before the telescope respectively. With the used telescope the diameter of the beam is reduced by a factor of $\frac{7}{15}$ to a diameter of $\approx 2\,mm$. After the telescope a polariser followed by a half wave plate allows to set the input polarisation to any arbitrary linear polarisation without loss of intensity. Thus the polarisation-maintaining fibre proved to be helpful to reduce intensity fluctuations after the polariser. The beam passes then the beam splitter to be characterised which is mounted on a 360°-rotation stage. Finally the polarisation of the beam is analysed in a free space polarimeter (Thorlabs PAX5710IR1-T). As only one of the beam splitters fulfils all requirements only the results for this beam



(a) Complete scan from 0° to 360° in rough steps (5°).

(b) Scan from −5° to 5° in fine steps (1°).

Figure 3.19: Measured Stokes parameters after the passing through the beam splitter. The input was P-polarised.

splitter are presented in the following.
The beam splitter has dimensions of $3.5 \times 3.5 \times 3\,mm^3$. For the measurement P-polarised light is used as input. The measured Stokes vector of the input light is $\vec{S}_{in} = (1, 0.00, 1.00, 0.00)^T$ (rounded on three digits). Then the beam splitter is placed in the beam and rotated around 360° (see figure 3.19 (a)). Of course, at angles of 45°, 135°, 225° and 315° the beam hits an edge of the beam splitter and thus it is not surprising that the beam splitter rotates the polarisation peculiarly. As can be seen in figure 3.19 (b) in a region ±5° from a surface of the beam splitter cube the polarisation change is nearly constant and the beam splitter only adds a phase of $\approx -\frac{\pi}{5}$.
To confirm that this is not just a polarising effect also H-, M- and V-polarised light as input has been used (under 0°):

$$\vec{S}_{in}^{H} = (1, 1.00, 0.00, -0.01)^T \Rightarrow \vec{S}_{out}^{H} = (1.00, -0.00, 0.00)^T \tag{3.3}$$
$$\vec{S}_{in}^{P} = (-0.00, 1.00, -0.00)^T \Rightarrow \vec{S}_{out}^{P} = (0.01, 0.81, -0.59)^T \tag{3.4}$$
$$\vec{S}_{in}^{V} = (-1.00, 0.00, -0.00)^T \Rightarrow \vec{S}_{out}^{V} = (-1.00, 0.00, -0.02)^T \tag{3.5}$$
$$\vec{S}_{in}^{M} = (-0.00, -1.00, 0.00)^T \Rightarrow \vec{S}_{out}^{M} = (-0.01, -0.82, 0.58)^T \tag{3.6}$$

And thus the relative phases agree very well with $\approx -\frac{\pi}{5}$. Together with the phase shift of the waveguide (see section 3.2.1) the remaining phase to be compensated is

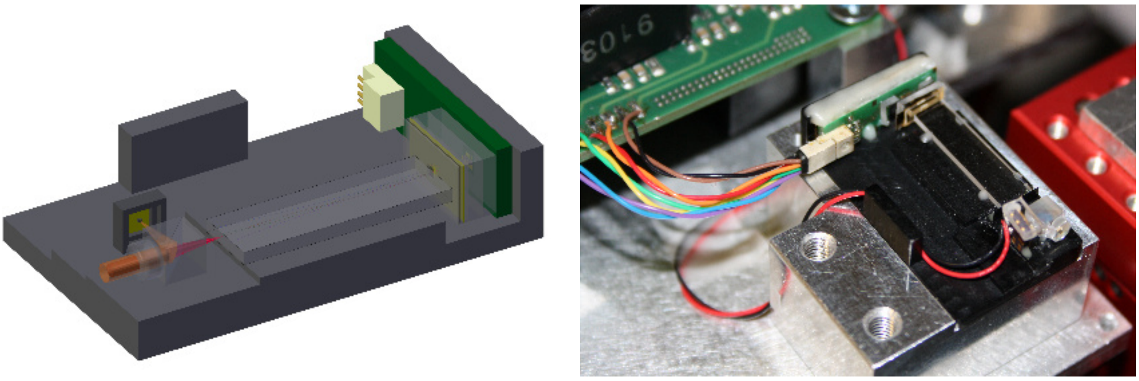
wavelength	$680\,nm$	$850\,nm$
R	$48.3\,\%$	$< 0.13\,\%$
T	$51.7\,\%$	$> 99.87\,\%$

Table 3.4: Splitting ratios of the DBS at the relevant wavelengths at +45°-polarised input light.

$\approx -\frac{\pi}{30}$.
Finally the splitting ratios for both wavelengths have been measured (see table 3.4). All in all this beam splitter is well-suited for this experiment.

3.3.5 Assembly of the Micro-optics

With all the single components characterised the complete module has to be assembled. The components shall be arranged on a micro-optical bench with several steps of different heights on which the components can be glued to (see figure 3.20). A CAD sketch of the micro-optical bench can be found in the appendix 8.1.



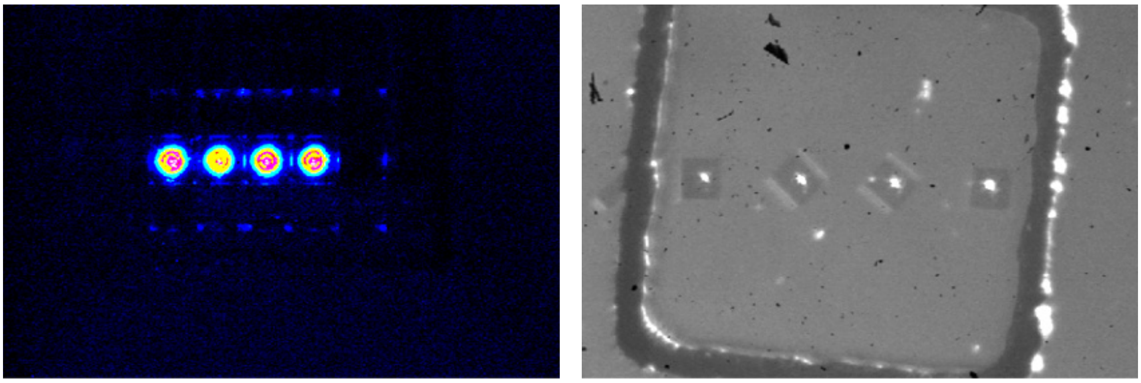
(a) Sketch of the assembled Alice unit (optics). (b) Image of the assembled Alice unit (optics).

Figure 3.20: Assembled Alice unit, sketch and photograph.

The assembly takes place in three major steps: First, the optics before the waveguide are glued together on the board with the VCSELs. Second, the most crucial step, these optics and the waveguide have to be glued to the micro-optical bench. And finally the beacon and the dichroic beam splitter together with the outcoupling lens must be placed on the micro-optical bench. As glue DYMAX OP-67-LS is used, a UV-curing adhesive. The advantage is that the curing time is less than $3\,s$ and that the glue is stable for at least eight months, so fast and stable alignment is possible. For curing a bright UV lamp is used (Model DYMAX BlueWave 75, $1.39\,W$ at $365\,nm$). The distance between all components have been determined using Zemax simulations (for the details of the simulations see [53]). All components have been aligned with vacuum tweezers and a 6-axis rotation stage (Model Luminos i6005).

First Step

For the first step the board of the VCSELs was lying on its back with a CCD camera looking from above and one looking from aside. The first component is a neutral density filter which is made out of a filter foil (Kodak Filter ND WRATTEN 2.0 OD) where the measured transmittance is 8.20 % (ND = 1.09) for infra-red light



(a) The four VCSELs after the microlens array.

(b) The four VCSELs after the polariser array.

Figure 3.21: The VCSELs after various steps during the first part of the assembly (high resolution images are in the electronic version of this thesis).

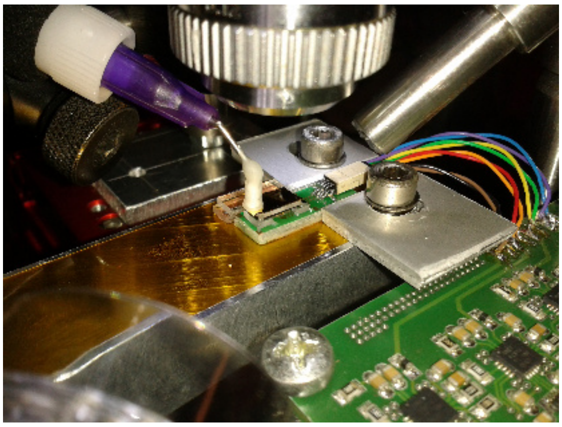
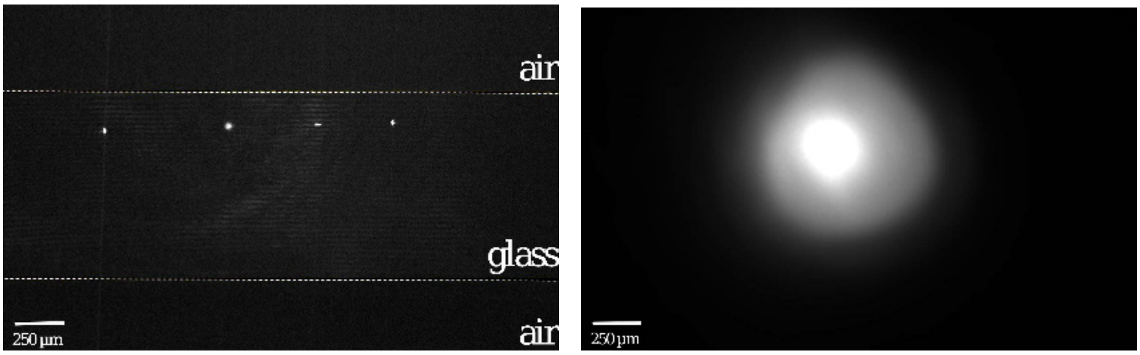


Figure 3.22: Photograph of the complete block with the VCSELs, ND-filter, MLA and polariser array.

at $850\,nm$. The filter is glued on two sides to spacer components (standard spacer, $1.14\,mm$ thickness) to ensure a minimal distance to the VCSELs, such that the bonding wires of the VCSELs are protected. In the next step the microlens array (MLA) is glued into the hole of one spacer component and then the complete block is glued onto the block with the ND-filter. The spacer component ensures the correct distance to the following polariser. Figure 3.21 (a) shows the picture of the upper CCD camera after this step with all four VCSELs turned on. Finally the polarisers are glued onto the MLA. It is important that the glass substrate must be on the side of the MLA, otherwise the glass will probably change the polarisation due to its birefringence. Figure 3.21 (b) shows the picture of the upper CCD camera after this final step with all four VCSELs turned on. The measured angle between the axis of the VCSELs and the axis of the polarisers is 0.67°. Finally the complete block (see figure 3.22) is glued to the micro-optical bench. The backside of the board of the VCSELs has been isolated with Kapton Polyimide.

Second Step

In the second step, the waveguide must be glued to the micro-optical bench, which is the most crucial step, because to get a high coupling into the waveguide all three angular and all three spatial degrees of freedom must overlap very well. The setup is rearranged: A $5\,mm$ lens maps the end of the waveguide onto a CCD camera. For roughly arranging the waveguide it is helpful to use the straight waveguides on both sides of the Alice circuit as these have a four times higher coupling to the output (of this straight waveguide). Once the waveguide is aligned roughly empirical fine tuning can lead to coupling efficiencies of $> 20\,\%$. Zemax simulations predict a maximal coupling efficiency of $60\,\%$. If VCSELs 0 and 3 are turned on one should see light from all four output ports as in figure 3.23 (a). In that case also VCSEL 1 and 2 should be coupled equally well. Finally three of the output ports (except for the main output) must be blocked. Another Kodak filter foil has been blackened from both sides with a felt-tipped pen (Edding 33) such that the transmittance is $3.1 \cdot 10^{-4}$ (ND = 3.51). Thus the other outputs are suppressed by at least four orders of magnitude (the suppression is even higher as the outcoupling angles differ for the four outputs, see figure 3.6 (b)). With a diamond saw a $100\,\mu m$ thick slit has been sawn into this blackened filter foil kept between two thin silicon wafer. With the 6-axis rotation stage the blackened foil has been arranged until only the main output couples through this slit.



(a) The four output ports of the waveguide.

(b) Red beacon VCSEL (outer circular area) and NIR signal VCSELs (inner circular area) overlapped on a CCD camera at a distance of $60\,cm$.

Figure 3.23: Pictures of the CCD camera after various steps during the second and third part of the assembly (high resolution images are in the electronic version of this thesis).

Third Step

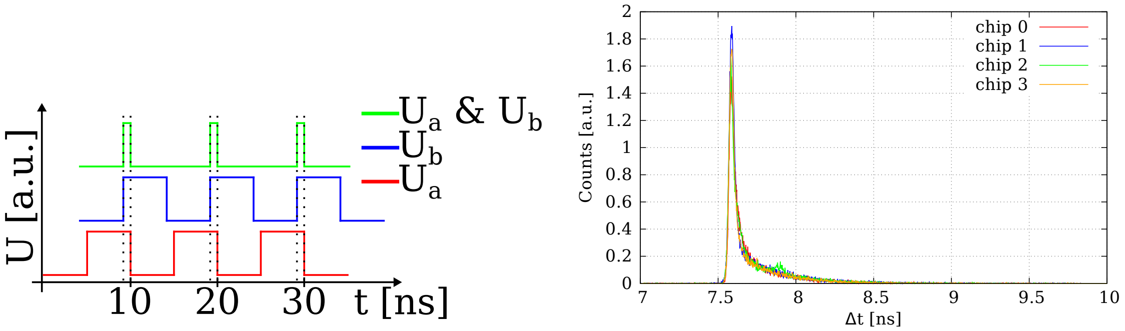
For the last step the outcoupling lens (Model LightPath 354130 with a focal length $f = 4.9\,mm$) is directly glued onto the dichroic beam splitter separately. It is important that no glue flows beneath the lens. If this happens it turned out that the glue can be removed with Acetone (but this should not be done too often as Acetone affects the anti-reflection coating on the outcoupling lens). In this step one should also glue the shortpass filter to the beam splitter (see section 3.3.3), as it is much easier to add the filter here than later in the complete module. During this assembly this was not done as the need for such a shortpass filter was yet unknown. Then the beam splitter with the lens is aligned in front of the waveguide such that the infra-red light beam is collimated. For this the CCD camera is placed in a distance of $\approx 60\,cm$. The VCSELs must be turned on very brightly and the exposure time of the CCD must be long. Finally a 50:50 beam splitter is added in the path and a second CCD camera is placed in the second arm of the BS (distance $\approx 13\,cm$ between outcoupling lens and the CCD camera). Then the beacon is aligned such that the red and infra-red light overlaps on both CCD cameras (see figure 3.23 (b)). If the light overlaps at two positions, it also overlaps at all other positions. The micro-optical bench is then placed in a protective casing with dimensions $154 \times 88 \times 47\,mm^3$ together with the driving electronics and the cooler fans (for a CAD sketch and photograph see appendix 8.1 and 8.2). Of course these dimensions are now larger than the dimensions of a smart phone, but in principle the driving electronics could be made completely out of integrated circuits and thus fit also directly onto the micro-optical bench.

3.3.6 Characterisation of the Transmitter

After the assembly the complete unit must be characterised in terms of pulse characteristics and quantum tomography of each polarisation state.

Pulse characteristics

The parameters for the driving electronics have to be adjusted such that the temporal shape of the pulses in all channels is indistinguishable. For the temporal tuning



(a) Generation of short electrical pulses using two delayed clocks and an AND-gate.

(b) Temporal shape of the final optical pulses.

Figure 3.24: Generation of the electrical pulses and temporal shape of the final optical pulses.

the 100 MHz clock is split into two clock signals a and b. With these two clocks one can generate electrical pulses of 5 ns length. These electrical pulses are added with an AND-gate so the maximal electrical pulse length is 5 ns. When these two clocks are individually delayed with 5 ps resolution by delays d_A and d_B one can set the start and end point of the electrical pulse (see figure 3.24 (a), more details in [53]). Next one has to measure the shape of the optical pulse (see figure 3.24 (b)).

Finally the intensities of the pulses must be matched. A constant current I_b drives the VCSELs slightly below the lasing threshold ($I_{th} = 0.40 - 0.71\,mA$). Then for a short time (if a & b is true) a strong modulation current $I_m \gg I_b, I_{th}$ is added which results in a coherent optical pulse. I_b and I_m must be chosen such that all channels have the same intensity. Table 3.5 summarises the set of final parameters which give identical optical pulses. Additional to the parameters in SI-units are the values shown which can be committed to the software ($alice - control$). The units can be converted according to

$$I_{b,m} = 0.1 + b, m \cdot 0.047\ [mA] \tag{3.7}$$

$$d_{A,B} = d_{a,b} \cdot 5\ [ps] \tag{3.8}$$

channel	0	1	2	3
I_b $[mA]$ / value b	0.194 / 2	0.194 / 2	0.194 / 2	0.147 / 1
I_b $[mA]$ / value m	11.05 / 233	11.66 / 246	12.09 / 255	12.09 / 255
d_A $[ps]$ / value d_a	50 / 250	59 / 295	80 / 400	26 / 130
d_B $[ps]$ / value d_b	82 / 410	132 / 660	108 / 540	55 / 275

Table 3.5: Final parameters for identical optical pulses in SI-units / values committed to the software.

Quantum state tomography

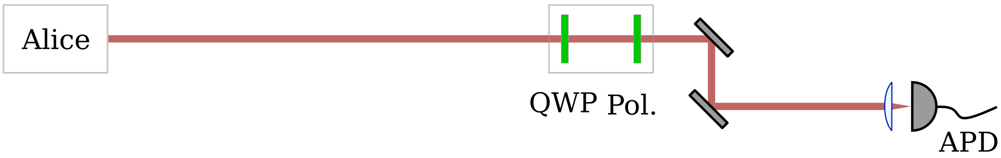


Figure 3.25: Experimental setup for the quantum state tomography. QWP: quarter wave plate. Pol: polariser. The quarter wave plate and the polariser are motorised.

To determine the source-intrinsic QBER E a complete quantum state tomography for each of the states is required. The experimental setup is shown in figure 3.25. The light from the Alice module passes the measurement apparatus and is then

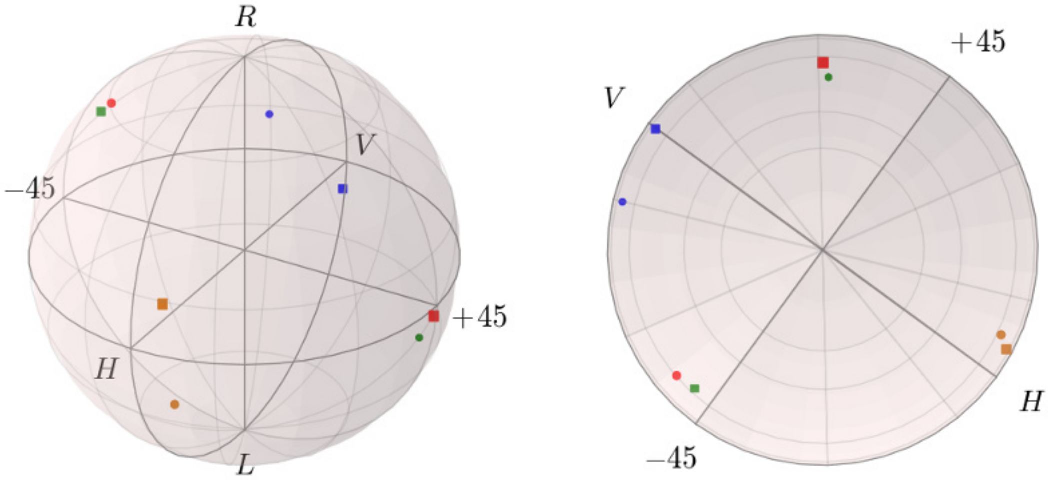
projection on	H	V	P	M	R	L
orientation QWP	0°	0°	45°	45°	0°	0°
orientation Pol	0°	90°	45°	135°	45°	135°

Table 3.6: Orientation for the QWP and the polariser. The horizontal axis is defined as 0°.

	V (channel 0)	M (channel 1)	P (channel 2)	H (channel 3)
S_1	-0.869(1)	-0.198(1)	-0.468(3)	0.920(1)
S_2	-0.362(4)	-0.841(3)	0.688(2)	0.174(2)
S_3	0.226(1)	0.462(3)	-0.516(6)	-0.281(3)
Π	96.8(4) %	98.0(4) %	97.9(7) %	97.8(3) %
E	6.55(5) %	7.95(15) %	15.60(10) %	4.00(5) %

Table 3.7: Measured (intensity) normalised Stokes vectors for all four channels (average value and standard deviation). Additional shown is the DOP and resulting QBER E.

coupled to an APD. The measurement apparatus consists of a motorised quarter wave plate followed by a motorised polariser. With this sequence one can project on



(a) Visualisation on the Poincaré sphere of the measured Stokes parameters (circles) and calculated corrected Stokes parameters after phase compensation (boxes).

(b) Projection on the linear polarisation plane of the Poincaré sphere of the measured Stokes parameters (circles) and calculated corrected Stokes parameters after phase compensation (boxes).

Figure 3.26: Visualisation on the Poincaré sphere of the measured and calculated corrected Stokes parameters for the BB84 protocol.

the six polarisation states of light. The orientation of the QWP and the polariser for the six projections can be found in table 3.6. Note that the horizontal axis is always defined as 0° in this work. As the gearing of the step motors suffers a little bit from hysteresis the best order of measuring is H $\rightarrow$ V $\rightarrow$ R $\rightarrow$ L $\rightarrow$ M $\rightarrow$ P, because the overall way the step motors have to drive is minimal in this case. Note that there are also other counter measures to prevent hysteresis. It must be taken care that the light beam is perpendicular to the measurement apparatus and that the quarter wave plate and the polariser are plane parallel, which can be achieved with high precision if one ensures that the back-reflections unite in the origin of the source. The measured Stokes vectors are given in table 3.7 (see also figure 3.26) with the QBERs calculated using equations 2.62 - 2.65.

The average QBER $E_{av} = 8.53\,\%$ is in strong contrast with the predictions made in [52] ($E_{av} < 0.11\,\%$), even if the final phase shift of $-\frac{\pi}{30}$ is taken into account. It is unclear, where this large discrepancy comes from, in principle this deviation could originate from

- the wrong angles of the polarisers or
- the complete polariser array could be rotated or
- a false reconstruction of the Mueller matrix of the waveguide.

In the latter case the calculated "optimal" input states are wrong. The main mistake was that the input states only have been calculated and never been confirmed by measurements. To ascertain what might have happened one can use the data for the retrieval of the Mueller matrix and try to calculate the output states with the rotated polariser array and the wrongly fabricated polariser angles, taking also into account the phase shift of the dichroic beam splitter. The calculation software was particularly developed in Java (see section 3.3.7). It shall be mentioned that the following calculations have been performed in [53] as well with MATLAB independently from the calculations here with Java. Both calculations yield the same results.

First, the Mueller matrix is calculated again from the available data. For the previous reconstruction a simple least-mean-square-fit was used without any restrictions. As the fitted matrix is then in general not unitary one gets in this case Stokes vectors with norm larger than 1 which does not represent any physical state. As in this case the QBER calculated with equations 2.62 to 2.65 becomes negative the whole optimisation algorithm cannot work meaningful. Similar problems can arise if the QBERs are computed via projections as it was done when the initial optimal input Stokes vectors have been computed. It shall be mentioned, that the Mueller matrix in general needs not to be unitary (as it can also describe polarising effects), but this is not the case for this waveguide array as the degree of polarisation before and after the waveguide is equal within the measurement accuracy. As any arbitrary unitary polarisation rotation can be described by the three Euler rotation angles it is reasonable to fit such a matrix with a least-mean-square-fit to the available data:

For each of the four waveguides the projections on all six polarisation basis states after the waveguide for all six polarisation input states have been measured (for each input port):

$$\sum_{j=0}^{5} \vec{S}_j^{out} = \sum_{j=0}^{5} M\left(\alpha,\beta,\gamma\right) \vec{S}_j^{in} \tag{3.9}$$

As there is only one measurement for each output state available the error can be approximated by the standard deviation of the total power in each basis for a single input state to upper-bound $\Delta I \geq \max\{\Delta I_H, \Delta I_V\}$. It shall be mentioned that assuming a Possion-distributed error this one measurement would be sufficient to estimate the error on the data. It shall be further noted that one can find better approximations for some of the approximations used below, which was only recognised at the very end of this work and thus these better estimates are not included in this work.

By use of propagation of error laws the error in the Stokes parameters can be estimated to be

$$\begin{aligned}
\Delta S_1 &= \left|\frac{\partial S_1}{\partial I_H}\Delta I_H\right| + \left|\frac{\partial S_1}{\partial I_V}\Delta I_V\right| \leq && (3.10)\\
&\leq \left|\frac{1}{I_H+I_V} - \frac{I_H-I_V}{\left(I_H+I_V\right)^2}\right|\Delta I + \left|\frac{-1}{I_H+I_V} - \frac{I_H-I_V}{\left(I_H+I_V\right)^2}\right|\Delta I = && (3.11)\\
&\overset{I_i\,\geq\,0}{=} \frac{\Delta I}{I_H+I_V}\left(\left|1-\frac{I_H-I_V}{I_H+I_V}\right| + \left|1+\frac{I_H-I_V}{I_H+I_V}\right|\right) = && (3.12)\\
&= \frac{\Delta I}{I_H+I_V}\left(\left|1-S_1\right| + \left|1+S_1\right|\right) = && (3.13)\\
&\overset{|S_1|\,\leq\,1}{=} \frac{2\Delta I}{I_H+I_V} && (3.14)
\end{aligned}$$

with S_1 defined as in equation 2.43. Analogous relations follow for ΔS_2 and ΔS_3. Note that the input and output Stokes vectors are error-prone. The error found with this method is between 0.4 % and 1.3 %. The least-mean-square-fit minimises the weighted sum of squared errors χ^2 (chi-squared statistic):

$$\chi^2 = \min_{\alpha,\beta,\gamma} \sum_{j=0}^{5} \frac{|\vec{S}_j^{out} - M\left(\alpha,\beta,\gamma\right)\vec{S}_j^{in}|^2}{\sigma_j^2} \tag{3.15}$$

where σ is the variance of the observed data which can be estimated with

$$\sigma_j^2 \approx \sum_{k=1}^{3} \left(\Delta S_k^j\right)^2 \approx 3\left(\Delta S^j\right)^2 \tag{3.16}$$

where $\Delta I \approx$ const. for a single input has been used. To quantify the quality of the fit one can evaluate the reduced chi-squared statistic:

$$\chi^2_{red} = \frac{1}{\nu}\chi^2 \tag{3.17}$$

where $\nu = N - n - 1$ is the number of degrees of freedom with N the number of measurements and n the number of fitted parameters. In the analysed data $\nu = 36 - 3 - 1 = 32$. With this method the minimum error was found for the set of Euler angles as presented in table 3.8:

	waveguide 0	waveguide 1	waveguide 2	waveguide 3
α [°]	-0.057	15.41	327.2	161.6
β [°]	208.1	212.3	212.6	149.0
γ [°]	2.807	13.29	332.4	166.6
χ^2_{red}	0.567	15.51	0.579	7.995

Table 3.8: Calculated Euler angles for a least-mean-square-fit together with the reduced chi-squared statistic.

For the reduced chi-squared statistic one can distinguish between the following four cases[57]:

1. $\chi^2_{red} \gg 1$ indicates a poor model fit.

2. $\chi^2_{red} > 1$ indicates that the fit was not able to capture all data.

3. $\chi^2_{red} = 1$ indicates a good match between model and observed data up to the error variance.

4. $\chi^2_{red} < 1$ indicates "over-fitting": the model fits improperly noise.

Comparing χ^2_{red} obtained from the fits in table 3.8 with these four cases one sees that the unitary matrix obviously is not describing the polarisation change in the waveguide. This can have now two different reasons:

1. There is strong polarisation-dependent loss (and thus the unitary model is wrong).

2. The measured data is inconsistent.

As the first case is non-physical (or at least other than characterised) the latter case is the most probable explanation. However, one can try to calculate the output states with this model. For the calculation of the complete module the actual input Stokes vectors have to be calculated. Assuming fully linearly polarised light (which is at extinction ratios $\geq 1:1150$ (see table 3.3) a reasonable assumption) the input

	V (channel 0)	M (channel 1)	P (channel 2)	H (channel 3)
S_1^{in}	-0.963	-0.115	-0.099	1
S_2^{in}	0.269	0.993	-0.995	0
S_3^{in}	0	0	0	0
S_1^{out}	-0.994	-0.063	0.074	0.984
S_2^{out}	-0.025	-0.389	0.430	0.053
S_3^{out}	-0.105	0.919	-0.900	0.172
E	0.29 %	30.5 %	28.5 %	0.82 %

Table 3.9: Calculated input and output Stokes vectors using equation 3.18 and 3.19 respectively for all four channels and resulting QBER E.

stokes vectors are given by

$$\vec{S}_{in} = \begin{pmatrix} 1 \\ \cos(2\beta') \\ \sin(2\beta') \\ 0 \end{pmatrix} \tag{3.18}$$

where β' is the measured angle from the polarisers in table 3.2. Note that now only relative angles are taken into account. In the calculation the complete array can be rotated by a matrix $M_{rot}(\delta)$ which aligns the polarisers before the waveguide and thus transforms the relative into absolute angles and also takes into account for suspected misplacement (that means rotation) of the complete array during the assembly which was found to be $\delta < 1°$ (see section 3.3.5). The rotation takes place by multiplying the initial Stokes vector $\vec{S}_{in}$ with the rotation matrix. After this the resulting vector is multiplied with the Mueller matrix $M_{Euler}(\alpha, \beta, \gamma)$ and finally gets a phase shift of $-\frac{\pi}{5}$:

$$\vec{S}_{out} = M_{-\frac{\pi}{5}} M_{Euler}(\alpha, \beta, \gamma) \, M_{rot}(\delta) \, \vec{S}_{in} \tag{3.19}$$

The results for the input Stokes vectors and calculated output Stokes vectors are shown in table 3.9 and show a large deviation from the measured Stokes vectors in table 3.7. But this was already expected as the model used to describe the waveguide is very bad (see values for χ^2_{red}).

To determine the origin of the errors one would have to remove the waveguide from the transmitter unit and characterise it again. However, it is possible to partially compensate for this by a unitary rotation. Of course, non-orthogonal states stay non-orthogonal after a unitary transformation but the overall QBER may be reduced. For the compensation it is convenient to use the transformation described in equation 2.52 because it utilises only standard optics. The three angles for the wave plates are calculated minimising the overall QBER E:

$$E = \min_{\alpha,\beta,\gamma} \sum_{i=H,P,V,M} \frac{E_i(\alpha,\beta,\gamma)}{4} \tag{3.20}$$

where $E_i(\alpha,\beta,\gamma)$ can be calculated from

$$\vec{S}^{out} = M_{\frac{\lambda}{2}}(\gamma)\, M_{\frac{\lambda}{4}}(\beta)\, M_{\frac{\lambda}{4}}(\alpha)\, \vec{S}^{in} \tag{3.21}$$

and with equations 2.62 to 2.65. This minimisation will give a set of angles (α,β,γ) for the wave plates (see table 3.10). The compensation can be tested by just adding the two quarter and the half wave plate in the setup of the tomography:

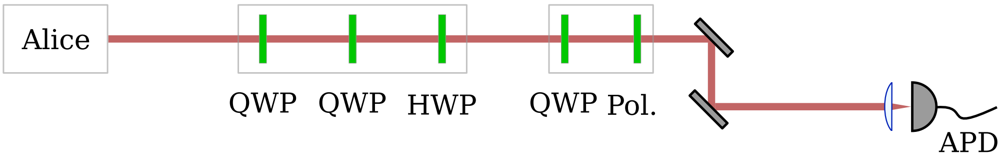


Figure 3.27: Experimental setup for the tomography of the module with compensation. QWP: quarter wave plate. HWP: half wave plate. Pol: polariser. The wave plates and the polarisers are motorised.

The compensation should be motorised as well to allow a more precise setting of the angles. Note that for the tomography of the compensation only the half wave plate was motorised resulting in a rough setting of the angles for the wave plates, but as the error scales with $\sin^2(\Delta\Theta)$ where $\Delta\Theta = \Theta^{cal} - \Theta^{actual} < 0.5°$ this error should be negligible. A larger error comes from one wave plate (Achromat $\frac{\lambda}{4}$ from B. Halle) which makes an error of 3.2 % which was measured with independent measurements with the polarimeter. For the real compensation in the receiver both problems will be solved, all wave plates will be motorised and only good wave plates with measured

	V (channel 0)	P (channel 1)	M (channel 2)	H (channel 3)
S_1^{cal}	-0.948	0.006	-0.162	0.927
S_2^{cal}	0.030	0.816	-0.858	0.156
S_3^{cal}	-0.195	0.542	0.442	0.269
E^{cal}	2.59 %	7.09 %	9.18 %	3.65 %
S_1^{meas}	-0.969	-0.530	-0.103	0.940
S_2^{meas}	-0.003	0.725	-0.841	0.129
S_3^{meas}	-0.135	-0.415	0.463	0.239
E^{exp}	1.54 %	13.8 %	7.97 %	6.57 %

Table 3.10: Calculated (using equation 3.21) and measured Stokes vectors for the corresponding set of angles ($\alpha = 43.0°, \beta = 45.8°, \gamma = 85.9°$) for the wave plates and resulting QBER E.

	V (channel 0)	M (channel 2)	H (channel 3)
S_1^{cal}	-0.961	-0.095	0.974
S_2^{cal}	0.049	-0.974	0.074
S_3^{cal}	-0.108	-0.020	0.051
E^{cal}	1.95 %	1.31 %	1.32 %
S_1^{meas}	-0.955	-0.043	0.981
S_2^{meas}	0.030	-0.973	0.039
S_3^{meas}	0.125	-0.035	0.059
E^{meas}	2.25 %	1.36 %	0.94 %

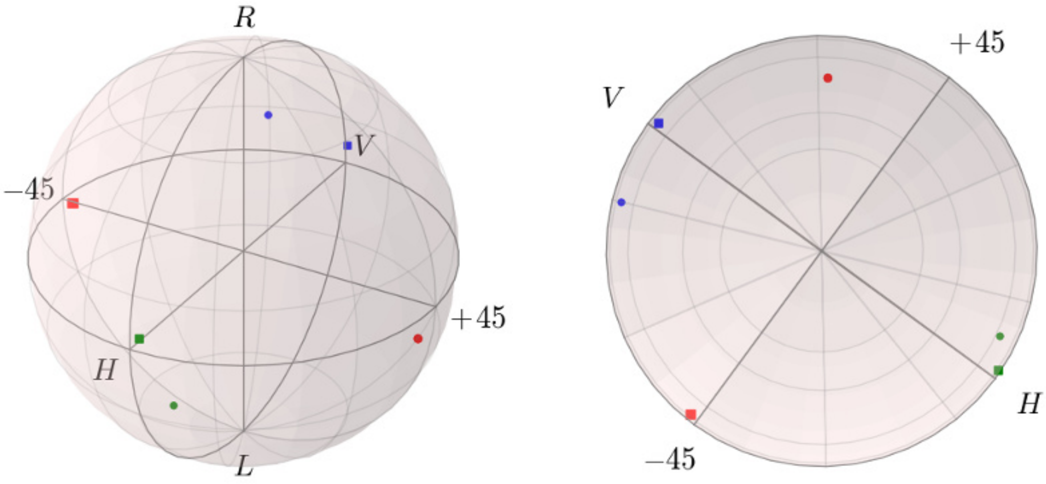
Table 3.11: Calculated (using equation 3.21) and measured Stokes vectors for the corresponding set of angles ($\alpha = 137.5°, \beta = 117.5°, \gamma = 74.5°$) for the wave plates and resulting QBER E.

errors $< 0.15\,\%$ will be used. The result of the tomography is shown in table 3.10. Except for channel 1 all measured Stokes parameters are within the error margin. These QBERs are still very high, but as these are close to the calculated values this cannot be further improved. To decrease the QBERs one would have to use polarising elements, but these are always connected with losses. One approach is to use the 3-State protocol and optimise for only three states. The best result was reached for using channel 0, 2 and 3. A calculation for the 3-State tomography is shown in table 3.11 (see also figure 3.28) together with the measured results after the compensation. Up to measurement errors the experimental results agree very well with the theoretical calculations. Which protocol can yield a higher secret key rate is calculated in section 3.4.3.

It shall be mentioned that the phase compensation found in table 3.10 was not optimal (due to a calculation error) which was noticed only at the very end of the experiment. The calculated results for the true optimal phase compensation is given in 3.12 which was not tested experimentally anymore as anyway another phase compensation (see section 3.4.3) is required. However, the results in table 3.11 indicate that the experimental results can be close to the calculated results. The average QBER for the BB84 protocol thus would be $E = 3.20\,\%$.

	V (channel 0)	M (channel 1)	P (channel 2)	H (channel 3)
S_1^{cal}	-0.949	-0.440	-0.217	0.974
S_2^{cal}	-0.180	-0.872	0.950	0.041
S_3^{cal}	-0.071	-0.086	-0.091	-0.073
E^{cal}	2.56 %	6.42 %	2.51 %	1.29 %

Table 3.12: Calculated (using equation 3.21) Stokes vectors for the corresponding set of angles ($\alpha = 138.8°, \beta = 122.2°, \gamma = 134.0°$) for the wave plates and resulting QBER E.



(a) Visualisation on the Poincaré sphere of the measured Stokes parameters (circles) and calculated corrected Stokes parameters after phase compensation (boxes).

(b) Projection on the linear polarisation plane of the Poincaré sphere of the measured Stokes parameters (circles) and calculated corrected Stokes parameters after phase compensation (boxes).

Figure 3.28: Visualisation on the Poincaré sphere of the measured and calculated corrected Stokes parameters for the BB84 protocol.

3.3.7 New Software

For the development of the Alice module there has also been a lot of software developed of which the most important shall be presented briefly here.

Tomography

For the tomography a new class Tomography.java has been added. It allows the following functions:

1. calculateStokes(): This function calculates the Stokes vectors from the raw-files from the tomography.

2. optimizeStokesEuler(): This function takes the measured Stokes vectors as input and outputs three Euler angles for a unitary transformation such that the QBER is minimised. The resulting Stokes vectors and QBERs for the single states and the average QBER are outputted as well.

3. optimizeStokesWavePlates(): Basically the same function as optimizeStokesEuler(), but the outputted angles are for the wave plate configuration in equation 2.52, which allows an easy implementation of the unitary transformation.

4. fitMuellerMatrix(): This function fits a unitary matrix in the tomography data obtained from the waveguide using the method of least squared. The quality of the fit is calculated with a Chi Square test.

5. simulateWaveGuide(): With this function the polarisation transformation of the complete module can be calculated taking into account the input angles from the fabricated polarisers, the fitted waveguide and the final phase added by the dichroic beam splitter.

6. simulateTomography(): This function allows to calculate arbitrary optical components. This can be used for the determination of the fast and slow axis of wave plates or to calculate the quality of the optical components.

RamTest

With the software available (*alice-control*) there was no option for sending a specific key, only single channels could be turned on and off. For play-back of a specific pattern from the RAM a new class RamTest.java has been added. Currently it allows two different modes:

1. Mode 1: In this mode a 1234-pattern is sent continuously, that means channel 0, 1, 2 and 3 in this order are active successively which is useful for testing purposes as it does not require any complex synchronisation.

2. Mode 2: In this mode the secure pseudo-random number generator (PRNG) from Java (this PRNG is in the SecureRandom class and generates cryptographically strong random numbers) generates 131056 8-bit signed integers i. 131056 is the current maximal key length. To get the key from the random numbers $|i| \bmod 4$ is calculated which activates channel 0, 1, 2 or 3. The key is also saved on the hard drive and is required for the key sifting. This $131056 \times 2\,bit$ long pattern is also sent continuously.

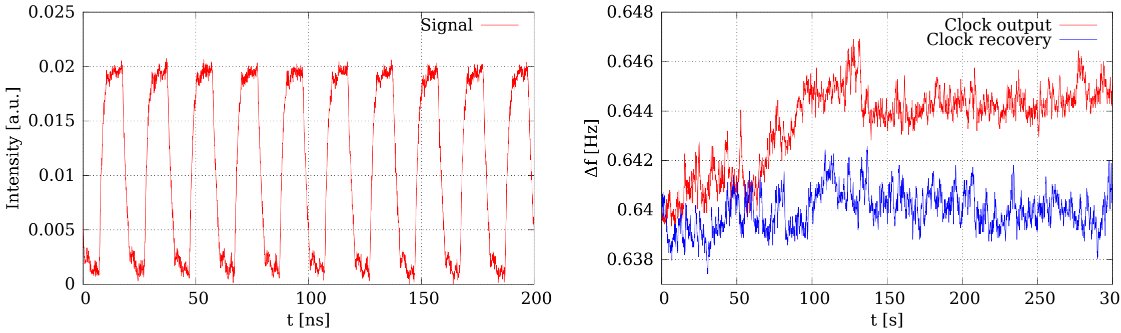
Together with the start of these patterns the beacon can send the "01010111" signal which can be retrieved at the receiver's side and indicates that the key is expected to arrive from now on. Note that both modes can also be operated in a mode when the pattern is sent only once, but this is not very useful as the key exchange time for both modes is $40\,ns$ and $1.31\,ms$ respectively.

3.4 The Receiver: Bob Module

3.4.1 Pulse Synchronisation

A synchronisation is required such that every detection event at Bob's side can be matched with a sent pulse at Alice's side. As already mentioned in section 3.3.3 the beacon laser is modulated with a rectangularly shaped signal with 100 *MHz* using the same clock as the signal VCSELs, so the modulation of the beacon also transmits the modulation of the signal VCSELs. If the beacon light is at least partially guided to a fast photodiode (fast in this manner means a bandwidth $\geq 100\,MHz$), then this allows to recover a 100 *MHz* clock signal by measuring the modulation of the received power. In this experiment a photodiode with exactly 100 *MHz* (Thorlabs DET210) is used. A clock recovery electronics recovers a 100 *MHz* signal (see figure 3.29 (a)) and outputs a 100 *kHz* signal due to the speed of the used electronics (output speed of the FPGA in the clock recovery electronics).

This fully suffices to achieve two synchronously running clocks. For getting a pulse synchronisation as well the following has been done: The beacon transmits the "01010101" signal continuously which serves as the clock signal. Once it is registered by the photodiode Bob's computer sends a start signal to the Alice unit which then sends one "01010111" signal with the beacon and at the same time starts to send the key. The receipt of the "01010111" signal is a start signal that from now on the pulses are expected with some small delay (due to the longer optical and electrical ways in the sender and the receiver). This delay must be measured once and is then fixed for all experiments (the exact value is saved in the sifting software, see also section 3.4.4). A possible way to measure this delay is sending a fixed pattern and then minimising the QBER by trying all possible delays. The same delay is then applied to all detected events in every key exchange with respect to the time when the "01010111" signal is received. Of course, always when the photodiode



(a) Recovery of the 100 *MHz* clock signal (output of the photodiode).

(b) Comparison of the fluctuations of the clock signal measured directly from the clock output on the Alice board (red) and from the clock recovery (blue).

Figure 3.29: Clock recovery and fluctuations.

loses the signal (for example if the incident angle is larger than the mirror range) the pulse synchronisation must be repeated (this feature is not yet implemented). This situation is not frequent as there is no spatial filtering or fibre-coupling before the photodiode. Note that in the current experiment Alice and Bob ran on the same computer, so the key exchange starts immediately when the photodiode registers the beacon laser, which is different from the case when the start signal is sent via Wi-Fi which might take a few $10\,ms$.
As can be seen from figure 3.29 (b) the frequency of the clock recovery is nearly constant ($f_{av} = 99999.3600\,Hz$ with a standard deviation of $0.0008\,Hz$). This can be compared to the frequency of the direct output of the clock of the Alice board ($f_{av} = 99999.3565\,Hz$ with a standard deviation of $0.0016\,Hz$. The fluctuations for 3.29 (b) are calculated using $\Delta f = 100\,kHz - f\,(t)$ where $f\,(t)$ is the frequency of the clock at time t measured with the internal clock of the timestamp card.

3.4.2 Active Basis Alignment

A problem of handheld devices is that they do not have any fixed reference frame. Thus a rotation around the beam axis transforms the polarisation which can of course not be compensated by the mirror control. The error introduced is given by

$$E_{rot} = \sin(\Theta)^2 \tag{3.22}$$

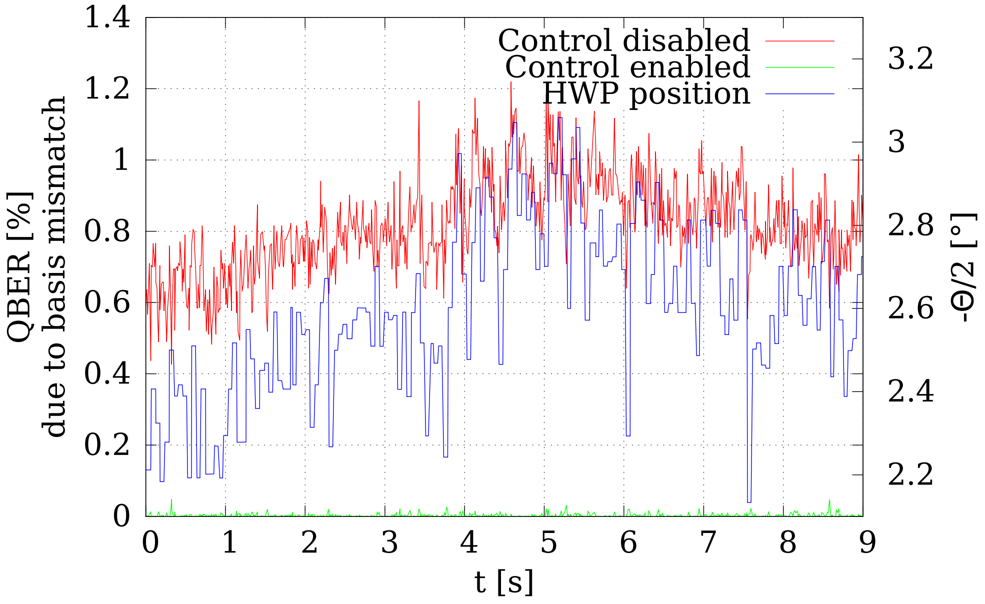


Figure 3.30: Introduced QBER E_{rot} due to basis mismatch without (red) and with (green) active basis alignment (calculated). Additionally shown is the position of the half wave plate (blue).

with Θ being the rotation angle. At an angle of $\Theta = 5.74°$ the introduced error reaches 1 %. If the module is integrated into a smart phone one can utilise the device orientation sensor to read out the device's orientation, calculate the angle of polarisation rotation Θ and send this angle via Wi-Fi to the receiver where a motorised half wave plate can rotate the polarisation back to its initial orientation. The angle between the fast axis of the wave plate and H must be $\frac{-\Theta}{2}$. In this experiment the sender module must be attached to a smart phone (tested with Huawei Y530-U00) as it has no own device orientation sensor. A measurement (see figure 3.30) showed that the introduced error (only due to this reference frame mismatch) is on average 0.86 % while with the active basis alignment the introduced error is $< 0.007\,\%$ (calculated) which makes it negligibly small. The control itself introduces an error $< 0.001\,\%$ (measured) which is obtained with the module at rest. The limiting factor is the speed of the motorised half wave plate. The rotation angle is updated on average every $11.5\,ms$ depending on the current traffic in the Wi-Fi network of which only every 5th event can be used due to the speed of the step motor, such that the half wave plate position is updated every $57.5\,ms$. As this rotation error with the control is anyway much smaller than the other introduced errors this control is sufficiently fast.
Note that the half wave plate should be placed only after the voicecoil mirror as it is only truly a half wave plate if the beam passes perpendicular through the wave plate.

3.4.3 New Phase Compensation

First measurements have been performed with the module mounted in front of the receiver (see figure 3.31) using a customised holder. These measurements showed large QBERs ($> 11\,\%$) at which QKD cannot generate secure keys anymore. This was even with the phase compensation obtained in 3.3.6. The most probable expla-

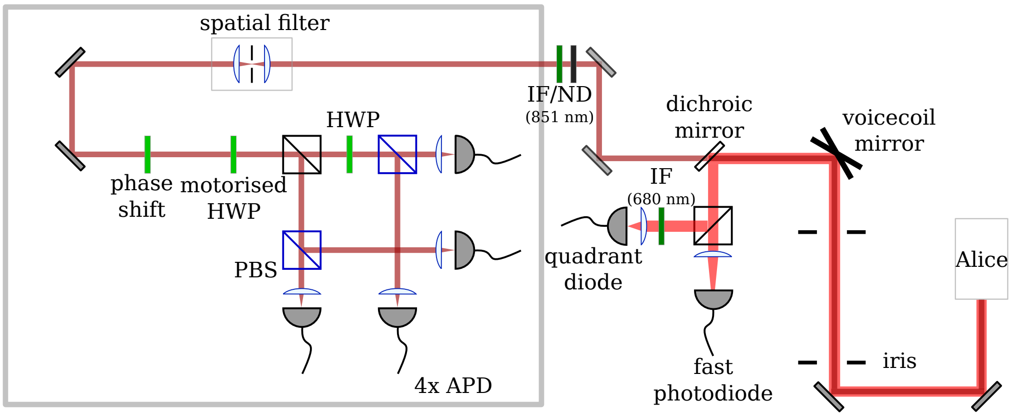


Figure 3.31: Experimental setup for measurements with the fixed Alice module. IF: interference filter. ND: neutral density filter. HWP: half wave plate. PBS: polarising beam splitter. APD: avalanche photodiode.

projection on	H	V	P	M	R	L
orientation QWP1	0°	0°	0°	0°	0°	0°
orientation QWP2	0°	0°	0°	0°	45°	45°
orientation HWP	0°	45°	22.5°	−22.5°	22.5°	−22.5°

Table 3.13: Possible set of orientations for the wave plates if the APD in the H-polarised arm of the PBS is used. The horizontal axis is defined as 0°.

nation are polarisation rotations or partially polarising effects in the receiver module. To find out what might have happened one can make another tomography with the receiver module. In principle the polarisation analysis unit projects on four of the six polarisation basis states and with the assumption that the degree of polarisation does not change in the receiver one could calculate the last two projections (up to a ± sign) and thus reconstruct the polarisation state. As the APDs do have slightly different quantum efficiencies (see section 4.2) and the coupling might differ it is more precise to use a single APD. For this the motorised phase compensation can be used for the six projections, if a polariser (in this case a PBS) is oriented along H before the APD (see table 3.13). In other words a tomography of the sender together with the receiver is performed.

The results are shown in table 3.14 which differs significantly from the results shown in table 3.7 confirming the polarisation changes. Calculations for a new phase compensation showed for four states a QBER of 14.36 % and for the three states a QBER of 5.67 %. This indicates partially polarising effects. In fact, the silver mirrors (Thorlabs protected silver coated mirror) have slightly different reflection coefficients at different angles of incidence (AOI) for S- and P-polarised light ($\Delta R \approx 0.5\,\%$ for 45° AOI and $\Delta R \approx 1.0\,\%$ for 12° AOI). In the experiment the AOIs are close to 45°, but the planes of incidence are not parallel for all mirrors. This was due to the fact that the Alice module does not emit parallel to its ground plate. In total seven mirrors are used (see figure 3.31). The dichroic beam splitter has different transmission coefficients for S- and P-polarisation as well ($\Delta T = 0.6\,\%$). Thus the receiver shows polarising effects which can be in principle compensated (for details see section 6.2).

However, calculations showed that this alone does not explain the large polarising effects. To get a better understanding of these effects the dichroic beam splitter (Semrock FF757-Di01) is characterised completely: First, the transmissions for S-

	channel 0	channel 1	channel 2	channel 3
S_1	-0.927	-0.953	-0.604	0.640
S_2	0.186	-0.281	0.456	-0.699
S_3	0.246	-0.047	0.573	-0.136

Table 3.14: Measured Stokes vectors with the tomography made with the receiver.

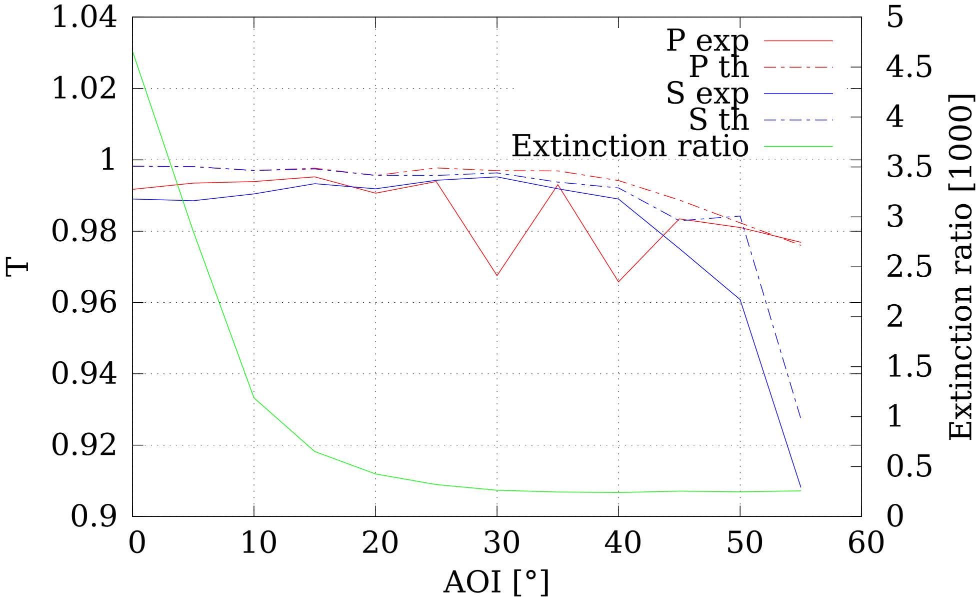


Figure 3.32: Transmittances for S- and P-polarisation as a function of the angle of incidence (AOI) for the dichroic mirror, measured experimentally (solid lines) and theoretically (dashed lines). Additionally shown the extinction ratio when the mirror is placed in between two crossed polarisers.

and P-polarisation are measured for different AOIs and compared to the theoretical values. Second, the dichroic mirror is placed in between two crossed polarisers and the extinction ratio is measured for different AOIs. The results are shown in figure 3.32: The measured transmittances show qualitatively a similar behaviour as the theoretical transmittances (calculated with the theory provided by Semrock). The extinction ratio between the crossed polarisers decreases almost exponentially with the AOI from 5000 under 0° to 200 under 45° AOI at which the dichroic mirror is specified for. Hence together with the results from the first measurement it is expected that the polarisation change by the dichroic mirror is a mixture of a unitary polarisation rotation and a non-unitary polarisation change. But one can also see that these polarisation changes are very small with a small AOI so it might probably help to work in this regime. As a second improvement all mirrors have been exchanged with protected gold mirrors which are known to have less effects on the polarisation for infra-red light, although according to Thorlabs $\Delta R = 0.8\,\%$ for S- and P-polarisation for 45° AOI, but these are only typical values so it is still possible, that changing the mirrors can improve the polarisation rotations as can be seen from the final tomography (table 3.15). Note that only the results for the final tomography is shown, reducing the AOI towards the dichroic mirror and exchanging the mirrors successively lowered the achievable QBER. It shall be further mentioned that there is no chance to make a tomography of this phase compensation as the wave plates for the tomography are already needed for the phase compensation.

	channel 0	channel 1	channel 2	channel 3
S_1	-0.929	-0.026	-0.452	0.977
S_2	0.266	-0.181	0.271	-0.126
S_3	0.138	0.978	-0.780	-0.041
S_1^{cal}	-0.970	-0.186	-0.330	0.973
S_2^{cal}	0.075	-0.977	0.881	-0.138
S_3^{cal}	0.078	0.045	-0.020	0.087
E^{cal}	1.52 %	1.16 %	5.93 %	1.37 %

Table 3.15: Measured Stokes vectors with the tomography made with the receiver after the improvements described above. Additional the calculated Stokes vectors for the corresponding set of angles ($\alpha = 51.6°, \beta = 0.0°, \gamma = 160.4°$) for the wave plates and resulting QBER E for the BB84 protocol.

However, one can compare the measured QBER to the calculated QBER.
The final question is, whether the 3-State protocol or the BB84 protocol can yield a higher secret key rate. For this equation 2.32 is evaluated for both protocols. For the 3-State protocol the calculated QBERs are $e_b = 1.16\,\%$, $\alpha = 0.41\,\%$ and thus $e_p = 4.11\,\%$, while for the BB84 protocol $e_b = e_p = 2.48\,\%$. Plugging these equations into 2.32 yields

$$R_{secret}^{BB84} = 0.43 \cdot R_{sifted}^{BB84} \tag{3.23}$$

$$R_{secret}^{3-State} = 0.43 \cdot R_{sifted}^{3-State} \tag{3.24}$$

which shows that it makes no difference for the secret key rate whether the 3-State protocol or the BB84 protocol is used. As the calculation of the finite effects (see section 5.1) or evaluating the protocol according to the SARG04 protocol (see section 5.2) requires four states the BB84 protocol has been implemented in the final experiment.

3.4.4 New Software

For the development of the Bob module there has also been a lot of software developed of which the most important shall be presented briefly here. The software for the mirror control is described in [51].

Alice on Android

For the active basis alignment as described in section 3.4.2 two parts are required: The software on the smart phone (client on Android) and the software for controlling the wave plates (server on Linux).
Once the Android App is started and connected to the Wi-Fi network the rotation angle is sent continuously over the network until the client disconnects. It is impor-

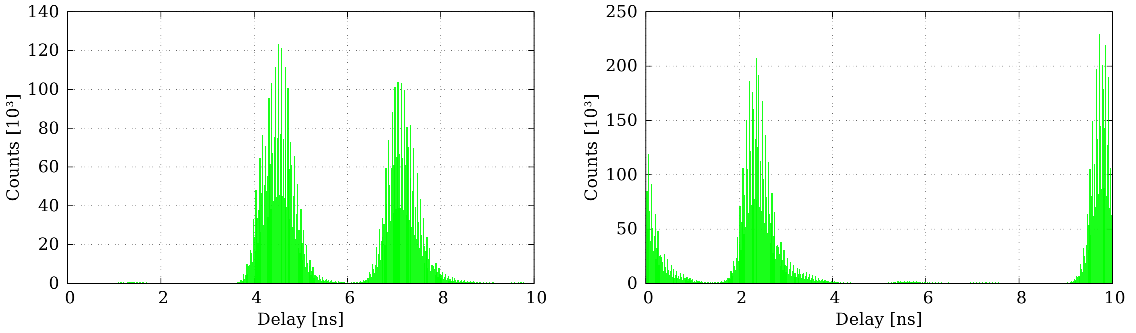
tant to calibrate the software before first usage (by placing the phone on the module at rest and measure the angle of rotation (average over a few seconds). This value must be saved in the variable "*calib*". If the server does not receive anything, the IP address and port must be checked (currently the server runs on 10.153.153.45:8000). After recalibrating or changing IP address or port the software must be recompiled.

Bob on Linux

When the Bob server is started the half wave plate is calibrated automatically. It must be taken care that the correct calibration angle from the phase compensation is used. The other wave plates can be calibrated in this step as well. Note that all step motors must be calibrated before first usage. After receiving the orientation of the smart phone the angle of rotation is converted to a wave plate position and sent to the step motor. As afore mentioned it is important that the correct port is opened on the server that the data from Alice can be accepted. Due to the speed of the step motor only every 5th event is sent to the step motor, all other events are withdrawn.

Read-out of the APDs & sifting

For the reading-out the APDs the main function in Bob.class in the freespace-project must be executed. Every detection event with timestamp and channel number will be saved on the hard drive until the program is stopped. Finally with the Sifting class one can generate and plot histograms with the function generatePhaseHist(). As can be seen from figure 3.33 (a) one will see two peaks with a temporal delay of 2.4 ns, even if only a single VCSEL from Alice is active, although all photons arrive at the same time at the polarisation analysis unit. As it turned out only APD channel 0 and channel 2 contribute to the second peak while all photons from the first peak originate from APD channel 1 and channel 3. Note that the height of the



(a) Histogram of the received pulses. The integration time was 8 s.

(b) Example histogram of the received pulses when the pulses arrive close to one of the clock signals.

Figure 3.33: Histograms of the received pulses.

peaks (or rather the distribution between both peaks) depends on the polarisation. The different optical path lengths in the polarisation analysis unit contribute with a maximal delay $< 0.1\,ns$ and the "longer" optical paths do not correlate with the delayed channels in the histogram. All fibres and cables have exactly the same length. Therefore the delay of $2.4\,ns$ must be accounted to the internal electronics of the APDs. This fact is confirmed by measuring the delays at the ends of the fibres always with the same APD which gives the same delay for all four fibres. With the shiftData() function one can shift all timestamps which is necessary if the pulses arrive close to one of the clock signals as shown in figure 3.33 (b), where the time windows have an overlap. Next, the function selectEvents() selects only events within the timing window which must be obtained from the histogram. Note that one has a timing window for channel 0 and 2 and a different timing window for channel 1 and 3 which must have the same size, otherwise an eavesdropper could launch a time-shift attack exploiting temporarily varying detection efficiencies[32]. After the selectEvents() function the dark count rate can be kept low (see section 4.1). Finally the postProcess() functions can calculate key rates and QBERs and also plot the results.

4 Experimental Part II: Tests and Results

In this chapter the final experimental results shall be presented. First, measurements of the dark count rate under various conditions, second, determination of the mean photon number and finally, experiments where secure keys are generated.

4.1 Dark Count Rate

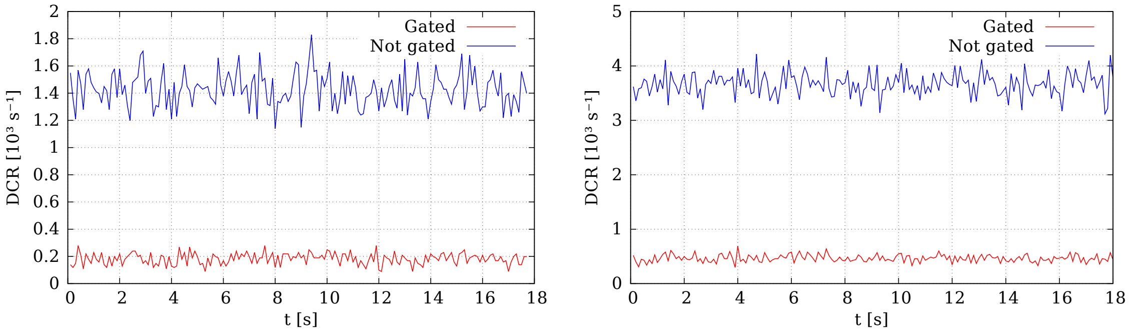
To determine the dark count rate (DCR) three different measurements have been performed: The normal dark count rate, the dark count rate if the detection events are gated within a time window and the dark count rate under daylight conditions (also if the detection events are gated). According to the specifications the APDs (PerkinElmer DTS SPCM-AQ4C) used have a DCR of typically $500\,s^{-1}$.

The observed dark count rate (always sum over all four channels, averaged over $18-25\,s$) with the beacon laser turned off is $1427\,s^{-1}\ \pm 40\,s^{-1}$ (see figure 4.1 (a)) while with the beacon laser turned on is $3669\,s^{-1}\ \pm 67\,s^{-1}$ (see figure 4.1 (b)). The second value is always the standard deviation of the data. If the events are gated in a specific timing window of $1280\,ps$ the average dark count rates for $100\,MHz$ repetition rate reduce to $182\,s^{-1}\ \pm 13\,s^{-1}$ and $466\,s^{-1}\ \pm 22\,s^{-1}$ respectively. The beacon output power (output power of the complete module) was $789\,\mu W$ and thus the beacon contributes to the dark counts because a 0 from the 01010101 signal is encoded with no power and a 1 with full power and each 0 or 1 is sent for $10\,ns$. Note that only $\frac{1}{4}$ of these dark counts contribute to the QBER, because $\frac{1}{2}$ of dark counts will be in the wrong basis and thus be removed during key sifting and $\frac{1}{2}$ of the remaining dark counts will be in the correct detector and thus not contribute to the QBER. Compared to a sifted key rate $R_{sifted} = 0.35 \cdot 10^6\,s^{-1}$ the QBER E_{dark} due to dark counts will be

$$E_{dark} = \frac{R_{dark}}{4R_{sifted}} = 0.03\,\% \tag{4.1}$$

which is negligibly small compared to other contributions to the QBER. Note that the beacon laser is linearly polarised, so the background counts are not equally distributed over all four channels.

Finally the dark count rate under "daylight-like" conditions has been estimated. For this the receiver is moved from the lab to the lecture hall H030 of the physics department of the Ludwig-Maximilian-University of Munich and the dark count rate

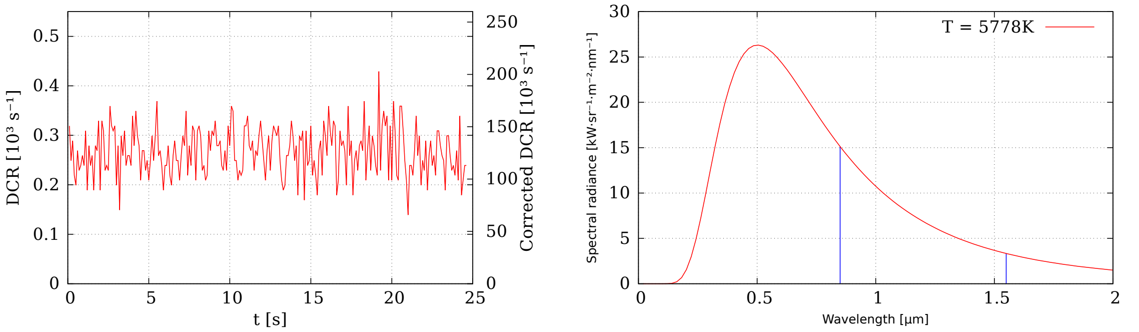


(a) Dark count rates without the beacon laser, with temporal filtering (red) and without temporal filtering (blue).

(b) Dark count rates with the beacon laser, with temporal filtering (red) and without temporal filtering (blue).

Figure 4.1: Dark count rates with and without the beacon laser, in both cases with and without temporal filtering. The measurement took place in the laboratory.

has been measured (on 19 December 2015, 1 pm, very cloudy weather) when the setup is oriented towards a window. Of course this can only indicate whether the dark count rate in field tests outside could be small enough as there are only a few windows in the lecture hall which of course also filter the incoming light. The intensity of the light at 851 nm in the lecture hall is measured with a power meter (Thorlabs PM100D) and a interference filter (851 nm, FWHM $= 10\,nm$, $T = 0.8$)) which is identical with the interference filter used in the receiver. The light intensity outside the building is also measured (same orientation and compass direction). The



(a) Dark count rate without the beacon laser and with temporal filtering and with the additional correction factor on the other axis. The measurement took place in the lecture hall H030.

(b) Spectral radiance of the sun approximated as a black body at 5778 K. The transmittance of the earth's atmosphere has not been taken into account. Additionally shown are the values for $\lambda = 0.85\,\mu m$ and $\lambda = 1.55\,\mu m$ (blue lines).

Figure 4.2: Dark count rates under "daylight-like" conditions and spectral radiance of the sun.

measured intensities are $I_{inside} = 18.5 \cdot 10^{-9} W/cm^2$ and $I_{outside} = 8.68 \cdot 10^{-6} W/cm^2$, so for calculating the dark count rate outside the correction factor is $\frac{I_{outside}}{I_{inside}} = 469.2$. The gated results (without the beacon laser, as the contributions after the correction are negligibly small) are shown in figure 4.2 (a). The average dark count rate is $266\,s^{-1} \pm 15\,s^{-1}$ and the expected dark count rate outside is thus $125032\,s^{-1}$. Together with the factor of $\frac{1}{4}$ (see above) the QBER due to dark counts would be

$$E_{dark} = \frac{R_{dark}}{4R_{sifted}} = 8.91\,\% \qquad (4.2)$$

For a comparison: To have $E_{dark} < 1\,\%$ one needs a sifted key rate $R_{sifted} > 12.5 \cdot 10^6\,s^{-1}$. One could argue that one should only multiply the additional dark count rate with the correction factor as the dark count rate in the lab mostly originates from thermally excited and trapped electrons in the semiconductor material inside the APDs. This assumption is supported by the fact that the dark count rate does not decrease if the entry interference filter is blocked (in the lab). However, multiplying only the additional dark count rate with the correction factor still yields an expected dark count rate of $39413\,s^{-1}$. Together with the other contributions (source- and receiver-intrinsic QBER) the overall QBER would exceed $11\,\%$.

To conclude this section, with the current setup it would not be possible to make the experiment outside (especially not if the weather is sunny). Possible improvements are an interference filter with a narrower bandwidth or changing the operating wavelength to higher wavelengths (e.g. telecom wavelengths at $\lambda = 1550\,nm$, as there are single photon detectors with high quantum efficiencies available and air has a transmission window at this wavelength). The big advantage is that there is far less background radiation at this wavelength (see figure 4.2 (b)): The ratio of the spectral radiances S is $\frac{S(1.55\,\mu m)}{S(0.85\,\mu m)} = 0.22$. It shall be mentioned that most ATMs are anyway inside, these ATMs could probably be equipped with the current receiver.

4.2 Determination of the Mean Photon Number

For the calculation of the secret key rate the mean photon number has to be estimated. This has been done with the APDs of the receiver. The setup is as in figure 3.31. First, the overall transmission through the receiver is determined with an additional laser at $850\,nm$, by dividing the power at the entrance of the receiver by the power behind the four multi-mode fibres. This transmission is $\tau_{Bob} = 0.244$, including all losses at mirrors, filters and fibre couplings. Then the Alice module sends all four states, one after the other periodically. The parameters for each state are aligned such that pulse shape and intensity are equal for all channels (see section 3.3.6). The rate detected by the APDs is not only due to the transmission smaller than the actual rate emitted by the module, but also due to the detector non-linearity and efficiency of the APDs. The actual total rate emitted by the Alice module (when the four states are sent one after another) is given by

$$R^{actual} = \frac{\sum_{k=1}^{4}\left(R_k \cdot c_k - R_k^{dark}\right)}{\eta\tau_{Bob}} \tag{4.3}$$

where R_k is the measured detection rate of the k-th APD, c is a correction factor, taking the non-linearity into account and η is the efficiency of the APDs.
Note that the APDs have slightly different efficiencies. This is measured by shining with a constant input signal towards the receiver and connecting always the same fibre to all four APDs one after another. The measured relative efficiencies are then:

APD	channel 0	channel 1	channel 2	channel 3
Av. rate $[s^{-1}]$	270179(1659)	259058(1713)	272174(1714)	258970(1871)
Rel. efficiency	1.04	1.00	1.05	1

Table 4.1: Relative efficiencies of the APDs normalised to the efficiency of channel 3. The absolute quantum efficiency is specified to be 38 %.

To show that these discrepancies of the efficiencies do not originate simply from differently connected fibres two additional measurements have been performed: The fibre is unplugged and plugged back to the APD, here the ratio of the rates is $\frac{R_{after}}{R_{before}} = \frac{240035}{239333} \approx 1.00$. And in a second measurement with strong wiggling of the fibre the ratio of the rates is $\frac{R_{after}}{R_{before}} = \frac{269735}{270179} \approx 1.00$ so one can trace the discrepancies of the efficiencies back to intrinsic discrepancies of the APDs.
The non-linearity of the APDs is mostly due to the deadtime of the detectors. During this time, after a detection event the detector cannot detect another photon. The correction factor is given by

$$c_k = \frac{1}{1 - t_D \cdot R_k} \tag{4.4}$$

where t_D is the deadtime of the detectors. According to the specifications $t_D = 50\,ns$ for $R_k < 5 \cdot 10^6 s^{-1}$. Equation 4.3 yields with the parameters mentioned above and the rates in table 4.2 an actual emitted rate $R^{actual} = 48.9 \cdot 10^6\, s^{-1}$.

APD	channel 0	channel 1	channel 2	channel 3
R_{raw} $[s^{-1}]$	1100268	1213751	605780	1023931
R_{dark} $[s^{-1}]$	415	429	393	434
c	1.06	1.06	1.03	1.05

Table 4.2: Rates and correction factors which are used to calculate the mean photon number. Also used is a quantum efficiency $\eta = 38\,\%$ (specified by PerkinElmer) and a transmission $\tau_{Bob} = 0.244$.

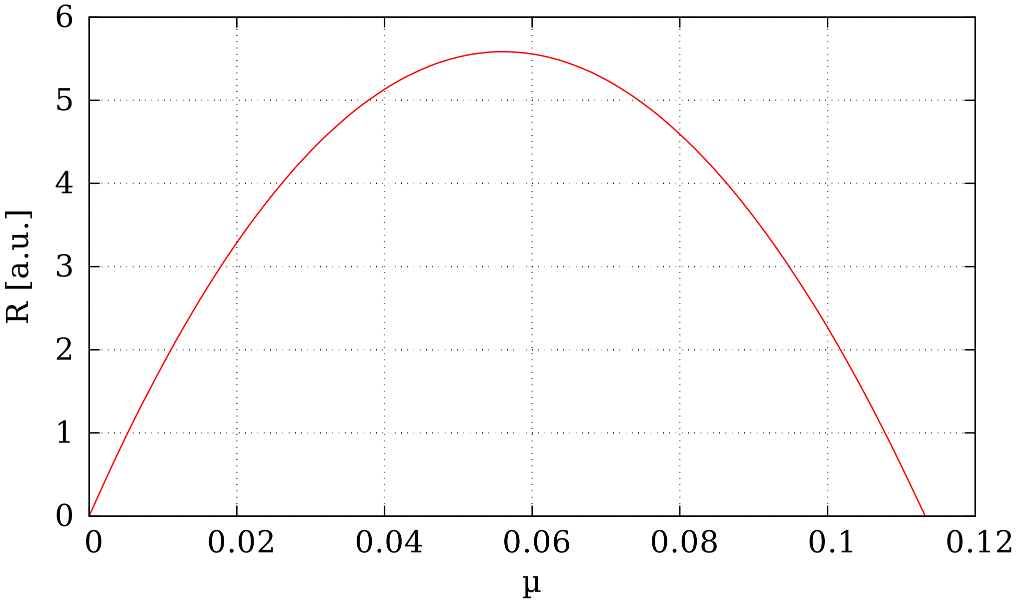


Figure 4.3: Secret key rate as a function of μ with a transmission $\tau_{Bob} = 0.244$, quantum efficiency $\eta = 38\,\%$ and QBER $E = 6.84\,\%$. For handheld operation the transmission is differently and thus also the optimal mean photon number.

Finally the mean photon number μ is given by

$$\mu = \frac{R^{actual}}{f_{laser}} \tag{4.5}$$

so the mean photon number for a laser repetition frequency of 100 MHz is $\mu = 0.49$. Note that this is only approximation which is valid if $\mu\tau_{Bob} \ll 1$ as in that case $1 - e^{-\mu\tau_{Bob}} \approx \mu\tau_{Bob}$ (see equation 2.37). Together with the measured QBER (see section 4.4) one can calculate the optimal mean photon number μ by maximising equation 2.32. Note that R_{sifted} is proportional to μ (see equation 2.37). The secret key rate as a function of μ with a fixed transmission (including the losses in the quantum channel and in the receiver) and QBER is shown in figure 4.3 and has a maximum at $\mu^{opt} = 0.056$. The initial mean photon number of $\mu = 0.49$ must be attenuated to the optimal mean photon number $\mu^{opt} = 0.056$ so an attenuation of

$$b = \frac{\mu^{opt}}{\mu} = 0.114 \tag{4.6}$$

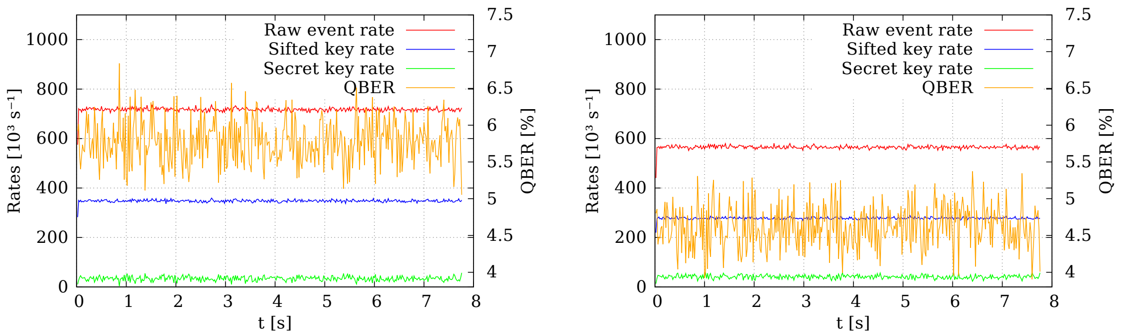
is required. The available neutral density filter are only specified for optical light and have different transmissions for infra-red light. The closest transmission to $b = 0.114$ is found for a combination of two ND-filters with ND = 0.4 and ND = 0.6. The measured transmission for light at 850 nm is

$$b' = \frac{62.2\,\mu W}{517.4\,\mu W} = 0.121 \tag{4.7}$$

so for infra-red light this combination is a ND-filter with ND = 0.917 (instead of ND = 1 for optical light). The set mean photon number is thus $\mu^{set} = 0.059$. Hence the achievable secret key rate is 99.7 % of the maximal achievable secret key rate with μ^{opt}.

4.3 Determination of the Detection Window

The detection window of 1280 ps in section 4.1 has been chosen such that the start and end of the received pulses have a signal-to-noise ratio (SNR) of 100, meaning that the number of counts within the pulse in the timeslots in the histogram are 100 times as high as the number of counts outside the pulse. In this case the contributions to the QBER due to dark counts is below 1 %. However, it turned out with smaller detection windows the QBER decreases together with raw and sifted key rate. The constant current through the VCSELs I_b leads to spontaneous emission which in turn contributes to the dark counts but as this current is constant the background counts should be equally distributed and thus with the threshold for the SNR as chosen above not contribute overly to the QBER. It shall be mentioned that the dark count rate in section 4.1 was measured without the infra-red VCSELs



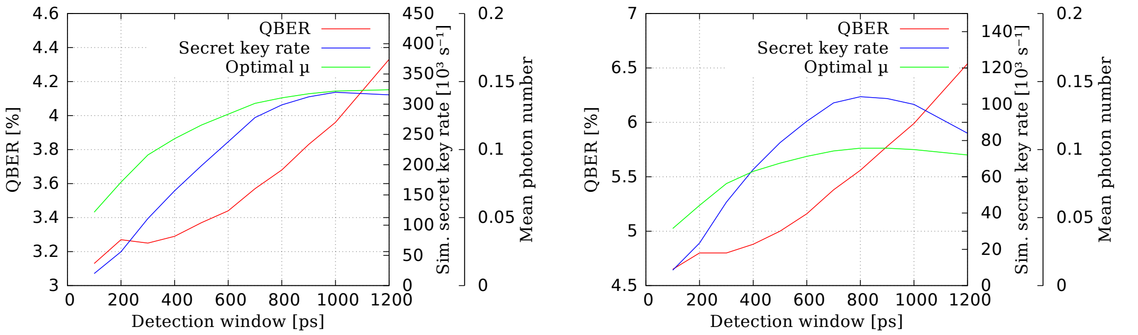
(a) Rates and QBER with a detection window of 1280 ps.

(b) Rates and QBER with a detection window of 740 ps.

Det. win.	**R.e.r.** $[10^3\,s^{-1}]$	**Si.k.r.** $[10^3\,s^{-1}]$	**Se.k.r.** $[10^3\,s^{-1}]$	**QBER** [%]
1280 ps	717.2	347.7	33.9	5.78
740 ps	564.8	278.0	41.1	4.62

(c) Rates and QBER for different detection windows (det. win.) for the same measurement. R.e.r.: raw event rate. Si.k.r.: sifted key rate. Se.k.r.: secret key rate.

Figure 4.4: Rates and QBER for the same measurement, but different detection windows.



(a) QBER, optimised secret key rate and optimal mean photon number as a function of the detection window size for measurement series 1.

(b) QBER, optimised secret key rate and optimal mean photon number as a function of the detection window size for measurement series 2.

Figure 4.5: Key parameters at different detection window sizes.

enabled. Comparing the histogram of the received pulses in a region where no pulse detected with a histogram of the previous dark count rate measurement in the same region gives rise to the fact that the dark count rate with the infra-red VCSELs enabled is 9.53 times as high as with the infra-red VCSELs disabled.

However, a simple evaluation of experimental data showed that for different detection windows (for example FWHM in the histogram which is 740 ps) the lower sifted key rate and lower QBER together still lead to a higher secret key rate (see figure 4.4 (a) and (b) and table 4.4 (c)). The QBER is reduced from 5.78 % to 4.62 % and thus the secret key rate is increased from $33.9 \cdot 10^3\,s^{-1}$ to $41.1 \cdot 10^3\,s^{-1}$. The size (FWHM) of this new detection window was now chosen arbitrarily as well. An optimisation algorithm could find the optimal size and position of the detection window by maximising the secret key rate and must be implemented in future work. However, empirical testing of a few detection window sizes and positions showed already improvements over the old detection window. Figure 4.5 shows the QBER as a function of the detection window size for two different measurement series. It shall be mentioned that the QBERs in measurement series 1 is lower than the QBERs in measurement series 2. The difference between the measurements are different neutral density filters (which should not influence the QBER as these filters are passed perpendicular) and a different phase compensation. The new phase compensation was calculated after a new tomography which took place prior to the key exchanges of measurement series 2. It seems that the transmitter was mounted with a different angle towards the receiver such that the non-unitary polarisation change is larger.

With the size of the detection window a new transmission can be calculated and thus together with the QBER an optimal mean photon number μ. With this new optimal μ the secret key rate can be calculated. Figure 4.5 (a) shows a possible maximal secret key rate of $319.8 \cdot 10^3\,s^{-1}$ at a QBER of 3.96 % for the first measurement series and figure 4.5 (b) a possible maximal secret key rate of $104.1 \cdot 10^3\,s^{-1}$ at a QBER of 5.56 % for the second measurement series. The size of the optimal

detection windows are 1000 ps and 800 ps respectively.
All following results are evaluated with these optimal detection windows, but as these different detection windows are always accompanied with different QBERs and transmissions, the chosen mean photon numbers were not optimal. However, section 4.6 will compute which key rates are possible with the optimal mean photon numbers. As already mentioned future work must implement an efficient algorithm capable of extracting even better detection windows. Hence the possible secret key rates could be even higher.

4.4 Experiments with fixed short Keys

For the final experiment two different types of keys have been exchanged: Short keys with a fixed pattern and long sequences of random keys, as they are required for Quantum Key Distribution. For the latter see the next section. The pattern for the short key is $|V\rangle \rightarrow |M\rangle \rightarrow |P\rangle \rightarrow |H\rangle$ which is sent periodically. Thus for these experiments no synchronisation is required as only four possible delays must be tested (by minimising the QBER).

4.4.1 Tests with a fixed Sender

Before the handheld tests the experiment was tested with the sending unit mounted in front of the receiver. As already mentioned in the previous section there have

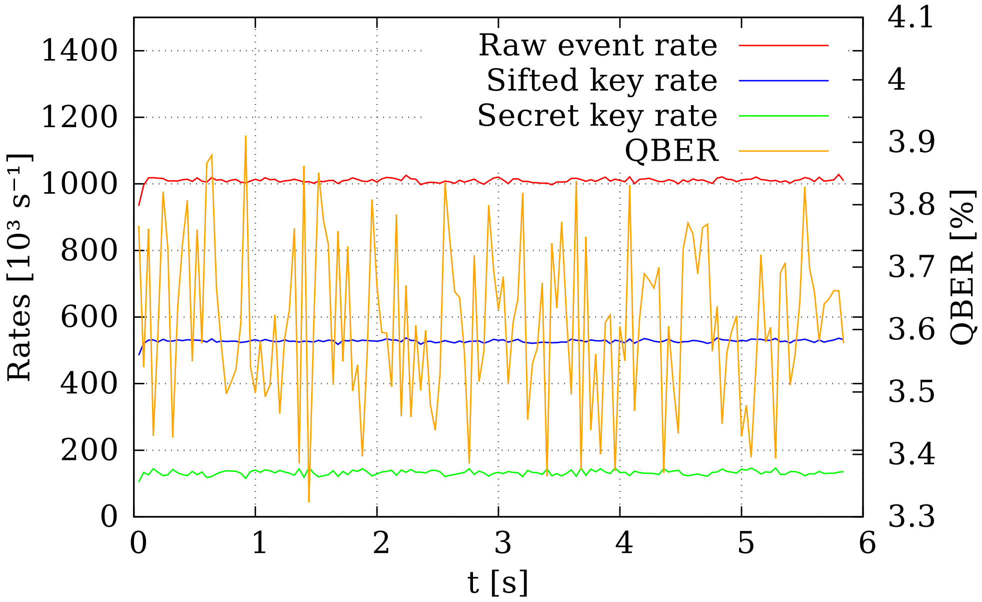


Figure 4.6: Key rates for tests with a fixed receiver (series 1): Raw (red), sifted (blue) and secret (green). Additionally shown is the QBER (orange). The key sent by Alice is 1100 and repeated periodically.

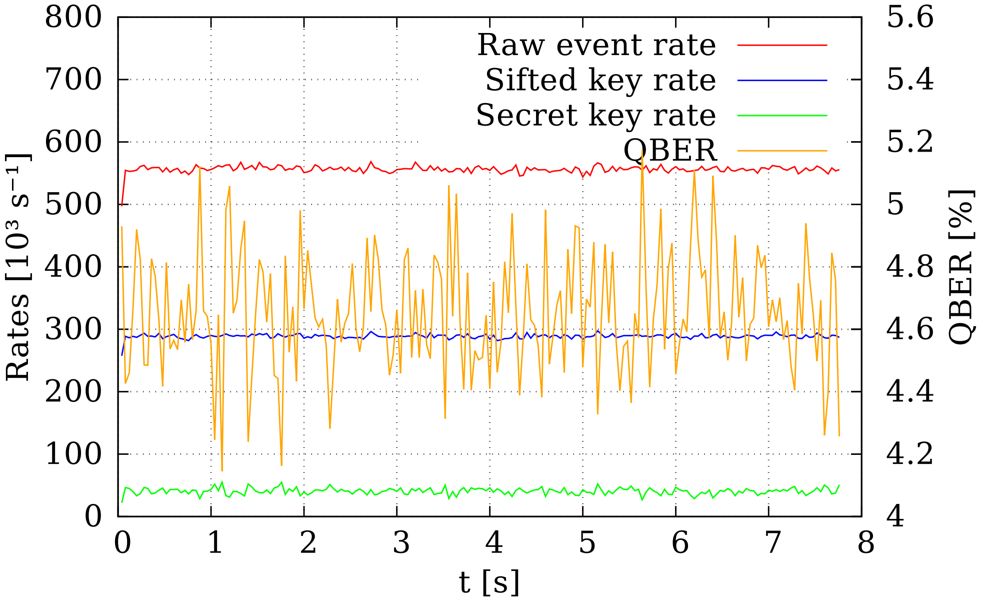


Figure 4.7: Rates for tests with a fixed receiver (series 2): Raw event (red), sifted key (blue) and secret key (green). Additionally shown is the QBER (orange). The key sent by Alice is 1100 and repeated periodically.

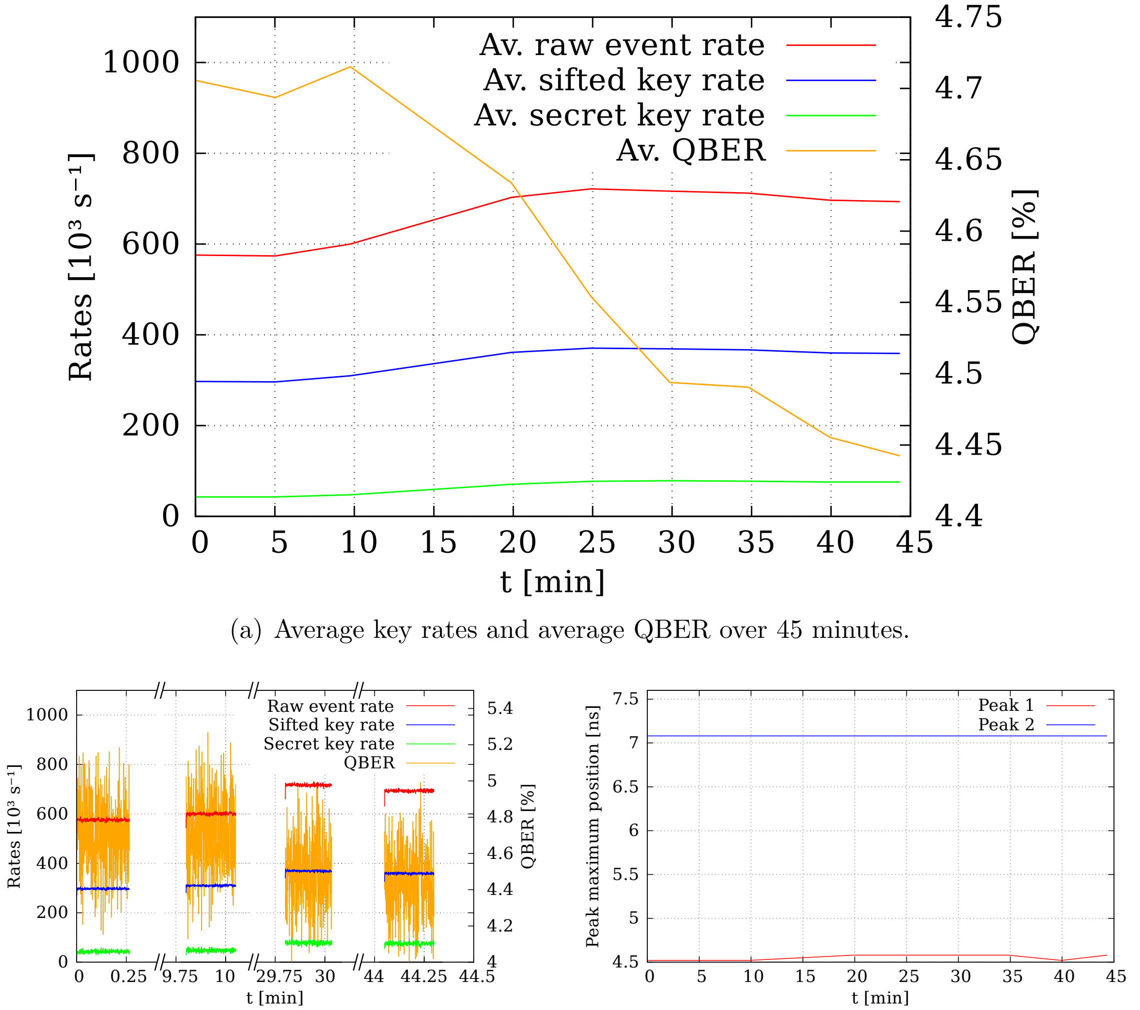
been two measurement series. In the measurement of the first series there have been 5897407 raw events measured. This results in 3082660 sifted bit, of which 111361 bit were wrong, corresponding to a QBER $E = 3.61\,\%$ (see figure 4.6). Calculating the extractable secret key, with an error correction efficiency assumed to be $f = 1.22$ as in the GYS-experiment[58] and equation 2.32, results in a secret key of 773775 bit length. Together with a key exchange time of $5.84\,s$ this corresponds to an average raw event rate of $1009.8 \cdot 10^3\,s^{-1}$, a sifted key rate of $527.9 \cdot 10^3\,s^{-1}$ and a secret key rate of $132.5 \cdot 10^3\,s^{-1}$.

In the measurement of the second series (for the differences see the above section) there have been 4315700 raw events measured. This results in 2240043 sifted bit, of which 104274 bit were wrong, corresponding to a QBER $E = 4.66\,\%$ (see figure 4.7). The extractable secret key length in this case is 314640 bit. Together with a key exchange time of $7.76\,s$ this corresponds to an average raw event rate of $556.1 \cdot 10^3\,s^{-1}$, a sifted key rate of $288.7 \cdot 10^3\,s^{-1}$ and a secret key rate of $40.5 \cdot 10^3\,s^{-1}$.

Note that measurement series 2 uses a different neutral density filter and smaller detection window and hence it is not surprising that the average key rates are lower compared to measurement series 1.

4.4.2 Long-time tests with a fixed Sender

In the next step it shall be determined how the key rates and QBER evolute in time in order to analyse drifts of the module and the electronics. This is especially interesting because the unit has very small dimensions and can, in principle, be



(a) Average key rates and average QBER over 45 minutes.

(b) Average key rates and average QBER over 45 minutes with a zoom into four time windows.

(c) Position of peak maximum 1 and peak maximum 2 in the histogram over 45 minutes.

Figure 4.8: Long-time measurement of the temporal evolution of the average key rates and QBERs (a), (b) and of the peak maximum positions (c).

implemented into every infrastructure and scenario. The operating distance only depends on the outcoupling optics. While the maximal distance is currently limited to a few metres, the operational range can easily be extended with a telescope to a few kilometres. Such long-distance applications usually require long key exchange times and thus it is interesting to know how stable the key rates and especially the QBER are. To study long-time effects on QBER and key rates the experiment ran for 45 minutes, again in the mode where a fixed short key is sent: 1100 (see figure 4.8). To reduce the amount of generated data the receiver saves every five minutes all events within a time window of approximately 20 s to the hard drive.

First, the histograms are considered (see figure 4.8 (c)): The positions of the first and second peak maximum (see also section 3.4.4) of the received pulses stays ap-

Time [min:s]	**Peak 1** [ns]	**Peak 2** [ns]	**R.e.r.** [$10^3\,s^{-1}$]
0:0	4.52	7.08	575.6
5:2	4.52	7.08	573.6
9:45	4.52	7.08	600.0
19:53	4.58	7.08	702.9
24:54	4.58	7.08	721.5
29:51	4.58	7.08	716.6
34:48	4.58	7.08	712.1
39:56	4.52	7.08	696.5
44:20	4.58	7.08	693.3
Time [min:s]	**Si.k.r.** [$10^3\,s^{-1}$]	**Se.k.r.** [$10^3\,s^{-1}$]	**QBER** [%]
0:0	297.1	42.9	4.71
5:2	296.4	42.9	4.69
9:45	309.7	47.6	4.72
19:53	361.2	70.6	4.63
24:54	370.6	77.1	4.55
29:51	369.0	78.4	4.49
34:48	367.0	77.6	4.49
39:56	359.9	75.8	4.46
44:20	359.0	75.6	4.44

Table 4.3: Data for the long-time measurement. R.e.r.: raw event rate. Si.k.r.: sifted key rate. Se.k.r.: secret key rate.

proximately constant meaning that also in long-time operation it is not required to adjust the detection windows. Second, the average raw detection, sifted key and secret key rates and the average QBERs are considered: The key rates and QBER within a 20 s measurement always show similar standard deviations. The average QBER remains almost constant over the complete measurement time of 45 minutes. Thus, the trend of a raising key rate (see figures 4.8 (a) and (b)) in time is possibly only due to better coupling to the receiver which could have become better in time, as the micro-optical bench is only fixed with tape in the protective casing. Longer and more extensive measurements could further help to explain these long-time effects more accurately. However, the experiment shows an almost stable secret key rate over a measurement time of 45 minutes proving the operational capability for other long-range scenarios. The data for the long-time measurement can be found in table 4.3.

4.4.3 Tests with a handheld Sender

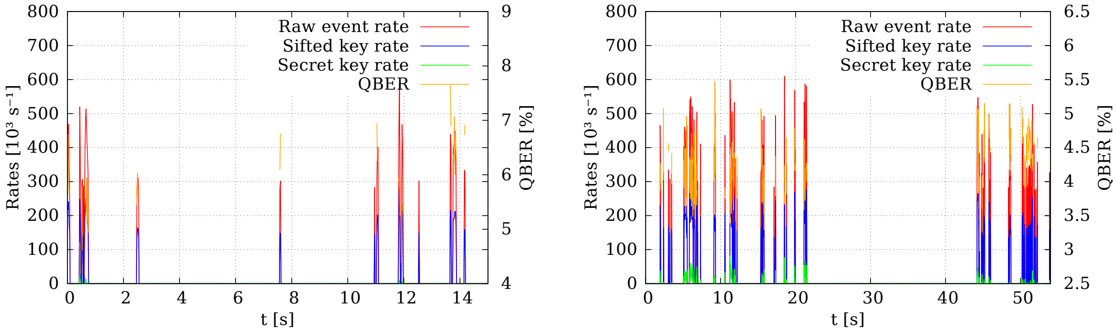
Finally also first tests with the handheld sender have been performed. These tests require additional filtering: In a handheld measurement there are typically time windows with no signal and thus these time windows have an average QBER of

#	**Time** [s]	**Raw events**	**Sifted bit**	**Secret bit**	**QBER** [%]
1	15	322694	157362	1662	5.90
2	21	745384	356953	93	6.27
3	54	1947938	949377	81948	4.24
4	22	1420124	659656	0	8.21
5	45	1341197	618807	0	7.62
6	20	639285	296666	0	7.77
7	44	1458579	676678	0	7.87
8	45	1101185	508320	241	7.49

Table 4.4: Data for the handheld measurements.

50 %. Hence from these time windows no secret key can be extracted. Another filter is applied by only taking time windows into account where the sifted key rate is above a threshold such that at least 10000 events are within this time window. For a time window of 66.7 ms this requires a sifted key rate of at least $150 \cdot 10^3\, s^{-1}$ that 10000 events or more are counted within this timing window. In that case the number of false events is small compared to the number of total events within that time window. In other words, the error on the QBER is low. It shall be mentioned that this threshold has been chosen arbitrarily. If this threshold is not exceeded all rates have been set to zero. One measurement took between 15 s and 54 s and the distance from the sender to the receiver (first pinhole) was approximately 30 cm.
The data for the handheld measurements can be found in table 4.4 (see also figures 4.9 and 8.6). In the best measurement (3) there have been 1947938 raw events measured. This results in 949377 sifted bit, of which 40254 bit were wrong, corresponding to a QBER $E = 4.24\,\%$. The extractable secret key length in this case is 81948 bit. This measurement took approximately 54 s resulting in a secret key rate of $1.5 \cdot 10^3\, s^{-1}$. Only after these handheld measurements it turned out that the active basis alignment did not work properly, that means the half wave plate corrected the polarisation only every $\approx 1\, s$. Although the device orientation sensor was still read out normally the sent data arrived only every $\approx 1\, s$ at the computer controlling the wave plate. Currently the most probable explanation is a large traffic congestion in the Wi-Fi network. As this problem occurred frequently during the final experiments some patch is required giving this data the highest priority in the traffic. Considering the data in table 4.4 it seems that the control did work normally until through measurement 3 as the QBER after this measurement increased significantly that in the following only in measurement 8 a secret key could be exchanged.
Apart from the active basis alignment and even better chosen detection windows there are a two further improvements which probably will increase the extractable secret key:

1. As described in section 3.4.3 there are still polarisation changing effects in the receiver which could be compensated for (see section 6.2). A reduction of these effects yields a lower QBER in general and thus the reduction of the key



(a) Measurement 1 after both filters.

(b) Measurement 3 after both filters.

Figure 4.9: Handheld measurements 1 and 3. For the exchanged raw, sifted and secret bit as well as the QBERs see table 4.4.

rate in the steps of error correction and privacy amplification could be smaller. Also for the tomography two additional mirrors (see figure 3.31) are used and thus the phase compensation takes these mirrors into account as well. With the relative efficiencies of the APDs (measured in section 4.2) and with an additional measurement of the coupling efficiencies and with the measurement of the exact splitting ratios of the beam splitters in the PAU (measured in [34]) one could make a tomography with the handheld module, as the PAU projects onto four polarisation states and the last component of the Stokes vector can be calculated (up to a ± sign). This is true as long as the degree of polarisation is close to one (which is a well-justified assumption). A requirement is that the active basis alignment works properly to achieve a high degree of polarisation.

2. The optimal mean photon number was calculated for the transmission with a fixed receiver. As the transmission in handheld experiments is much smaller one can calculate a better optimal mean photon number such that the amount of privacy amplification is minimised. The calculation can be performed analogously to the calculation in section 4.2 with the average transmission calculated from the handheld measurements. Note that for this calculation also the second filter should be applied, to get the best estimation of the transmission for the time windows of interest. A rough estimation is given in section 4.6.

Further experiments will show whether these improvements can indeed lead to higher secret key rates and are beyond the scope of this work.

Finally the coupling efficiency g in the handheld case can be calculated as well. To calculate this parameter both filters must be turned off as they reduce the number of detected raw events. To visualise the effects of both filters figure 4.10 shows the raw event rate of handheld measurement 3 with and without filtering. For the calculation of g also the average raw event rate without temporal filters has been calculated. The parameter g is then simply given by

$$g = \frac{R_{raw}^{handheld}}{R_{raw}^{fixed}} = \frac{133.2}{761.8} = 0.175 \tag{4.8}$$

which is approximately 55 % of the value found in [51] (here the average coupling efficiency was $g' = 0.316$, if other test persons are left out).

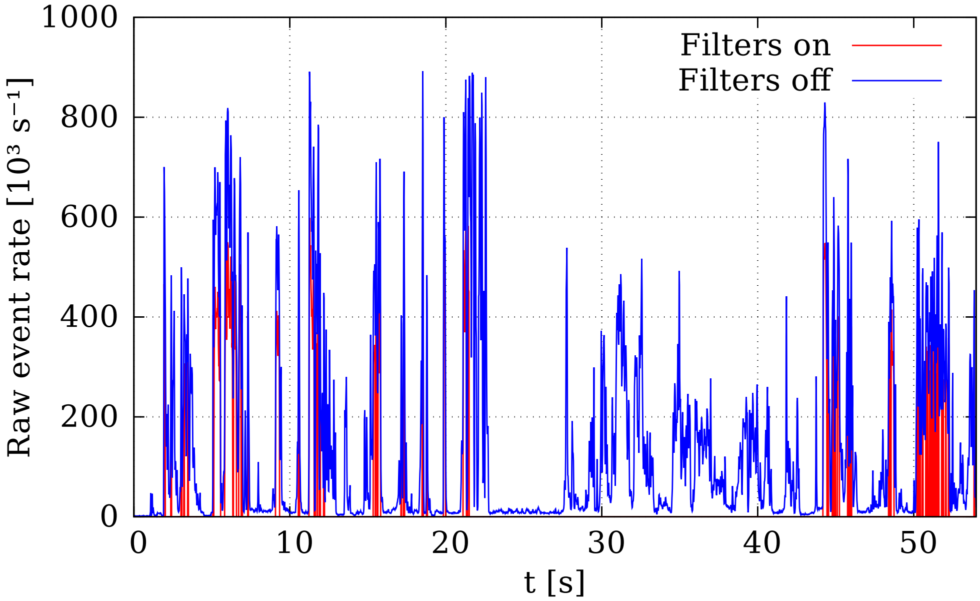


Figure 4.10: Comparison of the raw event rates in a handheld measurement with and without the filters (that means post-selection).

The difference can probably be explained by the fact, that the shortpass filter between the beacon laser and dichroic beam splitter distorts the beam profile of the beacon laser. Thus the beam is not perfectly collimated anymore and therefore the focused spot on the quadrant diode is now larger than initially. As the intensity differences in this larger spot are in this case smaller, the control does not work as good as originally. However, one can compensate for this by adjusting the parameters for the PI-control.
One can also calculate the average coupling efficiency only for the time windows of interest, namely those time windows when the sifted key rate exceeds the required threshold. For a particular measurement (see figure 4.10) the coupling efficiency is then $g = 0.701$, but the considered time windows only accounted for 8.20 % of all time windows.

It shall be mentioned that each data point in the figures with the rates and QBER corresponds to an average value over 66.7 ms. Consequently each measurement point has a distance of 66.7 ms to the next data point. Especially for the handheld measurements this is not always a good choice, as the intensities are fluctuating in these measurements very much. Strongly fluctuating links are studied in [59]. Here also a method is developed how one has to choose SNR thresholds in lossy and noisy channels and how the secret key can be extracted in such a case. Unfortunately this paper was only recognised after writing this thesis and thus the results of the paper are not included.

4.5 Experiments with random Keys

For a real QKD experiment it is not sufficient to send only the four states but also to send them in a complete random pattern. As already described in section 3.3.7, one can fill the FPGA with 131056 random numbers which are sent periodically. The synchronisation and sifting takes place as described in section 3.4.1 or alternatively by simply trying all 131056 possible delays (and thus without complex synchronisation). Currently there only have been experiments with a fixed receiver and random keys as the handheld experiments with short keys already indicated that further improvements are required. The exchanged key is saved to the hard drive (and not shown here as it would exceed 36 pages to display the key). In the measurement there have been 9820147 raw events detected. This results in 5073729 sifted bit, of which 238142 bit were wrong, corresponding to a QBER $E = 4.69\,\%$ (see figure 4.11). The extractable secret key length in this case is 734238 bit. Together with a key exchange time of $17.21\,s$ this corresponds to an average raw event rate of $570.6 \cdot 10^3\,s^{-1}$, a sifted key rate of $294.8 \cdot 10^3\,s^{-1}$ and a secret key rate of

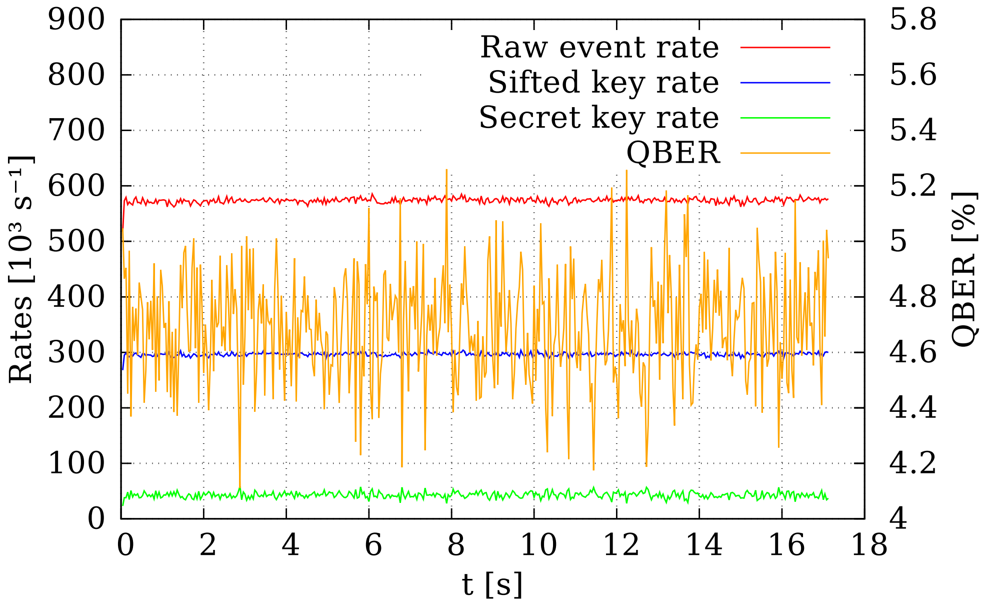


Figure 4.11: Key rates for tests with a fixed receiver and a random key: Raw (red), sifted (blue) and secret (green). Additionally shown is the QBER (orange).

$42.7 \cdot 10^3\,s^{-1}$. As expected the values for the key rates and QBERs are within the range of the long-time measurement (which was with short keys). The next steps must include a software patch that the random key can be longer than $131056\,bit$. For example it is thinkable that the key is loaded in blocks of $131056\,bit$. This pattern is sent in $1.31\,ms$ and in this time one can reload a new block of $131056\,bit$ through the USB connection which is capable of the required data rates. However, the SecureRandom class is, in the current implementation, not capable of generating secure random numbers at a speed of $10^8\,s^{-1}$. Slight modifications can increase the performance. As already mentioned the USB connection is capable of these data rates, but currently too much data is sent with every command to the FPGA which must be reduced to increase the speed of the reloading of the key. With these modifications it is expected that also arbitrarily long keys can be exchanged which must be tested in future work.

4.6 Achievable Key Rate

There have been some suggestions for improvements in the previous sections. This raises the question which achievable secret key rate is possible with the current setup. Section 4.3 already calculates the achievable secret key rate for static operation to be maximally $319.8 \cdot 10^3\,s^{-1}$. In this section the achievable secret key rate for the handheld case shall also be calculated. Not included in this estimation is an algorithm capable of finding the best detection window as in the calculation for the static case. The results in section 4.4.3 suggest that a QBER of 4.24 % in the handheld measurements is possible. The question whether this can be improved with the active basis alignment stays open, but it is expected that this QBER at least cannot be enhanced much. To reach in a handheld measurement such a QBER the basis alignment must have worked well. To estimate the transmission one cannot simply use

$$\tau_{handheld} = g\tau_{static} \tag{4.9}$$

with g being the coupling efficiency from section 4.4.3 as this is only an average coupling efficiency. After both temporal filters the coupling efficiency within the filtered time windows will be higher and these are the only time windows of interest. The transmission for the handheld case is thus calculated from these time windows. The average raw event rate only for the time windows of interest is $370.1 \cdot 10^3\,s^{-1}$, but these time windows account only for 8.20 % of all time windows. Thus the optimal mean photon number is $\mu^{opt} = 0.034$ and the maximally achievable secret key rate is $32.9 \cdot 10^3\,s^{-1} \times 0.082 = 2.70 \cdot 10^3\,s^{-1}$. One can derive this new optimal mean photon number analogously to the derivation in section 4.2.

However, tests must confirm whether such a key rate can be reached in practice. In any case the PI control must be re-adjusted such that the coupling efficiency reaches its initial value (see section 4.4.3). Thus the sifted key rate could be almost doubled.

5 Further Analysis

5.1 Finite Key Effects

So far the security proof[41] in which the secret key rate is calculated (see also section 2.3.4) only considered infinitely long keys. In this case the observed (estimated) error in the key is exactly the same as the real error. However, in a practical scenario, where the exchanged key has only a finite length and the error is estimated via a finite subset of the key, the assumption that the observed and real error is equal can be wrong, that means the real error could be smaller or larger than the observed error. The latter case is crucial for the security as in this case the suspected leakage of information to a potential eavesdropper is underestimated. This is called **finite key effects**. It shall be mentioned that in the first case the amount of privacy amplification is simply higher than required which is not a problem for the security.

As most QKD experiments are with fixed sender and receiver the exchanged keys are typically long and thus finite key effects become negligible. However, with moving receivers the maximal key exchange time is usually limited (especially in a handheld scenario) and hence it is interesting how the secret key rate evolves if finite key effects are taken into account. Most security proofs[60][61] for finite key effects assume an implementation of the decoy state protocol so that these proofs cannot easily be adapted for this work. However, a recent study[62] allows to calculate finite key effects for any prepare-and-measurement protocol like BB84. More generally fluctuating intensities lead to a further reduction in the secret key rate[63], but as this security proof for finite key effects assumes the implementation of the decoy state protocol as well intensity fluctuations in the finite key regime cannot directly be studied for this experiment. This last case would be very interesting for handheld scenarios (and also for any other moving transmitter or receiver) as these implementations typically have large intensity fluctuations as well as small key exchange times.

This chapter reviews the security proof in [62] and extends it further also to photon tagging. A QKD protocol is called **correct** if for any attack strategy Alice's key S_A equals Bob's key S_B and called ϵ_{cor}-correct if it is ϵ_{cor}-indistinguishable from a correct protocol, that means $P(S_A \neq S_B) \leq \epsilon_{cor}$.

A QKD protocol is called **secret** if for any attack strategy the parameter Δ' equals zero and called ϵ_{sec}-secret if it is ϵ_{sec}-indistinguishable from a secret protocol, that means

$$(1 - p_a)\Delta' \leq \epsilon_{sec} \tag{5.1}$$

where p_a is the probability that the protocol aborts and the parameter Δ' is given by

$$\frac{1}{2}|\rho_{SE} - \omega_S \otimes \rho_E|_1 \leq \Delta' \tag{5.2}$$

with ρ_{SE} being the quantum state that describes the correlation of Alice's key S_A and the eavesdropper E, ω_S being the fully mixed state on S_A and ρ_E denotes the state of system E. In other words Eve's knowledge about the key is small.
With these two definitions of correctness and secrecy one can define a QKD protocol to be **secure** if it is correct and secret and ϵ-secure if it is ϵ_{cor}-correct and ϵ_{sec}-secret and

$$\epsilon_{cor} + \epsilon_{sec} \leq \epsilon \tag{5.3}$$

For the BB84 protocol with a single photon source in the finite key regime to be ϵ-secure the secret key rate ([62], equation (2), here shown with the same symbols as in the original publication) is given by

$$R^f \geq n\left(q - h\left(E + \mu\right)\right) - f(E)h(E) - \log_2\left(\frac{2}{\epsilon_{sec}^2 \epsilon_{cor}}\right) \tag{5.4}$$

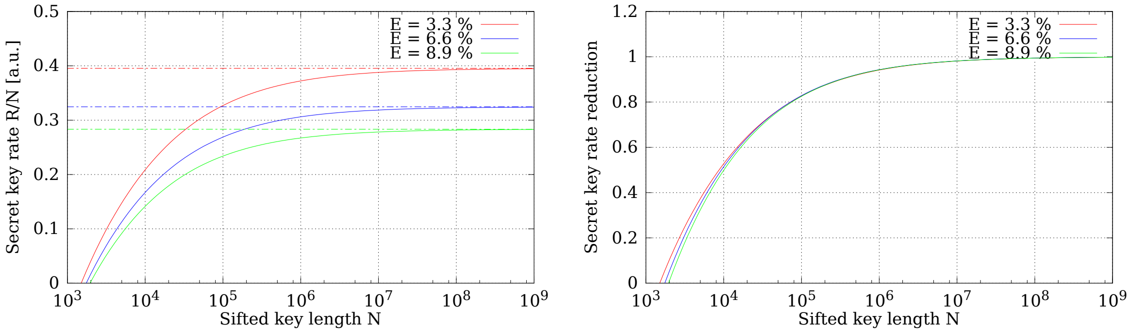
where

$$\mu = \sqrt{\frac{n+k}{nk}\frac{k+1}{k}\log\left(\frac{4}{\epsilon_{sec}}\right)} \tag{5.5}$$

with n, k the number of sifted events in the Z, X basis respectively, $h(x)$ the binary Shannon entropy (as defined in equation 2.27), E the QBER and $f(E)$ the error correction efficiency. The preparation quality q is defined as

$$q = -\log_2 \max|\langle\Psi_x \mid \Psi_z\rangle|^2 \tag{5.6}$$

with $|\Psi_x\rangle$ and $|\Psi_z\rangle$ being the states prepared in the X and Z basis respectively. For a symmetric basis encoding on Alice's side (and thus a symmetric basis choice on Bob's side) $n = k$. In a perfect scenario $q = 1$. To compare the results so far with the results in [62] the protocol is chosen to be ϵ-secure with $\epsilon = 10^{-10}$. Note that this boundary has been chosen in [62] absolute arbitrarily. The secret key rate $R/N = R/(n+k)$ for three in this experiment relevant exemplary QBERs is shown in figure 5.1 (a). As can be seen the secret key rate per N converges in the limit for very large N proving that the finite key effects become negligible in this limit. At $N = 312000$ the reduction of the secret key due to finite key effects reaches 10 %,



(a) Secret key rate as a function of the sifted key length for various QBERs E for a single photon sources and perfect state preparation. The limit $N \to \infty$ is shown as a dashed line.

(b) Secret key reduction due to finite key effects as a function of the sifted key length for various QBERs E for a single photon sources and perfect state preparation.

Figure 5.1: Finite key effects in an ideal scenario.

meaning that for such a key length the key must be shortened by 10 % which is approximately true for all considered QBERs (see figure 5.1 (b)).
However, the calculation above is only valid for a single photons source and perfect state preparation. Both these requirements are not met in the experiment so in the following these deviations shall be taken into account. First the preparation quality shall be calculated. For this the output states of the transmitter (see table 3.12) must be converted to Jones vectors using equations 2.72 - 2.74. The conversion (with the phase in units of *rad*) gives

$$|\Psi_x^1\rangle = |P\rangle = \begin{pmatrix} 0.626 \\ 0.780\, e^{0.376i} \end{pmatrix} \tag{5.7}$$

$$|\Psi_x^2\rangle = |M\rangle = \begin{pmatrix} 0.529 \\ 0.849\, e^{1.472i} \end{pmatrix} \tag{5.8}$$

$$|\Psi_z^1\rangle = |H\rangle = \begin{pmatrix} 0.993 \\ 0.114\, e^{-1.475i} \end{pmatrix} \tag{5.9}$$

$$|\Psi_z^2\rangle = |V\rangle = \begin{pmatrix} 0.166 \\ 0.986\, e^{-0.512i} \end{pmatrix} \tag{5.10}$$

and thus the relevant projections are

$$|\left\langle \Psi_x^1 \middle| \Psi_z^1 \right\rangle|^2 = 0.363 \tag{5.11}$$

$$|\left\langle \Psi_x^1 \middle| \Psi_z^2 \right\rangle|^2 = 0.703 \tag{5.12}$$

$$|\left\langle \Psi_x^2 \middle| \Psi_z^1 \right\rangle|^2 = 0.186 \tag{5.13}$$

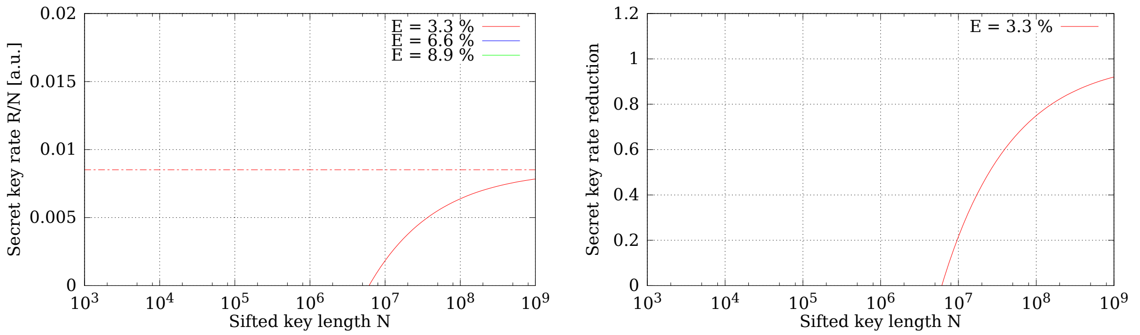
$$|\left\langle \Psi_x^2 \middle| \Psi_z^2 \right\rangle|^2 = 0.649 \tag{5.14}$$

Plugging these projections into equation 5.6 yields $q = 0.508$.

In the next step a weak coherent laser is assumed instead of a single photon source. Equation 5.4 in that case has to be modified to

$$R^f \geq n\left(q - \Delta - (1-\Delta)h\left(\frac{E+\mu}{1-\Delta}\right)\right) - f(E)h(E) - \log_2\left(\frac{2}{\epsilon_{sec}^2\epsilon_{cor}}\right) \qquad (5.15)$$

with Δ being defined as in equation 2.33. Note that without a proof this is not necessarily a tight bound, but at least a lower bound on the secret key rate. The secret key rate R/N for this realistic scenario is shown in 5.2. Only for a QBER of 3.3 % a secret key can be exchanged. The limit at which the secret key must be shortened by less than 10 % is only reached after a sifted key length of approximately 10^9. To classify the results the corresponding key exchange times are calculated at which this reduction is reached and summarised in table 5.1. Note that this exchange time corresponds to the time at which finite key effects become small. For the practical application it does not matter if this reduction is large as long as enough total secret bits have been exchanged, which is typically in a handheld scenario much smaller than 10^9 *bit*. For a comparison, a credit card number is not longer than 64 *bit* (dependent on the issuing network).



(a) Secret key rate as a function of the sifted key length for various QBERs E for a source as used in the experiment. The limit $N \to \infty$ is shown as a dashed line.

(b) Secret key reduction due to finite key effects as a function of the sifted key length for various QBERs E for a the source as used in the experiment.

Figure 5.2: Finite key effects in a realistic scenario.

scenario	key exchange time	exchanged bits
ideal st.	0.89 *s*	280800
ideal hh.	3.81 *s*	280800
realistic st.	793 *h*	$0.9 \cdot 10^8$
realistic hh.	3392 *h*	$0.9 \cdot 10^8$

Table 5.1: Key exchange times for the ideal static (st.) and handheld (hh.) case as well as the realistic scenarios in all cases for a QBER of 3.3 %.

5.2 The SARG04 protocol

So far only the implementation of the BB84 protocol with weak laser pulses as a photon source has been considered. For such a source the number of photons in a pulse is Poisson-distributed. The Photon Number Splitting attack or memory attack (see section 2.3.2) requires a mean photon number $\mu \ll 1$ (for only BB84). However, even if this condition is fulfilled, the probability for a multi photon pulse is non-zero resulting in a higher amount of privacy amplification during the classical post-processing as one can only generate a secret bit from a single photon pulse (see section 2.3.4). An expedient to use higher mean photon number was the decoy state protocol (see section 2.3.2) which is widely implemented in most experiments. Another solution is the SARG04 protocol[64][65] based on the BB84 protocol and specially developed to defeat PNS attacks. In implementations with weak coherent pulses SARG04 can thus yield higher secret key rates than BB84[65].
The SARG04 protocol is exactly the same at the level of quantum processing as the BB84 protocol, it differs only in the classical post-processing making it perfectly feasible to evaluate the experiment so far with the same data for SARG04. Alice starts with randomly sending one out of the four possible states as is the BB84 protocol. The classical bit values are now encoded in the basis choice, for example $|z+\rangle = |0\rangle$ and $|z-\rangle = |1\rangle$ correspond to logical bit 0 and $|x+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ and $|x-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ correspond to logical bit 1. After the quantum communication steps Alice reveals the state she sent together with one state from the conjugated basis, but she does not tell which state the sent state was. Thus Alice and Bob have *a priori* four different sifting sets:

$$s_1 = (|z+\rangle\,|x+\rangle) \tag{5.16}$$

$$s_2 = (|z+\rangle\,|x-\rangle) \tag{5.17}$$

$$s_3 = (|z-\rangle\,|x+\rangle) \tag{5.18}$$

$$s_4 = (|z-\rangle\,|x-\rangle) \tag{5.19}$$

Only if Bob's result is orthogonal to the result of one of the two disclosed states he knows with certainty that the sent state must have been the other disclosed state and thus he learns Alice's basis choice and consequently the bit value. It shall be mentioned that the sifting sets s_1 and s_4 or s_2 and s_3 are already sufficient which would be a better version of SARG04 as less classical communication ($1\,bit$ instead of $2\,bit$) is required for the announcement of the sifting set. For clarification assume Alice sent $|z+\rangle$ and she reveals s_2. A case differentiation (in the absence of errors) gives:

1. With probability $\frac{1}{2}$ Bob measures in the Z basis. Thus he measures $|z+\rangle$ which is consistent with both disclosed states, this measurement result would be possible if Alice had sent $|x-\rangle$ as well.

2. With probability $\frac{1}{4}$ Bob measures in the X basis and got $|x-\rangle$ as a result which

is also consistent with both states.

3. With probability $\frac{1}{4}$ Bob measures in the X basis and got $|x+\rangle$ as a result. Thus he knows that the sent state could not have been $|x-\rangle$ meaning that the sent state has been $|z+\rangle$.

Bob confirms whenever he measured a result which is not conclusive with both states and these events will be kept on both sides as sifted events. Note that for SARG04 the length of the sifted key is $\frac{1}{4}$ of the raw event length in contrast to BB84 where with a symmetric basis choice the length of the sifted key is $\frac{1}{2}$ of the raw event length. It shall be mentioned that in the presence of errors the sifted key length in SARG04 can increase.

The strength of SARG04 is that it protects secrecy also in two photon states. Suppose Eve kept a photon from a two photon pulse in an optical quantum memory. In BB84 by eavesdropping the classical channel Eve learns the basis and thus can measure the stored photon and learns therefore the bit value with probability 1. However, in SARG04 Eve learns only that the state is one of two non-orthogonal states. She can never distinguish these two states with certainty (however she can distinguish both cases with probability $\frac{1}{4}$). Eve can further attack three photon pulses (of which she keeps two photons) and measure both photons in the Z and X basis respectively. Then she has a success probability of $\frac{1}{2}$ that the measurement result of the measurement in the "wrong" basis contradicts one of the disclosed states. This suggests that SARG04 could be more robust against PNS attacks as BB84 if implemented with a weak laser source.

A comparison[66] of the secret key rates between BB84 and SARG04 gives

$$R_{secret}^{BB84} \geq -Q_\mu f(E_\mu) h(E_\mu) + Q_1(1 - h(e_1)) \tag{5.20}$$

$$R_{secret}^{SARG04} \geq -Q_\mu f(E_\mu) h(E_\mu) + Q_1 S_1(e_1) + Q_2 S_2(e_2) \tag{5.21}$$

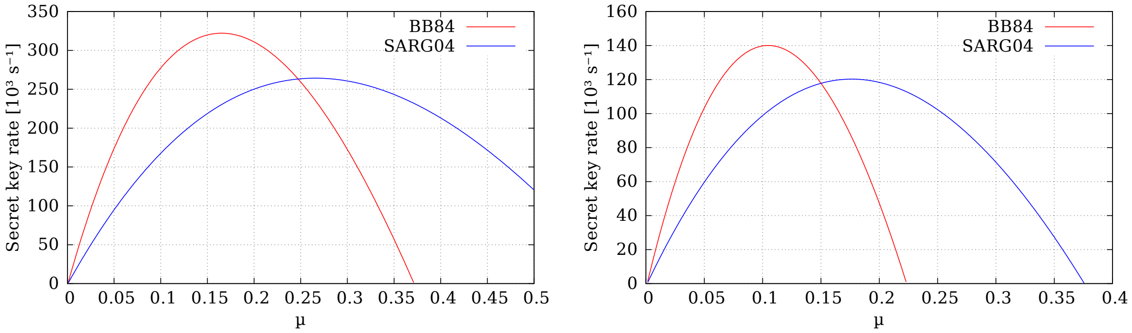
with Q_n and Q_μ the gain as defined in equations 2.21 and 2.22 respectively. The error of the single and two photon states e_1 and e_2 respectively are constrained by the overall QBER E_μ by

$$Q_1 e_1 \leq Q_\mu E_\mu \tag{5.22}$$

$$Q_1 e_1 + Q_2 e_2 \leq Q_\mu E_\mu \tag{5.23}$$

and $S_n(e_n)$ being Eve's uncertainty on the n photon pulse. In appendix D of reference [66] it is described how to compute these uncertainties. To compare both protocols the secret key rate as a function of μ is computed for fixed QBERs $E_\mu = 3.96\,\%$ and $E_\mu = 5.56\,\%$, the in section 4.3 proven to be possible QBERs for static operation. The error correction efficiency is assumed to be $f(E_\mu) = 1.22$ and transmission $\eta\tau_{tot} = 0.093$.

The results in figure 5.3 show that the BB84 protocol (even without decoy states) yields for both QBERs a 21.9 % and 16.4 %, respectively, higher maximal secret key rate than the SARG04 protocol meaning that for the transmission and QBERs



(a) Secret key rate as a function of μ for the BB84 protocol and the SARG04 protocol at $E_\mu = 3.96\,\%$ and $\eta\tau_{tot} = 0.093$.

(b) Secret key rate as a function of μ for the BB84 protocol and the SARG04 protocol at $E_\mu = 5.56\,\%$ and $\eta\tau_{tot} = 0.093$.

Figure 5.3: Comparison of the BB84 and SARG04 protocol for different QBERs.

relevant in this experiment the BB84 protocol is the better option. Likewise previous theoretical calculations[66] as well as experimental results[67] confirmed the superiority of BB84 over SARG04 at already moderate QBERs. In contrast further calculations[66] showed that SARG04 performs better at higher mean photon numbers as expected, as it partially defeats the PNS attack which is also true, when evaluating the key rates for the parameters of this experiment.

6 Improvements and next Steps

Although the experiment is already quite advanced there is still room for improvement, on the sender side as well as on the receiver side. Especially the classical communication is not implemented in the current experiment which would allow live-sifting, error correction and privacy amplification.

6.1 Improvements for the Sender

As already mentioned in section 3.2.1 the spectrum of the VCSELs does not overlap opening a spectral side channel allowing it to distinguish between the polarisation states without introducing any errors to the key. As already mentioned in principle this could be overcome by individual thermal tuning of the spectrum exploiting the thermal shift of the VCSELs ($\Delta\lambda = 0.06\,nm \cdot K^{-1}$) or by using MEMS-tunable VCSELs (exploiting a micro-electro-mechanical effect for tuning the cavity length and thus the wavelength). The latter is the more convenient option as the temperature gradient would have to be $11.8\,K \cdot (250\,\mu m)^{-1}$ which would be hard to achieve, even if one uses wires through which a current is driven for heating. However, there is no array of MEMS-tunable single-mode VCSELs at $850\,nm$ without packaging commercially available, but companies might be able to fabricate those upon request. MEMS-tunable VCSELs are capable of shifting the wavelength the required $0.71\,nm$.

The most easiest improvement for a revised version of the sender unit is a correct characterisation and verification of the waveguide birefringence to reduce the source-intrinsic QBER. In any case the calculated results should be experimentally verified. In principle a complete retrieval of the Mueller matrix is not necessary: If a waveguide is for example supposed to transmit the state $|H\rangle$ then one can project on $|H\rangle$ after the waveguide with a polariser and rotate the input polarisation such that the projection reaches a maximum. A complete tomography of such states should be done nevertheless to determine the phase between $|H\rangle$ and $|V\rangle$, which should be approximately equal for all four waveguides and thus can be compensated.

Some room for improvement is also at the design of the electronics. Currently the electronics consume $48\,W$ ($12\,V$ at $4\,A$) plus $2\,W$ from the cooler fans which is of course too much to support the module through a pure USB connection (USB 3.1 supply enough power). For a comparison: Eight AAA batteries have typically energies of $14.4\,Wh$ which allows $20\,min$ of operation (in this case another voltage controller is required and thus the estimation might change). Alternatively an accumulator of a modern smart phone has typically a capacity of 2000 mAh which would allow 4 min of operation. Of course the chips itself do not require that much power, with a better design the power consumption could be reduced resulting in less heat production and thus the coolers might not be required anymore making the device smaller.

As mentioned in section 3.3.5 there is a ND-filter (ND = 1.09 at 850 nm) between the VCSELs and the polarisers to prevent back-coupling into the VCSELs (the polarisers work totally in reflection), because the VCSELs are sensitive to optical feedback. Zemax simulations showed that this back-coupling is negligible (as the light will not be focused onto the VCSELs). By removing this filter in a revised version it is possible to gain a factor of $10^{1.09} = 12.3$ in the mean photon number. This would only be required if the decoy state protocol is implemented as this allows (dependent on the QBER) higher mean photon numbers. The decoy state protocol should be implemented in any case in a revised version.

6.2 Improvements for the Receiver

The results in section 3.4.3 still indicate that the receiver itself has partially polarising effects, meaning that the receiver has different transmission amplitudes t'_s and t'_p for S- and P-polarisation. Of course this increases the QBER and cannot be compensated with a unitary transformation (see section 3.4.3). Those effects can be compensated by introducing other partially polarising elements with exchanged amplitudes for S- and P-polarisation ($t_p = t'_s$ and $t_s = t'_p$). This is always accompanied with losses so the final secret key rate is the figure of merit to be optimised. The Mueller matrix which describes partially polarising optical components reads

$$M\left(p_H, p_V\right) = \frac{1}{2}\begin{pmatrix} p_H^2 + p_V^2 & p_H^2 - p_V^2 & 0 & 0 \\ p_H^2 - p_V^2 & p_H^2 + p_V^2 & 0 & 0 \\ 0 & 0 & 2p_H p_V & 0 \\ 0 & 0 & 0 & 2p_H p_V \end{pmatrix} \tag{6.1}$$

with $0 \leq p_H, p_V \leq 1$ being the transmission factors through the receiver for the H- and V-component of the electric field. An optical component with exchanged transmission amplitudes can be for example a tilted glass plate. According to the Fresnel equations the transmission and reflection coefficients for S- and P-polarised light at the air-glass interface (figure 6.1) are given by

$$t_s = \frac{2n_1 \cos\left(\alpha\right)}{n_1 \cos\left(\alpha\right) + n_2 \cos\left(\beta\right)} \tag{6.2}$$

$$t_p = \frac{2n_1 \cos\left(\alpha\right)}{n_2 \cos\left(\alpha\right) + n_1 \cos\left(\beta\right)} \tag{6.3}$$

$$r_s = \frac{n_1 \cos(\alpha) - n_2 \cos(\beta)}{n_1 \cos(\alpha) + n_2 \cos(\beta)} \tag{6.4}$$

$$r_p = \frac{n_2 \cos(\alpha) - n_1 \cos(\beta)}{n_2 \cos(\alpha) + n_1 \cos(\beta)} \tag{6.5}$$

With Snell's law one can eliminate the angle β:

$$n_1 \sin(\alpha) = n_2 \sin(\beta) \Rightarrow \cos(\beta) = \frac{\sqrt{n_2^2 - n_1^2 \sin^2(\alpha)}}{n_2} \tag{6.6}$$

that the Fresnel equations modify to (refractive index for air $n_1 \approx 1$):

$$t_s = \frac{2\cos(\alpha)}{\cos(\alpha) + \sqrt{n_2^2 - \sin^2(\alpha)}} \tag{6.7}$$

$$t_p = \frac{2\cos(\alpha)}{n_2 \cos(\alpha) + \frac{\sqrt{n_2^2 - \sin^2(\alpha)}}{n_2}} \tag{6.8}$$

$$r_s = \frac{\cos(\alpha) - \sqrt{n_2^2 - \sin^2(\alpha)}}{\cos(\alpha) + \sqrt{n_2^2 - \sin^2(\alpha)}} \tag{6.9}$$

$$r_p = \frac{n_2 \cos(\alpha) - \frac{\sqrt{n_2^2 - \sin^2(\alpha)}}{n_2}}{n_2 \cos(\alpha) + \frac{\sqrt{n_2^2 - \sin^2(\alpha)}}{n_2}} \tag{6.10}$$

The overall transmission coefficient is the product of the transmission coefficients at both transitions (air-glass and glass-air), neglecting multiple reflections (ghosting).

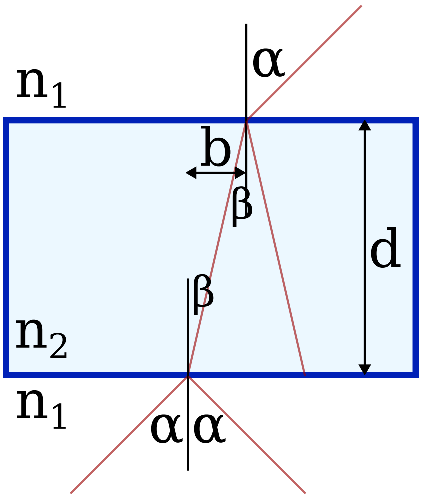


Figure 6.1: Definition of the coordinate system (plane of incidence) for the Fresnel equations above.

The total transmission for S- and P-polarisation at both interfaces is given by

$$t_s' = \frac{4n_2\cos(\alpha)\cos(\beta)}{(\cos(\alpha)+n_2\cos(\beta))^2} = \frac{4\cos(\alpha)\sqrt{n_2^2-\sin^2(\alpha)}}{\left(\cos(\alpha)+\sqrt{n_2^2-\sin^2(\alpha)}\right)^2} \tag{6.11}$$

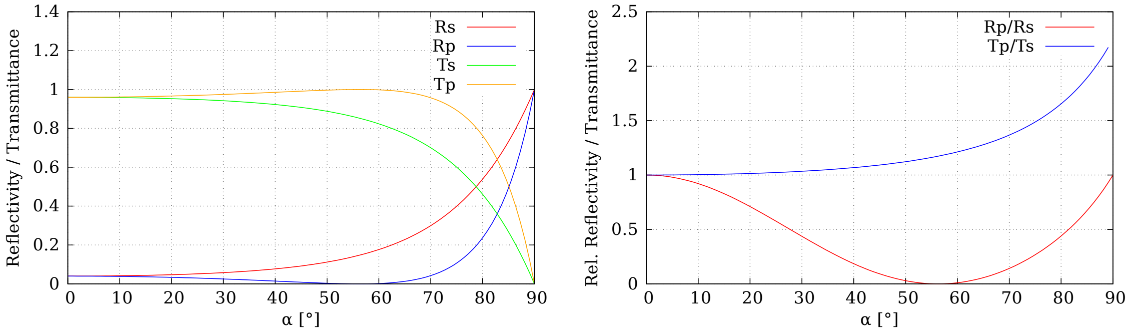
$$t_p' = \frac{4n_2\cos(\alpha)\cos(\beta)}{(n_2\cos(\alpha)+\cos(\beta))^2} = \frac{4\cos(\alpha)\sqrt{n_2^2-\sin^2(\alpha)}}{\left(n_2\cos(\alpha)+\frac{\sqrt{n_2^2-\sin^2(\alpha)}}{n_2}\right)^2} \tag{6.12}$$

With an additional anti-reflecting coating at the glass-air interface the transmission and reflection coefficients are simply given by equations 6.7 - 6.10 and ghosting is prevented. The degree of transmission or reflection is given by

$$T_i = \frac{\tan(\alpha)}{\tan(\beta)}t_i^2 \tag{6.13}$$

$$R_i = r_i^2 \tag{6.14}$$

for $i = s, p$ (see figure 6.2 (a)). Note that without absorption $R_i + T_i = 1$ holds.



(a) Reflectivity and transmittance for S- and P-polarisation at the air-glass transition with $n_{glass} = 1.5$.

(b) Relative reflectivity and transmittance for S- and P-polarisation at the air-glass transition with $n_{glass} = 1.5$.

Figure 6.2: Possibilities for different reflection and transmission coefficients at the air-glass transition.

Of course only the relative reflectivity and transmittance is important (figure 6.2 (b)). Depending on whether one needs a higher amplitude for S- or P-polarisation one can also rotate the glass plate by 90° around the beam propagation axis and thus change S- and P-polarisation. The parameters p_H and p_V for the Mueller matrix must be measured in an experiment and then one can calculate the achievable secret key rate.

7 Summary

In this work the feasibility for mobile free space Quantum Key Distribution for short distance secure communication has been explored. For this purpose a sender unit has been miniaturised. The mobile micro-optics based device, implementing the BB84 protocol, has an additional beacon laser which allows efficient beam tracking and controlling as well as clock synchronisation on the receiver's side. First key exchanges already have been performed in a proof-of-principle demonstration showing the potential of QKD on short distances.
The transmitter uses an array of four single-mode VCSELs at an operating wavelength of $850\,nm$. Operated in pulsed mode these VCSELs show a very low degree of polarisation. For a pulse length of $46\,ps$ the light is almost unpolarised. The pulse shape is tuned such that the temporal shape of the four VCSELs is indistinguishable. However, those VCSELs have small spectral discrepancies of $0.71\,nm$ opening side channels. This problem can be overcome by using MEMS-tunable VCSELs. The light is then focused with an microlens array through an array of polarisers, fabricated using focused ion beam milling. Thus the four polarisation states for the BB84 protocol can be set. Next the four laser beams are combined in a femto-second laser-written waveguide to one main beam. This spatially filters the light making it impossible to determine from which laser the pulse has been emitted. Finally the infrared laser is overlapped with a red beacon laser allowing a user to aim with the device. The beacon laser is modulated with $100\,MHz$ allowing to synchronise the receiver's clock with the clock of the sender by registering the power fluctuations of the visible laser with a fast photodiode in the receiver. The beacon laser can further be guided to an angle-resolving detector which allows tracking of the incident beam and controlling an electronically-driven mirror such that the incident angle at the polarisation analysis is always close to zero. In this case one can couple much light from a handheld device to fibre-coupled APDs. Further a spatial filter in the receiver prevents spatial mode side channels on this side. An Android App reading the device orientation sensor of a modern smart phone classically communicates with the receiver's computer via Wi-Fi which in turn can control a motorised wave plate compensating for rotated reference frames making the experiment fully reference-frame independent.

In the beginning of this work the theory behind cryptography and quantum cryptography is explained. The today commonly used public-key encryptions will be insecure in the presence of a quantum computer. Thus a quantum-safe key exchange method is required in the future. One possibility is Quantum Key Distribution which security relies only on physical laws and not on assumptions on the skills of an eavesdropper. Hence QKD is secure also in the future. Next, the secret key rate for a realistic scenario is calculated for two different protocols: The BB84 protocol and the 3-State protocol. Under equal conditions the BB84 performs better, but under certain circumstances (for example with a lower QBER) the 3-State protocol can be the better option.

Then the characterisation of some components for the sender unit is described, together with the assembly and characterisation of the device. Among the components is a dichroic beam splitter taken from an optical pick-up system of a DVD drive, which has excellent properties for the beam combination in the transmitter. The red beacon laser is also characterised, yet it turned out that it emits also in the near infra-red such that an additional shortpass filter between the beacon laser and the beam splitter becomes necessary. After the assembly the module has been characterised and showed large deviations from theoretical predictions. The reason for this could never been completely resolved. However, a unitary transformation could compensate most of these effects. On the receiver's side, as already mentioned, an active basis alignment system and a clock synchronisation has been developed. The receiver showed initially strong polarising effects which was mostly traced back to polarisation changes at a dichroic beam splitter which was used to split the red from the infra-red light in the receiver.

After that first experimental tests could be performed: Under lab conditions the receiver shows a negligible dark count rate while "daylight-like" conditions indicate, that there is some need for improvement if the experiment shall be operated outside, for example in a practical application like the authentication of a device to an ATM. After a calculation of the optimal mean photon number some real key exchange runs with short fixed patterns and long random keys have been performed: First tests with a static sender showed a secret key rate of $> 350 \cdot 10^3\,s^{-1}$ at a QBER of 6.65 % which leads to a secret key rate of $> 40 \cdot 10^3\,s^{-1}$. A long-time measurement over 45 minutes demonstrated stable QBERs and nearly stable secret key rates. Unfortunately the first handheld tests had too high QBERs which allowed only a secret key exchange in a few measurements. However, after a re-evaluation of the experimental data, that means using a smaller detection window which leads to smaller QBERs, an average of $1.5 \cdot 10^3\,s^{-1}$ for a handheld test has been reached, and for the static experiments the highest (average) secret key rate recorded was $113.5 \cdot 10^3\,s^{-1}$ at a QBER of 3.27 %. The parameters for such a setting have not been optimal, further experiments will surely be able to increase the secret key rate, in the static case as well as in the handheld experiments. Calculations showed that secret key rates of $319.8 \cdot 10^3\,s^{-1}$ and $2.70 \cdot 10^3\,s^{-1}$ respectively are possible.

A further analysis takes also finite key effects into account. These theoretical calculations show that under realistic conditions at least $5 \cdot 10^6$ sifted events are required to get a non-zero secret key. The experiment can also be evaluated for the SARG04 protocol, because at the level of quantum processing it is exactly the same as the BB84 protocol, only the classical post-processing is differently. For weak coherent laser pulses the SARG04 can have higher secret key rates as the BB84 protocol as it defeats the PNS attack. However, theoretical calculations showed that for parameters (transmission and QBER) relevant in this experiment the secret key rate of SARG04 compares worse against BB84, as for SARG04 a secret key rate of $264.3 \cdot 10^3\, s^{-1}$ is possible. In contrast BB84 is capable of a secret key rate of $322.1 \cdot 10^3\, s^{-1}$ at equal conditions.

Due to the results so far also some possible improvements and next steps for a revised version of the experiment are proposed. The improvements include MEMS-tunable VCSELs for closing the spectral side channel and a better electronics circuit on the sender's side and the compensation of polarising effects on the receiver's side (if this is still necessary). One could think even further about using stability sensors as used in modern cameras to further stabilise the link efficiency. As these sensors are also used in modern smart phones they are available on the micro-optics scale.

Summarising the progress achieved so far future mobile QKD is possible. QKD can enable secure short distance communication and it is believed that this opens new commercial possibilities although there is still need for more extensive research and development. However, exchanging banking information with an ATM is only one of many feasible applications. One could also think of a quantum network interface for a worldwide quantum internet or, if the outcoupling optics are changed and hence the operating distance is extended to a few kilometres, a widespread usage of QKD. This becomes so attractive as the transmitter is so small that it can be integrated into basically every infrastructure. The potential of QKD is a world with proven secure communication and privacy in everyday life.

8 Appendix

8.1 CAD Sketches

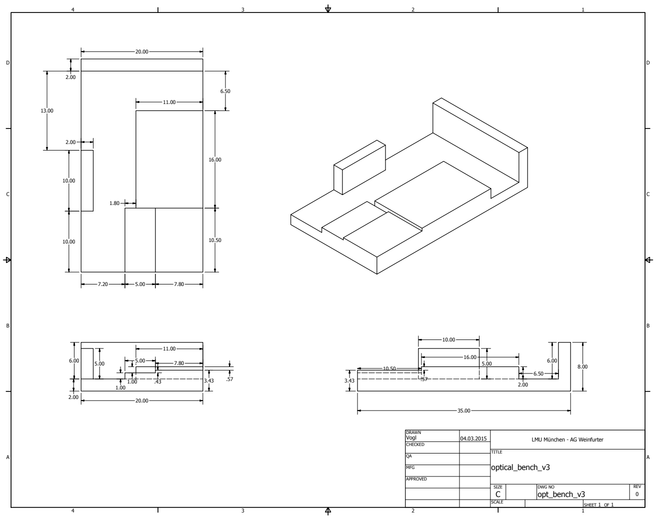


Figure 8.1: CAD sketch of the micro-optical bench. All units in *mm*.

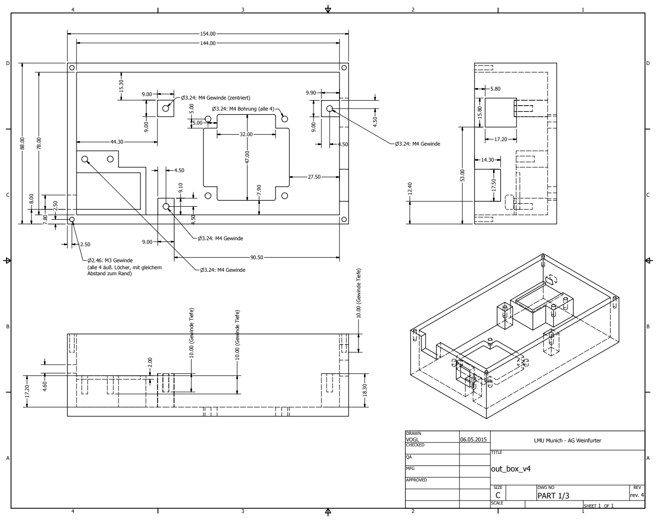


Figure 8.2: CAD sketch of the protective casing part 1. All units in *mm*.

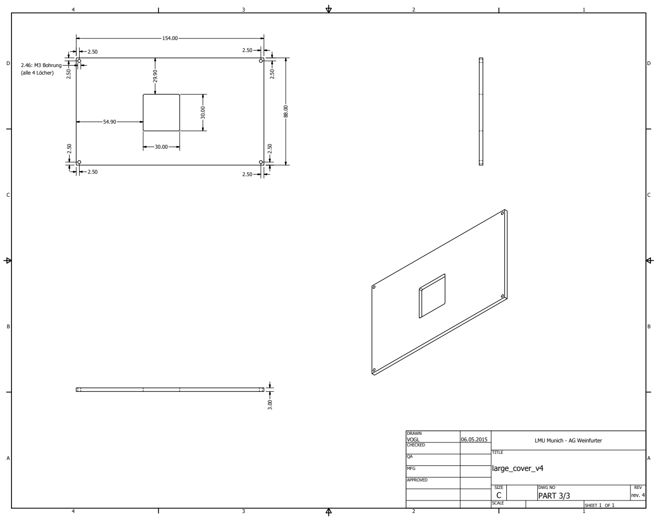


Figure 8.3: CAD sketch of the protective casing part 2. All units in *mm*.

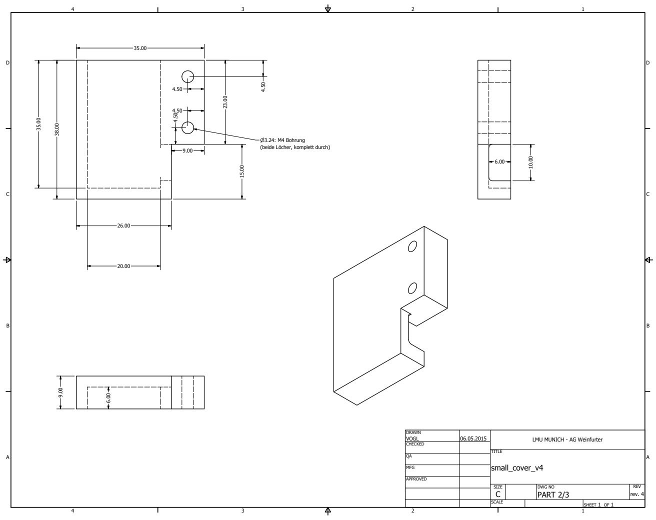


Figure 8.4: CAD sketch of the protective casing part 3. All units in *mm*.

8.2 Photographs

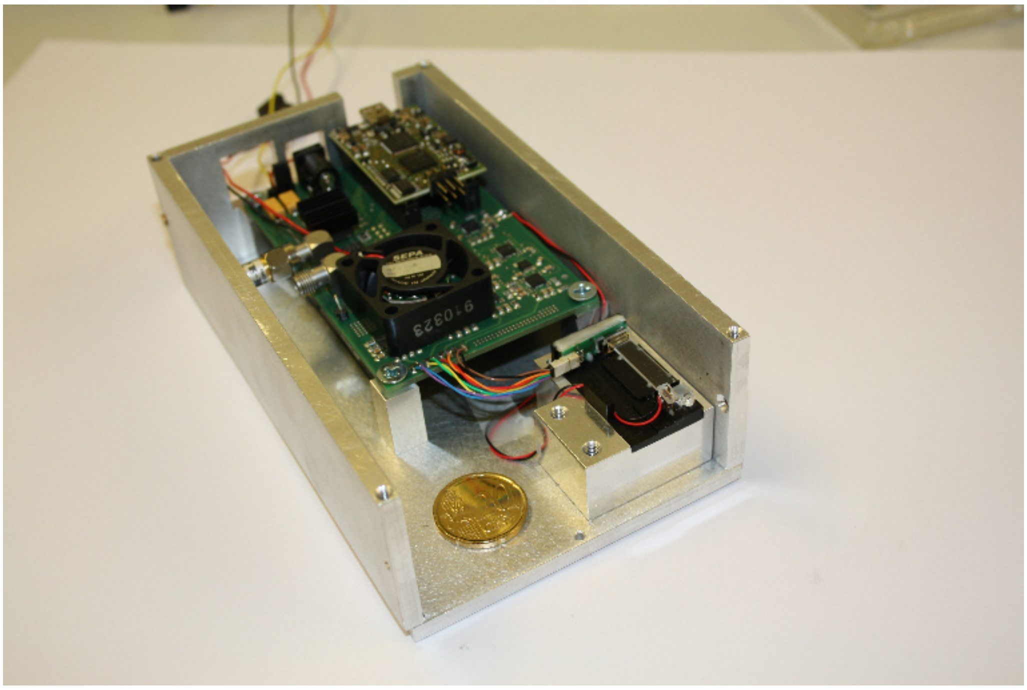
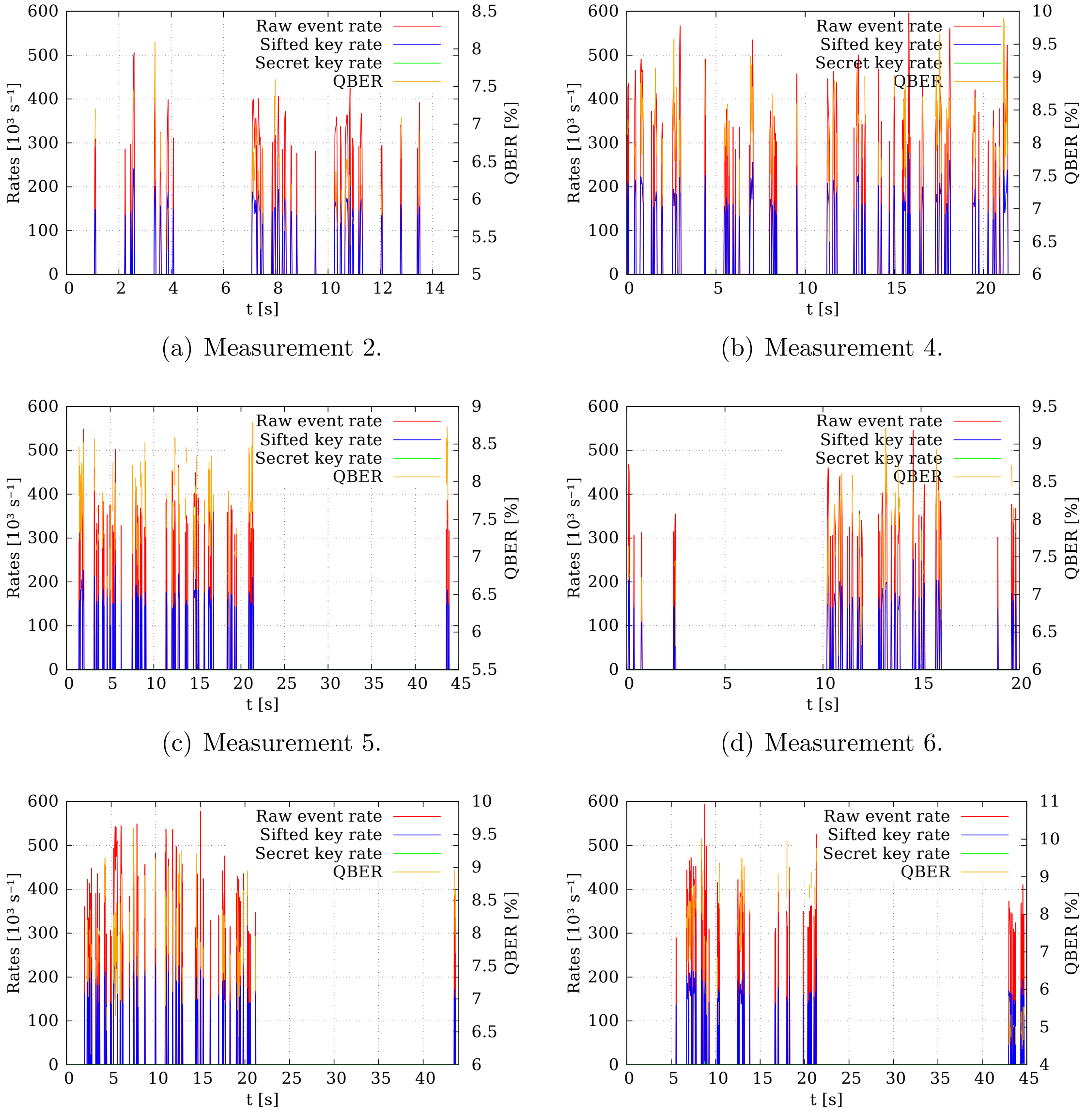


Figure 8.5: Photograph of the complete Alice module.

Photographs of the receiver are only in the electronic version of this thesis.

8.3 Additional Plots



(a) Measurement 2.

(b) Measurement 4.

(c) Measurement 5.

(d) Measurement 6.

(e) Measurement 7.

(f) Measurement 8.

Figure 8.6: Handheld measurements 2 and 4-8 after both temporal filters. For the exchanged raw, sifted and secret bit as well as the QBERs see table 4.4.

8.4 Trouble Shooting

The mirror control does not work and the TDC cannot be called.

Solution: The Alice module must be connected as last to the USB hub. Fx2 handling can get rid of this problem, but his is not implemented yet.

The calculated the phase compensation is completely different than the experimental results.

Solution: The software is expected to have the fast axis aligned as in the current setup. Fast and slow axis in the software can be exchanged by rotating the angle of the specific wave plates around 90°.

The mirror control changes from the plus to minus direction very frequently.

Solution: The distance between lens and quadrant diode is larger than the focal length. Thus an image inversion introduces a sign error.

More problems and solutions can be found in a documentary of the software which will be made available later.

9 Acknowledgement

Finally I want to thank everyone who accompanied me during my study and master thesis the last years:

- Prof. Dr. Harald Weinfurter for giving me the opportunity to work in his group and for enthusing me for the field of quantum information processing.
- Gwenaelle Mélen and Markus Rau, who worked with me on the project and made this work possible.
- Martin Zeitlmair for the assistance with the single photon spectrometer.
- All members of the Experimental Quantum Physics group, especially Dr. Wenjamin Rosenfeld, who always helped me with good advice.
- My family and friends, who have been part of my life so far.
- My girlfriend Eva Maria Hemauer for always being there when I needed you.
- Especially also my father, who encouraged me to embark upon a carrier in science.

Thank you very much to all of you!

Bibliography

[1] The Guardian, *The NSA files*, http://www.theguardian.com/world/the-nsa-files, called up January 10, 2016

[2] G. Brassard, *Cryptography in a Quantum World*, arXiv:1510.04256

[3] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Quantum cryptography*, Reviews of Modern Physics **74** (2002)

[4] C. Bennet, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *Experimental Quantum Cryptography*, Journal of Cryptology **5** (1992) 3-28

[5] ID Quantique, *Quantum-Safe Crypto*, http://www.idquantique.com/quantum-safe-crypto/network-encryption/, called up January 10, 2016

[6] M. Peev et al, *The SECOQC quantum key distribution network in Vienna*, New J. Phys. **11** (2009) 075001

[7] M. Sasaki et al, *Field test of quantum key distribution in the Tokyo QKD Network*, Optics Express **19**, 11, 10387-10409 (2011)

[8] Forbes, *Blueprints Of NSA's Ridiculously Expensive Data Center In Utah Suggest It Holds Less Info Than Thought*, http://www.forbes.com/sites/kashmirhill/2013/07/24/blueprints-of-nsa-data-center-in-utah-suggest-its-storage-capacity-is-less-impressive-than-thought/, called up January 10, 2016

[9] Wired, *The NSA Is Building the Country's Biggest Spy Center*, http://www.wired.com/2012/03/ff_nsadatacenter/all/, called up January 10, 2016

[10] N. Gisin, *Quantum Cryptography: where do we stand?*, arXiv:1508:00341

[11] United States National Security Agency (NSA), *Cryptography Today*, https://www.nsa.gov/ia/programs/suitedb_cryptography/, called up January 10, 2016

[12] D. Bruß & G. Leuchs, *Lectures on Quantum Information*, WILEY-VCH, First Edition (2006)

[13] M. Nielsen & I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Tenth Edition (2009)

[14] J. Stolze & D. Suter, *Quantum Computing*, WILEY-VCH, Second edition (2008)

[15] United States National Institute of Standards and Technology (NIST), *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*, Federal Information Processing Standards Publication 197 (2001)

[16] G. Vernam, *Secret signaling system*, Patent US1310719 A (1919)

[17] A. Bogdanov, D. Khovratovich, C. Rechberger, *Biclique Cryptanalysis of the Full AES*, Lecture Notes in Computer Science **7073**, pp. 344-371, Springer Berlin Heidelberg (2011)

[18] C. Pomerance, *A Tale of Two Sieves*, Notices of the AMS **43**, 12, pp. 1473-1485 (1996)

[19] R.Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21**, 2, pp. 120-126 (1978)

[20] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J.Sci.Statist.Comput. **26**, 1484 (1997)

[21] C. Bennet, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179 (1984)

[22] G. Brassard, *Brief History of Quantum Cryptography: A Personal Perspective*, arXiv:quant-ph/0604072

[23] P. D. Townsend, *Secure key distribution system based on quantum cryptography*, Electronics Letters **30**, 10, pp. 809-811 (1994)

[24] P. C. Sun, Y. Mazurenko, Y. Fainman, *Long-distance frequency-division interferometer for communication and quantum cryptography*, Opt. Lett. **20**, 9, pp.1062-1063 (1995)

[25] H.-K. Lo, X. Ma, K. Chen, *Decoy State Quantum Key Distribution*, Phys. Rev. Lett. **94**, 230504 (2005)

[26] T.Moroder, M. Curty, N. Lütkenhaus, *Detector decoy quantum key distribution*, arXiv:0811.0027

[27] X. Ma, B. Qi, Y. Zhao, H.-K. Lo, *Practical decoy state for quantum key distribution*, Phys. Rev. A **72**, 012326 (2005)

[28] J. W. Harrington, J. M. Ettinger, R. J. Hughes, J. E. Nordholt, *Enhancing practical security of quantum key distribution with a few decoy states*, arXiv:quant-ph/0503002

[29] S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, V. Makarov, *Controlling an actively-quenched single photon detector with bright light*, Opt. Express **19**, 23590 (2011)

[30] L. Lydersen, M. Akhlaghi, A. Majedi, J. Skaar, V. Makarov, *Controlling a superconducting nanowire single-photon detector using tailored bright illumination*, New J. Phys **13**, 113042 (2011)

[31] C. Kurtsiefer, P. Zarda, S. Mayer, H. Weinfurter, *The breakdown flash of Silicon Avalanche diodes - backdoor for eavesdropper attacks?*, Journal of Modern Optics **48**, 2039-2047 (2001)

[32] Y. Zhao, C. Fung, B. Qi, C. Chen, H. Lo, *Quantum Hacking: Experimental demonstration of time-shift attack against practical quantum key distribution systems*, Physical Review A, **78**, 042333 (2008)

[33] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth and H. Weinfurter, *Spatial Mode Side Channels in Free-Space QKD Implementations*, IEEE JSTQE **25**, 3 (2014)

[34] T. Vogl, *Security of a free space QKD-receiver module with angle-dependent detection efficiency mismatch*, Bachelor's Thesis (2014)

[35] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, A. J. Shields, *Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution*, Phys. Rev. X **5**, 031030 (2015)

[36] U. Vazirani,T. Vidick, *Fully device independent quantum key distribution*, arXiv:1210.1810v1 (2012)

[37] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, J.-W. Pan, *Measurement-Device-Independent Quantum Key Distribution over 200 km*, Phys. Rev. Lett. **113**, 190501 (2014)

[38] G. Brassard, L. Salvail, *Secret-key reconciliation by public discussion*, Eurocrypt, pp. 410-423 (1993)

[39] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, C. G. Peterson, *Fast, efficient error reconciliation for quantum cryptography*, Phys. Rev. A **67**, 052303 (2003)

[40] R. Gallager, *Low-Density Parity-Check Codes*, IRE Transactions on Information Theory (1962)

[41] C.-H. F. Fung, H.-K. Lo, *Security proof of a three-state quantum-key-distribution protocol without rotational symmetry*, Phys. Rev. A **74**, 042342 (2006)

[42] B.-S. Shi, Y.-K. Jiang, G.-C. Guo, *Quantum key distribution using different-frequency photons*, Applied Physics B **70**, 3, pp. 415-417 (2000)

[43] H. Bechmann-Pasquinucci, N. Gisin, *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography*, Phys. Rev. A **59**, 4238 (1999)

[44] A. Ekert, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 6, pp. 661-663 (1991)

[45] C. Bennett, G. Brassard, N. Mermin, *Quantum cryptography without Bell's theorem*, Phys. Rev. Lett. **68**, pp. 557-559 (1992)

[46] E. Diamanti, A. Leverrier, *Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations*, arXiv:1506.02888

[47] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, J.-W. Pan, *Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution*, Phys. Rev. Lett. **114**, 180502 (2015)

[48] C. Guerlin, J. Bernu, S. Deléglise, C. Sayrin, S. Gleyzes, S. Kuhr, M. Brune, J.-M. Raimond, S. Haroche, *Progressive field-state collapse and quantum non-demolition photon counting*, Nature **448**, pp. 889-893 (2007)

[49] C. Shannon, *A Mathematical Theory of Communication*, The Bell System Technical Journal **27**, pp. 379-423, 623-656 (1948)

[50] IEEE, *IEEE 802.11n Report*, `http://grouper.ieee.org/groups/802/11/Reports/tgn_update.htm`, called up January 10, 2016

[51] T. Vogl, *Construction of an electronically-driven mirror system for QKD*, Internship Report (2015)

[52] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, H. Weinfurter, *Design and Evaluation of a Handheld Quantum Key Distribution Sender module*, IEEE Journal of Selected Topics in Quantum Electronics **21**, 1 (2014/15)

[53] G. Mélen, *Integrated Quantum Key Distribution Sender Unit for Handheld Platforms*, PhD Thesis (to be published)

[54] C. Gebhardt, *Implementierung des Quantenschlüsselaustauschs auf einem mobilen Endgerät*, Bachelor's Thesis (2014)

[55] C.-S. Kim, S.-H. Ahn, D.-Y. Jang, *Review: Developments in micro/nanoscale fabrication by focused ion beams*, Vacuum **86**, 8, pp. 1014-1035 (2011)

[56] Z. Huang, N. Geyer, P. Werner, J. de Boor, U. Gösele, *Metal-Assisted Chemical Etching of Silicon: A Review*, Adv. Mater. **23**, 2 (2010)

[57] P. R. Bevington, D. K. Robinson, *Data Reduction and Error Analysis for the Physical Sciences*, McGraw-Hill Higher Education, Third Edition, pp. 194-197 (2002)

[58] C. Gobby, Z. L. Yuan, A. J. Shields, *Quantum key distribution over 122 km of standard telecom fiber*, Appl. Phys. Lett. **84**, 19, pp. 3762-3764 (2004)

[59] G. Vallone, D. G. Marangon, M. Canale, I. Savorgnan, D. Bacco, M. Barbieri, S. Calimani, C. Barbieri, N. Laurenti, P. Villoresi, *Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels*, Phys. Rev. A **91**, 042320 (2015)

[60] R. D. Somma, R. J. Hughes, *Security of decoy-state protocols for general photon-number-splitting attacks*, Phys. Rev. A **87**, 062330 (2013)

[61] M. Hayashi, R. Nakayama, *Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths*, New J. Phys. **16**, 063009 (2014)

[62] M. Tomamichel, C. C. W. Lim, N. Gisin, R. Renner, *Tight Finite-Key Analysis for Quantum Cryptography*, arXiv:1103.4130v2

[63] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, K. Tamaki, *Finite-key security analysis of quantum key distribution with imperfect light sources*, arXiv:1504.08151

[64] V. Scarani, A. Acín, G. Ribordy, N. Gisin, *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Phys. Rev. Lett. **92**, 057901 (2004)

[65] C. Branciard, N. Gisin, B. Kraus, V. Scarani, *Security of two quantum cryptography protocols using the same four qubit states*, Phys. Rev. A **72**, 032301 (2005)

[66] B. Kraus, C. Branciard, R. Renner, *Security of quantum-key-distribution using two-way classical communication or weak coherent pulses*, Phys. Rev. A **75**, 012316 (2005)

[67] Y.-C. Jeong, Y.-S. Kim, Y.-H. Kim, *An experimental comparison of BB84 and SARG04 quantum key distribution protocols*, Laser Phys. Lett. **11**, 095201 (2014)

Declaration of Authorship

English Version

I hereby certify that this thesis has been composed by me and is based on my own work, unless stated otherwise. No other's person work has been used without due acknowledgement in this thesis. All references and verbatim extracts have been quoted and all sources of information, including graphs and data sets, have been specially acknowledged.

Name:

Signature:

Place and Date:

German Version

Erklärung:

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

München,