Towards Compact High-Altitude-Platform Based Quantum Key Distribution

Jacob Birkmann

Munich 2019

Towards Compact High-Altitude-Platform Based Quantum Key Distribution

Master's Thesis
at the Faculty of Physics
of the Ludwig–Maximilians–University
Munich

handed in by
Jacob Birkmann

supervised by
Prof. Harald Weinfurter

Munich, 01.04.2019

Entwicklungen zum Quantenschlüsselaustausch mittels einer kompakten Höhenplattform

Masterarbeit
an der Fakultät für Physik
der Ludwig–Maximilians–Universität
München

vorgelegt von
Jacob Birkmann

betreut durch
Prof. Harald Weinfurter

München, den 01.04.2019

Contents

Chapter 1

Introduction

One important feature of life in our society is communication, may it be personal conversation or the exchange of information in a business or government setting. Irrespective of the medium, the transmission of information may be subject to malicious eavesdropping and manipulation attacks. For example the internet, currently one of the main means for global communication, with over 4.3 billion users as of March 2019[1], is continuously threatened by hacking attacks on private cloud storage (e.g. iCloud hack in 2014 [1]), political campaigns (e.g. 2016 Presidential Election in the US [2]) or critical infrastructure (e.g. 2017 attack on petrochemical plant in Saudi Arabia [3]). Not only stored data can be obtained and altered by hackers, but also direct communication is susceptible to their attacks. Again and again, both the public and security experts are alarmed by the vulnerability of our networks, but countermeasures are difficult to implement.

The possibly disastrous consequences of these threats makes secure digital communication obligatory and has lead to the development of a variety of classical encryption algorithms, especially over the past decades. Out of those, the group of asymmetric key encryption schemes, where different keys are used for encrpytion and decryption and the decryption key does not have to be shared, offers security based on the complexity of mathematical problems and the assumption of limited computational power. The most prominent example of an asymmetric cryptography scheme is the widely used RSA [4] algorithm, where a pair of public and private key is generated. With knowledge of the public key, breaking of the cryptosystem is possible only by factorising large numbers, so far not practical even with the best known classical algorithm. Yet, an implementation of the Shor algorithm [5] on a quantum computer will break the security. Moreover, it is neither proven that there exists no efficient classical factorization algorithm nor that so called post-quantum encryption algorithms[2] will never be efficiently broken by a quantum computer, due to the (exponentially) shorter runtime. Different security concerns exist also for modern examples of symmetric key encryption schemes, like the Advanced Encrpytion Standard (AES) [6], where the same pre-shared key is used for both encryption and decryption.

Only one of the symmetric schemes, the so called One-Time-Pad (OTP) [7], offers absolute (so called *information theoretic*) security, but the necessity to share a fully random secret key with the same length as the plaintext message between the communicating parties constrains

[1] `https://www.internetworldstats.com/stats.htm`, visited 2019-03-19.

[2] Classical algorithms with a complexity high enough to be considered robust against a quantum computer in a reasonable amount of time at the current state of knowledge.

the practicality of this kind of cryptosystem. This problem is tackled by the concept of quantum key distribution (QKD) [8, 9, 10] where the laws of quantum mechanics provide the possibility to share an unconditionally secure secret key between authenticated parties.

While first ideas to use quantum effects for secure storage of information emerged in the 1970s (published by Stephen Wiesner in 1983 [11]), the first proposal for a QKD protocol was presented by Charles Bennett and Gilles Brassard in 1984 (BB84) [12], where they used a set of non-orthogonal quantum states, for which quantum mechanics offers a possibility to detect eavesdropping. After the first experimental realization of QKD in 1992 [13] and ongoing developments in the theory of QKD, in particular of various protocols improving upon certain aspects of the QKD cryptosystem, the first companies offering commercial QKD systems emerged in the early 2000s. The existing QKD systems can be separated into fiber-based and free-space implementations, which have their respective advantages in different scenarios. While the former can make use of existing fiber networks to allow for efficient secure key exchanges in metropolitan environments (e.g. in Vienna [14] and Tokyo [15]), they are limited to maximal link distances of few hundred kilometers (current record 421 km [16]) due to losses in the optical fibers and noise of the system. Free-space implementations, on the other hand, possibly enable intercontinental key exchange, using satellite-to-ground communication, where the satellite might function as a trusted node. Amongst other quantum experiments, the Chinese research satellite Micius demonstrated a successful key exchange between a satellite and multiple ground stations [17, 18]. Besides the resource intensive approach used in this project (mass > 600 kg, cost $> \$100$m), there are also proposals to use much smaller satellites down to so called CubeSats for space-based QKD (review of different projects in [19]). The advantage of this nanosatellite platform is the small form factor, based on $10 \times 10 \times 10$ cm^3 units, allowing for economical testing of technologies in a space environment before eventually building up a large scale space-based QKD network.

As this idea is at the center of a current project in our group, this thesis deals with some of the developments necessary for the implementation of a polarization-encoding-BB84 QKD sender unit on both high-altitude platforms (HAPs) and CubeSats. These compact platforms set high requirements concerning the power consumption for the modules as well as the size and weight of the integrated payloads. Furthermore, the harsh environment in space requires to be able to sustain large temperature differences, mechanical stress and radiation on the components. Starting from the miniaturized QKD setup built within our group for a short range hand-held key exchange [20], the necessary modifications to meet the HAP and CubeSat requirements are developed. Theoretic estimations of the link efficiencies during operation in different scenarios are performed in order to assess the achievable secure key rates of the proposed implementation.

The organization of this work is as follows: Chapter 2 summarizes the physical and quantum mechanical concepts that are necessary for the secure key exchange. The theory of QKD is introduced in Chapter 3, where also classical cryptographic principles are included. The chapter ends with theoretic performance estimations for a HAP QKD system. The hand-held setup, on which the modifications are based, is described in Chapter 4, followed by the presentation of the developments during this Master's thesis (Chapter 5).

Chapter 2

Underlying physical concepts

Quantum Key Distribution was the first method proposed in the field of quantum information. It builds upon the most elementary principles of quantum mechanics that are the superposition principle, the principle of complementarity of certain measurements, and the no-cloning therorem. Before coming to the description of QKD, we thus introduce here the basic principles togetehr with the formal description of the polarization of light used to implement QKD in an experiment.

2.1 Quantum mechanics

2.1.1 Qubits

The basis for transferring digital information is the so called bit, which can have the values 0 and 1. As we are dealing with quantum information, the quantum counterpart qubit of this unit needs to be introduced.
The qubit is a two-state quantum system with the two orthogonal states states $|\Psi_0\rangle$ and $|\Psi_1\rangle$. The difference to the classical bit is, that the state $|\Psi\rangle$ can also be in a quantum mechanical superposition of $|\Psi_0\rangle$ and $|\Psi_1\rangle$:

$$|\Psi\rangle = \alpha\,|\Psi_0\rangle + \beta\,|\Psi_1\rangle \tag{2.1}$$

For a normalized state $|\Psi\rangle$, the complex amplitudes α and β are restricted by the normalization condition $|\alpha^2| + |\beta^2| = 1$. This equation holds for any two basis vectors $|\Psi_0\rangle$ and $|\Psi_1\rangle$ of the two-dimensional Hilbert space of the state $|\Psi\rangle$.

Physical manifestations of qubits are, for example, two energy states of an atom, spin-$1/2$ particles with spin up and spin down or the polarization of a photon.

2.1.2 Quantum mechanical measurements

If one wants to measure an observable A of a quantum state $|\Psi\rangle$, there exist different formulations describing the physical measurement process. Probably the most simple and straightforward formulation was given by John von Neumann [21], therefore called *von Neumann measurements.* For a given physical property there is an observable A, which is described by the Hermitian operator $\hat{A}$ with the eigenvalues $\{\lambda_n\}$ and the corresponding eigenstates $\{|\lambda_n\rangle\}$. Then the possible results of a measurement of A are the (real) eigenvalues. If the state $|\Psi\rangle$

is element of the same Hilbert space as A, it can be described as a linear combination of the $\{|\lambda_n\rangle\}$:

$$|\Psi\rangle = \Sigma_n a_n |\lambda_n\rangle \tag{2.2}$$

It is of course also possible to write the operator $\hat{A}$ in terms of its eigenstates and -values:

$$\hat{A} = \Sigma_n \lambda_n |\lambda_n\rangle \langle\lambda_n| = \Sigma_n \lambda_n \hat{P}_n \tag{2.3}$$

From equations 2.2 and 2.3 it is obvious, that the measurement of A on $|\Psi\rangle$ is simply the projection of the state onto the eigenstates of the measured operator. Thus, the probability to measure the state $|\Psi\rangle$ in one of A's eigenstates $|\lambda_n\rangle$ is

$$P(|\lambda_n\rangle) = |\langle\Psi|\lambda_n\rangle|^2. \tag{2.4}$$

Any two-dimensional Hilbert space is spanned by the eigenstates of the Pauli operators σ_X, σ_Y and σ_Z. As our experimental implementation uses the polarization degree of freedom of photons, we span the Hilbert space of polarizations with the three complementary bases B_X, B_Y and B_Z [22], whose basis vectors are the eigenstates of the Pauli operators σ_Z, σ_X and σ_Y, in that order. Basis B_X consists of the vectors $|H\rangle$ and $|V\rangle$, representing horizontal and vertical polarization, respectively. As a two-dimensional Hilbert space is fully described by two basis vectors, the vectors of the other two bases, $|P\rangle$ / $|M\rangle$ (diagonal/anti-diagonal) for B_Y and $|R\rangle$ / $|L\rangle$ (right-/left-circular) for B_Z, can be written as linear combinations of $|H\rangle$ and $|V\rangle$, which is summarized in Table 2.1. If the state to be measured, $|\Psi\rangle$, is prepared as $|H\rangle$ and a measurement in the B_X basis is performed, the measurement of the probabilities of the state to be $|H\rangle$ or $|V\rangle$ yields a unique result:

$$P(|H\rangle) = |\langle H|H\rangle|^2 = 1 \tag{2.5}$$
$$P(|V\rangle) = |\langle H|V\rangle|^2 = 0 \tag{2.6}$$

Measuring in the other two bases, however, will give no information at all about the polarization state $|\Psi\rangle$, as both results in this basis are equally probable:

$$P(|P\rangle) = |\langle H|P\rangle|^2 = |\frac{1}{\sqrt{2}}(\langle H|H\rangle + \langle H|V\rangle)|^2 = \frac{1}{2} \tag{2.7}$$
$$P(|M\rangle) = |\langle H|M\rangle|^2 = |\frac{1}{\sqrt{2}}(\langle H|H\rangle - \langle H|V\rangle)|^2 = \frac{1}{2} \tag{2.8}$$
$$P(|R\rangle) = |\langle H|R\rangle|^2 = |\frac{1}{\sqrt{2}}(\langle H|H\rangle + i\langle H|V\rangle)|^2 = \frac{1}{2} \tag{2.9}$$
$$P(|L\rangle) = |\langle H|L\rangle|^2 = |\frac{1}{\sqrt{2}}(\langle H|H\rangle - i\langle H|V\rangle)|^2 = \frac{1}{2} \tag{2.10}$$

The calculations for the other five possible polarizations of $|\Psi\rangle$ are done accordingly, showing that measuring a state in its preparation basis will have a conclusive outcome, while through the measurement in one of the complementary bases, no information can be gained. Furthermore, a measurement in a basis different from the preparation basis destroys all the polarization information. In the example of the initially prepared $|H\rangle$ photon, a measurement in the B_Y basis will project the state onto $|P\rangle$ with 50% probability. A further measurement in the B_X basis, which the state was prepared in initially, will have an uncorrelated outcome, i.e. it will be $|H\rangle$ or $|V\rangle$ with equal probability since the intermediate B_Y-measurement resulted in the preparation of $|P\rangle$ ($|M\rangle$, respectively).

Basis	Basis vectors	Polarization
B_X	$\|H\rangle$	Horizontal
	$\|V\rangle$	Vertical
B_Y	$\|P\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	+45° Diagonal
	$\|M\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	−45° Anti-Diagonal
B_Z	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + i\,\|V\rangle)$	Right-Circular
	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - i\,\|V\rangle)$	Left-Circular

Table 2.1: Basis states of B_X, B_Y and B_Z and their polarizations

2.1.3 No-cloning theorem

The preceeding section shows, that without knowing the preparation basis of the polarization of a single photon, there is no way to certainly determine its polarization state. For the security of the QKD protocols described in the next parts of this work, it is thus also crucial, that an attacker cannot simply make exact copies of the quantum state. Otherwise, an eavesdropper could make a copy and then simply wait until the preparation basis is announced (see Section 3.3.1) in order to gain all the information by the appropriate measurement. Yet, the impossibility of such a *perfect* cloning device was shown by Wootters and Zurek [23], proving the no-cloning theorem. The idea of their proof can be compactly summarized (as it was done, e.g., by Barnett [24]) as:

A perfect cloning device should take the original state $|\Psi\rangle$ and a blank state $|B\rangle$ and transform them into two copies of the original state,

$$|\Psi\rangle \otimes |B\rangle \longrightarrow |\Psi\rangle \otimes |\Psi\rangle \,. \tag{2.11}$$

This cloning might work for the qubit states $|0\rangle$ and $|1\rangle$,

$$|0\rangle \otimes |B\rangle \longrightarrow |0\rangle \otimes |0\rangle \,, \tag{2.12}$$

$$|1\rangle \otimes |B\rangle \longrightarrow |1\rangle \otimes |1\rangle \,, \tag{2.13}$$

but it is easy to show that it cannot work for a superposition state $\alpha\,|0\rangle + \beta\,|1\rangle$. The cloning device (defined by equations 2.12 and 2.13) would transform this as

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |B\rangle \longrightarrow \alpha\,|0\rangle \otimes |0\rangle + \beta\,|1\rangle \otimes |1\rangle \,, \tag{2.14}$$

which is obviously not the cloning transformation from equation 2.11, which would have had

$$\begin{aligned}(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha\,|0\rangle + \beta\,|1\rangle) = {} & \alpha^2\,|0\rangle \otimes |0\rangle + \alpha\beta\,|0\rangle \otimes |1\rangle \\ & + \alpha\beta\,|1\rangle \otimes |0\rangle + \beta^2\,|1\rangle \otimes |1\rangle\end{aligned} \tag{2.15}$$

as the result of the copying operation.

2.2 Polarization of light

2.2.1 Stokes formalism for the description of polarized light

One convenient way to mathematically describe and quantify the polarization of light is through the statistical method of the Stokes formalism [25]. The general Stokes vector

$$\vec{S} = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} \tag{2.16}$$

is calculated for light with intensity I as

$$\vec{S} = \begin{pmatrix} I \\ I_H - I_V \\ I_P - I_M \\ I_R - I_L \end{pmatrix}, \tag{2.17}$$

in terms of the six polarization states H, V, P, M, R and L, where I_i is the intensity of the i-polarized part of the light. For easier comparability, it is useful to work with the intensity-normalized Stokes vector

$$\vec{S}_{norm} = \begin{pmatrix} 1 \\ \frac{I_H - I_V}{I_H + I_V} \\ \frac{I_P - I_M}{I_P + I_M} \\ \frac{I_R - I_L}{I_R + I_L} \end{pmatrix}. \tag{2.18}$$

In this representation, the Stokes vectors of the polarizations H, V, P, M, R and L are

$$\vec{S}_{H/V} = \begin{pmatrix} 1 \\ \pm 1 \\ 0 \\ 0 \end{pmatrix}, \ \vec{S}_{P/M} = \begin{pmatrix} 1 \\ 0 \\ \pm 1 \\ 0 \end{pmatrix}, \ \vec{S}_{R/L} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \pm 1 \end{pmatrix}. \tag{2.19}$$

A common visualization of polarization states is the Poincaré sphere, where the intensity-normalized Stokes components S_1, S_2 and S_3 are the x-, y- and z-coordinates, respectively, as is shown in Figure 2.1. The degree of polarization (DOP) of light can be seen in the Poincaré representation, as it is the length of the intensity normalized Stokes vector, meaning that the Stokes vectors of fully polarized light end on the surface of the sphere, while (partially) polarized ones lie within it. This length is calculated as

$$DOP = \sqrt{S_1^2 + S_2^2 + S_3^2}. \tag{2.20}$$

2.2.2 Polarization analysis of light

In order to measure light with an unknown polarization, one has to determine the intensity (or power) contributions of the six different polarization components. This splitting of the incoming light is equivalent to projections onto the basis states of B_X, B_Y and B_Z and is

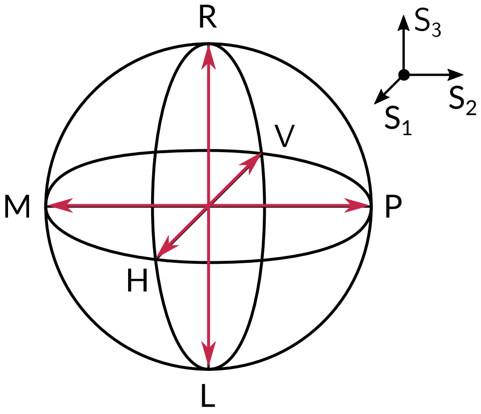

Figure 2.1: Representation of polarization states with the Poincaré sphere

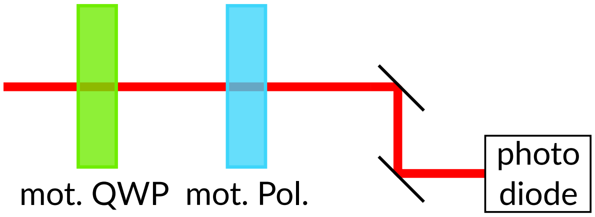

Figure 2.2: Setup for a tomography measurement consisting of motorized quarter wave plate and polarizer, while the intensity is measured with a photo diode. The two mirrors in front of the diode are used to align the beam.

Projection	H	V	P	M	R	L
QWP angle [°]	0	0	+45	+45	0	0
Pol. angle [°]	0	90	+45	-45	+45	-45

Table 2.2: Angles of the QWP and the polarizer necessary for the six projection measurements.

done by a combination of a quarter wave plate (QWP) and a linear polarizer, similar to the so called quantum state tomography (QST), depicted in Figure 2.2.

The projections are done by setting the correct angles at the QWP and the polarizer, as summarized in Table 2.2. The intensity of the light in these six polarization states is monitored by a photo diode and equation 2.18 is used to calculate the Stokes vector of the unknown polarization.

Chapter 3

Theory of quantum key distribution

Based on the features of quantum mechanics, this section presents the theoretic concept and gives the reason for the security of Quantum Key Distribution. After the presentation of some of the existing protocols and the flaws of imperfect practical implementations, theoretic secure key rate equations are used to estimate the performance of a long distance free-space QKD link.

3.1 Classical cryptography

In order to communicate confidential, sensitive or private information secretly, humankind has developed and used a multitude of methods of cryptography for thousands of years. There are some basic principles underlying any cryptographic system, from ancient roman ones to the ones securing our communication today.

3.1.1 Basic principles

If two parties by convention called Alice and Bob want to send each other (secret) messages in a secure way, they have to come up with a method which does not just send the message in its normal, plaintext form, as otherwise, a potential eavesdropper, usually called Eve, would easily be able to intercept the communication channel and read the sent message. To circumvent this, Alice encodes her plaintext message out of a set of messages M with a key from the set of all keys K using the encryption function e, arriving at the ciphertext, which is part of set C (see Figure 3.1). This ciphertext, optimally containing zero information about the original message, is sent to Bob, who is then able to read the message, using a key and the decryption function d. Eve is now still able to listen in to the communication channel between Alice and Bob, but without knowledge of the decryption key, she cannot optain more information about the message than its length.

One of the oldest encryption schemes is the well known Caesar Cipher, owing its name to the roman emperor Julius Caesar. It is a permutation cipher where every letter of the plaintext message is shifted by k letters for the ciphertext; an example for the encryption in the case $k = 7$ is shown in Table 3.1. This would transform the plaintext *et tu, brute* into *la ab, iybal*, which Bob could decrypt by using the inverse of the encryption function, namely, shifting every ciphertext character cyclically $k = 7$ letters to the left.

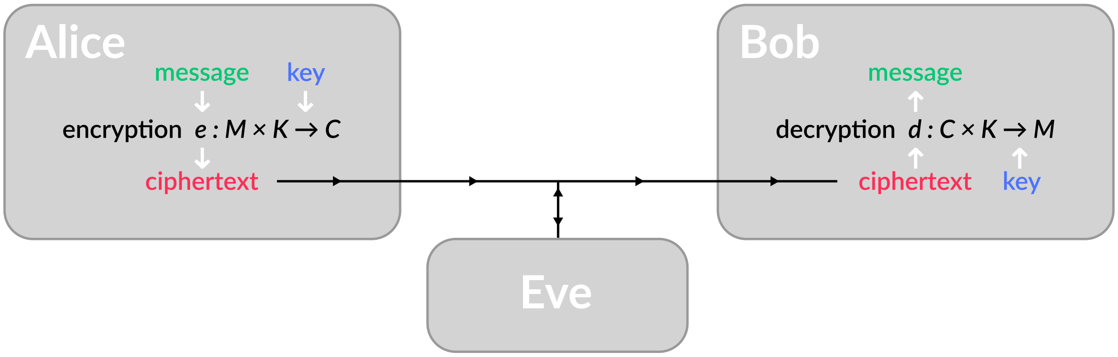
Alice
message
key
encryption $e : M \times K \to C$
ciphertext
Bob
message
decryption $d : C \times K \to M$
ciphertext
key
Eve

Figure 3.1: Model of a basic cryptographic system

The Caesar Cipher intuitively illustrates the concept of a cryptosystem using the same key for encryption and decryption of the plaintext message. This symmetric key concept is also used in some modern encryption algorithms, while others are part of the asymmetric cryptography schemes. These two groups of modern cryptography schemes, the symmetrical and asymmetrical key encryption, are introduced in the following.

a	b	c	d	e	f	g	h	...	x	y	z
h	i	j	k	l	m	n	o	...	e	f	g

Table 3.1: Encoding table for Caesar's cipher with $k = 7$

3.1.2 Asymmetrical key encryption

In an asymmetric key cryptosystem, sender and receiver use different keys for encoding and decoding of the message. If Bob wants other parties to be able to communicate with him in a secure way, he generates a pair of two keys, the public and the privat key. The public key is made available to anyone over a medium of Bob's choice, e.g. the internet, while Bob keeps his private key, making sure that it is inaccessible to any other party. The two keys are generated in a way, that anyone can encrypt their plaintext message with the public key, but the decryption only works with the use of the private key.

The process of the key generation and the security of the resulting encryption rely on mathematical *one-way functions*. These are calculations that are efficiently done in forward direction, whereas the inverse operation is computationally highly difficult. One widely used asymmetric encryption protocol is called RSA, after its inventors Rivest, Shamir and Adleman [4]. Here, the encryption is performed by the mathematical operation required to deduce the private key from the public key, the factorization of large numbers, which scales at least exponentially with the key length. With existing classical algorithms (the best known one, the General Number Field Sieve, has a runtime of order $\mathcal{O}(exp(\sqrt[3]{n}))$, the computation times for the factorization of a RSA key with currently used 2000 bit would take billions of years, surpassing the universe's lifetime.

However, there exists no proof that a classical algorithm doing the factorization efficiently will never be available. Furthermore, implementing the Shor algorithm [5] on a future quantum computer will decrease the complexity of the problem, resulting in polynomially scaling computation times, making attacks on the RSA encryption feasible. This clearly shows, that a solution for the long term security of encrypted messages is still to be found. For this reason, there is currently also a big quest for a so called post-quantum cryptoscheme, i.e. an asymmetric encryption robust against attacks with a quantum computer.

3.1.3 Symmetrical key encryption

Symmetric encryption demands, that identical keys are used for encryption by Alice and decryption on Bob's side.
The most widely implemented modern symmetrical key encryption scheme is the Advanced Encryption Standard (AES) [6]. This scheme substitudes and permutes blocks of the message bits (length ≤ 128) with a key of length n (n= 128, 192 or 256 [26]). This leads to 2^n possible outcomes that would all have to be tested in a brute force attack; for n = 128, these $2^{128} \approx 3.4 \cdot 10^{38}$ possible combinations would take a modern supercomputer with $\sim 10^{15}$ FLOPS around 10^{16} years. While there might currently exist no algorithm, quantum or classical, that provides an efficient attack on AES encryption, the so called reduced round variants of AES already show reduced security [26].

Another prominent example of a symmetrical encryption scheme is the One-Time-Pad (OTP), patented by G. Vernam in 1919 [7]. Given correct handling and implementation, the OTP provides unconditional information theoretic security. To achieve this goal, the users have to fulfil four tasks:

- The key has to be at least as long as the message that is to be encrypted.
- The key needs to be fully random.
- No key must be used more than once, not even in parts.
- Naturally, the key has to be stored securely, without any third party being able to access it.

If the communicating parties both hold a key, communication takes the following steps: Firstly, Alice encrypts her plaintext message by applying letterwise XOR operations between key and message. This ciphertext can then be transmitted to Bob, who decrypts it by applying a XOR operation with the same key onto the ciphertext. The randomness of the key-string (associated with maximum entropy) ensures maximum entropy and randomness also for the ciphertext. Thus it does not contain any information about the initial message at all, as was proven by C. Shannon [27]. For this reason, even if Eve would use a brute force attack of trying every possible key combination, this would keep her from accessing the original plaintext, as any message is now equally probable to result from such a brute force attack. The information theoretic security of the OTP is a great feature, but it comes with the problem of distribution, management and storage of large amounts of keys, that all symmetric key encrpytion schemes have. If this problem can be overcome, for which the next section introduces a possible solution, these encryption methods grant security, even after the advent of a quantum computer.

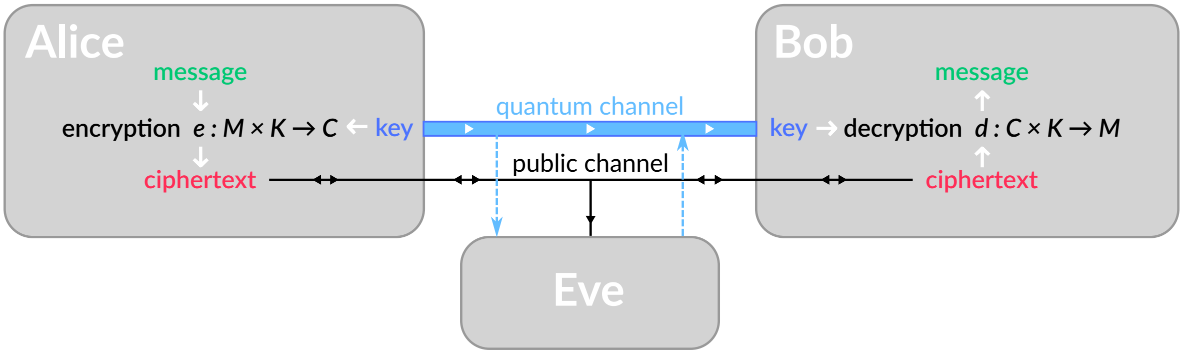
Alice
message
encryption $e: M \times K \rightarrow C$
key
ciphertext
quantum channel
public channel
Bob
message
key
decryption $d: C \times K \rightarrow M$
ciphertext
Eve

Figure 3.2: Model of the cryptographic process of QKD. The key generation and exchange happens over a quantum channel, which may be intercepted by Eve. All further communication uses an authenticated public channel, accessable but not alterable to Eve.

3.2 Concept of quantum key distribution

The problem of the key exchange for symmetric key encryption is tackled by the concept of quantum key distribution (QKD). The first proposal for a key exchange protocol was given in 1984 by C. H. Bennett and G. Brassard [12], hence it is given the name BB84.

A first step in this concept is to separate the process of generating and sharing a secret key from sending the encrypted ciphertext, where the former is done over a a so called *quantum channel*, sending single photons from Alice to Bob, while the latter uses a (possibly insecure, but authenticated) public channel, as it is illustrated in Figure 3.2. By this separation, the use of a classical symmetric encryption algortihm ensures information theoretic secure communication, if the key establishment over the quantum channel follows certain rules.

As section 2.1.2 shows, one cannot measure the unknown state of a single photon simultaneously in two conjugate bases. This means, that if Alice randomly sends bit values 0 or 1, and they are randomly prepared in one of the two bases, Bob as well as any eavesdropper have to somehow decide, in which basis they measure the photon. If the preparation and measurement bases match, the result will always be the sent bit; but in cases where the bases are different, the result will have no correlation with the initially prepared bit.

Additionally, the no-cloning theorem (Section 2.1.3) states, that Eve cannot perfectly copy the unknown single quantum state sent by Alice, but, as shown in Section 2.1.3, she rather introduces additional noise when trying to do so. Such copying would allow her to wait with the polarization measurement until after the basis announcement between Alice and Bob and thus obtain precise information about Alice's bit.

3.3 QKD Protocols

How the requirements on the key exchange are practically implemented, differs for the various protocols proposed. One basic distinction to categorize the wide variety of existing QKD protocols is a property of the signal carriers, namely them being continuous variables (CV, states sent defined on an infinite-dimensional Hilbert space) or discrete variables (DV, typically defined on two-dimensional Hilbert space) [8]. In the case of the information being carried by photons, the protocols use different Degrees of Freedom (DoF) of light, as the polarization or phase, for example, to encode the key bits.

3.3.1 BB84

As already mentioned, the first QKD protocol was proposed by Bennett and Brassard in 1984 [12]. In an exemplary implementation, the linear polarization states H, V, P and M of single photons are chosen to encode the key bits, where H and P encode the bit value 0, while V and M resemble bit 1. Hence, Alice needs a device capable of generating single photons with a precisely prepared polarization, while Bob has to be able to detect the sent qubits and distinguish the different polarization states. The choice of preparation basis, as well as the prepared bit value need to be fully random. The photons are sent to Bob over the quantum channel (see Figure 3.2) and randomly measured in one of the two bases. After this quantum communication step, Alice and Bob each hold non-identical raw keys of length N.

In a next step, the so called key sifting, Alice and Bob exchange their basis choice for the preparation and measurement of each bit over an authenticated classical channel. If they randomly decide between the two bases with equal probability, their choice will on average match in 50% of the cases [1]. Thus, bits with different preparation and measurement bases are discarded, leading to the sifted key with length $l_{sift} \approx {}^{N}\!/_{2}$. The so called quantum bit error ratio (QBER) quantifies the ratio between false and sifted bits and is defined as follows:

$$QBER = \frac{N_{wrong}}{N_{sifted}}. \tag{3.1}$$

Errors in the exchanged bit string can either be caused by imperfections in the preparation, transmission and detection of the signals or by the presence of an eavesdropper (see Section 2.1.2). In the security analysis, all errors are pessimistically attributed to this attacker Eve and thus, the QBER is a measure for the amount of information on the key an eavesdropper may maximally have. During the error correction step (see Section 3.3.5), the sifted keys of Alice and Bob are compared and erroneous bits are discarded. This yields the number of incorrect bits and thus the QBER, but during the process, more than only the false bits are exchanged and hence need to be discarded. The efficiency of the error correction algorithm is quantified by a factor $f_{EC} \geq 1$, where $f_{EC} = 1$ is the Shannon limit. The QBER accessed this way is then used to delete all the information Eve may have on the sifted and corrected key during privacy amplification (see Section 3.3.5). After Alice and Bob discard all the wrong bits in the sifted keys and delete the information of a potential eavesdropper, they end up with the extracted *secure key*. An upper bound on the secure key rate is given in [29]:

$$R_{sec,max} = R_{sift} \times max[1 - (f_{EC} + 1)H_2(E), 0], \tag{3.2}$$

with R_{sift} being the sifted key rate, i.e. the number of sifted bits multiplied by the repetition frequency of the source and divided by the number of sent bits N, and $H_2(E)$ as the binary Shannon entropy of $E \equiv$ QBER giving an estimate on the amount of key information accessible to an attacker,

$$H_2(E) = -E\log_2(E) - (1 - E)\log_2(1 - E). \tag{3.3}$$

The maximum tolerable QBER can be found by calculating the point where equation 3.2 drops to zero, yielding $E_{max} \approx 11\%$.

[1] There exist efficient implementations of the BB84 protocol, where an asymmetric basis choice is implemented, leading to a higher probability for a matching choice of basis [28].

3.3.2 SARG04

One problem for the security of the BB84 protocol is, that its original concept demands the use of single photons in the quantum communication process, as multiphoton pulses offer possibilities for an eavesdropper (see Section 3.4) to compromise the key exchange. As an alternative robust against these kinds of attacks, Scarani et al. [30] proposed a new protocol identical to BB84 on the quantum level, but with important differences in the sifting procedure. Using the B_X and B_Y basis from the BB84 protocol and renaming the states $|H/V\rangle \equiv |\pm x\rangle$ and $|P/M\rangle \equiv |\pm y\rangle$, the sifting goes as follows:

- Alice and Bob agree on the encoding $|\pm x\rangle \,\widehat{=} 0$ and $|\pm y\rangle \,\widehat{=} 1$.

- For each sent bit, Alice announces one the four pairs of a state of basis B_X and B_Y, $\{|+x\rangle, |+y\rangle\}, \{|+x\rangle, |-y\rangle\}$, $\{|-x\rangle, |+y\rangle\}$ and $\{|-x\rangle, |-y\rangle\}$, over the public channel, including the polarization of the prepared photon; the overlap between the two states of any pair is $1/\sqrt{2}$.

- Bob's random choice of measurement basis can either yield a conclusive or inconclusive result, illustrated with an example: Consider that Alice has prepared an $|+x\rangle$ photon and announced the set $\{|+x\rangle, |+y\rangle\}$. If Bob measures in the B_X basis, he will certainly obtain the result $|+x\rangle$; as this could mean that Alice has prepared either $|+x\rangle$ or $|+y\rangle$, he discards these cases, occuring with a probability of 50%, as inconclusive. In the cases where Bob chose to measure in the B_Y basis, he will get the results $|+y\rangle$ and $|-y\rangle$ with equal probability, but again the $|+y\rangle$ could have been generated by both of the states in the announced pair and is discarded. In this example, measurement in the B_Y basis, only the result $|-y\rangle$ is conclusive for Bob and tells him, that Alice has prepared $|+x\rangle$, giving the bit value 0.

With this sifting procedure, Eve will not be able to gain precise knowledge of the key bit from pulses with a single photon detected, nor from such with two photons detected. In order to employ a successful PNS attack (see Section 3.4.1), Eve can thus only use pulses containing three or more photons, making it applicable only in high loss regimes and thus extending the maximum tolerable loss.

3.3.3 DPS

The differential-phase-shift (DPS) scheme uses the relative phase between two sequential photon pulses to encode the key bits. In the original proposal [31], Inoue et al. described a sender device splitting a photon into three identical probability amplitudes separated by a time delay T. Alice modulates the phase difference between two sequential pulses by 0 or $\pm\pi$, encoding bit value 0 with $\Delta\phi = 0$ and 1 with $\Delta\phi = \pm\pi$. The detection on Bob's side is based on an interferometer with a time delay of T between its two paths. The setup for sender and receiver in this scheme is shown in Figure 3.3.

As it is shown in the lower right corner of Figure 3.3, this setup gives rise to four possible detection time instances at Bob's detectors. At time (ii), the pulse taking path a in Alice and the long path in Bob interferes with the one taking path b in the sender and the short one in the receiver interferometer. Similarly, for time instance (iii), interference between the probability amplitudes of path b with the long and c with the short path in Bob occurs. Bob's interferometer is adjusted in a way that detector 1 counts a signal for a phase difference of

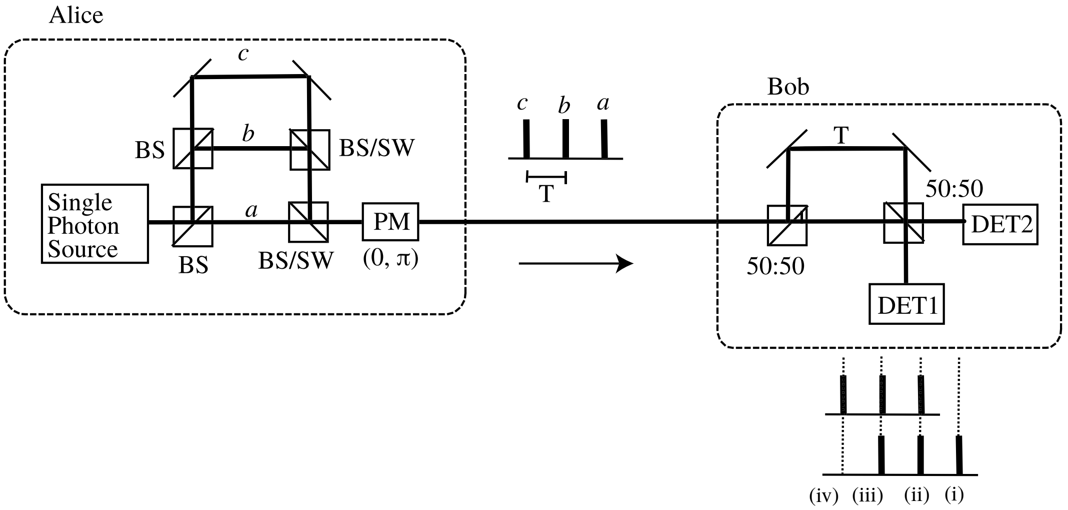

Figure 3.3: Setup of sender and receiver for the DPS protocol. BS: beam splitter, PM: phase modulator, SW: switch, DET: photon detector. A single photon is split into three parts with identical probability amplitudes by two beam splitters and the phases of the different pulses, delayed by T, are modulated. At the receiver, the puls train is split again into two arms of an interferometer with a delay T between the paths. Taken from [31]

the sequential pulses of $\Delta\phi = 0$ and detector 2 for $\Delta\phi = \pm\pi$. Whenever Bob measures a detector click at one of these two time instances, he notes the time and the number of the detector. He then tells Alice the time instances of the interfering cases, from which Alice knows, with her phase modulation information, which of Bob's detectors clicked. As they agreed to encode the bits in a specific way, Alice and Bob now have an identical string of bits and as only timing information has been shared, no bit information is leaked.

3.3.4 COW

The three protocols presented so far use the polarization and phase of photons, respectively, to transmit the bit information. Another approach is to use the arrival time of weak coherent pulses as data carrier, as it is done in the coherent one-way protocol [32]. Here, two-pulse sequences emitted by a weak coherent laser source with mean photon number μ are used to encode the key bits 0 and 1. The k-th bit is encoded with the two-pulse sequences

$$|0_k\rangle = |\sqrt{\mu}\rangle_{2k-1}\,|0\rangle_{2k} \text{ and} \tag{3.4}$$

$$|1_k\rangle = |0\rangle_{2k-1}\,|\sqrt{\mu}\rangle_{2k}\,. \tag{3.5}$$

Thus, bit value 0 is prepared as a pulse with intensity μ followed by an empty (or vacuum) pulse, while this order is reversed for bit value 1. Of course, the information if a pulse is empty or not could easily be obtained by an eavesdropper, hence checking the integrity of the communication needs to be done another way. This is ensured by exploiting the coherence of the laser source, which introduces a well-defined phase difference between any two consecutive non-empty pulses [32] that is being monitored with an interferometer setup in the detector

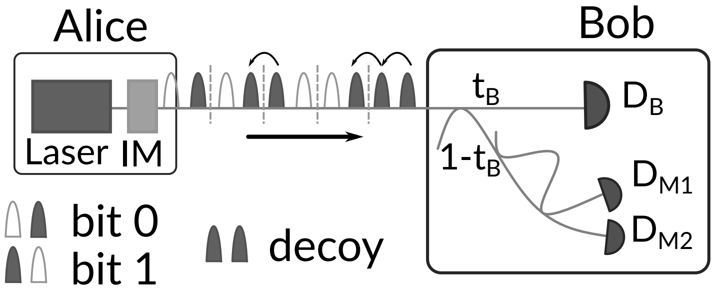

Figure 3.4: Schematic fibre based setup for sender and receiver in the COW scheme. IM: intensity modulator, D: detector. Alice randomly sends the pulse pairs "1", "0" and "decoy". In Bob's receiver, the incoming pulses are divided at an unbalanced $t_B : (1 - t_B)$ beamsplitter. The fraction t_B is detected with detector D_B on the data line, while the other fraction is, with a fibre interferometer, analyzed in the monitoring line for coherence. Arrows over the pulses indicate coherence for $\Delta\phi$. Adapted from [32].

system. If one only uses the states $|0_k\rangle$ and $|1_k\rangle$, this kind of two-pulse pair occurs for 1-0 bit sequences. To further check for coherence, so called *decoy sequences*[2]

$$|d_\mu\rangle = |\sqrt{\mu/2}\rangle_{2k-1}\,|\sqrt{\mu/2}\rangle_{2k} \tag{3.6}$$

are produced as a small fraction of the sent pulses. This decoy state is a superposition of the signal states (that can be seen as the eigenstates of the B_Z basis) and thus resembles one eigenstate of the B_Y basis. The integrity of the key exchange can be granted, as the coherence checked on the monitoring line is distributed not only across a bit separation (e.g. 1-0 bit sequence), but also within a two-pulse (decoy) sequence, through which PNS (also called zero-error) attacks can be detected. The reason for this is, that the superposition state $|d_\mu\rangle$ would lead to Eve introducing errors (see Section 2.1.2) when trying to employ this kind of attack.

The principle of coherence detection and data measurement on Bob's side is illustrated in Figure 3.4.

3.3.5 Basics of key-extraction

After the key bits are exchanged and the sifting is done, further classical post processing steps are required to distill the secret key. The first task is to correct the errors that are present in the keys of Alice and Bob. As already mentioned, the reasons for the errors can be imperfect preparation of the sent states, dark and background counts in Bob's detectors or the presence of an eavesdropper, intercepting the quantum communication. For the correction of these, an error correction algorithm (e.g. Cascade [33], LDPC [34]) locates and discards all the uncorrelated bits in Alice's and Bob's strings.

Once all erroneous bits are discarded from the key, the so called privacy amplification phase is performed. As Eve may have some information on the sifted and error corrected key, known to Alice and Bob as a measure of the QBER, security demands to delete this knowledge; for this purpose, universal hashing, reducing the key to R_{sec} from equation 3.2, is used [35].

[2] The principle of decoy states as a possibility to access some security parameters is introduced in Section 3.4.2

3.4 Eavesdropping attacks on imperfect implementations

3.4.1 Photon number splitting attack

The key rate analysis in Section 3.3.1 was done for a theoretically ideal implementation of the BB84 protocol with a perfect single photon source [36]. Due to the impracticality of single photon sources, most practical devices use attenuated lasers emitting so called weak coherent pulses (WCP). Due to the Poissonian statistics that these are governed by, the probability for a pulse with average photon number μ to contain n photons is

$$P_\mu(n) = \frac{\mu^n}{n!} e^{-\mu}. \tag{3.7}$$

This means that even if one chooses a mean intensity $\mu \ll 1$, there is a non-zero probability for a pulse to contain multiple photons (see Figure 3.5). If this is the case for a QKD pulse sent by Alice, an eavesdropper could employ the so called photon number splitting (PNS) attack [37, 38, 39]:

- Eve determines the number of photons in a pulse.
- Eve blocks all the pulses containing exactly one photon.
- From all multiphoton pulses she stores one photon and sends the remaining to Bob.
- After Alice and Bob exchanged their basis choice information during the sifting phase, Eve knows in which basis to measure her stored photon and can obtain all the key bits without introducing any error in the bit strings of Alice and Bob.

As we assume an all-powerful attacker Eve, having access to a lossless quantum channel, the limit for the applicability of this attack is given by $P_\mu(n > 1) > \eta P_\mu(n = 1)$ with the channel transmission η. This gives a threshold for the loss above which Eve can block all of the single photons without reducing the overall count rate. An overall transmission η where this inequality is not fulfilled forces Eve to reduce the number of her attacks accordingly.

To assess this problem, Gottesman et al. [29] extended equation 3.2 to give an upper bound of the secure key rate for devices using WCPs:

$$R_{sec,GLLP} = R_{sift} \times max\left[(1-\Delta) - f_{EC}(E)H_2(E) - (1-\Delta)H_2\Big(\frac{E}{1-\Delta}\Big), 0\right], \tag{3.8}$$

Here, $f_{EC}(E)$ is a factor quantifying the efficiency of the error correction ($f_{EC} \geq 1$, also see equation 3.2) and Δ is what they call the fraction of *tagged* bits. *Tagged* bits are the bits coming from multi-photon pulses emitted by Alice, enabling Eve to use the PNS attack, and the Δ is calculated as the probability of the occurence of such a pulse over the entire detection probability at Bob's detectors,

$$\Delta = \frac{P_\mu(n > 1)}{\eta P_\mu(n > 0)}, \tag{3.9}$$

where the overall transmission is the product of channel and receiver transmission, T_{chan} and T_{Bob}, with the efficiency of Bob's detectors η_D

$$\eta = T_{chan} \cdot T_{Bob} \cdot \eta_D. \tag{3.10}$$

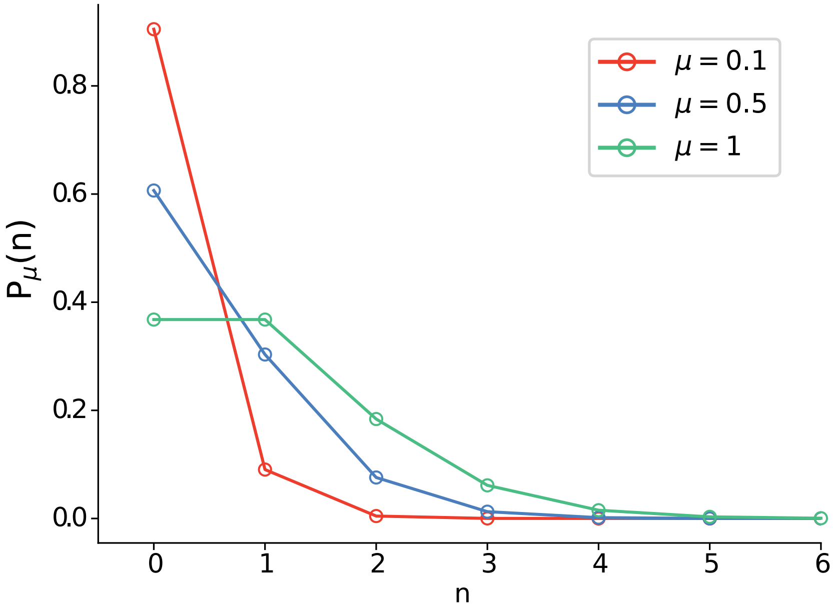

Figure 3.5: Poisson distribution for $\mu = 0.1, 0.5$ and 1.0.

Using the GLLP formula (3.8) to calculate the secure key rate, it is possible to extract a secure key from an exchange done using attenuated lasers, but the scaling of the key rate with the transmission is $\sim e^{2\log_{10}(\eta)}$. The consideration of PNS attacks in the security analysis of the BB84 protocol thus offers a solution for a key exchange with WCP sources, but it comes at the cost of reduced key rate and maximum tolerable loss.

3.4.2 Decoy extension of protocols as a countermeasure

Equation 3.8 allows to extract a secure key out of pulses exchanged with imperfect sources, but it severly limits the maximal usable mean photon number μ and the maximum tolerable loss. The former of those leads to lower key rates, as a large fraction of the pulses sent by Alice will be empty, while the latter puts a limit on the achievable link distance. As an alternative countermeasure for PNS attacks, the method of so called *decoy states* has been proposed by Hwang, Wang, Lo et al. [40, 41, 42].

The robustness of the decoy state method relies on the following idea: If Alice not only sends her signal pulses with intensity μ, but also randomly sends pulses with lower mean photon number $\nu < \mu$, a PNS attack by Eve will affect the photon number statistics of the two kinds of pulses differently, revealing a potential PNS attack. The non-orthogonality of coherent states $|\mu\rangle$ and $|\nu\rangle$ forbids Eve to distinguish between them before starting the PNS attack on a pulse, making it impossible to apply the attack only on the signal pulses. This allows Alice to send pulses with higher average intensity, leading to overall higher achievable secure key rates, and leads to a scaling of R_{sec} with the transmission similar to the ideal single photon case[3]. The result of this are greatly improved secure key rates and achievable link distances, as compared to the GLLP results, still without having to deal with impractical single photon sources.

[3] $R_{sec,single} \sim e^{\log_{10}(\eta)}, R_{sec,decoy} \sim e^{\log_{10}(\eta)}, R_{sec,GLLP} \sim e^{2\log_{10}(\eta)}$

In the following, a lower bound on the secure key rate is presented following the calculations and notation of Ma et al. [43] using the two decoy state protocol.

The pulses emitted by the WCP source may contain, in principle, any number of photons i. The probability, that an i-photon state is registered by Bob is given by

$$\eta_i = 1 - (1-\eta)^i, \tag{3.11}$$

with the overall transmission η from equation 3.10. An i-photon state sent by Alice leads to a detection event in the receiver with a probability

$$Y_i = Y_0 + (1 - Y_0)\eta_i. \tag{3.12}$$

This i-photon *yield* Y_i is comprised of the detectors' dark and background count rate Y_0 and the transmittance η_i. The probability that a bit of information is transmitted by an i-photon state is given by the product of Alice's probability to send that state (see equation 3.7) and Bob to detect it. This is called the i-photon *gain*

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}. \tag{3.13}$$

For a pulse with mean photon number μ, the *overall gain* is the sum over all possible gains Q_i

$$Q_\mu = \sum_{i=0}^{\infty} Q_i = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + (1 - Y_0)(1 - e^{-\eta\mu}). \tag{3.14}$$

These quantities of the quantum channel enter the lower bound of the secure key rate that is presented in [43]:

$$R_{sec,decoy} \geq q\Big[- Q_\mu f_{EC}(E_\mu) H_2(E_\mu) + Q_1(1 - H_2(e_1))\Big]. \tag{3.15}$$

E_μ is the average QBER of the signal and e_1 the one of the pulses containing a single photon, H_2 the binary Shannon entropy (see equation 3.3). The factor $q = q_{eff} \times f_{rep} \times p_\mu$ depends on the experimental implementation, with p_μ the probability that a signal pulse with intensity μ is sent, f_{rep} the repetition frequency of the source and q_{eff} an efficiency factor for the basis choice ($q_{eff} = \frac{1}{2}$ for the symmetric basis choice in BB84).

The different terms in equation 3.15 have the following functions: After the sifting (q), all the errors that are present in the exchanged bitstring need to be corrected and the information contained within them is therefore deleted ($-Q_\mu f_{EC}(E_\mu)H_2(E_\mu)$). Depending on the used error correction algorithm, this happens with a certain efficiency $f_{EC} \geq 1$, i.e. not only the erroneous bits are exchanged and hence discarded. The provably secure key can only be generated from the information gained from single photon pulses (Q_1); due to single photon errors e_1, Eve may still have some information on these bits and this has to be reduced to $I_{Eve} = 0$, which is done in the privacy amplification step ($-Q_1 H_2(e_1)$).

The equation for the lower bound on the secure key rate (3.15) makes use of the single photon gain and QBER, Q_1 and e_1, respectively. The loss of photons during transmission through the quantum channel as well as an error being due to a single photon pulse are probabilistic processes that can not be measured but have to be bounded from above and below by the measurement of other properties. One solution for this problem was presented by Ma et al. [43]: they use the measurable data of signal and decoy gain, Q_μ and Q_ν, and

QBER to calculate a lower bound on the single photon gain and an upper bound on the respective QBER for the example of a two decoy state implementation[4]:

$$Q_1 \leq Q_1^L = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\Big(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\Big) \tag{3.16}$$

$$e_1 \geq e_1^U = \frac{E_\nu Q_\nu e^\nu - \frac{1}{2} Y_0}{Y_1^L \nu} \tag{3.17}$$

According to equation 3.13, the lower bound on the single photon yield entering the calculation of e_1^U is $Y_1^L = Q_1^L \frac{e^\mu}{\mu}$.

By bounding the single photon pulse parameters Q_1 and e_1 from below and above, respectively, it is possible to achieve the previously described scaling of R_{sec} for WCP source QKD with the channel loss similar to the ideal single photon case, being a great improvement compared to the earlier security analyses for these kinds of sources.

3.4.3 Side channels

A key exchange with the techniques presented so far is unconditionally secure in theory, but any slight imperfections of the devices used in a real implementation may compromise this security, as they open so called side channels through which an eavesdropper could gain information on the key without being noticed. If, for example, the DoF used to encode the key bits is correlated to another DoF of the photons, a measurement of the second DoF (which thus acts as a quantum non-demolition (QND) measurement of the first DoF) could reveal the bit information without influencing the original one, and thus no error in Bob's measurement is introduced. Also exploitable by Eve are imperfections on the receiver side of the quantum communication, where attacks taking advantage of a detection efficiency mismatch [44], the detector dead time [45], a spatial mode side channel [46] or the blinding of the detectors [47] have been successfully shown.

3.5 Performance estimation for compact high-altitude QKD platforms

If one wants to know the achievable performance of a QKD setup, the secure key rate equations for different protocols with the specific system parameters have to be calculated. Firstly, this will tell the user if the system in question is principally able to grant a secure key exchange under the channel parameters present. Secondly, the different existing QKD protocols offer different performances and loss dependencies in certain regimes, which might make a protocol favourable for high link losses, while it performs not as good in regions of high transmission.

Our group is, apart from the short distance hand-held key exchange [20], especially interested in the implementation of a QKD sender device on an airborne or space-bound platform. A few years ago, a successful aircraft to ground QKD transmission [48] has been shown in our group. Taking this free-space link further, the possibilities for an implementation of a compact QKD sender unit within a flying high-altitude platform (HAP) are studied. The big advantage of a HAP for a key exchange lies in the so called *trusted node* configuration.

[4] i.e. the two decoy intensities are the vacuum intensity 0 and the weak decoy state with $\nu < \mu$

For this, the HAP exchanges secure keys with two ground stations, possibly separated by hundreds of kilometers, it passes on its flight, by which a secure key shared between the two ground stations can be generated.

In general, the achievable key rate of a QKD system is accessed by evaluating key rate formulas like 3.15. Within this section of my work, the results of this estimations for five different protocols, namely single photon and decoy state BB84, SARG04, DPS and COW, are presented (see Figure 3.6). We know the parameters of the chosen implementation, i.e., the properties of the used superconducting single photon detectors like dead-time, efficiency and dark count rate, and general numbers like repetition frequency and background radiation (see Table 3.2), allowing to calculate the resulting key rates. The average photon number μ of the used WCPs has to be optimized for every loss value, as it enters the different terms of the key rate formulas, leading to a varying optimal value over the loss region.

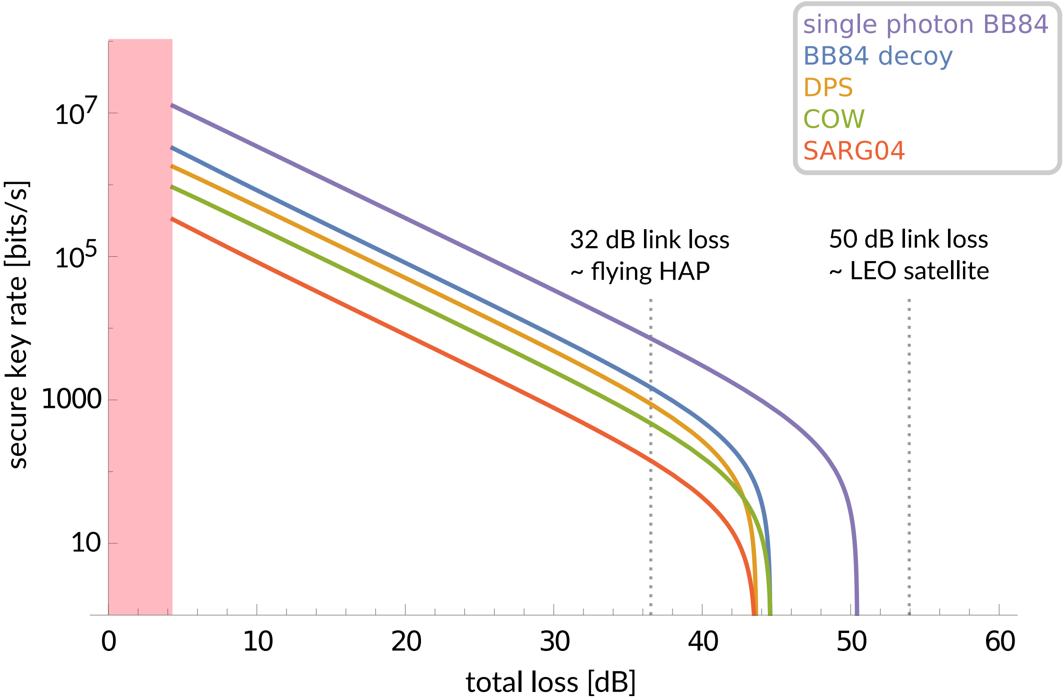

Figure 3.6: Estimations for the achievable secure key rate as a function of the total loss for different QKD protocols. The red area is the amount of loss that is due to detector efficiencies, present even for a lossless link. The two vertical lines mark estimated link losses for a flying high-altitude platform (HAP) and a low earth orbit (LEO) satellite, respectively.

The curves in Figure 3.6 show, that out of all practical protocols (excluding single photon BB84), BB84 with decoy states performs best in terms of both achievable key rate and maximum tolerable loss. For overall losses up to about 40 dB, all five curves show the same linear scaling (on the logarithmic scale) with increasing loss. For higher loss values, the key rate curves of the different protocols at some point drop drastically, marking where the estimated QBER reaches a point at which error correction and privacy amplification do not allow to extract a secure key anymore (see discussion of equation 3.3).

What needs to also be kept in mind is that COW and DPS were developed and proposed

detector efficiency	0.90
detector dark count rate	50 Hz
detector dead-time	10 ns
background count rate @ 850 nm	500 Hz
intrinsic QBER	0.02
coupling efficiency in the receiver	0.40

Table 3.2: Model parameters for the key rate estimations of Figure 3.6.

for fiber based systems, as phase encoding is more practical than the use of polarization in this case; as the interferometric evaluation of pulse pairs has the demand of single-mode photons, the use of (partly) phase based protocols like COW and DPS is challenging for free space implementations, where adaptive optics would need to transform the wavefronts of the impinging photons back to the single-mode regime, in order to avoid single-mode coupling losses. For DPS and COW, it can be seen, that for losses $\lesssim$ 42 dB, DPS has a higher achievable key rate, while for higher losses, COW performs better and reaches a higher maximum tolerable loss identical to BB84 with decoy states.

As the implementation of a QKD sender unit on a HAP is one of the ongoing developments in our group, performance estimations for the specific loss regions of the chosen platform need to be given. One key difference between free-space and fibre-based QKD systems is the scaling of loss with link distance, quadratic for the former and exponential for the latter. Apart from losses due to atmospheric turbulences (quantified by the *Fried parameter*) and absorption, one main source of loss for long distance free-space QKD links will be the geometric loss, depending on the beam divergence of the transmitter optics. For the model of an example HAP flying at an altitude of roughly 15 km, the overall link loss can be estimated with 32 dB[5]. Besides the named losses, this also contains, amongst other parameters, imperfections of telescope mirrors and propagation losses within the atmosphere. The expected loss of this kind of flying HAP would allow for a maximum secure key rate of $\sim 10^3$ bit/s with the decoy extension of the BB84 protocol implemented (see Figure 3.6) and lower rates for the other (practical) schemes. If one wants to take the free-space link further and use a CubeSat in a low earth orbit (LEO, altitude $\approx$ 500 km), the estimated link loss can be calculated from the flying HAP case. To extrapolate the total loss for a LEO satellite, the ratios of the used system parameters beam divergence (assumed for a 20 mm sender aperture in both cases), link distance and receiver telescope size (collected in Table 3.3) have to be taken into account. This leads to an expected satellite link loss of

$$L_{sat} = 32dB - \log_{10}\Big[(\frac{57\mu rad}{70\mu rad})^2 \cdot (\frac{30km}{500km})^2 \cdot (\frac{80cm}{60cm})^2\Big] \cdot 10dB \approx 55.7dB. \tag{3.18}$$

As the flying HAP system still had some room for improvement, especially in the receiver telescope mirror losses for light in our wavelength regime $\lambda = 850$ nm, this estimate is too pessimistic. Optimizing the sender and receiver for 850 nm, the link loss in the final CubeSat implementation may be reduced by around 6 dB, leading to an approximate link loss of $L_{sat} = 50$ dB as marked in Figure 3.6. It can be clearly seen, that the resulting total loss (link loss + receiver system losses) would not enable the user to obtain a secure key exchange,

[5] Private correspondence with Florian Moll, DLR Oberpfaffenhofen. The sender aperture on the HAP used for the simulation is 20 mm, while the ground station has a 60 cm receiver telescope.

	flying HAP	LEO satellite
beam divergence	57 μrad	70 μrad
link distance	30 km	500 km
receiver telescope diameter	60 cm	80 cm

Table 3.3: System parameters for the flying HAP and a LEO satellite.

not even in the theoretic single photon case. In order to generate a secure key, the overall loss would have to be reduced by roughly one order of magnitude, e.g., with a larger aperture in the satellite.

In addition to the system parameters, calculations of the key rate need an estimate of the QBER during operation at different link losses. The error ratio is influenced by the probability e_0 that a dark or background count leads to a wrong bit value; as these are random processes, the probability turns out to be $e_0 = \frac{1}{2}$. Second, the error intrinsic in the preparation and detection setup enters the overall QBER, resulting in the following equation from [43]:

$$E_\mu Q_\mu = e_0 Y_0 + e_{int}(1 - e^{-\eta\mu}). \tag{3.19}$$

Using this estimate, the equations for the protocols described in this work and shown in Figure 3.6 are summarized in the following:

- The blue curve for the decoy extension of the BB84 protocol is calculated with equation 3.15, using and additional dead-time correction factor c_{DT}, the model parameters and an optimized signal intensity μ for every loss value.

- For the ideal single photon BB84, the calculation in principle uses the same equation, but because of the perfect single photon pulses, it reduces to

  $$R_{sec,single} = c_{DT} \cdot q\Big[- Q_1 f_{EC}(E_1) H_2(E_1) + Q_1(1 - H_2(E_1))\Big], \tag{3.20}$$

  as the measured gain and QBER already are the values for the single photon case.

- As it is mentioned in the presentation of the four protocols used for the key rate estimations, the SARG04 scheme has a higher level of robustness against PNS attacks than BB84 (see Section 3.3.2) and enables the users to also distill the secure key bits from two-photon pulses. Employing this idea and combining the GLLP results with the decoy state extension, Fung et al. [49] state the secure key rate of the SARG04 protocol as

  $$\begin{aligned} R_{sec,SARG04} = c_{DT} \cdot \frac{1}{4} \cdot f_{rep} \cdot p_\mu \Bigg[& - Q_\mu f_{EC}(E_\mu) H_2(E_\mu) + \\ & + Q_1\Big[1 - H(Z_1|X_1)\Big] + Q_2\Big[1 - H(Z_2|X_2)\Big]\Bigg]. \end{aligned} \tag{3.21}$$

  Z_i and X_i are the phase and bit errors for i-photon pulses, respectively, and $H(Z_i|X_i)$ is the conditional entropy of the phase error given a certain bit error. The factor $\frac{1}{4}$ is due to the SARG04 sifting process, where only a fourth of the detection events leads to a conclusive result. This key rate formula was used for a practical implementation by Liu et al. [50], where they also give the necessary equations for a numerical simulation of the possible key rates.

- In the case of the DPS scheme, the formulation of the secure key rate given in [51] is adapted:
$$R_{sec,DPS} = f_{rep} \cdot Q_\mu \cdot c_{DT} \Big[\tau - f_{EC}(E_\mu) H_2(E_\mu) \Big], \tag{3.22}$$
where τ quantifies the fraction of bits discarded in the privacy amplification step,
$$\tau = -(1-2\mu)\log_2(1 - E_\mu^2 - (1-6E_\mu)^2/2). \tag{3.23}$$

- The concept of the COW protocol is translated into a key rate equation following the notation of [52] and especially the formulation in the supplementary material of [53]. They state the secure key rate of a COW key exchange as
$$R_{sec,COW} = t_B \cdot f_{rep} \cdot Q_\mu \cdot c_{DT} \Big[1 - E_\mu - (1-E_\mu) H_2(\frac{1-\xi}{2}) - f_{EC}(E_\mu) H_2(E_\mu) \Big], \tag{3.24}$$
with
$$\xi = (2V-1)e^{-\mu} - 2\sqrt{V(1-V)(1-e^{-2\mu})} \tag{3.25}$$
and the interference visibility V. t_B is, as introduced in Section 3.3.4, the fraction going through Bob's data line.

Chapter 4

Current state of the experimental QKD setup

The current QKD sender module was largely developed and built during the Ph.D. thesis of Gwenaelle Vest, with the aim of miniaturizing a QKD sender unit suitable for polarization encoded BB84-like protocol implementation. The following chapter, which summarizes the most important aspects of the driving electronics, the used microoptical components and the achieved results, mainly follows the Ph.D. thesis [54] and the Master's thesis by Peter Freiwang [55].

4.1 Sender Optics

The miniaturized sender consists of an array of vertical-cavity surface-emitting laser diodes (VCSELs) at 850 nm, a micro-lense array, sub-millimeter sized wiregrid polarizers as well as a femtosecond laser written waveguide circuit used for overlapping the pulses from the four VCSELs. Finally, the QKD pulses are overlapped with a bright beacon laser at 680 nm. An overview of this sender unit, having an overall volume of $35 \times 20 \times 8\ mm^3$, is shown in Figure 4.1.

4.1.1 VCSEL array

The weak coherent pulses (WCP) are produced by VCSELs [57], which consist of an active medium (direct bandgap semiconductor), placed within an optical cavity made from two distributed Bragg reflectors (DBRs). These DBRs are nano-fabricated from alternating layers with different refractive indices, in our case AlAs and GaAs, with thicknesses of one quarter of the wavelength. If the VCSEL is eletrically pumped, the carrier injection leads to a population inversion which in turn causes stimulated radiative recombination of electron-hole pairs. The contacts for this current supply are placed on both sides of the cavity.

Here, an array of twelve (single-mode) VCSELs, emitting photons at a wavelength of $\lambda = 850$nm and separated by a distance (pitch) of 250μm, are used. Four neighbouring ones are electrically connected to four different driver electronics. Operating the diodes in continuous-wave (CW) mode, the emitted light shows a high DOP of above 90% within the entire specified current region; if, on the other hand, the VCSELs are modulated with electrical pulses in the sub-nanosecond regime, the DOP almost vanishes, being one order of

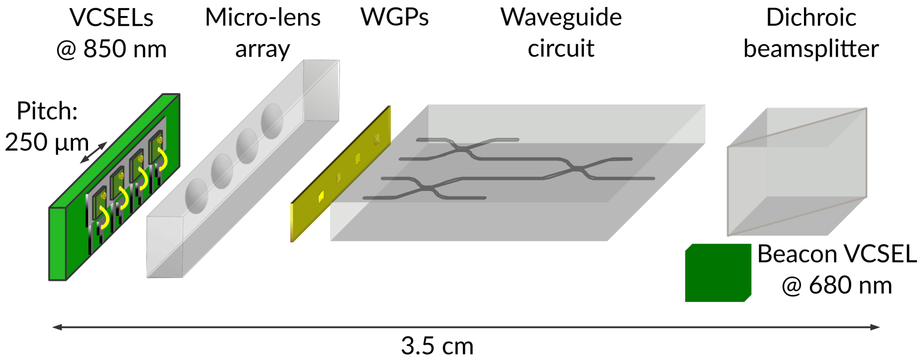

Figure 4.1: Overview of the micro-optical components, namely four VCSEL diodes separated by 250μm, followed by arrays of micro-lenses and wire-grid polarizers, as well as a waveguide chip. The chip's output signal is overlapped with a beacon laser at a dichroic beamsplitter. In addition to that, the handheld module also employs a collimation lens, attached to the beam splitter. Adapted from [56].

magnitude lower. As we want to obtain very short optical pulses, allowing for narrow time-filtering of the received signals, the VCSELs (supported modulation frequency up to 28 GHz) are driven with short pulses of about 100-200 ps at 100 MHz repetition frequency yielding the desired sub-nanosecond optical pulses. Thereby we can make use of this low DOP and set the four different linear polarizations necessary for BB84-like polarization encoding by inserting polarizers after the diodes.

4.1.2 Wire-grid polarizers

As can be seen in Figure 4.1, the polarization of the VCSEL pulses is set by an array of four wire-grid polarizers (WGPs) [54, 56, 58], having the same pitch as the VCSELs. The polarization dependent transmission of a WGP is based on its distinctive effect on differently polarized incoming light fields, namely a high transmission of light polarized orthogonal to the grid's stripes (transversal magnetic, TM) and strong reflection of light with perpendicular polarization (transversal electric, TE). The TM transmission is caused by plasmonic excitation in combination with a waveguiding effect of the slits, while TE waves are exponentially decaying within the depth of the grid for wavelengths above $\lambda_c \approx 2w$, where w is the width of the slits [54].

The decision for wire-grid micro-polarizers was made, because there exist standard processing techniques allowing to produce them in the needed size and transmission orientation. The method of choice in our group was to first use physical vapour deposition to obtain a 265 nm thick gold layer on glass substrate; in this metal layer, a focused ion beam (FIB) can write the slit structure with the necessary slit width and rotation (see Figure 4.2). Finding the optimal grid parameters, namely the thickness of the gold layer, the width of the slits and the slit period, is a non-trivial task and is done by Finite-Difference Time-Domain (FDTD) simulations, allowing to produce WGPs, which offer extinction ratios well exceeding 1:1000 and a transmission of 9%.

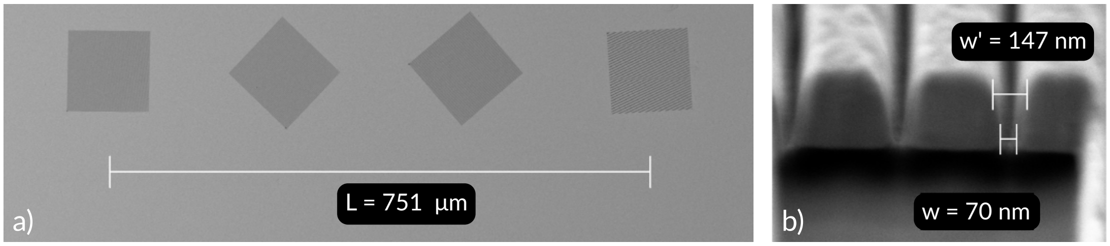

Figure 4.2: (a) Array of four 120 μm × 120 μm WGPs,with a pitch of 250 μm. The relative rotations of the polarizers are designed to compensate for the polarization rotation due to the waveguide's birefringence. (b) Close-up of the grid. The slit width decreases from 147 μm at the top to 70 μm at the bottom. Both scanning electron microscope images are taken from [54].

4.1.3 Waveguide circuit

The combination of the VCSELs and the WGPs produces laser pulses with a well defined linear polarization. For a secure QKD process, it is also obligatory to spatially overlap the four beams in such a way that the resulting beam offers no possibility to distinguish the four different sources. This is achieved by the implementation of a waveguide circuit that merges four input modes into one single output, as it is shown in Figure 4.3. The circuit in use is produced by the Group of Dr. R. Osellame at the Politecnico di Milano, Italy, via femtosecond laser writing. By irradiating a glass substrate with a tightly focused femtosecond-pulsed laser and moving the focus, the refractive index of the material is changed along the path of the focus ($\Delta n = 7 \times 10^{-5}$), which leads to waveguiding properties similar to glass fibres. By this process, single-mode waveguides with almost any desired geometry can be produced. If one brings two waveguides in close proximity on the order of the guided mode size (a few micrometers), the wave in one waveguide will evanescently couple to the other one, and vice versa, with the coupling ratio depending on the length of the interaction region [25].

In order to reduce the polarization dependence of these directional couplers in our waveguide chip, the waveguides do not lie within a horizontal plane, but are routed in a 3D geometry, allowing for a 50:50 splitting ratio for H- and V-polarized light at all three couplers. Despite careful manufacturing, small amounts of stress on the waveguides in the 3D structure lead to path-dependent phase shifts of the light propagating from the four inputs to the main output. This, however, can be compensated by coupling slightly rotated (relative to the standard BB84 polarization angles) polarization states into the waveguide chip, which is visible in the SEM picture of the WGP array in Figure 4.2 (a). The coupling is achieved by an array of four microlenses placed between the VCSELs and the polarizer array. The 50:50 couplers ensure that one fourth of the intensity from each input is guided to the main output with a propagation loss of only 0.5 dB/cm.

4.1.4 Quality of the state preparation by the sender module

The polarization properties of the short optical pulses emitted by the sender optics are investigated with a QST measurement, as it is introduced in section 2.2. The setup for this

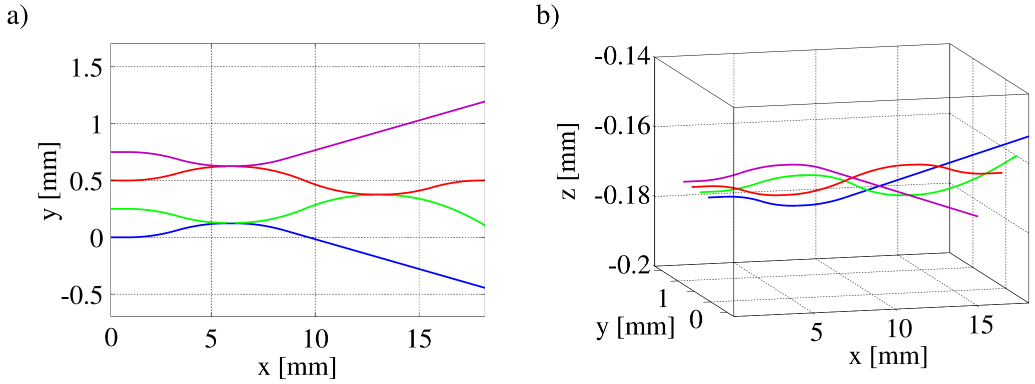

Figure 4.3: (a) Top and (b) perspective view of the four waveguides written into the glass substrate of the waveguide chip. (a) shows the interaction zones, where evanescent coupling between adjacent waveguides happens. In combination with the employed 3D structure, as seen in (b), this allows for almost entirely polarization independent splitting ratios at the three couplers, resulting in one quarter of the intensity at every input being guided to the single output used for QKD (red). Both pictures taken from [56].

theoretic output	V	M	P	H
measured Stokes components	$\begin{pmatrix}-0.9090(6)\\0.248(1)\\-0.295(1)\end{pmatrix}$	$\begin{pmatrix}-0.358(1)\\-0.9156(4)\\0.085(1)\end{pmatrix}$	$\begin{pmatrix}0.091(1)\\0.9730(3)\\-0.066(1)\end{pmatrix}$	$\begin{pmatrix}0.9460(5)\\-0.291(1)\\0.070(1)\end{pmatrix}$
DOP	0.9968(7)	0.9867(6)	0.9795(3)	0.9922 (6)
QBER	4.55(3)%	4.22(2)%	1.35(1)%	2.70(2)%

Table 4.1: Vectors of the Stokes components $(S_1\ S_2\ S_3)^\intercal$ of the four output states of the Alice module, measured via a QST, with the DOP and the QBER of the single states. The QBER averages to $3.21 \pm 0.01\%$. Data taken from [55].

measurement, slightly differing from the general one as an APD was used in this case, is shown in Figure 4.4. The results for measurements of the four output states are shown in Table 4.1. The individual QBER of the four output states is calculated in the Stokes formalism as:

$$QBER_H = \frac{1-S_1}{2} \tag{4.1}$$

$$QBER_V = \frac{1+S_1}{2} \tag{4.2}$$

$$QBER_P = \frac{1-S_2}{2} \tag{4.3}$$

$$QBER_M = \frac{1+S_2}{2} \tag{4.4}$$

The measured average QBER would be sufficient for a BB84 key exchange, but reducing it would benefit the maximally achievable secure key rate. In the handheld operation this was done by a compensation within the receiver via application of a global unitary rotation, resulting in an average QBER of 1.48%.

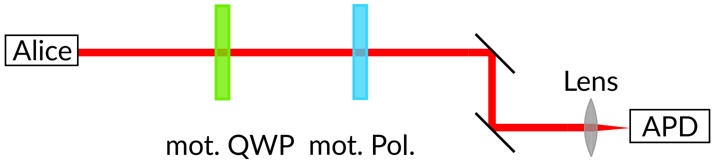

Figure 4.4: Experimental setup for the QST performed on the handheld Alice module. The motorized components, namely the QWP and the polarizer, are moved according to Table 2.2 and the transmitted light is focused onto an avalanche photo diode (APD).

4.2 Driving electronics

The VCSELs, being the only active element of the sender optics, have to be driven by an electronics system capable of setting the bias and modulation current, as well as their timing in order to achieve a high temporal overlap of the resulting optical pulses. The main elements of the electronics are shown in Figure 4.5 and are described in the following paragraphs.

FPGA

The fast logic, such as switching of the four VCSEL channels and setting of the other logic parts' parameters, is implemented within an FPGA. The FPGA in use is part of an embedded evaluation module (Cesys EFM01[1]), consisting of a Xilinx Spartan-3E FPGA and a USB2.0 controller (Cypress CY7C68013A), allowing for fast interaction between a PC and the FPGA. After being programmed, a microcontroller on the EFM01 receives and interprets commands from the user, sends them to the FPGA which translates them into bit-sequences transmitted to and controlling the different parts of the pulse generation and synchronization (PGS) unit.

Clock signal generation and distribution

The 100 MHz clock signal is generated by an oscillator (Crystek CCPD-033-50-100[2]) and subsequently split up to simultaneously feed the FPGA and two buffers (Micrel SY58603U[3]). From the buffers, the differential clock signal is split up again, supplying the four PGS units as well as a Receiver/Driver (Micrel SY100EP16V[4]), allowing for synchronization with external devices.

Pulse generation and synchronization

The PGS unit takes two identical copies of the clock signal and transforms them into an electric pulse of adjustable length driving a VCSEL diode. The process for this transformation goes as follows: The two clock signals, C_1 and C_2, are shifted with absolute delays d_1 and d_2 by the delay chip (Micrel SY89297U[5]), resulting in a relative delay $\Delta d = |d_2 - d_1|$[6]. The range of delay times is from 0 to 5 ns in steps of 5 ps. The FPGA also controls the *enable* pin of the delay chip, switching on the chosen VCSELs.

[1] `https://www.cesys.com/fileadmin/user_upload/documents/EFM01/ug110-efm01.pdf`

[2] `http://www.crystek.com/crystal/spec-sheets/clock/CCPD-033.pdf`

[3] `http://ww1.microchip.com/downloads/en/DeviceDoc/sy58603-5_eb.pdf`

[4] `http://ww1.microchip.com/downloads/en/DeviceDoc/sy100ep16v.pdf`

[5] `http://ww1.microchip.com/downloads/en/DeviceDoc/20005835A.pdf`

[6] The values of d_1 and d_2 are passed to the chip as two 10-bit sequences, that convert to delay times of $d[ps] = d[\text{bit value}] \times 5[\text{ps}]$.

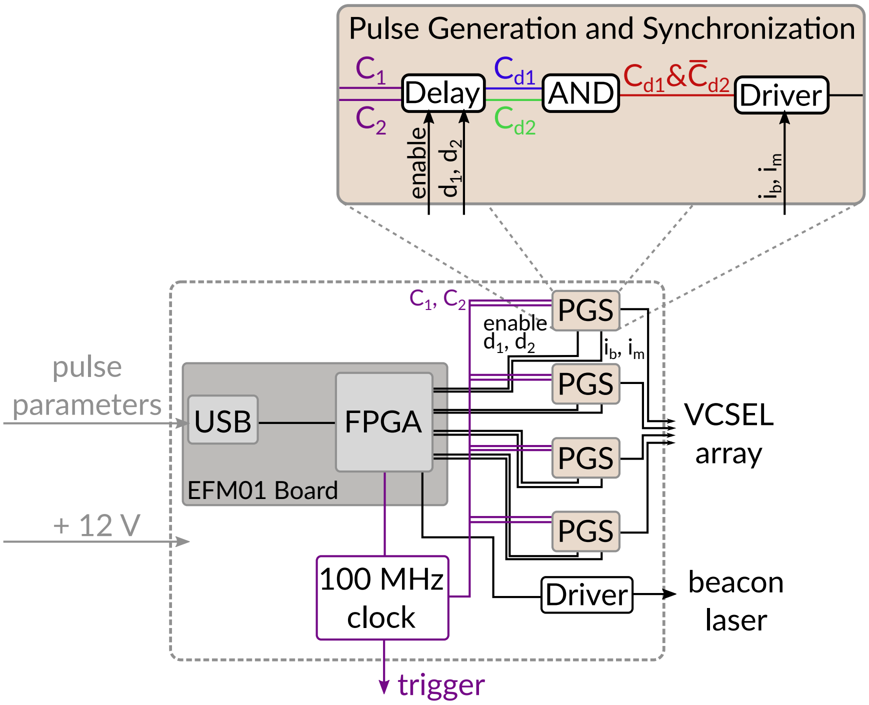

Figure 4.5: Simplified schematic of the driving electronics. In the PGS unit, the delay chip shifts two copies of the 100 MHz clock by values d_a, d_b, provided by the FPGA, which are then combined at an AND gate, from which the signal is fed into a laser driver chip, receiving the current parameters i_b, i_m from the FPGA. Adapted from [54].

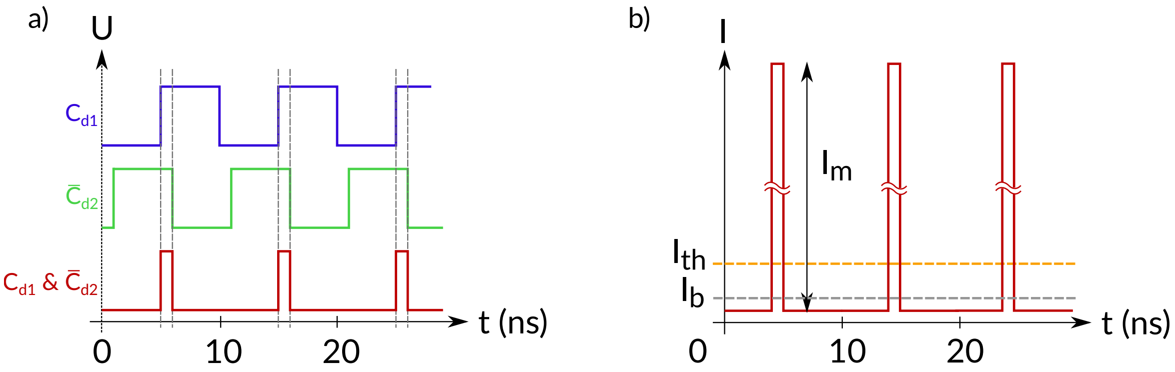

Figure 4.6: (a) Pulse generation with two shifted clock signals C_{d1} and $\overline{C}_{d2}$ and an AND gate. (b) Interpretation of the modulation and bias currents at the laser driver. The bias current I_b is chosen below the lasing threshold I_{th} of the VCSELs; the AC-coupled modulation leads to a signal swing of I_m around the average value I_b. Adapted from [54].

The shifted clock signals C_{d1} and C_{d2}, while one of them gets inverted, are guided to the inputs of a logic AND gate chip (Micrel SY55851[7]), delivering short electrical pulses with a duration of Δd (see Figure 4.6 a)), which are sent to the modulation input of the laser driver (Texas Instruments ONET4291VA[8]). The values for the bias i_b and modulation height i_m can be translated to current values as $I_b = 100\mu A + 47\mu A \cdot i_b$ and $I_m = 100\mu A + 68\mu A \cdot i_m$ with ranges $I_b \in [0.1, 12.1]$mA and $I_m \in [0.1, 17.4]$mA. The bias current I_b should be chosen below the threshold current of the VCSEL diodes in a way, that the modulation peaks rise well above this lasing threshold, allowing for low background intensity between the optical pulses. The combination of the AC-coupled modulation with the bias current results in a pulse driving the VCSEL as illustrated in Figure 4.6 b).

4.3 Receiver setup

In order to perform a key exchange using the polarization encoded BB84 protocol, a detection unit capable of measuring the polarization of weak pulses in two conjugate bases is needed; thus, the most important part of any BB84 receiver is a polarization analysis unit (PAU). For the case of our hand-held device, components for tracking the beacon beam and reference frame alignment for compensating tilts were added to enable a more convenient and efficient operation. In order to compare their bit-strings during post-processing, the internal clocks of Alice and Bob need to be synchronized, which is done via intensity modulation of the beacon laser with a frequency of 50 MHz. These components, as they are shown in Figure 4.7, and their operation in the receiver are explained in the following.

4.3.1 Polarization analysis unit

The detection and analysis of BB84 signals is done in the polarization analysis unit, set up with a 50/50 beam splitter (BS), two polarizing beam splitters (PBSs), a half wave plate (HWP) and a system of four fibre coupled avalanche photo diodes (APDs, PerkinElmer DTS

[7] `http://ww1.microchip.com/downloads/en/DeviceDoc/sy55851-51a.pdf`
[8] `http://www.ti.com/lit/ds/symlink/onet4291va.pdf`

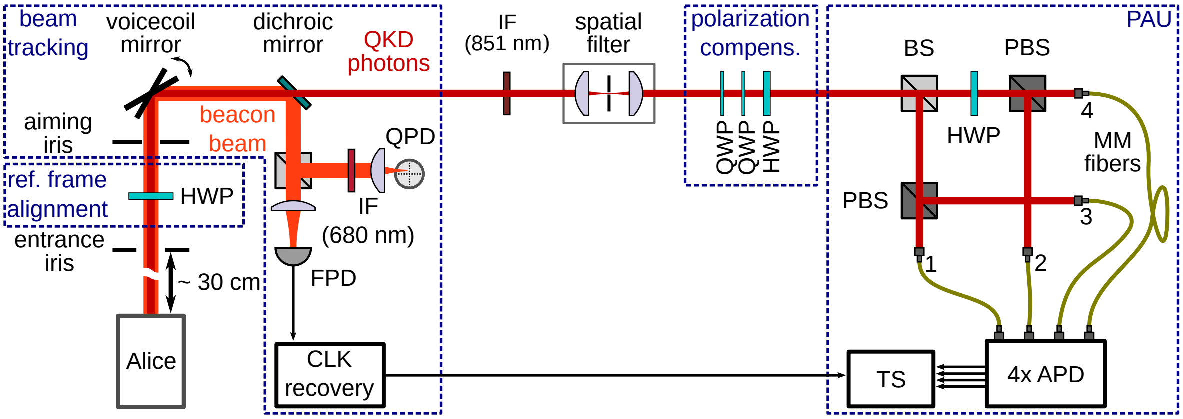

Figure 4.7: QKD receiver setup "Bob". The QKD photons, overlapped with the beacon beam, enter the receiver through an iris and pass trough a HWP that can be rotated to align the reference frames of Alice and Bob. The user holding the sender module has to aim the beacon laser at a second pinhole during a hand-held key exchange. The beam tracking and controlling is done with a voicecoil mirror and a quadrant photo diode (QPD), monitoring the direction of the beacon beam. The beacon is separated from the QKD signal at a dichroic mirror and split up at a beam splitter (BS) to use one portion for clock synchronization, done with a fast photo diode (FPD) detecting the beacon modulation. The beam tracking unit is followed by an interference filter (IF), used to suppress unwanted background, and a spatial filter, closing a potential spatial side channel. Before the photons enter the polarization analysis unit (PAU), two QWPs and one HWP apply a polarization compensation to the incoming light. The PAU consists of one BS, two polarizing beam splitters (PBS), a HWP and four fibre-coupled avalanche photo diodes (APDs).

SPCM-AQ4C[9]), seen on the right in Figure 4.7. The random choice of measurement basis on Bob's side, necessary for the BB84 protocol, is implemented passively using the random splitting process at the BS. In our setup, light reflected at the BS is measured in the H/V (also called B_X) basis, as the PBS in this arm is aligned to let H-polarized photons pass and reflects vertically polarized ones. So, theoretically, if a horizontally polarized photon takes this path, it will cause a click at detector 1 and no click at detector 3, and vice versa for V polarization. For the other case of a photon being P- or M-polarized, detectors 1 and 3 have equal click probability. For the light transmitted through the BS, a HWP applies a rotation: The wave plate's optical axis is aligned at a 22.5° angle to the vertical axis of the laboratory system, leading to a rotation of 45° of the linear polarizations in this reference frame (corresponding to a 90° rotation in the equatorial plane of the Poincaré sphere). As the following PBS is aligned in the same way as the one in the other arm, this rotation has the effect of switching the measurement basis to P/M ($\widehat{=} B_Y$).

4.3.2 Beam tracking and reference frame alignment

In free-space QKD the security can be potentially compromised by what is known as the spatial mode side channel [46]. In this attack, an eavesdropper makes use of the differences in the detection efficiencies depending on the alignment and spatial structure of the incoming beam. This side channel can be closed by reducing the acceptance angle using a spatial filter such that all detectors show equal dependence on the beam alignment. In our case, it consists of a small pinhole (d=30 μm) between two convex lenses (f=11 mm), leading to an acceptance angle of ±0.08°.

This countermeasure would seriously reduce the achievable coupling efficiency during hand-held use, as any motion of the operator's hand will lead to a link loss; for this reason, an active beam tracking system is part of the receiver module. This system utilizes the beacon beam, a quadrant photo diode (QPD) and an electrically controled voicecoil mirror (VM). Initially, the overlapped pair of signal and beacon beam needs to be aimed at the entrance pinholes and is reflected by the VM onto a dichroic mirror, separating the two beams. The reflected beacon beam is divided into two parts at a BS and the transmitted portion is focused onto a fast photo diode (FPD), registering the 50 MHz modulation of the beacon and sending this timing information to a detection timestamp unit (TS). The part of the beacon beam reflected at the BS is focused onto a QPD, which is aligned such, that the focus lies at its center when the coupling through the previously described spatial filter is optimal. If the beam emitted by Alice is tilted, this will lead to a shift of the focus position on the QPD, causing different intensity distributions over the diode's quadrants. This information is used to control the VM, allowing for a fast correction of the incident beam.

Since the reference frames of the hand-held sender and the receiver can be rotated with respect to each other, this needs to be adressed, as a reference frame mismatch will reduce the secret key fraction of the BB84 protocol. In order to not have the user manually keep the angular alignment, the adjustment of the reference frames is automatically done in the receiver module. For this purpose, a motorized HWP is controlled with the information from the gyroscopic motion sensor of a standard smartphone, being placed on top of the hand-held Alice module [59].

[9] `http://www.perkinelmer.com/CMSResources/Images/44-12495DTS_SPCM-AQ4C.pdf`

4.4 Hand-held link results

Using the components described in this section, our group successfully built a hand-held free-space QKD sender device implementing polarization encoded BB84 with faint laser pulses [20]. The beam tracking and reference frame alignment (Section 4.3.2) allowed four different untrained users to establish average link efficiencies of about 20% (relative to the fixed sender module) during an operation over a distance of 30 cm. Using the GLLP formula 3.8 for the asymptotic secure key rate extended by a preparation quality factor (see Equation 5.5 in Section 5.3.3). By this, secure key rates between 4.0 kbits/s and 15.3 kbits/s were calculated from the results of eight tests, two for each user. The secure key rates had a demonstrated average of 7.1 kbits/s. The overall QBER, averaged over all runs, amounts to 2.4%, which is reasonably close to the compensated preparation and measurement QBER of 1.48% (see Section 4.1.4).

The small form factor of the sender module makes it well suited for many compact free-space applications, possibly also for larger distances. If one thinks of a HAP- or space-based QKD sender device developed from this, a few other constraints besides the compactness have to be met. Some of these constraints, like the low power availability, for example, and the developed modifications applied to the sender setup are presented in the next chapter.

Chapter 5

Modifications and further developments of the QKD components

As the prior chapter shows, our group has succeeded in implementing a QKD sender module in a small, handheld device over the last few years. As an addition to the key exchange between a mobile, handheld sender and a stationary receiver unit, we want to develop a solution for QKD from a high-altitude platform to a stationary groundstation, as a means to overcome the distance limit of fiber based quantum communication. Within this chapter, the modifications necessary to meet the constraints of such platforms are motivated; this is followed by a presentation of the developments applied to our setup.

5.1 Motivation

For the implementation of the handheld QKD device the main requirement for the sender optics was to be miniaturized, in order to deploy the whole sender system, consisting of driving electronics and the optics, into a small box with the footprint of a modern smartphone. This miniaturization is a first necessary step towards scenarios where a QKD unit is implemented into a flying high-altitude platform (HAP), i.e. a stratospheric pseudo-satellite, or a small satellite.

One constraint these platforms impose is a limited power availability; this especially affects the design of the driving electronics. Another issue related to the power consumption of the electronics is heat management in the quantum transmitter package under such conditions.

5.2 Modular electronics design

In order to test different approaches and configurations of the driving electronics, a modular approach to the further electronic development was chosen. By *modular* we mean, that the controlling FPGA as well as the generation and distribution of precise clock signals is situated on a single mainboard, while pulse generation and the driving of the VCSEL diodes using different methods is realized on exchangeable additional boards ("Subboards"). My developments and tests are based on the work done by Clemens Sonnleitner during his Master's thesis [60].

5.2.1 Mainboard

The mainboard is equipped with the module's power supply, the clock generation and distribution and the FPGA used to control the functions of the PGS units. The clock signals and control parameters of the delay and laser driver chips are sent to the subboards via 16-pin connectors (Hirose FH12 16S-0.5H) and flexible flat cables, offering a small form factor, due to the pitch of the pins of 0.5 mm, and good differential transmission, allowing for impedance matching to the signals on the boards.

The first modification applied to the existing setup (Section 4.2) concerns the power supply, which is changed from the 12 V of the handheld module to 5 V on the mainboard. A power switching module (Texas Instruments LMZ10505[1]) converts this input voltage to 3.3 V, which is the supply voltage of all the integrated circuits (ICs), with a maximum current of 5 A.

The control of the pulse parameters is done similarly to the previous design, as the same Spartan-3E FPGA on the evaluation board (Cesys EFM01) is implemented. Additionally to the previous functions, new connections from the FPGA to the PGS units are implemented, enabling the setting and generation of pulses for the laser driver directly at the FPGA, thus potentially allowing to omit the delay chip and possibly the logic gate.

In order to achieve a better quality of our clock signals, a new oscillator as well as a new distribution concept was chosen. The 100 MHz clock chip (Texas Instruments LMK61E2-100M00[2]) offers very fast (20%-80%) rise-/fall-times of ≈ 120 ps and a sub-picosecond jitter. As we use differential signaling to achieve fast signaling with low noise, passively splitting up the clock signal into multiple parts can negatively affect the signal quality. For this reason, a 1:8 fanout buffer (Micrel SY58031U[3]) is used to produce eight identical copies of the clock signal in CML logic, while achieving rise-/fall-times of 60 ps. One of these signals is routed to a buffer chip (Micrel SY58604U[4]), providing the LVPECL output signal necessary for clock synchronization of external devices. A second copy is fed into the FPGA, allowing it to synchronize to the 100 MHz oscillator and thereby emit clock-synchronous pulses as well as modulate the beacon laser. The remaining six clock signals are routed to the subboard connectors 1-4, one to connector 1 and 2, each, and two to 3 and 4, respectively. This allows us to test different concepts for the management of the clock signals on different subboards. The design of the mainboard can be seen in Appendix A of [60] (Figure A.2).

5.2.2 Subboards

The subboards follow the basic design similar to the PGS units of the handheld module (Section 4.2), but some designs differ in a few key aspects. For one thing, the logic gate is exchanged for a different one (Micrel SY58051AU[5]), mainly due to availability issues.

The starting point for my developments were the subboards 0a and 0b, in C. Sonnleitner's nomenclature; for a full description of all the different subboards designed by Clemens, I refer to his thesis [60]. The main difference between type a and b is, that the former is intended for

[1] http://www.ti.com/lit/ds/symlink/lmz10505.pdf

[2] http://www.ti.com/lit/ds/snas676d/snas676d.pdf

[3] http://ww1.microchip.com/downloads/en/DeviceDoc/sy58031u.pdf

[4] http://ww1.microchip.com/downloads/en/DeviceDoc/sy58604u.pdf

[5] http://ww1.microchip.com/downloads/en/devicedoc/sy58051au.pdf

the use at connectors 1 and 2 of the mainboard, while the latter fits to the clock configuration of connectors 3 and 4.

Subboard 0a employs a clock management similar to the module of chapter 4, as it only receives one clock signal from the fanout buffer and splits that into two pulses, each entering one of the inputs of the delay chip. The shifting of the two clock signals works in the same way as described earlier, and the AND gate, while being a different chip, does the equivalent operation as the Micrel SY55851 used previously. It offers steep pulse flanks with rise-/fall-times of typically 20 ps, while inducing very little jitter in the order of few picoseconds. As there is only one differential clock signal occupying pins of the connectors, there is room for two additional GPIOs (general-purpose input/output) per channel, routed from the FPGA to connectors 1 and 2.

For connectors 3 and 4, a slightly different concept for pulse generation is tested: here, two distinct copies of the clock signal, coming from the 1:8 buffer, are routed to the connectors and guided to the subboards 0b. Avoiding the splitting of the differential clock signals should prevent additional deterioration of the signal quality, possibly resulting in improved control over the pulse parameters. With the current pin assignment at the connectors, the channel selection is performed at the delay chip.

Based on subboard 0b, a new approach where the delay chip is replaced by selectable hard-wired delays (subboard 2a) is developed. One reason to omit the delay chips used on other subboards is their high power consumption, that becomes a problem in some apllications. The passive hard-wired delays consist of meanders of different lengths for the respective signals of the clock pair. By choosing the overall length of each line, both the absolute delay of the two signals as well as the relative distance in time between them can be controlled with a resolution of 50 ps, which is illustrated in Figure 5.1. With concatenating delay meanders, they provide some flexibility in the timing.

The time delay Δt can be calculated from the path difference Δx via the speed of electromagnetic waves in the transmission line. If this signal speed is c_s, the delay is calculated as

$$\Delta t = \frac{\Delta x}{c_s}, \tag{5.1}$$

while c_s is given by

$$c_s \approx \frac{c_0}{\sqrt{\epsilon_{eff}}} \approx 0.59 \cdot c_0 \approx 1.8 \times 10^8 \frac{m}{s}. \tag{5.2}$$

Here, c_0 is the vacuum speed of light and ϵ_{eff} the effective dielectric constant for our copper microstrips on the PCB; its calculation follows [61]. This leads to a length of $\Delta x \approx 1$ cm for one 50 ps meander.

The main reason for the use of these hard-wired delays is, as already mentioned, that they basically do not need any power, whereas the delay chips have a considerable power consumption. With the supply voltage of 3.3 V and a typical input current of 195 mA for each of the four delay chips, they use 2.57 W. This wis no problem for the handheld module, as the power supply is not too much of an issue in this case; for the implementation into most HAPs, however, there are severe constraints on the power, as only few Watts will be available for the operation of the entire QKD module. Moreover, a high power consumption is accompanied

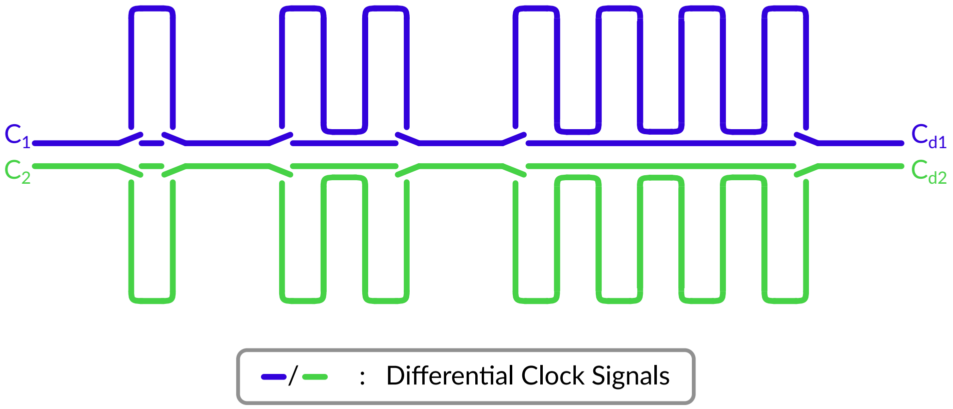

Figure 5.1: Schematic of the working principle of the configurable hard-wired delays. One loop of the meander corresponds to a signal delay of about 50 ps. For simplification, the differential clock signal pairs are drawn as single lines. The selection of the path is implemented using 0Ω SMD resistors.

by strong heat generation, which becomes especially problematic under low pressure or vacuum conditions. Furthermore, the passive shifting of the clock signals should only introduce minimal jitter or drifts during operation and the reliability of the pulse generation does only depend on the quality of the soldering.

5.2.3 Assembly of the circuit boards

As almost all the ICs used in the design of the different electronic modules have a QFN (Quad-Flat No-Leads) package, they can't be soldered to the printed circuit boards (PCBs) manually from the top with a soldering iron. For this reason, the process of reflow soldering was chosen for the assembly of the PCBs. Here, a stencil (thickness 150 μm) is used to apply a reflow soldering paste (Chipquik SMD291SNL50T3[6]) to the pads where ICs and other components need to be soldered to the circuit board. The temperature profile of the reflow oven (LPKF Proto Flow S[7]) needs to be carefully adjusted to the components, as the lowest maximum temperature rating of the used ICs must never be exceeded. Within these boundaries, the three phases of preheat, reflow and cooling can be adjusted to obtain optimal soldering results. The preheat phase has the purpose of gradually bringing all components to the same specified temperature, reducing stress due to thermal expansion. The soldering happens in the reflow phase, where the oven heats up to the peak temperature, that has to be above the melting point of the soldering paste, so that it connects the pads of the components with the ones on the board. After this, the temperature is held for a few seconds, the oven opens and starts the cooling phase, decreasing the temperature of the parts.

The used reflow profile for the assembly of the subboards is shown in Figure 5.2 with the parameters of Table 5.1.

[6] http://www.chipquik.com/datasheets/SMD291SNL50T3.pdf

[7] https://www.lpkf.com/de/branchen-technologien/forschung-in-house-pcb-prototyping/products/lpkf-protoflow-s/

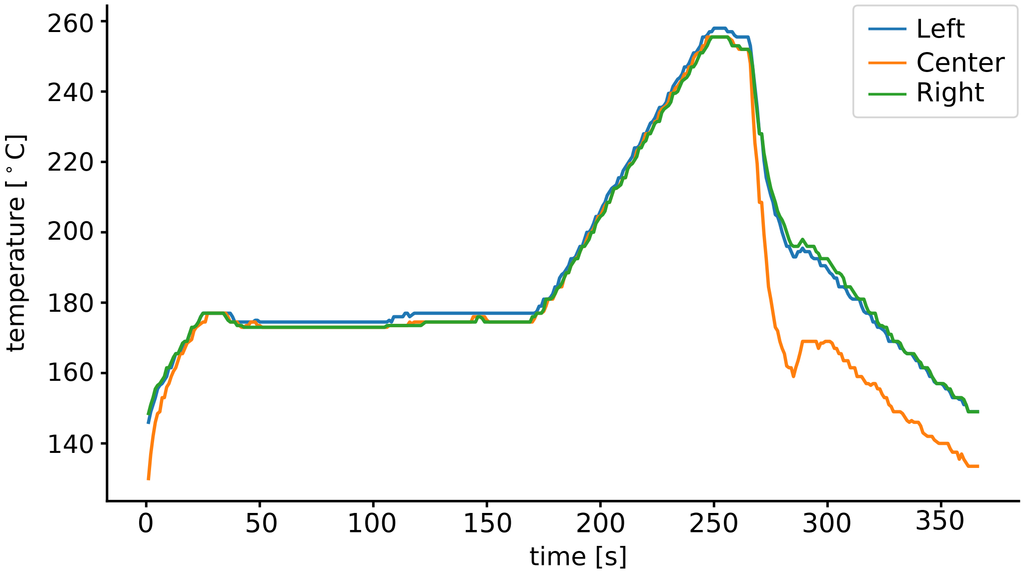

Figure 5.2: Temperature curves for the sensors in different parts of the reflow oven during the whole process. After the preheat phase, the maximum temperature of 255°C is reached in the reflow phase, followed by gradual cooling.

Phase	Temperature [°C]	Time [s]	Power [%]
Preheat	175	165	—
Reflow	255	100	100
Cooling	—	100	100

Table 5.1: Parameters for the different phases of the soldering profile.

5.2.4 Electrical characterization of the hard-wired delay PGS unit

In principle, the electronic pulses generated either by using a specific configurable hard-wired delay or the corresponding parameters for a delay chip should be identical. As it is not a priori known whether the SMD resistors used within the meanders conserve the differential signaling properties of the transmission lines, the compared subboards (0b and 2a) need to be electrically characterized. Measuring the signals shown in the schematic of Figure 4.6 is a difficult task, as the steep flanks and short widths of the pulses require a large bandwidth measurement device for precise investigation. Additionally, all signals in front of the laser driver IC are differential, which made the purchase of a fast differential oscilloscope probe (Teledyne LeCroy D620-A-PB2) necessary. This probe allows for the precise measurement of the signals using the full oscilloscope bandwidth of 4 GHz.

For comparison of the two delay concepts, subboard 2a with a hard-wired delay configuration of $\Delta t \approx 150$ ps and subboard 0b with corresponding delay parameters ($d_a = 0,\ d_b = 30$) were connected to connector 3 of the mainboard. The remaining control parameters were identical for both measurements, namely $i_b = 1$ and $i_m = 255$. The results of the measurements for subboard 2a can be seen in Figure 5.3 a) and c), while b) and d) show the pulses on subboard 0b. If one compares the pulses in a) and c), it can be seen that the quality of the clock signals is conserved well through the meanders and the SMD resistors, resulting in well defined short pulses after the AND gate. All signals in these two plots show the expected differential swing of $\Delta U = 800$mV. In parts b) and d), the signal coming from the laser driver is plotted and the approximate threshold voltage, after which lasing starts, $U_{th} \approx 1.63$ V are shown. The less intense peaks following the main ones with $\Delta t \approx 1$ ns are the portion of the signals reflected at the diodes due to imperfect impendance matching, as the VCSELs have impedances of $\approx 300\ \Omega$, while the laser driver should be terminated with 50 Ω[8]. The time difference of 1 ns is caused by the length of the cables (10 cm) used to connect the diodes to the subboards.

Overall, the results shown in Figure 5.3 prove that, with respect to the electric signals, the approach using configurable hard-wired delays seems feasible and should produce the desired optical pulses, which are investigated and characterized in the next section.

5.2.5 Optical pulse shapes using hard-wired delay pulse generation

To characterize how well the pulse generation using the configurable hard-wired delays works, as compared to the former scenario with the delay chips, a setup for the precise measurement of temporal shape of the emitted optical pulses is built (see Figure 5.4). For this purpose, one of the VCSELs in the array is connected to subboard 2a and its emitted light is collimated with a f = *11 mm* lens. The beam is then focused onto an APD with the signal output connected to an oscilloscope. While the pulse generation is done after connector 3, connector 1 is used to measure the 100 MHz clock and feed the signal into a second channel of the oscilloscope, so that the timing difference between the rising edge of the clock signals and the arrival of the optical pulses at the APD can be measured. The resulting values are plotted as a histogram, showing the temporal optical pulse shape. To compare the performance of

[8] In principle, these reflections could also be due to the measurement with the differential probe. This possibility is excluded here because the timing difference between signal and reflection fits very well to the used cable lengths. Furthermore, the high impedance probe is designed to not affect the measured signals in this way.

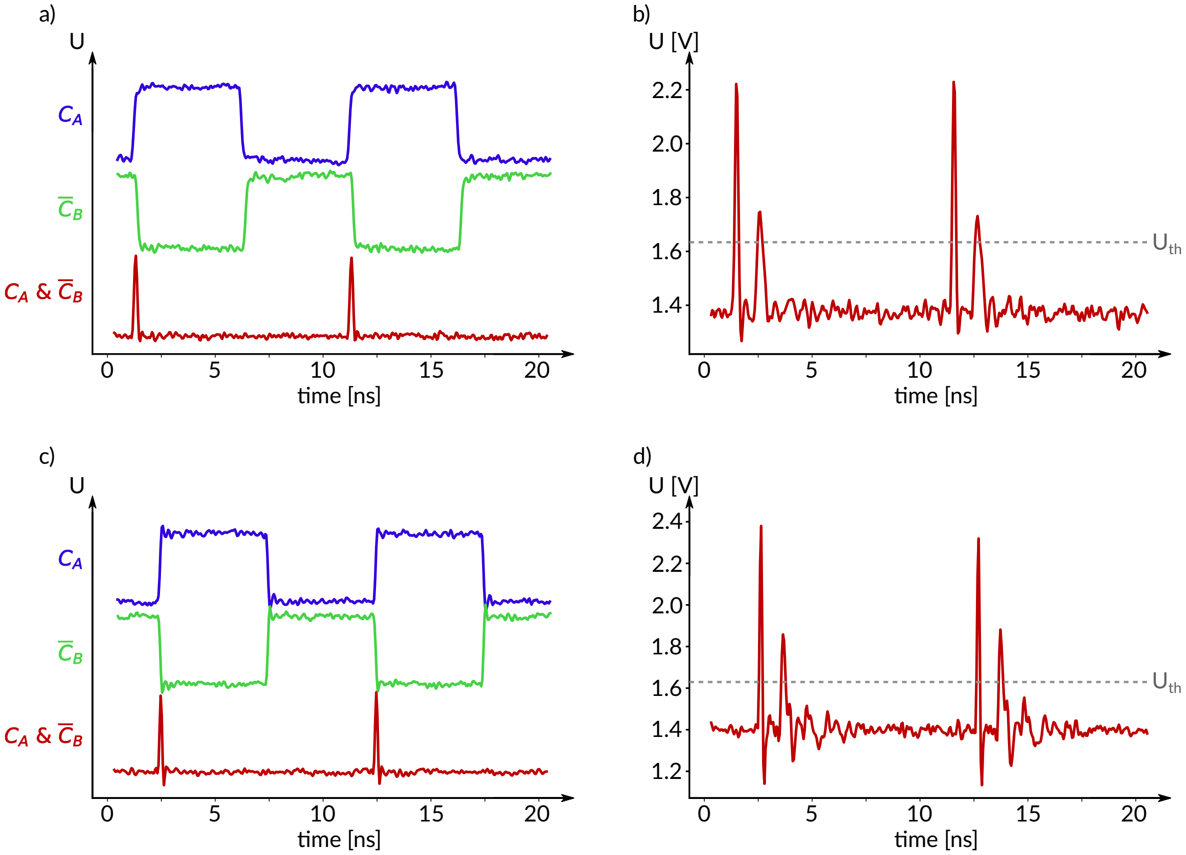

Figure 5.3: a) and c): Signals of the shifted clocks, C_a and $\overline{C}_b$, the pulse after the AND gate, $C_a\&\overline{C}_b$, for the hard-wired delay and the delay chip, respectively. The pulse after the gate IC (red) was shifted to be in the same time frame as the clock signals. b) and d): Laser driver signals received by the VCSEL, for hard-wired delay and delay chip, respectively. The dashed line marks the lasing threshold voltage of $U_{th} \approx 1.63$ V.

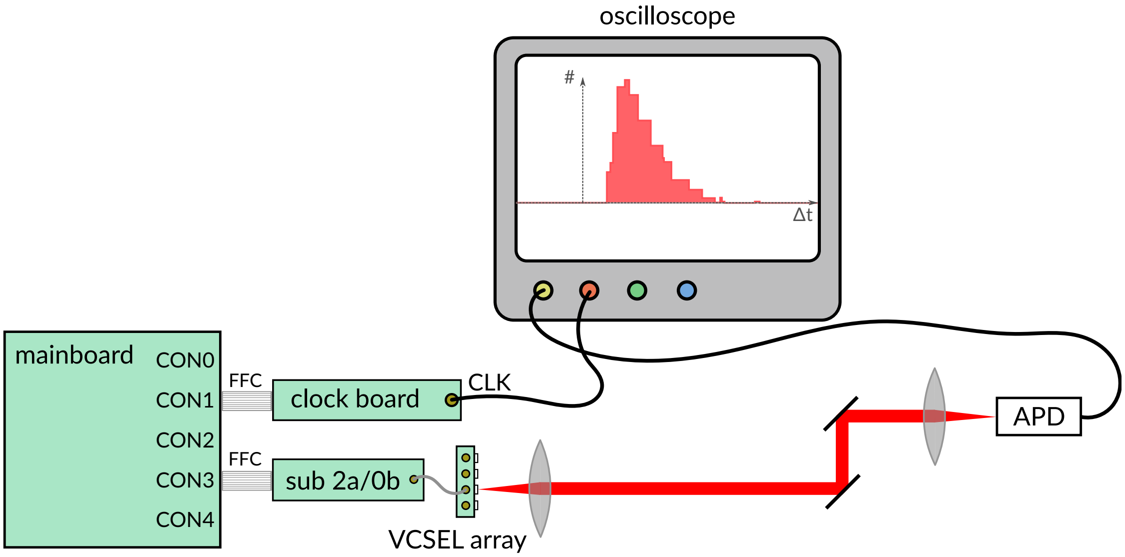

Figure 5.4: Schematic of the setup for the optical pulse shape measurement. A subboard for the clock measurement is attached to connector 1 and the pulse generation board (subboard 2a for hard-wired delays, 0b for delay chip) to connector 3 of the mainboard using flexible flat cables (FFC). One of the VCSELs is connected to and driven by the respective subboard. The measured photon pulse arrival times with respect to the 100 MHz clock are evaluated as a histogram at an oscilloscope.

the pulse generation with delay chip or hard-wired delay, the equivalent measurement is done with subboard 0b at connector 3.

The performance comparison of the two different delay concepts is done by implementing a hard-wired delay of $\approx 150ps$ on subboard 2a and using the corresponding delay parameters in the control programm for subboard 0b. The remaining control parameters for the pulse generation are set to the same values for both measurements, resulting in the histograms shown in Figure 5.5. It can be seen, that the reflections that were present in the electric pulses (see Figure 5.3) do not deteriorate the temporal shape of the emitted optical pulses. The reason for this most likely is, that these reflections are not backreflected from the laser driver IC with their full amplitude and thus do not exceed the lasing threshold voltage U_{th} once they arrive at the VCSEL. Despite the higher noise for the measurement with the delay chip, which is due to a shorter measurement time, it can clearly be seen, that the two methods result in almost identical pulses and that the implementation of hard-wired delays is a feasible approach to a compact and power efficient modification of the sender module's electronics.

5.3 A new concept for implementing the polarizer array

The gold-foil wiregrid polarizers used in the handheld module offer an excellent extinction, but come with the drawback of a time consuming and difficult fabrication process. An important aspect of the WGPs is their low transmittance of only about 10% as well as the reflection of the non-transmitted light, possibly back into the VCSEL diodes, which can potentially harm them. In order to improve on the transmission and simplify the frabrication process, we decided to develop a new fabrication process using a synthetic polarizer foil.

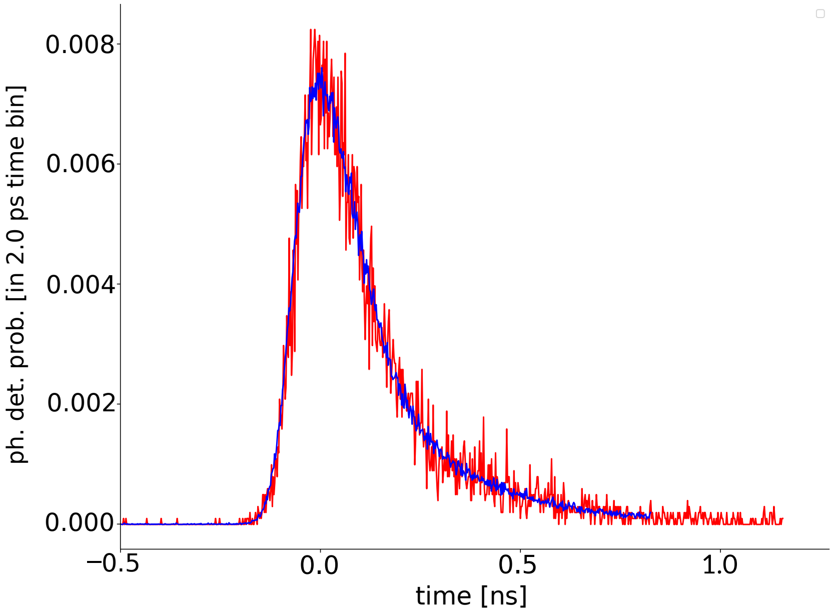

Figure 5.5: Optical shapes of the pulses generated with the delay chip (red) and the hard-wired delay (blue). The pulse control paramters are $i_b = 1, i_m = 255$ in both cases and $d_a = 0, d_b = 30$ for the delay chip.

5.3.1 Working principle of synthetic foil polarizers

One alternative to using miniaturized WGPs are synthetic foil polarizers. These so called Polaroid polarizers were developed in the first half of the 20. century by Edwin Land and his co-workers [62] and are based on the alignment of polymeric chains.

Different types of these sheet polarizers use a clear plastic sheet of polyvinyl alcohol (PVA) in its stretched state as a matrix. The stretching leads to the parallel alignment of the PVA molecules (molecular structure shown in Figure 5.6), in which different additional particles can be absorbed. If the stretched PVA sheet is, for example, doped with iodine, the result is an H type polarizer with a much larger absorption coefficient for light polarized parallel to the direction of the stretching, i.e. the alignment of the polymers, than for the polarization direction perpendicular to it. If one wants to select the wavelength range for which the sheet acts as a linear polarizer, dichroic dye molecules need to be absorbed in the PVA matrix. The polarization range of these L type polarizers can, by selection of a proper dye, be quite narrow, while light outside this wavelength region is only affected very little. Another possibility to make the stretched PVA dichroic, resulting in a polarizing effect, is to dehydrate the polymere, ending up with polyvinylene, the material for K type Polaroid polarizers.

For an in depth presentation of the scientific endeavours in the field of sheet polarizers, I refer the reader to the script of a talk given by E. Land [62], while a good summary of the optical properties of such polarizers is available in [63] and [64].

The polarizer foils we use are chosen specifically for our near-infrared wavelength of $\lambda = 850nm$ and offer sufficiently good performance, regarding the manufacturer's information[9]. The stated transmission of unpolarized light of above 35% is verified, while an extinction ratio

[9] https://www.itos.de/en/itos-polarizers/linear-polarizers/xp-ir2/

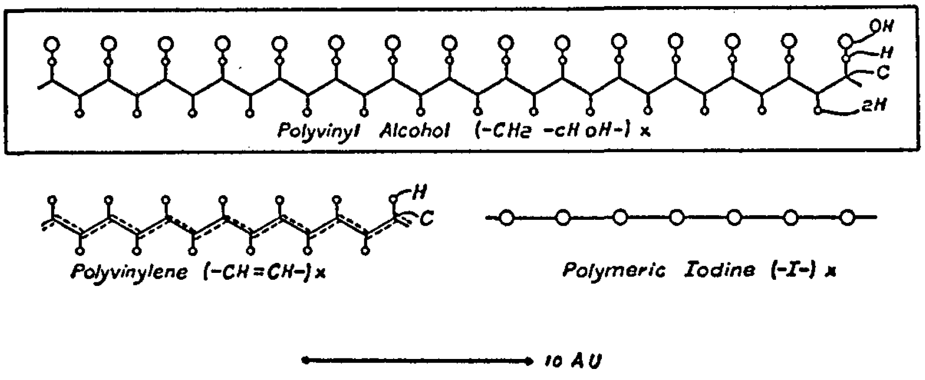

Figure 5.6: Approximate molecular structure of polyvinyl alcohol, polyvinylene and iodine doped PVA. Taken from [62].

of well above 1:10,000 for a macroscopic piece of foil is measured. During investigations with a tightly focused laser it was found, that the angle of transmitted polarization varies on the scale of a few millimeters, amounting to a rotation of 9° across the height of the foil (dimensions 60 mm × 55 mm). As the used area of the polarizer foil strips in the experiment is on the order of few micrometers, this deviation can be worked around by thoroughly measuring the transmission angle at each specific position and adjusting the cutting angle (see Seection 5.3.2) accordingly.

5.3.2 Assembly of the polarizer array

As the VCSEL diodes, as well as the waveguide inputs, have a pitch of 250μm, the same has to hold for the four poalrizers in the array. In the handheld module, this was achieved by FIB-writing the four wiregrid polarizers with centers separated by 250μm. As we want to use four differently oriented strips of polarizer foil, this induces a strong constraint on their widths. The structure of the array relative to the input facet of the waveguide circuit is shown in Figure 5.8.

It is crucial that all four polarizers are cut and mounted with precise angles relative to each other, as well as to their respective waveguide. To achieve the necessary precision, a wire saw coated with diamond particles was chosen for the cutting procedure, resulting in very straight, even edges. The mount used for the foil strips (see schematic in Figure 5.7) allows to select the precise cutting angle, relative to the transmission direction of the polarizer. After some manual postprocessing, namely deburring and cleaning the cut pieces, these strips can be placed parallel to each other and glued together with a two-component adhesive. The parallel adjustment of the strips becomes a lot less difficult, if the two outer strips are a bit wider than the inner two, as depicted in Figure 5.8. As our foil is about 410μm thick, the P- and H-polarizer strips are thicker than they are wide, which makes it highly difficult to place them in an upright position. As the wider V- and M-strips (width 500μm) easily stay upright, it is possible to fix the middle two polarizers between them by applying small pressure from both sides.

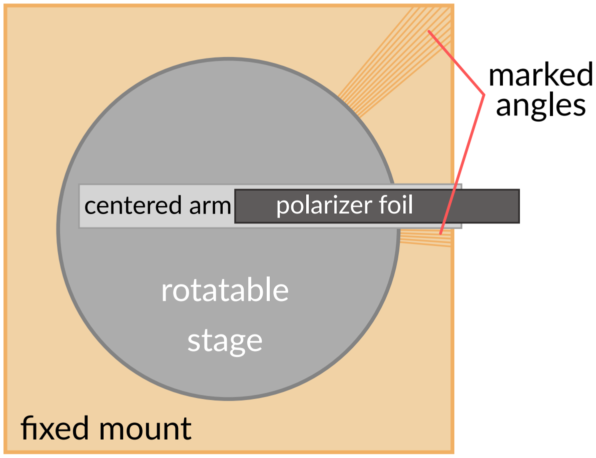

Figure 5.7: Mount used for setting of the cutting angles of the polarizer foil. A foil strip (width ≈ 6 mm) is fixed on an arm centered on a rotatable stage. Via the angles marked on the mount fixed to the saw (ranges $[-5°, +5°]$ and $[40°, 50°]$), the edge of this arm can be set to the specified angle.

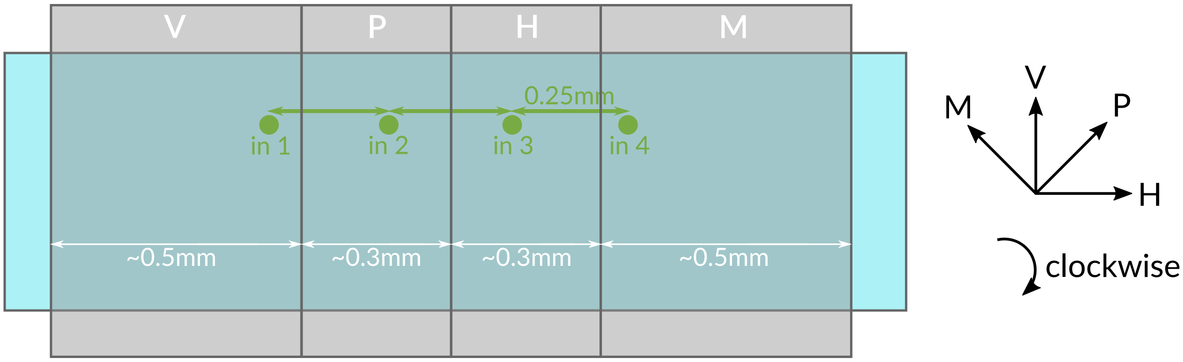

Figure 5.8: Structure of the polarizer array in relation to the waveguide inputs. The outer polarizer strips are a bit wider to allow for an easier handling.

5.3.3 Polarization compensation

In order to find the optimal orientations of the four polarizers for a specific waveguide chip, C. Sonnleitner investigated the polarization effects of the *Alice 2.0* chip [65] by measuring a quantum state tomography (QST) using different input polarizations [60]. The waveguide array is similar to the one used in the handheld experiment (Section 4.1.3), but slightly differs in its dimensions ($\sim$ 22mm × 5.5mm × 1.1mm) and some other physical properties. The birefringence, that is the refractive index difference for H- and V-polarization of the waveguides, is $\Delta n = 5.6 \cdot 10^{-5}$. A schematic picture of the waveguide is shown in Figure 5.9.

By measuring a QST with the six polarization states H, V, P, M, R and L for each waveguide input, one can, by least square fitting, evaluate a Mueller matrix M_{wg} ($wg \in \{1, 2, 3, 4\}$ for the four Alice 2.0 waveguides), describing the effect of the waveguide on an incoming polarization state (in terms of a Stokes vector $\vec{S_i}$) for the four different inputs:

$$\vec{S_o} = M_{wg}\vec{S_i}, \tag{5.3}$$

where $\vec{S_o}$ is the resulting output state.

By inverting equation (5.3), we can calculate the optimal input polarizations for the desired outputs H, V and P, M,:

$$\vec{S_o} = M_{wg}\vec{S_i} \Leftrightarrow \vec{S_i} = M_{wg}^{-1}\vec{S_o} \tag{5.4}$$

This inversion yields an optimal input state that may, even for the linear output polarizations, have a circularly polarized component. As the rotation of the preparation polarizers only allows to set linear polarizations, a compromise has to be found. This is done by scanning a region around the calculated linear polarizer angles, evaluating a QST at each position. The output states measured with this procedure were optimised for the optimal preparation quality of the four BB84 states. This preparation quality quantifies the mutual unbiasedness of the states prepared by Alice,

$$q = -\log_2 \max | \langle \Psi_X | \Psi_Y \rangle |^2, \tag{5.5}$$

where Ψ_X and Ψ_Y are states prepared in different bases. In the ideal case, $\Psi_X \in B_X$ and $\Psi_Y \in B_Y$ are perfectly prepared as the BB84 states H, V, P and M, resulting in a preparation quality $q = 1$, whereas imperfect preparation leads to factors $q < 1$ that negatively affect the achievable secret key fraction [66, 67].

5.3.4 Experimental results and comparison to former performance

The polarizer array was first investigated with a QST of the resulting polarization states. For this, the package of the four polarizers is picked up with a tweezer which is mounted on a three-axis translation stage. This allows to successively position each polarizer in the focus of a laser beam, which is then focused on a detector with a lens. The QST is performed with the usual setup of a motorized QWP and polarizer in front of the detector. As sufficient power was available using the laser, an optical power meter sensor was used here. Table 5.2 shows the results. It can be seen, that all measured angles are almost identical to the desired ones. The fact that they are all slightly rotated counterclockwise (relative to the beam direction, illustrated in Figure 5.8), ranging from 0.6° for the V-polarizer to 2.7° for H, can, to some degree, be attributed to a global rotation of the array, which may not be mounted perfectly

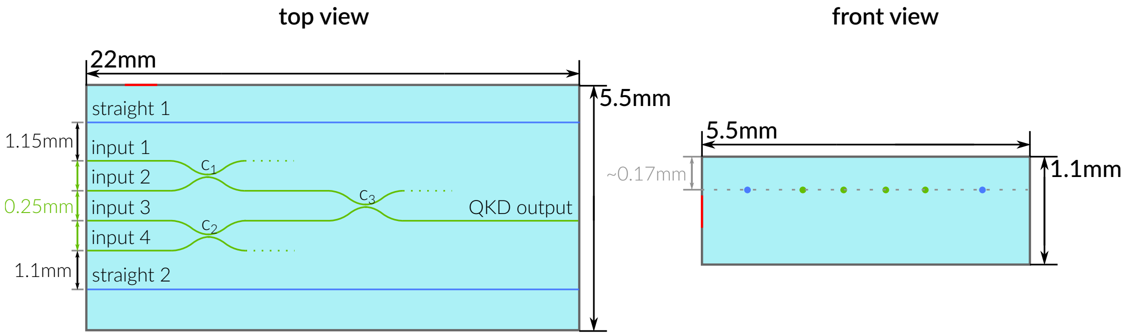

Figure 5.9: Top and front view of the Alice 2.0 waveguide chip. Only the QKD output is used for the experiments, the other three outputs leave the output facet at an angle. The two straight waveguides are used to enable easier coupling. Based on data taken from [65].

vertical in the tweezer, and partly to imperfections in the cutting and alignment process of the four polarizer pieces. While these angles can still be optimised, they already offer a preparation quality of $(88.7 \pm 0.1)\%$.

Despite the small deviations, these are very promising results, suggesting that this new kind of polarizer array may be well suited for implementation in our sender device. To investigate the expected performance in the assembled module setup, a measurement is conducted with the polarizer array mounted in front of their respective waveguide circuit inputs. The results of these measurements are shown in Table 5.3. Here it has to be taken into account, that the birefringence of the waveguide induces a phase shift of $\Delta\phi \approx 3\pi$ between H- and V-polarization. This does not affect the H- and V-polarized light, coupled into inputs 3 and 1, respectively, but it does change an input polarization of P to M, and vice versa. It can be seen, that the calculated compensation angles from Section 5.3.3 lead to outputs with a high preparation quality of 88.4% and an average preparation QBER of only 0.44%. This means, that the two bases used by Alice to encode her bits are quite well mutually unbiased, which is an important requirement for an efficient key exchange. For comparison, the hand-held sender module achieved a preparation quality of 75% [20].

Revisiting the drawbacks (see Section 5.3) of the formerly used WGPs, it has to be stated, that the transmission of unpolarized light through the macroscopic sheet polarizer is more than three times the transmission through the gold polarizers, namely 35%. Furthermore, the unwanted backreflection of the other polarization components is almost completely overcome with the synthetic polarizer strips. This will allow to omit the additional ND filter (transmission ≈ 8%, [54]) used in the hand-held optical package, resulting in a further increase of the overall module transmission by about one order of magnitude. One other important parameter of the polarizer array is the extinction ratio of the miniature foil polarizers. For all four polarizers, this was measured to be between 1:2000 and 1:2500, exceeding the performance of the WGPs of the hand-held module.

Polarizer	Alice 2.0 input	desired optimal input state	polarizer angle [°]	measured state	(2D) polarizer angle [°]	DOP
V	1	$\begin{pmatrix}-0.9893\\0.1461\\0\end{pmatrix}$	85.8	$\begin{pmatrix}-0.9927(1)\\0.1250(42)\\-0.0155(43)\end{pmatrix}$	86.4	1.001(1)
P	2	$\begin{pmatrix}0.0454\\0.9990\\0\end{pmatrix}$	42.5	$\begin{pmatrix}0.0435(43)\\0.99569(3)\\-0.0094(43)\end{pmatrix}$	43.7	0.9967(2)
H	3	$\begin{pmatrix}0.9744\\-0.2250\\0\end{pmatrix}$	-6.5	$\begin{pmatrix}0.9894(1)\\-0.1323(42)\\0.0080(43)\end{pmatrix}$	-3.8	0.9982(6)
M	4	$\begin{pmatrix}-0.2045\\-0.9789\\0\end{pmatrix}$	-50.9	$\begin{pmatrix}-0.1602(42)\\-0.9875(1)\\-0.0293(43)\end{pmatrix}$	-49.6	1.001(1)

Table 5.2: Summary of the expected and measured polarization states and angles, with the measured degree of polarization. The polarization states are expressed as the three Stokes components $(S_1\ S_2\ S_3)^\intercal$. The stated polarizer angle is calculated from the two-dimensional projection of the polarization state onto the xy-plane of the Poincaré sphere.

Alice 2.0 input	input polarizer angle [°]	measured output state	(2D) output polarization angle [°]	single state QBER	DOP
1	86.4	$\begin{pmatrix}-0.99638(3)\\-0.0147(43)\\-0.0776(4)\end{pmatrix}$	90.4	0.00181(1)	0.9995(3)
2	43.7	$\begin{pmatrix}-0.0004(43)\\-0.9929(1)\\-0.0666(43)\end{pmatrix}$	-45.0	0.00355(3)	0.9951(3)
3	-3.8	$\begin{pmatrix}0.9847(1)\\-0.0746(43)\\0.1442(42)\end{pmatrix}$	-2.2	0.0077(1)	0.9979(7)
4	-49.6	$\begin{pmatrix}0.0094(43)\\0.9906(1)\\0.1026(42)\end{pmatrix}$	44.7	0.00468(4)	0.9960(4)

Table 5.3: Summary of the measured output states of the waveguide circuit when used with the polarizer array. The stated polarizer angle is calculated from the two-dimensional projection of the polarization state onto the xy-plane of the Poincaré sphere. The four states have an average BB84 QBER of 0.44% and achieve a preparation quality of $(88.4 \pm 0.6)\%$.

5.4 Summary of the experimental results

Within this section, important developments in two key parts of the QKD sender unit were shown. Firstly, the applicability of the modular electronics design was proven by measuring the optical pulses emitted by the VCSELs connected to different subboards. Furthermore, a novel pulse generation scheme using configurable hard-wired delays instead of delay chips has been implemented and tested, showing almost identical results and thus allowing to reduce the power consumption of the module's electronics by about 50%. Secondly, the polarization preparation within the optical module was modified, using synthetic foil polarizers in place of the WGPs of the hand-held implementation. The results presented in this section show, that the developed preparation and assembly process yields polarizer arrays matching and exceeding the performance of the formerly used solution, while not showing some of their negative properties.

Chapter 6

Conclusion and outlook

QKD enables the authenticated users to securely generate and distribute a secret encryption key and is thus important for establishing a secure communication network, especially in light of the threat quantum computers pose for current cryptographic systems. For this, any practical QKD system has to be seemlessly combined with conventional communication infrastructure. Compact integration of a free-space QKD system is mandatory, as it will enable hand-held applications or possibly even key exchanges between a ground station and high-altitude platforms or satellites.

Within this work, some of the modifications on a hand-held QKD sender device necessary towards a high-altitude platform implementation have been introduced and developed. In addition, the performance of a realistic device and link parameters for a flying HAP and a LEO satellite have been analyzed, in order to quantify the achievable key rates for different implemented protocols. While this showed promising results for the HAP scenario with key rates in the range of kbit/s, it made it obvious that for a secure key exchange between a CubeSat and a ground station, the link efficiency will have to be significantly increased.

Concerning the modifications of the sender unit, first the pulse generation within the driving electronics has been tackled. By replacing the formerly used delay chips with stripline meanders of configurable length, the signal quality could be conserved while allowing for a significant reduction of the required power. Not only will this reduced power consumption of the driving electronics be advantageous in the low power environment of a HAP or satellite, but it will also lead to less heat generation, which could have been problematic in low pressure environments.

A second modification, this time of the optical package of the device, was the development and realization of a new concept for the polarizer array used to prepare the four linear BB84 polarization states. Using a synthetic polarizer foil, the undesirably low transmission of the formerly used WGPs (9%) could be increased to 35% without sacrificing the high degree of polarization (all above 1:2000); furthermore, significantly reducing the backreflection of non-transmitted light allows to omit the additional filter foil used between VCSELs and the WGP array in the hand-held module.

While these results are important steps towards the implementation of our compact QKD sender unit in a high-altitude environment, there are still open tasks: The characterization of the entire module under thermal vacuum conditions, or, in order to use the decoy state extension of the BB84 protocol, the possibility to switch between different pulse intensities. These steps will further enhance the applicability of this method for a variety of free-space-communication platforms.

Bibliography

[1] D. Lewis, “icloud data breach: Hacking and celebrity photos.” Forbes, `https://www.forbes.com/sites/davelewis/2014/09/02/icloud-data-breach-hacking-and-nude-celebrity-photos/#4466625a2de7`, 2014 (accessed on 2019-03-22).

[2] “2016 presidential campaign hacking fast facts.” CNN, `https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html`, 2018 (accessed on 2019-03-22).

[3] N. Perlroth and C. Krauss, “A cyberattack in saudi arabia had a deadly goal. experts fear another try..” New York Times, `https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html`, 2018 (accessed on 2019-03-22).

[4] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[6] NIST, “Announcing the advanced encryption standard.” Federal Information Processing Standards Publication, 197, 2001.

[7] G. S. Vernam, “Secret signaling system.” US PATENT US 1310719A, 1919.

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[10] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics*, vol. 8, no. 8, p. 595, 2014.

[11] S. Wiesner, “Conjugate coding,” *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[12] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pp. 175–179, 1984.

[13] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[14] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, *et al.*, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[15] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, "Field test of quantum key distribution in the tokyo qkd network," *Optics express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[16] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Physical review letters*, vol. 121, no. 19, p. 190502, 2018.

[17] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, p. 43, 2017.

[18] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, *et al.*, "Satellite-relayed intercontinental quantum network," *Physical review letters*, vol. 120, no. 3, p. 030501, 2018.

[19] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, "Satellite-based qkd," *Optics and Photonics News*, vol. 29, no. 2, pp. 26–33, 2018.

[20] G. Vest, P. Freiwang, J. Luhn, T. Vogl, M. Rau, W. Rosenfeld, and H. Weinfurter, "Quantum key distribution with a hand-held sender unit." in preparation, 2019.

[21] J. Von Neumann, *Mathematical Foundations of Quantum Mechanics: New Edition.* Princeton University Press, 2018.

[22] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Annals of Physics*, vol. 191, no. 2, pp. 363–381, 1989.

[23] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[24] S. Barnett, *Quantum information*, vol. 16. Oxford University Press, 2009.

[25] B. E. Saleh and M. C. Teich, *Fundamentals of photonics*, vol. 22. Wiley New York, 1991.

[26] J. Katz and Y. Lindell, *Introduction to modern cryptography.* CRC press, 2014.

[27] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[28] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[29] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.*, p. 136, IEEE, 2004.

[30] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, vol. 92, no. 5, p. 4, 2004.

[31] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Physical Review Letters*, vol. 89, no. 3, pp. 379021–379023, 2002.

[32] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, pp. 1–3, 2005.

[33] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 410–423, Springer, 1993.

[34] R. Gallager, "Low-density parity-check codes," *IRE Transactions on information theory*, vol. 8, no. 1, pp. 21–28, 1962.

[35] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[36] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," *Physical review letters*, vol. 89, no. 18, p. 187901, 2002.

[37] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Physical Review A*, vol. 51, no. 3, p. 1863, 1995.

[38] M. Dušek, O. Haderka, and M. Hendrych, "Generalized beam-splitting attack in quantum cryptography with dim coherent states," *Optics communications*, vol. 169, no. 1-6, pp. 103–108, 1999.

[39] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Physical Review Letters*, vol. 85, no. 6, p. 1330, 2000.

[40] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[41] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical review letters*, vol. 94, no. 23, p. 230503, 2005.

[42] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, no. 23, p. 230504, 2005.

[43] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A*, vol. 72, no. 1, p. 012326, 2005.

[44] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Physical Review A*, vol. 74, no. 2, p. 022313, 2006.

[45] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, no. 7, p. 073024, 2011.

[46] 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 Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 187–191, 2015.

[47] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature photonics*, vol. 4, no. 10, p. 686, 2010.

[48] S. Nauerth, F. Moll, M. Rau, J. Horwath, S. Frick, C. Fuchs, and H. Weinfurter, "Air to ground quantum key distribution," in *Quantum Communications and Quantum Imaging X*, vol. 8518, p. 85180D, International Society for Optics and Photonics, 2012.

[49] C. H. F. Fung, K. Tamaki, and H. K. Lo, "Performance of two quantum-key-distribution protocols," *Physical Review A - Atomic, Molecular, and Optical Physics*, vol. 73, no. 1, pp. 1–19, 2006.

[50] K. Liu, J. Wei, C.-M. Zhang, and Q. Wang, "Passive decoy-state quantum key distribution with the SARG04 protocol," *Journal of the Optical Society of America B*, vol. 35, no. 5, p. 1066, 2018.

[51] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, "2 ghz clock quantum key distribution over 260 km of standard telecom fiber," *Optics letters*, vol. 37, no. 6, pp. 1008–1010, 2012.

[52] C. Branciard, N. Gisin, and V. Scarani, "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography," *New Journal of Physics*, vol. 10, no. 1, p. 013031, 2008.

[53] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, *et al.*, "Chip-based quantum key distribution," *Nature communications*, vol. 8, p. 13984, 2017.

[54] G. Mélen, *Integrated Quantum Key Distribution Sender Unit for Hand-Held Platforms.* PhD thesis, Ludwig-Maximilians University Munich, 2016.

[55] P. Freiwang, "Towards hand-held quantum key distribution," Master's thesis, Ludwig-Maximilians University Munich, 2017.

[56] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, "Design and evaluation of a handheld quantum key distribution sender module," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, pp. 131–137, May 2015.

[57] R. Michalzik, *VCSELs: fundamentals, technology and applications of vertical-cavity surface-emitting lasers*, vol. 166. Springer, 2012.

[58] G. Mélen, W. Rosenfeld, and H. Weinfurter, "Impact of the slit geometry on the performance of wire-grid polarisers," *Optics Express*, vol. 23, no. 25, pp. 32171–32178, 2015.

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

[60] C. Sonnleitner, "Towards a practical integrated qkd sender," Master's thesis, Ludwig-Maximilians University Munich, 2018.

[61] E. Hammerstad and O. Jensen, "Accurate models for microstrip computer-aided design," in *Microwave Symposium Digest, 1980 IEEE MTT-S International*, pp. 407–409, IEEE, 1980.

[62] E. H. Land, "Some aspects of the development of sheet polarizers∗," *J. Opt. Soc. Am.*, vol. 41, pp. 957–963, Dec 1951.

[63] Y. Dirix, T. Tervoort, and C. Bastiaansen, "Optical properties of oriented polymer/dye polarizers," *Macromolecules*, vol. 28, no. 2, pp. 486–491, 1995.

[64] Y. Dirix, T. A. Tervoort, and C. Bastiaansen, "Optical Properties of Oriented Polymer/Dye Polarizers. 2. Ultimate Properties," *Macromolecules*, vol. 30, no. 7, pp. 2175–2177, 1997.

[65] R. Osellame, "Alice 2.0 report," tech. rep., Politecnico di Milano, 2015.

[66] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature communications*, vol. 3, p. 634, 2012.

[67] M. J. Hall, "Information exclusion principle for complementary observables," *Physical review letters*, vol. 74, no. 17, p. 3307, 1995.

Danksagung

Danke.

Danke an alle, die mich im Verlauf meines Studiums unterstützt und dadurch diese Masterarbeit ermöglicht haben.

Hervorzuheben ist hier insbesondere Prof. Dr. Harald Weinfurter, da er mir durch die Aufnahme in seine Gruppe die Möglichkeit zur Mitarbeit an solch spannenden Projekten geboten hat. Du warst stets freundlich, hilfreich und geduldig in Deiner Betreuung, wofür ich Dir sehr dankbar bin.

Ohne die tägliche Zusammenarbeit mit und Betreuung durch Peter hätte es diese Arbeit nicht gegeben, weshalb ich Dir zu immensem Dank verpflichtet bin. Ich konnte mich immer darauf verlassen, dass Du mir unter die Arme greifst, wenn ich einmal vor unlösbar scheinenden Problemen stehe. Außerdem hat nicht zuletzt unser gemeinsames Büro dazu geführt, dass ich im letzten Jahr nicht verzweifelt bin sondern, im Gegenteil, großen Spaß an der Arbeit hatte.

Persönlich bedanke ich mich hiermit auch bei Wenjamin, dafür, dass du trotz deiner vielen Aufgaben nie müde wurdest, mich bei verschiedensten Problemen zu unterstützen. Nicht selten konnte ich erst im Gespräch mit Dir die entsprechenden Lösungen finden.

Weiterhin gilt mein Dank allen Mitgliedern unserer Gruppe, die in jeder Situation hilfsbereit waren, sei es bezüglich fachlicher Fragen oder durch die Garantie einer guten und freundschaftlichen Stimmung in der Arbeitsgruppe. Ich werde stets mit guten Gedanken auf die vergangenen zwölf Monate mit Euch allen zurückblicken.

Zu guter Letzt danke ich meiner Familie und meinen Freunden, welche mir seit Beginn meines Studiums geholfen haben, eine gesunde Balance zwischen der Welt der Physik und einem entspannten Privatleben zu finden und zu halten.

Declaration

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

München, den 01.04.2019

Jacob Birkmann