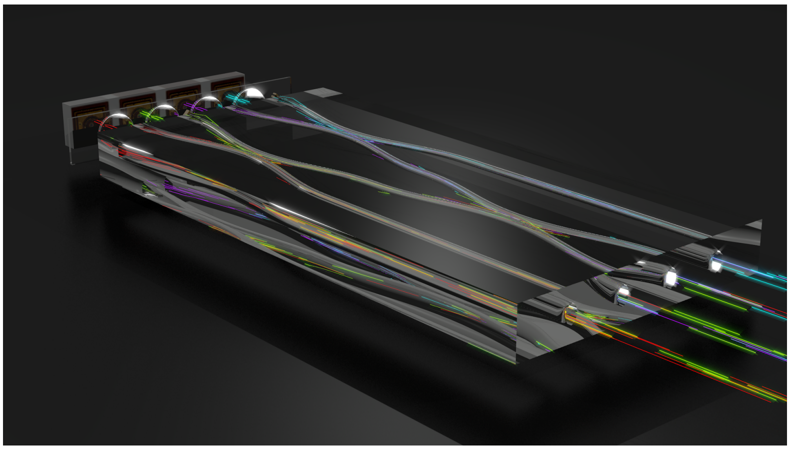
Department für Physik
Ludwig-Maximilians-Universität München

Master's Thesis

Quantum Key Distribution with Integrated Optical Circuits



Stefan Frick

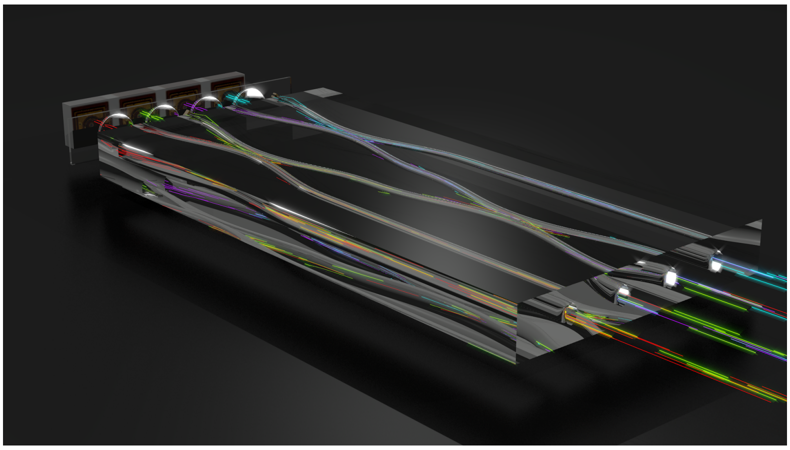
March 28, 2013

Supervised by
Prof. Dr. Harald Weinfurter

Department für Physik
Ludwig-Maximilians-Universität München

Masterarbeit

Quantenkryptografie mit Integrierten Optischen Schaltkreisen



Stefan Frick

28. März 2013

Betreut durch
Prof. Dr. Harald Weinfurter

"The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace."
Eric Hughes - A Cypherpunk's Manifesto

Contents

1 Introduction

In our modern society, information has become a valuable commodity, whose range of application extends from personalized advertisement on search engine web pages to governmental intelligence. Information leakage to the wrong hands can often cause severe damage to private persons or even nations. Therefore cryptography has been used by humanity for centuries, from first shift ciphers to modern public-key cryptography, to protect the valuable good information. Today, public-key encryption is the basis of all secure transactions taking place in the world wide web. Since the internet has gained such a big influence on our everyday life, the importance of those algorithms cannot be overstated.

Yet, in the last years more and more flaws were detected and could be exploited, in even the most modern cryptographic methods [1, 2]. Although those loopholes do not fully spoil the security of today's encryption methods, further developments in numerical mathematics could indeed make those algorithms obsolete, since they are not provable secure. In addition, Feynman proposed in 1982 a quantum device able of executing algorithms exploiting the laws of quantum mechanics, the quantum computer [3, 4]. Such a quantum computer, as shown by Shor in 1994 [5], is able to efficiently break modern encryption within reasonable times. Since first steps towards implementations of the quantum algorithm proposed by Shor were successfully taken [6–8], the only remaining provable secure encryption method known today is the one-time pad. This encryption method can be combined together with Quantum Key Distribution (QKD) to establish a long term secure communication between two nodes, commonly named Alice and Bob.

QKD [9] exploits the laws of quantum mechanics for a secure distribution of a key between two communication nodes, by transmitting quantum states over a so called quantum channel. Secure, in this manner, means that information leakage to an adversary by a possible attack on the key transmission can be detected by Alice and Bob. Therefore, the fraction of the key known to a third party can be estimated by an upper bound.

Since first commercially available QKD systems are already available [10] and trusted note networks were successfully demonstrated [11], the ambitious goal for the future is to establish a world-wide QKD network. As attenuation in fibers and free-space quantum channels, however, limits the transmission length of terrestrial QKD to a few 100 km, a global QKD network can only be achieved using satellite based systems [12, 13]. A big step towards such a satellite systems was recently demonstrated by Nauerth et.al. [14], where QKD with fast moving airborne platforms was found feasible. In addition in [15] it was shown, that QKD can be established with a free-space quantum channel over 144 km, comparable to a link with a satellite in low earth orbit.

A promising new development in the field of quantum optics are integrated optical circuits, which are wave guiding structures, fabricated by ultra-fast laser writing in a bulk glass sample or by lithography. The big advantages of integrated optics are, that many optical components can be combined "on-chip" in a small volume and that the fabrication process is rather easy.

By combining QKD with integrated optical circuits, it is possible to enable a complete new kind of portable hand-held QKD transmitter modules, which can be realized in a form factor so small, that even the integration of such devices into smartphones becomes conceivable in the future. A first demonstration of a hand-held QKD transmitter is presented in [16], which is aimed at future automated teller machine (ATM) applications.

In this Thesis I will present the work done towards a miniaturized QKD sender using integrated optical circuits.

2 Theoretical Prerequisites

In this chapter I want to present theoretical prerequisites and depict the requirements necessary for a successful QKD. The components designed, built and characterized as part of this thesis have to comply with these requirements.

I will start by giving the reader an idea of the scenario in which QKD finds its application and will describe the problems inherent to classical encryption methods nowadays and to which extend they can be regarded to be secure. QKD can overcome those problems by using one of various protocols which exploit the laws of quantum mechanics to establish a secure key distribution between two remote communication nodes. In the following the BB84 protocol [17] is introduced, since it is the most commonly known and used protocol for QKD.

2.1 QKD Scenario

A typical scenario in modern communication is that two parties commonly named Alice and Bob share a classical, bidirectional communication channel which they can use to exchange messages. In general, eavesdropping on such a communication cannot be ruled out, as such a channel typically bridges several hundreds of kilometers and is publicly accessible. Therefore the exchange of confidential information over a classical channel requires encryption.

To ensure that information stays unknown to a possible adversary, usually named Eve, modern asymmetric encryption methods, such as RSA [18], rely, only on the computational complexity of the encryption algorithm, assuming that an adversary will not have enough resources to break the encryption. In the example of RSA this complexity lies in the difficulty to prime factorize large numbers, since there is no existing, efficient (i.e. polynomially scaling) algorithm for that task. Yet, a breakthrough in mathematics could spoil the security of these methods.

Today, the one-time pad, also referred to as Vernam cipher, is the only method known, ensuring an information theoretically secure transmission of secret messages. The one-time pad needs a pre-shared key between Alice and Bob, beforehand the transmission. Alice uses the key to encrypt the message by adding every bit of the message to the key modulo 2. Bob uses the same key for the decryption of the message by subtracting the bit values of the key again. Therefore, methods using the same key for en- and decryption are called symmetric. The key has to be of the same length as the message and must only be used once, because only then the secrecy of the message is guaranteed. This is because, the randomness of the key is transferred to the encrypted message by the addition modulo 2, hence the encrypted text has full Shannon entropy [19]. Yet, on a long time scale Alice and Bob would have to meet over and over again to exchange new keys, which is a huge disadvantage of all symmetric encryption methods.

In 1984 Bennett and Brassard came up with an idea to circumvent this problem: the BB84 protocol. This protocol can be used to distribute a mutual key between Alice and Bob in a secure way by exploiting two fundamental properties of quantum mechanics.

First, quantum mechanics predicts, that a general, unknown quantum state can't be copied perfectly, as stated in the no-cloning theorem [20]. This can be easily seen, if one assumes an unitary copying operator U, such that

$$U|\,\Psi\rangle|\,i\rangle = |\,\Psi\rangle|\,\Psi\rangle, \tag{2.1}$$

where $|\,i\rangle$ is an initial state and $|\,\Psi\rangle$ is the state to copy. For $|\,\Psi\rangle = \alpha|\,a\rangle + \beta|\,b\rangle$ being a liner combination of two states then holds

$$U|\,\Psi\rangle|\,i\rangle = U\left(\alpha|\,a\rangle|\,i\rangle + \beta|\,b\rangle|\,i\rangle\right) = \alpha|\,a\rangle|\,a\rangle + \beta|\,b\rangle|\,b\rangle, \tag{2.2}$$

which, however, is unequal to $|\,\Psi\rangle|\,\Psi\rangle$. Thus, in general, an unknown quantum state cannot be cloned perfectly, only up to some fidelity.

A second property of quantum mechanics is, that in general one cannot measure a quantum system without perturbing it. Thus, any attempt of Eve to gain information from a quantum system, transmitted from Alice to Bob, will alter the transmitted state, which can be used to detect the adversary, as will be shown later.

By adding a unidirectional quantum channel, through which information encoded in quantum states can be transmitted from Alice to Bob, to the classical scenario described before, it is possible to make the laws of quantum mechanics available to communication applications (fig. 2.1). Analogously to classical information measured in bits, information encoded in quantum states is named qubit. A classical bit can either take the value '1' or '0', whereas a qubit $|\,\psi\rangle$ can be in any superposition of two states

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

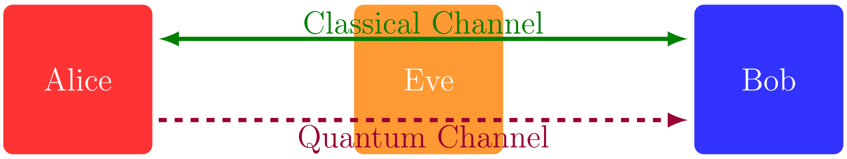


Figure 2.1: Scenario typical to modern communication. Alice and Bob share a classical communication channel on which, however, eavesdropping cannot prevented. In the QKD scenario a additional quantum channel is added to transmit quantum states from Alice to Bob.

where $|\alpha|^2 + |\beta|^2 = 1$ and $\alpha, \beta \in \mathbb{C}$. This means, that a qubit, contrary to a classical bit and in marked contrast to the human intuition, can take the values '0' and '1', corresponding to the respective states, at the same time.

The BB84 protocol is a possibility to use qubits transmitted via a quantum channel together with an authorized classical channel for a secure key generation between Alice and Bob.

2.2 The BB84 Protocol

The BB84 protocol consists in principle of six steps:

1. State Preparation,
2. Measurement,
3. Sifting,
4. Error Estimation,
5. Error Correction,
6. Privacy Amplification,

where only the first two are "quantum" and the others work in a complete classical way.

In the first step Alice starts with preparing a quantum state by randomly choosing one of two orthogonal bases, which are mutually unbiased to each other (see fig. 2.2). For example, such bases could be the eigenbases of the Pauli-Matrices σ_z and σ_x. Further Alice chooses, also randomly, whether she wants to prepare the $|\,0_i\rangle$ or $|\,1_i\rangle$ state, where $i \in \{x, z\}$ indicates the basis chosen before.

Note that the transformation between the bases is given by

$$|\,0_z\rangle = \frac{|\,0_x\rangle + |\,1_x\rangle}{\sqrt{2}} \tag{2.4}$$

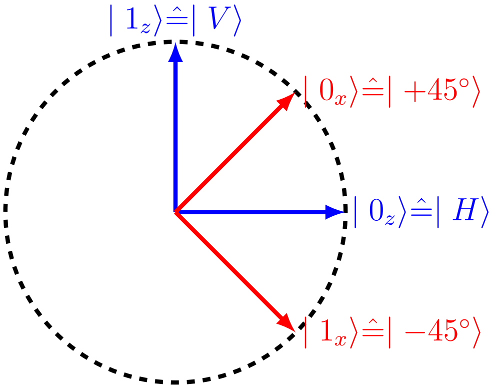

$| 1_z\rangle \hat{=} | V\rangle$
$| 0_x\rangle \hat{=} | +45°\rangle$
$| 0_z\rangle \hat{=} | H\rangle$
$| 1_x\rangle \hat{=} | -45°\rangle$

Figure 2.2: The four quantum states used for the BB84 protocol. The two mutually unbiased, orthogonal bases are depicted in blue and red, respectively. The vectors shown illustrate the states as polarizations of light. Each state confines an angle of 45° with his neighbor.

and

$$| 1_z\rangle = \frac{| 0_x\rangle - | 1_x\rangle}{\sqrt{2}}. \tag{2.5}$$

This leads to

$$|\langle 0_x \mid 0_z\rangle|^2 = |\langle 0_x \mid 1_z\rangle|^2 = |\langle 1_x \mid 0_z\rangle|^2 = |\langle 1_x \mid 1_z\rangle|^2 = \frac{1}{2}, \tag{2.6}$$

meaning that the outcomes '0' or '1', according to the states $| 0\rangle$ and $| 1\rangle$, are both found with probability 1/2, if the measurement is carried out in the opposite basis than the state was prepared in.

After preparing a photon in such a state, Alice sends the qubit two Bob, who measures the qubit in one of the two, again randomly chosen bases, and who will find the outcome '1' or '0'. If the basis choice of Alice and Bob coincide, Bob's outcome will always be identical with the state Alice prepared. Otherwise the result is uncorrelated.

In the third step, after the qubits are measured, Alice and Bob publicly announce their basis choices to each other and dismiss all measurements where they didn't coincide or the qubit was lost due to attenuation in the quantum channel. Doing so, they will lose half of the received signals on average, but will ideally end up with a perfectly correlated key, called sifted key. The whole procedure is displayed as an example in table 2.1.

At this point, it is worth to pause the description of the protocol to clarify the influence a possible eavesdropper has on the sifted key, since this motivates all of the following steps of the BB84 protocol.

Alice' Basis	X	X	Z	X	Z	Z	Z	X
Alice' State	$\mid 1_x\rangle$	$\mid 0_x\rangle$	$\mid 1_z\rangle$	$\mid 1_x\rangle$	$\mid 1_z\rangle$	$\mid 0_z\rangle$	$\mid 1_z\rangle$	$\mid 0_x\rangle$
Bob's Basis	X	Z	Z	Z	X	X	Z	X
Bob's Outcome	1	0	1	0	1	0	1	0
Sifted key	1		1				1	0

Table 2.1: An example for the procedure of the BB84 protocol. Where the basis choice of Alice and Bob coincide they find the same state and can thereby generate a mutual key.

The most straight forward attempt for an attack is the intercept and resend strategy, where an eavesdropper intercepts the transmission of the qubit and, as he cannot make a perfect copy of the qubit, measures it. The adversary then prepares a new qubit, according to the outcome of his measurement, and resends it to Bob. Since the basis choices have not been announced at this stage of the protocol Eve has to guess the basis and will thereby prepare a wrong state in 50% of the cases. Nevertheless, this erroneous states will only produce the wrong outcome at Bob's side in again 50% of the cases. This means that Eve will introduce an error of 25% in the sifted key. This error, found in the sifted key, is named quantum bit error ratio (QBER) analogously to the error in classical communication: the bit error ratio (BER). More sophisticated attacks, however, will lead to lower QBERs. Nevertheless, the QBER can always be used by Alice and Bob to determine an upper bound of the information an adversary has possibly gained by an attack.

In the 3rd step of the protocol, Alice and Bob now exploit the influence of Eve's measurements on the qubits by sacrificing a fraction of their exchanged key and compare it via the classical channel to determine the QBER.

Since also technical imperfections of the transmitter and receiver modules cause errors, eavesdropping and technical noise cannot be distinguished in general. Hence, measures, such as error correction and privacy amplification, have to be taken to distill a perfect secure key from the sifted key.

During the error correction step, wrong bits in Bob's version of the sifted key are reconciled. One of the most widely known algorithms applied for this, is CASCADE [21], where the parity of subsequently smaller getting blocks of key is recursively compared over the classical channel. If the parity of a block is the same, the block is assumed to be identical for Alice and Bob. If not, the block is subdivided into smaller parts and the parity is compared again. Of course the announcement of parities over the classical channel leaks information to the adversary, because the parity contains information about the bits in each block. In information theory it can be shown that the information one has to reveal for error correction is at least the Shannon entropy of the detected QBER $H_2(QBER)$.

The amount of information a possible adversary may know at this point of the protocol is the sum of the information gained by an attack as determined by the QBER and $H_2(QBER)$ leaked to Eve during the error correction process. The key is consequently shrunken during the privacy amplification step [22] by this amount of information Eve can possibly know. This is realized with so called hash functions, which are characterized by the fact that slightly different input values yield completely different output values. Hash functions used for privacy amplification accept the error corrected key as an input and transform it into a new key, shortened by the information an eavesdropper could have maximally obtained during the previous steps of the protocol. This is why Eve cannot know a single bit of the privacy amplified key, which is thereby perfectly secure for encrypting confidential messages with an one-time pad. For more detailed descriptions of error correction and privacy amplification refer to [9].

Realistic implementations of QKD transmitters often use attenuated laser light, since it offers a very convenient way of light generation. Lasers emit light in faint pulses with a mean photon number per pulse μ. These pulses cannot be regarded as true single photons, because the probability to find a pulse with n photons follows a Poissonian distribution

$$P(n) = \mathrm{e}^{-\mu^2} \cdot \frac{\mu^n}{n!}. \tag{2.7}$$

This lack of true single photon sources needs an adaption of the QKD protocol, which is realized within the decoy protocol described in e.g. [23, 24].

2.3 Stokes Vector, Mueller Calculus, and Degree of Polarization

One possible implementation for the BB84 protocol is to encode the qubits in polarization states of light. Any polarization can be described

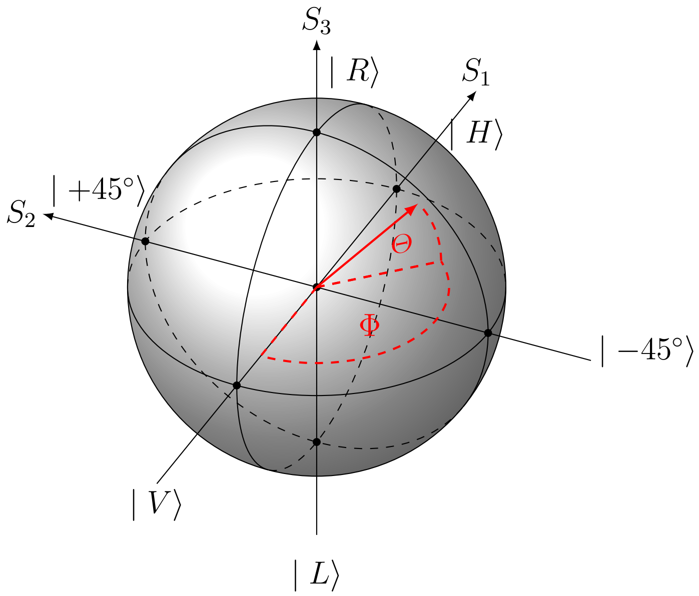


Figure 2.3: A polarization state represented as a vector on the Poincaré sphere, depicted in red and determined by the two angles Φ and Θ. The three Stokes parameters represent the projections on the principal axes of the sphere.

by two angles on the Poincaré sphere, the azimuth Φ and the elevation Θ as shown in figure 2.3. According to this vertical polarized light would correspond to an azimuth of $\Phi = 180°$ and an elevation of $\Theta = 0°$ and right circular light would correspond to an elevation of $\Theta = 90°$ and an undefined azimuth. Additionally it can be seen that, the vectors describing a horizontal and +45° polarization confine an angle of 90° on the Poincaré sphere, whereas in polarization space this angle sums up to 45°. The representation on the Poincaré sphere doubles the angle compared to the real polarization space.

The projections of the polarization vector on the principal axes of the Poincaré sphere yield the three Stokes parameters S_1, S_2 and S_3, respectively. A fourth Stokes parameter S_0 is used as a normalization and represents the intensity of the light. Since those four parameters are usually combined into the Stokes vector, the vector

$$\vec{S} = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{2.8}$$

would describe horizontally polarized light. This notation is also able to express light which is not fully or not at all polarized.

$$\vec{S} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{2.9}$$

describes completely unpolarized light, which would correspond to a point in the center of the Poincaré sphere, i.e. fully polarized states are drawn on the surface of the Poincaré sphere with radius S_0, wheres states describing partially polarized light are lying between the surface and the origin as it is depicted in figure 2.3.

With that, one can define the degree of polarization (DOP) of light as

$$\mathrm{DOP} = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0}, \tag{2.10}$$

which expresses the fraction of the intensity which is polarized. It is notable that the Stokes vector can be normalized by multiplying each stokes parameter with $1/S_0$. This normalized Stokes vector then describes light of intensity 1, where S_1, S_2 and S_3 all exhibit values ≤ 1.

Optical elements influencing the polarization of light can be described as matrices acting on the Stokes vector. This method is called Mueller calculus and the respective matrices are named Mueller matrices. For example the action of a horizontal polarizer on unpolarized light is described by

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ 0 \\ 0 \end{pmatrix}. \tag{2.11}$$

From that it can be seen that the intensity S_0 became half of the intensity before the polarizer, nevertheless the DOP increased from 0 to 1. In general, a polarizer, oriented in any direction, will always allow half of the unpolarized fraction contained in the light to pass, whereas the transmission of the polarized part depends on the orientation of the polarizer.

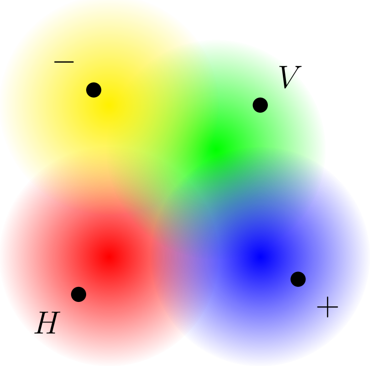


Figure 2.4: Illustration of only partially overlapped beams from four different laser diodes. The dots depict points where Eve can surely distinguish between the four settings, without measuring the polarization. The four different modes from the laser diodes are colored for better understanding.

2.4 Requirements for QKD Devices

A secure realization of a QKD sender and transmitter pair, not only has to comply with the protocol, but in addition the emergence of side channels has to be treated very carefully. In QKD side channels are giving an eavesdropper the possibility to gain information about the key, by exploiting an imperfect physical implementation of the cryptography.

Because the creation and preparation of photons in certain polarizations is technically relatively easy and since quantum channels for photons already exist in form of free-space optical links or optical fibers, many implementations [14, 15, 25] work with four different laser diodes to prepare the four polarization states $|\,H\rangle$, $|\,V\rangle$, $|\,{+45°}\rangle$ and $|\,{-45°}\rangle$ according to $|\,0_z\rangle$, $|\,1_z\rangle$, $|\,0_x\rangle$ and $|\,1_x\rangle$ from section 2.2. The use of four different laser diodes gives rise to many side channels, which have to be closed for a secure QKD device. In such an implementation, side channels are degrees of freedom which are coupled to the polarization and differ for the four diodes.

For example, the spatial modes emitted from those four diodes have to be perfectly overlapped. Otherwise, like shown in fig 2.4, an eavesdropper will immediately know which state Alice prepared, if he finds a photon in an area where it could only be emitted from one diode. By additionally blocking areas where the modes do overlap, Eve will gain the complete information about the key without introducing any QBER and therefore will not be detected.

Due to deviations in the manufacturing process of the laser diodes, one also has to check for the spectral indistinguishability of the four diodes. Supposed the laser diodes emit light on different wavelengths and/or their spectra have unequal bandwidths, the adversary is again placed in a situation, where he can distinguish perfectly between the four laser diodes and use it to gain full information about the key without perturbing the measurements on Bob's side.

Another side channel arises from timing issues. Since any of the four laser diodes consecutively prepares one of the polarizations states used for quantum cryptography, only one is switched on at a time. This happens with a certain repetition rate f_{rep} and a defined pulse width Δt. Meaning that if a certain state should be prepared, the respective laser diode should be turned on at times multiple to $T = 1/f_{rep}$ and is turned off again after Δt. In realistic implementations there will be slight differences between the electronics driving the laser diodes and between the diodes themselves, resulting in a different timing for the diodes. By resolving the pulses in time the eavesdropper could again distinguish between the four diodes.

Summing up, an Alice module preparing photons in different polarization states, must do this in a way, such that the photons, encoding the qubits, are identical in any other degree of freedom than the polarization.

Along with side-channels, an erroneous state preparation also shrinks the available key at the end of the protocol and can eventually spoil the security of the device. This can be easily seen for the case where the second basis deviates maximally, so that it coincides with the first basis. In this case, every time when Alice thinks she prepared a state in the $\{|+45°\rangle, |-45°\rangle\}$ bases and Bob then measures it in this basis, he will find the wrong outcome in 50%, yielding a QBER of 25%, which will be interpreted as the influence of an adversary and thus the key will be discarded. In fact, any interception by Eve wouldn't cause any further QBER because she only has to measure one basis. Yet, Eve doesn't know the basis Bob will measure the resent qubit in. Hence the resulting QBER will remain as high as 25%. However, if Bob's measurement is also erroneous the security of device is endangered.

Besides a proper state preparation, the random numbers determining the basis choice and the state prepared on Alice's side need to be generated in a way, such that an eavesdropper can neither predict nor influence them. As numbers from pseudo random number generators can be predicted, they cannot be used for a secure QKD setup. That is why hardware quantum random number generators relying on the laws of quantum mechanics [26] are needed for QKD applications. Or, as it is supposed to be said by John von Neumann: “Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.”

On the receiver side of a QKD setup, detectors sensitive to very weak intensities are necessary, since the information is encoded on the single photon level. For this purpose one has to use avalanche photo diodes (APDs) which suffer from dark counts and which will detect stray light from the environment, too. The clicks from an APD produced by dark counts and background, though, are equally distributed in time. Contrary to that, clicks occurring from light, which was send from the QKD transmitter, only appear at distinct time slots. These time slots are Δt long and start at times multiple to $1/f_{rep}$. By accepting only clicks within these time slots, the chance that a click from dark counts or background contributes to the measurement becomes small. This also imposes the generation of sufficiently short pulses on the QKD sender, since shorter pulse widths Δt enable a stricter time filtering, and thereby reduce the effect of background and dark counts. This is important, because those clicks increase the QBER and thereby limit the available secure key at the end of the protocol.

2.5 Scheme for a Hand-Held QKD Sender

Subject of this thesis are the characterization and setup of single components which are planed to become part of a hand-held QKD sender. A sketch of the final setup is shown in figure 2.5.

In this scheme, four vertical-cavity surface-emitting lasers (VCSELs), arranged in an array and used as a light source, are driven to emit light in faint pulses. VCSELs are well-suited for the application together with waveguides, since their round emission pattern couples efficiently to waveguides. In addition they exhibit a good power efficiency and thereby consume less energy for the same power output. Both properties make them well suited for a hand-held, portable QKD transmitter. The light from the VCSELs is focused by a micro-lens array onto the input facets of one of four waveguides, respectively.

Behind each of the micro-lenses a wire-grid polarizer, consisting of small gold stripes, is used to prepare the light emitted from each VCSEL in one of the four polarization states $\mid H\rangle$, $\mid V\rangle$, $\mid +45°\rangle$ or $\mid -45°\rangle$, corresponding to the state preparation step in the BB84 protocol.

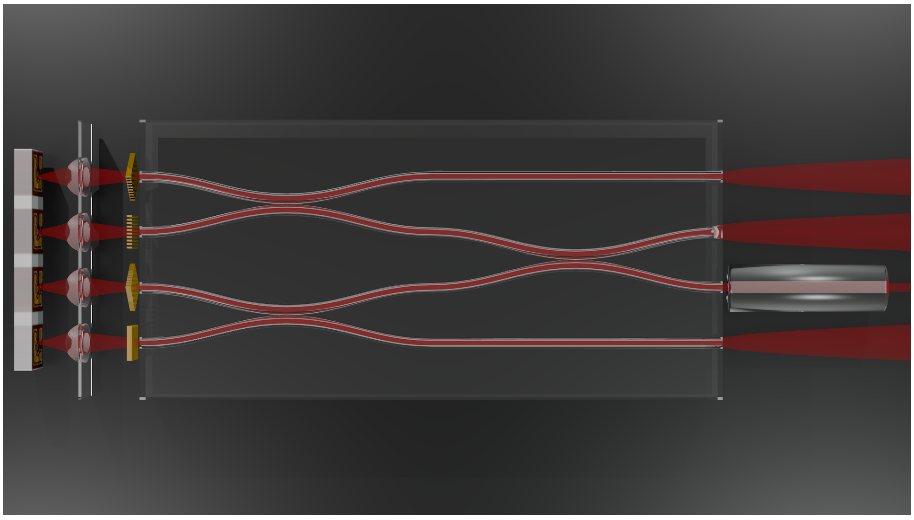


Figure 2.5: A sketch of the planned hand-held QKD sender (electronics not shown). The VCSEL array to the very left is used to produce short light pulses, which are focused using a micro-lens array onto the entrance of laser-written waveguides. Behind the lens array wire-grid polarizers are used to prepare the proper polarization states. The areas where waveguides are close to each other function as beam splitters, in this way they overlap the light from the four diodes in one spatial mode. One of the central two outputs, containing all the necessary polarizations, is collimated by a GRIN lens and used for QKD transmission.

The waveguides are laser written into a borosilicate glass substrate and are used to overlap the four polarizations into one indistinguishable spatial mode. Because for this purpose, the light has to be overlapped in a way similar to free-space beamsplitters, the waveguides are brought into close proximity, where energy from one waveguide can be transferred to another. At the end, all four polarizations needed for the BB84 protocol are contained in the center two outputs of the integrated optical circuit, from which one is selected as an output of the QKD transmission and collimated with a gradient-index (GRIN) lens.

The chapters of this thesis are each dedicated to one of those components and characterize their properties, as well as the experiments carried out with the respective components. Also the electronics designed and tested as part of this thesis are characterized in a dedicated chapter.

3 Laser-written Waveguides

Waveguides written with femtosecond laser pulses are a relatively new kind of optical components, and have gained more and more attention in the photonics community through the last decade [27–29]. Together with lithographically produced waveguides, they are often referred to as integrated optical circuits or integrated quantum gates. Such integrated optics offer a wide band of applications from single quantum gates [27] to first quantum simulators [28].

3.1 Manufacturing Process of Laser Written Waveguides

For the first, time Davis et al. showed in 1996, that a pulsed laser can permanently increase the index of refraction (IOR) in bulk glass [30]. They described a technique using an infrared pulsed laser which is tightly focused into a glass sample. Today it is known that the increase of the IOR is related to nonlinear absorption processes at high intensities, which lead to a creation of a free electron plasma. The energy contained in this plasma is then carried to the material lattice and causes the increase of the IOR [31]. By scanning a sample relative to the laser focus, waveguides can be written into a glass, even on three dimensional paths.

For more information on the fabrication process of laser written waveguides see [32] and its supplementary material, as well as [31].

As the waveguide is written transversal to the incident laser beam and the focus is slightly elliptic, the resulting waveguide will consequently have a subtle elliptic cross section, leading to birefringence within the waveguide. Birefringence causes all polarizations, which do not coincide with the ordinary or extra-ordinary axis of the waveguide, to be rotated.

Besides laser writing, there are also other techniques to manufacture integrated optics. For example, lithographically produced silica-on-silicon waveguides are used in [33]. Yet, these waveguides are more complex to produce, since masks are necessary for the lithographic process.

In addition these waveguides exhibit a birefringence about one magnitude stronger [32]. This is a main drawback, since birefringence destroys the polarization entanglement of photons used in quantum gates.

Compared with free-space optical components, all of these integrated optical circuits have the advantage, that their alignment is very robust in terms of thermal drifts and other influences from the environment. This robustness makes laser written waveguides well-suited for a hand-held QKD transmitter, which is carried around a lot and thereby exposed to many disturbances outside the lab.

All the waveguides used during this thesis were laser written into a borosilicate glass (EAGLE2000, Corning). Overall four different samples were produced in the group of Roberto Osellame at the Politecnico di Milano with different waveguide geometries as depicted in appendix A. All of the waveguides on these samples are specified to be single-mode for wavelengths above 808 nm.

3.2 Measurements of Birefringence on Straight Waveguides

As it was noted before, the laser written waveguides exhibit a small birefringence, as a consequence of their elliptic cross section. The effect of birefringence is that light polarized along two distinct orthogonal axes within the waveguide experiences two different IORs. These two axes are named ordinary and extraordinary and define the two IORs n_o and n_e, respectively. That is to say, an electromagnetic wave, which is polarized parallel to the ordinary axis $\mid o\rangle$ will "see" the IOR n_o. A wave, polarized parallel to the extraordinary axis $\mid e\rangle$, however, will "see" the IOR n_e. Hence, the two different waves will propagate with different phase velocities $v_{ph}^{(i)} = c/n_i$, where $i \in \{e, o\}$.

This modified phase velocity will lead to a phase φ a wave collects while propagating through a birefringent medium of length L compared to a wave in a homogeneous medium: $\varphi = 2\pi nL/\lambda$, where λ is the wavelength in vacuum and n the IOR in the medium. Further it holds that the phase difference between an ordinary and an extraordinary polarized wave is given by:

$$\Delta\varphi = \varphi_e - \varphi_o = \frac{2\pi(n_e - n_o)L}{\lambda} = \frac{2\pi\Delta nL}{\lambda}. \tag{3.1}$$

The measure $\Delta n = n_e - n_0$ is the difference of the IORs and is usually referred to as birefringence, whereas $\Delta\varphi$ is called the phase shift between the ordinary and extraordinary polarized wave.

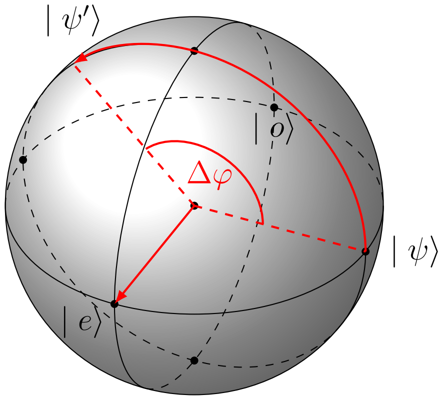


Figure 3.1: The influence of a birefringent medium on the state $|\,\psi\rangle = 1/\sqrt{2}(|\,o\rangle + |\,e\rangle)$ on the Poincaré sphere. Any state will be rotated around the $|\,e\rangle$-axis by $\Delta\varphi$.

A superposition of the two waves $|\,\psi\rangle = \alpha|\,o\rangle + \beta|\,e\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$, will then collect the phases:

$$|\,\psi'\rangle = \alpha\,\mathrm{e}^{i\varphi_o}\,|\,o\rangle + \beta\,\mathrm{e}^{i\varphi_e}\,|\,e\rangle. \tag{3.2}$$

As in quantum mechanics global phases have no influence on the measurement outcome, it is possible to add a global phase $-\varphi_o$ to this superposition:

$$\mathrm{e}^{-i\varphi_o}\,|\,\psi'\rangle = \mathrm{e}^{-i\varphi_o}\left(\alpha\,\mathrm{e}^{i\varphi_o}\,|\,o\rangle + \beta\,\mathrm{e}^{i\varphi_e}\,|\,e\rangle\right) = \alpha|\,o\rangle + \beta\,\mathrm{e}^{i\Delta\varphi}\,|\,e\rangle. \tag{3.3}$$

This result is displayed in figure 3.1 on the Poincaré sphere: the influence of a birefringent medium rotates the initial state $|\,\psi\rangle$ with $\alpha = \beta = 1/\sqrt{2}$ around the $|\,e\rangle$-axis by $\Delta\varphi$. In general any state on the Poincaré sphere will be rotated in such a way due to the birefringence, except for the states $|\,o\rangle$ and $|\,e\rangle$.

3.2.1 Measurement Setup

The setup used to characterize the birefringence of the waveguides is shown in figure 3.2. The light from a collimated laser beam with a wavelength of $\lambda = 848.5\,\mathrm{nm}$ was at first prepared in one of the four polarizations, H, V, $+45°$ or $-45°$ using a polarizer. The $\lambda/2$-plate, in front of the polarizers, was used to adjust the intensity by manipulating the incident polarization from the laser beam such that a maximal transmission through the polarizer was found. To guarantee a good preparation of the

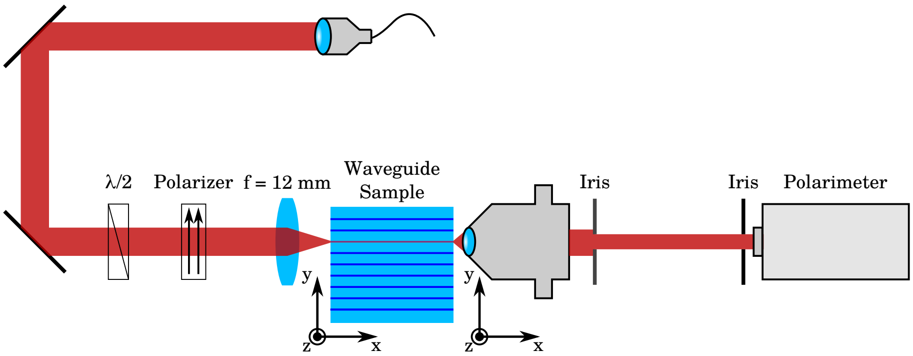


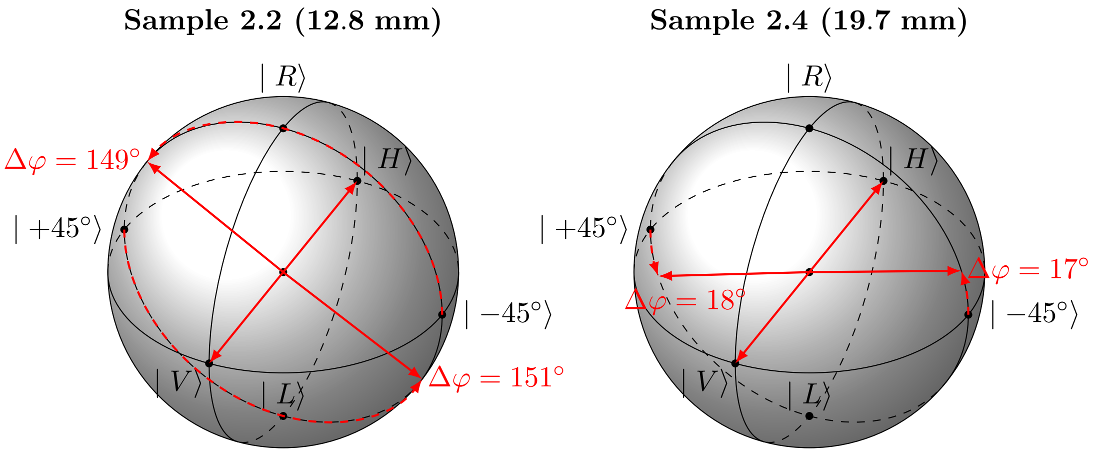
Figure 3.2: Setup for measuring the birefringence of the waveguides. The light of a collimated laser beam is prepared in of the polarization needed for QKD and then coupled into a waveguide written in a sample of bulk glass. After propagation through the waveguide, the light is collected again by a microscope objective and finally analyzed using a polarimeter. The two irises are used for spatial filtering of the waveguide mode. The fist $\lambda/2$-plate was only used to adjust the intensity behind the polarizer. For alignment the waveguide sample and the microscope objective where both placed on xyz-translation stages.

polarization, the polarizer was inserted right in front of the polarimeter and then adjusted to the respective polarizations.

The prepared light was then coupled into a straight waveguide, written inside a sample, and collected by a microscope objective at the end. For coupling light into the waveguide it is useful, that one can observe interference between the light going through the waveguide and the stray light propagating through the bulk glass, yielding elliptical and circular patterns depending on the displacement between the incident laser beam and the entrance facet.

Behind the objective two irises were used to avoid stray light, arising from imperfect coupling or losses during the propagation through the sample.

The polarization emerging from the end-facet of the waveguide was then analyzed using a polarimeter. The sample was aligned such that the ordinary and extraordinary axes of the waveguide coincide with the horizontal and vertical polarization. The states $|\pm 45°\rangle = 1/\sqrt{2}(|H\rangle \pm |V\rangle)$ will then be rotated around the H-V-axis on the Poincaré sphere. From this rotated polarization one can determine the phase shift $\Delta\varphi$ and thereby can make conclusions on the birefringence Δn using equation



Sample 2.2 (12.8 mm)

Sample 2.4 (19.7 mm)

Figure 3.3: The red arrows represent the output polarizations on the Poincaré sphere, as measured with the polarimeter for both samples. The horizontal and vertical polarizations are not rotated, whereas the ±45° polarizations are rotated with the phase shift indicated beneath the red arrows. The dashed arrows indicate the rotation direction.

(3.1).

However, there is no unique solution for Δn as multiples of 2π in $\Delta\phi$ cannot be resolved, because a phase shift corresponding to a full rotation will result in the same polarization again.

To additionally reveal a possible dependence of Δn on the wavelength, a different laser was used to measure the phase shift for different wavelengths. Since $\Delta\varphi$ is a function of λ, such a measurement also allows for conclusions on Δn and especially on the dispersion $d\Delta n/d\lambda$.

For mounting the samples on the xyz-translation stage, a sample holder was designed which is drawn in appendix B.

3.2.2 Birefringence Measurements

The birefringence of the waveguides was measured at the wavelength $\lambda = 848.5\,\text{nm}$ for two samples with different length. Therefore Sample 2.2 with a length of 12.8 mm and sample 2.4 with a length of 19.7 mm were inserted into the setup as depicted in figure 3.2.

For both samples the four input polarizations $|H\rangle$, $|V\rangle$, $|+45°\rangle$ and $|-45°\rangle$ where coupled into the straight waveguide on the sample and analyzed after the microscope objective using the polarimeter.

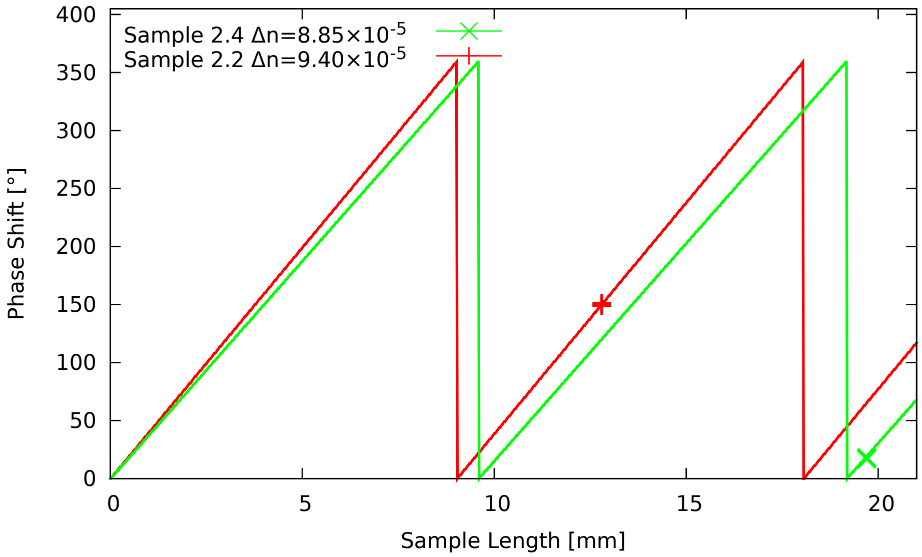


Figure 3.4: The phase shifts measured for both samples. The measured values for both samples are depicted with crosses, while the solid lines show the phase shift as a function of the sample length. These curves where fitted to the measured values to yield the values for the birefringence Δn.

The polarizations measured at the output of the waveguide are shown in figure 3.3 on the Poincaré sphere. In principle the opposite rotation direction would also be conceivable, because the measurement at the output only yields an absolute polarization, which also can be obtained by a counter clockwise rotation in figure 3.3 of an angle of $360° - \Delta\varphi$. However, the analysis of the phase shift found with the opposite rotation direction, yielded no reasonable results for the birefringence Δn, with respect to the second measurements mentioned before, using different wavelengths and the value for $\Delta n = 7 \cdot 10^{-5}$ measured by the group of Roberto Osellame for a wavelength of 808 nm.

The phase shifts depicted on the Poincaré sphere are drawn again in figure 3.4 as a function of the sample length L. To find a value for Δn the model function

$$\Delta\varphi = \frac{360° \cdot \Delta n \cdot L}{\lambda} \bmod 360°, \tag{3.4}$$

was used, and the birefringence Δn was optimized with least square fitting. Here, L is the length of the waveguides and $\lambda = 848.5\,\text{nm}$ the wavelength of the used laser diode. The modulo of 360° is necessary because, as said before, any rotation of 360° results in the same polarization again.

With this method a birefringence of $\Delta n = 9.4 \cdot 10^{-5}$ was found for sample 2.2. For sample 2.4 the birefringence was determined to be $\Delta n = 8.85 \cdot 10^{-5}$.

The depicted solutions assume one and two full revolutions of the phase shift in the waveguides, respectively. In principle, values of Δn resulting in no or multiple 2π revolutions are compatible with the measurements, however they are yielding values for Δn, incompatible with the measurement of the group of Roberto Osellame.

It should be stated that polarization rotations caused by birefringence are not a severe issue, when it comes to the efficiency of a future QKD transmitter. As long as the resulting output polarizations still confine an angle of 90° on the Poincaré sphere, the rotations can be compensated by the use of quarter- and half-wave plates at any point in the quantum channel. These measurements also confirm that it is possible to couple the four different polarizations into a straight waveguide, while preserving their relative angle on the Poincaré sphere.

3.2.3 Depolarization in the Sample

Birefringence causes different phase velocities. This often goes hand in hand with different group velocities, which are given by the dispersion $\partial n / \partial \lambda$ of the IOR:

$$v_{gr}^{(i)} = v_{ph}^{(i)}(1 + \frac{\lambda}{n_i} \frac{\partial n_i}{\partial \lambda}). \tag{3.5}$$

The group velocity is the speed with which a wave packet or light pulse travels through a medium. If a horizontally polarized pulse travels faster or slower then a vertically polarized one, a delay between those two pulses will become notable. Since those delays can differ strongly for $\mid H\rangle$ and $\mid V\rangle$, or for $\mid e\rangle$ and $\mid o\rangle$ respectively, the two polarizations could be distinguished by means of their timing. This problem, however, can be solved by adapting the timing of the electronics producing the pulses.

The much more precarious problem is that in birefringent media depolarization can occur if the delay $L/\Delta v_{gr}$ between $\mid H\rangle$ and $\mid V\rangle$ is larger then the coherence time T_c. In this case, the density matrix of a pure +45° polarization state $\mid +45°\rangle = 1/\sqrt{2}(\mid H\rangle + \mid V\rangle)$ in the eigenbasis of σ_z

$$\rho = \mid +45°\rangle\langle +45° \mid = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}, \tag{3.6}$$

will transform into a maximally mixed state

$$\rho = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \tag{3.7}$$

which represents an ensemble of states with 50% horizontally and 50% vertically polarized light. This, of course, spoils the complete QKD protocol: whenever Bob measures in the ±45° basis, he will only find the right outcome in half of the cases, since he is either measuring $\mid H\rangle$ or $\mid V\rangle$ in the ±45° basis. This would produce the same QBER as an eavesdropper would do.

If the delay is smaller than the coherence time, but not zero, the resulting state will be somewhere between the fully mixed and the pure state. The degree of this mixture can be expressed via the DOP. The DOP gives the percentage of the light which is perfectly polarized. This means that, if one analyzes light with a DOP of 95% using a perfect polarizer, half of the unpolarized optical power, i.e. 2.5%, will always be transmitted, no matter how the polarizer is oriented (see section 2.3).

This depolarization effect was first noticed, during measurements on the waveguides when rather low DOPs ($< 90\%$) appeared for the polarizations at the outputs of the waveguides. The use of a light source with a narrower bandwidth, and better spatial filtering using a second iris in the setup (fig. 3.2) solved this problem and increased the DOP to values $> 99\%$. Therefore it is conceivable, that the depolarization emerges due to different group velocities and stray light. Stray light, which is not coupled into the waveguide at the entrance facets or is lost during the propagation from the containing geometry, collects phases different from guided light, and thereby leads to the second type of depolarization. Depolarization occurring because of a difference in the group velocities, is reduced by using light sources with a narrow bandwidth, since a narrower bandwidth yields a higher coherence time.

To find a quantitative statement for the depolarization a laser with a narrow bandwidth of approximately 0.2 nm full width half maximum (FWHM) was coupled into the sample and his central wavelength was scanned by modulating the diode current. Figure 3.5 shows the spectra for the minimal and maximal current applied to the laser diode. It can be seen that an overall scanning range of about 6 nm was achieved by modulating the current from 40 mA to 185 mA.

The phase shift found for different wavelengths is shown in figure 3.6. It is obvious that the measured phase shift $\Delta\varphi$ for different wavelengths shows a steeper slope than it is expected for a constant birefringence of

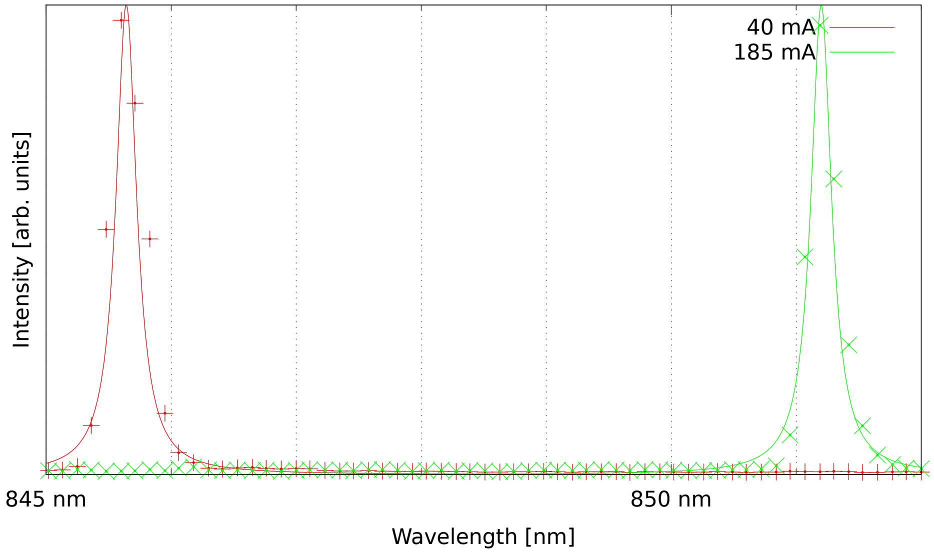


Figure 3.5: Two spectra of the narrow bandwidth laser used to measure the depolarization. An overall scanning range of approximately 6 nm was achieved. The points show the measured data from a spectrometer and the solid lines are fits to that data, with a fixed width of 0.2 nm. The resolution of the spectrometer is 0.13 nm/pixel.

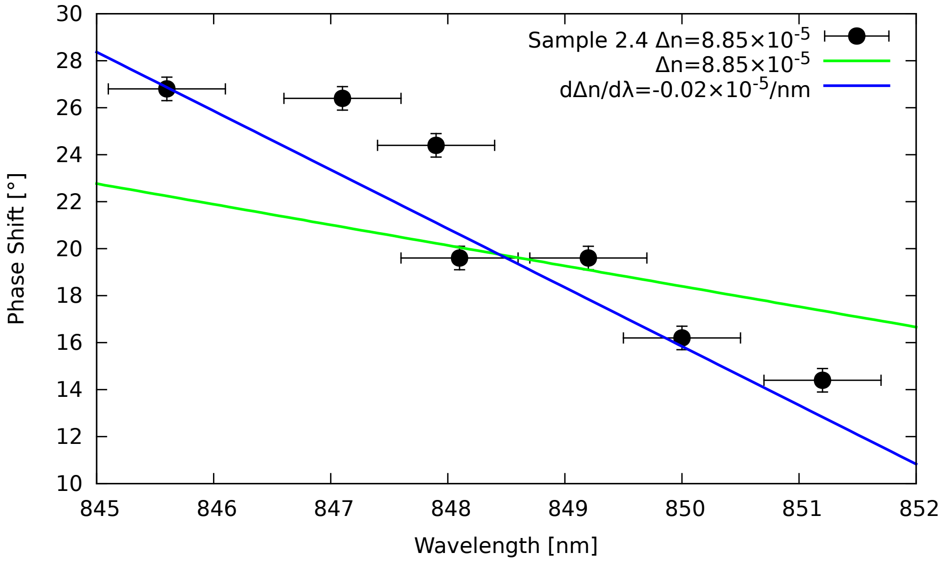


Figure 3.6: The rotation of the output polarization with respect to the central wavelength. The blue line shows the best fit with a constant dispersion for Δn. The green curves corresponds to the constant birefringence found in the previous section, where no dispersion $\frac{d\Delta n}{d\lambda} = 0$ was assumed. The error bars depict the measuring inaccuracy of the used spectrometer and the polarimeter.

$\Delta n = 8.85 \cdot 10^{-5}$. This difference can be explained, if one also assumes a dispersion for the birefringence, i.e. $\Delta n = \Delta n(\lambda)$. Therefore, the best fit to the data, where a linear dependence of Δn on λ was assumed, is also shown in figure 3.6. The function for the linear dependence of Δn is given by

$$\Delta n = \Delta n_0 + \frac{d\Delta n}{d\lambda} \cdot (\lambda - \lambda_0), \tag{3.8}$$

where $\Delta n_0 = 8.85 \cdot 10^{-5}$ and $\lambda_0 = 848.5\,\mathrm{nm}$. Together with equation (3.1), one finds for the phase shift

$$\Delta\varphi(\lambda) = \frac{360° \cdot L}{\lambda} \cdot \left(\Delta n_0 + \frac{d\Delta n}{d\lambda} \cdot (\lambda - \lambda_0)\right), \tag{3.9}$$

here the phase shift is now expressed in degree and the length is $L = 19.7\,\mathrm{mm}$ as this experiment was carried out with sample 2.4.

If one fits this function via $d\Delta n/d\lambda$ one finds the best fit for

$$\frac{d\Delta n}{d\lambda} = -0.02 \cdot 10^{-5}\,\frac{1}{\mathrm{nm}}. \tag{3.10}$$

The slope of this function, given in (3.9), at λ_0 can be found to be

$$\left.\frac{d\Delta\varphi}{d\lambda}\right|_{\lambda=\lambda_0} = -\frac{360° \cdot \Delta n_0 \cdot L}{\lambda_0^2} + \frac{360° \cdot L}{\lambda_0} \cdot \frac{d\Delta n}{d\lambda}. \tag{3.11}$$

With the same values as before this evaluates to

$$\left.\frac{d\Delta\varphi}{\lambda}\right|_{\lambda=\lambda_0} \approx \frac{2.5°}{nm}, \tag{3.12}$$

meaning that parts of the spectrum which are 1 nm away from the central wavelength will collect a phase shift of 2.5° relative to the central wavelength.

Since this value determines an upper bound for the spectral width of a light source needed to produce a certain DOP at the output of the waveguides, it is necessary to find the DOP as a function of the spectral FWHM.

For this purpose one regards the output polarization of light with a wavelength different to the central wavelength of the light source. Due to the fact, that a different phase shift will lead to a different polarization, this polarization is

$$\frac{1}{2}\frac{d\Delta\varphi}{d\lambda} \cdot (\lambda - \lambda_0) = \frac{1.25°}{nm} \cdot (\lambda - \lambda_0) \tag{3.13}$$

rotated relative to the polarization of the central wavelength λ_0. The factor 1/2 occurs due to the fact that the angle on the Poincaré sphere is the double of the angle in the polarization space.

By assuming a Gaussian intensity profile for the spectrum of a light source,

$$I(\lambda, \sigma) = \frac{1}{\sqrt{2\pi}\sigma}\, \mathrm{e}^{-\frac{(\lambda-\lambda_0)^2}{2\sigma^2}}, \tag{3.14}$$

one can define a fraction of the intensity that will be transmitted by a polarizer orthogonal to the polarization of the central wavelength.

The amount A of light polarized in any direction and transmitted through a polarizer is proportional to $\cos^2(\alpha)$, where α is the angle between the polarization of the light and the orientation of the polarizer. As a consequence from that, the amount of light with a Gaussian spectrum, which is transmitted through a polarizer orthogonal to the polarization of the central wavelength is given by

$$A\left(\sigma, \frac{d\Delta\varphi}{d\lambda}\right) = \int_{-\infty}^{\infty} I(\lambda, \sigma) \cdot \cos^2\left(\frac{1}{2}\frac{d\Delta\varphi}{d\lambda} \cdot (\lambda - \lambda_0)\right)\, d\lambda, \tag{3.15}$$

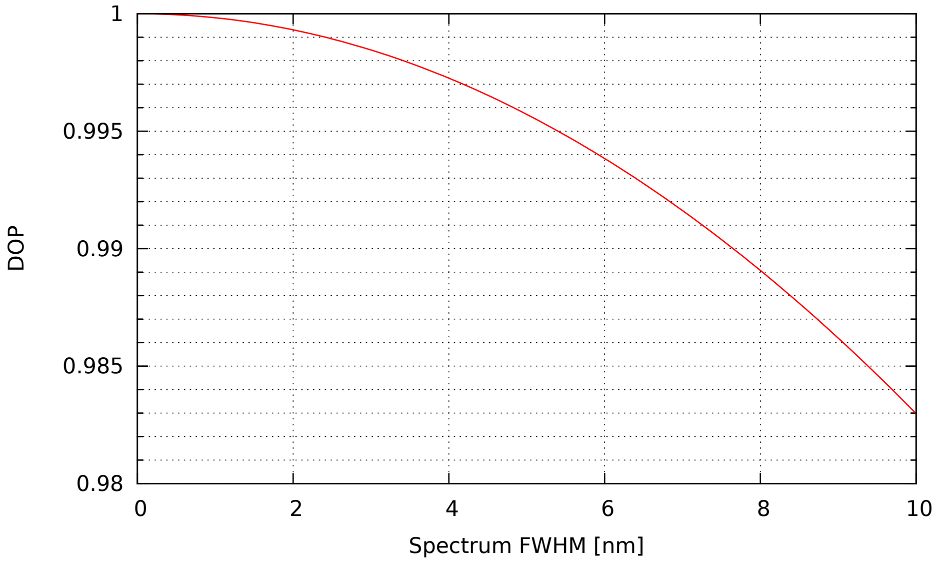


Figure 3.7: The calculated DOP of light at the output of the laser written waveguide. It is shown that the DOP decreases with the FWHM of the spectral distribution of a light source.

what evaluates to

$$A\left(\sigma, \frac{d\Delta\varphi}{d\lambda}\right) = \frac{1}{2}\left(1 - \exp\left(-\frac{1}{2}\left(\frac{d\Delta\varphi}{d\lambda}\right)^2 \sigma^2\right)\right). \qquad (3.16)$$

However, according to section 2.3 the amount going through the orthogonally oriented polarizer, is equal to half of the unpolarized fraction in the light and thereby for the DOP follows

$$\mathrm{DOP} = 1 - 2 \cdot A\left(\sigma, \frac{d\Delta\varphi}{d\lambda}\right) = \exp\left(-\frac{1}{2}\left(\frac{d\Delta\varphi}{d\lambda}\right)^2 \sigma^2\right). \qquad (3.17)$$

A plot of this result can be seen in figure 3.7, where σ was substituted with the FWHM ($FWHM = 2\sqrt{2\ \ln 2} \cdot \sigma$, for Gaussian distributions) and the previous found value for $d\Delta\varphi/d\lambda = 2.5°/\mathrm{nm}$ was inserted.

As a final result one can find the maximal FWHM of a spectrum which will correspond to a DOP of $1 - \varepsilon$:

$$\mathrm{FWHM} < \frac{2\sqrt{2\ln 2}}{d\Delta\varphi/d\lambda}\sqrt{-2\ln(1-\varepsilon)}. \qquad (3.18)$$

E.g., for an ε of 0.01, i.e. a loss of DOP of 1%, the FWHM of the light sources spectrum must be smaller than 7.3 nm. This result determines an upper bound for the bandwidth of the light sources used together with the laser written waveguides. The favored light sources are VCSELs which are characterized in the following chapter.

3.3 Measurements on Directional Couplers

The final waveguide structures required for the QKD sender are three integrated beam splitters (BSs) which overlap the light from four different diodes. Each BS is realized by writing the waveguides on paths, where they are brought in close proximity to each other on small path segments, like shown in figure 2.5.

Such an integrated BS relies on the fact that every mode confined in a waveguide reaches out beyond the confining geometry, since an electromagnetic field has to be steady at any point in space, also at borders between two different IORs. This field outside a waveguide is called evanescent and exponentially decays with the distance to the guiding structure.

If two waveguides are brought close to each other, their evanescent fields overlap, or even reach inside the guiding structure of the other waveguide. Through this coupling of the evanescent fields of two waveguides in close proximity, the energy can traverse from one waveguide to the other. This can be calculated with the help of the coupled-mode theory[34, 35].

All the measurements described in this section were performed on waveguides with one directional coupler, i.e. two inputs and two outputs. In the final scheme, depicted in figure 2.5, three BSs are used to overlap the light from four diodes.

3.3.1 Splitting Ratio

As a first step the splitting ratios of the integrated BS was measured for different input polarizations, using the same setup as for the measurements on straight waveguides, but with one variation. Light was coupled into one input of the BS as depicted in figure 3.8. Instead of measuring the polarization, an iris was used to successively filter one of the two output modes at a time. The power in these modes was then measured using a powermeter.

In a second step both outputs where imaged on a linear camera (Beamage-CCD23, Gentec) simultaneously, using the microscope objective. The

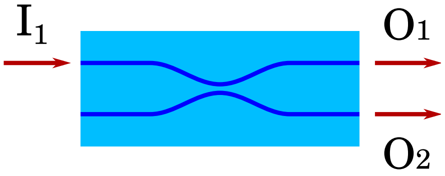


Figure 3.8: Definition of the in and outputs for the directional coupler. With the previous setup, light was coupled into one of the two inputs of an integrated BS I_i. The “transmitted” output is named O_1 and the “reflected” output is named O_2.

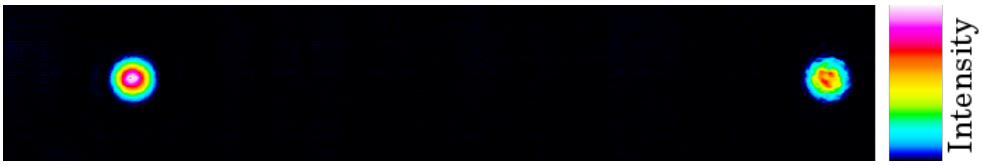


Figure 3.9: The two output modes of a directional coupler imaged with a linear camera. On the left side the output O_1 is visible and on the right side the output O_2. The bar indicates the color coding of the intensity from 0 at the bottom to 1 at the top.

pixel values of the two modes where then integrated over the same area and their mean values were compared to each other. A color coded picture of the two output modes of the BS can be seen in figure 3.9.

Both methods yielded very similar power spliting ratios as shown in table 3.1. The table shows the optical powers measured in the two outputs P_1 and P_2 for the respective outputs O_1 and O_2, as well as the mean pixel values M_1 and M_2 for the measurement using the linear camera. In both cases it became obvious that the directional coupler has a splitting ratio of approximately 2 : 3 for horizontally polarized light and 1 : 1 for vertical polarization.

Since two of the polarization states used for QKD, namely $\mid +45°\rangle$ and $\mid -45°\rangle$ are superpositions of $\mid H\rangle$ and $\mid V\rangle$ and the splitting ratio for the horizontal polarization is different from the splitting ratio for $\mid V\rangle$, one expects a change of those two polarization in the equatorial plane of the Poincaré sphere. The light in the first output O_1 will get closer to the horizontal axis and in the second output O_2 it will be changed towards the vertical axis. This can be seen by easy vector addition as depicted in figure 3.10, where the $\mid H\rangle$ component of $\mid \pm 45°\rangle$ becomes weaker relative to $\mid V\rangle$, hence changes the polarization towards the vertical axis.

	Powermeter			Camera		
Polarization	P_1	P_2	Ratio	M_1	M_2	Ratio
H	7.62 μW	5.16 μW	1.48	14.817	10.308	1.44
V	10.92 μW	11.21 μW	0.97	15.032	15.277	0.98
$+$	9.1 μW	7.82 μW	1.16	15.058	13.117	1.15
$-$	9.58 μW	8.66 μW	1.11	15.399	14.217	1.08

Table 3.1: Results for the splitting ratio measured with a powermeter and a camera. P_1 and P_2 represent the output powers in output O_1 and O_2, respectively. Analogously, M_1 and M_2 denote the mean pixel value on the camera.

Of course such a modified polarization, being essentially an imperfect state preparation, will increase the QBER measured on Bob's side and thereby shorten the key length. In addition, the security of the device is endangered, if one is not aware of this erroneous state preparation [36]. This is why it is important to know how exactly the polarization is modified, to be able to compensate for that.

The discrete change of the polarization caused by such a BS can be calculated in the following way, where a splitting ratio of 1 : 1 for vertical polarization and 2 : 3 for horizontal polarization was assumed.

The +45° polarization state is defined as $|+45°\rangle = 1/\sqrt{2}|H\rangle + 1/\sqrt{2}|V\rangle$. This state will be changed at the second output O_2 to

$$|+45°'\rangle = \frac{1}{N}\left(\sqrt{\frac{2}{5}}\frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}|V\rangle\right), \tag{3.19}$$

where the amplitudes corresponding to the respective splitting ratio are inserted. This state yields an output polarization α' of

$$\alpha' = \tan^{-1}\left(\frac{\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}}{\sqrt{\frac{2}{5}}\frac{1}{\sqrt{2}}}\right) = \tan^{-1}\left(\frac{\sqrt{10}}{2\sqrt{2}}\right) = 48.19°. \tag{3.20}$$

Note that for the coefficients used here, the square roots of the splitting ratios enter, as the intensity is proportional to the square of the field strength. Furthermore the re-normalization of the state in equation (3.19) has be neglected. This is feasible because in equation (3.20) only the ratio of the coefficients matters, any normalization would cancel out.

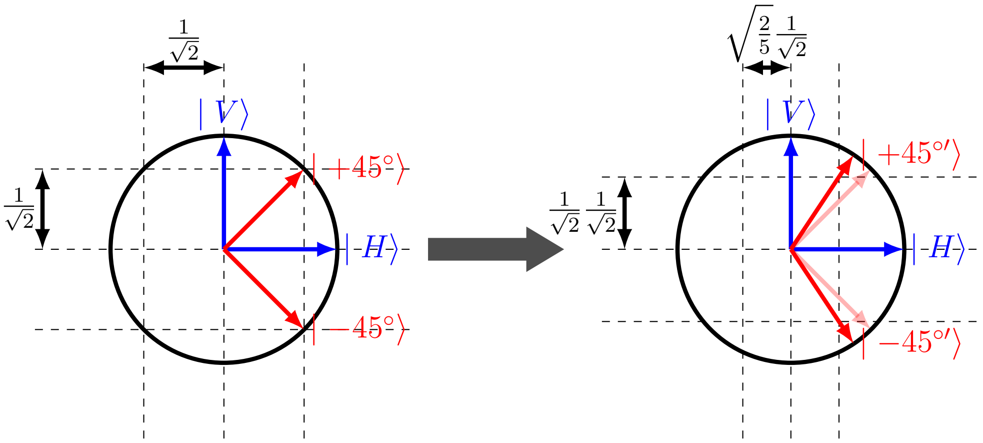


Figure 3.10: Change of the ±45° polarization due to different splitting ratios for H and V polarization. The resulting polarizations $|\pm45°'\rangle$ are modified towards $|V\rangle$ in O_2, because the horizontal polarization gets weaker relative to $|V\rangle$.

With that the expected polarization is changed by approximately 3.2° towards the vertical axis. Due to symmetry reasons, this also holds for the $-45°$ polarization, which is changed to $-48.19°$. For the first output O_1 one would expect, with the analog calculation, a change of $-2.6°$ to a polarization of 42.39°. As discussed before this polarization in O_1 is closer to $|H\rangle$ which has a polarization angle of 0°.

This imperfect state preparation can be corrected by preparing the input polarization α such that the rotation occurring at the BS will change the output polarization α' to an azimuth angle of ±45°. Due to the birefringence, though, it is impossible to find a linear polarization which results in ±45° polarized light at the outputs of the waveguides. However it is sufficient to find polarizations, which, both become polarized conjugate to the $H - V$ axis at the output (fig. 3.11).

To determine such an input state, one starts with the most general linear state $|\psi\rangle = \cos(\alpha)|H\rangle + \sin(\alpha)|V\rangle$ and finds with similar calculations as before the polarization angle α' at the output,

$$\alpha' = \tan^{-1}\left(\frac{\frac{1}{\sqrt{2}}\sin(\alpha)}{\sqrt{\frac{2}{5}}\cos(\alpha)}\right) = \tan^{-1}\left(\frac{\sqrt{5}\sin(\alpha)}{2\cos(\alpha)}\right). \tag{3.21}$$

Setting $\alpha' = 45°$ and solving for α then yields the proper input polarization: $\alpha = 41.8°$ for the output O_2. For output O_1 one finds with

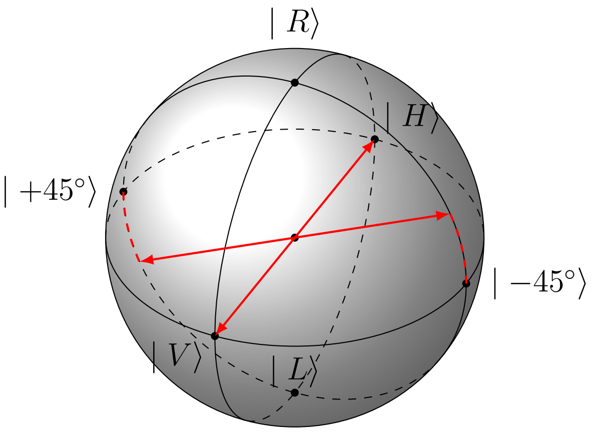


Figure 3.11: The four states sufficient for a QKD. The ±45° polarizations are rotated due to birefringence, yet they are orthogonal to the $H - V$ axis.

the same calculation an input polarization of $\alpha = 47.6°$. One can see that those input polarizations are changed by the exact same angle as the wrong output polarizations found by equation (3.20), only the direction is inverted. Again those values also hold for the $|-45°\rangle$ state for symmetry arguments.

Yet, besides the asymmetric splitting ratio, a second effect arising in laser-written waveguides has also an influence on the output polarizations, as discussed in the following section.

3.3.2 Measurement of Polarization Dependent Bending Losses

Because the waveguides have to be brought in close proximity to work as directional couplers, they have to follow a curved path. In these segments power is lost from the guided mode into the bulk glass. Again as a consequence of the birefringence, the loss in curved parts of the waveguides is dependent on the polarization of the light. This can be seen in figure 3.12, where the bending losses for horizontally and vertically polarized light is depicted for different bending radii.

This issue becomes very important, as higher losses for $|H\rangle$ than for $|V\rangle$ will again result in a change of the ±45° polarizations. However now, since the loss is always higher for $|H\rangle$, the resulting polarization is nearer to $|V\rangle$ in both outputs.

The directional couplers used in this thesis are written with a bending

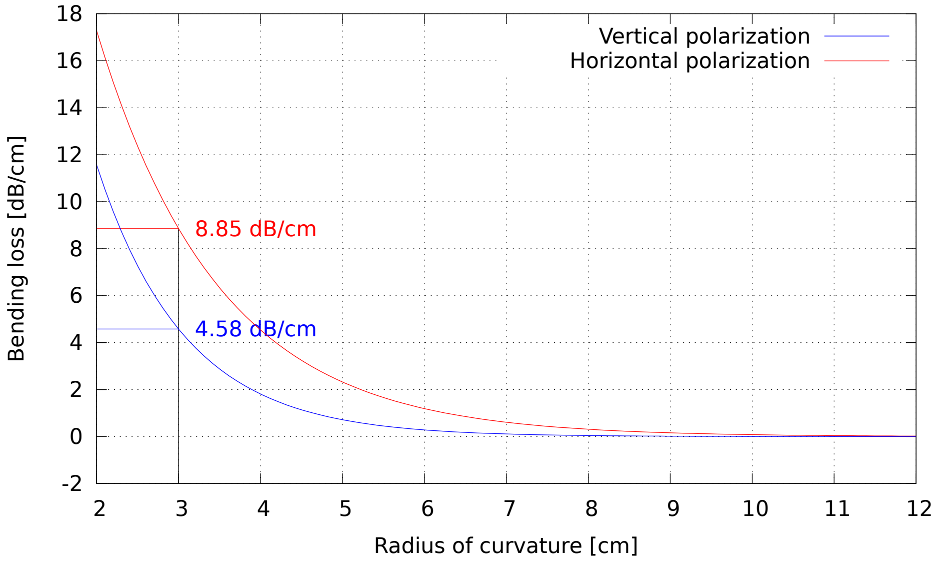


Figure 3.12: Bending losses in dB/cm for different bending radii and polarizations. The horizontal and vertical polarizations agree with the ordinary and extraordinary axes of the waveguide. The curves were supported by the group of Roberto Osellame.

radius of 3 cm and exhibit a bending loss of 4.58 dB/cm for vertically and 8.85 dB/cm for horizontally polarized light.

Thus, for a proper analysis of the bending loss, it is necessary to know the length of the curved path. This length, every photon has to travel, can be calculated as two times the path, depicted in red in figure 3.13, which consists of two circular segments. The bending radius of the used directional coupler is $R = 3\,\text{cm}$ and they start with a pitch of $250\,\mu\text{m}$, coming as close as $7\,\mu\text{m}$ to each other. Therefore the distance the two circular segments have to bridge is $(250 - 7)/2\,\mu\text{m} = 121.5\,\mu\text{m}$. With that the y-coordinate of the lower circle in figure 3.13 can be calculated by $y = -2 \cdot 3\,\text{cm} + 121.5\,\mu\text{m} = -59878.5\,\mu\text{m}$. In a last step the angle γ is found to be

$$\gamma = \frac{\pi}{2} - \sin^{-1}\left(\frac{59878.5\,\mu\text{m} - 121.5\,\mu\text{m}}{6\,\text{cm}}\right) = 63.65\,\text{mrad}. \tag{3.22}$$

Therefore, the length of the curved part in the BS is $l = 4{\cdot}\gamma{\cdot}R \approx 7.64\,\text{mm}$ and consequently the bending losses for the two polarization are

$$L_V = 4.58\,\text{dB/cm} \cdot 7.64\,\text{mm} = 3.50\,\text{dB}, \tag{3.23}$$

$$L_H = 8.85\,\text{dB/cm} \cdot 7.64\,\text{mm} = 6.76\,\text{dB}. \tag{3.24}$$

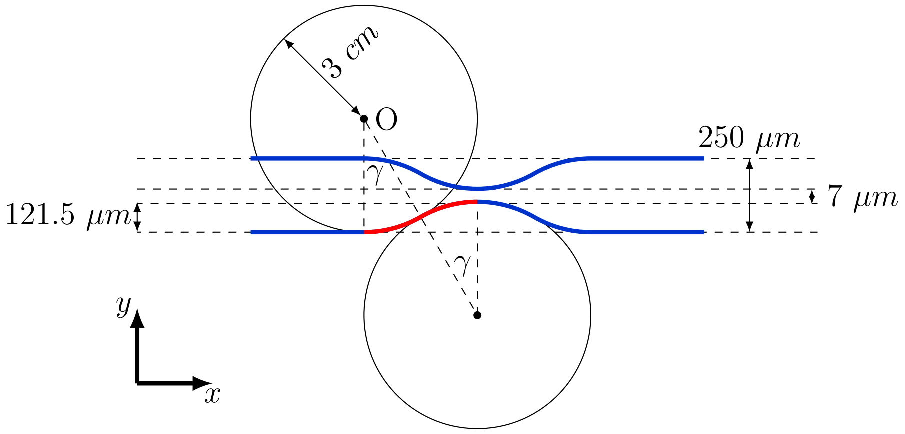


Figure 3.13: The length of the curved parts of the waveguides can be calculated from their geometry. The waveguides start with a distance of 250 µm and come as close as 7 µm. That means one combination of left and right curvature bridges a distance of 121.5 µm in y-direction.

This result can now be used to calculate the expected output polarization for a +45° input polarization. The analogue to equation (3.19), in this case, would be:

$$|\, +45^{\circ\prime}\rangle = \sqrt{10^{-0.676}}\frac{1}{\sqrt{2}}|\, H\rangle + \sqrt{10^{-0.350}}\frac{1}{\sqrt{2}}|\, V\rangle. \tag{3.25}$$

Together with equation (3.20) one finds an output polarization angle $\alpha' = 55.52°$ and a suited input polarization of $\alpha = 34.48°$. Both values are about 3 times further apart to the +45° polarization, than the values calculated for the polarization dependent splitting ratios.

Yet, the influence of bending losses and the asymmetric splitting ratio cannot be treated separately, as both effects emerge at the same time in a directional coupler. That is why the two effects have to be regarded simultaneously and both have to be combined:

$$|\, +45^{\circ\prime}\rangle = \sqrt{\frac{3}{5}}\sqrt{10^{-0.676}}\frac{1}{\sqrt{2}}|\, H\rangle + \frac{1}{\sqrt{2}}\sqrt{10^{-0.350}}\frac{1}{\sqrt{2}}|\, V\rangle \tag{3.26}$$

for output O_1 and

$$|\, +45^{\circ\prime}\rangle = \sqrt{\frac{2}{5}}\sqrt{10^{-0.676}}\frac{1}{\sqrt{2}}|\, H\rangle + \frac{1}{\sqrt{2}}\sqrt{10^{-0.350}}\frac{1}{\sqrt{2}}|\, V\rangle \tag{3.27}$$

+45°	Splitting Ratio		Bending Loss		Combined		Measurement	
	α'	α	α'	α	α'	α	α'	α
O_1	42.4°	47.6°	55.5°	34.5°	53.0°	37.0°	51°	42°
O_2	48.2°	41.8°	55.5°	34.5°	58.4°	31.6°	56°	38°

−45°	Splitting Ratio		Bending Loss		Combined		Measurement	
	α'	α	α'	α	α'	α	α'	α
O_1	−42.4°	−47.6°	−55.5°	−34.5°	−53.0°	−37.0°	−53°	−38°
O_2	−48.2°	−41.8°	−55.5°	−34.5°	−58.4°	−31.6°	−60°	−30°

Table 3.2: The summarized results for the rotations induced by an asymmetric splitting ratio and bending losses for ±45° polarized light. Denoted as α' is the output polarization with an input polarization of ±45°, α is the input polarization necessary to produce the desired output polarization of an azimuth angle of ±45°.

for output O_2. This combined state yields $\alpha'_1 = 53.04°$ and $\alpha_1 = 36.96°$ for the first output as well as $\alpha'_2 = 58.43°$ and $\alpha_2 = 31.57°$ for the second.

A summery of the calculations for the influence of the asymmetric splitting ratio and bending losses can be found in table 3.2, where the respective output polarizations α' for a ±45° input polarization is shown, as well as the input polarizations α needed to produce the desired output polarization with an azimuth angle of $\Phi = \pm 45°$.

This calculated values could be verified for −45° polarization, by using the setup shown in figure 3.2. Yet, here the polarizer was used to prepare the laser light in a horizontal polarization and a $\lambda/2$-plate was used behind the polarizer to adjust the input polarization to ±45° or such that this polarization is found at the output. With this polarization an $\alpha_1 = -38°$ and an $\alpha'_1 = -53°$ was measured for output O_1. For the second output an $\alpha_2 = -30°$ and $\alpha'_2 = -60°$ was found. These values found for the −45° polarization match the calculated values within ±2° accuracy.

The measurements of the +45° polarization yielded, with $\alpha_1 = 42°$ and $\alpha'_1 = 51°$ for the first and $\alpha_2 = 38°$, $\alpha'_2 = 56°$ for second output, results with less agreement to the expected polarizations. In the worst case α_2 deviates more then 6° from the predicted value. Nevertheless, the values for the +45° polarization still show the right qualitative behavior.

One possible explanation for the poorer agreement in the +45° case could be that, the rotation of the $\lambda/2$-plate misaligned the laser beam relative to the waveguide, and thereby the coupling for this polarization was not as good as for the −45° polarizations. Another possible explanation is, that the values for the bending loss and the splitting ratios differ slightly from those used for the calculations, and thereby the true rotation angle lies between the measured data for +45° and −45°.

Yet, the experiment described here proves that an input polarization α can be found and produced with linear polarizers in front of the waveguides, which yield output polarizations suitable for QKD.

4 Vertical Cavity Surface Emitting Lasers

This chapter is dedicated to the VCSELs [37] used as a light source for the planned hand-held QKD sender. VCSELs are a relatively new kind of laser diodes, which were first described in 1979 [38]. They use exactly like conventional edge-emitting laser diodes (EELs) the recombination processes between electrons and electron holes, which emerge at band gaps between p- and n-doped semiconductors. Nevertheless, the structural configuration of VCSELs is much different from EELs, what leads to different properties.

In the following sections those differences, together with the characteristics of the VCSELs tested here for the future QKD sender, will be discussed.

All the experiments presented in this chapter were measured using the test-electronics, built for the characterization of VCSEL driver chips which is described in chapter 5. The electronics can apply two different currents to the VCSELs. The so called bias current is a continuous part running all the time through the diode, whereas the modulation current is additionally applied for short times. In this way a VCSEL can be driven to emit light continuously as well as in short light pulses.

4.1 VCSEL Semiconductor Structure and Differences to EELs

The structure of a conventional EEL is depicted in figure 4.1. The active region of an EEL, where the recombination process is taking place, is located between a p- and an n-doped epitaxial layer. The cleaving edges of the crystal act as a Fabry-Pérot mirrors and form the cavity around the active region which amplifies the light. Since the active region is not radially symmetric with respect to the propagation direction of the emitted light, the emission pattern of an EEL is strongly elliptic.

In comparison to that, the schematic of a VCSEL is shown in figure

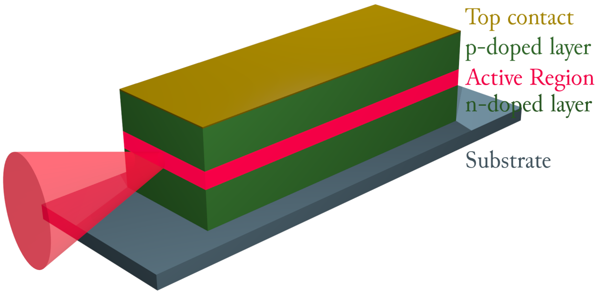


Figure 4.1: Structure of an EEL. The active region is located between two epitaxial layers. Light is emitted through the edge of the active region. The whole structure is placed on a substrate and a top contact is used to inject currents to the EEL. Picture analog to [37] p. 23.

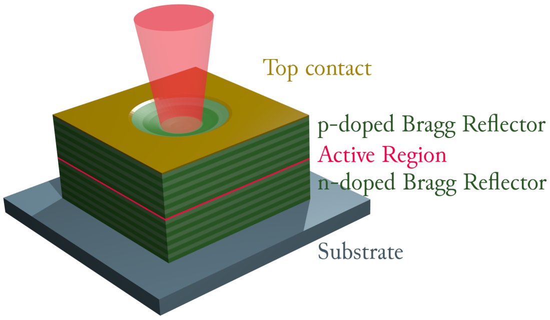


Figure 4.2: The active region of a VCSEL is positioned between p- and n-doped Bragg reflectors, which serve as a cavity. This structure is grown epitaxialy, by adding layers of different semiconductors with high and low IOR. Picture analog to [37] p. 23.

4.2. Although the semiconductor structure of VCSELs is the same as for EELs, in VCSELs, the doped semiconductors also take over the additional task of serving as the cavity. The p- and n-doped regions of a VCSEL are built in layers, exhibiting high and low IORs in alternating order. The thickness of these layers is matched to a quarter of the emission wavelength and thereby they form a Bragg reflector, which is much shorter than the cavity in EELs.

A characteristic property of all laser diodes is the threshold current, above which the optical power emitted from the diode suddenly increases. Above this current one describes a laser diode as "lasing". The current flow through the active region in a VCSEL is confined to a small diameter in the middle by, e.g., introducing an oxidized layer with high resistance [39] with an aperture in the middle. Thereby the active diameter of VCSELs can be defined, what leads to very low threshold currents compared to EELs.

Another difference to EELs is shown in the emission pattern of a VCSEL. As the active region is symmetric with respect to the beam axes, the mode emitted is circular and therefore couples better to fibers than EELs do. This property makes the use of VCSELs together with the integrated optics preferential.

Except for the measurements described in section 4.2, all experiments described in this chapter were carried out using the VCSEL array V25-850C4 distributed by VI Systems.

4.2 Temperature Dependence of Spectrum

Due to the very short cavity used in a VCSEL and the fact that the free spectral range of an optical resonator is inversely proportional to its length, the emitted wavelength of a VCSEL is mainly defined by the cavity. Contrary to that, EELs exhibit a much bigger cavity and thereby a smaller free spectral range. This means, that the number of possible modes, a EEL can lase in, is higher for the same bandwidth. Thereby a temperature induced shift of the gain peak in EELs will strongly change the emitted wavelength.

Because a QKD receiver will always need tight spectral filtering to minimize background from wavelengths different to the wavelength the transmitter uses to encode the qubits, it has to be ensured that the light source emits on a specific wavelength, even if exposed to different temperatures.

This is why the temperature dependence of a VCSEL was compared

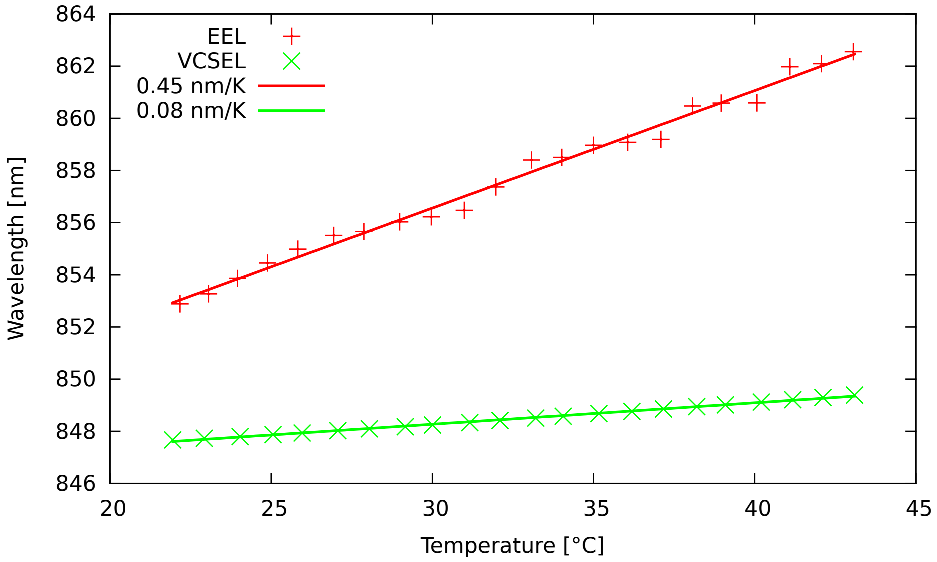


Figure 4.3: The temperature dependence of the spectrum of a VCSEL and an EEL compared. It can be seen that the temperature dependence of VCSELs is much weaker. The solid lines represent linear fits to the measured data, where slopes of 0.45 nm/K and 0.08 nm/K were found, respectively.

to an EEL by placing them in a diode mount featuring a small thermoelectrical element to control the temperature inside the mount. The light was then coupled into a spectrometer to analyze the temperature induced wavelength shift. As the cavity of VCSELs is very short, the effects from varying temperatures are expected to be rather small. Typical values for the variation of the wavelength in dependence of the temperature are $\partial\lambda/\partial T \approx 0.07\,\text{nm/K}$ [37].

For this measurement a VCSEL distributed by Roithner Lasertechnik (PM85-D1P0U) was used, since it is supported in a fitting package for the diode mount.

The results can be seen in figure 4.3. It is evident that the temperature dependence of the wavelength for the VCSEL is much weaker than for conventional EELs. The respective slopes of the linear fits, represented by the solid lines, are 0.45 nm/K for the EEL and 0.08 nm/K for the VCSEL.

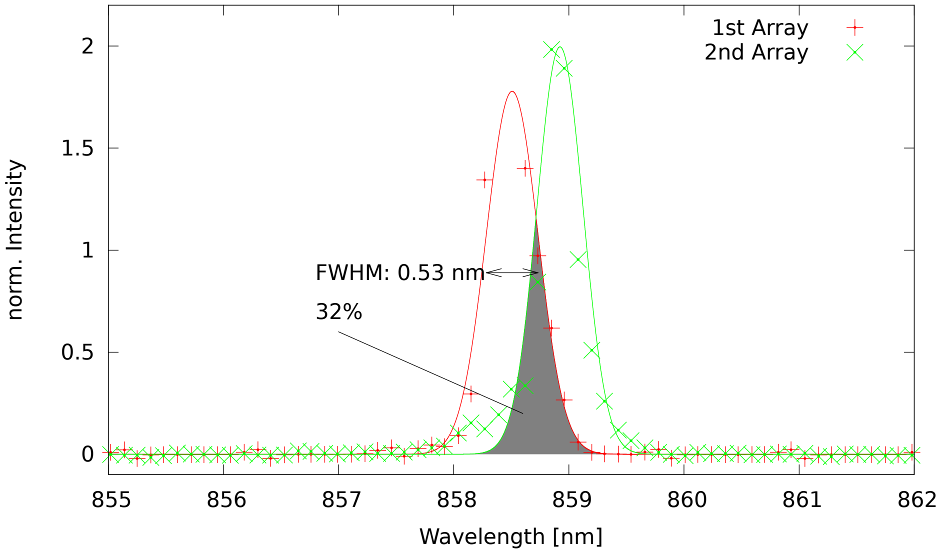


Figure 4.4: The measured spectrum and best-fit curves of two VCSELs from two different VCSEL arrays. The gray area shows the overlap between the two fitted curves of 32%. The curves and the data points are normalized.

4.3 Spectrum of the VCSEL Array

In chapter 2, the importance of the spectral indistinguishability between the four different laser diodes was emphasized. Any spectral aberration between the four laser diodes would enable an eavesdropper to distinguish the four laser diodes from each other, which then can be used to determine the key Alice and Bob exchanged without influence on the QBER.

To guarantee the security of a QKD device one has to ensure that this side channel is closed. For this purpose, one would have to compare the spectrum of all four diodes on one array, as it is used in the future transmitter. However this was not possible, since a successful bonding of more than one diode per array has not been achieved, at a time. Yet, for getting a first intuition of the spectra, two VCSELs from two different arrays were coupled into a spectrometer. Both diodes were operated at a bias current just above the threshold and the results were fitted by two Gaussian distributions, as shown in figure 4.4. Although the commonly accepted model function for laser diode spectra is the Voigt profile, the Gaussian profiles, here, also show a relatively good agreement to the data and make the FWHM comparable to the calculations from section

3.2.3. As a measure for the indistinguishability of the two diodes, the overlap of those two curves was calculated. The value of 32% found does surely not cope with the requirements for a secure QKD transmitter. Nevertheless, as the spectra were taken from two different arrays, which are not guaranteed to be grown on the same wafer, one can hope that spectra of VCSELs from the same array are in better agreement.

The measurement of only two VCSEL spectra is surely not enough for a sustained statement on the variance of the spectral distributions among different VCSELs. Therefore further measurements are necessary, especially on VCSELs on the same array and therefore grown on the same wafer.

Another requirement for the spectrum of the VCSELs, was mentioned in the previous chapter. Because the birefringence in the waveguides causes depolarization of the light depending on the spectral width, it is mandatory for the light source to have a sufficiently narrow bandwidth. In section 3.2.3 it was calculated, that a spectral bandwidth smaller than 7.3 nm causes a loss in DOP of less than 1%. The spectra shown in figure 4.4 are well below this value. However, one expects a spectral broadening for VCSELs in pulsed operation. This effect occurs, since the different driving currents during a pulse are probable to excite different modes of the VCSEL which emit light on different wavelengths.

The spectrum for the same VCSEL as shown before, depicted in red, is displayed in figure 4.5, where a minimal bias current of approximately 50 µA [40], well below the threshold, and a maximal modulation current of 12 mA was applied, with a duty cycle of 10% and a repetition rate of 100 MHz. The spectrum in pulsed mode can be found to be about two times broader than in continuous operation and is red shifted by about 1.1 nm. Nevertheless the FWHM of the spectrum is still well below the required 7.3 nm, calculated in chapter 3.

4.4 Degree of Polarization

The state preparation in the schematic described in section 2.5 is implemented by the use of polarizers, which prepare a pure polarization state, however at the expense of optical power. This power loss at a polarizer depends on the relative orientation between the incident polarization and the polarizer. In the case where the VCSEL emits light perfectly polarized orthogonal to the polarizer, no light at all will be transmitted through the polarizer. Contrary, the complete light will be transmitted

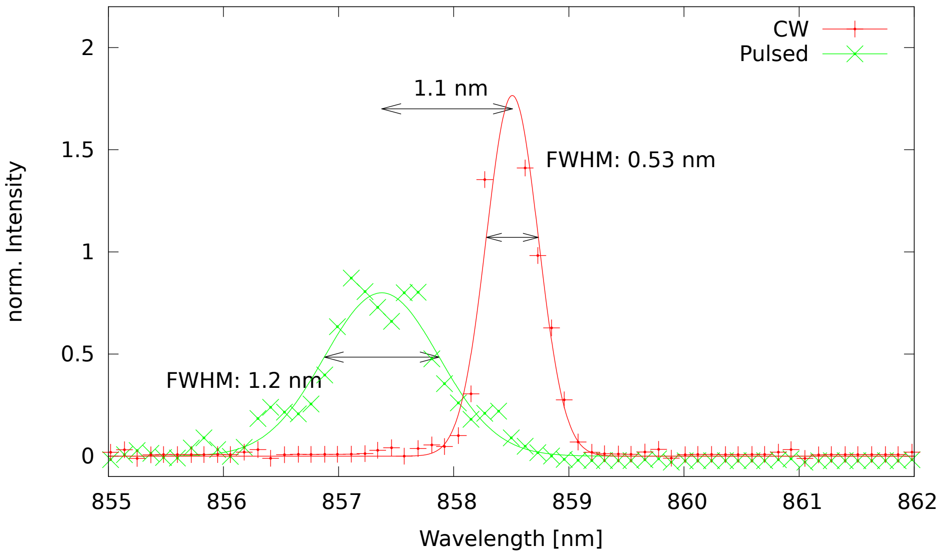


Figure 4.5: The spectrum of the same VCSEL as before also depicted in red, however, now driven in pulsed mode. The broadening of the spectrum is clearly visible.

if it is polarized along the polarizer's axis. According to chapter 2.3, half of any unpolarized fraction will always be transmitted, no matter how the polarizer is oriented.

The state preparation in the future QKD transmitter is realized by four different polarizers, each oriented to prepare one of the four states $|H\rangle$, $|V\rangle$, $|+45°\rangle$ or $|-45°\rangle$, respectively. This kind of state preparation has been used in earlier transmitters, however always in combination with conventional EELs. Since EELs are not symmetrical with respect to the emission direction, they show a high polarization with fixed orientations. Therefore EELs can be oriented such that intensity fluctuations, occurring from the state preparation using polarizers, can be avoided. Contrary to that VCSELs are symmetric with respect to the emitted laser beam, thereby they emit light in an unpredictable polarization or are not polarized at all. This is why intensity fluctuations between the four polarization states become possible.

Since intensity fluctuations change the mean photon number per pulse μ, which can enable an eavesdropper to distinguish between the four diodes and the possibility to adjust the intensities electronically is limited, the DOP becomes a decisive measure for the applicability of the VCSELs in a QKD scenario. The optimal value of the DOP would be DOP $= 0\%$, where in all polarizations half of the intensity could be found

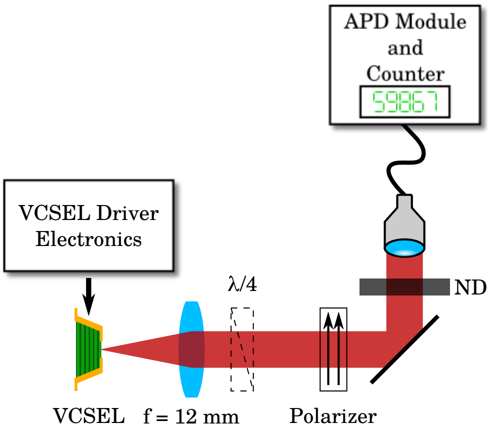


Figure 4.6: The setup used for measuring the DOP. The VCSEL can be operated either in pulsed or continuous mode. The light emitted is then collected by a lens and passes an optional $\lambda/4$-plate and a polarizer. The transmitted photons are counted using an APD module together with a counter. An neutral density filter (ND) was used to avoid saturation of the APD.

behind the polarizers.

Figure 4.6 shows the setup used to determine the DOP of the VCSELs. The light from one VCSEL was collected by an aspheric lens and, after a polarizer, coupled into a multi-mode fiber connected to an APD module. To analyze the light in all three directions of the Stokes vector, the polarizer was rotated to ±45°, H and V. A quarter waveplate was inserted, used together with the polarizer to analyze the light in the circular basis and a neutral density filter (ND) prevented the APD from saturating. The electronics can be used to drive the VCSEL with a continuous current as well as with short pulses. The DOP was analyzed for three different currents and in pulsed operation.

With the counts c_i being measured for the projection on one of the six polarizations during a time of 25 s, $i \in \{H, V, R, L, +, -\}$, the four stokes parameters are defined as follows:

$$
\begin{aligned}
S_0 &= (c_H + c_V + c_+ + c_- + c_R + c_L)/3, && (4.1)\\
S_1 &= c_H - c_V, && (4.2)\\
S_2 &= c_+ - c_-, && (4.3)\\
S_3 &= c_R - c_L, && (4.4)
\end{aligned}
$$

where the intensity S_0 is averaged over the three measurement bases.

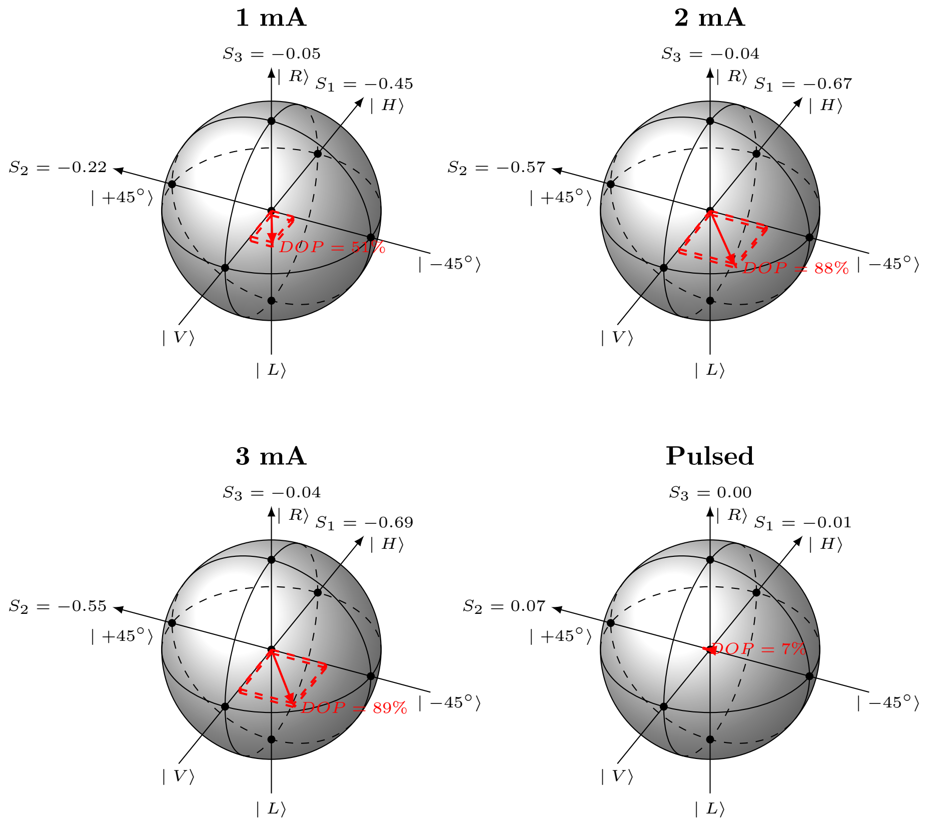


Figure 4.7: The results of the DOP measurements at different currents and during pulsed operation. The normalized values S_i/S_0 for the stokes parameters are given at the respective axes.

The DOP is then given by

$$\mathrm{DOP} = \frac{\sqrt{S_1^2 + S_2^2 + S_3^2}}{S_0}. \tag{4.5}$$

The results found are illustrated on the Poincaré sphere in figure 4.7, where the values of the Stokes parameters were normalized, to $S_0 = 1$, i.e. S_i was substituted by S_i/S_0. It can be seen that the DOP increases very fast from 51% to 88% between the currents from 1 mA to 2 mA. A further increase of the current to 3 mA yielded nearly the same DOP of 89%. This high values would be rather bad for a state preparation using polarizers, because the polarization would cause intensity deviations on the orthogonal states in the two bases used for QKD. Nevertheless, the DOP decreases dramatically in pulsed operation to only 7%. This effect can again be explained by different modes of the VCSEL occurring at different currents, which lase at different polarizations. The future

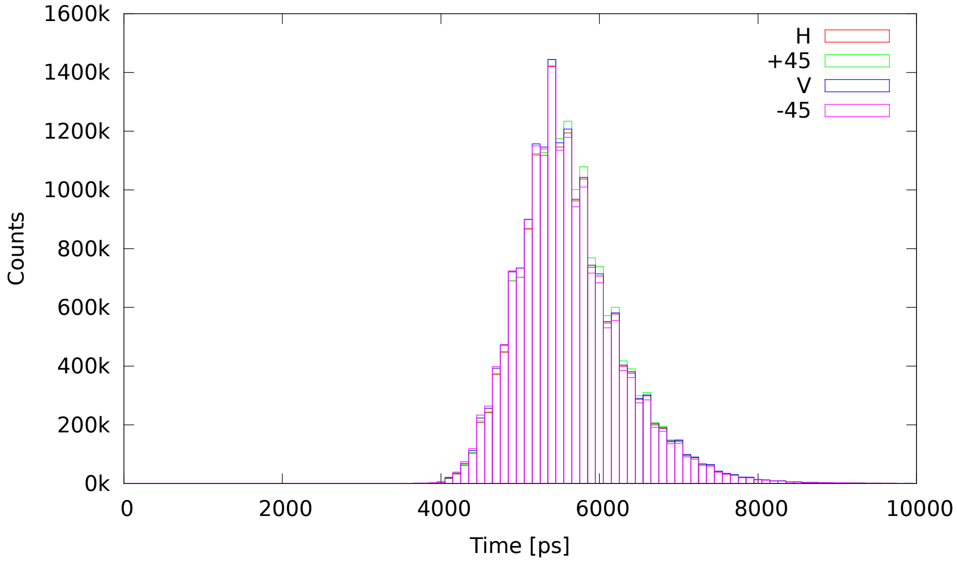


Figure 4.8: The pulses of one VCSEL, time resolved for the projections on the four different polarizations in the equatorial plane of the Poincaré sphere.

task of the VCSELs in the QKD sender is to produce light in pulses of approximately 1 ns length, so that the very low DOP of 7% can be assumed to be sufficiently small to produce similar intensities for all polarization states. The raw data of this measurement can be found in appendix C.

With this measurement, however, it is still possible, that different polarizations of the VCSEL are emitted at different times during one pulse. A weak polarization in every pulse, on average, does not guarantee a weak polarization at any time of the pulse. If for example a horizontal polarization is emitted at the rising edge of the light pulse and a vertical polarization at the falling edge, the overall intensities in one pulse would still be the same for both polarizations, resulting in a Stokes parameter $S_1 = 0$. Yet, in such a case the state preparation using polarizers would make the horizontal and vertical pulse distinguishable by resolving their pulse shapes in time.

This is why, the polarization of the VCSEL in pulse mode was further analyzed, by resolving the projections on H, V, $+45°$ and $-45°$ in time. For this purpose, instead of the counter, a time-to-digital converter (TDC) was connected to the APD module, which is able to resolve the arrival times of the photon clicks from the APD with a resolution of 100 ps, relative to a trigger signal from the driving electronics. The histogram of this arrival times can be seen in figure 4.8 for the four projections. Note that the measurement of these four projections is sufficient, since the state preparation with the polarizers only takes place in the equatorial plane of the Poincaré sphere. This is to say, every circular part S_3 of the polarization will be equally projected on all linear polarizations.

The pulses resolved in figure 4.8 show very similar time behavior for the four polarizations, and thereby it is excluded, that a possible eavesdropper could distinguish the four diodes by means of their timing. A different view would be, that for all times, the Stokes parameters S_1 and S_2 are close to zero, which guarantees balanced intensities between all linear polarizations.

Yet, the plot shown in figure 4.8 represents an average over many different individual pulses. Hence, it is still possible, that each pulse exhibits a certain polarization and only the average of many pulses is unpolarized. For testing such a behavior, it will become necessary to analyze each pulse individually in all four projections at the same time.

4.5 Power-Current Curve and Spatial Modes

For encoding information in faint laser pulses, it is necessary that the contrast of the VCSELs between being turned on and off has to be really high. Since the optical power output of every laser diode drastically increases over a certain current, high contrasts can be achieved if the VCSELs are modulated over this threshold current. This means that, the current applied to the VCSELs during the pulse duration has to be higher as the threshold current, whereas the bias current, running all the time, has to be well below the threshold. Yet, the bias current cannot be omitted since the amplitude achievable for short pulses with the modulation current is limited.

To determine suited values for the modulation and bias currents, it is thereby important to know the exact value of the threshold current. For this purpose the optical power output of a VCSEL was determined as a function of the current, where a sudden increase of the optical power marks the threshold current.

In figure 4.9 the setup used for measuring the power-current curve (P-I curve) is illustrated. The light emitted from a VCSEL is collimated and

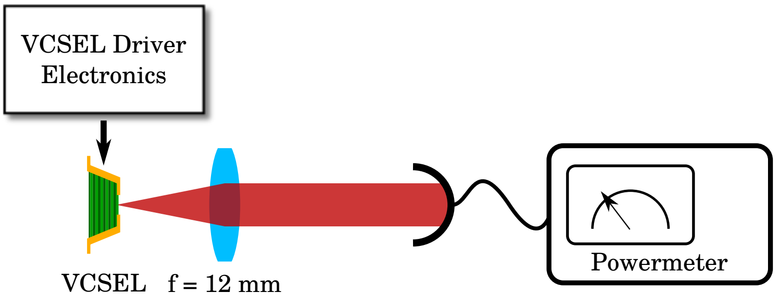


Figure 4.9: Setup for measuring the power-current curve. The light emitted by a VCSEL was colllimated by an aspheric lens and then measured using a powermeter.

measured using a powermeter. The electronics were used to scan the laser current between 0.5 mA and 3 mA.

The results of the measurement is plotted in figure 4.10. It can be seen that the slope rises at a current of 0.9 mA marked by the green arrows. The inset shows the interesting region on a larger scale. This result verifies a very low threshold current for the VCSELs used of 0.9 mA. Compared to that, typical values for the threshold current of EELs are on the order of a few tens mA.

Later the powermeter and the lens in figure 4.9 were replaced by a beam profiler in close proximity to the VCSEL to characterize the spatial modes appearing at different currents.

The results of this measurement is shown in figure 4.11. It can be seen that the VCSEL is emitting a Gaussian mode at the threshold current and slightly above at 1 mA. However for higher currents donut modes are found.

Those higher donut modes surely couple worse to the laser-written waveguides and can cause new problems concerning stray light and the resulting depolarization. However, in the future QKD transmitter the VCSELs are used to produce short light pulses, which will result in different modes than in continuous operation. Therefore further investigations of the spatial modes in pulsed operation is necessary.

The spatial modes for a VCSEL in pulsed mode could not been measured, since the pulsed modes yield a higher divergence, hence didn't fit on the beam profiler, even for the minimum possible distance.

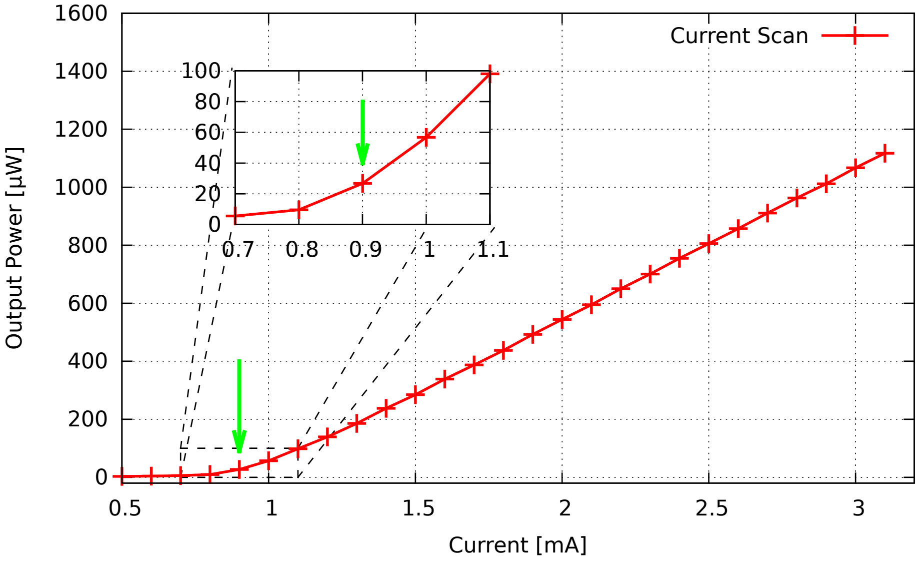


Figure 4.10: The output power of a VCSEL vs. the driving current. The green arrows mark the threshold current. The inset is a zoom into the region around the threshold.

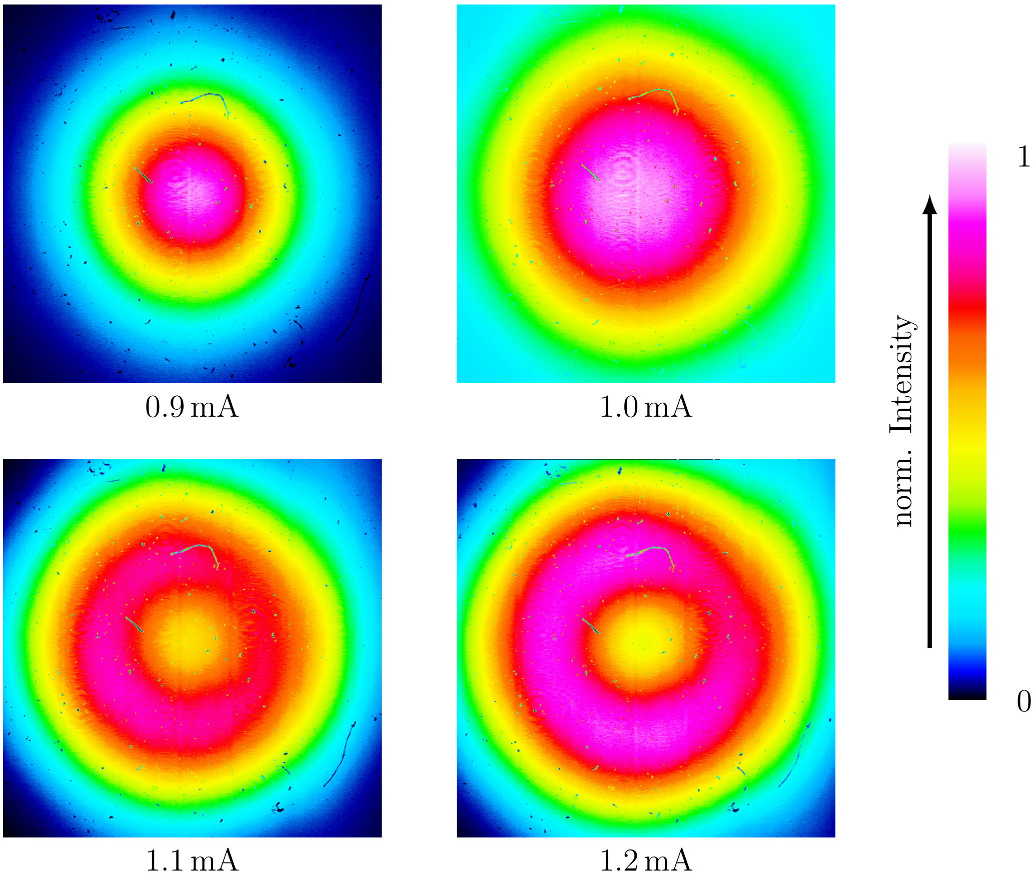


Figure 4.11: Four spatial modes emitted at different currents. The current increases from the top left to the bottom right picture. The intensity is color coded as indicated by the bar.

5 Electronics

VCSELs show electrical characteristics very different from conventional EELs and since there was no experience with this kind of laser diodes, the electronics for driving the VCSELs had to be designed from the scratch. Because VCSELs are already commonly used in classical optical communication, there is a rich supply of many different, commercially available integrated circuits (ICs) dedicated to drive VCSELs in pulsed operation. Of course all of those commercial chips are designed for a classical application. That is why, during this thesis three different VCSEL drivers were tested, to find an IC well suited for a QKD application. The electronics described in this chapter, were designed and built as evaluation boards for different driver ICs, to find a suited chip for the VCSELs used.

Finally, the results found with these different ICs could be used to design a first prototype of the electronics for a QKD transmitter.

5.1 Differences to Classical Optical Communication

When driving a laser diode with short current pulses two distinct currents, called bias and modulation current, describe, together with the pulse length Δt, the shape of the pulse. The bias current is a direct current (DC) part, running all the time through the diode, whereas the modulation current is only added during the pulse duration. The bias current is necessary, because the amplitude acheivable for the modulation current is limited for fast modulation times, since it is technologically challenging to supply high currents for short time intervals. Ideally this would result into a rectangular shape for the current applied to the VCSEL as seen in figure 5.1.

This way of creating current pulses is common to classical optical communication and QKD. Yet, the main difference between classical communication and QKD is, that in QKD it is necessary that the chance for any other laser diode emitting a photon at the same time as the laser diode used to generate the qubit does, has to be very low. That is because a photon, emitted simultaneously with the intended photon of distinct

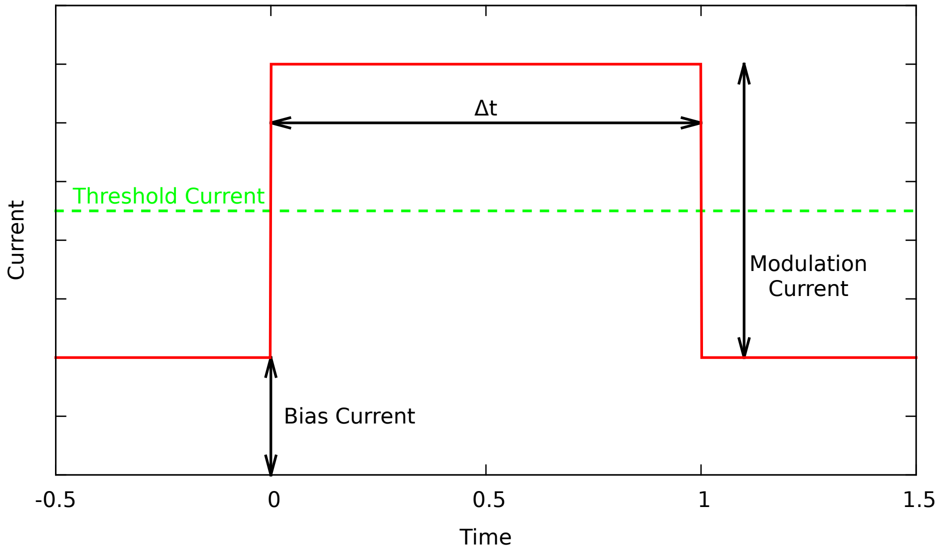


Figure 5.1: The current pulse applied to a VCSEL, with the time and current in arbitrary units. To achieve a high contrast between the on and off state of the diode, one has to ensure, that the bias current lies well below the threshold current and together with the modulation currents exceeds the threshold.

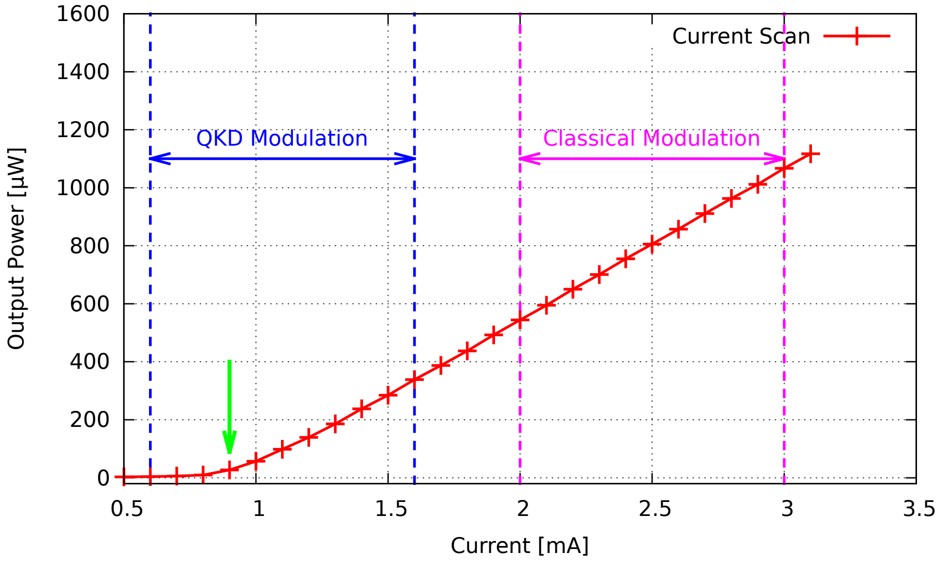


Figure 5.2: The difference between the modulations in quantum and classical communication. In the QKD application it is necessary to modulate the current over the threshold to achieve high contrasts. In classical communication, however, one can afford to modulate the current in the lasing regime, only. The threshold current is marked by the green arrow.

polarization, could cause an error in the sifted key, if it is received by Bob. This means that the contrast between the on and off state of the VCSELs must be very high, despite the presence of the necessary bias current.

To achieve the high contrasts needed in a QKD application, one can make use of the characteristic threshold current, every laser diode exhibits. Above this threshold current the diode lases and the emission of light suddenly increases by orders of magnitude. By setting the bias current below the threshold current, the intensity of light emitted during the off state of a VCSEL is very low. If one additionally ensures, that the bias current together with the modulation current exceeds the threshold current during the on state, one can realize very high contrasts for the VCSELs.

Contrary to that, in classical communication the bits are encoded in dark and bright light pulses. This means that, the bias current can be chosen above the threshold current and the modulation takes place in a region where the diode is always lasing.

This difference is explained in figure 5.2 with the characteristic threshold behavior found in section 4.5. It is obvious that the achieved contrast between the blue dashed lines, indicating the modulation for a QKD application, is much higher, than for the purple lines. In classical communication one can afford a lower contrast, since it is possible to define two power values which discriminate between the bit values '0' and '1'.

When it comes to short pulses, it is also important to consider the impedance inherent to the circuitry. This is because discontinuous jumps of the impedance, which, for example, occur between a power line and the VCSEL, reflect a part of the energy contained in an electrical pulse. Since the pulse gets reflected back and forth between two such jumps, this leads to a broadening in time. In classical communication, impedance matching can be accomplished very easily, since the impedance of laser diodes is rather constant in the lasing regime. However, similar to the output power, the impedance changes near the threshold current. That makes it impossible to match the impedance in QKD. The only possibility to reduce the influence of the unmatched impedance is to keep the transmission lines in the circuitry as short as possible

5.2 Finding a Suited VCSEL Driver Integrated Circuit

Since there is a vast amount of commercially available VCSEL drivers, three were pre-selected from the pool for further testing. Because the future design of the transmitter is aimed to become small, an important pre-selection criteria was the possibility to set the bias and modulation currents via a digital interface. In this way the design of the electronics can be kept simpler, as no additional circuitry is needed for this purpose. In addition, the drivers where chosen to be fast enough to produce pulse widths of the order of 1 ns. This means that the specified data rate had to be larger than 1 Gbps. With that criteria the three pre-selected ICs were the LTC5100 [41] (Linear Technology), the ONET4291VA [40] and the ONET8501V [42] (Texas Instruments).

Those three drivers are of course all designed for classical optical communication. Since the necessary high contrast and the required duty cycle of the diodes are rather untypical for classical communication, their practicability in a QKD scenario had to be tested. For this purpose two evaluation boards were built. One equipped with the LTC5100 and the other equipped with both the ONET4291VA and the ONET8501V.

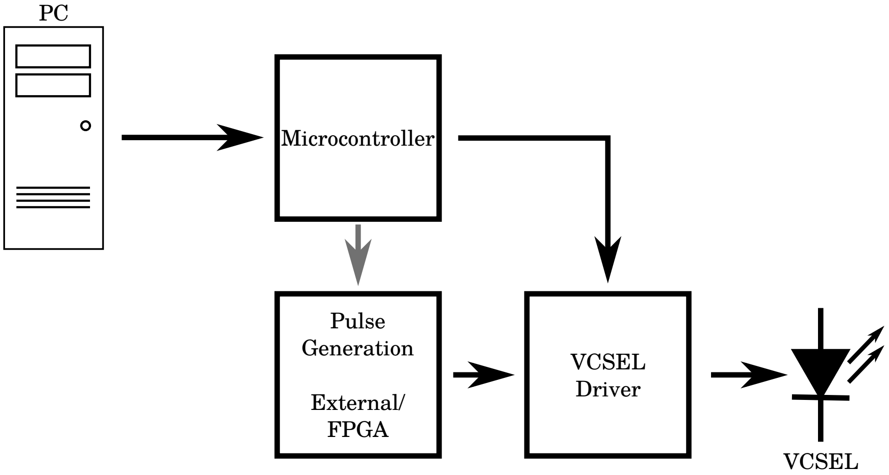


Figure 5.3: A sketch of the schematics of the evaluation boards. A microcontroller is used to control the bias and modulation currents, applied to the VCSEL via the driver ICs. The first evaluation board built for the LTC5100 used an external source for data input, whereas the second evaluation board, testing the ONET4291VA and ONET8501V, was equipped with and FPGA for generating short pulses.

All of the tested ICs accept a differential signal for the data input. A differential signal consists of two signal lines, where the digital signal is interpreted as '1' if the line denoted with "+" is at a higher potential than the "−" line and vice versa. During such times, the driver IC will, additionally to the bias current, apply the modulation current to the VCSEL. A logical '1' is represented by 1.4 V at the positive line and 1.0 V at the negative line. These "high" and "low" levels correspond to the international low voltage differential signaling (LVDS) standard.

Therefore, the schematics for both evaluation boards are in principle the same (fig. 5.3). A source of fast pulses is fed to the data input pins of the tested VCSEL driver, which translates the signal into currents running through the VCSEL.

For controlling the values of the modulation and bias currents, a microcontroller uses the digital interface of the driver. The microcontroller itself is connected to a PC over a serial interface.

The only difference between the two evaluation boards, is the source for short pulses. For the first evaluation board (LTC5100) an external pulse generator was used, whereas the second uses an on-board field-programmable gate array (FPGA). In both cases the pulses applied to the VCSEL drivers are emitted with a repetition rate of $f_{rep} = 100\,\mathrm{MHz}$

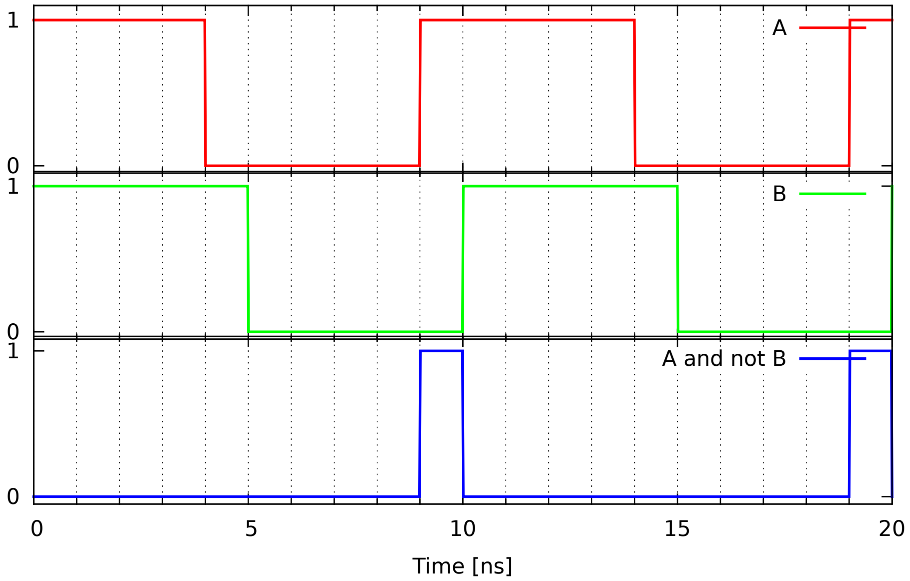


Figure 5.4: Principle of the short pulse generation on a FPGA. By shifting a clock signal with 50% duty cycle by 1 ns and then applying the logical operation $A \wedge \neg B$, short pulses with a width of 1 ns and a repetition rate of $f_{rep} = 100\,\mathrm{MHz}$ are created.

and a pulse width of $\Delta t \approx 1\,\mathrm{ns}$, i.e. the duty cycle of the VCSEL is $D = f_{rep} \cdot \Delta t = 10\%$.

The FPGA used on the second evaluation board comes with an on-chip digital clock manager (DCM), which was used to generate the short pulses in the following way. The DCM is able to delay a clock signal, with a duty cycle of 50%, in a phase locked loop from 0 ns to approximately 10 ns in steps of 40 ps. This was used to delay a 100 MHz-clock, produced by an oscillator outside the FPGA, by one nanosecond. If one calls the original clock signal A and the delayed clock signal B, the logical operation $A \wedge \neg B$ (A and not B) yields the required pulses of 1 ns width, with a duty cycle of 10% (see fig. 5.4).

The full schematics of both evaluation boards can be found in appendices D and E.

5.2.1 Contrast

A high contrast between the on and off state of a VCSEL is mandatory for successful QKD. Therefore, the setup displayed in figure 5.5 was used, to determine the contrast produced by the different ICs together

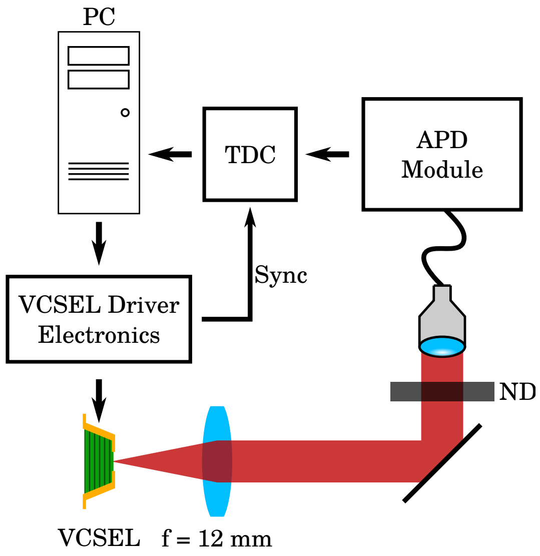


Figure 5.5: Setup used for determining the intensity contrast between the on and off state of the VCSELs. The VCSEL was driven with three different ICs and the resulting light pulses analyzed using an APD module and a TDC. The complete circuitry for driving the diode were controlled via a PC. The driving electronics and the TDC where synchronized via a 40 MHz reference signal.

with the VCSEL.

A PC was used to control the evaluation board which drove a VCSEL with short pulses. These pulses emitted from the VCSEL were collimated and coupled into an APD module. A saturation of the APD was avoided with a neutral density filter. The arrival times of the photons were analyzed using a TDC and the same PC again. It is notable that the same 100 MHz-clock used for the pulse generation on the FPGA was divided by a second on-chip DCM to 40 MHz and then used as a synchronization signal for the TDC. The frequency of this sync signal was defined by the TDC, which only accepts 40 MHz as a clock input.

Since, the external source was not able to produce 1 ns short pulses and a 40 MHz sync signal, at the same time. It was necessary for the first evaluation board, to analyze the arrival times using the histogram function of a digital storage oscilloscope (DSO) triggered with a synchronous signal.

The histograms of the arrival times for the different tested ICs are shown in figures 5.6, 5.7 and 5.8 for the LTC5100, ONET4291VA and ONET8501V, respectively.

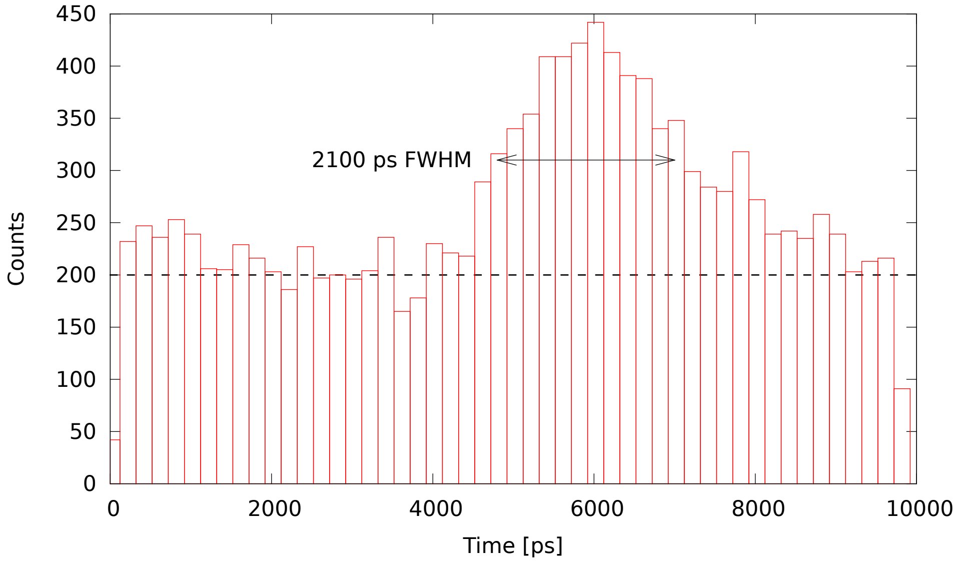


Figure 5.6: The arrival times of photons contained in the pulses produced, with the LTC5100 VCSEL driver.

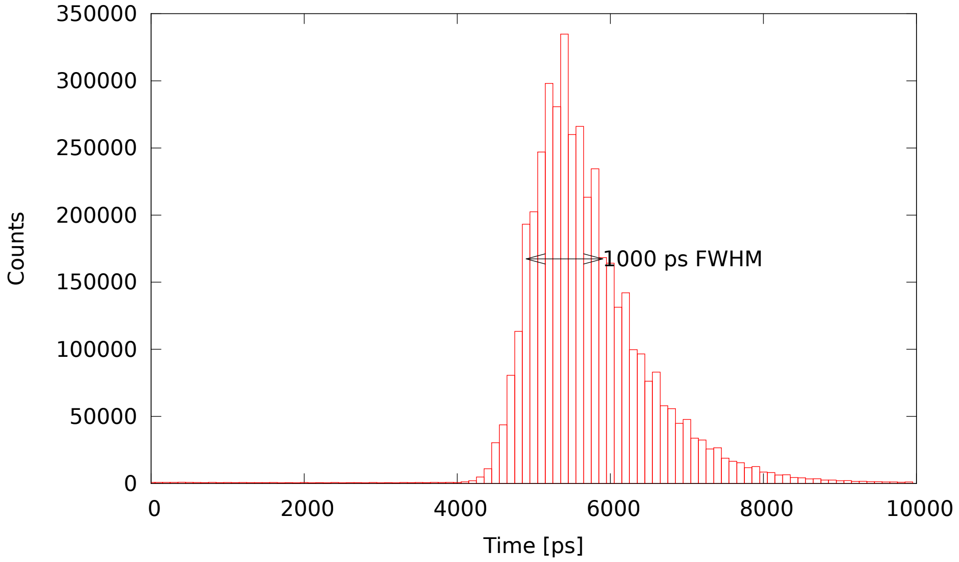


Figure 5.7: Arrival times for photons in a pulse produced with the ONET4291VA.

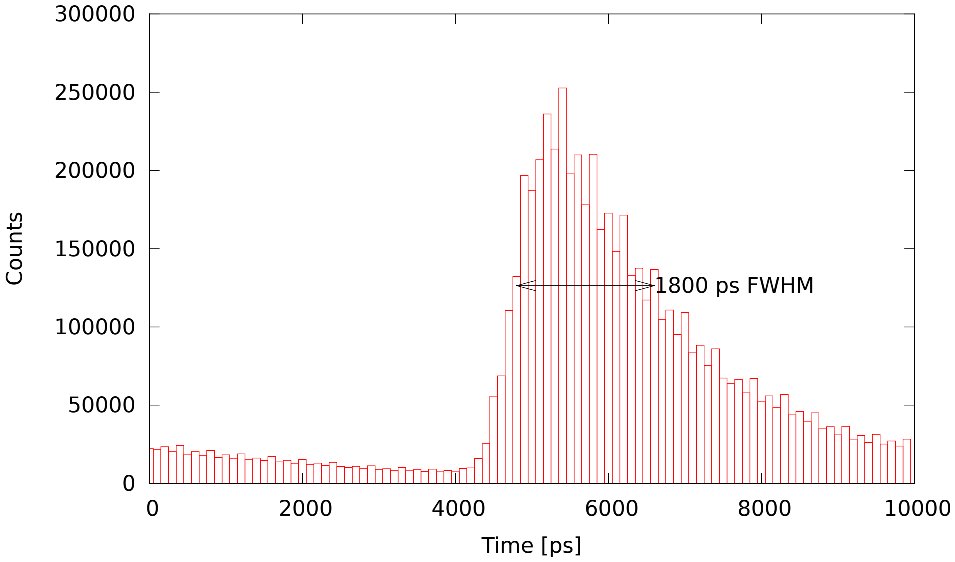


Figure 5.8: Arrival times for photons in a pulse produced with the ONET8501V.

What stands out most in these three plots is, that the contrast for the pulses produced with the LTC5100 is much worse than for the other two ICs. The LTC5100 has a slightly different internal design than the other two drivers. Instead of adding the modulation current to the bias current during times where the input signal is interpreted as a logical '1', it applies both currents to the diode and bypasses the modulation current to an internal current sink, at times when the input is interpreted as a '0'. This design yields theoretically the same current pulses, yet, obviously doesn't reach the necessary low bias current. The much lower total count rate shown in the plot is due to the different measurement method using the DSO and is not crucial for the contrast measurement.

The ONET4291VA and the ONET8501V were further investigated in terms of their pulse width as described in the following section.

5.2.2 Pulse Widths

All of the tested driver ICs have three current output pins. The first one delivers the bias current and is always connected over an inductor to the VCSEL. For the modulation current there are two output pins with opposite polarity. Thereby it is possible to connect a VCSEL to the driver ICs in two different ways. The first possibility, as it was used before to determine the contrast, is to connect the diode single ended,

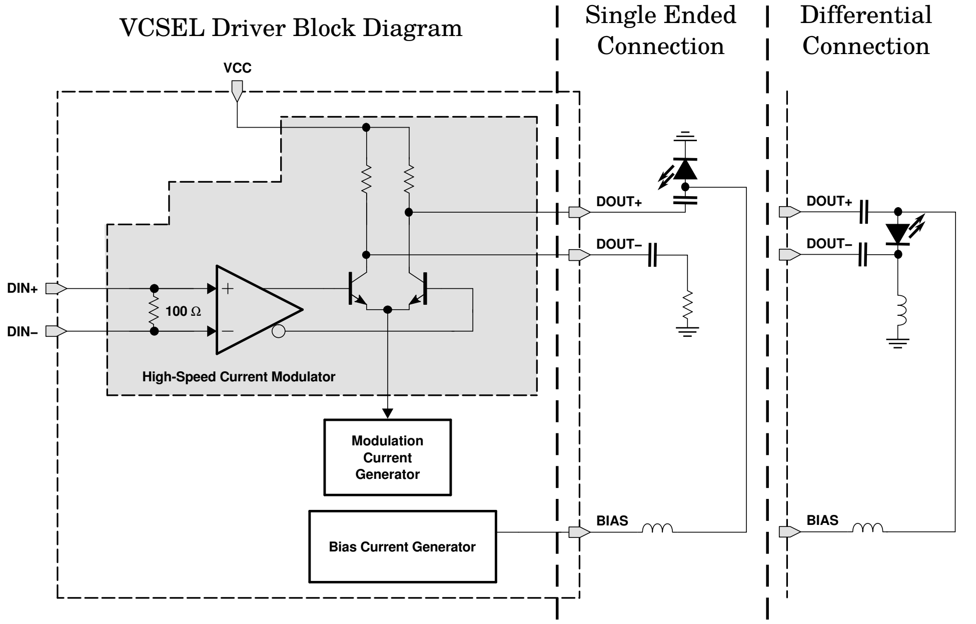


Figure 5.9: A simplified block diagram for the driver IC. The differential input signal DIN± is interpreted by a comparator. The inverted and normal output of the comparator then each control a transistor, for turning the modulation current on or off. The difference of the external differential wiring, compared to the single ended wiring is shown on the left side of the scheme, where circuitry at the output side of the IC is shown again. Block diagram inferred from datasheet [40].

like depicted as a block diagram in figure 5.9 on the left side. This means that the diode is only connected to the positive modulation output of the IC, whereas the negative output is connected to ground. Both outputs are always coupled over a capacitor, which serves as a high-pass filter and inhibits misrouting of the bias current. Analogously, the inductive coupling of the bias current inhibits the modulation current to flow back into the chip.

Additionally displayed in figure 5.9 is a simplified block diagram of a VCSEL driver. It can be seen that the voltages at the two differential input pins (DIN+ and DIN−) are interpreted by a comparator. If the voltage at the DIN+ pin is higher than at the DIN− pin, representing a logical '1', the normal output of the comparator is high, while the inverted output (denoted with the circle) is low. A low level at the inverted output causes a limited current flow through the respective transistor.

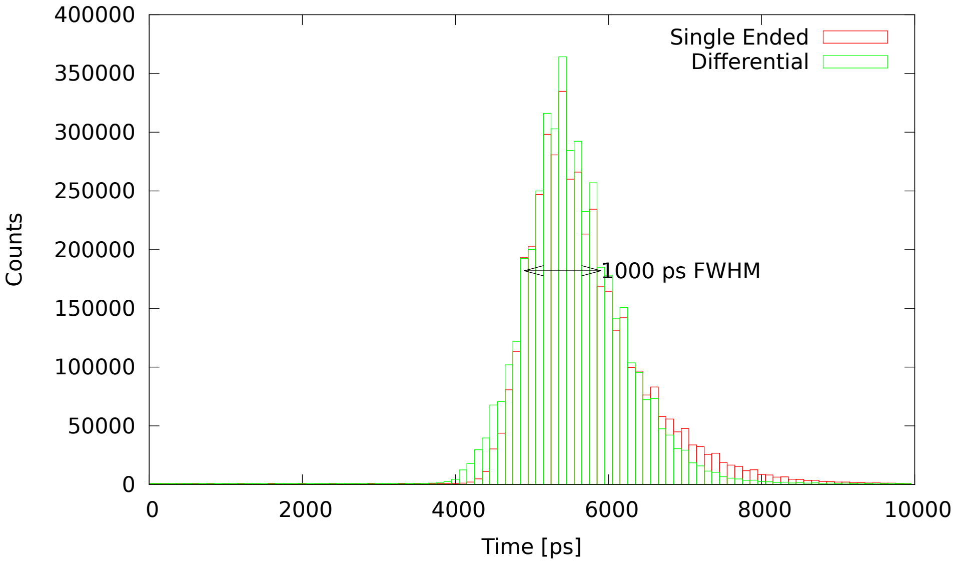


Figure 5.10: The arrival times for a single ended and a differentially connected VCSEL driven with the ONET4291VA.

Therefore, more current flows towards the DOUT+ pin and through the VCSEL. If the input levels are interpreted as a logical '0'. A high level at the inverted output "opens" the transistor, and the current is bypassed around the VCSEL.

The second way of connecting a laser diode to the driver IC is displayed on the right side in figure 5.9. Here both outputs, DOUT+ and DOUT−, of the driver are connected to the diode. That is why this kind of connection is called differential. If a VCSEL is differentially connected and the IC interprets the data input as a logical '1', the modulation current is flowing back into the driver chip and through the open transistor, corresponding to the normal output of the comparator. In addition to that, the current flow is immediately stopped when the voltages at the input pins are interpreted as a '0' by closing the transistor. In this way one expects a more symmetric response for the optical pulses the connected VCSEL produces, which does not necessarily mean that the pulses become shorter with respect to their FWHM.

Because shorter pulses allow for a stricter time filtering, the second evaluation board, was designed to support both methods of connecting the diode. The differences in the arrival times between those two methods are shown in figure 5.10 for the ONET4291VA and in figure 5.11 for the ONET8501V.

Especially for the ONET8501V an improvement of the pulse shape and

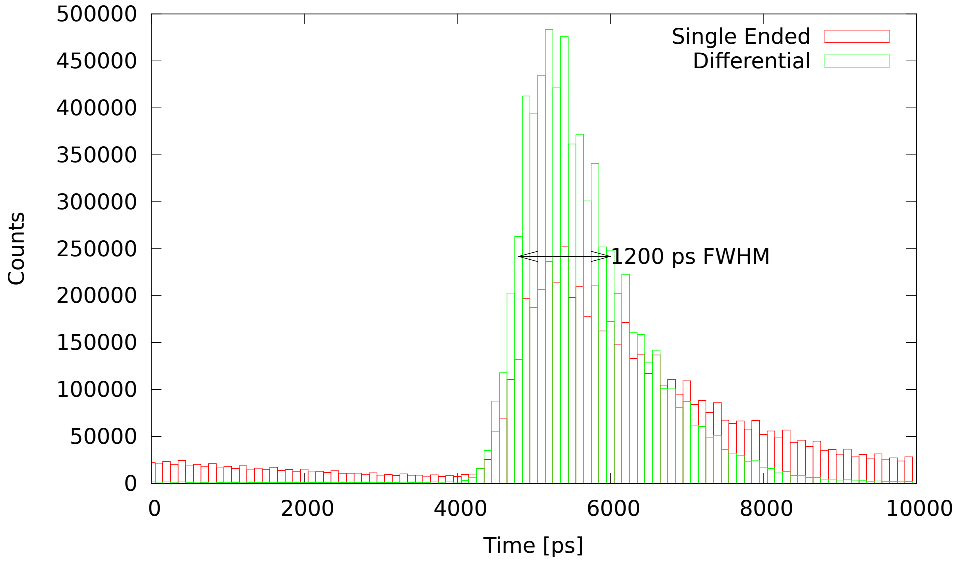


Figure 5.11: The arrival times for a single ended and a differentially connected VCSEL driven with the ONET8501V.

width is clearly visible. The pulse width could be reduced from 1.8 ns to 1.2 ns, yet the ONET4291VA still produces the shorter light pulses. It is also obvious that the contrast for the ONET8501V improved, however again the ONET4291VA shows a similarly good contrast, even in the single ended case.

The poorer performance of the ONET8501VA can be explained by the advanced features this chip has. For example an extra stage for over- and undershoot control is realized inside the chip with additional circuitry. This features, being normally an advantage, have obviously a negative effect on the pulse shape in the untypical application of QKD.

Note that the measured pulse shape is a convolution of the jitter of the APD and the actual optical pulse shape. If one assumes a Gaussian distribution for this jitter as well as for the optical pulse, the measured FWHM_m is given by

$$\mathrm{FWHM}_m = \sqrt{{\mathrm{FWHM}_{\mathrm{APD}}}^2 + {\mathrm{FWHM}_{\mathrm{pulse}}}^2}, \tag{5.1}$$

where the FWHMs below the square root are the FWHM of the APD and the pulse, respectively.

Because for four diodes, four additional lines are necessary in a differential design and the ONET4291VA showed a good behavior with a single ended connection, too, a first prototype of the electronics for a

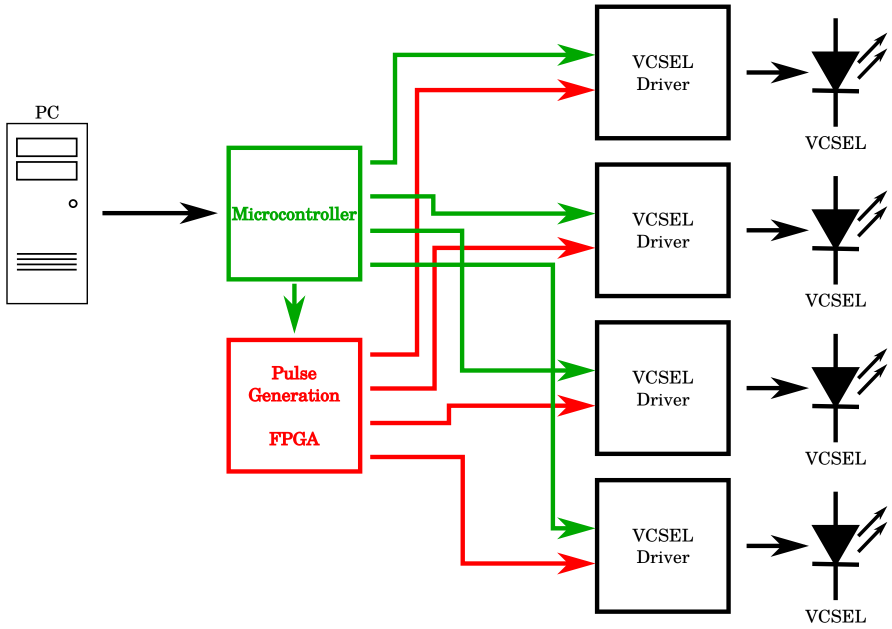


Figure 5.12: A block diagram for the circuitry of the prototype electronics of a QKD transmitter module. Short pulses are generated using a FPGA and are translated into modulation currents by four VCSEL drivers, each of which drives one VCSEL. In addition a microcontroller is used to set the bias and modulation currents of the drivers, as well as to control the FPGA.

QKD transmitter was designed with this IC used in a single ended design.

5.3 Prototype Electronics for a VCSEL Based QKD Transmitter Module

After a suited VCSEL driver was found, a first prototype for the electronics was designed. Figure 5.12 sketches the schematics of the prototype. The design is similar to the one of the second evaluation board, using a FPGA as a pulse generator and a microcontroller for setting the pulse widths produced by the FPGA and the modulation and bias currents of the four laser drivers.

A big difference between the designs, though, are the different requirements for the pulse generation on the FPGA. Whereas on the second evaluation board the same pulses were used for both ICs, it is now necessary to send pulses to the four different drivers for the diodes one after another.

This requires a new internal design of the FPGA, as can be seen in figure 5.13. In the upper part the internal circuitry of the FPGA used on the evaluation board is shown for comparison. The normal clock signal A and the inverse shifted clock signal $\neg B$ are and-gated at one lookup table (LUT) and then forwarded to both tested ICs. On the transmitter prototype, however, a third signal C_i, which determines whether the respective i^{th} VCSEL is active during the current pulse, needs to be evaluated at four different LUTs. Therefore the logical operation carried out on each of those four LUTs reads as $(A \wedge \neg B) \wedge C_i$.

Since all of the four laser diodes have to have the same temporal behavior, this method of producing short pulses, gave rise to another problem. The LUTs used to carry out the necessary logical operations written above, are physically located at different places in the FPGA, resulting in different propagation delays for the two clock signals A and B. Although the FPGA features so called dedicated clock routes, which are especially designed for carrying clock signals with a low propagation delay and jitter, the effect of the different delays could be seen clearly on the resulting pulses at the different outputs.

In figure 5.14 the pulses of the four LVDS signals obtained from the FPGA are shown, together with the logical interpretation of those signals. If one wants to calculate the overlaps of the signals, it is sufficient to compare the widths of the logical representations. In the worst case the overlap is only

$$\frac{345\,\mathrm{ps}}{1280\,\mathrm{ps}} \approx 0.27. \tag{5.2}$$

QKD is certainly not possible with an overlap of 27%, since this would open a side channel for an attack of a possible adversary. To compensate for that, it was attempted to insert additional gates and buffers, before the LUTs. Since those logical components individually delay the clock propagation, it should be possible to compensate for the different delays. However it turned out, that the different propagation times do not decouple, i.e. if an additional gate was inserted in front of one LUT, it also changed the delays on all the other LUTs.

With this method the overlap between the pulses could be slightly improved, as displayed in figure 5.15. The overlap in the worst case for the corrected delays yields

$$\frac{430\,\mathrm{ps}}{860\,\mathrm{ps}} = 0.5, \tag{5.3}$$

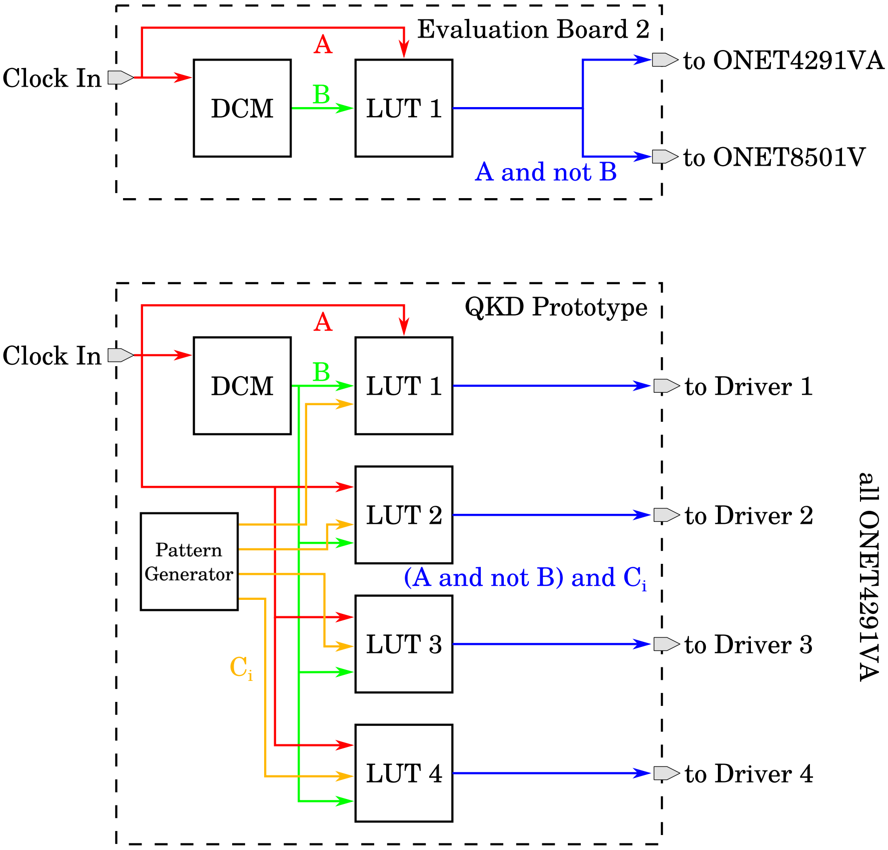


Figure 5.13: The additional requirements for the transmitter module impose a different internal design of the FPGA. Contrary to the design used on the evaluation board (top), the design used for the transmitter needs one LUT per driver IC. The additional signals C_i determine whether the i^{th} diode is active during the current pulse. Therefore all of the four LUTs have to carry out the logical operation $(A \wedge \neg B) \wedge C_i$. The signals C_i are produced by an additionally programmed pattern generator module on the FPGA.

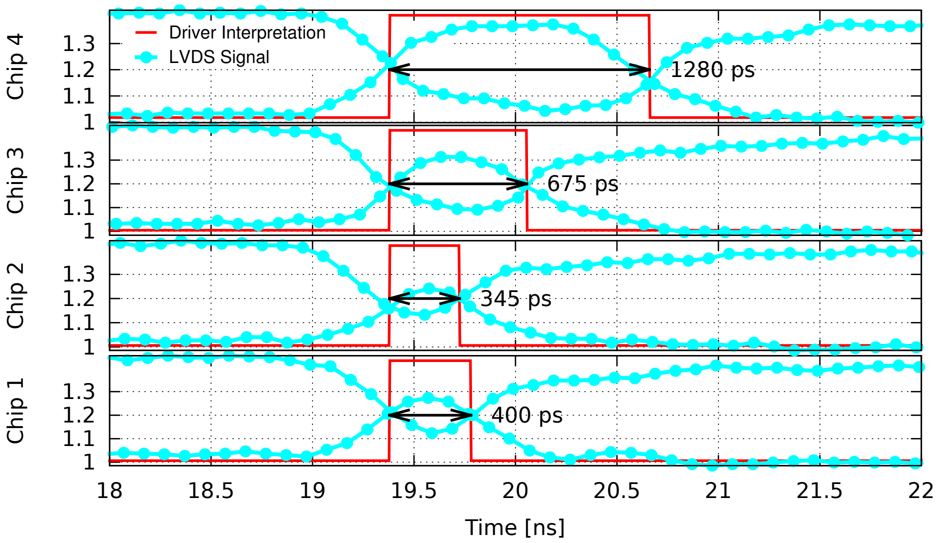


Figure 5.14: The differential signals for the pulses produced by the FPGA. The logical interpretation of those signals is denoted in red for every driver. The respective pulse widths vary due to different propagation delays for the LUTs in the FPGA. The y-axes show the voltage for the two differential lines according to the LVDS standard. All of those signals were individually triggered on a DSO.

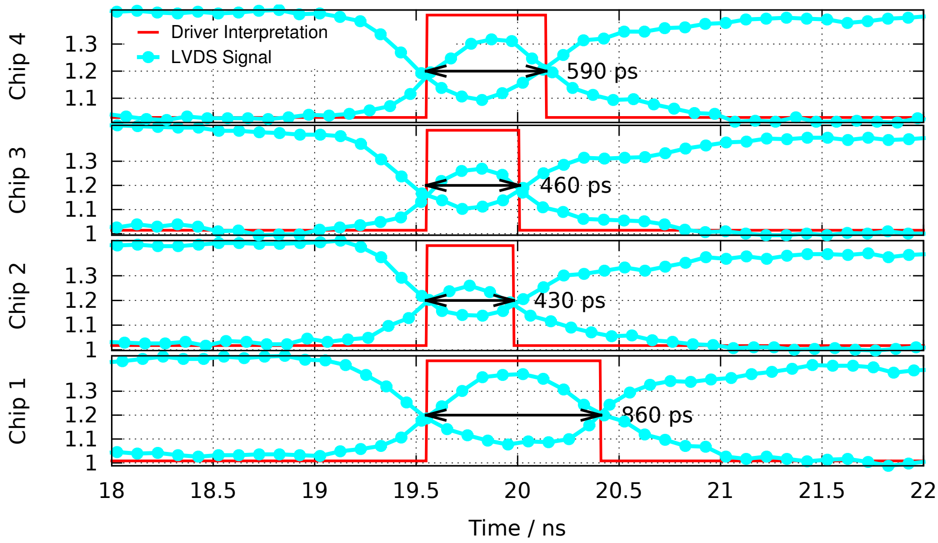


Figure 5.15: The differential signals for pulses after inserting additional logical elements. The difference between the pulse widths has improved, yet is still not sufficient for a secure QKD device. All of those signals were individually triggered on a DSO.

which is still not sufficient for QKD.

Yet, the electrical answer of the laser drivers, as seen in figure 5.16, show better correlations than the LVDS input signals do. The low bias currents and high modulations, needed for a QKD application as well as the duty cycle of only 10%, are a rather untypical configuration for the intended application of the IC. It is therefore conceivable, that the LVDS signal only functions as a trigger for the pulse generation, since the driver cannot achieve its specified data rate, what would explain the better overlap. Those pulses, though, were measured without a VCSEL connected to the drivers but connected to a 50 Ω resistor, therefore this result is only preliminary. For future tests it would be worth checking the optical pulses produced in this configuration. This could not be measured yet, since only one VCSEL on the array could successfully be bonded.

Depending on the results for the optical pulses, it may be necessary to add further circuitry to the electronics, which is dedicated to pulse shaping. Also, the delays between the different pulses for the respective driver chips have not been considered for this first prototype electronics, here compensation by additional delay lines may become necessary.

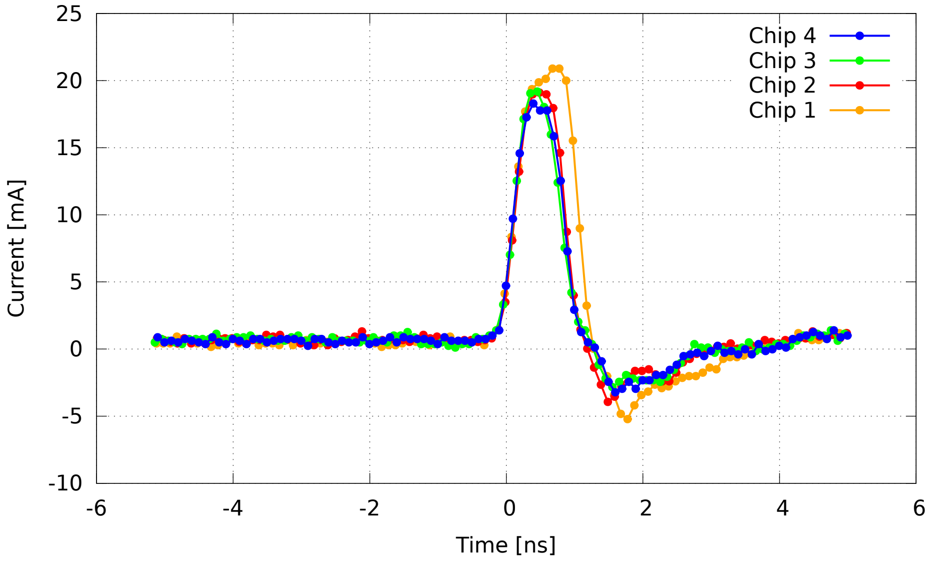


Figure 5.16: The electrical answers of the four driver ICs corresponding to the input signals in 5.15. The correlation is much better than for the LVDS signals. The y-axis shows the current corresponding to the voltage drop over a 50 Ω resistor, measured with the DSO. The x-axis is the time in ns. Every point on the curves corresponds to one sample from the oscilloscope.

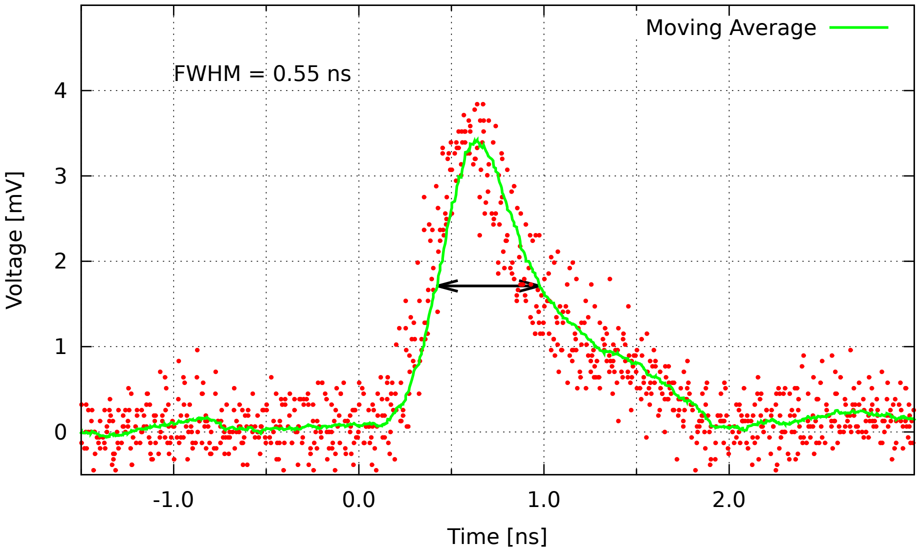


Figure 5.17: The voltage signal of a fast photodiode, while short pulses from one VCSEL were applied. The green curve is a moving average of the data points and yields a FWHM of 550 ps. The red points represent the samples measured on the DSO of 10 consecutive pulses.

Nevertheless, the prototype electronics were used to check the width of the optical pulse produced by the one functioning VCSEL. To this aim the light emitted from the VCSEL was collected and coupled onto a fast photodiode, which is specified for a bandwidth of 7 GHz. The voltage signal from the photodiode was then measured using a DSO with a bandwidth of 2 GHz.

The result of this measurement is displayed in figure 5.17, where a moving average was applied to the data to determine the FWHM. With that curve the FWHM and thereby the pulse width for the first VCSEL driven with the prototype electronics, was 550 ps. This pulse is surely short enough for the application in QKD, with respect to the certainly higher APD jitter at the receiver.

6 Conclusion and Outlook

This thesis describes the first steps towards a hand-held QKD sender, which has the potential to enable QKD in mobile hand-held scenarios. For this purpose, the characterization of the single components for a future miniaturized QKD device was performed in this work.

The laser written waveguides used in the future QKD transmitter for overlapping the light from four different VCSELs were characterized in terms of their birefringence and bending losses. As expected, a slight birefringence, emerging from the elliptical cross-section, could be verified. Additionally the dispersion of the birefringence was tested and analyzed with respect to depolarization, giving an upper bound for spectral widths of light sources used together with the integrated optics. Bending losses, which arise on curved sections depend on the polarization of the light. Together with asymmetric power splitting by a BS structure, a change of the ±45° polarizations occurs. It was shown that a compensation of those changes can be achieved by preparing quantum states in specific input polarizations and that laser-written waveguides are a well suited device to prepare the states required for QKD.

Since VCSELs exhibit a round emission pattern, which couples well into waveguides, and since they show a better power efficiency compared to EELs, they are considered to be well suited for a small, portable QKD transmitter. Their temperature dependence, was verified to be much smaller than for conventional EELs, which is a big advantage for a hand-held device. Their spectral distributions, were also found to be sufficiently small to fulfill the requirements imposed by the dispersion of the waveguides. In addition, the DOP of the light produced by the VCSELs is small enough, such that very low fluctuations in the pulse intensities are expected for the four different polarizations.

The electronics, necessary for driving the VCSELs in short pulses, were designed and tested for different dedicated VCSEL driver ICs. Those first evaluations boards, were used to select a suited IC for a QKD application. In terms of contrast and pulse width, the ONET4291VA was found to be the most applicable choice for the transmitter electronics. Finally, a first prototype of the circuitry for a VCSEL based QKD transmitter module, was designed. Further the pulse generation, using a FPGA

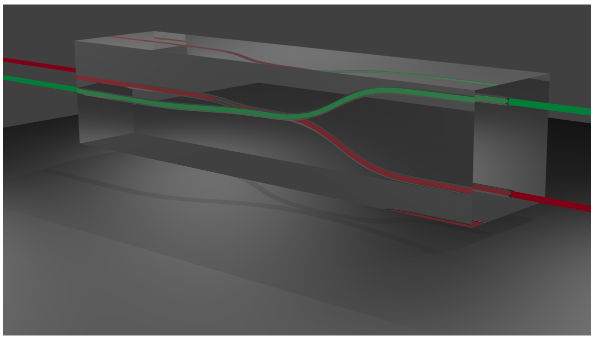


Figure 6.1: An alternative geometry for the integrated beamsplitters, where the possibility of a three dimensional path is used to exchange the bending between $| V\rangle$ and $| H\rangle$. Both waveguides of the directional coupler start and approach each other in a horizontal plane. However they, after brought into close proximity, move away from each other in vertical direction, following a true three dimensional path.

was implemented and found problematic, considering the deviating pulse widths for the four different VCSELs. However, additionally circuitry for pulse shaping can solve this problem.

Up to this point, the study of the single components revealed no unsolvable problems, which could prevent a realization of the QKD transmitter. Of course, there are still remaining task that need to be done, such as the investigation of laser written samples with more than one BS. Their splitting ratios and bending losses have to be studied very carefully, since they introduce additional changes of the polarization, which have direct consequences on the state preparation and consequently on the orientation of the polarizers.

In the scheme presented in section 2.5 the complete waveguide geometry is located in one plane. However the possibility to write three-dimensional paths could be used to realize a geometry like the one displayed in figure 6.1. By exchanging the direction of the bending, it may be possible to balance the polarization rotations caused by the losses occurring on curved paths.

The electronics, which, up to now, are only capable of emitting the four polarization in a predefined pattern, need to be expanded to a real random choice of the polarization states. For example the one-chip quantum random number generator described in [43], could be integrated for this purpose. In addition the optical pulse widths and delays have to be reviewed, using a VCSEL array with four functioning diodes. The experiments with the evaluation boards show that the electronics have to be probably extended by dedicated circuitry for pulse shaping and delay compensation.

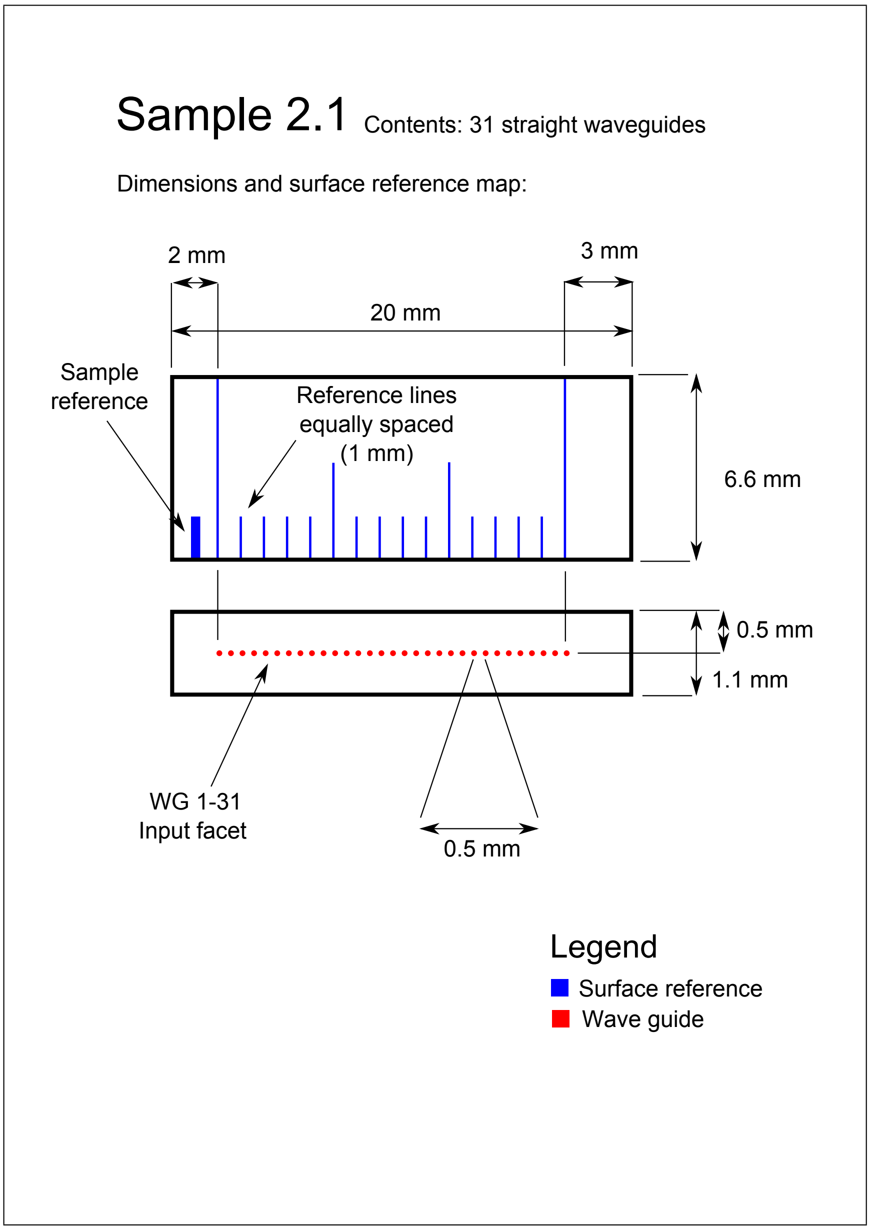
An additional task will be the alignment of the hand-held QKD transmitter relative to the receiver. For this purpose a closed-loop system, controlling the detection direction of the receiver, will be necessary [44, 45]. To align the degree of freedom, corresponding to rotations of the transmitter along the beam axis, one can use q-plates [46, 47], as an additional element at the output of the transmitter and at the entrance of the receiver. q-plates are an optical element, which transform the four polarization states used for QKD into four different and rotationally invariant states, along the beam axis. By the use of q-plates one can thereby compensate this one rotational degree of freedom.

Shortly mentioned during the presentation of the overall scheme of the future sender module, yet not discussed in this thesis, were the wire-grid polarizers used for the state preparation at the entrances of the waveguides. The polarizers were lithographically fabricated by Gwenaelle Vest according to e.g. [48], since commercial polarizers are not available sufficiently thin to apply them together with the micro lens array. The latest fabricated polarizers, now produced in a better equipped clean room with focused ion beam etching instead of e-beam lithography, showed contrasts on the order of 1 : 120, sufficient for the application in QKD.

With the progress achieved so far and the remaining tasks solved, the future portable QKD sender will enable QKD in real life. The very compressed form factor of the optics, being realized in one bulk of glass, is a promising approach for miniaturization. In fact, it is possible to realize the complete sender in such a small volume, that the integration of QKD transmitters in future smartphones becomes possible. This would enable a whole new class of applications for QKD, from drawing money at an ATM to secure exchange of highly confidential data. This possibility to establish a secure connection between two communication nodes at any time in any place, protected by the laws of nature, has the potential to establish a whole new level of privacy for governmental institutions as well as individual persons.

A Sample Geometries

The sample geometries as given by the group of Roberto Osellame. The here depicted drawings were delivered together with the samples.

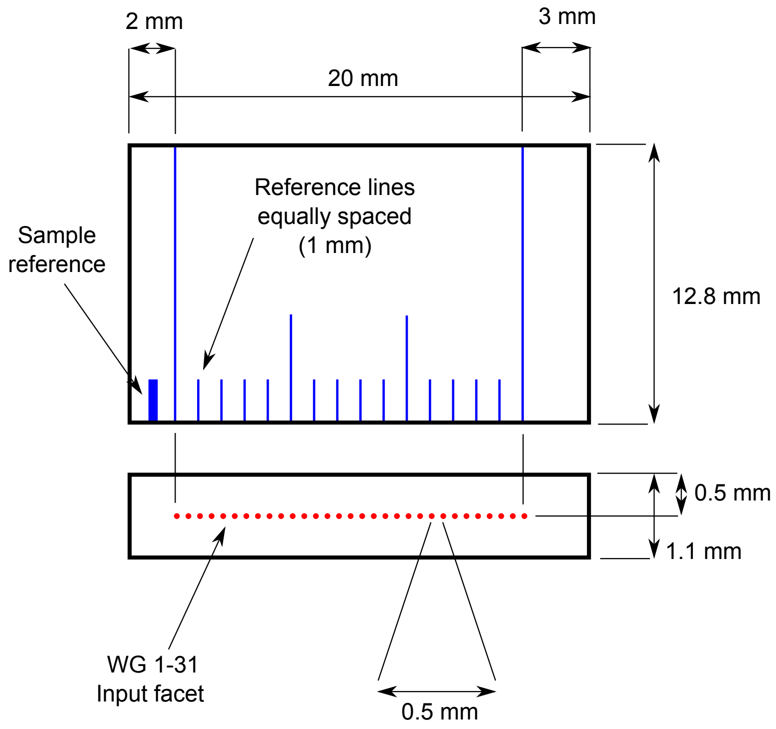


Sample 2.1 Contents: 31 straight waveguides

Dimensions and surface reference map:

Sample 2.2 Contents: 31 straight waveguides

Dimensions and surface reference map:



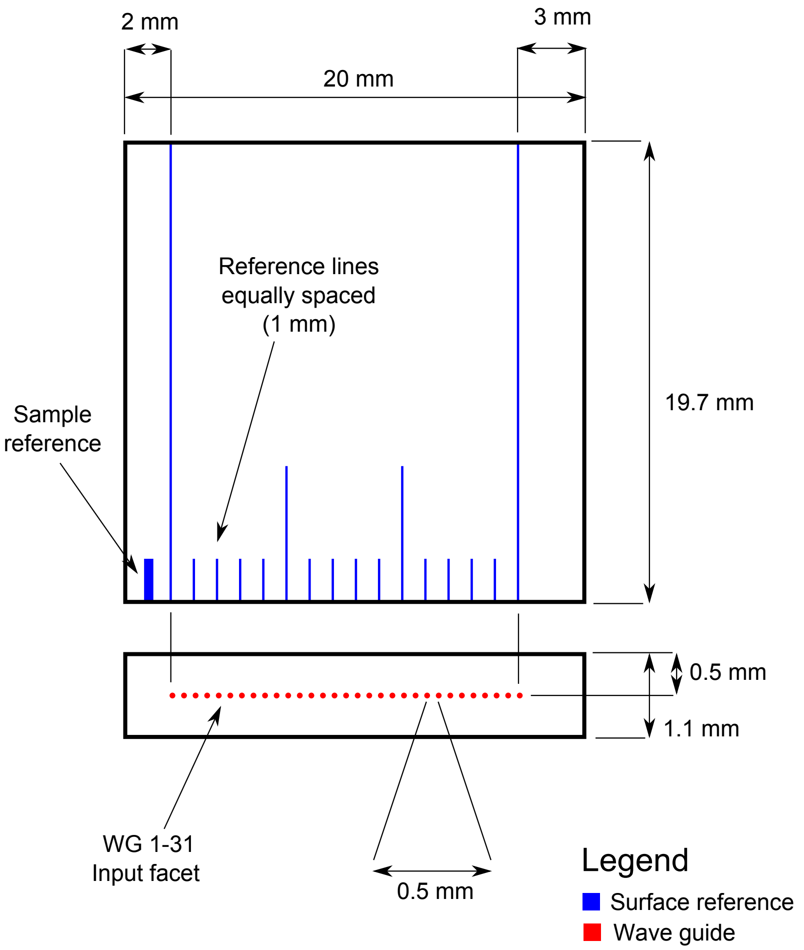
Legend

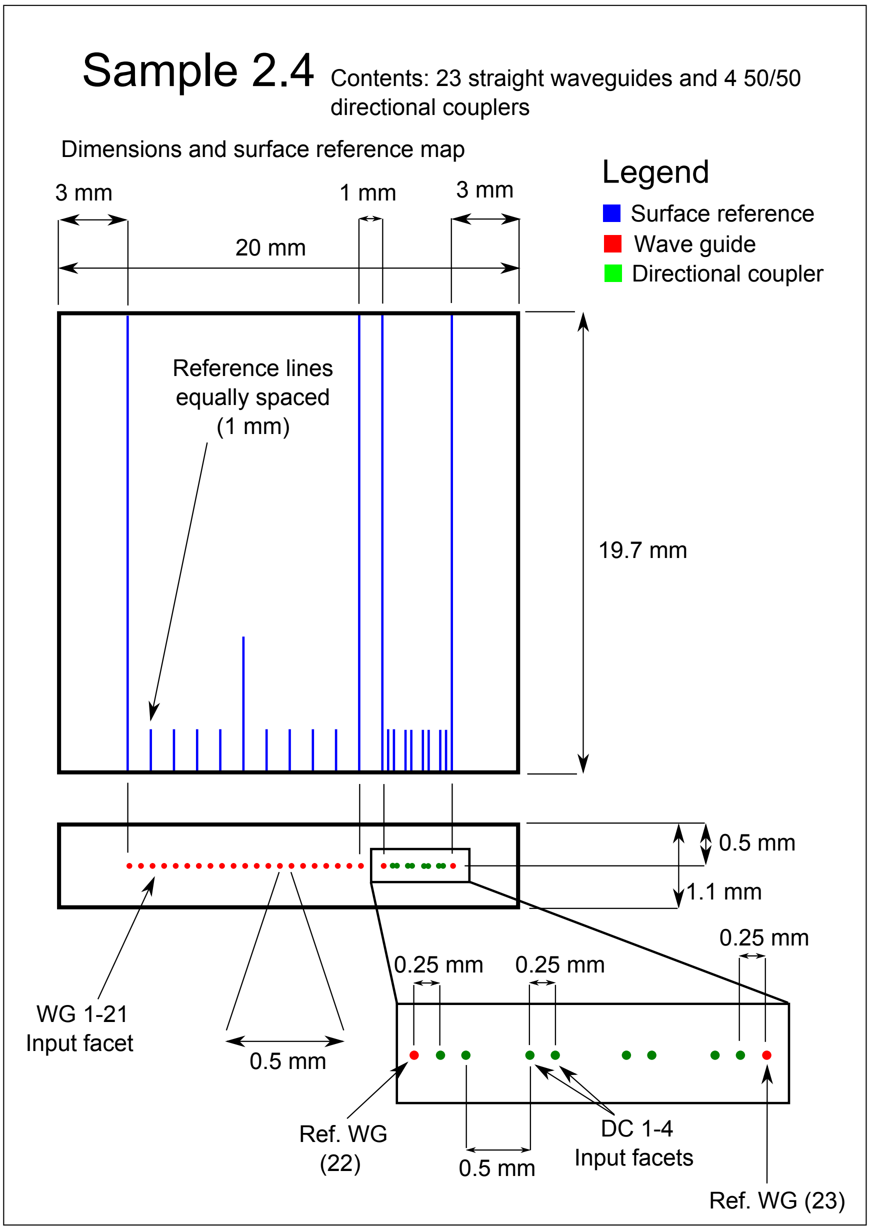
🟦 Surface reference

🟥 Wave guide

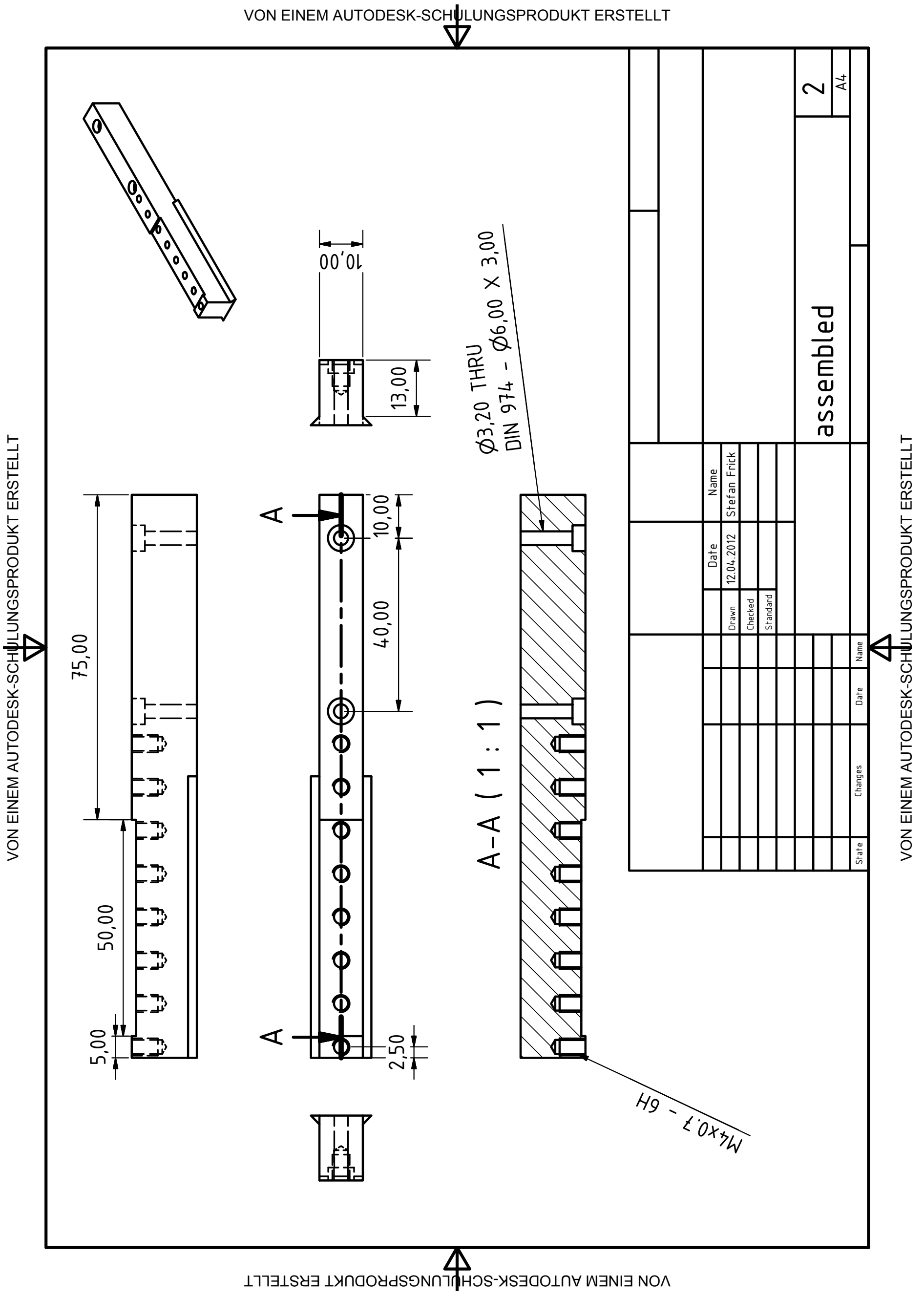
Sample 2.3 Contents: 31 straight waveguides

Dimensions and surface reference map




Sample 2.4
Contents: 23 straight waveguides and 4 50/50 directional couplers
Dimensions and surface reference map
Legend
🟦 Surface reference
🟥 Wave guide
🟩 Directional coupler
3 mm
1 mm
3 mm
20 mm
Reference lines equally spaced (1 mm)
19.7 mm
0.5 mm
1.1 mm
0.25 mm
0.25 mm
0.25 mm
WG 1-21 Input facet
0.5 mm
Ref. WG (22)
0.5 mm
DC 1-4 Input facets
Ref. WG (23)

B Sample Holder Drawing



The here depicted sample holder was designed to be mounted on a xyz-translations stage (Thorlabs, NanoMax300, MAX313D). The sample can be aligned with the help of the edges on the left part of the holder and clamped with standard “Clamping Arms” (PM3/M) for platform mounts, supported by Thorlabs.

C Raw Data for the DOP Measurements on VCSELs

The data given here are the average counts per second measured on the APD. This average was found by measuring every projection for $5 \times 5s$. The dark counts were only measured once for the measurements in continuous operation. For the pulsed operation they were measured again, because a weaker optical density filter was used.

Current	c_H	c_V	c_+	c_-	c_R	c_L	Dark Counts
1 mA	1141	2404	1271	1884	1731	1875	336
2 mA	3963	18218	4939	16993	10318	11225	336
3 mA	6045	30027	8116	27402	16681	18065	336
Pulsed	57673	59020	61823	54069	56409	56931	337

Table C.1: Raw data of the DOP measurement on a VCSEL.

D Schematics of the First Evaluation Board

E Schematics of the Second Evaluation Board

F Schematics of the Prototype Electronics for a QKD Transmitter Module

Bibliography

[1] T. Duong & J. Rizzo. Here Come The XOR Ninjas (2011)

[2] N. J. Alfardan & K. G. Paterson. Lucky Thirteen : Breaking the TLS and DTLS Record Protocols (2013)

[3] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics* **21**, 467 (1982)

[4] J. O. T.D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe. Quantum computers. *Nature* **464**, 45 (2010)

[5] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *of Computer Science, 1994 Proceedings., 35th* **20**, 352 (1994)

[6] C.-Y. Lu, D. Browne, T. Yang & J.-W. Pan. Demonstration of a Compiled Version of Shor's Quantum Factoring Algorithm Using Photonic Qubits. *Physical Review Letters* **99**, 1 (2007)

[7] B. Lanyon, T. Weinhold, N. Langford, M. Barbieri, D. James, A. Gilchrist & A. White. Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement. *Physical Review Letters* **99**, 5 (2007)

[8] A. Politi, J. C. F. Matthews & J. L. O. Brien. Shor's Quantum Factoring Algorithm on a Photonic Chip. *Science (New York, N.Y.)* **325**, 1221 (2009)

[9] N. Gisin, G. Ribordy, W. Tittel & H. Zbinden. Quantum cryptography. *Rev. Mod. Phys* **74**, 145 (2002)

[10] http://www.idquantique.com

[11] M. Peev, C. Pacher, A. Alleaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, F. S, S. Fossier, M. Fürst, J.-D. Gautier, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legre, R. Lieger, J. Lodewyck,

T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden & A. Zeilinger. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics* **11**, 075001 (2009)

[12] J. E. Nordholt, R. J. Hughes, G. L. Morgan, C. G. Peterson & C. C. Wipf. Present and future free-space quantum key distribution. In *Proc. SPIE 4635, Free-Space Laser Communication Technologies XIV, 116*, volume 4635 (2002)

[13] J. M. Perdigues Armengol, B. Furch, C. J. de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter & A. Zeilinger. Quantum communications at ESA: Towards a space experiment on the ISS. *Acta Astronautica* **63**, 165 (2008)

[14] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwarth, S. Frick & H. Weinfurter. Air to Ground Quantum Communication. *Nature Photonics (accepted)* (2013)

[15] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. Rarity, A. Zeilinger & H. Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Physical Review Letters* **98**, 010504 (2007)

[16] J. L. Duligall, M. S. Godfrey, K. a. Harrison, W. J. Munro & J. G. Rarity. Low cost and compact quantum key distribution. *New Journal of Physics* **8**, 249 (2006)

[17] C. H. Bennett & G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. Bangalore, India (1984)

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

[19] C. E. Shannon. A Mathematical Theory of Communication. *Mobile Computing and Communication Review* **5**, 3 (1948)

[20] W. K. Wootters & W. H. Zurek. A single quantum cannot be cloned. *Nature* **299**, 802 (1982)

[21] G. Brassard & L. Salvail. Secret-Key Reconciliation by Public Discussion. In T. Helleseth (Editor), *Advances in Cryptology - EUROCRYPT '93*, pages 410–423. Springer Berlin / Heidelberg (1994)

[22] C. H. Bennett, G. Brassard & J.-M. Robert. Privacy Amplification by Public Discussion. *SIAM J. Comput* **17**, 210 (1988)

[23] H.-K. Lo, X. Ma & K. Chen. Decoy State Quantum Key Distribution. *Physical Review Letters* **94**, 230504 (2005)

[24] X. Ma, B. Qi, Y. Zhao & H.-k. Lo. Practical Decoy State for Quantum Key Distribution. *Arxiv preprint quant-ph* (2008)

[25] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster & J. G. Rarity. A step towards global key distribution. *Nature* **419**, 450 (2002)

[26] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer & H. Weinfurter. High speed optical quantum random number generation. *Optics express* **18**, 13029 (2010)

[27] G. D. Marshall, A. Politi, J. C. F. Matthews, P. Dekker, M. Ams, M. J. Withford & J. L. O'Brien. Laser written waveguide photonic quantum circuits. *Optics express* **17**, 12546 (2009)

[28] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi & R. Osellame. Two-Particle Bosonic-Fermionic Quantum Walk via Integrated Photonics. *Physical Review Letters* **108**, 1 (2012)

[29] A. Crespi, R. Ramponi, R. Osellame, L. Sansoni, I. Bongioanni, F. Sciarrino, G. Vallone & P. Mataloni. Integrated photonic quantum gates for polarization qubits. *Nature communications* **2**, 566 (2011)

[30] K. M. Davis, K. Miura, N. Sugimoto & K. Hirao. Writing waveguides in glass with a femtosecond laser. *Optics letters* **21**, 1729 (1996)

[31] R. Osellame, G. Cerullo & R. Ramponi (Editors). *Femtosecond Laser Micromachining.* Springer Heidelberg Dordrecht London New York (2012)

[32] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi & R. Osellame. Polarization Entangled State Measurement on a Chip. *Physical Review Letters* **105**, 1 (2010)

[33] A. Politi, M. J. Cryan, J. G. Rarity, S. Yu & J. L. O'Brien. Silica-on-silicon waveguide quantum circuits. *Science (New York, N.Y.)* **320**, 646 (2008)

[34] A. Yariv. Coupled-mode theory for guided-wave optics. *IEEE Journal of Quantum Electronics* **9**, 919 (1973)

[35] B. E. Little & W. P. Huang. Coupled-Mode Theory for Optical Waveguides. *Progress in Electromagnatics Research* **10**, 217 (1995)

[36] D. Gottesman, H.-K. Lo, N. Lütkenhaus & J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.* **5**, 325 (2004)

[37] R. Michalzik (Editor). *VCSELs.* Springer Heidelberg Dordrecht London New York (2013)

[38] H. Soda, K. Iga, C. Kitahara & Y. Suematsz. GaInAs/InP surface emitting injection lasers. *Jpn. J. Appl. Phys.* **18**, 2329 (1979)

[39] D. L. Huffaker, D. G. Deppe, K. Kumar & T. J. Rogers. Native-oxide defined ring contact for low threshold vertical-cavity lasers. *Applied Physics Letters* **65**, 97 (1994)

[40] ONET4291VA - 1 GBPS TO 4.25 GBPS MULTI-RATE VCSEL DRIVER, Datasheet (2005)

[41] LTC5100 - 3.3V, 3.2Gbps VCSEL Driver, Datasheet (2003)

[42] 11 . 3 Gbps Differential VCSEL Driver With Output Waveform Shaping ONET8501V, Datasheet (2007)

[43] S. Tisa & F. Zappa. One-chip Quantum Random Number Generator. *Proc. of SPIE* **7236**, 72360J (2009)

[44] S. Frick. *Aufbau und Charakterisierung eines Laserausrichtungssystems in der Anwendung der Quantenkryptographie.* Bachelor's thesis, Ludwig-Maximilians-Universität München (2010)

[45] S. Sorg. *Optimierung und Erweiterung eines Strahlführungssystems für die Quantenkryptographie.* Bachelor's thesis, Ludwig-Maximilans-Universität München (2011)

[46] A. Laing, V. Scarani, J. G. Rarity & J. L. O'Brien. Reference-frame-independent quantum key distribution. *Physical Review A* **82**, 012304 (2010)

[47] V. D'Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci & F. Sciarrino. Complete experimental toolbox for alignment-free quantum communication. *Nature communications* **3**, 961 (2012)

[48] H. Tamada, T. Doumuki, T. Yamaguchi & S. Matsumoto. Al wire-grid polarizer using the s-polarization resonance effect at the 0.8-microm-wavelength band. *Optics letters* **22**, 419 (1997)

Danksagung

Zum Abschluss möchte ich Allen danken, die mich während meines Studiums und der Masterarbeit im letzten Jahr begleitet haben:

- Prof. Weinfurter dafür, dass er mir die Möglichkeit gab in seiner Arbeitsgruppe meine Masterarbeit anzufertigen
- Meinen Betreuern, Gwen, Markus und Sebastian, die mir immer mit gutem Rat zur Seite standen
- Sebastian, im Speziellen, für das Lektorat
- Allen Mitgliederen der Arbeitsgruppe Weinfurter für die gemeinsamen Mittagessen und dafür, dass es auch immer wieder andere Themen als die Physik zu besprechen gab.
- Beiden Daniels, für das ein oder andere gemeinsame Bier
- Kai, der mein Schatz an unnützem Wissen in den letzten Monaten verdoppelt hat
- Allen die dabei waren, für den Abend in der Hexenstube mit “Ballermann 6” und “Kammermusik”
- Meinen Kommilitonen: Michi, Katharina, Ike, Jonas, Felix, Katharina, Alex und Caro, mit denen man wunderbar feiern, diskutieren und lernen konnte
- Der quTools GmbH, die es mir auch im letzen halben Jahr ermöglichte meinen Kühlschrank zu füllen
- Allen Freunden aus der Heimat dafür, dass der Kontakt auch seit über fünf Jahren München, Köln, Leipzig, Augsburg, Stuttgart und Berlin noch immer so stark ist
- Meiner Oma, für die vielen CARE-Pakete
- Meinen Eltern dafür, dass sie mich erst auf die Schule und dann an die Universität geschickt haben und die letzen 26 Jahre immer unterstützt haben