Master's Thesis

Towards a practical integrated QKD sender

Ludwig Maximilian University of Munich

Clemens Sonnleitner

Munich 2018

Towards a practical integrated QKD sender

Master's Thesis

Faculty of Physics
Ludwig Maximilian University of Munich

Chair Prof. Dr. Theodor W. Hänsch
AG Prof. Dr. Harald Weinfurter

Handed in by:
Clemens Sonnleitner

January 24, 2018
Munich

Supervised by Prof. Dr. Harald Weinfurter

Entwicklungen für kompakte freistrahl QKD Sender

Masterarbeit

Fakultät für Physik
Ludwig-Maximilians-Universität München

Lehrstuhl Prof. Dr. Theodor W. Hänsch
AG Prof. Dr. Harald Weinfurter

Vorgelegt von:
Clemens Sonnleitner

München, den 24.01.2018

Betreut durch Prof. Dr. Harald Weinfurter

Abstract

Quantum key distribution (QKD) promises unconditional security for key distribution only based on quantum mechanical laws. Although the focus of research lies on long distance QKD, short range scenarios have a big field of application.

A miniature QKD sender, developed in our group by G. Mélen, implements the BB84 protocol and enables for short range free-space key exchange. The device uses weak coherent pulses from four Vertical-Cavity Surface-Emitting Lasers (VCSELs) at a wavelength of 850 nm. The preparation of the polarization states is done by wire-grid polarizers and the four spatial modes are overlapped using a waveguide circuit. An additional red beacon laser serves for aiming, beam tracking and clock generation.

One part of this thesis work were investigations on the optical waveguide circuit, where the temperature dependent change of the outputted polarizations has been characterized and optimized input polarizations have been evaluated.

The main part of this thesis deals with the development of new electronics for a QKD sender resulting in a modular design, which allows for fast testing of new pulse generation schemes. Here, the pulse generation based on delay meanders has been analyzed. The results suggest that the power consuming delay chips could be replaced, however at the cost of flexibility for adjusting the pulse shape and timing. The quality of the signal transmission from the mainboard to the subboard, which is one of the crucial points of a modular setup, shows good applicability.

Contents

1. Introduction

Most digital applications used by a great portion of the people in the world, only works by the exchange of data over the internet. In June 2017 the internet counted about 3.9 billion users which makes 52 % of the world population [1]. The emergence of this global network gave rise to new companies like Amazon, Alphabet Inc. (Google), and Facebook whose business model is built-on the interconnectedness of modern society and whose market capitalization significantly outruns the ones of traditional companies (Amazon: 624B USD, Alphabet Inc. 792B USD compared to VW AG: 93B USD, Daimler AG: 80B USD in January 2018[a]). Due to the possibilities of this network also the modus operandi of many traditional companies and institutions affiliated to governments changed drastically. But also the impact of the internet on the private life increases significantly especially with the emerge of smartphones and the Internet of Things (IoT). Beside the many positive aspects of an interconnected world also disputable facets like industrial espionage and cyberwarfare (e.g. Stuxnet which mainly targeted Iranian power plants [2–4]) have gained popularity.

One of the main problems of such a shared network is the secure communication in the presence of eavesdroppers, as the exchanged data can be recorded by everybody with physical access to the transmission line. The wish for secret communication not only in governmental institutions but also in industry and private use resulted in an enormous growth of the field of cryptography and gave rise to famous encryption schemes like AES and RSA, without which the modern internet would be unimaginable. These modern encryption schemes rely on complex mathematical functions and algorithms which are hard to solve on nowadays hardware in a reasonable amount of time. The security of these cryptosystems is not proven and the computational power of hardware is permanently rising which makes encryption schemes that are considered nowadays secure vulnerable in the future as it already happened before [5].

The only classical encryption scheme that is provable secure is Vernam's One-Time Pad [6], a symmetric cryptosystem. The problem with symmetric encryption schemes is the exchange of the private key. Quantum key distribution (QKD) schemes [7], as the famous BB84 protocol which was proposed by C. Bennett and G. Brassard in 1984 [8], are currently the only known ways for an unconditionally secure exchange of a secret key between two parties. The security of QKD is not

[a] Data from Bloomberg (www.bloomberg.com)

based on complex mathematical problems and assumptions on the technology but only on general laws of quantum physics. QKD relies on the exchange of quantum states (e.g. the polarization or phase degree of freedom of photons) which an attacker cannot measure without introducing errors [9]. As long as the error rate is not too high the legitimate users can apply classical privacy amplification methods to diminish the attackers knowledge of the key.

For the case of photons the sender and receiver can be connected either by optical fibers, where with nowadays technologies the practicable distance is limited to about 100–200 km [10–13], or over free space links even enabling for a key exchange between a satellite and an optical ground station where first experiments have been demonstrated recently [14, 15].

However, also short range QKD scenarios are interesting for a range of use-cases, like the transaction at an ATM or cantactless payment. A recently developed sender unit of our group [16, 17], implementing the BB84 protocol using attenuated laser pulses from four light sources (one for each polarization state), aims for these usage scenarios. The size of the optics of about $35 \times 20 \times 8\,\mathrm{mm}^3$ allows for the integration into conventional communication platforms like smartphones, pointing at the above mentioned usage scenarios.

In this thesis work investigations on the characteristics of a waveguide chip, which is used for the spatial overlap of the light sources, were done. At first the influences of temperature changes onto the transmitted polarization states were studied. This is necessary as an actual project of our group is the implementation of our sender module onto a small satellite (cubesat) where it undergoes huge temperature drifts. Furthermore, the four initial polarization states undergo a non unitary transformation, as the four waveguides behave slightly different. Here, a precompensation of this effect was done by evaluating and testing optimized input states.

The main part of this thesis work deals with the development of new electronics for a QKD sender which aims for lower power consumption, better stability and fast implementation possibility of new designs. Therefore, a modular design consisting of a mainboard, where the powering, management and clock generation of the module are placed and subboards, responsible for the modulation of the light sources connected via ribbon cables, has been developed. Several subboards with different pulse generation schemes have been designed and first investigations on the quality of the clock signal transmission from the mainboard to the subboards and an alternative pulse generation scheme were done.

This thesis is organized as follows. Chapter 2 introduces classical cryptography and establishes some theoretical background needed for the understanding of this thesis. In chapter 3 the actual state of our QKD experiment consisting of the miniaturized sender and a receiver optimized for hand-held key exchanges is described. The characterization of the waveguide circuit is outlined in chapter 4 and the development of the new electronics in chapter 5. Chapter 6 summarizes the results of this thesis work and shows remaining challenges and future tasks.

2. Theoretical fundamentals

In this chapter I will introduce the theoretical fundamentals and methods which are relevant for this thesis.

At the beginning classical cryptography will be introduced and the need for more powerful key distribution methods will be motivated. "Classical" means here, that no quantum theory is involved in the security principles. In the second section I will describe the basic concepts of quantum mechanics that are needed for the understanding of the following sections and the principles of QKD. In the last section of this chapter methods required for the description, preparation and measurement of polarization states are introduced.

2.1. Classical cryptography

Generally spoken, cryptography is the science of keeping secrets secret. In early times, cryptography was mostly about secure communication in the presence of eavesdroppers using encrypted messages. Nowadays, cryptography covers every topic related to the task of preserving secrets and for example also includes *data integrity* in the meaning that the receiver should be able to identify changes in the data he got and *authentication* which means that two communicating partners should be able to verify the identity of each other [18].

2.1.1. Basic concepts

A cryptosystem CS is a quintuple of the set of all plaintexts M (messages), the set of all keys K, the set of all ciphertexts C, the encryption function $e = M \times K \to C$ and the decryption function $d = C \times K \to M$

$$CS = (M, K, C, e, d) \tag{2.1}$$

An example of a cryptosystem is the *substitution* in which every character (with length n) of the plaintext is replaced by a different character (with length m). Mathematically spoken it is a function $f : A_1^n \to A_2^m$ and designed as an arithmetic function such as integer addition or integer multiplication. In practice most of the times it is achieved using a lookup table or *S-box*.

A possible example is [19]: Alphabet $A_1^1 = \{a, b, ..., z\}$ and $A_2^2 = \{1, 2, 3, 4, 5\}$ with the S-box given in table 2.1. By determining the row and column of every

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

Table 2.1.: Example of a S-box for encryption via substitution.

character in the plaintext one obtains the ciphertext. Here, the word `masterarbeit` results in `3211434415421142121524444`. A well-known example for a substitution cryptosystem is the German Enigma [20].

A special case of the substitution is the *permutation* $f : A^n \to A^n$. A simple example for $A_1 = A_2 = \{a, b, \ldots, z\}$ is the Caesar cipher (shift cipher), where the alphabet is shifted cyclically for a certain number (which is the key). The S-box for a caser cipher with $k = 5$ is denoted in table 2.2. The plaintext `aleaiactaest` results in `fqjfnfhyfjxy`. The cardinality of the possible keys is only 25 which makes it quite insecure.

a	b	c	d	e	f	g	h	i	…	v	w	x	y	z
f	s	h	i	j	k	l	m	n	…	a	b	c	d	e

Table 2.2.: Example for a Caeser chiffre with $k = 5$

Both presented cryptosystems on their own are typically not very secure, whereas a combination of both is used in modern chiffres: the plaintext is permuted and substituted multiple times to achieve a high complexity and incomparableness of the plaintext and the ciphertext.

Common cryptosystems can be divided into two groups by their type of key which will be presented in the next two subsections. The first group of algorithms are the symmetric-key systems, where the same key is used for encryption and decryption. The second group are the asymmetric-key algorithms which use distinct keys for encryption and decryption. Both will be explained further on the next pages.

2.1.2. Symmetric-Key Cryptography

In symmetric encryption schemes the sender and receiver share the same secret key that can be used for encryption and decryption of the message by a publicly known encryption and decryption scheme. The procedure works as follows: first, the sender ("Alice") and the receiver ("Bob") agree on a common key k which they keep secret. Alice encrypts the message m ("plaintext") she wants to transmit to Bob using an encryption algorithm e whereby she obtains the encrypted message ("ciphertext")

$c = e(k, p)$ which she sends to Bob. Bob uses the decryption algorithm d with the same key and recovers the message $m = d(k, c)$.

There exist two different types of functions (ciphers) performing the encryption, called block ciphers and stream ciphers. A block cipher processes the plaintexts in blocks with defined fixed binary length, which is also called the block length of the cipher. Stream ciphers operate on streams of plaintexts with arbitrary length, processing them character by character.

The big advantage of symmetric-key encryption is the possibility of a fast and efficient implementation in hard- and software [21–23] making them a well-suited candidate for the encryption of large amounts of data.

Two famous protocols implementing the generic encryption scheme described above are the Advanced Encryption Standard and the One-time Pad which I will describe in more detail.

AES

The Advanced Encryption Standard (AES) [24] is a block cipher and today's most present symmetric encryption scheme, widely used for example in the SSH protocol and WI-FI encryption via WPA2. It was standardized by the U.S. American National Institute of Standards and Technology (NIST) and superseded the famous Data Encryption Standard (DES) [25] in the early 2000s.

As the standardization process of AES is quite remarkable a short overview will be given. In 1997 NIST started an open selection process for a new encryption standard as successor of DES where proposals could be handed in from parties worldwide. The algorithms had to support a block size of at least 128 bit and key sizes of 128, 192 and 256 bit. At a conference in 1998 from the submitted 21 proposals 15 were accepted as candidates for the new standard. After a second conference in March 1999 and a public comment period, five of the fifteen algorithms were selected by NIST. In a second review period with further investigations on the proposals, where again the public was included, NIST selected the *Rijndael cipher* as new AES standard [26, 27].

Rijndael [28] was developed by Daemen and Rijmen and was developed for block and key sizes of 128, 160, 192, 224 and 256 bit which can be combined independently. AES is a subset of these possibilities and is defined for block lengths of 128 bit and key length of 128, 192 and 256 bit referred as AES-128, AES-192 and AES-256.

One has to remark, that it took more than ten years to find theoretical weaknesses which are nevertheless not relevant for practical attacks [29]. Until now, the security of AES is considered not to be broken which of course does not mean, that no applicable methods breaking the encryption scheme do exist.

One-Time Pad

Vernam's One-Time Pad [6, 30] is the most famous example of stream ciphers and the only encryption scheme, that is information theoretically absolutely secure which was proven by Shannon in 1949 [31], as no information can be retrieved from the ciphertext [32]. The plaintext, key and ciphertext are viewed as bit strings and for the encryption of the message stream m it is bitwise XORed with the key stream k whereas one obtains the ciphertext. Decryption is the inverse function and works by XORing again the ciphertext with the key. Summarized:

$$e_{\mathrm{OTP}}(k, m) := k \oplus m \quad \text{and} \quad d_{\mathrm{OTP}}(k, c) := k \oplus c$$

For the OTP it is essential that each bit of the key is chosen randomly and independently and that the key length is at least as long as the message. The key is also not allowed to be used twice. If the same key would be used for the messages m_1 and m_2, an attacker can derive $m_1 \oplus m_2$ from the two corresponding ciphertexts c_1 and c_2 by calculating [18]:

$$c_1 \oplus c_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \oplus k = m_1 \oplus m_2$$

and thereby gain information about the plaintexts.

The obvious disadvantage of Vernam's OTP is the required generation and secure transmission of truly random keys of sufficient length. An example where OTP was the Moscow-Washington hotline (a teleprinter) which was used during the cold war and for which keying tapes were exchanged via trusted couriers [33], which is not really practicable for general usage or encryption of nowadays amounts of data transmitted via the internet.

2.1.3. Asymmetric-Key Cryptography

As already meantioned, the conceptual problem in the symmetric way of encryption is, that Alice and Bob first have to share the secret key in a feasible and secure way. In 1976 W. Diffie and M. E. Hellman proposed a completely new type of encryption schemes called public-key cryptography [34] (or "asymmetric cryptography") where no pre-shared information has to exist.

Asymmetric encryption schemes are designed in a way so that the key that is used for encryption (public key) is a different one then the key used for decryption (secret key). The procedure works as follows: Bob generates a key pair consisting of the public key pk and the secret key sk. He publishes his public key over any medium (Internet, phone, etc.). Alice takes Bob's public key and encrypts the message with it using the encryption function e, thereby obtaining the ciphertext $c = e(pk, m) =: e_{pk}(m)$ which she sends to Bob. With his private key Bob can decrypt Alice's message $m = d(sk, c) =: d_{sk}(c)$.

A main requirement on asymmetric cryptosystems is, that the key for decryption of the message cannot be derived from the key for encryption and the ciphertext

in a reasonable amount of time, which can be realized by the usage of so-called mathematical one-way functions. These are functions that are easy to compute for every input, but the computation of the inverse function is practically infeasible.

The first public-key cryptosystem called RSA was published by R. L. Rivest, A. Shamir and L. Adleman in 1978 and is based on the factorization of large numbers [35]. Today it is still one of the most popular and most used asymmetric-key cryptosystems.

Typically, asymmetric-key schemes are very slow which makes them inconvenient for the encryption of big amounts of data. At the current state of technology one can assume that a block cipher algorithm is about 50 times and a stream cipher about 100 times faster than an asymmetric algorithm [25]. Nowadays, usually so-called hybrid crytosystems are used where a secret key is exchanged between the communicating partners via an asymmetric-key procedure and the communication itself is encrypted using this secret key and a symmetric-key system. Thereby the advantages of the asymmetric cryptosystem, that no secret has to be shared before the communication and the speed of symmetric cryptosystems are combined.

2.2. Quantum Key Distribution

The presented classical cryptosystems provide high security relying on the difficulty of calculating the inverse of one-way functions in reasonable amounts of time on classical computers. For asymmetric-key cryptography this security breaks if quantum properties are taken into account. In 1996 P. Shor published the now famous algorithm [36] which runs on a quantum computer and can compute the factorization of numbers in polynomial time. Quantum computers utilize quantum-mechanical phenomenas like superposition, interference and entanglement and are able to solve certain tasks more efficiently than any classical computers (e.g. prime factorization). In practice only the factorization of 15 has been done [37, 38] and there is still a long way to go for general quantum computers on a large scale. Nevertheless, the very opportunity makes it necessary to aim for other protocols.

Also from the quantum domain comes a solution for secure key distribution called quantum key distribution (QKD). The idea is, to securely exchange a key between two authenticated partners where the security is based on quantum mechanical laws, which are believed to hold instead of relying on assumptions on hardware or the unproven security of mathematical problems.

The general setup of QKD can be seen in figure 2.1: Alice and Bob are connected by a quantum channel over which Alice sends quantum states to Bob. Eve is allowed to interact with this channel without any restrictions (but still following the laws of physics). Using an authenticated classical channel from which Eve can copy all transmitted data but not alter it, they extract a common key from the data that was sent respectively received over the quantum channel via post-processing. With

this key, they can further communicate using a symmetric encryption scheme over the classical channel. Using Vernam's OTP, theoretically unconditional security can be achieved.

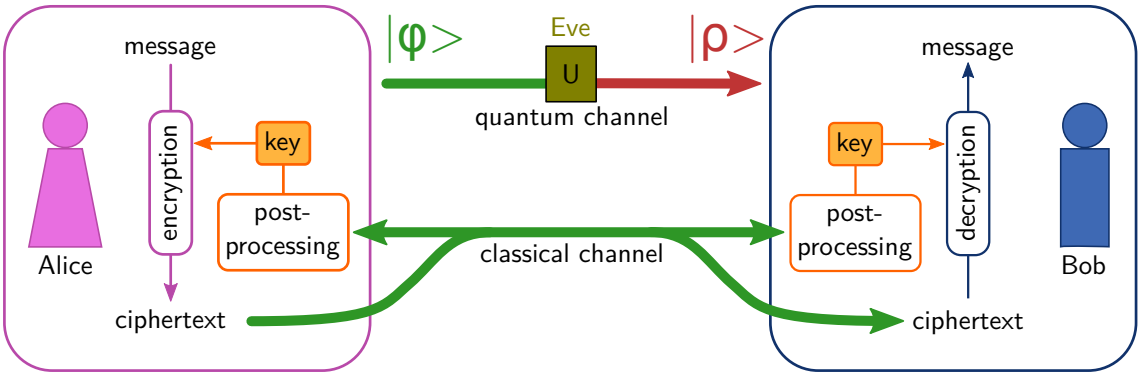


Figure 2.1.: Basic setting of QKD: Alice and Bob are linked by a quantum channel over which Alice sends quantum states $|\varphi\rangle$ with which Eve can interact without restrictions and make unitary measurements U. Bob measures the thereby altered states $|\rho\rangle$. An additional authorized classical channel is used for post-processing to generate the common key which is later used for symmetric encryption.

In this section I will introduce the quantum mechanical fundamentals needed for the understanding of QKD and present the BB84 protocol employed in this work. For a comprehensive overview consider [**Dusek2006**, 7, 39].

2.2.1. Fundamentals of quantum mechanics

The basic information unit of quantum information is the so-called qubit. In general any quantum mechanical two state system can be used for the realization of the qubit (e.g. spin 1/2-particle, polarization degree of light). In contrast to classical bits which only can be either 1 or 0, a qubit is a general quantum state $|\Psi\rangle$ (denoted in the so called "bracket" notation) in a two dimensional Hilbert space with the basis states $|0\rangle$ and $|1\rangle$ and can be described by:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.2}$$

where α and β are complex numbers which have to fulfill the normalization condition $|\alpha|^2 + |\beta|^2 = 1$.

For a two dimensional Hilbert space, three mutually unbiased (often also called "complementary") sets of basis vectors can be given. For the polarization degree of light these basis states correspond to the polarizations shown in table 2.3.

A measurement in quantum mechanics is described by hermitian operators A fulfilling equations of the form

$$A\,|a_i\rangle = a_i\,|a_i\rangle \tag{2.3}$$

Basis	Basis states	Polarization
B_X	$\|H\rangle$	Horizontally polarized
	$\|V\rangle$	Vertically polarized
B_Y	$\|P\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	Diagonally polarized
	$\|M\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	Anti-diagonally polarized
B_Z	$\|R\rangle = \frac{1}{\sqrt{2}}(\|H\rangle + \mathrm{i}\,\|V\rangle)$	Right-circularly polarized
	$\|L\rangle = \frac{1}{\sqrt{2}}(\|H\rangle - \mathrm{i}\,\|V\rangle)$	Left-circularly polarized

Table 2.3.: Bases and polarization states for QKD.

where $|a_i\rangle$ is called eigenstate and a_i eigenvalue of the operator A. It can be shown by the spectral theorem that for any hermitian operator A the set of eigenstates forms a complete basis spanning the Hilbert space. A measurement of an arbitrary state Ψ with the operator A will always give one of the possible outcomes a_i and the state will afterwards be $|a_i\rangle$. The probability p_i of getting a_i as measurement outcome when measuring a general state Ψ is given by:

$$p_i = |\langle a_i|\Psi\rangle|^2 \tag{2.4}$$

where $\langle a_i|$ is the hermitian conjugate of $|a_i\rangle$. For the example of table 2.3 when we assume we have the polarization states $|H\rangle$, $|V\rangle$, $|P\rangle$ and $|M\rangle$ and the two measurement basis B_X and B_Y, the measurement probabilities are given in table 2.4.

	$\|H\rangle$	$\|V\rangle$	$\|P\rangle$	$\|M\rangle$
$p_H(\|i\rangle)$	1	0	$\frac{1}{2}$	$\frac{1}{2}$
$p_V(\|i\rangle)$	0	1	$\frac{1}{2}$	$\frac{1}{2}$
$p_P(\|i\rangle)$	$\frac{1}{2}$	$\frac{1}{2}$	1	0
$p_M(\|i\rangle)$	$\frac{1}{2}$	$\frac{1}{2}$	0	1

Table 2.4.: Measurement outcome probabilities for measuring the states $|H\rangle$, $|V\rangle$, $|P\rangle$, $|M\rangle$ in the basis $B_X = \{|H\rangle, |V\rangle\}$ and $B_Y = \{|P\rangle, |M\rangle\}$.

From this example one can see that if a state is not measured in its eigenbasis, the measurement outcome is arbitrary which is one of the fundamental principles of QKD and the crucial property of mutually unbiased bases.

Another important quantum feature of the qubit is described by the *no-cloning theorem*, which states that it is impossible to copy an unknown quantum state [9]. This can be proved by assuming the existence of such a state copy machine performing an unitary transformation U (every quantum mechanic evolution in a closed system is unitary):

$$U|\Psi\rangle|\circ\rangle = |\Psi\rangle|\Psi\rangle \tag{2.5}$$

where $|\Psi\rangle = \alpha|\Psi_1\rangle + \beta|\Psi_2\rangle$ is the state that has to be copied and $|\circ\rangle$ is some initial

state. This leads to a contradiction:

$$\begin{aligned}|\Psi\rangle|\Psi\rangle &= \alpha^2|\Psi_1\rangle|\Psi_1\rangle + \alpha\beta|\Psi_1\rangle|\Psi_2\rangle + \beta\alpha|\Psi_2\rangle|\Psi_1\rangle + \beta^2|\Psi_2\rangle|\Psi_2\rangle \neq \\ &\neq \alpha|\Psi_1\rangle|\Psi_1\rangle + \beta|\Psi_2\rangle|\Psi_2\rangle = \\ &\overset{(2.5)}{=} \alpha U|\Psi_1\rangle|\circ\rangle + \beta U|\Psi_2\rangle|\circ\rangle = \\ &= U(\alpha|\Psi_1\rangle + \beta|\Psi_2\rangle)|\circ\rangle = \\ &= U|\Psi\rangle|\circ\rangle \end{aligned} \tag{2.6}$$

which shows that it is impossible to clone an unknown quantum states.

2.2.2. BB84

The first QKD protocol named BB84 was introduced by Bennett and Brassard in 1984 [8]. They describe the possibility of the public transmission of a random key between two parties using of qubits in two mutually unbiased bases by combining the no-cloning theorem and the indistinguishably of two orthogonal states in a basis that is diagonal to them (see table 2.4).

For BB84 to work Alice and Bob have to agree on a common reference frame for the definition of polarization states. They also have to agree on certain bit values for the polarizations (e.g. $|H\rangle$ and $|P\rangle$ are 0, $|V\rangle$ and $|M\rangle$ are 1). Alice randomly sends one of the polarization states $|H\rangle$, $|V\rangle$, $|P\rangle$ and $|M\rangle$ and Bob measures each received qubit randomly in either the B_X or the B_Y basis. The set of measurement results consisting of the basis choice and the measurement outcome is called *raw key*. Afterwards so-called *key sifting* is performed: Alice announces her preparation bases and Bob his measurement bases over the classical channel and both discard all raw key bits in which the preparation and measurement basis do not match as Bob's measurement outcome in these cases are random (see table 2.4). In an optimal scenario, not containing any losses or eavesdroppers, this *sifted key* is already the same for both parties and has half the length of the raw key.

An eavesdropper ("Eve") performing for example an intercept-resend attack (where she measures the polarization of the photons and sends the measurement outcome to Bob) can also only measure in random bases and therefore projects 50 % of the measurements onto the wrong basis introducing a so-called quantum bit error ratio (QBER) of 25 % which can be detected by Alice and Bob by comparing parts of the sifted key. An example of the protocol can be seen in figure 2.5. There exist more sophisticated attacks than the intercept-resend attack but it can be shown that even in the case of an optimal attack by an eavesdropper (bounded to the laws of quantum mechanics) a secure key can still be extracted for QBERs $\lesssim 11\,\%$ [7].

In a realistic environment also other things such as birefringence and depolarization effects can change the polarization state and therefore introduce errors. Final, classical post-processing, which consists of error correction [40, 41] and privacy amplification [42, 43] and is done by comparing part of the sifted key, removes all errors

Alice	Random bit	1	1	0	1	0	1	0	0
	Random basis	B_X	B_X	B_X	B_Y	B_X	B_X	B_Y	B_X
	Polarization state	$\|V\rangle$	$\|V\rangle$	$\|H\rangle$	$\|M\rangle$	$\|H\rangle$	$\|V\rangle$	$\|P\rangle$	$\|H\rangle$
Eve	Random basis	B_X	B_Y	B_X	B_X	B_Y	B_X	B_Y	B_Y
	Measured state	$\|V\rangle$	$\|M\rangle$	$\|H\rangle$	$\|V\rangle$	$\|P\rangle$	$\|V\rangle$	$\|P\rangle$	$\|M\rangle$
Bob	Random basis	B_X	B_Y	B_Y	B_Y	B_Y	B_Y	B_Y	B_X
	Measured state	$\|V\rangle$	$\|M\rangle$	$\|P\rangle$	$\|P\rangle$	$\|P\rangle$	$\|M\rangle$	$\|P\rangle$	$\|H\rangle$
	After sifting	1			0			0	0
	Error introduced by Eve	no			yes			no	no

Table 2.5.: Example of a BB84 key exchange with an eavesdropper performing an intercept-resend attack. Eve detects every qubit in a random state and sends a qubit according to her measurement outcome to Bob. Bob also measures in random bases and after sifting (Alice and Bob compare the basis used for preparing and measuring of the state over a classical channel and discard all measurement where they differ) the errors introduced by Eve can be seen.

and information that Eve may have gained at the cost of reduced key length.

2.2.3. QKD with attenuated laser pulses

For the security proof of the original BB84 protocol it is essential that single photons are used. As practical, highly efficient and reliable single photon sources are very difficult to implement, strongly attenuated laser pulses can be used for the generation of the polarization states requiring for a reconfiguration of the BB84 protocol. The number n of photons in a laser pulse is Poisson-distributed

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

where $P_\mu(n)$ describes the probability of a pulse with mean photon number per pulse μ to contain n photons. Multi-photon pulses are therefore unavoidable and can be used by Eve for the so-called *photon number splitting attack* (PNS) [44]. In this scenario Eve performs a so-called non-demolition measurement collapsing the pulse into a state with a fixed number of photons and still maintaining the polarization state. For multi-photon pulses she extracts part of the photons, stores them and sends the remaining ones to Bob. As soon as Alice publishes her preparation basis she measures the stored qubits and thereby gains information about the key without introducing any detectable errors. For optimizing her information gain Eve may block single-photon pulses and thereby reducing the transmission of the channel.

To tackle the problem of PNS, strongly attenuated laser pulses are used which makes multi-photon pulses very improbable but also reduces the total key rate sig-

nificantly as many states are so-called vacuum pulses not containing any photon. Knowing μ and thereby the fraction of multi-photon pulses as well as how many single-photon pulses might have been blocked from the transmission coefficient, Eve's knowledge can thereby be completely removed from the key [45].

In 2003 the so-called *decoy protocol* was proposed by Hwang et. al. [46] for preventing the PNS attack by sending additional random "decoy pulses" which are slightly weaker on average than the signal pulses. It is important that the Poisson-distributions of the decoy pulses and the signal pulses still overlap, such that Eve cannot distinguish them. Eve has to handle both in the same way and by evaluating the transmission of decoy and signal pulses separately, an attack can be detected. The protocol allows for a higher μ and higher key rates as the amount of information available to Eve can be determined more precisely.

2.2.4. Preparation quality

For realistic sender devices an important security indicator is the *preparation quality* q which indicates how well Alice prepares her BB84 states in the sense of mutually unbiased bases and enters the security proofs. It is defined as [47, 48]:

$$q = -\log_2 \max |\langle \Psi_x | \Psi_z \rangle|^2 \tag{2.8}$$

where Ψ_x and Ψ_z are the states, prepared in the diagonal bases $B_X = \{|0\rangle, |1\rangle\}$ and $B_Y = \{|P\rangle, |M\rangle\}$ with $|P/M\rangle := 1/\sqrt{2}\,(|0\rangle \pm |1\rangle)$. For $q = 1$ ideal states (belonging to mutually unbiased bases) would be emitted by Alice, values $q < 1$ reduce the secret key that can be extracted from the raw key.

2.2.5. Side-channels

Above we have considered the perfect case of BB84 QKD which guarantees the theoretical security of the distributed key. Real devices always differ from a perfect device which makes them vulnerable to so-called side-channel attacks. These attacks do not target the cryptographic concept itself but the physical implementation of it. In QKD this means, that an attacker can gain knowledge about the key without being detected.

Identifying possible attacks is a whole research field ("Quantum hacking") and lot of possible vulnerabilities have been found. Here I will only explain some relevant side-channels that play a major role in our implementation.

The possible side-channels can be divided into the ones on the sender side and the ones of the receiver side. Typically, the sender is less vulnerable to attacks, as one assumes that Alice can prepare the quantum signals in an environment that is not accessible to an attacker. Errors in the polarization of the prepared states can relatively easy be taken into account in the security proofs (see subsection 2.2.4).

Furthermore, it is important that the pulses only differ in the polarization degree of freedom and all other properties are indistinguishable as Eve could gain information about the states by measuring them without changing the polarization (like the photon number per pulse in the PNS attack). For a QKD implementation using photons as qubits, three possible quantities can differ, leading to side-channels: the wavelength, temporal degree of freedom of the pulses and the spatial mode. An indicator for the vulnerability can be given by the overlap of the corresponding quantity between different channels. The smaller the overlap, the more information an attacker can gain by exploiting the corresponding side-channel.

In contrast to the sender the complexity at the receiver side is way higher as one has to allow Eve to send in any additional signal. This makes it way harder to protect the receiver setup from attacks. An example exploiting this possibility is the so-called detector blinding attack [49]. Another possible side channel was investigated by our group [50] and concerns the detection probability for each state which can change with the angle of the input beam.

2.3. State Tomography

In this section methods required for the description, preparation and measurement of polarization states are introduced.

2.3.1. Stokes and Mueller formalism

For the description of the polarization state of light one can use the *Stokes vector* which is defined as [51]:

$$\vec{S}_N = \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} I \\ I_H - I_V \\ I_P - I_M \\ I_R - I_L \end{pmatrix} \tag{2.9}$$

where I is the total intensity and I_i the intensity of the i-th portion of the light.

The advantage of the Stokes formalism is that the polarization state is represented by a convenient vector whose components can be determined via measurements of intensities.

In most scenarios it is more comfortable to work with the *intensity normalized Stokes vector*:

$$\vec{S}_N = \begin{pmatrix} 1 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1 \\ \frac{I_H - I_V}{I_H + I_V} \\ \frac{I_P - I_M}{I_P + I_M} \\ \frac{I_R - I_L}{I_R + I_L} \end{pmatrix} \tag{2.10}$$

The polarizations H, V, P, M, R and L can thereby be described by:

$$H = \begin{pmatrix} 1 \\ +1 \\ 0 \\ 0 \end{pmatrix} \qquad P = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \qquad R = \begin{pmatrix} 1 \\ 0 \\ +1 \\ 0 \end{pmatrix}$$

$$V = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} \qquad M = \begin{pmatrix} 1 \\ 0 \\ 0 \\ +1 \end{pmatrix} \qquad L = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

The intensity normalized polarization states can be visualized using the *Poincaré-sphere* (see figure 2.2). Fully polarized states lie on the surface whereas partially polarized states lie inside the Poincaré sphere. This property can be qualified with the *degree of polarization* Π (DOP) which corresponds to the length of the intensity normalized Stokes vector and calculates as follows:

$$\Pi = \sqrt{S_1^2 + S_2^2 + S_3^2} \tag{2.11}$$

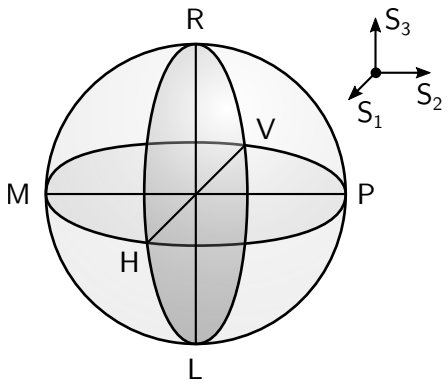


Figure 2.2.: Poincaré sphere representation of polarization states.

The effect of polarization manipulating components onto an initial polarization state S_i can be described using

$$\vec{S}_o = M \cdot \vec{S}_i \tag{2.12}$$

where M is a 4×4 *Mueller matrix* [52].

First we consider an ideal linear polarizer, transmitting only polarization compo-

nents having an angle θ with the horizontal axis of the system [51]:

$$M_{\text{polarizer}} = \frac{1}{2}\begin{pmatrix} 1 & \cos(2\theta) & \sin(2\theta) & 0 \\ \cos(2\theta) & \cos^2(2\theta) & \cos(2\theta)\sin(2\theta) & 0 \\ \sin(2\theta) & \cos(2\theta)\sin(2\theta) & \sin^2(2\theta) & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{2.13}$$

For a retarder plate having orthogonal "slow" and "fast" axes with an optical phase difference of δ and an angle of θ between the horizontal axis of the system and the fast axis, the Mueller matrix is given by [51]:

$$M_\delta = \\ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\delta)\sin^2(2\theta) + \cos^2(2\theta) & (1-\cos(\delta))\cos(2\theta)\sin(2\theta) & \sin(2\theta)\sin(\delta) \\ 0 & (1-\cos(\delta))\cos(2\theta)\sin(2\theta) & \cos(\delta)\cos^2(2\theta) + \sin^2(2\theta) & -\sin(\delta)\cos(2\theta) \\ 0 & -\sin(\delta)\sin(2\theta) & \sin(\delta)\cos(2\theta) & \cos(\delta) \end{pmatrix} \tag{2.14}$$

For a so-called quarter-wave plate ($\delta = \pi/2$) and a half-wave plate ($\delta = \pi$) this reduces to:

$$M_{\lambda/4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\theta) & \cos(2\theta)\sin(2\theta) & \sin(2\theta) \\ 0 & \cos(2\theta)\sin(2\theta) & \sin^2(2\theta) & -\cos(2\theta) \\ 0 & -\sin(2\theta) & \cos(2\theta) & 0 \end{pmatrix} \tag{2.15}$$

$$M_{\lambda/2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\theta) - \sin^2(2\theta) & 2\cos(2\theta)\sin(2\theta) & 0 \\ 0 & 2\cos(2\theta)\sin(2\theta) & \sin^2(2\theta) - \cos^2(2\theta) & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{2.16}$$

2.3.2. QBER in the Stokes formalism

In general the quantum bit error ratio is defined as the fraction of wrong bits N_{wrong} to the total number of received bits N_{total}:

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{N_{wrong}}{N_{total}} \tag{2.17}$$

The QBER of the four BB84 states can also be directly calculated from the components of the Stokes vector, as the intensity is proportional to the photon number [53]:

$$QBER_H = \frac{1 - S_1}{2} \tag{2.18}$$

$$QBER_V = \frac{1 + S_1}{2} \tag{2.19}$$

$$QBER_P = \frac{1 - S_2}{2} \tag{2.20}$$

$$QBER_M = \frac{1 + S_2}{2} \tag{2.21}$$

2.3.3. Polarization preparation

For the preparation of arbitrary polarization states a setup consisting of a firm polarizer followed by a motorized half-wave plate and a motorized quarter-wave plate can be used (see figure 2.3). The advantage of using a polarizer with constant angle at the beginning is, that the preparation unit is thereby immune to an elliptically polarized input beam which would modulate the intensity and thus require compensation [54].

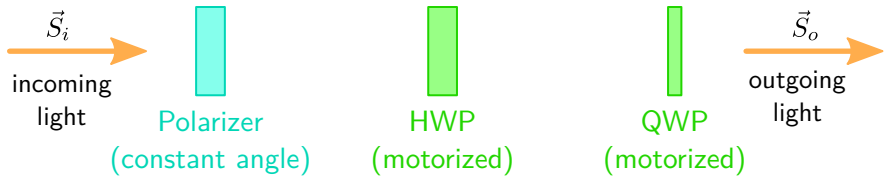


Figure 2.3.: Setup for the generation of arbitrary polarization states using a polarizer with a constant angle and a motorized HWP and QWP.

Using the Stokes and Mueller formalism described in subsection 2.3.1, one can calculate the angles of the HWP and QWP needed for a certain output state. In table 2.6 such angles are given for the HWP and QWP for the polarization preparation of H, V, P, M, R and L when the fixed polarizer is set to horizontal polarization.

Output polarization $\vec{S}_o$	H	V	P	M	R	L
Angle HWP	0°	45°	22.5°	−22.5°	−22.5°	22.5°
Angle QWP	90°	0°	−45°	−135°	−90°	−90°

Table 2.6.: Angles of the HWP and QWP from the horizontal axis of the system used for the preparation of certain polarization states with horizontal polarization at the input.

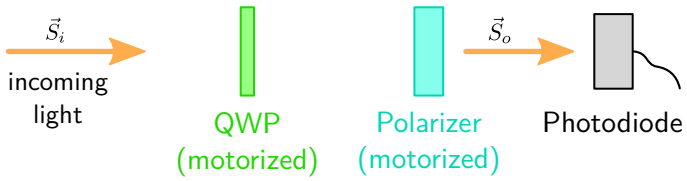


Figure 2.4.: Setup for the measurement of the Stokes parameters.

2.3.4. Polarization analysis

For the measurement of the polarization state (also referred to as state tomography) a motorized quarter-wave plate and a motorized polarizer have been used (see figure 2.4) with the angles shown in table 2.7. With the measured intensities of the six polarization states the Stokes vector can be calculated using equation (2.10).

$\vec{S}_o$	H	V	P	M	R	L
Angle QWP	0°	0°	22.5°	22.5°	0°	0°
Angle polarizer	0°	−90°	22.5°	−22.5°	−22.5°	22.5°

Table 2.7.: Angles of the QWP and polarizer from the horizontal axis of the system used for analysis of the polarization state.

3. The Hand-Held QKD Experiment

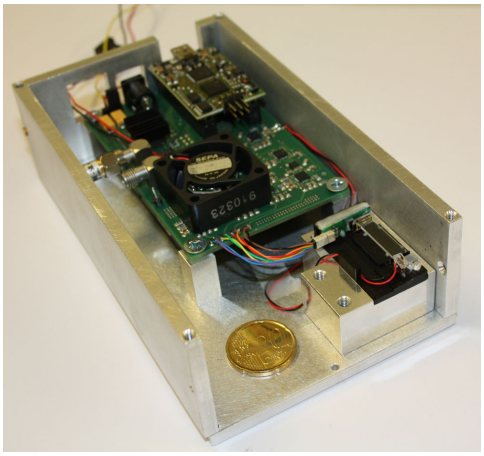
In this chapter the state of the QKD experiment of our group at the beginning of this thesis will be described. The first section illustrates the hand-held QKD transmitter developed by G. Mélen. In the second section I will describe the receiver module briefly that has mainly been developed by T. Vogl.

A more precise description is given in the thesis of G. Mélen [17] and T. Vogl [53]. An in depth analysis of the device with several improvements is given in the work of P. Freiwang [55] and a hand-held key exchange is analyzed in detail in the thesis of J. Luhn [56].

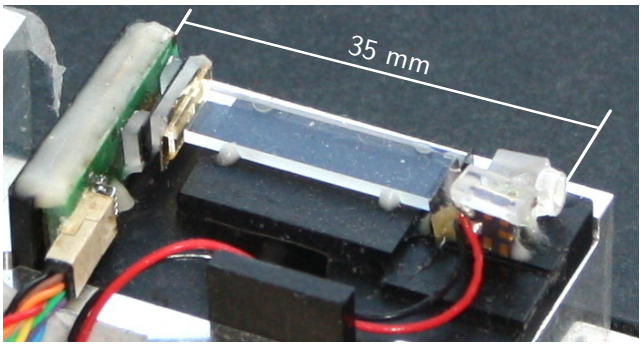
3.1. QKD Transmitter

The goal of G. Melen's work was the development of an integrable QKD sender for short-range free-space QKD scenarios e.g. a transaction using an ATM. Therefore, we focused onto the miniaturization of the optics.

In this section the integrated optics and the electronics of this module will be described. Pictures of the whole module and the optics can be seen in figure 3.1.



(a) Complete hand-held sender module including the electronics and the micro optics. (Taken from [53])



(b) Detailed view of the micro optics on the micro-optical bench. (Taken from [56])

Figure 3.1.: Pictures of the hand-held sender module developed by G. Mélen.

3.1.1. Optics

At first the optical part of the Alice module will be described. A sketch can be seen in figure 3.2. As already mentioned, the BB84 protocol is implemented by generating the four linear polarized states $|H\rangle$, $|V\rangle$, $|P\rangle$ and $|M\rangle$ with four independent light sources. In our module we use an array of vertical-cavity surface-emitting lasers ("VCSELs") with a pitch of 250 nm and a wavelength of 850 nm. The light is focused using a micro-lens array, polarized by wire-grid polarizers (fabricated by G. Mélen) and coupled into a waveguide circuit, which spatially overlaps the four inputs. The output beam is overlapped with a visible beacon laser (680 nm) used for aiming, beam tracking and clock synchronization with a dichroic beamsplitter and collimated with a lens. On the following pages I will present the different parts more precisely.

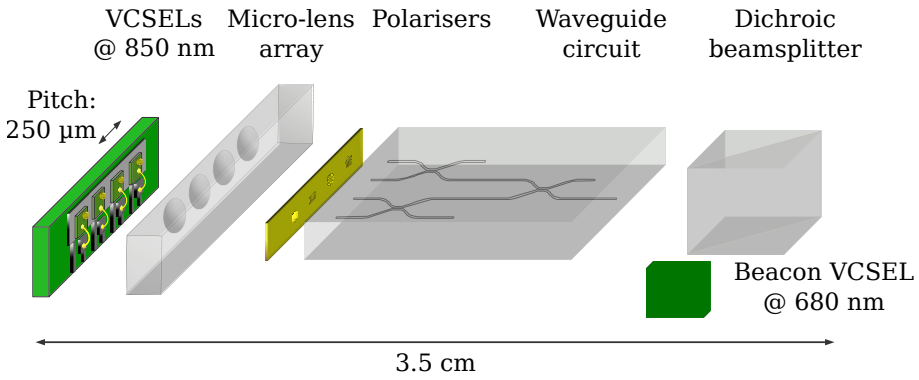


Figure 3.2.: Schematics of the sender module. An VCSEL array together with vour wirde grid polarizers generates the four polarization states which are coupled into an optical waveguide circuit for the spatial overlap. The resulting QKD signal beam is overlapped with a beacon laser used for beam tracking, clock synchronization and aiming purposes. (Taken from [57])

VCSEL array

Vertical cavity surface emmitting lasers (VCSELs) have their name from the property of emitting light perpendicular to their surface (contrary to edge-emitting lasers). They are built up of a cavity consisting of electrically conductive layer stacks forming the laser mirrors which provide optical feedback and layers with amplifying material inside. The mirrors are realized as distributed Bragg reflectors consisting of typically more than 20 alternating semiconductor layers pairs of high and low refractive index with a thickness of one quarter of the material wavelength. The electrical contact can be done using ohmic contacts on the surface and back side of the substrate and the specific structure confines the current to the center of

the inner cavity. By reducing the diameter of the active region to a few micrometers single transverse mode operation can be obtained. The most important advantages of VCSELs is the low threshold current of less than 1 mA and the high power conversion efficiency larger than 50 %, which both lead to low power consumption and dissipation. In addition they provide excellent digital modulation behavior and circular beam profiles with small divergence angles. Nowadays, VCSELs are one of the most used semiconductor laser sources and are they key components of computer mouses and optical data transmission devices, reaching a production rate of over 100 millions lasers per year in 2013 [58, 59].

In our setup we use an array of single mode VCSELs (VI Systems V25A-850C12SM) featuring data rates up to 28 Gbit s^{-1}. The benefit of using an VCSEL array is the very well defined pitch. Unfortunately, the analysis of the spectra (see figure 3.3) shows, that especially channel 3 and 4 do not overlap due to the very narrow spectral width of the lasers, which causes a significant side channel of the device (see subsection 2.2.5).

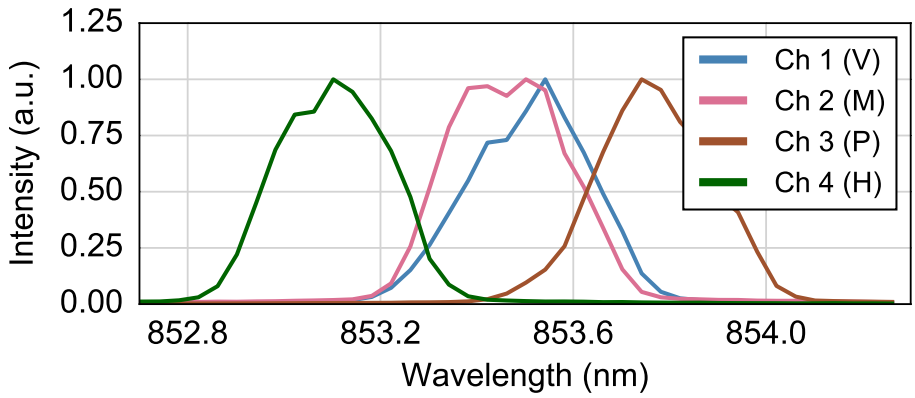


Figure 3.3.: Spectrum analysis of the four VCSELs. The spectra of channel 4 and 3 used for the horizontal and vertical polarizations do not overlap. (Taken from [60])

Polarizers

As already mentioned above, an array of four wire-grid polarizers is used to define the polarization of the light. They consist of a layer of gold deposited on a glass substrate where the grating was made by Focused Ion Beam milling (FIB) [61]. The polarizers reach an extinction ratio between 1150 and 1800 and a transmission of 9 % at a wavelength of 850 nm [17]. Furthermore, the orientation for each of the polarizers has been optimized to precompensate for polarization rotations due to birefringence of the waveguide circuit.

Unfortunately the setup of the FIB setup only allows for a rotational resolution of about 2° whereby the prepared angles differ from the calculated optimal ones as one can see in table 3.1.

Input port	1 (H')	2 (P')	3 (M')	4 (V')
Calculated optimal input angles	−1.0°	−43.9°	39.9°	86.8°
Prepared angles	−1.0°	−50.1°	44.6°	89°

Table 3.1.: Angles of the polarizers of the array. The calculated optimal input states should compensate for polarization-dependent effects of the waveguide circuit in a way that optimal BB84 states are obtained at the output of Alice. (Data taken from [17])

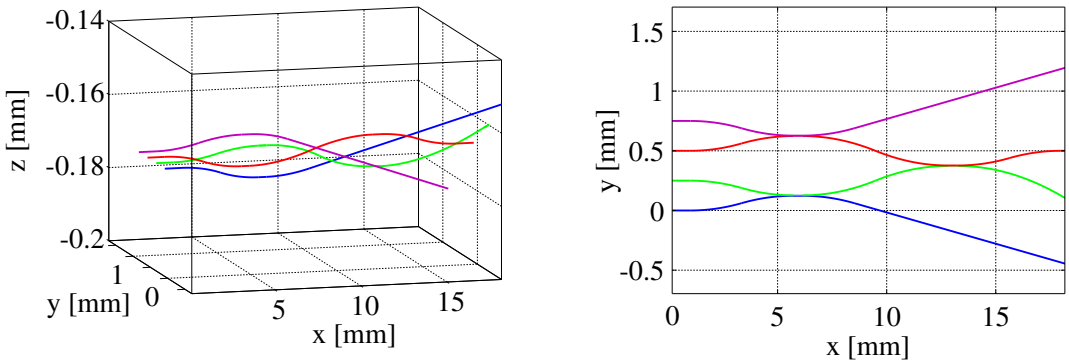
Waveguide chip

As the four BB84 states come from different light sources they do not spatially overlap and have distinct transverse modes, which would be potential side channels (see subsection 2.2.5). To overcome these problems a single-mode waveguide circuit has been written into a glass substrate by the group of Prof. Dr. R. Osellame at the Politecnico di Milano in Italy via femtosecond laser writing [62–65] overlapping the four inputs to one output that can be used further (the waveguide chip is called "Alice 1.0").

The principle of this method works as follows. Ultrashort laser pulses (femtosecond regime) are tightly focused to a certain position of the glass substrate. The deposition of energy in the material by a combination of multiphoton absorption and other effects entails high temperatures and pressures which lead to a densification of the material and thereby an increase of the refractive index in a small portion of the substrate [66, 67]. By using a transverse setup where the laser irradiates the substrate from above and the laser focus can be moved inside the glass substrate, optical waveguides and waveguide circuits can be written into the substrate in a three-dimensional configuration. This setup also leads to an elliptical cross section of the waveguides [68] as the waveguide size perpendicular to the beam propagation direction is approximately defined by the beam focal diameter ($2w_0$) and along the propagation direction the size scales with the confocal parameter ($b = 2\pi w_0^2/\lambda$) [63]. This effect can be reduced by the use of spatial and temporal beam-shaping techniques [63, 69]. A second effect comes from differences of the optical density along the longitudinal and transverse direction of the laser pulse and introduces stress birefringence leading to different refractive indices for the TE and TM polarized waves.

By bringing two waveguides in the glass substrate close together, directional couplers can be formed (corresponding to a beamsplitter in bulk optics). The splitting ratios directly depend on the distance of the two waveguides, the interaction length and the refractive index of the waveguides. Due to the fact, that the waveguides have an elliptical cross section the splitting ratios in planar couplers are different for H and V polarized light and result in rotations of the P and M polarizations [17]. To tackle this problem the waveguides can be written in a three-dimensional configuration into the glass substrate as demonstrated in [70].

The Alice 1.0 waveguide chip fabricated for our experiment consists of a 18 mm × 5.5 mm × 1.1 mm glass substrate (Corning® EAGLE$^{2000™}$) into which a waveguide circuit, consisting of four waveguides with a pitch of 250 µm at the inputs and three directional couplers with a coupling ratio of 50 %, was written by the method described above. In figure 3.4 the design of the waveguide circuit is illustrated. This waveguide circuit allows for the spatial overlap of the four VCSELs to one output (red in the figure) which can be used further. The other three outputs are blocked. In the thesis of P. Freiwang [55] the blockers are discussed in detail. Two additional straight waveguides were written close to the edges of the waveguide chip at the same depth and with the same physical properties as the inputs of the waveguide circuit to assist the coupling procedure.



(a) 3d view **(b)** Top view

Figure 3.4.: Overview of the Alice 1.0 waveguide circuit used for the overlapping of four inputs with a pitch of 250 µm to an output that can be used as output (red) for the BB84 protocol via the three directional couplers which act as 50:50 beamsplitters. The other three outputs are blocked. (Taken from [17])

As already mentioned above, the waveguides do not maintain the polarization due to birefringence of about $\Delta n = 6.9 \times 10^{-5}$ between the horizontal and vertical axis [17]. Matching the phase shift for four waveguides with the mentioned methods is nearly impossible, also due to additional birefringence induced by stress at the coupler areas which leads to a non uniform behavior of the four waveguides. By analyzing the rotation of the input polarization, this behavior can be compensated by a individual correction of the input states which was done in [71] for the Alice 1.0 waveguide chip.

3.1.2. Electronics

The main purpose of the driving electronics is to provide a reliable current source for the VCSELs. Furthermore, a full control of the pulse parameters has to be

warranted to fulfill the requirements that come with QKD e.g. the precise settings of the mean photon number per pulse μ as well as the temporal overlap of the optical pulses. In order to allow a narrow time filtering and therefore a high signal-to-noise ratio the pulse length has to be in the sub-nanoseconds regime.

In figure 3.5 the schematic of the electronics can be seen (for the detailed eagle layout see figure A.1 on page 61).

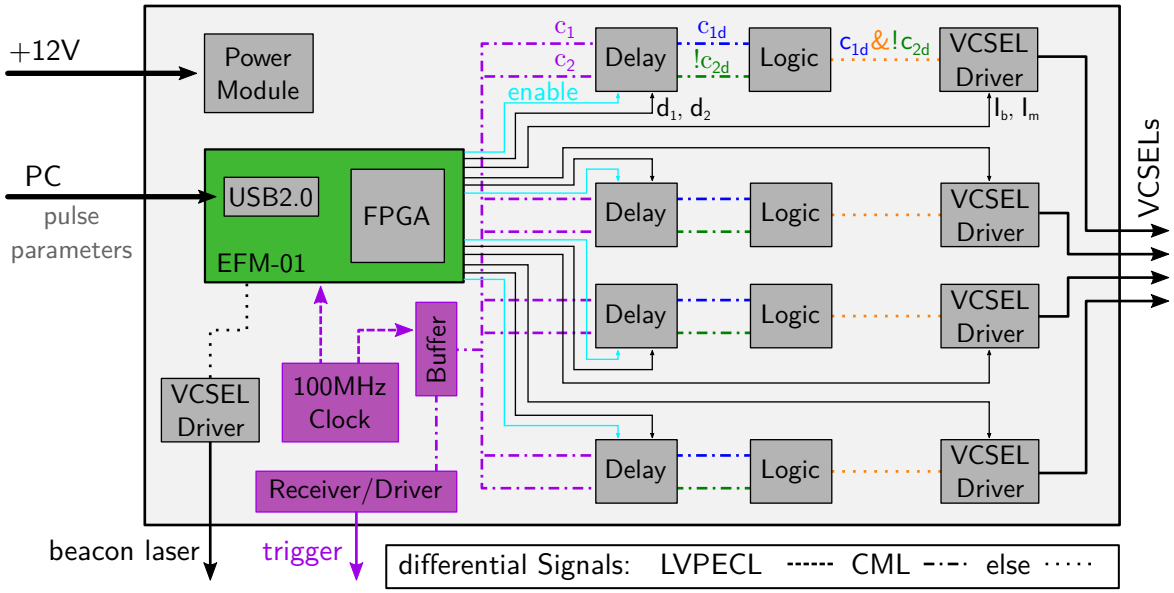


Figure 3.5.: Schematics of the driving electronics of the hand-held sender module. The module is managed by a FPGA breakout board (EFM-01) that controls the four pulse generation channels consisting of a delay IC (delay of channel1 and channel2 independently and enable), a logic AND gate and the VCSEL driver (pulse parameters I_{bias} and I_{mod}). A 100 MHz clock directly feeds the FPGA and over two buffers the delay chips and a transceiver that can be used to externally synchronize to the Alice module. The VCSEL driver for the beacon laser is directly modulated by the FPGA.

The control of the board is done by a Xilinx Spartan-3E FPGA, which is embedded on a ready-to-use breakout board (CESYS EFM-01[a]). The module also contains an USB2.0 controller (Cypress CY7C68013A), enabling for a fast interface between the sender module and a computer.

The pulse generation is implemented in the following way (schematic in figure 3.6a):
A 100 MHz clock signal (Crystek CCPD-033-50-100[b]) is transferred to the FPGA and two buffers (Micrel SY58603U[c]). The two buffers provide the clock signal

[a] https://www.cesys.com/fileadmin/user_upload/documents/EFM01/ug110-efm01.pdf
[b] http://www.crystek.com/crystal/spec-sheets/clock/CCPD-033.pdf
[c] http://ww1.microchip.com/downloads/en/DeviceDoc/sy58603-5_eb.pdf

for four dual-channel programmable delays (Micrel SY89297U[d]) and an ECL Receiver/Driver (Micrel SY100EP16V[e]). The ECL Receiver/Driver can be used for external synchronization purposes. The delay chips can shift two input signals independently in 5 ps steps over a delay range of 5 ns. The delay can be programmed using the FPGA over a 3-pin serial interface by setting two 10 bit latches. The *enable pin* of the delay ICs is controlled by the FPGA and used to switch on the chosen VCSELs. During the key exchange this function is used to select the state which should be sent. One of the outputs is inverted by exchanging the positive and negative wire of the CML signal and the two output signals are applied to an universal logic gate (Micrel SY55851[f]). The logic gate is configured as an AND-gate whereby a short electrical pulse is generated (see figure 3.6a). This short pulse is routed to the modulation input of a VCSEL driver (Texas Instruments ONET4291VA[g]) to trigger the modulation. The VCSEL driver can be controlled by the FPGA via three eight bit registers using a two-wire digital interface. General settings are stored in the first register. The bias and modulation current of the VCSEL are set by the other two registers. In open loop configuration, where no photodiode is attached for the control of the output, the bias current I_{bias} and modulation current I_{mod} calculate as follows:

$$I_{bias} = 100\,\mu\text{A} + 47\,\mu\text{A} \cdot r_{bias} \tag{3.1}$$

$$I_{mod} = 100\,\mu\text{A} + s_{mod} \cdot r_{mod} \tag{3.2}$$

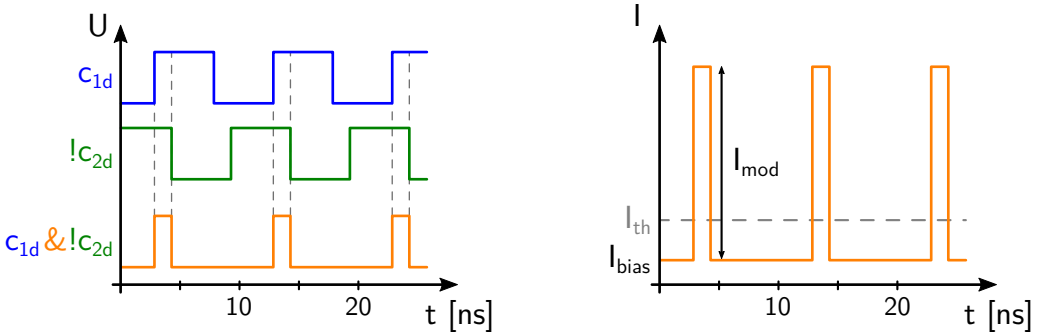
where $s_{mod} \in \{51\,\mu\text{A}, 68\,\mu\text{A}\}$ and r_{bias}, r_{mod} are the 8 bit values from the registers controlled by the FPGA. One can switch between two different modulation current modes via the first register for either a finer control (stepsize of 51 µA) or a bigger range (stepsize of 68 µA). The modulation output is AC coupled and combined with the bias signal over a bias-tee resulting in a pulse as shown in figure 3.6b.

An additional beacon laser is controlled by a further laser driver which is directly modulated by the FPGA. The beacon laser is used for aiming purposes and beam tracking at the receiver side. Furthermore it is used for clock synchronization.

The powering of the circuit is done by a 12 V power supply, which is converted by a high accurate switching power module capable of 5 A throughput (Texas Instruments LMZ22005[h]) to the 3.3 V required for all the ICs. In table 3.2 an overview of the power consumption of the electronics is given. Measurements under operation condition show a consumption of (6.1 ± 0.4) W which is slightly higher, which can partially be explained by the fact that not all values in the data sheets are given under load and further losses.

One can see, that especially the delay chips are very power consuming and thereby

[d] http://ww1.microchip.com/downloads/en/DeviceDoc/sy89297u.pdf
[e] http://ww1.microchip.com/downloads/en/DeviceDoc/sy100ep16v.pdf
[f] http://ww1.microchip.com/downloads/en/DeviceDoc/sy55851-51a.pdf
[g] http://www.ti.com/lit/ds/symlink/onet4291va.pdf
[h] http://www.ti.com/lit/ds/snvs686j/snvs686j.pdf



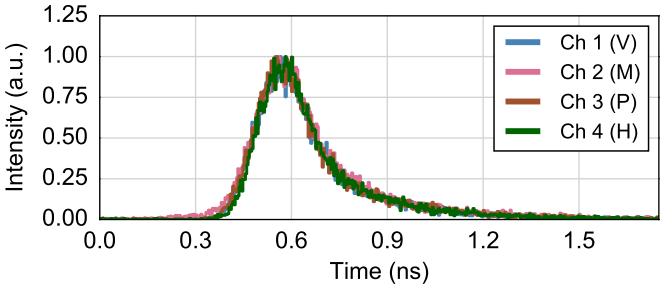
(a) Generation of short electrical pulses using a delay line and an AND-gate.

(b) Output of the VCSEL driver.

Figure 3.6.: Sketch of the pulse shapes of the electrical signals after the delay chip and the VCSEL driver. (Adapted from [17])

produce a lot of heat. The delay chips are specified for a maximal temperature of 80 °C, however, we measured temperatures of over 90 °C some seconds after switching on the device. To overcome the heat problem, the thermal pad of the delay IC packaging (quad-flat no-leads, QFN) is connected to the ground plane and the backside of the PCB where passive cooling elements are attached. From the inner ground plane the heat can dissipate over additional thermal vias placed next to the devices and distributed over the area of the circuit board. Theses thermal vias have a large surface area and are not plugged whereby the air can flow through them and the heat can be dissipated.

Figure 3.7 shows the pulse shape with a FWHM of 200 ps and the good temporal overlap of the very short pulses that can be derived with the electronics described above and the parameters given in the table next to the figure.



	Ch1	Ch2	Ch3	Ch4
d_a	29	40	89	82
d_b	89	137	133	110
b	2	6	1	4
m	194	248	155	242

Figure 3.7.: Temporal pulse shape measured using an oscilloscope and a fast Avalanche Photodiode with the parameters for the delay chips (delay channel a & b) and the laserdrivers (bias current b and modulation current m) given in the table. (Taken from [60])

Device	typ. input current @ 3.3 V [mA]	ICs on PCB [#]	Power [W]
CCPD-033 (clock oscillator)	55	1	0.18
SY58603 (CML Buffer)	39*	2	0.26
SY100EP16V (receiver/driver)	22	1	0.07
SY89297 (dual channel delay)	195	4	2.57
SY55851 (universal logic gate)	40*	4	0.53
ONET4291VA (VCSEL driver)	40	5	0.66
		estimated power consumption:	4.3 W
		including efficiency of power module ($\sim 90\,\%$):	4.8 W

Table 3.2.: Rough estimation of the power consumption of the electronics from the information given in the data sheets. For the devices where the currents are marked with * the numbers are not given under load which is one of the reasons why the real consumption is higher.

3.2. QKD Receiver

In this section I will present the stationary QKD receiver ("Bob"), consisting of a standard BB84 polarization analysis unit (PAU) and additional features allowing for hand held operation. For an overview see figure 3.8.

3.2.1. BB84 polarization analysis unit

The central element of the receiver is a polarization analysis unit (PAU), which is made up as follows: a passive, true random basis choice between the B_X basis and the B_Y basis is done by a 50:50 beam splitter (BS). For the B_X basis, a following polarizing beam splitter (PBS) transmits H-polarized light but reflects V-polarized light. In the other arm of the beam splitter a half wave plate (HWP) with an angle of 22.5° between the optical axis of the HWP and the vertical axis rotates the polarization by 45° (the so called "Hadamard-transformation"). By this the B_Y basis can be measured by adding a PBS similarly as for the B_X basis.

The four outputs of the PBS are coupled into multi-mode optical fibers attached to an avalanche photodiode array (APDs, Perkin Elmer DTS SPCM-AQ4C[i]) and the electrical pulses are sent to a timestamp unit which records the signals.

The functionality in the example of a H polarized photon looks like follows: with a probability of 50 % it gets deflected at the BS into the B_X analyzing path, where it is transmitted at the PBS and gets coupled into detector 1. If it is transmitted at the BS it becomes rotated by the HWP into a $|P\rangle$ state and then deflected or transmitted by the PBS with equal probability. For a photon in state $|P\rangle$ it is the

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

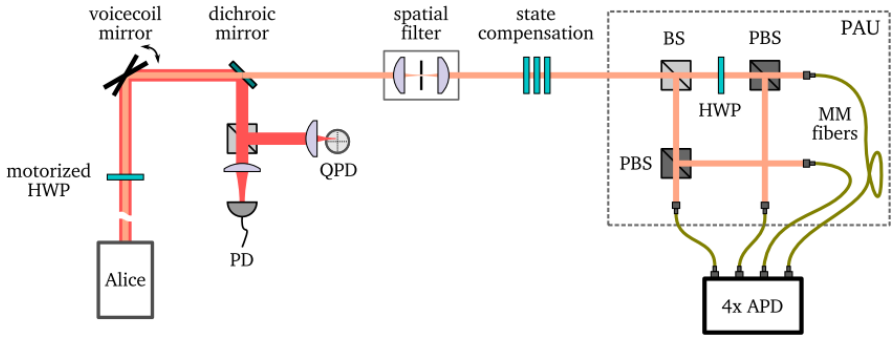


Figure 3.8.: Overview of the QKD receiver consisting of a polarization analysis unit (PAU), a voicecoil mirror enabling beam tracking together with the quadrant photo diode (QPD), a fast photodiode (PD) for synchronization. A motorized half-wave plate allows for the alignment of the reference frames. The spatial filter restricts the acceptance angle disabling spatial side channel attacks. Three wave plates placed in front of the PAU are used for the phase compensation of the polarization states. Silicon avalanche photo diodes (APDs) enable low noise single photon detection. (Taken from [56])

other way round. If it gets deflected into the B_X path, it will get transmitted or deflected by the PBS with 50 %. In the case where it is transmitted at the BS it will be converted into a photon in state $|V\rangle$ and then deflected by the PBS to detector 2. For the case of a photon in state $|V\rangle$ or $|M\rangle$ the procedure is analogue.

3.2.2. Additional features

Some additional elements have been added to the setup to enable hand-held QKD and to close some essential side channels and will be described here.

State compensation

For the polarization analysis unit the states have to be the four BB84 ones. As the photon polarizations are not necessarily in the respective basis a phase compensation setup is used to rotate them back to the H/V-P/M plane of the Poincaré sphere in front of the PAU.

The rotation is implemented by two quarter waveplates and one half waveplate in front of the PAU. With this three elements any unitary operation can be applied to the polarization state of the photons. The three waveplates are rotated in a way that the QBER is minimized.

Alice does not produce perfect BB84 states, meaning that they are not pairwise orthogonal and have a degree of polarization (DOP) < 1. Furthermore, the optical elements in Bob are not perfectly polarization independent and thereby deform the states in a non-uniform way. As only one unitary operation acting on all four states

can be applied the state compensation cannot guarantee that the receiver set up analyses perfect BB84 states, causing additional QBER.

Side-channels

As already mentioned in subsection 2.2.5 the spatial mode dependency of the detectors can lead to a significant side channel attack. To tackle this problem the angle of the incoming beam is restricted to $\pm 0.08°$ which corresponds to a window of 2.7 mm diameter at a distance of 1 m. The spatial mode filter is set up by a pinhole with a diameter of 30 µm placed between two lenses with a focal length of 11 mm.

Hand-held QKD

For a person holding the hand-held sender device it is not possible to aim well enough through this spatial filter to generate a key. Therefore, additional beam tracking is essential. For this the beacon laser is used which is separated from the signal beam using a dichroic mirror and part of the beacon light is focused onto a quadrant photo diode (QPD). This gives the reference signal for an electrically steerable voicecoil mirror which can compensate for an angle misalignment up to $\pm 3°$ from its zero position in both axes.

An user of the sender unit does not only jitter, but also may rotate the device around the optical axis. The receiver compensates for this rotation in a way that Alice and Bob have the same reference frame orientation (such that "horizontal", "vertical", "diagonal" and "anti-diagonal" have the same meaning in Alice and Bob). A misalignment would lead to a higher QBER and thus to reduced key rates. The error introduced by a rotation misalignment is given by:

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

with Θ being the angle between the two reference frames.

As the rotation cannot be corrected by the mirror control a half-wave plate controlled by a stepper motor is placed at the entrance of the receiver which adapts Bobs reference frame to the one of Alice. For the determination of the orientation of Alice, a smartphone is placed on the Alice module during key exchange. A Android app reads out the smartphones inertial measurement unit (typically consisting of an accelerometer and a gyroscope) and transmits these values via Wi-Fi with a repetition rate of 10 Hz to Bobs computer, which rotates the half-wave plate accordingly.

For aiming purposes two pinholes with a distance of about 15 cm have been placed in front of the voicecoil mirror. The user has to aim through both of them. An additional audio feedback is given to aid the holder of the sender unit at the aiming process. The deeper the pitch the better the coupling. A sharp sound (square wave) indicates a loss of coupling [56].

Using the optical and acoustic signals also an untrained user is capable of operating the hand-held sender at sufficient high key rates of several kbit s^{-1}.

Clock synchronization

Alice and Bob need to identify the received pulse with the corresponding sent pulse. Therefore, a clock synchronization is essential, as two separate free running clocks (one in the sender and one in the receiver) would run out of synchronization after short time. As described in subsection 3.1.2 the beacon laser is modulated with the clock of the sender. At the receiver a part of the beacon signal is coupled to an amplified photodiode feeding a clock recovery chip and a FPGA which reduces this signal to a 100 kHz signal that is inputted to the same timestamp unit as the QKD signal pulses.

With this scheme sufficient clock synchronization can be achieved but also lacks some functionality. One thing that could be improved is the behavior at beacon signal losses which happens quite often for hand-held scenarios. So far a relative complex post processing described in J. Luhns thesis compensates for this. Also no absolute clock synchronization is implemented which would allow for a real identification of pulses. In the actual status of the experiment this is not crucial as the key that Alice sends is known, has a definite length and is sent repeatedly. Thereby the global offset can be derived by comparing part of the measured events of Bob with the key.

Additionally, the clock synchronization enables for time filtering of the received pulses by only evaluating data in narrow time windows and thereby the background noise is reduced and the key rate increased.

4. Investigations on the Temperature Dependence and Precompensation of the Waveguide Circuit

In the first part of this thesis work, investigations on a waveguide chip (Alice 2.0) similar to the one described in the previous section (Alice 1.0) were done.

These were necessary for two reasons. One reason is, that during the measurements with the hand-held sender unit changes of the polarization states emitted by Alice over time were observed [55]. In figure 4.1 one can see the drift of the states over a period of 10 h immediately after switching on the sender unit and that especially the H and M polarized states drift extremely. A first assumption was that temperature changes caused by heat dissipation of the electronics and fluctuations of the room temperature lead to these drifts as the properties of the optical devices may change with varying temperature. The main suspect was the optical waveguide, as the polarization is defined by the wire grid polarizers and afterwards only the waveguide circuit and the beam splitters interact with the photons and thermal fluctuations may introduce stress which leads to birefringence. Another argument for investigations on the temperature dependence of the waveguide was, to evaluate the suitability of the sender unit in environments, such as on satellites, where it is subjected to temperature drifts.

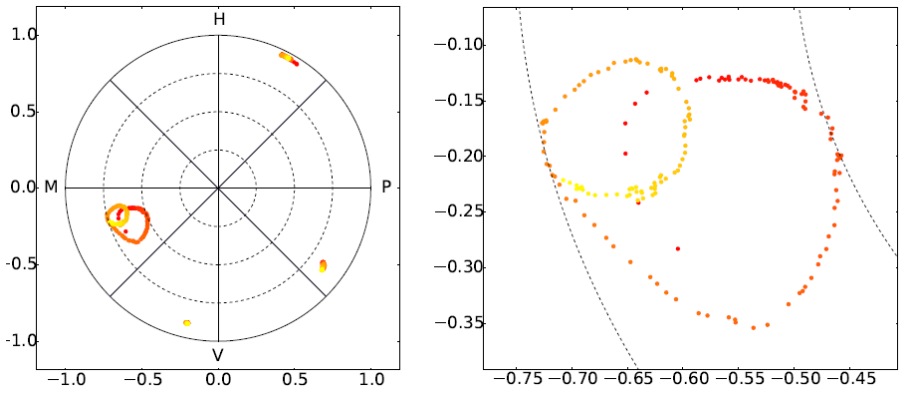


Figure 4.1.: Stability of the states over a period of 10 h. The states are projected onto the equatorial plane of the Poincaré sphere. (Taken from [55])

The second reason for the investigations was, that for the assembly of a new sender unit, where the new waveguide chip is implemented, optimal input states have to

be identified to achieve mutually unbiased output states (just like it happened for the Alice 1.0 waveguide chip).

The physical properties of the Alice 2.0 waveguide chip slightly differ from the ones of Alice 1.0 presented in chapter 3. The birefringence of the Alice 2.0 waveguides is $\Delta n = 5.6 \times 10^{-5}$ between the horizontal and the vertical axis [72] and the waveguide chip has slightly different dimensions (about 22 mm × 5.5 mm × 1.1 mm). In figure 4.2 the schematic top view of the Alice 2.0 waveguide chip can be seen. In table 4.1 the splitting ratios of the three couplers for horizontal and vertical polarized light are shown.

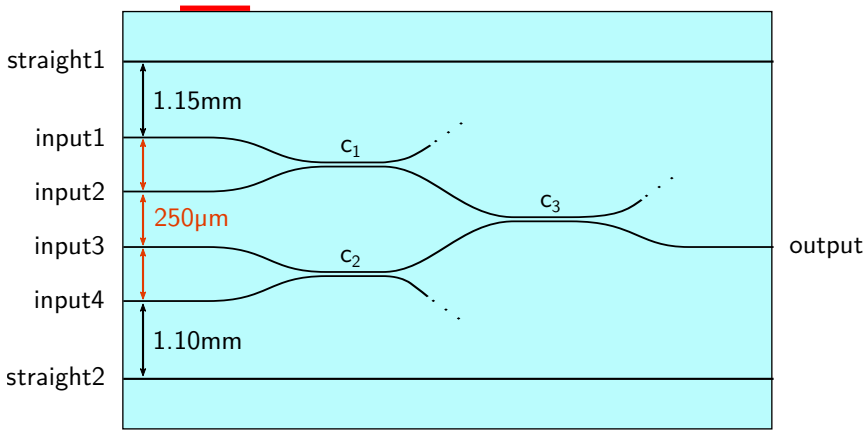


Figure 4.2.: Top view of the Alice 2.0 waveguide chip consisting of the four waveguides used for the spatial overlap of the four discrete light sources via three couplers and the two straight waveguides. (Data taken from [72])

	c_1	c_2	c_3
H	0.421	0.455	0.510
V	0.421	0.460	0.510

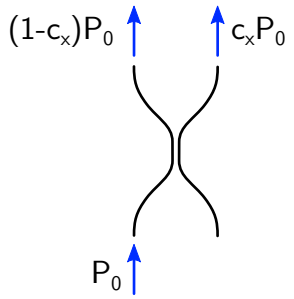


Table 4.1.: Splitting ratios of the directional couplers of the Alice 2.0 waveguide for H and V polarized light. (Data taken from [72])

4.1. Measurement Setup

In this section I will illustrate the setup for the measurements of the waveguide chip (for a sketch of the measurement setup see figure 4.3).

The light of a 850 nm laser is coupled into a single mode fiber to filter out side bands and a 3-paddle polarization controller is used to maximize the throughput of the following polarizer. The polarization of the light can be controlled by a polarization preparation unit made up of a fixed polarizer (set to H-polarization position), a half-wave plate and a quarter-wave plate controlled by stepper motors (see subsection 2.3.3). A coupling lens mounted onto a 3-axis translation stage with a focal length of 11 mm is used to mode match the laser light to the waveguide. Two coupling mirrors are used to couple the light into the waveguide circuit which is mounted onto a custom holder that can be precisely moved in all three dimensions by a 3-axis translation stage (NanoMax TS MAX301/M). A thermoelectric cooler (TEC) controlled by a combined Laser Diode and Temperature Controller (Thorlabs ITC102) is used to precisely regulate the temperature of the waveguide chip and hold it at a constant level during the measurement. An additional thermistor, placed close to the waveguide in the bulk material of the holder, is read out by a computer and used for monitoring and logging of the actual temperature. At the exit of the waveguide circuit an objective (Edmund Optics Din 20, $f_{eff} = 8.33\,\text{mm}$) collimates the beam and a lens with a focal length of 200 mm focuses the light onto a photodiode power sensor (Thorlabs S132C) read out by a power meter console (Thorlabs PM100D). A polarization analysis unit made up of a motorized quarter-wave plate, a motorized polarizer and the powermeter allows for a tomography of the polarization state (see subsection 2.3.4). Additional iris diaphragms placed in front of the photodiode and after the imaging optics filter out stray light .

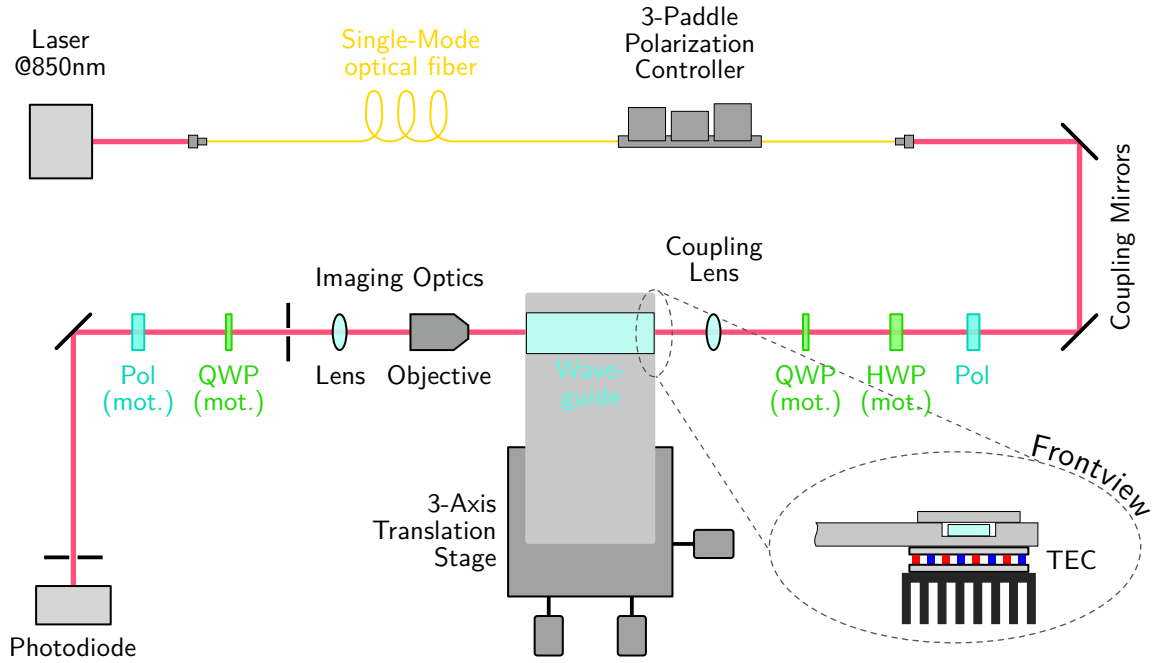


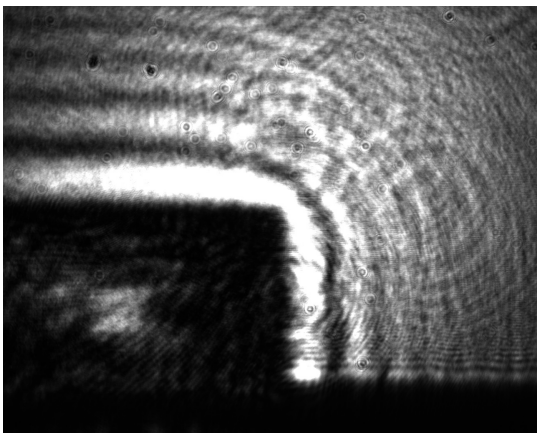
Figure 4.3.: Measurement setup for the characterization of the temperature dependence of the waveguide.

4.2. Coupling and Measurement Procedure

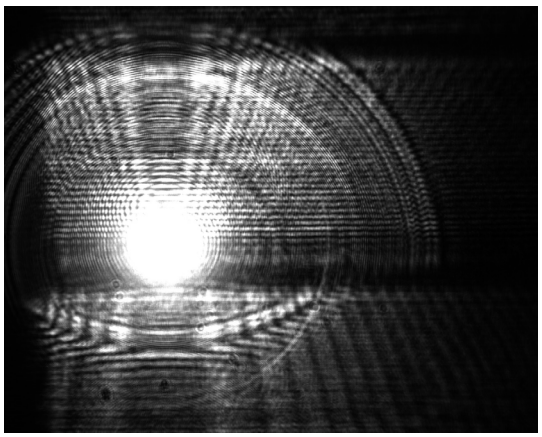
Due to the transparency of the waveguide chip reflections on the side walls of the optical chip and scattering adds to the signal coming from the waveguide. Furthermore, the many degrees of freedom which are partially related (a movement of the coupling mirrors also need a readjustment of the coupling lens and the waveguide and vice versa), makes it quite hard to couple into the waveguides efficiently. A procedure that worked quite well is the following: for a rough coupling the imaging optics have been removed and a CCD-camera has been placed directly behind the waveguide. Then the waveguide chip has been moved with the 3-axis translation stage, such that one of the two upper edges of the waveguide chip can be seen (see figure 4.4a) which is quite easy as they can be identified by a clear change of the interference picture above and below the edge of the waveguide chip. By adjusting the two coupling mirrors and the position of the coupling lens it was tried to align the laser beam parallel to the waveguide chip by adjusting the coupling mirrors. Using the dimensions from the data sheet of the optical chip, the chip was moved to the approximate position of one of the straight waveguides. Coupling to this waveguide is way easier than coupling to the ones of the Alice 2.0 part of the optical chip because it only has one output and can therefore also be seen on the CCD-camera at low coupling efficiencies. In figure 4.4b the picture of the CCD-camera when coupling to a straight waveguide is shown. In figure 4.4c an image when coupling to one of the Alice 2.0 waveguides is pictured. Due to the couplers in the Alice waveguide circuit three bright spots can be seen when coupling to one of the inputs. In the figure one is truncated due to the finite size of the CCD-chip.

After this rough coupling procedure the imaging optics have been placed after the waveguide chip and the CCD-camera behind it (in front of the quarter-wave plate). For further enhancement of the coupling a beam analyzer software has been used. All parameters have been fine-tuned to increase the maximum of the Gaussian profile. In this case there is an advantage of using a camera instead of a powermeter because the background is still quite high in this phase of the coupling procedure and with a camera the maximum could be enhanced. When using a powermeter it can happen that one couples worse into the waveguide and the background intensity increases more as this difference cannot be observed with a powermeter which integrates over its whole active area.

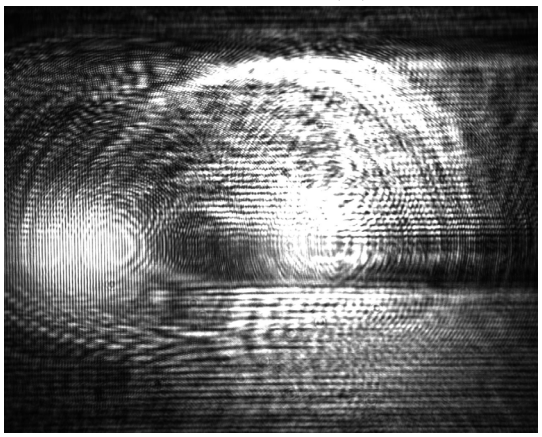
For the coupling to the inputs of the waveguide circuit the position of the waveguide and the imaging optics can be moved according to the specifications from the waveguide chips data sheet and only small optimizations have to be done for efficient coupling when everything is aligned in a good way. When coupling to the waveguide circuit one has to make sure to position the imaging optics to the correct output, as more outputs are emitting light but only one is designated as QKD output (see figure 3.4). After the coupling has been optimized the CCD-camera is removed and measurements can be started. With the setup described above the characterization of the temperature dependence and the optimization of the input states can be done.



(a) Edge of the waveguide chip.



(b) Coupling to a straight waveguide.



(c) Coupling to one of the Alice 2.0 waveguides. The third spot is truncated by the limited size of the CCD-chip.

Figure 4.4.: Pictures of the rough coupling procedure. Images are taken with a CCD-camera directly placed behind the waveguide chip.

4.3. Results and Discussion

In this section I will present the results for the measurement of the temperature dependence and the optimized input states.

4.3.1. Temperature dependence

For the characterization of the temperature dependence of the waveguides the procedure was as follows: the temperature at the waveguide chip has been set to a certain value and after the temperature leveled (about 10 min) which was monitored by the additional thermistor described in section 4.1 the light was coupled into one of the waveguides. Six polarization states (H, V, P, M, R and L) have been coupled to the input and a tomography of the polarization state after the output has been done for

each of them. This has been repeated for the four inputs of the waveguide circuit and the straight2 waveguide. The procedure was carried out for different temperatures, whereby a temperature range from about 15 °C to 45 °C was sampled.

In figure 4.5 the temperature dependent change of the output polarization states when always coupling the same input polarization states (H, V, P, M, R, L) into the waveguide can be seen at the example of the straight2 waveguide illustrated by different viewing angles onto the Poincaré sphere. The figures for the four inputs of the waveguide circuit can be seen in the appendix (figure B.1 to figure B.4).

The figures show, that changes of temperature induce a rotation of the states around the H/V axis of the Poincaré sphere of about 0.23 °/°C. Thereby the input states H and V do not change, but the states P, M, R and L show a drift depending on the temperature.

A possible explanation could be the change of the length of the waveguide chip and the resulting additional phase shift due to the birefringence (see subsection 3.1.1). The approximately gained phase shift can be calculated using:

$$l = \alpha \cdot L \cdot (T_2 - T_1) = \alpha \cdot L \cdot \Delta T \tag{4.1}$$

$$\Delta\phi = \frac{l}{L} \cdot \Delta\phi_0 \tag{4.2}$$

where l is the additional length caused by thermal expansion, $\alpha = 31.9 \times 10^{-7}\,°\mathrm{C}^{-1}$ the thermal expansion coefficient of the substrate material [73], T_1 and T_2 the temperatures, L the length of the waveguide chip at T_1, $\Delta\phi_0$ the intrinsic phase shift of the waveguide at T_1 and $\Delta\phi$ the resulting phase shift between the two states at different temperatures. From equation (4.1) and (4.2) follows:

$$\Delta\phi = \alpha \cdot \Delta T \cdot \Delta\phi_0 \tag{4.3}$$

The phase shift $\Delta\phi_0$ in the straight waveguide due to its birefringence Δn between the horizontal and vertical axis can be calculated using:

$$\Delta\phi_0 = \Delta n \frac{2\pi}{\lambda} L \tag{4.4}$$

With the values of the straight waveguide mentioned at the beginning of this chapter ($L \approx 22\,\mathrm{mm}$ and $\Delta n = 5.6 \times 10^{-5}$) and a wavelength of $\lambda = 850\,\mathrm{nm}$ the resulting phase shift is $\Delta\phi_0 \approx 2.9\pi$ which agrees to the data in figure 4.5 where the phase shift around the H/V-axis must be $(2n-1)\pi$ with $n \in \mathrm{N}$.

From equation (4.3) thereby follows for a temperature difference of 30 °C:

$$\Delta\phi_0 = 31.9 \times 10^{-7} \frac{1}{°\mathrm{C}} \cdot 30\,°\mathrm{C} \cdot 2.9\,\pi \approx 2.8 \times 10^{-4}\,\pi \approx 0.05° \tag{4.5}$$

which is far below the observed values and excludes the length expansion of the waveguide chip as source for the temperature dependent rotation of the polarization states.

In the appendix in figure B.5 for each input state the temperature dependent output states are plotted and a fit for every Stokes indices is done. The fits confirm, that the change of temperature only affects the Stokes parameters S_2 and S_3 whereas S_1 stays constant over temperature. The prefactors of the fits are almost the same for the straight waveguide and the four inputs of the waveguide circuit (see appendix figure B.6 - B.9) which excludes the couplers as source of this temperature dependent rotation of the states.

The observed temperature dependent behavior cannot describe the drift of the states described in the introduction of this chapter. On the one hand the temperature of the waveguide chip can be expected to be relatively stable as the room is air-conditioned and the range of the deviations in figure 4.1 exceeds the values coming from the waveguide chip. On the other hand, we have seen, that the temperature fluctuations act on all states in the same way and the drifts in figure 4.1 are state dependent.

4.3.2. Precompensated states

To figure out optimal input states for the yet unoptimized waveguide circuit of Alice 2.0 the following procedure has been carried out. For each of inputs to the common output a Mueller matrix describing the change of the polarization state was calculated by measuring the polarization at the output for six different input states (H, V, P, M, R, L). The change of the polarization vector by the waveguide circuit can be described by 2.12 (see subsection 2.3.1):

$$\vec{S}_o = M_{wg}\,\vec{S}_i \tag{4.6}$$

where $wg \in \{1, 2, 3, 4\}$ describes the four input ports of the Alice 2.0 waveguide circuit.
By fitting a Mueller matrix (assumed to be unitary) using a least square fit to the measured pairs of input and output state values and inversion of equation (4.6):

$$\begin{aligned} & \vec{S}_o = M_{wg}\,\vec{S}_i \\ \Leftrightarrow \quad & M_{wg}^{-1}\,\vec{S}_o = M_{wg}^{-1} M_{wg}\,\vec{S}_i \\ \Leftrightarrow \quad & \vec{S}_i = M_{wg}^{-1}\,\vec{S}_o \end{aligned} \tag{4.7}$$

one can calculate the optimal input polarization state for a desired output state using equation (4.7). As the optimal input state eventual also has a circular component which cannot be prepared using a polarizer, the circular component of the Stokes vectors have been set to 0 and the vector has been renormalized. For this case the

output states were it was tried to directly obtain H, V, P and M polarizations at the output and therefore the polarizations have already been mapped to designated input ports (H → input3, V → input1, P → input4, M → input2). In table 4.2 the calculated optimal input polarizations are shown. The preparation quality in this case is $q \approx 0.97$.

Alice 2.0 input	BB84 state	calculated optimal input state	polarizer angle [°]	measured output state	DOP
1	V	$\begin{pmatrix} -0.9938 \\ 0.1110 \\ 0 \end{pmatrix}$	86.8	$\begin{pmatrix} -0.9970 \\ 0.0138 \\ 0.0694 \end{pmatrix}$	0.9995
2	M	$\begin{pmatrix} 0.0567 \\ 0.9984 \\ 0 \end{pmatrix}$	43.4	$\begin{pmatrix} -0.0032 \\ -0.9946 \\ 0.0482 \end{pmatrix}$	0.9958
3	H	$\begin{pmatrix} 0.9754 \\ -0.2203 \\ 0 \end{pmatrix}$	-6.4	$\begin{pmatrix} 0.9954 \\ -0.0006 \\ -0.0866 \end{pmatrix}$	0.9989
4	P	$\begin{pmatrix} -0.1601 \\ -0.9871 \\ 0 \end{pmatrix}$	-49.6	$\begin{pmatrix} 0.0212 \\ 0.9970 \\ 0.0026 \end{pmatrix}$	0.9972

Table 4.2.: Calculated optimal input states by fitting Mueller matrices and measured resulting state and its degree of polarization (DOP). The input states have been prepared using the polarization state preparation unit described above.

In a further optimization step the area around the above calculated input polarizations has been scanned with a motorized polarizer placed in front of the waveguide chip. The resulting QBER for the different polarizer angles for the four states calculated using the equations from subsection 2.3.2 is shown in figure 4.6.

One can see, that a minimum for the individual QBERs can thereby be found at $86.3°, 42.9°, -6.3°$ and $-50.5°$. A more relevant property to optimize for is the preparation quality q (described in subsection 2.2.4). Therefore, from these measurement results a new set of optimal input polarization states has been evaluated aiming for a high preparation quality. The obtained set of polarizer angles is shown in table 4.3 (the corresponding output polarization states are visualized in figure 4.7) and result in a preparation quality of $q \approx 0.998$ (calculated by transforming the Stokes vectors into Jones vectors and using equation (2.8)). The values for the angles slightly differ from the minimums of the individual QBER values.

Using the values from table 4.3 the states emitted by Alice are pairwise orthogonal whereby the overall QBER coming from the non-uniform behavior of the waveguide

Alice 2.0 input	optimal polarizer angle [°]	measured output state	DOP
1	85.8	$\begin{pmatrix} -0.9991 \pm 0.0000 \\ -0.0204 \pm 0.0078 \\ 0.0347 \pm 0.0078 \end{pmatrix}$	0.9999±0.0003
2	42.5	$\begin{pmatrix} 0.0193 \pm 0.0078 \\ -0.9964 \pm 0.0001 \\ 0.0068 \pm 0.0078 \end{pmatrix}$	0.9966±0.0002
3	-6.5	$\begin{pmatrix} 0.9905 \pm 0.0001 \\ 0.0176 \pm 0.0078 \\ -0.1396 \pm 0.0076 \end{pmatrix}$	1.0004±0.0011
4	-50.9	$\begin{pmatrix} -0.0209 \pm 0.0078 \\ 0.9966 \pm 0.0001 \\ -0.0325 \pm 0.0078 \end{pmatrix}$	0.9973±0.0003

Table 4.3.: Angles for the polarizers placed in front of the Alice 2.0 waveguides optimized for maximal preparation quality from the data of figure 4.6. These should be used when implementing the tested waveguide chip into a QKD device.

circuit can be minimized leading to higher key rates. The optimized input states have been evaluated for a temperature of 22 °C.

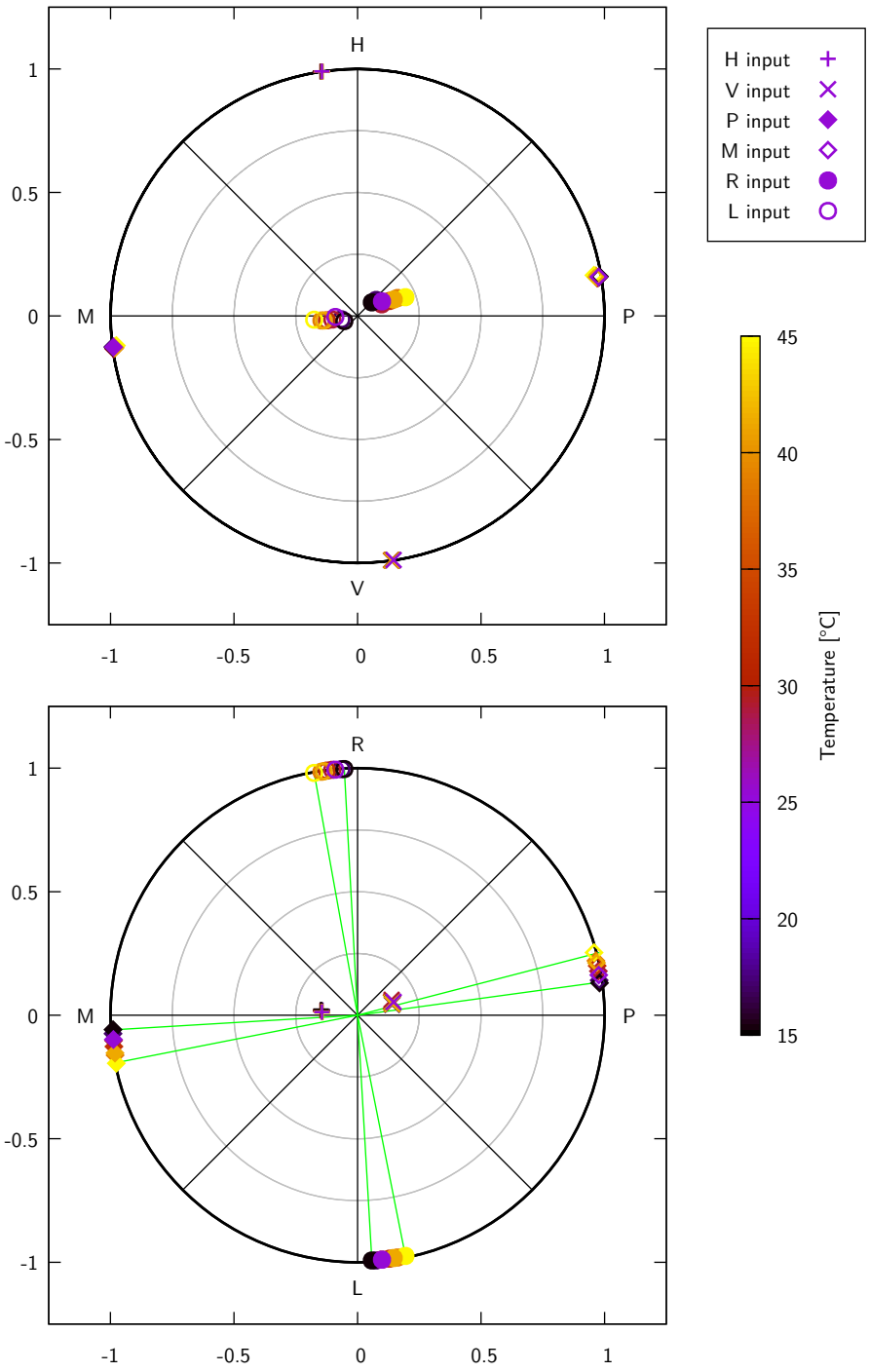


Figure 4.5.: Change of output states over a temperature range of about 30 °C in the straight2 reference waveguide. Plots for the other waveguides can be seen in the appendix.

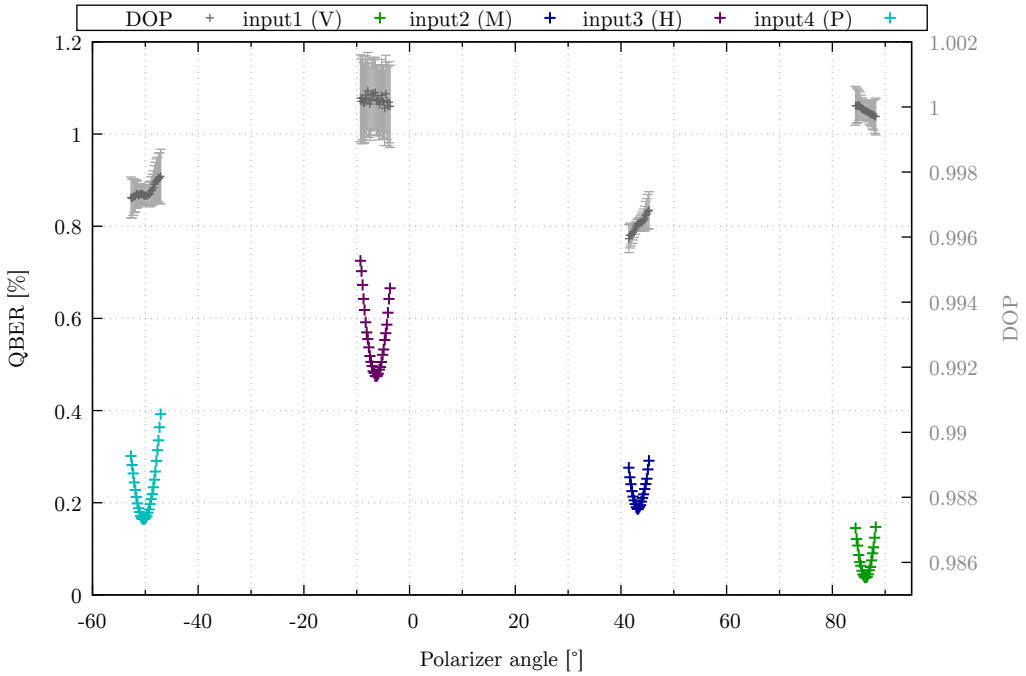


Figure 4.6.: Scan of polarizer orientations at the input of the waveguides close to the theoretical calculated optimal orientations from the Mueller matrix and resulting QBER compared to the BB84 states. Also plotted is the DOP of the output states.

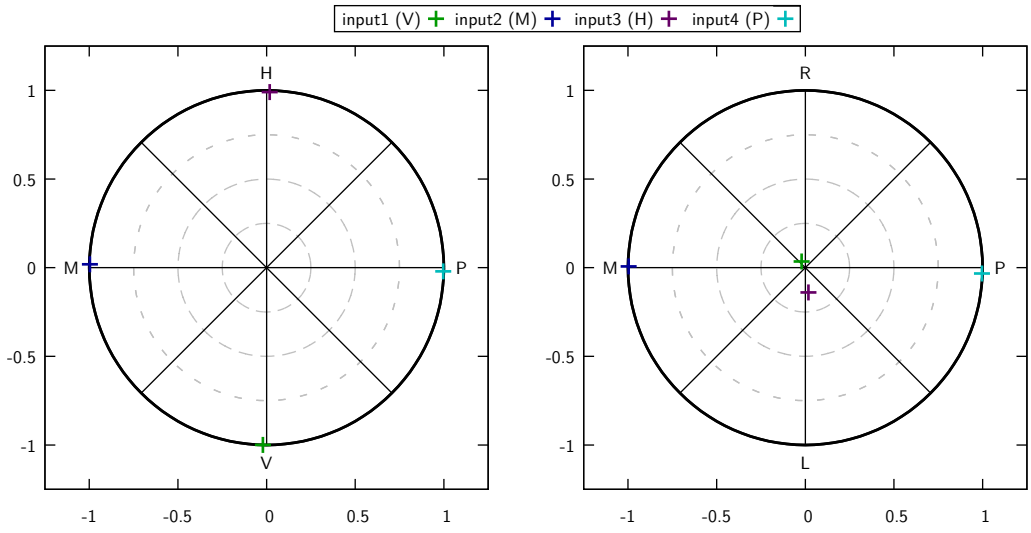


Figure 4.7.: Visualization of the measured output polarizations for the optimal polarizer angles optimized for a high preparation quality q.

5. Development of new Electronics for the Sender Unit

The major topic of this thesis, was the development of new electronics for a QKD sender unit. While still principally based on the previous, next design generations should fulfill additional requirements. The most important examples are a better stability, less electromagnetic emissions to avoid side channels, a lower power consumption and the possible integration into a cube sat. The implementation of the module into a cube sat requires some additional considerations respectively makes some even more important such as materials that do not evaporate under vacuum, heat management and the already mentioned power consumption.

As a first step, new electronics were designed to be modular in a way, that the control elements of the device, clock generation and distribution is on one PCB ("mainboard") and the parts responsible for the generation of the pulses for the VCSELs are on separate PCBs ("subboards") connected by cables to the mainboard. The modular setup enables for a faster and independent testing of different designs for the pulse generation and for the control electronics. Furthermore, a better understanding of the electronics and of the generation of short electrical pulses in the regime of few hundreds of picoseconds can be achieved. While a QKD sender with this scheme should still be possible it lays the basis for future designs. One crucial point in this approach is the transmission of the clock signals from the mainboard to the subboards via connectors and cables without introducing noise jitter or other signal distortions.

5.1. Handling of Fast Digital Signals

In our electronics logical signals with a length of few 100 ps are used and therefore I will present some considerations when working with such signals in this section. The book *High-speed digital design: A handbook of black magic* by H. Johnson and M. Graham [74] gives an in depth view.

5.1.1. Differential signaling

High speed data transmission usually is done by differential signaling and plays an important role in the design of our electronics. Therefore, it shall be introduced here briefly.

In single-ended signaling scenarios the transmitter and receiver have two connections where one is the dedicated signal line, used for the transmission of the data and the other is a common ground return shared by all devices. In differential signaling concepts the sender and receiver are also linked by two connections, but both carry the same signal with opposite polarity and none of the connections is used as backtrace for other signals.

The advantage of differential signaling obtained by this setup is that the receiver is able to reject any signal component that is *common* on both lines as it is designed such that it is only sensitive to the difference between the two signals. Typically, common signals come from external noise sources and as the receiver is not sensitive to common modes the noise has no influence. The reduced noise allows for the usage of lower voltage levels and currents and a more reliable communication than in the single-ended methods. A positive side effect is that the use of low voltage low current signaling usually results in a lower power consumption [75].

5.1.2. PCB design considerations

When designing a printed circuit board for fast signals, various issues have to be considered [74, 76–78]. The most important ones will be described below.

Crosstalk

One thing to consider is crosstalk which is mainly a result of mutual inductance between current loops inducing electro magnetic fields. The closer the signal traces are routed on the PCB, the higher the mutual inductance which makes them more susceptible to crosstalk. Especially in high-density connectors the different signal lines are within close proximity and therefore especially vulnerable to crosstalk. In differential signaling schemes most of the signal current flows through the differential pair of conductors and not via the ground return, reducing the current loop area and thereby the mutual inductance and the resulting crosstalk. Maintaining a small distance of the two striplines of the same pair ensures that both are equally exposed to stray inductance (which has thereby no impact by the nature of differential signaling).

As high frequency currents do not flow along the path of the smallest resistance but of the smallest impedance, placing ground planes between different signals results in multiple return paths for common-mode currents and thereby minimizes the current loops. Still, minimizing the crosstalk in a high-density PCB remains a non trivial task.

Impedance matching

An essential role in fast signaling is impedance matching of the transmission lines. Changes of the impedance at e.g. connectors induces reflections which leads to degra-

dations of the signal quality (see figure 5.1). The reflection coefficient Γ which gives the fraction of the signal that is reflected is given by:

$$\Gamma = \frac{Z_2 - Z_1}{Z_2 + Z_1} \tag{5.1}$$

where Z_1 is the impedance of the first signal line and Z_2 the one of the second. To minimize reflections all elements dealing with the signal (conductors, connectors, input stage of the receiver) should have the same impedance.

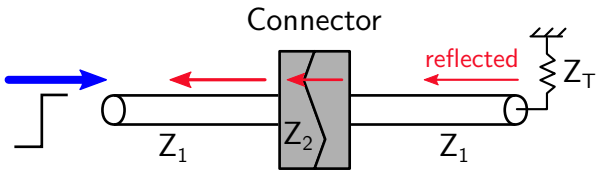


Figure 5.1.: A mismatch of the impedance ($Z_1 \neq Z_2$) leads to reflections for example at connectors but also at the termination resistance.

On a PCB the impedance of the transmission lines is defined by the physical properties of the conducting paths and layer materials. In our designs edge-coupled surface microstrip pairs are used whose differential impedance is influenced by the height t and width of the striplines w, their distance s, the thickness of the PCB between the layers h and the dielectric constant ϵ_r of the PCB material (also see figure 5.2). The impedance is given by [79, 80]:

$$Z_0[\Omega] = \frac{87}{\sqrt{\epsilon_r + 1.41}} \ln\left(\frac{5.98 \cdot h}{0.8 \cdot w + t}\right) \tag{5.2}$$

$$Z_{\text{diff,microstrip}}[\Omega] = 2Z_0\left(1 - 0.48 \cdot \exp\left(-0.96 \cdot \frac{s}{h}\right)\right) \tag{5.3}$$

where Z_0 is the impedance of a single surface microstrip and $Z_{\text{diff,microstrip}}$ the differential one. The formulas are valid for:

$$0.1 < \frac{w}{h} < 3.0 \qquad 1 < \epsilon_r < 15$$

One can see, that for an uncoupled pair of striplines (far away from each other) $Z_{\text{diff,microstrip}} \to 2Z_0$.

The end of the transmission lines should always be terminated by a resistor which reduces reflections and ringing. In the most simple case a resistance equal to the impedance of the transmission line can be used. For circuits which require high drive currents (like TTL or CMOS) more advanced termination schemes should be considered [74].

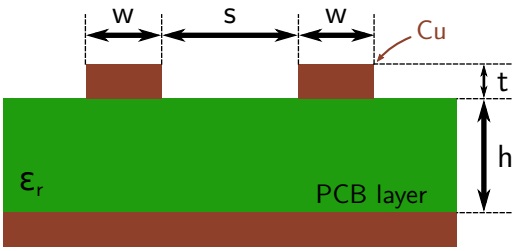


Figure 5.2.: Edge coupled differential surface microstrip.

Skew

For high-speed differential signal pairs it is important (beside being as short as possible), that the two conductors have the same length. Differences lead to imbalances of the timings of the two complementary signals. To avoid this problem meanders can be used to match the length. These should always be placed at the unmatched end of the transmission lines (see figure 5.3) [77].

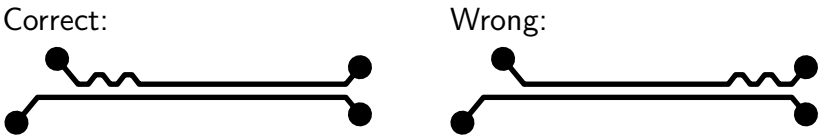


Figure 5.3.: Using meanders for length matching of differential signal striplines. The length matching should always be done at the mismatched ends.

5.2. Design Considerations

The short duration of the electrical pulses controlling the VCSELS (few 100 ps) places stringent requirements on the design of the module.

Therefore, a four layer PCB has been used where fast signals are routed on the top layer, over a ground plane (layer two) (see section 5.1). Layer three is used for the power supply of the devices and on the fourth layer additional conduction traces are placed (e.g. the optional 5 V power supply for the FPGA). The PCB layer structure and the thicknesses of the different layers can be seen in figure 5.4

The multi-layer design allows for a separation of signal traces reducing crosstalk and furthermore the differential signal lines routed on the top layer can be impedance matched by choosing appropriate dimensions of the signal wires using equations 5.2 and 5.3. As the layer thickness is determined by the PCB manufacturer (356 µm), the dielectric constant of the PCB material $\epsilon_r \approx 4.3$ and the copper layer thickness being 35 µm the only parameters that can be altered are the distance between the two striplines and their width. The two parameters also have to be chosen in a way, that they approximately fit to the pitch of the IC contacts which is 0.5 mm. For the

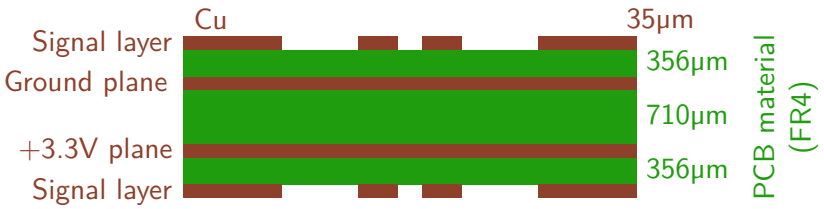


Figure 5.4.: Structure of the four layer PCB used for our design. All copper layers have a thickness of 35 µm Fast signals are routed on the top layer, the second layer is a ground layer, the third one is used for power transmission and the bottom plane is used for additional traces.

used width of 280 µm and distance of 150 µm the impedances are $Z_0 \approx 76.7\,\Omega$ and $Z_{\text{diff}} \approx 104\,\Omega$ the latter coming very close to the recommended value of 100 Ω.

For most applications the dissipation of the heat produced by the ICs plays an important role for the stability ob the device. As already mentioned in the description of the electronics of the hand-held device, most of the ICs in use have a "Quad Flat No Leads" (QFN) package where the main part of the heat (about 80 % [81]) is dissipated through an exposed pad at the bottom of the package. From there it is transferred to the ground plane and gets dissipated by thermal vias distributed over the board area. Additionally, on the backside of the PCB the vias are contacted to a larger metal area where heat sinks are attached.

5.2.1. Mainboard

At first, the mainboard will be described, which is responsible for the power supply, clock generation and distribution and the control of the module.

For the power supply of the module an input voltage of 5 V was chosen instead of an additional 12 V to 5 V voltage regulator of the previous design. For the conversion from 5 V to the 3.3 V, needed for most of the electronics, a switching power module (Texas Instruments LMZ10505[a]) with a maximum output current of 5 A and an efficiency of up to 96 % has been chosen.

For the control of the module the mainboard employs a Spartan-3E FPGA breakout board (EFM-01) similarly to the previous design. Additional to the electrical connections needed for the control of the ICs on the subboards, several GPIOs are routed from the FPGA to the subboard connectors to enable the testing of different subboard types. Moreover differential pairs are provided for the subboards to carry the fast signals from the FPGA enabling for for new pulse generation schemes.

The clock generation and distribution has been redesigned aiming for a better signal quality. The oscillator (Texas Instruments LMK61E2-100M00[b]) has a frequency of 100 MHz and features a very low jitter and fast rise and fall times (≈ 120 ps

[a] http://www.ti.com/lit/ds/symlink/lmz10505.pdf
[b] http://www.ti.com/lit/ds/snas676d/snas676d.pdf

from 20 to 80 %). The clock signal is fed into a fanout buffer (Micrel SY58031U[c]) which provides eight identical output copies of the signal with rise/fall times below 60 ps and CML signal levels. One of the clock signals is sent to a buffer IC (Micrel SY58604U[d]) which provides LVPECL outputs, such that external devices can be connected and thereby synchronized to the internal clock of the sender. One clock signal is fed to the FPGA board where it can be used for clock synchronous enabling of the four delay chips for sending BB84 key patterns and modulation of the beacon laser. The other six clock signals are routed to the connectors 1-4 providing clock signals for the subboards. As the clock signals are the most crucial ones and distortions would deteriorate the pulse quality, the strips carrying these signals are routed avoiding vias and other wires were placed as far away from them as possible to minimize crosstalk.

In table 5.1 the pin assignments of the FPGA and clock to the five connectors are shown. Also a general idea for the functions of the different pins is given. Until now, all laser drivers which were considered use a two-wire serial interface (consisting of a clock signal SCLK and data signal SDA) for communication. Pin 12 (SDA) and pin 14 (SCLK) are reserved for this purpose. The delay chips use a 3-wire serial interface (consisting of a clock signal SCLK, a data signal which is here named SDATA to not be confused with the one from the laser driver and a SLOAD signal used for the loading of the values of the shift register to the data latch register), pin 3 (SLOAD), pin 13 (SDATA) and pin 14 (SCLK) can here be used (the laser driver and the delay chip share the same clock signal). Pin 4 allows for the disabling of the delay chips for sending BB84 patterns. Of course these functionalities can be exchanged depending on the subboards and the FPGA design. For powering the subboard two pins are connected to the 3.3 V plane to provide a total current of 1 A (the connector has a current rating of 0.5 A per pin).

Flexible flat cables (FFC) and connectors (Hirose FH12_16S-0.5H) have been chosen for the connection between the mainboard and the subboards. These allow for a small form factor due to a pitch of 0.5 mm and a good transmission of the signals. When the differential signal pair is routed between two ground wires the differential impedance is 100 Ω allowing to directly connect the $Z_{diff} \approx 100$ microstrips on the mainboard to the subboards via the cable without changing the differential impedance and thereby avoiding backreflections.

As table 5.1 indicates, the functionality of the connectors differs. Connector 0 does not include a direct clock signal and could be used for a beacon subboard directly modulated by the FPGA. Connectors 1&2 carry two differential signal pairs from the FPGA and can thereby be used for example for testing the delay generation using the FPGA. Connector 3&4 have two separate clock signals which allows for the testing of hard-wired delays (will be explained in the next subsection) and also enables to check whether two different clock signal inputs for the delay ICs improve the signal quality of the outcome, as normally the specifications for the differential

[c] http://ww1.microchip.com/downloads/en/DeviceDoc/sy58031_2_3_eb.pdf
[d] http://ww1.microchip.com/downloads/en/DeviceDoc/sy58604u.pdf

Pin	Function	Connector 0	1	2	3	4
1	Power	+3.3 V				
2	Power	Ground				
3	GPIO (SLOAD)	**K14**	**C13**	**L13**	**L1**	**F1**
4	GPIO (/ENA,/ENB)	**J12**	**C14**	**L14**	**L2**	**G1**
5	Power	Ground				
6	GPIO/Clock	**D13**	**B12**	**G3**	CLK+	CLK+
7	GPIO/Clock	**D12**	**A12**	**H1**	CLK−	CLK−
8	Power	Ground				
9	GPIO/Clock	**H2**	CLK+	CLK+	CLK+	CLK+
10	GPIO/Clock	**H3**	CLK−	CLK−	CLK−	CLK−
11	Power	Ground				
12	GPIO (SDA)	F13	J13	K13	M13	N10
13	GPIO (SDATA)	A13	G14	N14	P11	N9
14	GPIO (SCLK)	H12	M12	M9	F14	F2
15	Power	Ground				
16	Power	+3.3 V				

Table 5.1.: Pin assignments of the FPGA and clock to the five connectors of the mainboard. Differential signal pairs coming from the FPGA are shown in bold. Suggestions for the application of the PINs are in brackets.

signals only support direct connections while trace branches change the impedance and termination resistance, which leads to a degradation of the signal quality due to reflections [82].

A picture of the board layout is shown in the appendix in figure A.2.

5.2.2. Subboards

Several sub-board have been designed to test different pulse generation schemes and get a better understanding of the generation of short electrical pulses in the pico second regime. An overview can be seen in table 5.2 and the corresponding PCB layouts can be found in table A.1 in the appendix. Subboards with "_test" at the end of the name indicate boards, where only part of the corresponding subboard is present to test the signal properties after certain ICs. Therefore, the striplines are connected to SMA-connectors which can be connected to an oscilloscope (see section 5.4). In principle the pulse generation for the VCSELs is built up of three

components as in the previous Alice design. Some sort of delay shifts two clock signals respective to each other and an AND-gate generates a short pulse out of them used for the modulation of a laser driver.

Subboard	Conn.	Delay	Logic	Laser driver	Purpose
previous design	—	SY89297U	SY55851A	ONET4291VA	
empty	0-4	—	—	—	testing signal quality
0a	1,2	SY89297U	SY58051AU	ONET4291VA	enabling of the pulsing using the laser driver
0b	3,4	SY89297U	SY58051AU	ONET4291VA	two clock inputs to delay
0b_test1	3,4	SY89297U	—	—	
0b_test2	3,4	SY89297U	SY58051AU	—	
1	1,2	NB6L295	SY58051AU	ONET1191V	new delay & laser driver
2a	3,4	hardwired	SY58051AU	ONET4291VA	hardwired delay with 10 cm
2a_test1	3,4	hardwired	—	—	
2a_test2	3,4	hardwired	SY58051AU	—	
3	(0,)1,2	—	SY58051AU	ONET4291VA	Delay using a FPGA
3_test	(0,)1,2	—	—	—	

Table 5.2.: Overview of the used ICs for the subboards and the connectors of the mainboard they are compatible with (Conn.). The inted purpose is also given (also see text). The ICs of the previous Alice module are given for comparison. Subboards that can be used for the determination of the signal properties after certain pulse generation steps are indicated with "_test" and features SMA connectors at the end of the signal traces.

The empty submodule is intended for testing the signal quality of all possible signals at the subboards and only features SMA connectors.

The design of Submodule 0a is close to that of the electronics on the hand-held sender module with the dual channel delay SY89297U (Micrel[e]) and the laser driver ONET4291VA (Texas Instruments[f]). Only the logic chip has been replaced by a different one (Micrel SY58051AU[g]), as the one from the previous module is no

[e]http://ww1.microchip.com/downloads/en/DeviceDoc/sy89297u_eb.pdf
[f]http://www.ti.com/lit/ds/symlink/onet4291va.pdf
[g]http://ww1.microchip.com/downloads/en/devicedoc/sy58051au.pdf

longer available. Additionally a connection to the enable pin of the VCSEL driver is available to check whether the enabling of the pulsing (for sending arbitrary QKD polarization patterns) can be done using the laser driver. So far this is done by the delay chip and this check is necessary for cases where no delay chips are used. Submodule 0b is similar, but the two inputs of the delay chip are connected to two separate clock lines to check, if this leads to better signal properties of the electrical pulses as already stated above.

In Submodule 1 the delay chip has been replaced by a different one (ON Semiconductor NB6L295[h]) as well as the laser driver (Texas Instruments ONET1191V[i]). Furthermore the modulation input of the laser driver is AC coupled as it is recommended by its data sheet. The replacement of the delay chip is just to check if it is applicable. The advantage of the new laser driver is a higher possible operation speed of $11.3\,\mathrm{Gbit\,s^{-1}}$ (compared to $4.25\,\mathrm{Gbit\,s^{-1}}$ of the ONET4291VA) and a higher possible modulation current of up to 40 mA (compared to 15 mA). The latter enables for a lower setting of the bias current. Thereby the spontaneous emission background can possibly be reduced, as random photon emissions are less probable due to the bigger difference between the lasing threshold of the VCSELs and the bias.

To tackle the problem of the high power consumption of the delay chip (see table 3.2) it has been replaced by a hardwired one in Submodule 2a. For that purpose one of the clock signals is delayed by a meandered stripline. For a certain delay length the difference in the timings calculates as follows:

$$\begin{aligned} \Delta t &= \frac{\Delta x}{c_{\mathrm{St}}} \\ c_{\mathrm{St}} &\approx \frac{c_0}{\sqrt{\epsilon_{eff}}} \approx 0.59 \cdot c_0 \approx 1.8 \times 10^8\,\mathrm{m\,s^{-1}} \end{aligned} \tag{5.4}$$

where c_{St} is the approximate signal velocity in the stripline, ϵ_{eff} the effective dielectric constant of the microstrip calculated following [83] and c_0 the speed of light in vacuum. In Submodule 2a the difference of length of the meandered striplines and the straight ones is 10 cm which should result in a delay of 556 ps. While having no power consumption and being intrinsically stable, the disadvantage of this solution is that the temporal pulse parameters (shape and timing) cannot be later tuned to optimize the temporal overlap to such one as it can be seen in figure 3.7.

Submodule 3 is designed such, that the delay can be generated using the FPGA. A difference of the delay of the two signals can for example be acquired by routing the clock signal over different path lengths within the FPGA. This has already been tested before in our group by S. Frick [84], but did not seem to be applicable for short pulses yet [17]. A better understanding of FPGAs can still allow for such a solution

[h] https://www.onsemi.com/pub/Collateral/NB6L295-D.PDF
[i] http://www.ti.com/lit/ds/symlink/onet1191v.pdf

as shown in principal in [85] for a delay resolution of 250 ps and [86] for a resolution of 105 ps and 13 ps. Also switching to a newer FPGA (like the Spartan6) which probably has better signal behavior can help avoiding the very power consuming delay chips and still maintain the possibility of adjustable delays.

5.3. PCB Assembly

Due to the fact that ICs packaged in QFN casings cannot be soldered manually using a soldering iron, the method of reflow soldering has been used for the assembling of the PCBs. Thus a new reflow oven (LPKF Proto Flow S) has been purchased.

Before the soldering process the PCBs have been dried for several hours at 110 °C to get rid of the moisture which can damage the PCB during the reflow process by introducing pressure when exposed to high temperatures [87]. Surface mount devices are also susceptible to this effect and should be baked when the moisture card enclosed with the devices indicates too high moisture levels or after storing at high moisture [88].

As solder paste "no-clean SAC305" which consists of 96.5 % tin, 3 % silver and 0.5 % copper (Chipquik SMD291SNL50T3) with particle sizes of type 3 corresponding to the definition in [89] (minimum of 80 % of the particles should have a size between 25 µm and 45 µm) was used. It was applied using a soldering stencil with a thickness of 120 µm. The ICs have been placed by hand using a microscope and a tweezer.

The process of reflow soldering can be divided in several zones. At the beginning the whole board is heated up to a certain temperature to avoid too much stress in the later reflow zone and get rid of volatile solvents. Afterwards the oven is heated up to the desired peak temperature whereby the solder paste melts and contacts to the pads of the devices. This peak temperature shall not be higher than the specified maximal temperature of the most sensitive component. At the end the parts are gradually cooled.

In table 5.3 the set temperatures for the reflow process of our electronics are shown and in figure 5.5 the measured temperature curves of the reflow soldering process can be seen where the three temperature measurement positions are in the left, middle and right part of the oven. The maximum temperature does not exceed 245 °C which is the maximal specified temperature of the clock oscillator. The effect that the right part of the oven cools down faster than the left part lies in the fact, that the ventilators which circulate the air inside of the oven rotate in the same direction. When the lid is opened for the insertion of the PCBs or at the end of the soldering process the warm air is removed faster on the right side of the oven.

Reflow step	Temperature	Time	Power (heating/cooling)
Preheat	175 °C	165 s	—
Reflow	245 °C	80 s	100 %
Cooling	—	100 s	100 %

Table 5.3.: Set parameters of the oven controller for the reflow process.

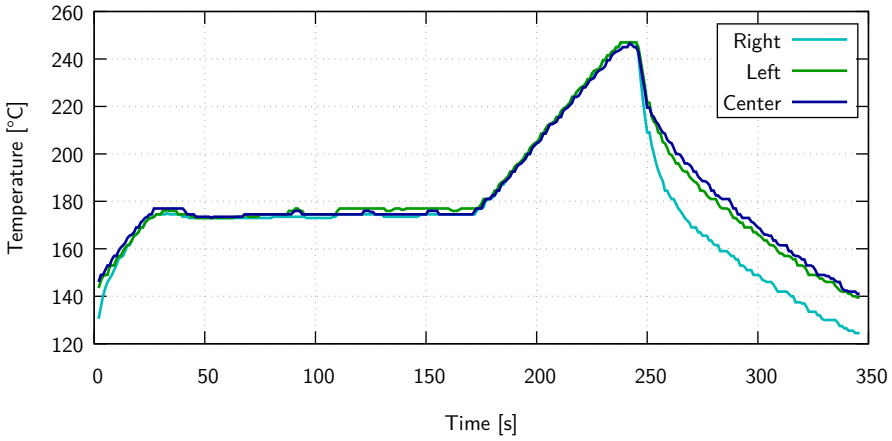


Figure 5.5.: Temperature curves in different parts of the oven during the reflow soldering process. The first part is the preheat part then follows the reflow process with a maximum temperature of 245 °C.

5.4. Characterization of the Circuits

First measurements have been done characterizing the quality of the transmission of the clock signal from the mainboard to subboards and of the signal delay using a meander.

The measurement of fast signals on the board is quite challenging, as every connected device attached to the circuit influences its properties (capacity, impedance). As we do not provide of a differential oscilloscope or a differential probe for measuring such signals the setup shown in figure 5.6 has been used. In this scheme the two signals traces are connected using the SMA connectors to 50 Ω coaxial cabels which are differentially terminated with a 100 Ω resistance close to the oscilloscope (Teledyne LeCroy Waverunner 640Zi). The oscilloscope inputs are set to a high input impedance of 1 MΩ. This setup attempts to maintain the 100 Ω differential impedance over the whole path. As the termination resistor is placed close to the oscilloscope additional noise may be introduced by the cables and the measurements most probably only give an upper limit of the noise and jitter. Also the digital nature of the oscilloscope may introduce errors in this picosecond regime. A differential probe might provide a substantially higher common-mode rejection ratio (CMRR) performance and possibly give better results as the ones shown below [90].

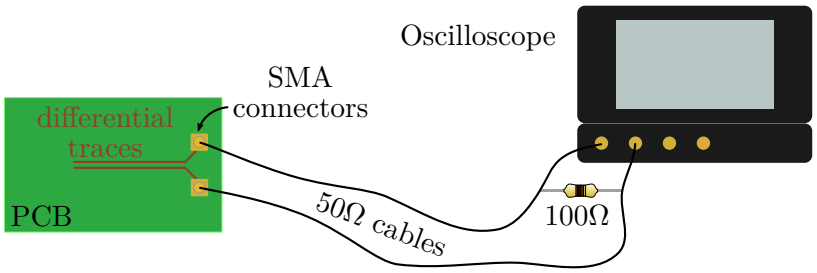


Figure 5.6.: Measurement setup for evaluating differential signals using an oscilloscope.

An important finding during the measurements was that the positive part of the clock oscillators differential signal is not functional. Possible reasons are that the contact is not connected or the device is faulty. Despite this, the output signal of the fanout chip is differential but probably this fault is the reason for the reduced duty cycle of the clock signal after the fanout chip. Nevertheless, it still allows to investigate the signal quality and the functioning of the following circuit parts.

5.4.1. Clock transmission

At first the transmission quality of the clock signal from the mainboard to the subboards via a FFC cable with a length of 5 cm has been evaluated as the quality of the clock signal is one of the most crucial points of the modular design. For these measurements Subboard 3_test was used, attached to connector 4 of the mainboard.

The differential clock signal was probed as shown in figure 5.6 and as reference for the measurements the signal from the buffer output was used. The reference signal was only used in single ended configuration (the positive output of the buffer) with the other output of the buffer terminated with 50 Ω.

Figure 5.7 shows the positive and negative part of the transmitted clock signal. As already stated above, one can see that the duty cycle of the clock is not the specified 50 %. The amplitude of the subboard signals is about 0.3 V which is 75 % of the specified 400 mV of the CML standard. This should be sufficient for the triggering of the following devices. The small peak most probably comes from an impedance mismatch at some point (probably only from the measurement setup) as it is not present in the signal from the buffer.

As a next step, we have determined the timing jitter of the clock signal going different paths of the circuit. The jitter of the signals is shown in figure 5.8. In this plot the timing jitter of the rising edges of the signal over one clock cycle has been compared. As expected, the distribution of the signals from the buffer is narrower with a standard deviation of $\sigma \approx 7.2\,\text{ps}$ compared to the one of the subboard ($\sigma \approx 18.4\,\text{ps}$) due to additional noise that is picked up at the longer traces and from the connectors.

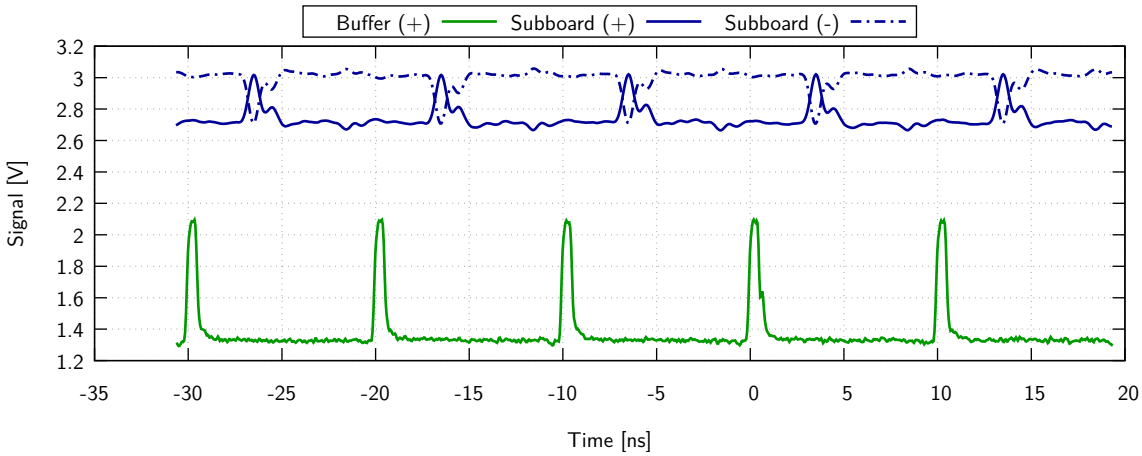


Figure 5.7.: Signal shapes of the buffer (used for triggering) and the clock signals at the subboard.

In figure 5.9 the jitter of the clock signal on the subboard relative to the one of the buffer is shown. The standard deviation in this case is about 8.6 ps. The offset on the time axis comes from the fact, that the signal paths are different and the latency of the buffer IC.

In summary, the achieved quality of the clock signal at the subboard seems sufficient for the operation of the module in this modular setup, as it is relatively small compared to the optical pulse length 200 ps of the VCSELs.

5.4.2. Hard-wired delay

Next the hard-wired signal delay using the meander of Subboard 2_test1 was characterized.

As the oscilloscope does not have enough input ports to measure signals of the subboard and the clock signal from the buffer simultaneously, the undelayed and delayed signal have been referenced to the buffer signal and measured successively (see figure 5.10 for the signal shapes and timings). Also plotted are the signals obtained from calculating the differential signal ("s" and "d", where s is already inverted) and the expected logical output from the AND gate. The width of this pulse is about 600 ps.

A histogram of the time difference of the rising edge from the buffer signal and the subboard signals has been evaluated for the two clock lines and is shown in figure 5.11. The second small peak in the data set of the time difference between the buffer and the delayed signal (at about 2450 ps) most likely comes from wrong triggering of the oscilloscope. The measured time difference of the mean of the two peaks is with 750 ps distinctively longer than the expected 556 ps. This may come from wrong assumptions for the effective dielectric constant as the dielectric constant of the PCB material is only loosely defined.

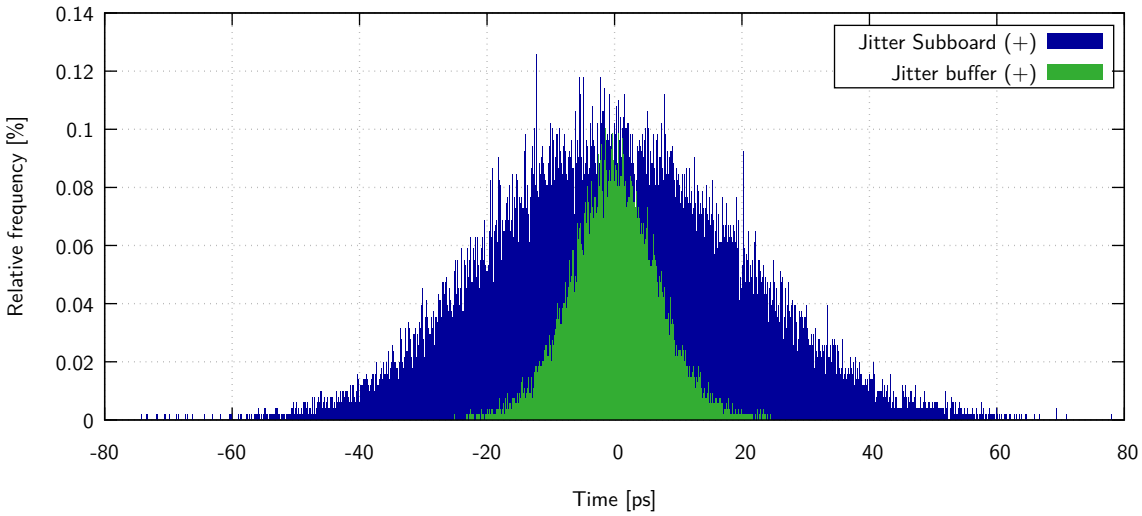


Figure 5.8.: Histogram of the timing jitter of the positive clock signal on the subboard within one cycle (blue) compared to the one of the positive buffer signal (green).

Using Subboard 2a_test2 which also contains the AND-gate, the above theoretically obtained value for the length of the pulse peak after the AND-gate was tested. In figure 5.12 one can see a histogram of the pulse length at the output of the gate with a mean value of about 660 ps which is comparable to the estimated value from above. The non Gaussian distribution cannot really be explained.

5.5. Conclusion

In this section a new series of prototype boards for the driving electronics of a QKD sender was developed. Reflow soldering of the small ICs has been used for the assembly of the PCBs. In summary the measurements show that in principle the transfer of the clock signal from the mainboard to the subboards is sufficient which allows for the modular design. Furthermore, it has been proved that the pulse generation scheme can be built up without the power consuming delay lines albeit at the cost of a constant pulse width and position. Further investigations are required to check for the applicability of this method. When going to shorter pulses the quality of the pulses may even improve as shorter meanders are sufficient whereby less jitter may be introduced. A further task, that has to be done is the testing of the other subboards, which also may lead to new applicable pulse generation schemes for our QKD sender. Additional impedance matching of the single stripline to 50 Ω may lead to better results but is very cost intensive as therefore the PCB layer thickness must be customized. Furthermore the electronics have to be tested with attached VCSELs to investigate the impact of the electrical pulses onto the optical ones.

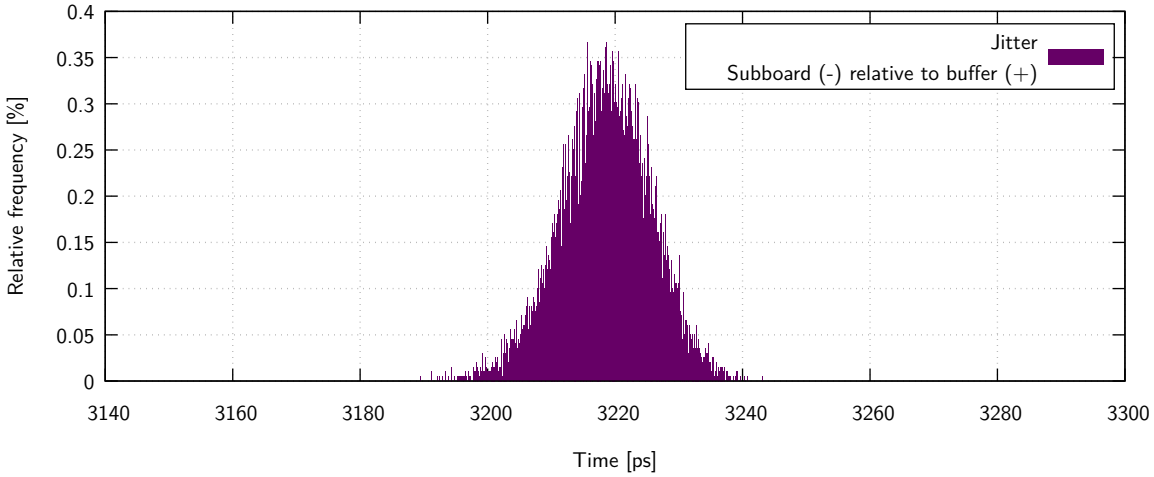


Figure 5.9.: Histogram of the jitter of the negative clock signal on the subboard to the positive one of the buffer. The offset reflects the fact that the two signals go different paths and the latency of the buffer IC.

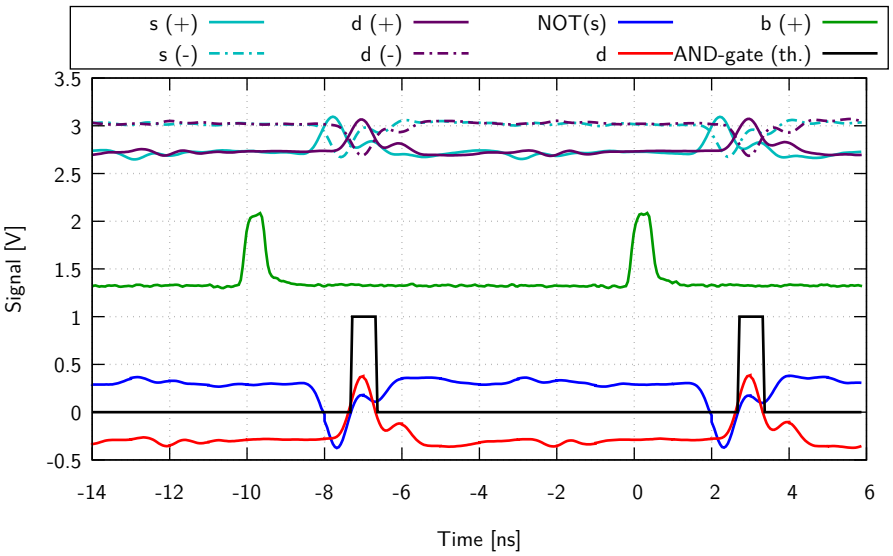


Figure 5.10.: Signal (s) and delayed signal (d) of Subboard 2_test1 referenced using the signal from the buffer (b). Also plotted is the calculated differential signal where the one of the short path already is inverted and the expected logical output pulse of the AND-gate.

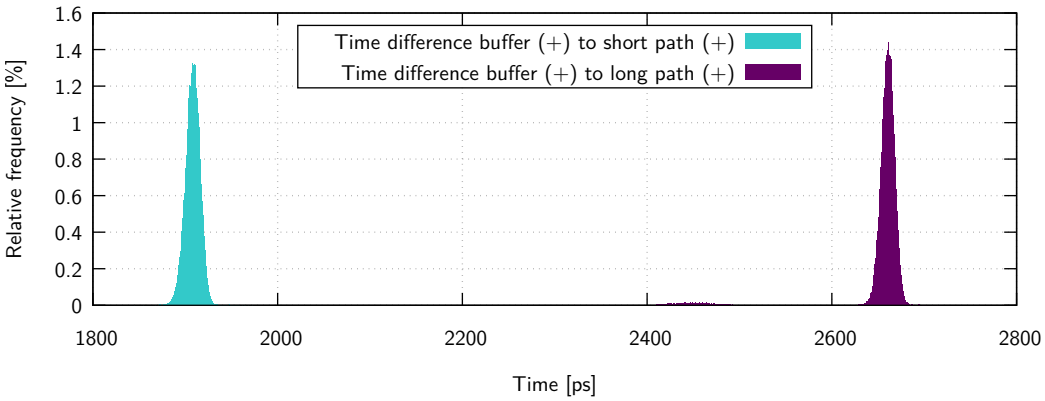


Figure 5.11.: Histograms of the time difference between the rising edge of the buffer (+) signal to the subboard (+) signal for the short path (light blue) and the meandered one (purple).

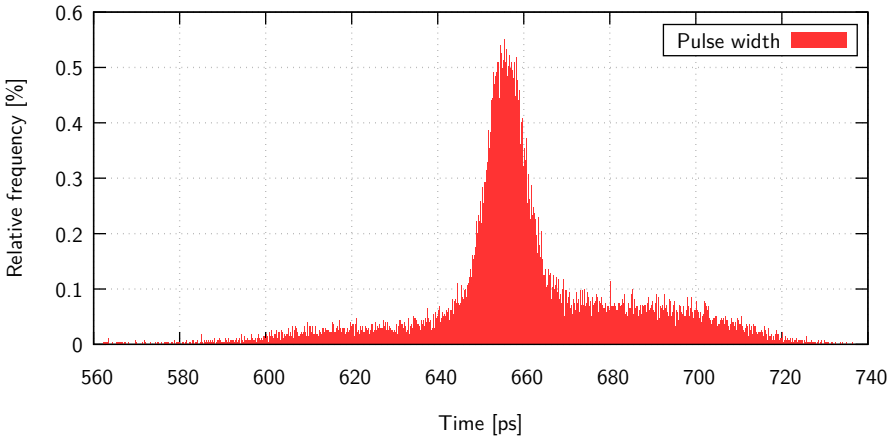


Figure 5.12.: Histogram of the length of the pulse obtained from the hard-wired delay with an AND gate attached (Subboard 2a_test2).

6. Summary and Outlook

Within this thesis investigantions on different components of a QKD sender unit were done, laying some of the groundwork for a new QKD sender. Therefore, a waveguide circuit implemented in a glass substrate has been characterized and new electronics for a QKD sender have been developed.

At first, investigations on a waveguide chip (named "Alice 2.0") designed for the spatial overlapping of four inputs to one output for the implementation of a QKD protocol similar to the one ("Alice 1.0") implemented in the hand-held sender of our group have been done.

Here, the temperature dependent change of polarization states passing the waveguide circuit have been evaluated which allows for a prediction of the polarization states emitted by the sender by simple measurements of the temperature of the waveguide. This is important in application scenarios where the sender is exposed to temperature drifts, such as an integration into a satellite.

Furthermore optimized input states for the waveguide circuit were evaluated allowing for a precompensation of the change of the polarization states caused by the waveguide circuit. By implementing these input polarizations a preparation quality q close to one can be achieved, reducing the QBER compared to an uncompensated setup and thereby increase the key rate of the QKD sender.

The main part of this thesis work was the development of new electronics for a QKD sender, aiming for a lower power consumption, which is essential for the implementation into a satellite, a better stability and the possibility for fast and independent testing of pulse generation schemes.

Therefore a modular device, consisting of a mainboard and several subboards connected via flexible flat cables (FFC) was designed and assembled. A new approach for the generation of the short pulses used for the modulation of the VCSEL driver by delaying a clock signal using meandered striplines has been investigated. The results indicate that the power consuming delay lines can be replaced by this solution and thereby the total power consumption can approximately be halfed at the cost of a fixed pulse width and timing. Measurements of the quality of the transmission of the clock signal from the mainboard to the subboards, which is a crucial point in such a modular design, has been investigated confirming the applicability of the modular setup.

While laying the basis for a new modular electrical design of a QKD sender, further aspects have to be taken into consideration. The pulse generation using the

hard-wired delay has to be probed with shorter meanders aiming for a pulse length of 200 ps and the impact of this pulse generation scheme onto the VCSEL driver and the resulting optical pulse has to be investigated. Furthermore, survey has to be done on the applicability of the different developed but not yet tested subboards.

A. Printed Circuit Board layouts

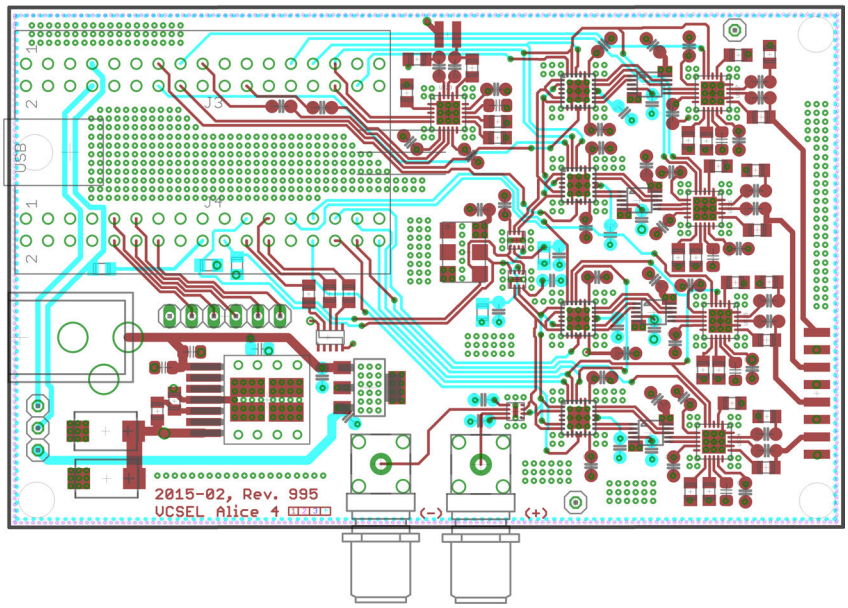


Figure A.1.: CAD file of the driving electronics of the hand-held QKD sender.

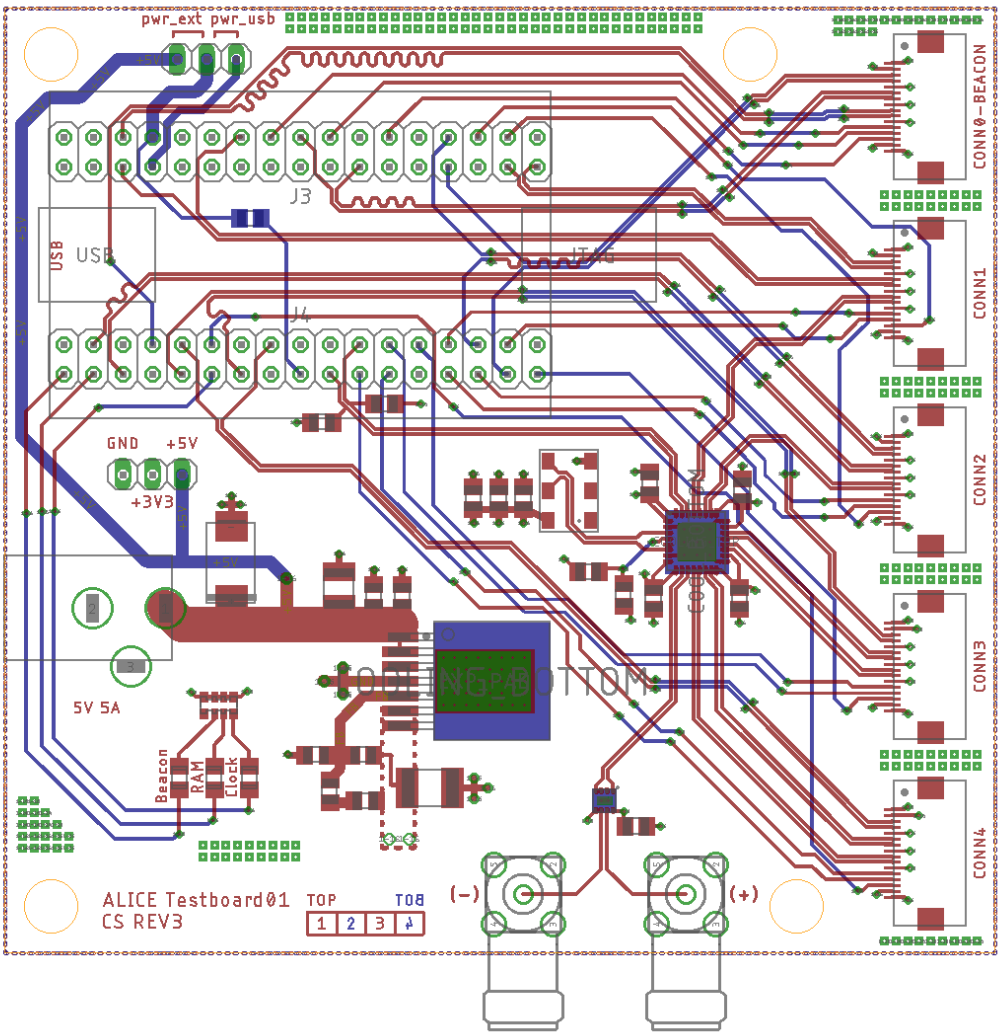


Figure A.2.: PCB board layout of the mainboard of the newly designed Alice testmodule.

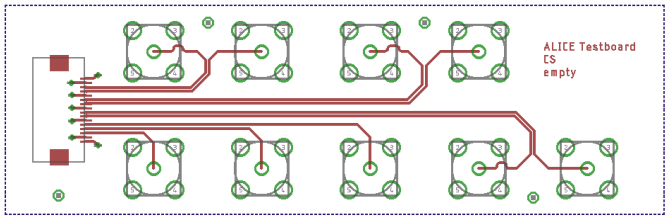
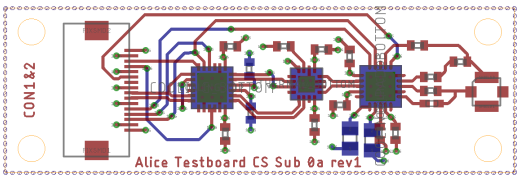
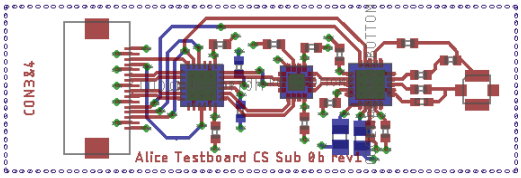
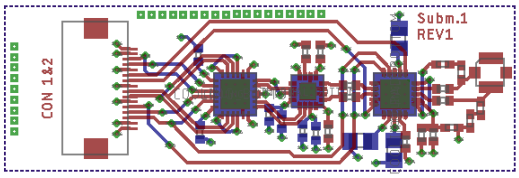
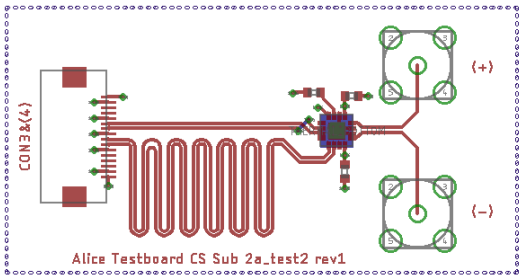
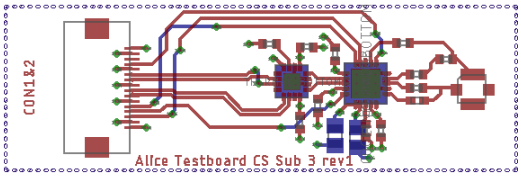
Subboard	PCB layout
empty	
0a	
0b	
1	
2a_test2	
3	

Table A.1.: PCB board layouts of the subboards (see subsection 5.2.2 and table 5.2). The boards indicated with "_test" have the same layout but some IC omitted and SMA connectors are attached at the end of the signal paths.

B. Additional Plots

On the following pages additional figures are placed that do not fit into the main part of this thesis.

Figure B.1 to figure B.4 are the results from the temperature dependence measurement of the Alice 2.0 waveguide chip for the waveguide circuit inputs depicted in the Poincaré sphere (see figure 4.5 for the results for the straight2 waveguide). One can see the rotation of the output states around the H/V axis of the Poincaré sphere.

Figure B.5 to figure B.9 shows the same measurement results, but for each of the input polarization states to the the varying output states are plotted and fits to the individual Stokes indices are done. The fits confirm, that the change of temperature only affects the Stokes parameters S_2 and S_3 whereas S_1 stays constant.

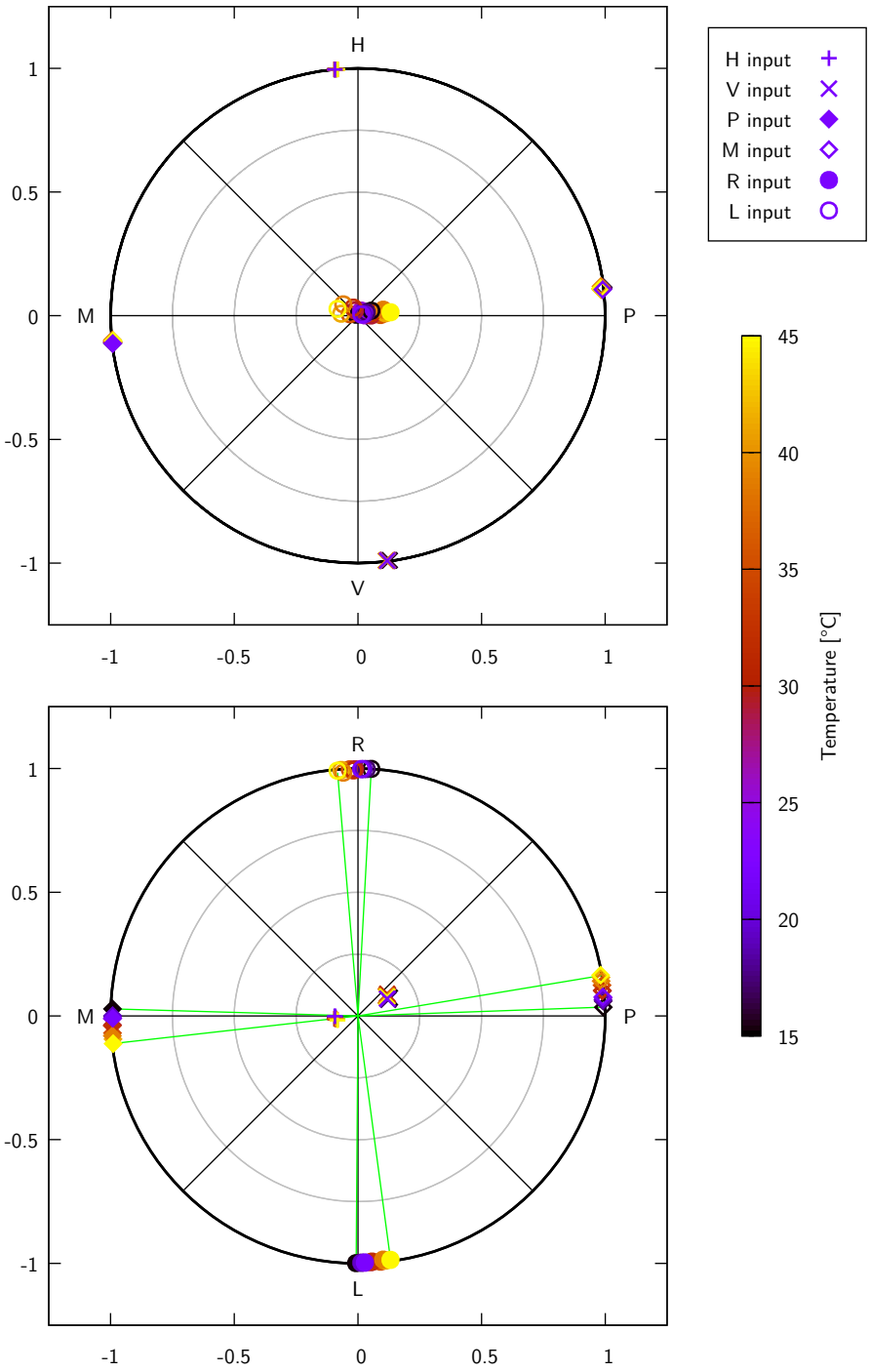


Figure B.1.: Change of output states for the notified input states coupled to input1

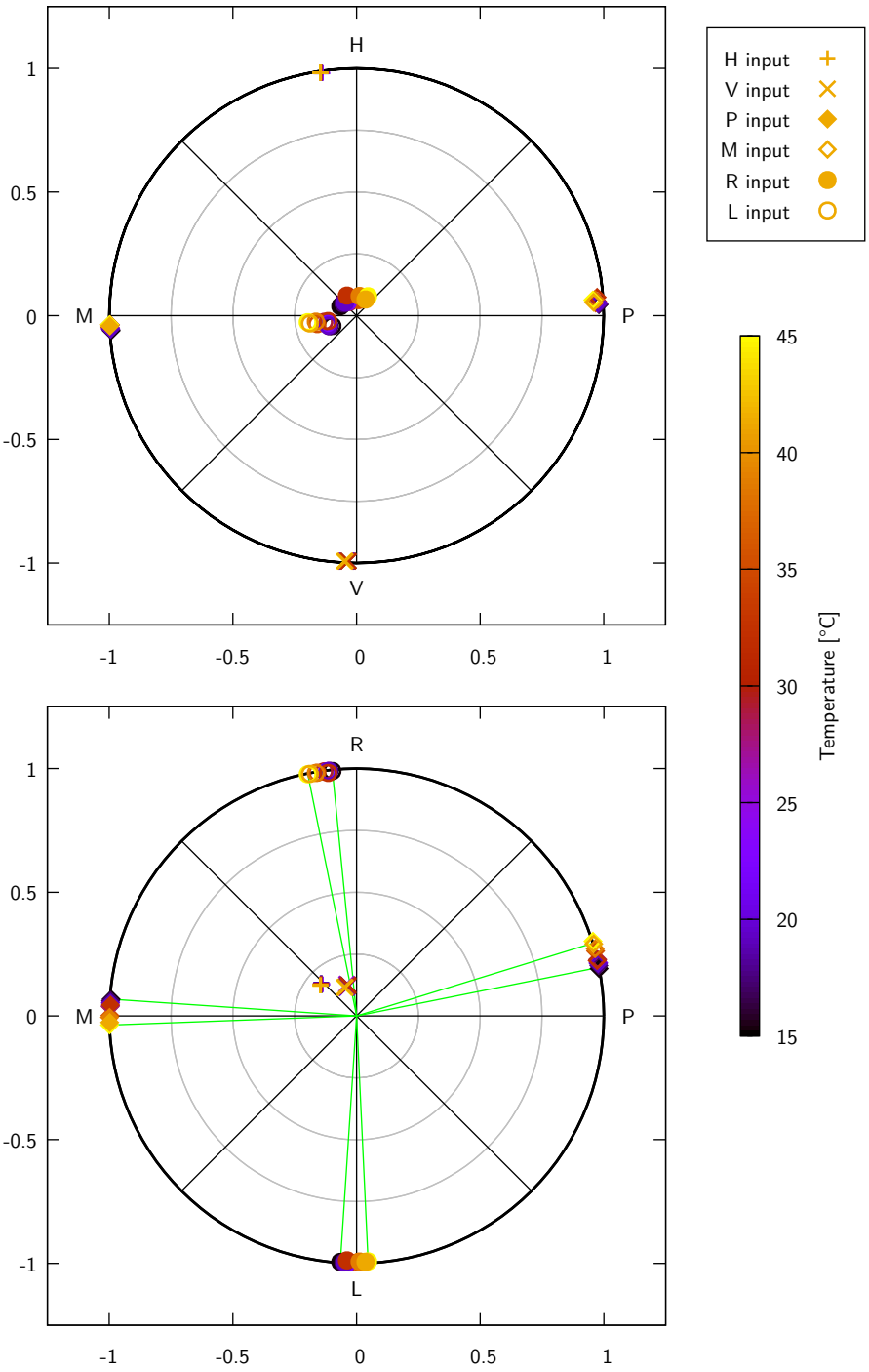


Figure B.2.: Change of output states for the notified input states coupled to input2

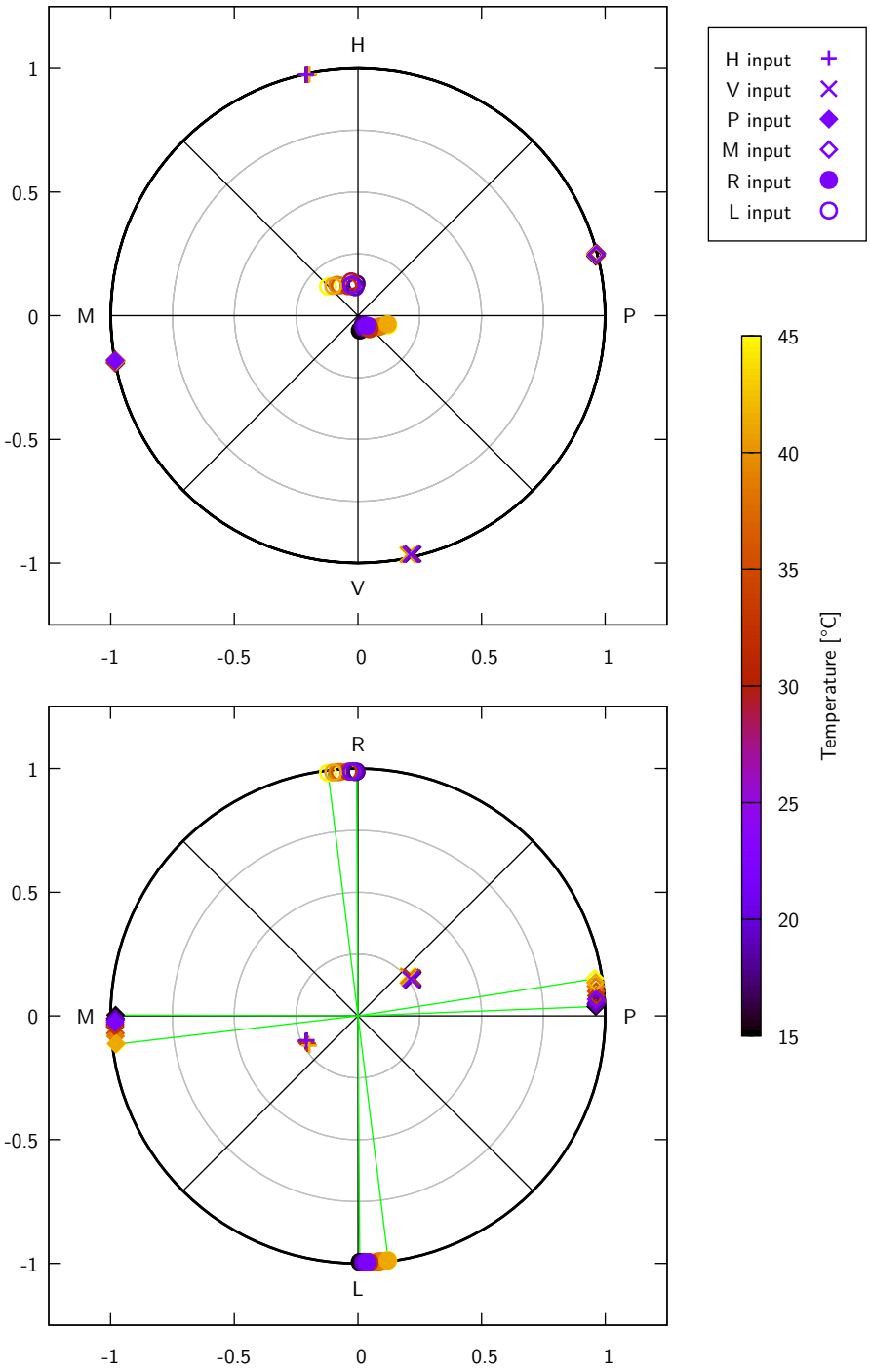


Figure B.3.: Change of output states for the notified input states coupled to input3

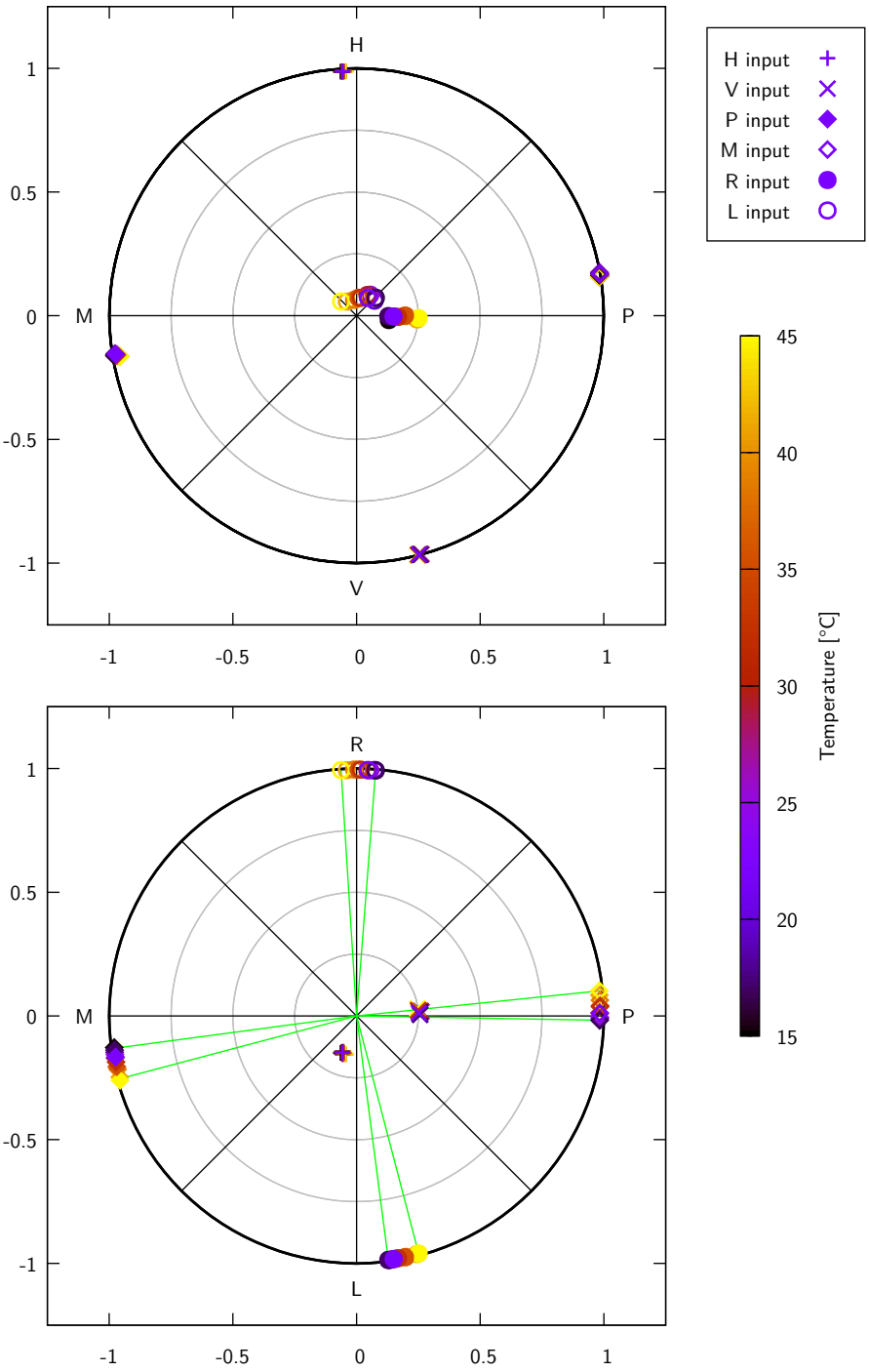


Figure B.4.: Change of output states for the notified input states coupled to input4

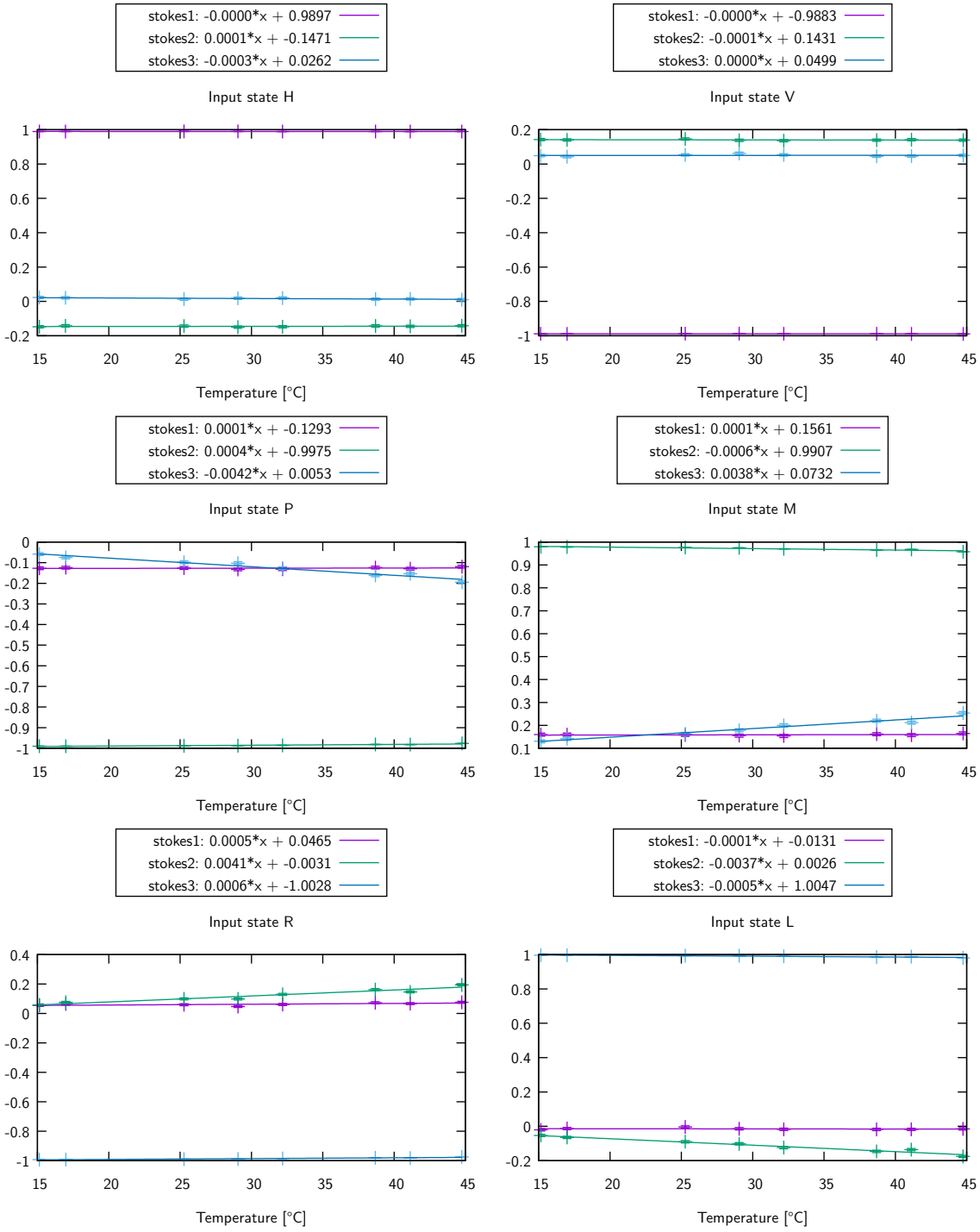


Figure B.5.: Change of output states over temperature of the straight2 waveguide with fits.

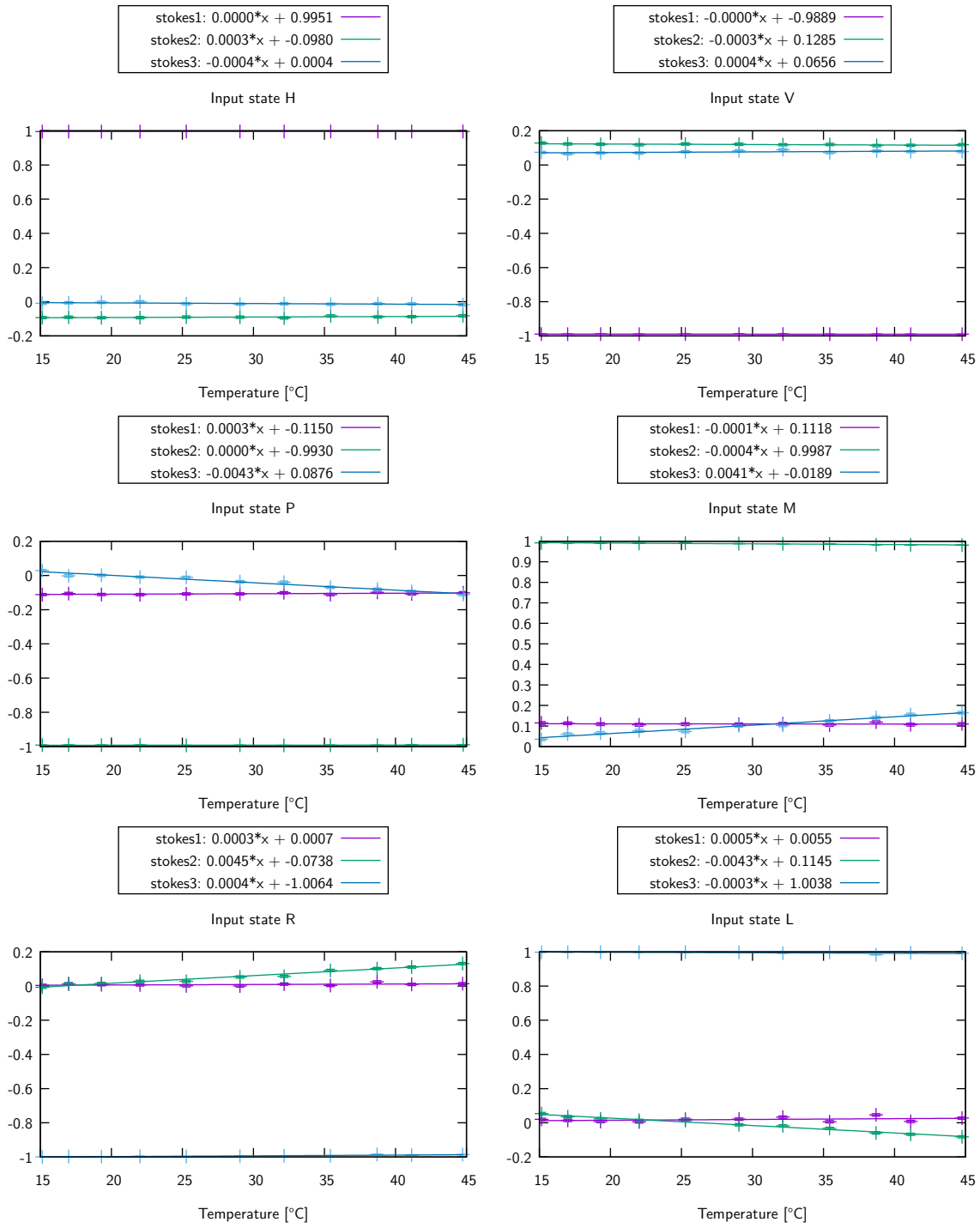


Figure B.6.: Change of output states over temperature when coupled to input1 with fits.

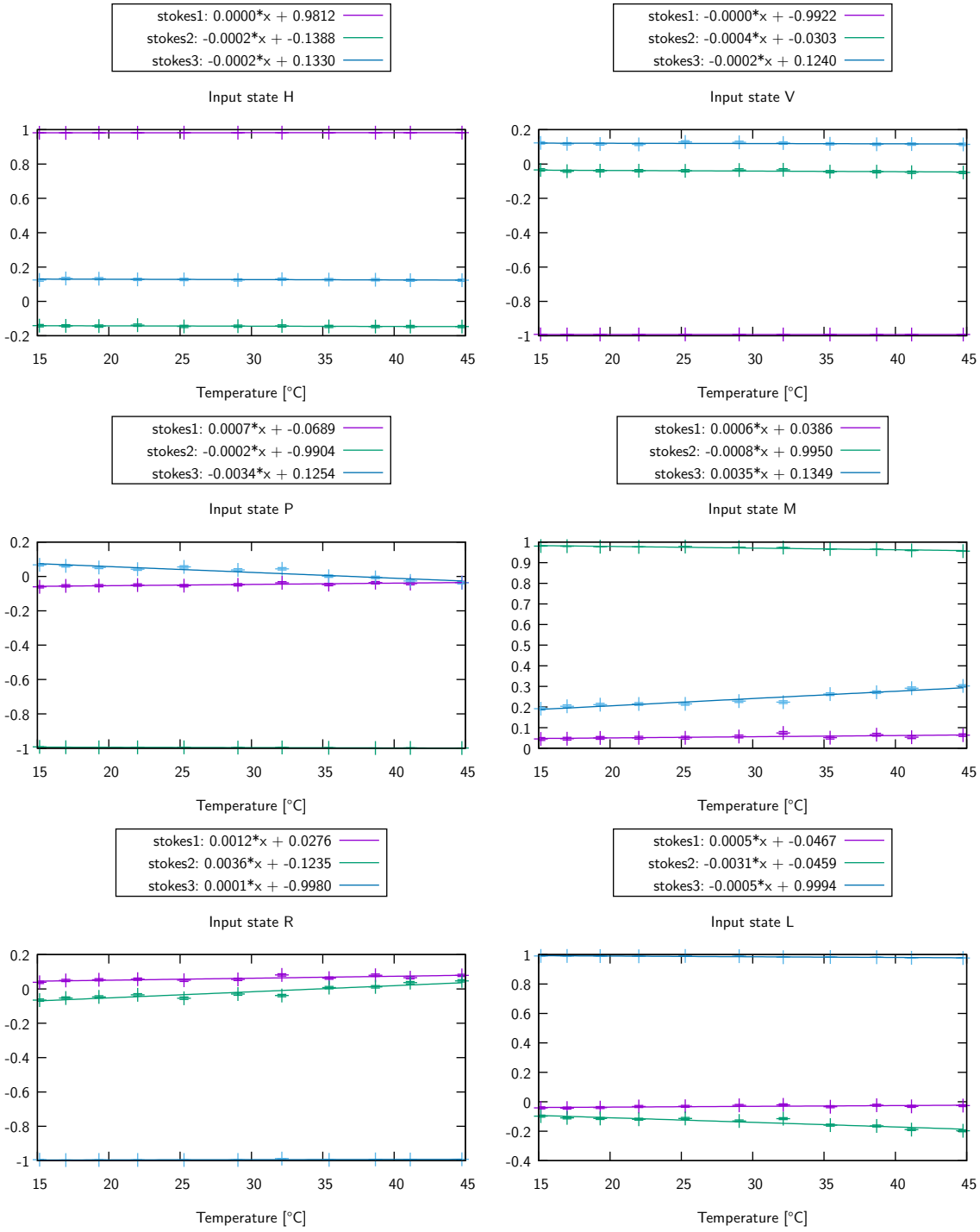


Figure B.7.: Change of output states over temperature when coupled to input2 with fits.

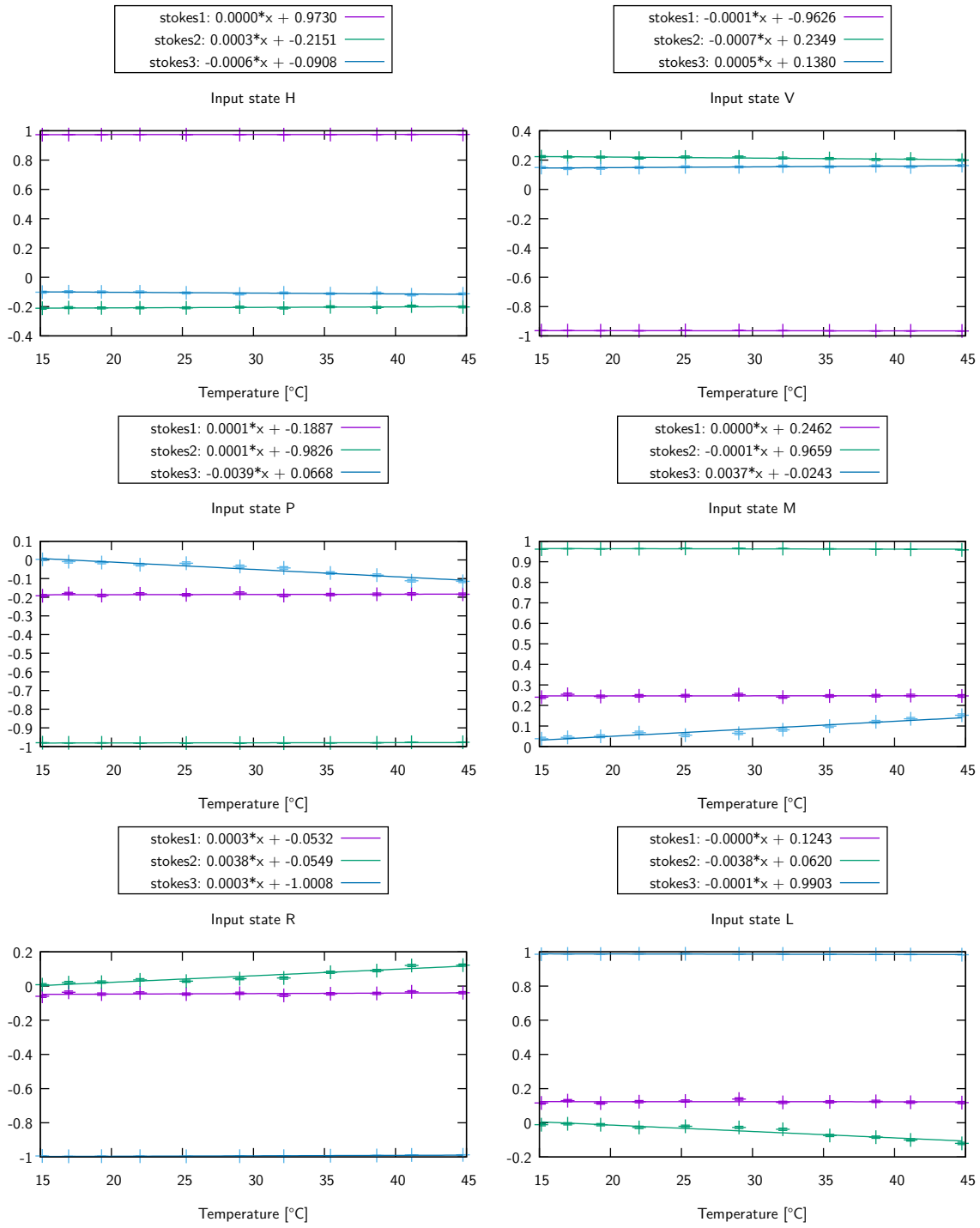


Figure B.8.: Change of output states over temperature when coupled to input3 with fits.

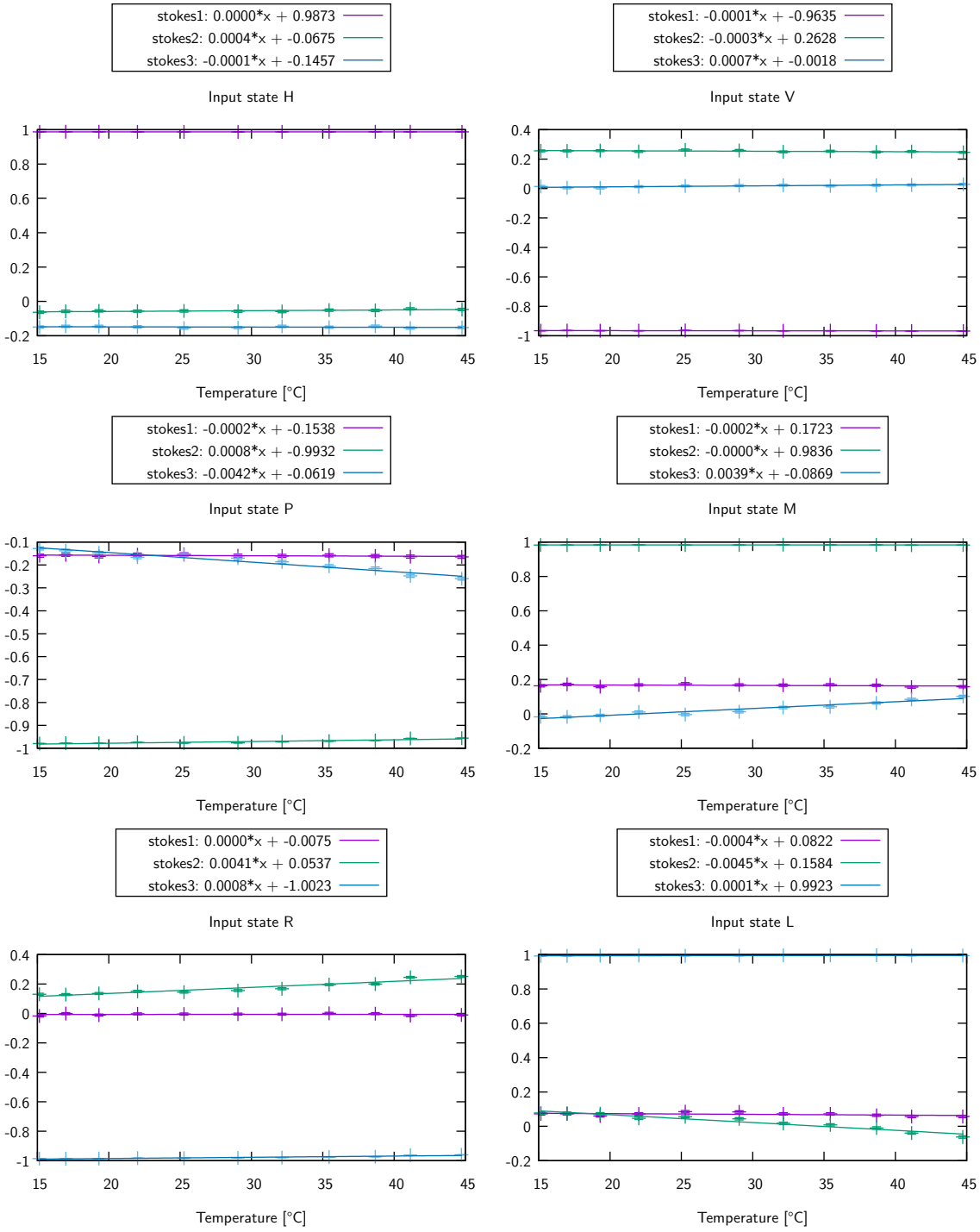


Figure B.9.: Change of output states over temperature when coupled to input4 with fits.

List of Figures

Bibliography

[1] *Internet usage statistics*. URL: http://www.internetworldstats.com/stats.htm (visited on 01/20/2018) (cit. on p. 1).

[2] C. Stöcker. *Stuxnet-Virus könnte tausend Uran-Zentrifugen zerstört haben*. Dec. 2010. URL: http://www.spiegel.de/netzwelt/netzpolitik/angriff-auf-irans-atomprogramm-stuxnet-virus-koennte-tausend-uran-zentrifugen-zerstoert-haben-a-736604.html (visited on 01/20/2018) (cit. on p. 1).

[3] D. Kushner. *The Real Story of Stuxnet*. Feb. 2013. URL: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/ (visited on 01/20/2018) (cit. on p. 1).

[4] E. Nakashima and J. Warrick. *Stuxnet was work of U.S. and Israeli experts, officials say*. 2012. URL: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.c6c1da6591a6 (visited on 01/20/2018) (cit. on p. 1).

[5] E. Biham and A. Shamir. "Differential Cryptanalysis of the Full 16-Round DES." *CRYPTO*. Ed. by E. F. Brickell. Vol. 740. Springer, 1992, p. 487. URL: http://dblp.uni-trier.de/db/conf/crypto/crypto92.html#BihamS92 (cit. on p. 1).

[6] G. S. Vernam. "Secret Signaling System". 1918. URL: http://www.cryptomuseum.com/crypto/files/us1310719.pdf (cit. on pp. 1, 6).

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. "Quantum cryptography". *Reviews of Modern Physics* 74 (2002), p. 145 (cit. on pp. 1, 8, 10).

[8] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*. Bangalore, 1984 (cit. on pp. 1, 10).

[9] W. K. Wootters and W. H. Zurek. "A single quantum cannot be cloned". *Nature* 299 (1982), p. 802 (cit. on pp. 2, 9).

[10] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. "Quantum Key Distribution over 67 km with a plug & play system" (2002) (cit. on p. 2).

[11] C. Gobby, Z. L. Yuan, and A. J. Shields. "Quantum key distribution over 122 km of standard telecom fiber". *Applied Physics Letters* 84 (2004) (cit. on p. 2).

[12] Z. L. Yuan and A. J. Shields. "Continuous operation of a one-way quantum key distribution system over installed telecom fibre". *Optics Express* 13 (2005), p. 660 (cit. on p. 2).

[13] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, et al. "Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding". *Phys. Rev. Lett.* 98 (1 Jan. 2007) (cit. on p. 2).

[14] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, et al. "Satellite-based entanglement distribution over 1200 kilometers". *Science* 356 (2017), p. 1140 (cit. on p. 2).

[15] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima. "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite". *Nature Photonics* (2017) (cit. on p. 2).

[16] G. Vest, M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, et al. "Design and Evaluation of a Handheld Quantum Key Distribution Sender module". *IEEE Journal on Selected Topics in Quantum Electronics* 21 (2014) (cit. on p. 2).

[17] G. Mélen. "Integrated Quantum Key Distribution Sender Unit for Hand-Held Platforms". Dissertation. Ludwig Maximilian University of Munich, 2016. URL: http://xqp.physik.uni-muenchen.de/publications/files/theses_phd/phd_melen.pdf (cit. on pp. 2, 19, 21–23, 26, 51).

[18] H. Delfs and H. Knebl. *Introduction to Cryptography*. 3rd ed. Springer-Verlag Berlin Heidelberg, 2007. ISBN: 978-3-540-49243-6 (cit. on pp. 3, 6).

[19] H. Reiser. *Vorlesung IT-Sicherheit, Kapitel 6: Kryptographische Grundlagen*. 2017. URL: http://www.nm.ifi.lmu.de/teaching/Vorlesungen/2017ws/itsec/_skript/itsec-k6-v12.0.pdf (cit. on p. 3).

[20] D. H. Hamer, G. Sullivan, and F. Weierud. "Enigma variations: An extended family of machines". *Cryptologia* 22 (1998), p. 211 (cit. on p. 4).

[21] T. Hoang and V. L. Nguyen. "An Efficient FPGA Implementation of the Advanced Encryption Standard Algorithm". *2012 IEEE RIVF International Conference on Computing Communication Technologies, Research, Innovation, and Vision for the Future*. Feb. 2012 (cit. on p. 5).

[22] O. Harrison and J. Waldron. "Practical symmetric key cryptography on modern graphics hardware". *USENIX Security Symposium* (2008), p. 195 (cit. on p. 5).

[23] A. Samiah, A. Aziz, and N. Ikram. "An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless St". *31st Annual International Computer Software and Applications Conference (COMPSAC 2007)*. Vol. 2. July 2007, p. 689 (cit. on p. 5).

[24] NIST. "Announcing the ADVANCED ENCRYPTION STANDARD". *Federal Information Processing Standards Publication* 197 (2001) (cit. on p. 5).

[25] L. R. Knudsen and M. J. Robshaw. *The Block Cipher Companion*. 2011. ISBN: 978-3-642-17341-7 (cit. on pp. 5, 7).

[26] *AES Development*. URL: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development (visited on 01/13/2018) (cit. on p. 5).

[27] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, et al. "Report on the development of the Advanced Encryption Standard (AES)". *Journal of Research of the National Institute of Standards and Technology* 106 (2001), p. 511 (cit. on p. 5).

[28] J. Daemon and V. Rijmen. *The Design of Rijndael. AES - The Advanced Encryption Standard*. Springer-Verlag Berlin Heidelberg, 2002. ISBN: 978-3-540-42580-9 (cit. on p. 5).

[29] A. Bogdanov, D. Khovratovich, and C. Rechberger. "Biclique cryptanalysis of the full AES". *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 7073 LNCS (2011), p. 344 (cit. on p. 5).

[30] G. S. Vernam. "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications". *Transactions of the American Institute of Electrical Engineers* XLV (Jan. 1926), p. 295 (cit. on p. 6).

[31] C. E. Shannon. "Communication Theory of Secrecy Systems.pdf". *Bell Labs Technical Journal* 28 (1949), p. 657 (cit. on p. 6).

[32] B. Schneider. *Applied Cryptography: protocols, algorithms, and source code in C*. Ed. by P. Sutherland. 2nd ed. John Wiley & Sons, Inc., 1996. ISBN: 0-471-11709-9 (cit. on p. 6).

[33] D. Kahn. *The Codebreakers. The Story of Secret Writing*. Simon and Schuster, 1996. ISBN: 978-0684831305 (cit. on p. 6).

[34] W. Diffie, W. Diffie, and M. E. Hellman. "New Directions in Cryptography". *IEEE Transactions on Information Theory* 22 (1976), p. 644 (cit. on p. 6).

[35] R. L. Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems". *Commun. ACM* 21 (Feb. 1978), p. 120 (cit. on p. 7).

[36] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" (1995), p. 124 (cit. on p. 7).

[37] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance". *Nature* 414 (2001), p. 883 (cit. on p. 7).

[38] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, et al. "Realization of a scalable Shor algorithm". *Science* 351 (2016), p. 1068 (cit. on p. 7).

[39] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. "The security of practical quantum key distribution". *Reviews of Modern Physics* 81 (2009), p. 1301 (cit. on p. 8).

[40] G. Brassard and L. Salvail. "Secret-Key Reconciliation by Public Discussion". *Advances in Cryptology — EUROCRYPT '93*. Ed. by T. Helleseth. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, p. 410 (cit. on p. 10).

[41] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson. "Fast, efficient error reconciliation for quantum cryptography". *Phys. Rev. A* 67 (5 May 2003) (cit. on p. 10).

[42] C. H. Bennett, G. Brassard, and J.-M. Robert. "Privacy Amplification by Public Discussion". *SIAM Journal on Computing* 17 (1988), p. 210 (cit. on p. 10).

[43] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. "Generalized privacy amplification". *IEEE Transactions on Information Theory* 41 (Nov. 1995), p. 1915 (cit. on p. 10).

[44] B. Huttner, N. Imoto, N. Gisin, and T. Mor. "Quantum cryptography with coherent states". *Phys. Rev. A* 51 (3 Mar. 1995), p. 1863 (cit. on p. 11).

[45] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. "Security of quantum key distribution with imperfect devices". *Quantum Information and Computation* 4 (2004), p. 325 (cit. on p. 12).

[46] W.-Y. Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". *Phys. Rev. Lett.* 91 (5 Aug. 2003) (cit. on p. 12).

[47] M. J. W. Hall. "Information Exclusion Principle for Complementary Observables". *Phys. Rev. Lett.* 74 (17 Apr. 1995), p. 3307 (cit. on p. 12).

[48] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. "Tight Finite-Key Analysis for Quantum Cryptography". *Nature Communications* 3 (2012), p. 634 (cit. on p. 12).

[49] V. Makarov, A. Anisimov, and J. Skaar. "Effects of detector efficiency mismatch on security of quantum cryptosystems". *Physical Review A - Atomic, Molecular, and Optical Physics* 78 (2008) (cit. on p. 13).

[50] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, et al. "Spatial mode side channels in free-space QKD implementations". *IEEE Journal on Selected Topics in Quantum Electronics* 21 (2015) (cit. on p. 13).

[51] E. Hecht. *Optics*. Addison Wesley, 2002. ISBN: 0-321-18878-0 (cit. on pp. 13, 15).

[52] S. N. Savenkov. "Jones and Mueller matrices: structure, symmetry relations and information content". *Light Scattering Reviews 4: Single Light Scattering and Radiative Transfer*. Ed. by A. A. Kokhanovsky. Berlin, Heidelberg: Springer, 2009, p. 71. ISBN: 978-3-540-74276-0 (cit. on p. 14).

[53] T. Vogl. “Mobile Free Space Quantum Key Distribution for short distance secure communication”. Master Thesis. Ludwig Maximilian University of Munich, 2016 (cit. on pp. 16, 19).

[54] M. Bass, ed. *Handbook of Optics II*. 2nd ed. McGraw-Hill Inc., 1995. ISBN: 0-07-047974-7 (cit. on p. 16).

[55] P. Freiwang. “Towards Hand-held Quantum Key Distribution”. Master’s Thesis. Ludwig Maximilian University of Munich, 2017 (cit. on pp. 19, 23, 31).

[56] J. Luhn. “Handheld Quantum Key Distribution”. Master’s Thesis. Ludwig Maximilian University of Munich, 2017. URL: http://xqp.physik.uni-muenchen.de/publications/files/theses_master/master_luhn.pdf (cit. on pp. 19, 28, 29).

[57] G. Mélen, T. Vogl, M. Rau, G. Corrielli, A. Crespi, R. Osellame, et al. “Integrated quantum key distribution sender unit for daily-life implementations”. 9762 (2016) (cit. on p. 20).

[58] R. Michalzik, ed. *VCSELs*. Springer Berlin Heidelberg, 2013. ISBN: 978-3-642-24985-3 (cit. on p. 21).

[59] K. Iga. “Surface-emitting laser-its birth and generation of new optoelectronics field”. *IEEE Journal of Selected Topics in Quantum Electronics* 6 (2000), p. 1201 (cit. on p. 21).

[60] G. Vest, P. Freiwang, J. Luhn, T. Vogl, M. Rau, W. Rosenfeld, et al. *Quantum key distribution with a hand-held sender unit*. In preparation (cit. on pp. 21, 26).

[61] G. Mélen, W. Rosenfeld, and H. Weinfurter. “Impact of the slit geometry on the performance of wire-grid polarisers”. *Optics Express* 23 (2015) (cit. on p. 21).

[62] K. M. Davis, K. Miura, N. Sugimoto, and K. Hirao. “Writing waveguides in glass with a femtosecond laser”. *Optics Letters* 21 (1996) (cit. on p. 22).

[63] R. Osellame, S. Taccheo, M. Marangoni, R. Ramponi, P. Laporta, D. Polli, et al. “Femtosecond writing of active optical waveguides with astigmatically shaped beams”. *Journal of the Optical Society of America B* 20 (2003) (cit. on p. 22).

[64] R. R. Gattass and E. Mazur. “Femtosecond laser micromachining in transparent materials”. *Nature Photonics* 2 (2008), p. 219 (cit. on p. 22).

[65] G. Della Valle, R. Osellame, and P. Laporta. “Micromachining of photonic devices by femtosecond laser pulses”. *Journal of Optics A: Pure and Applied Optics* 11 (2009) (cit. on p. 22).

[66] J. W. Chan, T. Huser, S. Risbud, and D. M. Krol. “Structural changes in fused silica after exposure to focused femtosecond laser pulses”. *Opt. Lett.* 26 (Nov. 2001), p. 1726 (cit. on p. 22).

[67] S.-H. Cho, H. Kumagai, and K. Midorikawa. "In situ observation of dynamics of plasma formation and refractive index modification in silica glasses excited by a femtosecond laser". *Optics Communications* 207 (2002), p. 243 (cit. on p. 22).

[68] M. Will, S. Nolte, B. N. Chichkov, and A. Tünnermann. "Optical properties of waveguides fabricated in fused silica by femtosecond laser pulses". *Appl. Opt.* 41 (July 2002), p. 4360 (cit. on p. 22).

[69] G. Cerullo, R. Osellame, S. Taccheo, M. Marangoni, D. Polli, R. Ramponi, et al. "Femtosecond micromachining of symmetric waveguides at 1.5 microm by astigmatic beam focusing." *Optics letters* 27 (2002), p. 1938 (cit. on p. 22).

[70] L. Sansoni, F. Sciarrino, G. Vallone, P. Mataloni, A. Crespi, R. Ramponi, et al. "Two-Particle Bosonic-Fermionic Quantum Walk via Integrated Photonics". *Phys. Rev. Lett.* 108 (1 Jan. 2012) (cit. on p. 22).

[71] M. Kögl. "Characterization of an optical chip for a miniaturized QKD sender unit". Bachelor Thesis. Ludwig-Maximilians-Universität, 2016 (cit. on p. 23).

[72] Group of Dr. R. Osellame. *Alice 2.0 report*. Milano, 2015 (cit. on p. 32).

[73] Corning. "Eagle 2000 Material Information". *Material Information* (2005) (cit. on p. 36).

[74] H. Johnson and M. Graham. *High-speed digital design: a handbook of black magic*. 1993. ISBN: 9780133957242 (cit. on pp. 43–45).

[75] Cypress Semiconductor Corporation. *AN-1106: LVDS vs . Low Voltage Differential Signaling*. 2001. URL: http://www.cypress.com/file/74061/download (cit. on p. 44).

[76] C. Sterzik. *Suggestions for High-Speed Differential Connections*. 2004 (cit. on p. 44).

[77] Texas Instruments. *SPRAAR7G - High-Speed Interface Layout Guidelines*. 2017. URL: http://e2e.ti.com/cfs-filesystemfile.ashx/__key/CommunityServer-Discussions-Components-Files/138/7571.High-Speed-Layout-Guidelines.pdf (cit. on pp. 44, 46).

[78] Texas Instruments. *Considerations for PCB Layout and Impedance Matching Design in Optical Modules*. 2011 (cit. on p. 44).

[79] *IPC-2251 - Design Guide for the Packaging of High Speed Electronic Circuits*. 2003 (cit. on p. 45).

[80] H. Kaup. "Characteristics of Microstrip Transmission Lines". *IEEE Transactions on Electronic Computers* EC-16 (1967), p. 185 (cit. on p. 45).

[81] PCBway. *PCB cooling*. URL: https://www.pcbway.com/blog/Engineering_Technical/PCB_cooling.html (visited on 01/10/2018) (cit. on p. 47).

[82] Texas Instruments. *AN-903 A Comparison of Differential Termination Techniques*. 2013 (cit. on p. 49).

[83] E. Hammerstad and O. Jensen. “Accurate Models for Microstrip Computer-Aided Design”. *1980 IEEE MTT-S International Microwave symposium Digest*. May 1980, p. 407 (cit. on p. 51).

[84] S. Frick. “Quantum Key Distribution with Integrated Optical Circuits”. Master Thesis. Ludwig-Maximilians-Universität, 2013 (cit. on p. 51).

[85] J. Li, Z. Zheng, M. Liu, and S. Wu. “Large Dynamic Range Accurate Digitally Programmable Delay Line with 250-ps Resolution”. *2006 8th international Conference on Signal Processing*. Vol. 1. 2006 (cit. on p. 52).

[86] Y.-y. Chen, J.-l. Huang, and T. Kuo. “Implementation of Programmable Delay Lines on Off-the-Shelf FPGAs”. *AUTOTESTCON* (2013) (cit. on p. 52).

[87] *Drying/Tempering PCB*. URL: https://www.multi-circuit-boards.eu/en/pcb-design-aid/surface/drying.html (visited on 01/10/2018) (cit. on p. 52).

[88] *IPC/JEDEC J-STD-020D.1 Moisture/Reflow Sensitivity Classification for Nonhermetic Solid State SMDs*. 2008 (cit. on p. 52).

[89] *IPC/JEDEC J-STD-005A Requirements for Soldering Pastes*. 2011 (cit. on p. 52).

[90] *Oscilloscope Fundamentals*. 2012. URL: https://www.ethz.ch/content/dam/ethz/special-interest/chab/chab-dept/research/documents/LPC/oscilloscopefundamentals.pdf (cit. on p. 53).

Danksagung

Abschließend möchte ich mich noch bei all denen bedanken, durch die das Gelingen dieser Arbeit ermöglicht wurde.

Als erstes möchte ich mich bei Prof. Dr. Harald Weinfurter für die Möglichkeit bedanken meine Masterarbeit in diesem spannenden Forschungsgebiet gemacht haben zu dürfen.

Besonderer Dank gilt auch meinem Schreibtischnachbarn Peter für die Zusammenarbeit und das angenehme Klima.

Dr. Wenjamin Rosenfeld für seine Geduld und Hilfe bei allen Fragen und auch allen anderen aus der Gruppe für die große Hilfsbereitschaft die sogar soweit geht, dass PINs abgeschliffen werden wenn bei EAGLE was schiefläuft. Vielen Dank auch Wenjamin, Peter und Gwen für's Korrekturlesen.

Dank gilt auch meinen beiden Brüdern die mich auch nervig ertragen und ganz besonders danken möchte ich meinen Eltern die mich immer unterstützen und mir große Vorbilder sind.

Erklärung

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

München, den 24. Januar 2018

Clemens Sonnleitner