
Field Test of a Quantum Key Distribution System

Feldtest eines Systems zum Quantenschlüsselaustausch

Zur Erlangung des Grades eines Doktors der Naturwissenschaften (Dr. rer. nat.)

Genehmigte Dissertation von Oleg Nikiforov aus Rostow

Tag der Einreichung: 19.12.2022, Tag der Prüfung: 13.02.2023

1. Gutachten: Prof. Dr. Thomas Walther

2. Gutachten: Prof. Dr. Gerhard Birkel

Darmstadt, Technische Universität Darmstadt



TECHNISCHE
UNIVERSITÄT
DARMSTADT

Fachbereich Physik

Institut für Angewandte
Optik

Laser und Quantenoptik

Field Test of a Quantum Key Distribution System
Feldtest eines Systems zum Quantenschlüsselaustausch

Accepted doctoral thesis by Oleg Nikiforov

Date of submission: 19.12.2022

Date of thesis defense: 13.02.2023

Darmstadt, Technische Universität Darmstadt

Bitte zitieren Sie dieses Dokument als:

URN: urn:nbn:de:tuda-tuprints-236344

URL: <http://tuprints.ulb.tu-darmstadt.de/23634>

Jahr der Veröffentlichung auf TUprints: 2024

Dieses Dokument wird bereitgestellt von tuprints,

E-Publishing-Service der TU Darmstadt

<http://tuprints.ulb.tu-darmstadt.de>

tuprints@ulb.tu-darmstadt.de

CC BY 4.0

Zusammenfassung

Die zunehmende Rechenleistung von klassischen und Quantencomputern gefährdet die bestehende Public-Key-Kryptographie. Die Quantenschlüsselverteilung (Englisch: Quantum Key Distribution; QKD) ist eine der möglichen Lösungen für dieses Problem. In den vergangenen Jahrzehnten entstand eine Vielfalt von QKD Protokollen, erste Unternehmen für Quantenkommunikation wurden gegründet und erste Länder begannen QKD in ihre Kommunikationsinfrastruktur zu integrieren. Die hohen Kosten und das Fehlen von QKD-Netzwerken ohne sogenannte Trusted Nodes erschweren jedoch die Verbreitung dieser Technologie.

Die vorliegende Arbeit beschreibt den Aufbau und die Leistungsfähigkeit eines Zwei-Parteien-QKD-Systems, das eine Variante des Bennet-Brassard-Mermin 92-Protokolls mit Time-Bin-Kodierung ist. Es wurde in einer realen Telekommunikationsumgebung in einem typischen Betriebsraum im Network Innovation Center der Deutschen Telekom Technik GmbH getestet. Dieses System ist ein Meilenstein für ein sternförmiges QKD-Netzwerk, dessen zentral gelegene Quelle die Qubits auf mehrere identisch aufgebaute weiter entfernte Empfänger verteilt.

Die größte Herausforderung für die Implementierung solcher Netzwerke ist der Aufbau und der Betrieb identischer faserbasierter Michelson-Interferometer, deren Armlängendifferenzen bis auf wenige Mikrometer genau übereinstimmen müssen. Während der aktuellen Arbeit wurde dafür eine passende Methode entwickelt. Sie besteht aus zwei Schritten: Präzises Vorschneiden der Bauteile für das Interferometer und eine mechanische Dehnung der Faser im fertigen Interferometer um die restlichen Ungenauigkeiten auszugleichen. Diese Methode erlaubt den Bau beliebig vieler Interferometer mit identischem Weglängenunterschied.

Das gewählte Protokoll ist sehr sensitiv gegenüber Phaseninstabilitäten. Daher muss die Phasendrift kompensiert werden, die durch die Temperaturdrift entsteht. Das entwickelte System zur Temperaturstabilisierung erreicht eine Langzeitstabilität von 3 mK pro Tag und fungiert gleichzeitig als ein Stellglied für die Phase mit einer minimalen Auflösung von 0.011π . Damit wird die Komplexität des Aufbaus vereinfacht im Vergleich zu anderen Implementierungen dieses Protokolls.

Nachdem das gesamte System aufgebaut wurde, konnte im Feldversuch ein stabiler Quantenschlüsselaustausch über eine Strecke von ca. 27 km Länge erreicht werden. Dabei waren alle Elemente des Systems in einem typischen Telekom-Betriebsraum platziert. Dieses Experiment war einer der ersten erfolgreichen Feldtests eines QKD-Systems in Deutschland. Es wurde eine mittlere Rate des gesiebten Schlüssels von 200 bit/s mit einer Quantenbitfehlerrate von ca. 3 % in einem fünfstündigen Austausch erreicht.

Abstract

Increasing computational power of classical and quantum computers endangers the existing public key cryptography. Quantum key distribution (QKD) is one of the solutions for this problem. In the past decades a zoo of protocols was suggested and implemented, first companies for quantum communication were founded and first countries started to integrate QKD into their communication infrastructure. However, the high costs and the lack of genuine QKD networks without trusted nodes make it difficult for the technology to gain widespread acceptance.

The present work describes the setup and the performance of a two-party QKD system, using a time-bin encoding variant of the Bennet-Brassard-Mermin 92 protocol in a real-world telecommunication environment inside a typical operating room at the Network Innovation Center of Deutsche Telekom Technik GmbH. This system is a milestone for a star-shaped QKD network, consisting of a centrally located qubit source, distributing the qubits to several identical receivers located elsewhere.

The main challenge for building such networks is the assembly and operation of identical fiber-based Michelson interferometers, whose arm-length differences must match within the micrometer range. During this work a suitable method was developed. It consists of two steps: a precise pre-cut of interferometer components and mechanical stretching of the fiber in one interferometer arm, until the residual mismatch is compensated. This method allows for assembly of arbitrary many identical interferometers for many-party QKD systems.

The chosen protocol is very sensitive to phase instabilities. Any phase drifts caused by temperature drifts must then be compensated. The developed temperature stabilization system provides a long-term stability of 3 mK per day and is at the same time able to adjust interferometer phases with a resolution down to 0.011π , reducing the complexity of the setup compared to other implementations of this protocol.

After the entire system was implemented, the field test achieved a stable quantum key distribution over a deployed link of approx. 27 km length, while all elements of the system were placed in a typical telecom operating room. This experiment was one of the first successful field tests of a QKD system in Germany. In a five hour long key exchange a mean sifted key rate of 200 bit/s with a quantum bit error rate of approx. 3% was achieved.

Contents

1. Introduction	1
2. Introduction to quantum key distribution	3
2.1. Quantum key distribution	4
2.1.1. The idea of quantum key distribution	4
2.1.2. Protocol classification	6
2.1.3. Security of quantum key distribution	6
2.1.4. Limitations of quantum key distribution systems	7
2.1.5. Quantum networks and commercialization	7
2.2. Time-bin encoding	8
2.2.1. Protocol scheme	9
2.2.2. Fiber-based Michelson interferometers	11
2.2.3. Time-multiplexing of time-bin encoding protocol	12
2.3. Generation of energy-time entangled photon pairs	13
2.3.1. Spontaneous parametric down-conversion	13
2.3.2. Efficiency measurement of the spontaneous parametric down-conversion in a crystal	14
2.4. Optical fibers and their application in communication	17
2.4.1. Optical glass fibers	17
2.4.2. Attenuation profile	18
2.4.3. Polarization of light within the glass fiber	19
2.4.4. Dispersion and non-linear effects	21
2.4.5. Fiber pigtailed components and fiber connections	21
2.4.6. Mechanical properties	23
2.5. White light interferometry for length measurements	25
3. Entangled-photon-pair source	29
3.1. Pulsed laser source	31
3.1.1. Seed laser	31
3.1.2. Pulse generation	33

3.1.3. Erbium-doped fiber amplifier	35
3.1.4. Fiber-coupled frequency conversion module	44
3.2. Spontaneous parametric down-conversion	51
4. Receiver modules	55
4.1. Receiver setup overview	57
4.2. Temperature stabilization and phase control for interferometers	58
4.2.1. Temperature stabilized container for interferometer	60
4.2.2. Setup for mechanical fiber length correction	62
4.2.3. Electronic system for temperature stabilization	62
4.3. Interferometer construction	64
4.3.1. Setup for precise fiber cutting	65
4.3.2. Interferometer assembly	67
4.3.3. Interferometer characterization	70
4.4. Photon detection and evaluation	71
4.4.1. Time tagging modules	71
4.4.2. Experiment control system	72
4.4.3. Control software for the quantum key distribution	74
4.4.4. Measurement procedure	77
5. Operation and performance of the QKD system	79
5.1. System in the laboratory environment	79
5.2. Deployed fiber	80
5.3. Performance of the receiver	82
5.3.1. Environment of the operation site	82
5.3.2. Long-term stability of the interferometers	84
5.3.3. Temperature dependence of interferometers phase	87
5.3.4. Interferometer length calibration	88
5.4. Quantum key distribution experiment	88
6. Conclusion and outlook	91
A. Power stabilization scheme for the erbium-doped fiber amplifier	95
B. Dual channel TEC and LD current controller	97
B.1. Introduction	97
B.2. Operation instructions	98
B.2.1. Before launch	98



- B.2.2. Operation 99
- B.3. Performance 101
- B.4. General functional scheme 102
- B.5. Rack 104
 - B.5.1. Main printed circuit board 105
 - B.5.2. Additional circuit board 106
- B.6. Cables and cable management 115
- B.7. Software 115
 - B.7.1. Arduino firmware 115
 - B.7.2. Python script 116
- B.8. Improvement suggestions and unresolved issues 118
- B.9. Combined LD source and TEC controller 119

- Bibliography** **134**
- List of figures** **140**
- List of tables** **141**
- Abbreviations** **143**
- List of publications** **147**

1. Introduction

No one shall be subjected to arbitrary interference with his privacy, family, home or *correspondence*, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Universal Declaration of Human Rights, Article 12 [1]

The speed of technological progress has increased dramatically in recent decades thanks to the widespread use of digital systems and new computing methods. This development culminated in the invention of the first quantum computers. Already their first calculations give mankind an idea of the boost they will provide to science and technology when further developed.

The growing computational capability of quantum, but also classical computers and the advancing digitalization of all areas of life are accompanied by an increasing danger for the confidentiality of communication, the storage of sensitive personal data and intellectual property. Most existing complexity-based public key encryption methods need to be strengthened or replaced. Quantum key distribution (QKD) - a method for secure key exchange based on the laws of quantum physics - offers a solution to this problem.

This promising method has received much attention over the last 25 years. The rapid development of quantum technologies and the increasing need for secure communication methods led this method to the threshold of commercial success. To make the final breakthrough, QKD needs the recognition of national IT security agencies, and a cost-to-benefit increase for the hardware. This is achieved by developing new and more efficient protocols or by cost reduction for the existing ones.

Also the telecommunication service providers closely follow the developments of QKD technology, or even take part in research projects. One of such projects is the innovation project "*Quantensichere Netze*" between Deutsche Telekom Technik GmbH and the Laser and Quantum Optics research group (LQO) at Technical University of Darmstadt, that was started during the work on this thesis. The scope of this project is a field test of a QKD system in a real-world telecommunication environment inside of a typical operation

room and using a real deployed fiber for the key exchange. The QKD system for this field test was also developed during the work on this thesis at LQO within the Collaborative Research Center *CROSSING: Cryptography-based security solutions* (Funded by the German Research Foundation).

Thus, the main aim of this work is the planning and assembly of a two-party QKD system, suitable for an upgrade into a several-party QKD network, and a subsequent field test of it at a facility of Deutsche Telekom. The main challenge of the project was the development of a straightforward method for assembly and operation of identical Michelson interferometers. They are necessary for the chosen time-bin entanglement protocol and must be suitable for work in the environment of a typical operating room of a telecommunication provider. For a potential N -party QKD network it is necessary to build and operate $N + 1$ of such identical interferometers.

The present work characterizes the implemented setup and describes the results obtained during the field test. The necessary theoretical prerequisites and the chosen protocol are presented in chapter 2. The implemented qubit source is described in chapter 3 and the qubit receiver in chapter 4. Subsequently, the field test is described in chapter 5, followed by a summary, discussion and outlook in chapter 6. Essential technical descriptions of important electronic parts are attached in appendix A (fiber amplifier stabilization system) and appendix B (temperature stabilization system for the interferometers).

2. Introduction to quantum key distribution

Modern highly developed cyber systems become increasingly complicated, offering a big attack surface for potential attackers. One of the targets is the confidentiality of communication: once it is broken, sensitive data, i.e. the login data for online banking, might be extracted and misused.

Many modern communication systems use public key encryption methods, like *Diffie-Hellmann* [2] or *Rivest-Shamir-Adleman* [3] encryption. Such asymmetric protocols require one publicly accessible key for the message encryption and a private key for its decryption, that is kept secret by the receiver. These methods are called complexity-based and were considered safe at the time – with a sufficiently long key – due to the lack of methods for efficient extraction of the private key from the public [4]. The underlying mathematical problems for those protocols are the prime factorization of discrete logarithms [5] and prime factorization of large numbers [6]. While no algorithms solving these problems in polynomial time are developed for classical computers yet, for quantum computers it exists already for more than two decades. Thus, a fast technical advance of quantum computers will unavoidably make the modern public key infrastructure obsolete once they are capable of executing *Shor's algorithm* to calculate private keys from the public keys for sufficiently long key lengths [7]. The solution for this problem must be found before it becomes critical.

One of the solutions for this problem is the search for harder mathematical problems, where quantum computers do not offer any computational advantage - the so-called *Postquantum cryptography* [8, 9]. The research on this topic is still ongoing, and first standardization attempts are being carried out by responsible organizations, like the National Institute of Standards and Technology and Deutsches Institut für Normung. Those protocols are promising, however, any estimation of the hardness of any complexity-based algorithm is not a final proof for its security.

The opposite of complexity-based protocols are information-theoretic secure protocols. The only known secure encryption protocol is the Vernam One-Time-Pad (OTP). It was suggested in 1926 [10], but its true importance was first recognised by Claude E. Shannon in 1949 [11]. This symmetric protocol utilizes a key that is used for both encryption and

decryption of the messages and must fulfill three conditions: the key is the same length as the message, the key is chosen randomly and it is used only once.

The OTP transforms the problem of encryption security into the problem of secure key distribution between the distant communicating parties. And quantum physics provides a solution: the quantum key distribution (QKD).

In the present chapter the theoretical prerequisites for QKD are given: the general idea of QKD (section 2.1), the implemented protocol (section 2.2), photon pair generation (section 2.3) required for the QKD and the description of optical fibers required for the implemented experiment (section 2.4).

2.1. Quantum key distribution

2.1.1. The idea of quantum key distribution

The general idea of QKD exploits quantum mechanical phenomena for key distribution in such a way that any potential eavesdropper always reveals himself trying to obtain the secret key. This is possible, due to a combination of several reasons: existence of conjugate observables, the no-cloning theorem and a state change of a quantum object due to a measurement on it. Conjugate observables in quantum mechanics are observables, fulfilling the Heisenberg uncertainty relation: they cannot be measured simultaneously and their operators do not commute, i.e. for the position and the momentum of a particle holds $\Delta x \Delta p \geq \hbar/2$. Further, the no-cloning theorem states the impossibility to copy an unknown state of a quantum object without disturbing it [12]. And according to one of the postulates of quantum mechanics, any measurement on a quantum object, in general transforms its state to the eigenstate corresponding to the measured eigenvalue [13].

Since the first QKD protocol Bennet-Brassard 84 (BB84) was suggested in 1984 [14], an entire zoo of other protocols was developed and analyzed [15–18]. Many of them can be described by the following generic algorithm. The description contains directly the case of an eavesdropper. Without him the key exchange works in the same way, the corresponding steps are just skipped. In general, Alice and Bob are two distant parties, desiring to communicate confidentially. Thus, they exchange symmetric keys using the QKD as follows:

1. Alice and Bob agree on at least two conjugated bases or observables and two eigenstates that can be prepared within the chosen basis, that correspond to bits "0" and "1". This choice defines the applied QKD protocol.
2. Alice chooses randomly one of the bases and a bit "0" or "1".

-
3. Alice prepares the photon in the state corresponding to the chosen bit and sends this *quantum bit (qubit)* to Bob.
 4. Eavesdropper Eve interferes and wants to determine the state of the qubit. She must guess the basis and she is wrong in half of all cases.
 5. Eve measures the state of the qubit within the chosen basis.
 6. Eve prepares a replacement for the detected qubit in the detected state of the basis she guessed and relays it to Bob. In half of the cases, the state of the replacement qubit does not match to the state of the original qubit.
 7. Bob randomly chooses a basis and measures the state of the received qubit.
 8. *Key sifting*: Alice and Bob publicly announce the bases they used and compare them. If the bases are not matching, they discard that particular event. Otherwise they keep all the bits that then add up to the *sifted key*. The qubits wrongly prepared by Eve generate errors within the sifted key.
 9. *Error correction*: After a certain amount of qubits were exchanged, Alice and Bob estimate the *quantum bit error rate (QBER)*, for example by publicly comparing parts of their sifted keys and calculating the ratio of error number to sample length. If the error exceeds a certain threshold (see section 2.1.3), the key is considered compromised and the key exchange starts over from step 2. Otherwise, error correcting algorithms are applied to remove any errors, that may be present due to various reasons.
 10. *Privacy amplification*: During the error correction additional information about the key is exchanged, so Eve's knowledge about the key grows. Thus, privacy amplification algorithms are applied, again reducing Eve's information. Both processes, error correction and privacy amplification shorten the key length.
 11. Finally, the *secret key* may be forwarded to some key management system, that is responsible for key storage, key forwarding and providing it to cryptographic applications.

Summarized, the potential adversary generally disturbs the state of each qubit. She tries to eavesdrop but cannot remain undetected, and she is not able to detect the entire information correctly, since she must choose between two conjugate bases.

2.1.2. Protocol classification

The QKD protocols are united by the use of quantum properties of the qubits. Apart from this, they vary strongly and can be divided into classes by different characteristics. Considering the type of observable and measurement outcomes, *discrete (DV)* or *continuous variable (CV)* protocols may be distinguished. The conjugated bases of DV protocols might be the non-orthogonal polarization bases [14, 19], qubit phase [20] or phase and time [21, 22]. In CV protocols the conjugated observables are the quadratures of the weak coherent pulses, that are used as qubits [23].

Considering the type of the state preparation, the protocols may be *prepare-and-measure* or *entanglement-based*. The former one is described in the generic protocol in section 2.1.1, where each qubit is prepared by Alice in a predetermined state individually and Bob possesses a receiver and measures the transmitted states. In the entanglement-based configuration, the source is typically not a part of any communication party and distributes entangled photons to Alice and Bob, possessing identical receivers. Here, the key does not exist before the qubit measurement, since the decision for the measurement basis is made at a later time, when the photon arrives at both receivers.

2.1.3. Security of quantum key distribution

The security of each QKD protocol must be considered individually. Typically, the security of an idealized protocol is much easier to prove than that with realistic devices. Imperfections of sources, quantum links and single photon detectors must be taken into account [16]. The security proofs for the most used protocols are still an on-going task and it constitutes a large research field.

Typically, security proofs consider adversaries to be only limited by the laws of quantum physics. Also, any noise constituting in a QBER even without the presence of an adversary is considered to be caused by him. To simplify the task of the security proof, several attack strategies are distinguished: *individual*, *joint* and *collective*. One example of an individual attack, aimed at individual qubits is the *intercept-resend attack*, that was described above in the description of a generic protocol in section 2.1.1. Collective attacks consider individual attacks on several qubits simultaneously, and the joint attacks are the most general class of attacks on qubits without any assumptions on the scenario [24].

The security proofs deliver critical QBER threshold values, that are used to determine, if a QKD session delivered a secure key. For example, for the BB84 protocol it is given by $\text{QBER}_{\text{crit}} = 11\%$ [25]. More details on the QKD security topic can be found in ref. [26].

While such formal proofs do not take into account the setup features, realistic devices inevitably open up side-channels: weak points of the experimental hardware, that may

be used for an attack. For example, the famous detector blinding attack on a QKD implementation, exploits the properties of the setup components in an untypical way [27].

For example, during the presented work in a collaboration with Alexandra Weber from the research group Modeling and Analysis of Information Systems at Technical University of Darmstadt, a CPU cache side channel in an implementation of some postprocessing algorithms was detected and mitigated [28]. This mitigated issue allowed an adversary to perform an indirect readout of the sifted key from the processor's cache during the error correction, exploiting the processor's access time to this cache.

2.1.4. Limitations of quantum key distribution systems

Implementations of QKD devices achieve different rates at different distances, depending on the given protocol and the type of the quantum channel. Glass fibers, with all their flexibility, possess a non-negligible attenuation coefficient α (see section 2.4) leading to an exponential decay of the intensity propagating through it. The rate is then $R \propto e^{-\alpha L}$, with the link length L . Free-space systems on the other hand are diffraction limited and the key rate is proportional to $1/L^2$.

There exists a fundamental limit for the maximum achievable key rate K in bits per channel use by any QKD implementation in a quantum channel with the transmittivity t_{link} , the so-called *Pirandola-Laurenza-Ottaviani-Banchi (PLOB) limit* [29]:

$$K = -\log_2(1 - t_{\text{link}}). \quad (2.1)$$

For a qubit source with a generation period of T the rate expressed in bits per second is given by $R = K/T$.

Another reason limiting the key distribution performance is the detector noise. Dark and afterpulsing events occur in all types of detectors, i.e. electrical pulses that are not triggered by an incoming photon, but appear spontaneously due to thermal or electronic noise. Accidental coincidences between dark counts and real photon detections contribute the main part to the QBER value. Once the real qubit arrival rate drops due to a high distance, the accidental coincidences start dominating, increasing the overall QBER, such that the critical QBER is achieved at some point. This constitutes a practical maximal key distribution distance, which is dependent on the used protocol.

2.1.5. Quantum networks and commercialization

The fundamental distance limit is a severe restriction for use cases of quantum communication technology. Several approaches to overcome this challenge are being developed:

trusted node networks and *all-quantum networks* [30]. The former solution requires trust into the nodes relaying the key. In such a node a number of Alice and Bob modules are hosted, and any relayed key is extracted in digital form. Thus, such nodes require not just QKD technique but also a strong security concept limiting access to tamper-proof rooms and cabinets with the sensitive equipment.

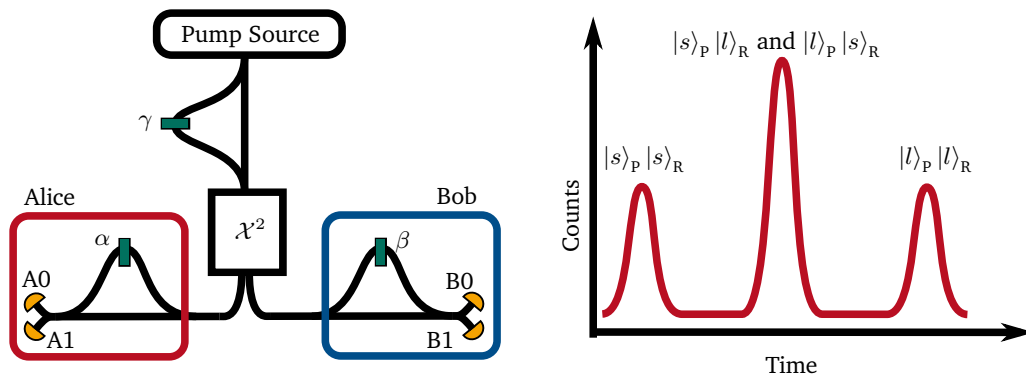
All-quantum networks require functioning *quantum repeaters* that have yet to be developed. Quantum repeaters should enable entanglement propagation for arbitrary distances by use of a chain of alternating entangled photon sources and entanglement swapping stations, where the entanglement between two distant photons is generated. This scenario offers higher key distribution confidentiality, however, at the cost of a much lower key rate.

Since no quantum repeaters has yet been developed, and the need for better communication encryption is growing, trusted node networks are being implemented at the moment. First commercial QKD networks are already implemented in China [31] and South Korea. In Great Britain a commercial metropolitan QKD network is being tested since the summer of 2022 and the European Commission started a number of projects to support the European Union's member states to begin with an implementation of their own quantum communication infrastructure (The Quantum Flagship [32], The Digital Europe Programme [33], Connecting Europe Facility [34] etc.). International Standards Development Organizations like the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the European Telecommunications Standards Institute (ETSI) are actively working on standardization of this technology [35, 36].

The research on QKD devices is still ongoing, aiming for hardware cost reduction and efficiency increase. This technology is at the moment at the threshold to become commercially successful. It will succeed once the standards and certification processes are adopted and the technology is certified by the national security agencies (e.g. the BSI in Germany).

2.2. Time-bin encoding

Despite an entire zoo of QKD protocols developed in the last four decades (see section 2.1.2), the overwhelming part of them focused on the improvement of the actual achievable key rates and distances between two communicating parties far away from each other. However, several attempts pursuing a quantum key distributing network without trusted nodes and quantum repeaters were also proposed and experimentally implemented [37–42]. Most of the implementations utilize polarization encoding, that is accompanied with challenges due to polarization drift inside the deployed fiber [43,



(a) Setup scheme. A0, A1, B0, B1: detectors, α , β , γ : phases of interferometers, \mathcal{X}^2 : pair generation device.

(b) Histogram of detected events with three time-bins. s , l denote short and long arms of pump (P) or receiver (R) interferometer.

Figure 2.1.: Time-bin encoding protocol.

44]. This effect can be compensated at the cost of increased setup complexity, when polarization compensations schemes are implemented [45–47].

In the present work a protocol was chosen which can later be adapted for a network use: a variant of Bennet-Brassard-Mermin 92 (BBM92) with time-bin encoding which is not affected by polarization drift of the quantum link. This is possible due to the source, placed between Alice’s and Bob’s receivers and the chosen orthogonal bases - the phase and the arrival time of the qubits. This protocol can be well combined with the wavelength-division multiplexing technique for distribution of the qubits to more than two parties [48, 49].

During the work on the present experiment, two further protocols that can be easily utilized for star-shaped networks received avid attention: the *measurement device independent* [18, 50–52] and the *twin-field* [53, 54] QKD protocol families.

2.2.1. Protocol scheme

The considered variant of the BBM92 QKD protocol was already suggested and implemented more than two decades ago, employing time-bin encoding [19, 21, 22, 55] and performing QKD at distances of up to 300 km [56–58].

A typical time-bin encoding setup scheme is shown in fig. 2.1(a). There, pulses from a laser source are sent first through an interferometer with a large arm-length difference $I = l - s$, with arm lengths l and s . This imbalance of the interferometer arms should be chosen in a way, that each pulse is divided into two pulses with a fixed time delay and

phase relation generated by the interferometer the pulse passed through. Due to this time delay, those pulses do not interfere with each other and are subsequently coupled into a component generating energy-time entangled photon pairs, i.e. a non-linear crystal for spontaneous parametric down-conversion (SPDC) (see section 2.3.1). The pulse intensity must be chosen such that in most cases, not more than one photon pair is generated by both of them. For SPDC the mean photon number per pulse is typically $\mu \ll 1$. The generated photon pair can be then described by:

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|s\rangle_{\text{p}} |s\rangle_{\text{p}} + e^{i\gamma} |l\rangle_{\text{p}} |l\rangle_{\text{p}}), \quad (2.2)$$

where $|s\rangle_{\text{p}}$ and $|l\rangle_{\text{p}}$ denote the photons created by the pump photon, that traveled through the short or the long interferometer arm of the pump source, and γ is the corresponding phase shift. Also, it should be noted, that both cases $|s\rangle_{\text{p}}$ and $|l\rangle_{\text{p}}$ were generated at different time periods due to the timing of the incoming pulses.

After the generation, the correlated photons are divided, either by frequency or polarization, as in the present experiment, and routed to Alice and Bob. There, they pass local interferometers, designed exactly as the source interferometer. Each photon decides individually and randomly, which path it takes at the receiver, resulting in a possible additional time delay. At the outputs of the interferometers the qubits are detected by single photon detectors and the arrival times are evaluated by the time tagging devices (not shown in the figure).

Considering the histogram of the remainders, obtained by reducing arrival times modulo the repetition period, three peaks at three distinct time-bins are recognizable, as shown in fig. 2.1(b). Each of the time-bins corresponds to the path that the pump pulse and the generated photons have taken: the left time-bin corresponds to short interferometer arms in the pump and the receiver interferometer, the right time-bin to long interferometer arms in both interferometers. The peak in the central time-bin has a doubled area, since at that time the photons are registered that took either the short arm at the pump interferometer and the long one at the receiver or vice versa.

The so-called *two-photon interference* [59, 60] can be observed in the central time-bin, if the arm length differences (the interferometer imbalancements) of all three interferometers ΔL_{imb} are vanishing pairwise, or are much lower than the coherence length of the used photons L_{coh} :

$$\Delta L_{\text{imb}} = |(l_{\text{k}} - s_{\text{k}}) - (l_{\text{l}} - s_{\text{l}})| \ll L_{\text{coh}} = \frac{\Delta\omega}{c_0}, \quad (2.3)$$

for any $k, l \in \{Alice, Bob, Source\}$ and s, l being the short and the long arms of individual interferometers, respectively. This phenomenon is responsible for correlations that can be observed by analyzing the coincident events of both receivers [21]:

$$P_{A_i, B_j}(\alpha, \beta, \gamma) = \frac{1}{4} \left(1 + (-1)^{i+j} \cos(\alpha + \beta - \gamma) \right), \quad (2.4)$$

with α, β and γ being the phases in interferometers of Alice, Bob and the source, and $i, j \in (0, 1)$ being the detector labels. For the overall phase $\alpha + \beta - \gamma = 2\pi n, n \in \mathbb{Z}$ Alice and Bob register their bit at the detectors with the same label. This formula is correct under the assumption of a perfect lossless setup with ideal 50:50 beam splitters.

For the key extraction the photon arrival times and the registering detector labels must be evaluated. Therefore, for key sifting Alice and Bob publicly announce, if they measured an event in the central or one of the satellite time bins and compare the outcomes. For example, if Alice registers an event in the left (early) time-bin, she announces a detection in a satellite time bin. If Bob also announces his detection to be in a satellite time bin, it follows, that both parties detected the photon in the early time-bin and they note the bit "0". If Bob announces the detection in the central time bin, the event record is discarded by both - they used unmatched bases. The same applies, if Alice's event is in the late time bin, that correspond to bit "1". In the case of detection in central peak by both parties, two photon interference is exploited and the detector labels are evaluated. If the overall phase of the three interferometers is correctly adjusted, the photons are detected at correlated detectors: $A0 \wedge B0$ and $A1 \wedge B1$. As bit values the detector labels are noted.

The implemented protocol BBM92 is equivalent to the BB84 [19], which was proven secure. Thus, the critical QBER for this protocol also amounts $QBER_{crit} < 11\%$ [25].

2.2.2. Fiber-based Michelson interferometers

For most experimental implementations of the time-bin protocol, a Michelson interferometer is used instead of a Mach-Zehnder interferometer (MZI). The reason is its polarization insensitivity to the incident light. In deployed fibers, environmental effects may change the birefringence of the fibers leading to a polarization change of the transmitted light wave with multiple rad/s [43, 44, 61]. This leads to a random polarization state of incoming photons (see section 2.4.3). In a MZI the photons pass through two independent interferometer arms with different lengths and different birefringence leading to different changes of the polarization in both arms lowering the interference contrast at the output. In a Michelson interferometer, the light reflected from the Faraday rotator mirrors in both interferometer arms has a polarization that is orthogonal to the incident light. Thus, the

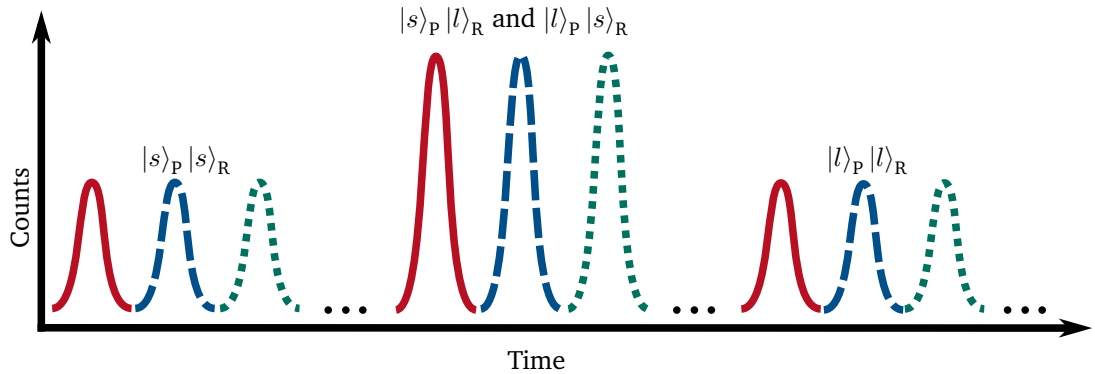


Figure 2.2.: Multiplexed time-bin coding. Correlated time-bins at different multiplexing stages are coloured equally.

light waves that propagated through different arms have matching polarization regardless of the polarization state of the light before the interferometer [62–64].

Acoustic noise has a detrimental influence on free space interferometers [65]. Fiber-based interferometers are also affected by it, they can be even utilized for sound detection [66]. Thus, for a stable phase detection of the incoming light, acoustic noise shielding is advisable.

2.2.3. Time-multiplexing of time-bin encoding protocol

A successful evaluation of the arrival time histogram is only possible, if the time-bins are well discriminable. Their distances and widths correspond to the interferometer imbalance and the pulse duration. Additionally, the dispersion properties, primarily chromatic dispersion (CD) (see section 2.4.4), of the planned communication link and the timing jitter of the used electronics - all phenomena, broadening the pulse duration, must be taken into account. Furthermore, the properties of the qubit generation stage have to be considered: the pulses must have enough energy to generate a suitable mean photon pair number per pulse μ and simultaneously not exceed its damage threshold limiting the pulse energy and the peak power of the pulses. Those parameters define the lowest experimental pump pulse duration.

For the presented experiment, the distance of the time bins, i.e. the interferometer imbalance is determined by the assembly method of the interferometers, where the mechanical stretching of the fiber is used to compensate the imbalance differences ΔL_{imb} (see chapter 4). In this case, the possible imbalance length can be several

times longer than the expected time bin width. This allows to multiplex the pulses in time, leading to interlaced time-bin histograms as shown in fig. 2.2. The number of multiplexed pulses can be arbitrarily large as long as the time bins remain discriminable.

2.3. Generation of energy-time entangled photon pairs

2.3.1. Spontaneous parametric down-conversion

For the presented QKD experiment, an on-demand generation of energy-time entangled photon pairs is required, with exactly one single generated pair per pump pulse. Simultaneously, the coherence length of the generated photons must be as high as possible to lower the requirements on the used interferometers (see section 2.2). Unfortunately, no sources combining both properties has been developed yet so other option had to be considered.

Therefore, to generate energy-time entangled photon pairs, a well-known solution was chosen – the spontaneous parametric down-conversion (SPDC). Experimentally observed already in 1965 [67], it is now used for more than twenty years for QKD experiments [15]. This method is reliable and well-developed both theoretically [60, 68] and experimentally [69].

During SPDC one photon of the energy $E_{\text{pump}} = \hbar\omega_p$, converts within a non-linear medium spontaneously to two energy-time entangled photons, called *signal* and *idler*, with the energies $E_{\text{signal}} = \hbar\omega_s$ and $E_{\text{idler}} = \hbar\omega_i$. Similarly to other non-linear optic effects (cf. section 3.1.4), both energy and momentum conservation play a major role for this process:

$$\omega_p = \omega_s + \omega_i \text{ and } \Delta k = |\mathbf{k}_p - \mathbf{k}_s - \mathbf{k}_i| = 0, \quad (2.5)$$

where \mathbf{k} are the wave vectors of interacting photons and Δk is the phase mismatch of interacting photons. For quasi-phase matched periodically-poled crystals with waveguides, this condition must be corrected by the terms contributed by the waveguide (Δk_{wg}) and by the crystal's periodic poling: $\frac{2\pi}{\Lambda}$, where Λ is the poling period width:

$$\Delta k = k_p - k_s - k_i - \frac{2\pi}{\Lambda} + \Delta k_{\text{wg}}. \quad (2.6)$$

Generally, different process types are distinguished, depending on the polarization of the interacting photons [70]. In the presented experiment the type II process was used, which means that the polarization of the signal and idler is well defined and orthogonal to each other. Thus, a polarizing beam splitter was used for separation of those photons during all experiments.

One drawback of SPDC limiting its usability for the experiment is the temporal statistics of the photon pair generation. For photon sources with a high aspect ratio between the widths of the photon spectrum and of the pump pulse spectrum, it is almost Poissonian [68, 71, 72], which means that the probability to generate n pairs of photons during some time interval δt is described by:

$$P_\mu(n) = \frac{\mu^n}{n!} \cdot \exp(-\mu), \quad (2.7)$$

with μ being the mean number of photon pairs in δt . Several photon pairs per pulse increase the probability that photons from non-correlated pairs are detected jointly, raising the QBER. To circumvent this problem, small values for μ are chosen, typically $\mu < 0.1$ [22, 56]. Unfortunately, this also decreases the probability to generate exactly one photon pair per pulse. From $\mu = 0.1$ results $P_{0,1}(1) = 0.09$, i.e. on average, just each 10th pulse contains exactly one pair of photons. However, unlike a high QBER, this is not a critical issue.

2.3.2. Efficiency measurement of the spontaneous parametric down-conversion in a crystal

To determine the required pump power for various values of μ , the SPDC efficiency of the crystals must be known. In fact, it can be explicitly calculated for a crystal with a waveguide, as the one used during this work, by [73]:

$$\frac{dP_{\text{SPDC}}}{d\lambda_s} = \frac{16\pi^3 \hbar d_{\text{eff}}^2 L^2 c_0}{\varepsilon_0 n_s n_i n_p \lambda_s^4 \lambda_i A_I} \text{sinc}^2\left(\frac{\Delta k L}{2}\right) P_{\text{pump}}, \quad (2.8)$$

with d_{eff} being the effective non-linear coefficient of the crystal, L - its length, $n_{s/i/p}$ - the refractive index of signal, idler or pump photon, $\lambda_{s/i}$ - the wavelengths of signal or idler photon, P_{pump} - pump power and A_I - the mode overlap area of the pump and frequency converted light. Waveguides with the widths and heights of just several micrometer keep A_I small throughout the entire crystal, yielding a higher frequency conversion efficiency than bulk crystals. However, unlike second harmonic generation (SHG), the intensity of SPDC is proportional to the pump power and not to its square. To adapt this formula for fiber-coupled crystals, the light coupling efficiencies from fiber to waveguide for the pump and generated photons must be taken into account, making it challenging to predict a realistic value.

Therefore, an experimental approach to determine the crystal's efficiency can be chosen. The SPDC efficiency denotes the probability for conversion of the pump photon into the entangled signal and idler photons:

$$\eta_{\text{SPDC}} = \frac{P_{\text{SPDC}}}{P_{\text{pump}}} = \frac{2 \cdot E_{\text{SPDC}} \cdot N_{\text{SPDC}}}{P_{\text{pump}} T_{\text{meas}}} = \frac{2 \cdot E_{\text{SPDC}} \cdot R_{\text{gen}}}{P_{\text{pump}}} \quad (2.9)$$

with R_{gen} being the generated photon rate (mean photon number during the measurement time T_{meas}), P_{pump} the mean pump power and E_{SPDC} the energy of the single generated photon. While it is quite straightforward to determine the pump power and the energy of the generated photons, the direct measurement of R_{gen} is challenging due to the peculiarities of single photon detection. Here, the detector's dead time τ_{dead} and the low detection probability η must be taken in account, since those effects lower the detected rate compared to the real rate.

Typically, depending on the detector type, the dead time is up to ten microseconds long. This amount of time cannot be neglected for the calculation of the real rate and must be corrected. In the following, it is assumed, that the generated photon rate hitting the detectors is nearly constant and the detectors generate one single pulse per each photon detection additionally to the unavoidable dark counts events.

Then, the amount of time per second, when the i -th detector with $i \in \{1, 2\}$ is not in the dead time, is $1 - R_{\text{meas},i} \tau_{\text{dead},i}$, with the measured rate R_{meas} . A hypothetical detector without the dead time would need only $(1 - R_{\text{meas},i} \tau_{\text{dead},i}) T_{\text{meas}}$ to detect the same amount of photons, that the real detector registers during T_{meas} . It would also detect a higher overall rate $R_{\text{ov},i}$, since no photon will be missed during the dead time [74]:

$$N_{\text{meas},i} = R_{\text{meas},i} T_{\text{meas}} = R_{\text{ov},i} T_{\text{meas}} (1 - R_{\text{meas},i} \tau_{\text{dead},i}). \quad (2.10)$$

This can be rearranged to a correction factor for single detectors:

$$R_{\text{ov},i} = \frac{R_{\text{meas},i}}{1 - R_{\text{meas},i} \tau_{\text{dead},i}}. \quad (2.11)$$

Analogously, an expression for the coincidence rate can be derived:

$$R_{\text{c,ov}} = \frac{R_{\text{c,meas}}}{(1 - R_{\text{real},1} \tau_{\text{dead},1})(1 - R_{\text{real},2} \tau_{\text{dead},2})}. \quad (2.12)$$

The overall rate R_{ov} for each detector is given by the combination of the dark count rate R_{dark} and the fraction of generated photons R_{gen} :

$$R_{ov,i} = \eta_i t_i R_{gen} + R_{dark,i}, \quad (2.13)$$

with η_i being the detector efficiency of i -th detector and t_i - the transmission of the connection. To identify the events that belong to entangled photons, a coincidence analysis must be performed. Choosing a coincidence window τ_c and assuming similarly long propagation paths for both photons of the entangled pair with the path length difference $\Delta s \ll c\tau_c$, the arrival times of all events are compared. The obtained coincidences belong either to the correlated photons or occur accidentally, due to dark counts etc: $R_{c,ov} = R_c + R_{c,acc}$ with:

$$R_c = \eta_1 \eta_2 t_1 t_2 R_{gen}. \quad (2.14)$$

Accidental coincidences are only possible between events that are not taken into account by R_c :

$$R_{c,ac} = (R_{ov,1} - R_c)(R_{ov,2} - R_c)\tau_c. \quad (2.15)$$

Combining the equations above and rearranging them, the generated photon pair rate R_{gen} is given by:

$$R_{gen} = \frac{1}{R_c} (R_{ov,1} - R_{dead,1}) (R_{ov,2} - R_{dead,2}), \quad (2.16)$$

where the coincidence of correlated events R_c yields:

$$R_c = \frac{1}{2} \left(R_{ov,1} + R_{ov,2} + \frac{1}{\tau_c} \right) + \sqrt{\frac{R_{c,ov}}{\tau_c} - R_{ov,1} R_{ov,2} + \frac{1}{4} \left(R_{ov,1} + R_{ov,2} - \frac{1}{\tau_c} \right)^2}, \quad (2.17)$$

that can be easily calculated from the measurement data with eq. (2.11) and eq. (2.12).

Spectral width of down-converted photons

From the phase mismatch function given by eq. (2.6), the spectral bandwidth of down-converted photons can be estimated. Assuming the degenerate case with $\omega_s + \omega_i = \omega_0$ and $\omega_p = 2\omega_0$, then the phase mismatch function Δk can be approximated around ω_0 by a Taylor series with $\omega_s = \omega_0 + \Omega$ and $\omega_i = \omega_0 - \Omega$ to [60]:

$$\Delta k = k_p(2\omega_0) - k_s(\omega_0) - k_i(\omega_0) - \frac{2\pi}{\Lambda} + \Delta k_{wg} \approx -(k'_s - k'_i)\Omega - \frac{1}{2}(k''_s - k''_i)\Omega^2, \quad (2.18)$$

assuming vanishing dependence of the two latter terms on frequency. In general $(k'_s - k'_i) \neq 0$ holds and is much larger than the quadratic term due to the different polarization directions of the signal and idler photons, and that can be neglected for most materials [60, 68]:

$$\Delta k \approx -(k'_s - k'_i)\Omega, \quad (2.19)$$

where k'_s and k'_i can be determined from the Sellmeier equations. For the magnesium-doped periodically poled lithium niobate (PPLN), that was used during this work, they are given in ref. [75]. The value for Δk can be determined from eq. (2.8), calculating the full width at half maximum (FWHM) of the sinus cardinalis:

$$\text{sinc}^2\left(\frac{L\Delta k}{2}\right) = \frac{1}{2}, \quad (2.20)$$

yielding $L\Delta k \approx 2.783$. Thus, using eq. (2.19), the FWHM can be expressed as:

$$\Delta\omega = \frac{2 \cdot 2.783}{L \cdot |k'_s - k'_i|}. \quad (2.21)$$

For the crystal used during this work, the value $\Delta\omega = 1.09$ nm was calculated, and the corresponding coherence length inside the optical glass fiber is $L_2 \approx 2$ mm. This value was verified by two methods: with a *grating spectrometer*¹ and with a *dispersion spectrometer*, where the spectral properties of the single photons are calculated from the impact of CD on their detection time, as described in reference [76]. Both methods delivered a value for $\Delta\omega_{\text{meas}} = (1.13 \pm 0.01)$ nm, which is in a good agreement with the expectation.

2.4. Optical fibers and their application in communication

In this section a brief description of the necessary basic principles and concepts for glass fiber technology and fiber-optical communication is given. The same effects and noise sources are valid for single photons as for classical laser pulses traveling through optical glass fibers, determining the most important parameters of the setup.

2.4.1. Optical glass fibers

A typical optical fiber is a cylindrical fiber consisting of core, cladding and coating as shown in fig. 2.3(a). The core has a slightly higher refractive index than the cladding

¹Andor Shamrock SR-500i Czerny-Turner spectrograph with iDus InGaAs 491 Detector, manufactured by Oxford Instruments plc, UK.

($\Delta n \approx 0.01$), achieved by adding dopant atoms to the host glass material [77]. The polymer coating protects the fiber from the potentially aggressive environment, while simultaneously increasing its flexibility thus preventing the fiber from cracking while twisting and curling. Other additional protection layers are often used, however, they only increase the fiber's mechanical robustness.

The light propagation can be described either as rays experiencing total internal reflection at the border between the core and the cladding or using the wave model of light. Within the latter model the propagating light modes can be described as solutions of the *Helmholtz equation* [77], whereby the number of modes transmitted within the fiber is depending on the radius of the fiber a , the transmitted wavelength and the refractive indices of the core and cladding. Different modes propagating through the fiber possess different group velocities leading to the group velocity dispersion, reducing the signal-to-noise ratio for communication with optical pulses [77, 78]. Therefore, single-mode fibers (SM fibers) that guide a single mode are more appropriate for optical communication. The intensity profile of the light-mode within the core of a SM fiber is similar to Gaussian distribution with a mode field diameter (MFD) larger than the diameter $2a$ of the glass fiber. Here, the MFD is defined as the radial distance of the points, where the intensity amounts to I_{\max}/e^2 of the the peak intensity I_{\max} .

Considering light propagation within the glass fibers, it is necessary to take into account the effects arising from the interaction of the light with the fiber material limiting the signal propagation capability of the transmission channel: absorption, polarization mode dispersion (PMD), CD, and nonlinear effects such as Raman and Brillouin scattering, the Kerr effect, four-wave mixing and self phase modulation just to name a few [77–79]. While most effects must be considered and compensated while operating classical optical communication systems, for QKD devices only few are relevant, being also highly critical. While the attenuation of the glass fiber reduces the effective distance of the key transmission, the CD reduces the maximal achievable key rate for our protocol and the PMD must be compensated to enable the key distribution in the first place.

2.4.2. Attenuation profile

The attenuation of light within the glass fiber α occurs due to the absorption and scattering of light. The attenuation coefficient is typically given in decibels per kilometer and is defined as: $\alpha = \frac{1}{L} 10 \log_{10}(P(0)/P(L))$, with $P(0)$ and $P(L)$ denoting the light beam power at the distances of 0 and L .

In fig. 2.4 the attenuation profile of a SM fiber, compliant with the ITU-T G.652 standard [80], is given. The presented range corresponds to the absolute absorption minimum of the glass fiber, that is limited mainly by *Rayleigh-scattering* at the wavelengths below

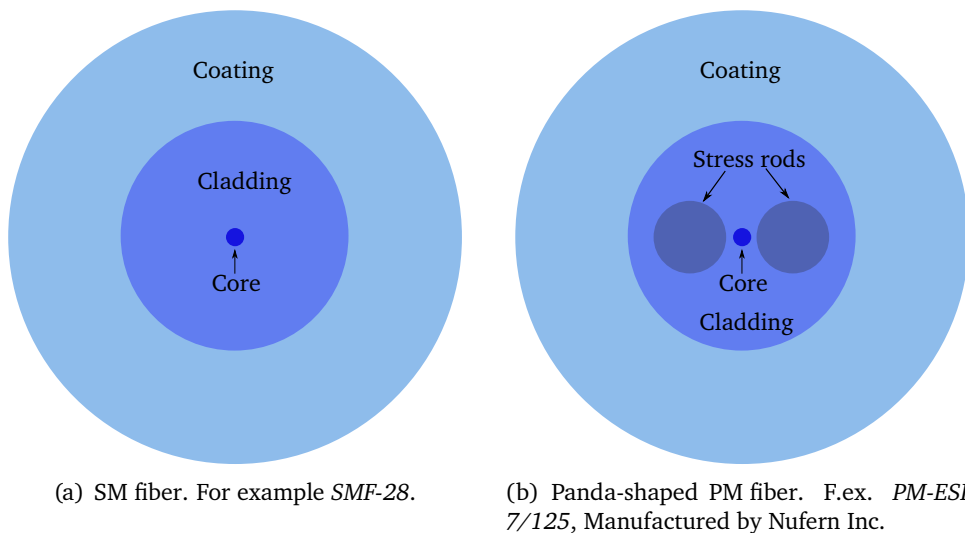


Figure 2.3.: Cross-sections of different glass fiber types. The pictures are at the correct scale.

1600 nm and infrared absorption above 1600 nm [77]. The peak at 1383 nm corresponds to the OH-ion absorption peak that is mostly suppressed for newer fibers [80]. Other effects such as ultraviolet light absorption and the presence of impurities also contribute to the loss, however to a much smaller degree.

Thus, the area shown represents the desired window for optical communication systems. In fig. 2.4 the typical frequency bands are shown: **Original**, **Extended**, **Short**, **Conventional**, **Long** and **Ultra** or **Extra-Long**. Each band contains a different number of channels of typically 100 GHz width. However, the channel width can vary according to the spectral grid standard of ITU-T [81]. The C-band has the lowest attenuation around 0.19 dB/km. With ultra-low loss fibers, that are being developed, even lower values of 0.1460 dB/km can be achieved [82].

QKD glass-fiber based systems typically utilize the C-band in order to achieve maximum transmission rates.

2.4.3. Polarization of light within the glass fiber

In a symmetrical fiber, like a SM fiber (fig. 2.3(a)), the polarization of a light wave generally changes randomly due to irregularities, stress and temperature-induced gradients of the

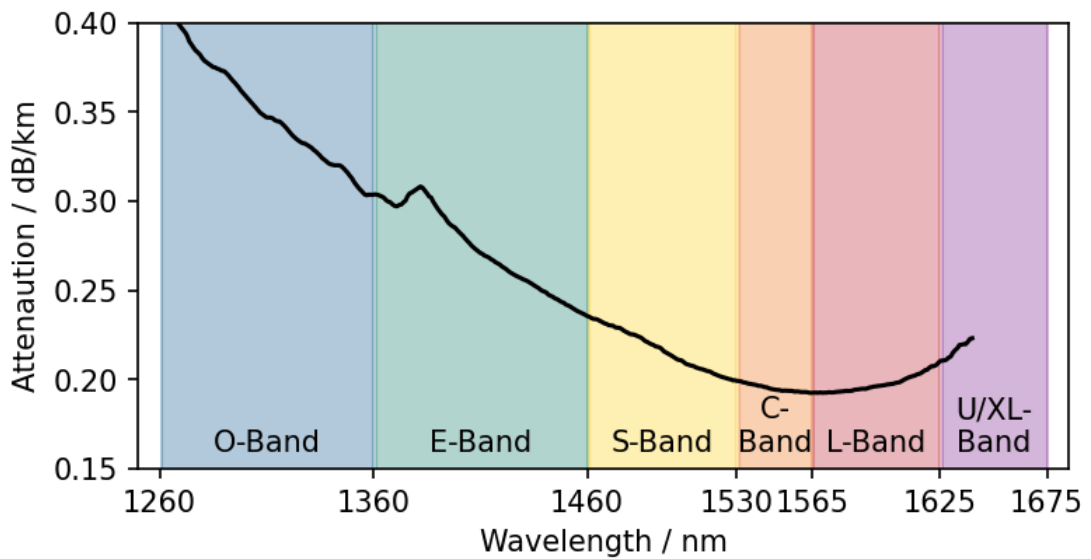


Figure 2.4.: Attenuation profile of a typical SM fiber and different communication bands. Data from an actual measurement.

effective refractive index within the fiber [77]. In PM fibers a higher birefringence is induced by a non-symmetrical structure of the fiber. The most typical structure, the panda shaped profile is shown in fig. 2.3(b). Stress rods are made of glass with slightly different refractive index compared to the cladding, defining the so-called *slow* and *fast* axis. The coupling between the polarization light modes propagating along those axes is almost removed, so that the modes propagate independently of each other with different group velocities corresponding to the names of the axes. For SM fiber those modes exist too, however they are coupled.

Thus, a linearly polarized light pulse, inserted into a fiber under a random angle splits into two sub pulses, propagating along those two axes each. Those pulses have different arriving times and a phase shift between the polarization modes, leading to a random polarization state at the output of the fiber. This effect is called the polarization mode dispersion (PMD) [77].

If a linearly polarized light wave is properly coupled into the fiber along either the fast or the slow axis, the resulting beam has the same polarization, since there is no other mode with different group velocity.

In SM fibers the birefringence can be changed by the environmental influences such as temperature and humidity changes, as well as mechanical stress, leading to a slow drift of the output polarization. Therefore, polarization based QKD systems must circumvent the PMD, e.g., by actively compensating the PMD of the quantum channel with polarization controllers [83–85].

2.4.4. Dispersion and non-linear effects

Light pulses are typically broadened in time after the propagation through the glass fiber due to different kinds of dispersion: polarization mode, modal, material, waveguide and non-linear dispersion. The modal dispersion disappears in SM fibers and the material and the waveguide dispersion is called chromatic dispersion (CD) and is an intrinsic property of the glass fiber, that arises from the dependence of the refractive index on the wavelength. This dispersion leads to the broadening of the pulse in time [77].

For telecommunication fibers the maximal values for attenuation, PMD and CD are specified in the ITU-T standard [80]. For example, SMF-28 is a fiber that complies with this standard and is widely used within long-haul telecommunication systems.

Non-linear effects such as Raman-, Brillouin- and Rayleigh scattering [77] act detrimentally on the optical communication, reducing the signal-to-noise ratio of the transmitted pulses. Since QKD systems work with light intensities on the single photon level, almost no influence of non-linear effects can be observed. They start playing a role only, if the quantum channel and classical channel are combined within one physical glass fiber. Then, the Raman-scattering leads to a higher noise within the wavelengths of the qubits, increasing the QBER.

2.4.5. Fiber pigtailed components and fiber connections

Glass fibers turned out to be reliable and cost-efficient light waveguides, that enable novel setups with much more compact components. Within more than forty years of development, a lot of fiber-coupled devices have been developed. In the experiments for the present work, only off-the-shelf components were used: fiber-pigtailed electro-optic modulators, pigtailed crystals for frequency conversion (cf. section 3.1.4 and section 3.2), pigtailed filters, 50:50- and 90:10- fiber-coupler, fiber optic circulators and Faraday rotator mirrors.

A disadvantage of those components is a much higher insertion loss compared to free space components. It varies typically from 0.3-1.2 dB depending on the components. Electro-optic modulators can even exceed 4 dB, since its integrated PPLN crystal exhibits a high light absorption. On the contrary, glass fibers allow for low losses within the

connecting sites. There are several ways to connect glass fibers to each other, resulting in different properties of the established connection: physical connectors, mechanical and fusion splicing.

A large number of connector types that have been developed, allows for a fast and safe detachment of fibers, varying in price and connection quality. Therefore, single connectors are attached to the ends of fibers and inserted into the mating sleeves. The connection typically exhibits a loss of 0.2-1 dB [86], depending on the connector type and the condition of the fiber's connection surface. A loose hanging connector leading to lateral, axial or angular displacement of the fiber cores with respect to each other in a micrometer range may cause a huge loss due to the relatively small MFDs of SM fibers (around 10 μm). Mismatching MFDs are also a common reason for losses at the fibers' connection sites [87].

For PM fibers, the connectors must be installed with respect to the polarization state of the fiber. According to the technical support team of the Thorlabs company, the alignment precision of the axes within a *FC/APC* connector, which was mainly used within this work, is $\pm 2^\circ$ [88]. So, a line of fibers connected via PM mating sleeves shows an increasing angle error when increasing the number of connected fibers and hence a polarization instability.

Fiber fusion splicing offers a method for fiber connection with a lower attenuation and better polarization maintaining at the splice joints. Here, a different MFD of the connecting fibers may lead to a high loss. For identical fiber diameters, losses below 0.01 dB can be typically reached [86]. Furthermore, a perfect orientation of stress rods in two pieces of identical fiber can be achieved. During this work, however, imperfect joints of different fiber types lead to a slow polarization change within the fiber (c.f. section 3.1.3). The techniques and the devices for fiber fusion splicing have been developed for decades already and good descriptions of this topic can be found in refs. [86, 87].

During this process, the fiber ends are heated with an electric discharge until they are melting. They are then put into contact with each other, so that the melted glass facets stick together and after cooling down, a permanent joint is created. Depending on the splicing device, up to eight degrees of freedom for fiber adjustment enable a nearly perfect adjustment of the lateral and axial position of the fibers and the orientation of the polarization maintaining stress rods. For the whole process, the polymer coating has to be removed beforehand and applied again onto the joint in order to recover the mechanical stability and flexibility of the fiber.

During this work two fusion fiber splicers were used. The splicer *FSM-100P*² allowed for the splicing of a variety of fibers, including polarization maintaining and multi-mode

²Manufactured by Fujikura, Inc.

fibers, that were used during the pump source assembly. Another device *FSM-60S* was used for splicing the single mode fibers SMF-28, used within the receivers. This splicer was used, since it allowed to splice shorter pieces of fiber than the former device. With the *FSR-05*³ device the fiber joints were recoated, using the high index recoating material *Angstrom Bond 950-200 UV*.

2.4.6. Mechanical properties

Since glass fibers found an application within the telecommunication industry, their properties are being continuously improved. Not only the optical but also mechanical characteristics, such as the Young modulus and the life expectancy under various conditions such as mechanical stress and different temperatures and humidity values are evaluated [89]. In particular, the mechanical properties of the splicing joints and the role of the polymer coating are of high interest.

The lifespan of the deployed telecommunication fibers amount to at least four decades [90] but can be limited by external influences: high transmission power, high humidity or mechanical stress [91]. Stress may be induced by small defects and impurities and by the difference of the thermal expansion coefficients of the core and the cladding. Furthermore, curling, coiling and twisting as well as mechanical tension sets the fiber under mechanical stress.

On the other hand, pulling on the fiber leads to a relative fiber length increase, also called the *normal strain* $\varepsilon = \Delta L/L$. The *tensile stress* $\sigma(\varepsilon) = F/A$, with F being the applied force and A the area of a cross-section perpendicular to the force is another important mechanical quantity, leading to Young modulus $E_g = \sigma(\varepsilon)/\varepsilon$, which is typically used to describe elastic properties of materials.

The Young modulus of the SMF-28 without coating amounts to $E_g \approx 70$ GPa [92–94]. The polymer coating gives the fiber more elasticity lowering this value down to 16.6 GPa [94].

Depending on the tension, its duration and the humidity of the environment, some cracks may emerge and grow spontaneously and at different speeds [91]. The force thresholds for instant tearing is found to be at (4.35 ± 1.45) N vs. (7.57 ± 2.51) N pulling force for the SMF-28 without and with the polymer coating respectively [94]. This corresponds to the stress values of 21.6 GPa and 37.6 GPa. Thus, the polymer coating increases the mechanical stability of SMF-28 significantly.

During the production, its entire length is subjected to a tensile stress greater than (690 MPa) for quality control. Furthermore, according to the applied stress design guide-

³Manufactured by Fujikura, Inc.

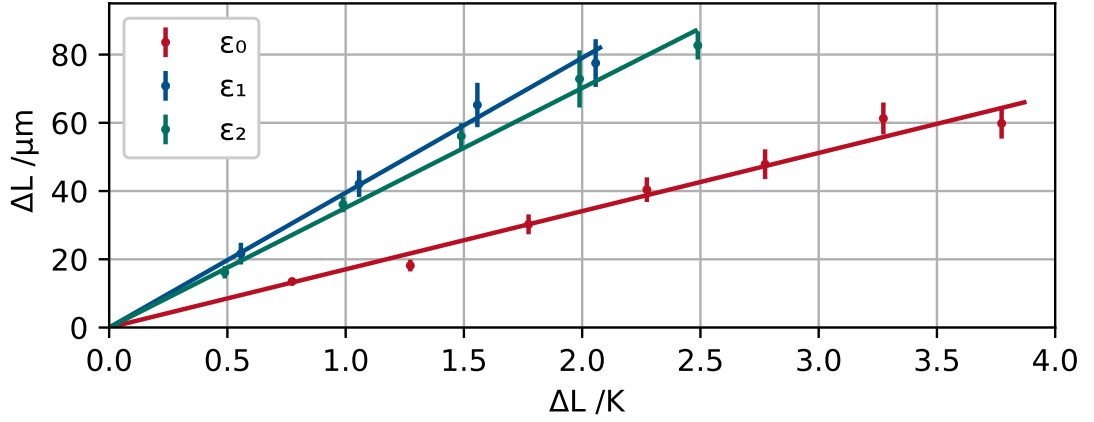


Figure 2.5.: Thermally induced elongation per meter of the *SMF-28* coiled fiber for strain values $\varepsilon_0 = 0$, $\varepsilon_1 \approx 1.2 \cdot 10^{-3}$ and $\varepsilon_2 \approx 3.7 \cdot 10^{-4}$. The straight lines are fitted to corresponding data sets.

lines [90] the standard single mode fiber used for telecommunication *SMF-28* [95] can be exposed to a mechanical stress up to 145 MPa without a significant impact on its life expectancy. Combined with the previously mentioned Young modulus E_g , this might lead to the strain of at least $\varepsilon = 2.0 \cdot 10^{-3}$. This constitutes a critical value for the method of interferometer assembly, presented in this work (c.f. section 4.1). However, this value is only an estimation for mechanical expansion of the fiber. For the estimation of the real time delay of the propagating light, not only the geometric length change, but also the refractive index variation due to the strain-optic and thermo-optic effects must be taken into account.

Main models for strain-optic effects do not take into account the temperature dependence of the system [96–98], stating that for the phase change $\Delta\phi$ induced by elongation ΔL the following relationship holds:

$$\Delta\phi = \frac{2\pi}{\lambda} (n\Delta L + \Delta nL) = \frac{2\pi}{\lambda} \left[1 - \frac{n^2}{2} (p_{12} - \sigma(p_{11} + p_{12})) \right], \quad (2.22)$$

with λ being the light wavelength, n the refractive index, σ_p the Poisson ratio of the fiber material and p_{11} , p_{12} the material dependent strain-optic coefficients. Experiments during the present work show that those coefficients are also dependent on the temperature of

the fiber as shown in fig. 2.5. There, the thermally induced elongation on the optical fiber length for several strain values is shown. The measurement method is described in section 2.5. Since the fiber is glued to a copper cylinder of 7 cm diameter during the experiment, this results in an additional mechanical tension and, thus, additional birefringence, besides the pulling force. The resulting value for the case without any active stretching $\varepsilon_0 = 0$ amounts to (47 ± 3) ps/(km K), which is above the value of 39 ps/(km K) reported in literature [99]. The difference can be explained by the birefringence from curling of the fiber.

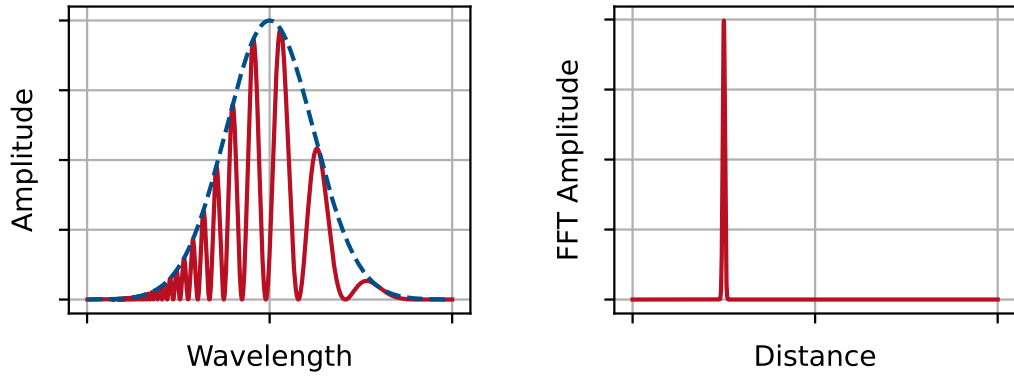
Two other different strain values $\varepsilon_1 \approx 1.2 \cdot 10^{-3}$ and $\varepsilon_2 \approx 3.7 \cdot 10^{-4}$ show stronger dependence of elongation on temperature. In literature no reliable experimental data for light delay as a function of the strain and temperature was found. Thus, the eq. (2.22) cannot be used for calculating the phase adjustment, since its simultaneous dependence on strain and temperature is unknown and can only be determined by experiment.

2.5. White light interferometry for length measurements

White light interferometry is a well established method that is used for distance, thickness and refractive index measurements in various scientific and engineering areas [100, 101]. This method was used for measuring the arm length differences of two interferometers already by Tittel et al. in 1998 [20] and enables measurement precision down to the sub-micron range, depending on the properties of the instruments used.

The method works as follows: The interferometers are connected in series, i.e. one of the outputs of the first is connected to the input of the second interferometer. Light of a broadband light source propagates through both interferometers and is analyzed with a spectrometer. In the case when the path length difference of a single interferometer is non-zero, an amplitude modulation in the optical spectrum of the output light is observable, as can be seen in fig. 2.6(a). After a Fourier transform, we obtain a value for the mismatch of the arm lengths of two interferometers ΔL (fig. 2.6(b)). The uncertainty of this method can be estimated by the FWHM of the Fourier peak, however, it is a rather conservative value. The non-vanishing width of the Fourier peak is due to the numerical and discrete nature of the Fourier transform algorithm.

Mathematically, this can be described by a plane wave $E = E_0 \exp(i(kz - \omega t))$ propagating through two Michelson interferometers with the arm-length differences $\Delta L_{\text{imb}} = |\Delta l_a - \Delta l_b| = |(l_a - s_a) - (l_b - s_b)|$ for s, l being the lengths of the short and the long



(a) Original optical spectrum of the light source (blue) and measured modulated optical spectrum (red). (b) Fourier transform of the modulated spectrum in (a).

Figure 2.6.: Functional principle of white light interferometry method for measurement of interferometer arm-length mismatches. Modulated optical spectrum in (a), measured by optical spectrum analyzer (OSA), can be transformed into a distance value by a FFT (b).


arms and any $a, b \in \{Alice, Bob, Source\}$. The intensity after the second interferometer without taking the intensity losses into account amounts then to:

$$I = 4 + 4 \cos(k\Delta l_a) + 4 \cos(k\Delta l_b) + 2 \cos(k(\Delta l_a + \Delta l_b)) + 2 \cos(k(\Delta l_a - \Delta l_b)). \quad (2.23)$$

The first three terms can be neglected, since the typical spectral analyzer cannot resolve such fast oscillations. With $k = \frac{2\pi n}{\lambda}$ one obtains $I = 4 + 2 \cos(2\pi n \Delta L / \lambda)$ which has a characteristic modulation as schematically shown in fig. 2.6(a). Performing a fast Fourier transformation with a python script, the value for ΔL is directly obtained.

Alternatively, a naive approach can be used for determining of ΔL . The minima of the spectrum occur at the wavelengths $\lambda_n, \lambda_{n+1} = \lambda_n + \Delta \lambda_n$, etc., which fulfill the condition for the destructive interference: $\Delta L = n \cdot \lambda_n = (n + 1) \cdot \lambda_{n+1}$. After eliminating of n , the arm-length difference is obtained by:

$$\Delta L = \frac{1}{2n} \left(\frac{\lambda_n^2}{\Delta \lambda_n - \lambda_n} \right). \quad (2.24)$$



The precision of both methods is matching within a fraction of their uncertainties with the measured data.

3. Entangled-photon-pair source

One of the main challenges of the present work was building and operating receiver modules. They are described in chapter 4 and in particular the difficulty of building Michelson interferometers with an extremely small interferometer delay difference is pointed out. Since it was unclear, how much effort the developing of the method for the interferometer assembly would require, a flexible qubit source was required. It had to enable a wide range of operational parameters and simultaneously provide a high reliability, compactness and robustness. All requirements on the photon-pair source pump combined are as follows:

- Operation of the qubit source and, particularly, the laser pump system in a pulsed operation mode, with flexible pulse duration in the range $\tau_{\text{pulse}} = 0.5\text{--}5$ ns, repetition rates (RRs) in the range $f_{\text{RR}} = 1\text{--}200$ MHz and output mean power of $P_{\text{pump}} \approx 20$ mW or more at 775 nm should be possible.
- Operation in challenging environment with a high acoustic noise (up to 90 dB), high temperature fluctuations ($T_{\text{lab}} = 13\text{--}30$ °C), variable humidity and air pressure should be ensured, in order to perform experiments in a typical telecom operating room at a facility of Deutsche Telekom.
- Conformity to the laser- and working safety policies of our collaboration partner, the Deutsche Telekom should be met. Since the experiments are conducted in a big laboratory, it is impossible to restrict access to experimental devices for external staff.
- Entangled photons should possess a wavelength corresponding to the telecom C-band in order to minimize the losses of qubits.

The simplest and most reliable method for generation of energy-time entangled photons was chosen the spontaneous parametric down-conversion (SPDC) (see section 2.3.1). This is a well known process that has been used to produce photon pairs for quantum key distribution (QKD) for more than twenty years [15].

Since the developed QKD system had to be fiber-based, SPDC with degenerate photon pairs within the optical communication C-band (see section 2.4.2) was pursued. One way to implement this scheme is to pump a non-linear crystal, typically a periodically poled potassium titanyl phosphate (PPKTP) or a periodically poled lithium niobate (PPLN) crystal with 775 nm light, in continuous wave (cw) or pulsed mode. Several potential experimental schemes for the pumping system could be considered: a titan:sapphire laser (TiSa) or a diode laser (DL), both at 775 nm or a frequency conversion of a 1550 nm amplified laser system.

A typical high power laser source at 775 nm is the TiSa [102]. It possesses a wide light emission range from 650 nm to 1000 nm and can be designed for operation in either cw or pulsed mode. However, a flexible RR, flexible pulse duration and potential switching to a cw operation is not straightforward to implement within a TiSa. Additionally, the costs for commercially available TiSas are significantly higher than possible alternatives without a clear advantage compared to other options.

Diode lasers (DLs) at 775 nm are available already for more than two decades. By now single-mode fiber-coupled DLs reach cw mean powers of several 100 mW with a modulation bandwidth of several GHz. However, pulses generated by current modulation suffer from spectral chirp, reducing the usefulness of such lasers for quantum information experiments (see Sec. 2.3). This drawback could be avoided by use of an intensity electro-optic modulator (EOM) generating nearly bandwidth-limited pulses [103]. Available PPLN based amplitude modulators for 775 nm are limited in the maximal input power by approx. 20 mW and possess a typical 4.5 dB insertion loss [104]. Thus, an additional pulse amplification is required: a titan:sapphire amplifier or a semiconductor optical amplifier (SOA). Unfortunately, due to self phase modulation, the pulses are broadened after the amplification [105, 106] in a SOA. Only recently newer EOMs with better performance have become available. Now, the maximal input power can reach ≈ 100 mW at 775 nm with the same insertion loss of 4.5 dB, making the implementation of this scheme generally possible [107].

The third option for the pump system, a frequency conversion, has been implemented. It consists of a cw light source, emitting light at 1550 nm, that is optically switched by an amplitude modulator, subsequently amplified by an erbium-doped fiber amplifier (EDFA) and then frequency-doubled. Optical fiber amplifiers allow for high gains and possess much lower nonlinearities compared to SOAs, yielding nearly transform-limited pulses by such a setup [103, 108]. Due to a well-developed optical telecommunication technology operating within the C-band, most required components are available in high quality: DLs and components for fiber amplifier, wavelength division multiplexing (WDM) modules, various filters, polarization-maintaining fibers (PM fibers), single-mode fibers (SM fibers) and, finally, numerous different frequency conversion modules.

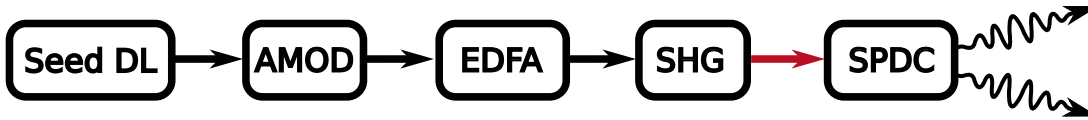


Figure 3.1.: Overview of the implemented entangled photon pair source. Seed DL: stabilized at $\lambda = 1550.5 \text{ nm}$ diode laser, delivering the signal to be amplified, AMOD: electro-optic amplitude modulator for pulse shaping, EDFA: Erbium-doped fiber amplifier, SHG: second harmonic generation, generating light at 775.25 nm (red), SPDC: spontaneous parametric down-conversion, generating two energy-time entangled photons.

The main advantage of this approach is its flexibility to adapt to different operating modes while maintaining a high spectral purity. Therefore, this scheme has been implemented and Fig. 3.1 demonstrates its overview. A frequency stabilized laser (Sec. 3.1.1) emits cw light. Optical pulses are generated by an EOM (Sec. 3.1.2), are then amplified within an EDFA (Sec. 3.1.3), followed by the light frequency conversion in a second harmonic generation (SHG) module (Sec. 3.1.4). Finally, those pulses are inserted into the SPDC module generating photon pairs (Sec. 3.2). For the time-bin encoding an additional Michelson interferometer (MI) is placed between the EDFA and the SHG module (not shown in figure). The MI is nearly identical to the interferometers (IFs) of the receivers and is described in chapter 4.

The entire setup is fiber-based. This is, i.a. necessary to comply to the safety regulations in a real world telecom environment. In order to minimize the losses, most components are spliced to each other. However, some single modules should be exchangeable, so they are connected by FC/APC connectors.

3.1. Pulsed laser source

3.1.1. Seed laser

As a laser source the frequency stabilized diode laser *Clarity NLL-1550-HP*¹ with an attached fiber optic isolator *IO-G-1550-APC*² is used. This laser emits linearly polarized light of power $P = (25.00 \pm 0.75) \text{ mW}$ at the wavelength of around $\lambda = 1550.5 \text{ nm}$. The laser can be operated either within *reference-* or *line-narrowing* modes with slightly different properties, given in table 3.1.

¹Manufactured by Wavelength References, Inc., Oregon, USA.

²Manufactured by Thorlabs, Inc.

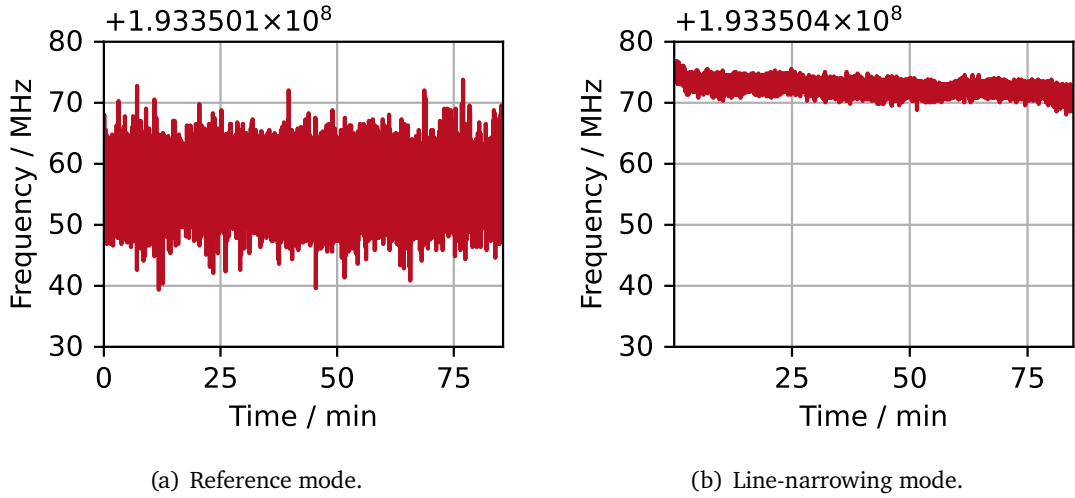


Figure 3.2.: Long term stability of the central frequency of the seed laser source.

Table 3.1.: Laser source properties in two operating modes from datasheet [111].

property	reference mode	line narrowing mode
wavelength	1550.515 61 nm	1550.5130 nm
short-term stability	<5 MHz	<1 MHz
line-width at FWHM	1 MHz	150 kHz

For frequency stabilization a gas cell containing hydrogen cyanide (HCN) is integrated into the device's chassis. The gas cell is a sealed glass tube with an aluminum housing containing 0.14 mg of HCN, stored under the pressure of 2.4 torr. This amount is considered to be harmless for humans [109]. The system is stabilized to the P11 line of the $2\nu_3$ rotational-vibrational band of $\text{H}^{13}\text{C}^{14}\text{N}$ [110], defining also the laser frequency.

The laser frequency in the reference mode $f = 193.3502$ THz lies almost exactly between the channels 33 and 34 of the C-band of the ITU-T grid, which is the international standard for spectral grids for WDM applications [81]. This is advantageous for later experiments on the Quantum Hub, as the spectra of photon-pairs generated by SPDC are symmetric around this wavelength, making their assignment to ITU-T channel pairs easier.

In the line-narrowing mode the stabilization is carried out in a different way. Here, the side of the absorption line is identified and a control loop maintains the frequency at this

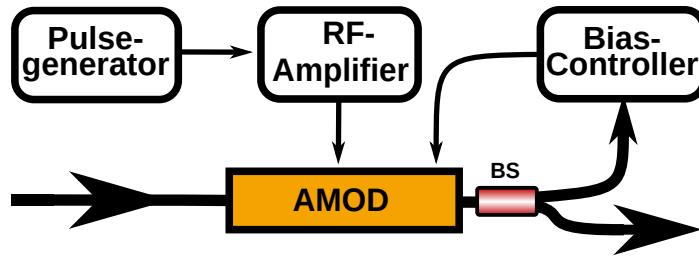


Figure 3.3.: Pulse generation module. AMOD: electro-optic modulator, rf-Amplifier: radio frequency amplifier, BS: fiber beam splitter, thick black line: optical fiber.

set point. Slight changes in ambient temperature or potential electric noise, e.g. noise coupled over the power line, may lead to a slow shift of the set frequency. In fig. 3.2(b) this shift amounts up to 4 MHz. The excellent long-term stability of the line-narrowing mode was used to analyze the phase stability of the Michelson interferometers during the development of their stabilization system.

3.1.2. Pulse generation

The pulse generation module is depicted in fig. 3.3. Blue lines denote PM fibers and black lines denote electrical connections. A fiber-pigtailed EOM *MAXAN-LN-10*³ with a nominal 10 GHz bandwidth and a nominal insertion loss of 2.9 dB shapes optical pulses from an incoming cw light beam. Required voltage for a switch from minimum to maximum transmission is around $V_{\pi} = 5.6$ V. The exact value depends on the RR of the incoming electrical pulse train. The level of this signal is adjusted by the radio frequency power amplifier (RF amplifier) *DR-DG-10-HO*⁴. The RF amplifier is powered by an additional power supply *Keithley 2231-A-30-3*⁵ (not shown in the figure).

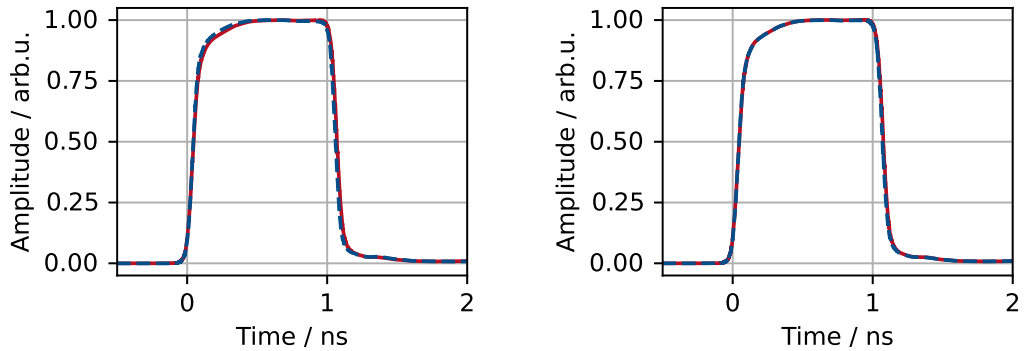
Electrical pulses are generated by a *HP 8131A High-Speed Pulse Generator*⁶ allowing to generate rectangular pulses at a RR up to 500 MHz and a pulse duration τ_{Pulse} down to ≈ 400 ps. The pulse generator can optionally generate double-pulse bursts (DPBs) with a minimal distance of 2 ns. By serial connection of two identical generators, the first generator triggers the second one and it is possible to generate bursts with four pulses (FPBs). This arrangement can be used for the QKD experiment to achieve the highest possible qubit rate by interlacing of the time-bins (see section 2.2).

³Manufactured by iXblue Photonics, France.

⁴Manufactured by iXblue Photonics, France.

⁵Manufactured by Tektronix Inc., USA.

⁶Manufactured by Keysight Technologies, Inc. (former HP and Agilent).



(a) Average shapes of single pulses for 1 MHz (red solid line) and 50 MHz (blue dashed line).

(b) Average shapes of single pulses at 1 MHz before (red solid line) and after (blue dashed line) amplification.

Figure 3.4.: Pulse shape for bursts of pulses as output from the EDFA. Pulse duration vary slightly depending on the RR.

A 90:10 fiber beam splitter *HPMFC-55-1-10-F-0.4-NNN-BBB-P-1*⁷ is attached to the EOM and the 10% output is inserted into the bias controller *MBC-DG-LAB*⁸. This device adjusts the minimum transmission voltage V_0 of the EOM, in order to prevent light leakage between the signal pulses, increasing the extinction ratio of the EOM.

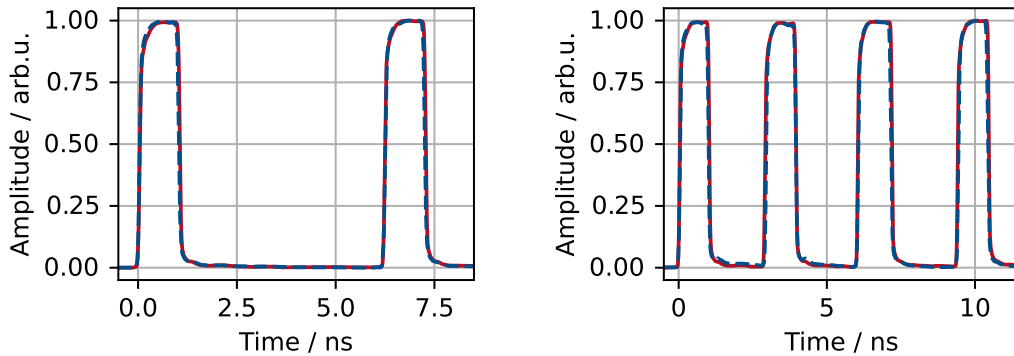
Pulse shapes for pulses at various RRs and burst configurations are shown in fig. 3.4 and fig. 3.5. In all figures the average of 1024 pulses is taken and the measurement is performed with the oscilloscope *86100B Infiniium DCA*⁹ with a $\tau_{\text{pulse,set}} = 1$ ns. All pulses are nearly rectangular shaped with almost no difference depending on the RR. Pulses amplified with an EDFA (see section 3.1.3) shown in fig. 3.4(b) are nearly identical to the original ones. The amplitudes of the pulses within one burst vary below 1 %, also for amplified pulses. The pulse duration $\tau_{\text{pulse,meas}}$ is nearly constant, except for the case of FPBs as shown in table 3.2. Here, the third pulse is significantly longer, than the others by approximately 15 %, due to an unknown reason. This must be taken in account during QKD, since the pulse energies vary corresponding to $\tau_{\text{pulse,meas}}$ (c.f. section 2.3.1).

The extinction ratio of the amplitude modulator is a very important property, especially if the pulses are designated to be amplified. While the manufacturer's data sheet states

⁷Manufactured by DPM Photonics, Inc, USA.

⁸Manufactured by iXblue Photonics, France.

⁹Manufactured by Agilent Technologies, Inc.



(a) Bursts of double pulses at 1 MHz (red solid line) and 50 MHz (blue dashed line). (b) Bursts of four pulses at 1 MHz (red solid line) and 50 MHz (blue dashed line).

Figure 3.5.: Pulse shape for bursts of two and four pulses at various RRs.

Table 3.2.: Measured FWHM pulse duration $\tau_{\text{pulse,meas}}$ of the amplified pulses at different RRs and within single-pulse (SP), double-pulse burst (DPB) or burst with four pulses (FPB). The uncertainty of the measurements amounts to 0.05 ns. $\tau_{\text{pulse,set}} = 1$ ns in all cases.

	RR / MHz	SP	DPB			FPB		
Pulse duration / ns	1	1.02	1.01	1.03	0.99	1.04	1.15	1.05
	50	1.01	0.99	1.00	0.96	1.00	1.10	0.99

the extinction ratio to be greater than 22 dB, the evaluation of fig. 3.4 leads to the value of roughly 30 dB. Further measurements in [112] evaluated the extinction rate to be 33 dB, which is a typical value for off-the-shelf amplitude modulators. The peak-to-peak timing jitter measured by the program of the oscilloscope at 50 MHz with single pulses amounts to $J_{\text{ptp}} = (80.6 \pm 4.6)$ ps. This is a small value compared to the pulse duration.

3.1.3. Erbium-doped fiber amplifier

Applications and principle of operation

Fiber amplifiers allow for light amplification in both cw and pulsed mode, provide low insertion loss, high gain (up to 40 dB [113]) as well as high power output [114] with

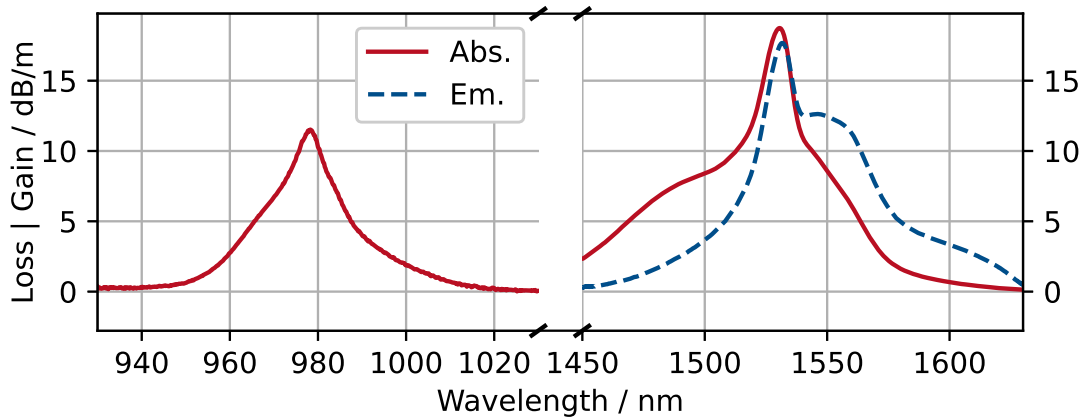


Figure 3.6.: Absorption and emission coefficients of erbium doped fiber. (Data is courtesy of Fibercore Inc.)

low excess noise (typically below 6 dB) [115] and excellent spectral properties [116]. As the name suggests, the central part of a fiber amplifier is an optical fiber doped with rare earth ions. The type of ions, i.e. their level scheme, determines the optical bandwidth for amplification and the required pump-wavelength: *ytterbium* doped amplifiers work in the range of 975-1200 nm [114], *praseodymium*-doped amplifiers work around 1300 nm (O-band) [113], *thulium*-doped amplifiers work around 1480-1530 nm (S-band) and 2000 nm [117, 118] and *erbium*-doped amplifiers in the range 1520-1600 nm (C- and L-band). While ytterbium-doped fiber amplifiers are often utilized for industrial material processing, the latter amplifiers are also intensely used within the optical communication, amplifying the optical O-, S-, C- and L- bands (see section 2.4.2).

The operation principle of a fiber amplifier is similar to a laser without a cavity. EDFA can be described as a three-level system [79, 119]. Population inversion is typically achieved by pumping with light at 980 nm or 1480 nm. Other possible pumping bands around 800 nm show much poorer performance in terms of gain and noise figure due to a high excited state absorption (ESA) [120, 121]. However, the ESA induced by pumping at 980 nm leads to a green glowing of the doped fiber during operation [122].

Example absorption and emission coefficients for a typical erbium-doped fiber are shown in fig. 3.6. The exact magnitude and the form of the absorption and emission cross section depends on the host glass material and the erbium ion concentration [79, 121]. For a given pump power and a given erbium-doped fiber type there exists an optimal

length of the doped fiber. This length corresponds to the value that should be optimized: output power, gain or noise figure [79]. For fiber lengths below 5 m pumping at 980 nm compared to 1480 nm leads to a higher gain and a lower noise figure [119]. However the quantum defect between the pump at 980 nm and the signal light at 1550 nm can lead to heat production within the doped fiber. Therefore, for high power applications, a suitable heat management needs to be implemented.

To achieve high output powers, double clad amplifiers have been developed. High power pump light is coupled into the inner cladding, while the signal light is guided in the core. The direction of the pumping light relative to the signal has a major influence on the output properties in terms of noise figure, amount of amplified spontaneous emission (ASE), gain and output power. Several studies have shown the advantages of the bidirectional pump compared to the pumping co- or contra-propagating to the seed-light [119, 123].

Structure of implemented amplifier

The implemented EDFA is built in the bidirectional pump configuration, using a polarization-maintaining erbium-doped fiber, since the frequency conversion is a polarization sensitive process. In order to minimize the losses, the fiber-pigtailed components are spliced to each other via optical fusion splicing. However, as the pigtailed fiber types usually do not match, their mode field diameter (MFD) mismatch still leads to considerable loss, especially between the erbium-doped and passive fiber.

Due to the high refractive index of the erbium-doped fiber core, in order to maintain the single-mode character of the output power, the core diameter of the fiber is significantly smaller than that of a SM fiber. For example, *DHB1500*¹⁰ has a nominal core diameter of 3 μm , while a telecom standardized SM fiber compliant to [80], i.e. *SMF-28*¹¹ has typically a core diameter of 8.2 μm . This also limits the maximum amount of power that can be guided in the core of the erbium-doped fiber to 700 mW according to the manufacturer.

The scheme of the EDFA that was built is shown in fig. 3.7. Most components are spliced to each other, except points where the flexibility of the source required the use of FC/APC connectors (denoted as blue points). The fibers are connected via mating sleeves *ADAFCPM2*¹² that are suitable for PM fibers.

The seed DL is described in section 3.1.1 and the optional pulse generating source has already been described in section 3.1.2. The pumping lasers and other attached devices for bidirectional pumping are identical: DL A and DL B, operating at 980 nm¹³

¹⁰Manufactured by Fibercore Inc.

¹¹Manufactured by Corning Inc.

¹²Manufactured by Thorlabs Inc.

¹³LU0975M500-1316N10A, manufactured by Lumics GmbH.

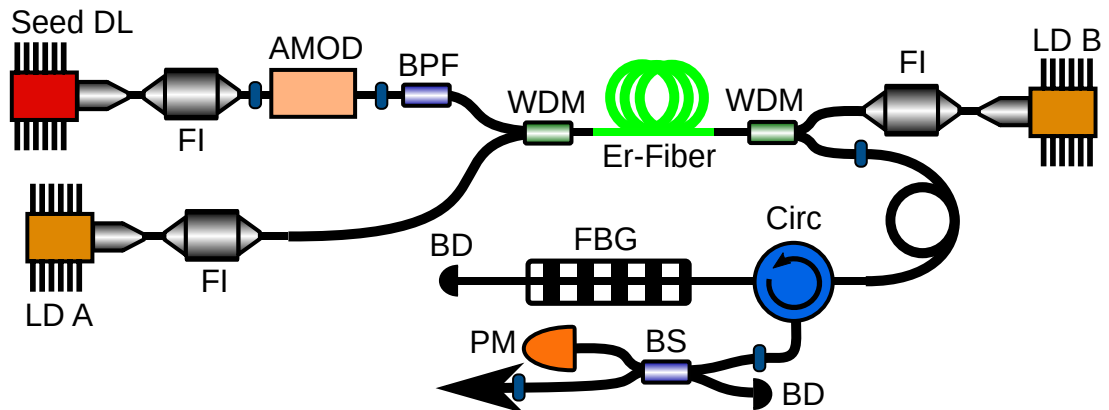


Figure 3.7.: Pumping laser system before frequency conversion. Seed DL: frequency stabilized laser, FI: Faraday Isolator, AMOD: electro-optic modulator for amplitude modulation, BPF: band-pass filter, WDM: wavelength-division multiplexer, Er-Fiber: erbium-doped fiber, DL A, DL B: pumping diode lasers, Circ: circulator, FBG: fiber Bragg grating, BS: beam splitter, PM: power meter, BD: beam dump, blue points: FC/APC connectors.

and emitting 0.5 W are set in temperature stabilized mounts¹⁴ and controlled by the self-made temperature and current controllers. In order to maintain a stable operation of the pumping lasers, a Faraday isolator (FI)¹⁵, blocking blocking counter-propagating light at 980 nm and a band-pass filter (BPF)¹⁶ (removing light at 1520-1620 nm) are inserted to the light path for filtering out the undesired light from the EDFA that might return back into the lasers. After passing those filters, the light is inserted into the erbium doped fiber *PM-ESF-7/125*¹⁷ by WDM modules¹⁸. All fiber coupled devices suffer from high insertion loss, typically in the range of 0.3-1.2 dB. As a result only around 0.3 W of pumping light from each pumping laser is inserted into the doped fiber and is usable as pump power.

The length of the erbium-doped fiber is (1.04 ± 0.01) m. This length turned out to be nearly optimal for cw operation with this pump power as determined experimentally. Additionally, different techniques were applied as described in section 2.4.5, in order to

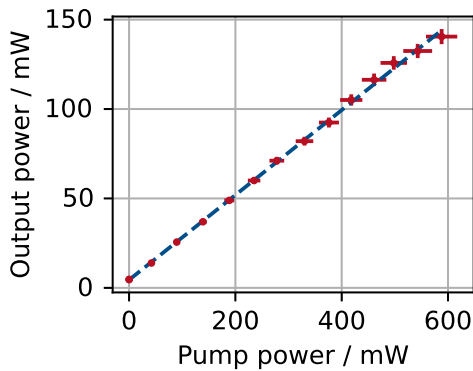
¹⁴*LM14S2*, manufactured by Thorlabs Inc.

¹⁵*IO-J-980APC*, manufactured by Thorlabs Inc.

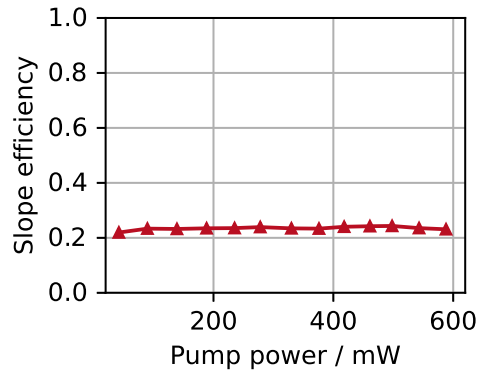
¹⁶*PMBPF-9855-30-80-NN-BB-1*, manufactured by DPM photonics, Inc.

¹⁷Manufactured by Nufern Inc.

¹⁸*PMWDM-P-1x2-980/1550-0-623-3.0x54-1m*, manufactured by AMS Technologies AG.



(a) Power characteristic of the spliced EDFA. The blue line is a linear fit to measured data (red).



(b) Slope efficiency of the spliced EDFA. No sign of saturation can be found.

Figure 3.8.: Performance of the spliced EDFA in cw operation regime.

minimize the MFD mismatch losses, since the core diameter and numerical aperture (NA) of the active and passive fibers are not matching.

Behind the amplifier, the residual pump light and ASE should be filtered out. For this purpose, a high power optical circulator¹⁹ with PM fibers and blocked fast polarization axis is attached. At port 2 of the circulator, the fiber Bragg grating²⁰ optimized for 1550.5 nm and with a reflection width of 1 nm full width at half maximum (FWHM) is reflects the amplified signal back into the circulator [124]. The potential ASE and residual pump light is collected by a beam dump²¹. Behind the circulator, a 90:10 beam splitter (BS) is attached. The 10% output allows for for the real-time analysis of the output signal, e.g. power, pulse-form or optical spectrum. The amplified light for further experiments comes from the 90% output port.

As already mentioned, the implemented EDFA can be operated both in cw as well as in pulsed mode. In the following sections, the properties of the described amplifier for these two operation modes are discussed.

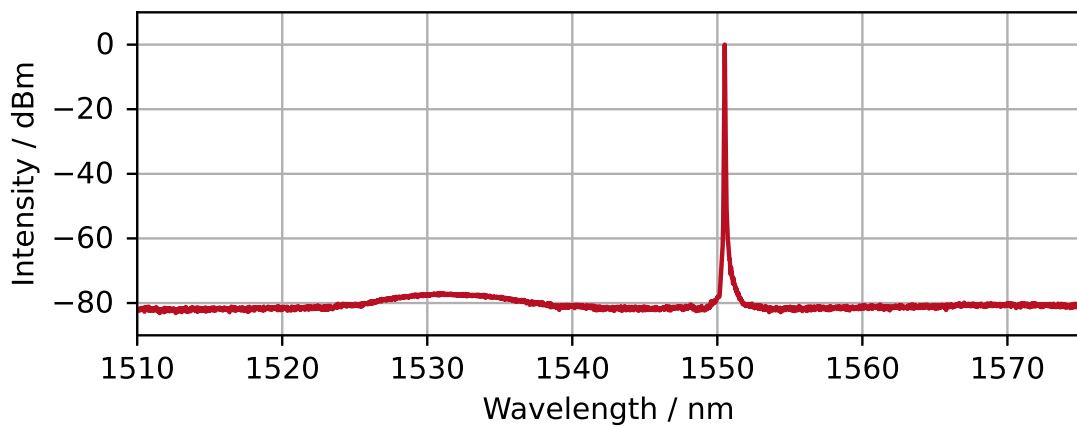


Figure 3.9.: Optical spectrum of the EDFA in cw operation regime. ASE around 1530 nm is suppressed by 77 dB.

Performance of the amplifier in cw operation mode

In cw mode the EDFA was seeded by the DL described in section 3.1.1 with $P_{\text{in}} = (25.00 \pm 0.75)$ mW without the pulse generating stage. The output power P_{out} is measured at the output of the circulator.

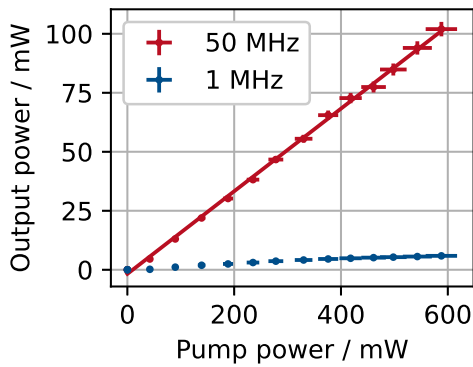
In fig. 3.8 the characteristic curve and the conversion efficiency of the EDFA in cw operation mode is given. In fig. 3.8(a) the fitted linear function (blue) is in good agreement with the data points (red). The resulting slope efficiency is $\eta_{\text{sl,cw}} = (23.73 \pm 0.22)$ %. The maximum achieved power amounts to $P_{\text{out}} = (140.5 \pm 4.2)$ mW. In fig. 3.8(b) the conversion efficiency as a function of pumping power is shown. It is nearly constant around 23 %, and, thus, has no evidence of saturation. Therefore, the achieved gain of the amplifier $G = P_{\text{out}}/P_{\text{in}} = 7.7$ dB could be increased by increasing the pump level.

The spectral properties of the output light are excellent (see fig. 3.9), showing an ASE suppression of at least 77 dB. This is a second indication of the EDFA operation far from its saturation regime, since no noise is observable.

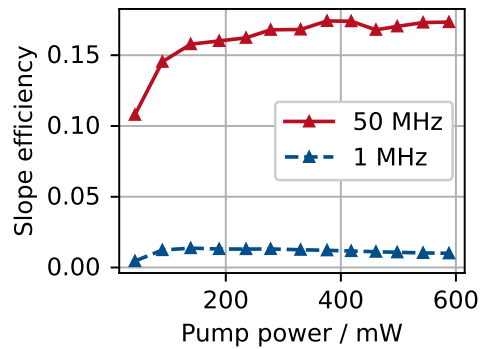
¹⁹HPPMCIR-4-A-1550-F-0-623-P(1)-2W-5.5x35-1m, manufactured by AMS Technologies AG.

²⁰Manufactured by Advanced Optics Solutions GmbH.

²¹FTAPC1, manufactured by Thorlabs Inc.



(a) Power characteristic of the spliced EDFA.



(b) Conversion efficiency of the spliced EDFA.

Figure 3.10.: Performance of the spliced EDFA in pulsed operation regime for 1 ns long pulses.

Performance of the amplifier in pulsed operation mode

Bursts of different pulse numbers at various RRs as seeding light, lead to a large variation of the output performance of the EDFA. In fig. 3.10 the characteristic curve and the conversion efficiency for two parameter settings are shown, indicating the upper and an exemplary lower limit of the EDFA performance. For the lower limit single pulses at 1 MHz are used. The upper bound is defined by the maximal possible burst number (FPB) and RR of the electronic pulse generators (50 MHz). Here, a slope efficiency of $\eta_{sl,pulsed} = (17.17 \pm 0.16)\%$ was achieved. Maximum observed gain in pulsed mode amounts to 28 dB for single pulses at 1 MHz, which is a typical gain value for EDFAs. Also in this case there is no sign of saturation visible, since the conversion efficiency in fig. 3.10(b) never drops.

Since the pulse duration within the same burst slightly varies around one nanosecond according to table 3.2, the pulse energies, calculated from those pulse duration values and mean output power vary correspondingly up to 15%. The values are shown in table 3.3. Such a huge variation must be taken into account during QKD experiments. The pulse shape after the amplification remains nearly identical, as shown in fig. 3.4(b).

Low seeding intensities from single pulses lead to higher intensity of ASE as can be seen in fig. 3.11. The ASE suppression is still more than 60 dB in this case, which is less than the 75 dB measured for FPB at 50 MHz that are comparable to cw operation. The observed

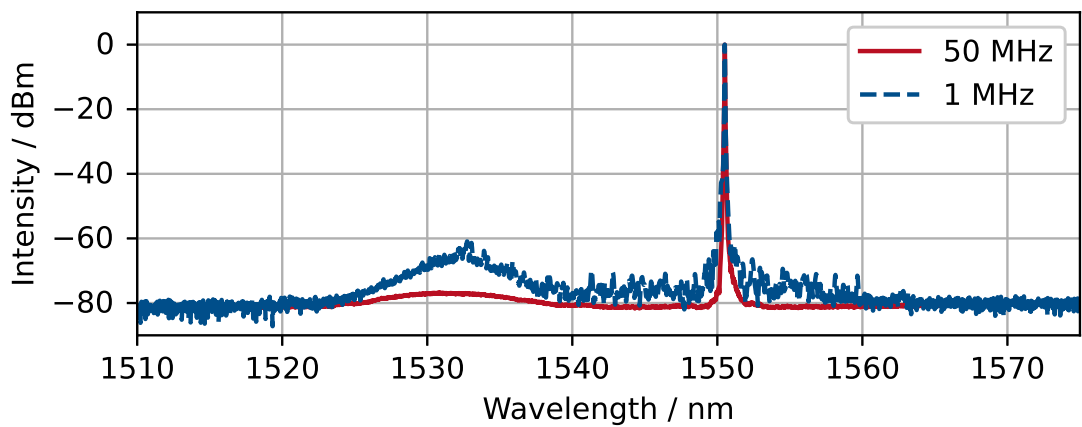


Figure 3.11.: Optical spectrum of the EDFA in the pulsed regime for 1 ns long pulses.

suppression is sufficient to prevent any disturbing effects at the frequency conversion stage, which can be seen in section 3.1.4.

Long-term stability of the fiber amplifier

Unfortunately, an additional challenge arose while splicing the erbium-doped fiber to the passive fibers of the WDM modules: polarization fluctuations of the output light. This issue was observed while using several types of erbium-doped fiber: *DHB1500* (bow-tie shaped fiber) as well as *PM-ESF-7/125* (panda shaped fiber) and the passive fiber *SM15-PS-U25D* (panda shaped fiber). The cross section of all three fibers i.e. the core diameter and the position and size of the stress elements, are different. It is highly likely that melting of stress elements in combination with the MFD loss minimizing procedures lead to a non-uniform splice, resulting in a coupling of the adjacent polarization modes, that in combination with thermal fiber expansion leads to polarization instabilities inside the fiber.

Optimizing of the splice programs did not lead to a measurable improvement. Introducing FC/APC connectors at the critical point would not solve this issue, since the connectors still have some orientation misalignment (see section 2.4.5) and the MFD mismatch would lead to larger losses. Therefore, an active power stabilization scheme was implemented. A polarization filter blocking the fast axis was integrated in the circulator at the output of the EDFA. Thereby, the polarization direction is fixed but polarization instabilities of

Table 3.3.: Measured pulse energies E_{Pulse} in nanojoule for pulses at different RRs and bursts with different pulse numbers. The pulse energies within single bursts vary up to 15 %.

	1 MHz	50 MHz
Single pulses	5.89 ± 0.18	1.43 ± 0.04
DPB, pulse 1	5.26 ± 0.20	0.876 ± 0.034
DPB, pulse 2	5.31 ± 0.20	0.885 ± 0.034
FPB, pulse 1	4.18 ± 0.20	0.483 ± 0.024
FPB, pulse 2	4.39 ± 0.21	0.504 ± 0.024
FPB, pulse 3	4.86 ± 0.21	0.554 ± 0.025
FPB, pulse 4	4.43 ± 0.21	0.499 ± 0.024

the input light are converted to power fluctuations. At the reference output of the EDFA a polarizing beam splitter (PBS)²², an attached photo diode and a transimpedance amplifier provide a voltage proportional to the incident intensity. The signal of the photo diode is evaluated by the PID regulator implemented in Python on a Raspberry Pi (RPI), model 3B. A more detailed description of the entire system can be found in appendix A.

In fig. 3.12 an exemplary performance of the EDFA with and without the stabilization system is shown. Intensity fluctuations of the unstabilized amplifier of about 10 % can be observed. Those fluctuations occurred on two time scales: fast (1 s) and slow (10 min). While the slow drift can be explained by the change of the ambient temperature and by the heat produced by the quantum defect of the EDFA, the fast drifts occur randomly and can be explained by the mechanical vibrations of the set-up and hence abrupt movement of the fiber, when the air conditioning is turned on and the air stream interacts with the fiber. The stabilized performance of the EDFA in cw operation regime, also shown in fig. 3.12 (red line), shows intensity fluctuations of 2 % peak-to-peak. For stabilization at any given intensity, new stabilization parameters must be found. Simple shielding of the EDFA by metal plates could also reduce the very fast oscillations.

²²PBC1550PM-APC manufactured by Thorlabs Inc.

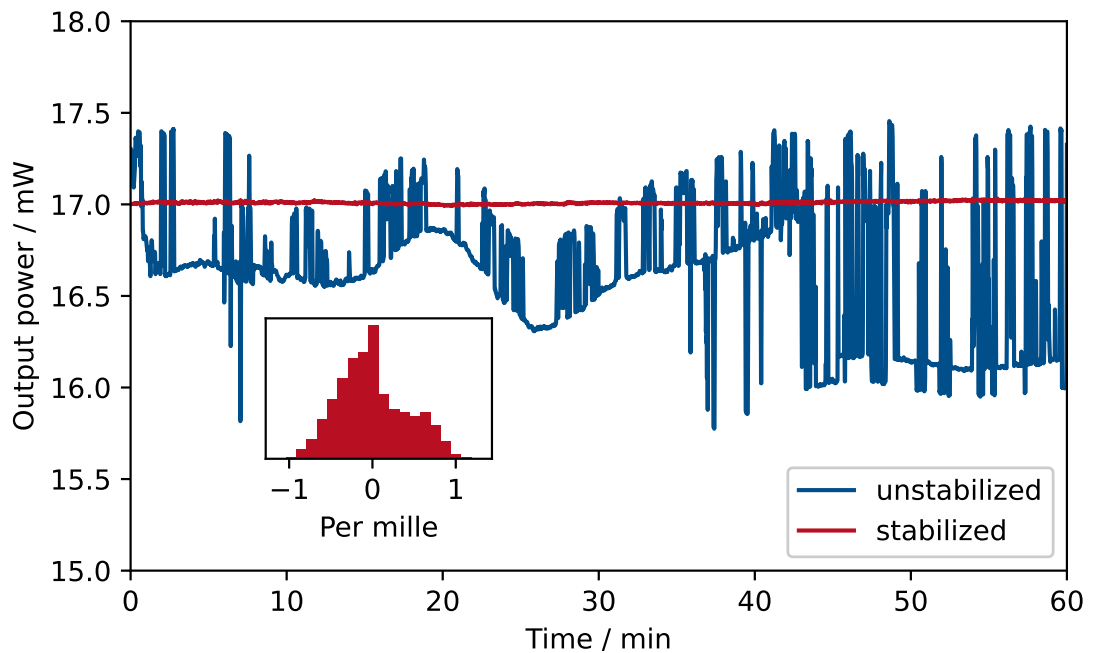


Figure 3.12.: Stability of the EDFA during cw operation for an arbitrarily chosen power. The inset shows a histogram of the stabilized case. Measured at the output of a polarizing beam splitter with an acquisition rate of 1 Hz.

3.1.4. Fiber-coupled frequency conversion module

Second harmonic generation

A phenomenon widely used in modern optics is the frequency conversion using birefringent optical crystals. Fast progress in the investigation of these phenomena was possible after invention of lasers [125] that provide high electric field amplitudes, required to generate a noticeable *non-linear* electric polarization \mathbf{P} within the crystals or other dielectric materials. In this case, polarization may be written as a Taylor series [70]:

$$\mathbf{P} = \epsilon_0 \left[\chi^{(1)} \mathbf{E}(t) + \chi^{(2)} \mathbf{E}^2(t) + \chi^{(3)} \mathbf{E}^3 + \dots \right], \quad (3.1)$$

with $\chi^{(1)}$ being the *linear* and $\chi^{(2)}$, $\chi^{(3)}$ etc. the non-linear optical susceptibility tensors of the third and fourth rank correspondingly [70]²³. For an incident plane light wave $E(t) = E_0 e^{-i\omega t} + c.c.$ the second order polarization becomes:

$$\mathbf{P}^{(2)} = \epsilon_0 \chi^{(2)} \mathbf{E}(t)^2 = \epsilon_0 \chi^{(2)} \left[\underbrace{\mathbf{E}_0^2 e^{i2\omega t} + c.c.}_{\text{second harmonic generation}} + \underbrace{2\mathbf{E}_0 \mathbf{E}_0^*}_{\text{optical rectification}} \right] \quad (3.2)$$

with the first term oscillating at twice the frequency of the incident wave. This term is denoted as second harmonic generation (SHG). The other term, optical rectification, is a further effect, that might be used e.g. for terahertz radiation generation [126]. Other non-linear effects exist, like *sum-* or *difference-frequency generation*, *optical parametric oscillation*, *Kerr-effect* etc. [70, 127], but are not required for this work. Some of those non-linear effects might be described in a semi-classical approach, where an incident light wave of high intensity induces an electron oscillation that generates a light wave with a wavelength distinct from the incoming one [70].

From the quantum mechanical point of view, during SHG two pump photons annihilate, generating a photon with the doubled frequency, ensuring the energy conservation [70]. This can be expressed for an arbitrary non-linear effect with three waves:

$$\omega_1 = \omega_2 + \omega_3 \quad (3.3)$$

For SHG it holds $\omega_1 = 2\omega_2$ with $\omega_2 = \omega_3$. Besides the conservation of energy, the conservation of momentum must be considered, taking into account the wave vector of the interacting waves \mathbf{k} with $k = \omega \cdot n(\omega)/c_0$:

$$\mathbf{k}_1 = \mathbf{k}_2 + \mathbf{k}_3 \quad (3.4)$$

For collinear wave vectors, this reduces to $\omega_1 n(\omega_1) = \omega_2 n(\omega_2) + \omega_3 n(\omega)$ and for SHG, finally, to $n(\omega_1) = n(2\omega_1)$, i.e. the refractive indices for fundamental and second harmonic wave must be equal.

In the general case of non-collinear wave vectors, there exist three methods for the phase matching function $\Delta k = |\mathbf{k}_1 - \mathbf{k}_2 - \mathbf{k}_3|$ to disappear: *critical*, *non-critical* and *quasi-phase matching*. For the critical phase matching, the crystal symmetries and correct orientation of the optical crystal according to the fundamental and SHG light are important. Non-critical phase matching exploits the temperature dependence of the refractive index of the crystal. Finally, the quasi-phase matching uses a periodic poling of the crystals as the crystals susceptibility $\chi^{(2)}$ is section-wise inverted within the crystal [70, 128]. All these

²³One should not mix up the tensor product used in this equation with the scalar product.

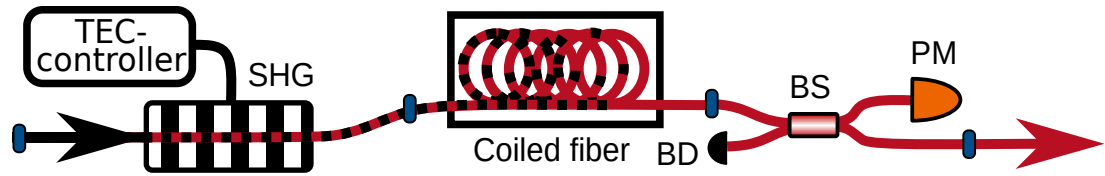


Figure 3.13.: Scheme of the SHG part of the set-up. The fundamental wave at 1550 nm (black) is going through the non-linear crystal (SHG), generating light at 775 nm (red) and being filtered out in a coiled fiber, that is put in a box absorbing the dissipated light for security reasons. After the filtering, in a 90:10 beam splitter (BS), the generated light intensity is observed in a power meter (PM), the last port is coupled to a beam dump (BD). The SHG-module is controlled in temperature by a thermoelectric cooler (TEC)-controller. Blue marks denote the fiber connections via FC/APC connectors in mating sleeves.

methods possess different advantages and disadvantages and their application strongly depends on the properties of the crystal that is used. Quasi-phase matching allows for the use of materials with higher nonlinear coefficients, but without possibility for critical or non-critical phase-matching.

The conversion efficiency within some crystals can be dramatically increased by confining the light in waveguides. In contrast to a free space wave, having it highest intensity within its Rayleigh length around the focus, waveguides spatially confine the pumping beam to an area of a few square micrometers throughout the entire crystal length [129]. One of the best performing waveguides developed so far are the *ridge* waveguides – a thin rim (around 10 μm), cut from the surface of the crystal, having a higher refractive index difference to the outside medium than the *indiffused* waveguides.

For the presented experiment the frequency transition from 1550 nm to 775 nm and back is required. For this the quasi-phase matched crystal PPLN was considered due to its excellent non-linear efficiency and high damage threshold.

In fig. 3.13 the setup for SHG generation is shown. Here, the pumping light at 1550 nm is inserted into an zinc-oxide doped PPLN ($\text{ZnO}:\text{LiNbO}_3$) of 34 mm length²⁴. This is a fiber-coupled crystal with a ridge waveguide and angled-cut anti-reflection coated facets that is used for type-0 SHG. Doping of the PPLN with magnesium oxide or zinc oxide reduces the so-called photodarkening effect: the photorefractive damage due to *green-* or *blue-induced*

²⁴WH-0775-000-F-B-C, Manufactured in 2018 by NTT Electronics Corp., Yokohama, Japan.

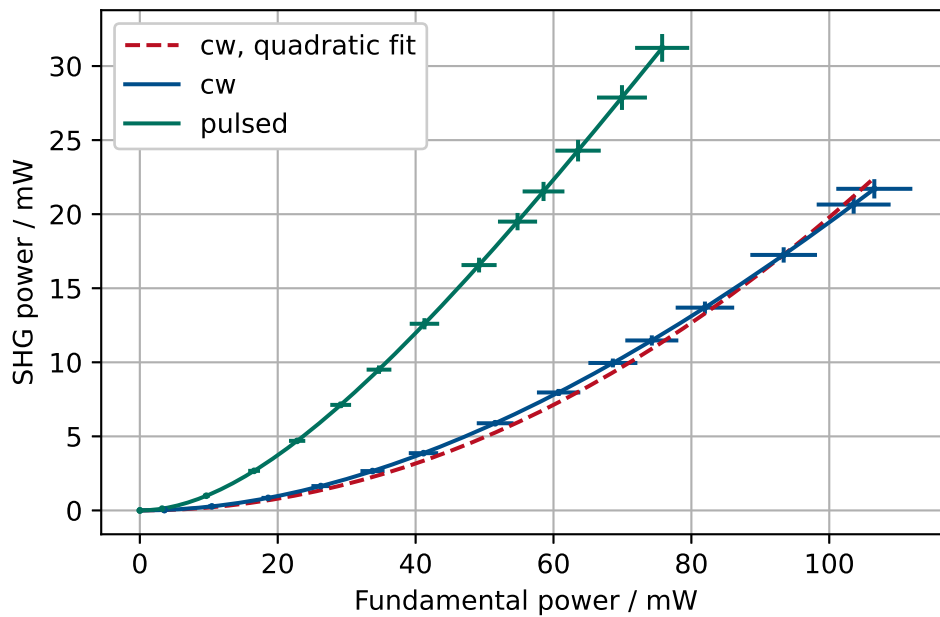


Figure 3.14.: Average optical power of SHG light in the cw (blue solid and red dashed line) and pulsed (green line, FPB at 50 MHz and 1 ns) regimes as a function of the average fundamental power. Red dashed line denotes a fit with eq. (3.5), green and blue lines denote a fit with eq. (3.7) to pulsed and cw operation data correspondingly.

infrared absorption [130]. Type-0 process means, that the polarization of the generated photons is parallel to the polarization of the incident pump photon.

This crystal is stabilized in temperature by the TEC Controller *TED200C*²⁵ at $T_{op} = 43.5^\circ\text{C}$. The remaining pump light is filtered by a tightly coiled fiber (see section 3.1.4). Subsequently, a 90:10 fiber beam splitter was placed for monitoring the 775 nm light intensity. This value can be used for the stabilization of the pump power, as described in section 3.1.3.

This setup is operated in both modes, cw as well as pulsed. Since the efficiency of the SHG process is for low pump powers proportional to the squared amplitude of the fundamental wave, the efficiency of the pulsed operation is expected to be much higher than that of the cw operation mode. This can be observed in fig. 3.14.

²⁵Manufactured by Thorlabs Inc.

Already from eq. (3.2) it may be expected, that the SHG electric field amplitude is proportional to the squared field amplitude of the fundamental wave. Generally, it is possible to give an explicit analytic formula for the SHG output power for free space crystals [70, 131]:

$$P_{\text{SHG}} = \eta P_{\text{fund}}^2 \quad (3.5)$$

with η being the *Boyd-Kleinman* efficiency, that is a function of the nonlinear crystal coefficient, refractive indices of the interacting waves, pump wavelength, crystal length and the focus parameters for the crystal. Taking into account the pump depletion of the fundamental wave, reducing the available pump power along the crystal, the SHG power amounts to [132]:

$$P_{\text{SHG}} = \tanh^2 \left(\sqrt{\eta P_{\text{fund}}} \right) P_{\text{fund}}. \quad (3.6)$$

The explicit formula for η from [131] does not fit to the used fiber coupled crystal with a waveguide, but the estimation still holds true. Furthermore, the coupling efficiencies for the optical fibers c_{in} and c_{out} must be taken into account. Thus, the expected output power of the crystal is given by:

$$P_{\text{SHG}} = c_{\text{out}} c_{\text{in}} \tanh^2 \left(\sqrt{\eta c_{\text{in}} P_{\text{fund}}} \right) P_{\text{fund}}. \quad (3.7)$$

In fig. 3.14 the achieved mean SHG power for cw and pulsed operating modes are shown. Data obtained in the cw operation mode are shown in blue. Red dashed curve is a fit of eq. (3.5), yielding $\eta = (1.979 \pm 0.022)/\text{W}$ or $\eta = (198 \pm 2) \%/ \text{W}$, which is higher, than the data sheet value of 50 %/W.

Another curve fitted on the same data is given by eq. (3.7). However, for obtaining realistic fit parameters with small errors, some further simplification had to be done, e.g. the coupling coefficients were set equal: $c_{\text{in}} = c_{\text{out}}$. It can be clearly seen, that this model fits the data better than eq. (3.5). This means, that the effect of pump depletion must be taken into account already during cw operation regime.

Green color denotes the data for pulsed operation mode with FPB at 50 MHz and 1 ns and a fit by eq. (3.7). This operation mode shows the maximal mean power that can be achieved by the current setup, so no other pulsed mode configurations will be discussed. For the correct fit, the pulsed nature of the pumping light must be taken into account. Assuming square shaped pulses of 1 ns duration (cf. section 3.1.2) the effective fundamental power is calculated by:

$$P_{\text{fund}} = \frac{P_{\text{measured}}}{f_{\text{RR}} \cdot \tau_{\text{fund}}} = \frac{P_{\text{measured}}}{4 \cdot 50 \text{ MHz} \cdot 1 \text{ ns}} = \frac{P_{\text{measured}}}{0.2}. \quad (3.8)$$

Table 3.4.: Fit parameter results for SHG with model eq. (3.7) for cw and pulsed operation mode with FPB at $f_{RR} = 50$ MHz and $\tau_{fund} = 1$ ns.

mode	c_{in}	η
cw	0.7394 ± 0.0007	$(6.39 \pm 0.02)/W$
pulsed	0.7506 ± 0.0002	$(5.72 \pm 0.01)/W$

The same must be applied to the mean power of the converted light.

The fit parameter values are shown in table 3.4. As expected, the coupling efficiencies as well as the conversion efficiencies for the cw and pulsed case are similar. The maximal SHG power obtained during this experiment amounts to $P_{SHG,cw} = (21.71 \pm 0.65)$ mW for cw mode and $P_{SHG,pulsed} = (31.51 \pm 0.94)$ mW for the pulsed mode. This leads to a maximum peak power of approximately $\hat{P} = 157$ mW, assuming the square shaped pulses of one nanosecond duration. The pulse duration variation within the single pulses of one burst is expected to be comparable with pulse duration reduction due to SHG. Therefore, it will not be discussed further here.

An optical spectrum for the SHG wave is shown in fig. 3.15. It is identical for both operation modes, cw and pulsed and shows excellent purity. Within the entire range of the optical spectrum analyzer of 700 – 1600 nm, no light at any wavelengths except the peaks at the SHG and fundamental wavelengths can be observed. The SHG peak is very symmetric, presenting a single mode at 775.25 nm. Although the 1550.5 nm light is filtered out with a suppression of more than 79 dB (see section 3.1.4), a peak is visible at this wavelength. It is a well-known artifact of the optical spectrum analyzer due to second-order diffracted 775.25 nm light [133].

Filtering of the fundamental light

For filtering of the fundamental light after the SHG module, the macrobending induced wavelengths dependent loss within the fiber was used. In a bent fiber the geometric shape of the fiber changes, leading to an asymmetry of the optical paths within the fiber, depending on the transverse position of the fiber. Additionally, the refractive index changes due to the mechanical compression on the inner side and stretching on the outer side of the curve. This causes a leakage of light, that affects mostly the higher propagation modes and modes with big MFD. The losses are proportional to the wavelength and the curvature of the waveguide. For the loss estimation the properties of the fiber such as the

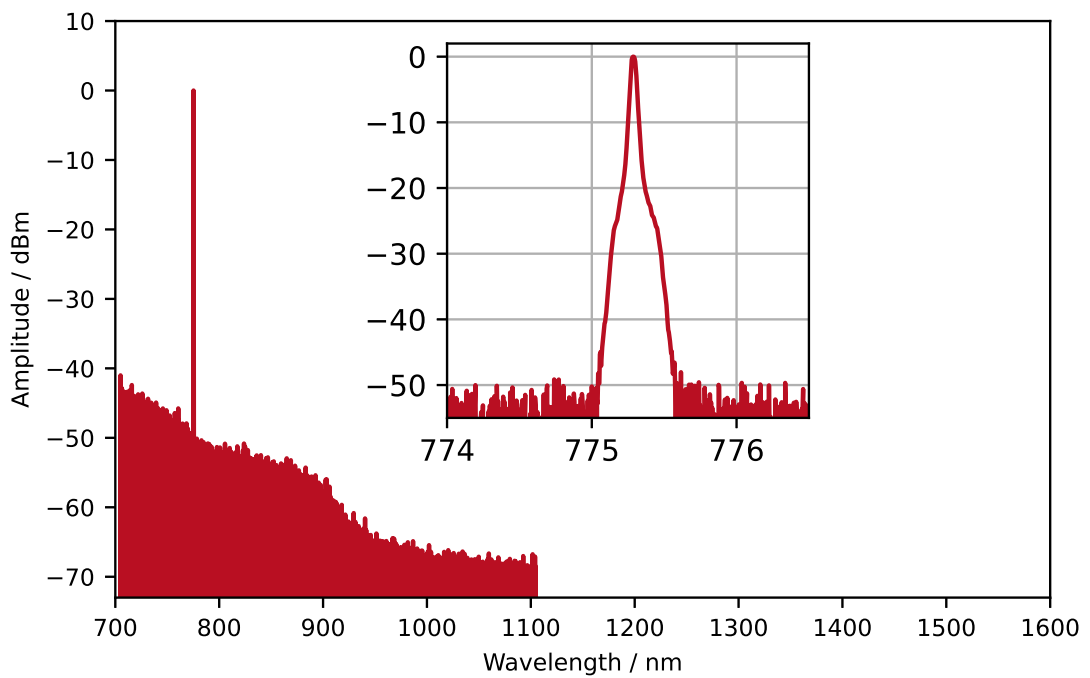


Figure 3.15.: Optical spectrum of the SHG in both, pulsed and cw regimes. The peak at 1550 nm is an artifact caused by the second order of diffraction of 775 nm in the optical spectrum analyzer (OSA).

core diameter and the refractive indices of core and cladding at the desired wavelength have to be known [134–137].

While this phenomenon is considered as disturbing in optical communication systems (it can be even used for eavesdropping of classical communication [138]), it can be used for construction of band-pass filters [139]. In the process, the wavelengths below the fiber's cutoff are filtered out due to the increased loss of high LP modes. The upper pass bound wavelength consists of an exponential decay, or (in logarithmic depiction) a flat edge with a slope dependent on the coil radius, and the number of coils [135–137, 139].

In the described experiment, 5 m of the tightly coiled PM fiber *PM780-HP*²⁶ was utilized. A black anodized cylinder with a diameter of 31 mm was used as a coil. The fiber was

²⁶Manufactured by *Nufern, Inc.*

wound around the cylinder and put into a light-proof black box that absorbs the dissipated pump light.

To estimate the filtering efficiency several tests have been conducted: measurement of the attenuation at 1550 nm, measurement of the attenuation at 775 nm and polarization maintaining properties of the coiled fiber. For those tests the EDFA in the cw regime and the powermeter *S132C*²⁷ as a detector were utilized. Inserting light at 1550 nm or 775 nm into the loose fiber and the coiled two meter long fiber, measuring the transmitted power and comparing the results, we could determine the associated losses. For the 1550 nm we estimate in this way the lower limit of the discrimination to 79 dB and for 775 nm the insertion loss is at <0.5 dB. Additionally, no polarization cross-talk in the coiled fiber was observed.

For the experiment, a five meter long fiber has been used for the filtering of the fundamental light, which is 2.5 times longer than the tested fiber. A corresponding increase of the fundamental light suppression is expected.

3.2. Spontaneous parametric down-conversion

As already discussed in section 2.2, one of the central parts of the experiment is the spontaneous parametric down-conversion (SPDC). It is a non-linear process that, unlike second harmonic generation (SHG), can only be described by quantum mechanics (see section 2.3.1). For the present experiment, SPDC generates energy-time entangled photons, that are subsequently used as qubits.

In fig. 3.16 the setup used for SPDC is shown. Here, a magnesium oxide doped PPLN²⁸ (MgO:LiNbO₃) of 24 mm length is used. This crystal is a fiber-coupled crystal with a ridge waveguide of $10 \times 10 \mu\text{m}^2$ cross-section, that is used for type-II SPDC, i.e. the polarization of the generated photons are orthogonal to each other. A TEC controller *TED200C*²⁹ stabilizes the crystal temperature at $T_{\text{SPDC}} = 40^\circ\text{C}$, at which wavelength degenerate photons at $\lambda_i = \lambda_s = 1550.5 \text{ nm}$ are emitted, as was shown by Daniel Hoffmann in his Master's thesis [140].

After the crystal, a series of filters is placed for the pump light suppression while keeping the generated qubits. The first band pass filter³⁰ is of 5 nm width in order to let only the degenerate or nearly degenerate entangled photon pairs pass. The suppression around the pass band amounts to at least 45 dB for the wavelength 1400 – 1620 nm [141]. The long

²⁷Manufactured by *Thorlabs, Inc.*

²⁸*RDC-T0775-P15P78AL0*, manufactured by AdvR, Inc., Bozeman, USA.

²⁹Manufactured by *Thorlabs, Inc.*

³⁰*PMBPF-1550-5-13.5-NN-BB-1*, manufactured by DPM photonics, Inc.

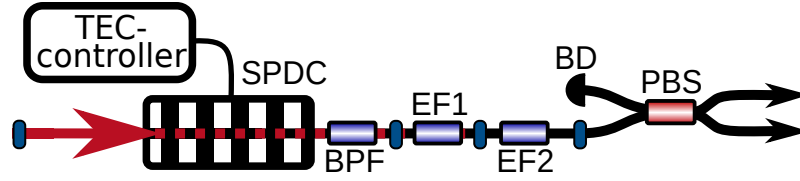


Figure 3.16.: Scheme of the components used for SPDC. Red line: light at 775 nm , black line: light at 1550 nm , SPDC: non-linear crystal, TEC-controller: temperature stabilization system, BPF: 5 nm band-pass filter, EF1, EF2: long-pass filters, PBS: polarization beam splitter, BD: beam dump for light isolation, blue points: FC/APC connectors.

pass filters³¹ possess a stop band isolation in the range 770 – 980 nm a 62 dB suppression according to their datasheet. Some tests carried out by Maximilian Tippmann measured a suppression of approximately 68 dB and 71 dB [141].

After the filtering, a fused fiber polarization splitter *PFC1550A*³² is placed for separation of qubits corresponding to each other and subsequent routing to Alice and Bob.

With the method discussed in section 2.3.2 the overall photon pair generation efficiency η_{SPDC} can be determined:

$$\eta_{\text{SPDC}} = \frac{N_{\text{SPDC}}}{N_{\text{pump}}} = (5.174 \pm 0.050) \times 10^{-10} \quad (3.9)$$

This value is a slope of the linear fit of the number of generated pairs and the pump power, shown in fig. 3.17. This value must be treated with caution for several reasons. On the one hand some spurious photons from the pulsed source are still present at the crystal output, that are hard to quantify and eliminate. On the other hand, the detector performance efficiency was assumed to be corresponding to the set value and the probability for afterpulses was assumed to be vanishing, i.e. no spontaneous electric pulses after the pulse of a real photon occurred. However, those effects are not negligible, as was shown later by Philipp Kleinpass and Maximilian Mengler [112, 142]. The corrected efficiency value was measured later to $\eta_{\text{SPDC,corrected}} = (7.6 \pm 0.5) \cdot 10^{-10}$ by Erik Fitzke.

The internal arrival probabilities per channel extracted from the model in section 2.3.2 amount to $V_1 = (0.15862 \pm 0.00005)$ and $V_2 = (0.22836 \pm 0.00008)$, which means that less than one quarter of all generated photons arrive at the detectors. Here, the detector efficiencies were taken in account. The chain of the applied filters and PBS add up to

³¹*PMBPF-1550-20-210-NN-BB-1*, manufactured by dpm Photonics, Inc.

³²Manufactured by Thorlabs, Inc.

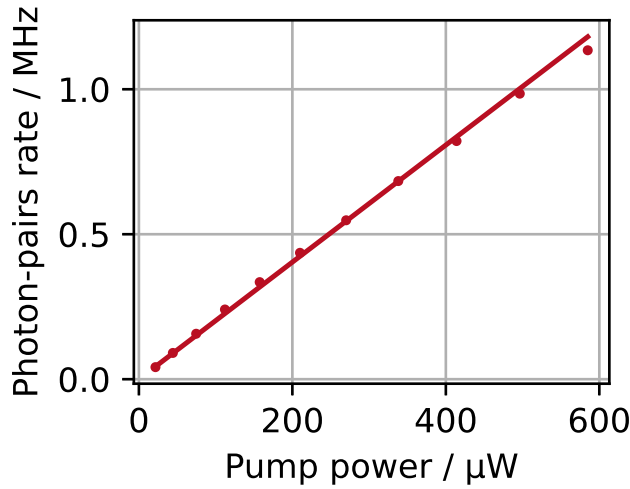


Figure 3.17.: Photon pair generation rate as a function of the pump power. Uncertainties are smaller than the data points.

2.36 dB insertion loss, further estimating a loss of 0.2 dB for each FC/APC connectors and assuming a coupling efficiency of 50 % from crystal facet to optical fiber, an overall loss of 6.16 dB corresponding to $\approx 24\%$ transmission is explained, that roughly matches the calculated values for photon arrival probabilities.

As discussed in section 2.2, it is important to know the mean photon pair number per pulse μ generated by the pulsed source at various configurations. It can be calculated by:

$$\mu = \eta \frac{\lambda_{\text{pump}}}{c_0 h} \frac{P_{\text{mean}}}{f_{\text{RR}}}, \quad (3.10)$$

with c_0 - the speed of light, h - Planck constant and P_{mean} - mean pump power at the wavelength λ_{pump} with the repetition frequency f_{RR} . For the configuration from the previous section 3.1.4 the achievable mean photon pair number per pulse $\mu = 0.468$ is more than sufficient for the planned QKD experiment.

4. Receiver modules

In the present chapter the setup and the properties of the receivers are explained. First a short overview of alternative implementations of the receiver is given and the motivation for the chosen solution is elaborated. Then, the implemented setup and its properties are discussed.

The general setup of a receiver consists of several parts and is depicted in fig. 4.1. As already explained in section 2.3, for the two photon interference each receiver possesses an imbalanced Michelson interferometer with an arm-length difference introducing a time delay longer than the pump pulse duration and should allow for fine adjustment of the phase. The qubits are detected at the outputs of the interferometers by single photon detectors. The arrival times and the detector number are evaluated by a time-tagging module and the events are evaluated by the computer. For maximal visibility of the two-photon interference (TPI) the arm-length differences of all interferometers should be identical (cf. section 2.2).

For the timing evaluation of detected events it is often required to have a time synchronization channel between the communication parties and the source (not in fig. 4.1), that is either a GPS or an atomic clock or a light pulse train being distributed via a separate channel parallel to the quantum channel.

For practicability reasons receivers are mostly all-fiber based [20] or implemented within integrated chips [22]. Both methods have their advantages and disadvantages. Integrated photonic chips possess high attenuation coefficients (depending on the material in the range of 0.3-3 dB/cm), and are not polarization-insensitive. On the other hand, automated mass production of such chips in photonic foundries will reduce the costs and size while providing high speed, high quality and reproducibility of the fabricated devices.

Fiber based interferometers are polarization insensitive and might be produced by using off-the-shelf components. With unknown inaccuracies of those components and taking into account the strict precision demands on the interferometer arm-length differences, a solution for the interferometer assembly must be found. As one of the assembly preparation steps, the precise cutting of the fiber components is a major challenge here. Furthermore, for the stable two-photon interference signal with a fixed interferometer (IF) phase, the environmental influences, such as the noise and temperature fluctuations should be

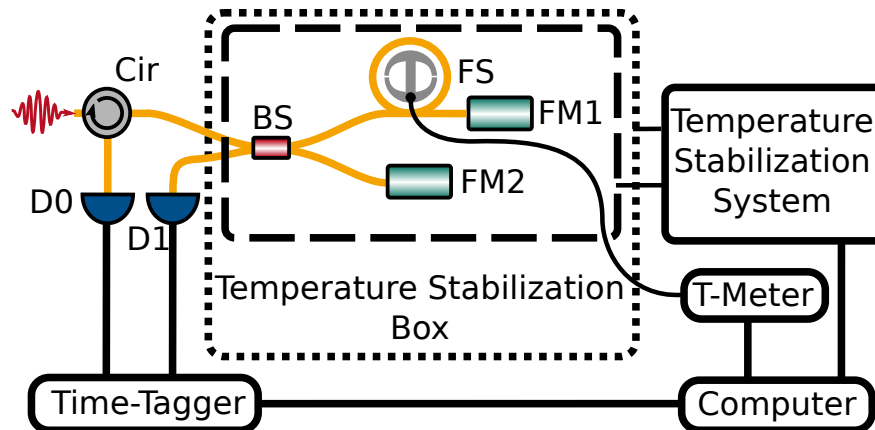


Figure 4.1.: Scheme of the implemented receiver module. Yellow lines denote standard single mode fibers SMF-28, black lines denote electrical connections. Photons enter the circulator (CIR) at the input of the receiver, located before the Michelson interferometer, consisting of a 50:50 beam splitter (BS). The long arm of the interferometer is mounted around the fiber stretcher (FS) and the Faraday rotator mirrors (FM1 and FM2) reflect the incident photons that are then detected by the single photon avalanche detectors (SPADs) D0 and D1. The arrival times of the photons are measured by a time-tagger and evaluated by the computer. T-meter is a multimeter for reference temperature measurements at the fiber stretcher. Clock synchronization for the time tagger is not shown in the picture. Long term stability and phase adjustment is performed by the remotely controlled two-stage temperature stabilization system.

minimized or canceled out. However, all these difficulties can be overcome with relatively simple means so that an implementation with optical fibers was chosen to realize the interferometers

In most reported experiments up to now, the receivers implement two stabilization systems: temperature stabilization for the long-term stability of the interferometers and an active phase control system for fast phase adjustment.

The first stabilization system cancels the slow temperature drift in the laboratory on the scale of minutes and hours in order to keep the the difference of the IF delay constant and hence the interference contrast maximal. It is usually implemented as a control loop with a PID controller adjusting the current through thermoelectric coolers (TECs) which are heating or cooling a sink with the mounted IF components [56].

The second, fast phase adjustment system must hold the desired phase at a given value on the time scale from milliseconds to minutes and compensate eventual fast phase distortions. This can be achieved by adding an electro-optic modulator [143], an adjustable delay line [144] or a fine temperature tuning [20].

For the present quantum key distribution (QKD) experiment the latter method was chosen combining the long- and the short-term stabilization systems, which led to a simplified overall setup. Furthermore, a method for a reproducible and precise construction of an all-fiber interferometer was developed and tested. Its main principle is to cut the interferometer parts as precisely as possible and subsequently to adjust the residual inaccuracies by the combination of a mechanical and a thermal fiber stretching. Simultaneously, the phase of the interferometers is also being set by small temperature adjustments.

The chosen solutions for IFs setup components, as well as for temperature and phase control lead to a significant simplification of the overall setup, enabling for a fast and cost-efficient assembly of arbitrarily many IFs. In the following sections, parts of this setup are described. First, an overview of the entire receiver is given in section 4.1. Then, the temperature stabilization system is described in section 4.2 and the interferometer assembly, including the developed method for precise fiber cutting in section 4.3. Finally, the description of the system for the measurement and evaluation of detected photons is given in section 4.4.

4.1. Receiver setup overview

In fig. 4.1 the implemented receiver setup is depicted. It consists of a Michelson interferometer (circulator, 50:50 beam splitter, two Faraday rotator mirrors (FMs) and a static fiber stretcher (see section 4.2.2) for inaccuracy correction), a two-stage temperature adjustment system for long-term stabilization and phase adjustment (tailored container boxes (dotted and dashed) and electronic stabilization system), a photon detection unit (SPADs and the time-tagging module) and a control unit (computer).

During the presented work several rounds for building interferometers and stabilization systems were done. Here, only the last iteration is shown that achieved the best performance. In the following, in some figures, old interferometers or other devices may appear. They are properly indicated.

All implemented receivers consist of identical components and are built in an identical way. The only differences arise from inaccuracies within the used components and slight errors introduced during their assembly into the entire interferometer. The interferometers

consist of a circulator *FCIR-55-1-NNN-BBB-1*¹, a 50:50 beam-splitter *10202A-50*², and two FMs *FRM-15-25-NC*³. All components are polarization insensitive and the fiber (SMF-28) is used without the fiber buffer for better contact to the thermal bath (cf. section 4.2.3).

The fibers of the pigtailed components are joined by fiber fusion splicing with each other in order to reduce the losses within the interferometers. During the assembly, the maximal error estimated by the automated evaluation program of the splicer was only 0.02 dB, which is much smaller than the typical loss of an FC connector (0.25 dB [145]). The joints are then recoated with a high index material in order to restore the mechanical properties of the fibers, especially reducing its fragility during bending. At the input of the receiver FC/APC ferrules and at the detector outputs FC/PC ferrules are attached.

The source interferometer is distinct from the receiver interferometers only by use of the polarization sensitive high power circulator *PM CIR-55-C-1-02-NNN-BBB-1*⁴ with both axes working and a polarization-maintaining fiber (PM fiber), since the in- and outgoing light has to be linearly polarized for the subsequent second harmonic generation (SHG) (cf. section 3.1.4). Due to the properties of the Michelson interferometers discussed in section 2.2.2, the output light's polarization is orthogonal to the incoming light and must be aligned back along the slow axis of the PM fiber in order to meet the correct polarization for pumping of the SHG stage. This is achieved by splicing the output FC/APC pigtailed connector with an angle offset of 90° to the third port of the fiber circulator.

For the experiment the SPADs *ID220*⁵ for photon detection are used. The arrival times of the photons are subsequently evaluated by the *ID900*⁶ and the measured time stamps are transferred for evaluation to a personal computer via an ethernet connection. There, the sifted key is evaluated and, in particular, the quantum bit error rate (QBER) calculated, which is later used for the phase adjustment of the IFs by changing the set temperature of the internal stabilization loop of the self-made stabilization system presented in section 4.2.

4.2. Temperature stabilization and phase control for interferometers

The temperature and phase stabilization system consists of several parts. The passively and actively stabilized interferometer containers are described in section 4.2.1, the fiber

¹Manufactured by dpmPhotonics, Inc.

²From Thorlabs. Inc.

³Provided by Laser2000 GmbH.

⁴Provided by dpmPhotonics, Inc.

⁵Provided by ID Quantique, Switzerland.

⁶Provided by ID Quantique, Switzerland.

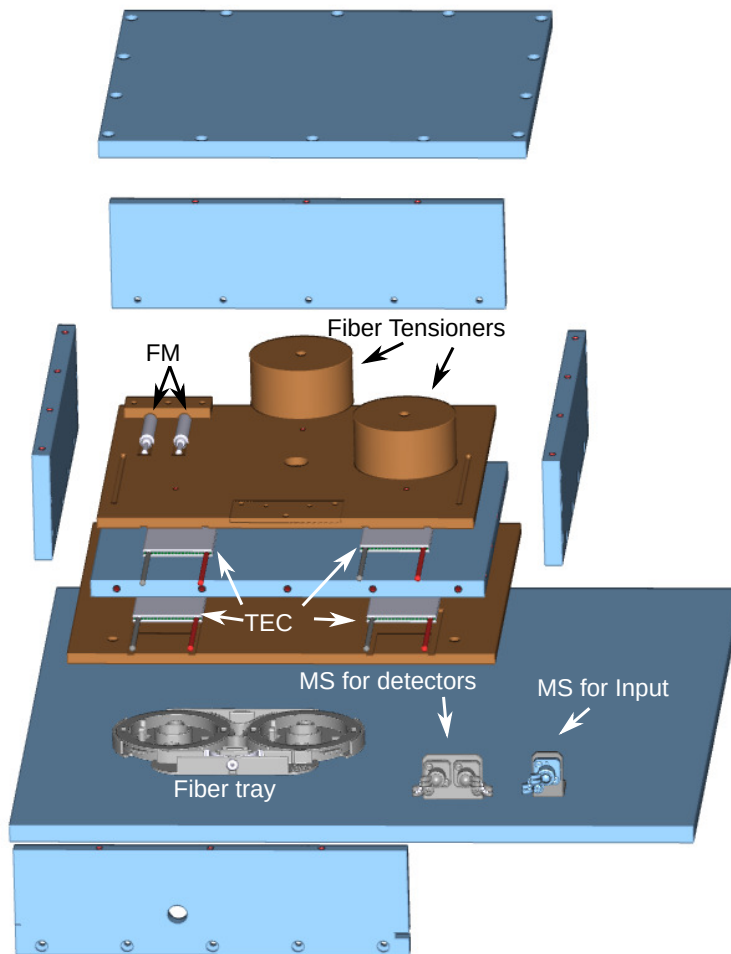


Figure 4.2.: Exploded-view CAD drawing of the temperature stabilized box with internal devices. Glass fiber and electrical cables are not shown. FM - Faraday mirror, TEC - thermoelectric cooler, MS - mating sleeve for optical fiber connectors.

stretching device in section 4.2.2 and a two-channel electronic system for a two-stage stabilization of it is explained in section 4.2.3.

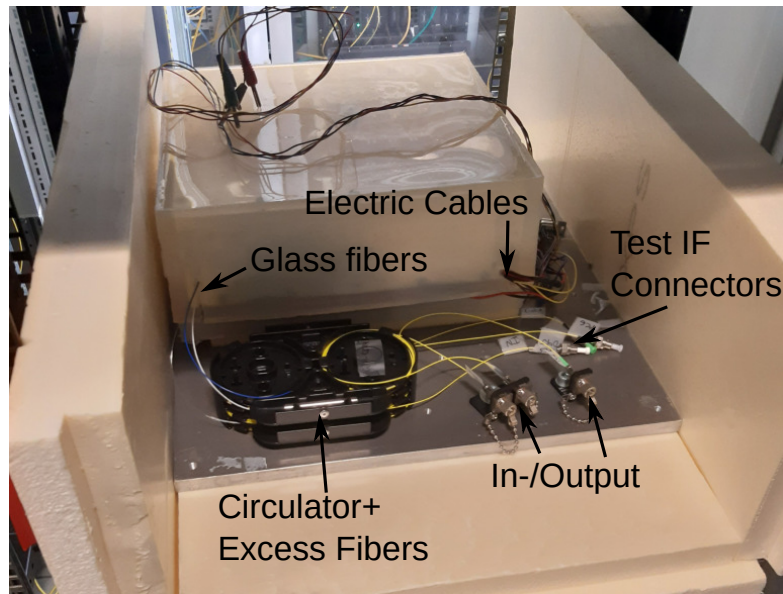


Figure 4.3.: External view of the stabilized box with a silicon isolation layer, inside a polystyrene box. Here only bottom and side walls are shown. Test IF connectors - connectors of a second interferometer built inside the box.

4.2.1. Temperature stabilized container for interferometer

The stabilization container consists of several layers, which are either actively or passively stabilized. In the following, the layers are described from the inside to the outside.

The two inside layers are a metal box and a box inlay - a plate with tailored mounts for the fiber interferometer shown in fig. 4.2, which are actively stabilized with a two channel electronic system described in section 4.2.3. Those components are made of metal plates of 1 cm thickness with a considerable heat capacitance, much larger as that of the glass fiber. Green plates in the figure are made of copper and blue plates of aluminum. Fiber tensioners are made of copper, but brass is also possible. More about them and their use can be found in section 4.2.2. The exploded-view drawing in fig. 4.2 shows also most components of the interferometers with their mountings, except for the fibers, electric cables and six thermistors that were built in at different positions. The interferometer components are mounted on the top copper plate and a part of fiber is wound around the fiber tensioner or a simple copper cylinder with the same diameter, if no length correction is required. This plate is mounted on four TECs, controlled by the first stabilization loop.

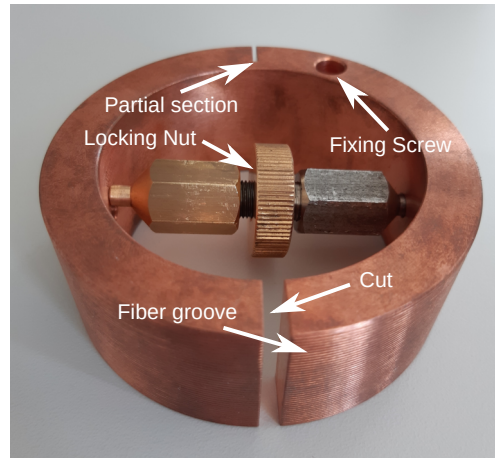


Figure 4.4.: Static tensioner for the optical glass fiber. The glass fiber is wound around the cylinder in the thread-shaped milling. The tension is achieved by moving the nuts on the bolt inside the cylinder, the nut in the middle locks the tensioner.

The surrounding aluminum box is controlled by the second loop, using another four TECs. Cables and optical glass fibers are fed through holes in the aluminum box at different spots to prevent fiber breakage during handling. After installing the interferometer inside the box, the empty space inside is filled with polystyrene flakes to minimize temperature instabilities caused by air convection inside the box.

The six thermistors are distributed at different positions in the system. Two of them that are part of the stabilization loops are located directly on one of the TECs of those loops. Three other thermistors for temperature observation are located correspondingly outside the box, in the wall of the aluminum box and on the top of one of the fiber tensioners. Close to the latter one, the sixth thermistor is located for verification of the measured temperature by an external multimeter *Keithley 2010*.

In addition to the actively stabilized layers, two passive layers have been added. For minimization of the heat exchange at the surface of the aluminum boxes, a silicon layer was added, completely covering the box from all sides. And, finally, a polystyrene box was added as shown in fig. 4.3. Those two layers are expected to also suppress the acoustic noise in the lab, but no significant effect on the key distribution was observed.

4.2.2. Setup for mechanical fiber length correction

The fiber tensioner for the thermo-mechanical inaccuracy correction method described above must fulfill several requirements. It must apply static tension for long periods of time without reduction of the applied pulling force. Simultaneously, the device must not cause any fiber cracks and allow to distribute the tension uniformly on the entire fiber length. Finally, the device must possess a sufficiently high heat capacity to keep the fiber temperature stable and to provide successful phase adjustments.

In fig. 4.4 such a device is shown. It consists of a copper cylinder with a diameter of 8 cm with a cut on the front side and a partial section in the back, enabling a slight spreading of it. The glass fiber is wound around the cylinder and put into the thread-shaped milled groove to prevent unwanted movement of the fiber across the surface and to maximize its contact surface for better thermal contact. The spreading of the cylinder and, thus, the stretching of fiber is done by moving a bolt against a nut inside the cylinder, pressing from the inside at its opposite sides and deforming it. The fiber tensioner is fastened on a copper plate by a single fixing screw.

The section of optical fiber to be stretched is glued to the cylinder surface with the heat resistant glue *WIKO SG140 20*⁷ at two positions, enabling an uniform distribution of the tension on the entire fiber between those sites. Here, only the fiber coating is glued to the copper, i.e. too high tension may lead to a detachment of the coating and the cladding of the fiber. However, this was never observed during the experiments. This glue can be dissolved by dichloromethane, which does not affect the polymer coating of the fibers, as was tested several times.

If for some interferometer no fiber length correction is necessary, a fiber stretcher may be replaced by a simple solid cylinder with similar spiral-shaped grooves on the surface.

4.2.3. Electronic system for temperature stabilization

In fig. 4.5 a simplified scheme for the developed two channel stabilization device is shown. There, a microcontroller manages two temperature regulation loops. The first loop (shown in red) controls the internal parts, where the interferometer is stretched. The second loop (shown in blue) stabilizes the surrounding box. Additionally, three thermistors are installed for temperature observation on the stretching spool, at the inside of the box and outside the box. The microcontroller can be controlled manually or digitally via the USB connection to a remote PC.

The designed temperature range was 23-70 °C with a resolution of 0.5-4 mK (depending on the temperature, see appendix B.3) and the designed long term temperature stability of

⁷Manufactured by WIKO Klebtechnik e.K.

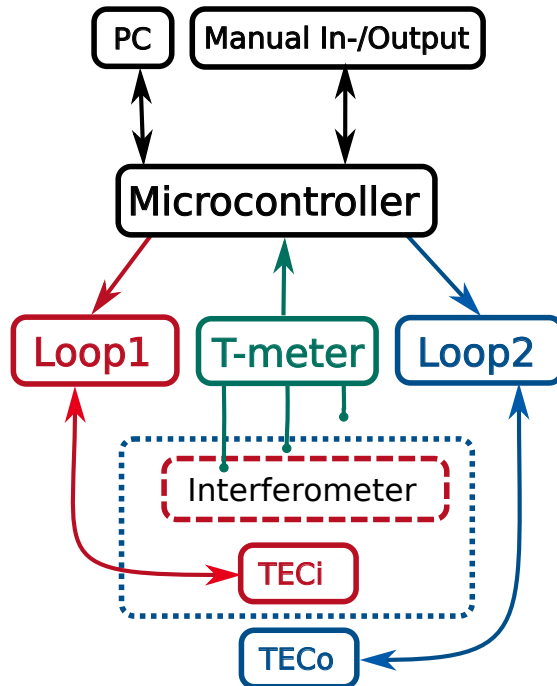


Figure 4.5.: Simplified scheme of the implemented electronic temperature controller for the interferometers. A microcontroller controls two stabilization loops: one loop stabilizes the interferometer and the inner components (shown in red), the second loop stabilizes the surrounding box (shown in blue). Additional thermometers (T-meter) monitor the temperature at the interferometer, in the box and outside.

the device is 2 mK per day for each channel. The overall electric power of both regulated loops amounts to approximately 480 W. With the chosen TECs *O6.0-51.4 (TEC1-12706)*⁸ the overall thermal power of at least $Q_c = 360$ W is achieved, where Q_c is the maximal thermal power, that can be transported from the TEC's cold to the warm side at a temperature difference of $\Delta T \approx 10$ °C, i.e. ten degrees above the room temperature [146].

The developed device can easily be adapted for use with only one channel, or with one temperature controller channel and a diode laser (DL) current source at the second channel. A detailed scheme, operation and assembly instructions, an electric scheme as well as a firmware description can be found in appendix B.

⁸Manufactured by Roßmann Electronic GmbH.

4.3. Interferometer construction

For building interferometers with arm-length inaccuracies of several micrometers, several steps are required.

One of the most important parts of the developed method for interferometer assembly and operation is the precise cutting of the fibers and fiber-pigtailed components. In the present section the developed and successfully tested method is presented.

In order to observe two-photon interference, the difference of Michelson interferometers in different receivers located at the communicating parties must be much lower than the coherence length of single photons acting as qubits. For our setup, this length corresponds to approx. 2 mm of glass fiber as discussed in section 2.3.

Thus, it is required to compensate for deviations of the fiber lengths introduced e.g. by manufacturing tolerances of the fibers inside of the metal ferrules of components such as beam splitters and Faraday rotator mirrors. For measuring the differences of the interferometers we used the white light interference method, suggested for this kind of measurement already by Tittel et al. [20]. It is described in detail in section 2.5.

In addition to the determination of the light propagation distances, a method for precise and reproducible cutting of the glass fiber and fiber pigtailed parts was required. Such a method was developed and improved throughout bachelor theses of Leon Baack [147] and Leonard Wegert [148] and the master thesis of Lucas Bialowons [149]. The general idea was to apply tension to the fiber and cut it at carefully selected positions. Achieved cutting precisions lie in the range of several 100 μm for a single part. Further improvement of the cutting method would lead to a dramatic increase of the complexity of the cutting setup. Instead, a way to correct the introduced errors by mechanical stretching of the fiber was developed. The mechanical properties of the glass fiber result in a possible mechanical stretching coefficient of at least $\Delta L/L = 2.0 \cdot 10^{-3}$ as described in section 2.4.6.

This means, that the maximal error that might be corrected is depending on the arm length difference of the Michelson interferometers (MIs). On the other hand, the maximal arm length difference of single interferometers is limited by the long term temperature stability of the interferometer. Increasing arm length difference leads to an increase of the thermally induced phase fluctuations and, thus, to an increased quantum bit error rate (QBER).

Furthermore, as explained in section 2.2 for the time-bin protocol, the arm length difference must be longer than the pump pulse duration, which limits the key rate. If the pulse duration is much shorter than the time-delay induced by the interferometer, time multiplexing for pulses can be applied in order to increase the key rate, as described in section 2.2.3.

Taking into account all of the above and evaluating one first attempt to build the interferometers with an arm delay of approx. 9 ns, an arm length difference of 63 cm corresponding to a time delay of approx. 6.1 ns and enabling a correction of errors up to 1.2 mm was chosen. This estimation neglected the opto-mechanical effect within the fibre, that would expectedly increase this value allowing for correction of even larger inaccuracies (section 2.4.6). This value was chosen such that the time bins are well separated for various scenarios, even when chromatic dispersion (CD) of the fiber or the timing jitter and minimal pulse lengths of the pulse generators would have a negative impact on the time bin width.

In the following section (4.3.1) the method for the precise fiber cutting and interferometer assembly are presented. Subsequently, the assembly process is described in section 4.3.2 and the characterization of individual built interferometers is presented in section 4.3.3. The overall performance of the entire quantum key distribution (QKD) system and the achieved key rate is evaluated in the next chapter (chapter 5).

4.3.1. Setup for precise fiber cutting

It is reasonable to expect systematic deviations in the length of the fiber put inside the component housings of the off-the-shelf fiber pigtailed components, required for this experiment. Later in this work they are called *intrinsic inaccuracies*. Quantitative estimations for these inaccuracies could not be gained from the manufacturers, however, from the geometric dimensions, they can be estimated to be up to millimeter range, which lies in the same magnitude as the coherence length of the used qubits (see section 3.2). Those relative errors might be measured by the white light interferometry method described in section 2.5 in combination with some reference part. Some experiments carried out by Lucas Bialowons showed intrinsic inaccuracies up to 3 mm [149], which could be successfully compensated by the presented method.

The procedure of the precise fiber cutting is depicted in fig. 4.6 and consists of the following steps:

1. Mounting of the fiber pigtailed device or one fiber end on a tailored mount, which depends on the type of the component. The mounting should enable putting of components in a reproducible way at the very same spot to minimize extrinsic errors. This holder must be fixed and the components to be cut, must be clamped or screwed tight by a metal plate with a rubber layer to prevent sliding. For bare glass fiber a fiber holder can be used for fixing the fiber end. Such fiber holders are typically used for fiber preparation and handling during the fiber cleaving and fiber fusion splicing.

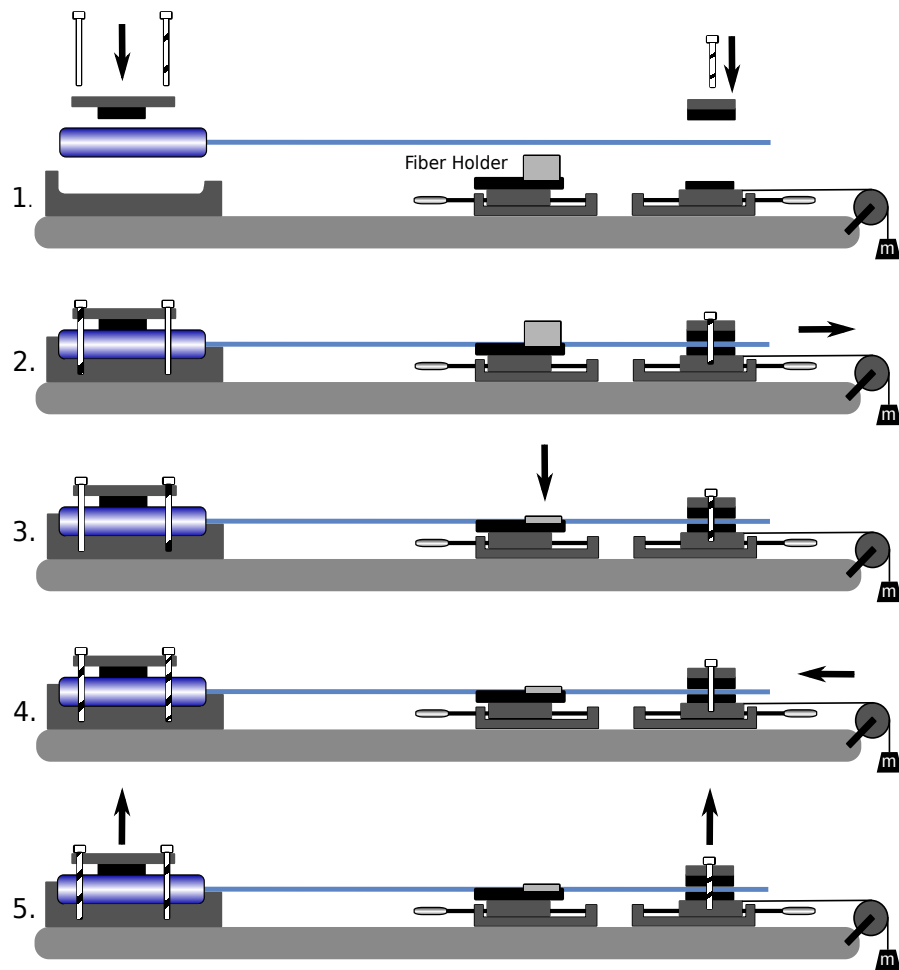


Figure 4.6.: Steps for precise cutting of fiber and fiber pigtailed components. The component to be cut (blue cylinder with the blue fiber pigtail) is mounted on a special cutting setup. 1: Mounting of the component on the setup. 2: Pulling on the fiber with a small force. 3: Closing the lid of the fiber holder. 4: Removing the mechanical tension. 5: Moving of the component with attached fiber holder to the fiber cleaver.

The other fiber end must be fixed on a linear translation stage, which is later used to apply tensile force to the fiber. The fiber holder is mounted on a different stage

and, thus, can be adjusted to compensate the intrinsic inaccuracies of the pigtailed components by moving its position along the fiber axis.

2. Stretching of the fiber by pulling at the loose end. The force, that can be used here, is limited by the mechanical properties of the fiber (see section 2.4.6) and the fiber pigtailed components, that are usually glued to the fiber. For our experiments we used a force of about 2 N. The force application is completed by hanging some weight on a strap and shifting the right translation stage until the entire force is applied to the fiber.
3. Mounting the fiber holder on the fiber. This is done by closing of the lid of the fiber holder that is later used for fiber fusion splicing. During the subsequent fiber cleaving process, the fiber will be cleaved at a well-defined distance from the holder. Then, the length from the left mount to the fiber holder is fixed and reproducible.
4. Releasing the fiber tension and removing the component from the setup. This is done by shifting the right stage back, taking the force from the fiber. The stage with the fiber holder must also be moved to the left subsequently, because of the remaining tension in the fiber.
5. Removing the component without opening of the fiber holder by opening the screwed mounts. Here, the fiber holder must not be opened. Otherwise, the precise position on the glass fiber is lost and the process must start from the beginning. After the moving, the fiber can be cleaved.

The presented method was evaluated by building two sets of interferometers: three at the first time and five at the second time [149]. The conclusion is, that this setup allows for reproducible cutting of components for arbitrary many interferometers with a precision of a few hundred micrometers.

4.3.2. Interferometer assembly

One straightforward approach for interferometer assembly is a direct splicing of single interferometer parts directly after cutting them. This approach was used for the successful showcase of the precise fiber cutting method shown in section 4.3.1 and the thermo-mechanical inaccuracies compensation as described in section 2.4.6, that was completed during the present work.

Since the original fiber pigtails of the Faraday rotator mirrors (FMs) were over one meter long, only two splices for each interferometer were required - one per interferometer (IF)

arm. Thus, only four components for each interferometer had to be cut: both FMs and two fibers of the beam splitter. The latter were chosen to be identical and the entire arm-length difference was implemented by cutting the Faraday rotator mirrors' pigtailed at different lengths.

For the optical fiber, the variations of the length and phase due to temperature fluctuations are proportional to the fiber length:

$$\frac{dL_{\text{opt}}}{dT} = \frac{\partial L}{\partial T}n + L \frac{\partial n}{\partial T} = L \left(\alpha n + \frac{\partial n}{\partial T} \right) \quad (4.1)$$

with the refractive index n and the linear expansion coefficient α of the glass fiber. Due to the high thermal conductivity of the inner copper plate, the long and short arm of the interferometer undergo almost identical temperature changes, compensating the thermal expansion of the fiber except for the arm-length difference. In other cases, when both arms are not stored closely, the high fiber length can lead to an increased thermal fiber length fluctuation and thus, to a worse phase stability of the interferometer. This means, it is advisable to minimize the length of all fibers in the interferometer, also to simplify the handling.

Thus, for the beam splitter pigtailed, a remaining fiber length was chosen to be 30 cm to be able to handle it during the splicing procedure. The remaining fiber length of one FM was set to 35 cm and of the second FM to 98 cm

After the length of individual components was chosen, the cutting method from section 4.3.1 was applied to prepare all fiber components for the interferometers. After adjusting the setup for a certain length, pieces for all interferometers were cut, before rearranging the setup for the next length.

After all components were prepared, the designated connections were spliced together and recoated (see section 2.4.5).

This method does not allow for compensating the intrinsic inaccuracies of the single IF parts and rely on their small size. During the master's thesis of Lucas Bialowons this component preparation method has been improved by application of the white light interferometry described in section 2.5. This enabled the measurement of the intrinsic fiber length differences inside of the FMs and beam splitter, which originated during their production and their systematic elimination. This allowed for easier assembly of a large number of interferometers for the many-party QKD system. For more details please refer to [149].

After the splice, the interferometers are mounted into the stabilization boxes and into the fiber tensioner for optical length correction as described in section 4.2.2.

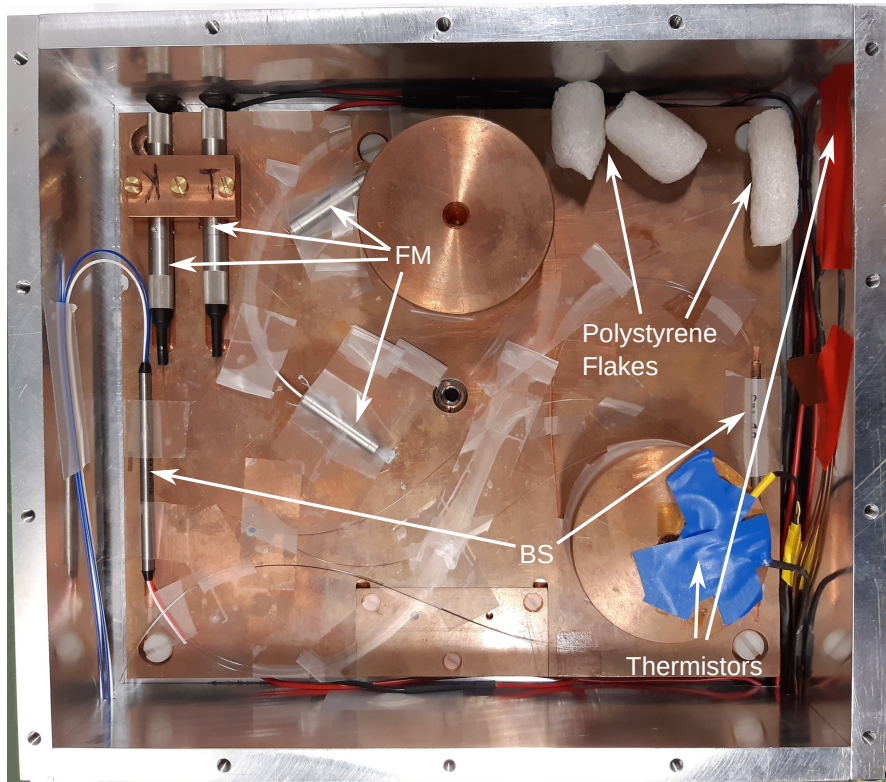


Figure 4.7.: Inside view of the stabilization box with two installed interferometers. FM - Faraday rotator mirror, BS - fiber beam splitter. Polystyrene flakes fill the entire free space after finished installation to prevent convection. Thermistors are for temperature observation inside the box. Adhesive film is used to keep fibers and cables in place.

During the installation of the fiber interferometers inside the stabilization containers it is advisable to apply the heat conducting paste for component housings and adhesive film for glass fixing at the copper plate and tensioner. One stabilized box can accommodate several interferometers, if correctly installed. In fig. 4.7 an open stabilization box with two built-in interferometers is shown. In the presented case, the fiber tensioner is replaced by a solid cylinder, since no fiber length correction on this interferometer must be performed.

Table 4.1.: IF losses and the relative loss ratios of short-to-long arms for each interferometer.

Name	Loss in dB	relative short-to-long arm loss ratio
Source	1.77 ± 0.02	0.98
Alice	0.94 ± 0.02	1.01
Bob	1.52 ± 0.01	0.91

4.3.3. Interferometer characterization

The values for arm-length difference mismatch between the interferometers ΔL were measured to $\Delta L_{\text{Alice,Source}} = (540 \pm 5) \mu\text{m}$, $\Delta L_{\text{Source,Bob}} = (242 \pm 5) \mu\text{m}$ and $\Delta L_{\text{Alice,Bob}} = (782 \pm 7) \mu\text{m}$, using the white-light interferometry method (see section 2.5). This is comparable to the coherence length of the used single photons, but still below the maximal inaccuracy value 1.2 mm that can be corrected by the thermo-mechanical stretching method.

As described in section 2.2 not only the arm-length difference deviations between two MIs but also the unequal loss values in different interferometer arms of all interferometers reduce the interference contrast. That means, that the interferometer components should be chosen, if possible, with matching insertion loss values, that are as low as possible.

For the used FMs the insertion loss according to the datasheets was in the range of 0.3-0.5 dB, for the fiber beam splitter in the range of 0.1-0.44 dB and the circulator losses are below 0.8 dB. During the splice process some small additional losses were introduced, as estimated by the automatic splicer's evaluation program up to 0.02 dB. All in one this led to the losses inside of the assembled interferometers as shown in table 4.1. The loss ratio measurement was done by inserting short pulses in the interferometer and comparing the areas of the two pulses coming out, that are reflections by the two IF arms.

In this table, some deviation of the insertions losses among all interferometers can be observed. Potential phase modulators, as used by other implementations [143], would increase them by at least a factor of two. Furthermore, the asymmetry of the interferometer arm losses acts detrimental for the minimal achievable QBER during the key exchange. Bob's interferometer asymmetry of 0.91 is significant and can be directly observed by time-bin histograms, however, the QKD results are still acceptable by means of the QBER.

The temperature stability and the phase sensitivity of the interferometer were found to be dependent on the fiber tension as already discussed in section 2.4.6. More detailed analysis of thermal and phase stability can be found in chapter 5.

4.4. Photon detection and evaluation

This section provides an overview of the processes and procedures, required to start the experiment, to conduct it and to complete it successfully, which includes also the quasi real-time evaluation of the exchanged key. Therefore, in section 4.4.1 the description of the applied time-tagging modules is given, which is used to synchronize the entire experiment (see section 4.4.2). Then, the implemented software for measurement and evaluation is described in section 4.4.3 and, finally, the measurement procedure is explained, required for a successful key distribution experiment.

4.4.1. Time tagging modules

Detecting the arriving qubits is one of the most important parts of the experiment. As already mentioned, single photon avalanche detectors (SPADs) *ID220* with maximal detection efficiency of up to 20 %, a dead time adjustable in the range of 1-25 μs and a timing resolution of 150 ps has been used [150].

Measurement of the arrival times of the received single photons detected by the SPADs requires a detection system with high resolution, low timing jitter and high repetition rates. The commercial *time-taggers*, sometimes called *time-to-digital converters* can now achieve resolutions down to one picosecond with a root-mean-square (rms) jitter of several tens of picoseconds with several tens of megahertz acquisition rate, however, there are many trade-offs between those values, depending on the solution and the used architecture.

For a chosen interferometer time-delay of 6.1 ns and with the detector dead times of one microsecond, the resolution in the range of below one nanosecond at the acquisition rate of one megahertz is required, which is much lower than the possible performance of commercial products. Thus, during the present work, several attempts for building a home-made time-tagger have been made.

The first attempt was implemented during the bachelor's thesis of Kai Roth [151]. Then, the open source system, developed by S. Polyakov from *NIST* [152], consisting of the *Altera Cyclone II* field-programmable gate array (FPGA) on an evaluation board *Xylo-EM*⁹, connected via USB-2.0 to a PC was used. As a result, a resolution below 0.5 ns was achieved, however, the reliability of the signal detection was low: some real signals were lost and some non-existent signals were detected. Thus, this solution could not be used for the QKD experiment.

Since no reason for the issue described above was found, a second attempt was done by Stefan Schürl and Kai Roth during their Master's theses with another FPGA (*Spartan*

⁹Manufactured by KNJN, USA.

6 LX9) and another evaluation board (*Logi-Pi*¹⁰), connected to the *Raspberry PI 4* [153, 154]. Here, a resolution below 0.1 ns was achieved, however only at a repetition rate of up to 1 kHz. Increasing the rate lead to a significant data loss, making the second solution not acceptable for the main experiment.

The solution that was used in the QKD experiment is the *ID900 Time Controller*¹¹, a combination of a four channel pattern generator and a four channel time-tagger, that can be optionally operated in two modes. The high speed mode with the resolution of 100 ps, a rms timing jitter of 28 ps and an acquisition rate of up to 100 MHz according to its datasheet is by far sufficient for the presented experiment [155].

Since the focus of the experiment was the proof-of-principle for the interferometer assembly method and its test as a part of a QKD system in the harsh environment of a real-world operation site of a optical communication provider, it was sufficient to use one device with its four input channels for the experiment and not provide physically distinct devices for both communicating parties.

4.4.2. Experiment control system

For successful detection of qubits corresponding to each other and precise measurement of their arrival times, synchronization of the qubit source and both receivers is essential. In other QKD implementations, for this purpose an additional laser pulse source is used, generating a clock signal, that is sent along the qubits either multiplexed over the quantum channel or over a dedicated service channel. Alternatively, a GPS clock based synchronization was performed.

For the present experiment the synchronization was performed with the *time controller ID900* from ID Quantique (see section 4.4.1). Since the device possesses four input channels, for the proof-of-principle experiment a single ID900 is sufficient. This means that the receiver modules are not independent and must be placed close to each other. Furthermore, synchronisation between the qubit source and the receivers could be also easily achieved by electric cables, since the source and the receivers were located in the same operation room.

The scheme for the dynamic processes during the QKD is shown in fig. 4.8. Here, for simplicity only the relevant parts are displayed. The time controller ID900 is the central part of the experiment, measuring electric signal arrival times from the four SPADs of Alice and Bob. For their correct measurement the qubit source pulses are synchronized with the clock signal of the time controller. Additionally, at the beginning, the time controller

¹⁰Manufactured by ValentF(x), USA.

¹¹Manufactured by ID Quantique SA, Switzerland.

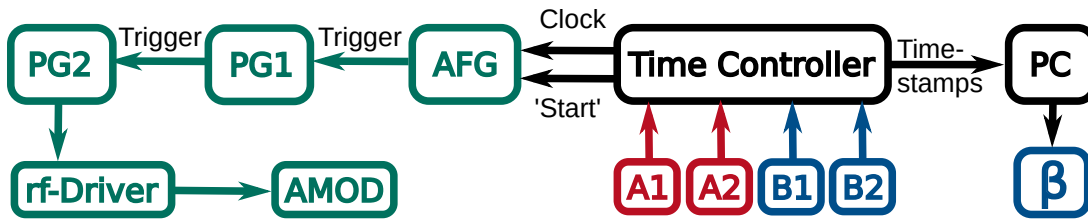


Figure 4.8.: Scheme of the processes for the QKD experiment: qubit generation (green), data acquisition from Alice (red) and Bob (blue) and evaluation and active phase adjustment (black). AFG: arbitrary function generator, PG1, PG2: pulse generators, rf-Driver: radio frequency amplifier, AMOD: amplitude modulator, A1,A2: Alice’s detectors, B1,B2: Bob’s detectors, PC: personal computer, β : phase of Bob’s interferometer.

generates an additional one-time pulse triggering the qubit generation and simultaneously resetting and starting the internal clock for measurement of the qubit arrival times.

The clock and the starting signal are consumed by the arbitrary function generator (AFG) *Tektronix AFG3052C*, generating a signal with up to 50 MHz output frequency. This triggers an optional chain of *HP 8131A High-Speed Pulse Generators*¹². Each of them can generate a burst of two successive square shaped pulses for each incoming trigger event, effectively doubling the frequency of the signal generated by the AFG. Then, the pulse train is amplified by the radio frequency driver of the electro-optic modulator, that cuts optical pulses used for qubit generation. The properties of such pulses are discussed in section 3.1.2. The generated qubits (not shown in the figure) are routed to the detectors of Alice and Bob. After being detected by the SPADs and ID900, the time stamps of the qubits are transferred to a computer, where the qubit statistics, particularly the QBER is evaluated and used for adjustment of the phase at Bob’s interferometer. As shown in section 2.2, adjusting the phase of one interferometer is sufficient for maintaining the key distribution process. The signal connections between the subsystems are implemented with coaxial cables.

Even though the relevant components are controlled by a computer, the operation of the entire system from start to finish requires manual intervention, since a lot of important subsystems were analog. For example, the erbium-doped fiber amplifier (EDFA) could not be controlled from the evaluation computer without a lot of additional work adapting the analog controlled current drivers of pump lasers. The operation schedule, including preparation, and the used software are described in the following sections.

¹²Manufactured by Keysight Technologies, Inc (former HP and Agilent).

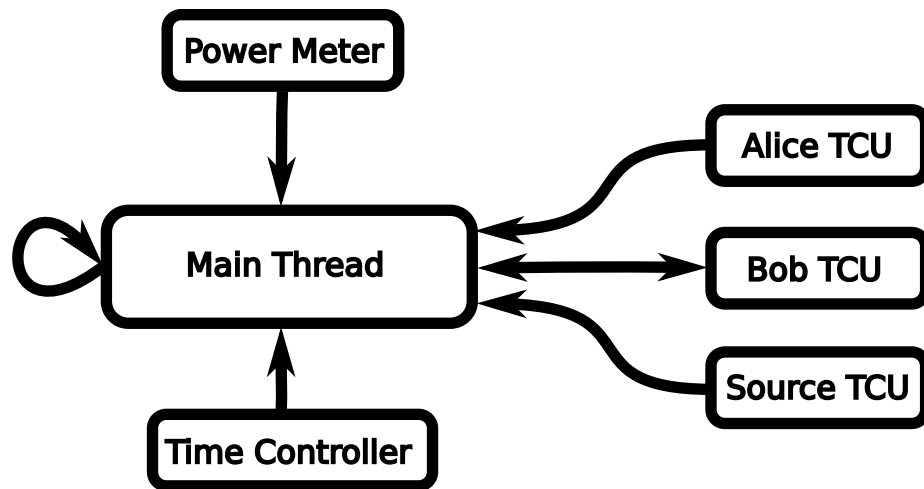


Figure 4.9.: Data flow diagram for the measurement and evaluation script of the experiment. The main thread manages the physical devices represented by depicted objects, running measurement iterations and storing the most relevant data. TCU: temperature controlling unit of the interferometer.

4.4.3. Control software for the quantum key distribution

The use of one single time controller, that is responsible for both, the clock signal and the detection time evaluation, simplifies the operating and evaluation software compared to the case of separated time-tagging devices¹³. Due to specifics of the data transfer from the time controller to the PC, no possibility for a quasi real time data evaluation was found. To circumvent this problem, the measurements were carried out iteratively: first, the measurement was performed during a certain time period (typically one minute), then the data was evaluated, and, depending on the results, the phase of Bob's IF was adjusted. Subsequently, the next iteration was started until the maximum number of iterations was reached or the program was stopped manually by input from keyboard.

This scheme was implemented in a *Python 3* script. The data flow between the logical elements of the script are shown in fig. 4.9. Those elements correspond to the threads and objects implemented in the script. The main thread manages the time controller, starting the measurements as well as receiving and evaluating the time-stamps. Simultaneously, in sub threads it monitors the peripheral devices: the status of participating temperature

¹³I would like to thank my colleague Erik Fitzke, for providing the major part of the python code for the control and data evaluation of the time controller ID900.

controllers and the pump power of the qubit generation stage, measured by the power meter. The use of parallel threads enables the simultaneous communication with the time controller and other devices, and prevents a measurement abortion in the case of any errors with the peripheral devices. After the measurement time, the data is evaluated. Based on these results, at the end of each iteration the script adjusts Bob's temperature, if required, then stores the evaluation results in memory besides logging it into a text file and several graphs of QBER and sifted key rate. If any errors occur during the measurement, they are either ignored (in case of sub threads), or the script aborts.

Data evaluation algorithm

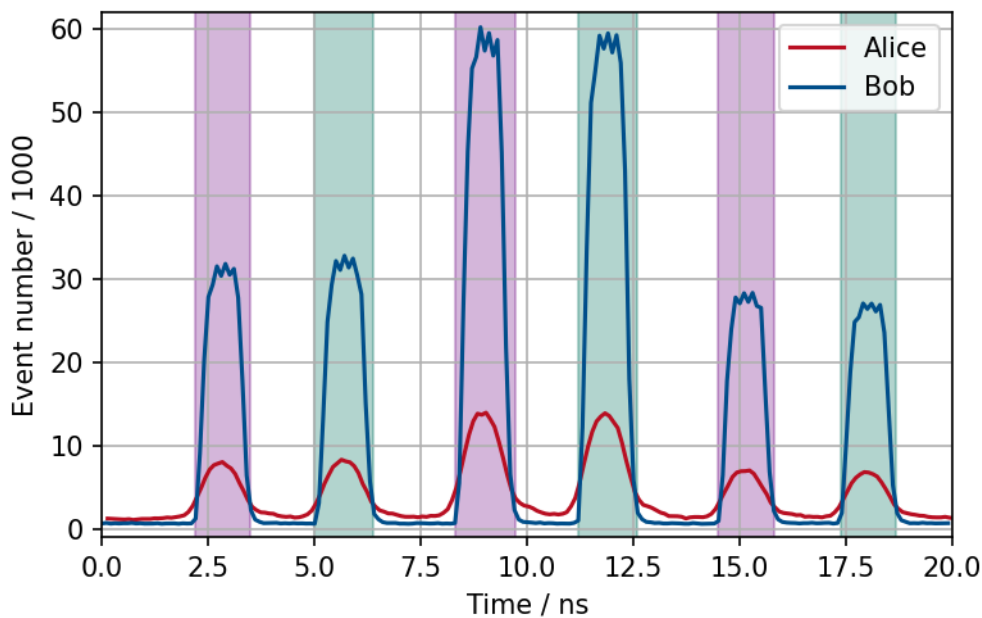


Figure 4.10.: Typical time-bin histogram for time-multiplexed pulses for a key exchange period of one minute. Purple and green highlighted areas denote corresponding time bins, from which the key is extracted. Alice's histogram has a smaller amplitude and a slightly higher width compared Bob's signal due to the 6.75 dB attenuation and the chromatic dispersion of the fiber link, while Bob is connected directly to the source.

One of the central parts of the script is the data evaluation. The time controller reports a list of time-stamps of events registered at its four digital inputs. In this unsorted list not just real photon detections but also dark events and afterpulsing events are included. As described in section 2.2 this list for each channel can be sorted into a histogram, like the one shown in fig. 4.10, by calculating the remainder of the time-stamp value divided by the qubit generation repetition rate. Here, the qubit time-of-flight offsets between the channels must be taken in account. This is necessary to identify time-stamps of correlated qubits. This requires a calibration measurement, where only one qubit at the time is travelling through the communicating link. This is the case at the maximum frequency of 2 kHz for the link of approximately 27 km length.

Once the histograms for each channel of both parties are created, the events are sorted into the time bins and the key sifting is performed. Afterwards, the QBER and the two-photon visibility V are determined and exported together with the sifted key. These values are later used to determine if a phase adjustment is required.

In fig. 4.10 an exemplary histogram for one measurement iteration is shown. Here, two multiplexed time-bin sets are highlighted by the purple and green colors. The amplitude on Alice's side is smaller suffers losses induced by the deployed fiber link. The amplitude of the corresponding side peaks differs slightly as well, due to the asymmetry of the losses inside the interferometers, as discussed in section 4.3.3. This leads to the minimum achievable QBER greater than zero. The minimum experimentally observed QBER was at 2%.

Phase adjustment algorithm

The phase adjustment algorithm within the script is responsible for setting the correct overall phase of the system. The QBER was taken as the measure, determining the necessity of temperature change, because this is the value, which all parties will share, when the devices are not in the same operation room, but distributed at distant operation sites. Therefore, the temperature of the interferometers is not suitable as a controlling function, since it is a local measure, that is in general not publicly announced. The implemented algorithm is a state machine, starting from the arbitrary system phase and utilizing the QBER for state transition:

1. At the very beginning, the system is in the state of initialization. Until the $\text{QBER} < 8\%$ for two consecutive iterations, the temperature is increased: $T_{\text{set,new}} = T_{\text{set,old}} + 5 \text{ mK}$. After the initialization, the QBER is checked again after each iteration. Then the following cases are distinguished:
2. If $\text{QBER} < 6\%$, the temperature remains unchanged, the device stays in this state.

-
3. If $6\% < \text{QBER} < 8\%$ for two consecutive iterations, the temperature is adjusted: $T_{\text{set,new}} = T_{\text{set,old}} + 2 \text{ mK}$. Here, the direction of the temperature adjustment is guessed.
 4. If $8\% < \text{QBER} < 11\%$, the temperature is adjusted: $T_{\text{set,new}} = T_{\text{set,old}} - 4 \text{ mK}$. If the system is in this state it is probable that the previous adjustment did not go well and the temperature must be lowered again.
 5. If $\text{QBER} > 11\%$, the temperature initialization must be performed again. Go to state 1.

This algorithm is able to keep the QBER low, but can still be improved. It has no resemblance to the typical control loops, since it is a challenge to construct from the QBER a typical error function, where the value of the error function directly determines the direction, in which the controlled parameter has to go.

4.4.4. Measurement procedure

Since the python script cannot control the entire experiment, a special sequence of operation steps must be executed. It consists of several steps, combining the preparation and readiness checks, running the python program and manual control of the EDFA. All steps are listed as follows:

1. Check on the temperatures stabilization of all IFs. It must be running for at least 30 min.
2. Check of the IFs lengths. They must be matching by white-light interferometry (see section 2.5). However, this step is optional, if the system was operated in the previous days and the stabilization was not turned off in-between.
3. Start of all electronic components of the source, the time tagger and the SPADs.
4. Perform the offset calibration by performing the steps 5 to 8 with the 2 kHz repetition rate and evaluating the results.
5. Start of the python script for the measurement with the desired parameters.
6. Turning on the EDFA manually. If it is turned on earlier, while the pulse generation is turned off, there is a chance of a spontaneous lasing pulse of high peak intensity, that might destroy source components, e.g. non-linear crystals.

-
7. Observation of the measurement, until it stops.
 8. Turning off the EDFA
 9. Preparation for the next measurement or shutting down the system, except for the interferometer temperature controllers.

In the case of some critical error when the measurement is automatically aborted, the EDFA must be turned off first, before restarting the QKD session from step 5.

5. Operation and performance of the QKD system

The main goal of the present work is the implementation and the first test of a quantum key distribution (QKD) system exposed to a typical environment of telecommunication infrastructure: work in typical operation rooms using a real-world communication link of a metropolitan network as the quantum channel. This was performed together with our partner Deutsche Telekom Technik GmbH, in a testing laboratory of the Network Innovation Center (NIC) with a fiber link deployed between Darmstadt and Griesheim.

Until a successful result was achieved, several revisions of the system were performed, e.g., the free space qubit source was replaced with an all-fiber source to comply with the laser- and work-safety guidelines of Deutsche Telekom. Furthermore, two iterations of the stabilization system and two iterations for assembly of the interferometers were required. In the present work only the last iteration is described.

In the following sections, the operation room at NIC including the operating conditions there (see section 5.1) and the deployed fiber link (section 5.2) are described. Afterwards, the performance of the receiver, in particular, its long-term temperature stability is shown in section 5.3. Subsequently, the entire QKD experiment is described, including the overall scheme (section 4.4.2), its control and evaluation system (section 4.4.3) and its results that are compared to theory (section 5.4).

5.1. System in the laboratory environment

The experiments at the Deutsche Telekom facility were performed in some operating room of NIC of Deutsche Telekom Technik GmbH (DTT) at Heinrich Hertz Straße 3-7 in Darmstadt, Germany. The test site was a typical server room with more than 150 m² area, filled with several rows of integrated 19-inch rack cabinets, used for various equipment tests. The room was intensively used by several working groups in parallel, i.e. staff members were often there and only two integrated rack cabinets and a little space nearby for two further racks and a table could be used for the experiment.

The default climate conditions inside the operation rooms of DTT are defined by the *Class 3.1* model from standard *ETSI EN 300 019-1-3 V2.4.1* [156, 157]. This model specifies allowed temperature and humidity inside the server rooms to be in the range 10-35 °C and 10-80 % correspondingly for at least 90 % of the time. This is a huge parameter space that would become challenging for some of the components, i.e. the single photon avalanche detectors (SPADs) and the interferometer (IF) temperature stabilization system. Therefore, the climate environment was monitored before and during the field test.

The operating room was located on the sixth floor and had glass facades in eastern, southern and western direction. The direct sun radiation was mostly blocked by rolling shutters and blinds, yet added up considerably and heated up the room. Depending on the weather outside, the climate control managed to keep the room temperature approximately constant. Nevertheless, rapid temperature and air pressure fluctuations inside the room were sometimes observed. Typical day/night temperature fluctuations were measured with two *Datalogger RHT50*¹, up to 5 °C peak-to-peak, with a slope of up to 0.3 °C/h. In exceptional cases the temperature was measured to be as low as 13 °C and as high as 28 °C.

Humidity and air pressure were monitored as well. However, no clear evidence was found that they are affecting the QKD system as much as the unstable temperature. Also, their changes were always accompanied by temperature changes which made a clear distinction impossible.

Numerous devices inside the described server room, especially those requiring active cooling, generated a high level of acoustic noise. It was measured by the *Digital Sound Level Meter 5175*², resulting in values in the range 77 – 88 dB, depending on the position within the room and the presence of devices with fans nearby.

For operation inside this room the test devices must comply with the laser- and health safety regulations of Deutsche Telekom Technik. Several adaptations have been done on the qubit source for this, i.e. all free-space components were replaced by fiber-based ones. Furthermore, test operation was only allowed in the presence of a supervising person.

5.2. Deployed fiber

For the field test a deployed optical fiber link was used to investigate the impact of the weather and other environmental conditions on the quantum channel.

In fig. 5.1 an approximate route of the deployed quantum channel is shown. It consists of two parallel fibers, that are spliced together in Griesheim, forming a single loop. The

¹Manufactured by Extech Instruments, USA.

²Manufactured by PeakTech Prüf- und Messtechnik GmbH, Germany.



Figure 5.1.: Approximate route of the used optical communication fiber, deployed between Darmstadt and Griesheim. The qubits are generated in a lab at the Network Innovation Center (NIC) in Darmstadt, then sent to Griesheim, turned around there and detected again at NIC. Entangled qubits are detected directly at NIC, without leaving the lab. (Map source: Google Maps 2021 [158])

source and both receivers are close to each other in the operating room of NIC and the qubits for Alice travel through the deployed optical fiber link to Griesheim and back, to be detected by the Alice receiver, while Bob's qubits are routed directly from the source to Bob's receiver over a short fiber. The deployed link length was measured to be $L_{\text{link}} = 26.82 \text{ km}$ by the *optical time-domain reflectometry device*³.

The measurements of attenuation profile (AP), chromatic dispersion (CD) and polarization mode dispersion (PMD) were performed by the *Network test platform*⁴ and the following results were measured: the attenuation of the link $A = (6.75 \pm 0.01) \text{ dB}$,

³FTB-7400D-2347B-EA, manufactured by Exfo Inc., Canada.

⁴MTS-6000A V2, manufactured by Viavi Solutions Deutschland GmbH.

the CD coefficient measured over the OESCL bands (see section 2.4.2) $D_{CD} = (16.68 \pm 0.02) \text{ ps}/(\text{nm} \cdot \text{km})$ and the PMD coefficient D_{PMD} vary in the range $0.020\text{--}0.029 \text{ ps}/\sqrt{\text{km}}$. The value range for PMD was measured on different days and no verifiable reason for different values was found. It could be for example explained by different weather conditions on those days, influencing the thermal expansion of the deployed line. All of the measured values are in accordance with the values established by the international standard for single-mode fiber (SM fiber) for telecommunication [80], which comprises a maximal value for AP of $0.35 \text{ dB}/\text{km}$, a maximal PMD coefficient of $0.2 \text{ ps}/\sqrt{\text{km}}$ and a CD within the range $13.3\text{--}18.6 \text{ ps}/(\text{nm} \cdot \text{km})$.

5.3. Performance of the receiver

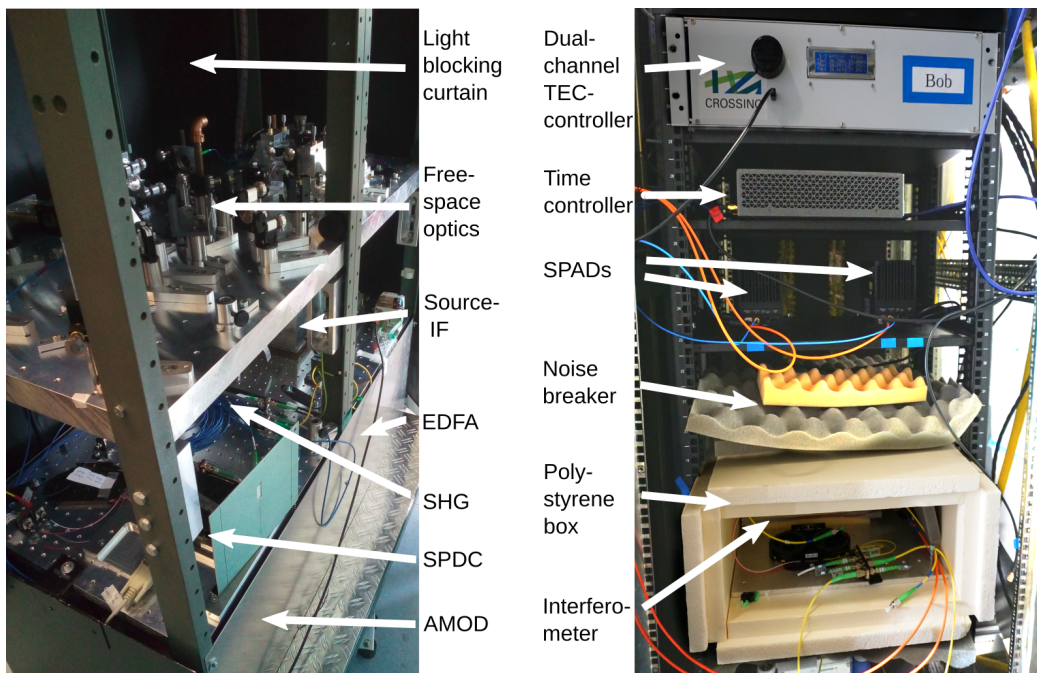
5.3.1. Environment of the operation site

For the experiment two integrated 19-inch rack cabinets were used as receiver containers (see fig. 5.2(b), cf. chapter 4). Nearby two movable cabinets and a table were placed. In the first cabinet the qubit source optics (cf. chapter 3) was placed as shown in fig. 5.2(a). And in the other cabinet various additional equipment, like optical spectrum analyzer (OSA), oscilloscopes, current sources, multimeters etc. were stored. The table was used for PC-controlled operation of the system.

The source cabinet and the stored source components are shown in fig. 5.2(a) (cf. source scheme in fig. 3.1). The cabinet is covered by a black laser light blocking curtain during operation (open in the picture). The free space optic components located on the top shelf belong to an earlier revision of the source and are not used for the actual experiment. The electro-optic modulator and erbium-doped fiber amplifier (EDFA) are located on the lowest shelf and are shielded by aluminum panels in addition to the curtain. Two crystals for frequency conversion via second harmonic generation (SHG) and spontaneous parametric down-conversion (SPDC), as well as the source's IF are placed on the middle shelf.

Inside the receiver cabinets (shown in fig. 5.2(b)) several adaptations were made before the installation. For example, the transparent cabinet doors were shaded with black anodized aluminum foil to isolate the system from ambient light. Furthermore, the active ventilation holes on the bottom of the cabinets were covered to prevent direct air stream of the laboratory ventilation system from unbalancing the stabilized system.

The components within the cabinet are located as follows. On the top, the self-made dual-channel thermoelectric cooler (TEC) controller (cf. section 4.2.3) is located. Just below, there is a time controller, evaluating the detection times of the incoming events.



(a) Source cabinet. IF: interferometer, EDFA: Erbium-doped fiber amplifier, SHG: second harmonics generation stage, SPDC: spontaneous parametric down-conversion stage, EOM: electro-optic modulator

(b) Bob's receiver cabinet. SPAD: single photon avalanche detector. Receiver cabinet of Alice is similarly arranged, except for the time-controller.

Figure 5.2.: Qubit source and Bob's receiver in the operation room during the field-test

Then, one shelf below, the SPADs are located. This arrangement prevents contact of the SPADs with warm air from the coolers of other devices rising up.

The interferometer and its stabilizing setup are located in the bottom of the cabinet. The interferometer is inside its actively stabilized metal box which is covered by a silicone insulation layer. The complete arrangement is placed inside a polystyrene box, which is placed at the bottom of the cabinet. Unlike shown in the picture, the polystyrene box is closed during the operation.

The acoustic noise inside the integrated racks, where Alice and Bob are placed, was measured to be in the range 76.5 – 79 dB and the silicone and polystyrene layers were measured to reduce the noise by approximately 9 dB and 10 dB, respectively. The noise breaker made of foam is applied to reduce the acoustic noise amplitude inside the box by

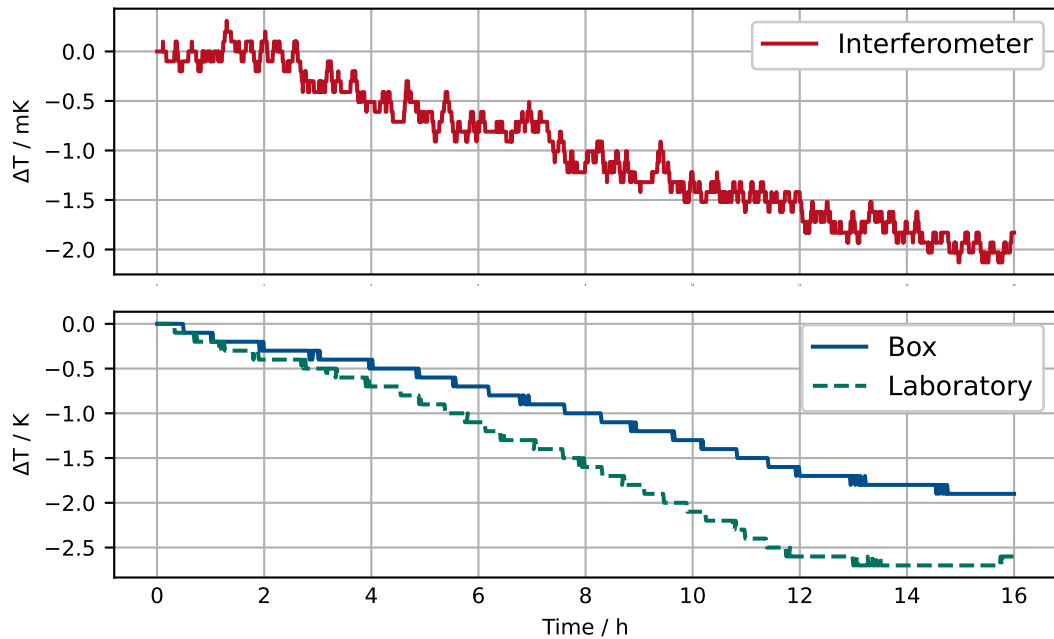


Figure 5.3.: Long-term temperature stability of the interferometer in the laboratory environment. Two data loggers are placed in the polystyrene box and outside the box. Measurement started after 24 h warm-up.

scattering the sound waves at their surface. However, no clear evidence for improvement of the QKD in terms of quantum bit error rate (QBER) due to the noise isolation was observed. Nevertheless, this does not falsify the hypothesis of the detrimental influence of acoustic noise on the Michelson interferometer performance (see section 2.2.2).

5.3.2. Long-term stability of the interferometers

Besides the acoustic noise isolation, the passive stabilization from the polystyrene box has a positive impact on the temperature stability of the entire system, as shown in fig. 5.3. The set temperatures of the interferometers and of the surrounding box are about 7°C and 5°C above the room temperature to create a heat current from the inside to the outside. Furthermore, the stabilization systems work best at 5°C above the room temperature [159]. In the upper panel the temperature change inside the aluminum box, at the fiber stretcher

close to the interferometer is shown, measured by the multimeter *Hewlett Packard 3478A*⁵ with a four-terminal sensing method [160]. In the lower panel the temperature changes measured by two data logger *RHT50* inside and outside the box are shown. The system was actively stabilized and the measurement was taken after a 24 h long warm-up. It is clearly visible, that the passive isolation by polystyrene does not prevent the temperature from dropping or rising, but slows down and delays these processes, acting as a low-pass filter for fast day/night temperature fluctuations. Furthermore, one can see the temperature drift of the interferometer following the overall trend of the room temperature, however with an amplitude that is smaller by a factor of 1000. This can also be observed in the overall phase of all interferometers during the QKD experiments. This instability of $\Delta T = 2 \text{ mK}$ in 16 h is close to the specified datasheet value of 2 mK/d of the used TECs (see section 4.2.3). This slow drift cannot be explained solely by the wire resistance fluctuation of the control loop, since the estimated resistance change due to the room temperature fluctuation amounts to approx. $\Delta R \lesssim 6 \text{ m}\Omega$. This changes the temperature measured by the controller by merely $\Delta T \approx 6 \text{ }\mu\text{K}$.

The easiest solution for this issue is the set point adjustment of the temperature stabilization system, based on some error function. For the QKD experiment, the QBER is exploited for this purpose, since it is evaluated anyway (see section 4.4.3).

Additionally to the long-term temperature stability, an important property of the stabilization device is the temperature adjustment time, i.e. time needed for the device to be stable enough to start the QKD after a significant set temperature change. In fig. 5.4 such a scenario is shown. The set point of the internal control loop was increased by 2 K and the temperature at different locations inside the stabilized box was measured by different thermometers. The thermometers were not calibrated to absolute values, so the relative temperatures are presented and the starting point of the three curves differ from each other. The time needed for the three sensors to report a stable temperature depends on their position within the box and the method that is used for measurement. The sensor used by the stabilization loop is located close to the TECs and reported the fastest adjustment. The multimeter *Keithley 2010*⁶ and the additional reference thermometer of the self-made stabilization system measure the temperature at exactly the same spot inside the fiber stretcher, maximally far located from all TECs. The signal difference

⁵HP 3478A achieves a resolution of 0.15 mK with an absolute accuracy below 3 mK in the relevant temperature range of 20-32 °C according to the data sheet. Similar to the multimeter Keithley 2010, low accuracy can be ignored, since the precision of the device is much more important.

⁶Keithley 2010 achieves according to the data sheet a resolution of $1.5 \times 10^{-5} \text{ K}$ with an absolute accuracy below 1.5 mK in the relevant temperature range of 20-32 °C. During all measurements the correct absolute temperature value is less important than the precision of the measurements, which is much higher than the accuracy, as can be seen later.

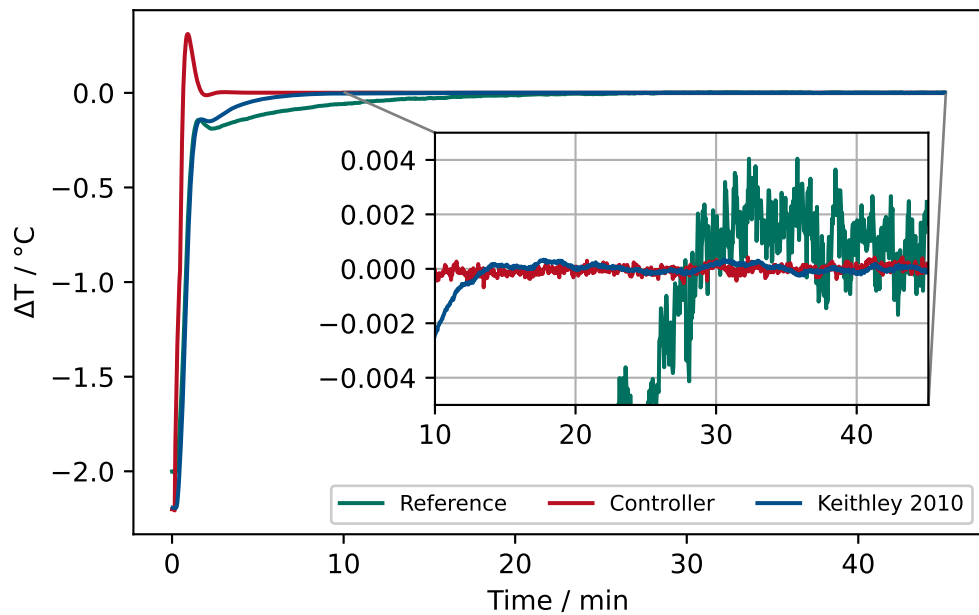


Figure 5.4.: Typical temperature curves during a temperature change of 2 K. The signal of the temperature controller used for stabilization, self-made reference thermometer of the temperature controller and the measurement by an external multimeter *Keithley 2010*.

between them is explained by the measurement method. While the high-end multimeter applies the four-terminal sensing method [160], the third sensor is self-made (see section 4.2.3 and appendix B) and lacks precision, as can be clearly seen in the figure and by evaluation of the standard deviation for the last fifteen minutes of the measurement: $\Delta T_{\text{MM}} = 1.3 \times 10^{-4} \text{ K}$, $\Delta T_{\text{Controller}} = 1.4 \times 10^{-4} \text{ K}$ and $\Delta T_{\text{self-made}} = 1.1 \times 10^{-3} \text{ K}$. In the following, the values of the self-made sensors are ignored. Possible improvements to increase this sensor's precision are described in appendix B.8.

From fig. 5.4 it can be concluded, that already after about 15 min the interferometer is stabilized at the new set temperature. For smaller temperature steps, this is achieved even faster.

The presented results are typical and were observed throughout the entire field test session. Assembled electronic devices proved their durability, being in operation around

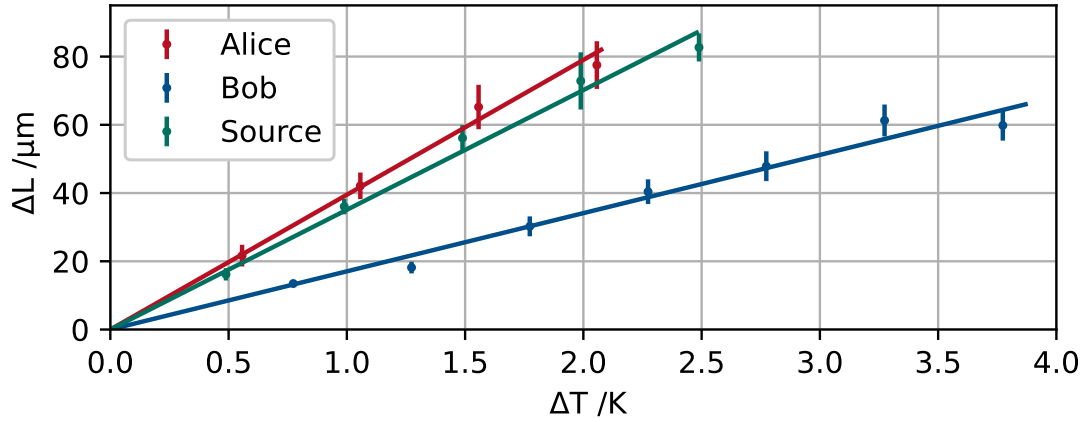


Figure 5.5.: Thermal elongation of the SMF-28 coiled fiber without strain (Bob) and with different strain forces (Alice and Source). The straight lines are fitted to corresponding data sets. Same figure as fig. 2.5.

the clock for nearly four years since the first experiments with only short pauses in between and without major problems.

5.3.3. Temperature dependence of interferometers phase

One of the most important properties of the implemented receiver system is the ability to adjust the overall phase by changing its temperature. From $\phi = 2\pi L/\lambda$ the phase sensitivity of the fiber S can be derived:

$$S = \frac{d\phi}{dT} = \frac{2\pi}{\lambda} \cdot \frac{dL_{\text{opt}}}{dT} = \frac{2\pi}{\lambda} \left(\frac{n}{L} \frac{dL}{dT} + \frac{dn}{dT} \right), \quad (5.1)$$

with the vacuum wavelength λ , the fiber length L and the refractive index n . The derivative of the optical path length dL_{opt}/dT , that is affected by the thermo-mechanic effect and also implicitly the strain-optic, can be measured directly for different fiber strain. The results are shown in fig. 5.5. There, the temperature and the corresponding optical length of the fiber was measured using the white-light interferometry method described in section 2.5, utilizing the interferometers of Alice, Bob and Source. A linear function is fitted to the experimental data, yielding the desired value of dL_{opt}/dT as their slopes. As described

in section 4.3.3 the fibers in the source’s and Alice’s IFs are stretched, which leads to the conclusion that dL_{opt}/dT is directly related to the applied strain.

The determined values for the phase sensitivities yield $S_{\text{Alice}} = (0.051 \pm 0.003) \pi/\text{mK}$, $S_{\text{Bob}} = (0.022 \pm 0.001) \pi/\text{mK}$ and $S_{\text{Source}} = (0.045 \pm 0.003) \pi/\text{mK}$. The minimum set temperature resolution is around 0.5 mK at room temperature (see fig. B.8).

Based on these results, Bob’s interferometer is used to adjust the overall phase during QKD due to its low phase sensitivity S_{Bob} , providing higher resolution of phase control than the other IFs. However, any of the three IFs is in principal suitable for this task. The values presented here are in good agreement with the values determined by Lucas Bialowons for the improved QKD system that was assembled later: $0.033 - 0.084 \pi/\text{mK}$ [149].

5.3.4. Interferometer length calibration

Before the start of the QKD session the length of all interferometers must be matched to each other. As described in chapter 4, first the fiber in Alice’s and the source’s interferometers is elongated by the mechanical stretcher and stabilized at a certain temperature. Then, the temperature working point for these is determined iteratively by measuring of the pairwise imbalance difference of all interferometers by white-light interferometry as described in section 2.5 and sweeping the temperature of one interferometer. Once enough data points are collected, the working point temperature can be determined by linear extrapolation. Such data sets and fitted lines are shown in fig. 5.5, however the data is shown relative to the working point.

Every day, before the QKD experiment is started, it must also be ensured, that the interferometers are still at their temperature working points corresponding to their vanishing imbalance differences. Again, the white light interferometry method is applied here. After experimenting with maximally stretched interferometers for several weeks the fiber durability under stress and the stress constancy has been observed. Once adjusted, the system stayed around these points even with changing temperature of the environment.

5.4. Quantum key distribution experiment

The very first successful QKD was achieved in the operating room of the NIC. Therefore no reference data for the performance of the setup inside a lab exists. Thus, only the field test results are described in the present section.

An exemplary result for the QKD measurement session is shown in fig. 5.6. Both the sifted key rate and the QBER for a five hour long key exchange are shown. The sifted key rate oscillates around the mean value of $R_{\text{sifted}} = (205 \pm 15) \text{ bit/s}$, while the

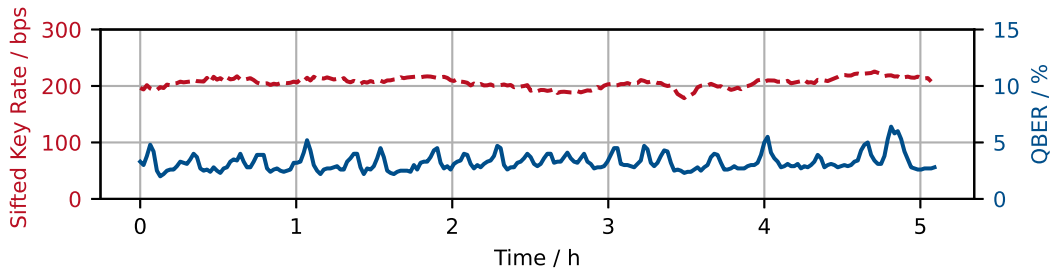


Figure 5.6.: Sifted key rate and QBER for a five hour long QKD experiment.

mean QBER amounts to $(3.2 \pm 0.7) \%$. This particular measurement was performed with the following parameters: the source generated double-pulse burst (DPB) at 50 MHz frequency, with the mean photon number per pulse $\mu \approx 0.057$. The detectors' efficiencies were set to $\eta_{\text{detection}} = 20 \%$ and $\tau_{\text{dead}} = 10 \mu\text{s}$. These settings were found to deliver the best performance in terms of rate, since shorter dead times lead to a higher afterpulsing probability, reducing the effective time, when the detector is ready for the photon detection.

This result can be compared to the theoretically expected result, derived from a model developed by Erik Fitzke [161], amounting to $R_{\text{sifted,theory}} \approx 193 \text{ bit/s}$ with a minimal $\text{QBER}_{\text{min,theory}} \approx 3.5 \%$.

In fig. 5.7 the evolution of the temperatures corresponding to the key exchange in fig. 5.6 is shown. The receiver temperatures there are measured by multimeters. Alice measured with *HP 3478A* and Bob was observed with *Keithley 2010*. While the lab temperature slowly increases by 0.7 K, and Alice's temperature remains constant within the range of 1 mK, Bob's temperature is reduced by 115 mK in order to keep the overall system phase constant. The phase in the beginning of the measurement already corresponded to a low QBER value, so that no big temperature hops were observed.

Unfortunately, until the end of the field test session, some systematic connection problems between the PC and the time controller were occurring and could not be solved. This issue appeared every couple of hours, quite irregularly, and limited the duration of the long-term measurements to several hours. Even a fast restart of the measurement often led to a loss of the correct system phase.

Several QKD experiments were carried out without the source IF, that was replaced by the pulse source option to generate DPBs and bursts with four pulses (FPBs) (see section 3.1.2). Then a secure key exchange was achieved, however with a minimum QBER of about 7%. Better values could not be achieved, due to two main reasons. The first reason is the timing jitter between the consecutive pulses, replacing the source interferometer

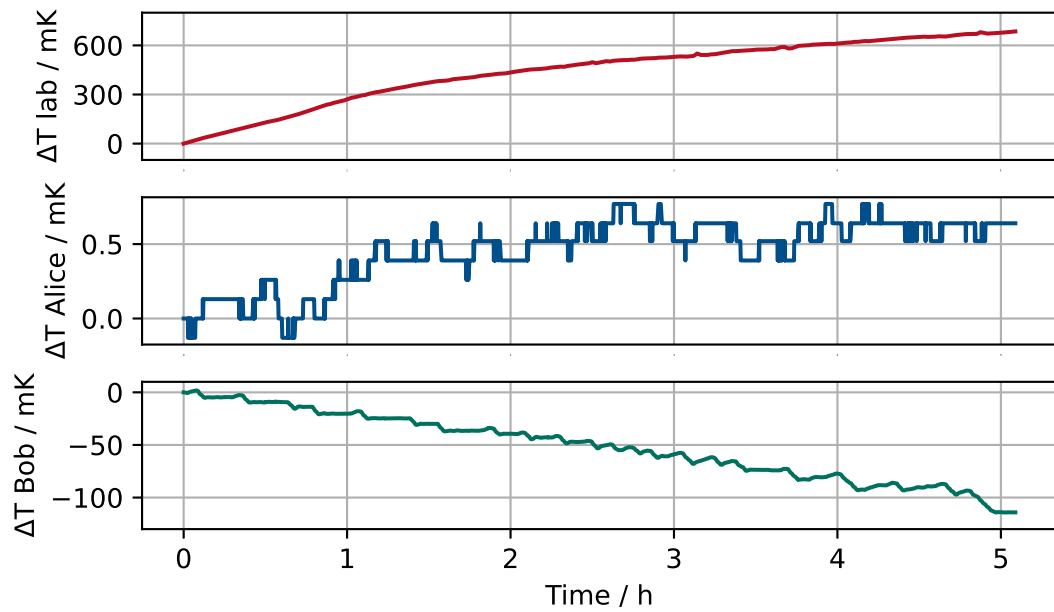


Figure 5.7.: Temperatures during the key exchange. Laboratory temperature falls, Alice's remains constant, Bob's must be corrected.

and the second reason is the impossibility to precisely adjust the time between the pulses to the interferometer imbalance. This made it impossible to fulfil the requirements on the matching length of the interferometers.

6. Conclusion and outlook

In this work, a two-party quantum key distribution (QKD) system and its test results in a real-world telecommunication environment are presented. The setup was developed in the framework of two collaborative projects. The first project was carried out within the scope of the collaborative research center CROSSING at the Technical University of Darmstadt. This project's goal was to build a Quantum Key Hub - a star-shaped QKD network with four communication parties, that are able to exchange keys pairwise and independently from each other. During the present work an important milestone of this project was achieved: a two-party proof-of-principle system was implemented and tested.

The other project is the innovation project "Quantensichere Netze" in collaboration with the Deutsche Telekom Technik GmbH. The main goal here was to test the implemented QKD system in a harsh real world operating room of Telekom, using a deployed fiber link. This field test was carried out between summer 2019 and spring 2020, making it one of the first successful field test of a QKD system in a telecommunication environment in Germany.

A time-bin encoded variant of the Bennet-Brassard-Mermin 92 (BBM92) protocol was implemented in the presented QKD system. The entire system, consisting of a qubit source and two receivers, is all-fiber based in order to comply with the safety regulations of Deutsche Telekom.

The implemented qubit source consists of a pump system, a Michelson interferometer, and a crystal for energy-time entangled pair generation via spontaneous parametric down-conversion (SPDC). According to the protocol, the interferometers possess a large imbalance - the arm length difference is larger than the pulse length $c_0\tau_{\text{pulse}}$, with c_0 speed of light in fiber. The pump source can be operated both in the continuous wave (cw) as well as in the pulsed regimes and achieves in the pulsed regime at 775.25 nm with 200 MHz and 1 ns average powers up to 31.51 mW. The corresponding mean photon number of photons per pump pulse is then $\mu = 0.318$.

Each receiver consist of a Michelson interferometer, identical to the source interferometer, two single photon avalanche detectors and a time-tagging module, which is shared by both receivers and is required for registering the qubit arrival times. One of the main challenges during the present work was to develop a method for a straightforward assembly

and operation of identical Michelson interferometers for the source and the receivers, as required by the chosen time-bin entanglement protocol: the pairwise differences of imbalance of the individual interferometers must be much lower than the coherence length of the single photons, i.e., $|\Delta L_{\text{Alice}} - \Delta L_{\text{Bob}}| \ll \Delta\omega_{\text{qubit}}/c_0$. It was solved by a two-step method: the interferometer components were pre-cut with a precision of approximately 100 μm . Subsequently, the residual inaccuracies were eliminated by the mechanical stretching of the fiber in the long arm of the interferometer. The length of fibers in those arms was chosen such that the stretching does not decrease the fiber's life expectancy. The corresponding strain was found to be at least $\varepsilon = 2 \cdot 10^{-3}$. The chosen assembly method is effective and simple. It makes building up of arbitrarily many nearly identical interferometers possible, which is a prerequisite for network operation.

Another challenge that had to be overcome during the interferometer implementation, is the development of a temperature stabilization system, required to stabilize the phase of the fiber based interferometers. The chosen solution led to a reduction of the setup complexity compared to previously implemented experiments: the same controller provided a long-term temperature stability of the interferometer container and allowed for fine-tuning of the interferometers' phase by slight adjustment of the temperature. The phase sensitivity due to temperature was found to be strain dependent. In the case without strain, the value $S_{\varepsilon=0} = 0.022 \pi/\text{mK}$ was measured, which is slightly higher than the value reported in literature. The long-term temperature stability showed a dependence on the day-night temperature cycle in the operating room, resulting in a drift of up to 3 mK/d and was easily compensated by the adjustment of the stabilization system's set point. A patent application for those interferometer building and operating methods has been initiated.

Due to the large imbalance of the interferometers, the protocol was adapted to use time multiplexing of the time bins for the key exchange. This allows for an increase of the nominal key rate by a factor of two during the experiment. While a bigger increase is theoretically possible, the hardware proved to be the limiting factor in this case.

During the present work a lot of effort was put into the development of home-made time tagging modules based on field-programmable gate arrays. Unfortunately no satisfactory results could be achieved. The devices either did not register all of the incoming events or did not achieve the desired data transmission rate, required for the experiment.

The entire system successfully exchanged quantum keys during the field test. The source and both receivers were located in an operator room of the Network Innovation Center (NIC) of Deutsche Telekom Technik. The key distribution between the qubit source and Alice's receiver was performed over a 27 km long deployed fiber link, while the qubits to Bob were routed directly to Bob's receiver. The quantum bit error rate (QBER) was used for the overall phase control of the system by adjusting the temperature of Bob's

interferometer. Typically, sifted key rates of approx. 200 bit/s and a QBER of approx. 3 % over five hours operation could be achieved.

As already described, the present work was a milestone towards the main goal of the CROSSING project – the Quantum Hub. After the completion of the laboratory work for this thesis, a star-shaped network comprised of four communication parties successfully demonstrated by the research group. For this experiment both the source and the receivers were slightly improved:

- The pump source was upgraded. From then on it was made digitally controllable to achieve a higher degree of automatization for the whole system.
- The qubit-generating crystal was replaced by another crystal generating broadband photon pairs, that were then distributed either by an arrayed waveguide grating module or by a wavelength selecting switch.
- The interferometer assembly method was improved by incorporating the white light interferometry (see section 2.5) method already during the interferometer assembly process. This allowed for further reduction of interferometer inaccuracies that had to be compensated in this work.

The still ongoing work pursues now a spatial separation of the communicating parties of the implemented Quantum Hub. To achieve this, the parties will be situated at various locations in Darmstadt, creating the first metropolitan QKD network without trusted nodes in Germany.

In parallel, an efficiency improvement of the source through the use of silicon nitride chips is being investigated. Such chip-based sources, exploiting four-wave mixing in integrated ring resonators, can be used to generate energy-time entangled photon pairs with tailored spectral properties. Ideally, they would match the 100 GHz wide C-band channel, both by bandwidth and the central frequency.

Further improvements of the electronic systems can be implemented, i.e. as suggested in appendix B.8 or an upgrade of the photon detectors and the pulse generators. However, while these adaptations increase the technical readiness level of the system, the number of communicating parties or the achievable key rate, they are more of an engineering nature than a scientific advance.

A. Power stabilization scheme for the erbium-doped fiber amplifier

Due to polarization instabilities, an active stabilization system for the implemented erbium-doped fiber amplifier (EDFA) has been developed. The working idea is very simple: the photo diode observes the intensity of the optical signal of EDFA and can translate with the transimpedance amplifier its output current into a voltage, that is then forwarded to the Expander Pi, on top of the Raspberry Pi. Z-diode prevents voltages exceeding the Expander Pi's analog-to-digital converter (ADC) input limit of 4.096 V to avoid its damage. In Raspberry Pi a python library for PID controllers implements a controller, which adjusts the digital-to-analog converter (DAC) output voltage of Expander Pi¹ and thus, the EDFA's pump laser. The electrical scheme of the system part, that is attached to the Expander Pi, is shown in fig. A.1 and the bill of material is given in table A.1.

For this system two optional photo diodes can be used. The *FDS02*² is a silicon diode, suitable for visible light and the light at 775 nm and *FGA01FC*³ is an InGaAs diode, that is used for 1550 nm and other near-infrared light. For pulsed operation with higher frequency, as used in the presented experiment, an operation amplifier with a higher bandwidth as *AD822* should be used.

¹Manufactured by AB Electronics UK.

²Manufactured by Thorlabs GmbH.

³Manufactured by Thorlabs GmbH.

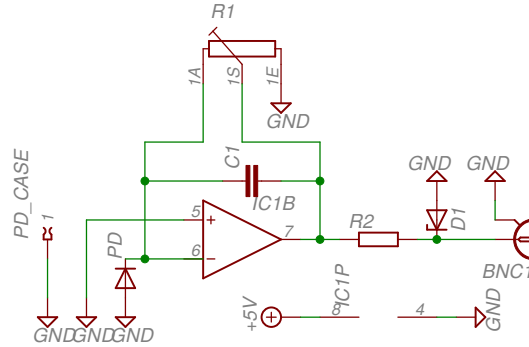


Figure A.1.: Scheme for the stabilization system for the EDFA. The source for 5 V may act as a typical USB power supply. the BNC is connected to the ADC hat of the Raspberry Pi.

Table A.1.: Bill of materials for stabilization system

Label	Device	Description
PD	FDS02 or FGA01FC	Photodiode, two options
IC1	AD822	Operation Amplifier
C1	Ceramic capacitor	1 nF
R1	Potentiometer	100 k Ω
R2	Resistor	50 Ω
D1	Z-Diode	A z-diode for 3.9 V
BNC1	Female BNC adapter	Bayonet Neill Concelman adapter for coaxial cables
-	Micro-USB plug	Plug for current source
-	Raspberry Pi 3b	Mini-Computer
-	Expander-Pi	analog I/O hat for Raspberry Pi

B. Dual channel TEC and LD current controller

B.1. Introduction

In this section the assembly and operations instructions for a temperature controller is given. The device can be optionally used as a single or a double channel thermoelectric cooler (TEC) controller (TECC) or as a TEC controller and a laser diode current source. It can either be managed by a rotary encoder as stand-alone device or it can be digitally controlled via USB using a self-developed protocol, enabling almost real-time adjustment of temperature set points with a high resolution ($< 1 \times 10^{-3} \text{ }^\circ\text{C}$) and a high repeatability ($\approx 1 \times 10^{-3} \text{ }^\circ\text{C}$). However, the long- and short-term performance of the temperature control is strongly dependent on the TEC controller, that was integrated into the device. For the present experiment, the *PTC10000* from *Wavelength Electronics, Inc.* [159] was used.

The section is organized as follows. First, the operation instructions for the device are given in appendix B.2. Then the designed performance (appendix B.3) and the overall scheme for a two channel TEC controller is described (appendix B.4). After the general description, the individual parts, the printed circuit board layouts and the assembly instructions are described in appendix B.5. Additionally, a comment on cables is given in appendix B.6 and a short description of the software, i.a. of the communication protocol for the remote control is given in appendix B.7. And, finally, a list with proposed improvements is presented (appendix B.8) and the description for use of the device as a combined laser current driver and TEC controller and other potential options are given in appendix B.9.

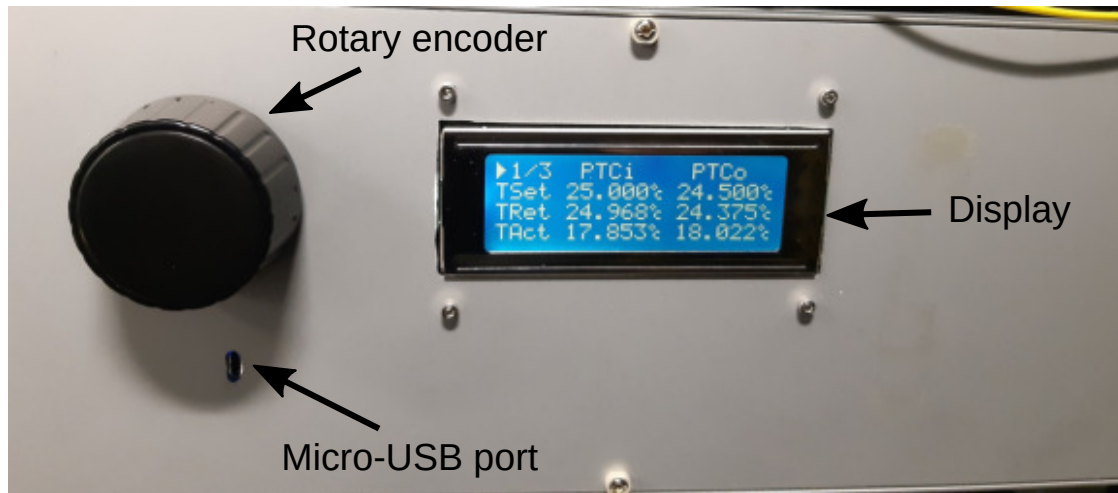


Figure B.1.: Front panel elements of the controller. The menu shown at display features three pages (see appendix B.2). For manual operation, the cursor position (here shown in the upper left corner) can be set by turning the rotary encoder knob. Settings are entered by pushing the button. The micro USB port enables software updates and access to the Arduino remote control of the device.

B.2. Operation instructions

B.2.1. Before launch

Before turning the device on, make sure it is properly connected. Furthermore, make sure that the device of which the temperature shall be stabilized is connected to the electrical ground (see appendix B.8) and the connection cables do not hang around unstrapped.

Take in account that a safety mechanism is implemented, preventing an excessive heating or cooling: if the set temperature is larger than the actual temperature by more than 2°C or smaller by 0.5°C at any channel, both channels are turned off automatically.

After a sudden shutdown, or after an Arduino restart, the device starts in an emergency recovery mode, if one of the channels was active before the shutdown. If the stabilized device is inside the safety margin described above, the device is directly turned on with the settings from before the shutdown. If the stabilized device is already outside the safety margin, the emergency mode is disabled and the operation must be started actively by a manual input or with a remote command (see appendix B.2 and appendix B.7).

```

1/3 ▶PTCi*  PTCo**
TSet 12.345% 12.345%
TRet 12.345% 12.345%
TAct 12.345% 12.345%

```

Figure B.2.: Main menu 1, showing the state of the TECCs and the relevant temperatures.

```

Set Temperature?
T=25.000% U=2.000V
YES          ▶NO

```

Figure B.3.: Confirmation question completing the temperature adjustment process.

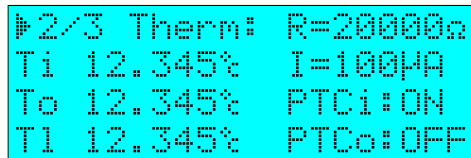
B.2.2. Operation

In the present section, the manual method for operation of the dual channel thermoelectric cooler controller (TECC) is described. For the remote operation over the USB refer to appendix B.7. Both methods provide access to all relevant functionalities of the device, but the manual method is much slower. The front panel with the operational elements is shown in fig. B.1.

For the manual operation, the display and the rotary encoder are sufficient. The three main and several secondary menus and error messages are shown at the display and the rotary encoder allows for the choosing of the correct settings in all menus. The menus are defined within the firmware of the Arduino (see appendix B.7). Throughout the entire firmware the channels are referred to as the inner (i) and the outer (o) channel, since they control the inner and the outer TEC control loops of the interferometer boxes. The PI-controllers of both channels are referred to as *PTC* due to the used model *PTC10000*. This device consumes a set temperature (*TSet*), delivers a monitor signal for this set temperature (*TRet*) and reports the actual temperature *TAct* of the stabilized device. The difference between *TSet* and *TRet* arises from missing temperature calibration, that is not necessary for device operation at the quantum key distribution (QKD) experiment (cf. appendix B.5.1).

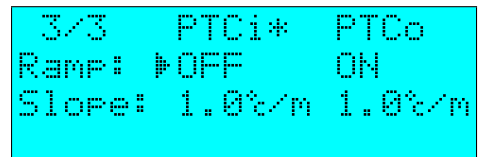
Immediately after the start, a boot message with the device name and the firmware version is shown as depicted in fig. B.6. The device name can be changed within the firmware. Please refer to appendix B.7.

In fig. B.2 the first main menu with an overview over the temperatures described above for both channels is shown. The temperatures appear in a table, column-wise corresponding to the different channels *PTCi* or *PTCo*. The first asterisk behind the channel name denotes the channel activity (both channels active in fig. B.2). The second asterisk denotes the enabled temperature ramp that is described later. The ramp at channel 2 active in fig. B.2.



```
2/3 Therm: R=200000Ω
Ti 12.345% I=100mA
To 12.345% PTCi:ON
Tl 12.345% PTCo:OFF
```

Figure B.4.: Main menu 2, showing the temperatures of the external thermistors. Also, here the state of the TECs can be changed.



```
3/3 PTCi* PTCo
Ramp: OFF ON
Slope: 1.0%/m 1.0%/m
```

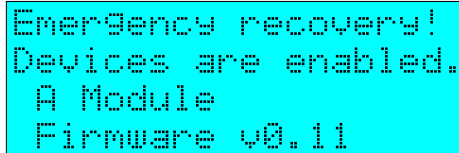
Figure B.5.: Main menu 3, enabling automatic temperature ramps.

For temperature adjustments, choose a channel by moving the triangle-shaped cursor with the rotary encoder. Then, press the encoder knob and choose the temperature digit by digit by rotating the rotary knob and confirming the choice by pressing it. After all five digits have been chosen, input confirmation is required, as shown in fig. B.3. After confirming the new temperature, the display returns to menu 1 and shows the updated temperatures.

The second main menu is shown in fig. B.4. Here, the individual channels can be turned on and off (in the bottom right corner) and the values of optional external thermistors are shown: the temperatures of inner box (T_i), outer box (T_o) and lab temperature (T_l). Furthermore, in the top right corner of the display, there are options for the resistance of the thermistors and the value for the current that is chosen at the option slider on the PI controllers *PTC10000* within the presented dual channel TECC. Those options are obsolete for the present experiment and can be removed in future firmware updates (cf. appendix B.8).

The third main menu only shows settings for potential temperature ramps. This functionality can be used to automatically ramp up the temperature with a defined maximum slope. This option is necessary e.g. when the device is used to control the temperature of optical crystal, which could be damaged by fast temperature variations. For the presented experiment this option is usually not applied. After several tests, the implemented firmware ramp was found to be unreliable as listed in appendix B.8. If required, use a remote script to adjust the temperature in small successive steps.

All operations changing the device status (channel activity, channel ramp and ramp slope setting) are followed by a confirmation request, analogous to the one presented in fig. B.3. While operating the device remotely, no security questions appear: neither on the display, nor over the remote communication protocol!



```
Emergency recovery!  
Devices are enabled.  
A Module  
Firmware v0.11
```

Figure B.6.: Boot message in case of the emergency boot. Otherwise only module name and the firmware version is shown. A is an example for name.



```
EEPROM wiped.  
  
▶OK
```

Figure B.7.: Memory clearing warning.

As already mentioned in appendix B.2.1, the device may start in an emergency mode, if one of the channels was active before Arduino shut down. Then, the boot message is extended with a warning about the active devices as shown in fig. B.6. Long pressing on the rotary encoder while in the main menu 1 (fig. B.2), wipes the settings that are stored in the long term storage: activity status of the channels, set temperature, thermistor resistance and its current. Afterwards, the message shown in fig. B.7 appears.

B.3. Performance

For the presented experiment, the relative temperature stability was important, so no calibration for absolute scale was carried out. The relative precision is provided by the PTC10000 controller, which has a long-term stability of 2 mK/d according to the datasheet [159]. During the experiment much better performance of the devices was observed. The accessible operation range is 23-70 °C and the resolution lies within the range 0.5-4 mK as shown in fig. B.8. However, operation at lower temperatures can be achieved by changing the setting within Arduino's firmware (see appendix B.7). The expected resolution T_{Res} is nonlinear, due to the nonlinear dependence of the set temperature from the set voltage. This resolution is calculated with the Steinhart-Hart equation for the used 20 k Ω thermistors TCS620 [162]:

$$T(U) = \frac{1}{A + B \cdot \log(U/I) + C \cdot \log^3(U/I)}, \quad (\text{B.1})$$

with coefficients $A = 9.6542E - 4$, $B = 2.3356E - 4$, $C = 7.7781E - 8$, $I = 100 \mu\text{A}$ and the 16-bit resolution of the used digital-to-analog converters (DACs):

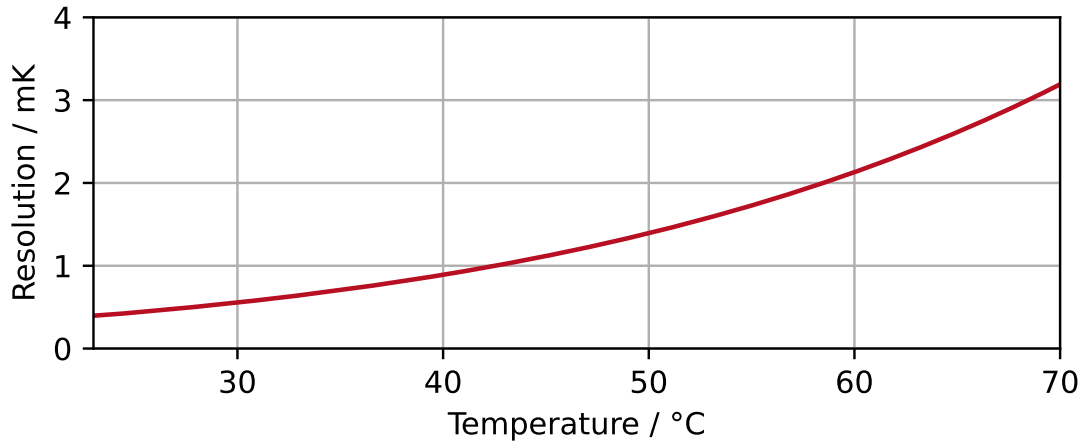


Figure B.8.: Setting resolution as function of the temperature. The resolution is not-linear, due to the temperature dependence of the thermistor resistance.

$$T_{\text{Res}}(U) \approx T(U + \frac{5V}{2^{16}}) - T(U). \quad (\text{B.2})$$

B.4. General functional scheme

In fig. B.9 the basic scheme of the two channel TEC controller stabilizing the interferometer is shown. The central part of the controller is the *Arduino Micro*¹. Its micro-controller chip *ATmega32u4* communicates via the USB port with an external client running on a PC, controls two TEC controllers (TECC1, TECC2) *PTC10000*² and additionally monitors the temperature over the external thermistors (T-meter). In order to enhance the resolution of the operation, external analog-to-digital converter (ADC)s (24 bits) and DACs (16 bits) are used, providing higher resolution than those of the Arduino. For the device, 20 kΩ thermistors *TCS620*³ [162] were used. Please note, that the option sliders on both *PTC10000* were put on enabled for the options *remote enable* and 100 μA. Two TECC channels and corresponding TECs are either denoted as channel 1 and 2 or as *internal* and

¹Manufactured by *Atmel*, a part of *Microchip Technology Inc.*

²Manufactured by *Wavelength Electronics, Inc.*

³Manufactured by *Wavelength Electronics, Inc.*

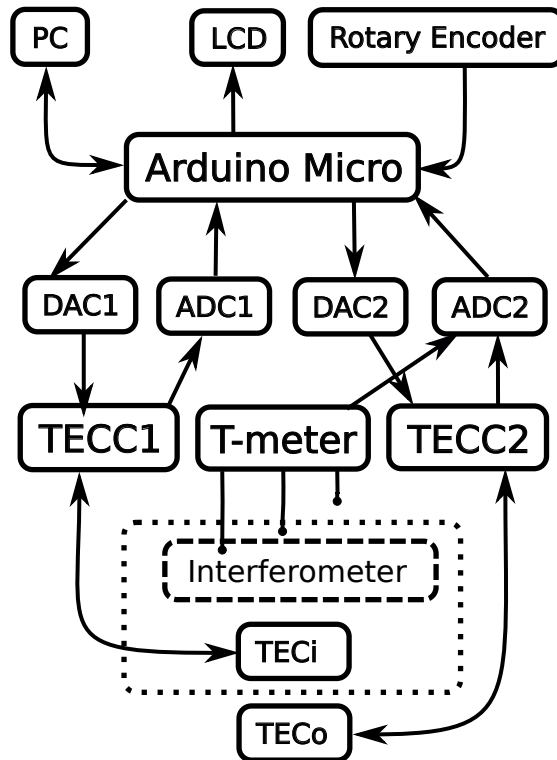


Figure B.9.: Functional diagram of the dual channel TEC- and LD-current controller. LCD - display, DAC - digital-to-analog converter, ADC - analog-to-digital converter, TEC - thermoelectric cooler, TECC - thermoelectric cooler controller, T-meter - thermometer, not used for regulation.

outside channel, referring to the stabilization of the internal or external box, described in section 4.2.1.

The microcontroller board and supporting circuits are placed on two circuit boards. The first one is a printed circuit board (PCB), see appendix B.5.1) contains all necessary devices including Arduino board and one TECC, and can perform as a single channel temperature control system. The second board (appendix B.5.2) contains either the second TECC (TECC2 with TECo) or the optional laser diode current driver. If neither is required, it is not necessary to install it. Circuits required for external thermistors are also placed on the second (additional) circuit board.

The assembled device can provide up to 10 A current at 30 V for each of the TEC controller channels. However, in the implemented version only 6.5 A at 24 V for each channel are available, due to the currently installed current sources.

The entire system, including the cooler and the current sources, is enclosed by a 19-inch rack with the height of three standard rack units (approx. 13.3 cm). Within the next sections, the whole system will be presented from the outside to the inside. First, the housing, voltage supply and external connectors are described. Then, the first circuit board with the micro-controller and the first channel PI regulator. Finally, the second circuit board with the second TECC and external thermistors are described.

B.5. Rack

In fig. B.10 an assembled device with opened front panel is shown. As a housing a 19-inch rack *BGT 384-240 IZ*⁴ was used. The IEC-60320 C14 type power-connector *FEH 2101* with an interference suppression filter is connected to the three independent voltage supplies. Two identical switching power supplies *LS150-24*⁵ deliver 6.5 A at 24 V and provide energy for the PI regulators, mounted on the PCBs. The third source - a gate-drive transformer *774-8213*⁶ provides 1 A at 12 V and supplies the PCBs and the cooling fans⁷ inside the rack. All power supplies as well as the power connector are located in the rear part of the rack, leaving space for the eurocard-sized PCBs and the fans in the middle, just behind the front plate. In fig. B.10 only one fan is shown, It is possible to put a second one on the bottom side of the rack between the PCBs or side-by-side with the first cooler. The fan is powered by the small power supply.

On the right side of the rack two connectors are placed: one DE-9 female D-sub connector for four external thermistors and one 9W4 male mixed type D-sub connector with four high-current pins for TEC connections and five conventional pins for thermistors. Close to the connectors a button for a hard reset of the Arduino is placed, enabling an Arduino reset without restarting the entire system. This button should be hidden to prevent any unwanted resets of the Arduino by incident. The position of the button and the cable interfaces also have to be chosen with respect to the rack cabinet, where it will be mounted later. In five of six devices assembled up to now, the connectors were placed at the right rearwards side of the rack, as shown in fig. B.10

⁴Manufactured by *Fischer Elektronik GmbH & Co. KG*.

⁵Manufactured by *TDK-Lambda*.

⁶Manufactured by *RS Components Handelsgesellschaft m.b.H.*

⁷Model *Noctua NF-A12x15 PWM*.

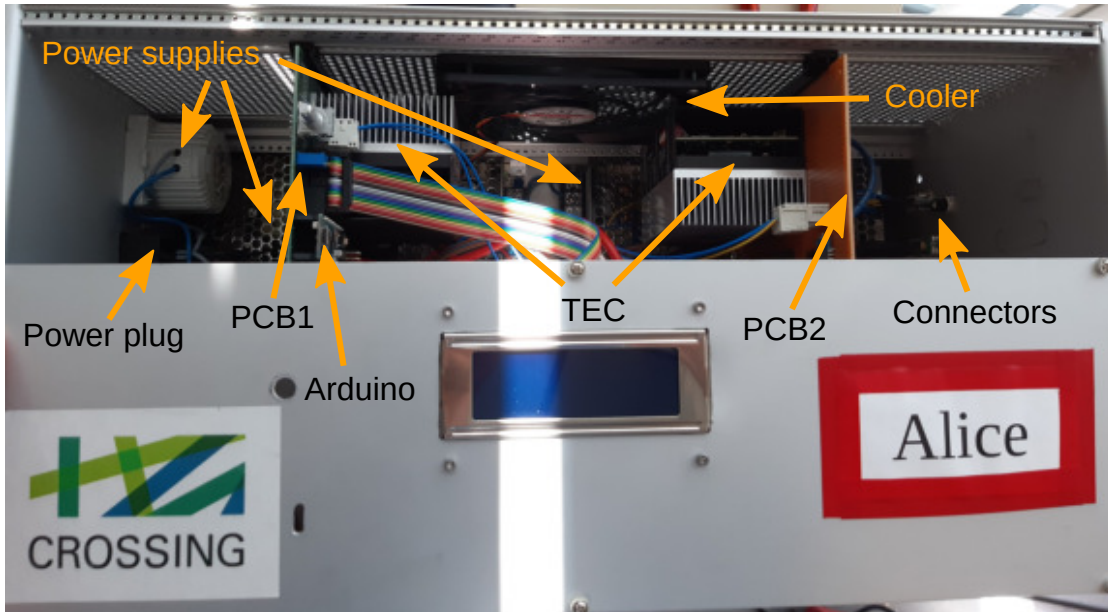


Figure B.10.: Device rack with assembled components.

The front plate of the rack has a feedthrough for the USB-Micro port of the Arduino, and drilled holes for the rotary encoder and the display (see fig. B.1).

B.5.1. Main printed circuit board

The electrical scheme of the main PCB is presented in fig. B.14. Here, the second revision of the board is presented, containing improvements and an optimized layout compared to the previous prototype. Information about the previous board revision can be found in [163].

The board contains an Arduino Micro, which is the central object controlling the TECs and the communication to the PC. The Arduino's digital outputs and inputs are connected to the rotary encoder and the LDC for manual system control. The connection is realized with flat ribbon cables and the connectors are mounted on the board.

The Arduino is also connected digitally via the SPI protocol with the external DACs (*AD5683*) and ADCs (*AD7192*) in order to provide a high temperature resolution. Analog signal lines are impedance-matched to the amplifiers *AD8534*. Those *rail-to-rail* amplifiers

provide a good impedance matching for voltages of 0-5 V. Zener diodes (5.1 V) connected parallel to the ADCs' inputs prevent their overload.

The voltage reference *ADR445B* provides a stable reference voltage of 5 V for the ADCs, increasing the repeatability of the ADC operation. The ERNI connector is connected as a standard Euro-rack connector with 12 volts to the small power supply. See scheme appendix B.5.1 for details.

The main PCB board allows for controlling the PTC10000, it does not provide any power supply nor connections to the TECs, since the TECC possesses comfortable screw contacts for wires directly from the 24 V supply. The correct wire size corresponding to the desired current was determined according to the DIN norm VDE 0298-4 [164]. For the implemented devices, stranded wires with 1.5 mm² cross-sectional area were used. The wires of the control loop (TEC and thermistor wires of the TECC) lead to the D-sub connector, mounted on the rack side (see appendix B.5).

Interfaces to the LCD as well as to the additional PCB (see appendix B.5.2) are optimized for the use of a flat ribbon cable for easy handling.

Interface *DEV2* is a connection to the additional PCB providing necessary inputs and collecting the output of the second TECC or a LD current driver, that is mounted on the second PCB. Within this connection, one digital, one analog output, ground reference and six analog inputs are combined, enabling flexible connection to any device at the second channel, that match the interface.

The parts that are mounted are listed in the table B.1. Mounting should be started on the side with integrated circuit parts. After finishing the bottom side, one can continue on the top side of the board. Generally, it is advised to mount smaller parts first and move continuously to bigger ones, starting with the surface-mounted resistors on the bottom side and finishing with the TEC (PTC10000) and cooler elements on the top side. The layout of the top and bottom sides is shown in fig. B.11 and fig. B.12.

B.5.2. Additional circuit board

An electrical scheme of this additional printed circuit board is shown in fig. B.13. The additional PCB possesses only few components: the TEC controller and the current source for the external thermistors *LM334*. Therefore, they were built manually with generic breadboards, so no PCB layout was completed. However, for a better and more comparable performance, this board can also be fabricated by machine. The required parts are listed in table B.2.

For a precise temperature measurement, a stable, temperature-independent current source is required. The *LM134* has an outstanding performance, but was not available for a purchase. Instead, the current reference *LM334* was used as a current source. The

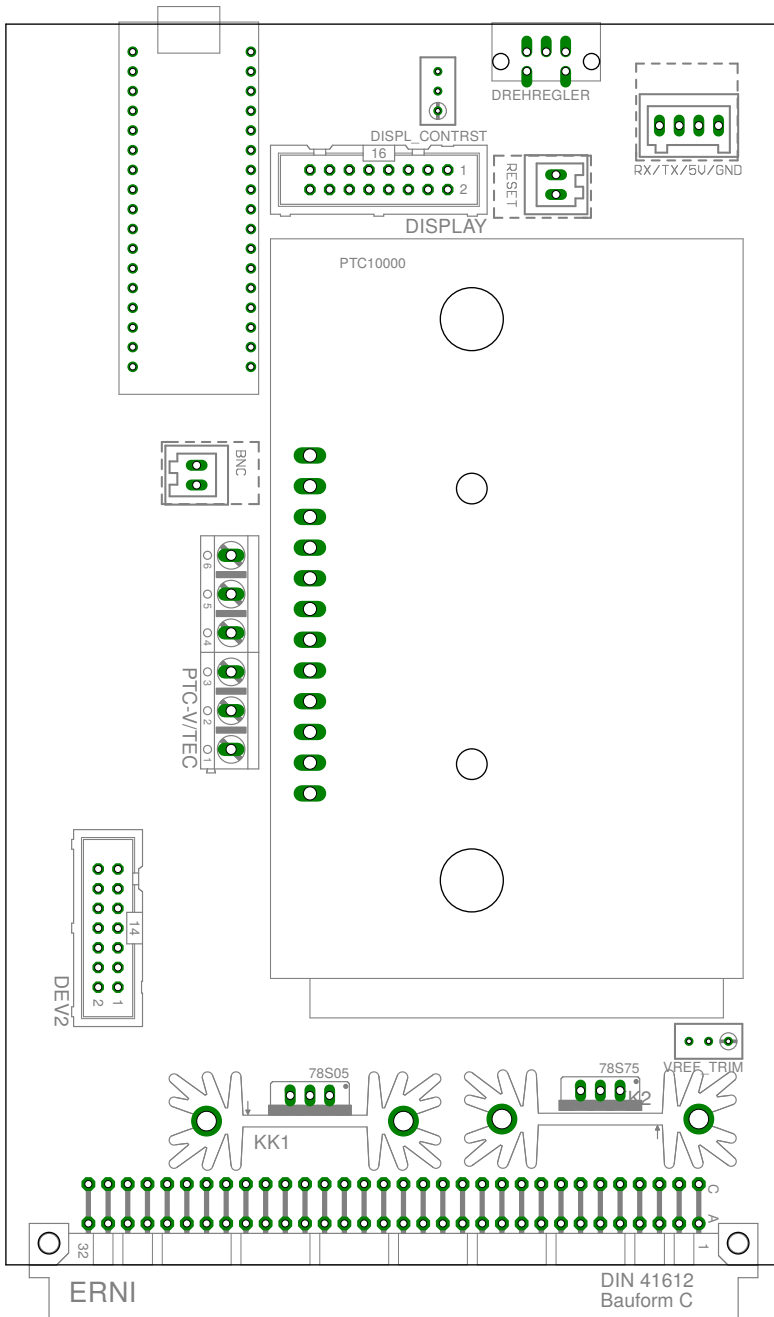


Figure B.11.: Top side of the main PCB.

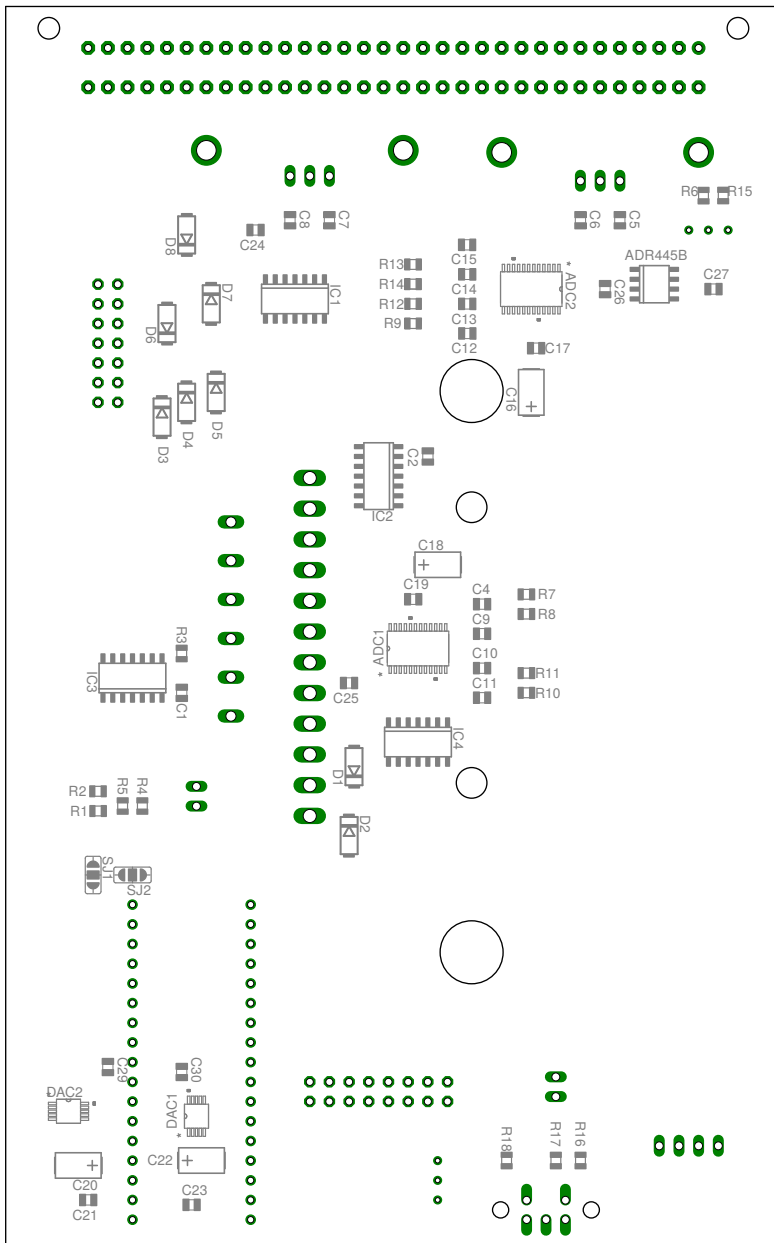


Figure B.12.: Bottom side of the main PCB.

Table B.1.: Bill of materials for board 1

Label on board	Device	Description	Package
C1, C2, C4, C6, C8, C9, C10, C11, C12, C13, C14, C15, C17, C19, C21, C23, C24, C25, C26, C27	C-EUC0805	Capacitor, SMD, 0.1 μ F, 50 V, \pm 5%	0805
C5, C7	C-EUC0805	Capacitor, SMD, 0.22 μ F, 25 V, \pm 5%	0805
C16, C18, C20, C22	CPOL-EUCT6032	Electrolytic capacitor, SMD, 10 μ F, 25 V, \pm 10%	2312
C29, C30	C-EUC0805	Capacitor, SMD, 10 nF, 50 V, \pm 5%	0805
R1, R2, R3, R4, R5, R16, R17, R18	R-EU_R0805	Resistor, SMD, 10 k Ω , 0.125 W, 1%	0805
R6	R-EU_R0805	Resistor, SMD, 100 k Ω , 0.125 W, 1%	0805
R7, R8, R9, R10, R11, R12, R13, R14	R-EU_R0805	Resistor, SMD, 100 Ω , 0.125 W, 1%	0805
R15	R-EU_R0805	Resistor, SMD, 1 k Ω , 0.125 W, 1%	0805
DISPL_CONTRST, VREF_TRIM	R-TRIMM3296W	Trimm resistor, 10 k Ω , \pm 10%	3296W
D1, D2, D3, D4, D5, D6, D7, D8	1SMB5918BT3G	Zener diode, 5.1 V, 3 W, \pm 5%	DO-214AA
IC1, IC2, IC3, IC4	AD8534	Operational amplifier	SOIC-14
ADC1, ADC2	AD7192BRUZ	Analog-to-Digital converter, two-channel, 24-Bit	TSSOP-24
ADR445B	ADR445BRZ	Voltage reference, 5 V	NSOIC-8
DAC1, DAC2	AD5683R-3	Digital-to-Analog converter, 16 bit, 5 V	MSOP10
78S05	78S05	Voltage Regulator, 5 V	TO-220-3
78S75	78S75	Voltage Regulator, 7.5 V	TO-220-3

Label on board	Device	Description	Package
KK1, KK2	SK104-PAD	Heatsink for Voltage Regulator, 14 K/W	-
DREHREGLER	STEC11B09	Rotatory encoder with taster, horizontal, PCB mounted	-
ERNI	VG64	PCB Eurocard connector socket, 64-pin type C/AC, 2.54 mm	VG64
PTC-V/TEC	AK500/6	Screwing contact, 6 pins, 5 mm	-
RX/TX/5V/GND	733-334	WAGO connector socket, 4 pins	-
RESET	733-332	WAGO connector socket, 2 pins	-
DEV2	ML14	Harting connector, 14 pins	-
DISPLAY	ML16E	Harting connector, 16 pins	-
ARDUINO_MICRO	Arduino Micro	Microcontroller board, Micro USB, mounted on pin headers	-
PTC10000	PTC10000	TEC PI-Controller	-

Table B.2.: Bill of materials for board 2

Label on board	Device	Description	Package
DEV2	ML14	Harting connector, 14 pins	-
RX/TX/5V/GND	733-334	WAGO connector socket, 4 pins	-
ERNI	VG64	PCB Eurocard connector socket, 64-pin type C/AC, 2.54 mm	VG64
I1,I2,I3	LM344	Three terminal adjustable current source	TO-92
Cooler	-	Heat sink for TO-92	-
R16, R17, R18	-	Resistor, 680 Ω , 5%	0414

resistor values $R_1 = R_2 = R_3 = 680 \Omega$ were calculated with formula 3 from [165], such that: $I_{\text{set}} \approx 100 \text{ mA}/^\circ\text{C}$.

However, the obtained performance was not sufficient, since fast temperature fluctuations were observed, amounting up to 0.1 K peak-to-peak, and exceeding the desired millikelvin range. The reason for this might be the current reference heating up and causing current fluctuations. To prevent this issue, the device should be used as a zero temperature coefficient current source, as described in its data-sheet [165] (see appendix B.8).

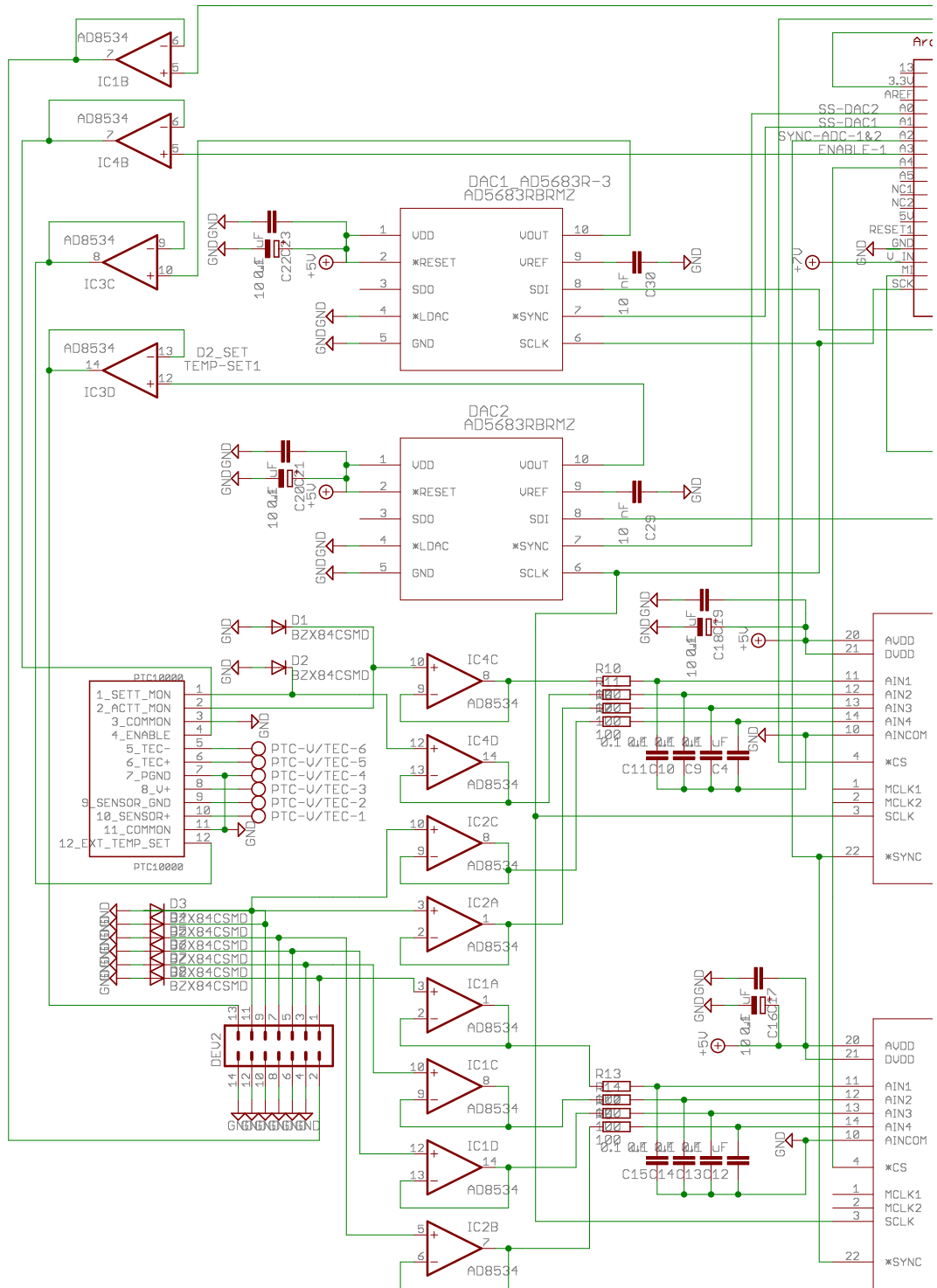
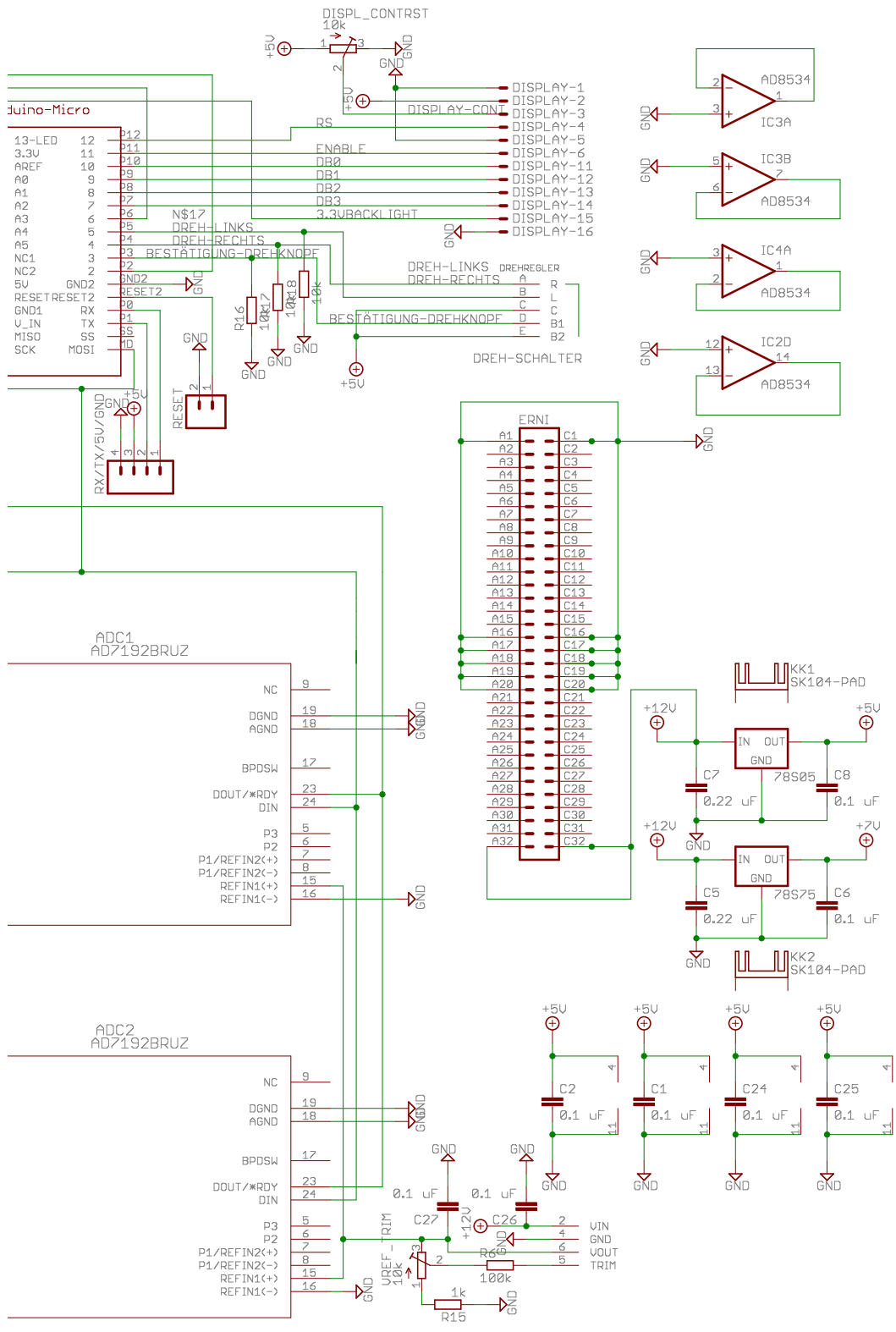


Figure B.14.: Electric scheme of the main PCB.



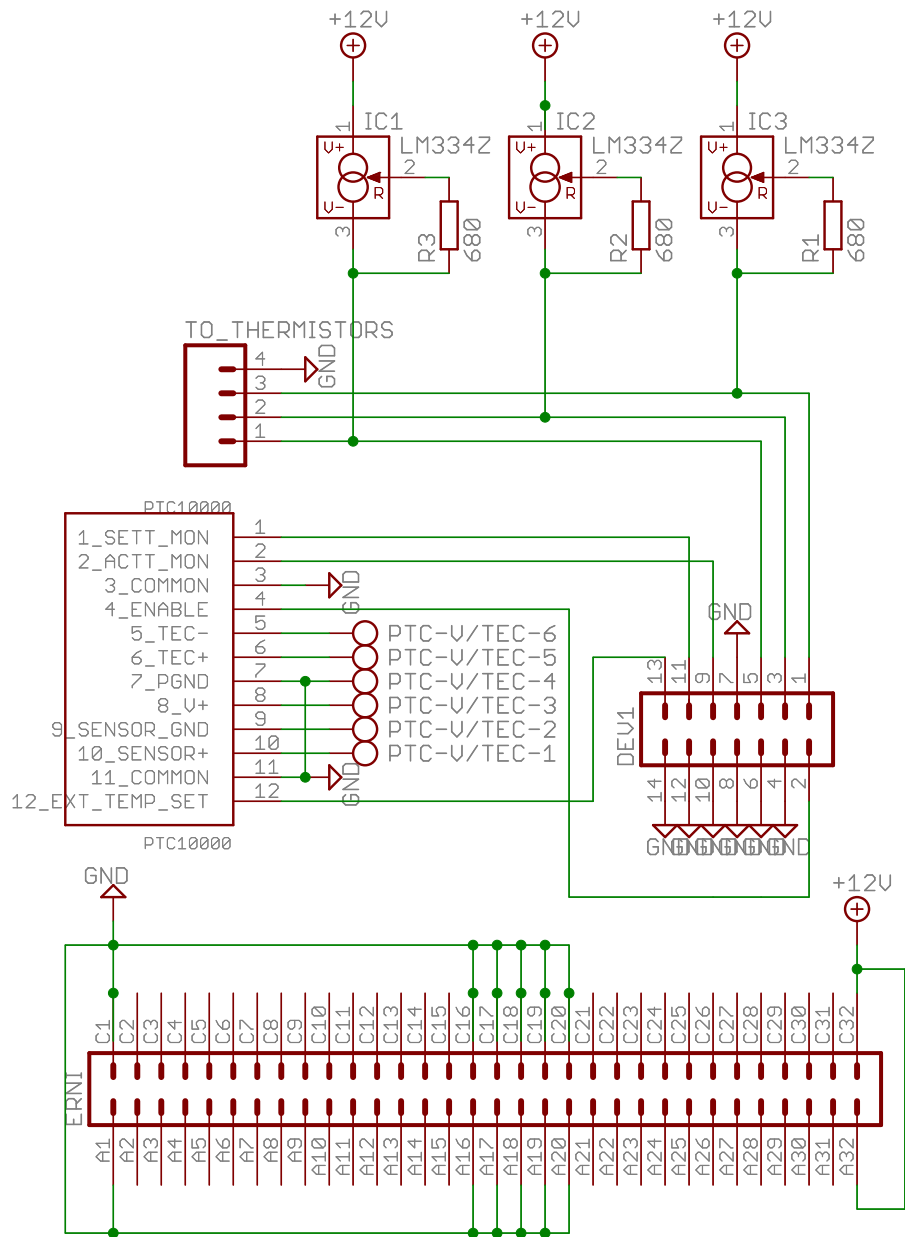


Figure B.13.: Electric scheme of the additional PCB.

B.6. Cables and cable management

With respect to the DIN standard VDE 0298-4 [164], stranded wires with 1.5 mm^2 cross-section area were used for TEC circuits within the implemented devices, both inside the rack and as connection to the stabilized device. For thermistor connections stranded wires with 0.22 mm^2 cross-sectional area were used.

Long cables may be an issue for the performance of the entire temperature stabilized system due to two main reasons: the cables' dielectric absorption [166] and its temperature fluctuation. Since the TEC current is oscillating during the stabilization process, the cables may be considered as capacitors, being charged and then discharged again. The dipoles in the dielectric material (cable insulation) need a short time period, denoted as relaxation time, to orient themselves according to the electrical field after each current polarity change. During this time, the voltage value that is measured at the thermistor cables is erroneous. Each cable movement or touch leads to a spike in voltage, causing an erroneous behaviour of the TECC and decreasing the overall temperature stability.

Furthermore, according to the Steinhart-Hart equations B.1 for the used thermistor *TCS620* [162], a resistance change of the cable by only 1Ω leads to a systematic error of about 1 mK at TECC. Depending on the cable length, thickness and its position relative to the heat sources within the rack, resistance changes in this range are a realistic scenario.

Therefore, all cables should be isolated thermally and fastened on the racks and housings to minimize the influence of the described phenomenon.

B.7. Software

The implemented software consists of two parts: the Arduino program (further referred to as *firmware*) and a Python program for remote control of the Arduino over a serial USB interface, enabling to control the entire implemented system remotely. In the following subsection a short description of both parts of the software is given.

B.7.1. Arduino firmware

The implemented firmware for the Arduino Micro allows for a reproducible and flexible manipulation of the entire dual channel temperature controller. Depending on the version of the software, different options and safety precautions are implemented, such as an automatic deactivation of the device, in case of a large deviation of the actual from set temperature (occurring, e.g., in the case that the set temperature is much smaller than

the room temperature). The software version is shown at the startup of the device for several seconds.

Before updating the firmware to the device, the name of the device (*NAME*) within the source code should be modified (line 30). This will simplify the communication of the device with the PC.

The *dacRange* (line 42) sets the output range of the external DAC and the corresponding resolution for the temperature settings. As default, higher resolution was chosen, limiting the minimal possible temperature. The temperature range is then 23-70 °C. The lower bound can be decreased down to zero degrees, if the *dacRange* is set to 0. In this case, the resolution decreases also by factor of 2 compared to fig. B.8 and further actions are required because temperatures below the dew point can be set. The minimal possible temperature can be set in line 1237.

The firmware is capable of communication over the serial USB interface, providing the collected information and reacting to the remote adjustments of the settings. For communication, a proprietary protocol is used, consisting of text commands with the characters octothorpe (#) and semicolon. While the former denotes the start and the end of a command, the semicolon separates the commands from the parameters. For example `#SET_TEMP_ONE;25.1234#` sets the temperature of the first TECC to 25.1234 °C. The temperature of both channels can be set with the resolution shown on fig. B.8, even though it is possible to send parameters with microkelvin precision. Since no calibration of the absolute temperatures was done the value temperature is only approximately correct, with a systematic error up to 1 °C. All implemented commands and their applications are listed in table B.3.

B.7.2. Python script

A Python 3 script for communication over Arduino's USB is implemented. It provides an interface for the proprietary USB communication protocol. For more details, please refer to the docstring comments of the script.

Table B.3.: Commands for communication with the system over USB serial connection.

Command	Notes
SET_TEMP_ONE	set temperature at ch.1, Parameter: float number
SET_TEMP_TWO	set temperature at ch.2, Parmeter: float number
ENABLE_PTC_ONE	enable TECC at ch. 1
ENABLE_PTC_TWO	enable TECC at ch. 2
DISABLE_PTC_ONE	disable TECC at ch. 1
DISABLE_PTC_TWO	disable TECC at ch. 2
TOGGLE_PTC_ONE	toggle output of TECC at ch. 1
TOGGLE_PTC_TWO	toggle output of TECC at ch. 2
SET_SLOPE_PTC_ONE	set ramp slope at ch. 1
SET_SLOPE_PTC_TWO	set ramp slope at ch. 2
ENABLE_RAMP_ONE	enable ramp at ch. 1
ENABLE_RAMP_TWO	enable ramp at ch. 2
DISABLE_RAMP_ONE	disable ramp at ch. 1
DISABLE_RAMP_TWO	disable ramp at ch. 2
WRITE_TO_EEPROM	save settings to local
GET_NAME	query the name of the device: A,B,C,D or Q
GET_DATA	query all temperature data. The name of the device, the time since the start of the arduino in ms, set temperature, set temperature monitor and actual temperature for both channels, and temperature of all three external thermistors are then returned.
GET_VERSION	query the firmware version
STATUS_IN	query the status of TECC at ch. 1
STATUS_OUT	query the status of TECC at ch. 2
T_IN_SET	query set temperature at ch. 1
T_IN_RET	query the monitor of set temperature at ch. 1
T_IN_ACT	query the actual temperature at ch. 1
T_OUT_SET	query set temperature at ch. 2
T_OUT_RET	query the monitor of set temperature at ch. 2
T_OUT_ACT	query the actual temperature at ch. 2
T_EXT_1	query temperature at external thermistor 1
T_EXT_2	query temperature at external thermistor 2
T_EXT_3	query temperature at external thermistor 3
NO_VALID_TEMP	error: set temperature invalid
NO_VALID_SLOPE	error: ramp slope invalid
NO_VALID_COMMAND	error: command not recognised
EXIT	exit serial communications over USB

B.8. Improvement suggestions and unresolved issues

During the prototyping period (several month) and at least four years of a non-stop operation with only a few breaks, a number of issues and errors were detected and resolved. However, several issues are still present. Since they are either not reproducible or very rare, they are hard to identify and to correct. In the present section their short description is given. Also, some strategies to avoid them and how to proceed in case of their occurrence are briefly described. Furthermore, some ideas for general performance improvement of the implemented device are shown.

- Temperatures that are shown at the display are not correct, since no calibration was performed. Different values of the set temperature, monitor of set temperature and actual temperature can be explained by different lead resistances within the PCBs and cables, that were often self-made. For the QKD experiment only relative temperatures are relevant, however, a proper calibration of the device might be helpful for other use cases.
- External thermistors show a jitter up to 0.1 °C, that cannot be verified by external devices⁸. A potential reason might be the temperature influence on the current reference *LM334*. To avoid it, other configuration with *LM334* as a zero temperature coefficient current source [165] can be used. Alternatively, the reference *REF200* with good thermal characteristics ([167], p.5) can be applied.
- Rarely, when the front plate is touched by a hand without an electrostatic discharge preventing wrist strap, the display shows some erratic output. Restart Arduino with the hard reset button then. The front panel is grounded, but the error is still occurring sometimes.
- While handling USB cables, after connection to the PC, the Arduino restarts or freezes. Restart Arduino with the hard reset button then.
- Very seldom, after an Arduino restart, the device does not show the actual temperature and set temperature saved in the electrically erasable programmable read-only memory (EEPROM), but 25.000 °C. Furthermore, the device is turned on, even if it is not shown on the front menu page, heating or cooling the device to 25 °C without updating any temperatures in the main menu 1 (shown in fig. B.2). Please, switch to the second menu page (fig. B.4) and turn off both channels as soon as possible, or turn both channels off by a remote command over USB. The reason for this issue is unknown due to its rare occurrence.

⁸7.5-digit multimeter Keithley 2010 from Tektronix, Inc.

-
- Sometimes, the USB connection is lost, due to some failure in the communication with the PC or due to some cable issues. Before restarting the python script, please disconnect the USB cable from the PC and then connect it again. Otherwise, the corresponding COM port will still be busy and not available for a new communication session.
 - Due to some errors during the assembly and connection of the TECs, some stabilized devices (the interferometer boxes) are connected to the 24 V potential. Removing this issue requires a complete reassembly of the TEC connections. Please make sure, that the stabilized device is connected to ground. This issue has not been observed with the next box revision.
 - The temperature ramp, implemented within the firmware is not reliable. Please use a python script for driving a temperature ramp remotely.
 - The Arduino can be exchanged after turning off the power and opening the front panel. After turning the device on again, please wipe the EEPROM manually or remotely.
 - The firmware and the remote control script for PC could be updated to send an emergency recovery warning over the serial interface to the remote PC after an emergency start.
 - The firmware and the remote control script for PC might be updated to enable EEPROM wipe remotely.
 - A firmware upgrade for better usability might be done, e.g. the options for choosing the thermistor current at the PI-controllers *PTC1000* and the resistance of the thermistors in menu 2 (cf. fig. B.4) should be removed. In some versions of the firmware it is already impossible to choose those options, but they still appear.

B.9. Combined LD source and TEC controller

The present two channel device was successfully tested as a LD current source and temperature controller during the project of Yannic Wolf [168]. For this purpose, instead of the additional PCB an evaluation board for the current source *PLD6500*⁹ was used.

⁹Manufactured by *Wavelength Electronics Inc.*

Bibliography

- [1] UN General Assembly et al. “Universal Declaration of Human Rights”. In: *UN General Assembly* 302.2 (1948), pp. 14–25.
- [2] W. Diffie and M. Hellman. “New directions in cryptography”. In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. doi: 10.1109/TIT.1976.1055638.
- [3] R. L. Rivest, A. Shamir, and L. Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. In: *Commun. ACM* 21.2 (1978), pp. 120–126. doi: 10.1145/359340.359342.
- [4] Johannes Buchmann. *Einführung in die Kryptographie*. 5th ed. Springer, 2010.
- [5] Kevin S McCurley. “The discrete logarithm problem”. In: *Proc. of Symp. in Applied Math.* Vol. 42. USA. 1990, pp. 49–74.
- [6] Kefa Rabah. “Review of Methods for Integer Factorization Applied to Cryptography”. In: *Journal of applied Sciences* 6.1 (2006), pp. 458–481.
- [7] P. W. Shor. “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”. In: *SIAM J. Comput.* 26.5 (1997), pp. 1484–1509.
- [8] Johannes A Buchmann et al. “Post-quantum cryptography: state of the art”. In: *The new codebreakers* (2016), pp. 88–108.
- [9] Daniel J Bernstein and Tanja Lange. “Post-quantum cryptography”. In: *Nature* 549.7671 (2017), pp. 188–194.
- [10] G. S. Vernam. “Cipher printing telegraph systems: For secret wire and radio telegraphic communications”. In: *Journal of the A.I.E.E.* 45.2 (1926), pp. 109–115.
- [11] C. E. Shannon. “Communication theory of secrecy systems”. In: *Bell Labs Technical Journal* 28.4 (1949), pp. 656–715.
- [12] William K Wootters and Wojciech H Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (1982), pp. 802–803.

-
-
- [13] Claude Cohen-Tannoudji, Bernard Diu, and Franck Laloë. *Quantenmechanik*. 4th ed. de Gruyter, 2009.
- [14] C. Charles Bennett and Giles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *2 International Conference on Computers*. Vol. 175. IEEE. 1984, p. 8.
- [15] Nicolas Gisin et al. “Quantum cryptography”. In: *Rev. Mod. Phys.* 74.1 (2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145.
- [16] Valerio Scarani et al. “The security of practical quantum key distribution”. In: *Reviews of modern physics* 81.3 (2009), p. 1301.
- [17] Matthias Geihs et al. “The Status of Quantum-Key-Distribution-Based Long-Term Secure Internet Communication”. In: *IEEE Transactions on Sustainable Computing* 6.1 (2021), pp. 19–29. DOI: 10.1109/TSUSC.2019.2913948.
- [18] Feihu Xu et al. “Secure quantum key distribution with realistic devices”. In: *Rev. Mod. Phys.* 92.2 (2020), p. 025002. DOI: 10.1103/RevModPhys.92.025002.
- [19] Charles H. Bennett, Gilles Brassard, and N. David Mermin. “Quantum cryptography without Bell’s theorem”. In: *Phys. Rev. Lett.* 68.5 (1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557.
- [20] W. Tittel et al. “Long-distance Bell-type tests using energy-time entangled photons”. In: *Physical Review A* 59 (1998), p. 4150. DOI: 10.1103/PhysRevA.59.4150.
- [21] W. Tittel et al. “Quantum Cryptography Using Entangled Photons in Energy-Time Bell States”. In: *Phys. Rev. Lett.* 84.20 (2000), pp. 4737–4740. DOI: 10.1103/PhysRevLett.84.4737.
- [22] T. Honjo et al. “Long-distance entanglement-based quantum key distribution over optical fiber”. In: *Opt. Express* 16.23 (2008), pp. 19118–19126. DOI: 10.1364/OE.16.019118.
- [23] Eleni Diamanti and Anthony Leverrier. “Distributing secret keys with quantum continuous variables: principle, security and implementations”. In: *Entropy* 17.9 (2015), pp. 6072–6092.
- [24] Eli Biham et al. “Security of quantum key distribution against all collective attacks”. In: *Algorithmica* 34.4 (2002), pp. 372–388.
- [25] P. W. Shor and J. Preskill. “Simple proof of security of the BB84 quantum key distribution protocol”. In: *Physical review letters* 85.2 (2000), pp. 441–444.
- [26] Renato Renner. “Security of quantum key distribution”. In: *International Journal of Quantum Information* 6.01 (2008), pp. 1–127.

-
-
- [27] Lars Lydersen et al. “Hacking commercial quantum cryptography systems by tailored bright illumination”. In: *Nature Photonics* 4.10 (2010), pp. 686–689.
- [28] Alexandra Weber et al. “Cache-Side-Channel Quantification and Mitigation for Quantum Cryptography”. In: (2021), pp. 235–256. DOI: 10.1007/978-3-030-88428-4_12.
- [29] Stefano Pirandola et al. “Fundamental limits of repeaterless quantum communications”. In: *Nature communications* 8.1 (2017), pp. 1–15.
- [30] Miralem Mehic et al. “Quantum Key Distribution: A Networking Perspective”. In: *ACM Comput. Surv.* 53.5 (2020), pp. 1–41. DOI: 10.1145/3402192.
- [31] Yu-Ao Chen et al. “An integrated space-to-ground quantum communication network over 4,600 kilometres”. In: *Nature* 589.7841 (2021), pp. 214–219. DOI: 10.1038/s41586-020-03093-8.
- [32] European Commission. *Quantum Flagship*. <https://qt.eu/about-quantum-flagship/>. Accessed on 25.11.2022. Dec. 2022.
- [33] European Commission. *The Digital Europe Programme*. <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>. Accessed on 25.11.2022. Dec. 2022.
- [34] European Commission. *Connecting Europe Facility*. <https://ec.europa.eu/inea/en/connecting-europe-facility>. Accessed on 25.11.2022. Dec. 2022.
- [35] European Telecommunications Standards Institute. *Industry Specification Group (ISG) on Quantum Key Distribution (QKD)*. <https://www.etsi.org/committee/qkd>. Accessed on 25.11.2022. Dec. 2022.
- [36] Marius Loeffler et al. *Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution*. https://openqkd.eu/wp-content/uploads/2021/03/OPENQKD_CurrentStandardisationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf. Accessed on 25.11.2022. Dec. 2022.
- [37] Eric Y. Zhu et al. “Toward a reconfigurable quantum network enabled by a broadband entangled source”. In: *J. Opt. Soc. Am. B* 36.3 (2019), B1–B6. DOI: 10.1364/JOSAB.36.0000B1.
- [38] W. Grice et al. “Multi-client quantum key distribution using wavelength division multiplexing”. In: *Quantum Communications and Quantum Imaging IX*. Vol. 8163. International Society for Optics and Photonics. SPIE, 2011, pp. 89–95. DOI: 10.1117/12.893788.

-
-
- [39] Florian Kaiser et al. “Polarization entangled photon-pair source based on quantum nonlinear photonics and interferometry”. In: *Optics Communications* 327 (2014), pp. 7–16. DOI: 10.1016/j.optcom.2014.03.056.
- [40] Sören Wengerowsky et al. “An entanglement-based wavelength-multiplexed quantum communication network”. In: *Nature* 564.7735 (2018), pp. 225–228. DOI: 10.1038/s41586-018-0766-y.
- [41] Sören Wengerowsky et al. “Entanglement distribution over a 96-km-long submarine optical fiber”. In: *Proceedings of the National Academy of Sciences* 116.14 (2019), pp. 6684–6688. DOI: 10.1073/pnas.1818752116.
- [42] Sören Wengerowsky et al. “Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre”. In: *npj Quantum Information* 6.1 (2020), p. 5. DOI: 10.1038/s41534-019-0238-8.
- [43] Yu-Yang Ding et al. “Polarization variations in installed fibers and their influence on quantum key distribution systems”. In: *Opt. Express* 25.22 (2017), pp. 27923–27936. DOI: 10.1364/OE.25.027923.
- [44] Rende Liu et al. “Analysis of polarization fluctuation in long-distance aerial fiber for QKD system design”. In: *Optical Fiber Technology* 48 (2019), pp. 28–33.
- [45] Jie Chen et al. “Active polarization stabilization in optical fibers suitable for quantum key distribution”. In: *Opt. Express* 15.26 (2007), pp. 17928–17936. DOI: 10.1364/OE.15.017928.
- [46] G. B. Xavier et al. “Active polarization control for quantum communication in long-distance optical fibers with shared telecom traffic”. In: *Microwave and Optical Technology Letters* 53.11 (2011), pp. 2661–2665. DOI: <https://doi.org/10.1002/mop.26320>.
- [47] Dong-Dong Li et al. “Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback”. In: *Opt. Express* 26.18 (2018), pp. 22793–22800. DOI: 10.1364/OE.26.022793.
- [48] Wen-Tan Fang et al. “On-chip generation of time-and wavelength-division multiplexed multiple time-bin entanglement”. In: *Opt. Express* 26.10 (2018), pp. 12912–12921. DOI: 10.1364/OE.26.012912.
- [49] Erik Fitzke et al. “Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding”. In: *PRX Quantum* 3.2 (2022), p. 020341. DOI: 10.1103/PRXQuantum.3.020341.

-
- [50] Yan-Lin Tang et al. “Measurement-Device-Independent Quantum Key Distribution over Untrusted Metropolitan Network”. In: *Phys. Rev. X* 6.1 (2016), p. 011024. DOI: 10.1103/PhysRevX.6.011024.
- [51] Siddarth Koduru Joshi et al. “A trusted node-free eight-user metropolitan quantum communication network”. In: *Science Advances* 6.36 (2020), eaba0959. DOI: 10.1126/sciadv.aba0959.
- [52] Muneer Alshowkan et al. “Reconfigurable Quantum Local Area Network Over Deployed Fiber”. In: *PRX Quantum* 2.4 (2021), p. 040304. DOI: 10.1103/PRXQuantum.2.040304.
- [53] Xiaoqing Zhong et al. “Simple multiuser twin-field quantum key distribution network”. In: *Physical Review Applied* 17.1 (2022), p. 014025.
- [54] Chang Hoon Park et al. “ $2 \times N$ twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing”. In: *npj Quantum Information* 8.1 (2022), pp. 1–12.
- [55] J. Brendel et al. “Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication”. In: *Phys. Rev. Lett.* 82.12 (1999), pp. 2594–2597. DOI: 10.1103/PhysRevLett.82.2594.
- [56] I. Marcikic et al. “Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber”. In: *Phys. Rev. Lett.* 93.18 (2004), p. 180502. DOI: 10.1103/PhysRevLett.93.180502.
- [57] Hiroki Takesue et al. “Long-distance entanglement-based quantum key distribution experiment using practical detectors”. In: *Opt. Express* 18.16 (2010), pp. 16777–16787. DOI: 10.1364/OE.18.016777.
- [58] Takahiro Inagaki et al. “Entanglement distribution over 300 km of fiber”. In: *Opt. Express* 21.20 (2013), pp. 23241–23249. DOI: 10.1364/OE.21.023241.
- [59] James D Franson. “Bell inequality for position and time”. In: *Physical review letters* 62.19 (1989), p. 2205.
- [60] Zhe-Yu Jeff Ou. *Multi-photon quantum interference*. Vol. 43. Springer, 2007.
- [61] Ken-ichiro Yoshino et al. “Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days”. In: *Opt. Express* 21.25 (2013), pp. 31395–31401. DOI: 10.1364/OE.21.031395.
- [62] M.A. Davis A.D. Kersey M.J. Marrone. “Polarisation-insensitive fibre optic Michelson interferometer”. In: *Electronics Letters* 27.6 (1991), 518–520(2).

-
- [63] Mario Martinelli. “A universal compensator for polarization changes induced by birefringence on a retracing beam”. In: *Optics Communications* 72.6 (1989), pp. 341–344. DOI: [https://doi.org/10.1016/0030-4018\(89\)90436-7](https://doi.org/10.1016/0030-4018(89)90436-7).
- [64] V. Secondi, F. Sciarrino, and F. De Martini. “Quantum spin-flipping by the Faraday mirror”. In: *Phys. Rev. A* 70.4 (2004), p. 040301. DOI: [10.1103/PhysRevA.70.040301](https://doi.org/10.1103/PhysRevA.70.040301).
- [65] Marco Pisani. “Multiple reflection Michelson interferometer with picometer resolution”. In: *Opt. Express* 16.26 (2008), pp. 21558–21563.
- [66] Li Liu et al. “Fiber-Optic Michelson Interferometric Acoustic Sensor Based on a PP/PET Diaphragm”. In: *IEEE Sensors Journal* 16.9 (2016), pp. 3054–3058. DOI: [10.1109/JSEN.2016.2526644](https://doi.org/10.1109/JSEN.2016.2526644).
- [67] Joseph Anthony Giordmaine and Robert C Miller. “Tunable coherent parametric oscillation in LiNb O 3 at optical frequencies”. In: *Physical Review Letters* 14.24 (1965), p. 973.
- [68] James Schneeloch et al. “Introduction to the absolute brightness and number statistics in spontaneous parametric down-conversion”. In: *Journal of Optics* 21.4 (2019), p. 043501. DOI: [10.1088/2040-8986/ab05a8](https://doi.org/10.1088/2040-8986/ab05a8).
- [69] Christophe Couteau. “Spontaneous parametric down-conversion”. In: *Contemporary Physics* 59.3 (2018), pp. 291–304.
- [70] Robert W Boyd. *Nonlinear optics*. Academic press/Elsevier, 2008.
- [71] Wolfgang Mauerer et al. “How colors influence numbers: Photon statistics of parametric down-conversion”. In: *Phys. Rev. A* 80.5 (2009), p. 053815. DOI: [10.1103/PhysRevA.80.053815](https://doi.org/10.1103/PhysRevA.80.053815).
- [72] M. Avenhaus et al. “Photon Number Statistics of Multimode Parametric Down-Conversion”. In: *Phys. Rev. Lett.* 101.5 (2008), p. 053601.
- [73] Marco Fiorentino et al. “Spontaneous parametric down-conversion in periodically poled KTP waveguides and bulk crystals”. In: *Opt. Express* 15.12 (2007), pp. 7479–7488.
- [74] Majeed M. Hayat, Sergio N. Torres, and Leno M. Pedrotti. “Theory of photon coincidence statistics in photon-correlated beams”. In: *Optics Communications* 169.1 (1999), pp. 275–287. DOI: [https://doi.org/10.1016/S0030-4018\(99\)00384-3](https://doi.org/10.1016/S0030-4018(99)00384-3).

-
-
- [75] O Gayer et al. “Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric LiNbO₃”. In: *Applied Physics B* 91.2 (2008), pp. 343–348.
- [76] Sabine Euler et al. “Spectral characterization of SPDC-based single-photon sources for quantum key distribution”. In: *The European Physical Journal Special Topics* 230.4 (2021), pp. 1073–1080.
- [77] Bahaa EA Saleh and Malvin Carl Teich. *Fundamentals of Photonics*. 2nd ed. John Wiley & Sons, 2007.
- [78] Rajiv Ramaswami, Kumar Sivarajan, and Galen Sasaki. *Optical Networks: A Practical Perspective*. Morgan Kaufmann, 2009.
- [79] Philippe M Becker, Anders A Olsson, and Jay R Simpson. *Erbium-doped fiber amplifiers: fundamentals and technology*. Elsevier, 1999.
- [80] Telecommunication Standardization Sector of ITU. *Characteristics of a single-mode optical fibre and cable*. en. Standard G.652. Geneva, CH: International Telecommunication Union, 2016. URL: <https://www.itu.int/rec/T-REC-G.652-201611-I>.
- [81] Telecommunication Standardization Sector of ITU. *Spectral grids for WDM applications: DWDM frequency grid*. en. Standard G.694.1. Geneva, CH: International Telecommunication Union, 2012. URL: <https://www.itu.int/rec/T-REC-G.694.1/en>.
- [82] S. Ten. “Ultra low-loss optical fiber technology”. In: *2016 Optical Fiber Communications Conference and Exhibition (OFC)*. 2016, pp. 1–3.
- [83] Fadri Grünenfelder et al. “Simple and high-speed polarization-based QKD”. In: *Applied Physics Letters* 112.5 (2018), p. 051108.
- [84] Cheng-Zhi Peng et al. “Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding”. In: *Phys. Rev. Lett.* 98.1 (2007), p. 010505. DOI: 10.1103/PhysRevLett.98.010505.
- [85] Yicheng Shi et al. “Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber”. In: *Applied Physics Letters* 117.12 (2020), p. 124002.
- [86] *Single Fiber Fusion Splicing*. Application Note AN103. Corning Inc., 2017. URL: <https://www.corning.com/media/worldwide/coc/documents/Fiber/application-notes/AN103.pdf>.

-
- [87] A.D. Yablon. *Optical Fiber Fusion Splicing*. Springer Series in Optical Sciences. Springer, 2005. ISBN: 9783540231042.
- [88] Technical support. *Thorlabs, GmbH*. Personal communication. Sept. 13, 2019.
- [89] G.S. Glaesemann and S.T. Gulati. “Design methodology for the mechanical reliability of optical fiber”. In: *Optical Engineering* 30 (1999), pp. 709–715.
- [90] R. J. Castilone. *Mechanical Reliability, Applied Stress Design Guidelines*. White Paper WP5053. Corning Inc., 2001. URL: <https://www.corning.com/microsites/coc/oem/documents/specialty-fiber/WP5053-Mech-Rel-Applied-Stress-Design-Guide.pdf>.
- [91] G. Scott Glaesemann. *Optical Fiber Mechanical Reliability, Review of research at Corning’s Optical Fiber Strength Laboratory*. White Paper WP8002. Corning Inc., 2017. URL: <https://www.corning.com/media/worldwide/coc/documents/Fiber/white-paper/WP8002.pdf>.
- [92] M. Bousonville et al. “New Phase Stable Optical Fiber”. In: *Proceedings of Beam Instrumentation Workshop MOPG033* (2012).
- [93] João M. P. Coelho et al. “3D Finite Element Model for Writing Long-Period Fiber Gratings by CO₂ Laser Radiation”. In: *Sensors* 13.8 (2013), pp. 10333–10347. DOI: 10.3390/s130810333.
- [94] Paulo Antunes et al. “Mechanical Properties of Optical Fibers”. In: *Selected Topics on Optical Fiber Technology*. IntechOpen, 2012. Chap. 19. DOI: 10.5772/26515.
- [95] *Corning SMF-28 Ultra Optical Fiber, Product Information*. Corning Inc. July 2014. URL: <https://www.corning.com/media/worldwide/coc/documents/Fiber/SMF-28%20Ultra.pdf>.
- [96] Axel Bertholds and Rene Dandliker. “Determination of the individual strain-optic coefficients in single-mode optical fibres”. In: *Journal of lightwave technology* 6.1 (1988), pp. 17–20.
- [97] S-Y Huang, James N Blake, and Byoung Yoon Kim. “Perturbation effects on mode propagation in highly elliptical core two-mode fibers”. In: *Journal of Lightwave Technology* 8.1 (1990), pp. 23–33.
- [98] C. D. Butter and G. B. Hocker. “Fiber optics strain gauge”. In: *Appl. Opt.* 17.18 (1978), pp. 2867–2869. DOI: 10.1364/AO.17.002867.
- [99] R. Slavik et al. “Ultralow thermal sensitivity of phase and propagation delay in hollow core optical fibres”. In: *Scientific Reports* 5 (2015), p. 15447.

-
-
- [100] Dan P Popescu et al. “Optical coherence tomography: fundamental principles, instrumental designs and biomedical applications”. In: *Biophysical reviews* 3.3 (2011), pp. 155–169.
- [101] Josef F Bille. “High resolution imaging in microscopy and ophthalmology: new frontiers in biomedical optics”. In: (2019).
- [102] Tetsushi Takano et al. “10 W injection-locked single-frequency continuous-wave titanium: sapphire laser”. In: *Optics Express* 29.5 (2021), pp. 6927–6934.
- [103] K. Schorstein and T. Walther. “A high spectral brightness Fourier-transform limited nanosecond Yb-doped fiber amplifier”. In: *Applied Physics B: Lasers and Optics* 97.3 (2009), pp. 591–597. DOI: 10.1007/s00340-009-3691-9.
- [104] Ed Miao. *Eospace Inc.* Personal communication. 2018.
- [105] M. Osinski and J. Buus. “Linewidth broadening factor in semiconductor lasers—An overview”. In: *IEEE Journal of Quantum Electronics* 23.1 (1987), pp. 9–29. DOI: 10.1109/JQE.1987.1073204.
- [106] Mijanur Rahim and Md. Asrafal Sekh. “Pulse Broadening in Semiconductor Optical Amplifier”. In: *13th International Conference on Fiber Optics and Photonics*. Optical Society of America, 2016, W3A.36. DOI: 10.1364/PHOTONICS.2016.W3A.36.
- [107] Philippe Griveau. *iXblue Photonics SAS*. Personal communication. Mar. 31, 2021.
- [108] Daniel Kiefer, Sebastian Hepp, and Thomas Walther. “High average power transform limited picosecond laser with flexible repetition rate and pulse duration”. In: *Opt. Lett.* 45.16 (2020), pp. 4488–4491. DOI: 10.1364/OL.397893.
- [109] *Safety Data Sheet per OSHA Guidelines for Wavelength Reference Absorption Cell - Hydrogen Cyanide*. Part Number: HCN-13-H(48)-2.4-FCAPC/PD. Wavelength References Inc. Oct. 2016. URL: <https://www.wavelengthreferences.com/wp-content/uploads/Data-Clarity.pdf>.
- [110] William C. Swann and Sarah L. Gilbert. “Line centers, pressure shift, and pressure broadening of 1530-1560 nm hydrogen cyanide wavelength calibration lines”. In: *J. Opt. Soc. Am. B* 22.8 (2005), pp. 1749–1756. DOI: 10.1364/JOSAB.22.001749.
- [111] *Clarity Precision Frequency Standard Narrow Line Semiconductor Laser*. Wavelength References Inc. Dec. 2020. URL: <https://www.wavelengthreferences.com/wp-content/uploads/Data-Clarity.pdf>.

-
- [112] Philipp Kleinpaß. “Time-resolved tomography measurements of a single-photon avalanche diode”. B.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2020.
- [113] Casimer DeCusatis and Carolyn J Sher DeCusatis. *Fiber Optic Essentials*. Elsevier, 2006.
- [114] Daniel Kiefer. “Ultraviolette Laser zur Kühlung relativistischer Ionenstrahlen”. PhD thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2019.
- [115] M. Movassaghi et al. “Noise Figure of Erbium-Doped Fiber Amplifiers in Saturated Operation”. In: *J. Lightwave Technol.* 16.5 (1998), p. 812.
- [116] Remus Nicolaescu et al. “Ultranarrow-linewidth, efficient amplification of low-power seed sources by a fiber amplifier”. In: *Appl. Opt.* 38.9 (1999), pp. 1784–1787. DOI: 10.1364/AO.38.001784.
- [117] B. Cole and M. L. Dennis. “S-band amplification in a thulium doped silicate fiber”. In: *OFC 2001. Optical Fiber Communication Conference and Exhibit. Technical Digest Postconference Edition (IEEE Cat. 01CH37171)*. Vol. 2. 2001, TuQ3–TuQ3. DOI: 10.1109/OFC.2001.927375.
- [118] Z. Li et al. “Thulium-doped fiber amplifier for optical communications at 2 μm ”. In: *Opt. Express* 21.8 (2013), pp. 9289–9297. DOI: 10.1364/OE.21.009289.
- [119] Abdollah Malakzadeh, Rasoul Pashaie, and Mohsen Mansoursamaei. “Gain and noise figure performance of an EDFA pumped at 980 nm or 1480 nm for DOFSs”. In: *Optical and Quantum Electronics* 52.2 (2020), p. 75.
- [120] C. R. Giles and E. Desurvire. “Modeling erbium-doped fiber amplifiers”. In: *Journal of Lightwave Technology* 9.2 (1991), pp. 271–283. DOI: 10.1109/50.65886.
- [121] William J Miniscalco. “Erbium-doped glasses for fiber amplifiers at 1500 nm”. In: *Journal of Lightwave Technology* 9.2 (1991), pp. 234–250.
- [122] SK Taherunnisa et al. “Effect of up-conversion luminescence in Er³⁺ doped phosphate glasses for developing Erbium-Doped Fibre Amplifiers (EDFA) and G-LED’s”. In: *Optical Materials: X* 3 (2019), p. 100034. DOI: <https://doi.org/10.1016/j.omx.2019.100034>.
- [123] Prachi Shukla and Kanwar Preet Kaur. “Performance analysis of EDFA for different pumping configurations at high data rate”. In: *International Journal of Engineering and Advanced Technology (IJEAT)* 2.5 (2013), pp. 487–490.

-
-
- [124] Till Dolejsky. “Hong-Ou-Mandel-experiment with SPDC photons for the quantum hub project”. B.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2019.
- [125] PA Franken et al. “Generation of optical harmonics”. In: *Physical Review Letters* 7.4 (1961), p. 118.
- [126] J. A. Fülöp et al. “Design of high-energy terahertz sources based on optical rectification”. In: *Opt. Express* 18.12 (2010), pp. 12311–12327. DOI: 10.1364/OE.18.012311.
- [127] Nikogosyan D.N. Dmitriev V.G. Gurzadyan G.G. *Handbook of Nonlinear Optical Crystals*. 3rd ed. Springer Series in Optical Sciences. Springer, 1999.
- [128] David S Hum and Martin M Fejer. “Quasi-phasematching”. In: *Comptes Rendus Physique* 8.2 (2007), pp. 180–198.
- [129] S Tanzilli et al. “PPLN waveguide for quantum communication”. In: *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics* 18.2 (2002), pp. 155–160.
- [130] Y Furukawa et al. “Green-induced infrared absorption in MgO doped LiNbO₃”. In: *Applied Physics Letters* 78.14 (2001), pp. 1970–1972.
- [131] GD Boyd and DA Kleinman. “Parametric interaction of focused Gaussian light beams”. In: *Journal of Applied Physics* 39.8 (1968), pp. 3597–3639.
- [132] Shekhar Guha and Leonel Pastor Gonzalez. *Laser beam propagation in nonlinear optical media*. Vol. 1. CRC Press Boca Raton, FL, USA, 2014.
- [133] AQ6370C Optical Spectrum Analyzer. 4th ed. IM AQ6370C-01EN. Yokogawa Meters and Instruments Corporation. Aug. 2013. URL: <https://cdn.tmi.yokogawa.com/IMAQ6370C-01EN.pdf>.
- [134] Dietrich Marcuse. “Curvature loss formula for optical fibers”. In: *JOSA* 66.3 (1976), pp. 216–220.
- [135] A Zendehnam et al. “Investigation of bending loss in a single-mode optical fibre”. In: *Pramana* 74.4 (2010), pp. 591–603.
- [136] Ross T Schermer and James H Cole. “Improved bend loss formula verified for optical fiber by simulation and experiment”. In: *IEEE Journal of Quantum Electronics* 43.10 (2007), pp. 899–909.
- [137] Christian Schulze et al. “Mode resolved bend loss in few-mode optical fibers”. In: *Optics express* 21.3 (2013), pp. 3170–3181.

-
- [138] Mable P. Fok et al. “Optical Layer Security in Fiber-Optic Networks”. In: *IEEE Transactions on Information Forensics and Security* 6.3 (2011), pp. 725–736. DOI: 10.1109/TIFS.2011.2141990.
- [139] S. Z. Muhd-Yassin et al. “All fiber optical band-pass filter using macro-bending approach”. In: *2012 IEEE 3rd International Conference on Photonics*. 2012, pp. 242–245.
- [140] Daniel Hofmann. “Characterisation of a photon-pair source for quantum key distribution in a telecommunication network”. M.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2019.
- [141] Maximilian Jörg Tippmann. “Development of a pulsed all-fiber SPDC photon pair source”. M.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2020.
- [142] Maximilian Mengler. “Charakterisierung der Effizienz und des Jitters von Einzelphotonendetektoren mittels POVMs”. B.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2020.
- [143] M.S. Elezov et al. “Active and passive phase stabilization for the all-fiber Michelson interferometer”. In: *Journal of Physics: Conference Series* 1124 (2018), p. 051014. DOI: 10.1088/1742-6596/1124/5/051014.
- [144] P. Toliver et al. “Continuously active interferometer stabilization and control for time-bin entanglement distribution”. In: *Opt. Express* 23.4 (2015), pp. 4135–4143. DOI: 10.1364/OE.23.004135.
- [145] Thorlabs Inc. online. Accessed on 31.12.2021. URL: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=6246.
- [146] Roßmann Electronic GmbH. *Thermoelectric cooler O6.0-51.4 (TEC1-12706)*. online. Accessed on 02.09.2022. URL: <https://cdn-reichelt.de/documents/datenblatt/C800/TECB1.pdf>.
- [147] Leon Baack. “Optimisation of parts of a set-up for quantum key distribution”. B.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2018.
- [148] Leonard Wegert. “Preparations for Assembling Franson Interferometers in a Quantum Key Distribution Setup”. B.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2019.
- [149] Lucas Bialowons. “Completion of a 4-Party Time-bin Entanglement QKD System”. M.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2021.
- [150] ID Quantique Inc. *Infrared Single-Photon Counter*. July 28, 2015.

-
- [151] Kai Roth. “Development of an electronic system for time measurements in an Alice-/Bob- module”. B.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2016.
- [152] Sergey Polyakov, Alan Migdall, and Sae Woo Nam. *Simple and Inexpensive FPGA-based Fast Multichannel Acquisition Board*. online. Accessed on 05.09.2022. URL: <https://www.nist.gov/services-resources/software/simple-and-inexpensive-fpga-based-fast-multichannel-acquisition-board-0>.
- [153] Stefan Schürl. “Development of an FPGA-based system for high-precision time measurement”. M.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2017.
- [154] Kai Roth. “Development of a Key Management System for Quantum Key Distribution”. M.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2019.
- [155] ID Quantique Inc. *Time Controller*. online. Accessed on 29.11.2022. URL: <https://www.idquantique.com/quantum-sensing/products/id900-time-controller/>.
- [156] Volker Fürst. *Deutsche Telekom Technik GmbH*. Personal communication. Nov. 20, 2022.
- [157] *Environmental Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment; Classification of environmental conditions; Stationary use at weatherprotected locations*. en. Standard EN 300 019-1-3 v2.4.1. European Telecommunications Standards Institute, 2014. URL: https://www.etsi.org/deliver/etsi_en/300001_300099/3000190103/02_04_01_60/en_3000190103v020401p.pdf.
- [158] Google Maps. *Darmstadt*. <https://goo.gl/maps/pNjml2cx6RVM9Zun8>. Accessed on 15.11.2021. Nov. 2021.
- [159] Wavelength Electronics Inc. *TEC Controller PTC10000 Datasheet*. online. Accessed on 20.09.2022. URL: <https://www.teamwavelength.com/download/Datasheets/ptcseries.pdf>.
- [160] Jonathan D. Weiss, Robert J. Kaplar, and Kenneth E. Kambour. “A derivation of the van der Pauw formula from electrostatics”. In: *Solid-State Electronics* 52.1 (2008), pp. 91–98. DOI: 10.1016/j.sse.2007.07.029.

-
- [161] Erik Fitzke, Florian Niederschuh, and Thomas Walther. “Generating Functions and Automatic Differentiation for Photon-Number-Resolved Simulations with Multimode Gaussian States”. In: *arXiv preprint arXiv:2209.05330* (2022).
- [162] Wavelength Electronics Inc. *Thermistor TCS620 Datasheet*. online. Accessed on 20.09.2022. URL: <https://www.teamwavelength.com/download/Datasheets/TCS-series-thermistors.pdf>.
- [163] Lukas Brozio. “Optimisation of a Temperature Stabilisation for a Quantum Hub”. B.Sc. Thesis. Darmstadt, Germany: Technische Universität Darmstadt, 2015.
- [164] *DIN VDE 0298-4*. de. Standard 0298-4. Deutsches Institut für Normung. URL: https://www.vde-verlag.de/buecher/leseprobe/9783800746910_PROBE_01.pdf.
- [165] Texas Instruments Inc. *Current reference LM334 Data Sheet*. online. Accessed on 31.08.2022. URL: <https://www.ti.com/lit/ds/symlink/lm134.pdf?ts=1629265180023>.
- [166] D. Grand and S. Wurcer. *Avoiding Passive-Component Pitfalls*. en. Application Note AN-348. Norwood, USA: Analog Devices. URL: <https://www.analog.com/media/en/technical-documentation/application-notes/500824934643930414583807523874018494695982855668424783486554001060AN348.pdf>.
- [167] Texas Instruments Inc. online. Accessed on 31.08.2022. URL: <https://www.ti.com/lit/ds/symlink/ref200.pdf>.
- [168] Yannic Wolf. “Aufbau einer Temperatur- und Stromsteuerung für eine Laserdiode”. Undergraduate research project. Darmstadt, Germany: Technische Universität Darmstadt, 2016.

List of Figures

2.1. Time-bin encoding protocol.	9
2.2. Multiplexed time-bin coding. Correlated time-bins at different multiplexing stages are coloured equally.	12
2.3. Cross-sections of different glass fiber types. The pictures are at the correct scale.	19
2.4. Attenuation profile of a typical single-mode fiber (SM fiber) and different communication bands. Data from an actual measurement.	20
2.5. Thermally induced elongation per meter of the <i>SMF-28</i> coiled fiber for strain values $\varepsilon_0 = 0$, $\varepsilon_1 \approx 1.2 \cdot 10^{-3}$ and $\varepsilon_2 \approx 3.7 \cdot 10^{-4}$. The straight lines are fitted to corresponding data sets.	24
2.6. Functional principle of white light interferometry method for measurement of interferometer arm-length mismatches. Modulated optical spectrum in (a), measured by optical spectrum analyzer (OSA), can be transformed into a distance value by a FFT (b).	26
3.1. Overview of the implemented entangled photon pair source. Seed DL: stabilized at $\lambda = 1550.5$ nm diode laser, delivering the signal to be amplified, AMOD: electro-optic amplitude modulator for pulse shaping, EDFA: Erbium-doped fiber amplifier, SHG: second harmonic generation, generating light at 775.25 nm (red), SPDC: spontaneous parametric down-conversion, generating two energy-time entangled photons.	31
3.2. Long term stability of the central frequency of the seed laser source.	32
3.3. Pulse generation module. AMOD: electro-optic modulator, rf-Amplifier: radio frequency amplifier, BS: fiber beam splitter, thick black line: optical fiber.	33
3.4. Pulse shape for bursts of pulses as output from the erbium-doped fiber amplifier (EDFA). Pulse duration vary slightly depending on the repetition rate (RR).	34
3.5. Pulse shape for bursts of two and four pulses at various RRs.	35

3.6. Absorption and emission coefficients of erbium doped fiber. (Data is courtesy of Fibercore Inc.)	36
3.7. Pumping laser system before frequency conversion. Seed DL: frequency stabilized laser, FI: Faraday Isolator, AMOD: electro-optic modulator for amplitude modulation, BPF: band-pass filter, WDM: wavelength-division multiplexer, Er-Fiber: erbium-doped fiber, DL A, DL B: pumping diode lasers, Circ: circulator, FBG: fiber Bragg grating, BS: beam splitter, PM: power meter, BD: beam dump, blue points: FC/APC connectors.	38
3.8. Performance of the spliced EDFA in continuous wave (cw) operation regime.	39
3.9. Optical spectrum of the EDFA in cw operation regime. Amplified spontaneous emission (ASE) around 1530 nm is suppressed by 77 dB.	40
3.10. Performance of the spliced EDFA in pulsed operation regime for 1 ns long pulses.	41
3.11. Optical spectrum of the EDFA in the pulsed regime for 1 ns long pulses. . .	42
3.12. Stability of the EDFA during cw operation for an arbitrarily chosen power. The inset shows a histogram of the stabilized case. Measured at the output of a polarizing beam splitter with an acquisition rate of 1 Hz.	44
3.13. Scheme of the SHG part of the set-up. The fundamental wave at 1550 nm (black) is going through the non-linear crystal (SHG), generating light at 775 nm (red) and being filtered out in a coiled fiber, that is put in a box absorbing the dissipated light for security reasons. After the filtering, in a 90:10 beam splitter (BS), the generated light intensity is observed in a power meter (PM), the last port is coupled to a beam dump (BD). The second harmonic generation (SHG)-module is controlled in temperature by a TEC-controller. Blue marks denote the fiber connections via FC/APC connectors in mating sleeves.	46
3.14. Average optical power of SHG light in the cw (blue solid and red dashed line) and pulsed (green line, burst with four pulses (FPB) at 50 MHz and 1 ns) regimes as a function of the average fundamental power. Red dashed line denotes a fit with eq. (3.5), green and blue lines denote a fit with eq. (3.7) to pulsed and cw operation data correspondingly.	47
3.15. Optical spectrum of the SHG in both, pulsed and cw regimes. The peak at 1550 nm is an artifact caused by the second order of diffraction of 775 nm in the OSA.	50

3.16. Scheme of the components used for spontaneous parametric down-conversion (SPDC). Red line: light at 775 nm , black line: light at 1550 nm , SPDC: non-linear crystal, TEC-controller: temperature stabilization system, BPF: 5 nm band-pass filter, EF1, EF2: long-pass filters, PBS: polarization beam splitter, BD: beam dump for light isolation, blue points: FC/APC connectors.	52
3.17. Photon pair generation rate as a function of the pump power. Uncertainties are smaller than the data points.	53
4.1. Scheme of the implemented receiver module. Yellow lines denote standard single mode fibers SMF-28, black lines denote electrical connections. Photons enter the circulator (CIR) at the input of the receiver, located before the Michelson interferometer, consisting of a 50:50 beam splitter (BS). The long arm of the interferometer is mounted around the fiber stretcher (FS) and the Faraday rotator mirrors (FM1 and FM2) reflect the incident photons that are then detected by the single photon avalanche detectors (SPADs) D0 and D1. The arrival times of the photons are measured by a time-tagger and evaluated by the computer. T-meter is a multimeter for reference temperature measurements at the fiber stretcher. Clock synchronization for the time tagger is not shown in the picture. Long term stability and phase adjustment is performed by the remotely controlled two-stage temperature stabilization system.	56
4.2. Exploded-view CAD drawing of the temperature stabilized box with internal devices. Glass fiber and electrical cables are not shown. FM - Faraday mirror, TEC - thermoelectric cooler, MS - mating sleeve for optical fiber connectors.	59
4.3. External view of the stabilized box with a silicon isolation layer, inside a polystyrene box. Here only bottom and side walls are shown. Test IF connectors - connectors of a second interferometer built inside the box. . .	60
4.4. Static tensioner for the optical glass fiber. The glass fiber is wound around the cylinder in the thread-shaped milling. The tension is achieved by moving the nuts on the bolt inside the cylinder, the nut in the middle locks the tensioner.	61
4.5. Simplified scheme of the implemented electronic temperature controller for the interferometers. A microcontroller controls two stabilization loops: one loop stabilizes the interferometer and the inner components (shown in red), the second loop stabilizes the surrounding box (shown in blue). Additional thermometers (T-meter) monitor the temperature at the interferometer, in the box and outside.	63

4.6. Steps for precise cutting of fiber and fiber pigtailed components. The component to be cut (blue cylinder with the blue fiber pigtail) is mounted on a special cutting setup. 1: Mounting of the component on the setup. 2: Pulling on the fiber with a small force. 3: Closing the lid of the fiber holder. 4: Removing the mechanical tension. 5: Moving of the component with attached fiber holder to the fiber cleaver.	66
4.7. Inside view of the stabilization box with two installed interferometers. FM - Faraday rotator mirror, BS - fiber beam splitter. Polystyrene flakes fill the entire free space after finished installation to prevent convection. Thermistors are for temperature observation inside the box. Adhesive film is used to keep fibers and cables in place.	69
4.8. Scheme of the processes for the QKD experiment: qubit generation (green), data acquisition from Alice (red) and Bob (blue) and evaluation and active phase adjustment (black). AFG: arbitrary function generator, PG1, PG2: pulse generators, rf-Driver: radio frequency amplifier, AMOD: amplitude modulator, A1,A2: Alice’s detectors, B1,B2: Bob’s detectors, PC: personal computer, β : phase of Bob’s interferometer.	73
4.9. Data flow diagram for the measurement and evaluation script of the experiment. The main thread manages the physical devices represented by depicted objects, running measurement iterations and storing the most relevant data. TCU: temperature controlling unit of the interferometer. . .	74
4.10. Typical time-bin histogram for time-multiplexed pulses for a key exchange period of one minute. Purple and green highlighted areas denote corresponding time bins, from which the key is extracted. Alice’s histogram has a smaller amplitude and a slightly higher width compared Bob’s signal due to the 6.75 dB attenuation and the chromatic dispersion of the fiber link, while Bob is connected directly to the source.	75
5.1. Approximate route of the used optical communication fiber, deployed between Darmstadt and Griesheim. The qubits are generated in a lab at the Network Innovation Center (NIC) in Darmstadt, then sent to Griesheim, turned around there and detected again at NIC. Entangled qubits are detected directly at NIC, without leaving the lab. (Map source: Google Maps 2021 [158])	81
5.2. Qubit source and Bob’s receiver in the operation room during the field-test	83
5.3. Long-term temperature stability of the interferometer in the laboratory environment. Two data loggers are placed in the polystyrene box and outside the box. Measurement started after 24 h warm-up.	84

5.4. Typical temperature curves during a temperature change of 2 K. The signal of the temperature controller used for stabilization, self-made reference thermometer of the temperature controller and the measurement by an external multimeter <i>Keithley 2010</i>	86
5.5. Thermal elongation of the <i>SMF-28</i> coiled fiber without strain (Bob) and with different strain forces (Alice and Source). The straight lines are fitted to corresponding data sets. Same figure as fig. 2.5.	87
5.6. Sifted key rate and quantum bit error rate (QBER) for a five hour long QKD experiment.	89
5.7. Temperatures during the key exchange. Laboratory temperature falls, Alice's remains constant, Bob's must be corrected.	90
A.1. Scheme for the stabilization system for the EDFA. The source for 5 V may act as a typical USB power supply. the BNC is connected to the ADC hat of the Raspberry Pi.	96
B.1. Front panel elements of the controller. The menu shown at display features three pages (see appendix B.2). For manual operation, the cursor position (here shown in the upper left corner) can be set by turning the rotary encoder knob. Settings are entered by pushing the button. The micro USB port enables software updates and access to the Arduino remote control of the device.	98
B.2. Main menu 1, showing the state of the TECCs and the relevant temperatures.	99
B.3. Confirmation question completing the temperature adjustment process.	99
B.4. Main menu 2, showing the temperatures of the external thermistors. Also, here the state of the TECs can be changed.	100
B.5. Main menu 3, enabling automatic temperature ramps.	100
B.6. Boot message in case of the emergency boot. Otherwise only module name and the firmware version is shown. <i>A</i> is an example for name.	101
B.7. Memory clearing warning.	101
B.8. Setting resolution as function of the temperature. The resolution is non-linear, due to the temperature dependence of the thermistor resistance.	102
B.9. Functional diagram of the dual channel TEC- and LD-current controller. LCD - display, DAC - digital-to-analog converter, ADC - analog-to-digital converter, TEC - thermoelectric cooler, TECC - thermoelectric cooler controller, T-meter - thermometer, not used for regulation.	103
B.10. Device rack with assembled components.	105
B.11. Top side of the main PCB.	107

B.12.Bottom side of the main PCB.	108
B.14.Electric scheme of the main PCB.	112
B.13.Electric scheme of the additional PCB.	114

List of Tables

3.1. Laser source properties in two operating modes from datasheet [111]. . .	32
3.2. Measured FWHM pulse duration $\tau_{\text{pulse,meas}}$ of the amplified pulses at different RRs and within single-pulse (SP), double-pulse burst (DPB) or burst with four pulses (FPB). The uncertainty of the measurements amounts to 0.05 ns. $\tau_{\text{pulse,set}} = 1$ ns in all cases.	35
3.3. Measured pulse energies E_{Pulse} in nanojoule for pulses at different RRs and bursts with different pulse numbers. The pulse energies within single bursts vary up to 15%.	43
3.4. Fit parameter results for SHG with model eq. (3.7) for cw and pulsed operation mode with FPB at $f_{\text{RR}} = 50$ MHz and $\tau_{\text{fund}} = 1$ ns.	49
4.1. interferometer (IF) losses and the relative loss ratios of short-to-long arms for each interferometer.	70
A.1. Bill of materials for stabilization system	96
B.1. Bill of materials for board 1	109
B.2. Bill of materials for board 2	111
B.3. Commands for communication with the system over USB serial connection.	117

Abbreviations

ADC	analog-to-digital converter
AFG	arbitrary function generator
AP	attenuation profile
ASE	amplified spontaneous emission
BB84	Bennet-Brassard 84
BBM92	Bennet-Brassard-Mermin 92
BPF	band-pass filter
BS	beam splitter
CD	chromatic dispersion
cw	continuous wave
DAC	digital-to-analog converter
DL	diode laser
DPB	double-pulse burst
DTT	Deutsche Telekom Technik GmbH
EDFA	erbium-doped fiber amplifier
EEPROM	electrically erasable programmable read-only memory
EOM	electro-optic modulator
ESA	excited state absorption
ETSI	European Telecommunications Standards Institute
FI	Faraday isolator
FM	Faraday rotator mirror
FPB	burst with four pulses

FPGA field-programmable gate array
FWHM full width at half maximum
HCN hydrogen cyanide
IF interferometer
ITU-T International Telecommunication Union Telecommunication Standardization Sector
LQO Laser and Quantum Optics research group
MFD mode field diameter
MI Michelson interferometer
MZI Mach-Zehnder interferometer
NA numerical aperture
NIC Network Innovation Center
OSA optical spectrum analyzer
OTP Vernam One-Time-Pad
PBS polarizing beam splitter
PCB printed circuit board
PMD polarization mode dispersion
PM fiber polarization-maintaining fiber
PPKTP periodically poled potassium titanyl phosphate
PPLN periodically poled lithium niobate
QBER quantum bit error rate
QKD quantum key distribution
RF amplifier radio frequency power amplifier
RPi Raspberry Pi
RR repetition rate
SHG second harmonic generation
SM fiber single-mode fiber
SOA semiconductor optical amplifier
SPAD single photon avalanche detector
SPDC spontaneous parametric down-conversion

TEC thermoelectric cooler

TECC thermoelectric cooler controller

TiSa titan:sapphire laser

TPI two-photon interference

WDM wavelength division multiplexing

List of publications

Journal publications

O. Nikiforov, E. Fitzke, F. Wissel, M. Gunkel, Th. Walther. "Test of time-bin entanglement quantum key distribution with robust interferometer assemblies under realistic operating conditions", to be submitted.

E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, Th. Walther, F. Wissel, M. Gunkel. "Scalable Network for Simultaneous Pairwise Quantum Key Distribution via Entanglement-Based Time-Bin Coding". In: *PRX Quantum*. 2.3 (2022).

M. Geihs, O. Nikiforov, D. Demirel, A. Sauer, D. Butin, F. Günther, G. Alber, Th. Walther, J. Buchmann. "The Status of Quantum-Key-Distribution-Based Long-Term Secure Internet Communication". In: *IEEE Transactions on Sustainable Computing* 6.1 (2021), honored with the Collaboration Award of CROSSING.

A. Weber, O. Nikiforov, A. Sauer, J. Schickel, G. Alber, H. Mantel, Th. Walther. "Cache-Side-Channel Quantification and Mitigation for Quantum Cryptography". In: *European Symposium on Research in Computer Security*, (2021), honored with the Collaboration Award of CROSSING.

S. Euler, E. Fitzke, O. Nikiforov, D. Hoffmann, T. Dolejsky, Th. Walther. "Spectral characterization of SPDC-based single-photon sources for quantum key distribution". In: *The European Physical Journal Special Topics* 230.4 (2021).

O. Nikiforov, L. Drzewietzki, S. Stutz, S. Breuer. "Passively mode-locked quantum dot laser subject to dual long cavity time-delayed optical feedback". In: *Materials Today: Proceedings* 7 (2019).

O. Nikiforov, L. Jaurigue, L. Drzewietzki, K. Lüdge, S. Breuer. "Experimental demonstration of change of dynamical properties of a passively mode-locked semiconductor laser subject to dual optical feedback by dual full delay-range tuning". In: *Opt. Express* 13.24 (2016).

Conference contributions

O. Nikiforov, E. Fitzke, D. Hofmann, K. Roth, Th. Walther. "Test of a time-bin entanglement-based QKD System in a commercial optical link". In: *QCALL-Conference (Quantum Communication for All)*, Mondello, Italy (2019).

O. Nikiforov, Th. Walther. "Entangled photon pair source". In *DPG Frühjahrstagung*, Mainz, Germany (2017).

S. Schürl, K. Roth, O. Nikiforov, Th. Walther. "An FPGA based detection system for QKD". In *DPG Frühjahrstagung*, Mainz, Germany (2017).

O. Nikiforov, S. Stutz, L. Drzewietzki, and S. Breuer, "Repetition rate linewidth reduction to 50 Hz of a passively mode-locked quantum dot laser subject to optical feedback by two long external cavities". In: *European Conference on Lasers and Electro-Optics and European Quantum Electronics Conference*, Munich, Germany, (2017).

O. Nikiforov, L. Jaurigue, L. Drzewietzki, K. Lüdge, S. Breuer. "Repetition rate linewidth reduction to 50 Hz of a passively mode-locked quantum dot laser subject to optical feedback by two long external cavities". In: *European Conference on Lasers and Electro-Optics and European Quantum Electronics Conference*, Munich, Germany, (2015).

Technical reports

P. M. Notz, O. Nikiforov, Th. Walther. "Software bundle for data post-processing in a quantum key distribution experiment." Technical Report TUD (2020).

O. Nikiforov, A. Sauer, J. Schickel, A. Weber, G. Alber, H. Mantel, Th. Walther. "Side-channel analysis of privacy amplification in postprocessing software for a quantum key distribution system." Technical Report TUD-CS-2018-0024 (2018).

Erklärungen laut Promotionsordnung

§ 8 Abs. 1 lit. c PromO

Ich versichere hiermit, dass die elektronische Version meiner Dissertation mit der schriftlichen Version übereinstimmt.

§ 8 Abs. 1 lit. d PromO

Ich versichere hiermit, dass zu einem vorherigen Zeitpunkt noch keine Promotion versucht wurde. In diesem Fall sind nähere Angaben über Zeitpunkt, Hochschule, Dissertationsthema und Ergebnis dieses Versuchs mitzuteilen.

§ 9 Abs. 1 PromO

Ich versichere hiermit, dass die vorliegende Dissertation selbstständig und nur unter Verwendung der angegebenen Quellen verfasst wurde.

§ 9 Abs. 2 PromO

Die Arbeit hat bisher noch nicht zu Prüfungszwecken gedient.

Darmstadt, 19.12.2022

O. Nikiforov